Produits polarisés de courbes elliptiques à multiplication complexe et applications aux courbes de petit genre

Fabien Narbonne

DOCTORAT BRETAGNE LOIRE / MATHSTIC

UNIVERSITÉ DE RENNES 1

THÈSE DE DOCTORAT DE

L'UNIVERSITÉ DE RENNES 1

ÉCOLE DOCTORALE N° 601
Mathématiques et Sciences et Technologies de l'Information et de la Communication
Spécialité : *Mathématiques et leurs Interactions*

Par
Fabien NARBONNE

Produits polarisés de courbes elliptiques à multiplication complexe et applications aux courbes de petit genre

Thèse présentée et soutenue à Rennes, le 08/09/2022
Unité de recherche : IRMAR, UMR CNRS 6625 Institut de Recherche Mathématique de Rennes (IRMAR)

Rapportrices et rapporteurs avant soutenance :

Valentijn KAREMAKER, Assistant Professor, Utrecht University
David KOHEL, Professeur, Aix-Marseille Université

Composition du Jury :

Présidente :	Elisa LORENZO GARCÍA, Maîtresse Assistante, Université de Neuchâtel
Examinatrices et examinateurs :	Jeroen SIJSLING, Professeur, Ulm Universität
Dir. de thèse :	Christophe RITZENTHALER, Professeur, Université de Rennes 1

Remerciements

Ces quatre années de thèse ont été pour moi à la fois une aventure merveilleuse et un parcours difficile. Ce qui est certain c'est que seul ça aurait été beaucoup moins merveilleux et beaucoup plus difficile. Il convient donc, comme le veut la tradition, d'accorder quelques mots aux très nombreuses personnes qui ont joué un rôle central ou marginal dans l'accomplissement de ce projet.

Tout d'abord, je souhaite remercier Christophe qui m'a fait découvrir ce domaine fabuleux qu'est la géométrie sur les corps finis. Lorsque j'étais en Master, il assurait un cours sur ce thème et je commençais déjà à venir l'embêter dans son bureau pour lui poser des questions relatives à de jolis problèmes que son cours me permettait de mieux comprendre. Outre ses qualités scientifiques, ce sont aussi ses qualités humaines qui m'ont permis de venir à bout de ce projet. Sa patience pour répondre à mes nombreuses interrogations, toujours avec bienveillance, m'a permis de m'épanouir sereinement dans ce domaine et de le faire mien. Son soutien pendant les périodes difficiles m'a aussi été salvateur, il m'a appris que parfois quand on ne trouve rien, il vaut mieux faire une pause, prendre du recul et s'y repencher plus tard à tête reposée. Enfin, Christophe a toujours eu comme priorité mon intégration dans la communauté scientifique et m'a toujours conseillé au mieux dans ce sens. Je réalise combien il est précieux de l'avoir eu comme encadrant et je suis fier qu'on ait parcouru ce petit bout de route ensemble.
Merci à Valentijn Karemaker et David Kohel d'avoir accepté de bien vouloir rapporter cette thèse. La qualité de leurs remarques a rendu possible cette forme finale de ma thèse qui dépasse mes espérances. Merci aussi à Elisa Lorenzo Garcìa et Jeroen Sijsling de me faire l'honneur de faire parti du jury.

Je tiens aussi à remercier Markus Kirschmer qui a répondu avec patience à mes nombreux mails et à mes questions relatives aux réseaux hermitiens. Merci pour toutes ces explications et ces codes qu'il m'a gentiment transmis. Je remercie également Francesc Fité et Xevi Guitart pour ces riches correspondances que nous avons entretenu autour des courbes qui ont pour corps de modules $\mathbb{Q}$. Leur aide, leur soutien et leur gentillesse

m'ont apporté le courage de mener à bien mon second projet qui est l'objet du Chapitre 4. Merci à Marco Streng pour ses conseils et recommandations qui, je l'espère, aboutiront prochainement à la généralisation du Chapitre 4 aux ordres non-maximaux. Enfin, merci à Harun Kir qui m'a partagé avec enthousiasme son travail sur les formes quadratiques qui fournit un angle d'attaque différent de celui proposé dans le Chapitre 4 et qui, heureusement, aboutit à des résultats similaires. Confronter nos résultats m'a permis de me sentir plus serein et je le remercie pour toute la gentillesse qu'il m'a témoigné dans nos échanges.

La vie sociale au sein du laboratoire a aussi joué un rôle important dans le bon déroulement de mon doctorat. Discuter des soucis que nous rencontrions tous et toutes avec les autres doctorant·es et nous soutenir était, je pense, nécessaire pour tout le monde. Je remercie particulièrement Alice, Victor, Loulou et Titouan pour les moments précieux que nous avons partagé. Je salue aussi l'organisation des séminaires doctorants Pampers qui nous permettaient de nous réunir toutes et tous autour d'un café, d'un gâteau et de jolies mathématiques toutes les semaines. Merci aussi aux (anciens) post-doc Julien et Giulio qui ont été des super copains en mon début de thèse mais qui ont dû partir à cause de leur carrière.

Le soutien amical qui m'a de loin été le plus indispensable au cours de cette thèse est bien entendu celui de la Mounette. Merci à tous·tes les colocs qui y sont passé·es ou qui y sont resté·es, merci à Idris, Tien Phong, Mimi, Coco, Tiphaine, Prune, Nura, Yannick et Shella. Je conserve des souvenirs tendres des moments que nous avons passé ensemble autour d'une bière, d'une tisane, d'un jeu ou de tout en même temps. Ce sont des moments précieux avec de belles personnes qui m'ont aidé à croire qu'un monde moins nul est possible. Un grand merci à Mimi qui est toujours un aussi chouette copain depuis la L3, avec qui j'ai toujours autant de plaisir à discuter de jolies maths et de politique. Merci à Prune dont la douce présence et la désinvolture légendaire m'apportent calme et sérénité et merci à Coco de toujours venir nous visiter malgré sa trahison de notre beau ciel gris pour le soleil toulousain. Enfin, merci à Shella qui m'accompagne depuis tant d'années et qui réchauffe toujours mon petit coeur d'amour tendre et d'authenticité. Merci pour ta présence et ton courage au cours des épreuves que nous avons dû traverser.

Merci aux copain·es pas ou plus de Rennes mais qui sont toujours présent·es quand nos routes peuvent se croiser. Merci à Loulou-le-normand pour ses tentatives pour m'apprendre quelques trucs en musique. Un grand merci à Kütle pour ces longues discussions énergiques sur tout et surtout rien et pour son altruisme à toute épreuve. Merci à Nathan

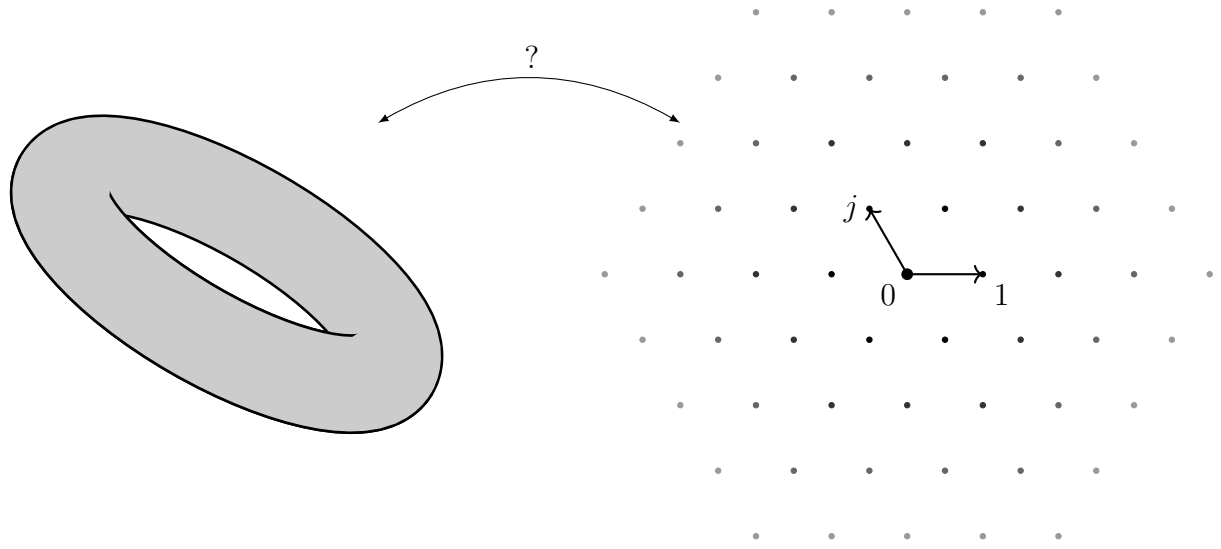
d'être toujours là depuis l'internat et pour ses Tours-Rennes à vélo pour me rendre visite. Merci aussi à Guigui, Momo et Natha d'égayer mes soirées tourangelles depuis le lycée.

Merci à mes parents de m'accueillir dans leur cocon familial où je peux me ressourcer et profiter de moments calmes dans leur douce campagne. Un grand merci à Aline, mon admirable frangine, d'être toujours un modèle de force et de courage pour son petit frère.

SOMMAIRE

Introduction

Dans cette thèse nous souhaitons étudier les liens fascinants et surprenants entre certaines variétés algébriques et les réseaux hermitiens. Les variétés algébriques sont souvent décrites comme le lieu d'annulation de polynômes à plusieurs variables tandis que les réseaux hermitiens sont des objets issus de l'algèbre linéaire. Bien que d'apparences très différentes ces deux mondes sont parfois liés entre eux par ce qu'on appelle des *équivalences de catégories*. Ces liens tissés entre différents domaines des mathématiques permettent d'énoncer des problèmes complexes dans l'un et de le résoudre plus facilement en les traduisant dans l'autre.



Courbe complexe de genre 1 Réseau hermitien

FIGURE 1 – Représentation imagée des objets manipulés dans cette thèse.

Les variétés algébriques qui nous intéressent ici sont les variétés abéliennes polarisées isogènes à un produit de courbes elliptiques à multiplication complexe par un ordre [1] R dans un corps quadratique imaginaire $K = \mathbb{Q}\left(\sqrt{-d}\right), d \in \mathbb{N}^*$. Avant d'expliquer plus en détail tous ces termes et pourquoi ces variétés en particulier nous intéressent il convient de faire un petit retour historique sur l'origine des équivalences de catégories dont il sera question.

Aperçu historique

En 1985, le mathématicien Jean-Pierre Serre a donné un cours à Harvard dans lequel il proposait l'étude du nombre maximum de points rationnels que peut avoir une courbe algébrique C de genre g sur un corps fini $\mathbb{F}_q$. On pose alors

$$N_q(g) = \max\{\#C(\mathbb{F}_q) \text{ avec } C \text{ de genre } g \text{ sur } \mathbb{F}_q\}.$$

Il s'intéressait d'une part à l'étude de $N_q(g)$ lorsque g est petit et d'autre part à son comportement asymptotique lorsque g est grand par rapport à q. Ces deux questions en ont soulevé d'autres et ont inspiré les mathématicien·nes jusqu'à aujourd'hui donnant naissance à un domaine des mathématiques à part entière [2]. Pendant longtemps les seules traces de ce cours étaient les notes manuscrites d'un des participants au cours, Fernando Gouvêa. Heureusement, ces notes ont récemment été éditées et mises à jour grâce au concours de nombreuses personnes, voir [Ser20].

Intéressons nous à la première question ; celle du nombre maximum de points que peut avoir une courbe de petit genre ($g = 1, 2$ ou 3) sur un corps fini $\mathbb{F}_q$. Une façon détournée pour étudier les courbes de petit genre est de considérer leur *jacobienne*. À une courbe algébrique C de genre g on peut toujours associer une variété abélienne $\mathrm{Jac}(C)$ de dimension g, i.e. une variété algébrique projective munie d'une structure de groupe, ainsi qu'une *polarisation principale* a_C sur $\mathrm{Jac}(C)$, un objet relié à un fibré ample sur $\mathrm{Jac}(C)$ dont la définition précise n'a pas encore d'importance. Par exemple toutes les courbes algébriques

1. Nous appellerons de tels ordres des *ordres quadratiques imaginaires* ou des ordres quadratiques au lieu d'ordres dans un corps quadratique imaginaire. Il ne sera question à aucun moment dans cette thèse de corps quadratique réel, i.e. $K = \mathbb{Q}\left(\sqrt{d}\right)$ avec un entier sans facteur carré $d > 0$.

2. On peut notamment citer le site `https://www.manypoints.org/` qui répertorie l'état des connaissances actuelles sur $N_q(g)$ pour des petits q et g.

de genre 1 ayant un point rationnel (dites *courbes elliptiques*) peuvent être munie d'une structure de groupe qui fait d'elles leur propre jacobienne. En revanche, les courbes de genre supérieur ne peuvent jamais être munie d'une structure de groupe satisfaisante. La variété jacobienne est en cela un outil très puissant qu'on peut associer aux courbes pour venir pallier le manque de structure algébrique de ces dernières. L'avantage du petit genre est que toutes les variétés abéliennes munies d'une *polarisation principale indécomposable* de dimension 2 (resp. 3) sont (resp. *géométriquement*) la jacobienne d'une courbe algébrique. Obtenir des informations sur l'existence de telle ou telle variété abélienne permet donc de déduire des résultats d'existence sur les courbes elles-mêmes sans en donner des équations explicites.

Un premier résultat est la borne dite de Hasse-Weil-Serre ([Ser20, Theorem 2.1.1.])

$$N_q(g) \leq q + 1 + gm$$

avec $m = \left\lfloor 2\sqrt{q} \right\rfloor$ où $\lfloor x \rfloor$ désigne le plus petit entier inférieur ou égal au réel x. Cette borne est intéressante uniquement pour le petit genre car on sait qu'asymptotiquement elle est assez mauvaise. En effet, dans [VDd83] les auteurs montrent que $\limsup_g \frac{N_q(g)}{g} \leq \sqrt{q} - 1$ (si la borne était bonne on obtiendrait une majoration par $2\sqrt{q}$). Une courbe C de genre g sur $\mathbb{F}_q$ atteignant cette borne supérieure, i.e. $\#C(\mathbb{F}_q) = q+1+gm$, est dite *optimale*. Par exemple, pour $q = 11$ et $g = 2$, la borne nous indique que $N_{11}(2) \leq 11 + 1 + 2 \times 6 = 24$, une courbe de genre 2 sur $\mathbb{F}_{11}$ aura toujours moins de 24 points sur $\mathbb{F}_{11}$. On peut vérifier que la courbe [3] définie par $C\colon y^2 = 5x^6 - 3x^4 - 3x^2 + 5$ sur $\mathbb{F}_{11}$ (illustrée Figure 2) est de genre 2 et a bien 24 points rationnels (22 points affines et 2 points à l'infini [4]). De telles courbes n'existent pas toujours mais si elles existent la géométrie de leur jacobienne est extrêmement contrainte. En effet, Serre avait remarqué qu'une courbe optimale a sa jacobienne *isogène* à un produit de courbes elliptiques elles-mêmes optimales. C'est-à-dire qu'il existe un morphisme surjectif $\mathrm{Jac}(C) \to E^g$ où g est le genre de C. Il a aussi utilisé des foncteurs, $L \mapsto L \otimes_R E$ et $L \mapsto \mathrm{Hom}_R(L, E)$, définis de façon très générale pour E un objet d'une catégorie abélienne et $R \to \mathrm{End}(E)$ un morphisme d'anneaux, qui transforment les R-modules finiment présentés, en objets de cette catégorie (voir [Ser20, Section 3.8] pour plus de détails sur la construction de ces foncteurs).

3. Pour trouver C, il m'a suffit de boucler naïvement sur l'ensemble des courbes hyperelliptiques de genre 2 sur $\mathbb{F}_{11}$ et de calculer le nombre de points pour chacune d'elles.

4. L'équation donnée définit une courbe avec un point singulier à l'infini. Lorsqu'on écrira « la courbe $C\colon y^2 = f(x)$ pour $\deg f \geq 4$ » il s'agira de la courbe désingularisée (en éclatant le point à l'infini).

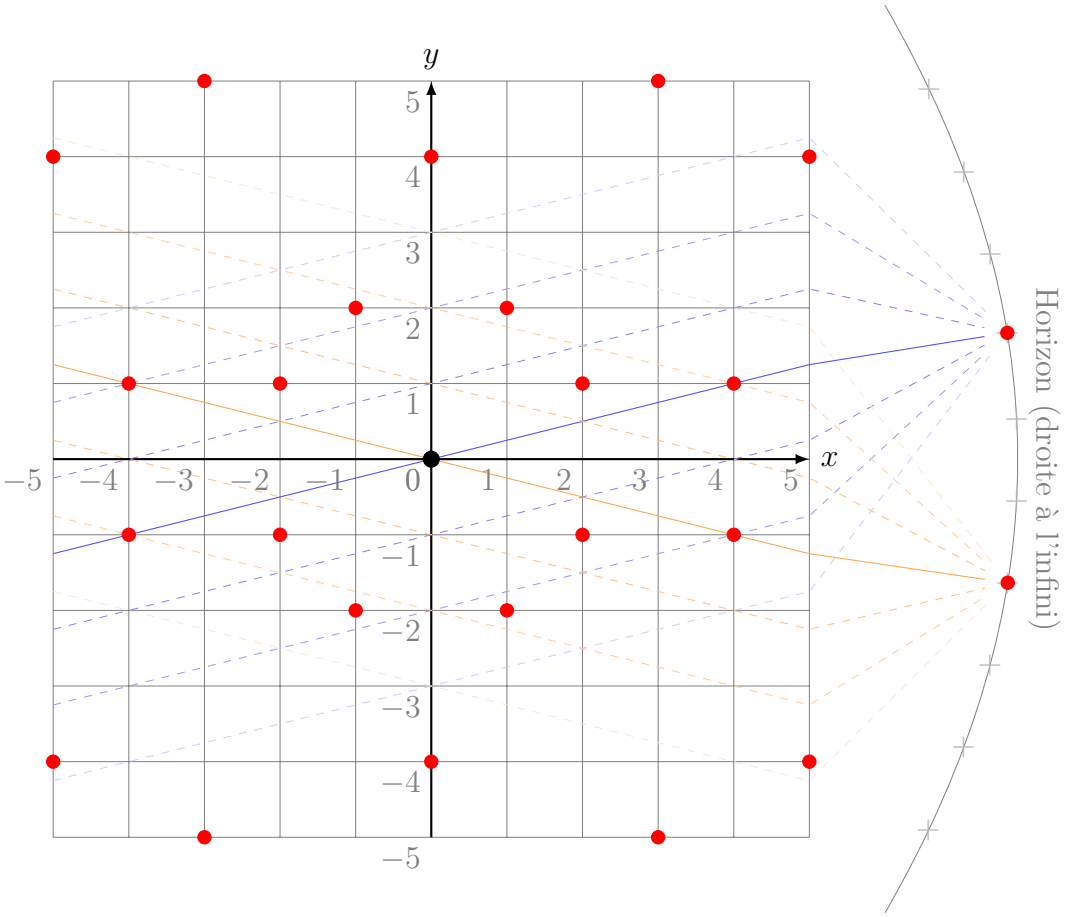


FIGURE 2 – Les 24 points rationnels de la courbe optimale définie par $C\colon y^2 = 5x^6 - 3x^4 - 3x^2 + 5$ sur $\mathbb{F}_{11}$.

Dans le cas où la catégorie abélienne considérée est la catégorie des variétés abéliennes sur un corps k et $R = \mathrm{End}(E)$ avec E une courbe elliptique il montre qu'en se restreignant aux R-modules finiment présentés L qui sont sans torsion on obtient des variétés abéliennes isogènes à E^g. Il remarque aussi qu'en munissant le réseau L d'une forme hermitienne définie positive H la variété abélienne obtenue peut être munie d'une polarisation ayant des propriétés similaires à celles du réseau hermitien (L, H). Par exemple, la dimension de la variété obtenue à partir de d'un réseau hermitien (L, H) est le *rang* de L, i.e. $\mathrm{rk}\, L = \dim_K(KL)$ avec $K = \mathrm{Frac}\, R$. De plus, la variété polarisée (A, a) est indécomposable si, et seulement si, le réseau hermitien est aussi indécomposable (i.e., ils ne sont pas isomorphes au produit de deux sous-variétés polarisées ou sous-réseaux hermitiens).

Ou encore, le degré de la polarisation a correspond au cardinal du quotient $[L^* \colon \phi_H(L)]$ où L^* désigne l'ensemble des formes antilinéaires $L \to R$ sur L et ϕ_H le morphisme

$$\begin{aligned} \phi_H \colon \quad L &\longrightarrow L^* \\ y &\longmapsto (x \mapsto H(x,y)). \end{aligned}$$

Le cas $\deg a = 1$ (a est une polarisation *principale*) correspond alors aux réseaux dits *unimodulaires* (les réseaux (L,H) tels que ϕ_H est un isomorphisme). Il montre alors que le foncteur $L \mapsto L \otimes_R E$ est une équivalence de catégories sous les trois conditions suivantes :

— k est un corps fini $\mathbb{F}_q$,

— E est une courbe elliptique ordinaire,

— R est un anneau d'entiers engendré par le morphisme de Frobenius

$$\begin{aligned} \mathrm{Frob} \colon \quad E &\longrightarrow E \\ P &\longmapsto P^q. \end{aligned}$$

Grâce à des résultats d'existence de tels réseaux hermitiens il en a déduit l'existence de certaines courbes optimales et réciproquement il a pu constater que certaines courbes optimales n'existent pas si les réseaux correspondants n'existent pas [Ser20, Theorem 3.9.6.]. Je me permets d'illustrer cette équivalence par deux exemples. Reprenons le cas $g = 2$ et $k = \mathbb{F}_{11}$ à la lumière de ce résultat mais oublions la courbe de la Figure 2. L'anneau engendré par le morphisme de Frobenius des courbes elliptiques optimales correspondantes est l'anneau

$$R = \mathbb{Z}[\mathrm{Frob}] \simeq \mathbb{Z}[X] / \left\langle X^2 - mX + q \right\rangle = \mathbb{Z}[X] / \left\langle X^2 - 6X + 11 \right\rangle \simeq \mathbb{Z}\left[\sqrt{-2}\right],$$

de discriminant -8. Il s'agit de l'anneau des entiers du corps $\mathbb{Q}\left(\sqrt{-2}\right)$. Il existe un unique réseau hermitien unimodulaire indécomposable de rang 2 sur cet anneau. Ce réseau hermitien est le R-module libre R^2 muni de la forme hermitienne H définie par

$$H(x,y) = {}^t\overline{x} \begin{pmatrix} 2 & 1+\sqrt{-2} \\ 1-\sqrt{-2} & 2 \end{pmatrix} y$$

qui est de déterminant 1, ce qui confirme que le réseau (R^2, H) est unimodulaire. La matrice définissant H est la matrice $G(e_1, e_2) = (H(e_i, e_j))$, où $b = (e_1, e_2)$ est la base canonique de R^2. On l'appelle matrice de Gram de H dans la base b, elle définie totalement

H. Cette matrice est obtenue grâce à l'algorithme[5] développé dans [Sch98]. Sous réserve qu'on puisse trouver une courbe elliptique E telle que $\mathrm{End}(E) \simeq R$ (ce que l'on peut toujours faire, cela n'est pas une vraie restriction), toutes les hypothèses de l'équivalence énoncée par Serre sont vérifiées. Il existe donc des courbes optimales de genre 2 sur $\mathbb{F}_{11}$, ce que confirme bien entendu la courbe de la Figure 2. Si on considère maintenant le cas $g = 2$ et $k = \mathbb{F}_{13}$, la borne de Hasse-Weil-Serre indique que $N_{13}(2) \leq 28$. L'anneau engendré par le morphisme de Frobenius d'une courbe optimale est $R = \mathbb{Z}[X]/\langle X^2 - mX + q\rangle \simeq \mathbb{Z}[j]$ avec $j = \frac{1+\sqrt{-3}}{2}$. Il s'agit aussi d'un anneau d'entiers donc les hypothèses de l'équivalence énoncée par Serre sont vérifiées. En revanche, il était déjà bien connu en 1985 qu'il n'existe pas de réseau hermitien unimodulaire indécomposable sur R (voir [HN65] ou [Fei78] ou encore [Hof91, Theorem 8.1] ou [Sch98, Table 1] pour des références plus modernes). Il n'existe donc pas de courbe optimale de genre 2 sur $\mathbb{F}_{13}$.

Ces deux foncteurs ont été largement étudiés par la suite, par exemple le foncteur $\mathrm{Hom}_R(\_, E)$ est étudié dans [JKP+18] ou, plus récemment, dans [IKY22] et le foncteur $\_ \otimes_R E$ dans [AK17]. En particulier, dans [JKP+18], les auteurs montrent cette équivalence lorsque l'anneau d'endomorphismes R est engendré par le morphisme de Frobenius sans forcément qu'il soit un anneau d'entiers. Ils montrent aussi un résultat similaire lorsque E est *supersingulière*[6] et $k = \mathbb{F}_p$ ou $\mathbb{F}_{p^2}$ et ils donnent une condition nécessaire et suffisante pour que $\mathrm{Hom}_R(\_, E)$ soit une équivalence de catégories lorsque k est un corps quelconque. Ils énoncent aussi des résultats semblables en remplaçant la courbe elliptique E par une variété abélienne B de dimension supérieure. Malheureusement, dans [JKP+18] les auteurs ne considèrent que des variétés abéliennes sans polarisation et que des réseaux sans formes hermitiennes. C'est une des contributions que nous avons apportées dans [KNRR21] où nous avons montré que l'équivalence de catégories tient toujours lorsque $\mathrm{End}(E) = \mathbb{Z}[\mathrm{Frob}]$ en munissant d'une part les réseaux d'une forme hermitienne et d'autre part les variétés abéliennes de polarisations. Plus récemment, l'équivalence a été élargie en prenant en compte les polarisations aussi dans les cas E supersingulière et $k = \mathbb{F}_p$ ou $\mathbb{F}_{p^2}$ (voir [IKY22, Corollary 4.6]).

5. Une base de données de tels réseaux calculés à l'aide de cet algorithme est disponible sur le site de Rainer Schulze-Pillot `https://www.math.uni-sb.de/ag/schulze/Hermitian-lattices/`.

6. Il n'y a que trois types d'anneau d'endomorphismes pour une courbe elliptique : $\mathbb{Z}, \mathbb{Z}[X]/\left(X^2 + aX + b\right)$ avec $a^2 - 4b < 0$, i.e. un ordre quadratique imaginaire, ou alors un ordre dans une algèbre de quaternion. Dans le second cas on dit que la courbe est à *multiplication complexe* abrévié CM. Dans le dernier cas, on dit alors que la courbe est *supersingulière* (voir [Sil09, Theorem III.9.3]). En caractéristique 0 seuls les deux premiers cas peuvent apparaître tandis que sur un corps fini seuls les deux derniers sont possibles.

En conclusion de ce passage historique, Serre s'est servi de constructions de variétés abéliennes (principalement polarisées indécomposables) isogènes à un produit de courbes elliptiques E^g à partir de réseaux hermitiens pour en déduire l'existence de certaines courbes lorsque cette courbe E a de bonnes propriétés. En choisissant cette courbe E comme étant optimale on obtient l'existence ou non de courbes optimales de genre g. L'utilité de ces foncteurs ne s'arrête pas là [7]. En choisissant d'autres courbes elliptiques la construction est toujours valide et on peut obtenir l'existence de courbes de genre g avec des propriétés différentes (avec un nombre minimal de points, ou de défaut n, i.e. optimale à n points près).

Nous pouvons désormais présenter les deux projets qui ont motivé mes recherches durant ces quatre années. Le premier, [KNRR21], est dans la continuité de ce qui vient d'être évoqué. Nous y étudions les variétés abéliennes polarisées sur un corps fini isogènes à un produit de courbes elliptiques (à CM) par l'intermédiaire du foncteur $\mathrm{Hom}_R(\_, E)$, étudié d'abord par Serre mais repris à la lumière de l'article [JKP+18]. Le second, [Nar22], en revanche change de cadre. Nous étudions toujours des variétés abéliennes polarisées isomorphes à un produit de courbes elliptiques (à CM) mais sur $\mathbb{C}$ (ou $\overline{\mathbb{Q}}$), par l'intermédiaire d'un autre foncteur, noté $\mathbf{F}_h$, qui m'a semblé plus facile à manipuler dans ce cadre que $\mathrm{Hom}_R(\_, E)$, et pour des courbes elliptiques à CM par un ordre qui est maximal. Cette restriction nous impose de ne travailler que sur certaines classes d'isomorphisme de produits de courbes elliptiques au lieu de travailler sur la classe d'isogénie toute entière. Pour chacun des deux projets j'ai souhaité résumer schématiquement ce que nous y faisions, dans la Figure 6 pour le premier projet et dans la Figure 7 pour le second.

Premier projet : équivalence sur les corps finis

Lorsqu'on a théoriquement une équivalence de catégories entre les variétés abéliennes (principalement) polarisées et les réseaux hermitiens (unimodulaires) se pose alors naturellement la question de leur énumération. Comment énumérer de tels objets et, si nous arrivons à classifier les réseaux qui nous intéressent, peut-on reconstruire les variétés abéliennes en question (et les courbes correspondantes lorsque ces variétés sont des jacobiennes) ? Dans [KNRR21] nous proposons un tel algorithme et donnons des exemples d'existence (ou non) de variétés abéliennes et de courbes (ainsi que leur reconstruction

7. Voir aussi [IKY22] pour l'utilisation du foncteur $\mathrm{Hom}_R(\_, E)$ pour la résolution de problèmes de Gauss.

grâce aux *thêta constantes*) pour les genre $g = 2, 3$ et même 4. Dans cette section, j'illustre les méthodes que nous avons développées en essayant de fournir des exemples qui me semblent pertinents et, si possible, différents de ceux proposés dans [KNRR21].

D'autres foncteurs plus généraux existent. Par exemple, dans [Del69] Pierre Deligne montre une équivalence entre les variétés abéliennes ordinaires sur $\mathbb{F}_q$ et certains $\mathbb{Z}$-modules libres de rang fini. Dans [CS15] les auteurs étendent la construction de Deligne aux variétés abéliennes dont le polynôme caractéristique du Frobenius n'a pas de racine réelle. Plus récemment, dans [CS21], ces mêmes auteurs ont généralisé l'équivalence à toutes les variétés abéliennes sur $\mathbb{F}_q$ sans restriction. Dans [Mar20a], l'auteur propose des algorithmes effectifs d'énumération de ces variétés grâce au foncteur de Deligne.

La classification des réseaux hermitiens unimodulaires sur un ordre maximal R de rang $\dim(KL) = g$ donné dans un corps quadratique imaginaire $K = \mathrm{Frac}(R)$ est un cas particulier d'une théorie plus large qui classifie ces objets sur un ordre maximal dans un corps de nombres (voir [Sch98] ou [Kir19]). Nous avons commencé par rappeler cette théorie, en particulier la *méthode du voisin*, dans [KNRR21, Section 2.2] puis nous nous sommes intéressés aux réseaux qui ne sont pas sur un ordre maximal. Classifier de tels réseaux ne pose pas de grandes difficultés lorsqu'ils sont *projectifs* (voir la discussion faite dans la Section 1.2.4). Cependant, la classification des réseaux non projectifs a demandé des efforts supplémentaires que nous n'avons pu relever que grâce aux spécificités des ordres dans les corps quadratiques (voir [KNRR21, Algorithm 2]). Cette classification mène malheureusement à des algorithmes bien moins efficaces que ceux qui énumèrent les réseaux projectifs.

Revenons aux *thêta constantes* que je me suis gardé de définir jusqu'à maintenant. La théorie des variétés abéliennes sur $\mathbb{C}$ est bien connue (j'en parle plus en détails dans la section suivante de l'introduction puis dans la Section 2.2). À l'aide d'un fibré ample $\mathscr{L}$ sur une variété abélienne A, on peut définir des fonctions $\psi_{\mathscr{L}^r}$ qui pour $r \geq 3$ définissent un plongement projectif de la variété A, il s'agit du Théorème de Lefschetz [Deb05, Théorème VI.3.5]. Ces plongements peuvent être rendus explicites par le choix adapté d'une base de l'espace des sections du fibré $\mathscr{L}$. Les *fonctions thêta* fournissent de telles bases et leurs valeurs en 0, appelées *thêta constantes*, déterminent totalement la variété A et le fibré [8] $\mathscr{L}$ (voir la section 2.2.3 où je rappelle dans les grandes lignes la théorie des fonctions thêta sur $\mathbb{C}$ en m'appuyant sur [Deb05]). Dans les années 60, David Mumford a publié une série

8. La donnée d'un fibré en droite est essentiellement la même chose que la donnée d'une polarisation donc étant donnée une variété polarisée (A, a), la connaissance des thêta constantes adaptées à a détermine la variété polarisée.

d'articles ([Mum66, Mum67a, Mum67b]) dans lesquels il généralise notamment la théorie des fonctions thêta aux variétés abéliennes sur n'importe quel corps de caractéristique différente de 2. Il définit les *thêta constantes algébriques* qui, à l'instar de leurs homonymes complexes, fournissent un plongement projectif et caractérisent la variété abélienne et le fibré ample associé.

Il reste à savoir comment calculer explicitement ces thêta constantes étant donné un réseau hermitien unimodulaire indécomposable (L, H) correspondant à une variété abélienne (A, a). Les *formules de Thomae* permettent en particulier de calculer les thêta constantes d'une courbe elliptique E puis d'en déduire celles de la variété polarisée $(E^g, \ell\lambda_0)$ où ℓ est un entier positif et λ_0 la polarisation produit. Ensuite, étant donnée une isogénie polarisée $f\colon (A_0, \mathscr{L}_0) \to (A, \mathscr{L})$, c'est-à-dire une isogénie qui respecte les polarisations associées aux fibrés $\mathscr{L}_0$ et $\mathscr{L}$ (i.e., $f^*\mathscr{L} = \mathscr{L}_0$), telle qu'on connaît les thêta constantes de $(A_0, \mathscr{L}_0)$ alors on peut calculer les thêta constantes de $(A, \mathscr{L})$ grâce aux *formules d'isogénie* développées dans [CR15]. Mettant bout à bout les formules d'isogénie et de Thomae, on sait que si on arrive à expliciter une isogénie polarisée

$$f\colon (E^g, \ell\lambda_0) \to (A, a),$$

appelée une $(\ell, \dots, \ell)$-isogénie, on sera en mesure de déterminer les thêta constantes de (A, a). Maintenant, prenons le problème à l'envers et supposons que nous ayons une telle isogénie polarisée. Son image par le foncteur $\mathrm{Hom}_R(\_, E)$ donne une isométrie [9]

$$\mathrm{Hom}_R(f, E)\colon (L, H) \to \left(R^g, \frac{1}{\ell}H_0\right)$$

où H_0 est la forme hermitienne canonique sur K^g. Remarquons que si on arrive à exhiber une famille de g vecteurs $u_1, \dots, u_g$ de L tous de norme $H(u_i, u_i) = \ell$ alors l'inclusion $N = \bigoplus_i Ru_i \to L$ fournit une isométrie $(N, H) \simeq (R^g, \ell H_0) \hookrightarrow (L, H)$. En prenant son *dual* on obtient l'isométrie désirée $(L^\#, H) = (L, H) \to (R^g, \ell H_0)^\# = \left(R^g, \frac{1}{\ell}H_0\right)$ où le dual d'un réseau hermitien (M, H) est défini par $M^\# = \{v \in KM, H(v, M) \subseteq R\}$.

Ceci nous amène naturellement à un autre problème qui nous a intéressé, qui est celui de l'existence de familles orthogonales de g vecteurs $u_1, \dots, u_g$ de même norme ℓ d'un réseau hermitien unimodulaire (L, H). Étonnamment, l'existence de familles orthogonales de même norme ne dépend que de l'espace hermitien ambiant (V, H) avec $V = KL$, et non du réseau L que l'on regarde dedans. En dimension g impaire, on peut toujours

9. Le foncteur est *contravariant* ; il inverse le sens des flèches.

trouver de telles familles mais en dimension paire ça n'est plus le cas. L'existence de telles familles pour g pair est équivalente à $\det(V,H) = 1 \in \mathbb{Q}^*/N(K^*)$ où $\det(V,H)$ désigne le déterminant de la matrice de Gram dans n'importe quelle base [10] de V et $N(x) = x\overline{x}$ est l'application norme de K. Pour des raisons théoriques nous avons besoin que l'entier ℓ soit impair, ce qui ne pose pas de problème lorsque g est impair et R de conducteur impair (en particulier cela fonctionne lorsque R est maximal). Mais encore une fois, pour certains réseaux cette condition n'est pas satisfaisable [11] pour g pair (voir [KNRR21, Section 2.3] pour plus de détails).

Nous résumons dans la Figure 3 la stratégie globale de calcul des thêta constantes d'une variété abélienne principalement polarisée sur $\mathbb{F}_q$ isogène à E^g à partir de la donnée du réseau hermitien unimodulaire $(L,H) = \mathrm{Hom}_R((A,a),E)$, expliquée dans les deux paragraphes ci-dessus.

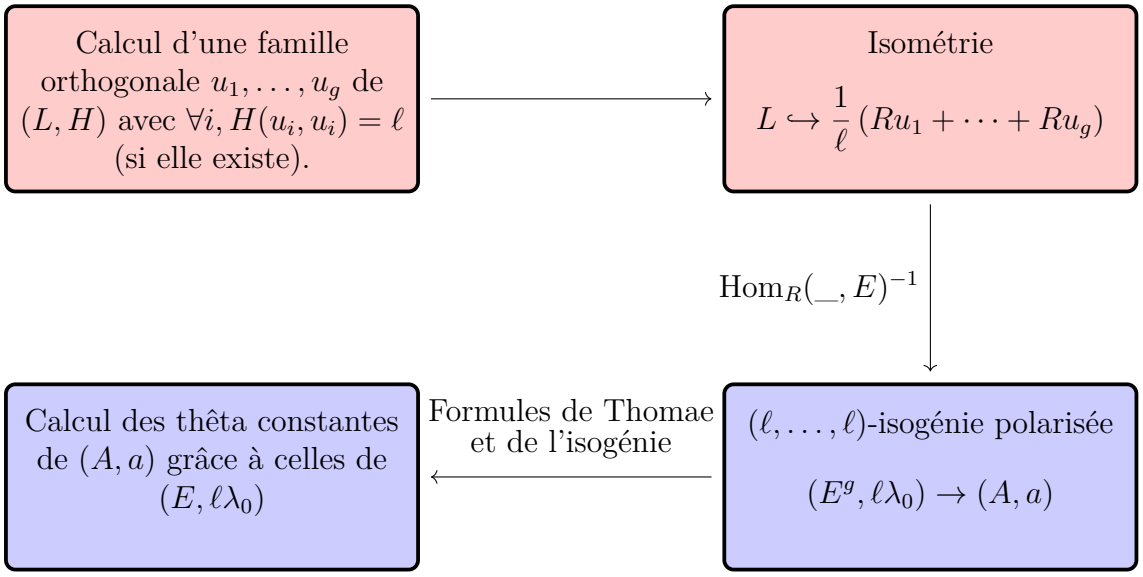


FIGURE 3 – Calcul des thêta constantes d'une variété abélienne (A,a) principalement polarisée à l'aide du réseau $(L,H) = \mathrm{Hom}_R((A,a),E)$.

Le calcul des thêta constantes est riche en applications. Nous allons en présenter quelques-unes. Pour cela revenons aux petits genres $g = 2, 3$ et 4.

10. Cette quantité n'est bien définie qu'à la norme d'un élément de K^* près mais cela n'est pas un problème car on regarde sa classe dans $\mathbb{Q}^*/N(K^*)$.

11. Pour certains réseaux hermitiens unimodulaires, dits *pairs*, la norme de tous leurs vecteurs est paire. Ceci ne peut arriver que pour des réseaux de rang pair.

Nous l'avons déjà dit, en genre 2 toute variété abélienne principalement polarisée indécomposable est la jacobienne d'une courbe algébrique. Les thêta constantes algébriques calculées sur une telle variété abélienne nous permettent de reconstruire la courbe associée en lui donnant des équations explicites pour $g = 2$ et 3. Pour $g = 2$ il s'agit d'appliquer la méthode décrite dans [CR15]. Avant de nous aventurer à expliquer le cas du genre 3, arrêtons-nous sur un nouvel exemple. Prenons $g = 2$ et $k = \mathbb{F}_{53}$. La borne de Hasse-Weil-Serre indique que $N_{53}(2) \leq 82$. L'anneau d'endomorphismes engendré par le morphisme de Frobenius d'une courbe elliptique optimale sur $\mathbb{F}_{53}$ est isomorphe à $R = \mathbb{Z}[X]/\langle X^2 - 14X + 53\rangle \simeq \mathbb{Z}[2i]$, de discriminant -16. Il existe une unique classe d'isométrie de réseaux hermitiens unimodulaires indécomposables sur cet anneau. Il s'agit du réseau libre R^2 muni de la forme hermitienne définie par la matrice de Gram

$$\begin{pmatrix} 2 & -1+2i \\ -1-2i & 3 \end{pmatrix} \tag{1}$$

dans la base canonique de R^2. L'anneau R n'est pas intégralement clos et donc l'équivalence énoncée par Serre ne permet pas d'affirmer l'existence d'une courbe optimale à partir d'un tel objet. En revanche, l'équivalence démontrée dans [KNRR21] le permet. Par ailleurs, on peut trouver deux vecteurs orthogonaux u et v dans R^2 de norme 3 pour la forme hermitienne (1) qui permettent de calculer les thêta constantes algébriques grâce à la méthode illustrée dans la Figure 3. En utilisant la méthode évoquée plus haut, on peut reconstruire la courbe d'équation $y^2 = -3x^6 + 31x^4 + 31x^2 - 3$, illustrée dans la Figure 4 (elle n'a que des points affines avec ce modèle).

À l'instar de la dimension 2, les variétés abéliennes principalement polarisées indécomposables (A, a) de dimension 3 sur un corps k sont aussi toutes des jacobiennes de courbes. Mais elles le sont seulement *géométriquement*. Ceci signifie que $(A, a)_{\overline{k}}$, notre variété regardée sur $\overline{k}$, est la jacobienne d'une courbe C_0 sur $\overline{k}$. La courbe C_0 est toujours isomorphe à une courbe C_1 sur k, on dit que C_1 est un *modèle* de C_0 sur k. Cependant, il se peut que $\mathrm{Jac}(C_1)$ ne soit pas isomorphe à (A, a) sur k auquel cas (A, a) n'est pas la jacobienne d'une courbe sur k. On appelle cette obstruction à être *rationnellement* une jacobienne, l'*obstruction de Serre*. À titre d'exemple, dans le cas de la recherche des courbes optimales sur $\mathbb{F}_q$, si (A, a) est la jacobienne de C_0 sur $\bar{\mathbb{F}}_q$ mais que $\mathrm{Jac}\, C_1$ n'est pas isomorphe à (A, a) alors C_1 a $q+1-3m$ points rationnels au lieu de $q+1+3m$. Autrement dit, C_1 atteint la borne inférieure de points que peut avoir une courbe de genre 3 sur $\mathbb{F}_q$. Heureusement, on peut calculer algébriquement l'obstruction de Serre à l'aide des thêta

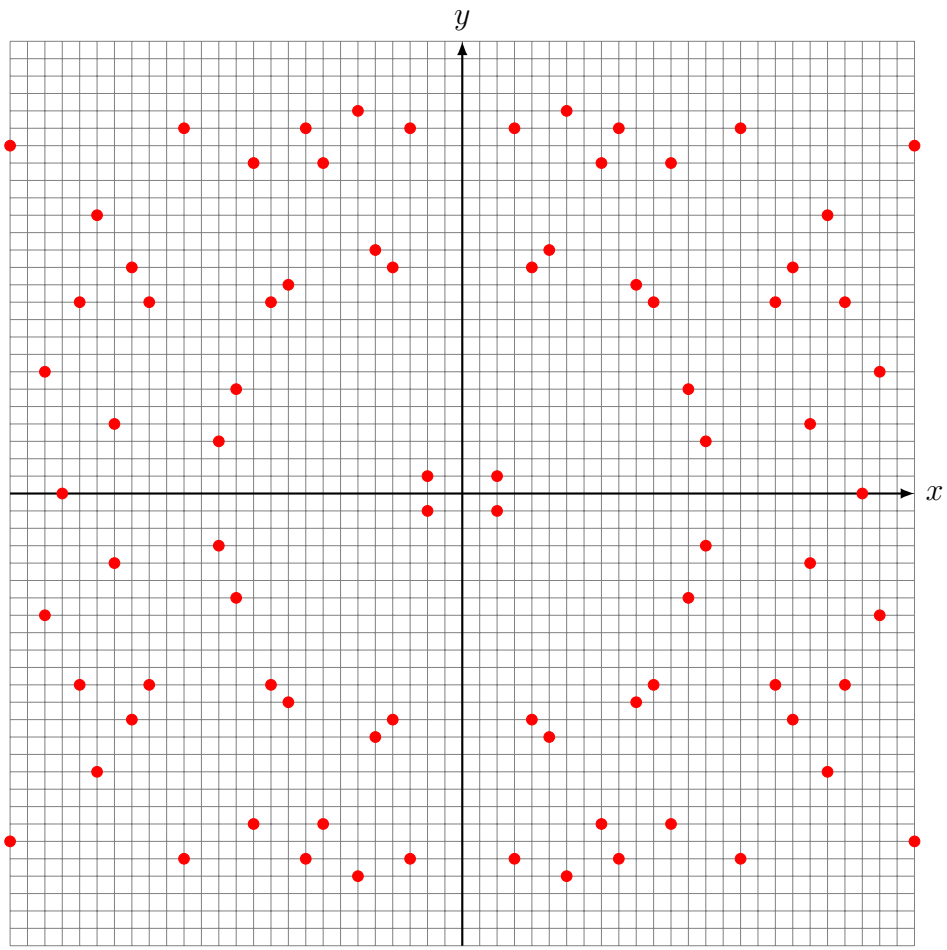


FIGURE 4 – Les 82 points rationnels de la courbe optimale de genre 2 définie par $C\colon y^2 = -3x^6 + 31x^4 + 31x^2 - 3$ sur $\mathbb{F}_{53}$.

constantes.

Dans [Rit10] l'auteur montre qu'une variété abélienne principalement polarisée indécomposable (A, a) de dimension 3 sur un corps k est la jacobienne d'une courbe C sur k si, et seulement si, une certaine forme modulaire, χ_{18}, le produit de 36 thêta constantes dites *paires*, est un carré dans k. Il prouve aussi que χ_{18} est nulle en les thêta constantes si, et seulement si, la courbe C correspondante est *hyperelliptique*[12] ([Rit10, Proposition 2.4]), i.e. il existe un polynôme $f \in k[x]$ tel que C ait un modèle de la forme $y^2 = f(x)$.

Ceci nous permet donc de tester si une variété est la jacobienne d'une courbe C. Si c'est

12. Les courbes de genre 2, comme celles illustrées dans les Figure 2 et 4, ont toujours un modèle hyperelliptique contrairement aux courbes de genre 3 qui sont génériquement des quartiques planes lisses (voir la courbe (2)).

le cas on peut alors la reconstruire en distinguant le cas C hyperelliptique ou non. Si C est hyperelliptique on peut utiliser [Wen01] pour construire un modèle C_0 de C sur $\bar{\mathbb{F}}_q$, puis on peut en déduire un modèle C_1 de C_0 sur $\mathbb{F}_q$ en calculant les invariants de Shioda (voir [LR12]). Si C est non-hyperelliptique alors les formules de Weber ([Web76] ou [Fio16]) fournissent un premier modèle de C_0 sur $\mathbb{F}_{q^s}$ qu'on peut descendre en une courbe C_1 sur $\mathbb{F}_q$. Cependant, il se peut que C_1, la courbe obtenue sur $\mathbb{F}_q$ dans les deux cas, ne soit pas isomorphe à C sur $\mathbb{F}_q$ auquel cas on énumère toutes les *tordues* de C_1 sur $\mathbb{F}_q$ grâce à [LR12] (pour le cas hyperelliptique) ou [LRRS14] (pour le cas non-hyperelliptique).

Donnons maintenant un exemple d'application à l'existence de certaines courbes de genre 3. Si $q = 103$, la borne de Hasse-Weil-Serre donne $N_{103}(3) \leq 1 + 103 + 3\left\lfloor 2\sqrt{103}\right\rfloor = 164$. L'anneau d'endomorphismes engendré par le morphisme de Frobenius d'une courbe elliptique optimale est

$$R \simeq \mathbb{Z}[X]/\left\langle X^2 - 20X + 103\right\rangle \simeq \mathbb{Z}[2j] = \mathbb{Z}\left[\sqrt{-3}\right].$$

Il s'agit d'un anneau de discriminant -12, qui n'est pas un anneau d'entiers. En dimension 3, il existe deux réseaux hermitiens unimodulaires indécomposables qui sont tous deux libres (isomorphes à R^3) et qui ont pour matrices de Gram respectives

$$\begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1+\sqrt{-3} \\ 1 & 1-\sqrt{-3} & 3 \end{pmatrix} \text{ et } \begin{pmatrix} 2 & 1 & 2 \\ 1 & 2 & 2+\sqrt{-3} \\ 2 & 2-\sqrt{-3} & 5 \end{pmatrix}.$$

Pour chacun des réseaux hermitiens on peut calculer une famille orthogonale de vecteurs de même norme $\ell = 3$. Ceci nous permet de calculer les thêta constantes associées aux variétés correspondantes. Chacune d'elles est une variété abélienne principalement polarisée indécomposable de dimension 3 sur $\mathbb{F}_{103}$ mais il peut y avoir une obstruction à ce qu'elles soient la jacobienne d'une courbe sur $\mathbb{F}_{103}$. Pour chacune d'elles on calcule la valeur de χ_{18} en les thêta constantes obtenues et on trouve pour la première $\chi_{18} = 88$ qui n'est pas un carré modulo 103 et $\chi_{18} = 4 = 2^2$ qui est un carré. On en déduit que le premier réseau hermitien correspond à une variété polarisée sur $\mathbb{F}_{103}$ qui n'est **pas** la jacobienne d'une courbe sur $\mathbb{F}_{103}$. En revanche, la seconde variété n'a pas d'obstruction ; il s'agit bien d'une jacobienne et puisque $\chi_{18} \neq 0$ la courbe associée est non-hyperelliptique. On peut la reconstruire [13] et on trouve la quartique lisse définie par

13. J'ai choisi un autre modèle avec une équation plus compacte et plus de symétries que le modèle

$$C\colon 81x^4 + 12x^3 + 49x^2y^2 + 85x^2 + xy^2 + x + 96y^4 + 22y^2 + 19 = 0 \qquad (2)$$

et représentée Figure 5 (il manque les deux points à l'infini $[26\colon 1\colon 0]$ et $[-26\colon 1\colon 0]$). On peut alors en déduire que, bien qu'il existe deux classes d'isomorphisme de variétés abéliennes principalement polarisées indécomposables de dimension 3 sur $\mathbb{F}_{103}$ isogènes à E^3, il n'existe qu'une seule classe d'isomorphisme de courbes optimales et non pas deux.

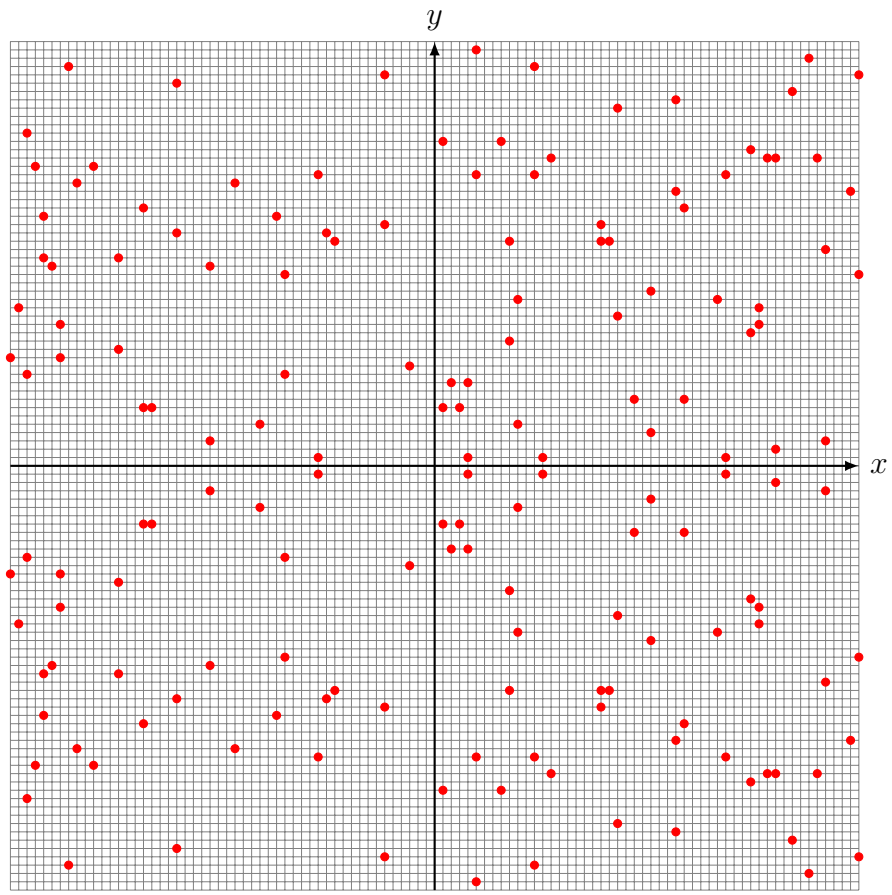


FIGURE 5 – Les 164 points rationnels de la courbe optimale de genre 3 sur $\mathbb{F}_{103}$ définie en (2).

Concernant la dimension 4 la situation est encore bien plus compliquée qu'en dimension 3. En effet, en dimension 4 certaines variétés abéliennes principalement polarisées indécomposables ne sont pas des jacobiennes du tout (même géométriquement). En fait, muni d'une topologie adéquate, le lieu des jacobiennes est un fermé de Zariski de co-

calculé par les algorithmes.

dimension 1 dans les variétés abéliennes principalement polarisées de dimension 4. Le complémentaire du lieu des jacobiennes est donc un ouvert dense. En cela on peut dire que « peu » de variétés abéliennes sont des jacobiennes. De manière générale déterminer le lieu des jacobiennes parmi les variétés abéliennes de dimension g est le célèbre problème de Schottky et fait l'objet de recherches actives (voir [Gru12] ou [Deb95]). Je me permets donc d'appeler l'obstruction d'une variété abélienne à être géométriquement une jacobienne pour $g > 3$ l'*obstruction de Schottky*. Sur $\mathbb{C}$, en dimension 4, la forme modulaire d'Igusa de poids 16 décrit le lieu des jacobiennes ou des variétés abéliennes principalement polarisées décomposables. On a pu montrer dans [KNRR21, Theorem 5.8] que la version algébrique de la forme d'Igusa continue de décrire le lieu des jacobiennes sur n'importe quel corps de caractéristique différente de 2. Ceci nous a permis, grâce au calcul des thêta constantes, de déterminer si certaines variétés correspondaient géométriquement à des jacobiennes. Malheureusement, l'obstruction de Serre dont on a discuté pour le genre 3 existe dès que $g \geq 3$ et nous ne sommes pas en mesure de la calculer ou de la décrire pour $g > 3$ comme on l'a fait à l'aide de la forme χ_{18} pour $g = 3$. Ainsi, si on identifie une jacobienne à l'aide de la forme d'Igusa, nous sommes toujours incapables d'en déduire l'existence d'une courbe optimale. Cependant, nous nous en sommes servis pour montrer qu'il n'existe pas de courbes optimales de genre 4 sur certains corps finis. Par exemple, si on considère $k = \mathbb{F}_{113}$ la borne de Hasse-Weil-Serre donne la majoration $N_{113}(4) \leq 198$. L'anneau d'endomorphismes engendré par le morphisme de Frobenius d'une courbe elliptique optimale est

$$R = \mathbb{Z}[X]/\left\langle X^2 - 21X + 113 \right\rangle \simeq \mathbb{Z}\left[\frac{1+\sqrt{-11}}{2}\right].$$

Il existe 3 réseaux hermitiens unimodulaires indécomposables sur R. Pour chacun d'eux on peut trouver une famille orthogonale de vecteurs de même norme $\ell = 3$ qui nous permet de calculer les thêta constantes puis les valeurs de la forme d'Igusa. On trouve comme valeurs respectives $37, 51$ et $99 \in \mathbb{F}_{113}$. Aucune n'est nulle ce qui signifie qu'aucune des variétés abéliennes correspondantes n'est la jacobienne d'une courbe sur $\bar{\mathbb{F}}_{113}$ donc il n'existe pas non plus de courbe optimale de genre 4 sur $\mathbb{F}_{113}$. On peut mener le même calcul pour $p = 383$ qui correspond au discriminant -11 lui aussi. Les valeurs de la forme d'Igusa appliquée aux thêta constantes calculées donnent respectivement $377, 161$ et 202. La conclusion est donc la même pour $\mathbb{F}_{383}$. Dans [Zay16, Corollary 3.9] l'auteur montre plus généralement que, pour le discriminant -11, il n'existe pas de courbe optimale de

genre 4 (donc pas de jacobienne rationnelle) sur $\mathbb{F}_q$ pour $q \leq 10^4$ et $\mathrm{char}(\mathbb{F}_q) \neq 3$.

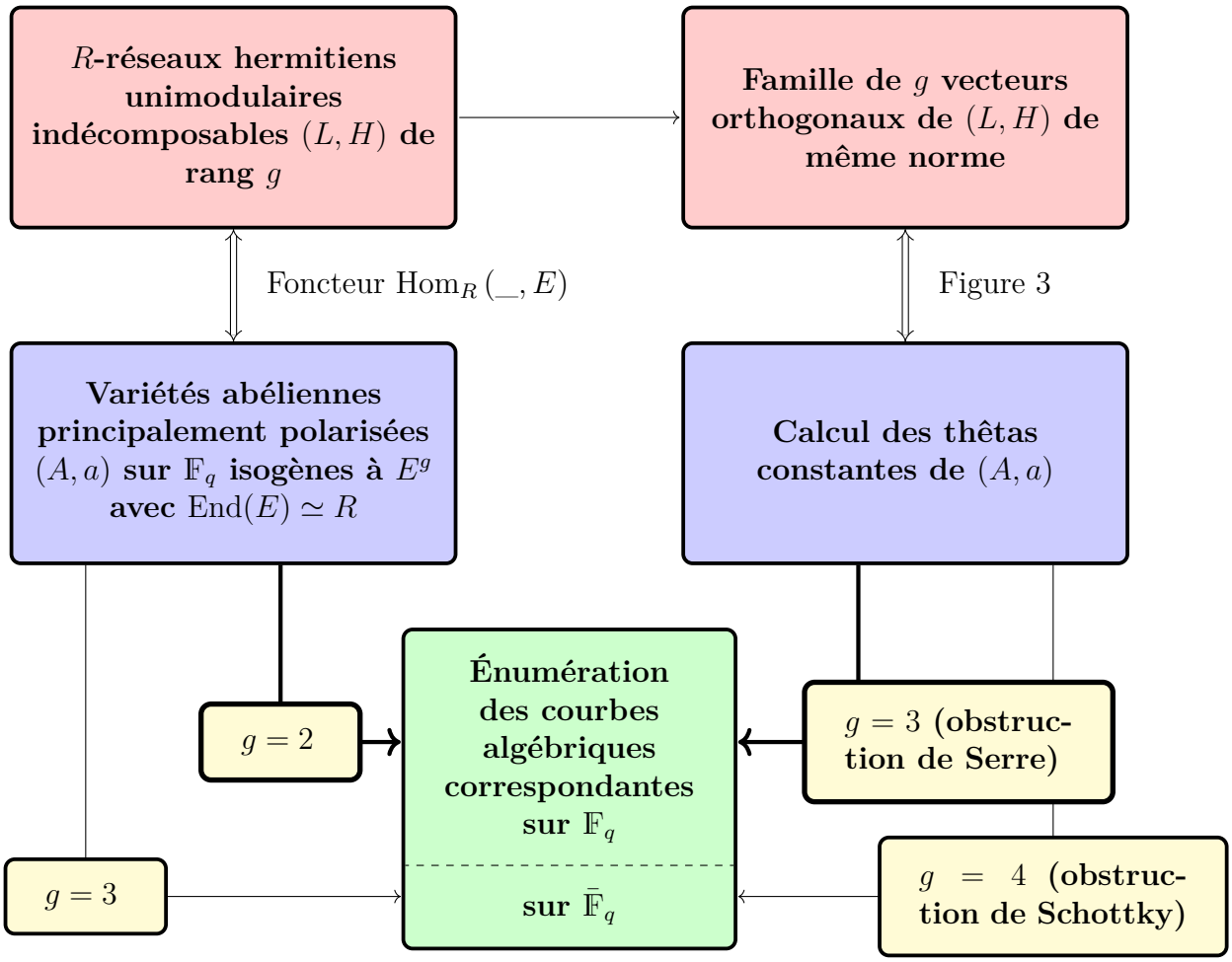


FIGURE 6 – Aperçu de l'algorithme développé dans [KNRR21].

Second projet : équivalence sur les complexes

Il existe une vaste littérature autour des variétés abéliennes complexes ([BL94], [Mum70], [Deb05] et bien d'autres encore). Un résultat fondamental, qui fournit une intuition remarquable aux mathématicien·nes qui travaillent sur les variétés abéliennes, est le fait qu'il existe une équivalence de catégories entre les variétés abéliennes sur le corps des nombres complexes et les *tores complexes* dits *polarisables* donnée par $A \mapsto A(\mathbb{C})$ (voir [Mil08, Theorem 2.9]).

Un tore est simplement le quotient $X = V/\Gamma$ d'un espace vectoriel complexe V de dimension finie par un sous-groupe Γ engendré par une $\mathbb{R}$-base de V. Un tel sous-groupe Γ est appelé un $\mathbb{Z}$-réseau de V. Je me permets d'insister sur le $\mathbb{Z}$ pour désigner le réseau Γ pour le différencier des réseaux sur un anneau R (ou R-réseaux) qu'on a mentionnés dans la section précédente et dont il sera encore question ici. Un tore V/Γ (ou un $\mathbb{Z}$-réseau Γ) est dit polarisable lorsqu'il existe une forme hermitienne [14] h définie positive sur V qui prend des valeurs entières sur Γ, i.e. $h(\Gamma, \Gamma) \subseteq \mathbb{Z}$. On pourrait être tenté de définir un foncteur associant à un tore V/Γ le $\mathbb{Z}$-réseau Γ correspondant $V/\Gamma \mapsto \Gamma$. Malheureusement, bien que fidèle ce foncteur n'est pas plein et donc n'est pas une équivalence de catégories, même en le considérant sur son image essentielle. Cependant, lorsque le tore V/Γ provient d'une variété abélienne isogène [15] à un produit de courbes elliptiques à multiplication complexe (CM) alors le réseau Γ a une structure plus riche. En effet, il peut alors être muni d'une structure de R-module où R est un ordre quadratique dans $K = \mathbb{Q}\left(\sqrt{-d}\right)$. Restreint à ces tores, le foncteur $V/\Gamma \mapsto \Gamma$ décrit alors une équivalence de catégories vers la catégorie des R-réseaux (voir [Nar22, Theorem 1] ou Théorème 2.2.27) qui, composé avec le foncteur $A \mapsto A(\mathbb{C})$ induit une équivalence de la catégorie des variétés abéliennes complexes isomorphes à un produit de courbes elliptiques à CM par un ordre maximal R vers la catégorie des R-réseaux

$$\begin{array}{rccl} \mathbf{F}\colon & \boldsymbol{\mathcal{A}}_R & \to & \boldsymbol{\mathcal{L}}_R \\ & A \text{ telle que } A(\mathbb{C}) \simeq V/\Gamma & \mapsto & \Gamma \\ & (\mathbb{C} \otimes L)/L & \leftarrow\!\shortmid & L. \end{array}$$

En munissant les objets de $\boldsymbol{\mathcal{A}}_R$ de polarisations (catégorie notée $\boldsymbol{\mathcal{A}}_R^p$) et en munissant les réseaux L de formes hermitiennes H qui en font des réseaux *entiers*, i.e. $H(L, L) \subseteq R$ (catégorie notée $\boldsymbol{\mathcal{L}}_R^{h,int}$). On obtient une équivalence de catégories similaire (voir [Nar22, Theorem 2])

$$\mathbf{F}_h\colon \boldsymbol{\mathcal{A}}_R^p \to \boldsymbol{\mathcal{L}}_R^{h,int}.$$

Cependant, il faut noter que les flèches dans ces catégories ne sont plus les morphismes de variétés (resp. les applications R-linéaires) mais les isogénies polarisées (resp. les isométries). Ces deux foncteurs $\mathbf{F}$ et $\mathbf{F}_h$ ont de bonnes propriétés. Ils commutent tous les deux avec les produits, en particulier, il font correspondre les variétés abéliennes polarisées

14. Je note h les formes hermitiennes sur les tores pour les distinguer des formes H sur les R-réseaux.
15. Dans [Nar22], je ne traite que le cas isomorphe, voir la Section 2.2.4 pour une généralisation.

indécomposables aux réseaux hermitiens entiers indécomposables. De plus, ils respectent le degré des isogénies. En particulier, $\mathbf{F}_h$ envoie les variétés abéliennes principalement polarisées sur des réseaux unimodulaires. En petite dimension ($g = 2$ et 3) $\mathbf{F}_h$ fait donc correspondre les jacobiennes de courbes sur $\mathbb{C}$ aux réseaux hermitiens unimodulaires indécomposables.

Cette équivalence $\mathbf{F}_h$ m'a permis dans [Nar22] de généraliser les résultats obtenus dans [GHR19]. Dans [GHR19] les auteurs s'intéressaient à la question d'énumérer toutes les (classes d'isomorphisme de) courbes algébriques de genre 2 sur $\overline{\mathbb{Q}}$ dont la jacobienne est isomorphe au carré d'une courbe elliptique à multiplication complexe par un ordre maximal dans un corps quadratique imaginaire K qui ont pour *corps de modules* $\mathbb{Q}$.

On rappelle qu'étant donnée une courbe C sur un corps k et $k' \to k$ une extension de corps, s'il existe une courbe C' définie sur k' et un isomorphisme sur k entre C et ${C'}_k = C' \times_{k'} k$ (C' « regardée » sur k) alors on dit que C' est un *modèle* de C sur k' et que k' est un *corps de définition* de C. Si on considère C sur $\overline{\mathbb{Q}}$ on appelle corps de modules de C le sous-corps de $\overline{\mathbb{Q}}$ fixé par le groupe

$$\left\{\sigma \in \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right), C^\sigma \simeq C\right\}.$$

Il s'agit de l'intersection de tous les corps de définition de C. Si C est de genre 1 alors le corps de modules est toujours un corps de définition. Étonnamment, les courbes de genre supérieur n'admettent pas toujours de modèle sur leur corps de modules. Une autre façon équivalente de définir le corps de modules en caractéristique nulle [16] est de considérer l'*espace de modules* M_g des courbes de genre g sur $\overline{k}$. Il s'agit de l'ensemble des classes d'isomorphisme des courbes algébriques de genre g et cet ensemble peut lui-même être muni d'une structure de variété algébrique. Si on considère une courbe C, sa classe d'isomorphisme est alors un point de M_g et on peut considérer le corps résiduel de ce point (le plus petit sous-corps k' de $\overline{k}$ tel que ce point est k'-rationnel). Le corps résiduel de la classe de C dans l'espace de modules M_g est le corps de modules de C (cette définition, bien que moins intuitive que la précédente justifie beaucoup mieux l'appellation « corps de modules »).

Une motivation pour classifier les courbes ayant pour corps de modules $\mathbb{Q}$ (et de manière équivalente leur jacobienne) est la classification des algèbres de $\overline{\mathbb{Q}}$-endomorphismes $\mathrm{End}_{\overline{\mathbb{Q}}}(A) \otimes \mathbb{Q}$ que peut avoir une variété abélienne A sur $\mathbb{Q}$. Ce problème se place dans

16. Voir [Bai62] ou [Hug06, Section 1.7] pour une discussion plus approfondie.

la compréhension de la conjecture qui, étant donnés deux entiers $g, d \geq 1$, demande si l'ensemble des algèbres d'endomorphismes des variétés abéliennes de dimension g sur une extension de degré d de $\mathbb{Q}$ est fini. Cette conjecture, énoncée pour les corps de nombres, est attribuée à Coleman dans [BFGR06]. Le cas $g = 1$, i.e. pour les courbes elliptiques, est un cas particulier de la théorie de la multiplication complexe. En effet, si on considère une courbe E sur un corps k de degré d sur $\mathbb{Q}$ alors elle est soit à multiplication complexe par un ordre R de corps des fractions $K = \mathbb{Q}\left(\sqrt{-d}\right)$, soit $\mathrm{End}_{\overline{\mathbb{Q}}}(E) = \mathbb{Z}$. Le dernier cas donne l'algèbre $\mathrm{End}(E) \otimes \mathbb{Q} = \mathbb{Q}$. Si E est à multiplication complexe par [17] $\mathscr{O}_K$ alors son j-invariant est de degré le *nombre de classes* [18] $h_K = \#\,\mathrm{Cl}(\mathscr{O}_K)$ de K sur $\mathbb{Q}$ et est contenu dans k car $\mathbb{Q}(j(E))$ est le corps de modules de E (voir [Sil94, Theorem II.4.3]). Or pour un entier n donné il existe un nombre fini de corps quadratiques imaginaires K de nombre de classes n (il s'agit la conjecture de Gauss [19] démontrée en 1934 par Hans Heilbronn). Ainsi le nombre d'algèbres d'endomorphismes de courbes elliptiques sur un corps de degré d est précisément le nombre de corps quadratiques imaginaires dont le nombre de classes divise d plus un (pour le cas $\mathrm{End}(E) = \mathbb{Z}$). Bien que la conjecture soit toujours ouverte dans le cas $g = 2$ et $d = 1$ pour les variétés abéliennes simples, i.e. pour les surfaces abéliennes sur $\mathbb{Q}$ qui ne se décomposent pas en un produit de deux sous-variétés, les auteurs de [FG20] ont apporté une réponse complète dans le cas non-simple, c'est-à-dire pour les surfaces abéliennes A géométriquement décomposées, i.e. $A_{\overline{\mathbb{Q}}} \simeq E \times E'$ où E et E' sont des courbes elliptiques. Ils ont montré qu'il existe exactement 92 algèbres d'endomorphismes de telles surfaces abéliennes ([FG20, Corollary 1.3]).

Si on considère le travail des auteurs de [GHR19] sous le prisme de l'équivalence de catégories entre les variétés abéliennes sur $\overline{\mathbb{Q}}$ isomorphes à un produit de courbes elliptiques à multiplication complexe par un ordre maximal R et les réseaux hermitiens entiers développée dans [Nar22, Theorem 2] alors ils ont traité le cas où le réseau L est libre, i.e. le cas où le réseau admet une R-base ($L \simeq R^g$). Considérer les courbes dont la jacobienne est isomorphe à un produit de courbes elliptiques non-isomorphes donne simplement lieu à l'étude de réseaux hermitiens (L, H) où L n'admet pas de base.

Maintenant, qu'on sait qu'attraper un réseau hermitien entier (L, H) revient à attraper une variété abélienne polarisée de $\boldsymbol{\mathcal{A}}_R^p$, comment savoir si cette variété a pour corps de modules $\mathbb{Q}$? Peut-on le déterminer directement à partir du réseau hermitien ou

17. On peut supposer $R = \mathscr{O}_K$ l'ordre maximal de K car des variétés abéliennes isogènes ont la même algèbre d'endomorphismes.

18. Voir Définition 1.1.13 pour une définition du *groupe des classes* $\mathrm{Cl}(R)$ d'un ordre R.

19. Plus précisément la conjecture affirme que $h_{\mathbb{Q}(\sqrt{-d})} \underset{d\to\infty}{\longrightarrow} +\infty$.

doit-on calculer les thêta constantes de la variété ou la courbe comme nous l'avons fait dans [KNRR21] ? Malheureusement, le calcul des thêta constantes semble beaucoup plus compliqué à cause de la caractéristique nulle d'une part et à cause de la dimension paire ($g = 2$) d'autre part. Heureusement, j'ai pu traduire l'action du groupe $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$ sur les courbes dans le monde des réseaux hermitiens et j'ai ainsi pu déterminer le corps de modules des courbes directement à partir du réseau hermitien correspondant. En d'autres termes, étant donnée une variété abélienne polarisée (A, a) de $\boldsymbol{\mathcal{A}}_R^p$, un réseau hermitien $\mathbf{F}_h(A, a) = (L, H) \in \boldsymbol{\mathcal{L}}_R^{h,int}$ et un automorphisme $\sigma \in \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$ j'ai pu décrire $\mathbf{F}_h(A^\sigma, a^\sigma)$ en termes de (L, H) et σ (dans le but de comparer (A, a) et (A^σ, a^σ)). Comment faire ? L'idée est de décrire l'action de $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$ en décrivant l'action de chacune des composantes de sa décomposition en produit semi-direct $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) \simeq \mathrm{Gal}\left(\overline{\mathbb{Q}}/K\right) \rtimes \mathrm{Gal}\left(K/\mathbb{Q}\right)$.

L'action de $\mathrm{Gal}\left(K/\mathbb{Q}\right) = \langle x \mapsto \overline{x} \rangle$ est facile à décrire, c'est l'action par conjugaison complexe intuitive composante par composante qu'on pourrait s'attendre à trouver. Soit (L, H) un réseau hermitien et supposons L plongé dans un K-espace vectoriel muni d'une base $b = (x_1, \ldots, x_g)$, i.e $L \subseteq K^g$. On rappelle que la forme hermitienne H est alors complètement déterminée par les valeurs qu'elle prend sur b, i.e par sa matrice de Gram $G(b) = (H(x_i, x_j))_{i,j}$. On peut alors décrire l'action de la conjugaison complexe sur les réseaux à travers le foncteur $\mathbf{F}_h$ ([Nar22, Theorem 3]).

Théorème (Description de l'action de $\mathrm{Gal}(K/\mathbb{Q})$)**.** *Soit $(A, a) \in \boldsymbol{\mathcal{A}}_R^p$ sur $\overline{\mathbb{Q}}$. Soit $\mathbf{F}_h(A, a) = (L, H)$ alors il existe une isométrie*

$$\mathbf{F}_h\left(\overline{A}, \overline{a}\right) \simeq \left(\overline{L}, \overline{H}\right)$$

où $\overline{H}$ désigne la forme hermitienne sur K^g dont la matrice de Gram est $\overline{G(b)}$ avec $G(b)$ la matrice de Gram de H dans une base b.

L'action de $\mathrm{Gal}\left(\overline{\mathbb{Q}}/K\right)$ n'est pas beaucoup plus compliquée à décrire mais demande un peu plus de travail pour la formuler rigoureusement. Dans [Sil94, Chapter II], l'auteur développe la théorie des courbes elliptiques sur $\mathbb{C}$ à multiplication complexe par un ordre maximal R. Rappelons tout d'abord que les courbes elliptiques complexes sont équivalentes aux tores complexes [20] de dimension 1 par [Mil08, Theorem 2.9] par exemple. En d'autres termes, étant donnée une courbe elliptique E sur $\mathbb{C}$, il existe un isomorphisme

20. Contrairement aux tores de dimension $g \geq 2$ il n'est pas nécessaire de demander à ce que ces tores soient polarisables car en dimension 1 c'est toujours le cas.

$E(\mathbb{C}) \simeq \mathbb{C}/\Lambda$. Nous noterons E_Λ pour signifier l'unique [21] courbe elliptique dont les points complexes sont $\mathbb{C}/\Lambda$. Un premier résultat qui expliquera pourquoi nous avons librement jonglé entre $\mathbb{C}$ et $\overline{\mathbb{Q}}$ dans cette section est le fait que toute courbe elliptique sur $\mathbb{C}$ à multiplication complexe par un ordre maximal R admet un modèle [22] sur $\overline{\mathbb{Q}}$ ([Sil94, Proposition 2.1.(c)]). L'auteur montre aussi qu'il existe un morphisme de groupe surjectif $F\colon \mathrm{Gal}\left(\overline{\mathbb{Q}}/K\right) \to \mathrm{Cl}(R)$ tel que $E_\Lambda^\sigma \simeq E_{F(\sigma)^{-1}\Lambda}$ où $\mathrm{Cl}(R)$ désigne le *groupe des classes* de R. On a alors $\mathbf{F}\left(A^\sigma\right) \simeq \mathfrak{a}\mathbf{F}(A)$ où $\mathfrak{a} = F(\sigma)^{-1}$. En d'autres termes, l'action d'un élément σ de $\mathrm{Gal}\left(\overline{\mathbb{Q}}/K\right)$ se fait par produit tensoriel par $F(\sigma)^{-1}$ sur le réseau correspondant. Il reste à savoir ce qu'il se passe si le produit est polarisé. La forme hermitienne qu'on obtient est conservée à un facteur près qui permet au réseau tensorisé de conserver des propriétés similaires à celui de départ. Plus précisément, on a le résultat suivant ([Nar22, Theorem 4]).

Théorème (Description de l'action de $\mathrm{Gal}\left(\overline{\mathbb{Q}}/K\right)$)**.** *Soit* $(A, a) \in \boldsymbol{\mathcal{A}}_R^p$ *sur* $\overline{\mathbb{Q}}$*. Soit* $\mathbf{F}_h(A, a) = (L, H), \sigma \in \mathrm{Gal}\left(\overline{\mathbb{Q}}/K\right)$ *et* $F(\sigma) = \dot{\mathfrak{a}}^{-1} \in \mathrm{Cl}(R)$ *où* $\mathfrak{a}$ *est un idéal* [23] *de* R*. Alors il existe une isométrie*

$$\mathbf{F}_h\left(A^\sigma, a^\sigma\right) \simeq \left(\mathfrak{a}L, \frac{1}{N(\mathfrak{a})}H\right)$$

où $N(\mathfrak{a}) = \#\left(R/\mathfrak{a}\right)$ *est la norme de* $\mathfrak{a}$*.*

Ceci nous permet d'écrire l'Algorithme 1 qui, étant donnés un ordre maximal R et un entier g, énumère les variétés abéliennes de $\boldsymbol{\mathcal{A}}_R^p$ qui ont pour corps de modules $\mathbb{Q}$.

Grâce à ces deux théorèmes et à l'Algorithme 1 qui en découle nous avons pu étendre les résultats de [GHR19] aux courbes de genre 2 sur $\overline{\mathbb{Q}}$ dans le cas où leur jacobienne est isomorphe à un produit de deux courbes elliptiques non isomorphes. Nous avons ainsi pu prouver l'existence de 91 courbes vérifiant ces hypothèses, venant compléter la liste des 46 courbes dont la jacobienne est un carré déjà trouvées dans [GHR19]. Nous avons aussi pu mener les calculs pour $g = 3$ et nous avons trouvé 33 courbes ayant corps de modules $\mathbb{Q}$ (il manque uniquement le résultat du calcul pour $\mathbb{Q}\left(\sqrt{-4027}\right)$ qui est toujours en cours).

21. Pour pouvoir parler d'unicité il faut bien entendu fixer de manière canonique l'isomorphisme $E(\mathbb{C}) \simeq \mathbb{C}/\Lambda$. Ceci peut être fait à l'aide des fonctions $\wp$ de Weierstrass (voir [Nar22, Section 3.2.1]).

22. Mieux ! Elle admet un modèle sur $\mathbb{Q}\left(j(E)\right)$ ([Sil94, Theorem 4.3]) qui est une extension de degré $\#\,\mathrm{Cl}(R)$ de $\mathbb{Q}$.

23. Il n'est pas nécessaire de supposer que $\mathfrak{a} \subseteq R$, on peut se contenter de $\mathfrak{a}$ idéal fractionnaire mais cela me permet de définir sa norme plus facilement juste en dessous.

Algorithme 1 Énumération des éléments de $\mathcal{A}_R^p$ ayant pour corps des modules $\mathbb{Q}$.

Entrée : Un entier g et un ordre maximal R.

Sortie : La liste des réseaux unimodulaires indécomposables (L, H) correspondant aux objets de $\mathcal{A}_R^p$ de corps de modules $\mathbb{Q}$.

LList $\leftarrow$ {réseaux hermitiens unimodulaires de rang g}/ $\simeq$
LList$_{\mathrm{FM}-\mathbb{Q}} \leftarrow$ { } ▷ Liste des variétés abéliennes avec corps de modules $\mathbb{Q}$.
for $(L, H) \in$ LList **do**
    bool $\leftarrow$ True
    for $\mathfrak{a} \in$ {générateurs de Cl(R)} **do**
        bool $\leftarrow$ bool et $(L, H) \simeq \left(\mathfrak{a}L, \frac{1}{N(\mathfrak{a})}H\right)$.
    if bool et $(L, H) \simeq \left(\overline{L}, \overline{H}\right)$ **then**
        LList$_{\mathrm{FM}-\mathbb{Q}} \leftarrow$ LList$_{\mathrm{FM}-\mathbb{Q}} \cup \{(L, H)\}$
return LList$_{\mathrm{FM}-\mathbb{Q}}$

Structure de la thèse

Comme nous l'avons motivé ci-dessus les réseaux hermitiens et les variétés abéliennes polarisées isogènes à un produit de courbes elliptiques à multiplication complexe sont, sous de bonnes hypothèses, liés entre eux par des équivalences de catégories. Ceci nous permet de traduire des problèmes dans le monde de la géométrie algébrique et de les résoudre grâce aux réseaux hermitiens. Nous proposons alors de diviser cette thèse en deux parties principales. Dans un premier temps nous présentons les objets au centre de notre attention : en premier lieu les réseaux hermitiens (Chapitre 1), puis les variétés abéliennes (Chapitre 2). Dans un second temps, j'ai reproduit les deux projets qui sont le cœur de mes recherches durant ces 4 dernières années, [KNRR21] et [Nar22], aux Chapitres 3 et 4 respectivement.

Dans le Chapitre 1 nous souhaitons présenter les outils nécessaires à la compréhension des réseaux hermitiens.

Puisque les réseaux que nous considérerons seront tous des R-modules pour R un ordre quadratique, il convient de commencer par l'étude de ces ordres. On peut considérer les *idéaux fractionnaires*, que nous y étudierons, comme des réseaux de dimension 1. Dans la Section 1.1, nous ferons quelques rappels généraux sur les anneaux d'entiers dans les corps de nombres, puis nous rappellerons les résultats essentiels concernant les idéaux fractionnaires, le groupe des classes, etc.

Dans la section suivante nous présenterons les réseaux hermitiens sur un ordre qua-

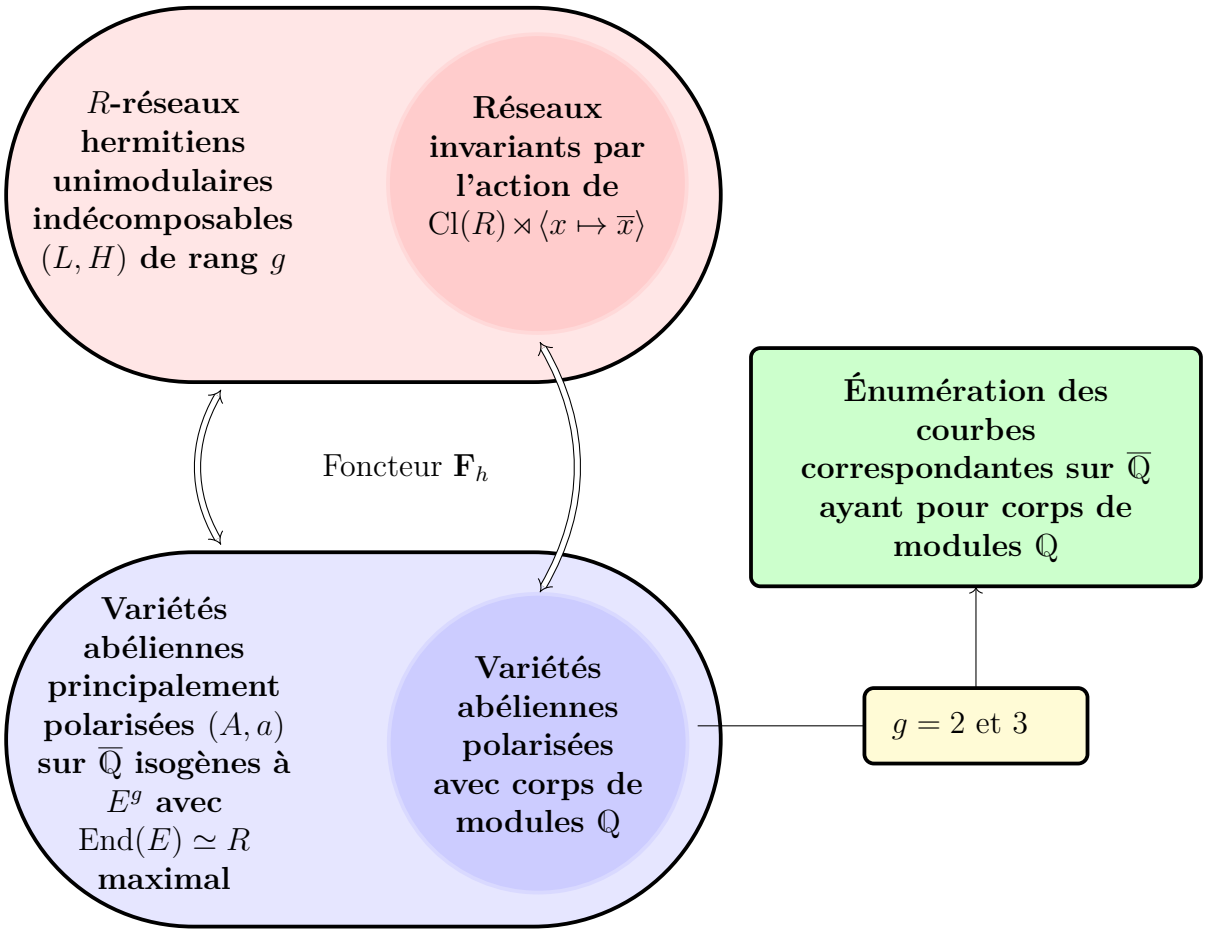


FIGURE 7 – Aperçu de l'algorithme développé dans [Nar22].

dratique. Nous y introduirons les outils essentiels à l'étude des réseaux ; les pseudo-bases, la classe de Steinitz, la notion de modularité, en particulier l'unimodularité et enfin le scale, le dual et le volume d'un réseau hermitien. Nous terminerons cette section par un aperçu de la classification des réseaux hermitiens unimodulaires sur un ordre maximal et nous esquisserons les idées générales de la classification sur un ordre quelconque (que l'on pourra retrouver en détails dans [KNRR21, Section 2.2]). Cette classification est bien entendu centrale dans la suite puisqu'elle nous permettra de classifier les variétés abéliennes principalement polarisées isogènes à un produit de courbes elliptiques à multiplication complexe.

Dans le chapitre 2 nous présenterons la théorie des variétés abéliennes et des polarisa-

tions. Nous commencerons par présenter les variétés abéliennes sur le corps des nombres complexes (Section 2.2) car leur étude est grandement facilitée par l'équivalence qui les lient aux tores complexes. Par ailleurs, la compréhension des variétés abéliennes complexes fournit une intuition précieuse à la mathématicienne souhaitant étudier les variétés abéliennes sur un corps quelconque.

Une fois le matériel nécessaire développé nous énoncerons la première équivalence de catégories qui nous intéresse, le Théorème 2.2.29 pour l'équivalence sans les polarisations puis le Théorème 2.2.33 dans la Section 2.2.4. Les résultats que j'y énonce sont légèrement différents de ceux de [Nar22] car j'ai voulu étendre l'équivalence aux ordres non-maximaux.

Bien que les équivalences soient étendues aux ordres non-maximaux, pour en déduire des résultats sur les corps de modules comme nous l'avons fait dans [Nar22] au cas non-maximal nous devrions aussi traduire l'action de $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$ sur les réseaux hermitiens sur un ordre non-maximal. C'est un projet que je souhaite mener très prochainement mais que je n'ai malheureusement pas encore fait. Je pense que l'action galoisienne se traduit de la même façon pour les ordres maximaux et plusieurs personnes m'ayant demandé de faire les calculs dans les cas non-maximaux j'ai pensé qu'il serait utile de les faire figurer dans cette thèse. C'est l'un des deux objectifs de l'Annexe A où j'ai d'une part reproduit les calculs heuristiques (donc sous réserve que l'action galoisienne agit de la même façon sur les réseaux sur un ordre non-maximal). D'autre part, j'y ai aussi fait figurer la classification des ordres quadratiques dont le groupe des classes est d'exposant 1 ou 2 en m'appuyant sur la classification dans le cas maximal faite dans [EKN20]. Cette dernière classification est complète sous l'hypothèse de Riemann généralisée.

Je tiens à préciser que la totalité des résultats énoncés dans les Chapitres 1 et 2 ne sont pas nouveaux (à l'exception des Théorèmes 2.2.29 et 2.2.33). Ils sont soit connus dans la littérature, auquel cas je fournis des références, soit ce sont des résultats issus de [KNRR21] (Chapitre 3) ou [Nar22] (Chapitre 4). Cependant, pour que la présentation de ces chapitres ne soit pas une énumération froide de résultats je me suis permis d'apporter quelques démonstrations qu'il m'a plu d'imaginer ou de reproduire même si les résultats énoncés sont déjà connus. Éloigné du soucis de démontrer des résultats nouveaux je me suis permis, pour certaines démonstrations, de les faire dans des cas particuliers seulement et non en toute généralité. La lectrice curieuse pourra se reporter aux références citées en début de section ou de chapitre pour apprécier des démonstrations plus complètes ou dans des cadres plus généraux.

J'ai essayé autant que possible de m'appuyer sur des références accessibles à tout le

monde gratuitement. Il me semble important de favoriser autant que possible les voies d'accès à la connaissance qui ne passent pas par l'intermédiaire des grosses maisons d'éditions internationales qui cloisonnent la recherche scientifique à un petit monde restreint aux universités et institutions capables de se payer leurs « services ». Je recommande particulièrement la lectrice de visiter les sites de Keith Conrad [24] et James Milne [25] que j'ai cité à de nombreuses reprises tout au long de ma rédaction. Malheureusement, beaucoup de résultats apparaissent exclusivement dans des journaux onéreux et je n'ai pas pu faire autrement que de les citer.

24. `https://kconrad.math.uconn.edu/`
25. `https://jmilne.org/math/index.html`

Chapitre 1

RÉSEAUX HERMITIENS

Dans ce chapitre je souhaite rappeler les outils nécessaires à la compréhension et à la manipulation des réseaux hermitiens. Dans la Section 1.1 je rappelle la théorie arithmétique des ordres dans les corps quadratiques imaginaires. Ce cadre particulier permet une description très précise de ces ordres. Ils sont tous de la forme $R = \mathbb{Z}[f\omega]$ où $K = \mathbb{Q}(\omega)$ est le corps des fractions de R, l'anneau $\mathbb{Z}[\omega] = \mathscr{O}_K$ est l'ordre maximal (ou, de manière équivalente, l'anneau des entiers) de K et f est un entier positif, appelé le *conducteur* de R (dans $\mathscr{O}_K$). Comprendre les ordres quelconques demande une bonne compréhension de l'arithmétique des ordres maximaux $\mathscr{O}_K = \mathbb{Z}[\omega]$. Ces ordres sont un cas particulier d'*anneaux de Dedekind*, plus généralement de l'anneau des entiers $\mathscr{O}_K$ d'un corps de nombre K est un anneau de Dedekind. Il existe une vaste littérature sur les anneaux de Dedekind, voir par exemple [Conb], [Lan94] ou [Mil20]. Pour une théorie arithmétique sur des ordres quelconques on peut se référer à [BS66, Chapter 2] ou alors à [Mar20a] où l'auteur propose des algorithmes de calcul efficaces du monoïde des classes $\mathrm{ICM}(R)$ d'un ordre R (il s'agit du monoïde multiplicatif des classes d'idéaux fractionnaires de R modulo les idéaux principaux). Malheureusement, ces références ne sont pas suffisamment spécifiques pour l'étude des ordres dans les corps quadratiques et nous nous référerons donc à [Cox85, Section II.7] où l'étude est restreinte à ces ordres. L'étude de $\mathrm{ICM}(R)$ peut être considérée comme l'étude des réseaux de rang 1 sur un ordre R, i.e. l'étude des R-modules L finiment présentés sans torsion tels que $\dim_K(KL) = 1$. Le groupe de Picard (ou groupe des classes) de R, $\mathrm{Cl}(R)$, formé des inversibles de $\mathrm{ICM}(R)$, correspond aux réseaux sur R de rang 1 dits *projectifs*. Il est donc parfaitement normal de bien les comprendre avant d'attaquer l'étude des réseaux quelconques.

La Section 1.2 est dédiée à l'étude des réseaux sur un ordre. Encore une fois, beaucoup de références traitent l'étude des réseaux sur un anneau de Dedekind. On pourra se référer au très classique [O'M63] ou alors à [Sch85] qui aborde des problématiques plus récentes

sur ces réseaux. La classification de ces réseaux vus comme R-modules où R est un ordre dans un corps quadratique imaginaire peut être facilement décrite. Un R-réseau peut toujours s'écrire sous la forme

$$L = \mathfrak{a}_1 x_1 \oplus \cdots \oplus \mathfrak{a}_g x_g$$

où $\mathfrak{a}_i$ est un idéal (fractionnaire) de R inversible[1] dans un ordre R_i et $(x_1, \ldots, x_g)$ une base de l'espace vectoriel KL. La famille $(\mathfrak{a}_i, x_i)$ est appelée une *pseudo-base* de L. La classe d'isomorphisme du R-module L est alors caractérisée par la suite d'ordres $R \subseteq R_1 \subseteq \cdots \subseteq R_g \subseteq \mathscr{O}_K$ ainsi que par la classe du produit $\mathrm{st}(L) = \mathfrak{a}_1 \cdots \mathfrak{a}_g \in \mathrm{Pic}(R_g)$, appelée *classe de Steinitz* de L (voir [BF60] ou [LW85, Theorem 7.1]). Bien qu'il n'existe pas qu'une unique pseudo-base de L, la famille des ordres $(R_1, \ldots, R_g)$ et la classe de Steinitz $\mathrm{st}(L)$ ne dépendent pas de la pseudo-base choisie. Lorsque $R = \mathscr{O}_K$, i.e. R est maximal, on a évidemment $(R_1, \ldots, R_g) = (R, \ldots, R)$, ainsi la classe d'isomorphisme de L ne dépend que de son rang g ainsi que de sa classe de Steinitz (voir [Cona, Theorem 13], [Mil20, Theorem 3.31] ou encore [O'M63, 8:5 et 8:8] pour une preuve de ce résultat pour R un anneau de Dedekind). Intéressons nous maintenant aux *réseaux hermitiens*, i.e. les couples (L, H) où L est un R-réseau et H une forme hermitienne sur KL. La classification de tels objets à isométrie près est une tâche bien plus difficile que la classifications des classes d'isomorphisme des réseaux que nous venons de décrire.

En 1957, dans [Kne57] Martin Kneser développe une méthode pour définir des réseaux hermitiens à partir de leur réseaux *voisins*. Cette méthode des voisins de Kneser est ensuite reprise et améliorée notamment dans [Iya69], [Hof91] ou [Sch98]. Dans [Iya69] l'auteur calcule le nombre de réseaux hermitiens unimodulaires sur $\mathbb{Z}[i]$ de rang $g \leq 7$, les réseaux qu'il étudie sont tous libres car $\mathbb{Z}[i]$ est principal. En revanche, dans [Hof91] (puis généralisé dans [Sch98]) l'auteur se place dans le cadre plus large de l'étude de $\mathscr{O}_K$-réseaux hermitiens où $k \to K$ est une extension de degré 2 et k un corps de nombre. Il démontre notamment que pour tout discriminant $\Delta \notin \{-3, -4, -7\}$ d'un corps quadratique imaginaire K, il existe un réseau hermitien unimodulaire indécomposable de rang 2 et il en existe un libre pour ces discriminants excepté pour $\Delta = -15$. Il montre aussi un résultat similaire pour $\Delta \notin \{-3, -4, -7, -11\}$ pour $g = 3$. Il est intéressant de noter que, pour des motivations similaires à celles de Serre (cf. Introduction), certains de ces résultats étaient déjà connus. Par exemple, dans [HN65] les auteurs montrent qu'il

1. Ceci signifie que $R_i = R_{\mathfrak{a}_i}$, l'anneau multiplicateur de $\mathfrak{a}_i$ (voir Proposition 1.1.17).

n'existe pas de courbes dont la jacobienne est isomorphe à E^2 pour E à multiplication complexe par l'ordre maximal de $\mathbb{Q}\left(\sqrt{\Delta}\right)$ pour $\Delta \in \{-3, -4, -7, -15\}$ en accord avec les résultats de Hoffman [2]. Nous expliquerons succinctement dans la Section 1.2.3 en quoi consiste cette méthode des voisins et pourquoi, combinée à la *formule des masses de Siegel*, elle permet de produire des algorithmes efficaces qui classifient les réseaux hermitiens sur un ordre maximal. Enfin, nous expliquerons schématiquement comment nous avons pu adapter cette classification aux réseaux hermitiens sur un ordre qui n'est pas maximal comme nous l'avons fait dans [KNRR21].

1.1 Ordres dans un corps quadratique imaginaire

Dans cette section on s'intéresse à l'étude d'ordres dans un corps quadratique imaginaire. Ces anneaux jouent un rôle central dans cette thèse car ils interviennent comme un des trois (resp. deux) types d'anneaux d'endomorphismes possibles que peut avoir une courbe elliptique (resp. en caractéristique nulle). Nous souhaitons donc développer les outils nécessaires à leur utilisation. Les ordres sont définissables plus généralement dans un corps de nombres, i.e. une extension finie de $\mathbb{Q}$. Nous commençons donc l'étude par cette définition générale et nous nous restreindrons aux corps quadratiques imaginaires lorsque ce sera nécessaire.

1.1.1 Anneaux d'entiers et factorisation en idéaux premiers

Pour cette section on pourra se référer au très complet [Mil20, Chapter 2] pour la théorie des entiers algébriques et [Mil20, Chapter 3] pour les résultats sur les anneaux de Dedekind. Le [Mil20, Theorem 3.29] montre que les anneaux d'entiers d'un corps de nombre sont des anneaux de Dedekind.

Définition 1.1.1. *Soit K un corps de nombres. Un sous-anneau R de K est un ordre si*

- *Il engendre K sur $\mathbb{Q}$, i.e. $R\mathbb{Q} = K$.*
- *C'est un $\mathbb{Z}$-réseau dans K, i.e. R est de type fini sur $\mathbb{Z}$.*

Puisqu'un ordre est un sous-anneau de K (de caractéristique nulle) il contient $\mathbb{Z}$. La première hypothèse implique alors que $\mathrm{Frac}(R) = K$ (on a même pour tout $\alpha \in K$, il existe $n \in \mathbb{N}$ tel que $n\alpha \in R$).

2. Hoffman lui-même cite Serre dans son introduction pour motiver ses résultats.

Exemple 1.1.2. *L'anneau des entiers de Gauss, $R = \mathbb{Z}[i]$, est un ordre dans le corps $\mathbb{Q}(i)$. On vérifie facilement que $R = \{a + ib \,|\, a, b \in \mathbb{Z}\}$ ce qui prouve que R est de type fini sur $\mathbb{Z}$ et que $R\mathbb{Q} = \mathbb{Q}(i)$. On peut montrer de la même manière que $\mathbb{Z}[2i]$ et plus généralement $\mathbb{Z}[fi]$ pour tout $f \in \mathbb{N}^*$ sont aussi des ordres dans $\mathbb{Q}(i)$ (on verra même que ce sont les seuls).*

Exemple 1.1.3. *Le sous-anneau $R = \mathbb{Z}\left[\frac{i}{2}\right]$ de $\mathbb{Q}(i)$ en revanche n'est pas un ordre bien que $R\mathbb{Q} = \mathbb{Q}(i)$. En effet, pour toute famille finie $(a_1, \ldots, a_m)$ d'éléments de R il existe n suffisamment grand tel que $\frac{1}{2^n} \notin \mathbb{Z}a_1 + \cdots + \mathbb{Z}a_m$. Donc R n'est pas de type fini sur $\mathbb{Z}$.*

D'après la définition, on peut toujours écrire un ordre R de la forme $R = \mathbb{Z}[a_1, \ldots, a_m]$. C'est un résultat classique de théorie des nombres qu'alors les éléments de R sont des *entiers algébriques*, i.e. leur polynôme minimal sur $\mathbb{Q}$ est unitaire à coefficients dans $\mathbb{Z}$. D'autre part, l'anneau $\mathscr{O}_K$ formé de tous les entiers algébriques de K est un $\mathbb{Z}$-module libre de rang $d = [K\colon \mathbb{Q}] = \dim_{\mathbb{Q}}(K)$. L'anneau $\mathscr{O}_K$ est donc un ordre qui contient tous les ordres, on l'appelle l'*ordre maximal* de K.

On peut décrire explicitement les ordres dans un corps quadratique (pas nécessairement imaginaire) comme dans la proposition suivante.

Proposition 1.1.4. *Soit $K = \mathbb{Q}\left(\sqrt{d}\right)$ avec d un entier sans facteur carré. Alors*

- *$\mathscr{O}_K = \mathbb{Z}\left[\sqrt{d}\right]$ si $d = 2, 3 \mod 4$*
- *$\mathscr{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ sinon.*

On pose $\omega_K = \sqrt{d}$ ou $\omega_K = \frac{1+\sqrt{d}}{2}$ suivant les cas.

Démonstration. On pourra consulter la très belle introduction de [Mil20] où ce résultat est démontré. □

Exemple 1.1.5. *L'anneau des entiers de Gauss $\mathbb{Z}[i]$ de l'Exemple 1.1.2 est l'ordre maximal du corps $\mathbb{Q}(i)$. C'est une conséquence de la Proposition 1.1.4 mais on peut aussi le voir en constatant que $\mathbb{Z}[i]$ est un anneau principal ce qui implique qu'il est maximal (la réciproque n'est pas vraie, $R = \mathbb{Z}\left[\sqrt{-13}\right]$ est maximal mais n'est pas principal).*

On peut se demander si les anneaux $\mathscr{O}_K$ ont des propriétés arithmétiques similaires à celles de l'anneau $\mathbb{Z}$. C'est le cas de $\mathbb{Z}[i]$ vu dans l'Exemple 1.1.2 qui est aussi euclidien (donc principal, factoriel). Malheureusement, pour beaucoup d'autres anneaux similaires ce n'est plus vrai. Prenons $R = \mathbb{Z}\left[\sqrt{-13}\right]$ par exemple. On a

$$14 = 2 \times 7 \text{ et } 14 = \left(1 + \sqrt{-13}\right)\left(1 - \sqrt{-13}\right) \tag{1.1}$$

pourtant $2, 7, 1+\sqrt{-13}$ et $1-\sqrt{-13}$ sont irréductibles. L'anneau $\mathbb{Z}\left[\sqrt{-13}\right]$ n'est donc même pas factoriel. En revanche, nous allons voir que, même s'il n'y a pas unicité de la décomposition en facteurs premiers des éléments d'un ordre maximal $\mathscr{O}_K$, on a toujours unicité de la décomposition en idéaux premiers des idéaux de $\mathscr{O}_K$.

Si on revient à l'exemple précédent de $\mathscr{O}_K = \mathbb{Z}\left[\sqrt{-13}\right]$ on a

$$\langle 14\rangle = 14\mathscr{O}_K = \mathfrak{p}_1^2\mathfrak{p}_2\mathfrak{p}_3 \text{ avec } \mathfrak{p}_1 = \left\langle 2, 1+\sqrt{-13}\right\rangle, \mathfrak{p}_2 = \left\langle 7, 1+\sqrt{-13}\right\rangle, \mathfrak{p}_3 = \left\langle 7, 6+\sqrt{-13}\right\rangle$$

où les $\mathfrak{p}_i$ sont des idéaux premiers. Ceci ne contredit pas les deux factorisations de (1.1) car $\langle 2\rangle = \mathfrak{p}_1^2, \langle 7\rangle = \mathfrak{p}_2\mathfrak{p}_3$ et $\left\langle 1+\sqrt{-13}\right\rangle = \mathfrak{p}_1\mathfrak{p}_2$ et $\left\langle 1-\sqrt{-13}\right\rangle = \mathfrak{p}_1\mathfrak{p}_3$ donc les factorisations en idéaux premiers induites par la relation (1.1) sont identiques.

Proposition 1.1.6. *Soit R un ordre dans un corps de nombres K et $\mathfrak{a}$ un idéal de R alors*

1. *Le quotient $R/\mathfrak{a}$ est fini.*
2. *On peut toujours trouver au plus $\dim_{\mathbb{Q}}(K)$ éléments de $\mathfrak{a}$ qui engendrent l'idéal.*

Démonstration. 1. Le fait que le quotient soit fini peut se faire à l'aide des formes de Smith. En effet, $\mathfrak{a}$ est un sous-$\mathbb{Z}$-module de R qui est libre de rang $d = [K\colon \mathbb{Q}]$ (car $\mathbb{Z}$-module de type fini sans torsion et $R\mathbb{Q} = K$) en particulier $\mathfrak{a}$ est aussi libre de rang disons d'. Puisque $\mathfrak{a}\mathbb{Q} = \mathfrak{a}R\mathbb{Q} = K$ alors $d' = d$. Donc $\mathfrak{a}$ est un sous-$\mathbb{Z}$-module de R de même rang. En considérant une $\mathbb{Z}$-base $(a_1, \ldots, a_d)$ de $\mathfrak{a}$ dans $R \simeq \mathbb{Z}^d$ et en prenant la forme de Smith $A' = PAQ = \operatorname{diag}(\delta_1, \ldots, \delta_d), \delta_i \in \mathbb{N}^*, \delta_i|\delta_{i+1}$ avec $A = (a_1 \ldots a_d)$ et $P, Q \in \mathrm{GL}_d(\mathbb{Z})$ on a

$$R/\mathfrak{a} \simeq \mathbb{Z}^d/A\mathbb{Z}^d \simeq \mathbb{Z}^d/A'\mathbb{Z}^d \simeq \mathbb{Z}/\delta_1\mathbb{Z} \times \cdots \times \mathbb{Z}/\delta_d\mathbb{Z}$$

donc le quotient est fini (en termes d'ensembles, le quotient de R-modules est bien le même que le quotient de $\mathbb{Z}$-modules).

2. Par ce qui précède $\mathfrak{a} = \mathbb{Z}a_1 + \cdots + \mathbb{Z}a_d = Ra_1 + \cdots + Ra_d$.

□

Définition 1.1.7. *Soit $\mathfrak{a}$ un idéal non nul dans un ordre R, on pose $N_R(\mathfrak{a}) = \#(R/\mathfrak{a}) = [R\colon \mathfrak{a}]$, la norme de $\mathfrak{a}$ dans R. On notera très souvent $N(\mathfrak{a})$ au lieu de $N_R(\mathfrak{a})$ lorsqu'il n'y a pas d'ambiguïté sur l'ordre dont il est question.*

On énonce le théorème suivant qu'on ne démontrera pas. On trouvera une démonstration de ce dernier dans [Mil20, Proposition 4.1.(b)].

Théorème 1.1.8. *Soit $\mathscr{O}_K$ l'anneau des entiers algébriques d'un corps de nombres K. Alors*

1. *Pour tout idéal $\mathfrak{a}$ de $\mathscr{O}_K$ il existe une unique factorisation en idéaux premiers de $\mathfrak{a}$.*
2. *Si $\mathbb{Q} \to K$ est une extension galoisienne alors*

$$\prod_{\sigma \in \mathrm{Gal}(K/\mathbb{Q})} \mathfrak{a}^\sigma = N(\mathfrak{a})\mathscr{O}_K.$$

Le premier point du Théorème 1.1.8 est vrai plus généralement dans ce qu'on appelle les *anneaux de Dedekind*. Une façon de les définir est de dire qu'ils satisfont cette propriété d'unique factorisation en idéaux premiers. Bien que tous les anneaux d'entiers algébriques soient des anneaux de Dedekind, il existe des anneaux de Dedekind qui ne sont pas des anneaux d'entiers. Par exemple l'anneau $\mathbb{Z}\left[\frac{i}{2}\right]$ de l'Exemple 1.1.3 n'est pas un anneau d'entier (ce n'est même pas un ordre) pourtant c'est un anneau de Dedekind (car il s'agit de la localisation en 2 de $\mathbb{Z}[i]$ qui est un anneau de Dedekind).

Exemple 1.1.9. *Si on considère une extension quadratique $\mathbb{Q} \to K$ et qu'on note $x \to \overline{x}$ l'unique automorphisme non trivial de $\mathrm{Gal}(K/\mathbb{Q})$ alors tout idéal $\mathfrak{a}$ de $\mathscr{O}_K$ satisfait $\mathfrak{a}\overline{\mathfrak{a}} = N(\mathfrak{a})\mathscr{O}_K$.*

1.1.2 Idéaux fractionnaires et groupes des classes

Soit K un corps de nombres et R un ordre dans K. On considère $\mathfrak{a}$ un sous-R-module de K de type fini. On peut alors écrire $\mathfrak{a} = R\alpha_1 + \cdots + R\alpha_n$ avec $\alpha_i \in K$. D'après la définition d'un ordre, il existe $n \in \mathbb{N}^* \subseteq K$ tel que pour tout i on a $n\alpha_i \in R$. Donc $n\mathfrak{a} \subseteq R$ ce qui signifie que $n\mathfrak{a}$ est un idéal de R. Réciproquement, pour $\mathfrak{a}$ un idéal de R alors pour tout élément $\alpha \in K, \alpha\mathfrak{a}$ est un sous-R-module de K de type fini.

Définition 1.1.10. *Un sous-R-module $\mathfrak{a}$ de K de type fini est appelé un idéal fractionnaire de R. Un idéal fractionnaire $\mathfrak{a}$ est dit inversible s'il existe un autre idéal fractionnaire $\mathfrak{b}$ tel que $\mathfrak{ab} = \langle \alpha\beta, \alpha \in \mathfrak{a}, \beta \in \mathfrak{b} \rangle = R$. On dit alors que $\mathfrak{b}$ est l'inverse de $\mathfrak{a}$ et on note $\mathfrak{b} = \mathfrak{a}^{-1}$.*

L'ensemble des idéaux fractionnaires inversibles forme un groupe noté $I(R)$.

Si $\mathfrak{a}$ est un idéal fractionnaire, d'après ce qui précède cela revient à dire que $\mathfrak{a} = \alpha\mathfrak{b}$ avec $\alpha \in K$ (une fraction) et $\mathfrak{b}$ un idéal de R, d'où le nom *idéal fractionnaire* de R.

Exemple 1.1.11. *Les idéaux d'un ordre sont des idéaux fractionnaires de R d'après la Proposition 1.1.6.2*

Exemple 1.1.12. *D'après le Théorème 1.1.8 pour tout idéal $\mathfrak{a}$ d'un ordre maximal $\mathscr{O}_K$ on a*

$$\mathfrak{a}\mathfrak{b} = N(\mathfrak{a})\mathscr{O}_K \text{ avec } \mathfrak{b} = \prod_{\sigma \in \mathrm{Gal}(K/\mathbb{Q})\setminus\{\mathrm{id}\}} \mathfrak{a}^{\sigma}$$

donc $\mathfrak{a}$ est inversible d'inverse $\frac{\mathfrak{b}}{N(\mathfrak{a})}$.

Dans le cas particulier où K est une extension quadratique de $\mathbb{Q}$ on a $\mathfrak{a}^{-1} = \frac{\overline{\mathfrak{a}}}{N(\mathfrak{a})}$.

Pour tout élément $\alpha \in K, \alpha R$ est un idéal fractionnaire inversible d'inverse $\alpha^{-1}R$. Ces idéaux sont appelés idéaux fractionnaires principaux et forment un sous-groupe $P(R)$ de $I(R)$.

Définition 1.1.13. *Le quotient de groupes $\mathrm{Cl}(R) = I(R)/P(R)$ est appelé groupe des classes d'idéaux de R ou plus simplement* groupes des classes *de R. Son cardinal est fini et est appelé* nombre de classes *de R.*

Certaines autrices préfèrent appeler $\mathrm{Cl}(R)$ le groupe de Picard de R et garder le nom groupe des classes pour $\mathrm{Cl}(\mathscr{O}_K)$, l'ordre maximal ce qui permet de parler du groupe des classes $\mathrm{Cl}(K)$ de K ou du nombre des classes h_K de K (en référence à $\mathscr{O}_K$) sans ambiguïté.

Il est intéressant de noter que $\mathrm{Cl}(\mathscr{O}_K)$ ne contient qu'un élément si, et seulement si, $\mathscr{O}_K$ est principal. En effet, un idéal $\mathfrak{a} \subseteq R$ a alors une classe triviale dans $\mathrm{Cl}(\mathscr{O}_K)$ ce qui revient à dire qu'il existe $\alpha \in K, \mathfrak{a} = \alpha R$. Autrement dit, $\mathfrak{a}$ est principal. On interprète souvent le groupe $\mathrm{Cl}(\mathscr{O}_K)$ comme un groupe qui mesure à quel point $\mathscr{O}_K$ n'est pas principal. S'il est trivial $\mathscr{O}_K$ est un anneau principal, si $\#\,\mathrm{Cl}(\mathscr{O}_K) = 2, \mathscr{O}_K$ n'est pas principal, mais presque (il n'existe qu'une classe d'idéaux non-principaux).

Ce n'est malheureusement pas vrai pour un ordre quelconque. Il existe des ordres R ayant un groupe des classes trivial mais qui ne sont pas principaux pour autant. C'est le cas de $\mathbb{Z}\left[\sqrt{-3}\right]$, son groupe des classes est trivial pourtant il n'est pas principal. Par exemple, l'idéal $\mathfrak{a} = \left\langle 2, 1+\sqrt{-3}\right\rangle \subseteq \mathbb{Z}\left[\sqrt{-3}\right]$ n'est pas principal et, en particulier, il n'est pas inversible.

Il est évident que la formule $\mathfrak{a}\overline{\mathfrak{a}} = N(\mathfrak{a})R$ ne peut être vraie pour tout idéal d'un ordre quadratique quelconque car elle implique que $\mathfrak{a}$ est inversible d'inverse $\frac{1}{N(\mathfrak{a})}\overline{\mathfrak{a}}$. En revanche, elle est vraie pour les idéaux inversibles même lorsque l'ordre n'est pas maximal.

Proposition 1.1.14. *Soit R un ordre quadratique imaginaire.*

1. *Pour tout idéal inversible* $\mathfrak{a}$ *de* R *on a* $\mathfrak{a}\overline{\mathfrak{a}} = N(\mathfrak{a})R$. *En particulier, la classe de* $\overline{\mathfrak{a}}$ *est l'inverse de celle de* $\mathfrak{a}$ *dans le groupe* $\mathrm{Cl}(R)$.
2. *Soit* $\mathfrak{a}$ *et* $\mathfrak{b}$ *deux idéaux inversibles de* R. *Alors on a* $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$.

Preuve pour des cas particuliers. La preuve de ces résultats dans toute leur généralité nous emmènerait trop loin c'est pourquoi je propose une preuve de 1. et 2. dans le cas particulier où $\mathfrak{a} = \alpha R$ avec $\alpha \in R$. Pour le cas général voir [Cox85, Lemma 7.14.].

1. Soit $\alpha \in R = \mathbb{Z}[\omega]$ et soit $\chi = X^2 + aX + b$ le polynôme minimal de ω. Alors αR est un sous-$\mathbb{Z}$-module de rang 2 de $R = \mathbb{Z} + \mathbb{Z}\omega$. Si $\alpha = n + m\omega$, la matrice de présentation de αR est donnée par

$$M = \begin{pmatrix} n & -bm \\ m & n - am \end{pmatrix},$$

   i.e. $\alpha R = M\mathbb{Z}^2$ avec la base de $\mathbb{Z}^2$ donnée par $(1, \omega)$. On a alors

$$N(\alpha R) = [R\colon \alpha R] = [\mathbb{Z}^2\colon M\mathbb{Z}^2] = \det M = n^2 - anm + bm^2 = (n + m\omega)(n + m\overline{\omega}).$$

   On a donc bien $\alpha R\overline{\alpha R} = N(\alpha)R$ (sans hypothèse de maximalité de R).

2. On souhaite désormais montrer que $N(\alpha\mathfrak{a}) = N(\alpha)N(\mathfrak{a})$ pour $\alpha \in R, \mathfrak{a} \subseteq R$. On a l'inclusion $\alpha\mathfrak{a} \subseteq \alpha R$ qui induit une factorisation de la projection canonique $\pi\colon R \to R/\alpha R$

$$\begin{array}{ccc} R & & \\ \downarrow{\scriptstyle \widetilde{\pi}} & \searrow^{\pi} & \\ R/\alpha\mathfrak{a} & \xrightarrow{p} & R/\alpha \end{array}$$

   On a $\ker p \circ \widetilde{\pi} = \widetilde{\pi}^{-1} \ker p = \ker \pi = \alpha R$ donc $\ker p = \widetilde{\pi}(\alpha R) = \alpha R/\alpha\mathfrak{a} \simeq R/\mathfrak{a}$ et puisque π est surjective on a $\operatorname{im} \pi = R/\alpha$. En appliquant le théorème d'isomorphisme à p on a

$$(R/\alpha\mathfrak{a})/\ker p \simeq R/\alpha$$

   ce qui donne $N(\alpha\mathfrak{a}) = (\#\ker p)N(\alpha) = N(\alpha)N(\mathfrak{a})$.

□

Remarque 1.1.15. *Remarquons que pour montrer* $N(\alpha\mathfrak{a}) = N(\alpha)N(\mathfrak{a})$ *on a pas fait usage de l'invertibilité supposée de* $\mathfrak{a}$. *Pour cause, elle n'est pas nécessaire. On peut alors*

se demander si la formule

$$N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$$

est toujours vraie lorsque $\mathfrak{a}$ *ou* $\mathfrak{b}$ *est inversible. La réponse est oui et c'est même une équivalence. On en propose une démonstration, spécifique aux ordres quadratiques, dans le Corollaire 1.1.18 qui est une conséquence immédiate de la Proposition 1.1.17. C'est un résultat vrai plus généralement pour les idéaux fractionnaires des ordres dans les corps de nombres (voir [Mar20b, Proposition 2.4]).*

Une conséquence intéressante de ces propriétés multiplicatives est qu'elles nous permettent de définir la norme de n'importe quel idéal fractionnaire. En effet, pour tout idéal fractionnaire $\mathfrak{a}$ il existe un élément $\alpha \in R$ tel que $\alpha\mathfrak{a} \subseteq R$, i.e. $\alpha\mathfrak{a}$ est un idéal et on pose alors

$$N(\mathfrak{a}) = \frac{N(\alpha\mathfrak{a})}{N(\alpha R)} = \frac{N(\alpha\mathfrak{a})}{N(\alpha)}.$$

On peut vérifier grâce aux propriétés multiplicatives de la norme que cette définition ne dépend pas de l'élément α qu'on choisit.

Idéaux quotients et invertibilité

On énonce la proposition suivante, très facile, qui permet de classifier les ordres dans les corps quadratiques imaginaires.

Proposition 1.1.16. *Soit* K *un corps quadratique imaginaire,* $S = \mathbb{Z}[\omega]$ *un ordre et* $R \subseteq S$ *un sous-ordre. Alors il existe* $f \in \mathbb{N}^*$ *tel que* $R = S[f\omega]$.

Démonstration. Par les mêmes arguments que dans la preuve de la Proposition 1.1.6.1 le quotient de groupes S/R est fini. On note f son cardinal. On a alors $fS \subseteq R$, donc $\mathbb{Z}[f\omega] \subseteq R$. D'autre part, $\#S/\mathbb{Z}[f\omega] = f$ donc $R = \mathbb{Z}[f\omega]$. □

L'entier f est appelé le *conducteur* de R dans S. On parlera du conducteur de R sans préciser l'ordre pour désigner le conducteur de R dans l'ordre maximal $\mathscr{O}_K$.

Soit R un ordre dans un corps quadratique imaginaire K. Pour tout idéaux fractionnaires $\mathfrak{a}, \mathfrak{b}$ de R on pose

$$(\mathfrak{a}\colon \mathfrak{b}) = \{\alpha \in K, \alpha\mathfrak{b} \subseteq \mathfrak{a}\}$$

appelé l'idéal quotient de $\mathfrak{a}$ et $\mathfrak{b}$.

Proposition 1.1.17. *Soient* $\mathfrak{a}, \mathfrak{b}$ *deux idéaux fractionnaires d'un ordre* R.

1. *L'idéal quotient* $(\mathfrak{a}\colon \mathfrak{b})$ *est un* R*-idéal fractionnaire.*
2. *L'idéal fractionnaire* $\mathfrak{a}$ *est inversible dans* R *si, et seulement si,* $(R\colon \mathfrak{a})\,\mathfrak{a} = R$.
3. *L'idéal quotient* $R_{\mathfrak{a}} = (\mathfrak{a}\colon \mathfrak{a})$ *est un ordre contenant* R *appelé l'anneau multiplicateur de* $\mathfrak{a}$*. Cet ordre est caractérisé par les identités*

$$R_{\mathfrak{a}} = \max_{R\subseteq S}\{S \text{ tel que } \mathfrak{a}S = \mathfrak{a}\} = \min_{R\subseteq S}\{S \text{ tel que } \mathfrak{a}S \text{ est inversible}\}.$$

   où la relation d'ordre prise sur les ordres est l'inclusion.
4. *Si* $\mathfrak{a}$ *est un idéal pour tout ordre* $R \subseteq S \subseteq R_{\mathfrak{a}}$ *de conducteur* f *de* R *dans* S *on a*

$$N_S(\mathfrak{a}) = fN_R(\mathfrak{a}).$$

5. *Si* $\mathfrak{a}$ *est un idéal inversible dans* R *alors pour tout sur-ordre* S *de* R *on a* $N_S(\mathfrak{a}S) = N_R(\mathfrak{a})$.

Démonstration. 1. Puisque $\mathfrak{a}$ et $\mathfrak{b}$ sont des R-modules, il est clair que $(\mathfrak{a}\colon \mathfrak{b})$ en est un aussi. Par ailleurs, si on considère $n \in \mathbb{Z}$ tel que $nR \subseteq \mathfrak{b}$ on a

$$n\,(\mathfrak{a}\colon \mathfrak{b}) = (\mathfrak{a}\colon \mathfrak{b})\,nR \subseteq (\mathfrak{a}\colon \mathfrak{b})\,\mathfrak{b} \subseteq \mathfrak{a}$$

donc $(\mathfrak{a}\colon \mathfrak{b})$ apparaît comme sous-$\mathbb{Z}$-module d'un $\mathbb{Z}$-module de libre de rang fini, il est donc aussi fini sur $\mathbb{Z}$ donc sur R. C'est donc un idéal fractionnaire de R.

2. Si $(R\colon \mathfrak{a})\,\mathfrak{a} = R$ alors $\mathfrak{a}$ est inversible d'inverse $\mathfrak{a}^{-1} = (R\colon \mathfrak{a})$. Réciproquement si $\mathfrak{a}$ est inversible alors

$$(R\colon \mathfrak{a}) = \{\alpha \in K, \alpha\mathfrak{a} \subseteq R\} = \{\alpha \in K, \alpha R \subseteq \mathfrak{a}^{-1}\} = \{\alpha \in K, \alpha \in \mathfrak{a}^{-1}\} = \mathfrak{a}^{-1}.$$

3. On sait déjà que $(\mathfrak{a}\colon \mathfrak{a})$ est un $\mathbb{Z}$-module de type fini (donc stable par somme), il contient 1. Il reste à savoir s'il est stable par produit. Soient $\alpha, \beta \in R_{\mathfrak{a}}, \alpha\beta\mathfrak{a} \subseteq \alpha\mathfrak{a} \subseteq \mathfrak{a}$ donc $\alpha\beta \in R_{\mathfrak{a}}$. Puisque $\mathfrak{a}$ est un idéal fractionnaire $R \subseteq R_{\mathfrak{a}}$. On remarque que, par définition, $R_{\mathfrak{a}}$ est le plus grand sur-ordre S de R tel que l'ensemble $\mathfrak{a}$ est un S-idéal. D'autre part, pour tout sur-ordre S de $R_{\mathfrak{a}}$ on a bien évidemment

$$S = R_{\mathfrak{a}}S = \mathfrak{a}\,(R_{\mathfrak{a}}\colon \mathfrak{a})\,S = \mathfrak{a}S\,(R_{\mathfrak{a}}\colon \mathfrak{a})\,S$$

ce qui prouve que $\mathfrak{a}S$ est inversible dans S.

Nous ne montrerons pas que $\mathfrak{a}$ est inversible dans $R_\mathfrak{a}$ car cela nous emmenerait trop loin. La lectrice curieuse pourra se référer à [BL94] ou [Mar20a]. C'est un résultat qui est vrai plus généralement dans les anneaux dits *de Goreinstein* (voir [BL94, Proposition 2.7]). Les ordres quadratiques imaginaires sont de tels anneaux car ils sont monogènes, i.e. $R \simeq \mathbb{Z}[X]/\langle \mu(X) \rangle$ avec μ unitaire (voir [BL94, Example 2.8]).

4. On a un diagramme commutatif où les lignes sont des suites exactes de groupes

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathfrak{a} & \longrightarrow & R & \longrightarrow & R/\mathfrak{a} & \longrightarrow & 0 \\ & & \| & & \downarrow{\scriptstyle \iota} & & \downarrow{\scriptstyle \bar{\iota}} & & \\ 0 & \longrightarrow & \mathfrak{a} & \longrightarrow & S & \longrightarrow & S/\mathfrak{a} & \longrightarrow & 0 \end{array}$$

   En y appliquant le lemme du serpent on a un isomorphisme $\operatorname{coker} \bar{\iota} \simeq \operatorname{coker} \iota$ ce qui donne

$$(S/\mathfrak{a})/(R/\mathfrak{a}) \simeq S/R \text{ donc } N_S(\mathfrak{a}) = fN_R(\mathfrak{a})$$

5. D'après [Cox85, Corollary 7.17] on peut supposer $\mathfrak{a}$ premier à f, le conducteur de R dans S, quitte à le multiplier par un idéal fractionnaire principal. On a alors, d'après [Cox85, Proposition 7.20], $\mathfrak{a} = R \cap (\mathfrak{a}S)$ et l'isomorphisme $R/\mathfrak{a} \simeq S/\mathfrak{a}S$ qui donne $N_S(\mathfrak{a}S) = N_R(\mathfrak{a})$.

□

On remarque qu'on peut aussi caractériser $R_\mathfrak{a}$ de la façon suivante grâce aux points 4 et 5 de la proposition

$$R_\mathfrak{a} = \min_{R \subseteq S} \{S \text{ tel que } N_S(\mathfrak{a}S) = N_R(\mathfrak{a})\} = \max_{R \subseteq S} \{S \text{ tel que } N_S(\mathfrak{a}S) \neq N_R(\mathfrak{a})\}.$$

Dans la suite on notera $f_\mathfrak{a}$ le conducteur de R dans $R_\mathfrak{a}$. On a toujours la relation $N_{R_\mathfrak{a}}(\mathfrak{a}) = f_\mathfrak{a} N_R(\mathfrak{a})$.

Corollaire 1.1.18. *Soient $\mathfrak{a}$ et $\mathfrak{b}$ deux idéaux de R, un ordre dans un corps quadratique imaginaire. Supposons $\mathfrak{b}$ inversible. Alors*

$$N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b}).$$

Démonstration. On remarque que $R_\mathfrak{ab} = R_\mathfrak{a}$ car $\mathfrak{ab}R_\mathfrak{a} = \mathfrak{a}R_\mathfrak{a}\mathfrak{b} = \mathfrak{ab}$ et $\mathfrak{ab}$ est inversible dans $R_\mathfrak{a}$. Donc par la Proposition 1.1.14.2 on a $N_{R_\mathfrak{a}}(\mathfrak{ab}) = N_{R_\mathfrak{a}}(\mathfrak{a})N_{R_\mathfrak{a}}(\mathfrak{b}R_\mathfrak{a})$. D'après la

Proposition 1.1.17.(4) et 1.1.17.(5) on a donc

$$N_{R_\mathfrak{a}}(\mathfrak{ab}) = f_\mathfrak{a} N_R(\mathfrak{ab}) \tag{1.2}$$

et, d'autre part,

$$N_{R_\mathfrak{a}}(\mathfrak{ab}) = N_{R_\mathfrak{a}}(\mathfrak{a}) N_{R_\mathfrak{a}}(\mathfrak{b}R_\mathfrak{a}) = f_{R_\mathfrak{a}} N_R(\mathfrak{a}) N_R(\mathfrak{b}). \tag{1.3}$$

donc par les relations (1.2) et (1.3) on a

$$N_R(\mathfrak{ab}) = f_{R_\mathfrak{a}} N_R(\mathfrak{ab}) = f_{R_\mathfrak{a}} N_R(\mathfrak{a}) N_R(\mathfrak{b}) \text{ donc } N_R(\mathfrak{ab}) = N_R(\mathfrak{a}) N_R(\mathfrak{b}).$$

□

1.2 Réseaux hermitiens sur un ordre quadratique

1.2.1 Définition générales

Soit R un ordre dans un corps quadratique imaginaire $K = \mathbb{Q}\left(\sqrt{-d}\right)$. Un *$R$-réseau* L est un R-module de type fini sans torsion. Le K-espace vectoriel $KL = L \otimes_R K$ est alors de dimension finie, on pose $\mathrm{rk}(L) = \dim_K(KL)$ le *rang* de L.

L'automorphisme non trivial $\alpha \to \overline{\alpha}$ de $\mathrm{Gal}(K/\mathbb{Q})$ est la conjugaison complexe. Ceci nous permet de définir des formes hermitiennes H sur les K-espaces vectoriels V comme étant une application $H\colon V \times V \to K$ linéaire par rapport à la première variable et antisymétrique, i.e. $H(x,y) = \overline{H(y,x)}$. On dira que H est positive si pour tout $v \in V, H(v,v) \geq 0$ et elle est définie si $H(v,v) \neq 0$ pour $v \neq 0$. Dans la suite nous ne considérerons que des formes hermitiennes définies positives. Un couple (V,H) où V est un K-espace vectoriel et H une forme hermitienne définie positive est appelé un *espace hermitien*.

Un *R-réseau hermitien* est un couple (L,H) où L est un R-réseau et H est une forme hermitienne sur l'espace vectoriel $V = KL$. L'idéal fractionnaire $\mathfrak{s}(L) = H(L,L) \subseteq K$ est appelé le *scale* du R-réseau hermitien (L,H). On appelle le *dual* du R-réseau hermitien (L,H) le réseau défini par

$$L^\# = \{v \in KL, H(v,L) \subseteq R\}.$$

Un réseau hermitien (L,H) est dit *entier* si $L \subseteq L^\#$, i.e. si $\mathfrak{s}(L)$ est un idéal de R.

On dit qu'un réseau hermitien (L, H) est $\mathfrak{a}$-*modulaire* si $L = \mathfrak{a}L^{\#}$. Dans ce cas $\mathfrak{s}(L) = \mathfrak{a}$, en effet,

$$H(L, L) = H(\mathfrak{a}L^{\#}, L) = \mathfrak{a}H(L^{\#}, L) = \mathfrak{a}.$$

En revanche, la réciproque n'est pas vraie. Dans le cas où (L, H) est R-modulaire on dira qu'il est *unimodulaire*.

Soit (L, H) un réseau hermitien de rang g. Étant donnée une famille $b = (x_1, \ldots, x_g)$ de g vecteurs de KL on pose $G(b) = (H(x_i, x_j))_{1 \leq i,j \leq g}$ la *matrice de Gram* de la famille b. On définit $\mathfrak{v}(L)$ le *volume* de (L, H) comme étant l'idéal fractionnaire engendré par

$$\{\det G(b), b \text{ famille de } g \text{ vecteurs de } KL\}.$$

Une autre notion dont on aura besoin pour définir l'équivalence de catégories dans la section 2.2.4 est le rééchelonnage. Soit (V, H) un espace hermitien et α un réel strictement positif. On pose (V^{α}, H^{α}) l'espace V muni de la forme $H^{\alpha} \colon (x, y) \mapsto \alpha H(x, y)$. De même (L^{α}, H^{α}) désigne le réseau L dans l'espace hermitien (V^{α}, H^{α}). Bien que les ensembles de vecteurs de ne soient pas modifiés par le rééchelonnage on les note tout de même V^{α} et L^{α} pour se permettre l'abus de parler de l'espace hermitien V^{α} ou du réseau hermitien L^{α} sous-entendu les espaces V ou L munis de la forme H^{α}.

On dira que deux R-réseaux hermitiens (L_1, H_1) et (L_2, H_2) sont *isométriques* s'il existe une application R-linéaire $\iota \colon L_1 \longrightarrow L_2$ telle que pour tout $x, y \in L_1, H_2(\iota(x), \iota(y)) = H_1(x, y)$. On notera parfois

$$\iota \colon (L_1, H_1) \longrightarrow (L_2, H_2)$$

une telle application et on dira que ι est une *isométrie*. La relation « être isométrique à » définit une relation d'équivalence sur les réseaux hermitiens et la classe d'équivalence d'un réseau pour cette relation est appelée *classe d'isométrie*.

La lectrice attentive aura remarqué qu'on a parfois parlé de réseau sans préciser l'anneau R dont il est question. De la même façon, dans la définition du scale, du volume ou du dual, la forme H n'est pas précisée alors qu'elle est nécessaire. Nous commettrons souvent ces abus pour ne pas alourdir les notations. Nous préciserons la forme H lorsque ce sera nécessaire.

Exemple 1.2.1. *Étant donné un ordre R le R-module $L = R^g$ est un R-réseau. Pour toute matrice hermitienne G, i.e. telle que ${}^t\overline{G} = G$ on peut définir une forme hermitienne définie par $H_G(v, w) = {}^t v G \overline{w}$ en représentant les vecteurs de $KL = K^g$ dans la base canonique*

fournie par R^g. Dans ce cas, (R^g, H_G) est entier si, et seulement si, la matrice G est à coefficients dans R et c'est un réseau unimodulaire si (R^g, H_G) est entier et $\det G = 1$.

Exemple 1.2.2. *Un autre exemple simple de réseau est celui des idéaux fractionnaires. Un idéal fractionnaire est par définition un R-réseau de rang* 1. *On remarque alors que, contrairement aux réseaux sur $\mathbb{Z}$, les R-réseaux ne sont pas toujours libres. En effet, si R est un ordre tel que $\#Cl(R) \geq 2$ ou R non maximal alors R a des idéaux non principaux, donc ils n'admettent pas de R-base en tant que R-modules.*

1.2.2 Réseaux sur un ordre maximal $\mathscr{O}_K$

Lorsqu'on se restreint aux réseaux sur un anneau R de Dedekind, la théorie est très bien connue, voir [O'M63] par exemple. Puisqu'on souhaite continuer de travailler avec des formes hermitiennes on a besoin de conjugaison complexe et donc on se restreindra à R un ordre maximal dans un corps quadratique imaginaire. Il faut noter que beaucoup de résultats qu'on énoncera sur les réseaux restent vrais plus généralement sur des réseaux sur un anneau de Dedekind.

Pseudo-bases et classes de Steinitz

Un outil central dans l'étude des réseaux sur les anneaux de Dedekind est l'existence de pseudo-bases. Une pseudo-base d'un R-réseau L de rang g est la donnée d'une base $(x_1, \ldots, x_g)$ de KL et d'idéaux fractionnaires $\mathfrak{a}_1, \ldots, \mathfrak{a}_g$ tels que

$$L = \mathfrak{a}_1 x_1 + \cdots + \mathfrak{a}_g x_g.$$

Étant donnée une pseudo-base $(\mathfrak{a}_i, x_i)$ de L classe de Steinitz de L, notée $\mathrm{st}(L)$, est définie comme étant la classe du produit $\mathfrak{a}_1 \cdots \mathfrak{a}_g$ dans $\mathrm{Cl}(R)$. On résume les propriétés principales des pseudos-bases dans la proposition suivante.

Proposition 1.2.3. *Soit L un réseau sur un anneau de Dedekind R alors :*

1. *L admet une pseudo-base.*
2. *La classe de Steinitz de L est indépendante de la pseudo-base.*
3. *La donnée du rang d'un réseau L et de sa classe de Steinitz détermine la classe d'isomorphisme*[3] *du réseau L.*

3. En tant que R-module.

4. *Soient L, M deux réseaux dans un K-espace vectoriel. Alors il existe une base $(x_1, \dots, x_g)$ de V telle que*

$$L = \mathfrak{a}_1 x_1 + \cdots + \mathfrak{a}_g x_g \text{ et } M = \mathfrak{a}_1\mathfrak{r}_1 x_1 + \cdots + \mathfrak{a}_g\mathfrak{r}_g x_g$$

où $\mathfrak{a}_i$ et $\mathfrak{r}_i$ sont des idéaux fractionnaires de R. Les idéaux $\mathfrak{r}_i$ ainsi définis sont uniques et sont appelés les facteurs invariants de M dans L.

Démonstration. Voir [Cona, Theorem 6] pour le point 1., [Cona, Theorem 13] pour les points 2. et 3. et [O'M63] pour le 4. (et 1. car le 4. implique le 1). □

Une remarque importante est que, d'après le point 3. de la proposition ci-dessus, tout réseau $L = \mathfrak{a}_1 x_1 \oplus \cdots \oplus \mathfrak{a}_g x_g$ est isomorphe à $\mathfrak{a}_1 \cdots \mathfrak{a}_g \oplus R \oplus \cdots \oplus R$. Ainsi, les réseaux sur un anneau de Dedekind ne sont pas tous libres, mais presque. Un réseau est libre si, et seulement si, sa classe de Steinitz est triviale, i.e. si $\mathfrak{a}_1 \cdots \mathfrak{a}_g$ est principal.

Les scales, volumes et notions de $\mathfrak{a}$-modularités peuvent se reformuler facilement en termes de pseudo-bases du R-réseau d'un réseau hermitien (L, H).

Proposition 1.2.4. *Soit (L, H) un R-réseau hermitien avec R l'ordre maximal d'un corps quadratique imaginaire K. Soit $L = \mathfrak{a}_1 x_1 + \cdots + \mathfrak{a}_g x_g$ une pseudo-base de L. Alors*

1. *Le scale $\mathfrak{s}(L)$ vérifie*
$$\mathfrak{s}(L) = \sum_{i,j} \mathfrak{a}_i \overline{\mathfrak{a}_j} H(x_i, x_j).$$

2. *Le volume $\mathfrak{v}(L)$ vérifie*
$$\mathfrak{v}(L) = N(\mathfrak{a}_1 \cdots \mathfrak{a}_g) \det\left(G(x_1, \dots, x_g)\right) R.$$
Remarquons que $\mathfrak{v}(L)$ est toujours un idéal fractionnaire principal engendré par un nombre rationnel. On confondra parfois l'idéal fractionnaire $\mathfrak{v}(L)$ et son unique générateur positif.

3. *Si $M \subseteq L$ alors $[L\colon M] = \#(L/M) = \mathfrak{v}(M)/\mathfrak{v}(L)$.*

4. *Le réseau dual vérifie*
$$L^{\#} = \overline{\mathfrak{a}_1}^{-1} x_1^{\#} + \cdots + \overline{\mathfrak{a}_g}^{-1} x_g^{\#}$$
où $\left(x_i^{\#}\right)$ est la base duale de (x_i), i.e. $H\left(x_i, x_j^{\#}\right) = \delta_{ij}$ avec $\delta_{ii} = 1$ et 0 sinon. En particulier, $\mathfrak{v}\left(L^{\#}\right) = \mathfrak{v}(L)^{-1}$.

5. *On a toujours* $\mathfrak{v}(L) \subseteq \mathfrak{s}(L)^g$.

6. *Un réseau hermitien* (L, H) *est* $\mathfrak{a}$*-modulaire si, et seulement si,*

$$\mathfrak{s}(L) \subseteq \mathfrak{a} \text{ et } \mathfrak{v}(L) = \mathfrak{a}^g$$

Démonstration. 1. On a tout simplement

$$H(L, L) = H\left(\bigoplus_i \mathfrak{a}_i x_i, \bigoplus_j \mathfrak{a}_j x_j\right) = \sum_{i,j} \mathfrak{a}_i \overline{\mathfrak{a}_j} H(x_i, x_j).$$

2. En se rappelant qu'étant donnée une famille $(x_1, \ldots, x_g)$ et $\lambda \in K$ on a $\det(G(\lambda x_1, \ldots, x_g)) = \lambda\overline{\lambda}\det(G(x_1, \ldots, x_g))$ on a

$$\begin{aligned}
\mathfrak{v}(L) &= \langle\{\det G(b)\}\rangle \\
&= \langle\{\det(G(\alpha_1 x_1, \ldots, \alpha_g x_g)), \alpha_i \in \mathfrak{a}_i\}\rangle \\
&= \langle\{\alpha_1\overline{\alpha_1}\cdots\alpha_g\overline{\alpha_g}\det(G(x_1, \ldots, x_g)), \alpha_i \in \mathfrak{a}_i\}\rangle \\
&= \mathfrak{a}_1\overline{\mathfrak{a}_1}\cdots\mathfrak{a}_g\overline{\mathfrak{a}_g}\det(G(x_1, \ldots, x_g)) \\
&= N(\mathfrak{a}_1)\cdots N(\mathfrak{a}_g)\det(G(x_1, \ldots, x_g))R \text{ (d'après la Proposition 1.1.17)} \\
&= N(\mathfrak{a}_1\cdots\mathfrak{a}_g)\det(G(x_1, \ldots, x_g))R.
\end{aligned}$$

3. Prenons les facteurs invariants $\mathfrak{r}_i$ de M dans L. Alors ce sont alors des idéaux de R et on a

$$L/M \simeq R/\mathfrak{r}_1 + \cdots + R/\mathfrak{r}_g.$$

Donc $[L\colon M] = N(\mathfrak{r}_1 \ldots \mathfrak{r}_g) = \mathfrak{v}(M)/\mathfrak{v}(L)$.

4. On a $H(\overline{\mathfrak{a}_1}^{-1}x_1^\# + \cdots + \overline{\mathfrak{a}_g}^{-1}x_g^\#, L) \subseteq R$ donc $\overline{\mathfrak{a}_1}^{-1}x_1^\# + \cdots + \overline{\mathfrak{a}_g}^{-1}x_g^\# \subseteq L^\#$. Réciproquement, soit $x \in L^\#, x = \lambda_1 x_1^\# + \cdots + \lambda_g x_g^\#$ on a alors

$$H(x, \mathfrak{a}_i x_i) = \lambda_i\overline{\mathfrak{a}_i} \subseteq R \text{ donc } \lambda_i \in \overline{\mathfrak{a}_i}^{-1}.$$

Par ailleurs, $G\left(x_1^\#, \ldots, x_g^\#\right) = G(x_1, \ldots, x_g)^{-1}$ donc $\mathfrak{v}\left(L^\#\right) = \mathfrak{v}(L)^{-1}$.

5. On écrit $L = \mathfrak{a}_1 x_1 \oplus \cdots \oplus \mathfrak{a}_g x_g$ et on pose $g_{ij} = H(x_i, x_j)$ de telle sorte que $G(x_1, \ldots, x_g) = (g_{ij})$. On remarque que pour tout $i, j, H(\mathfrak{a}_i x_i, \mathfrak{a}_j x_j) = \mathfrak{a}_i\overline{\mathfrak{a}_j}g_{ij} \subseteq$

$\mathfrak{s}(L)$. Donc

$$\begin{aligned}\mathfrak{v}(L) &= \mathfrak{a}_1\overline{\mathfrak{a}_1}\dots\mathfrak{a}_g\overline{\mathfrak{a}_g}\det((g_{ij}))\\ &= \mathfrak{a}_1\overline{\mathfrak{a}_1}\dots\mathfrak{a}_g\overline{\mathfrak{a}_g}\sum_{\sigma\in\mathfrak{S}_g} g_{1\sigma(1)}\dots g_{g\sigma(g)}\\ &= \sum_{\sigma\in\mathfrak{S}_g} \mathfrak{a}_1\overline{\mathfrak{a}_{\sigma(1)}}g_{1\sigma(1)}\dots\mathfrak{a}_g\overline{\mathfrak{a}_{\sigma(g)}}g_{g\sigma(g)} \subseteq \mathfrak{s}(L)^g.\end{aligned}$$

6. Supposons $\mathfrak{s}(L)\subseteq\mathfrak{a}$ et $\mathfrak{v}(L)=\mathfrak{a}^g$. On a alors $H(L,L)\subseteq\mathfrak{a}$ donc $H\left(\mathfrak{a}^{-1}L,L\right)\subseteq R$ autrement dit $\mathfrak{a}^{-1}L\subseteq L^\#$ donc $L\subseteq\mathfrak{a}L^\#$.
   Par ailleurs, $\mathfrak{v}\left(\mathfrak{a}L^\#\right)=N(\mathfrak{a})^g\frac{1}{\mathfrak{v}(L)}=\overline{\mathfrak{a}}^g=\mathfrak{a}^g=\mathfrak{v}(L)$ (remarquons que si $\mathfrak{v}(L)=\mathfrak{a}$ ou $\mathfrak{s}(L)=\mathfrak{a}$ alors l'idéal fractionnaire $\mathfrak{a}$ satisfait $\mathfrak{a}=\overline{\mathfrak{a}}$). Il s'agit donc de l'inclusion de deux réseaux de même volume donc $L=\mathfrak{a}L^\#$.
   Réciproquement, si $L=\mathfrak{a}L^\#$ alors $\mathfrak{s}(L)=H(L,L)=\mathfrak{a}$ et $\mathfrak{v}(L)=N(\mathfrak{a})^g\frac{1}{\mathfrak{v}(L)}$ donc $\mathfrak{v}(L)^2=N(\mathfrak{a})^g=\mathfrak{a}^{2g}$ donc $\mathfrak{v}(L)=\mathfrak{a}^g$ (par unicité de la décomposition en idéaux premiers par exemple).

□

1.2.3 Classification des réseaux hermitiens unimodulaires

L'objectif de cette section est la classification des réseaux hermitiens unimodulaires (indécomposables) à isométrie près. Classifier ces objets est une tâche compliquée. Nous nous proposons donc de commencer par un cas élémentaire : le rang 1. Ce cas là n'est fait que dans un but pédagogique, il n'est pas nécessaire pour la suite.

Échauffement : classification des réseaux unimodulaires de rang 1

Soit (L,H) un R-réseau hermitien unimodulaire avec R un ordre (pas forcément maximal) dans un corps quadratique imaginaire K. On pose $h_0\colon K\times K\to K,(x,y)\mapsto x\overline{y}$ la forme hermitienne canonique sur K. Par définition, L est de rang 1 donc il existe un isomorphisme $\iota\colon KL\to K$ qui induit une isométrie $\iota\colon(KL,H)\to(K,\delta h_0)$ où $\delta=H(x,x)$ et $x=\iota^{-1}(1)$. Puisque ι est un morphisme de R-modules $\mathfrak{a}=\iota(L)$ est un R-idéal fractionnaire. On a alors

$$L=\mathfrak{a}x.$$

Puisque (L,H) est unimodulaire, $H(L,L)=H(\mathfrak{a}x,\mathfrak{a}x)=\mathfrak{a}\overline{\mathfrak{a}}H(x,x)=R$. En particulier, cela implique que $\mathfrak{a}$ est un idéal inversible. Ainsi, d'après la Proposition 1.1.14,

$H(L,L) = N(\mathfrak{a})H(x,x)R = R$ ce qui implique $\delta = H(x,x) = \frac{1}{N(\mathfrak{a})}$.

Réciproquement, tous les réseaux hermitiens (L,H) de la forme $L = \mathfrak{a}x$ avec $\mathfrak{a}$ idéal fractionnaire inversible et $H(x,x) = \frac{1}{N(\mathfrak{a})}$ sont bien des réseaux hermitiens unimodulaires.

On peut résumer ceci en un théorème.

Théorème 1.2.5. *Soit (L,H) un R-réseaux hermitien unimodulaire de rang 1 alors*

$$(L,H) \simeq \left(\mathfrak{a}, \frac{1}{N(\mathfrak{a})}h_0\right)$$

pour un certain $\mathfrak{a}$ inversible et h_0 la forme hermitienne canonique sur K. En particulier, on a une bijection

$$\{R\text{-réseaux hermitiens unimodulaires de rang } 1\} / \simeq \longleftrightarrow \mathrm{Cl}(R).$$

On a vu dans la Proposition 1.2.3 que tout R-réseaux L de rang g peut s'écrire comme somme directe $L = \bigoplus_{i=1}^{g} \mathfrak{a}_i x_i$ avec $\mathfrak{a}_i$ un R-idéal fractionnaire et $x_i \in K$. Une spécificité du rang 1 est que le $\mathfrak{a}_1$, l'unique idéal fractionnaire intervenant dans l'écriture de L est inversible lorsque L est unimodulaire. Plus généralement, lorsque tous les $\mathfrak{a}_i$ sont inversibles (c'est le cas par exemple lorsque R est maximal) on dit que le module est *projectif*. Malheureusement, pour $g \geq 2$, tous les réseaux hermitiens unimodulaires ne sont pas projectifs et cela pose problème pour les classifier à partir de la classification des $\mathscr{O}_K$-réseaux que nous allons expliciter.

Classification des réseaux indécomposables unimodulaires sur $\mathscr{O}_K$

Dans ce paragraphe nous souhaitons aborder la classification des R-réseaux hermitiens unimodulaires (L,H) avec R un ordre maximal. C'est à dire que nous souhaitons obtenir un algorithme qui étant donné un ordre maximal R et un rang g renvoie un représentant de chaque classe d'isométrie de réseau hermitien unimodulaire sur R. Nous nous appuierons essentiellement sur les articles [Hof91], [Sch98] ainsi que sur l'habilitation de Markus Kirschmer [Kir16].

Le cadre placé par ces trois auteurs est très large [4], ils considèrent un réseau (L,H) hermitien sur un ordre $\mathscr{O}_K$ où $k \to K$ est une extension de degré 2 de corps de nombres et H est une forme hermitienne sur KL par rapport à l'unique automorphisme non trivial

4. Markus Kirschmer traite aussi le cas où $k = K$ et le cas où R est un ordre dans une algèbre de quaternions.

de $\mathrm{Gal}(K/k)$. Nous nous contenterons du cas où L est un réseau sur l'ordre maximal d'un corps quadratique imaginaire K (i.e. $k = \mathbb{Q}$). D'autre part, les auteurs classifient les réseaux $\mathfrak{a}$-modulaires pour un idéal $\mathfrak{a}$ de R. Nous ne nous intéressons qu'aux réseaux unimodulaires, i.e. pour $\mathfrak{a} = R$. Ceci permet de simplifier certains énoncés et donc de faciliter la lecture. Malgré toutes ces restrictions, nous ne détaillerons pas toutes les étapes de la méthode car ceci nous emmènerait trop loin.

Une première remarque facile est qu'une isométrie entre (L, H) et (L', H') induit une isométrie entre les espaces ambiants de chaque réseau. Il est donc tout naturel de commencer par la classification des espaces hermitiens (V, H).

Définition 1.2.6. *Soit (V, H) un espace hermitien sur un corps quadratique imaginaire K avec H définie positive. On définit le déterminant de (V, H), noté $\det(V, H)$ par la classe de $\det(G(b))$ dans $\mathbb{Q}^*/N(K)^*$ avec b une base quelconque de V.*

On peut alors citer le théorème suivant qui affirme que l'ensemble classes d'isométries des espaces hermitiens de dimension donnée sur un corps quadratique imaginaire K est paramétré par le groupe $\mathbb{Q}^*/N(K^*)$.

Théorème 1.2.7 (Classification des espaces hermitiens)**.** *Soient (V, H) un espace hermitien de dimension g sur K avec H définies positives. Alors (V, H) la classe d'isométrie de (V, H) est déterminée par*

- *sa dimension g*
- $\det(V, H) \in \mathbb{Q}^*/N(K)^*$.

En particulier, (V, H) est isomorphes à K^g muni de la forme hermitienne donnée par la matrice diagonale $\begin{pmatrix} 1 & & \mathbf{0} \\ & \ddots & \\ \mathbf{0} & & d \end{pmatrix}$ *où $d = \det(V, H) \in \mathbb{Q}^*/N(K^*)$.*

Démonstration. C'est une conséquence d'un théorème de principe local-global de Minkowski, Hasse, Landherr, Kneser et Springer (voir [Sch85, Theorem X.6.1]) qui affirme que deux espaces hermitiens sont isomorphes si, et seulement si, leurs localisés sont isomorphes en chaque place. Pour comprendre en détails en quoi il implique le théorème énoncé ci-dessus, voir [Kir16, Remark 3.4.2]). □

Dans [Hof91, Corollary 3.7] l'auteur montre qu'il existe une bijection entre l'ensemble des classes d'isométrie d'espaces hermitiens (V, H) qui contiennent un réseau hermitien

unimodulaire et le groupe quotient $\mathrm{Cl}(R)/\mathrm{Cl}(R)^2$ donnée par

$$(L,H) \subseteq (V,H) \longmapsto \mathrm{st}(L).$$

Ceci nous permet de déterminer efficacement au préalable quels espaces hermitiens nous intéressent.

On pourrait espérer avoir un principe local-global sur les réseaux hermitiens eux-mêmes pour pouvoir tester l'isométrie entre deux réseaux localement. Malheureusement, tester l'isométrie localement ne suffit pas. Prenons par exemple sur $R = \mathbb{Z}[i]$ les deux réseaux libres R^2 munis des formes hermitiennes définies par les matrices de Gram respectives

$$\begin{pmatrix} 1 & 0 \\ 0 & 5 \end{pmatrix} \text{ et } \begin{pmatrix} 2 & i \\ -i & 3 \end{pmatrix}.$$

Il existe une isométrie localement pour chaque place archimédienne ou non. Pourtant il n'existe pas d'isométrie globale entre les deux réseaux car le premier réseau est décomposable et le second ne l'est pas (ou car le premier représente 1 et pas le second).

On pose $\Omega \subseteq \mathbb{Z}$, l'ensemble des nombres premiers. Soit (V,H) un K-espace hermitien de dimension g. Pour tout $p \in \Omega$ on pose $K_p = K \otimes_{\mathbb{Q}} \mathbb{Q}_p$, $R_p = R \otimes_{\mathbb{Z}} \mathbb{Z}_p$ et $V_p = V \otimes_{\mathbb{Q}} \mathbb{Q}_p$. Si p est inerte ou ramifié dans K alors K_p est un corps, autrement $K_p \simeq \mathbb{Q}_p \times \mathbb{Q}_p$. L'ensemble V_p est toujours un K_p-module libre de rang g et on peut étendre H en l'unique forme hermitienne sur V_p toujours notée H vérifiant

$$\begin{aligned} H\colon \quad V_p \times V_p &\longrightarrow K_p \\ (v_1 \otimes \lambda_1, v_2 \otimes \lambda_2) &\longrightarrow H(v_1,v_2) \otimes \lambda_1\lambda_2. \end{aligned}$$

On appellera alors indifféremment espace hermitien sur anneau k un couple (W,H) de la forme (V,H) pour $k = K$ ou (V_p,H) pour $k = K_p$. On pose aussi le *groupe unitaire* et *spécial unitaire* d'un espace hermitien (W,H) sur k

$$U(W,H) = \{\alpha \in \mathrm{GL}(W,k)/\alpha \text{ isométrie}\} \text{ et } SU(W,H) = \{\alpha \in U(W,H), \det\alpha = 1\}.$$

Définition 1.2.8. *Soit (L,H) un réseau hermitien. On pose*

- $\mathrm{cl}(L) = \{M$ *réseau tel* $\exists \alpha \in U(V,H), L = \alpha M\}$
- $\mathrm{gen}(L) = \{M$ *réseau tel que* $\forall p \in \Omega, \exists \alpha_p \in U(V_p,H), L_p = \alpha_p M_p\}$

L'ensemble $\mathrm{gen}(L)$, appelé le *genre* de L, mesure à quel point le principe local-global

échoue pour le réseau L, on note alors $h(\mathrm{gen}(L))$ ou $h(L)$ son cardinal et on l'appelle le nombre de classes de L.

Nous reprenons la description de la *méthode du voisin* décrite dans les articles [Hof91] et [Sch98]. La différence essentielle entre les deux articles est le fait que dans [Hof91] l'auteur suppose que L est de rang impair [5] et que $\mathrm{Cl}(R)$ est d'exposant 2. Schiemann introduit un autre objet $\mathrm{gen}^0(L) \subseteq \mathrm{gen}(L)$ appelé le *genre spécial* de L qui satisfait $\mathrm{gen}^0(L) = \mathrm{gen}(L)$ sous les hypothèse de Hoffman. Cependant, il peut être intéressant de souligner que dans [Hof91] il y a beaucoup de schémas explicatifs illustrant le graphe des voisins d'un réseau, que nous verrons bientôt, qui facilitent grandement la compréhension de la méthode.

Définition 1.2.9 ($\mathfrak{p}$-voisin d'un réseau hermitien)**.** *Soit (L, H) un réseau hermitien entier de $V = KL$ et $\mathfrak{p}$ un idéal premier de R qui ne divise pas $\mathfrak{v}(L)$, le volume de (L, H).*

1. *Un réseau $M \subseteq V$ est un $\mathfrak{p}$-voisin de L si (M, H) est entier et il existe des isomorphismes de R-modules*

$$M/L \cap M \simeq R/\mathfrak{p} \text{ et } L/L \cap M \simeq R/\overline{\mathfrak{p}}.$$

2. *Un vecteur x est dit admissible si $x \in L \setminus \mathfrak{p}L$ et $N(\mathfrak{p})$ divise $H(x, x)$. Le $\mathfrak{p}$-voisin de L à un vecteur admissible x est*

$$L(\mathfrak{p}, x) = \mathfrak{p}^{-1}x + \{y \in L, H(x, y) \in \mathfrak{p}\}.$$

S'il n'y a pas d'ambiguïté sur l'idéal considéré on notera $L(x)$ au lieu de $L(\mathfrak{p}, x)$. On pose aussi $L_x = \{y \in L, H(x, y) \in \mathfrak{p}\}$.

Le [Sch98, Lemma 2.2] montre que les $\mathfrak{p}$-voisins d'un réseau L sont exactement les réseaux de la forme $L(x)$ pour un vecteur admissible x de L. D'autre part, les $\mathfrak{p}$-voisins de L ont le même volume que L et, puisque les $\mathfrak{p}$-voisins sont en plus entiers, alors ils sont unimodulaires lorsque L l'est.

Définition 1.2.10. *Soit (L, H) un réseau hermitien et $\mathfrak{p} \in K$. On pose*

$$\mathfrak{N}(L, \mathfrak{p}) = \{M \text{ réseau }, \exists \beta \in U(V, H), \exists L_0 = L, L_1, \ldots, L_m = \beta M \\ \text{tels que } L_i \text{ est un } \mathfrak{p}\text{-voisin de } L_{i+1}\}.$$

5. Ceci n'est pas une vraie restriction car en classifiant les réseaux hermitiens de rang m, il classifie aussi ceux de rang plus petit $n < m$ qui apparaissent comme facteurs dans la décomposition orthogonale des réseaux de rang m.

On définit aussi le graphe $NG(L, \mathfrak{p})$ *des* $\mathfrak{p}$*-voisins de* L *où les sommets sont* $\mathrm{cl}(M)$ *pour* $M \in \mathfrak{N}(L, \mathfrak{p})$ *et il existe une arête (orientée) d'un sommet* S_1 *vers un sommet* S_2 *s'il existe un représentant* M *de* S_1 *et un représentant* N *de* S_2 *tels que* N *est un* $\mathfrak{p}$*-voisin de* M*.*

Dans [Sch98, Section 4.1] l'auteur fournit une description précise de pseudo-bases du $\mathfrak{p}$-voisin d'un réseau L associé à un vecteur admissible x. Lorsque $\mathfrak{p} \cap \mathbb{Z} = p > 2$ et tel que $L_{\mathfrak{p}}$ est unimodulaire alors $\mathfrak{N}(L, \mathfrak{p}) \subseteq \mathrm{gen}(L)$. Par ailleurs, grâce à des résultats d'approximation forte, Shimura explique comme déterminer un ensemble fini S d'idéaux premiers décomposés de R tels que pour tout $L' \in \mathrm{gen}(L)$, il existe $\mathfrak{p} \in S$ tel que $L' \in \mathfrak{N}(L, \mathfrak{p})$ (voir [Shi64, Theorem 5.24 et proof 5.28]). Autrement dit, étant donné un réseau hermitien unimodulaire (L, H) il est possible de déterminer toutes les classes d'isométrie d'éléments de $\mathrm{gen}(L)$ uniquement en itérant des $\mathfrak{p}$-voisins de L sur un ensemble fini d'idéaux premiers connus au préalable.

On peut définir la *masse* de L définie par

$$\mathrm{Mass}(L) = \sum_{L' \in \mathrm{gen}(L)} \frac{1}{\#\,\mathrm{Aut}(L')}.$$

Cette quantité peut-être calculée uniquement à partir de *facteurs locaux* de L grâce aux valeurs de certaines L-séries (voir [Kir16, Theorem 4.2.3]). Ceci permet, à chaque nouveau $\mathfrak{p}$-voisin de L calculé non-isométrique à un réseau déjà connu de $\mathrm{gen}(L)$ de tester si on a déjà tous les éléments de $\mathrm{gen}(L)$ sans calculer tous les $\mathfrak{p}$-voisins successifs pour $\mathfrak{p} \in S$.

Nous savons donc qu'étant donné un réseau hermitien unimodulaire L on est capable de déterminer $\mathrm{gen}(L)$. Il reste à expliquer comment déterminer un tel réseau dans chaque genre d'un espace hermitien donné (V, H). On rappelle qu'on sait déterminer exactement quels espaces hermitiens contiennent un réseau unimodulaire. Il s'agit des espaces hermitiens K^g munis de la forme $\begin{pmatrix} 1 & & \mathbf{0} \\ & \ddots & \\ \mathbf{0} & & d \end{pmatrix}$ où $d = N(\mathfrak{a})$ pour $[\mathfrak{a}] \in \mathrm{Cl}(R)/\,\mathrm{Cl}(R)^2$. On peut alors construire le réseau $L_0 = R^{g-1} \oplus \mathfrak{a}^{-1}$ qui est unimodulaire dans (V, H). Dans [Jac62], Jacobowitz classifie les réseaux hermitiens sur les corps locaux. Sa classification implique qu'il n'existe qu'un ou deux genres de réseaux unimodulaires dans un K-espace hermitien. Lorsque le rang g est impair ou que K n'est pas dyadique (i.e. $2 \nmid \Delta$) alors il n'existe qu'un seul genre de réseaux unimodulaires dans (V, H) donné par $\mathrm{gen}(L_0)$ (voir [Jac62]). Si g est pair et K dyadique alors il peut exister un autre genre dont on peut

construire un représentant grâce aux invariants locaux [Kir16, Corollary 3.3.20].

Pour résumer, voici comment on procède pour classifier les réseaux hermitiens unimodulaires sur un ordre maximal.

1. On énumère tous les espaces hermitiens contenant un réseau hermitien unimodulaire. Ce sont exactement les espaces de la forme K^g munis de la forme hermitienne dont la matrice de Gram dans la base canonique est $\begin{pmatrix} 1 & & \mathbf{0} \\ & \ddots & \\ \mathbf{0} & & d \end{pmatrix}$ où $d = N(\mathfrak{a})$ pour $[\mathfrak{a}] \in \mathrm{Cl}(R)/\mathrm{Cl}(R)^2$.

2. Dans chaque espace hermitien construire un représentant par genre. On a toujours le représentant $L_0 = R^{g-1} \oplus \mathfrak{a}^{-1}$ mais il peut y en avoir un second genre si g pair et K dyadique que l'on détermine à l'aide d'invariants locaux.

3. Dans chaque genre construire les $\mathfrak{p}$-voisins successifs du réseau obtenu à l'étape précédente pour $\mathfrak{p} \in S$ où S est un ensemble fini d'idéaux premiers décrit par Shimura. Vérifier avec la formule des masses à chaque nouvelle classe d'isométrie si on a déjà énuméré toute le genre. Si oui, c'est terminé pour ce genre. Si non, choisir un idéal premier de S distinct de $\mathfrak{p}$ et réitérer l'opération précédente.

4. (Facultatif) Si on ne souhaite classifier que les réseaux indécomposables on peut les trier à posteriori parmi les réseaux unimodulaires classifiés.

Exemples de classifications à l'aide de la méthode des voisins

On donne quelques exemples pour illustrer cette classification.

Soit $R = \mathbb{Z}[\omega]$ avec $\omega = \frac{1+\sqrt{-15}}{2}$ l'ordre maximal de $K = \mathbb{Q}\left(\sqrt{-15}\right)$. Son nombre de classe est 2, plus précisément on a

$$\mathrm{Cl}(R) = \{[R], [\mathfrak{a}]\} \text{ avec } \mathfrak{a} = \langle 3, 1+\omega \rangle .$$

Il existe deux espaces hermitiens [6] K^g contenant au moins un réseau hermitien unimodu-

6. Il est intéressant de constater qu'il existe tout de même d'autres classes d'isométrie d'espaces hermitiens que ces deux là. Par exemple, celui donné par la matrice diagonale diag $\left(1, \ldots, \frac{1}{7}\right)$ n'est pas isométrique aux deux cités mais il ne contient pas de réseau unimodulaire d'après [Hof91, Corollary 3.7].

laire. Ces espaces sont donnés par les matrices hermitiennes

$$I_g = \begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{pmatrix} \text{ et } D_g\left(\frac{1}{3}\right) = \begin{pmatrix} 1 & & \\ & \ddots & \\ & & \frac{1}{3} \end{pmatrix}$$

car $N(\mathfrak{a}) = 3$ et deux représentants de genre de ces espaces sont les réseaux donnés par $L_0 = R^g$ et $L_\mathfrak{a} = R^{g-1} \oplus \mathfrak{a}$ respectivement. On sait par ailleurs qu'il n'y a pas d'autre genre dans ces espaces car K n'est pas dyadique ($\Delta = -3 \times 5$). Il suffit alors d'appliquer la méthode des voisins pour chacun d'eux pour déterminer toutes les classes d'isométries pour chaque genre.

Prenons $g = 2$ et $\mathfrak{p} = \langle 17, 5 + \omega \rangle$ et commençons par le réseau L_0 (le cas libre). On note e_1, e_2 la base canonique de K^2. La masse du réseau L_0 est $\frac{1}{4}$ et le groupe $\mathrm{Aut}(L_0)$ des automorphismes de L_0 est engendrée par les isométries $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ et $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ et a donc pour cardinal 8. On calcule 6 $\mathfrak{p}$-voisins de L_0 mais dans ceux-ci il n'y a qu'une seule classe d'isométrie différente de celle de L_0. Il s'agit du réseau L_0' donné par $Ru_1 \oplus Ru_2$ où $u_1 = e_1$ et $u_2 = (-3 - 2\omega)e_1 + e_2$. On peut calculer le cardinal du groupe des automorphismes de L_0' et on trouve 8. Puisque

$$\frac{1}{8} + \frac{1}{8} = \frac{1}{4} = \mathrm{Mass}(L_0)$$

on sait qu'on a identifié toutes les classes d'isométrie de réseaux unimodulaires de $\mathrm{gen}(L)$ et donc de l'espace hermitien (K^2, I_2) (encore une fois car K n'est pas dyadique).
Considérons maintenant $L_\mathfrak{a} = R \oplus \mathfrak{a}$ dans l'espace $\left(K^2, D_2\left(\frac{1}{3}\right)\right)$. Sa masse est $\frac{1}{3}$ et son groupe des automorphismes est d'ordre 4. On trouve encore 10 $\mathfrak{p}$-voisins de $L_\mathfrak{a}$ qui ne comptent qu'une seule classe d'isométrie différente de celle de $L_\mathfrak{a}$. On la note $L_\mathfrak{a}'$. Son groupe des automorphismes est d'ordre 12, or

$$\frac{1}{4} + \frac{1}{12} = \frac{1}{3} = \mathrm{Mass}(L_\mathfrak{a}).$$

On peut donc en conclure qu'il existe deux espaces hermitiens contenant des réseaux hermitiens unimodulaires. Chaque espace ne contient qu'un seul genre. Deux représentants des genres sont donnés par L_0 et $L_\mathfrak{a}$ et $\mathrm{gen}(L_0) = \{\mathrm{cl}(L_0), \mathrm{cl}(L_0')\}$ et $\mathrm{gen}(L_\mathfrak{a}) = \{\mathrm{cl}(L_\mathfrak{a}), \mathrm{cl}(L_\mathfrak{a}')\}$. Les réseaux L_0 et $L_\mathfrak{a}$ sont évidemment décomposables et c'est aussi

le cas de L'_0. En revanche, le réseau $L'_{\mathfrak{a}}$ est lui indécomposable. On en conclue qu'il existe une unique classe de réseau hermitien unimodulaire indécomposable de rang 2 sur $R = \mathbb{Z}\left[\frac{1+\sqrt{-15}}{2}\right]$. La lectrice curieuse pourra comparer ce processus à [Hof91, Figure 5] (l'auteur traite le cas $g = 3$ mais celui-ci implique le cas $g = 2$ que nous venons de traiter car les réseaux $L_0, L'_0, L_{\mathfrak{a}}$ et $L'_{\mathfrak{a}}$ interviennent dans la décomposition orthogonale des réseaux de rang 3).

Prenons un autre exemple, celui de $R = \mathbb{Z}[\omega]$ avec $\omega = \sqrt{-14}$ dans $K = \mathbb{Q}\left(\sqrt{-14}\right)$ de discriminant $4 \times -14 = -56$. On a $\mathrm{Cl}(R) \simeq \mathbb{Z}/4\mathbb{Z}$, engendré par la classe de $\mathfrak{a} = \langle 3, 1+\omega\rangle$. On a alors $\mathrm{Cl}(R)/\mathrm{Cl}(R)^2 \simeq \mathbb{Z}/2\mathbb{Z}$ (toujours engendré par la classe de $\mathfrak{a}$), il y a donc deux classes d'isométrie d'espaces hermitiens contenant chacun au moins un réseau unimodulaire. Le corps K est dyadique et il peut donc y avoir deux genres distincts par espace hermitien lorsque ce dernier est de dimension paire. Des classes d'isométrie des espaces hermitiens en question sont données par les matrices

$$I_g = \begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{pmatrix} \text{ et } D_g\left(\frac{1}{3}\right) = \begin{pmatrix} 1 & & \\ & \ddots & \\ & & \frac{1}{3} \end{pmatrix}.$$

Commençons par le premier espace. On pose $\mathfrak{p} = \langle 5, 1+\omega\rangle$. Il s'agit d'un idéal premier de R non ramifié. On considère $L_0 = R^2$ de masse $\frac{3}{2}$ et dont le groupe des automorphismes est d'ordre 8. Il a 3 $\mathfrak{p}$-voisins qui représentent tous des classes d'isométrie distinctes de $\mathrm{cl}(L_0)$. Si on regarde la somme des inverses de l'ordre de leurs groupes d'automorphismes respectifs on a

$$\frac{1}{8} + \frac{1}{8} + \frac{1}{4} + \frac{1}{4} = \frac{3}{4} < \frac{3}{2}.$$

Ces trois classes supplémentaires ne suffisent donc pas à obtenir tous les représentants de $\mathrm{gen}(L_0)$. En considérant les $\mathfrak{p}$-voisins des nouvelles classes obtenues on trouve trois nouvelles classes distincte des 4 précédentes telles que

$$\sum \frac{1}{\#\,\mathrm{Aut}\,(L)} = \frac{3}{4} + \frac{5}{8} = \frac{11}{8} < \mathrm{Mass}(L)$$

où la somme est prise sur les classes d'isométrie obtenue en considérant les $\mathfrak{p}$-voisins de L_0 puis les $\mathfrak{p}$-voisins de des derniers. En itérant une fois de plus on trouve un dernier réseau dont le groupe des automorphismes est de cardinal 8. Puisque $\frac{11}{8} + \frac{1}{8} = \frac{3}{2}$ il s'agit de la

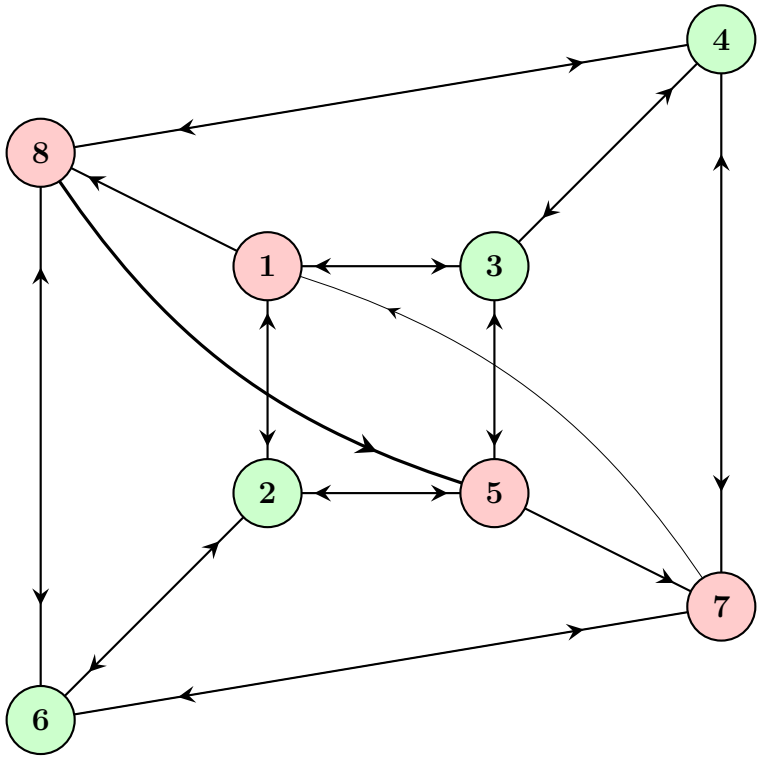


FIGURE 1.1 – Graphe des $\left\langle 5, 1+\sqrt{-14}\right\rangle$-voisins correspondant au réseau L_0 dans l'espace $\left(\mathbb{Q}\left(\sqrt{-14}\right)^2, I_2\right)$.

classe d'isométrie manquante.

Pour illustrer cet exemple j'ai représenté le graphe des voisins dans la Figure 1.1. Chaque sommet correspond à la classe d'isométrie d'un réseau du genre de L_0 et L_0 est représenté par le sommet 1. Si le réseau j est un $\mathfrak{p}$-voisin du sommet i alors on relie i et j par une arête orientée de i vers j. Par exemple, puisque le réseau L_0 a trois voisins distincts, le sommet 1 pointe vers 3 sommets distincts ; ce sont les réseaux correspondants aux sommets $2, 3$ et 8. En calculant les $\mathfrak{p}$-voisins des réseaux $2, 3$ et 8 on obtient les réseaux $4, 5$ et 6. Le réseau manquant est le réseau 7 qu'on obtient en itérant une fois de plus. Les couleurs des sommets correspondent au cardinal du groupe des automorphismes du réseau (cardinal 8 pour rouge et 4 pour vert). Un phénomène qui peut se produire mais qui n'apparaît pas dans cet exemple est le fait qu'un réseau peut être isométrique à un de ses $\mathfrak{p}$-voisins.

Il existe un autre genre que $\mathrm{gen}(L_0)$ dans l'espace hermitien (K^2, I_2), dont les normes de tous les éléments des réseaux sont paires. Ceci n'est possible que parce que $g = 2$ et K

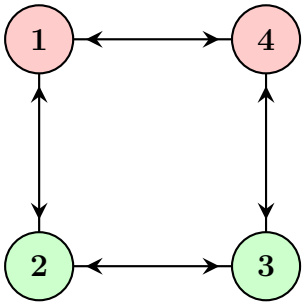


FIGURE 1.2 – Graphe des $\left\langle 5, 1+\sqrt{-14}\right\rangle$-voisins correspondant aux réseaux pairs dans l'espace $\left(\mathbb{Q}\left(\sqrt{-14}\right)^2, I_2\right)$.

dyadique. La masse de ce genre est

$$\frac{1}{8}+\frac{1}{8}+\frac{1}{4}+\frac{1}{4}=\frac{3}{4}.$$

Son graphe des voisins est représenté par le graphe de la Figure 1.2, beaucoup plus simple que le précédent (même code couleur).

On peut faire la même chose pour l'autre espace hermitien et on trouve alors encore deux genres composés deux 8 classes d'isométries pour le genre correspondant au réseau $R \oplus \mathfrak{a}$ et 4 classes pour le genre correspondant aux réseaux pairs.

On a donc obtenu les 32 classes d'isométrie des réseaux hermitiens unimodulaires. Il n'en existe pas d'autres. On peut trier les réseaux hermitiens qui sont décomposables de ceux qui ne le sont pas. On trouve alors un total de 14 classes d'isométrie de réseaux hermitiens unimodulaires indécomposables de rang 2 sur $\mathbb{Z}\left[\sqrt{-14}\right]$.

Même si ça n'arrive pas dans tous les exemples traités ici, il est possible que le graphe des $\mathfrak{p}$-voisins d'un réseau L ne représente pas la totalité de $\mathrm{gen}(L)$ auquel cas il faut choisir un autre idéal premier et déterminer son graphe des voisins.

1.2.4 Réseaux sur un ordre quelconque R

Pseudo-bases et classes de Steinitz

À l'instar des réseaux sur un anneau de Dedekind, les R-réseaux L sur un ordre quadratique dans K admettent une pseudo-base et on peut décrire leur classe de R-isomorphisme grâce à des invariants. Plus précisément, on a la proposition suivante (voir [BF60] pour une démonstration pour R un ordre quadratique ou [LW85, Theorem 7.1]

pour une généralisation aux *ordres de Bass* dont les idéaux admettent 2 générateurs).

Proposition 1.2.11. *Soit R un ordre dans un corps quadratique imaginaire K. Soit L un réseau sur R alors*

1. *Il existe des R-idéaux fractionnaires $\mathfrak{a}_1, \dots, \mathfrak{a}_g$ et une base $x_1, \dots, x_g$ de KL tels que*

$$L = \mathfrak{a}_1 x_1 \oplus \cdots \oplus \mathfrak{a}_g x_g \text{ et } R_{\mathfrak{a}_1} \subseteq \cdots \subseteq R_{\mathfrak{a}_g}.$$

2. *La classe d'isomorphisme de L est uniquement déterminée par la famille d'ordres $(R_{\mathfrak{a}_1}, \dots, R_{\mathfrak{a}_g})$ ainsi que par la classe du produit $\mathfrak{a}_1 \cdots \mathfrak{a}_g$ dans $\mathrm{Pic}(R_{\mathfrak{a}_g})$.*

Une famille telle $(\mathfrak{a}_i, x_i)$ telle que $L = \mathfrak{a}_1 x_1 \oplus \cdots \oplus \mathfrak{a}_g x_g$ et $R_{\mathfrak{a}_1} \subseteq \cdots \subseteq R_{\mathfrak{a}_g}$ est appelée une pseudo-base de L. L'existence de pseudo-bases permet de généraliser un certain nombre d'expressions de la Proposition 1.2.4 aux ordres non-maximaux. Il faut tout de même faire attention au fait que lorsque $\mathfrak{a} \subseteq R$ est un idéal fractionnaire non inversible alors l'identité $\mathfrak{a}\overline{\mathfrak{a}} = N(\mathfrak{a})R$ n'est jamais satisfaite (en revanche on a $\mathfrak{a}\overline{\mathfrak{a}} = N_{R_\mathfrak{a}}(\mathfrak{a})R_\mathfrak{a} = f_\mathfrak{a} N_R(\mathfrak{a})R_\mathfrak{a}$ d'après la Proposition 1.1.17).

Classification des réseaux hermitiens unimodulaires sur R

La classification des réseaux hermitiens unimodulaires (L, H) sur un ordre non-maximal R dans K est décrite en détails dans [KNRR21, Section 2.2]. Elle utilise la classification des réseaux hermitiens $\mathfrak{a}$-modulaires sur $\mathscr{O}_K$ que nous n'avons traité que pour le cas $\mathfrak{a} = R$. C'est pourquoi nous ne la décrirons pas précisément ici. Cependant, nous allons brièvement discuter de cette classification en nous restreignant aux réseaux L dits *projectifs*. On dit que L est projectif s'il existe une pseudo-base

$$L = \mathfrak{a}_1 x_1 \oplus \cdots \oplus \mathfrak{a}_g x_g$$

telle que tous les idéaux fractionnaires $\mathfrak{a}_i$ sont inversibles dans R. Il s'agit des réseaux L tels que la famille d'ordres satisfait $R_1 = R_2 = \cdots = R_g = R$.

Considérons (L, H) un R-réseau hermitien $\mathfrak{a}$-modulaire avec L projectif. Alors le $\mathscr{O}_K$-réseau $M = \mathscr{O}_K L$ est $\mathfrak{a}\mathscr{O}_K$-modulaire. En effet,

$$H(M, M) = \mathscr{O}_K \overline{\mathscr{O}_K} H(L, L) = \mathfrak{a}\mathscr{O}_K.$$

Par ailleurs,

$$\begin{aligned}
\mathfrak{v}(M) &= N_{\mathscr{O}_K}(\mathfrak{a}_1 \cdots \mathfrak{a}_g \mathscr{O}_K) \det(G(x_1, \ldots, x_g))\mathscr{O}_K && \text{Proposition 1.2.4.(2)} \\
&= N_R(\mathfrak{a}_1 \ldots \mathfrak{a}_g) \det(G(x_1, \ldots, x_g))\mathscr{O}_K && \text{Proposition1.1.17.(5)} \\
&= \mathfrak{v}(L)\mathscr{O}_K \\
&= \mathfrak{a}^g \mathscr{O}_K \\
&= (\mathfrak{a}\mathscr{O}_K)^g.
\end{aligned}$$

Ceci prouve, d'après la Proposition 1.2.4.(6), que M est bien $\mathfrak{a}\mathscr{O}_K$-modulaire. Il est intéressant de remarquer que ce n'est jamais vrai lorsque L n'est pas projectif. En effet, on a alors $\mathfrak{a}_g$ est un idéal fractionnaire inversible de $R_g = R_{\mathfrak{a}_g}$ et $R \subsetneq R_g$. On note $f_{\mathfrak{a}_g}$ le conducteur de R dans $R_{\mathfrak{a}_g}$. Ainsi, en appliquant les points (4) et (5) de la Proposition 1.1.17 on a

$$N_{\mathscr{O}_K}(\mathfrak{a}_1 \cdots \mathfrak{a}_g) = N_{R_g}(\mathfrak{a}_1 \cdots \mathfrak{a}_g) = f_{\mathfrak{a}_g} \cdot N_R(\mathfrak{a}_1 \cdots \mathfrak{a}_g) > N_R(\mathfrak{a}_1 \cdots \mathfrak{a}_g)$$

si bien que lorsque L n'est pas projectif il ne suffit pas d'énumérer les $\mathscr{O}_K$-réseaux unimodulaires M et de chercher à partir de ceux-ci les R-réseaux L qui sont unimodulaires comme nous l'avons fait dans [KNRR21, Algorithme 3]. On peut tout de même affirmer, même dans le cas non projectif, que M est toujours entier et on a des inclusions

$$fM^{\#,\mathscr{O}_K} \subseteq L \subseteq M,$$

où f est le conducteur de R dans $\mathscr{O}_K$ et $M^{\#,\mathscr{O}_K} = \{v \in K, H(v, M) \subseteq \mathscr{O}_K\}$. Ces inclusions nous permettent de réduire les $\mathscr{O}_K$-réseaux $M = \mathscr{O}_K L$ à un ensemble fini qui nous sert ensuite à retrouver les L dans le cas non-projectif ([KNRR21, Lemma 2.12 et Algorithm 2]).
Malheureusement, cela se fait au prix d'un temps de calcul bien plus coûteux que pour le cas projectif mais nous avons bon espoir qu'il existe des améliorations conséquentes de [KNRR21, Algorithm 2].

Chapitre 2
VARIÉTÉS ABÉLIENNES

Dans cette section nous souhaitons présenter le matériel nécessaire à la compréhension des variétés abéliennes avec lesquelles nous souhaitons travailler ; les variétés abéliennes isogènes à un produit de courbes elliptiques. Nous commencerons naturellement dans la Section 2.1 par l'étude des variétés abéliennes sur un corps quelconque où nous définirons les variétés abéliennes, leur *duale*, les *polarisations* et des constructions de variétés abéliennes polarisées particulières ; les *jacobiennes* de courbes.

Bien que cela ne semble pas intuitif au premier abord, la lectrice qui ne souhaite pas s'encombrer du formalisme des variétés abéliennes quelconques pourra passer directement à la Section 2.2 qui traite du cas particulier des variétés abéliennes sur le corps des nombres complexes. Bien entendu, nous y parlerons de variétés abéliennes, de duales et de polarisations définies dans la Section 2.1. Cependant, les variétés abéliennes complexes sont équivalentes à la catégorie des *tores complexes* dits *polarisables* qui offrent une interprétation de tous ces objets en termes d'algèbre linéaire complexe. On pourra alors penser à une variété abélienne complexe A comme un quotient V/Γ d'un espace vectoriel complexe de dimension finie par un $\mathbb{Z}$-réseau de V, à la variété abélienne duale $\widehat{A}$ comme au tore dual $V^*/\widehat{\Gamma}$ où V^* désigne l'espace des formes antilinéaire de V et $\widehat{\Gamma} = \{\ell \in V^*, \operatorname{im} \ell(\Gamma) \subseteq \mathbb{Z}\}$ et à une polarisation a sur A comme à une forme hermitienne h sur V ayant de bonnes propriétés sur le réseau Γ ($\operatorname{im} h(\Gamma, \Gamma) \subseteq \mathbb{Z}$). Nous commencerons par une étude générale des tores complexes dans la Section 2.2.1 puis nous présenterons spécifiquement les tores de dimension 1 et nous verrons qu'ils correspondent aux courbes elliptiques complexes dans la Section 2.2.2. Dans le but d'étendre l'équivalence nous présenterons l'étude des fonctions thêta dans la Section 2.2.3 et nous verrons comment les *thêta constantes* permettent de paramétrer l'espace de modules des variétés abéliennes d'un type fixé. Enfin, nous aborderons spécifiquement l'étude des variétés abéliennes complexes isogènes à un produit de courbes elliptiques à multiplication complexe par un même corps quadratique

K dans la Section 2.2.4. Nous verrons que dans ce cas particulier on peut raffiner l'équivalence avec les tores complexes et que les réseaux Γ intervenant dans le quotient V/Γ de tels variétés peuvent être munis d'une structure de R-module où R est un ordre dans K. Nous verrons alors de nouvelles équivalences de catégories qui permettent de décrire ces variétés et leur polarisation dans un cadre plus général que celui de [Nar22] (où nous nous restreignons aux courbes elliptiques à multiplication complexe par un ordre maximal R).

Dans la Section 2.3 nous abordons l'étude des variétés abéliennes sur les corps finis. Bien qu'à l'instar des complexes il existe des équivalences de catégories spécifiques aux corps finis (voir [CS21]). Les objets équivalents sont bien moins intuitifs que dans le cas des nombres complexes. Nous énoncerons tout de même une équivalence de catégories entre certaines variétés abéliennes sur les corps finis et certains réseaux qui n'est pas celle de [CS21] mais une autre plus spécifique aux objets que nous souhaitons étudier. Il s'agit de l'équivalence définie initialement par Serre dans [Ser20] reprise à la lumière de [JKP$^+$18]. Elle ne concerne que les variétés abéliennes isogènes à un produit de courbes elliptiques contrairement à celle développée dans [CS21] qui est définie pour toutes les variétés abéliennes sur les corps finis.

Nous nous référerons à [Mil08], [Mum70] et [SC86] pour la théorie des variétés abéliennes sur un corps quelconque. Pour la théorie sur $\mathbb{C}$ nous nous référerons principalement à [Deb05] et [BL94]. Concernant les variétés abéliennes sur les corps finis nous nous appuierons principalement sur [Rit17].

2.1 Variétés abéliennes sur un corps quelconque

2.1.1 Définitions et propriétés générales

Définition 2.1.1. *Une variété abélienne A sur un corps k est une variété algébrique complète, connexe et géométriquement réduite munie d'une structure de groupe $+$ telle que les opérations*

$$A \times A \to A, (x, y) \mapsto x + y \text{ et } A \to A, x \mapsto -x$$

sont des morphismes de variétés.

La lectrice attentive aura constaté que, bien qu'on parle de variétés *abéliennes* et que je me sois permis de noter « $+$ » la loi de groupe d'une variété abélienne quelconque, aucune hypothèse de commutativité n'est mentionné dans la définition. C'est, en effet,

une conséquence des hypothèses qu'on impose à ces objets. Nous énonçons des propriétés essentielles dont on pourra trouver une démonstration dans [Mum70, II.Question 4.(i) et (ii)] et [Mil08, Theorem 6.4].

Proposition 2.1.2. *Soit A une variété abélienne sur un corps k. Alors*

— *La variété sous-jacente est projective et lisse en tout point.*

— *Le groupe sous-jacent est commutatif.*

Un morphisme de variété $f\colon A \to B$, où A et B sont des variétés abéliennes de même dimension g est appelé une *isogénie* si c'est un morphisme surjectif ou de manière équivalente si son noyau est fini. On appelle *degré* de l'isogénie f, noté $\deg f$, le cardinal de son noyau en tant que schéma en groupe [1]. Un exemple important d'isogénies est la multiplication par n, noté $[n]_A\colon A \longrightarrow A$. Lorsque $\operatorname{char} k \nmid n$ on a $\ker[n]_A \simeq (\mathbb{Z}/n\mathbb{Z})^{2g}$. En particulier, $\deg[n]_A = n^{2g}$.

2.1.2 Variété abélienne duale et polarisations

On rappelle qu'un *faisceau inversible* $\mathscr{L}$ sur une variété $(X, \mathcal{O}_X)$ est un $\mathcal{O}_X$-module localement libre de rang 1. Étant donnés deux faisceaux inversibles $\mathscr{L}_1$ et $\mathscr{L}_2$ on peut définir un nouveau faisceau inversible $\mathscr{L}_1 \otimes \mathscr{L}_2$ et pour tout $\mathscr{L}$ il existe un faisceau inversible $\mathscr{L}^{-1}$ tel qu'on ait un isomorphisme de $\mathcal{O}_X$-modules $\mathscr{L} \otimes \mathscr{L}^{-1} \simeq \mathcal{O}_X$ (voir [Har77, Proposition 6.12] par exemple). Ceci permet de définir le *groupe de Picard* de X, noté $\operatorname{Pic}(X)$, comme l'ensemble des classes d'isomorphisme de faisceaux inversibles sur X.

Étant donné un faisceau inversible $\mathscr{L}$ sur une variété Y et un morphisme $f\colon X \longrightarrow Y$, on peut définir le faisceau inversible $f^*\mathscr{L}$ sur X par $f^*\mathscr{L} = f^{-1}\mathscr{L} \otimes_{f^{-1}\mathcal{O}_Y} \mathcal{O}_X$ où $f^{-1}\mathscr{L}(U) = \varinjlim_{f(U)\subseteq V} \mathscr{L}(V)$ qui est naturellement un $f^{-1}\mathcal{O}_Y$-module et le morphisme $f^{-1}\mathcal{O}_Y \to \mathcal{O}_X$ induit aussi une structure de $f^{-1}\mathcal{O}_Y$-module sur $\mathcal{O}_X$.

Par exemple, si A est une variété abélienne sur k, qu'on considère le morphisme de translation par un élément $x \in A(k)$,

$$\begin{array}{rccc} t_x\colon & A & \longrightarrow & A \\ & z & \longmapsto & z + x \end{array}$$

1. Il est possible que, pour des isogénies inséparables, les points de $\ker f$ ne soient pas fermés. Il faut donc considérer le schéma en groupe $\ker f$ et pas seulement ses points $\ker(f)\,(\overline{k})$.

et $\mathscr{L}$ un faisceau inversible sur A alors $t_x^{-1}\mathscr{L}(U) = \mathscr{L}(U-x)$ et on a

$$\begin{aligned} t_x^{-1}\mathcal{O}_A(U) = \mathcal{O}_A(U-x) &\longrightarrow \mathcal{O}_A(U) \\ u &\longmapsto (z \mapsto u(z+x)). \end{aligned}$$

où les éléments de $\mathcal{O}_A(U-x)$ sont considérés comme des fonctions pour des ouverts affines U.

Un théorème central dans l'étude des variétés abéliennes est le suivant qu'on retrouvera dans [SC86, Theorem V.6.7].

Théorème 2.1.3 (Théorème du carré)**.** *Soit $\mathscr{L}$ un faisceau inversible sur une variété abélienne A sur k et $x, y \in A(k)$ alors,*

$$t_{x+y}^*\mathscr{L} \otimes \mathscr{L} \simeq t_x^*\mathscr{L} \otimes t_y\mathscr{L}.$$

L'application définie par

$$\begin{aligned} \phi_{\mathscr{L}}\colon \quad A(k) &\longrightarrow \operatorname{Pic}(A) \\ x &\longmapsto t_x^*\mathscr{L} \otimes \mathscr{L}^{-1} \end{aligned}$$

est un morphisme de groupes car

$$\phi_{\mathscr{L}}(x+y) = t_{x+y}^*\mathscr{L}\otimes\mathscr{L}^{-1} \simeq \left(t_x^*\mathscr{L} \otimes t_y\mathscr{L} \otimes \mathscr{L}^{-1}\right)\otimes\mathscr{L}^{-1} = (t_x^*\mathscr{L}\otimes\mathscr{L}^{-1})\otimes(t_y^*\mathscr{L}\otimes\mathscr{L}^{-1}).$$

La définition précise de la *variété abélienne duale* $\widehat{A}$ de A peut être trouvée dans [SC86, Chapter V.§9]. Il s'agit d'une variété abélienne de dimension $\dim A$ telle que pour tout corps K on a $\widehat{A}(K) = \operatorname{Pic}^0(A_K)$ où $\operatorname{Pic}^0(A)$ est l'ensemble des classes d'isomorphisme de faisceaux inversibles $\mathscr{L}$ tels que $\forall x \in A\left(\overline{k}\right), t_x^*\mathscr{L} \simeq \mathscr{L}$. Cette variété $\widehat{A}$ satisfait les propriétés qu'on attend d'un dual, à savoir que son dual, le bidual de A, est canoniquement isomorphe à A. Par ailleurs, à tout morphisme $f\colon A \to B$ on peut associer un morphisme $\widehat{f}\colon \widehat{B} \longrightarrow \widehat{A}$ dit *dual* tel que son dual est exactement f sous l'identification canonique de A et B avec leur biduaux.

On définit alors une *polarisation* a sur A comme un morphisme $a\colon A \to \widehat{A}$ tel que $a_{\overline{k}} = \phi_{\mathscr{L}}$ où $\mathscr{L}$ est un faisceau inversible ample sur $A_{\overline{k}}$. Il s'agit toujours d'une isogénie et le degré de la polarisation est son degré en tant qu'isogénie. Lorsqu'une polarisation a est de degré 1, i.e. elle définit un isomorphisme entre A et sa duale, alors la polarisation est dite *principale*. Un couple (A, a) formé d'une variété abélienne A et d'une polarisation

a sur A est appelé *variété abélienne polarisé*. On dit qu'un morphisme entre variétés abéliennes $f\colon A \to B$ est polarisée pour des polarisations a de A et b de B si $a = \widehat{f}bf$, i.e. si le diagramme suivant commute

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \downarrow{\scriptstyle a} & & \downarrow{\scriptstyle b} \\ \widehat{A} & \xleftarrow[\widehat{f}]{} & \widehat{B}. \end{array}$$

Puisque la polarisation a est une isogénie alors f doit aussi en être une. On dit alors que $f\colon (A,a) \longrightarrow (B,b)$ est une isogénie polarisée pour simplifier.

Une variété abélienne polarisée (A,a) est dite décomposable s'il existe deux variétés abéliennes polarisées (A_1,a_1) et (A_2,a_2) de dimension ≥ 1 et un isomorphisme polarisée $(A,a) \to (A_1,a_1) \times (A_2,a_2)$.

2.1.3 Jacobiennes de courbes algébriques

La variété jacobienne

Le langage des faisceaux inversibles est commode pour définir les polarisations et la variété abélienne duale mais ils ne sont malheureusement pas très intuitifs à manipuler. Lorsqu'on manipule des variétés algébriques projectives, leur groupe des faisceaux inversibles est isomorphe à leur groupe des *diviseurs de Weil* que nous allons définir. Ces derniers offrent donc un outil similaire au faisceaux inversibles mais ont l'avantage d'être très intuitifs sur des courbes. Plutôt que de rentrer dans les détails techniques de concepts déjà très documentés j'ai préféré, dans cette section, développé des exemples pour illustrer les objets définis à la lumière des résultats cités. La lectrice curieuse pourra se référer à [Har77, Section II.6] pour une étude détaillée des diviseurs et des faisceaux inversibles et [SC86, Chapter VII] pour plus de détails sur les variétés jacobiennes.

Définition 2.1.4. *Soit C une courbe algébrique*[2] *sur k. Un diviseur de Weil*[3] *sur C est une somme formelle $D = \sum_i n_i P_i, n_i \in \mathbb{Z}$ de points fermés de C tel que* $\mathrm{Supp}(D) = \{i, n_i \neq 0\}$*, le support de D, est fini. Le degré de D, noté* $\deg D$*, est défini par $\sum_i n_i \in \mathbb{Z}$.*

2. On appelle courbe algébrique une variété algébrique projective lisse de dimension 1.

3. Les diviseurs de Weil sont définis plus généralement sur schéma noethériens intègres et séparés réguliers comme des sommes formelles de fermés de codimension 1 mais leur manipulation est moins intuitive et nous ne les aborderons que de manière détournée et sans les nommer dans la Section 2.1.3.

Lorsque $n_i \geq 0$ pour tout i, le diviseur est dit effectif, on notera alors $D \geq 0$ et $D \geq D'$ signifiera que $D - D' \geq 0$.

On pose $\mathrm{Div}(C)$ *le groupe des diviseurs de* C.

Pour tout P point fermé de C l'anneau $\mathcal{O}_{C,P}$ est un anneau local à valuation discrète, c'est à dire qu'il ne possède qu'un seul idéal maximal et ce dernier est principal. On pose $t_P \in \mathcal{O}_{C,P}$ une uniformisante de l'anneau, i.e. un générateur de l'unique idéal maximal $\mathfrak{m}_P$ de $\mathcal{O}_{C,P}$. Pour tout $f \in k(C), P \in C$ et $P \in U$ ouvert, on peut écrire $f = \frac{f_1}{f_2}$ car $k(C) = \mathrm{Frac}(\mathcal{O}_C(U))$ on pose $v_P(f) \in \mathbb{Z}$ l'entier $n - d$ où $\langle f_{1,P} \rangle = \mathfrak{m}_P^n$ et $\langle f_{2,P} \rangle = \mathfrak{m}_P^d$, appelé la valuation de f en P. Cet entier ne dépend ni des représentants f_1, f_2 choisis, ni de l'ouvert U. Il s'agit de l'unique entier m satisfaisant $f = ut^m \in \mathrm{Frac}\,(\mathcal{O}_{C,P})$ avec u inversible dans $\mathcal{O}_{C,P}$. Lorsque $v_P(f) < 0$ on dit que f a un *pôle* d'ordre $v_P(f)$ en P et si $v_P(f) < 0$ on dit que f a un *zéro* d'ordre $v_P(f)$ en P. On pose alors

$$\mathrm{div}(f) = \sum_P v_P(f)P.$$

Puisque $\{P / v_P(f) \neq 0\}$ est fini (voir [Har77, Lemma II.6.1]), $\mathrm{div}(f)$ est un diviseur appelé *diviseur principal*. On pose alors la relation d'équivalence $D \sim D'$ s'il existe $f \in k(C)$ tel que $D - D' = \mathrm{div}(f)$, deux tels diviseurs sont dits *linéairement équivalents*. On pose $\mathrm{Cl}(C)$, le *groupe des classes de diviseurs*, le quotient de $\mathrm{Div}(C)$ par le sous-groupe engendré par les diviseurs principaux. Tous les diviseurs principaux sont de degré 0 (ils ont autant de pôle que de zéros comptés avec l'ordre de multiplicité). Par conséquent, le morphisme $\deg\colon \mathrm{Cl}(C) \to \mathbb{Z}$ est bien défini (voir [Har77, Corollary 6.10]). La prochaine proposition établit le lien entre les diviseurs de Weil et les faisceaux inversibles (voir [Har77, Proposition II.6.11 et Proposition II.6.13] pour une discussion plus complète incluant les *diviseurs de Cartier*, ou [Vak, Proposition 1.4] sans les diviseurs de Cartier).

Pour un diviseur $D = \sum n_P P$ on peut définir un faisceau inversible $\mathscr{L}(D)$ par

$$\mathscr{L}(D)(U) = \{f \in k(U), D_{|U} + \mathrm{div}(f) = \sum_{P \in U} n_P P + \sum v_P(f)P \geq 0\}.$$

Proposition 2.1.5. *Soit C une courbe. L'application*

$$\begin{aligned} \mathrm{Div}(C) &\longrightarrow \mathrm{Pic}(C) \\ D &\longmapsto \mathscr{L}(D) \end{aligned}$$

définit un isomorphisme de groupes.

On se permettra donc de confondre $\mathrm{Div}(C)$ et $\mathrm{Pic}(C)$. En particulier, on considérera $D = \sum n_P P$ tel que $\sum n_P = 0$ comme un élément de $\mathrm{Pic}^0(C)$.

Étant donné un morphisme fini entre deux courbes $\varphi\colon C \longrightarrow C'$ on pose

$$\varphi^* Q = \sum_{\varphi(P)=Q} v_P(t) P$$

où t est l'image d'une uniformisante de $k(C')$ en Q dans $k(C)$. On peut alors définir $\varphi^* \sum n_Q Q = \sum n_Q \varphi^* Q$ qui permet de définir un morphisme

$$\varphi^*\colon \mathrm{Div}(C') \longrightarrow \mathrm{Div}(C).$$

Par ailleurs, $\varphi^* \operatorname{div} f = \operatorname{div} \varphi^{\#} f$ où $\varphi^{\#}\colon \mathcal{O}_{C'} \to \mathcal{O}_C$. Donc le morphisme passe au quotient et φ^* définit donc un morphisme $\mathrm{Cl}(C') \longrightarrow \mathrm{Cl}(C)$. On a alors pour tout $\varphi\colon C \to C'$ la relation

$$\deg \varphi^* D = \deg \varphi \cdot \deg D \tag{2.1}$$

(voir [Har77, Proposition II.6.9]).

Définition 2.1.6. *Soit C/k une courbe algébrique de genre g. Il existe une variété abélienne principalement polarisée, appelée la jacobienne de C et notée $\mathrm{Jac}(C)$ de dimension g telle que $(\mathrm{Jac}(C))(k) = \mathrm{Pic}^0(C_{\overline{k}})^{\mathrm{Gal}(\overline{k}/k)}$ et $\mathrm{Jac}(C)(k') = \mathrm{Pic}^0(C_{k'})$ pour tout corps k' tel que $C(k') \neq \emptyset$.*

On se restreint désormais au cas où $C(k) \neq \emptyset$, on choisit alors $P_0 \in C(k)$, un point rationnel. On pose $C^{(g)}$ le quotient de C^g par l'action du groupe des permutations à g éléments qui agit naturellement en permutant les coordonnées. La variété $C^{(g)}$ est de dimension g et non singulière. On note $[P_1, \ldots, P_g]$ la classe de $(P_1, \ldots, P_g) \in C^g$ dans $C^{(g)}$.

On a la proposition suivante (voir [SC86, Theorem VII.5.2.(a)]).

Proposition 2.1.7. *Soit $P_0 \in C\left(\overline{k}\right)$. L'application*

$$\begin{array}{rccc} f^{P_0}\colon & C^{(g)} & \longrightarrow & \mathrm{Jac}(C) \\ & [P_1, \ldots, P_g] & \longmapsto & P_1 + \cdots + P_g - gP_0 \end{array}$$

est birationnelle dominante, i.e. elle est surjective et f^{P_0} restreinte à un ouvert de $C^{(g)}$ définit un isomorphisme.

Polarisation principale de la variété jacobienne

On se restreint toujours au cas où C a un point rationnel P_0. Étant donnée une variété algébrique X sur un corps k, on pose Y une sous-variété fermée de X de codimension 1 et η le point générique de Y. Alors $\mathcal{O}_{X,\eta}$ est un anneau local de dimension $\operatorname{codim}(Y) = 1$ (voir [Liu02, Exercise 2.5.2] par exemple). On peut donc définir pour tout $f \in k(X), v_Y(f)$ comme étant l'unique entier n tel que $f = ut^n \in \operatorname{Frac}(\mathcal{O}_{X,\eta})$ où u est un inversible de $\mathcal{O}_{X,\eta}$ et t est une uniformisante. De la même façon que pour les courbes, si $v_Y(f) \geq 1$ on dit que f a un *zéro* d'ordre $v_Y(f)$ en Y et si $v_Y(f) < 0$ on dit que f a un *pôle* d'ordre $v_Y(f)$ en Y. On peut alors définir un faisceau $\mathscr{L}_Y$ sur X défini sur tout ouvert U par

$$\mathscr{L}_Y(U) = \{f \in k(U), f \text{ a au plus un pôle d'ordre 1 en } U \cap Y \text{ et aucun pôle dans } U \setminus Y\}.$$

Il s'agit d'un faisceau inversible. On pose W^{g-1} l'image de l'application

$$\begin{array}{rcl} C^{(g-1)} & \longrightarrow & \operatorname{Jac}(C) \\ [P_1, \ldots, P_{g-1}] & \longmapsto & P_1 + \cdots + P_{g-1} - (g-1)P_0. \end{array}$$

On peut alors citer le résultat principal concernant les polarisations sur les jacobiennes (voir [SC86, Theorem VII.6.6 et Summary VII.6.11]).

Proposition 2.1.8. *La variété W^{g-1} définie ci-dessus est une sous-variété fermée de* $\operatorname{Jac}(C)$ *de codimension* 1. *On pose $\mathscr{L}_{P_0} = \mathscr{L}_{W^{g-1}}$. Alors l'application*

$$\begin{array}{rccl} \phi_{\mathscr{L}_{P_0}} \colon & \operatorname{Jac}(C) & \longrightarrow & \widehat{\operatorname{Jac}(C)} \\ & x & \longmapsto & t_x^* \mathscr{L}_{P_0} \otimes \mathscr{L}_{P_0}^{-1} \end{array}$$

est une polarisation principale sur la variété abélienne $\operatorname{Jac}(C)$ *telle que* $\left(\operatorname{Jac}(C), \phi_{\mathscr{L}_{P_0}}\right)$ *est indécomposable.*

2.1.4 Exemples

Jacobienne de la droite projective

On considère $C = \mathbb{P}^1$ la droite projective sur un corps k. Soient $P = [a\colon b], Q = [c\colon d] \in \mathbb{P}^1\left(\overline{k}\right)$ deux points fermés distincts alors $f = \frac{bx-ay}{dx-cy}$ satisfait $\operatorname{div}(f) = P - Q$. Autrement dit, il n'existe qu'une seule classe de diviseurs de degré 1, l'application $\deg\colon \operatorname{Pic}(\mathbb{P}^1) \to \mathbb{Z}$ est un isomorphisme et $\operatorname{Pic}^0(\mathbb{P}^1) = \{0\}$.

Réciproquement, une courbe C telle que pour tout $P, Q \in C\left(\overline{k}\right)$ il existe $f \in k(C)$ telle que $P - Q = \operatorname{div} f$ permet de définir un morphisme

$$\begin{array}{rl} C & \longrightarrow \mathbb{P}^1 \\ R \neq Q & \longmapsto [f(R)\colon 1] \\ Q & \longrightarrow [1\colon 0] = \infty. \end{array}$$

Puisque $\varphi^*([0\colon 1]) = P$ d'après (2.1) φ est un morphisme de degré 1 donc une application birationnelle. Puisque C est lisse c'est un isomorphisme.

Jacobienne d'une courbe elliptique

Soit $E\colon y^2 + yh(x) = f(x) \subseteq \mathbb{P}^2$ avec h de degré au plus 1 et f de degré au plus 3 une courbe plane de genre 1 sur un corps k. On pose $P_0 = \infty = [0\colon 1\colon 0]$ le point à l'infini. On considère deux points P et Q de $E\left(\overline{k}\right)$ (pas nécessairement distincts). Par ces deux points passe une unique droite L d'équation affine $L\colon a_0 y + b_0 x + c_0 = 0$ (si $P = Q$ prendre la tangente à E en P). D'après le théorème de Bézout L intersecte E en 3 points fermés P, Q, R (comptés avec multiplicité donc pas forcément distincts). On considère $\alpha = a_0 u + b_0 v + c_0 \in \overline{k}(E) \simeq \operatorname{Frac}\left(\overline{k}[u,v]/\left\langle v^2 - u^3 - au - b\right\rangle\right)$ qui satisfait $\deg(\operatorname{div}\alpha) = 0$ car c'est un diviseur principal. Par ailleurs, α s'annule exactement en P, Q et R en affine et n'a pas de pôle affine (c'est un polynôme). On a donc $\operatorname{div}\alpha = P + Q + R - 3\infty$, i.e.

$$(P - \infty) + (Q - \infty) + (R - \infty) = 0 \in \operatorname{Pic}^0(E).$$

Par ailleurs, pour tout point affine $R_0 = [x_0\colon y_0\colon 1] \in E\left(\overline{k}\right)$ on a $\operatorname{div}(u - x_0) = R_0 + \widetilde{R_0} - 2\infty$ où $\widetilde{R_0} = [x_0\colon -y_0 - h(x_0)\colon 1]$. D'où l'on déduit

$$(P - \infty) + (Q - \infty) = (\widetilde{R} - \infty) \in \operatorname{Jac}(E).$$

L'application

$$\begin{array}{rccc} f^\infty\colon & E & \longrightarrow & \operatorname{Jac}(E) \\ & P & \longrightarrow & P - \infty \end{array}$$

est injective car si $P - \infty \sim Q - \infty$ alors $P \sim Q$ donc $P = Q$ car s'ils sont distincts alors $E \simeq \mathbb{P}^1$ d'après le paragraphe précédent. D'après la Proposition 2.1.7, f^∞ est un isomorphisme. On peut alors identifier E avec $\operatorname{Jac}(E)$ et transporter la loi de groupe de $\operatorname{Jac}(E)$ sur E avec pour élément neutre ∞ de la manière suivante. Soient $P, Q \in E\left(\overline{k}\right)$

distincts alors la droite L passant par P et Q intersecte $E\left(\overline{k}\right)$ en R et on pose $\widetilde{R} = P+Q$ le symétrique de R par rapport à la droite $y = 0$. Pour $P' \in E\left(\overline{k}\right)$ en considérant la tangente à E en P' on a $2P' + R' = 0$ ce qui permet de définir $\widetilde{R'} = 2P'$ comme le symétrique de R' par rapport à $x = 0$. Il est intéressant de noter que si P et Q (pas forcément distincts) sont k' rationnels alors $P + Q$ est aussi k' rationnel.

Nous avons illustré cette construction dans la Figure 2.1 sur la courbe elliptique $E\colon y^2 = x^3 + 3x + 1$ sur $\mathbb{F}_{11}$. Nous avons représenté les points rationnels de la courbe E dans un repère $\mathbb{F}_{11}^2 = [\![-6, 5]\!]^2$ plus le point à l'infini. La droite bleue est l'unique droite [4] $\mathscr{D}\colon y = \frac{1}{2}x - 1 = 6x - 1$ passant par $P = [-5\colon 2\colon 1]$ et $Q = [-3\colon 3\colon 1]$. Comme expliqué plus haut, $\mathscr{D}$ coupe E en 3 points (comptés avec multiplicité) de E donc coupe E en un troisième point R (qui est rationnel comme promis). Le point $P+Q = [0\colon 1\colon 1]$ est défini comme le symétrique $\widetilde{R}$ de R par rapport à $y = 0$.

Nous avons aussi voulu illustrer le calcul de $2P'$ pour le point $P' = [3\colon 2\colon 1]$. L'unique droite qui coupe E en P' avec multiplicité 2 est la tangente à E en P' qui est visuellement beaucoup moins intuitive à se représenter que dans le cas réel mais dont une équation est donnée par

$$x\frac{\partial f}{\partial x}(P) + y\frac{\partial f}{\partial y}(P) + z\frac{\partial f}{\partial z}(P) = 0$$

(voir [Rit17, Exercise 2.7]) où $f(x, y, z) = y^2z - x^3 + 3xz^2 + z^3$ qui donne l'équation de droite (en affine) $y = 2x - 4$. Comme prévu cette droite coupe $E\left(\mathbb{F}_{11}\right)$ en un unique autre point $R' = [-2\colon 3\colon 1]$ dont le symétrique par $y = 0$ donne $\widetilde{R'} = 2P' = [-2\colon -3\colon 1]$.

Jacobienne d'une courbe de genre 2

On considère une courbe hyperelliptique plane C sur un corps k quelconque et de genre 2, c'est à dire

$$C\colon y^2 + yh(x) = f(x)$$

où f est de degré 5 ou 6 et h de degré au plus 2. Pour tout point affine $P_0 = [x_0\colon y_0\colon 1] \in C\left(\overline{k}\right)$ on définit $\widetilde{P_0} = [x_0\colon -y_0 - h(x_0)\colon 1]$ son conjugué. On considère 4 points affines P_1, P_2, P_3, P_4 de la courbe tels qu'il n'y ait pas un point et son conjugué parmi ces 4 points. On considère b, le polynôme interpolateur des abscisses de ces points (comptées

4. Bien sûr cette droite ne possède qu'un nombre fini de points rationnel et la représenter par une droite réelle est un abus qui a seulement un but pédagogique. Puisque $6x - 1 = -5x + 10$ par exemple on aurait aussi pu choisir une autre représentation réelle de la droite $\mathscr{D}$ mais cette dernière serait passée par les mêmes coordonnées entières de $[-6, 5]^2$.

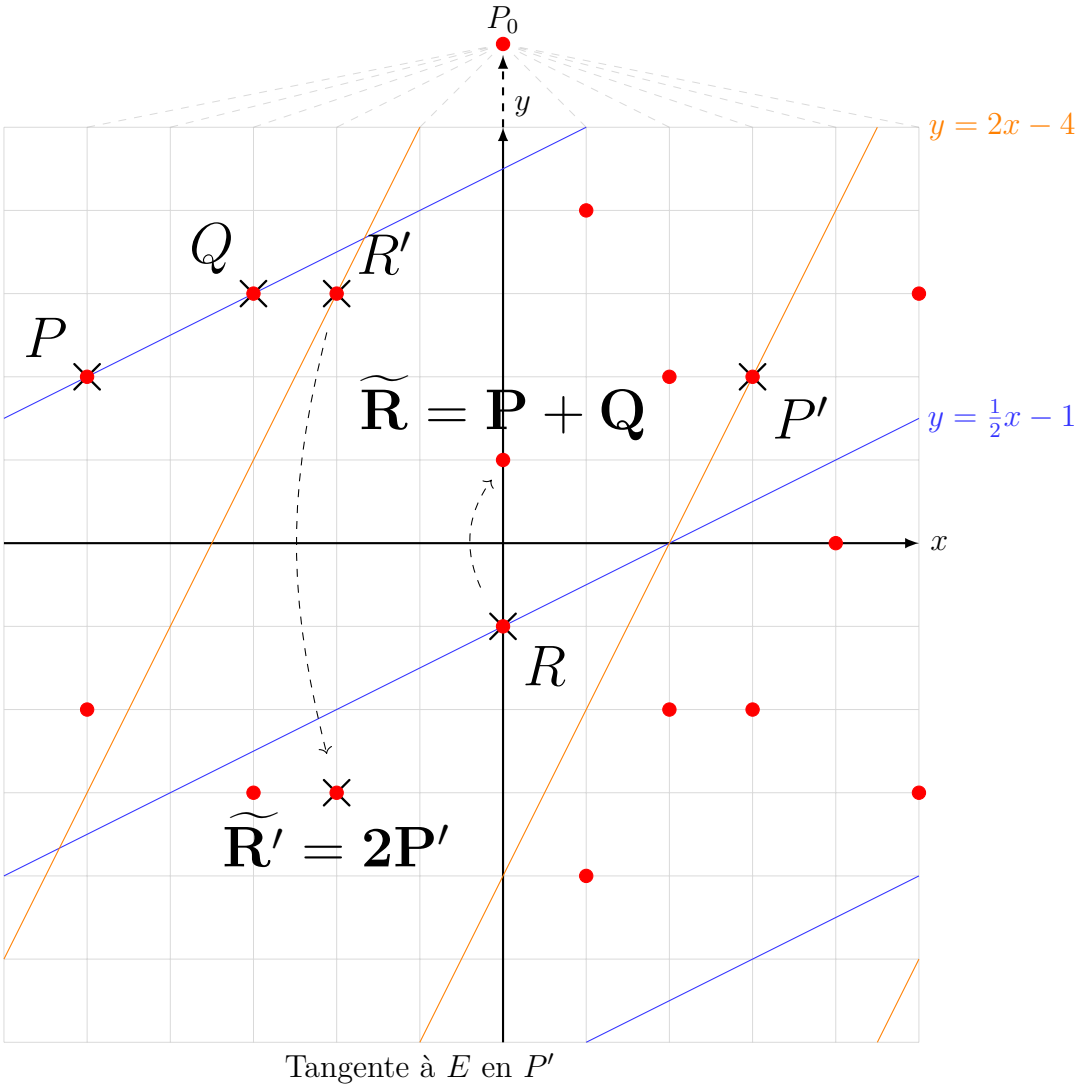


FIGURE 2.1 – Loi de groupe de la courbe elliptique d'équation $E\colon y^2 = x^3 + 3x + 1$ sur $\mathbb{F}_{11}$

avec multiplicité), i.e b est de degré $4-1=3$ et $b(x_i)=y_i$ avec $P_i=[x_i\colon y_i\colon 1]$. On voit immédiatement que le système

$$\begin{cases} y^2+yh(x)=f(x) \\ y=b(x) \end{cases}. \tag{2.2}$$

se résout très facilement dans $\overline{k}$ et donne 6 solutions (x,y). Autrement dit, la courbe $y=b(x)$ intersecte C en 6 points affines exactement (comptés avec multiplicité). On les notes $P_1,\ldots,P_4$ pour les 4 qu'on a déjà et R_1 et R_2 pour les deux nouveaux. La fonction $\alpha=v-b(u)\in\overline{k}(C)=\mathrm{Frac}\left(\overline{k}[u,v]/\left\langle v^2+vh(u)-f(u)\right\rangle\right)$ satisfait donc

$$\mathrm{div}(\alpha)=P_1+\cdots+P_4+R_1+R_2-6\infty=0\in\mathrm{Jac}(C).$$

Par ailleurs, pour tout $P_0\in C\left(\overline{k}\right)$ on a $\mathrm{div}(u-x_0)=P_0+\widetilde{P_0}-2\infty$. On en déduit que

$$(P_1+P_2-2\infty)+(P_3+P_4-2\infty)=\widetilde{R_1}+\widetilde{R_2}-2\infty$$

ce qui décrit la loi d'addition de la jacobienne de C.

Remarquons qu'on a supposé qu'il n'y ait pas un point et son conjugué parmi les 4 points mais on peut passer outre cette hypothèse en interpolant C seulement pour les points d'abscisse distincte puis en considérant la cubique $y^2+yh(x)=b(x)$ au lieu de $y=b(x)$.

Nous proposons d'illustrer cette méthode en reprenant la courbe hyperelliptique optimale $C\colon y^2=5x^6-3x^4-3x^2+5$ donnée dans l'introduction (Figure 2). Nous souhaitons faire la somme des points

$$P_1=[-2\colon 1\colon 1], P_2=[0\colon 4\colon 1], P_3=[1\colon -2\colon 1] \text{ et } P_4=[2\colon 1\colon 1].$$

Le polynôme interpolateur est $b(x)=-x^3+2x^2+4x+4$, i.e. $b(-2)=1, b(0)=4, b(1)=-2$ et $b(2)=1$. Nous avons tracé le graphe réel de b dans un domaine fondamental de $\mathbb{R}^2$ par l'action de $11\mathbb{Z}\times 11\mathbb{Z}$ pour en avoir une représentation imagée dans $(\mathbb{Z}\times\mathbb{Z})/(11\mathbb{Z}\times 11\mathbb{Z})\simeq\mathbb{F}_{11}^2$. La courbe $y=b(x)$ coupe bien C en 6 points affines dont les deux nouveaux sont $R_1=[4\colon -1\colon 1]$ et $R_2=[5\colon 4\colon 1]$. Ceci permet de définir la somme $[P_1,P_2]+[P_3,P_4]=[\widetilde{R_1},\widetilde{R_2}]$. Nous illustrons la construction dans la Figure 2.2.

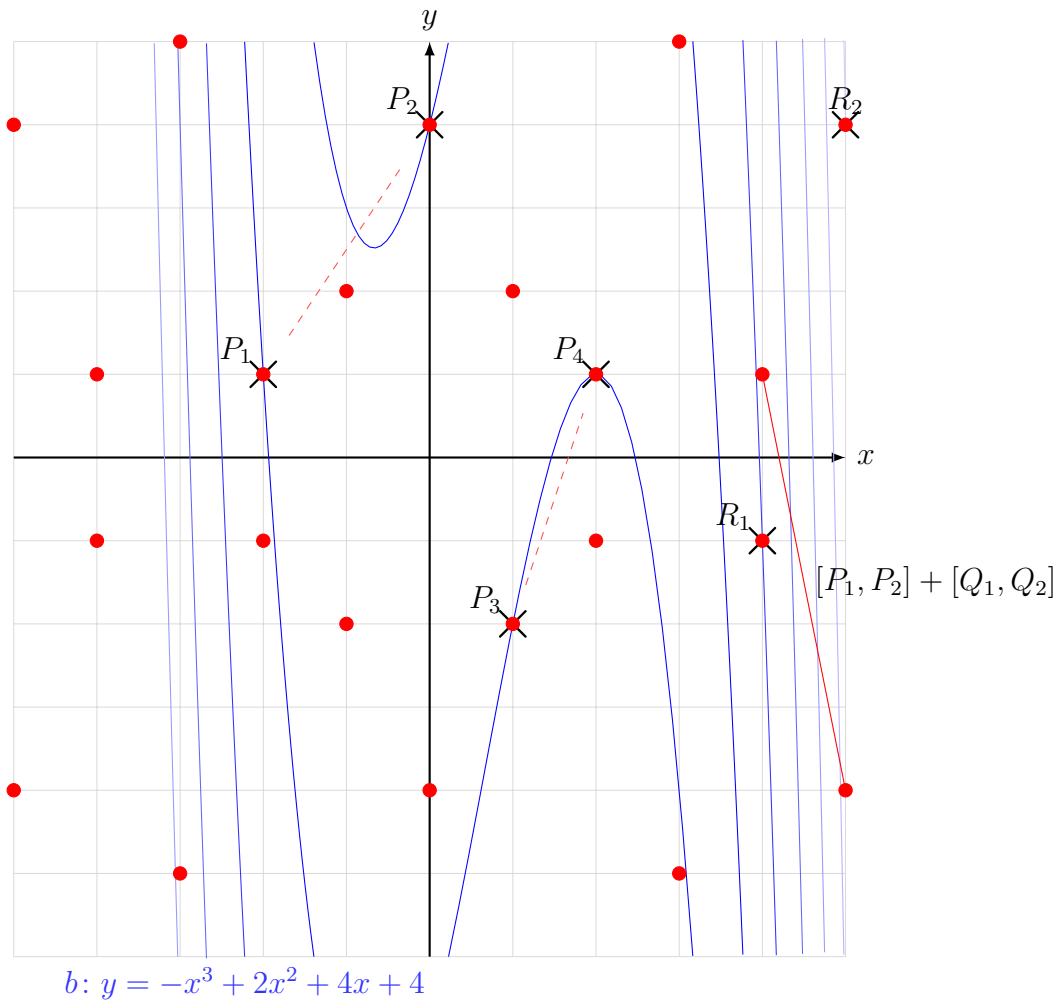


FIGURE 2.2 – Loi de groupe sur la jacobienne la courbe hyperelliptique de genre 2 d'équation $C\colon y^2 = 5x^6 - 3x^4 - 3x^2 + 5$ sur $\mathbb{F}_{11}$.

Jacobienne d'une courbe hyperelliptique

On considère plus généralement une courbe hyperelliptique de genre g définie par

$$C\colon y^2 = f(x)$$

avec $f \in k[x]$ tel que $\deg f = 2g+1$ ou $2g+2$. Dans cette section nous souhaitons expliquer comment sommer des points de la jacobienne de ce type de courbe. Malheureusement, si $g \geq 3$ en essayant d'appliquer la même technique que pour le genre 2 de la section précédente, si on interpole C en $2g$ points on obtient un polynôme b de degré $2g-1$ qui coupe C en $4g-2 > 3g$ points affines et donc le fait que $\operatorname{div}(v-b) = 0$ ne nous aide pas vraiment. On va cependant expliquer comment affiner ce diviseur à l'aide du pgcd de deux diviseurs que nous allons définir tout de suite.

Nous allons suivre les explications très détaillées des autrices de [MWZ96]. Des algorithmes très généraux ([MWZ96, Algorithm 1 et 2]) y sont développé pour sommer n'importe quels points de la jacobienne d'une courbe hyperelliptique sur un corps de n'importe quelle caractéristique. Par simplicité nous allons seulement décrire la somme de points dont les abscisses sont distinctes et les ordonnées non nulles.

Pour cela nous avons besoin de quelques notions supplémentaires. Soient $D_1 = \sum_P n_P P$ et $D_2 = \sum_P m_P P$ deux diviseurs d'une courbe hyperelliptique C et ∞ le point à l'infini. On pose $\operatorname{pgcd}(D_1, D_2)$ le diviseur de degré 0 défini par

$$\operatorname{pgcd}(D_1, D_2) = \sum_P \min(n_P, m_P)P - \left(\sum_P \min(n_P, m_P)\right)\infty.$$

On a les deux relations immédiates depuis la définition pour tout diviseur D_1, D_2, D et toutes fonctions $\alpha, \beta \in \overline{k}(C) \simeq \operatorname{Frac}\left(\overline{k}[u,v]/\langle v^2 - f(u)\rangle\right)$.

$$\operatorname{pgcd}(D_1 + D, D_2 + D) = \operatorname{pgcd}(D_1, D_2) + D - (\deg D)\,\infty \tag{2.3}$$

$$\operatorname{pgcd}(\operatorname{div}\alpha, \operatorname{div}(\alpha+\beta)) = \operatorname{pgcd}(\operatorname{div}\alpha, \operatorname{div}\beta). \tag{2.4}$$

En prenant $D = \operatorname{div}\alpha$ dans la première relation on voit que pgcd est bien défini dans le quotient $\operatorname{Pic}(C)$ et donc sur le sous-groupe $\operatorname{Pic}^0(C) = \operatorname{Jac}(C)$.

On considère $2g$ points affines $P_1 = [x_1\colon y_1\colon 1], \ldots, P_{2g} = [x_{2g}\colon y_{2g}\colon 1]$ de la courbe C. On pose alors les fonctions $a = \prod(u - x_i)$ et $b \in \overline{k}[u]$ le polynôme interpolateur de (x_i, y_i)

de plus petit degré, i.e. b de degré $2g-1$ et pour tout $b(x_i) = y_i$ ou, de manière équivalente $b = y_i \mod (u - x_i)$. On voit alors que $b^2 - f = 0 \mod a$ et on pose $aa' = b^2 - f$. On remarque que

$$\sum_i P_i - 2g\infty = \mathrm{pgcd}\left(\mathrm{div}\, a, \mathrm{div}(b - v)\right). \tag{2.5}$$

En effet, $\mathrm{div}\, a = \sum_i P_i + \sum_i \widetilde{P_i} - 2g\infty$ où $\widetilde{P_i} = [x_i\colon\ -y_i\colon 1] \in C$ et $b - v$ s'annule en P_i pour tout i mais pas en $\widetilde{P_i}$, d'où la relation [5] (2.5). L'idée est d'écrire $\sum_{i=1}^{2g} P_i - 2g\infty = \sum_{j=1}^{g} R_i - g\infty \in \mathrm{Jac}(C)$ ainsi on aura

$$\left(\sum_{i=1}^{g} P_i - g\infty\right) + \left(\sum_{i=g+1}^{2g} P_i - g\infty\right) = \sum_{i=1}^{g} R_i - g\infty \in \mathrm{Jac}(C).$$

D'après la Proposition 2.1.7, on peut toujours représenter les points de $\mathrm{Jac}(C)$ de cette manière et d'après la relation (2.5) on peut toujours l'écrire sous la forme $\mathrm{pgcd}(\mathrm{div}\, a, \mathrm{div}(b - v))$ (voir [MWZ96, Théorème 42] pour la démonstration dans le cas général).

On remarque, en appliquant la relation (2.3), que

$$\begin{aligned}
\mathrm{pgcd}(\mathrm{div}(a), \mathrm{div}(b - v)) &= \mathrm{pgcd}(\mathrm{div}(a) + \mathrm{div}(b + v), \mathrm{div}(b - v) + \mathrm{div}(b + v)) \\
&= \mathrm{pgcd}(\mathrm{div}(a) + \mathrm{div}(b + v), \mathrm{div}(b^2 - f)) \\
&= \mathrm{pgcd}(\mathrm{div}(a) + \mathrm{div}(b + v), \mathrm{div}(a) + \mathrm{div}(a')) \\
&= \mathrm{pgcd}(\mathrm{div}(b + v), \mathrm{div}(a')) \in \mathrm{Jac}(C)
\end{aligned} \tag{2.6}$$

En posant $b' = -b \mod a'$, écrivons $b' = -b + ha'$ on a alors, d'après la relation (2.4),

$$\mathrm{pgcd}(\mathrm{div}(a'), \mathrm{div}(b + v)) = \mathrm{pgcd}(\mathrm{div}(a'), \mathrm{div}(b + v - ha')) = \mathrm{pgcd}(\mathrm{div}(a'), \mathrm{div}(b' - v)).$$

On peut alors construire une suite (a_n, b_n) telle que $a_0 = a, b_0 = b$ et $a_{n+1} = a'_n, b_{n+1} = b'_n$ comme ci-dessus jusqu'à avoir $\deg a_n \leq g$. Les $u_j \in \overline{k}$ tels que $a_n(u_j)$ sont les abscisses des points R_j tels que

$$\sum_{i=1}^{2g} P_i - 2g\infty = \sum_{j=1}^{g} R_j - g\infty.$$

Leurs ordonnées sont données par $v_j = b_n(u_j)$.

Si on reviens au genre $g = 2$, on a vu que $\mathrm{div}(b)$ permet directement de décrire la

5. Cette relation est toujours vraie sans hypothèse sur les coordonnées des P_i mais elle demande plus de travail et une définition différente de b.

somme de deux points de la jacobienne. Si on applique l'algorithme décrit on obtient le polynôme a' de degré $\deg(b^2 - f) - \deg(a) = 6 - 4 = 2$ dont les racines sont les abscisses de $\widetilde{R_1}$ et $\widetilde{R_2}$. D'autre part, b' est de degré ≤ 1 et $y = b'(x)$ décrit donc une droite. En reprenant l'exemple de la Figure 2.2 on calcule $a'(x) = x^2 + 2x - 2 = (x-4)(x-5)$ et $b'(x) = 6x - 1$. On retrouve bien les points $\widetilde{R_1} = [4\colon b'(4) = 1\colon 1]$ et $\widetilde{R_2} = [5\colon b'(5) = -4\colon 1]$

2.1.5 Lieu des jacobiennes parmi les variétés abéliennes

Dans cette section nous souhaitons énoncer les théorèmes de Torelli qui permettent d'établir un lien entre les courbes algébriques de genre g et les variétés abéliennes de dimension g pour $g = 1, 2$ et 3 par l'intermédiaire des jacobiennes. On va voir que toutes les variétés abéliennes principalement polarisées indécomposables de dimension $g = 1, 2$ et 3 sont la jacobienne d'une courbe (avec une nuance à apporter pour $g = 3$). Déterminer le lieu des jacobiennes parmi l'espace de modules des variétés abéliennes de dimension $g \geq 4$ est un problème difficile appelé le *problème de Schottky*.

L'application d'Abel-Jacobi $C \longmapsto (\mathrm{Jac}(C), j)$ qui associe à une courbe sa jacobienne polarisée induit une application entre les espaces de modules

$$\begin{array}{rccc} [\mathrm{Jac}]\colon & M_g & \longrightarrow & A_g \\ & [C] & \longmapsto & [\mathrm{Jac}(C), j] \end{array}$$

où M_g est l'espace de modules formé des classes d'isomorphisme de courbes de genre g sur un corps k et A_g est celui des classes d'isomorphisme (polarisé) de variétés abéliennes principalement polarisées indécomposables de dimension g sur k. Lorsque k est un corps parfait et $g \geq 2$, d'après [SC86, Corollary 12.2], l'application [Jac] est injective. Par ailleurs, lorsque $g \leq 3$ et k est algébriquement clos alors toutes les variétés abéliennes principalement polarisées indécomposables sont isomorphes à la jacobienne d'une courbe (voir [OU73]). En d'autres termes, l'application [Jac] est aussi surjective. Pour $g = 2$, l'hypothèse k algébriquement clos peut-être abandonnée car toutes les courbes de genre 2 sont hyperelliptiques (voir [Lau01, Appendice, Théorème 4]). En genre 3, c'est toujours vrai à une nuance près. Étant donnée une variété abélienne principalement polarisée indécomposable (A, a) sur une corps k alors $(A, a)_{\overline{k}}$, la variété (A, a) « vue sur $\overline{k}$ », est la jacobienne d'une courbe C_0 sur $\overline{k}$ d'après [OU73]. Peut-on alors toujours descendre C_0 en une courbe C sur k (i.e. $C_{\overline{k}} \simeq_{\overline{k}} C_0$) telle que $\mathrm{Jac}(C) \simeq_k (A, a)$? La réponse est non. Plus précisément, on peut toujours descendre C_0 en une courbe C_1 sur k mais il se peut

que $\mathrm{Jac}(C_1)$ ne soit pas isomorphe à (A, a) sur k (même si, par définition de C_1, leur deux jacobiennes sont isomorphes sur $\overline{k}$). Lorsque $\mathrm{Jac}(C_1)$ n'est pas isomorphe à (A, a) alors (A, a) n'est pas la jacobienne d'une courbe sur k. Le fait qu'une variété abélienne polarisée (A, a) sur k soit la jacobienne d'une courbe géométriquement (c'est-à-dire sur $\overline{k}$) mais pas rationnellement (pas sur k) est appelé l'*obstruction de Serre*. On résume cela plus précisément dans le théorème suivant (voir [Lau01, Appendice, Théorème 4 et 5]).

Théorème 2.1.9. *Soit (A, a) une variété abélienne polarisée de dimension $g > 1$ sur un corps k. Supposons que (A, a) est isomorphe à la jacobienne d'une courbe C_0 sur $\overline{k}$. Alors*

- *Si C_0 est hyperelliptique alors il existe une courbe C sur k telle que $C_{\overline{k}} \simeq C_0$ et $\mathrm{Jac}(C) \simeq (A, a)$ (autrement dit il n'y a jamais d'obstruction pour les courbes hyperelliptiques).*
- *Si C_0 n'est pas hyperelliptique alors il existe une courbe C sur k telle que $C_{\overline{k}} \simeq C_0$ et un morphisme de groupes*

$$\varepsilon\colon \mathrm{Gal}(k^{sep}/k) \longrightarrow \{-1, 1\}$$

tel que $\mathrm{Jac}(C) \simeq (A, a)_\varepsilon$ où $(A, a)_\varepsilon$ est la tordue de (A, a) par le caractère ε. De plus (A, a) est la jacobienne d'une courbe sur k si, et seulement si, ε est trivial.

Dans [Lau01, Appendice] Serre montre ces résultats de descente du corps de définition pour des extensions k_1/k galoisiennes. Partant d'une variété abélienne (A, a) de dimension 2 ou 3 qui est géométriquement isomorphe à la jacobienne d'une courbe C_0 sur $\overline{k}$ on peut supposer que C_0 et $\mathrm{Jac}(C_0)$ sont définies sur une extension finie k_1 de k car elles sont définies par des polynômes à coefficients (en nombre fini) dans $\overline{k}$. Si k est parfait alors k_1 est galoisienne. Sinon, Serre explique qu'on peut tout de même descendre les isomorphismes sur k.

C'est grâce à ces résultats qu'énumérer les variétés abéliennes principalement polarisées de dimension 2 sur un corps k parfait permet d'énumérer les courbe de genre 2. Pour le genre 3 l'énumération tient toujours lorsque k est algébriquement clos. Si k n'est pas algébriquement clos on peut toujours énumérer les courbes sous réserve d'être capable de calculer l'obstruction de Serre pour chaque variété abélienne polarisée. Ce calcul peut-être fait si on connaît les *thêta constantes* associées à la variété.

2.2 Variétés abéliennes complexes

Dans cette section nous allons définir beaucoup de foncteurs et de catégories (surtout dans la Section 2.2.4) pour décrire des liens aussi précis que possible entre les variétés abéliennes complexes et les réseaux hermitiens par l'intermédiaire des tores complexes. Nous définirons des catégories et des foncteurs adaptés au besoin de considérer les polarisations ou non. Pour aider la lectrice à se repérer parmi toutes les notations nous fixons ici quelques conventions. Toutes les catégories et les foncteurs seront notés en gras et les catégories seront notées en gras calligraphique. Par exemple nous noterons le foncteur, déjà évoqué, qui définit l'équivalence de catégories entre les variétés abéliennes complexes et les tores complexes polarisables par

$$\mathbf{H}_{\mathbb{C}} \colon A \longmapsto A(\mathbb{C})$$

(nous le notons $\mathbf{H}_{\mathbb{C}}$ car $\mathrm{Hom}(\mathrm{Spec}(\mathbb{C}), \_)$ est trop long à écrire). Ou encore, la catégorie des R-réseaux hermitiens entiers sera notée $\boldsymbol{\mathcal{L}}_K^{h,int}$.

2.2.1 Généralités sur les tores complexes

Définition 2.2.1. *Soit V un $\mathbb{C}$-espace vectoriel de dimension g et Γ un $\mathbb{Z}$-réseau plein de V, i.e. un sous-groupe discret de V tel que $\dim_{\mathbb{Q}}(\Gamma \otimes \mathbb{Q}) = 2g$. Le quotient $X = V/\Gamma$ est appelé tore complexe et on définit sa dimension par $\dim X = g$.*

On peut aussi définir un $\mathbb{Z}$-réseau de V comme un sous-groupe de V engendré par une $\mathbb{R}$-base de V.

Exemple 2.2.2. *Par exemple pour $V = \mathbb{C}$ et $\Gamma = \mathbb{Z}[i] = \mathbb{Z} + i\mathbb{Z}, X = \mathbb{C}/\Gamma$ est un tore complexe.*

Remarquons que les tores complexes sont naturellement munis d'une structure de variété complexe et de groupe données par le quotient. Ces deux structures sont compatibles l'une avec l'autre, i.e. pour un tore complexe X les deux applications

$$X \times X \to, (x, y) \mapsto x + y \text{ et } X \to X, x \mapsto -x$$

sont holomorphes. Ceci montre que les tores complexes sont des groupes de Lie complexes.

Définition 2.2.3. *Un morphisme f entre deux tores complexes X et X' est un morphisme*

de groupes holomorphe

$$f\colon X \to X'.$$

Proposition 2.2.4. *Soient $X = V/\Gamma$ et $X' = V'/\Gamma'$ deux tores complexes et $f\colon X \to X'$ un morphisme de tores complexes. Alors f se relève en une unique application $\mathbb{C}$-linéaire $f_{an}\colon V \to V'$, appelée représentation analytique de f, telle que le diagramme suivant commute*

$$\begin{array}{ccc} V & \xrightarrow{f_{an}} & V' \\ {\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle\pi'} \\ X & \xrightarrow{f} & X'. \end{array}$$

Démonstration. Puisque V et V' sont connexes, les morphismes π et π' sont les revêtements universels de X et X' respectivement. Ceci prouve que f se relève en une application holomorphe $\widetilde{f}\colon V \to V'$. Puisque f est un morphisme de groupe on a pour tout $(v,w) \in V, \widetilde{f}(v+w) - \widetilde{f}(v) - \widetilde{f}(w) \in \Gamma'$. Puisque $(v,w) \mapsto \widetilde{f}(v+w) - \widetilde{f}(v) - \widetilde{f}(w)$ est continue et Γ' est discret, il existe un unique $\gamma' \in \Gamma'$ tel que $\widetilde{f}(v+w) - \widetilde{f}(v) - \widetilde{f}(w) = \gamma'$ donc

$$\left(\widetilde{f}(v+w) + \gamma'\right) - \left(\widetilde{f}(v) + \gamma'\right) - \left(\widetilde{f}(w) + \gamma'\right) = 0$$

ce qui prouve que l'application donnée par $f_{\mathrm{an}} = \widetilde{f} + \gamma'$ est un morphisme de groupe holomorphe. On a alors pour tout $a, b \in \mathbb{Z} \setminus \{0\}, v \in V, b f_{\mathrm{an}}\left(\frac{a}{b}v\right) = f_{\mathrm{an}}(av) = a f_{\mathrm{an}}(v)$ donc f_{an} est $\mathbb{Q}$-linéaire. Finalement, pour tout $v \in V$, l'application

$$\begin{array}{rccc} s_v\colon & \mathbb{C} & \longrightarrow & V' \\ & \lambda & \longmapsto & f_{\mathrm{an}}(\lambda v) - \lambda f_{\mathrm{an}}(v) \end{array}$$

est holomorphe et identiquement nulle sur $\mathbb{Q}$. Donc f_{an} est $\mathbb{C}$-linéaire. L'unicité découle du fait que deux relèvements linéaires $\widetilde{f_1}$ et $\widetilde{f_2}$ coïncident sur Γ donc sur une $\mathbb{C}$-base de V. □

Par définition de f_{an} on a $f_{\mathrm{an}}(\Gamma) \subseteq \Gamma'$. Ainsi f_{an} induit un morphisme de groupe $f_{\mathrm{rat}} = f_{\mathrm{an}|\Gamma}\colon \Gamma \to \Gamma'$ appelé représentation rationnelle de $f\colon X \to X'$.

On notera $\mathrm{Hom}_{\mathbb{C}}(\Gamma, \Gamma')$ l'ensemble des représentations analytiques des morphismes de $\mathbb{C}/\Gamma$ dans $\mathbb{C}/\Gamma'$.

Lorsqu'un morphisme $u\colon X \to X'$ est surjectif et que $\dim X = \dim X'$, on dit que u est une *isogénie*. Le noyau d'une isogénie est toujours fini et son cardinal est appelé le *degré* de u et noté $\deg u = \#\ker u$.

Exemple 2.2.5. *Un exemple important d'isogénie est la multiplication par n dans un tore complexe, noté $[n]_X \colon X \to X, x \mapsto nx$. Lorsqu'il n'y a pas d'ambiguité on la note $[n]$ en omettant le X. Le morphisme est bien surjectif car $\rho_a([n]) \colon V \to V$ l'est.*

Les isogénies jouent un rôle absolument central dans l'étude des tores complexes et plus généralement dans l'étude des variétés abéliennes. Une des raisons pour lesquelles la notion d'isogénies est aussi importante est la suivante.

Proposition 2.2.6. *Soit $f \colon X \to X'$ une isogénie de degré d, alors il existe une unique isogénie $\widetilde{f} \colon X' \to X$ telle que $\widetilde{f} \circ f = [d]_X$. On a alors $f \circ \widetilde{f} = [d]_{X'}$.*

Démonstration. Puisque $\ker f$ est de cardinal d, par le théorème de Lagrange $[d]_X(\ker f) = \{0\}$ donc $\ker f \subseteq \ker[d]_X$ et, par la propriété universelle du quotient, il existe un morphisme de groupe $\widetilde{f}$ tel que

$$\begin{array}{ccc} X & \xrightarrow{[d]_X} & X \\ {\scriptstyle f}\downarrow & \nearrow_{\widetilde{f}} & \\ X'. & & \end{array}$$

Le morphisme $\widetilde{f}$ est bien surjectif car $[d]_X$ l'est. C'est donc une isogénie.

Finalement, on remarque que $(f \circ \widetilde{f}) \circ f = f \circ [d]_X = [d]_{X'} \circ f$ donc $X' = Im(f) \subseteq \ker(f \circ \widetilde{f} - [d]_{X'})$ donc $f \circ \widetilde{f} = [d]_{X'}$. □

Cette proposition est très importante car elle permet de montrer que la relation définie par $X \sim X'$ s'il existe une isogénie entre X et X' est une relation d'équivalence. Elle permet de répartir les tores complexes en classes d'isogénie, une classification moins contraignante que les classes d'isomorphismes.

2.2.2 Courbes elliptiques complexes

Dans cette section nous souhaitons décrire le lien entre les tores complexes et les variétés abéliennes complexes en dimension 1 spécifiquement. Nous aurons besoin de matériel supplémentaire pour aborder les dimensions supérieures.

Fonctions $\wp$ de Weierstrass et $\mathbb{Z}$-réseau

On pose pour $\Lambda \subseteq \mathbb{C}$ un $\mathbb{Z}$-réseau. La fonction définie pour tout $z \notin \Lambda$ par

$$\wp(z, \Lambda) = \frac{1}{z^2} + \sum_{\omega \in \Lambda \setminus \{0\}} \left(\frac{1}{(z-\omega)} - \frac{1}{\omega^2} \right)$$

est appelée fonction $\wp$ de Weierstrass.
Nous noterons simplement $\wp(z)$ au lieu de $\wp(z, \Lambda)$ lorsqu'il n'y a pas d'ambiguïté. Nous énonçons sans démonstration le résultat très classique suivant qui résume les propriétés essentielles de de $\wp$. On pourra trouver une démonstration dans [Sil09, Chapter VI].

Théorème 2.2.7. *Soit $\Lambda \subseteq \mathbb{C}$ un $\mathbb{Z}$-réseau.*

1. *La fonction $\wp$ est bien définie, Λ-périodique et holomorphe sur $\mathbb{C} \setminus \Lambda$.*
2. *Le corps des fonctions méromorphes $\mathbb{C}(\Lambda)$ sur $X = \mathbb{C}/\Lambda$ est donné, à une translation près, par le corps $\mathbb{C}(\wp, \wp')$.*
3. *Les fonctions $\wp$ et $\wp'$ sont liées par la relation*

$$\wp'(z) = 4\wp(z) - g_4(\Lambda)\wp(z) - g_6(\Lambda)$$

   où $g_{2k}(\Lambda) = \sum_{\omega \in \Lambda \setminus \{0\}} \omega^{-2k}$.
4. *Soit $E\colon y^2 = 4x^3 - g_4(\Lambda)x - g_6(\Lambda)$ alors l'application définie par*

$$\begin{aligned} \phi_\Lambda\colon \quad \mathbb{C}/\Lambda &\longrightarrow E(\mathbb{C}) \subseteq \mathbb{P}^2(\mathbb{C}) \\ z \neq 0 &\longmapsto [\wp(z)\colon \wp'(z)\colon 1] \end{aligned}$$

   et $\phi_\Lambda(0) = [0\colon 1\colon 0]$ est un isomorphisme de groupes de Lie.
5. *Pour tout $A, B \in \mathbb{C}$ tels que $A^3 - 27B^2 \neq 0$ il existe un unique réseau $\Lambda \in \mathbb{C}$ tel que $g_4(\Lambda) = A$ et $g_6(\Lambda) = B$. En particulier, pour toute courbe elliptique $E\colon y^2 = 4x^3 - Ax - B$ il existe un réseau Λ qui définit un isomorphisme $\phi_\Lambda\colon \mathbb{C}/\Lambda \to E(\mathbb{C})$.*

On écrira parfois E_Λ pour désigner une courbe elliptique telle qu'on a un isomorphisme $\phi_\Lambda\colon \mathbb{C}/\Lambda \to E(\mathbb{C})$.

Le point 4. prouve en particulier que pour tout tore complexe X de dimension 1 il existe un plongement holomorphe de X dans un espace projectif. Ceci n'est malheureusement pas vrai pour les tores de dimension supérieure comme nous le verrons dans la Section 2.2.3.

Morphismes et isogénies

On considère un morphisme de groupe de Lie $f\colon X \to X'$ (f est un morphisme de groupes et un morphisme de variétés complexes) avec $X = \mathbb{C}/\Lambda$ et $X' = \mathbb{C}/\Lambda'$ deux tores

complexes. Comme le montre la Proposition 2.2.4, f se relève en une application linéaire f_{an}

$$\begin{array}{ccc} \mathbb{C} & \xrightarrow{f_{\text{an}}} & \mathbb{C} \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi'} \\ \mathbb{C}/\Lambda & \xrightarrow{f} & \mathbb{C}/\Lambda'. \end{array}$$

Les applications linéaires partant de $\mathbb{C}$ sont définies par leur image de 1 nous identifierons donc souvent f_{an} avec $f_{\text{an}}(1) \in \mathbb{C}$. Ceci nous permet d'identifier l'anneau d'endomorphisme d'un tore complexe X à un sous-anneau de $\mathbb{C}$,

$$\text{End}(X) \simeq \text{End}_{\mathbb{C}}(\Lambda) = \{\alpha \in \mathbb{C}, \alpha\Lambda \subseteq \Lambda\}.$$

Proposition 2.2.8. *Soit $\Lambda \subseteq \mathbb{C}$ un $\mathbb{Z}$-réseau. Alors $\text{End}_{\mathbb{C}}(\Lambda)$ est soit $\mathbb{Z}$ soit un ordre dans un corps quadratique imaginaire.*

Dans le cas où $\text{End}_{\mathbb{C}}(\Lambda) \neq \mathbb{Z}$ on dit que $X = \mathbb{C}/\Lambda$ ou Λ, par abus, est à *multiplication complexe*, noté CM, sous-entendu qu'il existe un endomorphisme de X donc la représentation analytique est la multiplication par un « vrai »complexe.

Exemple 2.2.9. *Soit K un corps quadratique imaginaire et $K \to \mathbb{C}$ un plongement. Soit R un ordre quelconque dans K et $\mathfrak{a}$ un idéal fractionnaire inversible. Le $\mathbb{Z}$-réseau $\Lambda = \mathfrak{a} \subseteq \mathbb{C}$ a pour anneau d'endomorphisme*

$$\begin{aligned} \text{End}_{\mathbb{C}}(\Lambda) &= \{\alpha \in \mathbb{C}, \alpha\mathfrak{a} \subseteq \mathfrak{a}\} \\ &= \{\alpha \in K, \alpha\mathfrak{a} \subseteq \mathfrak{a}\} \\ &= [\mathfrak{a} \colon \mathfrak{a}] = R_{\mathfrak{a}}. \end{aligned}$$

Donc $\text{End}_{\mathbb{C}}(\mathfrak{a}) = R_{\mathfrak{a}}$. Ceci n'est pas étonnant car on sait qu'une courbe elliptique E_Λ admet toujours une polarisation principale $a_{0,E}$ qui, comme on le verra plus tard dans la Proposition 2.2.32, induit sur Λ une structure $\text{End}(E)$-réseau hermitien unimodulaire (Λ, h_0) et, d'après le Théorème 1.2.5, cela implique que l'idéal fractionnaire intervenant dans l'écriture en pseudo-base de $\Lambda = \mathfrak{a} \cdot 1$ est un $\text{End}(E)$-inversible.

Par ailleurs, pour tout morphisme endomorphisme de E_Λ (resp. de $\mathbb{C}/\Lambda$) on peut associer un endomorphisme de $\mathbb{C}/\Lambda$ (resp. de E_Λ) via les isomorphismes ϕ_Λ de telle sorte

que le diagramme suivant commute

$$\begin{array}{ccc} E(\mathbb{C}) & \xrightarrow{f} & E(\mathbb{C}) \\ \downarrow{\scriptstyle \phi_\Lambda} & & \downarrow{\scriptstyle \phi_\Lambda} \\ \mathbb{C}/\Lambda & \xrightarrow[z\mapsto \alpha z]{\alpha} & \mathbb{C}/\Lambda. \end{array}$$

Ceci définit un isomorphisme $[\,]\colon \mathrm{End}(E) \to \mathrm{End}_{\mathbb{C}}(\Lambda)$ qui, d'après [Sil94, Proposition 1.1] est l'unique isomorphisme satisfaisant la relation suivante sur les différentielles

$$\forall \omega \in \Omega(E), [\alpha]^*\omega = \alpha\omega.$$

D'après [Sil09, Théorème VI.5.3], la correspondance

$$\begin{array}{rl} \{\text{tores complexes de dimension 1}\} & \longleftrightarrow \{\text{Courbes elliptiques sur } \mathbb{C}\} \\ \mathbb{C}/\Lambda & \longmapsto E/E(\mathbb{C}) = \phi_\Lambda(\mathbb{C}/\Lambda) \\ \mathbb{C}/\Lambda \text{ avec } g_4(\Lambda) = A \text{ et } g_6(\Lambda) = B & \longleftarrow\!\shortmid E\colon y^2 = 4x^3 - Ax - B \end{array}$$

est une équivalence de catégories.

2.2.3 Fonctions thétas

Nous avons déjà évoqué à plusieurs reprises l'équivalence de catégorie entre les variétés abéliennes complexes et les tores polarisables donné par $A \mapsto A(\mathbb{C})$. Par définition une variété abélienne A est projective donc $A(\mathbb{C}) \subseteq \mathbb{P}^n(\mathbb{C})$ pour un certain n. La question réciproque se pose ; étant donné un tore complexe polarisable peut-on reconstruire la variété abélienne correspondante ? En d'autres termes, peut-on construire un plongement (holomorphe) projectif d'un tore polarisable ?

Nous l'avons déjà fait dans la section 2.2.2 à l'aide des fonctions $\wp$ de Weierstrass. Malheureusement, ces fonctions ne se généralisent pas facilement aux dimensions supérieures bien qu'on puisse les retrouver à l'aide de fonctions thêta.

Pour reprendre les termes de [Deb05, Section I.1.3.1], étant donné un tore complexe polarisable $X = V/\Gamma$, l'idée générale pour construire des fonctions holomorphes de X

dans $\mathbb{P}^n(\mathbb{C})$ est de construire un diagramme commutatif

$$\begin{array}{ccc} V & \xrightarrow{\widetilde{u}} & \mathbb{C}^{n+1} \setminus \{0\} \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle p} \\ X & \xrightarrow{u} & \mathbb{P}^n(\mathbb{C}) \end{array} \tag{2.7}$$

où π et p sont les morphismes canoniques et les $n+1$ composantes $\widetilde{u}_0, \ldots, \widetilde{u}_n$ de $\widetilde{u}$ sont des fonctions holomorphes. Pour qu'un tel diagramme commute il faut que pour tout $z \in V, \gamma \in \Gamma, p \circ \widetilde{u}(z+\gamma) = u \circ \pi(z+\gamma) = u \circ \pi(z) = p \circ \widetilde{u}(z)$, donc

$$\widetilde{u}_i(z+\gamma) = f_\gamma(z)\widetilde{u}_i(z) \tag{2.8}$$

où f_γ est une fonction holomorphe qui ne s'annule pas (la même pour tous les $\widetilde{u}_i$). Les fonctions thêta permettent de construire de telles fonctions holomorphes et ce sont les seules façon d'en construire (voir [Deb05, Corollaire IV.3.4]).

Fonctions thêta et tores polarisables

Définition 2.2.10. *Soit Γ un $\mathbb{Z}$-réseau dans un espace vectoriel complexe V. On appelle fonction thêta associée à Γ toute fonction holomorphe non identiquement nulle $\vartheta \colon V \to \mathbb{C}$ telle que pour tout $\gamma \in \Gamma$ il existe une forme linéaire a_γ et une constante b_γ telles que*

$$\forall z \in V, \vartheta(z+\gamma) = e^{2i\pi(a_\gamma(z)+b_\gamma)}\vartheta(z).$$

On appelle la famille $(a_\gamma, b_\gamma)_{\gamma\in\Gamma}$ le type de ϑ.

On dira qu'une fonction thêta est *triviale* si elle ne s'annule pas. Le produit de deux fonctions thêta ϑ_1 et ϑ_2 de type respectifs (a^1_γ, b^1_γ) et (a^2_γ, b^2_γ) est une fonction thêta de type $(a^1_\gamma + a^2_\gamma, b^1_\gamma + b^2_\gamma)$. Deux fonctions thêta sont dites *équivalentes* si leur quotient ne s'annule pas.

Exemple 2.2.11. *1. Si on pose $\vartheta(z) = e^{\langle z,z\rangle}$ où $\langle \_, \_\rangle$ est une forme bilinéaire (pas forcément symétrique) alors $\vartheta(z+\gamma) = e^{\langle z,z\rangle+\langle z,\gamma\rangle+\langle\gamma,z\rangle+\langle\gamma,\gamma\rangle}$ c'est donc une fonction thêta de type $(a_\gamma = \langle \_, \gamma\rangle + \langle\gamma, \_\rangle, b_\gamma = \langle\gamma,\gamma\rangle)$. Puisque c'est une exponentielle elle ne s'annule pas et est donc une fonction thêta triviale. En fait, toutes les fonction thêta triviales s'écrivent de cette façon.*

2. *Soit τ une matrice carrée de taille g symétrique dont la partie imaginaire est définie positive. On peut définir pour tout vecteur colonne à coefficients réels a et b la fonction thêta de Riemann*

$$\vartheta \begin{bmatrix} a \\ b \end{bmatrix} (z, \tau) = \sum_{m \in \mathbb{Z}^g} \exp\Big(i\pi({}^t(m+a)\tau(m+a) + 2{}^t(m+a)(z+b) \Big).$$

Il s'agit d'une fonction thêta associée au réseau $\Gamma_\tau = \mathbb{Z}^g + \tau\mathbb{Z}^g$.

L'application $a\colon \Gamma \times V \to \mathbb{C}, (\gamma, z) \mapsto a_\gamma(z)$ est $\mathbb{Z}$-linéaire en la première variable et peut donc se prolonger en une forme $\mathbb{R}$-linéaire en la première variable et $\mathbb{C}$-linéaire en la seconde sur $V \times V$. On définit alors la *forme de Riemann* associée à ϑ par

$$\omega(x, y) = a(x, y) - a(y, x)$$

qui est une forme $\mathbb{R}$-bilinéaire prenant des valeurs entières sur Γ satisfaisant pour tout $x, y \in V, \omega(ix, iy) = \omega(x, y)$ (voir [Deb05, Proposition IV.1.3] pour les détails). La forme de Riemann associée à deux fonctions thêta équivalentes est la même. On peut définir

$$h(x, y) = \omega(x, iy) + i\omega(x, y)$$

et on peut vérifier que la forme $h\colon V \times V \to \mathbb{C}$ ainsi définie est une forme hermitienne positive (voir [Deb05, Proposition IV.1.5]). On peut aussi montrer ([Deb05, Exercice IV.3]) que toute fonction thêta est équivalente à une fonction thêta dite *normalisée* satisfaisant $a = \frac{1}{2i}h$ et $\operatorname{im} b_\gamma = -\frac{1}{4}h(\gamma, \gamma)$ si bien que

$$\vartheta(z + \gamma) = \alpha(\gamma) e^{\pi h(\gamma, z) + \frac{\pi}{2} h(\gamma, \gamma)} \vartheta(z)$$

où $\alpha\colon \Gamma \to U(1), \gamma = e^{2i\pi \operatorname{re}(b_\gamma)}$ et satisfait

$$\alpha(\gamma_1 + \gamma_2) = \alpha(\gamma_1)\alpha(\gamma_2)(-1)^{\omega(\gamma_1, \gamma_2)}$$

(ce n'est donc pas un morphisme de groupe mais presque, on appelle α un *semi-caractère* de Γ). On appelle aussi le couple (h, α) le *type* de la fonction ϑ. Bien qu'on ait déjà défini le type d'une fonction thêta par le couple (a_γ, b_γ) il n'y aura pas d'ambiguïté sur le type dont on parle puisque les objets dans les couples sont différents. L'avantage de travailler avec les types de la forme (h, α) est que la forme hermitienne h est définie directement à

partir de la forme de Riemann ω qui, comme on l'a dit plus haut, est un invariant de la classe d'équivalence de la fonction ϑ contrairement aux types (a_γ, b_γ).

On remarque aussi que la somme de fonctions thêta de même type est toujours une fonction thêta de ce type. De même le produit par un scalaire non nul ne change pas le type d'une fonction thêta. On peut alors définir l'espace vectoriel des fonctions thêta de type (h, α) (on rajoute la fonction nulle qui, par définition, n'est pas une fonction thêta).

Un résultat essentiel, déjà évoqué, qui illustre l'efficacité des fonctions thêta est le suivant.

Proposition 2.2.12 ([Deb05, Corollaire IV.3.4] et [Deb05, Corollaire IV.3.5])**.** *Soit X un tore complexe et $u\colon X \to \mathbb{P}^n(\mathbb{C})$ une application holomorphe. Il existe des fonctions thêta normalisées $\vartheta_1, \dots, \vartheta_n$ de même type (h, α) telles que*

$$\forall x \in X, u(x) = [\vartheta_1(x), \dots, \vartheta_n(x)]\,.$$

Par ailleurs, si il existe $x \in X$ tel que $u^{-1}\{u(x)\}$ est fini alors h est définie positive[6]*.*

On dira qu'une forme définie positive h sur V telle que $\operatorname{im} h(\Gamma, \Gamma) \subseteq \mathbb{Z}$ est une *polarisation* sur le tore $X = V/\Gamma$. On dira qu'un tore X tel qu'il existe une telle forme h est *polarisable* et qu'un couple (X, h) où h est une polarisation sur X est un tore *polarisé*.

On remarque que le fait que les fonctions thêta aient le même type revient à satisfaire la relation (2.8). Il reste à établir à quelles conditions sur X il existe « suffisamment » de fonctions thêta de même type pour qu'une telle application u soit un plongement. Sans surprise, cette condition sera l'existence d'une polarisation sur X.

Fibrés en droites holomorphes, fonctions thêta et plongement projectif

Dans cette section nous voulons introduire les *fibrés en droites* et expliquer le lien entre ces objets et les fonctions thêta. En particulier, nous introduirons des fibrés en droites de type (h, α) dont l'*espace des sections* est l'espace vectoriel des fonctions thêta de type (h, α). On verra aussi que tout fibré en droites est de cette forme, c'est le Théorème de Appell-Humbert [Deb05, Théorème V.5.10]. Enfin, nous verrons que des fibrés en droites ayant une *classe de Chern* h définie positive permettent de construire explicitement des plongements holomorphes du tore correspondant dans $\mathbb{P}^n(\mathbb{C})$, il s'agit du Théorème de

6. Dans [Deb05, Corollaire IV.3.5] l'auteur annonce seulement qu'il existe une *forme de Kähler* sur X. Voir les remarques [Deb05, III.1.1 et III.5.3] pour le lien avec les formes hermitiennes définies positives h.

Lefschetz [Deb05, Théorème VI.3.5]. Nous ne ferons que résumer grossièrement la théorie développée dans [Deb05]. Rentrer dans les détails nous emmènerait trop loin, en particulier nous ne parlerons pas de diviseurs qui fournissent une autre interprétation des fibrés en droites et offrent donc des outils supplémentaires pour démontrer les résultats qui nous intéressent.

Définition 2.2.13. *Soit X une variété complexe connexe. Un fibré en droites sur X est un couple (F,p) où F est une variété complexe et $p\colon F \to X$ est une application holomorphe surjective telle qu'il existe un recouvrement ouvert (U_α) de X et des isomorphismes $\psi_\alpha\colon p^{-1}(U_\alpha) \to U_\alpha \times \mathbb{C}$ tels que pour tout α,β la composition $\psi_\alpha\psi_\beta^{-1}\colon (U_\alpha \cap U_\beta)\times\mathbb{C} \to (U_\alpha\cap U_\beta)\times\mathbb{C}$ est donnée par*

$$\psi_\alpha\psi_\beta^{-1}(x,t) = (x, g_{\alpha\beta}(x)t) \tag{2.9}$$

où $g_{\alpha\beta}$ est une fonction holomorphe sur $U_\alpha\cap U_\beta$ qui ne s'annule pas qu'on appelle fonction de transition. On dit que (F,p) est trivialisé sur le recouvrement (U_α).

Une section du fibré (F,p) est une fonction holomorphe $s\colon X \to F$ qui satisfait $p\circ s = \mathrm{Id}_X$.

On dit que deux fibrés en droites (F,p) et (F',p') sur X sont isomorphes s'il existe une application holomorphe $u\colon F \to F'$ telles que $p'\circ u = p$ et telle que u soit linéaire sur les fibres, i.e. sur une trivialisation (U_α) commune à (F,p) et (F',p') on a

$$u({\psi_\alpha}^{-1}(x,t)) = {\psi'_\alpha}^{-1}(x, h_\alpha(x)t)$$

avec h_α holomorphe sur U_α et ne s'annule pas.

On pose $\Gamma(X,F)$ l'espace vectoriel des sections du fibré (F,p) où les lois d'addition et de produit externe sont définies localement sur les fonctions holomorphes de la seconde composante, i.e. si on note $s_{|U_\alpha}(x) = (x, s_\alpha(x))$

$$(s+s')_{|U_\alpha}(x) = (x, s_\alpha(x) + s'_\alpha(x)) \text{ et } \lambda s_{|U_\alpha}(x) = (x, \lambda s_\alpha(x)).$$

On définit aussi le tiré en arrière par $u\colon X \to Y$ d'un fibré (F,p) sur Y, noté u^*F, par

$$u^*F = \{(x,\ell) \in X \times F, u(x) = p(\ell)\}.$$

L'application u induit une application linéaire sur les sections donnée par

$$\begin{aligned} \Gamma(u)\colon \qquad \Gamma(Y,F) &\longrightarrow \Gamma(X,u^*F) \\ s_{|U}(y) = (y,s(y)) &\longmapsto \Gamma(u)(s)_{|u^{-1}U}\colon x \mapsto (x,s(u(x))) \end{aligned}$$

Exemple 2.2.14. *1. L'exemple le plus simple de fibré en droites est le fibré trivial, défini par la première projection $F_0 = X \times \mathbb{C} \to X$ dont l'espace des sections peut être identifié aux fonctions holomorphes sur X de la façon suivante*

$$\begin{aligned} \mathcal{O}(X) &\longrightarrow \Gamma(X,F_0) \\ s &\longmapsto (x \mapsto (x,s(x)))\,. \end{aligned}$$

2. Soit V un espace vectoriel complexe. Un autre exemple très important est le fibré sur $\mathbb{P}(V)$ donné par

$$F = \{(x,v) \in \mathbb{P}(V) \times V, v \in \ell_x = \mathrm{Vect}(x)\}$$

noté $\mathcal{O}_{\mathbb{P}(V)}(-1)$.

La donnée des fonctions de transistion $g_{\alpha\beta}$ définies par (2.9) permet de reconstruire le fibré (F,p) correspondant en identifiant le point $(x,t) \in U_\alpha \times \mathbb{C}$ et $(x, g_{\alpha\beta}(x)t) \in U_\beta \times \mathbb{C}$ pour tout $x \in U_\alpha \cap U_\beta, t \in \mathbb{C}$. Ceci fournit une définition alternative de fibré en droites sur X ; c'est la donnée d'un recouvrement (U_α) de X et de fonctions holomorphes $g_{\alpha\beta}$ qui ne s'annulent pas, définies sur $U_\alpha \cap U_\beta$ et qui satisfont pour tout α, β, γ la relation

$$g_{\alpha\alpha} = g_{\alpha\beta}g_{\beta\gamma}g_{\gamma\alpha} = \mathrm{id} \ \text{ sur } U_\alpha \cap U_\beta \cap U_\gamma.$$

On dit alors que le fibré (F,p) ou F est défini par le couple formé de la trivialisation et des fonctions de transition $((U_\alpha),(g_{\alpha\beta}))$ abrégé $(U_\alpha, g_{\alpha\beta})$. L'avantage de cette construction est qu'elle nous permet de définir de nouveaux fibrés en droites à partir de fibrés existant. Si (F,p) est défini par les fonctions de transition $g_{\alpha\beta}$ sur un recouvrement U_α on peut définir F^{-1}, appelé le *dual* de F, le fibré défini par les fonctions de transition $\left(\frac{1}{g_{\alpha\beta}}\right)$ sur la même trivialisation. De même pour (F',p') un autre fibré caractérisé par les fonctions de transition $(h_{\alpha\beta})$ (on peut les supposer définis sur le même recouvrement quitte à choisir des recouvrements plus fins) on définit le *produit tensoriel* de F et F', noté $F \otimes F'$, par le fibré défini par les fonctions de transition $g_{\alpha\beta}h_{\alpha\beta}$. Ceci munit l'ensemble des classes d'isomorphisme de fibrés en droites d'une structure de groupe qu'on note $\mathrm{Pic}(X)$.

On peut alors montrer qu'une section d'un fibré $(U_\alpha, g_{\alpha\beta})$ revient à la donnée de fonctions holomorphes $s_\alpha \colon U_\alpha \to \mathbb{C}$ satisfaisant pour tout $\alpha, \beta, s_\alpha = g_{\alpha\beta} s_\beta$.

Exemple 2.2.15. *On considère $X = \mathbb{P}(V)$ où V est de dimension n. Choisir un recouvrement de X peut se faire en fixant une base (e_α) de V. Les ouverts U_α sont alors identifiés avec l'image par $\pi \colon V \to \mathbb{P}(V)$, la projection canonique, des hyperplans affines*

$$H_\alpha = \left\{ \sum_{i=1}^{n} \lambda_i e_i, \lambda_\alpha = 1 \right\} \subseteq V, \alpha = 1, \dots, n.$$

La projection π définit alors un isomorphisme π_α de H_α sur son image dans $\mathbb{P}(V)$.

On peut alors vérifier que

$$\begin{array}{rccc} \psi_\alpha \colon & p^{-1}(U_\alpha) & \longrightarrow & U_\alpha \times \mathbb{C} \\ & (x, v) & \longmapsto & \left(x, \frac{v}{\pi_\alpha(x)}\right) \end{array}$$

où $\frac{v}{\pi_\alpha(x)}$ est un abus de notation qui désigne l'unique scalaire $t \in \mathbb{C}$ tel que $v = t\pi_\alpha(x)$. On peut alors vérifier que $\psi_\alpha \psi_\beta^{-1}(x, t) = \left(x, \frac{\lambda_\alpha}{\lambda_\beta} t\right)$ où $x = [\lambda_1 \colon \dots \colon \lambda_n]$. Autrement dit, les fonctions de transition satisfont $g_{\alpha\beta}([\lambda_1 \colon \dots \colon \lambda_n]) = \frac{\lambda_\alpha}{\lambda_\beta}$. Une section est alors la donnée d'une famille de fonctions holomorphes $(s_1, \dots, s_n)$ telles que

$$\forall \alpha, \beta, s_\beta = \frac{\lambda_\beta}{\lambda_\alpha} s_\alpha.$$

On voit immédiatement que les fonctions $s_\alpha^j = \frac{\lambda_j}{\lambda_\alpha}$ sont des sections du fibré dual $\mathcal{O}_{\mathbb{P}(V)}(-1)^{-1} = \mathcal{O}_{\mathbb{P}(V)}(1)$. En fait cette famille forme une base des sections de ce fibré. Toute section non nulle de $\mathcal{O}_{\mathbb{P}(V)}(1)$ s'annule sur un hyperplan de $\mathbb{P}(V)$. Remarquons que $\mathcal{O}_{\mathbb{P}(V)}(-1) \otimes \mathcal{O}_{\mathbb{P}(V)}(1)$ est isomorphe au fibré trivial, dont l'espace des sections est l'ensemble des fonctions holomorphes sur $\mathbb{P}(V)$ qui est réduit aux fonctions constantes. Étant données une section s de $\mathcal{O}_{\mathbb{P}(V)}(-1)$ et une section non nulle s' de $\mathcal{O}_{\mathbb{P}(V)}(1)$, ss' définit une fonction holomorphe sur $\mathbb{P}(V)$ qui est donc constante et s'annule car s' s'annule, c'est donc la section nulle. Donc s est aussi la section nulle et $\mathcal{O}_{\mathbb{P}(V)}(-1) = \{0\}$ [7].

Si on considère un fibré en droites $p \colon F \to X$ et un sous espace vectoriel de dimension

7. Merci à Fabien Kutle qui a pensé à cette jolie preuve lors de nos longues discussions mathématiques. En sachant que $\Gamma\left(\mathbb{P}(V), \mathcal{O}_{\mathbb{P}(V)}(r)\right)$ est isomorphe à l'espace des polynômes homogènes de degré r on pourrait montrer par le même argument que $\Gamma\left(\mathbb{P}(V), \mathcal{O}_{\mathbb{P}(V)}(-r)\right) = \{0\}$, avec $\mathcal{O}_{\mathbb{P}(V)}(r) = \mathcal{O}_{\mathbb{P}(V)}(1) \otimes \cdots \otimes \mathcal{O}_{\mathbb{P}(V)}(1)$ et $\mathcal{O}_{\mathbb{P}(V)}(-r) = \mathcal{O}_{\mathbb{P}(V)}(r)^{-1}$.

finie V de $\Gamma(X,F)$ de base $s_1,\dots,s_n$ alors on peut définir une application méromorphe

$$\begin{array}{rccc} \psi_V\colon & X & \dashrightarrow & \mathbb{P}(V) \\ & x & \longmapsto & [s_1(x)\colon \dots \colon s_n(x)]. \end{array} \tag{2.10}$$

La flèche en pointillés indique que la fonction ψ_V n'est pas définie partout ; elle n'est pas définie sur le lieu des zéros communs à toutes les sections s_i.

On sait désormais qu'étant donné un fibré sur un tore complexe on peut construire des fonctions holomorphes de celui-ci dans l'espace projectif. Cependant, on ne sait pas, a priori, comment en construire. On va voir comment en construire et on verra que cette construction les donne tous (à isomorphisme près).

Soit (h,α) un type de fonctions thêta normalisées sur un tore $X = V/\Gamma$. On pose F le quotient de $V\times\mathbb{C}$ par l'action de Γ donnée par

$$(z,t)\cdot\gamma = \left(z+\gamma, \frac{\vartheta(z+\gamma)}{\vartheta}t\right)$$

où ϑ est une fonction thêta normalisée de type (h,α), i.e. $\frac{\vartheta(z+\gamma)}{\vartheta} = \alpha(\gamma)e^{\pi h(\gamma,z)+\frac{\pi}{2}h(\gamma,\gamma)}$. La première projection $p\colon F\to V/\Gamma$ fait de (F,p) un fibré en droites sur X dit de *type* (h,α) que l'on note $F(h,\alpha)$. On peut alors décrire très facilement la structure du sous-groupe de $\mathrm{Pic}(X)$ engendré par les fibrés de type (h,α) (pour h,α parcourant les types) comme suit

$$F(h_1,\alpha_1)\otimes F(h_2,\alpha_2) = F(h_1+h_2,\alpha_1\alpha_2).$$

On peut alors citer le Théorème de Appell-Humbert.

Théorème 2.2.16 ([Deb05, Théorème V.5.10])**.** *Tout fibré en droites $F\to X$ sur un tore complexe X est isomorphe à un fibré $F(h,\alpha)$ pour un unique couple (h,α) appelé le type de F.*

Et le Théorème de Lefschetz.

Théorème 2.2.17 ([Deb05, Théorème VI.3.5])**.** *Soit X un tore complexe et F un fibré en droites de type (h,α) sur X. Si h est définie positive alors $\psi_{\Gamma(X,F^r)}$ (définie en (2.10)) est un plongement holomorphe pour $r\geq 3$.*

Ainsi, toute forme hermitienne définie positive h telle que $\operatorname{im} h(\Gamma,\Gamma)\subseteq\mathbb{Z}$ fournit des plongements projectifs. D'autre part, les plongements projectifs ne peuvent être obtenus

qu'à partir d'une telle forme d'après la Proposition 2.2.12. On synthétise ces résultats dans le théorème suivant.

Théorème 2.2.18. *Soit $X = V/\Gamma$ un tore complexe. Alors il existe un plongement holomorphe de X dans un espace projectif si, et seulement s'il existe une forme hermitienne h sur V définie positive telle que* $\operatorname{im} h(\Gamma, \Gamma) \subseteq \mathbb{Z}$*, i.e. si X est un tore polarisable.*

Il peut paraître surprenant qu'on ait expliciter de tels plongements pour un tore de dimension 1 quelconque, sans hypothèse d'existence de telle forme. Ce n'est pas une contradiction ; un réseau $\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ admet toujours une telle forme hermitienne. Par exemple celle donnée par

$$h_\Lambda(x, y) = \frac{x\overline{y}}{\operatorname{im}(\omega_1\overline{\omega_2})}$$

convient.

Le théorème de Riemann-Roch ([Deb05, Théorème VI.2.2]) donne la dimension de l'espace des fonctions thêta du fibré $F(L, \alpha)$. On remarque que si h provient d'une polarisation principale et que X est de dimension g, le théorème de Lefschetz et le Théorème de Riemann-Roch montrent que $\psi_{\Gamma(X, F(3H, \alpha^3))}$ est un plongement de X dans $\mathbb{P}^{3^g}(\mathbb{C})$.

Tores polarisables et variétés abéliennes complexes

Dans la Section 2.2.3 il n'était question que de tores complexes et non de variétés abéliennes. D'après le théorème de Chow une variété complexe compacte X peut être munie d'une structure de variété algébrique complexe si, et seulement s'il existe un plongement holomorphe de X dans un espace projectif. C'est donc le cas pour les tores complexes polarisables uniquement.
Réciproquement, pour toute variété abélienne complexe A, il existe un espace vectoriel V et un réseau Γ tel que $A(\mathbb{C}) \simeq V/\Gamma$ (voir par exemple le tout début du livre [Mum70, Chapter I.(1)] ou encore [Mil08, Proposition 2.7.(b)]). Il est clair que puisqu'une variété abélienne A est une variété projective alors $A(\mathbb{C}) \subseteq \mathbb{P}^n(\mathbb{C})$ pour un certain n et donc V/Γ est un tore polarisable. On résume cela dans le théorème suivant (qu'on retrouvera [Mil08, Theorem 2.9]).

Théorème 2.2.19. *Le foncteur*

$$\mathbf{H}_{\mathbb{C}} \colon A \mapsto A(\mathbb{C})$$

définit une équivalence de catégories entre les variétés abéliennes complexes et les tores complexes polarisables.

Dans cette section nous souhaitons détailler d'avantage les liens entre les variétés abéliennes et les tores complexes polarisables. Comment interprète-t-on la variété duale à travers le foncteurs ? Qu'en est-il des isogénies ? De leur degré ? Des polarisations ?

Étant donné un morphisme $f\colon A \to A'$ tel que $A(\mathbb{C}) \simeq V/\Gamma$ et $A'(\mathbb{C}) \simeq V'/\Gamma', \varphi = \mathbf{H}_{\mathbb{C}}(f)\colon V/\Gamma \to V'/\Gamma'$ est un morphisme de tores complexes. Si f est une isogénie, i.e. un morphisme surjectif et $\dim A = \dim A'$ alors φ est une isogénie aussi car f est surjective. Par ailleurs, puisqu'on est en caractéristique 0, f est nécessairement une isogénie séparable et les points de son noyau sont formés des points fermés donc dans $A(\mathbb{C})$. On en déduit donc que

$$\begin{aligned}
\deg f &= \#(\ker f)(\mathbb{C}) \\
&= \#\left\{\pi(x), \varphi(\pi(x)) = 0\right\} && \text{avec } \pi\colon V \to V/\Gamma \text{ la projection canonique} \\
&= \#\left\{\pi(x), \varphi_{\mathrm{an}}(x) + \Gamma \subseteq \Gamma'\right\} \\
&= \#\left(\Gamma/\varphi_{\mathrm{an}}^{-1}(\Gamma')\right) \\
&= \#\left(\varphi_{\mathrm{an}}(\Gamma)/\Gamma'\right) && \text{car } \varphi_{\mathrm{an}} \text{ est bijective} \\
&= \#\left(\varphi_{\mathrm{rat}}(\Gamma)/\Gamma'\right) && \text{car } \varphi_{\mathrm{rat}} = \varphi_{\mathrm{an}|\Gamma} \text{ par définition}
\end{aligned}$$

d'où

$$\deg f = [\Gamma'\colon \varphi_{\mathrm{rat}}(\Gamma)]\,. \tag{2.11}$$

Par ailleurs, si $A(\mathbb{C}) \simeq V/\Gamma$ alors la variété abélienne duale $\widehat{A}$ de A satisfait la relation $\widehat{A}(\mathbb{C}) \simeq V^*/\widehat{\Gamma}$ où V^* désigne l'espace des formes antilinéaire sur V et

$$\widehat{\Gamma} = \{\ell \in V^*, \ell(\Gamma) \subseteq \mathbb{Z}\}$$

(voir la construction après [Mum70, Chapter II.9 Corollary 86] ou encore [BL94, Section 2.4]). D'autre part, si $f\colon A \to A'$ est un morphisme de variétés abéliennes et $\varphi = \mathbf{H}_{\mathbb{C}}(f), \mathbf{H}_{\mathbb{C}}(A) = V/\Gamma$ et $\mathbf{H}_{\mathbb{C}}(A') = V'/\Gamma'$ alors le morphisme dual $\widehat{f}\colon \widehat{A'} \to \widehat{A}$ vérifie $\mathbf{H}_{\mathbb{C}}\left(\widehat{f}\right)_{\mathrm{an}} = \varphi_{\mathrm{an}}^*$ où

$$\begin{aligned}
\varphi_{\mathrm{an}}^*\colon \quad V'^* &\longrightarrow V^* \\
\ell &\longmapsto \ell \circ \varphi_{\mathrm{an}}.
\end{aligned}$$

Considérons maintenant une polarisation $a\colon A \to \widehat{A}$, i.e. un morphisme de la forme $a = a_{\mathscr{L}}\colon x \mapsto t_x^*\mathscr{L} \otimes \mathscr{L}^{-1}$ avec $\mathscr{L}$ un fibré en droites ample et où t_x désigne la translation

par x de A dans A. Un tel morphisme satisfait toujours $\widehat{a} = a$ en identifiant canoniquement A avec son bidual (toujours vrai sans condition d'amplitude sur le fibré $\mathscr{L}$). D'autre part, $\rho_h = \mathbf{H}_{\mathbb{C}}(a)_{\mathrm{an}} \colon V \to V^*$ doit satisfaire $\rho_h^* = \rho_h$ et induit donc une forme hermitienne $h(x,y) = \rho_h(x)(y)$. Il s'agit de la première classe de Chern du fibré $\mathscr{L}(h,\alpha)$ induit sur A. Lorsque $\mathscr{L}$ est ample, la forme h est définie positive. On peut alors compléter l'équivalence de catégories $\mathbf{H}_{\mathbb{C}}$ en une équivalence entre la catégorie des variétés abéliennes complexes polarisées et les tores polarisés, notée $\mathbf{H}^p_{\mathbb{C}} \colon (A,a) \mapsto (\mathbf{H}_{\mathbb{C}}(A) = A(\mathbb{C}), h)$, avec h la forme induite par $\rho_h = \mathbf{H}_{\mathbb{C}}(a)$. On définit un morphisme de variétés abéliennes polarisées $f \colon (A,a) \to (A',a')$ non pas comme un morphisme entre les variétés abéliennes sous-jacente mais on veut en plus que le morphisme commute avec les polarisations de la manière suivante

$$\begin{array}{ccc} A & \xrightarrow{f} & A' \\ \downarrow{\scriptstyle a} & & \downarrow{\scriptstyle a'} \\ \widehat{A} & \xleftarrow[\widehat{f}]{} & \widehat{A'} \end{array} ,$$

i.e. $a = \widehat{f} a' f$. Cette condition impose que A et A' soient de même dimension et que f soit une isogénie. On parlera alors d'isogénies polarisées et non de morphismes polarisés pour être plus précis. On peut définir exactement la même notion d'isogénies polarisées pour les tores complexes polarisés, i.e. un morphisme de tores polarisés $\varphi \colon (V/\Gamma, \rho_h) \to (V'/\Gamma', \rho_{h'})$ est un morphisme de tores qui satisfait $\rho_h = \varphi_{\mathrm{an}}^* \rho_{h'} \varphi_{\mathrm{an}}$. On peut vérifier que c'est équivalent à pour tout x, y de V

$$h'\left(\varphi_{\mathrm{an}}(x), \varphi_{\mathrm{an}}(y)\right) = h(x,y).$$

Autrement dit, les morphismes polarisés entre tores polarisés ont pour représentation analytique des isométries entre les espaces hermitiens sous-jacent.

Thêta constantes et espaces de modules

Nous profitons d'avoir développé la théorie des fonctions thêta sur $\mathbb{C}$ pour donner un aperçu des *thêta constantes* dans ce même cadre. Ces thêta constantes paramètrisent l'espace de modules des variétés abéliennes d'un type donné, c'est-à-dire que calculer les thêta constantes associées à une variété abélienne polarisée permet de décrire complètement sa classe d'isomorphisme.
Il est possible de développer une théorie similaire sur n'importe quel corps de caractéris-

tique différente de 2. C'est ce qu'a fait David Mumford dans les trois articles [Mum66], [Mum67a] et [Mum67b]. Malheureusement, décrire cette merveilleuse théorie nous mènerait trop loin et je ne le ferai donc pas dans ce manuscrit.

Soit h une polarisation sur un tore $X = V/\Gamma$. D'après [Deb05, Proposition VI.1.1], il existe une $\mathbb{Z}$-base $(\gamma_1, \dots, \gamma_{2g})$ de Γ telle que la forme réelle bilinéaire non dégénérée $\omega = \operatorname{im} h$ s'écrive

$$\begin{pmatrix} 0 & \Delta \\ -\Delta & 0 \end{pmatrix}$$

où Δ est une matrice diagonale de coefficients $d_1 | \cdots | d_g$ entiers positifs. On appelle Δ le type de la polarisation h (ou du tore polarisé (X, h)).

On veut paramétrer les classes d'isomorphisme de tores polarisés (X, h) où h est de type fixé Δ. D'après les conditions de Riemann ([Deb05, Théorème VI.1.3]) il existe toujours une base de V telle que dans cette base

$$\Gamma = \Gamma_\tau = \tau\mathbb{Z}^g \oplus \Delta\mathbb{Z}$$

où τ est une matrice carrée symétrique de partie imaginaire définie positive. Puisqu'on a fixé une base $\mathscr{B} = (\gamma_1, \dots, \gamma_g)$ de V on peut l'identifier à $\mathbb{C}^g$. On peut alors identifier X à $X_\tau = \mathbb{C}^g/\Gamma_\tau$. On pose

$$\mathscr{H}_g = \left\{\tau \in M_g(\mathbb{C}), {}^t\tau = \tau \text{ et } \operatorname{im}\tau \text{ définie positive}\right\}$$

le demi-espace de Siegel. Il s'agit d'un espace analytique de dimension $\frac{g(g+1)}{2}$.

Deux tores $(X_{\tau'}, h')$ et (X_τ, h) sont isomorphes si, et seulement si, il existe une application $\mathbb{C}$-linéaire u telle que

— $u(\Gamma_{\tau'}) = \Gamma_\tau$

— u est une isométrie entre les espaces hermitiens, i.e. $h = u^*h' \colon (x, y) \mapsto h'(u(x), u(y))$.

La première condition se traduit par le fait que la matrice N de u dans les $\mathbb{Z}$-bases $(\gamma_1, \dots, \gamma_{2g})$ et $\left(\gamma'_1, \dots, \gamma'_{2g}\right)$ de Γ_τ et $\Gamma_{\tau'}$ vérifie $\sigma_\Delta(N) = M$ où

$$\begin{aligned} \sigma_\Delta \colon \quad M_{2g}(\mathbb{Z}) &\longrightarrow M_{2g}(\mathbb{Q}) \\ P &\longmapsto \begin{pmatrix} I_g & 0 \\ 0 & \Delta \end{pmatrix}^{-1} P \begin{pmatrix} I_g & 0 \\ 0 & \Delta \end{pmatrix} \end{aligned}$$

telle que ${}^tM = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ et $\tau' = (a\tau + b)(c\tau + d)^{-1}$. La seconde par le fait, qu'avec les mêmes notations, on ait

$$MJ{}^tM = J$$

avec $J = \begin{pmatrix} 0 & I_g \\ -I_g & 0 \end{pmatrix}$ (voir [Deb05, Chapitre VII, Section 1.] pour les détails). On note avec $\mathrm{Sp}_{2g} = \{M \in \mathrm{GL}_{2g}(\mathbb{Q}), MJ{}^tM = J\}$ le groupe symplectique. Autrement dit, (X_τ, h) et $(X_{\tau'}, h')$ sont isomorphes (i.e. il existe une isogénie polarisée entre les deux) si, et seulement s'il existe une matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ dans le groupe

$$G_\Delta = \sigma_\Delta\left(M_{2g}(\mathbb{Z})\right) \cap \mathrm{Sp}_{2g}(\mathbb{Q})$$

telle que $\tau' = (a\tau + b)(c\tau + d)^{-1}$.

On en déduit que l'ensemble $\mathscr{A}_{g,\Delta} = \mathscr{H}_g/G_\Delta$ des orbites de $\mathscr{H}_g$ par l'action du groupe G_Δ paramétrise l'ensemble des classes d'isogénie polarisée des variétés abéliennes de type Δ. D'après [Deb05, Théorème 1.2] et [Deb05, Proposition 1.3], on peut même munir $\mathscr{A}_{g,\Delta}$ d'une structure de d'espace analytique, qu'on appelle *espace de modules* de tores polarisés de type Δ.

Lorsqu'on considère des espaces de modules de certains objets dont on souhaite classifier ou paramétriser les classes d'isomorphisme, on considère l'ensemble de ces objets qu'on quotiente par des sous-ensemble jusqu'à ce que chaque élément du quotient représente une classe d'isomorphisme comme nous venons de le faire pour l'ensembles des tores polarisés de type Δ représentés par $\mathscr{H}_g$ puis quotienté par l'action de G_Δ. Cependant, on souhaite que cet ensemble ait une structure similaire à celle des objets que l'on considère. En l'occurrence, nous considérions des tores complexes qui ont une structure d'espace analytique[8] et on vient de voir que l'espace qui les paramètrise, $\mathscr{A}_{g,\Delta}$, peut aussi être muni d'une structure d'espace analytique. C'est bien, mais on voudrait mieux. En effet, dans la section précédente on a montré, grâce aux théorèmes de Chow, que les tores polarisables ont une structure supplémentaire surprenante : ce sont des variétés algébriques projectives. Pour le moment notre espace $\mathscr{A}_{g,\Delta}$ n'a pas l'air de pouvoir être muni d'une telle structure algébrique. Cependant, nous allons procéder comme nous l'avons déjà fait pour les tores complexes que nous souhaitions plonger dans un espace projectif au début de la Section 2.2.3 ; nous allons chercher des « fonctions » $\mathscr{H}_g \to \mathbb{P}^n(\mathbb{C})$ compatibles avec

8. Mieux ! De variété complexe lisse, mais on ne peut pas tout avoir...

l'action de G_Δ pour construire des fonctions holomorphes [9] de $\mathscr{A}_{g,\Delta}$ dans $\mathbb{P}^n(\mathbb{C})$. Malheureusement, le théorème de Chow ne nous permettra pas de conclure de la même façon que nous l'avons fait pour les tores. En effet, quand on plongeait un tore dans $\mathbb{P}^n(\mathbb{C})$ c'est le fait que ce tore était une variété lisse et compacte qui nous permettait de conclure que son plongement était en fait une variété algébrique projective lisse. Notre espace analytique $\mathscr{A}_{g,\Delta}$ n'est pas lisse. Par exemple, d'après [Deb05, Théorème 1.5], pour $g \geq 3$ les points lisses de $\mathscr{A}_{g,\Delta}$ sont exactement les classes d'isomorphisme des tores polarisés qui ont pour groupe d'automorphisme $\{\pm \mathrm{id}\}$. Pourtant, nous allons voir que $\mathscr{A}_{g,\Delta}$ peut être muni d'une structure de variété quasi-projective, i.e. isomorphe au complémentaire d'une variété algébrique projective dans une autre.

Approche intuitive des formes modulaires Reprenons l'idée diagramme commutatif (2.7). Si on a une application holomorphe $u\colon \mathscr{A}_{g,\Delta} \longrightarrow \mathbb{P}^n(\mathbb{C})$ alors elle se relève en une application holomorphe $\widehat{u}\colon \mathscr{H}_g \longrightarrow \mathbb{C}^{n+1} \setminus \{0\}$ telle que le diagramme suivant commute

$$\begin{array}{ccc} \mathscr{H}_g & \xrightarrow{\widetilde{u}} & \mathbb{C}^{n+1} \setminus \{0\} \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle p} \\ \mathscr{A}_{g,\Delta} & \xrightarrow{u} & \mathbb{P}^n(\mathbb{C}) \end{array} \tag{2.12}$$

où $\pi\colon \mathscr{H}_g \longrightarrow \mathscr{A}_{g,\Delta}$ est le revêtement universel de $\mathscr{A}_{g,\Delta}$ et p la projection canonique. Ceci signifie que les composante $\widetilde{u}_i$ de $\widetilde{u}$ ne doivent pas toutes s'annuler simultanément et doivent satisfaire pour tout $M \in G_\Delta, \tau \in \mathscr{H}_g$,

$$\widetilde{u}_i(M \cdot \tau) = f_M(\tau)\widetilde{u}_i(\tau)$$

avec f_M une fonction holomorphe indépendante de i qui ne s'annule pas. Si on se rappelle bien le début de la Section 2.2.3, nous avions immédiatement après défini les fonctions thêta qui allaient plus tard intervenir comme les composantes des fonctions $\widetilde{u}$ définies alors et donc fournir des fonctions holomorphes (voire des plongements pour les tores chanceux) dans un espace projectif. Nous allons donc définir un analogue des fonctions thêta pour les espaces de modules ; les formes modulaires.

Revenons un peu en arrière où nous avons défini les fonctions thêta de Riemann dans

9. Quitte à rajouter des structures aux éléments de $\mathscr{A}_{g,\Delta}$ pour le faire grossir.

l'Exemple 2.2.11. Nous rappelons qu'elles sont définies pour deux vecteurs réels a et b par

$$\vartheta \begin{bmatrix} a \\ b \end{bmatrix} (z, \tau) = \sum_{m \in \mathbb{Z}^g} \exp\left(i\pi ({}^t(m+a)\tau(m+a) + 2{}^t(m+a)(z+b) \right)$$

et qu'il s'agit d'une fonction thêta associée au réseau $\Gamma_\tau = \mathbb{Z}^g + \tau\mathbb{Z}^g$. D'autre part, Debarre montre que la famille de fonctions thêta de Riemann $\left(\vartheta \begin{bmatrix} a \\ 0 \end{bmatrix} (\_, \tau) \right)_{a \in \Delta^{-1}\mathbb{Z}^g/\mathbb{Z}^g}$ forme une base de l'espace des sections du fibré $F(h, \alpha)$ où h est définie par $h(z, z') = {}^t z \left(\operatorname{im} \tau\right)^{-1} \overline{z'}$ de type Δ et

$$\begin{aligned} \alpha \colon \quad \tau\mathbb{Z}^g \oplus \Delta\mathbb{Z}^g &\longrightarrow \{-1, 1\} \\ \tau p + \Delta q &\longmapsto (-1)^{{}^t p \Delta q}. \end{aligned}$$

Par hypothèse, la matrice $\operatorname{im} \tau$ est définie positive donc h est définie positive. Si $m | \Delta$ alors $F_m = F\left(\frac{1}{m} h, \alpha_m\right)$ où $\alpha_m(\tau p + \Delta q) = (-1)^{{}^t p \left(\frac{1}{m}\Delta\right) q}$ est un fibré en droites sur X_τ car $\frac{1}{m} h$ est de type $\frac{1}{m}\Delta$ et α_m est un semi-caractère. Puisque $\frac{1}{m} h$ est définie positive, d'après le Théorème de Lefschetz (Théorème 2.2.17), pour $m \geq 2, \psi_{F_m^m} = \psi_{F(h,\alpha)}$ définit une application holomorphe vers un espace projectif et, si $m \geq 3$, il s'agit d'un plongement holomorphe projectif. En particulier, pour $m \geq 2$ les $\vartheta \begin{bmatrix} a \\ 0 \end{bmatrix} (\_, \tau)$ ne s'annulent jamais toutes simultanément.

Définition 2.2.20 (Formes modulaires)**.** *Soit G un sous-groupe de $\mathrm{Sp}_{2g}(\mathbb{Q})$ et $k \in \mathbb{Q}$. On appelle forme modulaire de poids k pour G toute fonction holomorphe $f \colon \mathscr{H}_g \longrightarrow \mathbb{C}$ telle que pour tout $M \in G_\Delta, \tau \in \mathscr{H}_g$ on ait*

$$f(M \cdot \tau) = \det(c\tau + d)^k f(\tau).$$

On pose

$$G_\Delta(\Delta) = \left\{ \begin{pmatrix} I_g + \Delta a & \Delta b \Delta \\ c & I_g + d\Delta \end{pmatrix} \in \mathrm{Sp}_{2g}(\mathbb{Z}), a, b, c, d \in M_g(\mathbb{Z}) \right\}$$

qui est un sous-groupe de G_Δ et

$$G_\Delta^0 = \left\{ \begin{array}{l} \begin{pmatrix} I_g + \Delta a & \Delta b \Delta \\ c & I_g + d\Delta \end{pmatrix} \in \mathrm{Sp}_{2g}(\mathbb{Z}), a, b, c, d \in M_g(\mathbb{Z}) \text{ les coefficients} \\ \text{diagonaux des matrices } \Delta^{-1} a {}^t b \Delta^{-1} \text{ et de } c {}^t d \text{ sont des entiers pairs} \end{array} \right\}$$

qui est un sous-groupe de $G_\Delta(\Delta)$.

Proposition 2.2.21. *Supposons* $4|d_1$ *alors pour* $a \in \Delta^{-1}\mathbb{Z}^g/\mathbb{Z}^g$, *la fonction*

$$\begin{array}{rcl} \mathscr{H}_g & \longrightarrow & \mathbb{C} \\ \tau & \longmapsto & \vartheta \begin{bmatrix} a \\ 0 \end{bmatrix} (0, \tau) \end{array}$$

est une forme modulaire de poids $\frac{1}{2}$ *pour* G^0_Δ.

On déduit du diagramme (2.12) que cette fonction descend en une fonction holomorphe $\psi \colon \mathscr{A}^0_{g,\Delta} = \mathscr{H}_g/G^0_\Delta \longrightarrow \mathbb{P}^{d_1 \cdots d_g - 1}(\mathbb{C})$ (car l'espace des sections de $F(h, \alpha)$ est de dimension $\det \Delta$ lorsque h est de type Δ d'après le Théorème de Riemann-Roch). Plus précisément, on a le théorème suivant ([Deb05, Théorème 4.1]).

Théorème 2.2.22. *Pour* $d_1 \geq 4$ *pair, la fonction* $\psi \colon \mathscr{A}^0_{g,\Delta} \longrightarrow \mathbb{P}^{d_1 \cdots d_g - 1}(\mathbb{C})$ *est un plongement holomorphe. Elle induit un isomorphisme entre* $\mathscr{A}_{g,\Delta}$ *et une sous-variété quasi-projective de* $\mathbb{P}^{d_1 \cdots d_g - 1}(\mathbb{C})$.

D'après un théorème de Grauert et Remmert ([BL94, Theorem A.5]) on peut munir aussi $\mathscr{A}_{g,\Delta}$ et $\mathscr{A}_{g,\Delta}(\Delta) = \mathscr{H}_g/G_\Delta(\Delta)$ d'une structure de variété quasi-projective.

Une interprétation intéressante de ces résultats est qu'il existe une variété quasi-projective $\mathscr{A}_{g,\Delta}$ qui paramétrise les tores polarisés (donc les variétés abéliennes) d'un certain type Δ dès lors que $4|d_1$. C'est à dire que la donnée des thêta constantes associée à une variété abélienne polarisée détermine la classe d'isomorphisme de cette dernière.
On peut aussi donner une interprétation des espaces $\mathscr{A}_{g,\Delta}(\Delta)$ et $\mathscr{A}^0_{g,\Delta}$ comme des variétés paramétrisant les variétés abéliennes de type Δ munies d'une structure supplémentaire (une Δ-*structure* pour $\mathscr{A}_{g,\Delta}(\Delta)$ et une Δ-*structure orthogonale* pour $\mathscr{A}^0_{g,\Delta}$).

Comme cela a déjà été dit, grâce aux travaux de David Mumford, il est possible de paramétrer les espaces de modules des variétés abéliennes sur des corps quelconques de caractéristique différente de 2 grâce à des constructions similaires de thêta constantes dites algébriques. Dans [KNRR21] nous expliquons comment calculer ces thêta constantes algébriques associées à la classe d'isomorphisme d'une variété abélienne polarisée isogène à un produit d'une courbe à multiplication complexe par un ordre quadratique à partir des thêta constantes de cette courbe. Nous nous en servons pour calculer l'obstruction de Serre d'une variété abélienne principalement polarisée indécomposable de dimension 3 à être une jacobienne sur $\mathbb{F}_q$, pour calculer l'obstruction de Schottky d'une telle variété en dimension 4 à être une jacobienne sur $\bar{\mathbb{F}}_q$ et enfin, en genre 2 et 3 nous nous en servons pour reconstruire un modèle explicite d'une courbe lorsque la variété abélienne polarisée en question est une jacobienne.

2.2.4 Produits de courbes elliptiques complexes

Dans cette section on souhaite montrer que le foncteur qui à une variété abélienne complexe polarisée isogène à un produit de courbes elliptiques à multiplication complexe sur un même corps (mais pas forcément un même ordre) associe le réseau hermitien sous-jacent est une équivalence de catégories puis étudier ce qu'il se passe lorsqu'on considère les polarisations.

On pose :

$\boldsymbol{\mathcal{A}}_K$: Catégorie des variétés abéliennes complexes isogènes [10] à un produit de courbes elliptiques à multiplication complexe par un ordre de K.

$\boldsymbol{\mathcal{A}}_K^p$: Catégorie des variétés abéliennes complexes polarisées dont la variété abélienne sous-jacente est isogène à un produit de courbes elliptiques à multiplication complexe par un ordre de K. On pose $\boldsymbol{\mathcal{A}}_R^p$ la sous-catégorie de $\boldsymbol{\mathcal{A}}_K^p$ formée des variétés abéliennes isomorphes à un produit de courbes elliptiques à multiplication complexe par un sur-ordre de R.

$\boldsymbol{\mathcal{L}}_K$: Catégorie des sous-groupes d'un K espace vectoriel V de dimension finie qui sont des R-réseaux pour un certain ordre R de K.

$\boldsymbol{\mathcal{L}}_K^{h,int}$: Catégorie des R-réseaux hermitiens entiers pour tout ordre $R \subseteq K$, i.e. la catégorie des réseaux hermitiens (L, H) tels que L est un R-module, H une forme hermitienne sur KL et $H(L, L) \subseteq R$. On pose $\boldsymbol{\mathcal{L}}_R^{h,int}$ la sous-catégorie de $\boldsymbol{\mathcal{L}}_K^{h,int}$ formée des R-réseaux hermitiens entiers à R fixé.

Comme on peut le voir en dimension 1 l'ordre R qui fait d'un sous groupe $\mathfrak{a}$ de K un R-réseau n'est pas unique ; pour tout sous-ordre R' de R, $\mathfrak{a}$ est un R'-réseau. Ceci nous amène à définir, à l'instar de la dimension 1 l'anneau multiplicateur d'un R-réseau L.

Définition 2.2.23. *Soit L un R-réseau. On pose $R_L = \{\alpha \in K, \alpha L \subseteq L\}$. C'est un ordre de K qui contient R on l'appelle l'anneau multiplicateur de L.*

Pour $\mathfrak{a}$ de rang 1 c'est la définition de $R_{\mathfrak{a}}$. Il n'y a donc pas de conflit de notation.

On se permet de rappeler qu'un R-réseau L « ne transporte pas la donnée R » dans le sens qu'étant donné l'ensemble (ou le groupe peu importe) L il n'est pas possible de savoir si L est un R'-réseau pour $R' \subseteq R_L$. En revanche, on peut reconstituer R_L à partir de L. On rappelle aussi que c'est, comme pour le rang 1, le plus grand ordre S tel que L

10. D'après [Kan11, Theorem 2], une variété abélienne est isogène à E^g avec E à CM si, et seulement si, A est isomorphe à un produit de courbes elliptiques à CM.

est un S-module.
Ceci nous permet de clarifier un point subtilement passé sous le tapis jusqu'ici. Étant donnés deux objets L et L' de $\boldsymbol{\mathcal{L}}_K$, une flèche entre L et L' est un morphisme de $R_L \cap R_{L'}$-modules. Si on ne souhaite pas faire intervenir les anneaux multiplicateur dans la définition on peut voir les flèches comme les restrictions d'applications K-linéaires sur les espaces ambiants.

D'autre part, les flèches $f\colon (A,a) \to (A',a')$ dans la catégorie $\boldsymbol{\mathcal{A}}_K^p$ ne sont pas des simples morphismes entre les variétés abéliennes sous-jacentes A et A'. On demande encore que les morphismes respectent aussi les polarisations, i.e. $a = \widehat{f}a'f$, c'est à dire que f soit une isogénie polarisée. De même pour les flèches dans $\boldsymbol{\mathcal{L}}_K^{h,int}$, on veut que ce soient des isométries. En particulier, le foncteur d'oubli de la polarisation $(A,a) \mapsto A$ (resp. de la forme hermitienne $(L,H) \mapsto L$) n'est pas un foncteur plein entre $\boldsymbol{\mathcal{A}}_K^p$ et $\boldsymbol{\mathcal{A}}_K$ (resp. entre $\boldsymbol{\mathcal{L}}_K^{h,int}$ et $\boldsymbol{\mathcal{L}}_K$).

Variétés abéliennes, réseaux et polarisations

Étant donné un corps quadratique imaginaire K on fixe une bonne fois pour toutes des extensions de corps

$$\mathbb{Q} \to K \to \overline{\mathbb{Q}} \to \mathbb{C}$$

et on s'y référera implicitement lorsqu'on écrira des choses comme $\mathbb{C}L = L \otimes_R \mathbb{C}$ pour un R-réseau L étant sous-entendu qu'on étend les scalaires sur L pour le transformer en $\mathbb{C}$ espace vectoriel grâce au morphisme $K \to \mathbb{C}$ sus-cité.

Soit $R = \mathbb{Z}[\omega]$ un ordre dans un corps quadratique imaginaire K. On pose $\alpha_R = \operatorname{im}\omega$, où im désigne la partie imaginaire.

Lemme 2.2.24. *Le nombre α_R ne dépend du choix du générateur de la $\mathbb{Z}$-algèbre R qu'au signe près. Pour fixer ce choix on impose $\alpha_R > 0$.*

Démonstration. Soit ω et ω' deux générateurs de la $\mathbb{Z}$-algèbre R, i.e. $R = \mathbb{Z}[\omega] = \mathbb{Z}[\omega']$. On a alors $(1,\omega)$ et $(1,\omega')$ qui sont des $\mathbb{Z}$-bases de R. On pose $\omega' = a + b\omega$ et $\omega = a' + b'\omega'$ donc $\omega = a' + b'a' + bb'\omega$. Ceci impose que $bb' = 1$, i.e. $b, b' \in \{-1, 1\}$ et $a = \pm a'$. On en déduit que $\operatorname{im}\omega = \pm \operatorname{im}\omega'$ donc la partie imaginaire d'un générateur de la $\mathbb{Z}$-algèbre R ne dépend pas du générateur choisi au signe près donc α_R est bien défini. □

Lemme 2.2.25. *Soit $\mathfrak{a}$ un sous R-module de $\mathbb{C}$ alors $\mathfrak{a}$ est un R-idéal si, et seulement si,* $\operatorname{im}\mathfrak{a} \subseteq \alpha_R\mathbb{Z}$.

Démonstration. Si $\mathfrak{a}$ est un idéal ses éléments s'écrivent $a+b\omega$ avec $a,b\in\mathbb{Z}$ donc $\operatorname{im}\mathfrak{a}\subseteq(\operatorname{im}\omega)\mathbb{Z}=\alpha_R\mathbb{Z}$.

Réciproquement, supposons $\operatorname{im}\mathfrak{a}\subseteq\alpha_R\mathbb{Z}$ soit $a+b\omega\in\mathfrak{a}$ avec $a,b\in\mathbb{Q}$ alors $b\in\mathbb{Z}$ par hypothèse. D'autre part, $(a+b\omega)\omega=a\omega+b\omega^2=a\omega+b(\operatorname{Tr}(\omega)\omega-N(\omega))=-bN(\omega)+(a+\operatorname{Tr}(\omega)b)\omega$. Donc $(a+\operatorname{Tr}(\omega)b)\alpha_R\in\alpha_R\mathbb{Z}$ donc $a\in\mathbb{Z}$. Ceci prouve que $a+b\omega\in R$ donc $\mathfrak{a}\subseteq R$. □

Remarque 2.2.26. *On peut même préciser les choses un peu plus. Étant donné un sous-groupe $\mathfrak{a}$ de $\mathbb{C}$ qui est un R-idéal pour un certain ordre d'un corps quadratique imaginaire K et on pose $\mathscr{O}_K=\mathbb{Z}[\omega_K]$ l'ordre maximal et $\alpha_K=\operatorname{im}\omega_K$. On a alors $\operatorname{im}\mathfrak{a}\subseteq\alpha_R\mathbb{Z}\subseteq\alpha_K\mathbb{Z}$ d'après le Lemme 2.2.25, car $\alpha_R=f'\alpha_K$ pour un certain conducteur $f'\geq 1$. En d'autres termes $\frac{1}{\alpha_K}\operatorname{im}\mathfrak{a}\subseteq\mathbb{Z}$. Maintenant, oublions R et concentrons nous uniquement sur le groupe $\mathfrak{a}$ et l'ordre $\mathscr{O}_K$. On connait bien les sous-groupes de $\mathbb{Z}$; il existe un unique entier positif f tel que $\frac{1}{\alpha_K}\operatorname{im}\mathfrak{a}=f\mathbb{Z}$, i.e. $\operatorname{im}\mathfrak{a}=f\alpha_K\mathbb{Z}$. Posons $S=\mathbb{Z}[f\omega_K]$. C'est le plus petit sous-ordre R de $\mathscr{O}_K$ pour lequel $\mathfrak{a}$ est un R-idéal. On peut donc conclure que l'ensemble des ordres R satisfaisant les hypothèses du Lemme 2.2.25, i.e. $\mathfrak{a}$ est un R-module et $\operatorname{im}\mathfrak{a}\subseteq\alpha_R\mathbb{Z}$, sont les ordres vérifiant*

$$S\subseteq R\subseteq R_{\mathfrak{a}}.$$

Heuristiquement, c'est l'ensemble des ordres coincés entre « être un R-module », c'est à dire les sous-ordres de $R_{\mathfrak{a}}$, et « être un sous-ensemble de R ». On peut aussi le décrire par l'ensemble des $\mathbb{Z}[f'\omega_K]$ avec $f'|f$ (donc $R_{\mathfrak{a}}$ convient toujours).

On pose $\boldsymbol{\mathcal{T}}_K$ la catégorie des tores complexes $X=V/\Gamma$ tels qu'il existe un isomorphisme $X\simeq\mathbb{C}^g/\prod_{i=1}^g\Lambda_i$ où Λ_i est à multiplication complexe par une extension quadratique imaginaire K, i.e. $\operatorname{End}(\Lambda_i)=\{\alpha\in\mathbb{C},\alpha\Lambda_i\subseteq\Lambda_i\}=R_i$ un ordre dans K.

Proposition 2.2.27. *Le foncteur défini par*

$$\begin{array}{rccc}\mathbf{T}\colon & \boldsymbol{\mathcal{T}}_K & \longrightarrow & \boldsymbol{\mathcal{L}}_K\\ & V/\Gamma & \longmapsto & \Gamma\\ & V/\Gamma\xrightarrow{\varphi}V'/\Gamma' & \longmapsto & \Gamma\xrightarrow{\varphi_{rat}}\Gamma'\end{array}$$

est une équivalence de catégories.

Démonstration. On va montrer que $\mathbf{T}$ est un foncteur plein, fidèle et essentiellement surjectif ce qui montrera que c'est une équivalence de catégories (bien que ce soit un

résultat extrêmement classique, on peut le retrouver par exemple dans [Lei14, Proposition 1.3.18] que je cite surtout pour dire que je trouve que c'est un petit chef-d'œuvre de pédagogie que je recommande vivement).

T est essentiellement surjectif : Soit $L \in \boldsymbol{\mathcal{L}}_K$ et $R = R_L$ son anneau multiplicateur. D'après la Proposition 1.2.11, L admet une pseudo-base, i.e. il existe des idéaux fractionnaires $\mathfrak{a}_i$ de R et des sur-ordres R_i de R tels que $R_i \subseteq R_{i+1}$, $\mathfrak{a}_i$ inversible dans R_i et $L = \mathfrak{a}_1 x_1 + \cdots + \mathfrak{a}_g x_g$. En posant $\Lambda_i = \mathfrak{a}_i$ on a bien $L \simeq \prod_i \Lambda_i$. Tous les idéaux fractionnaires sont des $\mathbb{Z}$-modules libres de rang 2 donc L est de rang $2g$ sur $\mathbb{Z}$ et puisque R est quadratique imaginaire $\mathfrak{a}_i\mathbb{R} = \mathbb{C}$. On pose Γ l'image de L dans $V = \mathbb{C}L$ (par l'inclusion [11] $L \to KL = L \otimes_R K \to KL \otimes_K \mathbb{C}$). Puisque Γ est de rang $2g$ et est engendré par une base du $\mathbb{R}$-espace vectoriel sous-jacent de V. Le quotient $X = V/\Gamma$ est donc bien un tore complexe, i.e. $\mathbf{T}(X) = L$ et $\mathbf{T}$ est essentiellement surjectif.

T est fidèle : On doit montrer que l'application

$$\begin{aligned} \mathrm{Hom}(V/\Gamma, V'/\Gamma') &\longrightarrow \mathrm{Hom}(\Gamma, \Gamma') \\ \varphi &\longmapsto \mathbf{T}(\varphi) = \varphi_{\mathrm{rat}} \end{aligned}$$

est injective. Deux morphismes de tores complexes de $\mathrm{Hom}(V/\Gamma, V/\Gamma')$ ayant la même représentation rationnelle coïncident sur le réseau Γ qui, rappelons-le, est engendré par une $\mathbb{R}$-base de V. Ainsi, leurs représentations analytiques coïncident aussi et donc, en passant au quotient, les morphismes de tores complexes coïncident aussi.

T est plein : On doit montrer que l'application

$$\begin{aligned} \mathrm{Hom}(V/\Gamma, V'/\Gamma') &\longrightarrow \mathrm{Hom}(\Gamma, \Gamma') \\ \varphi &\longmapsto \mathbf{T}(\varphi) = \varphi_{\mathrm{rat}} \end{aligned}$$

est surjective. On considère un morphisme R-linéaire $\Phi\colon \Gamma \to \Gamma'$ entre deux R-réseaux inclus dans des $\mathbb{C}$-espaces vectoriels V et V' qu'ils engendrent. On considère $\widetilde{\Phi} = \Phi \otimes_{\mathbb{Z}} \mathrm{id}_{\mathbb{R}}\colon \mathbb{R}\Gamma = V \to \mathbb{R}\Gamma' = V'$. On a $\Phi = \Phi_{|\Gamma}$ et puisque $\mathbb{R}R = \mathbb{C}$, pour tout

11. La première inclusion provient du fait que L est sans torsion et la seconde du fait que les extensions de corps sont toujours fidèlement plates.

$\lambda = a + b\omega \in \mathbb{C}, a, b \in \mathbb{R}$ on a pour tout $v \in V$,

$$\begin{aligned}\widetilde{\Phi}(\lambda v) &= a\widetilde{\Phi}(v) + b\widetilde{\Phi}(\omega v) \text{ par } \mathbb{R}\text{-linéarité de } \widetilde{\Phi} \\ &= a\widetilde{\Phi}(v) + b\omega\widetilde{\Phi}(v) \text{ par } R\text{-linéarité de } \Phi \\ &= \lambda\widetilde{\Phi}.\end{aligned}$$

Donc $\widetilde{\Phi}$ est $\mathbb{C}$-linéaire et vérifie $\widetilde{\Phi}(\Gamma) \subseteq \Gamma'$. Elle définit donc un morphisme de tores complexes φ sur les quotients dont elle est la représentation analytique. Ainsi $\mathbf{T}(\varphi) = \varphi_{\text{rat}} = \Phi$ ce qui conclut la preuve.

□

Remarque 2.2.28. *Ici l'inverse du foncteur* $\mathbf{T}$ *est facile à expliciter*

$$\begin{array}{rccc}\mathbf{L}\colon & \boldsymbol{\mathcal{L}}_K & \longrightarrow & \boldsymbol{\mathcal{T}}_K \\ & L & \longmapsto & \mathbb{C}L/L \\ & L \to L' & \longmapsto & \mathbb{C}L/L \to \mathbb{C}L'/L'\end{array}$$

et on aurait aussi pu montrer que $\mathbf{L} \circ \mathbf{T} = \mathrm{Id}_{\boldsymbol{\mathcal{T}}_K}$ *et* $\mathbf{T} \circ \mathbf{L} = \mathrm{Id}_{\boldsymbol{\mathcal{L}}_K}$ *(donc mieux qu'une équivalence de catégories, on est pas seulement naturellement isomorphe au morphisme identité).*

Théorème 2.2.29 (Première équivalence de catégories)**.** *La composition* $\mathbf{F}_K = \mathbf{T} \circ \mathbf{H}_{\mathbb{C}}$ *restreinte à* $\boldsymbol{\mathcal{A}}_K$ *définit une équivalence de catégories entre* $\boldsymbol{\mathcal{A}}_K$ *et* $\boldsymbol{\mathcal{L}}_K$*.*

Démonstration. D'après le Théorème 2.2.27 $\boldsymbol{\mathcal{T}}_K$ est équivalente à $\boldsymbol{\mathcal{L}}_K$. Il suffit alors de montrer que tous les tores de la catégorie $\boldsymbol{\mathcal{T}}_K$ sont polarisables et correspondent donc bien à des variétés abéliennes par l'équivalence $\mathbf{H}_{\mathbb{C}}\colon A \mapsto A(\mathbb{C})$. Pour ceci, il suffit de prendre un réseau $L \in \boldsymbol{\mathcal{L}}_K$ et $R = R_L$. On considère une pseudo base de L, i.e. $L = \mathfrak{a}_1 x_1 + \cdots + \mathfrak{a}_g x_g$ et un entier n tel que pour tout $i, n\mathfrak{a}_i \subseteq R$. La multiplication par n fournit alors une inclusion

$$[n]\colon L \to Rx_1 + \cdots + Rx_g \simeq R^g.$$

En munissant l'espace vectoriel K^g de la forme hermitienne canonique $H_0(x, y) = {}^t x\overline{y}$ qui fait de (R^g, H_0) un réseau entier. On peut tirer en arrière cette forme grâce à $[n]$ en $H(x, y) = H_0(nx, ny)$ qui fait de (L, H) un réseau hermitien entier, i.e. $H(L, L) \subseteq R$. Grâce au Lemme 2.2.25 on a alors $\operatorname{im} H(L, L) \subseteq \alpha_R\mathbb{Z}$, avec $\alpha_R = \operatorname{im}\omega > 0$ où ω est un générateur de la $\mathbb{Z}$-algèbre R, donc $\operatorname{im} h(L, L) \subseteq \mathbb{Z}$ où $H = \alpha_R h$. Donc L est un $\mathbb{Z}$-réseau polarisable et donc $\mathbb{C}L/L$ provient d'une variété abélienne par le foncteur $A \mapsto A(\mathbb{C})$. □

Le foncteur noté $\mathbf{F}$ dans [Nar22] était juste $\mathbf{F}_K$ restreint aux variétés abéliennes isomorphes à un produit de courbes elliptiques toutes à multiplication complexe par $\mathscr{O}_K$.

Proposition 2.2.30. *Soit $(V/\Gamma, h)$ un tore polarisé, i.e. $h(\Gamma,\Gamma) \subseteq \mathbb{Z}$ tel qu'il existe un isomorphisme $\Gamma \simeq \prod_{i=1}^{g} \Lambda_i$ avec Λ_i à multiplication complexe par une extension quadratique imaginaire K, i.e. $\mathrm{End}(\Lambda_i) = R_{\Lambda_i}$ est un ordre dans K. Alors Γ est un R-réseau avec $R = R_\Gamma = R_{\Lambda_1} \cap \cdots \cap R_{\Lambda_g}$. Par ailleurs, $(\Gamma^{\alpha_R}, h^{\alpha_R})$ est un réseau entier qui satisfait*

$$\deg \rho_h = \left[\widehat{\Gamma} \colon \rho_h(\Gamma)\right] = \left[(\Gamma^{\alpha_R})^{\#} : \Gamma^{\alpha_R}\right].$$

Démonstration. Si pour tout i, Λ_i est un R-module alors on peut munir le produit $\prod \Lambda_i$ d'une structure de R-module composante par composante, puis le réseau Γ grâce à l'isomorphisme $\Gamma \simeq \prod \Lambda_i$. Il est clair que $R = \bigcap R_{\Lambda_i}$ convient et que $R_\Gamma = R$. D'autre part, $h(\Gamma,\Gamma)$ est un sous R-module de $\mathbb{C}$ qui satisfait $\operatorname{im} h(\Gamma,\Gamma) \subseteq \mathbb{Z}$ donc

$$\operatorname{im} \mathfrak{s}\left(\Gamma^{\alpha_R}\right) = \operatorname{im} \alpha_R h(\Gamma,\Gamma) \subseteq \alpha_R \mathbb{Z}.$$

D'après le Lemme 2.2.25, ceci signifie que $\mathfrak{s}\left(\Gamma^{\alpha_R}\right)$ est un R-idéal, i.e. le réseau hermitien $(\Gamma^{\alpha_R}, h^{\alpha_R})$ est entier.

Enfin,

$$\begin{aligned}
\deg \rho_h &= \left[\widehat{\Gamma} \colon \rho_h(\Gamma)\right] \text{ (d'après la relation (2.11))} \\
&= \left[\rho_h^{-1}\left(\widehat{\Gamma}\right) : \Gamma\right] \\
&= \#\{v \in V, \operatorname{im} h(v,\Gamma) \subseteq \mathbb{Z}\}/\Gamma \\
&= \#\{v \in V, (\operatorname{im}\omega) h(v,\Gamma) \subseteq R\}/\Gamma \text{ (d'après le Lemme 2.2.25)} \\
&= \#((\Gamma^{\alpha_R})^{\#}/\Gamma) \\
&= \left[(\Gamma^{\alpha_R})^{\#} : \Gamma^{\alpha_R}\right].
\end{aligned}$$

□

Remarque 2.2.31. *On rappelle que d'après la Proposition 1.2.11, on peut toujours écrire un R-réseau L sous la forme*

$$L = \mathfrak{a}_1 x_1 \oplus \cdots \oplus \mathfrak{a}_g x_g$$

avec $R \subseteq R_1 = R_{\mathfrak{a}_1} \subseteq \cdots \subseteq R_g = R_{\mathfrak{a}_g}$. Dans ce cas $R_L = R_1$. En revanche, si on choisit une pseudo-base quelconque $\mathfrak{b}_1 y_1 \oplus \cdots \mathfrak{b}_g y_g$, c'est-à-dire sans condition d'inclusion sur les

anneaux $R_{\mathfrak{b}_j}$, alors il n'est pas garanti que R_L soit un des $R_{\mathfrak{b}_j}$. En effet, si on pose $L = \mathfrak{a} \oplus \mathfrak{b}$ avec $R_{\mathfrak{a}} = \mathbb{Z}[2\omega]$ et $R_{\mathfrak{b}} = \mathbb{Z}[3\omega]$ où $\mathscr{O}_K = \mathbb{Z}[\omega]$ alors, d'après la Proposition 2.2.30, $R_L = R_{\mathfrak{a}} \cap R_{\mathfrak{b}} = \mathbb{Z}[6\omega]$. Cependant, la Proposition 1.2.11 implique en particulier que R_L est un invariant de la classe d'isomorphisme de L donc, dans tous les cas $R_{\mathfrak{b}_1} \cap \cdots \cap R_{\mathfrak{b}_g} = R_1 = R_L$.

On pose $\boldsymbol{\mathcal{T}}_R^p$ la catégorie des tores complexes polarisés $(X = V/\Gamma, h)$ tels qu'il existe un isomorphisme $X \simeq \mathbb{C}^g / \prod_{i=1}^g \Lambda_i$ où Λ_i est à multiplication complexe par un ordre S tel que $R \subseteq S$.

Proposition 2.2.32. *Le foncteur défini par*

$$\begin{aligned} \mathbf{T}_R^p \colon \qquad \boldsymbol{\mathcal{T}}_R^p &\longrightarrow \boldsymbol{\mathcal{L}}_R^{h,int} \\ (V/\Gamma, h) &\longmapsto (\Gamma^{\alpha_R}, h^{\alpha_R}) \,. \end{aligned}$$

est une équivalence de catégories.

Démonstration. La démonstration de ce résultat est extrêmement similaire à celle du Théorème 2.2.27. Je vais tout de même la détailler pour mettre en valeur les raisons pour lesquelles on est forcés de fixer un ordre R pour énoncer l'équivalence de catégories contrairement au Théorème 2.2.27 où cette restriction n'était pas nécessaire.

$\mathbf{T}_R^p$ est essentiellement surjectif : Soit (L, H) un réseau hermitien entier alors $\mathbb{C}L/L$ est un tore complexe pour les mêmes raisons que dans la démonstration du Théorème 2.2.27. Par ailleurs, par définition $H(L, L)$ est un R-idéal donc $\operatorname{im} H(L, L) \subseteq \alpha_R \mathbb{Z}$ et donc $\operatorname{im} h(L, L) \subseteq \mathbb{Z}$ où $H = \alpha_R h$. Si bien que $(\mathbb{C}L/L, h)$ est un tore polarisé tel que $\mathbf{T}_R^p(\mathbb{C}L/L, h) = (L, H)$.

$\mathbf{T}_R^p$ est fidèle : Un morphisme polarisé entre des tores complexes induit un morphisme (le même) entre les tores sous-jacent (en oubliant les formes hermitiennes). Le foncteur est alors fidèle pour exactement les mêmes raisons que celles évoquées dans la démonstration de la Proposition 2.2.27.

$\mathbf{T}_R^p$ est plein : On considère une isométrie entre deux R-réseaux hermitiens

$$\Phi \colon (\Gamma, \alpha_R h) \to (\Gamma, \alpha_R h').$$

L'isométrie Φ définit alors une isométrie entre les espaces hermitiens correspondant $(\Gamma, h) \to (\Gamma', h')$ (il s'agit de la même application Φ) qui passe au quotient. Donc Φ provient bien, par $\mathbf{T}_R^p$, d'un morphisme de tores polarisés.

□

Attention au fait qu'on ne peut pas définir d'équivalence aussi générale dans le cas polarisé que dans le cas non polarisé. En effet, l'application qu'on voudrait définir sur le modèle du foncteur de la Proposition 2.2.27 est

$$(V/\Gamma, h) \longmapsto (\Gamma^{\alpha_{R_\Gamma}}, h^{\alpha_{R_\Gamma}}),$$

où $V/\Gamma \in \boldsymbol{\mathcal{T}}_K$ et h est une forme hermitienne telle que $(V/\Gamma, h)$ est polarisé. Ce n'est pas un foncteur. Si on considère $(V/\Gamma, h)$ et $(V'/\Gamma', h')$ avec $R_\Gamma \neq R_{\Gamma'}$ et f la représentation analytique d'un morphisme de tores polarisés $(V/\Gamma, h) \to (V'/\Gamma', h')$ alors f_{rat} ne définit **pas** une isométrie $(\Gamma, \alpha_{R_\Gamma} h) \to (\Gamma', \alpha_{R'_\Gamma} h')$ car

$$\forall x, y \in V, h'(f(x), f(y)) = h(x, y)$$

donc $\alpha_{R_{\Gamma'}} h'(f(x), f(y)) \neq \alpha_{R_\Gamma} h(x, y)$ pour $h(x, y) \neq 0$ car $\alpha_{R_{\Gamma'}} \neq \alpha_{R_\Gamma}$. En revanche, le foncteur est bien défini lorsqu'on fixe l'ordre R au préalable.

Théorème 2.2.33 (Seconde équivalence de catégories)**.** *La composition* $\mathbf{F}_R^h = \mathbf{T}_R^p \circ \mathbf{H}_{\mathbb{C}}^p$ *restreinte à* $\boldsymbol{\mathcal{A}}_R^p$ *définit une équivalence de catégories entre* $\boldsymbol{\mathcal{A}}_R^p$ *et* $\boldsymbol{\mathcal{L}}_R^{h,int}$.

Démonstration. Le foncteur $\mathbf{H}_{\mathbb{C}}^p$ restreint à la sous-catégorie $\boldsymbol{\mathcal{A}}_R^p$ des variétés abéliennes complexes polarisées définit une équivalence sur son image essentielle, $\boldsymbol{\mathcal{T}}_R^p$. Il suffit alors de considérer $\mathbf{T}_R^p \circ \mathbf{H}_{\mathbb{C}}^p$. □

Dans [Nar22] l'équivalence noté $\mathbf{F}_h$ était le foncteur $\mathbf{F}_{\mathscr{O}_K}^h$.

Ces foncteurs $\boldsymbol{\mathcal{T}}_R^p$ décrivent tous des équivalences de catégories pour chaque R choisi. Cependant, le fait qu'ils aient des images différentes pour une même variété abélienne peut être déstabilisant. La proposition suivante détaille la préimage essentielle des réseaux hermitiens unimodulaires par le foncteur $\mathbf{T}_R^p$.

Proposition 2.2.34. *Soit* $g \geq 1$ *un entier. L'équivalence* $\mathbf{F}_R^h$ *définit une correspondance*

$$\left\{ \begin{array}{l} (A, a) \in \boldsymbol{\mathcal{A}}_R^p \text{ principalement polarisée telle que} \\ A \simeq E_1 \times \cdots \times E_g / \bigcap_{i=1}^{g} \mathrm{End}(E_i) \simeq R \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{l} (L, H) \in \boldsymbol{\mathcal{L}}_R^{h,int} \\ \text{unimodulaire de rang } g \end{array} \right\}.$$

Démonstration. Soit (L, H) un R-réseau hermitien unimodulaire. On remarque que

$$\mathfrak{s}(L) = H(L, L) = H(R_L L, L) = R_L H(L, L) = R_L R = R_L$$

or, par hypothèse, $\mathfrak{s}(L) = R$ donc $R = R_L$. Par la Proposition 1.2.11, on peut trouver une pseudo-base de L, i.e.

$$L = \mathfrak{a}_1 x_1 \oplus \cdots \oplus \mathfrak{a}_g x_g$$

telle que $R_{\mathfrak{a}_1} \subseteq \cdots \subseteq R_{\mathfrak{a}_g}$ si bien que $R = R_L = R_{\mathfrak{a}_1}$. Donc en posant $\Lambda_i = \mathfrak{a}_i x_i$ on a bien $\boldsymbol{\mathcal{T}}_R^p(\mathbb{C}L/L, h) = (L, H)$ où $H = \alpha_R$. D'après la Proposition 2.2.30 on a bien $\deg \rho_h = 1$ donc $(\mathbb{C}L/L, h)$ provient bien d'une variété abélienne principalement polarisée (A, a), i.e. $\mathbf{H}_{\mathbb{C}}^p(A, a) = (\mathbb{C}L/L, h)$ et pour E_i telle que $E_i(\mathbb{C}) \simeq \mathbb{C}/\Lambda_i$ on a bien $\mathrm{End}(E_1) = R$ et $R \subseteq \mathrm{End}(E_i)$.

Réciproquement, étant donnée une variété abélienne principalement polarisée (A, a) telle que $A \simeq E_1 \times \cdots \times E_g$ où $\bigcap_{i=1}^g \mathrm{End}(E_i) = R$, la Proposition 2.2.30 implique que le réseau $(L, H) = \mathbf{F}_R^h(A, a)$ est un R-réseau unimodulaire. □

Une conséquence intéressante de la Proposition 2.2.34 est que si $(A, a) \in \boldsymbol{\mathcal{A}}_R^p$ est une variété abélienne principalement polarisée telle que $A \simeq E_1 \times \cdots \times E_g$ avec $\bigcap \mathrm{End}(E_i) = S$ où $R \subseteq S$ est un sur-ordre strict de R alors $\mathbf{F}_R^h(A, a)$ n'est **pas** unimodulaire. On peut le voir « à la main ». On pose $f > 1$ le conducteur de R dans S. Puisque (A, a) est unimodulaire, $\mathbf{H}_{\mathbb{C}}^p(A, a) = (V/\Gamma, h)$ avec $\deg \rho_h = 1$. D'après cette même proposition $\mathbf{F}_S^h(A, a)$ est unimodulaire donc $H(L, L) = S$ où $\mathbf{T}_S^h(V/\Gamma, h) = (\Gamma, \alpha_S h) = (L, H)$. Par ailleurs, $\boldsymbol{\mathcal{T}}_R^p(V/\Gamma, h) = (L, \alpha_R h) = (L, H')$ mais $\alpha_R = f\alpha_S$ donc $H' = fH$ et $H'(L, L) = fH(L, L) = fS \subseteq R$. On retrouve sans surprise que (L, H') est un réseau hermitien entier mais il n'est pas unimodulaire.

On peut conclure par le corollaire suivant qui classifie les variétés abéliennes principalement polarisées sur $\mathbb{C}$, isomorphes à un produit de courbes elliptiques à multiplication complexe par un même corps quadratique imaginaire K, en termes de réseaux hermitiens unimodulaires.

Corollaire 2.2.35. *Soit $g \geq 1$ un entier. Les équivalences $\mathbf{F}_R^h$ induisent une correspondance*

$$\{(A, a) \in \boldsymbol{\mathcal{A}}_K^p \text{ principalement polarisée}\} \longleftrightarrow \dot{\bigcup_{R \subseteq \mathscr{O}_K}} \left\{ \begin{array}{l} (L, H) \in \boldsymbol{\mathcal{L}}_R^{h,int} \\ \text{unimodulaire de rang } g \end{array} \right\}.$$

Ce dernier résultat ainsi que la Proposition 2.2.34 étendent [Nar22, Theorem 2] qui ne traitait que le cas maximal. Cependant, dans [Nar22] je poursuis en traduisant l'action du groupe $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$ sur les réseaux à travers le foncteur $\mathbf{F}^h_{\mathcal{O}_K}$. Au moment où j'écris ces lignes je n'ai pas vérifié que cette traduction continue de fonctionner dans le cas non-maximal et permet donc d'énumérer la totalité des courbes de genre 2 sur $\overline{\mathbb{Q}}$ à jacobienne géométriquement décomposée en un produit de courbes elliptiques à multiplication complexe par un ordre quadratique imaginaire ayant pour corps des modules $\mathbb{Q}$. Les outils que j'ai utilisé dans le cas d'un ordre maximal s'étendent aux ordres non-maximaux (voir [Lan87]). J'ai donc bon espoir que la traduction de l'action galoisienne sur les réseaux sur un ordre quelconque soit similaire à celle faite pour le cas maximal à savoir qu'un réseau hermitien unimodulaire indécomposable (L, H) sur un ordre R quelconque correspond à la jacobienne d'une courbe ayant pour corps des modules $\mathbb{Q}$ si, et seulement si, il existe des isométries

$$(L, H) \simeq \left(\overline{L}, \overline{H}\right) \text{ et } \forall \mathfrak{a} \in \mathrm{Cl}(R), (L, H) \simeq \left(\mathfrak{a}L, \frac{1}{N(\mathfrak{a})} H\right). \tag{2.13}$$

Je me suis permis de fournir dans l'Annexe A la classification des ordres quadratiques imaginaires [12] qui peuvent intervenir pour de telles courbes ainsi que l'énumération de ces courbes pour chaque ordre sous réserve que les conditions (2.13) traduisent bien le fait que les jacobiennes correspondantes ont corps de modules $\mathbb{Q}$ pour R non-maximal aussi. J'insiste sur le fait que ces calculs ne sont qu'heuristiques et nécessitent des efforts supplémentaires pour être certifiés.

12. À savoir les ordres R tels que $\mathrm{Cl}(R)$ est d'exposant 1 ou 2.

2.3 Variétés abéliennes sur les corps finis

La particularité principale des variétés abéliennes sur un corps fini est la présence du morphisme de Frobenius sur celles-ci. Le *polynôme caractéristique* du morphisme de Frobenius d'une variété abélienne, que l'on définira dans la Section 2.3.1, est un invariant de la classe d'isogénie qui la caractérise totalement. Par ailleurs, les conjectures de Weil permettent de faire le lien entre le *polynôme de Weil* d'une courbe et son nombre de points rationnels sur n'importe quelle extension. Nous verrons alors que le polynôme de Weil associé à une courbe est le même [13] que le polynôme caractéristique de sa jacobienne. D'autre part, lorsque cette courbe est *optimale*, c'est-à-dire que son nombre de points atteint la borne supérieure de Hasse-Weil-Serre alors sa jacobienne est isogène à un produit de courbes elliptiques. Tous les résultats cités dans la Section 2.3.1 sont déjà bien connus, les démonstrations présentes ne sont là parce qu'il m'a plu de les y faire figurer. Dans la Section 2.3.2, je rappelle comment déduire d'un réseau hermitien unimodulaire (L, H) correspondant par le foncteur $\mathtt{Hom}_R(\_, E)$ de Serre à une variété abélienne principalement polarisée (A, a), une isogénie polarisée

$$\varphi\colon (E_1 \times \cdots \times E_g, \ell\lambda_0) \longrightarrow (A, a).$$

Nous l'avons décrit brièvement dans [KNRR21, Section 3.3] mais nous n'avons détaillé que le cas $E_1 = \cdots = E_g = E$ car le cas général nous aurait été inutile. Pourtant, sous réserve que les algorithmes de thêta constantes que nous avons utilisé soient implémentés pour un produit de courbes elliptiques différentes [14], le fait de considérer des courbes différentes apporterait des avantages significatifs tant pour les temps de calcul que pour la diversité des variétés abéliennes que nous serions alors capable de déterminer (notamment celles de dimension paire pour lesquelles les méthodes proposées dans [KNRR21] rencontrent beaucoup d'obstacles [15]).

13. En renversant l'ordre des coefficients (voir Proposition 2.3.6).
14. Ce qui est théoriquement parfaitement possible.
15. Potentielle inexistence de familles orthogonales de même norme (même pour les réseaux sur un ordre maximal), réseaux dont tous les vecteurs sont de norme paire, etc.

2.3.1 Quelques généralités

Conjectures de Weil pour les courbes algébriques

En 1949, André Weil conjecture un certain nombre de résultats relatifs au nombre de points rationnels d'une variété abélienne définie sur un corps fini. Ces conjectures ont été démontrées par Weil lui-même pour le cas des courbes algébriques puis en 1974 par Pierre Deligne dans le cas général. Nous n'aurons besoin de les énoncer que dans le cadre des courbes algébriques où l'énoncé a l'avantage d'être plus concis que dans le cadre général. Soit C une courbe algébrique sur un corps fini $\mathbb{F}_q$. On appelle *fonction Zéta* associée à C sur $\mathbb{F}_q$ la série formelle

$$\zeta(C,T) = \exp\left(\sum_{n=1}^{\infty} \#C\left(\mathbb{F}_{q^n}\right)\frac{T^n}{n}\right).$$

On a le célèbre théorème suivant. Outre les travaux de Weil et Deligne on pourra en trouver une preuve dans [Rit17, Section 6.1].

Théorème 2.3.1 (Conjectures de Weil)**.** *Soit C une courbe algébrique sur $\mathbb{F}_q$ de genre g alors*

Rationalité : *On a $\zeta(C,T) \in \mathbb{Q}(T)$*

Équation fonctionnelle : *On a la relation*

$$\zeta\left(C, \frac{1}{qT}\right) = \frac{1}{(qT^2)^{g-1}}\zeta(C,T).$$

Hypothèse de Riemann : *Il existe un polynôme $f(T) \in \mathbb{Z}[T]$ de degré $2g$ dont les racines dans $\overline{\mathbb{Q}}$ sont de module $\sqrt{q}$ tel que*

$$\zeta(C,T) = \frac{f(T)}{(1-T)(1-qT)}.$$

Avec les notations ci-dessus, on appelle f le *polynôme de Weil* de la courbe C. La connaissance du polynôme de Weil permet de calculer le nombre de points d'une courbe C sur toutes les extensions finies de $\mathbb{F}_q$. En effet, on a le corollaire suivant.

Corollaire 2.3.2. *Soit C une courbe de genre g sur $\mathbb{F}_q$ telle que $\zeta(C,T) = \frac{f(T)}{(1-T)(1-qT)}$*

avec $f(T) = \prod_{i=1}^{2g}(1-\alpha_i T)$ *alors*

$$\#C\left(\mathbb{F}_{q^n}\right) = 1 + q^n - \sum \alpha_i^n.$$

Démonstration. On a

$$\begin{aligned}
\ln(\zeta(C,T)) &= \ln(f(T)) - \ln(1-T) - \ln(1-qT) \\
&= \sum_{i=1}^{2g} \ln(1-\alpha_i T) + \sum_{n=1} \frac{T^n}{n} + \sum_{n=1} \frac{(qT)^n}{n} \\
&= \sum_{n=1}^{\infty} (1 + q^n - \sum_{i=1}^{2g} \alpha_i^n) \frac{T^n}{n} \\
&= \sum_{n=1}^{\infty} \#C(\mathbb{F}_{q^n}) \frac{T^n}{n}.
\end{aligned}$$

□

Une autre conséquence très importante des conjectures de Weil est la borne de Hasse-Weil-Serre.

Corollaire 2.3.3 (Borne de Hasse-Weil-Serre)**.** *Soit C une courbe algébrique de genre g sur $\mathbb{F}_q$ alors*

$$\#C(\mathbb{F}_q) \leq q + 1 + g\left\lfloor 2\sqrt{q} \right\rfloor.$$

Démonstration. On pose $f(T) = \prod_{i=1}^{2g}(1-\alpha_i T)$, i.e. les racines de f sont les α_i^{-1}. D'après l'équation fonctionnelle on a $T^{2g} f\left(\frac{1}{qT}\right) = f(T)$. On pose $\overline{\alpha_i} = \frac{q}{\alpha_i}$, il est clair que $\overline{\alpha_i}^{-1}$ est aussi une racine de f. Lorsque α_i n'est pas réel alors $\overline{\alpha_i}$ est distinct de α_i donc $(1-\alpha_i T)(1-\overline{\alpha_i} T)$ divise f. En revanche, α_i est réel si, et seulement si $\alpha_i \in \{\pm\sqrt{q}\}$ et si q n'est pas un carré, puisque f est à coefficients entiers on a $(1-\alpha_i T)(1-\overline{\alpha_i} T)$ qui divise f (le polynôme minimal de $\pm\sqrt{q}$ est $X^2 - q$).
Le cas restant est si $\alpha_i = \pm\sqrt{q}$ est entier, i.e. q est un carré. La section suivante est nécessaire pour traiter ce cas, je le fais tout de même ici mais j'invite la lectrice à se reporter à la section suivante pour les résultats cités ainsi que les notations que j'utilise. Si α_i était de multiplicité impaire on aurait $f(T) = -q^g T^{2g} + \dots$ ce qui est absurde car le coefficient dominant de f est $\chi_{\mathrm{Jac}(C)}(0) = \det F_{\mathrm{Jac}(C)}$ d'après la Proposition 2.3.6, avec $F_{\mathrm{Jac}(C)} \in \mathrm{End}\left(T_\ell\left(\mathrm{Jac}(C)\right)\right)$ et $\det F_{\mathrm{Jac}(C)} = \deg F = q^g$ d'après [Rit17, Proposition 7.4.1 et Proposition 7.4.5].

Finalement, quitte à réarranger les α_i, on peut écrire $f(T) = \prod_{i=1}^{g}(1-\alpha_i T)(1-\overline{\alpha_i}T)$. D'après le Corollaire 2.3.2, on a alors $\#C(\mathbb{F}_q) = q+1-\sum_i^g(\alpha_i+\overline{\alpha_i})$. On remarque que $x_i = 1+\alpha_i+\overline{\alpha_i}+\left\lfloor 2\sqrt{q}\right\rfloor$ est un entier strictement positif car $-\alpha_i-\overline{\alpha_i} \leq |\alpha_i|+|\overline{\alpha_i}| = 2\sqrt{q}$ et $\alpha_i+\overline{\alpha_i}$ est un entier. On a alors, à l'aide de l'inégalité arithmético-géométrique

$$\frac{1}{g}\sum_{i=1}^{g} x_i \geq \left(\prod_{i=1}^{g} x_i\right)^{\frac{1}{g}} \geq 1 \tag{2.14}$$

qui donne $\#C(\mathbb{F}_q) \leq q+1+g\left\lfloor 2\sqrt{q}\right\rfloor$. □

Une courbe C sur $\mathbb{F}_q$ atteignant cette borne supérieur, i.e. $\#C(\mathbb{F}_q) = q+1+g\left\lfloor 2\sqrt{q}\right\rfloor$ est appelée une *courbe optimale*.

Polynôme caractéristique du morphisme de Frobenius d'une variété abélienne

Soit A une variété abélienne sur un corps k et ℓ un entier premier à $p = \mathrm{char}(k)$. On appelle

$$T_\ell(A) = \varprojlim A[\ell^n]\left(\overline{k}\right)$$

le *ℓ-module de Tate* de A. On rappelle que $A[n]$ désigne le noyau de l'isogénie de multiplication par n, i.e. $\ker\left([n]_A \colon A \longrightarrow A\right)$. Puisqu'on a supposé ℓ et p premiers entre eux on a $A[\ell^n]\left(\overline{k}\right) \simeq (\mathbb{Z}/\ell^n\mathbb{Z})^{2g}$ si bien que $T_\ell(A) \simeq \mathbb{Z}_\ell^{2g}$. On pose $V_\ell(A) = T_\ell(A)\otimes\mathbb{Q}_\ell$ qui est un $\mathbb{Q}_\ell$-espace vectoriel de dimension $2g$.

Tout endomorphisme u de A est un morphisme de $\mathbb{Z}$-modules et commute donc avec $[\ell^n]_A$, il définit donc un morphisme $u_\ell \colon T_\ell(A) \to T_\ell(A)$ et donc un endomorphisme du $\mathbb{Q}_\ell$-espace vectoriel $V_\ell(A)$ et on pose $\chi_u = \det(T\,\mathrm{id} - u) \in \mathbb{Q}_\ell[T]$ son polynôme caractéristique.

On a [Rit17, Proposition 7.4.5] qui prouve que χ_u ne dépend pas de l'entier ℓ choisi.

Proposition 2.3.4. *Soit A une variété abélienne définie sur $\mathbb{F}_q$ et ℓ premier à q. Soit $u \in \mathrm{End}(A)$ alors le polynôme caractéristique χ_u de u_ℓ est à coefficients dans $\mathbb{Z}$ et ne dépend pas de ℓ.*

On considère maintenant

$$\begin{array}{rccc} F_A\colon & A & \longrightarrow & A \\ & P & \longmapsto & P^q \end{array}$$

le morphisme de Frobenius de A. C'est un élément de $\mathrm{End}(A)$ et on appelle $\chi_A = \chi_{F_A}$ le *polynôme caractéristique* de A. C'est un outil très puissant puisque, comme l'affirme la

proposition suivante, le polynôme caractéristique d'une variété abélienne sur $\mathbb{F}_q$ détermine sa classe d'isogénie.

Proposition 2.3.5. *Soient A et B deux variétés abéliennes sur $\mathbb{F}_q$. Alors*

- $\chi_{A\times B} = \chi_A\chi_B$.
- *S'il existe un morphisme dont le noyau est fini $A \to B$ alors $\chi_A|\chi_B$.*
- *S'il existe un morphisme surjectif $A \to B$ alors $\chi_B|\chi_A$.*
- *A et B sont isogènes si, et seulement si $\chi_A = \chi_B$.*

Pour une preuve des deux premiers points et d'une implication du quatrième voir [Rit17, Proposition 7.4.7 et Theorem 7.4.6]. Pour le troisième il suffit de passer au dual et remarquer que $\chi_{\widehat{A}} = \chi_A$. Pour une preuve du dernier point voir [Tat66]. Finalement, la proposition suivante permet d'établir un lien entre le polynôme de Weil d'une courbe et le polynôme caractéristique de sa jacobienne.

Proposition 2.3.6. *Soit C une courbe algébrique sur $\mathbb{F}_q$ et $f(T) \in \mathbb{Z}[T]$ son polynôme de Weil. Alors*

$$\chi_{\mathrm{Jac}(C)} = T^{2g} f\left(\frac{1}{T}\right).$$

Le corollaire suivant montre que la structure de la variété jacobienne d'une courbe optimale est extrêmement contrainte par cette condition.

Corollaire 2.3.7. *Soit C une courbe optimale de genre g sur $\mathbb{F}_q$. Alors $\mathrm{Jac}(C)$ est isogène à E^g où E est une courbe elliptique optimale sur $\mathbb{F}_q$.*

Démonstration. Par définition, $\#C(\mathbb{F}_q) = q + 1 + gm$ où $m = \left\lfloor 2\sqrt{q} \right\rfloor$. Or, d'après la preuve du Corollaire 2.3.3, on a $\#C(\mathbb{F}_q) = q + 1 - \sum_{i=1}^{g}(\alpha_i + \overline{\alpha_i})$ où α_i^{-1} et $\overline{\alpha_i}^{-1}$ sont les racines de f donc $\sum_{i=1}^{g}(\alpha_i + \overline{\alpha_i}) = -gm$. Si on reprend les $x_i = 1 + \alpha_i + \overline{\alpha_i} + m$ définis dans la preuve du Corollaire 2.3.3 on a alors $\sum_{i=1}^{g} x_i = g - gm + gm = g$ et donc on est dans un cas d'égalité de l'inégalité arithmético-géométrique (2.14) qui implique que tous les x_i sont égaux à 1, i.e. $\alpha_i + \overline{\alpha_i} = -m$ pour tout i. Ainsi

$$f(T) = \prod_{i=1}^{g}(1 - \alpha_i T)(1 - \overline{\alpha_i} T) = \prod_{i=1}^{g}(qT^2 + mT + 1) = (qT^2 + mT + 1)^g = f_E(T)^g$$

où E est une courbe elliptique ayant $q + 1 + m$ points et f_E est son polynôme de Weil. On a alors par la Proposition 2.3.5

$$\chi_{\mathrm{Jac}(C)}(T) = T^{2g} f(1/T) = (T^2 f_E(T))^g = \chi_E(T)^g = \chi_{E^g}(T).$$

Donc $\mathrm{Jac}(C)$ et E^g sont isogènes. □

2.3.2 Cas des produits de courbes elliptiques sur un corps fini

Dans cette section nous allons rappeler la définition de $\mathtt{Hom}_R(\_, E)$ défini par Serre et qui est une équivalence de catégories entre les R-réseaux hermitiens finiment présentés sans torsion et les variétés abéliennes isogènes à un produit de courbes elliptiques E sur un corps fini $\mathbb{F}_q$ où $R = \mathrm{End}(E) = \mathbb{Z}[\pi]$ avec π le morphisme de Frobenius sur E. Nous commencerons par définir le foncteur dans un cadre plus large que celui des modules sans torsion et des corps finis, nous énoncerons certaines propriétés générales avant d'énoncer l'équivalence. Dans un second temps nous essaierons d'adapter l'équivalence pour faire correspondre des réseaux hermitiens à des variétés polarisées. Pour l'étude générale du foncteur on s'appuiera sur [JKP+18] et pour les résultats concernant les polarisations nous suivrons [KNRR21, Section 3.1].

Le foncteur $\mathtt{Hom}_R(\_, E)$

Variétés abéliennes isogènes à un produit de courbes elliptiques Considérons une courbe elliptique sur un corps k ayant pour anneau d'endomorphisme $R = \mathrm{End}(E)$ et A une variété abélienne sur k. Alors le groupe $\mathrm{Hom}(A, E)$ a une structure naturelle de R-module à gauche. Ce module est réduit à $\{0\}$ si A n'est pas isogène à une variété de la forme $A \simeq A' \times E'$ avec E' isogène à E. En effet, si un morphisme non nul existe $f\colon A \longrightarrow E$ alors, d'après la Proposition 2.3.5, $\chi_E | \chi_A$. Plus généralement, si A isogène à $A_1 \times A_2$ avec $\mathrm{Hom}(A_2, E) = \{0\}$ alors $\mathrm{Hom}(A, E) \simeq \mathrm{Hom}(A_1, E)$.

Ainsi, étudier les modules de la forme $\mathrm{Hom}(A, E)$ se réduit au cas A isogène à E^g. La construction $\mathrm{Hom}(\_, E)$ qui à une variété abélienne A isogène à un produit de courbes elliptiques associe le R-module $\mathrm{Hom}(A, E)$ est fonctorielle. En effet, étant donnée un morphisme $f\colon A \to B$ entre deux telles variétés abéliennes on peut construire un morphisme

$$\begin{array}{rccc} \mathrm{Hom}(f, E)\colon & \mathrm{Hom}(B, E) & \longrightarrow & \mathrm{Hom}(A, E) \\ & \alpha & \longmapsto & \alpha \circ f \end{array}$$

qui est bien un morphisme de R-modules. On appelle $\mathrm{Hom}(\_, E)$ ce foncteur.

Nous souhaiterions maintenant définir un foncteur qui à des R-modules associe des variétés abéliennes isogènes à un produit de courbes elliptiques. Soit L un R-module

finiment présenté, i.e. il existe une suite exacte

$$R^m \longrightarrow R^n \longrightarrow L \longrightarrow 0$$

L'application $R^m \longrightarrow R^n$ peut être identifiée avec sa matrice $M \in M_{n,m}(R)$ dans les bases canoniques de R^m et R^n. Sa transposée ${}^tM \in M_{m,n}(R)$ induit naturellement un morphisme

$$E^n \xrightarrow{{}^tM} E^m$$

dont le noyau est noté $\mathtt{Hom}_R(L, E)$. Remarquons que la matrice M (ou de manière équivalence la présentation de L) n'intervienne pas dans la définition de $\mathtt{Hom}_R(L, E)$. Pour cause cette définition est indépendante de la présentation.

Par exemple, si on considère le R-module R/aR, avec $\alpha \in R$ on a une présentation

$$R \xrightarrow{\alpha} R \xrightarrow{p} R/aR \to 0$$

où p est la projection canonique on voit alors facilement que $\mathtt{Hom}_R(R/aR, E) = E[\alpha] = \ker(\alpha \colon E \to E)$. En particulier, pour $n \in \mathbb{N}^*, \mathtt{Hom}_R(R/nR, E) = E[n]$. Un autre exemple est celui du module R, on a une présentation

$$0 \to R \to R \to 0$$

si bien que $\mathtt{Hom}_R(R, E) = E$.

On énonce dans la proposition suivante les propriétés essentielles satisfaites par le foncteur $\mathtt{Hom}_R(\_, E)$ (voir [JKP+18, Proposition 4.3, Theorem 4.4 et Theorem 4.7] pour des énoncés plus généraux et des preuves).

Proposition 2.3.8. *Soit E une courbe elliptique sur un corps k. On pose $R = \mathrm{End}(E)$, L un R-module à gauche finiment présenté sans torsion et $A = \mathtt{Hom}_R(L, E)$. Alors*

1. *Le schéma en groupe A est une variété abélienne isogène*[16] *à $E^{\mathrm{rk}\, L}$.*
2. *Le foncteur $\mathtt{Hom}_R(\_, E)$ est exact.*
3. *Pour tout idéal $\mathfrak{a} \subseteq R$ on a $\mathtt{Hom}_R(R/\mathfrak{a}R, E) \simeq E[\mathfrak{a}] = \bigcap_{\alpha \in \mathfrak{a}} \ker \alpha$ et $\mathtt{Hom}_R(\mathfrak{a}, E) \simeq E/E[\mathfrak{a}]$.*
4. *On a $\widehat{A} \simeq \mathtt{Hom}_R(L^*, E)$ où L^* est l'ensemble des formes antilinéaires de L.*

16. On rappelle que le rang d'un R-réseau L est l'entier $\dim(KL)$ où $K = \mathrm{Frac}(R)$.

On énonce l'équivalence de catégories sur les corps fini. Voir [JKP+18, Theorem 7.6]

Théorème 2.3.9. *Soit E une courbe elliptique telle que* $\mathrm{End}(E) = \mathbb{Z}[\pi]$ *où π le morphisme de Frobenius de E. Alors* $\mathtt{Hom}_R(\_, E)$ *et* $\mathrm{Hom}(\_, E)$ *sont des équivalences de catégories inverses l'une de l'autre.*

Les auteurs montrent plus généralement que le foncteur $\mathtt{Hom}_R(, E)$ est toujours plein et fidèle et décrivent son image essentielle dans [JKP+18, Theorem 4.8] sans condition sur le corps sur lequel est défini E ni sur son anneau d'endomorphismes. Ils donnent aussi une condition nécessaire et suffisante pour que $\mathtt{Hom}_R(\_, E)$ soit une équivalence de catégories pour E une courbe elliptique ordinaire sur un corps quelconque avec multiplication complexe (voir [JKP+18, Theorem 7.7]).

Cas des polarisations Désormais on se place dans les conditions de l'équivalence énoncée dans le Théorème 2.3.9, i.e. E est une courbe elliptique sur $\mathbb{F}_q$ telle que $R = \mathrm{End}(E) = \mathbb{Z}[\pi]$ où π est le morphisme de Frobenius. Toutes les variétés abéliennes considérées dans cette section seront isogènes à un produit de E et donc correspondent, via $\mathrm{Hom}(\_, E)$, à des R-modules finiment présentés sans torsion, c'est-à-dire à des R-réseaux. On pose $K = \mathrm{Frac}\, R$ et on considère une telle variété A et une polarisation $a\colon A \to \widehat{A}$. On pose

$$\rho = \mathrm{Hom}(a, E)\colon L^* \to L.$$

On a $\rho^* = \rho$ car $\widehat{a} = a$. Puisque $\mathrm{Hom}(\_, E)$ est exact et contravariant ρ est injective et donc $\rho \otimes_R \mathrm{id}_K\colon V^* \to V$, où $V = KL$, est bijective (on la note toujours ρ). L'application $\rho^{-1}\colon V \to V^*$ définit une forme hermitienne $H(x, y) = \rho^{-1}(x)(y)$. Cette forme hermitienne est définie positive d'après [KNRR21, Lemma 3.10] et l'image de L^* dans L par ρ est $L^\# = \{v \in V, H(v, L) \subseteq R\}$. Autrement dit, le réseau hermitien $(L^\#, H)$ est entier.

On peut alors énoncer l'équivalence qui nous intéresse (voir [KNRR21, Theorem 3.3]).

Théorème 2.3.10. *Soit E une courbe elliptique sur $\mathbb{F}_q$ et $R = \mathrm{End}(E) = \mathbb{Z}[\pi]$ avec π le morphisme de Frobenius sur E. Alors* $\mathtt{Hom}_R(\_, E)$ *définit une équivalence de catégories entre les R-réseaux hermitiens (L, H) tels que $(L^\#, H)$ est entier et les variétés abéliennes polarisées (A, a) isogènes à un produit de E.*

Son inverse est donnée par

$$\begin{aligned}\mathrm{Hom}(\_, E)\colon \begin{Bmatrix}(A,a)\ \textit{variété polarisée telle que}\\ A\ \textit{isogène à un produit de } E\end{Bmatrix} &\longleftrightarrow \begin{Bmatrix}(L,H)\ R\textit{-réseau hermitien}\\ \textit{tel que } (L^{\#},H)\ \textit{entier}\end{Bmatrix}\\ (A,a) &\longmapsto (\mathrm{Hom}(A,E),H)\ \textit{avec}\\ &\quad H\colon (x,y)\mapsto \mathrm{Hom}(a,E)^{-1}(x)(y).\end{aligned}$$

De plus, si $\mathrm{Hom}((A,a),E) = (L,H)$ *alors* $\deg a = [L\colon L^{\#}]$.

On a donc une correspondance entre les variétés abéliennes principalement polarisées isogènes à un produit de E et les R-réseaux hermitiens unimodulaires.

De même que dans la Section 2.2.4 où nous énoncions des équivalences sur les complexes, lorsque nous considérons la catégorie des variétés abéliennes polarisées (resp. des réseaux hermitiens) les morphismes entre les objets sont les isogénies polarisées (resp. les isométries). Ce ne sont plus simplement les morphismes entre les variétés (resp. réseaux) sous-jacentes. Une autre façon de le dire est que le foncteur d'oubli de la polarisation $(A,a)\mapsto A$ n'est pas plein sur les catégories considérées (de même pour le foncteur d'oubli de la forme hermitienne).

Sous-réseaux orthogonaux Dans le but de calculer les thêta constante d'une variété abélienne polarisée (A,a) isogène à E^g nous pouvons calculer les thêta constantes de la courbe E (munie de sa polarisation principale) à l'aide des formules de Thomae et d'en déduire celles de $(E^g,\ell\lambda_0)$ où ℓ est un entier et λ_0 la polarisation produit des polarisations principales sur E. Il est ensuite possible de calculer les thêta constantes de (A,a) connaissant le noyau d'une isogénie polarisée $(E^g,\ell\lambda_0)\longrightarrow(L,H)$ grâce aux formules d'isogénie.

Dans [KNRR21, Section 3.3] nous avons détaillé comment traduire ce problème dans le monde des réseaux hermitiens via le foncteur $\mathtt{Hom}_R(\_,E)$ de la section précédente et comment calculer en pratique le noyau d'une telle isogénie polarisée.

Il faut noter que les formules de Thomae permettent de calculer les fonctions thêta de $(E_1\times\cdots\times E_g,\ell\lambda_0)$ et qu'il est théoriquement parfaitement possible de calculer les thêta constantes de (A,a) à partir du noyau d'une isogénie polarisée

$$(E_1\times\cdots\times E_g,\ell\lambda_0)\longrightarrow(A,a).$$

Les avantages de considérer un produit de courbes elliptiques différentes sont les suivants

Noyaux plus petits : En s'autorisant des courbes différentes de E on pourrait obtenir des ℓ plus petits. Ce paramètre est extrêmement limitant dans nos calculs (en pratique il faut déjà plusieurs heures pour calculer les thêta constantes de (A, a) à partir de celles de $(E^g, \ell\lambda_0)$ pour $g = 3$ et $\ell = 11$).

Description de plus de variétés abéliennes (surtout en dimension paire) : Comme expliqué dans [KNRR21, Section 3.3], trouver une telle isogénie polarisée $(E^g, \ell\lambda_0) \longrightarrow (A, a)$ revient à trouver une famille de g vecteurs orthogonaux de norme ℓ dans $(L, H) = \mathtt{Hom}_R((A, a), E)$. Or, lorsque $\det(KL, H) \neq 1 \in \mathbb{Q}^*/N(K^*)$ et g est pair, il n'existe tout simplement pas de famille de g vecteurs orthogonaux de même norme dans (KL, H). En revanche, comme nous allons le voir, il existe toujours des familles orthogonales qui permettent de produire des isogénies polarisées avec des produits de courbes elliptiques distinctes.

Nous n'avons pas étudié ces constructions dans [KNRR21] pour une raison très simple ; le calcul des thêta constantes, bien que théoriquement faisable, n'est pas implémenté pour un produit de courbes elliptiques distinctes. Il est cependant possible d'implémenter ce calcul et c'est pour cela que je souhaite développer ces constructions ici.

Il est important de noter que, bien que le fait de considérer un produit de courbes potentiellement distinctes lève de nombreuses barrières pour décrire les variétés abéliennes principalement polarisées, il reste malgré tout des obstacles. Dans le but de calculer les thêta constantes nous avons besoin que ℓ soit impair [17]. Or, nous avons vu dans la Section 1.2.3 qu'il se peut que certains réseaux hermitiens unimodulaires n'aient que des vecteurs de norme paire [18] auquel cas le fait de considérer un produit de courbes elliptiques distinctes ne changera rien au problème.

On rappelle (Proposition 1.2.11) qu'étant donné un réseau L sur un ordre quadratique R, il existe toujours une suite d'ordres $R \subseteq R_1 \subseteq \cdots \subseteq R_g \subseteq \mathscr{O}_K$, des idéaux fractionnaires $\mathfrak{a}_1, \ldots, \mathfrak{a}_g$ tels que $\mathfrak{a}_i$ inversible dans R_i et une base $(x_1, \ldots, x_g)$ de $V = KL$ tel que L s'écrit sous la forme

$$L = \mathfrak{a}_1 x_1 \oplus \cdots \oplus \mathfrak{a}_g x_g.$$

Les ordres $R_1 \subseteq \cdots \subseteq R_g$ et la classe de Steinitz $\mathrm{st}(L)$ de L, i.e. la classe de $\mathfrak{a}_1 \ldots \mathfrak{a}_g$ dans

17. Cette condition est aussi théoriquement dépassable mais son implémentation semble bien plus difficile que d'implémenter le cas de produit de courbes distinctes.

18. Ceci ne peut se produire qu'en dimension paire et si K est un corps dyadique, i.e. 2 divise le discriminant de K (voir Section 1.2.3).

$\mathrm{Cl}(R_g)$ déterminent la classe d'isomorphisme de L.

Lemme 2.3.11. *Avec les notations ci-dessus. Soit (L, H) un réseau hermitien unimodulaire sur un ordre quadratique R. On pose $\mathfrak{a} = \mathfrak{a}_1 \cdots \mathfrak{a}_g$ un représentant de la classe de Steinitz de L et on pose $d^{-1} = N_{R_g}(\mathfrak{a})$. Alors il existe un entier $\ell \geq 1$ et un sous-module de L de la forme $N = Ru_1 \oplus \cdots \oplus Ru_{g-1} \oplus \mathfrak{a}u_g$ tel que la famille $(u_1, \ldots, u_g)$ est orthogonale et $H(u_i, u_i) = \ell, i \leq g-1$ et $H(u_g, u_g) = \ell d$.*

Démonstration. On montre que $\mathfrak{v}(L) = R_g$ (la Proposition 1.2.4 ne concerne que les ordres maximaux, nous allons cependant nous en inspirer). On reprend les notations du paragraphe avant le Lemme. À l'instar du cas maximal on a toujours [19]

$$\begin{aligned}
\mathfrak{v}(L) &= \mathfrak{a}_1\overline{\mathfrak{a}_1} \cdots \mathfrak{a}_g\overline{\mathfrak{a}_g} \det(G(x_1, \ldots, x_g)) \\
&= N_{R_1}(\mathfrak{a}_1)R_1 \cdots N_{R_g}(\mathfrak{a}_g)R_g \det(G(x_1, \ldots, x_g)) \\
&= N_{R_g}(\mathfrak{a}_1 R_g)R_1 \cdots N_{R_g}(\mathfrak{a}_g)R_g \det(G(x_1, \ldots, x_g)) \\
&= N_{R_g}(\mathfrak{a}_1 \cdots \mathfrak{a}_g) \det(G(x_1, \ldots, x_g))R_g \\
&= d^{-1} \det(G(x_1, \ldots, x_g))R_g.
\end{aligned}$$

D'autre part, on a toujours $\mathfrak{v}(L) = \mathfrak{v}(L^{\#})^{-1}$ en tant que R_g-idéal fractionnaire. Ainsi, puisque $L = L^{\#}$ on a $\mathfrak{v}(L)^2 = R_g$. Malheureusement, dans la preuve de la Proposition 1.2.4, nous avons utilisé l'unique décomposition en facteurs premiers pour conclure ce qui n'est pas vrai pour les ordres non maximaux. Nous allons cependant essayer de nous y ramener. D'après [Cox85, Corollary 7.17] on peut toujours trouver $n \in R_g$ tel que $n\mathfrak{v}(L)$ est un idéal de norme première au conducteur f de R_g dans $\mathscr{O}_K$, on a alors

$$\begin{aligned}
(n\mathfrak{v}(L))^2 &= n^2 R_g \\
(n\mathfrak{v}(L))^2 \mathscr{O}_K &= n^2 \mathscr{O}_K \\
(n\mathfrak{v}(L)\mathscr{O}_K)^2 &= n^2 \mathscr{O}_K.
\end{aligned}$$

Donc, d'après l'unicité de la décomposition en idéaux premiers de $\mathscr{O}_K$ on a, en prenant l'intersection avec $R_g, n\mathfrak{v}(L)\mathscr{O}_K = n\mathscr{O}_K$ et puisque n et $n\mathfrak{v}(L)$ sont de norme première à f on a $n\mathfrak{v}(L) = nR_g$, i.e. $\mathfrak{v}(L) = R_g$ (voir [Cox85, Proposition 7.20]).

On en déduit que $d^{-1} \det(G(x_1, \ldots, x_g)) = 1$, i.e. $\det(KL, H) = d \in \mathbb{Q}^*/N(K^*)$.

19. Il peut être utile de se remémorer la Proposition 1.1.17 pour toutes les manipulations sur les normes des idéaux fractionnaires.

Autrement dit, (V, H) est isomorphe au K-espace hermitien K^g muni de la forme hermitienne donnée par la matrice de Gram $H_0 = \begin{pmatrix} 1 & & \\ & \ddots & \\ & & d \end{pmatrix}$. On pose alors $v_i \in V$ tel que $H(v_i, v_i) = 1, i \leq g-1$ et $H(v_g, v_g) = d$. Puisque L est un réseau, il existe $\alpha \in R$ tel que $\alpha(Rv_1 + \cdots + \mathfrak{a}v_g) \subseteq L$. En posant $u_i = \alpha v_i$ et $\ell = N(\alpha)$ on a le résultat annoncé. □

Proposition 2.3.12. *Soit (A, a) une variété abélienne principalement polarisée sur $\mathbb{F}_q$ isogène à un produit de E telle que $\mathrm{End}(E) = \mathbb{Z}[\pi]$ alors il existe un entier ℓ, une courbe elliptique E' et une isogénie polarisée*

$$\varphi\colon (E^{g-1} \times E', \ell\lambda_0) \to (A, a).$$

Démonstration. On pose $(L, H) = \mathrm{Hom}((A, a), E)$ et on reprend les notations du Lemme 2.3.11. On a alors $N = Ru_1 + \cdots + \mathfrak{a}u_g$ sous-module de L (remarquons que l'inclusion $N \hookrightarrow L$ est une isométrie). On a alors en passant l'inclusion au dual

$$L^\# = L \xrightarrow{\iota} N^\# = Ru_1^\# + \cdots + \mathfrak{a}^\# u_g^\#$$

avec $(u_j^\#)$ la base duale de (u_j), i.e. telle que $H(u_i, u_i^\#) = 1$ et $\mathfrak{a}^\# = [R\colon \mathfrak{a}]$ (même démonstration que pour le cas maximal de la Proposition 1.2.4). Puisque (u_i) est déjà une famille orthogonale on a $u_i^\# = \frac{1}{H(u_i,u_i)} u_i$. On remarque qu'on a une isométrie naturelle $(N^\#, H) \simeq \left(R^{g-1} \oplus \mathfrak{a}^\#, \frac{1}{\ell} H_0^{-1}\right)$ avec H_0 la matrice de la démonstration ci-dessus.

Remarquons que, quitte à remplacer $\mathfrak{a}$ par un autre représentant, on peut supposer $\mathfrak{a}^\#$ idéal de R (ainsi $d = N_{R_g}(\mathfrak{a}^\#)$ est entier). On pose $E' = E/E\left[\mathfrak{a}^\#\right]$ Par ailleurs, d'après la Proposition 2.3.8 et le Théorème 2.3.10, $\mathrm{Hom}((E', a_{E',0}), E) \simeq (\mathfrak{a}^\#, h)$ est un réseau hermitien unimodulaire (avec $a_{E',0}$ la polarisation principale sur E'). D'après, le Théorème 1.2.5 ceci implique que $h = \frac{1}{N(\mathfrak{a}^\#)} h_0 = \frac{1}{d} h_0$ où h_0 est la forme hermitienne canonique sur K, i.e. $h_0(x, y) = x\overline{y}$.

Avec $(A, a) = \mathtt{Hom}_R((L, H), E)$ et en composant l'isométrie ι avec le foncteur $\mathtt{Hom}_R(\_, E)$ on a donc une isogénie polarisée

$$\varphi = \mathtt{Hom}_R(\iota, E)\colon (E^{g-1} \times E', \ell\lambda_0) \simeq \mathtt{Hom}_R((N^\#, H), E) \to (A, a).$$

□

Il reste cependant à déterminer comment calculer en pratique le noyau de l'isogénie

polarisée φ. Puisque φ est une isogénie polarisée, par définition on a $\ell\lambda_0 = \widehat{\varphi} a \varphi$ ce qui implique que $\ker\varphi \subseteq E^{g-1}[\ell] \times E'[\ell]$. On a déjà expliqué dans [KNRR21, Section 3.3] comment décrire le noyau d'une isogénie polarisée provenant d'une isométrie $L_1 \to L_2$ cependant l'algorithme n'est effectif que dans le cas où L_2 est libre.

On rappelle qu'étant donnée une isométrie (nous n'écrivons pas les formes hermitiennes pour alléger) $\iota\colon L_1 \to L_2$ et des présentations $R^{m_i} \xrightarrow{T_1} L_i$, l'isométrie ι se relève en une matrice $P \in M_{m_2,m_1}(R)$ telle que

$$\begin{array}{ccc} R^{m_1} & \xrightarrow{T_1} & L_1 \\ \downarrow{\scriptstyle P} & & \downarrow{\scriptstyle \iota} \\ R^{m_2} & \xrightarrow{T_2} & L_2 \end{array}$$

le noyau de $\varphi = \mathtt{Hom}_R(\iota, E)$ satisfait

$$\ker\varphi = \mathtt{Hom}_R(T_2, E)^{-1} \ker {}^tP.$$

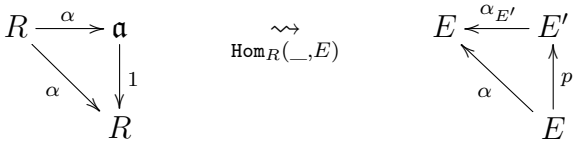
Le fait de choisir L_2 libre permettait notamment de choisir $m_2 = g$ et $T_2 = \mathrm{id}$, si bien que $\ker\varphi = \ker {}^tP$. Il suffisait alors de calculer l'action de ${}^tP$ sur $E[\ell]^g \simeq (\mathbb{Z}/\ell\mathbb{Z})^{2g}$. Le fait de choisir L_2 non libre nous empêche malheureusement de prendre $m_2 = g$ et T_2 est alors nécessairement non triviale. Dans notre cas avec $L_2 = N^{\#} = R^{g-1} \times \mathfrak{a}^{\#}$ on peut prendre $R^{m_2} = R^{g-1} \times R^2$ et T_2 l'identité sur les $g-1$ premières composantes et une présentation de $\mathfrak{a}^{\#}$ sur les deux dernières.

On constate alors qu'il suffit pour un idéal $\mathfrak{a}$ de R, une présentation $T\colon R^2 \to \mathfrak{a}$ de $\mathfrak{a}$, un entier ℓ et G un sous-groupe de $E[\ell]^2$ d'être capable de décrire la préimage de $G, \mathtt{Hom}_R(T, E)^{-1}G$ dans $E'[\ell]$ où $E' = E/E[\mathfrak{a}]$. Soient α, β des générateurs du R-module $\mathfrak{a}$, on a alors la présentation $T\colon R^2 \xrightarrow{\begin{pmatrix}\alpha & \beta\end{pmatrix}} \mathfrak{a}$ qui devient

$$E^2 \xleftarrow{\begin{pmatrix}\alpha_{E'} \\ \beta_{E'}\end{pmatrix}} E'$$

en composant par $\mathtt{Hom}_R(\_, E)$ avec $\alpha_{E'} = \mathtt{Hom}_R(\alpha, E)\colon E' \to E$. Ainsi $\mathtt{Hom}_R(T, E)^{-1}G = \alpha_{E'}^{-1}G \cap \beta_{E'}^{-1}G$. On veut maintenant expliquer comment décrire le groupe $\alpha_{E'}^{-1}$. On a des

diagrammes commutatifs



où $p\colon E \to E'$ est la projection canonique et $E \xrightarrow{\alpha} E$ l'endomorphisme α. On a alors $\alpha_{E'}^{-1}G = p\alpha^{-1}G$. En effet, $\alpha^{-1}G = (\alpha_{E'}p)^{-1}G = p^{-1}\alpha_{E'}^{-1}G$ donc $p\alpha^{-1}G = \alpha_{E'}^{-1}G$ car p surjective.

On remarque que pour G un sous-groupe de la ℓ-torsion de E si $x \in \alpha^{-1}G \cap \beta^{-1}G$ alors $x \in E[d\ell]$ où $d = N(\mathfrak{a})$ avec $\mathfrak{a} = \langle \alpha, \beta \rangle$. En effet, si on a $N(\alpha) = \overline{\alpha}\alpha$ donc $\ell N(\alpha)x \in \overline{\alpha}\ell\alpha(x) = 0$ de même pour β. Alors

$$x \in E[N(\alpha)\ell] \cap E[N(\beta)\ell)] = E[\mathrm{pgcd}(N(\alpha), N(\beta))\ell] = E[d\ell].$$

On obtient alors l'Algorithme 2.

Algorithme 2 Calcul de la préimage de $\begin{pmatrix}\alpha_{E'}\\ \beta_{E'}\end{pmatrix} : E' \to E^2$

Entrée : Un idéal $\mathfrak{a} = \langle \alpha, \beta \rangle$, la projection canonique $p\colon E \to E' = E/E[\mathfrak{a}]$ et un sous-groupe G de $E[\ell]^2$.

Sortie : La préimage de G par $\begin{pmatrix}\alpha_{E'}\\ \beta_{E'}\end{pmatrix} : E' \to E^2$.

1: $d \leftarrow N(\mathfrak{a})$
2: Calculer une base (e_1, e_2) de $E[d\ell]$ vu comme un $\mathbb{Z}/d\ell\mathbb{Z}$-module.
3: Calculer une base (f_1, f_2) de $E[\ell]$ vu comme un $\mathbb{Z}/\ell\mathbb{Z}$-module.
4: Calculer $\Pi = \begin{pmatrix}\pi(e_1) & \pi(e_2)\end{pmatrix} \in M_2(\mathbb{Z}/d\ell\mathbb{Z})$.
5: Écrire $\alpha = a_1 + a_2\pi$ et $\beta = b_1 + b_2\pi$ et les identifier[20] avec $M_\alpha = a_1 I_2 + a_2\Pi$ et $M_\beta = b_1 I_2 + b_2\Pi$.
6: Calculer $M_\alpha^{-1}G$ et $M_\beta^{-1}G$ où G est identifier à un sous-groupe de $(\mathbb{Z}/d\ell\mathbb{Z})^2$ via les inclusions $G \subseteq E[\ell] \simeq (\mathbb{Z}/\ell\mathbb{Z})^2 \subseteq (\mathbb{Z}/d\ell\mathbb{Z})^2$.
7: Reconnaître $M_\alpha^{-1}G \cap M_\beta^{-1}G \subseteq (\mathbb{Z}/d\ell\mathbb{Z})^2$ comme un sous groupe G_0 de $E[d\ell]$.
8: **return** $p(G_0) \subseteq E'[\ell]$.

Combiné à [KNRR21, Algorithm 5] l'Algorithme 2 nous permet plus généralement de

calculer le noyau d'isogénies polarisées de la forme

$$\varphi\colon (E_1 \times \cdots \times E_g, \ell\lambda_0) \to (A, a)$$

où $E_i = \mathtt{Hom}_R(\mathfrak{a}_i, E)$.

Pour obtenir de telles décompositions il suffit alors d'adapter [KNRR21, Algorithm 4] en cherchant les vecteurs de norme ℓ dans $\mathfrak{a}_i^{-1}L$ au lieu de L.

Chapitre 3

CALCUL DE LA CLASSE D'ISOGÉNIE D'UN PRODUIT DE COURBES ELLIPTIQUES

SPANNING THE ISOGENY CLASS OF A POWER OF AN ELLIPTIC CURVE

MARKUS KIRSCHMER, FABIEN NARBONNE, CHRISTOPHE RITZENTHALER, AND DAMIEN ROBERT

Abstract. Let E be an ordinary elliptic curve over a finite field and g be a positive integer. Under some technical assumptions, we give an algorithm to span the isomorphism classes of principally polarized abelian varieties in the isogeny class of E^g. The varieties are first described as hermitian lattices over (not necessarily maximal) quadratic orders and then geometrically in terms of their algebraic theta null point. We also show how to algebraically compute Siegel modular forms of even weight given as polynomials in the theta constants by a careful choice of an affine lift of the theta null point. We then use these results to give an algebraic computation of Serre's obstruction for principally polarized abelian threefolds isogenous to E^3 and of the Igusa modular form in dimension 4. We illustrate our algorithms with examples of curves with many rational points over finite fields.

1. Introduction

Let $g, m \geq 1$ be integers, p be a prime, $q = p^m$ and $\mathscr{W}$ be the isogeny class of a given dimension-g abelian variety A over $\mathbb{F}_q$. The elements of $\mathscr{W}$ will be the $\mathbb{F}_q$-isomorphism classes of abelian varieties over $\mathbb{F}_q$ which are $\mathbb{F}_q$-isogenous to A. Thanks to the work of Tate [Tat66] and Honda [Hon68], one knows that the Weil polynomial W is an invariant on $\mathscr{W}$. One can also characterize the finite list $S(q, g)$ of possible Weil polynomials for given q and g. These finite lists have been made explicit up to genus 5 [Hal10; HS12; Hay19]. Representing now an isogeny class $\mathscr{W}$ by a polynomial $W \in S(q, g)$, a harder task is to describe the finite set of elements (i.e. $\mathbb{F}_q$-isomorphism classes of abelian varieties) inside $\mathscr{W}$. Currently, there is no unified nor complete way to achieve this task. To our best knowledge, one can get a full abstract description

(1) for $g = 1$ [Wat69];
(2) for ordinary abelian varieties [Del69; Ser85; How95; Mar19; JKP+18];
(3) for abelian varieties $A \sim E^g$ where E is a supersingular elliptic curve either over $\mathbb{F}_p$ or over $\mathbb{F}_{p^2}$ with trace $\pm 2p$; [JKP+18];
(4) when $q = p$ and W has no real root [CS15];
(5) for p-rank $g - 1$ simple abelian varieties over fields of odd characteristics [OS20].

Roughly speaking, the above descriptions functorially relate $\mathbb{F}_q$-isomorphism classes of (non-polarized) abelian varieties in $\mathscr{W}$ and certain finitely generated modules over orders in products of number fields or quaternion algebras. Notice that even for $g = 2$, the situation is still incomplete as far as we know: there are only partial results for supersingular and superspecial abelian surfaces [IKO86; XYY19; HNR09] and p-rank 1 split isogeny classes seem untouched.

The situation is even more critical if one is interested in $\mathbb{F}_q$-isomorphism classes of *polarized* abelian varieties in $\mathscr{W}$. Since the distinction is important for one of our goal (identifying Jacobians in the isogeny class), we denote the $\mathbb{F}_q$-isomorphism classes of principally polarized abelian varieties isogenous to A by $\mathscr{W}_1$. Notice that there is no inclusion between the elements of $\mathscr{W}$ and $\mathscr{W}_1$ since the notions of isomorphism classes are distinct. When the abelian varieties in $\mathscr{W}$ are isogenous to products of non-isogenous ordinary simple abelian varieties, there are algorithms to enumerate the elements of $\mathscr{W}$ or $\mathscr{W}_1$ (see [Mar19]). The LMFDB database is currently keeping track of the cardinality of these sets for small values of g and q [DKR+20].

Date: April 2020.
2010 *Mathematics Subject Classification.* 14H42,14G15, 14H45, 16H20.
Key words and phrases. hermitian lattice, order in quadratic field, isogeny class, polarization, curves with many points over finite fields, Siegel modular form, theta constant, theta null point, algorithm, Igusa modular form, Serre's obstruction, Schottky locus.

In the present article, we consider a different case from [Mar19], namely $\mathscr{W}$ is the isogeny class of the g-th power of an ordinary elliptic curve $E/\mathbb{F}_q$. Let π be the Frobenius endomorphism of E and $R = \mathbb{Z}[\pi, q/\pi] = \mathbb{Z}[\pi]$. The set S_E of $\mathbb{F}_q$-isomorphism classes of elliptic curves $\{E_1, \dots, E_r\}$ isogenous to E is in bijection with the ideal class monoid $\mathrm{ICM}(R)$ of R. Moreover, it is always possible to identify in this set or directly construct one elliptic curve isogenous to E with minimal endomorphism ring, i.e. equal to R (see the discussion at the beginning of Section 3.3). We will assume from now on that this is our curve E. The functor given in [JKP+18] which associates to any $A \in \mathscr{W}$ the finitely generated torsion-free R-module (or in short R-lattice) $\mathrm{Hom}(A, E)$ of rank g is an equivalence of categories and provides an inverse denoted $\mathscr{F}_E$. Note that this functor is distinct from the one used for instance in [Mar19] (it is contravariant and exact) and there is no easy way to compare them away from projective R-modules. But both functors lead to the conclusion that the elements in $\mathscr{W}$ are represented by products of elliptic curves $E_1, \dots, E_g$ in S_E corresponding to a sequence of orders $R \subset \mathrm{End}(E_1) \subset \dots \subset \mathrm{End}(E_g)$ and invertible $\mathrm{End}(E_i)$-ideal classes I_i with a given fixed product $I_1 \cdots I_g$ in $\mathrm{ICM}(R)$ (see [Kan11, Th.1], [Mar19], [JKP+18, Th.3.2]).

Since we are interested in $\mathbb{F}_q$-isomorphisms classes of polarized abelian varieties, we need to translate the notion of polarization in the category of R-lattices through the functor $\mathrm{Hom}(A, E)$. We show in Theorem 3.3 and Corollary 3.6 that this can indeed be done: the elements in $\mathscr{W}_1$ are in correspondence with the unimodular positive definite hermitian R-lattice (L, h) of rank g (see Section 2.1 for a review on these notions for lattices). This result is no surprise to the specialists as it generalizes a similar result of Serre [Lau18, Appendix] when R is the maximal order in $\mathbb{Q}(\pi)$ and is analogue of the result of [How95; Mar19] using a different functor.

How to enumerate the lattices (L, h)? This is part of a broader and beautiful theory which has been developed for general orders in number fields or quaternion algebras. However, even in the case of imaginary quadratic orders, the algorithms have been mainly implemented in the case where R is a maximal order, cf. [Sch98; Kir19]. In Section 2.2, we recall some elements of this theory restricted to imaginary quadratic orders and show how to adapt these algorithms when R is not maximal. This generalization comes at the price of much slower algorithms which can be sped up if one restricts to lattices which are projective R-modules (or equivalently to abelian varieties which are products of elliptic curves with endomorphism rings isomorphic to R). While our method for enumerating projective R-modules is quite efficient, we believe that there is still lot of room for improvements in the general case.

Such descriptions, though powerful, do not allow to get a real grasp on a given polarized variety $(A, \mathscr{L})$. In particular, given an abstract description of an element in $\mathscr{W}_1$, one would like for instance to see if it is the Jacobian of a curve and if so, to give an equation of the curve. For this, we have to jump back to the algebraic geometry side and associate to the abstract description some data describing the embedding $\phi_{\mathscr{L}^i}$, $i \geq 3$, of A into a projective space $\mathbb{P}^N$. When $p \neq 2$, Mumford showed how to extend the classical theory over $\mathbb{C}$ by using an algebraic version of the theta constants, called a *theta null point*. These constants are projectively the image by $\phi_{\mathscr{L}^i}$ of $0 \in A$ for a careful choice of basis of $\mathbb{P}^N$. However, if this data is not available before hand for at least one principally polarized abelian variety in $\mathscr{W}_1$, the only known method to compute it is to work with a lift of A and its polarization to $\mathbb{C}$, perform analytic computations with enough precision, hopefully recognize algebraic numbers and eventually reduce the result over the finite field. When A is simple, this is the classical setting of the Complex Multiplication methods (see for instance [CFA+06, Chap.18]) but the output is heuristic when $g > 2$ [Sut11; Str14].

In our case, we will take advantage that it is easy to compute the theta null point on $A_0 = E^g \in \mathscr{W}_1$ with the product polarization $\mathscr{L}_0$. It boils down to computing the (projective) thetanull point on E. The formula for their fourth power is a particular case of Thomae's formula. We will give an elementary proof of this result and show that one can take arbitrary fourth roots (see Lemma 4.6 and Corollary 4.8). Doing so, we will also prepare for a 'modular version' of the thetanull point that we will need later and take great care of the constant involved.

We also show how to deduce from the lattice description (L, h) of $(A, \mathscr{L}) \in \mathscr{W}_1$ an isogeny $f : A_0 \to A$ such that $f^*\mathscr{L} = \mathscr{L}_0^\ell$ for a certain $\ell \geq 1$. This is achieved by looking for g orthogonal vectors of norm ℓ in $L^\#$ (a certain dual of L for h), see Section 2.3. We can then give f through an explicit maximal isotropic kernel K in $A_0[\ell]$, see Section 3.3. The explicit *isogeny formula* developed in [CR15] allows then to transport the thetanull point on $(A_0, \mathscr{L}_0)$ to the one on $(A, \mathscr{L})$. This leads to the following overview of our algorithm.

Algorithm 1 Overview of the full algorithm

Input: An integer $g > 1$ and the Weil polynomial W of an ordinary elliptic curve over $\mathbb{F}_q$ (with some technical restrictions, see the discussion below).

Output: The theta null points of all indecomposable principally polarized abelian varieties with Weil polynomial W^g.

1: Let $R = \mathbb{Z}[x]/(W)$ and compute an elliptic curve $E/\mathbb{F}_q$ such that $\mathrm{End}(E) = \mathbb{Z}[\pi] \simeq R$ (see Section 3.3).
2: Use Algorithm 2 (resp. 3) to get a list of all (resp. all projective) indecomposable unimodular positive definite hermitian R-lattices (L, h) up to isometry.
3: Apply Algorithm 5 to compute a maximal isotropic kernel K of an isogeny $f : E^g \to \mathscr{F}_E(L)$ for each (L, h).
4: **return** the output of Algorithm 6 on each $((E)_{i=1,\dots,g}, K)$.

In practice, there are restrictions on the W for which this algorithm is going to work. Indeed, the current implementation of the isogeny formula imposes several constraints on the kernel K of f. We list them below, starting from what would require the most work if one intends to remove it. This should be taken with a grain of salt as it is of course impossible to predict possible obstacles without an actual study.

(1) The algorithm imposes p to be odd since it uses theta structures of even level;
(2) The algorithm imposes to look for f such that $f^*\mathscr{L} = \mathscr{L}_0^\ell$ for an integer $\ell > 0$, whereas the strategy would work with $f^*\mathscr{L}$ any completely decomposable polarization. Because of this, f does not always exist (see Example 2.24). We give necessary and sufficient conditions for its existence in Theorem 2.16 (for instance, it does always exist is g is odd);
(3) The algorithm imposes ℓ to be coprime to $2p$, see Remark 4.1. We work out in Section 2.3 a thorough local analysis of the lattices which gives a refinement of Theorem 2.16. For instance, when g is odd it is sufficient that the conductor of R is odd to find such an ℓ;
(4) Even when ℓ is coprime to $2p$, we have to discard cases when the kernel K from Algorithm 1 is not isomorphic as an abstract group to $(\mathbb{Z}/\ell\mathbb{Z})^g$. Notice that when ℓ is square free, K is necessarily isomorphic to $(\mathbb{Z}/\ell\mathbb{Z})^g$ so the algorithm always works. We did not try to get a proof of the existence of such a good ℓ and we pragmatically chose to test the group structure of a given kernel K until we get the required abstract group isomorphism.

The full cost of the algorithm is hard to estimate: it heavily depends on the smallest good ℓ one can find (when it exists) and it is an open question to find an upper bound in terms of R and g for the maximum of the minimal ℓ for a given $\mathscr{W}_1$. Once ℓ is given, a lower bound for the complexity is given by the one of Algorithm 6 which is $O(\ell^g)$. Be aware that this hides a large constant, since the computations have to be performed on the extension of $\mathbb{F}_q$ where all ℓ-torsion points of E are defined. Typically, the algorithm works for a given element of $\mathscr{W}_1$ in reasonable time when ℓ is smaller than 41 (resp. 19, resp. 7) for $g = 2$ (resp. 3, resp. 4). Then the full cost depends also on the cardinality of $\mathscr{W}_1$ which can be computed by [HK89b] for $g = 2$ and 3. When $R = \mathrm{End}(E)$ is maximal, a lower bound for this cardinality grows linearly in $(\mathrm{disc}(R))^{g^2/4}$ for fixed g.

The restrictions above artificially increase the smallest ℓ we would like to consider. We therefore urge the reader to consider Algorithm 1 as a proof of concept, allowing computations which were completely out of reach before for various classes $\mathscr{W}_1$ in dimension $2, 3$ and 4 with R maximal or not (see Section 5).

We finally move to one last new algorithmic result. In Section 4.3, we show how to evaluate a Siegel modular form χ of level $\mathrm{Sp}_{2g}(\mathbb{Z})$ and even weight[1] at a principally polarized abelian variety $(A, \mathscr{L})/\mathbb{F}_q$ when χ is defined as a homogeneous polynomial P in the theta constants with coefficients in $\mathbb{F}_q$. A Siegel modular form is a section of a power of the Hodge bundle on the universal abelian variety, so to give it a value only makes sense once a $\mathbb{F}_q$-rational basis of regular differentials on A is fixed. We show that choosing such a basis yields a particular affine lift of the theta null point on $(A, \mathscr{L})$ which we call a *modular lift* (see Definition 4.3). The coordinates of a modular lift are characterized, up to a common sign, by considering all products of two theta coordinates as Siegel modular forms of weight 1. Evaluating χ is then computing

[1] when g is odd, all of them have even weight.

the value of P in the coordinates of the modular lift. We show that a certain affine version of the isogeny formula preserves the modular lift property (see Theorem 4.5). Since in our Thomae's formula for elliptic curves we took care of having such a modular lift, we can therefore carry it to $(A, \mathscr{L})$ through the isogeny (see Algorithm 7) and perform the computation of the modular form on $(A, \mathscr{L})$.

As an application and in order to illustrate our algorithms, we consider curves over $\mathbb{F}_q$ with many points. A curve C of genus $g \geq 1$ over $\mathbb{F}_q$ has at most $1 + q + g\lfloor 2\sqrt{q} \rfloor$ and when this bound is reached, we say that C is a *defect*-0 *curve*. The best upper bounds are known only for $g \leq 2$ and sparse families of g, q. If C is a defect-0 curve, then its Jacobian $\operatorname{Jac} C$ is isogenous to E^g where E has trace $-\lfloor 2\sqrt{q} \rfloor$. If E is ordinary (which is always the case for instance when $q = p^m$ with $m = 1$ or 3 and $q \neq 2, 3$ [Ser85, p. II.6.4]), we can try to find $\operatorname{Jac} C$ among the indecomposable principally polarized abelian varieties $(A, \mathscr{L})$ in the isogeny class of E^g.

When $g = 2$, each such $(A, \mathscr{L})$ is automatically the Jacobian of a defect-0 curve. It is therefore enough to know that an indecomposable principally polarized abelian surface isogenous to E^2 exists which can already be obtained on the lattice side of the picture using [Hof91] and [Ser85, Th.3.9.1]. Now, if one wants an equation of the curve, it can be provided using Algorithm 1.

When $g = 3$, although each $(A, \mathscr{L})$ is geometrically the Jacobian of a unique curve $C/\mathbb{F}_q$, there may be an obstruction, called *Serre's obstruction*, for C to have defect-0. Fortunately, the modular form χ_{18} which is a Siegel modular form of weight 18 defined as the product of the 36 even theta constants determines this obstruction as we shall recall in Section 5. Since we can compute algebraically the values of χ_{18} at all $(A, \mathscr{L})$ in the isogeny class of E^3, we can compute the obstruction for each of them and check if a defect-0 genus-3 curve exists over $\mathbb{F}_q$. This gives the first *provable* computation of this obstruction as, so far, one had only a heuristic method using lifting and approximations over $\mathbb{C}$ [Rit10].

We conclude with an example in genus 4. We first show that Igusa modular form cuts the locus of Jacobians and decomposable principally polarized abelian varieties over any algebraically closed field of characteristic different 2 (see Theorem 5.8). We then use this to show that a certain class of isogeny does not contain Jacobians (see Example 5.9).

The code and examples of our algorithms are available at [KNR+20]. In the future, we hope to improve the overall speed of the algorithm (for instance by working with A_0 products of distinct elliptic curves E_i instead of E^g) and waive the technical limitations above. Notice that the method presented here may be adapted to other cases: one could replace E ordinary with E supersingular over $\mathbb{F}_p$ or over $\mathbb{F}_{p^2}$ with trace $\pm 2p$; one could also replace E by a principally polarized abelian variety B for which a thetanull point is known (with some restrictions, see [AK18] and [JKP+18, Sec.8]).

Acknowledgements. We would like to thank Andrew Sutherland who kindly provided us a fast `Magma` code to check when an ordinary elliptic curve has minimal endomorphism ring and Jeroen Sijsling for helping us using his `Magma` packages. We also thank Valentijn Karemaker and Stefano Marseglia for discussions about the references in the introduction.

2. Hermitian lattices

2.1. **Basic definitions and notations.** Let $F = \mathbb{Q}(\sqrt{d})$, where $d < 0$ is a squarefree negative integer. The discriminant d_F of F equals d if $d \equiv 1 \pmod 4$ and $4d$ otherwise. The non-trivial Galois involution of $F/\mathbb{Q}$ will be denoted by $\bar{\cdot}$. Further, let

$$\mathrm{Nr}\colon F \to \mathbb{Q},\ x \mapsto x\overline{x} \quad \text{and} \quad \mathrm{Tr}\colon F \to \mathbb{Q},\ x \mapsto x + \overline{x}$$

be the usual norm and trace of $F/\mathbb{Q}$.

Definition 2.1. A *hermitian space* (V, h) over F is a finite dimensional vector space V over F equipped with a sesqui-linear map $h\colon V \times V \to F$ such that

(1) $h(\alpha v + \beta v', w) = \alpha h(v, w) + \beta h(v', w)$ for all $\alpha, \beta \in F$ and all $v, v', w \in V$.
(2) $h(v, w) = \overline{h(w, v)}$ for all $v, w \in V$.

The *rank* of a hermitian space (V, h) is the dimension of V over F. For a tuple $b = (b_1, \dots, b_r) \in V^r$ we define its *Gram matrix* by

$$\mathrm{Gram}(b) = (h(b_i, b_j)) \in F^{r\times r} .$$

Every hermitian space (V, h) in this paper is assumed to be *non-degenerate*, i.e. if $v \in V$ with $h(v, w) = 0$ for all $w \in V$ then $v = 0$. This is equivalent to say that the *Gram matrix* of any basis b of V is invertible.

Definition 2.2. Let b be a basis of a hermitian space (V, h). Then

$$\det(V, h) := \det(\mathrm{Gram}(b))$$

is called the *determinant* of (V, h). It is well defined when viewed as an element of $\mathbb{Q}^*/\mathrm{Nr}(F^*)$.

Definition 2.3. Two hermitian spaces (V, h) and (V', h') over F are called *isometric* if there is an isomorphism $\varphi\colon V \to V'$ such that $h'(\varphi(v), \varphi(w)) = h(v, w)$ for all $v, w \in V$. The map φ is then called an *isometry* between (V, h) and (V', h'). Moreover,

$$\mathrm{U}(V, h) = \{\varphi\colon V \to V \mid \varphi \text{ is an isometry}\} \quad \text{and} \quad \mathrm{SU}(V, h) = \{\varphi \in \mathrm{U}(V, h) \mid \det(\varphi) = 1\} .$$

are the *unitary* and *special unitary groups* of (V, h) respectively.

Let $\mathscr{P}$ denote the set of prime numbers. For $p \in \mathscr{P} \cup \{\infty\}$ let $F_p := \mathbb{Q}_p \otimes_{\mathbb{Q}} F$ be the completion of F at p. Let (V, h) be a hermitian space over F. The map h extends to $V_p := F_p \otimes_F V$ by linearity. This yields a hermitian space (V_p, h) over F_p. If $p = \infty$, then $\mathbb{Q}_\infty = \mathbb{R}$ and (V_∞, h) is a hermitian space over $F_\infty = \mathbb{C}$. The signature of this complex hermitian space is called the signature of (V, h).

The following local-global principle is well known.

Theorem 2.4 (Landherr)**.** *Two hermitian spaces over F are isometric if and only if they are isometric over every place of $\mathbb{Q}$.*

Hermitian spaces over $\mathbb{C}$ are parameterized by their signatures while hermitian spaces over $\mathbb{Q}_p$ are parameterized by their ranks and determinants (viewed as elements of $\mathbb{Q}_p^*/\mathrm{Nr}(F_p^*)$). We will only deal with positive definite spaces, i.e. spaces with $h(v, v) > 0$ for all non-zero $v \in V$. For these spaces, we can make Landherr's theorem more explicit.

Remark 2.5. Let g be a positive integer and let $\mathscr{P}_{\mathrm{ns}}$ be the set of primes which do not split in F.

(1) Let (V, h) be a positive definite hermitian space of rank g. Since $\mathbb{Q}_p^*/\mathrm{Nr}(F_p^*)$ has at most two elements, the isometry type of (V, h) is uniquely determined by

$$I := \{p \in \mathscr{P} \mid \det(V, h) \notin \mathrm{Nr}(F_p^*)\} \subseteq \mathscr{P}_{\mathrm{ns}} .$$

The product formula for Hasse's norm residue symbols shows that I is a finite set of even cardinality.

(2) Let $I \subseteq \mathscr{P}_{\mathrm{ns}}$ be a finite subset of even cardinality. There exists a positive definite hermitian space (V, h) of rank g such that

$$I = \{p \in \mathscr{P} \mid \det(V, h) \notin \mathrm{Nr}(F_p^*)\} .$$

Moreover, this space admits the Gram matrix

$$\mathrm{diag}(1, \dots, 1, a)$$

with some positive integer a whose prime divisor are in $I \cup \{q\}$ for some prime q. This gives a method to construct a positive definite hermitian space of rank g with given determinant, see [Kir16, Section 3.4] for details.

For the remainder of this section, let (V, h) be a hermitian space over F of rank g. Further let R be an *order* in F, that is a subring of F which is a free $\mathbb{Z}$-module of rank 2. The ring of integers $\mathscr{O}$ of F is an order and it contains every other order R of F. Thus the index $f := [\mathscr{O} : R]$ is finite and it is called the *conductor* of R in F. Note that R is the unique quadratic order of discriminant $f^2 d_F$. Moreover,

$$\mathscr{O} = \mathbb{Z}[\omega] \quad \text{and} \quad R = \mathbb{Z}[f\omega] \quad \text{where } \omega = \frac{d_F + \sqrt{d_F}}{2} .$$

A *fractional R-ideal* $\mathfrak{a}$ is an R-submodule of F which has rank 2 over $\mathbb{Z}$. It is said to be an *invertible* R-ideal if there exists a fractional R-ideal $\mathfrak{b}$ such that $\mathfrak{a}\mathfrak{b} = R$. Given two fractional R-ideals $\mathfrak{a}, \mathfrak{b}$ we can define the

fractional R-ideal $(\mathfrak{a} : \mathfrak{b}) = \{x \in F, x\mathfrak{b} \subseteq \mathfrak{a}\}$ called the *colon-quotient* of $\mathfrak{a}$ and $\mathfrak{b}$. The particular case $(\mathfrak{a} : \mathfrak{a})$ is called the *multiplicator ring* of $\mathfrak{a}$. It is the unique order in F for which $\mathfrak{a}$ is invertible.

Definition 2.6. An *R-lattice* of rank r is a finitely generated R-submodule of V such that $FL := L \otimes_R F$ has dimension r. If $r = g$ we call L a *full* R-lattice in V.

The following result is due to Borevich and Faddeev [BF60].

Proposition 2.7. *Let L be a full R-lattice in V. Then there exist a basis $(x_1, \ldots, x_g)$ of V, some fractional ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_g$ of R and a chain of orders $R \subseteq R_1 \subseteq \cdots \subseteq R_g$ such that $\mathfrak{a}_i$ is an invertible R_i-ideal and*

$$L = \mathfrak{a}_1 x_1 \oplus \cdots \oplus \mathfrak{a}_g x_g \, .$$

The list of pairs $(\mathfrak{a}_i, x_i)_{i=1,\ldots,g}$ is called a pseudo-basis *of L.*

In the implementation of our algorithms we represent an R-lattice either via a pseudo basis or a $\mathbb{Z}$-basis and we use the results of [BF60] to switch between these two types of representations.

Definition 2.8. Let L be an R-lattice in V.

(1) The *dual lattice* of L is
$$L^{\#} = \{x \in V \mid h(x, L) \subseteq R\} \, .$$
(2) The lattice L is called *integral* if $L \subseteq L^{\#}$ and *unimodular* if $L = L^{\#}$.
(3) An integral R-lattice L is called even, if $h(x, x) \in 2\mathbb{Z}$ for all $x \in L$; otherwise it is called odd.
(4) The lattice L is called *decomposable* if there exists two non-trivial R-submodules L_1, L_2 of L such that $L = L_1 \oplus L_2$ and $h(x_1, x_2) = 0$ for all $x_i \in L_i$. If this is the case, we write $L = L_1 \perp L_2$.
(5) If L is a free R-lattice with basis b, then $\det(L) := \det(\mathrm{Gram}(b))$ is the *determinant* of L. It is a well defined element in $\mathbb{Q}^* / \mathrm{Nr}(R^*)$.
(6) Given $a_1, \ldots, a_g \in \mathbb{Q}^*$, we denote by
$$\langle a_1, \ldots, a_g \rangle$$
the free hermitian R-lattice (L', h') of rank g having an orthogonal basis $(b_1, \ldots, b_g)$ such that $h'(b_i, b_i) = a_i$ for all $1 \leq i \leq g$.

Let L be an R-lattice with pseudo-basis $(\mathfrak{a}_i, x_i)$. Denote by $(x_i^{\#})$ the dual basis (x_i), i.e. the basis of V such that $h(x_i, x_i^{\#}) = \delta_{i,j}$ for all $1 \leq i, j \leq g$. Then

$$L^{\#} = \bigoplus_{i=1}^{g} \overline{(R : \mathfrak{a}_i)} x_i^{\#} \, .$$

From this fact and the relation $(R : (R : \mathfrak{a})) = \mathfrak{a}$ it is easy to see that $(L^{\#})^{\#} = L$.

Lemma 2.9. *Let L be an R-lattice in (V, h) and let $L_1, \ldots, L_n$ be $\mathbb{Z}$-submodules of L. For $a \in F$ let*

$$f_a \colon V \times V \to \mathbb{Q}, \ (x, y) \mapsto \mathrm{Tr}(ah(x, y)) \, .$$

The following are equivalent:

(1) *$L = L_1 \perp \ldots \perp L_n$ is an orthogonal decomposition into R-lattices.*
(2) *$L = \bigoplus_i L_i$ and $f_1(L_i, L_j) = f_{\sqrt{d}}(L_i, L_j) = \{0\}$ for all $i \neq j$.*

Proof. We only need to prove that (2) implies (1). Let $x \in L_i$ and $y \in \bigoplus_{j \neq i} L_j$. Then $f_1(x, y) = f_{\sqrt{d}}(x, y) = 0$ and thus $\mathrm{Tr}(ah(x, y)) = 0$ for all $a \in F$. Since $F/\mathbb{Q}$ is separable, it follows that $h(x, y) = 0$. Let $r \in R$. Then $h(rx, y) = 0$ and thus $f_a(rx, y) = 0$ for all $a \in F$. Hence $rx \in \mathbb{Q}L_i \cap L = L_i$. So L_i is indeed an R-module. □

If (V, h) is positive definite, then so is the rational bilinear map f_1 from above. In this case, a well known result of Kneser shows that there exists a unique decomposition of L as in Lemma 2.9 (2) into minimal $\mathbb{Z}$-submodules. It can be computed as in [HV98, Algorithm 4.5]. Hence the previous lemma shows that any positive definite hermitian R-lattice L has a unique decomposition into indecomposable sublattices and it yields a method to compute these sublattices.

For a prime $p \in \mathscr{P}$ let $R_p := \mathbb{Z}_p \otimes_{\mathbb{Z}} R$ and $L_p := R_p \otimes_R L$ be the completions of R and L at p. Then L_p is an R_p-lattice in (V_p, h). The introduced notion for R-lattices carries over to R_p-lattices. For example we call an R_2-lattice L even, if $h(x, x) \in 2\mathbb{Z}_2$ for all $x \in L$.

2.2. **Enumeration of positive definite unimodular hermitian lattices.** Let $R = \mathbb{Z}[\omega f]$ be the order of conductor f in F. In this section, we present an algorithm to enumerate all positive definite unimodular R-lattices of a given rank.

Definition 2.10. Let L and L' be full R-lattices in the hermitian spaces (V, h) and (V', h'). The lattices L and L' are said to be isometric, if there exists an isometry φ from (V, h) to (V', h') such that $\varphi(L) = L'$. In this case, we write $L \cong L'$. Further let

$$\mathrm{cls}(L) = \{\varphi(L) \mid \varphi \in \mathrm{U}(V, h)\} \quad \text{and} \quad \mathrm{Aut}(L) = \{\varphi \in \mathrm{U}(V, h) \mid \varphi(L) = L\}$$

be the *isometry class* and the *automorphism group* of L. Similarly one defines isometries between the completions L_p and L'_p at a prime p. The *genus* of L is

$$\mathrm{gen}(L) := \{L' \subset V \mid L' \text{ is an } R\text{-lattice such that } L_p \cong L'_p \text{ for all } p \in \mathscr{P}\}\,.$$

When R is the maximal order, the following remark shows how to find a lattice in a given genus.

Remark 2.11. Every $\mathscr{O}_p$-lattice L_p admits an orthogonal decomposition

$$L_p = L_1 \perp \ldots \perp L_r \quad \text{such that } p^{s_i} L_i^{\#} = L_i$$

for some integers $s_1 < \ldots < s_r$. Jacobowitz [Jac62] shows that $(s_1, \ldots, s_r)$ together with the ranks and determinants of the lattices L_i uniquely describe the isometry class of L_p unless $p = 2$ and $F_2/\mathbb{Q}_2$ is ramified. For the remaining case, he shows that some additional invariants are needed.
Let G be a genus of hermitian $\mathscr{O}$-lattices. Suppose that for each prime p, we are given the p-adic local invariants of the lattices in G. Then we can construct an $\mathscr{O}$-lattice in G as follows.

(1) Since the local invariants yield the determinant of L_p, we can construct a hermitian space (V, h) over F that contains this genus using Remark 2.5.
(2) Fix any $\mathscr{O}$-lattice L in V. Then the set of all primes p where L_p has the wrong invariants is finite.
(3) If L_p has the wrong invariants, let X be any $\mathscr{O}$-lattice in some hermitian space (V', h') over F such that X_p has the correct invariants. Approximate an isometry between (V'_p, h') and (V_p, h) by some F-linear map $\varphi\colon V' \to V$. If the approximation is good enough, then $\varphi(X)_p$ has the same invariants as X_p. Then there exists $a, b \in \mathbb{Z}$ such that

$$p^a L_p \subseteq \varphi(X)_p \subseteq p^b L_p\,.$$

Now the lattice $(\varphi(X) + p^a L) \cap p^b L$ coincides with L at all places different from p and it has the correct invariants at p. So if we iterate this step, we end up with an $\mathscr{O}$-lattice in G.

A different approach is suggested in [Kir16, Section 3.5].

Let L be an R-lattice in a positive definite hermitian space over F. The analogue of Landherr's theorem does not hold for hermitian R-lattices, i.e. the genus of L does not necessarily consist of a single isometry class. However, the genus of L is a disjoint union of finitely many isometry classes

$$\mathrm{gen}(L) = \biguplus_{i=1}^{h(L)} \mathrm{cls}(L_i)\,. \tag{1}$$

The number of classes $h(L)$ is called the *class number* of (the genus of) L. There are only very few partial results like [HK89a; HK89b] on how to deduce the class number from local invariants and these only deal with $\mathscr{O}$-lattices.

Thus an important problem is to work out the class number $h(L)$ or more generally to make the decomposition in Equation (1) explicit. This can be done by Kneser's neighbour method. It is explained in great detail in [Sch98] for $\mathscr{O}$-lattices. Note that this is all we need, since we will reduce the case that R is non-maximal to this special case in Algorithm 2.

The basic idea of Kneser's method the following: Let $\mathfrak{p}$ be a prime ideal of $\mathscr{O}$ over $p > 2$ such that L_p is unimodular. An $\mathscr{O}$-lattice L' in V is called a $\mathfrak{p}$-neighbour of L if $L/(L \cap L') \cong \mathscr{O}/\mathfrak{p}$ and $L'/(L \cap L') \cong \mathscr{O}/\overline{\mathfrak{p}}$. Any $\mathfrak{p}$-neighbour of L lies in $\mathrm{gen}(L)$ and the $\mathfrak{p}$-neighbours of L can be enumerated quickly. Strong approximation yields a finite set S of unramified prime ideals of $\mathscr{O}$ such that given $L' \in \mathrm{gen}(L)$, there exists a sequence of $\mathscr{O}$-lattices $L = L_0, L_1, \ldots, L_r \cong L'$ such that L_i is a $\mathfrak{p}_i$-neighbour of L_{i-1} for some $\mathfrak{p}_i \in S$. In fact, Shimura [Shi64, Theorem 5.24 and its proof 5.28] shows how to choose such a set S. Note that if g is even, his

description makes use of the groups $\{\det(g) \mid g \in \mathrm{Aut}(L_p)\}$ at primes p that ramify in F. These groups have recently been worked out in [Kir19]. So the isometry classes in $\mathrm{gen}(L)$ are found by repeatedly computing $\mathfrak{p}$-neighbours for some $\mathfrak{p} \in S$.

Note that this procedure can be sped up considerably by using Siegel's mass formula as a stopping condition: Since isometric lattices have isomorphic automorphism groups, the *mass* of L

$$\mathrm{Mass}(L) := \mathrm{Mass}(\mathrm{gen}(L)) = \sum_{i=1}^{h(L)} \frac{1}{\#\,\mathrm{Aut}(L_i)}$$

is a well-defined positive rational number, which only depends on the genus of L. It can be computed a priori using Siegel's mass formula, which expresses $\mathrm{Mass}(L)$ in terms of special values of L-series and local factors that depend on the genus of L. The local factors have been worked out by Gan and Yu [GY00] for all primes p, except if $p = 2$ ramifies in F. In this exceptional case the local factors can be worked out as explained in [Kir16, Sections 4.3 and 4.5].

So if $R = \mathscr{O}$ is maximal, we can construct lattices in a given genus and enumerate the isometry classes in this genus. We will now extend these methods to enumerate the isometry classes of positive definite unimodular R-lattices. Note that these lattices might lie in non-isometric hermitian spaces.

Lemma 2.12. *Let L be a unimodular hermitian R-lattice. Then $M := \mathscr{O}L$ is an integral $\mathscr{O}$-lattice and*

$$fM^{\#,\mathscr{O}} \subseteq L \subseteq M\,.$$

Proof. The fact that M is integral and the inclusion $L \subseteq M$ are clear. Suppose now $z \in fM^{\#,\mathscr{O}}$. Hence $h(z/f, M) \subseteq \mathscr{O}$. This implies $h(z, L) \subseteq f\mathscr{O} \subseteq R$. So $z \in L^{\#,R} = L$. □

Algorithm 2 Enumeration of unimodular positive definite hermitian R-lattices of rank g.

Input: An order R of conductor f in an imaginary quadratic number field F and an integer $g \geq 1$.
Output: A set $\mathscr{L}$ of R-lattices representing the isometry classes of positive definite, unimodular hermitian R-lattices of rank g.

$\mathscr{L} \leftarrow \emptyset$.
Let $p_1, \ldots, p_s$ be the prime divisors of fd_F that do not split in F.
for all subsets $I \subseteq \{p_1, \ldots, p_s\}$ of even cardinality **do**
    Using Remark 2.5 construct some positive definite hermitian form $h\colon F^g \times F^g \to F$ such that
$$\{p \in \mathscr{P} \mid \det(F^g, h) \notin \mathrm{Nr}(F_p^*)\} = I\,.$$
    Using Remark 2.11 find $\mathscr{O}$-lattices $G_1, \ldots, G_r$ representing the genera of all integral $\mathscr{O}$-lattices M in (F^g, h) such that $fM^{\#,\mathscr{O}} \subseteq M$.
    for $1 \leq i \leq r$ **do**
        Let $M_1, \ldots, M_s$ represent the isometry classes of $\mathscr{O}$-lattices in $\mathrm{gen}(G_i)$ using Kneser's method.
        if $R = \mathscr{O}$ **then**
            $\mathscr{L} \leftarrow \mathscr{L} \cup \{M_1, \ldots, M_s\}$.
        else
            for $1 \leq j \leq s$ **do**
                Let $L_1, \ldots, L_t$ be orbit representatives of the action of $\mathrm{Aut}(M_j)$ on
$$\{L \subseteq M_j \mid L \text{ a unimodular } R\text{-lattice containing } fM_j^{\#,\mathscr{O}} \text{ with } \mathscr{O}L = M_j\}\,.$$
                $\mathscr{L} \leftarrow \mathscr{L} \cup \{L_1, \ldots, L_t\}$.
            end for
        end if
    end for
end for
return $\mathscr{L}$.

Proposition 2.13. *Algorithm 2 which takes as input an order R of conductor f in an imaginary quadratic field and an integer $g \geq 1$ outputs the list of R-lattices representing the isometry classes of positive definite, unimodular hermitian R-lattices of rank g.*

Proof. Let L be a unimodular, full R-lattice in a positive definite hermitian space (V, h') of rank g. We first show that the set $\mathscr{L}$ returned by the algorithm contains a lattice isometric to L. Let p be a prime not dividing fd_F. Then L_p is a unimodular $\mathscr{O}_p$-lattice. If p splits in F, then $\det(V_p, h') \in \mathbb{Q}_p^* = \mathrm{Nr}(F_p^*)$. Suppose now p is non-split. By [Jac62, Proposition 4.4] L_p admits an orthogonal basis. Hence $\det(V_p, h')$ has a representative in $\mathbb{Z}_p^* \subseteq \mathrm{Nr}(F_p^*)$. So Landherr's theorem implies that (V, h') is isometric to one of the spaces (F^g, h) the algorithm considers. After replacing L by an isometric copy, we may therefore assume that $M := \mathscr{O}L$ is one of the lattices M_j in line 7. Proposition 2.12 shows $fM_j^{\#,\mathscr{O}} \subseteq L \subseteq M_j$. Thus $\mathscr{L}$ contains an R-lattice isometric to L.
Next we show that $\mathscr{L}$ does not represent any isometry class twice. Suppose $L_1, L_2 \in \mathscr{L}$ are isometric. This isometry extends to an isometry between $\mathscr{O}L_1$ and $\mathscr{O}L_2$. By construction, this implies $\mathscr{O}L_1 = \mathscr{O}L_2$. Hence L_1 and L_2 are in the same orbit under $\mathrm{Aut}(\mathscr{O}L_1)$. This shows $L_1 = L_2$. □

If we restrict ourselfs to projective unimodular R-lattices, we can speed up Algorithm 2 considerably. To this end, let L be a full, projective R-lattice in a positive definite hermitian space (V, h) over F and set $M = \mathscr{O}L$. The R-lattice L has a pseudo-basis

$$L = \bigoplus_{i=1}^{g} \mathfrak{a}_i x_i$$

with invertible fractional ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_g$ of R since L is a projective R-module. Let $(x_1^\#, \ldots, x_g^\#)$ denote the dual basis of $(x_1, \ldots, x_g)$. Then

$$M = \bigoplus_{i=1}^{g} \mathscr{O}\mathfrak{a}_i x_i, \quad L^{\#,R} = \bigoplus_{i=1}^{g} \overline{(R : \mathfrak{a}_i)} x_i^\# \quad \text{and} \quad M^{\#,\mathscr{O}} = \bigoplus_{i=1}^{g} \overline{(\mathscr{O} : \mathscr{O}\mathfrak{a}_i)} x_i^\# = \mathscr{O}L^{\#,R}\,.$$

Since $(R : \mathfrak{a}_i)$ is an invertible R-ideal, we see that $L^{\#,R}$ is projective as well.

Proposition 2.14. *Let L be a full, projective R-lattice in a hermitian space (V, h) and let $M = \mathscr{O}L$. Let Φ be the bilinear map defined by*

$$\Phi\colon M/fM \times M/fM \to \mathscr{O}/R \cong \mathbb{Z}/f\mathbb{Z},\ (x, y) \mapsto h(x, y) + R\,. \tag{2}$$

Then the following hold.

1. *If L is a unimodular R-lattice, then M is a unimodular $\mathscr{O}$-lattice.*
2. *If M is a unimodular $\mathscr{O}$-lattice, then the following are equivalent:*
   (a) *L is a unimodular R-lattice.*
   (b) *L is an integral R-lattice.*
   (c) *L/fM is an isotropic subspace of $(M/fM, \Phi)$, i.e. $\Phi(x, y) = 0$ for all $x, y \in L/fM$.*

Proof. (1) The discussion before the proposition shows that $L = L^{\#,R}$ implies $M = M^{\#,\mathscr{O}}$. (2b) $\implies$ (2a): We have $L \subseteq L^{\#,R}$ by assumption. Equality follows from the fact that the projective R-modules L and $L^{\#,R}$ both have index f^g in $M = M^{\#,\mathscr{O}} = \mathscr{O}L^{\#,R}$. The implications (2a) $\implies$ (2b) $\iff$ (2c) are clear. □

Algorithm 3 Enumeration of projective unimodular R-lattices of rank g.

Input: An integer $g \geq 2$ and an order R in F.

Output: A set of representatives of the isometry classes of projective, positive definite, unimodular hermitian R-lattices of rank g.

1: Fix a chain of minimal overorders $R = \mathscr{O}^{(0)} \subsetneq \mathscr{O}^{(1)} \subsetneq \ldots \subsetneq \mathscr{O}^{(r)} = \mathscr{O}$.
2: Using Algorithm 2 compute a set $\mathscr{S}$ of representatives of isometry classes of unimodular hermitian $\mathscr{O}$-lattices of rank g.
3: **for** $i = r, \ldots, 1$ **do**
4: Let p be the index of $\mathscr{O}^{(i-1)}$ in $\mathscr{O}^{(i)}$.
5: $\mathscr{T} \leftarrow \emptyset$.
6: **for** $M \in \mathscr{S}$ **do**
7: Let $\mathscr{V}$ represent the orbits of all g-dimensional isotropic subspaces of $(M/pM, \Phi)$ under the action of $\mathrm{Aut}(M)$ where Φ is chosen as in Equation (2).
8: **for** $V \in \mathscr{V}$ **do**
9: Let L be the full preimage of V under the canonical epimorphism $M \to M/pM$.
10: If L is an integral $\mathscr{O}^{(i-1)}$-lattice with $\mathscr{O}^{(i)}L = M$ then include L to the set $\mathscr{T}$.
11: **end for**
12: **end for**
13: $\mathscr{S} \leftarrow \mathscr{T}$.
14: **end for**
15: **return** $\mathscr{S}$.

Proposition 2.15. *Algorithm 3 which takes as input an order R in an imaginary quadratic field and an integer $g \geq 2$ outputs the list of R-lattices representing the isometry classes of positive definite, unimodular, projective hermitian R-lattices of rank g.*

Proof. After line 2, $\mathscr{S}$ is a set of representatives of the isometry classes of projective, unimodular hermitian $\mathscr{O}^{(r)}$-lattices. Let L be a projective unimodular hermitian $\mathscr{O}^{(r-1)}$-lattice. Then $M := \mathscr{O}^{(r)}L$ is a projective unimodular hermitian $\mathscr{O}^{(r)}$-lattice. So without loss of generality $M \in \mathscr{S}$. Thus Proposition 2.14 shows that the set $\mathscr{T}$ in line 13 contains an $\mathscr{O}^{(r-1)}$-lattice isometric to L. Suppose it contains two such lattices L_1 and L_2. Then there is an isometry $\sigma\colon L_1 \to L_2$ which induces an isometry $\mathscr{O}^{(r)}L_1 \to \mathscr{O}^{(r)}L_2$. But then $\mathscr{O}^{(r)}L_1 = M = \mathscr{O}^{(r)}L_2$ and $\sigma \in \mathrm{Aut}(M)$. Hence L_1 and L_2 are in the same $\mathrm{Aut}(M)$-orbit. This shows that $L_1 = L_2$. Hence after line 13, $\mathscr{S}$ is a set of representatives of the isometry classes of projective, unimodular hermitian $\mathscr{O}^{(r-1)}$-lattices. By induction it follows that after r iterations, $\mathscr{S}$ represents the isometry classes of projective, unimodular hermitian R-lattices. □

Note that Algorithm 3 calls Algorithm 2. But if $R = \mathscr{O}$ is maximal, the expensive steps 11–14 of Algorithm 2 are skipped. They are replaced by a much more refined descent in lines 3–13 of Algorithm 3, which is based on Proposition 2.14.

Also note that in Algorithm 3 it would be possible to go from $\mathscr{O}$-lattices to R-lattices directly. But then it would be much more difficult to find the desired (projective) R-lattices between fM and M.

2.3. **Orthogonal families inside a lattice.** Let (V, h) be a positive definite hermitian space over F of rank g. Let R be the order in F of conductor f.

In this section, we give necessary and sufficient conditions for a unimodular hermitian R-lattice to contain a free R-sublattice isometric to $\langle \ell, \ldots, \ell \rangle$ for some $\ell \in \mathbb{N}$, which we may require to be odd. Such a free sublattice will be needed in Section 3.3, where we provide an algorithm for finding a good isogeny from our target principally polarized abelian variety to a totally decomposable one. But we also think that this problem arises naturally and should deserve more investigations around the smallest values of ℓ that can be obtained.

We will prove the following result.

Theorem 2.16. *Let L be a full R-lattice in (V, h). Then the following hold:*

(1) *There exists an orthogonal basis $(b_1, \ldots, b_g) \in L^g$ of V.*

(2) *There exists an integer ℓ and a free R-sublattice L' of L such that $L' \cong \langle \ell, \dots, \ell \rangle$ if and only if g is odd or* $\det(V,h) \in \mathrm{Nr}(F^*)$.
(3) *Let L be unimodular and let $a \in \mathbb{Z} \setminus \{0\}$. Suppose g is odd or* $\det(V,h) \in \mathrm{Nr}(F^*)$. *There exists some positive integer ℓ coprime to a and a free R-sublattice L' of L such that $L' \cong \langle \ell, \dots, \ell \rangle$ if and only if the following conditions hold.*
   (a) *For all primes $p \mid a$ the module L_p is free over R_p.*
   (b) *If a is even then there exists some $\ell_2 \in \mathbb{Z}_2^*$ such that $L_2 \cong \langle \ell_2, \dots, \ell_2 \rangle$.*
   (c) *If g is even, then* $\det(L_p, h) \in \mathrm{Nr}(R_p^*)$ *for all odd primes p such that $p \mid \gcd(a, f)$.*

Remark 2.23 below shows how to check the conditions (a)–(c) in part 3 of Theorem 2.16. Let L be an R-lattice L in V. Then we can find an orthogonal basis of V in L as follows. For any positive rational number ℓ the map

$$q_\ell \colon V \to \mathbb{Q},\ v \mapsto \mathrm{Tr}(h(v,v)/\ell)$$

is a positive definite quadratic form on the $\mathbb{Q}$-space V and

$$\{v \in L \mid h(v,v) = \ell\} \subseteq \{v \in L \mid q_\ell(v) = 2\}\,.$$

Note that the right hand side is finite and it can be enumerated using the Fincke-Pohst algorithm [FP85]. This allows us to compute the set of vectors in (L,h) of norm ℓ.

It is now clear how to find an orthogonal basis as in Theorem 2.16. For part (1), we use the usual Gram-Schmidt process. For parts (2) and (3), we apply Algorithm 4 to $\ell = 1, 2, 3, \dots$ until we find a suitable basis. As all our algorithms, its complexity is at least exponential in the rank g. We could not find in the literature any result about a possible upper bound on ℓ when it exists.

Algorithm 4 Computation of an orthogonal family of g vectors of norm ℓ

Input: A full R-lattice L in V and a rational number $\ell > 0$.
Output: An orthogonal basis of V consisting of vectors in L of norm ℓ if possible; otherwise $\emptyset$.

function BackTrack(F, S)
  if $\#F = g$ **then return** F **end if**
  if $\#F + \dim\langle S \rangle < g$ **then return** $\emptyset$ **end if**
  Pick some $v \in S$.
  if $h(v,f) = 0$ for all $f \in F$ **then**
    $T \leftarrow$ BackTrack($F \cup \{v\}$, $\{w \in S \mid h(v,w) = 0\}$)).
    if $T \neq \emptyset$ **then return** T **end if**
  end if
  return BackTrack(F, $S \setminus \{v\}$).
end function
if $\ell^g \cdot \det(V,h) \notin \mathrm{Nr}(F^*)$ **then return** $\emptyset$ **end if**
$S \leftarrow \{v \in L \mid h(v,v) = \ell\}$.
return BackTrack($\emptyset$, S).

The remainder of this section gives a proof of Theorem 2.16. We start by giving a classification of all free unimodular hermitian R_p-lattices which admit an orthogonal basis. If R_p is maximal, this follows from Jacobowitz classification of local hermitian lattices [Jac62].

Proposition 2.17. *Let L be a free, unimodular hermitian R_p-lattice of rank g. Then*

$$L = L_1 \perp \dots \perp L_r$$

for some free unimodular hermitian R_p-sublattices L_i of rank at most 2. If one of p, g or L is odd, then all L_i can be chosen to have rank 1.

Proof. Let $(b_1, \dots, b_g)$ be a basis of L. Suppose first that $h(b_i, b_i) \in \mathbb{Z}_p^*$ for some i. Then $L = R_p b_i \perp \sum_{j \neq i} R_p(b_j - \frac{h(b_j,b_i)}{h(b_i,b_i)} b_i)$. Suppose now that such an index i does not exist. Since L is free and unimodular, there exist $1 \leq i < j \leq g$ such that $h(b_i, b_j) \in R_p^*$. If $p \neq 2$, we can replace b_i with $b_i' := b_i + 1/(2h(b_j, b_i))b_j$.

Then $h(b_i', b_i') \in \mathbb{Z}_p^*$ and we obtain a splitting $L = Rb_i' \perp L'$ as before. If $p = 2$, we may assume that $h(b_i, b_j) = 1$. Then $L = (R_p b_i \oplus R_p b_j) \perp L'$ where

$$L' = \bigoplus_{k \neq i,j} R_p(b_k - \frac{h(b_j, b_j)h(b_k, b_i) - h(b_k, b_j)}{h(b_i, b_i)h(b_j, b_j) - 1} b_i - \frac{h(b_i, b_i)h(b_k, b_j) - h(b_k, b_i)}{h(b_i, b_i)h(b_j, b_j) - 1} b_j) \,.$$

So in any case, we obtain a decomposition $L = L_1 \perp L'$ with free, unimodular lattices L_1 and L' such that the rank of L_1 is at most 2. The first assertion now follows by induction on the rank g and we have also seen that we can choose all L_i of rank 1 when p is odd.
Suppose now $p = 2$ and also suppose that g or L is odd. If L is odd, we can choose the vector b_1 in our original basis such that $h(b_1, b_1) \in \mathbb{Z}_2^*$. If g is odd, then one of the L_i must have rank 1. So in both cases, there exists a summand $L_i = R_2 x_1$ of rank 1. Suppose $L_j = R_2 x_2 \oplus R_2 x_3$ is binary. If $h(x_2, x_2) \in \mathbb{Z}_2^*$ or $h(x_3, x_3) \in \mathbb{Z}_2^*$, we can split L_j just as before. So suppose $h(x_2, x_2), h(x_3, x_3) \in 2\mathbb{Z}_2$. Let $x_2' := x_2 + x_1$. Then as before $L_i \oplus L_j = (R_2 x_2' \oplus R_2 x_3) \perp R_2 x_1'$ for some $x_1' \in L_i \oplus L_j$. But now $h(x_2', x_2') \in \mathbb{Z}_2^*$ and thus $L_i \oplus L_j$ has an orthogonal basis. Iterating this argument shows that L has an orthogonal basis. □

Remark 2.18. Let L be a free unimodular hermitian R_p-lattice.

(1) If $p = 2$ and the rank of L is odd, then L is odd.
(2) L has an orthogonal basis if and only if $p > 2$ or L is odd.

The classification of all free unimodular hermitian R_p-lattices which have an orthogonal basis more or less boils down to a description of the norm group $\mathrm{Nr}(R_p^*)$. To this end, let

$$\mathbb{Z}_p^{*2} = \{u^2 \mid u \in \mathbb{Z}_p^*\} = \{\mathrm{Nr}(u) \mid u \in \mathbb{Z}_p^*\}$$

be group of squares in $\mathbb{Z}_p^*$.

Lemma 2.19. *If p is odd, then*

$$\mathrm{Nr}(R_p^*) = \begin{cases} \mathbb{Z}_p^* & \text{if } p \nmid f d_F, \\ \mathbb{Z}_p^{*2} & \text{if } p \mid f d_F \end{cases}$$

and

$$\mathrm{Nr}(R_2^*) = \begin{cases} \mathbb{Z}_2^* & \text{if } 2 \nmid d_F \text{ and } 4 \nmid f, \\ \mathbb{Z}_2^{*2} \uplus (1 - \frac{d_F}{4})\mathbb{Z}_2^{*2} & \text{if } 8 \mid d_F \text{ and } 2 \nmid f, \\ \mathbb{Z}_2^{*2} & \text{if } 2^5 \mid f^2 d_F, \\ \mathbb{Z}_2^{*2} \uplus 5\mathbb{Z}_2^{*2} & \text{otherwise.} \end{cases}$$

Proof. We have $\mathbb{Z}_p^{*2} \subseteq \mathrm{Nr}(R_p^*) \subseteq \mathbb{Z}_p^*$ and the structure of $\mathbb{Z}_p^*/\mathbb{Z}_p^{*2}$ is well known. In particular, the square classes can be distinguished modulo $4p$. Any unit $u \in R_p = \mathbb{Z}_p[f\omega]$ is of the form $u = x + yf\omega$ with $x, y \in \mathbb{Z}_p$ and

$$\mathrm{Nr}(u) = (x + yf\omega)\overline{(x + yf\omega)} = x^2 + xyfd_F + y^2 f^2 \frac{d_F^2 - d_F}{4} \in \mathbb{Z}_p^* \,.$$

The result now follows by a case by case discussion of the possible p-adic valuations of f and d_F. □

Corollary 2.20. *Let L be a free unimodular hermitian R_p-lattice of rank g. Let $u \in \mathbb{Z}_p^*$ be a representative of $\det(L) \in \mathbb{Z}_p^*/\mathrm{Nr}(R_p^*)$. If $p > 2$, then $L \cong \langle 1, \ldots, 1, u\rangle$.*

Proof. Let $\varepsilon \in \mathbb{Z}_p^*$ be a non-square. Proposition 2.17 shows that $L \cong \langle u_1, \ldots, u_g\rangle$ with $u_i \in \{1, \varepsilon\}$. It is well known that there exists some $U \in \mathrm{GL}_2(\mathbb{Z}_p)$ such that ${}^tU \,\mathrm{diag}(1,1)U = \mathrm{diag}(\varepsilon, \varepsilon)$. Hence $\langle 1, 1\rangle \cong \langle \varepsilon, \varepsilon\rangle$ and thus we can assume that $u_1 = \ldots = u_{g-1} = 1$. □

Proposition 2.21. *Let L be a free, odd, unimodular hermitian R_2-lattice of rank $g \geq 2$. Let $u \in \mathbb{Z}_2^*$ be a representative of $\det(L) \in \mathbb{Z}_2^*/\mathrm{Nr}(R_2^*)$.*

(1) *If R_2 is maximal or $3 \in \mathrm{Nr}(R_2^*)$ or $7 \in \mathrm{Nr}(R_2^*)$, then $L \cong \langle 1, \ldots, 1, u\rangle$.*
(2) *If $g > 2$ and the conditions in (1) are not satisfied then either*

$$L \cong \langle 1, \ldots, 1, u\rangle \quad \text{or} \quad L \cong \langle 1, \ldots, 1, 3, 3, u\rangle$$

but not both.

(3) *If $g = 2$ and the conditions in (1) are not satisfied then either $L \cong \langle 1, u\rangle$ or $u \equiv 1, 5 \pmod{\mathrm{Nr}(R_2^*)}$ and $L \cong \langle 3, 3u\rangle$.*

Proof. If R_2 is maximal, the result follows from [Jac62, Theorem 7.1 and Proposition 10.4]. Suppose now R_2 is not maximal. Proposition 2.17 shows that $L \cong \langle u_1, \dots, u_g\rangle$ with $u_i \in \mathbb{Z}_2^*$. If $3 \in \mathrm{Nr}(R_2^*)$ or $7 \in \mathrm{Nr}(R_2^*)$ we may assume that $u_i \in \{1, 5\}$ for all i. As in the proof of Corollary 2.20 we conclude that $u_1 = \cdots = u_{g-1} = 1$. The first assertion follows.
Suppose now $3, 7 \notin \mathrm{Nr}(R_2^*)$ and $g \geq 3$. [O'M63, Theorem 93:16] yields some $T \in \mathrm{GL}_g(\mathbb{Z}_2)$ and $e \in \{1, 3\}$ such that

$$^tT \operatorname{diag}(u_1, \dots, u_g)T = \operatorname{diag}(1, \dots, 1, e, e, \prod_i u_i) .$$

Hence $L \cong \langle 1, \dots, 1, e, e, u\rangle$. It remains to show that $M := \langle 1, \dots, 1, 1, 1, u\rangle$ and $N := \langle 1, \dots, 1, 3, 3, u\rangle$ are not isometric. Let V be the ambient hermitian space of M and N. Let X and Y be the $\mathbb{Z}_2$-lattices M and N equipped with the bilinear form $V \times V \to \mathbb{Q}_2, (x, y) \mapsto \mathrm{Tr}(h(x, y)/2)$. Lemma 2.19 shows that $R_2 = \mathbb{Z}_2 \oplus \alpha\mathbb{Z}_2$ for some $\alpha \in R_2$ with $\mathrm{Tr}(\alpha) = 0$ and $n := \mathrm{Nr}(\alpha) \in 4\mathbb{Z}_2$. Hence $X = X_0 \perp X_1$ where X_0 and X_1 are free with Gram matrices $\operatorname{diag}(1, \dots, 1, u)$ and $\operatorname{diag}(n, \dots, n, un)$. Similarly $Y = Y_0 \perp Y_1$ where Y_0 and Y_1 are free with Gram matrices $\operatorname{diag}(1, \dots, 1, 3, 3, u)$ and $\operatorname{diag}(n, \dots, n, 3n, 3n, un)$. Suppose M and N are isometric hermitian R_2-lattices. Then X and Y are isometric bilinear $\mathbb{Z}_2$-lattices. By [O'M63, Theorem 93:29 (ii)], this implies that X_0 is isometric to Y_0, which is impossible since the two ambient quadratic spaces have different Hasse-Witt invariants. The case $g = 2$ follows along the same lines. □

The above proof shows that the possible cases in part (2) and (3) of Proposition 2.21 can be distinguished as follows.

Remark 2.22. Let $L \cong \langle u_1, \dots, u_g\rangle$ where $u_i \in \mathbb{Z}_2^*$ and $g \geq 2$. Write $u = \prod_i u_i$. Suppose that R_2 is not maximal and that $3, 7 \notin \mathrm{Nr}(R_2^*)$. Then $L \cong \langle 1, \dots, 1, u\rangle$ if and only if $\prod_{i<j}(u_i, u_j)_2 = 1$ where $(\_, \_)_2$ denotes the Hilbert-Symbol of $\mathbb{Q}_2$.

We are now ready to prove the main result of this section.

Proof of Theorem 2.16. The first assertion is the Gram-Schmidt process. For the remainder let $\mu \in \mathbb{N}$ be a representative of $\det(V, h) \in \mathbb{Q}^*/\mathrm{Nr}(F^*)$. Let (V', h') be a hermitian space over F with Gram matrix $\mu \cdot I_g$. If g is odd or $\det(V, h) \in \mathrm{Nr}(F^*)$, then (V, h) and (V', h') have the same rank, the same determinant and the same signature. Hence they are isometric by Landherr's Theorem. Thus (V, h) contains a free R-lattice $M \cong \langle \mu, \dots, \mu\rangle$. Let $m \in \mathbb{N}$ such that $L' := mM \subseteq L$. Then $L' \cong \langle \ell, \dots, \ell\rangle$ where $\ell = m^2\mu$. Conversely, if such a lattice L' exists and g is even, then $\det(V, h) = \ell^g \in \mathrm{Nr}(F^*)$. This proves the second assertion.
Suppose now L has a sublattice L' as in (3). For any prime divisor p of a, we have

$$L'_p \subseteq L_p \subseteq L_p^{\#} \subseteq (L'_p)^{\#} = L'_p .$$

Hence $L_p = L'_p \cong \langle \ell, \dots, \ell\rangle$ and if g is even, then $\det(L_p, h) = \ell^g \in \mathrm{Nr}(R_p^*)$. Finally suppose that the three conditions of part (3) hold. If g is even and a is odd, set $r = 1$. If g and a are both even let $r \in \mathbb{N}$ such that $r/\ell_2 \in \mathrm{Nr}(R_2^*)$. If g is odd, we also choose some integer r, but much more carefully. For all $p \mid a$ the assumption that L_p is free and unimodular implies $\det(L_p, h) \in \mathbb{Z}_p^*$. Hence we may assume that the representative $\mu \in \mathbb{N}$ of $\det(V, h)$ from above is coprime to a. Dirichlet's theorem on primes in arithmetic progressions yields some prime r such that

$$\begin{aligned} r &\equiv \ell_2 \pmod{\mathrm{Nr}(R_2^*)} \text{ if } 2 \mid a, \\ r &\equiv \mu \pmod{\mathrm{Nr}(R_p^*)} \text{ for all } 2 \neq p \mid a, \\ r &\equiv \mu \pmod{\mathrm{Nr}(F_p^*)} \text{ for all } p \mid \mu d_F \text{ and } p \nmid a. \end{aligned}$$

Notice that if $2 \mid a$, then $\ell_2 \equiv \ell_2^g \equiv \mu \pmod{\mathrm{Nr}(F_2^*)}$ and for $p \nmid ra\mu d_F$ we have $r/\mu \in \mathbb{Z}_p^* \subseteq \mathrm{Nr}(F_p^*)$. Hence $r/\mu \in \mathrm{Nr}(F_p^*)$ for all primes $p \neq r$. The product formula for norm symbols and Hasse's norm theorem imply that $r/\mu \in \mathrm{Nr}(F^*)$.
So whether g is even or odd, we have $r^g/\mu \in \mathrm{Nr}(F^*)$. As in part (2) it follows that (V, h) has a Gram matrix $r \cdot I_g$. Thus (V, h) contains a full R-lattice $M \cong \langle r, \dots, r\rangle$. Corollary 2.20, condition (3c) and the choice of r show that for $p \mid a$ there exists some local isometry $\sigma_p \colon M_p \to L_p$. Since M has an orthogonal basis,

we may assume that $\det(\sigma_p) = 1$. Strong approximation yields some $\sigma \in \mathrm{SU}(V,h)$ such that $\sigma(M)_p = L_p$ for all $p \mid a$, cf. [Kne66]. Hence there exists an integer b coprime to a such that $b\sigma(M) \subseteq L$. Then $L' := b\sigma(M) \cong \langle \ell, \dots, \ell \rangle$ with $\ell = b^2 r$. This proves the third assertion. □

Remark 2.23. Let L be a unimodular R-lattice in (V,h) given by a pseudo basis $L = \bigoplus_{i=1}^{g} \mathfrak{a}_i x_i$. Then the conditions in part (3) of Theorem 2.16 can be checked as follows.

(1) The R_p-module L_p is free if and only $\mathfrak{a}_i R_p$ is principal for all i. Since R is Gorenstein, the latter condition holds if and only if the conductor of R and the conductors of the multiplicator rings of all $\mathfrak{a}_i$ have the same p-adic valuation. In particular, this holds if R_p is maximal.

(2) Let $p > 2$ be a prime such that $p \mid \gcd(a, f)$ and suppose L_p is free. For $1 \le i \le g$ pick some $a_i \in \mathfrak{a}_i$ such that $a_i R_p = \mathfrak{a}_i R_p$. Then $L_p = \bigoplus_i R_p b_i$ with $b_i = a_i x_i$ and thus $\det(L_p, h) = \det(\mathrm{Gram}(b))$. This can be used to check the condition (3c) as the norm group $\mathrm{Nr}(R_p^*)$ has been worked out in Lemma 2.19.

(3) Suppose $2 \mid a$, L_2 is free and g is odd. The existence of ℓ_2 is guaranteed whenever R_2 is maximal or $3 \in \mathrm{Nr}(R_2^*)$ or $7 \in \mathrm{Nr}(R_2^*)$ since in these cases all free unimodular R_2-lattices in (V_p, h) of determinant $\det(L_p, h)$ are isometric, cf. Proposition 2.21. So suppose we are not in this case. Since the square classes of $\mathbb{Z}_2^*$ are represented by $\{1,3,5,7\}$, there are at most 4 possibilities for ℓ_2. As before we obtain an R_2-basis of L_2. The proof of Proposition 2.17 yields an orthogonal basis of L_2 and thus $u_1, \dots, u_g \in \{1,3,5,7\}$ such that $L_2 \cong \langle u_1, \dots, u_g \rangle$. By Remark 2.22 we have $L_2 \cong \langle \ell_2, \dots, \ell_2 \rangle$ if and only if $\ell_2 \equiv \prod_i u_i \pmod{\mathrm{Nr}(R_2^*)}$ and $\prod_{i<j} (u_i, u_j)_2 = (\ell_2, \ell_2)_2^{(g-1)/2}$. This gives an effective method to find the element ℓ_2 or to show that it does not exist.

(4) Suppose $2 \mid a$, L_2 is free and g is even. If $2 \nmid f d_F$ then $L_2 \cong \langle 1, \dots, 1 \rangle$ by [Jac62, Proposition 10.4]. So we may assume that $2 \mid f d_F$ and we compute a Gram matrix G of L_2. The existence of ℓ_2 implies that $\det(G) \in \mathrm{Nr}(R_2^*)$ and L_2 is odd. The first condition is readily checked and the second holds if and only if some diagonal entry of G lies in $\mathbb{Z}_2^*$. Suppose these conditions both hold. As in in the case of odd ranks, the existence of ℓ_2 is now guaranteed whenever R_2 is maximal or $3 \in \mathrm{Nr}(R_2^*)$ or $7 \in \mathrm{Nr}(R_2^*)$. In the other cases, the proof of Proposition 2.17 shows how to compute $u_1, \dots, u_g \in \{1,3,5,7\}$ such that $L_2 \cong \langle u_1, \dots, u_g \rangle$. Then $L_2 \cong \langle \ell_2, \dots, \ell_2 \rangle$ if and only if $\prod_{i<j} (u_i, u_j)_2 = (\ell_2, \ell_2)_2^{g/2}$. This again yields an effective method to decide if $\ell_2 \in \{1,3,5,7\}$ exists.

Example 2.24. Let $F = \mathbb{Q}(\sqrt{-10})$ and let $\mathfrak{p}$ be the (non-principal) prime ideal of $\mathscr{O}$ over 2. Equip F^2 with the hermitian form h induced by $\mathrm{diag}(1,2)$. Then

$$L := \mathfrak{p} \cdot (2,0) \oplus \frac{1}{4}\mathscr{O} \cdot (\sqrt{-10} + 2, 1)$$

is a unimodular (and projective) $\mathscr{O}$-lattice in (F^2, h) but $\det(F^2, h) = 2$ is not a norm in F.

Example 2.25. Let $R = \mathbb{Z}[2i]$ be the order of conductor 2 in $\mathbb{Q}(i)$. Let L be the free hermitian R-lattice with Gram matrix

$$G = \begin{pmatrix} 3 & 2i & 2i-1 \\ -2i & 3 & 2i+1 \\ -2i-1 & -2i+1 & 3 \end{pmatrix} \in R^{3\times 3}.$$

The determinant of G is 1, so L is unimodular. We find that $L_2 \cong \langle 1,3,3 \rangle$ and $\mathrm{Nr}(R^*) = \mathbb{Z}_2^{*2} \uplus 5\mathbb{Z}_2^{*2}$. Now $(1,3)_2^2 \cdot (3,3)_2 = -1$ but $(1,1)_2^3 = (5,5)_2^3 = +1$. Hence $L_2 \ncong \langle \ell_2, \ell_2, \ell_2 \rangle$ for any $\ell_2 \in \mathbb{Z}_2^*$. In particular, L does not contain a free R-sublattice $L' \cong \langle \ell, \ell, \ell \rangle$ for any odd integer ℓ.

3. The description of polarized abelian varieties in terms of lattices

We set up the essential tools to introduce the equivalence of categories which allows us to interpret certain polarized abelian varieties as hermitian lattices.

3.1. **The equivalence of categories.** Let $\mathscr{C}$ be an abelian category, let E be an object of $\mathscr{C}$ and let R be a ring. Fix a morphism $\rho\colon R \to \mathrm{End}(E)$. Let L be a finitely presented left R-module and let

$$R^m \xrightarrow{\varphi} R^n \to L \to 0$$

be a finite presentation. We identity the map $\varphi \in M_{n,m}(R)$ with its image in $M_{n,m}(\mathrm{End}(E))$ by the map induced by ρ, where $M_{n,m}(R)$ denotes the ring of matrices with n rows and m columns with coefficients in R. It defines a morphism

$$E^n \xrightarrow{{}^t\varphi} E^m.$$

The object $\ker({}^t\varphi)$ does not depend on the presentation of L and [Ser85, III.Sec.8.1] uses this to define the functor $\mathscr{F}_E$ as $\mathscr{F}_E(L) = \ker({}^t\varphi)$ on objects. Let us look now on what $\mathscr{F}_E$ does on arrows. Let $f : L_1 \to L_2$ be a morphism of R-modules. Given finite presentations $R^{m_i} \xrightarrow{\varphi_i} R^{n_i} \to L_i \to 0$ of L_i we can lift f to a commutative diagram of R-modules as follows.

$$\begin{array}{ccccccc} R^{m_1} & \xrightarrow{\varphi_1} & R^{n_1} & \longrightarrow & L_1 & \longrightarrow & 0 \\ \downarrow{\scriptstyle G} & & \downarrow{\scriptstyle F} & & \downarrow{\scriptstyle f} & & \\ R^{m_2} & \xrightarrow{\varphi_2} & R^{n_2} & \longrightarrow & L_2 & \longrightarrow & 0. \end{array}$$

We can define $\mathscr{F}_E(f)$ as the map induced by ${}^tF$ by restriction to $\ker({}^t\varphi_2) \to \ker({}^t\varphi_1)$

$$\begin{array}{ccccccc} E^{m_2} & \xleftarrow{{}^t\varphi_2} & E^{n_2} & \longleftarrow & \ker({}^t\varphi_2) & \longleftarrow & 0 \\ \downarrow{\scriptstyle {}^tG} & & \downarrow{\scriptstyle {}^tF} & & \downarrow{\scriptstyle \mathscr{F}_E(f)} & & \\ E^{m_1} & \xleftarrow{{}^t\varphi_1} & E^{n_1} & \longleftarrow & \ker({}^t\varphi_1) & \longleftarrow & 0. \end{array}$$

We now focus on the case where $\mathscr{C}$ is the category of group schemes over $\mathbb{F}_q$ (with $\mathbb{F}_q$-morphisms), $E/\mathbb{F}_q$ is an ordinary elliptic curve and $R = \mathrm{End}(E)$. The ring R is an order in an imaginary quadratic field $F = \mathrm{Frac}\, R$. Denote by $\pi \in R$ the Frobenius endomorphism of E. Let $R - \mathrm{Mod}_{\mathrm{f.p}}$ be the category of finitely presented torsion-free left R-modules (this is the category of R-lattices from Section 2) and Ab_E be the sub-category of $\mathscr{C}$ of abelian varieties $\mathbb{F}_q$-isogenous to a power of E.

Theorem 3.1. *Let E be an ordinary elliptic curve over $\mathbb{F}_q$. Then $\mathscr{F}_E$ defines an equivalence of categories between $(R - Mod_{f.p})^{opp}$, the opposite category of $R - Mod_{f.p}$, and Ab_E if, and only if, $R = \mathbb{Z}[\pi]$. Moreover the functor $\mathscr{F}_E$ is exact.*

The reader can refer to [JKP+18, Theorem 7.6] and [JKP+18, Theorem 4.4] for proofs.

Remark 3.2. Serre also introduces another functor $M \mapsto M \otimes E := \mathrm{Coker}\, \varphi$ which is further studied in [Lau18, Appendice], [JKP+18, section 8] or [AK18]. This functor is covariant but not exact. We also prefer to use $\mathscr{F}_E$ since the theory is settled for an arbitrary order R whereas Serre only develops it for the maximal order. In general there is no easy way to compare the two functors if the R-module is not projective. Notice that the image of a projective R-module $L \in (R - \mathrm{Mod}_{\mathrm{f.p}})^{\mathrm{opp}}$ by $\mathscr{F}_E$ is an abelian variety A isomorphic to a product of elliptic curves $E_i \sim E$ such that $\mathrm{End}(E_i) = R$ for all $1 \leq i \leq g$. Indeed, for an R-ideal I_i such that $E_i = \mathscr{F}_E(I_i)$, $\mathrm{End}(E_i) \simeq (I_i : I_i)$ and since R is Gorenstein, I_i is invertible if and only if $(I_i : I_i) = R$ [Mar19, Prop.2.1].

Notice that if E is such that $R = \mathrm{End}(E) \supset \mathbb{Z}[\pi]$ then the image of $\mathscr{F}_E$ consists of the abelian varieties isomorphic to products of elliptic curves E_i such that the conductor of $\mathrm{End}(E_i)$ divides the conductor of $\mathrm{End}(E)$, as subrings of the maximal order of $F = \mathrm{Frac}(R)$ (see [JKP+18, Theorem 7.5]). However, if $R \neq \mathrm{End}(E)$, it may occur that $\mathscr{F}_E(L)$ is not even an abelian variety (see [JKP+18, Remark 4.6]).

Notice that, given an ordinary elliptic curve $E/\mathbb{F}_q$ with Frobenius endomorphism π, for each order R containing $\mathbb{Z}[\pi]$, there exists an elliptic curve over $\mathbb{F}_q$, isogenous to E, with endomorphism ring isomorphic to R (see [Wat69, Theorem 4.2]). Hence, in what follows, we will always assume that the assumption $R = \mathbb{Z}[\pi] = \mathrm{End}(E)$ is satisfied. Also notice that the main result of [JKP+18] is more general and can also deal with certain supersingular elliptic curves.

3.2. **Polarizations.** Let A be an abelian variety over $\mathbb{F}_q$ isogenous to a power of an elliptic curve E such that $R = \mathrm{End}(E) = \mathbb{Z}[\pi]$. Let us recall that a polarization is an isogeny $\phi_{\mathscr{L}} \colon A \to \widehat{A}$ with $\mathscr{L}$ an ample line bundle. Let L be a R-lattice. As in [JKP+18, Sec.4.3], we denote L^* the R-lattice $\mathrm{Hom}_R(L, R)$ with the action of $r \in R$ on $\alpha \in L^*$ given by $r.\alpha(x) = \alpha(\bar{r}x)$. We want to translate polarizations in the category of R-lattices.

Theorem 3.3. *Let $E/\mathbb{F}_q$ be an ordinary elliptic curve with $R = End(E) = \mathbb{Z}[\pi]$ where π is the Frobenius endomorphism of E. Let $F = \mathrm{Frac}(R)$. The functor $\mathscr{F}_E$ defines an equivalence of categories between polarized abelian varieties A which are isogenous to E^g and positive definite hermitian R-lattices (L, h) of rank g where $h(x, y) = \Lambda(x)(y)$ with $\Lambda : L \otimes F = V \to V^*$ a linear map such that $\Lambda^{-1}(L^*) \subset L$. Moreover the degree of the polarization is equal to $[L : \Lambda^{-1}(L^*)]$.*

Notice also that, since $\mathscr{F}_E$ is exact, a hermitian lattice (L, h) is indecomposable (see Definition 2.8) if and only if the corresponding polarized abelian variety (A, a) is indecomposable (i.e. (A, a) is not the product of two non-trivial polarized abelian sub-varieties).

Remark 3.4. In [Ser85, Chap.III.Sec.8], Serre uses the functor $M \to M \otimes E$ to get Theorem 3.3 under the hypothesis that R is the maximal order. In another direction, [AK18, Th.A] gets a similar result for arbitrary R (not necessarily quadratic) but only for projective modules.

Before giving various lemmas which will culminate in the proof of Theorem 3.3, in order to stick with the terminology of Section 2 and to lead to an algorithmic version of the theorem, we now give its translation in terms of the dual lattice $L^\# = \{x \in V, h(x, L) \subseteq R\}$.

Lemma 3.5. *With the notation above, $\lambda := \Lambda^{-1}$ is an isomorphism between the R-modules $L^\#$ and L^*.*

Proof. Notice that $x \in V$ belongs to $\mathrm{Im}\lambda$ if and only if $\Lambda(x) \in L^*$ which is the case if and only if $\forall y \in L, h(x, y) = \Lambda(x)(y) \in R$. This means, by definition, $x \in L^\#$. Hence, $L^\# = \mathrm{Im}\lambda$. □

Under this isomorphism, one obtains a more natural functor as follows.

Corollary 3.6. *Let $E/\mathbb{F}_q$ be an ordinary elliptic curve with $R = End(E) = \mathbb{Z}[\pi]$ where π is the Frobenius endomorphism of E. There is an equivalence of categories between polarized abelian varieties A which are isogenous to E^g and positive definite hermitian R-lattices (L, h) of rank g such that $L^\#$ is integral. Moreover, the degree of the polarization is equal to $[L : L^\#]$.*

Hence, the isomorphism classes of principally polarized abelian varieties in the isogeny class E^g correspond to the isometry classes of unimodular positive definite hermitian R-lattices.

The rest of the section is devoted to the proof of Theorem 3.3, which will use several lemmas.

In [JKP+18, Th.4.7], it is shown that the dual of $A = \mathscr{F}_E(L)$ is functorially isomorphic to $\mathscr{F}_E(L^*)$. Hence we can relate polarizations and injective morphisms from $L^* \to L$. Now, a morphism $\lambda \colon L^* \to L$ also induces a sesquilinear form

$$H_\lambda \colon L^* \times L^* \to R, (\alpha, \beta) \mapsto \alpha\lambda\beta.$$

We first prove the following lemma.

Lemma 3.7. *The form H_λ is hermitian if and only if there exists a line bundle $\mathscr{L}$ on $A = \mathscr{F}_E(L)$ such that $\mathscr{F}_E(\lambda) = \phi_{\mathscr{L}}$.*

Proof. Let $f : E^g \to A$ be an isogeny induced by an inclusion $\iota : L \to N \simeq R^g$. Observe that the isogeny $a = \mathscr{F}_E(\lambda)$ is of the form $\phi_{\mathscr{L}}$ if and only if $a' = \hat{f}af$ is of the form $\phi_{\mathscr{L}'}$ for a line bundle $\mathscr{L}'$ on E^g. The direct implication is obvious since $\hat{f}af = \phi_{f^*\mathscr{L}}$. As for the other direction, let ℓ be any prime distinct from the characteristic of $\mathbb{F}_q$. By [Mum08, Th.2, p.188], the form $e_\ell(x, a'y)$ is skew-symmetric and therefore the form $e_\ell(x, ay)$ is as well. Still using [Mum08, Th.2], we then have that there exists a line bundle $\mathscr{M}$ such that $2a = \phi_{\mathscr{M}}$ and [Mum08, Th.3,p.231] shows that there exists $\mathscr{L}$ such that $\mathscr{M} \simeq \mathscr{L}^2$ hence $a = \phi_{\mathscr{L}}$.

Now, denote $\lambda' = \iota\lambda\iota^*$ so that $\mathscr{F}_E(\lambda') = a'$. Similarly, the form H_λ is hermitian if and only if the form $H_{\lambda'}$ is. This equivalence can be checked on the F-vector spaces FL and FN where ι is an isomorphism. There

we have that $H_{\lambda'}(\alpha', \beta') = \alpha'(\iota\lambda\iota^*)\beta' = H_\lambda(\alpha'\iota, \beta'\iota)$, so it is only a change of basis and the equivalence is clear.

We can therefore assume that $A = \mathscr{F}_E(R^g) = E^g$. Let $\lambda_0 : R^* \to R$ be the isomorphism defined by $\alpha \mapsto \alpha(1)$. Since the dual of E is only defined up to isomorphisms, we can assume by composing with an isomorphism that $\mathscr{F}_E(\lambda_0) : E \to \hat{E}$ is the unique principal polarization $P \mapsto \mathscr{O}([O] - [P])$ on E. Then the product polarization $a_0 = \mathscr{F}_E(\Lambda_0)$ where $\Lambda_0 : (R^g)^* \to R^g$ is defined by $(\alpha_1, \dots, \alpha_g) \mapsto (\alpha_1(1), \dots, \alpha_g(1))$. Now let $M = \lambda\Lambda_0^{-1} \in \mathrm{End}(R^g) = M_g(R)$. Since $\Lambda_0 M^* \Lambda_0^{-1} = {}^t\bar{M}$, the Rosati involution $\dagger$ induced by a_0 on $\mathrm{End}(E^g) = M_g(R)$ is $M \mapsto {}^t\bar{M}$. Hence, ${}^t\bar{M} = M$ if and only if $(a_0^{-1}a)^\dagger = (a_0^{-1}a)$ i.e. $a = \phi_{\mathscr{L}}$ by [Mil86, Prop.17.2]. On the other hand, the form H_λ is hermitian if and only if ${}^t\bar{M} = M$. □

Lemma 3.8. *Let L be a R-lattice of rank g and $\lambda\colon L^* \to L$ injective such that H_λ is hermitian. Then there exists a free over-lattice $L \overset{\iota}{\hookrightarrow} N = \bigoplus_{i=1}^g Re_i$ and integers $(\ell_i)_{1\le i\le g}$ such that if $\lambda' = \iota\lambda\iota^*$, then $H_{\lambda'} : N^* \times N^* \to R$ satisfies $H_{\lambda'}(e_i^*, e_j^*) = \ell_i\delta_{ij}$.*

Proof. Since λ is injective, the hermitian form H_λ is non-degenerate. As in Theorem 2.16(1), we can find a basis (α_i) of $V^* = FL^*$ of vectors of L^* which is orthogonal for H_λ, i.e., $\alpha_i\lambda\alpha_j = \ell_i\delta_{ij}$ with $\ell_i \in \mathbb{Z}$. Consider $N' = \bigoplus_{i=1}^g R\alpha_i \subseteq L^*$ and then $N = N'^* \supseteq L^{**} \simeq L$, the last isomorphism being the evaluation map $ev : L \to L^{**}$. Denote by $\iota\colon L \to N$ the injection and (e_i) the dual basis of (α_i). Noticing that $\alpha_i^{**} = \alpha_i \circ ev^{-1}$, we get that

$$H_{\lambda'}(e_i^*, e_j^*) = \alpha_i^{**}(\iota\lambda\iota^*)\alpha_j^{**} = \alpha_i\lambda\alpha_j = \ell_i\delta_{ij}.$$

□

Lemma 3.9. *Let $f\colon A \to B$ be an isogeny and $\mathscr{L}$ be an invertible line bundle on B. Then $\mathscr{L}$ is ample if and only if $f^*\mathscr{L}$ is ample.*

Proof. An isogeny is a finite faithfully flat morphism. So ampleness ascends along the isogeny, since it is finite, by [GD64, p. II.5.1.12], and descends since it is faithfully flat [GD64, p. IV.2.7.2] (the proof holds for relative ampleness but it is easy to adapt it for ampleness, see also [Liu02, Exercise 5.1.29]). □

Lemma 3.10. *Let L be a R-lattice and $A = \mathscr{F}_E(L)$ be the corresponding abelian variety. Let $\lambda : L \to L^*$ be such that H_λ is hermitian and $a = \mathscr{F}_E(\lambda)\colon A \to \widehat{A}$ be the corresponding isogeny. Then there exists an isogeny $f\colon E^g \to A$, integers $(\ell_i)_{1\le i\le g}$, a map $D \in End(E^g) : (x_1, \dots, x_g) \mapsto (\ell_1 x_1, \dots, \ell_g x_g)$ and a commutative diagram*

$$\begin{array}{ccc} A & \xrightarrow{a} & \widehat{A} \\ {\scriptstyle f}\uparrow & & \downarrow{\scriptstyle \widehat{f}} \\ E^g & \xrightarrow{a_0 \circ D} & \widehat{E^g} \end{array}$$

FIGURE 1. Fundamental diagram

where a_0 is the product polarization on E^g. Moreover a is a polarization if and only if $\ell_i > 0$ for all i, or equivalently if and only if H_λ is positive definite on FL^*.

Proof. Let $\iota : L \hookrightarrow N = \bigoplus_{i=1}^g Re_i$ and $\lambda' = \iota\lambda\iota^*$ be as in Lemma 3.8. Consider the isomorphism $u\colon N \xrightarrow{\sim} R^g$ given by the basis (e_i) of N. Hence we have

$$\begin{array}{ccccccccc} & & & & L^* & \xrightarrow{\lambda} & L & & \\ & & & & {\scriptstyle \iota^*}\uparrow & & \downarrow{\scriptstyle \iota} & & \\ (R^g)^* & \xrightarrow[\Lambda_0]{\sim} & R^g & \xrightarrow[u^*]{\sim} & N^* & \xrightarrow{\lambda'} & N & \xrightarrow[u]{\sim} & R^g. \end{array}$$

We obtain the desired diagram by composing this diagram by $\mathscr{F}_E$ and taking $f = \mathscr{F}_E(u\iota)$.
Since H_λ is hermitian, there exists a line bundle $\mathscr{L}$ on A such that $a = \phi_{\mathscr{L}}$. Since $a_0 D$ is the pullback of a by f the isogeny a is a polarization if and only $a_0 D$ is a polarization by Lemma 3.9 below. Moreover, $a_0 D$ is a polarization of E^g if and only if $\ell_i > 0$ for all i. As in the first part of Lemma 3.7, we can conclude that H_λ is positive definite if and only if $H_{\lambda'} = \operatorname{diag}(\ell_1, \dots, \ell_g)$ is, and we have the final equivalence of the lemma. □

Remark 3.11. The fact that H_λ is a hermitian form on L^* and not on L is a bit cumbersome. Since λ is injective, it induces an isomorphism $\Lambda := (\lambda \otimes_R \mathrm{Id}_F)^{-1} \colon L \otimes F = V \to V^*$. This defines a hermitian form on V given by

$$h \colon V \times V \to F, (x, y) \mapsto \Lambda(x)(y)$$

which makes (L, h) a hermitian R-lattice.

Proof of Theorem 3.3. Simply combine Lemmas 3.7 and 3.10 with Remark 3.11 to get h on $L \times L$ instead of H_λ on $L^* \times L^*$. The final statement about the degree of the polarization is easily obtained using [JKP+18, Theorem 4.4] which computes the degree of an isogeny corresponding to an inclusion of lattices with equal rank $\iota \colon L \to M$ by $\deg \mathscr{F}_E(\iota) = [M \colon \iota(L)]$. □

3.3. **Description of the abelian variety as a quotient of E^g.** Let (L, h) be a hermitian lattice with $L^\#$ integral. The goal of this section is to compute the kernel of the isogeny $f \colon E^g \to A = \mathscr{F}_E(L)$ of Corollary 3.10 obtained by the inclusion $L \hookrightarrow R^g$ induced by ι in Lemma 3.8 after identification of $N = \bigoplus Re_i$ with R^g.

As a first step, to apply Corollary 3.6, we need to start with an explicit elliptic curve $E/\mathbb{F}_q$ with ring of endomorphism $\mathbb{Z}[\pi]$. If q is small, it is efficient to use an algorithm which determines the endomorphism ring of an ordinary elliptic curve [EL10] or [BS11]. In the package implemented, we consider a version of the latter kindly provided by Sutherland and apply it to the list of elliptic curves with a given trace (which can be naively obtained from the list of all elliptic curves by computing the trace on each of them). If the discriminant of $\mathbb{Z}[\pi]$ is small, the best way to obtain E is to compute a root j over $\mathbb{F}_q$ of the Hilbert class polynomial of $\mathbb{Z}[\pi]$ and find among the elliptic curves with j-invariant j the one with the right trace. We refer to [Eng09; Sut11] for algorithms to compute this class polynomial. Note that the complexity of the rest of the algorithm strongly depends on the discriminant of $\mathbb{Z}[\pi]$, so choosing this second method, this step is never the bottleneck of the whole algorithm.

Given an inclusion of equal rank g R-lattices $\iota \colon L_1 \to L_2$ and surjective morphisms $T_i \colon R^{m_i} \to L_i$ we can lift ι to $P \in M_{m_2, m_1}(R)$

$$\begin{array}{ccc} R^{m_1} & \xrightarrow{T_1} & L_1 \\ {\scriptstyle P}\downarrow & & \downarrow{\scriptstyle \iota} \\ R^{m_2} & \xrightarrow{T_2} & L_2 \end{array}$$

by computing the image of the canonical basis of R^{m_1} by $\iota \circ T_1$ and taking any preimages by T_2. Since the morphisms T_i are surjective, $\mathscr{F}_E(T_i)$ are injective and the kernel of the corresponding isogeny $\mathscr{F}_E(\iota) = f \colon \mathscr{F}_E(L_2) \to \mathscr{F}_E(L_1)$ can be computed by $\ker f = \mathscr{F}_E(T_2)^{-1} \ker {}^tP$.

In the present situation, $L_1 = L, L_2 = N = \bigoplus Re_i, m_2 = g$ and $T_2 = \mathrm{Id}$. It remains to make T_1 and the (e_i) explicit. Consider a pseudo-basis $L = \mathfrak{a}_1 x_1 \oplus \cdots \oplus \mathfrak{a}_g x_g$. Since the $\mathfrak{a}_i$ are fractional R-ideals they have at most 2 generators. Hence, L is generated by $g \le r \le 2g$ generators. So, T_1 is the surjective morphism $R^r \twoheadrightarrow L$ sending the canonical basis of R^r on the generators of L. Applying the functor $\mathscr{F}_E$ to the composition leads to the commutative diagram

$$\begin{array}{ccc} E^r & \xleftarrow{\mathscr{F}_E(T_1)} & A \\ {\scriptstyle {}^tP}\uparrow & \nearrow_{f} & \\ E^g & & \end{array}$$

and $\ker f = \ker(\mathscr{F}_E(T_1) \circ f) = \ker {}^tP$. By Figure 1, one sees that $\ker f \subseteq \ker D = \prod_{i=1}^g E[\ell_i] \subseteq E[\ell]^g$ with $\ell = \operatorname{lcm}(\ell_i)$ and D the map of Lemma 3.10. Thus, it is enough to compute the action of ${}^tP$ on a basis

of the ℓ-torsion of E^g to have the whole kernel. To go on, we will assume that ℓ is prime to $\operatorname{char}\mathbb{F}_q$ so $E[\ell] \simeq (\mathbb{Z}/\ell\mathbb{Z})^2$ is étale and we can work with geometric points.

Let clarify how to compute the family $(e_i)_{1\leq i\leq g}$. Let us recall that we defined it as the dual basis of an orthogonal family of L^* so they satisfy $e_i^*\lambda' e_j^* = \ell_i\delta_{ij}$. This means that $\lambda'(e_i^*) = \ell_i e_i$ and then $h(e_i, e_i) = \frac{1}{\ell_i}$ (see proof of Lemma 3.5). Consider an orthogonal family $(u_i)_{1\leq i\leq g}$ of vectors of $L^\#$ of norm $(\ell_i)_{1\leq i\leq g}$ and let $e_i = \frac{1}{\ell_i}u_i$. By the inclusion $\bigoplus_{i=1}^g Ru_i \subseteq L^\#$ we have

$$L \subseteq \left(\perp_{1\leq i\leq g} Ru_i\right)^\# = \perp_{1\leq i\leq g}(Ru_i)^\# = \perp_{1\leq i\leq g} Re_i.$$

Hence, if we find an orthogonal family $(u_i)_{1\leq i\leq g}$ of $L^\#$ with norm $(\ell_i)_{1\leq i\leq g}$ then $(e_i)_{1\leq i\leq g} = (1/\ell_i \cdot u_i)_{1\leq i\leq g}$ is an orthogonal family of norm $(1/\ell_i)_{1\leq i\leq g}$ suited for the inclusion $\iota\colon L \to \bigoplus_{i=1}^g Re_i$.

We summarize these computations in Algorithm 5.

Algorithm 5 Computation of the kernel of an isogeny $E^g \to A$

Input: A R-lattice (L, h) and E an elliptic curve over $\mathbb{F}_q$ with $\operatorname{End}(E) = \mathbb{Z}[\pi] \simeq R$.
Output: A basis of the kernel of an isogeny $f : E^g \to \mathscr{F}_E(L)$ such that the polarization a on L induced by h satisfies $\hat{f}af$ is a completely decomposable polarization.

1: Compute an orthogonal family $(u_i)_{1\leq i\leq g}$ of $L^\#$ of norms $\ell_i \in \mathbb{Z}$ using the Gram-Schmidt process (when $\ell_1 = \ldots = \ell_g$, use Algorithm 4). Define $e_i = u_i/\ell_i$, $\ell = \operatorname{lcm}(\ell_i)$, $N = \bigoplus_{i=1}^g Re_i$ and ι the inclusion of L in N.
2: Compute a pseudo-basis $L = \mathfrak{a}_1 x_1 \oplus \cdots \oplus \mathfrak{a}_g x_g$ given by $1 \leq r \leq 2g$ generators. Let $T_1\colon R^r \to L$ be a surjective morphism that sends the canonical basis of R^r on the generators of L.
3: Let P be the matrix of the morphism $\iota \circ T_1 : R^r \to N$ in the canonical basis of R^r and the basis (e_i) of N.
4: Compute a basis (b_0, b_1) of $E[\ell]$. This allows us to identify $E[\ell]$ with $(\mathbb{Z}/\ell\mathbb{Z})^2$ and let $\mu\colon E[\ell]^{2g} \to (\mathbb{Z}/\ell\mathbb{Z})^{2g}$ be the isomorphism induced by the identification.
5: Compute the action of the Frobenius π on (b_0, b_1) as a matrix $\Pi \in M_2(\mathbb{Z}/\ell\mathbb{Z})$.
6: Create a matrix $Q \in M_{2r,2g}(\mathbb{Z}/\ell\mathbb{Z})$ by replacing each entry $a + b\pi$ of ${}^tP$ by $aI_2 + b\Pi$.
7: Compute a basis $\mathscr{B}$ of $\ker Q \in (\mathbb{Z}/\ell\mathbb{Z})^{2g}$.
8: **return** $\mu^{-1}(\mathscr{B})$.

We will use this algorithm with the additional condition $\ell_1 = \ldots = \ell_g$. Indeed, in Section 4, we need more specific properties about the kernel K of the isogeny in order to be able to compute the theta null point on A using the current algorithms. We first require that $\ell = \ell_1 = \ldots = \ell_g$ is odd and prime to q (see Remark 4.1 for the condition ℓ odd). We have discussed in Theorem 2.16, when this can be achieved. By [Mil86, Prop.16.8], K is a maximal isotropic subgroup of $E[\ell]^g$ for the Weil pairing on E^g induced by the product polarization. However for the algorithms we also need K to be of rank g, that is isomorphic as a group to $(\mathbb{Z}/\ell\mathbb{Z})^g$. We call such a K a *totally isotropic* subgroup. Equivalently, for an abelian variety A_0, $K \subset A_0[\ell]$ is a *totally isotropic* subgroup of level ℓ if it is isotropic, and one can find a symplectic decomposition $A_0[\ell] = K \oplus K'$. If K is maximal isotropic, it is always totally isotropic when ℓ is square free, but this can fail if ℓ has a square factor (for instance $A_0[\ell]$ is maximal isotropic in $A_0[\ell^2]$). We adopt a pragmatic approach here and test that a given K has indeed the right group structure. In every computation we made, when an odd ℓ exists, we always found one for which K was totally isotropic.

4. Theta structures and a modular interpretation of the isogeny formula

In this section, k is any field of characteristic $p \neq 2$. We will first recall in Section 4.1 how to use the so-called isogeny formula to derive the theta null point on a target abelian variety from a (well-chosen) isogenous one. Then, in Section 4.2, we will show that the isogeny formula is actually valid over the universal abelian scheme. Although the proof basically follows the same lines as the proof over a field, this result, and the notation introduced there, will be useful in Section 4.3, where we will derive a precise affine version of the isogeny formula. More precisely, we introduce a particular choice of affine lifts of the theta null points

which we call *modular*, since they are derived from interpreting the theta constants as modular forms, and we show in Theorem 4.5 that the isogeny formula respects the modular lifts. In Section 4.4, we explain how to compute k-rational modular lifts for a product of elliptic curves with a product polarization. Combining the 'modular' isogeny formula and these initial modular lifts allow us in Section 4.5 to compute values of Siegel modular forms of even weight given as polynomials in the theta constants with coefficients in k on the span of the isogeny class (see Theorem 4.9 and Algorithm 7).

4.1. **Input for the isogeny formula over k.** Let $(A, \mathscr{L}, \Theta_{\mathscr{L}})/k$ be a principally polarized abelian variety of dimension g with a totally symmetric theta structure $\Theta_{\mathscr{L}}$ of level n on $\mathscr{L}$. This implies that n is even which we assume from now on (until the end of this section). Let K be a k-rational totally isotropic subgroup for the Weil pairing of $\mathscr{L}^\ell$, with ℓ prime to np or to n if $p = 0$.

In [CR15; LR15], an algorithm (which we call the *isogeny formula* and implemented in the package `Avisogenies` [BCR10]) is given to compute the isogeny $f : (A, \mathscr{L}, \Theta_{\mathscr{L}}) \to (B, \mathscr{M}, \Theta_{\mathscr{M}})$ where $B = A/K$, $f^*\mathscr{M} = \mathscr{L}^\ell$ and $\Theta_{\mathscr{M}}$ is the unique symmetric theta structure of level n on $\mathscr{M}$ compatible with $\Theta_{\mathscr{L}}$ (the unicity comes from the fact that ℓ is prime to n). More precisely the algorithm takes as input the (projective) theta null point $\theta^A(0) \coloneqq \left(\theta^A_{i\in Z(\overline{n})}(0)\right) \in \mathbb{P}(\bar{k})^{n^g-1}$ of A, where $Z(\overline{n}) = (\mathbb{Z}/n\mathbb{Z})^g$, along with the theta coordinates of the geometric points of K (or suitable equations giving the kernel K) and outputs the theta null point $\theta^B(0) \coloneqq \left(\theta^B_{i\in Z(\overline{n})}(0)\right)$ of B along with the equations for the isogeny f. We usually take $n = 4$ (since this is the smallest even n which gives an embedding of the variety into projective space) and the theta null point completely characterizes $(B, \mathscr{M})$ up to $\bar{k}$-isomorphism. We will describe in more details (a generalisation of) this algorithm in Section 4.2. In this section we explain how to compute the inputs for the isogeny formula in our situation.

Let E/k be an elliptic curve. If $(B, \mathscr{M})$ is isogenous to E^g, we show how to compute $\theta^B(0)$ of level 4 by applying the algorithm with $A = \prod_{i=1}^g E_i$ where E_i are elliptic curves over k isogenous to E and $\mathscr{L}$ the principal product polarization on A. For this, we need three elements as inputs for the algorithm:

- compute a totally isotropic kernel K such that $B = A/K$. When k is a finite field and $E = E_1 = \ldots = E_g$ is ordinary, we have seen in Section 3.3 how to do this effectively;
- compute the theta null point $\theta^A(0)$ of level 4 on $(A, \mathscr{L})$. As we deal with the product polarization, the coordinate $\theta^A_{i_1,\ldots,i_g}(0)$ of $\theta^A(0)$ is equal to $\prod_{1\le j\le g} \theta^{E_j}_{i_j}(0)$. Getting the theta null point on an elliptic curve (over a field of odd characteristic) is a classical result. In Corollary 4.8, we give an even more precise version of this to which we refer now and that we use in Step 1 and 2 of Algorithm 6.
- compute the theta coordinates of the points in the kernel K. Likewise since we have a product polarization, $\theta^A_{i_1,\ldots,i_g}(x_1, \ldots, x_g) = \prod_{1\le j\le g} \theta^{E_j}_{i_j}(x_j)$. Computing the theta coordinates $\left(\theta^{E_i}_j(x_i)\right)_{j\in\mathbb{Z}/4\mathbb{Z}}$ is also classical [Mum07b], [Cos11, Chapter 5], and is implemented in `Avisogenies` [BCR10].

We therefore get the following algorithm 6.

Algorithm 6 Computation of the theta null point of level 4 on the quotient variety

Input: Elliptic curves E_i/k with equation $y^2 = (x - e_{1i})(x - e_{2i})(x - e_{3i})$ where k is of characteristic p different from 2, a k-rational totally isotropic subgroup K of $A = \prod_i E_i$ of order prime to $2p$ (or just prime to 2 if $p = 0$).

Output: The theta null point $\theta^B(0)$ of level 4 on $B = A/K$ with $\mathscr{M}$ the polarization induced by the product polarization on A.

1: For all $1 \leq i \leq g$, define $\theta_0'^{E_i} = \sqrt[4]{e_{1i} - e_{3i}}, \theta_1'^{E_i} = \sqrt[4]{e_{1i} - e_{2i}}, \theta_2'^{E_i} = \sqrt[4]{e_{2i} - e_{3i}}$ for arbitrary choices of the roots.

2: Compute $\theta_0^{E_i}(0) = \theta_0'^{E_i} + \theta_1'^{E_i}$, $\theta_2^{E_i}(0) = \theta_0'^{E_i} - \theta_1'^{E_i}$ and $\theta_1^{E_i}(0) = \theta_3^{E_i}(0) = \theta_2'^{E_i}$ for all $1 \leq i \leq g$.

3: Compute $\theta^A_{(i_1,\ldots,i_g)}(0) = \theta^{E_1}_{i_1}(0) \cdots \theta^{E_g}_{i_g}(0)$ for all $(i_1, \ldots, i_g) \in Z(\overline{4})$.

4: For all $1 \leq i \leq g$ and for all $x = (x_1, \ldots, x_g) \in K \setminus \{0\}$, compute the theta coordinates $\left(\theta_j^{E_i}(x_i)\right)_{j \in \mathbb{Z}/4\mathbb{Z}}$, using [Cos11, Chapter 5],

5: Compute for all $j = (j_1, \ldots, j_g) \in Z(\overline{4})$ and for all $x = (x_1, \ldots, x_g) \in K \setminus \{0\}$ $\theta^A_j(x) = \theta^{E_1}_{j_1}(x_1) \cdots \theta^{E_g}_{j_g}(x_g)$.

6: Use [CR15]taking as input $\theta^A(0)$ and the theta coordinates of the points of K and output $\theta^B(0)$.

7: **return** $\theta^B(0) \in \mathbb{P}(\bar{k})^{4^g-1}$.

Remark 4.1. Some remarks on the code:

- The original version of `Avisogenies` assumed ℓ to be a prime. The only modification to the code we had to make is on how to construct a matrix $F \in \mathrm{Mat}_r(\mathbb{Z})$ such that ${}^tFF = \ell\mathrm{Id}$ used by Koizumi's formula Eq. (6). The integer r depends on ℓ being a square (hence $r = 1$), ℓ being a sum of two positive squares (hence $r = 2$) or a sum of four positive square (hence $r = 4$). Adapting the construction of F to ℓ odd non prime is straightforward by multiplicativity of the complex norm (if $r = 2$) or of the quaternionic norm (if $r = 4$).
- The restriction ℓ odd is not necessary in theory if some great care is taken. First the lift from level n to level ℓn is more complicated since we cannot work only on the points in the kernel K. We first need to compute a basis of points P_i such that nP_i is a basis of K (this was given to us for free before by the CRT). Furthermore this basis has to be compatible with the level n structure on A, so this may require first to act by an automorphism of the theta structure to make the level n structure on A compatible with $K[n]$. Secondly, if ℓ is not odd, then there may be several symmetric theta structures on B compatible with the one on A. So the isogeny formula in this case yields several solutions. This has not yet been implemented in [BCR10].

4.2. **The isogeny formula on the universal abelian scheme.** In this section we reformulate the isogeny formulae from [CR15] to show that the formulae are polynomials with coefficients in $\mathbb{Z}[\frac{1}{\ell n}]$ in the coordinates of the points of K. Since the fine moduli scheme (or stack if $n \leq 2$) $\mathscr{A}_{g,n}$ of abelian varieties with a symmetric theta structure of level n is smooth (or by rigidity [MFK94, § 6]), the isogeny formula is thus valid on the universal abelian variety defined over $\mathbb{Z}[\frac{1}{\ell n}]$. Though well known to experts, this is not completely obvious in the formulation of [CR15] since the authors only work with fields and implicitly use divisions in their equations.

We first give some motivations for this result. In Section 4.3 we give an algebraic modular interpretation of the isogeny formula by first considering the analytic modular interpretation over $\mathbb{C}$. It is then possible, by standard lifting arguments to extend this result to ordinary abelian varieties over a finite field. But, while possible, this is a bit painful to do properly since we want to control the lifts of the endomorphisms along with the differentials, and then give an algebraic meaning to the reduction of the period matrix modulo p. By contrast, showing that the isogeny formula is actually defined over $\mathbb{Z}[\frac{1}{\ell}]$ yields a much simpler proof that the analytic interpretation holds algebraically. Indeed, by smoothness, the modular interpretation is ultimately a statement about the equality of two multivariate polynomials defined over $\mathbb{Z}[\frac{1}{\ell}]$. But this equality holds when it holds over $\mathbb{C}$. In addition, this proof holds for all abelian varieties rather than just the ordinary ones. The notations introduced in this section will also be useful in Section 4.3 where we keep track of each modular factor at each step of the algorithm.

In order to avoid heavy notation, we will often let the theta structure $\Theta_{\mathscr{L}}$ (and eventually the polarization $\mathscr{L}$) be implicit, along with the coordinate group $Z(\overline{n})$.

Assume from now on that n is (even and) greater or equal to 4 and ℓ prime to n. Mumford constructs in [Mum67] the universal abelian variety $\mathscr{X}_{g,n} \to \mathscr{A}_{g,n}$ with a totally symmetric normalized relatively ample line bundle[2] and a symmetric theta structure of level n over $\mathbb{Z}[1/n]$ [3] as a quasi-projective scheme. Moreover Mumford uses Riemann's relations [Mum67, p. 83] to define a projective scheme $\overline{\mathscr{X}}_{g,n} \to \overline{\mathscr{A}}_{g,n}$ (where the equations of $\overline{\mathscr{A}}_{g,n}$ are given by evaluating the Riemann's relations on the zero section, together with the symmetry relations $\theta_i(0) = \theta_{-i}(0)$) and an embedding of $\mathscr{X}_{g,n} \to \mathscr{A}_{g,n}$ into $\overline{\mathscr{X}}_{g,n} \to \overline{\mathscr{A}}_{g,n}$ (so that $\mathscr{X}_{g,n}$ is the pullback of $\overline{\mathscr{X}}_{g,n}$ to $\mathscr{A}_{g,n}$). We denote $(\theta_i)_{i\in Z(\overline{n})}$ the theta coordinates on either $\mathscr{X}_{g,n}$ or $\overline{\mathscr{X}}_{g,n}$ and $(\theta_i(0))_{i\in Z(\overline{n})}$ the theta null point coordinates on either $\mathscr{A}_{g,n}$ or $\overline{\mathscr{A}}_{g,n}$ coming from the section $s : \overline{\mathscr{A}}_{g,n} \to \overline{\mathscr{X}}_{g,n}$ (which restricted to $\mathscr{A}_{g,n}$ corresponds to the zero section).

On $\overline{\mathscr{X}}_{g,n}$, we have an explicit action λ of the Heisenberg group $\mathcal{H}(\overline{n})$ on $\mathscr{L}_{\overline{\mathscr{X}}_{g,n}}$ [Mum67, Step 1, p. 84]. Writing $\mathcal{H}(\overline{n}) = \mathbb{G}_m \times Z(\overline{n}) \times \hat{Z}(\overline{n})$ where $\hat{Z}(\overline{n}) \simeq \oplus_{i=1}^{g} \mu_n$ is the Cartier dual of $Z(\overline{n})$, this canonical action is given by $\lambda(i).\theta_j = \theta_{i+j}$ for $i \in Z(\overline{n})$ and $\lambda(i).\theta_j =< i, j > \theta_j$ for $i \in \hat{Z}(\overline{n})$ where $< i, j >$ is the canonical pairing between $Z(\overline{n})$ and its Cartier dual $\hat{Z}(\overline{n})$. Acting on the zero section s gives a canonical basis of n-torsion.

Mumford's isogeny theorem [Mum66] then describes the universal isogeny (with a descent of level of the theta structure)

$$\pi_1 : \mathscr{X}_{g,\ell n} \to \mathscr{X}_{g,n}, (\theta_i)_{i\in Z(\overline{\ell n})} \mapsto (\theta_i)_{i\in Z(\overline{n})\subset Z(\overline{\ell n})}. \tag{3}$$

On $\mathscr{X}_{g,\ell n}$ the level ℓn theta structure induces a symplectic basis of the ℓn-torsion, and in particular a symplectic decomposition $K_1 \oplus K_2$ of the ℓ-torsion. Concretely over a field k, $K_1 = \{(< i, j > \theta_j(0))_{j\in Z(\overline{\ell n})}\}_{i\in \hat{Z}(\overline{\ell})}$ is the kernel of π_1, while $K_2 = \{(\theta_{i+j}(0))_{j\in Z(\overline{\ell n})}\}_{i\in Z(\overline{\ell})}$ is such that $\pi_1(K_2) = \{(\theta_{i+j}(0))_{j\in Z(\overline{n})}\}_{i\in Z(\overline{\ell})}$ is the kernel of the contragredient isogeny $\tilde{\pi}_1$.

Using π_1, we can now describe the isogeny formula in three steps.

Step 1. Denote $\Pi_1 : \mathscr{X}_{g,\ell n} \to \mathscr{X}_{g,n}^{\ell^g}, (\theta_i)_{i\in Z(\overline{\ell n})} \mapsto \left(\pi_1(\lambda(i)(\theta_j))_{j\in Z(\overline{\ell n})}\right)_{i\in Z(l)}$, where λ is the action of the Heisenberg group $\mathcal{H}(\overline{\ell n})$ described above. For $j \in Z(\overline{\ell})$ the component Π_1^j of Π_1 is given by

$$\Pi_1^{j\,*}(\theta_i^{\mathscr{X}_{g,n}}) = \theta_{i+j}^{\mathscr{X}_{g,\ell n}}, \quad i \in Z(\overline{n}). \tag{4}$$

The image of the restriction of Π_1 to $\mathscr{A}_{g,\ell n}$ (seen as the zero section of $\mathscr{X}_{g,\ell n}$) then describes the moduli scheme $\mathscr{T}_{g,n,\ell}$ of abelian varieties with a level n symmetric theta structure together with the points of an isotropic kernel of the ℓ-torsion.

It is easy to see that π_1 extends to a morphism $\overline{\pi}_1 : \overline{\mathscr{X}}_{g,\ell n} \to \overline{\mathscr{X}}_{g,n}$. Since the action λ is defined on $\overline{\mathscr{X}}_{g,\ell n}$, we can also extend Π_1 to a morphism $\overline{\Pi}_1 : \overline{\mathscr{X}}_{g,\ell n} \to \overline{\mathscr{X}}_{g,n}^{\ell^g}$. Let $\overline{T}$ be the image of $\overline{\mathscr{A}}_{g,\ell n}$. By construction $\mathscr{T}_{g,n,\ell}$ embeds into $\overline{T}$ and since we have explicit equations for $\overline{\mathscr{A}}_{g,\ell n}$ we have equations for $\overline{T}$.

By construction, given a k-point (A_0, K_0) of $\mathscr{T}_{g,n,\ell}$, geometric points of $\Pi_1^{-1}(A_0, K_0) \to \mathscr{A}_{g,\ell n}$ corresponds to abelian varieties $B_{0,\overline{k}} \in \mathscr{A}_{g,\ell n}(\overline{k})$ with a level ℓn symmetric theta structure such that the universal isogeny π_1 restricted to B_0 is the contragredient isogeny of $A_{0,\overline{k}} \to A_{0,\overline{k}}/K_{0,\overline{k}}$. In particular, starting with our abelian variety $(A, \mathscr{L})/k$, if k' is an étale extension of k such that all points of K are defined, then fixing an isomorphism $Z(\overline{\ell}) \to K$ over k' yields a k'-point of $\mathscr{T}_{g,n,\ell}$. A k"-point in $\Pi_1^{-1}(A, K)$ then correspond to a theta structure on $(B, \mathscr{M}^{\ell})$ defined over k" such that the contragredient isogeny $\tilde{f} : B \to A$ is given by the pullback of π_1 to B.

The discussions in [LR16, Corollary 3.6, Proposition 3.7], [Rob10, Algorithm 4.4.10]), [CR15, § 4.1], [LR12b] can then be reinterpreted as a way to use Riemann relations to give explicit equations for $\overline{\Pi}_1^{-1}(A, K)$ and $\Pi_1^{-1}(A, K)$.

[2] See [Mum67, Definition p.78] for the definition of these terms.

[3] The irreducible components are defined over $\mathbb{Z}[1/n, \zeta_n]$ since over this ring all points of the level n Heisenberg group $\mathcal{H}(\overline{n})$ are defined.

Step 2. Now let $r = 1$ if ℓ is a square, $r = 2$ if ℓ is a sum of two squares and $r = 4$ otherwise (the reason of our choice of r will appear in Step 3). On $\mathscr{A}_{g,\ell n}$ the Segre embedding yields a map $\pi_2 : \mathscr{A}_{g,1} \to \mathscr{A}_{rg,\ell n}$, which sends the universal abelian variety $\mathscr{X}_{g,\ell n}$ to $\mathscr{X}^r_{g,\ell n}$ with its product theta structure [Mum66, Lemma 1, p. 323]. Concretely,

$$\pi_2^*(\theta^{\mathscr{X}_{rg,\ell n}}_{i_1,\dots,i_r}) = \theta^{\mathscr{X}_{g,\ell n}}_{i_1} \cdot \dots \cdot \theta^{\mathscr{X}_{g,\ell n}}_{i_r} \tag{5}$$

In particular, π_2 sends the theta null point of level ℓn of $(B, \mathscr{M}^\ell)$ to the theta null point of $(B^r, \mathscr{M}^\ell \star \dots \star \mathscr{M}^\ell)$ [4].

Step 3. Let F be an $r \times r$ matrix with integral coefficients such that ${}^tFF = \ell\mathrm{Id}$ (see Remark 4.1). Then the Koizumi-Kempf formula [Koi76; Kem89] yields a map $\pi_3 : \mathscr{A}_{rg,\ell n} \to \mathscr{A}_{rg,n}$ which corresponds to the isogeny $F : \mathscr{X}^r_{g,\ell n} \to \mathscr{X}^r_{g,\ell n}$ along with the descent of product theta structure from level ℓn to level n. The formula is given, for $(i_1, \dots, i_r) \in Z(\overline{n})^r$, by

$$\pi_3^*(\theta^{\mathscr{X}_{rg,n}}_{i_1,\dots,i_g}) = F^*(\theta^{\mathscr{X}_{g,n}}_{i_1} \cdot \dots \cdot \theta^{\mathscr{X}_{g,n}}_{i_r}) = \sum_{\substack{(j_1,\dots,j_r) \in Z(\overline{\ell n})^r \\ F(j_1,\dots,j_r) = (i_1,\dots,i_r)}} \theta^{\mathscr{X}_{g,\ell n}}_{j_1} \cdot \dots \cdot \theta^{\mathscr{X}_{g,\ell n}}_{j_r}. \tag{6}$$

Since Eq. (6) is homogeneous, this is well defined for projective coordinates.

In particular, π_3 uses F to send $(B^r, \mathscr{M}^\ell \star \dots \star \mathscr{M}^\ell)$ to $(B^r, \mathscr{M} \star \dots \star \mathscr{M})$, from which $(B, \mathscr{M})$ can be recovered by projecting to one of the factor.

The *isogeny formula* is then the composition $\pi_3 \circ \pi_2 \circ \Pi_1^{-1}$.

Theorem 4.2. *Let n be an even integer greater or equal to 4 and ℓ be an integer prime to n. The image of $\Pi_1 \times \pi_3 \circ \pi_2 : \mathscr{A}_{g,\ell n} \to \mathscr{T}_{g,n,\ell} \times \mathscr{A}_{g,n}$ induces a modular correspondence defined over $\mathbb{Z}[\frac{1}{\ell n}]$.*

Let k be a field of characteristic prime to ℓn. If (A, K) is a k-point of $\mathscr{T}_{g,n,\ell}$, then $\pi_3 \circ \pi_2 \circ \Pi_1^{-1}(A, K)$ only has a single $\overline{k}$-point (with multiplicity ℓ^g and which is actually defined over k), corresponding to A/K.

This point can be computed in $O(\ell^{g \max(1, r/2)})$ operations in k where, by assumption, k contains the field of definition of the geometric points of K.

Proof. The first part follows from the steps above. For the statement over a field k, by construction, each geometric point in $\Pi_1^{-1}(A, K)$ corresponds to $B = A/K$ with a level ℓn structure compatible with the level n structure on A. Descending the product level ℓn structure via F then induce the same level n structure on B.

For the complexity estimate, writing equations for Π_1^{-1} is in $O(\ell^g)$ operations, the Segre embedding only depends on n so is absorbed by the big O notation, and computing π_3 requires $O(\ell^{r/2})$ operations, hence the total complexity. We refer to [CR15] for more details. □

4.3. **Modular interpretation.** Consider again the algorithm from Theorem 4.2 but suppose now that we would like to apply it to an affine lift of a theta null point of $(A, \mathscr{L}, \Theta_{\mathscr{L}})$. Notice that the choice of an affine lift is induced by the choice of a trivialization of $\mathscr{L}$ since the θ^A_i are sections of a power of $\mathscr{L}$. Since π_1, π_2 and π_3 are well defined as affine morphisms (using the exact same equations), we can also interpret the isogeny formula $\pi_3 \circ \pi_2 \circ \Pi_1^{-1}$ as an *affine isogeny formula*, yielding an affine lift of the theta null point of $B = A/K$.

In this section, we want to achieve two goals: give the precise relation between affine lifts on A and B through the affine isogeny formula (Theorem 4.5) and also show that we can compute Siegel modular forms constructed as polynomials in the theta constants.

For both purposes, we will need modularity and we therefore start with some classical notions on Siegel modular forms (see for instance [Cha86; DM69; FC90; BGH+08]). As before, let $g \geq 1$, n even and greater or equal to 4. Let $\pi : \mathscr{X}_{g,n} \to \mathscr{A}_{g,n}$ be the universal abelian variety with a totally symmetric normalized relatively ample line bundle and a symmetric theta structure of level n over $\mathbb{Z}[\frac{1}{n}]$ and $s : \mathscr{A}_{g,n} \to \mathscr{X}_{g,n}$ be the zero section. We denote $\mathcal{H} = \wedge^g(s^*\Omega_{\mathscr{X}_{g,n}}) = \wedge^g(\pi_*\Omega_{\mathscr{X}_{g,n}})$ the Hodge line bundle.

[4] If $\mathscr{L}_1$ is a line bundle on A_1 and $\mathscr{L}_2$ is a line bundle on A_2 we use the notation $\mathscr{L}_1 \star \mathscr{L}_2$ to denote the line bundle $p_1^*\mathscr{L}_1 \otimes p_2^*\mathscr{L}_2$ where p_i is the projection $A_1 \times A_2 \to A_i$.

Let R be a commutative ring with all residue fields k of characteristic $p = 0$ or prime to n. Recall that a (scalar) Siegel modular form χ of integral weight $\rho \geq 1$ and level n [5] over R is a section of $\mathcal{H}^\rho$ on $\mathscr{A}_{g,n} \otimes R$ [6]. For a given $(A, \mathscr{L}, \Theta_{\mathscr{L}}) \in \mathscr{A}_{g,n}(k)$ and w_A a basis of k-rational regular differentials on A, it can also be seen as a function $\chi : (A, \mathscr{L}, \Theta_{\mathscr{L}}, w_A) \mapsto k$, such that $\chi(A, \mathscr{L}, \Theta_{\mathscr{L}}, \lambda w_A) = (\det \lambda)^\rho \cdot \chi(A, \mathscr{L}, \Theta_{\mathscr{L}}, w_A)$ for any $\lambda \in \mathrm{GL}_g(\overline{k})$. Likewise, a Siegel modular form χ of weight ρ and level 1 [7] is a section of $\mathcal{H}^\rho$ on the algebraic stack $\mathscr{A}_{g,1}$ of principally polarized abelian schemes. In that case, we simply write $\chi(A, \mathscr{L}, w_A)$.

Let $\mathscr{L}_{\mathscr{X}_{g,n}}$ be the totally symmetric normalized relatively ample line bundle on $\mathscr{X}_{g,n}$ as in Section 4.2. Let $\iota : \operatorname{Spec} k \to \mathscr{A}_{g,n} \xrightarrow{s} \mathscr{X}_{g,n}$ corresponding to a closed point $(A, \mathscr{L}, \Theta_A) \in \mathscr{A}_{g,n}(k)$. We have that $\iota^* \theta^{\mathscr{X}_{g,n}}(0) = \theta^A(0)$, as projective coordinates. In the special case where $k = \mathbb{C}$, let Ω be a Riemann matrix in the Siegel upper half-space $\mathbb{H}_g$ and let us denote $\vartheta \left[\begin{smallmatrix} x_1 \\ x_2 \end{smallmatrix}\right](0, \Omega)$, the value at 0 of the classical theta function with characteristic $(x_1, x_2) \in \mathbb{Q}^{2g}$ [Mum07a, p.192]. We will refer to these complex values as *theta constants* (in contrast with the theta coordinates when speaking about the $\theta_i^A(0)$). Following [Mum07c, Prop. 5.11] (see also loc. cit. Definition. 5.8 and p. 36), if $(A, \mathscr{L}, \Theta_A) = \mathbb{C}^g/(\mathbb{Z}^g + \Omega\mathbb{Z}^g)$, with its associated polarization induced by $\mathrm{Im}\Omega^{-1}$ and associated canonical symmetric level structure induced by the canonical symplectic basis on the lattice, then $(\theta_i^A(0))_{i \in Z(\overline{n})}$ is projectively equal to $(\vartheta \left[\begin{smallmatrix} 0 \\ i/n \end{smallmatrix}\right](0, \Omega/n))$ for arbitrary lifts of $i \in Z(\overline{n})$ to $\mathbb{Z}^g$. In fact Mumford shows this equality for the adically defined theta functions. For the level n algebraic theta functions, it suffices to remark that both the algebraic $\theta_i(z)$ and analytic $\vartheta \left[\begin{smallmatrix} 0 \\ i/n \end{smallmatrix}\right](z, \Omega/n)$ theta functions satisfy the canonical irreducible representation of the Heisenberg group of level n [Mum66, Theorem 2 and definition p. 297].

We will use this projective equality to fix a particular choice of affine lifts over any field in the following way. Because of the transformation formula [Mum07a, Cor.5.11], if we define for any $i, j \in Z(\overline{n})$,

$$\chi_{ij}(A, \mathscr{L}, \Theta_A, (2i\pi dz_1, \ldots, 2i\pi dz_g)) = \vartheta \left[\begin{smallmatrix} 0 \\ i/n \end{smallmatrix}\right](0, \Omega/n) \cdot \vartheta \left[\begin{smallmatrix} 0 \\ j/n \end{smallmatrix}\right](0, \Omega/n) \tag{7}$$

we get Siegel modular forms of weight 1 and level n over $\mathbb{C}$. Since the Fourier coefficients of the theta constants belong to $\mathbb{Z}$, by the q-expansion principle [FC90, p.140], this definition can be extended to a section of $\mathcal{H}$ over $\mathbb{Z}[\frac{1}{n}]$ and therefore over R. Since the sections $(\chi_{ij})_{i,j \in Z(\overline{n})}$ and $(\theta_i^{\mathscr{X}_{g,n}}(0)\theta_j^{\mathscr{X}_{g,n}}(0))_{i,j \in Z(\overline{n})}$ are equal up to a constant over $\mathbb{C}$, for any $(A, \mathscr{L}, \Theta_A) \in \mathscr{X}_{g,n}(k)$ and w_A a basis of k-rational regular differentials on A, $\chi_{ij}(A, \mathscr{L}, \Theta_A, w_A)$ is an affine lift of $\theta_i^A(0) \cdot \theta_j^A(0)$. This allows the following definition.

Definition 4.3. Let $(A, \mathscr{L}, \Theta_{\mathscr{L}}) \in \mathscr{A}_{g,n}(k)$ and w_A a basis of regular differentials on A. A *modular lift*, denoted $\theta^A(0, \sqrt{w_A}) = (\theta_i^A(0, \sqrt{w_A}))_{i \in Z(\overline{n})}$, is an affine lift of $\theta^A(0)$ such that for all $i, j \in Z(\overline{n})$, $\theta_i^A(0, \sqrt{w_A}) \cdot \theta_j^A(0, \sqrt{w_A}) = \chi_{ij}(A, \mathscr{L}, \Theta_{\mathscr{L}}, w_A)$. Notice that the modular lift is unique up to a common sign.

Remark 4.4. We consider the two by two products because they give modular forms of weight one. The $\theta^A(0, \sqrt{w_A})$ themselves would be modular forms of weight one half. But the line bundle $\mathscr{L}_{\mathscr{A}_{g,n}}$ does not descend on $\mathscr{A}_{g,1}$, only to a μ_2-gerbe of $\mathscr{A}_{g,1}$ [Can16]. Since we only need to compute modular forms of integral weight, this *ad hoc* definition is sufficient and requires less abstract material. Notice also that as a consequence of [Mum67, p. 82] and [Can16, Th. 4.2.1], $\mathscr{L}^2_{\mathscr{A}_{g,n}} \simeq \mathcal{H}$, which gives another purely algebraic proof of the modularity of $s^*(\theta_i^{\mathscr{X}_{g,n}} \cdot \theta_j^{\mathscr{X}_{g,n}})$. In particular, a choice of basis of regular differentials gives a trivialization of $\mathcal{H}$, so a trivialization of $\mathscr{L}^2_{\mathscr{A}_{g,n}}$ and corresponding affine lifts for the χ_{ij}.

If we start with a principally polarized abelian variety $(A, \mathscr{L})$ over a field k with a k-rational basis of regular differentials w_A, we may need to go to an extension to build the level n structure $\Theta_{\mathscr{L}}$ on A. Hence the $\theta_i^A(0, \sqrt{w_A})$ are not necessarily defined over k. However, consider a Siegel modular form χ of level 1 and of integral weight $\rho \geq 1$, written as a homogeneous polynomial P of degree 2ρ in the theta constants of level $\Theta_{\mathscr{L}}$ and with coefficients in k. As 2ρ is even, we can express P as polynomial Q in pairs of theta constants, and therefore $P(\theta^A(0, \sqrt{w_A})) = Q((\chi_{ij}(A, \mathscr{L}, \Theta_{\mathscr{L}}, w_A))) = \chi(A, \mathscr{L}, w_A) \in k$. This is important for our application to the modular form χ_{18} in dimension $g = 3$ (see Section 5.2).

[5] Here by level n we mean the level group $\Gamma_g(n, 2n)$ of matrices $\gamma \in \mathrm{Sp}_{2g}(\mathbb{Z})$ such that $\gamma = \begin{bmatrix} A & B \\ C & D \end{bmatrix} \equiv \mathrm{Id} \pmod{n}$ and $2n$ divides the diagonals of B and C.

[6] At least when $g > 1$. When $g = 1$ we also need to check that the modular form stays bounded at infinity, or algebraically that the evaluation on the Tate curve is given by a Laurent series in q with no negative terms.

[7] Meaning the full level group $\Gamma_g = Sp_{2g}(\mathbb{Z})$ and not $\Gamma_1(1, 2)$.

Theorem 4.5. *Let $(A, \mathscr{L}, \Theta_{\mathscr{L}}) \in \mathscr{A}_{g,n}(k)$. Let ℓ be an integer prime to np (or to n if $p = 0$). Let K be a k-rational totally isotropic subgroup for the Weil pairing of $\mathscr{L}^\ell$. Let $f : (A, \mathscr{L}, \Theta_{\mathscr{L}}) \to (B, \mathscr{M}, \Theta_{\mathscr{M}})$ where $B = A/K$, $f^*\mathscr{M} = \mathscr{L}^\ell$ and $\Theta_{\mathscr{M}}$ be the unique symmetric theta structure of level n on $\mathscr{M}$ compatible with $\Theta_{\mathscr{L}}$. Let w_A be a basis of k-rational regular differentials on A and $(\theta_i^A(0, \sqrt{w_A}))_{i \in Z(\overline{n})}$ be a modular lift. Finally, let $r = 1, 2$ or 4 depending on ℓ being a square, a sum of two square or not. Then the affine isogeny formula $\pi_3 \circ \pi_2 \circ \Pi_1^{-1}$ yields the products $(\theta_{i_1}^B(0, \sqrt{w_B}) \times \cdots \times \theta_{i_r}^B(0, \sqrt{w_B}))_{i_1, \ldots, i_r \in Z(\overline{n})}$ where w_B is such that $f^* w_B = w_A$. Note that the product is uniquely defined except if $r = 1$ in which case we get all constants up to a common sign.*

Proof. Using the results of Section 4.2, the statement of this theorem makes sense over $\mathbb{Z}[\frac{1}{n\ell}]$. We will thus prove this theorem for $\mathscr{X}_{g,n} \to \mathscr{A}_{g,n}$ over $\mathbb{Z}[\frac{1}{n\ell}]$, the result will then be valid for any field of characteristic prime to $n\ell$.

We note that the theta coordinates computed by the isogeny formula give sections of the very ample line bundle $\mathscr{L}_{\mathscr{A}_{rg,n}}$ of $\mathscr{A}_{rg,n}$ over B^r. Thus the s_i can also be interpreted as sections of $\mathscr{L}^r_{\mathscr{A}_{g,n}}$ over B. We are thus trying to prove the equality of two sections of $\mathscr{L}^r_{\mathscr{A}_{g,n}}$, i.e. that for any $i_1, \ldots, i_r$ the corresponding theta null point of coordinates $(i_1, \ldots, i_r)$ computed by the isogeny formula is equal to $(\theta_{i_1}^B(0, \sqrt{w_B}) \cdots \theta_{i_r}^B(0, \sqrt{w_B}))$.

Since $\mathscr{A}_{g,n}$ is smooth, $\mathscr{L}_{\mathscr{A}_{g,n}}$ is without torsion, so we only need to check this equality over $\mathbb{C}$. The abelian variety $A/\mathbb{C}$ is isomorphic to a torus $A \simeq \mathbb{C}^g/(\mathbb{Z}^g \oplus \Omega\mathbb{Z}^g)$. First it is easy to check that if we change our affine lift by multiplying it by $\lambda \in \mathbb{C}$, then the result of the isogeny formula is multiplied by λ^r. Indeed in Step 1 (in affine coordinates), the affine lift of the points of K are normalized with respect to the affine lifts of the theta null point. Multiplying the theta null point by λ multiply the points $Q \in \Pi_1^{-1}(A, K)$ by λ. Then applying the Segre embedding multiply the theta null point by λ^r, and Koizumi's formula does not change this constant.

Changing the basis of regular differentials by a matrix $M \in \mathrm{GL}_g(\mathbb{C})$ changes the value of a modular lift by $\lambda = \sqrt{\det(M)}$ for a fixed choice of the square root, since their pair products are weight 1 modular forms. This changes both the modular forms $(\theta_{i_1}^B(0, \sqrt{w_B}) \cdots \theta_{i_r}^B(0, \sqrt{w_B}))$ and the result of the isogeny formula by a factor λ^r. So we may fix the differentials on A to be $w_A = (2i\pi dz_1, \ldots, 2i\pi dz_g)$ of $\mathbb{C}^g$.

By Eq. (7), the corresponding modular lift of the theta null point on A is then given by the analytic theta constants $\theta_i^A = \vartheta \left[\begin{smallmatrix} 0 \\ i/n \end{smallmatrix}\right](0, \Omega/n)$ (where we do a slight abuse of notations in identifying $i \in Z(\overline{n})$ to a fixed lift to $\mathbb{Z}^g$).

We can then keep track of the constants in each of the three steps of the isogeny formula of Section 4.2.

Step 1: we compute an affine lift of a theta null point of level ℓn on B, such that the isogeny theorem applied to $\tilde{f}$ gives our theta null point on A. From our hypothesis, K corresponds to the subgroup $\frac{1}{\ell}\mathbb{Z}^g/\mathbb{Z}^g$, so $B = \mathbb{C}^g/(\mathbb{Z}^g \oplus \ell\Omega\mathbb{Z}^g)$ and $f : z \mapsto \ell z$. The contragredient isogeny $\tilde{f} : B \to A$ is then given by $\tilde{f} : B \to A, z \mapsto z$. So we see that one possible lift for the theta null point of level ℓn on B is given by $\vartheta \left[\begin{smallmatrix} 0 \\ \frac{i}{\ell n} \end{smallmatrix}\right](0, \frac{\ell\Omega}{\ell n})$. By plugging any i divisible by ℓ we see that the constant involved in Step 1 is 1. Indeed, the isogeny theorem (the pullback $\tilde{f}$ of π_1 to B) is simply given in terms of analytic theta coordinates by

$$\left(\vartheta \left[\begin{smallmatrix} 0 \\ \frac{i}{\ell n} \end{smallmatrix}\right](z, \frac{\ell\Omega}{\ell n})\right)_{i \in Z(\overline{\ell n})} \mapsto \left(\vartheta \left[\begin{smallmatrix} 0 \\ \frac{i}{\ell n} \end{smallmatrix}\right](z, \frac{\Omega}{n})\right)_{i \in Z(\overline{\ell n}), \ell | i} = \left(\vartheta \left[\begin{smallmatrix} 0 \\ \frac{i}{n} \end{smallmatrix}\right](z, \frac{\Omega}{n})\right)_{i \in Z(\overline{n})}.$$

Algebraically, this means that we are computing $(\theta_i^{B, \mathscr{M}^\ell}(0, \sqrt{w'_B}))_{i \in Z(\overline{\ell n})}$ where w'_B is such that $\tilde{f}^* w_A = w'_B$. By definition of the contragredient isogeny, we have that $w'_B = w_B/\ell$ (as seen analytically by the fact that the map f above acts by ℓ on the tangent space).

Step 2: the Segre embedding simply consists on taking the sections induced by the basis of regular differentials on B^r given by the pullbacks of the differentials w'_B by the projections on each factor. Notice that the theta constants on B^r are then easily related to the ones on B since $\vartheta \left[\begin{smallmatrix} 0 & 0 \\ b_1 & b_2 \end{smallmatrix}\right](0, \ell\mathrm{diag}(\Omega, \Omega)) = \vartheta \left[\begin{smallmatrix} 0 \\ b_1 \end{smallmatrix}\right](0, \ell\Omega)\vartheta \left[\begin{smallmatrix} 0 \\ b_2 \end{smallmatrix}\right](0, \ell\Omega)$.

Step 3: For this step, we need a version of Equation (6) taking into account the possible multiplicative constant. This is given for instance in [Cos11, Théorème 7.2.1]

$$c \cdot \vartheta \left[\begin{smallmatrix} 0 \\ i_1 \end{smallmatrix}\right](Y_1, \ell\Omega/n) \cdots \vartheta \left[\begin{smallmatrix} 0 \\ i_r \end{smallmatrix}\right](Y_r, \ell\Omega/n) = \sum_{[t_1, \ldots, t_r] \in \mathrm{Mat}_{r \times g}(\mathbb{Z})F^{-1}/\mathrm{Mat}_{r \times g}(\mathbb{Z})} \vartheta \left[\begin{smallmatrix} 0 \\ j_1 \end{smallmatrix}\right](X_1 + t_1, \Omega/n) \cdots \vartheta \left[\begin{smallmatrix} 0 \\ j_r \end{smallmatrix}\right](X_r + t_r, \Omega/n), \tag{8}$$

where $F \in M_r(\mathbb{Z})$ is such that ${}^tFF = \ell\mathrm{Id}$, Y in $(\mathbb{C}^g)^r$, $X = YF^{-1} \in (\mathbb{C}^g)^r$, $i \in \mathbb{Q}^r$, $j = iF^{-1}$ and

$$c = [\mathrm{Mat}_{r\times g}(\mathbb{Z})F^{-1} : \mathrm{Mat}_{r\times g}(\mathbb{Z})] = [\mathrm{Mat}_{r\times g}(\mathbb{Z}) : \mathrm{Mat}_{r\times g}(\mathbb{Z})F] = \ell^{gr/2}.$$

Taking into account that $F^{-1} = \frac{1}{\ell}\,{}^tF$, that the kernel of F in $Z(\overline{\ell})^r$ is exactly the image of ${}^tF$, and taking $Y_i = 0$, we can rewrite Eq. (8) in terms of modular lifts

$$c \cdot \theta^{B,\mathscr{M}}_{i_1}(0, \sqrt{w'_B}) \cdots \theta^{B,\mathscr{M}}_{i_r}(0, \sqrt{w'_B}) = \sum_{\substack{(j_1,\dots,j_r)\in Z(\overline{\ell}n)^r \\ F(j_1,\dots,j_r)=(i_1,\dots,i_r)}} \theta^{B,\mathscr{M}^\ell}_{j_1}(0, \sqrt{w'_B}) \cdots \theta^{B,\mathscr{M}^\ell}_{j_r}(0, \sqrt{w'_B}).$$

Since $w'_B = w_B/\ell$ we have $\theta^B(0, \sqrt{w'_B}) = \ell^{-1/2} \cdot \theta^B(0, \sqrt{w_B})$. This kills the constant c and we get the result (up to a fixed sign if $r = 1$ because there is no way to choose a canonical square root of ℓ in a field k in general). □

This theorem shows that, given a Siegel modular form χ of *even* weight as a polynomial P in the theta constants with coefficients in k, we can compute the value $\chi(B, \mathscr{M}, \Theta_B, w_B)$ from the corresponding modular lift on $(A, \mathscr{L})$. In practice [BCR10] does not compute all products $(\theta^B_{i_1}(0, \sqrt{w_B}) \cdot \dots \cdot \theta^B_{i_r}(0, \sqrt{w_B}))_{i\in Z(\overline{n})}$ but only the products $t_i := (\theta^B_i(0, \sqrt{w_B}) \cdot \theta^B_0(0, \sqrt{w_B}) \cdot \dots \cdot \theta^B_0(0, \sqrt{w_B}))_{i\in Z(\overline{n})}$, since this is enough for isogenies. It is also enough in our case: the weight being even means that each monomials of P in the theta constants has a degree multiple of 4 (and hence of r). We then get

$$\chi(B, \mathscr{M}, \Theta_{\mathscr{M}}, w_B) = P(\theta^B_i(0, \sqrt{w_B})) = t_0^{-\frac{(r-1)\rho}{r}} \cdot P(t_i).$$

The modular forms we will consider are written as polynomials in the theta constants with half characteristics and not in the algebraic theta of level 4. However it is easy to convert one into the other: see Remark 4.7

4.4. **An algebraic version of Thomae's formula.** If $E : y^2 = F(x)$ is an elliptic curve defined over k, we would like to compute the modular lift of the theta null point of level 4 with respect to the k-rational differential $w = dx/y$. Over $k \subset \mathbb{C}$, the expression of the fourth powers of theta constants can be seen as an elementary case of Thomae's formula [Mum07b, p.121] for hyperelliptic curves (although a sign remains unspecified). For dimension 1, one could also use σ functions as in [Akh90, p.55], but one still only gets expression for the fourth powers of the theta constants. We will reprove these formulas in the following lemma and show that one can take arbitrary fourth roots. This will be useful for the computation of Siegel modular forms of even weight at $(B, \mathscr{M}, w_B)$ in the isogeny class of E^g.

Lemma 4.6 (Analytic form of Thomae's formula)**.** *Let E be an elliptic curve with Weierstrass equation $y^2 = F(x)$ defined over over $\mathbb{C}$. Let e_1, e_2, e_3 be the roots of F. Fix arbitrarily three fourth roots a_1, a_2, a_3 of $e_i - e_j$ for $(i, j) \in ((2, 3), (1, 2), (1, 3))$. There exists a basis δ_1, δ_2 of $H_1(E, \mathbb{Z})$ such that if we denote $[\omega_1, \omega_2] = [\int_{\delta_1} dx/y, \int_{\delta_2} dx/y]$ then $\tau = \omega_2/\omega_1 \in \mathbb{H}_1$ and*

$$\sqrt{c} \cdot \vartheta \left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right](\tau) = a_3, \quad \sqrt{c} \cdot \vartheta \left[\begin{smallmatrix} 1/2 \\ 0 \end{smallmatrix}\right](\tau) = a_2, \quad \sqrt{c} \cdot \vartheta \left[\begin{smallmatrix} 0 \\ 1/2 \end{smallmatrix}\right](\tau) = a_1$$

with $c = \frac{2i\pi}{w_1}$ for an arbitrary fixed square root of c.

Proof. Let $\tau \in \mathbb{H}_1$ and denote

$$\vartheta_{00}(z) = \vartheta \left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right](z, \tau),\ \vartheta_{10}(z) = \vartheta \left[\begin{smallmatrix} 1/2 \\ 0 \end{smallmatrix}\right](z, \tau),\ \vartheta_{01}(z) = \vartheta \left[\begin{smallmatrix} 0 \\ 1/2 \end{smallmatrix}\right](z, \tau),$$

and $\vartheta_{11}(z) = \vartheta \left[\begin{smallmatrix} 1/2 \\ 1/2 \end{smallmatrix}\right](z, \tau)$. When z does not appear, it denotes the corresponding value at $z = 0$. As in [FK01, p.125], let us consider the map $\phi : \mathbb{C} \to \mathbb{P}^2$ given by

$$(\vartheta^2_{00}(z)\vartheta_{11}(z) : \vartheta_{00}(z)\vartheta_{01}(z)\vartheta_{10}(z) : \vartheta^3_{11}(z)).$$

Using the divisors of these sections, one can prove that the image by ϕ of $\mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z})$ is the elliptic curve

$$E_2 : Y_2^2 Z_2 = X_2(\beta X_2 - \alpha Z_2)(\alpha X_2 + \beta Z_2)$$

where $\alpha = \vartheta^2_{10}\vartheta^2_{00}$ and $\beta = \vartheta^2_{01}\vartheta^2_{00}$. Letting $Y_2 = Y_1\vartheta_{10}\vartheta_{01}/\vartheta^2_{00}, X_2 = X_1$ and $Z_2 = Z_1$, we can transform further in

$$E_1 : Y_1^2 Z_1 = X_1(X_1 - \alpha/\beta Z_1)(X_1 + \beta/\alpha Z_1).$$

Then letting $Z_1 = (\vartheta_{01}^2\vartheta_{10}^2)Z_0$ and finally $Y_1 = Y_0/(\vartheta_{01}\vartheta_{10})$ and $X_1 = X_0$ one gets

$$E_0 : Y_0^2 Z_0 = X_0(X_0 - \vartheta_{10}^4(0)Z_0)(X_0 + \vartheta_{01}^4(0)Z_0)$$

Let us study the regular differential $w_0 = d(X_0/Z_0)/(Y_0/Z_0) = \frac{1}{\vartheta_{00}^2} \cdot d(X_2/Z_2)/(Y_2/Z_2)$ on E_0. Since $w_2 = d(X_2/Z_2)/(Y_2/Z_2)$ is regular, $\phi^*(w_2)$ is a constant multiple of dz. Now

$$\begin{aligned}
\phi^* w_2 &= 2 \cdot \frac{\vartheta_{00}(z)'\vartheta_{11}(z) - \vartheta_{11}(z)'\vartheta_{00}(z)}{\vartheta_{10}(z)\vartheta_{01}(z)} \\
&= -2\frac{\vartheta'_{11}(0)\vartheta_{00}(0)}{\vartheta_{10}(0)\vartheta_{01}(0)} && \text{(evaluating at } z = 0) \\
&= 2\pi\frac{\vartheta_{00}\vartheta_{10}\vartheta_{01}\vartheta_{00}}{\vartheta_{10}\vartheta_{01}} && \text{(Jacobi identity } \vartheta'_{11} = -\pi\vartheta_{00}\vartheta_{01}\vartheta_{10}) \\
&= 2\pi\vartheta_{00}^2.
\end{aligned}$$

Hence if $\psi_0 : \mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z}) \to E_0$ is the isomorphism composed from ϕ and the changes of variables we get that $\psi_0^* w_0 = 2\pi dz$ (notice that this is not the natural $2i\pi dz$ we chose before but we will take care of the extra factor i when we choose the fourth root).

Now, let us start with $E : y^2 = F(x)$. If we make the change of variable $X = x - e_2$, $Y = y$, then we get $E' : Y^2 = X(X - (e_1 - e_2)Z)(X + (e_2 - e_3)Z)$. If we integrate $w = d(X/Z)/(Y/Z)$ along a basis of the homology of E', we get a torus $\mathbb{C}/(\omega_1\mathbb{Z} + \omega_2\mathbb{Z})$ and up to a change of the order in the basis, we can assume that $\tau = \omega_2/\omega_1 \in \mathbb{H}_1$ and $\psi : \mathbb{C}/(\omega_1\mathbb{Z} + \omega_2\mathbb{Z}) \to E'$ an isomorphism such that $\psi^* w = dz$. Let $s : \mathbb{C}/(\omega_1\mathbb{Z} + \omega_2\mathbb{Z}) \xrightarrow{\sim} \mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z})$ such that $z \mapsto z/\omega_1$. The composition

$$\begin{array}{ccc}
\mathbb{C}/(\omega_1\mathbb{Z} + \omega_2\mathbb{Z}) & \xleftarrow{\psi^{-1}} & E' \\
\downarrow{\scriptstyle s} & & \downarrow{\scriptstyle \mu} \\
\mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z}) & \xrightarrow[\psi_0]{} & E_0
\end{array}$$

defines an isomorphism $\mu : E' \to E_0$ such that $(X : Y : Z) \to (a^2X : a^3Y : Z)$ with $a \in \mathbb{C}^*$. After a possible change in the generators of the homology of E' (by a lift to $\mathrm{SL}_2(\mathbb{Z})$ of a change of basis of $E'[2]$), we can even assume that μ maps the roots 0 to 0, $e_1 - e_2$ to ϑ_{10}^4/a^2 and $e_2 - e_3$ to ϑ_{01}^4/a^2. Note that $e_1 - e_3 = (\vartheta_{10}^4 + \vartheta_{01}^4)/a^2 = \vartheta_{00}^4/a^2$. Now $\mu^* w_0 = w/a = (\psi^{-1})^* \circ s^* \circ \psi_0^*\, w_0 = 2\pi/\omega_1 \cdot w$. Hence $a = \omega_1/2\pi$. This means that we have the equalities

$$a_2^4 = e_1 - e_2 = -c^2\vartheta_{10}^4, \quad a_1^4 = e_2 - e_3 = -c^2\vartheta_{01}, \quad a_3^4 = e_1 - e_3 = -c^2\vartheta_{00}.$$

To conclude, we must show that we can choose the basis of homology for E in order to choose the fourth root of unity arbitrarily and get the correct result up to a common fourth root of unity. As the two-torsion points are now fixed, this boils down to find some matrices in $\mathrm{SL}_2(\mathbb{Z})$ which are congruent to the identity modulo 2. If we call $S = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $T = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, let $H =< S^2, T^2, (ST)^3, (STS)^2 >$ and $(\alpha_1, \alpha_2, \alpha_3) = (i\sqrt{c}\vartheta_{01}, i\sqrt{c}\vartheta_{10}, i\sqrt{c}\vartheta_{00})$. Notice that the α_is do depend on τ but also on ω_1. The actions of S and T on the lattice induce actions on the α_i which can be computed through the classical transformation formula [Mum07a, Th.7.1]. Namely

$$\left\{\begin{array}{lcl} S.\alpha_1 &=& \alpha_3, \\ S.\alpha_2 &=& e^{i\pi/4}\alpha_2, \\ S.\alpha_3 &=& \alpha_1, \end{array}\right. \text{ and } \left\{\begin{array}{lcl} T.\alpha_1 &=& \sqrt{-i}\alpha_2, \\ T.\alpha_2 &=& \sqrt{-i}\alpha_1, \\ T.\alpha_3 &=& \sqrt{-i}\alpha_3. \end{array}\right.$$

Hence we get

$$\left\{\begin{array}{lcl} S^2.\alpha_1 &=& \alpha_1, \\ S^2.\alpha_2 &=& i\alpha_2, \\ S^2.\alpha_3 &=& \alpha_3, \end{array}\right. , \left\{\begin{array}{lcl} T^2.\alpha_1 &=& -i\alpha_1, \\ T^2.\alpha_2 &=& -i\alpha_2, \\ T^2.\alpha_3 &=& -i\alpha_3, \end{array}\right.$$

and

$$\left\{\begin{array}{lcl}(ST)^3.\alpha_1 &=& i\alpha_1,\\ (ST)^3.\alpha_2 &=& i\alpha_2,\\ (ST)^3.\alpha_3 &=& i\alpha_3,\end{array}\right. , \quad \left\{\begin{array}{lcl}(STS)^2.\alpha_1 &=& -i\alpha_1,\\ (STS)^2.\alpha_2 &=& -\alpha_2,\\ (STS)^2.\alpha_3 &=& -\alpha_3.\end{array}\right.$$

The group μ_4^3 has generators $u_1 := (i,1,1), u_2 := (1,i,1), u_3 := (1,1,i)$. The expressions above show that $g_1 = (ST)^3(STS)^2$ (resp. $g_2 = S^2$, resp. $g_3 = g_1^3 g_2^3 (ST)^3$) acts on $(\alpha_1,\alpha_2,\alpha_3)$ as u_1 (resp. u_2, resp. u_3). Starting from (a_1,a_2,a_3) it is therefore possible to find a τ such that $(a_1,a_2,a_3) = (\sqrt{c}\vartheta_{01}, \sqrt{c}\vartheta_{10}, \sqrt{c}\vartheta_{00})$. □

Remark 4.7. The algebraic theta functions of level 4, $(\theta_1,\theta_2,\theta_3,\theta_4)$ analytically correspond to the theta functions $(\vartheta\left[\begin{smallmatrix}0\\ i/4\end{smallmatrix}\right](z,\Omega/4))_{i\in\mathbb{Z}/4\mathbb{Z}}$. Going to these functions from the standard level $(2,2)$ analytic theta $\vartheta\left[\begin{smallmatrix}a/2\\ b/z\end{smallmatrix}\right](2z,\Omega)$ is given by a change of variables [Mum07a], [Cos11, p. 38]

$$\begin{aligned}\theta_0(z) &= \vartheta\left[\begin{smallmatrix}0\\ 0\end{smallmatrix}\right](z,\Omega) + \vartheta\left[\begin{smallmatrix}1/2\\ 0\end{smallmatrix}\right](z,\Omega), \quad \theta_1(z) = \vartheta\left[\begin{smallmatrix}0\\ 1/2\end{smallmatrix}\right](z,\Omega) + \vartheta\left[\begin{smallmatrix}1/2\\ 1/2\end{smallmatrix}\right](z,\Omega),\\ \theta_2(z) &= \vartheta\left[\begin{smallmatrix}0\\ 0\end{smallmatrix}\right](z,\Omega) - \vartheta\left[\begin{smallmatrix}1/2\\ 0\end{smallmatrix}\right](z,\Omega), \quad \theta_3(z) = \vartheta\left[\begin{smallmatrix}0\\ 1/2\end{smallmatrix}\right](z,\Omega) - \vartheta\left[\begin{smallmatrix}1/2\\ 1/2\end{smallmatrix}\right](z,\Omega),\end{aligned} \tag{9}$$

where $\theta_i(z) = \vartheta\left[\begin{smallmatrix}0\\ i/4\end{smallmatrix}\right](z,\Omega/4)$.

The functions $\vartheta\left[\begin{smallmatrix}a/2\\ b/2\end{smallmatrix}\right](2z,\Omega)$ also have algebraic analogues as partial Fourier transforms over $Z(\overline{2})$ of the functions θ_i as explained in [Mum66, p. 334] and [Rob10, Exemple 4.4.9]. If θ_i is a theta function of level n, the partial Fourier transform is given for $\alpha \in \hat{Z}(\overline{2})$ by

$$\theta\left[\begin{smallmatrix}\alpha\\ i\end{smallmatrix}\right] = \sum_{j\in Z(\overline{2})} \alpha(j)\theta_{i+j}. \tag{10}$$

Analytically, $\theta\left[\begin{smallmatrix}\alpha\\ i\end{smallmatrix}\right](z) = \vartheta\left[\begin{smallmatrix}\alpha/2\\ 2i/n\end{smallmatrix}\right](2z, 2\Omega/n)$, so if $n=4$ we do recover the theta functions of level $(2,2)$.

All these expressions for the theta constants over $\mathbb{C}$ are true over k. Indeed, pairing them will give modular forms with integral Fourier expansion, so we get similar expression for the modular lift, up to a common sign which can be swallowed in the choice of the fourth root.

Corollary 4.8 (Algebraic form of Thomae's formula)**.** *Let E be an elliptic curve with Weierstrass equation $y^2 = F(x)$ defined over a field k of characteristic $p \neq 2$. Let e_1,e_2,e_3 be the roots of F in $\bar{k}$. Fix arbitrarily three fourth roots a_1,a_2,a_3 of $e_i - e_j$ for $(i,j) \in ((2,3),(1,2),(1,3))$. Then there is a level 4 symmetric theta structure on E, such that a modular lift of the theta null point on E with respect to the regular differential dx/y is*

$$\begin{aligned}\theta_0^E(0_E,\sqrt{dx/y}) &= a_2+a_3, \qquad \theta_1^E(0_E,\sqrt{dx/y}) = a_1,\\ \theta_2^E(0_E,\sqrt{dx/y}) &= -a_2+a_3, \qquad \theta_3^E(0_E,\sqrt{dx/y}) = a_1.\end{aligned} \tag{11}$$

Proof. Define $\theta\left[\begin{smallmatrix}0\\ 0\end{smallmatrix}\right](0_E) = a_3, \theta\left[\begin{smallmatrix}1/2\\ 0\end{smallmatrix}\right](0_E) = a_2, \theta\left[\begin{smallmatrix}0\\ 1/2\end{smallmatrix}\right](0_E) = a_1$. First we note that the first part of Lemma 4.6 is valid algebraically: we just need to replace the argument involving divisors by the algebraic Riemann relations instead. Indeed it is easy to check that the theta null point defined satisfy the Riemann relation $\theta\left[\begin{smallmatrix}0\\ 0\end{smallmatrix}\right](0_E)^4 = \theta\left[\begin{smallmatrix}1/2\\ 0\end{smallmatrix}\right](0_E)^4 + \theta\left[\begin{smallmatrix}0\\ 1/2\end{smallmatrix}\right](0_E)^4$ (this is the standard Jacobi relation to which Riemann relations reduce to in genus 1 [Mum66, p. 353]). Since we also have that $\theta\left[\begin{smallmatrix}0\\ 0\end{smallmatrix}\right](0_E)\theta\left[\begin{smallmatrix}1/2\\ 0\end{smallmatrix}\right](0_E)\theta\left[\begin{smallmatrix}0\\ 1/2\end{smallmatrix}\right](0_E) = a_1a_2a_3 \neq 0$, the theta null point we compute is valid projectively by [Mum66, p. 353]. This also proves that each choice of fourth root is valid.[8]

It remains to check that the affine lift given by Eq. (11) corresponds to the trivialization coming from the differential $w = dx/y$. Since the construction is valid over the universal elliptic curve with a level 4 symmetric theta structure, whose moduli space is defined over $\mathbb{Z}[1/2]$, by considering the pullback to $\mathbb{C}$ we may assume that E is defined over $\mathbb{C}$, as in the proof of Theorem 4.5. Looking at the proof of Lemma 4.6,

[8] Alternatively, the affine modular action of $\Gamma/\Gamma(4,8)$ induces a projective action [Cos11, Lemme 6.2.1] which holds true algebraically, as automorphisms of the Heisenberg group of level 4. So the same generators g_1, g_2 and g_3 as in the end of Lemma 4.6 acts by fourth-root of unity projectively.

we see that the isomorphism between E and E' does not change the differential w, while the one from E' to E_0 acts by $a = 2\pi/\omega_1$. Correcting for this last factor yields

$$\theta\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](0_E, \sqrt{dx/y}) = a_3, \quad \theta\left[\begin{smallmatrix}1/2\\0\end{smallmatrix}\right](0_E, \sqrt{dx/y}) = a_2, \quad \theta\left[\begin{smallmatrix}0\\1/2\end{smallmatrix}\right](0_E, \sqrt{dx/y}) = a_1. \tag{12}$$

Applying the linear change of variable Eq. (9) to Eq. (12) yields Eq. (11). □

4.5. **Computing a Siegel modular form on the isogenous variety.** Combining Corollary 4.8 with Theorems 4.2 and Theorem 4.5 gives the following theorem and Algorithm 7.

Theorem 4.9. *Let g be a positive integer, $(E_i/k)_{1\leq i\leq g}$ be elliptic curves, K be a k-rational totally isotropic subgroup of $\prod_i E_i$ of order ℓ^g prime to $2p$ (or just prime to 2 if $p = 0$). Let $B = (E_1 \times \cdots \times E_g)/K$ with the principal polarization induced by the product polarization on $E_1 \times \cdots \times E_g$ and let $f : \prod_i E_i \to B$ be the quotient isogeny. Finally define w_B such that $f^* w_B = (p_1^* dx_1/y_1, \ldots, p_g^* dx_g/y_g)$ where $p_i : E_1 \times \cdots \times E_g \to E_i$ is the canonical projection. Let $r = 1, 2$ or 4 depending on ℓ being a square, a sum of two squares or not. Algorithm 7 computes the products $\theta^B_{i_1}(0, \sqrt{w_B}) \cdots \theta^B_{i_r}(0, \sqrt{w_B})$ of any r modular lifts in time $O(\ell^{g \max(1, r/2)})$ operations in the field of definition of the points of K. Given a Siegel modular form χ of even weight as a polynomial P in the theta constants with coefficients in k, Algorithm 7 also computes the value $\chi(B, \mathscr{M}, w_B) \in k$.*

Remark 4.10. We can make several comments about this result.

- Note that during the execution of the algorithm, we only need to take care to compute the modular lift of the theta null point. Indeed, apart from the theta null point, we only need to compute projective coordinates for the points in the kernel, the computation of Π_1^{-1} will take care of normalizing these coordinates with respect to our choice of affine lift of the theta null point.
- We only require χ to be of even weight w if $r = 4$. Otherwise given the r-fold products

$$\theta^B_{i_1}(0, \sqrt{w_B}) \cdots \theta^B_{i_r}(0, \sqrt{w_B})$$

  we can evaluate a modular form of odd weight.
- We do not need to evaluate all the r-fold products, but only the ones of the form

$$t_i = \theta^B_i(0, \sqrt{w_B}) \cdots \theta^B_i(0, \sqrt{w_B})$$

  (provided $\theta^B_0(0, \sqrt{w_B}) \neq 0$). If χ is of weight w, it can then be evaluated as $\chi(B, \mathscr{M}, w_B) = P(t_i)/t_0^{w(r-1)/2}$.
- If the modular form χ that can be written as a polynomial with respect to the level 2 theta constants, we can do the whole isogeny computation in level 2. This gains a factor 2^g in the number of coordinates to compute.

Algorithm 7 Algebraic computation of the theta null point and a Siegel modular form of even weight

Input: Elliptic curves E_i/k with equation $y^2 = (x - e_{1i})(x - e_{2i})(x - e_{3i})$ where k is of characteristic p different from 2, a k-rational totally isotropic subgroup K of $A = \prod_i E_i$ of order ℓ^g prime to $2p$ (or just prime to 2 if $p = 0$). A Siegel modular form χ of even weight as a polynomial P in the theta constants with coefficients in k.

Output: The theta null point of level 4 and the value $\chi(B, \mathscr{M}, w_B)$ where $B = A/K$ with $\mathscr{M}$ the polarization induced by the product polarization on A and w_B such that $f^* w_B = (p_1^* dx_1/y_1, \dots, p_g^* dx_g/y_g)$ where $f : A \to B$ is the quotient isogeny and $p_i : E_1 \times \cdots \times E_g \to E_i$ is the canonical projection.

1: For all $1 \le i \le g$, define $\theta_0'^{E_i} = \sqrt[4]{e_{1i} - e_{3i}}, \theta_1'^{E_i} = \sqrt[4]{e_{1i} - e_{2i}}, \theta_2'^{E_i} = \sqrt[4]{e_{2i} - e_{3i}}$ for arbitrary choices of the roots.

2: Compute $\theta_0^{E_i}(0, \sqrt{dx_i/y_i}) = \theta_0'^{E_i} + \theta_1'^{E_i}$, $\theta_2^{E_i}(0, \sqrt{dx_i/y_i}) = \theta_0'^{E_i} - \theta_1'^{E_i}$ and $\theta_1^{E_i}(0, \sqrt{dx_i/y_i}) = \theta_3^{E_i}(0, \sqrt{dx_i/y_i}) = \theta_2'^{E_i}$ for all $1 \le i \le g$.

3: Compute all $\theta^A_{(i_1,\dots,i_g)}(0, \sqrt{w_A}) = \theta^{E_1}_{i_1}(0, \sqrt{dx_1/y_1}) \cdots \theta^{E_g}_{i_g}(0, \sqrt{dx_n/y_n})$ for all $(i_1, \dots, i_g) \in Z(\overline{4})$.

4: For all $1 \le i \le g$ and for all $x = (x_1, \dots, x_g) \in K \setminus \{0\}$, compute the theta coordinates $\left(\theta_j^{E_i}(x_i)\right)_{j \in \mathbb{Z}/4\mathbb{Z}}$.

5: Compute for all $j = (j_1, \dots, j_g) \in Z(\overline{4})$ and for all $x = (x_1, \dots, x_g) \in K \setminus \{0\}$ $\theta_j^A(x) = \theta_{j_1}^{E_1}(x_1) \cdots \theta_{j_g}^{E_g}(x_g)$.

6: Use the affine version of the isogeny formula to compute $t_i = \theta_i^B(0, \sqrt{w_B}) \cdot \theta_0^B(0, \sqrt{w_B}) \cdots \theta_0^B(0, \sqrt{w_B})$ which is a product of r factors with $r = 1$ if ℓ is a square, $r = 2$ if ℓ is the sum of two positive squares and $r = 4$ otherwise.

7: **return** $(t_i)_{i \in Z(\overline{4})}$ and $t_0^{-\frac{(r-1)\rho}{r}} \cdot P(t_i)$.

5. Application to defect-0 curves of genus at most 4

Let C be a curve of genus $g > 0$ over $\mathbb{F}_q$ with $q = p^m$. The Hasse-Weil-Serre bound asserts that $\#C(\mathbb{F}_q) \le 1 + q + gm$ where $m = \lfloor 2\sqrt{q} \rfloor$. A curve which number of rational points reaches with bound is called a *defect-0 curve*. When $g > 2$, it is not known in general for a given field $\mathbb{F}_q$ whether a defect-0 curve $C/\mathbb{F}_q$ of genus g exists. If it does, $\operatorname{Jac} C$ is isogenous to the g-power of an elliptic curve E with trace $-m$. In order to see if such a curve exists, we therefore start by enumerating the indecomposable principally polarized abelian varieties $(A_i, \mathscr{L}_i)$ of dimension g in the isogeny class of E^g. When m is prime to q and hence E is ordinary, we have seen in Section 3.3 how to describe all of them as a quotients of E^g by given maximal isotropic subgroups $K \subset E[\ell_1] \times \cdots \times E[\ell_g]$. When we can moreover choose $\ell = \ell_1 = \ldots = \ell_g$ odd, prime to the characteristic of $\mathbb{F}_q$ (see the condition in Theorem 2.16) and K totally isotropic, we can use Algorithm 6 to compute the theta null point of level 4 for each $(A_i, \mathscr{L}_i)$.

Now, we need to single out the ones which are Jacobians of curves of genus g over $\mathbb{F}_q$. By [OU73], we know that any indecomposable principally polarized abelian variety $(A, \mathscr{L})$ of dimension $g \le 3$ is the Jacobian of a curve C_0 of genus g over $\bar{\mathbb{F}}_q$. When $g = 4$, this is not the case, but we will be able to distinguished them computing a certain Siegel modular form using Algorithm 7, see Section 5.3. However if $(A, \mathscr{L})$ is a Jacobian of dimension 4 over $\bar{\mathbb{F}}_q$ there is currently no way to check if it is also a Jacobian over $\mathbb{F}_q$. As for $g \le 3$, notice that there is a big difference between the genus 2 and genus 3 case when dealing with the existence of C over $\mathbb{F}_q$. For the genus 2, this is automatic: the existence of an indecomposable principally polarized abelian surface over $\mathbb{F}_q$ in the class of E^2 is enough to ensure the existence of the curve C. For genus 3 curves though, there may be an arithmetic obstruction as we shall recall in Section 5.2. As we shall see this obstruction can be computed from the value of a Siegel modular form.

For $g = 2$ or 3, we can even get an equation for the curve C when it exists. In genus 2, the construction of such a curve from its theta null point is classical and we refer for instance to [CR15] ; in genus 3, the formulae depend on the curve being hyperelliptic or not, which can be distinguished by exactly one of the 36 even theta coordinates being 0 or none. In the hyperelliptic case, one can use [Wen01][9] to construct first a model C_1 over $\bar{\mathbb{F}}_q$. Then one computes Shioda invariants[10] and then reconstruct via [LR12a] when $p > 7$.

[9] [BIL+16] noticed that there are some mistakes in this article of Weng and [LSV21, Appendix] gives a correct implementation (see also [Sij20]). However, we did not try to implement the reconstruction in the genus 3 hyperelliptic case.

[10] or computes them directly from the theta constants using for instance [Lor19] and overpass the difficulties mentioned above.

In the non-hyperelliptic case, one can use Weber's formulae ([Web76, p.108], see also [Fio16]) to get first a curve C_1 over an extension $\mathbb{F}_{q^e}$ of $\mathbb{F}_q$ ($p \neq 2$). To get an equation of C_0 over $\mathbb{F}_q$, we implemented an explicit Galois descent taking advantage of the fact that C_1, being given with its full level-2 structure, has all its bitangents defined over $\mathbb{F}_{q^n}$. Hence, all isomorphisms between C_1 and its Galois conjugates over $\mathbb{F}_e$ are defined over $\mathbb{F}_{q^e}$ as well.

It may still be that $\operatorname{Jac} C_0$ is not isomorphic over $\mathbb{F}_q$ to the chosen $(A, \mathscr{L})$ as C_0 may be a twist of the right curve C. If the geometric automorphism group of C is trivial (which can be read from the automorphism group of the lattice), then the curve has no automorphism, hence no non-trivial twist and $C_0 \simeq C$. Otherwise, one has to compute the list of all twists: in the hyperelliptic case see [LR12a, Sec.4.6] (implemented in `Magma`), and in the non-hyperelliptic case see [LRR+14, Sec.4].

To conclude, it is then enough to check among the twists which ones are defect-0 curves over $\mathbb{F}_q$, which can be achieved through naive point counting algorithms. Hence for $g = 2$ and 3 our algorithms provide an explicit list of all isomorphism classes of defect-0 curves over $\mathbb{F}_q$.

Remark 5.1. A different way to do so is to pick a random $\mathbb{F}_q$-rational divisor $D \in \operatorname{Jac} C'(\mathbb{F}_q)$, and check if $(1+q-\operatorname{Trace}(E))^g D = 0$. A better way would be to select the right Galois descent directly by keeping track of the Galois action on the two torsion points of E^g through the isogeny. This could actually be achieved since a more general isogeny formula exists which can also be applied to an arbitrary torsion point of E^g. We did not implement this method yet.

5.1. **Curves of genus 2.** Let us give some examples to illustrate our algorithms. We start with a very simple one.

Example 5.2. Let $E/\mathbb{F}_{61} : y^2 = x^3 + 11x + 17$ be an elliptic curve such that $R := \mathbb{Z}[\pi] = \mathbb{Z}[w]$ with $w = \frac{1+\sqrt{-19}}{2}$. When $g = 2$, the algorithm developed in Section 2 shows that there is only one indecomposable unimodular positive definite R-lattice of rank 2, namely R^2 with the hermitian form $h = \begin{bmatrix} 2 & -\bar{w} \\ -w & 3 \end{bmatrix}$ (this can alternatively be seen from Schiemann's tables [Sch]). Hence $A = \mathscr{F}_E(R^2) = E^2$ with the polarization $\mathscr{L}$ induced by h is the only Jacobian inside the isogeny class of E^2. Using Algorithm 5 one can check that there is a polarized isogeny f from $A_0 = E^2$ with the product polarization to $(A, \mathscr{L})$ with kernel $K \subset A[\ell]$ with $\ell = 3$. Explicitly K is generated by the two affine points of E^2

$$((51a^3 + 39a^2 + 36a + 13, 59a^3 + 43a^2 + 48a + 35), (3a^3 + 31a^2 + 38a + 4, 44a^3 + 22a^2 + 19a + 11)),$$

$$((58a^3 + 30a^2 + 23a + 36, 14a^3 + 55a^2 + 47a + 45), (51a^3 + 39a^2 + 36a + 13, 2a^3 + 18a^2 + 13a + 26))$$

where $a \in \mathbb{F}_{61^4}$ has minimal polynomial $x^4 + 3x^2 + 40x + 2$. We can also compute the theta null point which we express in the classical basis of theta constants characteristics. For instance $\theta^B_{00}(0) = \vartheta\left[\begin{smallmatrix} 00 \\ 00 \end{smallmatrix}\right](0)$ is equal to

$$43b^{11} + 34b^{10} + 28b^9 + 11b^8 + 6b^7 + 19b^6 + 30b^5 + 27b^4 + 27b^3 + b^2 + 30b + 59$$

where $b \in \mathbb{F}_{61^{12}}$ with minimal polynomial $x^{12} + 2x^8 + 42x^7 + 33x^6 + 8x^5 + 38x^4 + 14x^3 + x^2 + 15x + 2$. Using the reconstruction method explained above, we find $C : y^2 = 45x^6 + 13x^5 + 25x^4 + 23x^3 + 3x^2 + 20x + 13$.

Consider the complex expression $\chi_5(\tau) = \prod_{\epsilon \text{ even}} \vartheta[\epsilon](\tau)$. Then $\chi_{10} = \chi_5^2$ is a Siegel modular form of weight 10 and level Γ_2 defined over $\mathbb{Z}$. Using Algorithm 7, we find that $\chi_{10}(A, \mathscr{L}, w_A) = 22$ where w_A is the basis of differentials constructed in Theorem 4.9. There is a well-known relation with between χ_{10} and the discriminant of $C : y^2 = f(x)$ (which is 2^8 times the discriminant of f) up to the choices of bases of regular differentials. One must have that $\chi_{10}(A, \mathscr{L}, w_A)/(2^{12} \cdot \operatorname{Disc}(C))$ is a 10th power of the determinant of the change of bases, hence a 10th power in $\mathbb{F}_q$. This is indeed the case.

Example 5.3. In a similar way, we can work out an example over $k = \mathbb{F}_{5^3}$ with a non-maximal order of discriminant -2^4. In that case there is a unique defect-0 curve of genus 2 over k, namely $C : y^2 = 3x^6 + 3x^4 + 3x^2 + 3$.

Example 5.4. Let us consider now the case $k = \mathbb{F}_{271}$ with a non-maximal order of discriminant -60. In that case, there are 9 indecomposable principally polarized abelian surfaces in the isogeny class. For only two of them, there exists an odd ℓ ($\ell = 5$) and one can write down the corresponding curves, namely $y^2 = 65x^6 + 167x^5 + 63x^4 + 49x^3 + 63x^2 + 167x + 65$ and $y^2 = 89x^6 + 224x^5 + 155x^4 + 16x^3 + 155x^2 + 224x + 89$.

For the seven other cases, such an ℓ does not exist: Theorem 2.16 shows that either there is no orthogonal basis with the same odd norm for two of them, or no orthogonal basis with the same norm for the last 5 of them.

5.2. **Curves of genus 3.** In his lectures at Harvard in 1985, Serre found that a principally polarized abelian variety $(A, \mathscr{L})$ of dimension $g > 2$ defined over a perfect field k, which is geometrically a Jacobian, is not necessarily a Jacobian over k (unlike in dimension 1 or 2). The obstruction is given by a quadratic character of $\mathrm{Gal}(\bar{k}/k)$ and is called *Serre's obstruction*. This obstruction is always trivial for hyperelliptic curves. When $k \subset \mathbb{C}$ and $g = 3$, this character can be computed in terms of the value of the modular form defined over $\mathbb{C}$ by $\chi_{18}(\tau) = -\frac{1}{2^{28}} \cdot \prod_\epsilon \vartheta[\epsilon](\tau)$, where the product is over the 36 even theta constants ([Ser85], [LR08], [Mea08], [LRZ10]). Using lifting techniques, one can thus get the obstruction for certain $(A, \mathscr{L})$ when k is a finite field of characteristic different from 2 and therefore address the question of maximal number of points of genus 3 curves (see for instance [Rit10]). However, the numerical approximations during the computation of the value of the modular form lead to heuristic results only.

The techniques developed in Section 4.3 allows us to directly work out these computations over an (extension) of the finite field. In [Igu67], it is proved that χ_{18} is a modular form of degree 18 and level 1 and therefore it induces an element of $\Gamma(\mathscr{A}_{3,1}(\mathbb{C}), \mathcal{H}^{18})$. Then [Ich96, Prop.3.4] proved that actually $\chi_{18} \in \Gamma(\mathscr{A}_{3,1}(\mathbb{Z}), \mathcal{H}^{18})$. In [LRZ10, Th.1.3.3], over a number field, and in Proposition [Rit10, Prop.2.3], over a field k of characteristic different from 2, it is proved for a principally polarized abelian threefold $(A, \mathscr{L})/k$ and any choice of k-rational basis of regular differentials w_A on A, that $\chi_{18}(A, \mathscr{L}, w_A)$ is a non-zero square in k if and only if $(A, \mathscr{L})$ is the Jacobian of a non-hyperelliptic curve of genus 3 over k. Using Algorithm 7, we can compute this value and check whether $(A, \mathscr{L})$ is the Jacobian of a non-hyperelliptic genus 3 curve over k without computing the equation of the curve. Note that as we started with $(A, \mathscr{L})/\mathbb{F}_q$ indecomposable, if $\chi_{18}(A, \mathscr{L}, w_A) = 0$, then $(A, \mathscr{L})$ is the Jacobian of a hyperelliptic genus 3 curve over $\mathbb{F}_q$.

Example 5.5 (A unique defect-0 curve without non-trivial automorphism). Let consider the question of the existence of defect-0 curve of genus 3 over $\mathbb{F}_q$ with $q = 10313$. If there is such a curve $C/\mathbb{F}_q$ then $\mathrm{Jac}\, C \sim E^3$ with E of trace $-m = -203$. The curve E has therefore complex multiplication by the maximal order $\mathscr{O} = \mathbb{Z}[\omega]$ of $\mathbb{Q}(\omega)$ where $\omega = \frac{1+\sqrt{-43}}{2}$. As $\mathscr{O}$ has class number 1, there is a unique (non-polarized) abelian variety in the class of E^3 up to isomorphism, namely E^3 itself. Moreover using Algorithm 3 (see also [Sch98]), we find 5 isomorphism classes of indecomposable positive definite unimodular hermitian $\mathscr{O}$-lattices (L, h_i) leading to 5 indecomposable principally polarized abelian threefolds (E^3, a_i). In Table 1, we give h by its Gram matrix in the canonical basis of $\mathscr{O}^3$. For each lattice (L, h_i), we also give the smallest odd ℓ determined by Algorithm 4. Recall that it determines the degree ℓ^3 of the isogeny we will compute using the Algorithm 7. We also display in Table 1 the order of the automorphism group of (L, h_i), and if $\chi := \chi_{18}(E^3, a_i, w_{E^3}) = 0$ or if it is a square in $\mathbb{F}_q$.

We see that only a_1 leads to a non-trivial obstruction and therefore to a non-hyperelliptic defect-0 curve. This result agrees with the heuristic result which can be deduced from [Rit10, Table 2]. An equation of C is

$$\begin{aligned} x^4 \;+\; & 7780x^3y + 8862x^3 + 456x^2y^2 + 2118x^2y + 1846x^2 + 5713xy^3 + 10064xy^2 + 7494xy \\ +\; & 6469x + 7559y^4 + 9490y^3 + 7458y^2 + 214y + 6746 = 0. \end{aligned}$$

Moreover by Torelli theorem [Mat58, p.790-792], since $\mathrm{Aut}(E^3, a_1) \simeq \mathrm{Aut}(L, h_1) \simeq \{\pm 1\}$ and C is non-hyperelliptic, the automorphism group of C is trivial. As far as we know, this is the first example of a finite field for which one can ensure that the defect-0 curves have no extra-automorphism. As recalled in [Rit11], most of the methods developed to find curves of genus 3 with many points use the existence of extra-automorphisms. The question of existence of a defect-0 curve over $\mathbb{F}_{10313}$ could not have been solved in this way.

Example 5.6. Let $q = 131$. As previously, the existence of a defect-0 curve of genus 3 over $\mathbb{F}_q$ leads to consider indecomposable unimodular positive definite $\mathscr{O}$-lattices L_i of rank 3, where $\mathscr{O}$ has discriminant -40. The class number of $\mathscr{O}$ is 2 and we find 12 L_i, out of which 6 are not free and the largest ℓ we have to

Case	Gram matrix of h_i	ℓ	$\#Aut(L,h_i)$	Is $\chi=0$?	Is χ a square?
1	$\begin{pmatrix} 3 & 1 & 1-\overline{\omega} \\ 1 & 4 & 2 \\ 1-w & 2 & 5 \end{pmatrix}$	11	2	no	yes
2	$\begin{pmatrix} 3 & 1+\overline{\omega} & 2-\overline{\omega} \\ 1+w & 5 & -2-\overline{\omega} \\ 2-w & -2-w & 5 \end{pmatrix}$	9	12	no	no
3	$\begin{pmatrix} 2 & -1 & 1 \\ -1 & 4 & 1-\overline{\omega} \\ 1 & 1-w & 4 \end{pmatrix}$	9	4	no	no
4	$\begin{pmatrix} 3 & 1 & -1-\overline{\omega} \\ 1 & 3 & -1 \\ -1-w & -1 & 5 \end{pmatrix}$	11	4	no	no
5	$\begin{pmatrix} 3 & -1 & -1-\overline{\omega} \\ -1 & 3 & 0 \\ -1-w & 0 & 5 \end{pmatrix}$	11	4	no	no

TABLE 1. Example 5.5.

consider is 19. We get 11 defect-0 curves of genus 3 over $\mathbb{F}_q$ up to $\mathbb{F}_q$-isomorphism, for instance

$$\begin{aligned} x^4 &+ 72x^3y + 111x^3z + 55x^2y^2 + 99x^2yz + 47x^2z^2 + 8xy^3 + 95xy^2z \\ &+ 74xyz^2 + 30xz^3 + 39y^4 + 53y^3z + 58y^2z^2 + 40yz^3 + 59z^4 = 0 \end{aligned}$$

which has an automorphism group of order 2.

Example 5.7. Let $q = 97$. As previously, the existence of a defect-0 curve of genus 3 over $\mathbb{F}_q$ leads to consider indecomposable unimodular positive definite R-lattices of rank 3, where R has discriminant -27 and therefore is not the maximal order of $\mathrm{Frac}(R)$. Our algorithms finds 4 indecomposable unimodular positive definite R-lattices and there is one lattice which is not projective, namely $R^2 \oplus \mathscr{O}$. This leads to 4 indecomposable principally polarized abelian threefolds over $\mathbb{F}_q$ isogenous to E^3 where $E/\mathbb{F}_q : y^2 = x^3 + 92x + 10$. For three of them, Serre's obstruction is trivial, so we get exactly three defect-0 curves of genus 3 over $\mathbb{F}_q$ up to $\mathbb{F}_q$-isomorphism for instance

$$\begin{aligned} x^4 &+ 63x^3y + 28x^3z + 10x^2y^2 + 81x^2yz + 43x^2z^2 + 89xy^3 + 10xy^2z + 70xyz^2 + 45xz^3 \\ &+ 24y^4 + 55y^3z + 77y^2z^2 + 35yz^3 + 54z^4 = 0 \end{aligned}$$

with an automorphism group of order 6.

5.3. **Curves of genus 4.** Jacobians of curves of genus 4 are not dense in the moduli space $\mathscr{A}_{4,1}$. They form a codimension-1 variety which we shall characterize thanks to the Igusa modular form J of level 1 and weight 8. The modular form J is defined over $\mathbb{C}$ as a homogeneous polynomial of degree 16 in the theta constants with integer coefficients, see for instance [Igu81a, p.538] or in [Igu81b] (with the choice of characteristics from [CKS19]). It is therefore an element of $\Gamma(\mathscr{A}_{4,1}(\mathbb{Z}), \mathcal{H}^8)$ and its values can be computed using Algorithm 7. We will also need the following result below. In [BG92], the first term in the Fourier expansion of J is computed and its constant coefficient is -2^{16}. This means that the Siegel modular form J does not vanish identically on $\mathscr{A}_{4,1} \otimes k$ for any algebraically closed field k of characteristic different from 2.

Igusa proves that the Igusa modular form is related to the classical Schottky modular form by

$$J = \frac{1}{2^6 \cdot 3^2 \cdot 5 \cdot 7} \cdot \left(\left(\sum \vartheta[\epsilon](\tau)^8 \right)^2 - 2^4 \sum \vartheta[\epsilon](\tau)^{16} \right)$$

the sums being over all even characteristics. Hence, over $\mathbb{C}$, this form is zero precisely on the locus of principally polarized abelian varieties of dimension 4 which are decomposable or a Jacobian. Following the same lines as [Rit10, Prop.2.3], this can be extended to any field of characteristic different from 2.

Theorem 5.8. *Let $(A, \mathscr{L})$ be an indecomposable principally polarized abelian variety of dimension 4 over an algebraically closed field k of characteristic different from 2 and w_A a basis of regular differentials. Then $J(A, \mathscr{L}, w_A) = 0$ if and only if $(A, \mathscr{L})$ is the Jacobian of a curve of genus 4 over k.*

Proof. Let $\mathscr{A}_{4,1}$ be the moduli stack of principally polarized abelian schemes of relative dimension 4 and let us denote by $\mathscr{T}$ the Torelli locus (the image of the moduli stack of genus 4 curves of compact type). Following [MO13, p.554], it is a reduced and closed substack of $\mathscr{A}_{4,1}$. Moreover for any algebraically closed field k, $\mathscr{T}(k)$ coincides with the disjoint union of the set of Jacobians of genus 4 curves and the set of decomposable principally polarized abelian varieties of dimension 4 defined over k.

Over $\mathbb{C}$, $\mathscr{T}(\mathbb{C}) = (J = 0)_{red}(\mathbb{C})$. This shows that $\mathscr{T} \otimes \mathbb{Q} = (J = 0)_{red} \otimes \mathbb{Q}$. Taking the schematic closure over $\mathbb{Z}[\frac{1}{2}]$ we get $\mathscr{T} \supset \overline{\mathscr{T} \otimes \mathbb{Q}} = \overline{(J = 0)_{red} \otimes \mathbb{Q}} \subset (J = 0)_{red}$ in $\mathscr{A}_{4,1}$ We need to prove that the two inclusions are equalities, i.e. that none of the loci $\mathscr{T}$ or $(J = 0)_{red}$ has a vertical component. For $(J = 0)_{red}$ this is the case since the modular form $J \in \Gamma(\mathscr{A}_{4,1} \otimes \mathbb{Z}[\frac{1}{2}], \mathcal{H}^{\otimes 8})$ is primitive and the fibers of $\mathscr{A}_{4,1}$ are irreducible (see for instance the proof of [FC90, Lemma 3.2, p. 163]). Similarly, for $\mathscr{T}$, this is true because we can lift any genus 4 curve in a special fiber to characteristic 0.

From this we deduce that $J(A, \mathscr{L}, w_A) = 0$ if and only if $(A, \mathscr{L}) \in \mathscr{T} \otimes k$. Since we have assumed that the polarization $\mathscr{L}$ is indecomposable, this is the case if and only if $(A, \mathscr{L})$ is a Jacobian. □

As we only need to check if the value of J is zero or not, we can work with any affine lift of the theta null point. However, if it is zero and $(A, \mathscr{L})$ is therefore a Jacobian over the algebraic closure, there is currently no way to ensure that it is also a Jacobian over the ground field.

Example 5.9. Let us consider the case of defect-0 genus 4 curves C over $\mathbb{F}_{59}$. The Jacobian of C would be isogenous to E^4 with E an elliptic curve with $\mathrm{End}(E)$ of discriminant -11. There are three indecomposable principally polarized abelian varieties in the class of E^4. We can check (using for the three of them the value $\ell = 3$) that for none of them the Igusa form is 0. Hence there is no defect-0 curve of genus 4 over $\mathbb{F}_{59}$ as it is confirmed in the manYPoints tables [GHL+09] or [Zay16, Th.1.1].

It would be more interesting to look at one unknown entry of these tables, like for instance $q = 89$. However in this case the discriminant of the associated elliptic curve is 32 and our algorithms are not efficient enough to work it out yet.

References

[Akh90] N. I. Akhiezer. *Elements of the theory of elliptic functions*. Vol. 79. Translations of Mathematical Monographs. Translated from the second Russian edition by H. H. McFaden. Amer. Math. Soc., 1990 (cit. on p. 26).

[AK18] Z. Amir-Khosravi. "Serre's tensor construction and moduli of abelian schemes". In: *Manuscripta Math.* 156.3-4 (2018), pp. 409–456 (cit. on pp. 4, 15, 16).

[BIL+16] J. S. Balakrishnan, S. Ionica, K. Lauter, and C. Vincent. "Constructing genus-3 hyperelliptic Jacobians with CM". In: *LMS J. Comput. Math.* 19.suppl. A (2016), pp. 283–300 (cit. on p. 30).

[BS11] G. Bisson and A. V. Sutherland. "Computing the endomorphism ring of an ordinary elliptic curve over a finite field". In: *J. Number Theory* 131.5 (2011), pp. 815–831 (cit. on p. 18).

[BCR10] G. Bisson, R. Cosset, and D. Robert. "AVIsogenies". Magma package devoted to the computation of isogenies between abelian varieties. 2010. URL: http://avisogenies.gforge.inria.fr. Free software (LGPLv2+), registered to APP (reference IDDN.FR.001.440011.000.R.P.2010.-000.10000). (Cit. on pp. 20, 21, 26).

[BF60] Z. I. Borevich and D. K. Faddeev. "Integral representations of quadratic rings". In: *Vestnik. Leningrad. Univ.* 15.19 (1960), pp. 52–60 (cit. on p. 6).

[BG92] B. Brinkmann and L. Gerritzen. "The lowest term of the Schottky modular form". In: *Math. Ann.* 292.2 (1992), pp. 329–335 (cit. on p. 33).

[BGH+08] J. H. Bruinier, G. van der Geer, G. Harder, and D. Zagier. *The 1-2-3 of modular forms*. Universitext. Lectures from the Summer School on Modular Forms and their Applications held in Nordfjordeid, June 2004, Edited by Kristian Ranestad. Springer, 2008 (cit. on p. 23).

[Can16] L. Candelori. *The transformation laws of algebraic theta functions*. 2016. arXiv: 1609.04486 (cit. on p. 24).

[CS15] T. G. Centeleghe and J. Stix. "Categories of abelian varieties over finite fields, I: Abelian varieties over $\mathbb{F}_p$". In: *Algebra Number Theory* 9.1 (2015), pp. 225–265 (cit. on p. 1).

[Cha86] C.-L. Chai. "Siegel moduli schemes and their compactifications over **C**". In: *Arithmetic geometry (Storrs, Conn., 1984)*. Springer, 1986, pp. 231–251 (cit. on p. 23).

[CKS19] L. Chua, M. Kummer, and B. Sturmfels. "Schottky algorithms: classical meets tropical". In: *Math. Comp.* 88.319 (2019), pp. 2541–2558 (cit. on p. 33).

[CFA+06] H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen, and F. Vercauteren, eds. *Handbook of elliptic and hyperelliptic curve cryptography*. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2006, pp. xxxiv+808 (cit. on p. 2).

[Cos11] R. Cosset. "Application des fonctions thêta à la cryptographie sur courbes hyperelliptiques". PhD thesis. Université Nancy-I, 2011 (cit. on pp. 20, 21, 25, 28).

[CR15] R. Cosset and D. Robert. "An algorithm for computing (ℓ, ℓ)-isogenies in polynomial time on Jacobians of hyperelliptic curves of genus 2". In: *Math. Comp.* 84.294 (2015), pp. 1953–1975 (cit. on pp. 2, 20–23, 30).

[DM69] P. Deligne and D. Mumford. "The irreducibility of the space of curves of given genus". In: *Inst. Hautes Études Sci. Publ. Math.* 36 (1969), pp. 75–109 (cit. on p. 23).

[Del69] P. Deligne. "Variétés abéliennes ordinaires sur un corps fini". In: *Invent. Math.* 8 (1969), pp. 238–243 (cit. on p. 1).

[DKR+20] T. Dupuy, K. Kedlaya, D. Roe, and C. Vincent. *Isogeny Classes of Abelian Varieties over Finite Fields in the LMFDB*. 2020. arXiv: 2003.05380 (cit. on p. 1).

[EL10] K. Eisenträger and K. Lauter. "A CRT algorithm for constructing genus 2 curves over finite fields". In: *Arithmetics, geometry, and coding theory (AGCT 2005)*. Vol. 21. Sémin. Congr. Soc. Math. France, Paris, 2010, pp. 161–176 (cit. on p. 18).

[Eng09] A. Enge. "The complexity of class polynomial computation via floating point approximations". In: *Mathematics of Computation* 78.266 (2009), pp. 1089–1107 (cit. on p. 18).

[FC90] G. Faltings and C.-L. Chai. *Degeneration of abelian varieties*. Vol. 22. Ergebnisse der Mathematik und ihrer Grenzgebiete (3). With an appendix by David Mumford. Springer, 1990 (cit. on pp. 23, 24, 34).

[FK01] H. M. Farkas and I. Kra. *Theta constants, Riemann surfaces and the modular group*. Vol. 37. Graduate Studies in Mathematics. An introduction with applications to uniformization theorems, partition identities and combinatorial number theory. Amer. Math. Soc., 2001 (cit. on p. 26).

[FP85] U. Fincke and M. Pohst. "Improved methods for calculating vectors of short length in a lattice, including a complexity analysis". In: *Math. Comp.* 44.170 (1985), pp. 463–471 (cit. on p. 11).

[Fio16] A. Fiorentino. *Weber's formula for the bitangents of a smooth plane quartic*. 2016. arXiv: 1612.02049 (cit. on p. 31).

[GY00] W. T. Gan and J.-K. Yu. "Group schemes and local densities". In: *Duke Math. J.* 105.3 (2000), pp. 497–524 (cit. on p. 8).

[GHL+09] G. van der Geer, E. W. Howe, K. E. Lauter, and C. Ritzenthaler. "Tables of Curves with Many Points". 2009. URL: www.manypoints.org (cit. on p. 34).

[GD64] A. Grothendieck and J. Dieudonné. "Eléments de géométrie algébrique". In: *Publ. math. IHES* 20.24 (1964), p. 1965 (cit. on p. 17).

[Hal10] S. Haloui. "The characteristic polynomials of abelian varieties of dimensions 3 over finite fields". In: *J. Number Theory* 130.12 (2010), pp. 2745–2752 (cit. on p. 1).

[HS12] S. Haloui and V. Singh. "The characteristic polynomials of abelian varieties of dimension 4 over finite fields". In: *Arithmetic, geometry, cryptography and coding theory*. Vol. 574. Contemp. Math. Amer. Math. Soc., 2012, pp. 59–68 (cit. on p. 1).

[HK89a] K. Hashimoto and H. Koseki. "Class numbers of definite unimodular Hermitian forms over the rings of imaginary quadratic fields". In: *Tohoku Math. J. (2)* 41.1 (1989), pp. 1–30 (cit. on p. 7).

[HK89b] K. Hashimoto and H. Koseki. "Class numbers of positive definite binary and ternary unimodular Hermitian forms". In: *Tohoku Math. J. (2)* 41.2 (1989), pp. 171–216 (cit. on pp. 3, 7).

[Hay19] D. Hayashida. "The characteristic polynomials of abelian varieties of higher dimension over finite fields". In: *J. Number Theory* 196 (2019), pp. 205–222 (cit. on p. 1).

[HV98] B. Hemkemeier and F. Vallentin. "Incremental algorithms for lattice problems". In: *Electronic Colloquium on Computational Complexity*. Vol. 52. revision 1. 1998 (cit. on p. 6).

[Hof91] D. W. Hoffmann. "On positive definite hermitian forms". In: *Manuscripta Math.* 71 (1991), pp. 399–429 (cit. on p. 4).
[Hon68] T. Honda. "Isogeny classes of abelian varieties over finite fields". In: *J. Math. Soc. Japan* 20 (1968), pp. 83–95 (cit. on p. 1).
[How95] E. W. Howe. "Principally polarized ordinary abelian varieties over finite fields". In: *Trans. Amer. Math. Soc.* 347.7 (1995), pp. 2361–2401 (cit. on pp. 1, 2).
[HNR09] E. W. Howe, E. Nart, and C. Ritzenthaler. "Jacobians in isogeny classes of abelian surfaces over finite fields". In: *Ann. Inst. Fourier (Grenoble)* 59.1 (2009), pp. 239–289 (cit. on p. 1).
[IKO86] T. Ibukiyama, T. Katsura, and F. Oort. "Supersingular curves of genus two and class numbers". In: *Compos. Math.* 57.2 (1986), pp. 127–152 (cit. on p. 1).
[Ich96] T. Ichikawa. "Theta constants and Teichmüller modular forms". In: *J. Number Theory* 61.2 (1996), pp. 409–419 (cit. on p. 32).
[Igu81a] J. Igusa. "On the irreducibility of Schottky's divisor". In: *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* 28.3 (1981), 531–545 (1982) (cit. on p. 33).
[Igu81b] J. Igusa. "Schottky's invariant and quadratic forms". In: *E. B. Christoffel.* Birkhäuser, 1981, pp. 352–362 (cit. on p. 33).
[Igu67] J. Igusa. "Modular forms and projective invariants". In: *Amer. J. Math.* 89 (1967), pp. 817–855 (cit. on p. 32).
[Jac62] R. Jacobowitz. "Hermitian forms over local fields". In: *Amer. J. Math.* 84 (1962), pp. 441–465 (cit. on pp. 7, 9, 11, 13, 14).
[JKP+18] B. W. Jordan, A. G. Keeton, B. Poonen, E. M. Rains, N. Shepherd-Barron, and J. T. Tate. "Abelian varieties isogenous to a power of an elliptic curve". In: *Compos. Math.* 154.5 (2018), pp. 934–959 (cit. on pp. 1, 2, 4, 15, 16, 18).
[Kan11] E. Kani. "Products of CM elliptic curves". In: *Collect. Math.* 62.3 (2011), pp. 297–339 (cit. on p. 2).
[Kem89] G. Kempf. "Linear systems on abelian varieties". In: *American Journal of Mathematics* 111.1 (1989), pp. 65–94 (cit. on p. 23).
[Kir16] M. Kirschmer. "Definite quadratic and hermitian forms with small class number". Habilitation. RWTH Aachen University, 2016 (cit. on pp. 5, 7, 8).
[Kir19] M. Kirschmer. "Determinant groups of Hermitian lattices over local fields". In: *Arch. Math.* 113.4 (2019), pp. 337–347 (cit. on pp. 2, 8).
[KNR+20] M. Kirschmer, F. Narbonne, C. Ritzenthaler, and D. Robert. "FromLatticesToModularForms". Computation of modular forms in the isogeny class spanned by products of elliptic curves. Apr. 2020. URL: https://gitlab.inria.fr/roberdam/fromlatticestomodularforms (cit. on p. 4).
[Kne66] M. Kneser. "Strong approximation". In: *Algebraic Groups and Discontinuous Subgroups (Proc. Sympos. Pure Math., Boulder, Colo., 1965).* Amer. Math. Soc., 1966, pp. 187–196 (cit. on p. 14).
[Koi76] S. Koizumi. "Theta relations and projective normality of abelian varieties". In: *American Journal of Mathematics* (1976), pp. 865–889 (cit. on p. 23).
[LR08] G. Lachaud and C. Ritzenthaler. "On some questions of Serre on abelian threefolds". In: *Algebraic geometry and its applications.* Vol. 5. Ser. Number Theory Appl. World Sci. Publ., 2008, pp. 88–115 (cit. on p. 32).
[LRZ10] G. Lachaud, C. Ritzenthaler, and A. Zykin. "Jacobians among abelian threefolds: a formula of Klein and a question of Serre". In: *Math. Res. Lett.* 17.2 (2010) (cit. on p. 32).
[LSV21] J.-C. Lario, A. Somoza, and C. Vincent. "An inverse Jacobian algorithm for Picard curves". In: *Res. Number Theory* 7.2 (2021), p. 32 (cit. on p. 30).
[Lau18] K. Lauter. "On maximal genus 3 curves over finite fields with an appendix by J. P. Serre." In: *Compos. Math.* 154.5 (2018), pp. 934–959 (cit. on pp. 2, 15).
[LR12a] R. Lercier and C. Ritzenthaler. "Hyperelliptic curves and their invariants: geometric, arithmetic and algorithmic aspects". In: *J. Algebra* 372 (2012), pp. 595–636 (cit. on pp. 30, 31).

[LRR+14] R. Lercier, C. Ritzenthaler, F. Rovetta, and J. Sijsling. "Parametrizing the moduli space of curves and applications to smooth plane quartics over finite fields". In: *LMS J. Comput. Math.* 17.suppl. A (2014), pp. 128–147 (cit. on p. 31).

[Liu02] Q. Liu. *Algebraic geometry and arithmetic curves*. Vol. 6. Oxford Graduate Texts in Mathematics. Translated from the French by Reinie Erné, Oxford Science Publications. Oxford University Press, 2002 (cit. on p. 17).

[Lor19] E. Lorenzo García. *On different expressions for invariants of hyperelliptic curves of genus 3*. To appear in Journal of the Math. Soc. Japan. 2019. arXiv: 1907.05776 (cit. on p. 30).

[LR12b] D. Lubicz and D. Robert. "Computing isogenies between abelian varieties". In: *Compos. Math.* 148.5 (2012), pp. 1483–1515 (cit. on p. 22).

[LR15] D. Lubicz and D. Robert. "Computing separable isogenies in quasi-optimal time". In: *LMS J. Comput. Math.* 18 (1 2015), pp. 198–216 (cit. on p. 20).

[LR16] D. Lubicz and D. Robert. "Arithmetic on Abelian and Kummer Varieties". In: *Finite Fields and Their Applications* 39 (2016), pp. 130–158 (cit. on p. 22).

[Mar19] S. Marseglia. "Computing abelian varieties over finite fields isogenous to a power". In: *Res. Number Theory* 5.4 (2019), Paper No. 35, 17 (cit. on pp. 1, 2, 15).

[Mat58] T. Matsusaka. "On a theorem of Torelli". In: *Amer. J. Math.* 80 (1958), pp. 784–800 (cit. on p. 32).

[Mea08] S. Meagher. "Twists of genus 3 and their Jacobians". PhD thesis. Rijksuniversiteit Groningen, 2008 (cit. on p. 32).

[Mil86] J. S. Milne. "Abelian varieties". In: *Arithmetic geometry (Storrs, Conn., 1984)*. Springer, 1986, pp. 103–150 (cit. on pp. 17, 19).

[MO13] B. Moonen and F. Oort. "The Torelli locus and special subvarieties". In: *Handbook of moduli. Vol. II*. Vol. 25. Adv. Lect. Math. (ALM). Int. Press, 2013, pp. 549–594 (cit. on p. 34).

[Mum66] D. Mumford. "On the equations defining abelian varieties. I". In: *Invent. Math.* 1 (1966), pp. 287–354 (cit. on pp. 22–24, 28).

[Mum67] D. Mumford. "On the equations defining abelian varieties. II". In: *Invent. Math.* 3 (1967), pp. 75–135 (cit. on pp. 22, 24).

[Mum07a] D. Mumford. *Tata lectures on theta. I*. Modern Birkhäuser Classics. With the collaboration of C. Musili, M. Nori, E. Previato and M. Stillman, Reprint of the 1983 edition. Birkhäuser, 2007 (cit. on pp. 24, 27, 28).

[Mum07b] D. Mumford. *Tata lectures on theta. II: Jacobian theta functions and differential equations. With the collaboration of C. Musili, M. Nori, E. Previato, M. Stillman, and H. Umemura. Reprint of the 1984 edition*. Modern Birkhäuser Classics. Birkhäuser, 2007 (cit. on pp. 20, 26).

[Mum07c] D. Mumford. *Tata lectures on theta. III*. Modern Birkhäuser Classics. With collaboration of Madhav Nori and Peter Norman, Reprint of the 1991 original. Birkhäuser, 2007 (cit. on p. 24).

[Mum08] D. Mumford. *Abelian varieties*. Vol. 5. Tata Institute of Fundamental Research Studies in Mathematics. With appendices by C. P. Ramanujam and Yuri Manin, Corrected reprint of the second (1974) edition. Published for the Tata Institute of Fundamental Research, Bombay; by Hindustan Book Agency, New Delhi, 2008 (cit. on p. 16).

[MFK94] D. Mumford, J. Fogarty, and F. Kirwan. *Geometric invariant theory*. Vol. 34. Springer, 1994 (cit. on p. 21).

[O'M63] O. T. O'Meara. *Introduction to quadratic forms*. Springer, 1963 (cit. on p. 13).

[OU73] F. Oort and K. Ueno. "Principally polarized abelian varieties of dimension two or three are Jacobian varieties". In: *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* 20 (1973), pp. 377–381 (cit. on p. 30).

[OS20] A. Oswal and A. N. Shankar. "Almost ordinary abelian varieties over finite fields". In: *J. Lond. Math. Soc. (2)* 101.3 (2020), pp. 923–937 (cit. on p. 1).

[Rit10] C. Ritzenthaler. "Explicit computations of Serre's obstruction for genus-3 curves and application to optimal curves". In: *LMS J. Comput. Math.* 13 (2010), pp. 192–207 (cit. on pp. 4, 32, 33).

[Rit11] C. Ritzenthaler. "Optimal curves of genus 1, 2 and 3". In: *Actes de la Conférence "Théorie des Nombres et Applications"*. Vol. 2011. Publ. Math. Besançon Algèbre Théorie Nr. Presses Univ. Franche-Comté, Besançon, 2011, pp. 99–117 (cit. on p. 32).

[Rob10] D. Robert. "Theta functions and cryptographic applications". PhD thesis. Université Henri-Poincarré, Nancy 1, France, 2010 (cit. on pp. 22, 28).

[Sch] A. Schiemann. "Tables of Hermitian lattices". URL: www.math.uni-sb.de/ag/schulze/Hermitian-lattices (cit. on p. 31).

[Sch98] A. Schiemann. "Classification of Hermitian forms with the neighbour method". In: *J. Symbolic Comput.* 26.4 (1998), pp. 487–508 (cit. on pp. 2, 7, 32).

[Ser85] J.-P. Serre. "Rational points on curves over finite fields". Lectures given at Harvard, notes by F.Q. Gouvéa. 1985 (cit. on pp. 1, 4, 15, 16, 32).

[Shi64] G. Shimura. "Arithmetic of the unitary group". In: *Annals of Mathematics* 79.2 (1964), pp. 369–409 (cit. on p. 7).

[Sij20] J. Sijsling. "Curve reconstruction". Magma code for reconstructing hyperelliptic curves of genus up to 3 from their period matrices. Dec. 2020. URL: https://github.com/JRSijsling/curve_reconstruction (cit. on p. 30).

[Str14] M. Streng. "Computing Igusa class polynomials". In: *Math. Comp.* 83.285 (2014), pp. 275–309 (cit. on p. 2).

[Sut11] A. V. Sutherland. "Computing Hilbert class polynomials with the Chinese remainder theorem". In: *Math. Comp.* 80.273 (2011), pp. 501–538 (cit. on pp. 2, 18).

[Tat66] J. Tate. "Endomorphisms of abelian varieties over finite fields". In: *Invent. Math.* 2 (1966), pp. 134–144 (cit. on p. 1).

[Wat69] W. Waterhouse. "Abelian varieties over finite fields". In: *Annales scientifiques de l'E.N.S.* 2.4 (1969), pp. 521–560 (cit. on pp. 1, 15).

[Web76] H. Weber. *Theory of abelian functions of genus 3. (Theorie der Abelschen Functionen vom Geschlecht 3.)* 1876 (cit. on p. 31).

[Wen01] A. Weng. "A class of hyperelliptic CM-curves of genus three". In: *J. Ramanujan Math. Soc.* 16.4 (2001), pp. 339–372 (cit. on p. 30).

[XYY19] J. Xue, T.-C. Yang, and C.-F. Yu. "Supersingular abelian surfaces and Eichler class number formula". In: *Asian Journal of Mathematics* 23.4 (2019), pp. 651–680 (cit. on p. 1).

[Zay16] A. Zaytsev. "Optimal curves of low genus over finite fields". In: *Finite Fields Appl.* 37 (2016), pp. 203–224 (cit. on p. 34).

Universität Paderborn, Fakultät EIM, Institut für Mathematik, Warburger Str. 100, 33098 Paderborn, Germany
E-mail address: markus.kirschmer@math.upb.de

Univ Rennes, CNRS, IRMAR - UMR 6625, F-35000 Rennes, France.
E-mail address: fabien.narbonne@univ-rennes1.fr

Univ Rennes, CNRS, IRMAR - UMR 6625, F-35000 Rennes, France.
E-mail address: christophe.ritzenthaler@univ-rennes1.fr

INRIA Bordeaux–Sud-Ouest, 200 avenue de la Vieille Tour, 33405 Talence Cedex, France and Institut de Mathématiques de Bordeaux, 351 cours de la liberation, 33405 Talence cedex, France
E-mail address: damien.robert@inria.fr

Chapitre 4

PRODUITS POLARISÉS DE COURBES ELLIPTIQUES À MULTIPLICATION COMPLEXE ET CORPS DE MODULES $\mathbb{Q}$

POLARIZED PRODUCTS OF ELLIPTIC CURVES WITH COMPLEX MULTIPLICATION AND FIELD OF MODULI $\mathbb{Q}$

A PREPRINT

Fabien Narbonne*

March 2022

ABSTRACT

Let R be the maximal order in a quadratic imaginary field K. We give an equivalence of categories between the category of polarized abelian varieties isomorphic to a product of elliptic curves over $\mathbb{C}$ with complex multiplication (CM) by R and the category of integral hermitian R-lattices. Then we apply this equivalence to enumerate all the genus 2 and 3 curves with field of moduli $\mathbb{Q}$ and with Jacobian isomorphic to a product of elliptic curves with CM by R.

Introduction

Let E be an elliptic curve over $\mathbb{C}$ with complex multiplication by a maximal order R in a quadratic imaginary field K. Then E admits a model over $\overline{\mathbb{Q}}$, it even admits one over $\mathbb{Q}(j(E))$, which has degree $\#\operatorname{Cl}(R)$ over $\mathbb{Q}$, and not over any sub-extension. It may then be surprising that powers of CM elliptic curves may be defined over smaller fields than expected, sometimes even over $\mathbb{Q}$. In [FG20, Theorem 1.1 and 1.2] the authors show for instance that there are abelian surfaces defined over $\mathbb{Q}$, $\overline{\mathbb{Q}}$-isogenous to the square of a CM elliptic curve, for exactly 45 discriminants. From this they deduce, [FG20, Corolarry 1.3] that there are exactly 92 $\overline{\mathbb{Q}}$-endomorphism algebras of geometrically split abelian variety over $\mathbb{Q}$. This study is motivated by the conjecture on the possible finiteness of the set of endomorphism rings of abelian varieties of a given dimension over a fixed degree extension field of $\mathbb{Q}$.

A weaker requirement is to ask for the field of moduli of a (polarized) abelian variety to be $\mathbb{Q}$. In [GHR19] the authors give the finite list of indecomposable principally polarized abelian surfaces (also known as Jacobian of genus 2 curves) with field of moduli $\mathbb{Q}$ which are isomorphic to E^2.

In the present article, we address the case of abelian varieties isomorphic to products $E_1 \times \cdots \times E_g$, $g > 1$, of elliptic curves with CM by a maximal order R and we give an exhaustive list of these principally polarized abelian varieties for the case $g = 2$ in Table 1 and a partial list for $g = 3$ in Table 2. Before explaining the structure of the paper and our strategy, we want to point out that we strongly believe that the restriction on R being maximal can be dropped and we hope to work on it soon. Once this will be done, one would have an even stronger extension of *loc. cit.* since every abelian variety *isogenous* over $\overline{\mathbb{Q}}$ to E^g is actually isomorphic to a product of elliptic curves with CM by (possibly distinct) orders in $K = \operatorname{Frac} R$ ([Kan11, Th.2]). We also hope to address the finer question of the descent of the principally polarized abelian variety over its field of moduli.

In Section 1 we recall some properties of the classical equivalence of categories between the complex abelian varieties and polarizable tori and how it behaves with polarizations. Polarizations on abelian varieties give rise to positive definite hermitian forms with a compatibility condition on the lattice.

In Section 2 we restrict the equivalence of categories to the abelian varieties isomorphic to the product of elliptic curves with complex multiplication by R. The complex tori V/Γ associated to those abelian varieties have additional

*Univ Rennes, CNRS, IRMAR - UMR 6625, F-35000 Rennes, France.
Email address: fabien.narbonne@univ-rennes1.fr

structure ; we can endow their lattice Γ with a structure of R-module. The corresponding hermitian form endows on the R-module Γ a structure of *integral hermitian lattice* (up to rescaling the hermitian form which only depends on R). This restriction leads to an equivalence of categories between polarized abelian varieties isomorphic to a product of elliptic curves with CM by R and integral hermitian R-lattices (Theorem 2). Moreover, hermitian forms corresponding to principal polarization give *unimodular lattices* through the equivalence. We may note that a similar functor is developed in [JKP$^+$18] in a much wider frame since it is defined for any field, not only $\mathbb{C}$. Under some conditions it is also an equivalence of categories. However, we chose to focus our attention on a much simpler functor since we will need to refine it in the next section.

The goal of Section 3 is to translate the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on abelian varieties $\overline{\mathbb{Q}}$-isomorphic to $E_1 \times \cdots \times E_g$ into the category of integral hermitian lattices through the previous functor. The action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ can be decomposed into two steps: the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ and the action of $\mathrm{Gal}(K/\mathbb{Q})$, the complex conjugation. The latter is a continuous action and it is therefore easier to handle. For the first one, we use the existence of a surjective morphism $F\colon \mathrm{Gal}(\overline{\mathbb{Q}}/K) \to \mathrm{Cl}(R)$ such that the action by conjugation of $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/K)$ on abelian varieties corresponds to the tensor product of the associated lattice by a representative of $F(\sigma)$ (and a rescaling of the hermitian form).

Still, for both actions, we need to rigidify the choice of the target objects under the previous equivalences of categories, which are defined only up to $\mathbb{C}$-isomorphisms. Indeed, unlike [GHR19] where the compatibilities between the various abelian varieties and their conjugate were obvious, we could not find a simple way to impose them from abstract nonsense. We therefore use the explicit algebraization by the Weiestrass function for elliptic curves to be able to work out the explicit Galois action on the associated hermitian R-lattices (see Proposition 2) and we then extend it, component by component to products of elliptic curves in order to obtain our main results (Theorems 3 and 4). Notice that the main difficulty is to be able to keep the abelian varieties, their isogenies *and* their analytic representation defined over $\overline{\mathbb{Q}}$ to be able to translate the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Finally, in Section 4, we look when $\mathbb{Q}$ is the field of moduli of the indecomposable principally polarized abelian varieties $A \simeq E_1 \times \cdots \times E_g$ where E_i has with CM by R. We first extend the result of [GHR19] showing that if $\mathbb{Q}$ is the field of moduli then $\mathrm{Cl}(R)$ has exponent dividing g. We also show that the Steinitz class of the R-lattice associated to A is of order at most 2 (see Proposition 9). From this, we deduce the surprising Corollary 1 that odd-dimensional A with field of moduli $\mathbb{Q}$ must be isomorphic to the power of an elliptic curve.

For a given dimension g, under the Extended Riemann Hypothesis there are only finitely many R which are of exponent g. Their list is known up to $g = 8$, see [EKN20]. However, we do explicit computation with our Algorithm 1 only for $g = 2$ and 3 as the computations become quickly time-consuming when g and the discriminant are growing. For $g = 2$, we find 137 indecomposable principally polarized abelian varieties with field of moduli $\mathbb{Q}$ completing the 46 found in [GHR19]. For $g = 3$, we find 33 up to one missing discriminant.

Acknowledgments

I would like to acknowledge Francesc Fité and Xavier Guitart who motivated this project and helped until its fulfilment.

In addition, I want to thank Marco Streng for its attention and advice along the way of this work.

I would also like to address a special thank to Markus Kirschmer for his advice and patience answering all of my questions about hermitian lattices. He also gave me an extension of the Magma library of [KNRR21] to handle more efficiently the classification of free hermitian unimodular R-lattices which we used for the computation of the dimension $g = 3$ case in Section 4.3.

Finally, I want to thank Harun Kir for the rich discussions we had on this subject and for its precious support for this work.

1 Complex abelian varieties and complex tori

1.1 Abelian varieties and polarizable tori

Let us first recall that there is an equivalence of categories between abelian varieties over $\mathbb{C}$ and the category of polarizable tori given by $\mathbf{T}\colon A \mapsto A(\mathbb{C})$, see [Mil08, Theorem 2.9]. A *complex torus* is a quotient of groups $X = V/\Gamma$ with V a complex vector space of finite dimension and Γ a $\mathbb{Z}$-*lattice* of V, i.e., a subgroup of V generated by a real basis. A torus $X = V/\Gamma$, or a lattice $\Gamma \subseteq V$, is said to be *polarizable* if there exists a positive definite hermitian form

$h\colon V \times V \to \mathbb{C}$ such that

$$\operatorname{im} h(\Gamma, \Gamma) \subseteq \mathbb{Z}$$

where im is the imaginary part. Morphisms of complex tori are morphisms of groups $\varphi\colon X = V/\Gamma \to X' = V'/\Gamma'$. Such maps can be lifted to a linear maps $\varphi_{\text{an}}\colon V \to V'$ that sends Γ on Γ' called the *analytic representation* of φ. The group morphism $\varphi_{\text{rat}} = \varphi_{\text{an}|\Gamma}\colon \Gamma \to \Gamma'$ is called the *rational representation* of φ. We denote the set of the analytic representations of morphisms between X and X' by $\operatorname{Hom}_{\mathbb{C}}(\Gamma, \Gamma')$. We will often consider analytic representations directly as morphisms of polarizable tori.

A surjective morphism $f\colon A \to B$ between abelian varieties A and B over $\mathbb{C}$ of equal dimension is called an *isogeny*, its kernel is finite and its cardinality $\#\ker f$ is called the *degree* of f, denoted $\deg f$. We will also call *isogeny* the corresponding morphism of tori $\varphi\colon V/\Gamma \to V'/\Gamma'$ by the functor $\mathbf{T}$. The degree of φ is defined in the same way $\deg \varphi = \#\ker \varphi$. Moreover, it satisfies

$$\deg \varphi = (\Gamma'\colon \varphi_{\text{an}}(\Gamma)) = \deg f$$

with $(\Gamma'\colon \varphi_{\text{an}}(\Gamma)) = \#(\Gamma'/\varphi_{\text{an}}(\Gamma))$, the index of $\varphi_{\text{an}}(\Gamma)$ in Γ'.

1.2 Duality

Let V be a dimension g complex vector space and $\Gamma \subseteq V$ a $\mathbb{Z}$-lattice. The dual lattice associated to Γ is defined by

$$\widehat{\Gamma} = \{\ell \in V^*, \operatorname{im} \ell(\Gamma) \subseteq \mathbb{Z}\}$$

where V^* denotes the set of antilinear forms $\ell\colon V \to \mathbb{C}$. This defines the dual complex torus of V/Γ, denoted $\widehat{V/\Gamma} := V^*/\widehat{\Gamma}$.

If A is a complex abelian variety such that $A(\mathbb{C}) \simeq V/\Gamma$ then there exists an isomorphism $\widehat{A}(\mathbb{C}) \simeq \widehat{V/\Gamma}$, where $\widehat{A}$ is the dual abelian variety of A (see [Mum70]). Moreover, for $f\colon A \to B$ a morphism and $\varphi = \mathbf{T}(f)\colon V/\Gamma \to V'/\Gamma'$ we have $\mathbf{T}(\widehat{f})_{\text{an}} = \varphi_{\text{an}}^*$ with

$$\begin{array}{rccc} \varphi_{\text{an}}^*\colon & V'^* & \longrightarrow & V^* \\ & \ell & \longmapsto & \ell \circ \varphi_{\text{an}} \end{array}$$

where $\widehat{f}\colon \widehat{B} \to \widehat{A}$ is the dual morphism of f (see [BL04, Section 2.4]).

1.3 Polarizations and hermitian forms

Let A be an abelian variety and let $\mathscr{L}$ be a line bundle. We consider the map

$$\begin{array}{rccc} a_{\mathscr{L}}\colon & A & \longrightarrow & \widehat{A} \\ & x & \longmapsto & t_x^*\mathscr{L} \otimes \mathscr{L}^{-1}. \end{array}$$

with t_x the translation by x map. Consider isomorphisms $A(\mathbb{C}) \simeq V/\Gamma$ and $\widehat{A}(\mathbb{C}) \simeq V^*/\widehat{\Gamma}$. Let $h = c_1(\mathscr{L})$ be the first Chern class of $\mathscr{L}$ which we identify with a hermitian form on V (see [BL04, Lemma 2.4.5]). Then the map $\rho_h \in \operatorname{Hom}_{\mathbb{C}}(\Gamma, \widehat{\Gamma})$ defined by

$$\begin{array}{rccc} \rho_h\colon & V & \longrightarrow & V^* \\ & v & \longmapsto & h(v, \_). \end{array}$$

is the analytic representation of $a_{\mathscr{L}}$. A polarization on an abelian variety A is an isogeny $a_{\mathscr{L}}$ with $\mathscr{L}$ an ample line bundle. In this case, its first Chern class h is a positive definite hermitian form (see [BL04, Proposition 4.5.2]).

A couple (A, a) with A an abelian variety and a a polarization is called a *polarized abelian variety*. Morphisms of polarized abelian varieties are defined by maps $f\colon (A, a) \to (B, b)$ such that $\widehat{f}bf = a$ and we call them *polarized isogenies*. A *polarized torus* is a couple $(V/\Gamma, \rho_h)$ (also denoted by (Γ, h)) with V/Γ a complex torus and $\rho_h \in \operatorname{Hom}_{\mathbb{C}}(\Gamma, \widehat{\Gamma})$ induced by a positive definite hermitian form h, i.e., $\rho_h(v) = h(v, \_)$. We define in the same way morphisms, $\varphi\colon (V/\Gamma, \rho_h) \to (V'/\Gamma', \rho_{h'})$ between polarized tori. Their analytic representation must satisfy $\varphi_{\text{an}}^*\rho_{h'}\varphi_{\text{an}} = \rho_h$ which means that for $v, w \in V$,

$$\rho_h(v)(w) = h(v, w) = h'(\varphi_{\text{an}}(v), \varphi_{\text{an}}(w)).$$

In particular, analytic representations of polarized isogenies define isometries on the associated hermitian vector spaces. In the following we will call a couple (V, h) made of a $\mathbb{C}$-vector space and h a positive definite hermitian form a hermitian space. Since, the functor $\mathbf{T}$ is an equivalence of categories, it also defines an equivalence of categories $\mathbf{T}^p$ between polarized abelian varieties and polarized tori $(A, a) \mapsto (X = \mathbf{T}(A), \rho_h = \mathbf{T}(a))$.

For any group schemes A and B over a field k there is an isomorphism of groups

$$A(k) \times B(k) \simeq (A \times_k B)(k).$$

We can apply it to abelian varieties over $\mathbb{C}$. For $A(\mathbb{C}) \simeq V_A/\Gamma_A$, $B(\mathbb{C}) \simeq V_B/\Gamma_B$ and $(A \times B)(\mathbb{C}) \simeq V/\Gamma$ we have

$$V/\Gamma \simeq (V_A/\Gamma_A) \times (V_B/\Gamma_B).$$

Hence, $\Gamma \simeq \Gamma_A \times \Gamma_B$ and in terms of categories, the functor $\mathbf{T}$ commutes with products. In the same way the functor $\mathbf{T}^p$ also commutes with products.

2 Totally split CM abelian varieties and R-module structure

Let R be the maximal order of a quadratic imaginary field $K = \mathbb{Q}(\sqrt{-d})$ with d a positive square-free integer. A R-lattice is a finitely presented, torsion free R-module. We denote by $\boldsymbol{\mathcal{L}}_R$, the category of R-lattices. In this section we want to show that there exist equivalences of categories

- between $\boldsymbol{\mathcal{A}}_R$, the category of complex abelian varieties isomorphic to a product of elliptic curves with CM by R, and $\boldsymbol{\mathcal{L}}_R$.
- between $\boldsymbol{\mathcal{A}}_R^p$, the category of complex polarized abelian varieties isomorphic to a product of elliptic curves with CM by R, and $\boldsymbol{\mathcal{L}}_R^{h,int}$, the category of integral hermitian R-lattices, i.e., R-lattices equipped with a positive definite hermitian form H on KL, such that $H(L, L) \subseteq R$.

For the rest of the article we fix field extensions

$$\mathbb{Q} \longrightarrow K \longrightarrow \overline{\mathbb{Q}} \longrightarrow \mathbb{C}.$$

2.1 Elliptic curve with complex multiplication over $\mathbb{C}$

Let $R = \mathbb{Z}[\omega]$ be a maximal order of an imaginary quadratic field $K = \mathbb{Q}(\sqrt{\Delta})$ with $\Delta < 0$ the discriminant of $K/\mathbb{Q}$. We chose ω a generator of R with $\alpha_R = \operatorname{im}\omega > 0$. Notice that α_R does not depend on the chosen generator ω with positive imaginary part.

Let E be an elliptic curve over $\mathbb{C}$ with complex multiplication by R, i.e., there exists a ring isomorphism $\mathrm{End}(E) \simeq R$. Let $\Lambda \subseteq \mathbb{C}$ be a lattice and consider any isomorphism $\eta\colon \mathbb{C}/\Lambda \xrightarrow{\sim} E(\mathbb{C})$, in this case we will denote E by E_Λ. By [Sil94, Proposition II.1.1.] there is a unique isomorphism

$$[.]_E\colon R \xrightarrow{\sim} \mathrm{End}(E)$$

characterized by the commutativity of the diagram of Figure 1. For any $\alpha \in R$,

$$\begin{array}{ccc} \mathbb{C}/\Lambda & \xrightarrow{z\mapsto\alpha z} & \mathbb{C}/\Lambda \\ {\scriptstyle\eta}\downarrow & & \downarrow{\scriptstyle\eta} \\ E_\Lambda(\mathbb{C}) & \xrightarrow{[\alpha]} & E_\Lambda(\mathbb{C}). \end{array}$$

Figure 1: The bracket isomorphism

We will always use this isomorphism when we identify R with $\mathrm{End}(E)$.

According to [Sil94, Proposition 2.1] all CM elliptic curves over $\mathbb{C}$ admit a model over $\overline{\mathbb{Q}}$. We denote by $\mathrm{Ell}(R)$ the set of isomorphism classes of elliptic curves over $\overline{\mathbb{Q}}$ with CM by R. We recall from [Sil94, Proposition 1.2] that $\mathrm{Cl}(R)$, the class group of R, acts simply transitively on $\mathrm{Ell}(R)$ and the action is given by

$$\mathfrak{a} \star E_\Lambda = E_{\mathfrak{a}^{-1}\Lambda}.$$

The action is well defined on the isomorphism classes because another representative $\mathfrak{b}$ of the class of $\mathfrak{a}$ in $\mathrm{Cl}(R)$ differs from $\mathfrak{a}$ by a scalar and then $\mathfrak{a}^{-1}\Lambda$ and $\mathfrak{b}^{-1}\Lambda$ are homothetic lattices.

2.2 Totally split complex tori and R-module structure

Let L be a R-lattice, i.e., a finitely presented, torsion free R-module. Since R is maximal, L is a module over a Dedekind domains and by [O'M00, Theorem 81.3], we can always write L as a sum

$$L = \bigoplus_{i=1}^{g} \mathfrak{a}_i x_i$$

with a basis $x_1, \dots, x_g$ of the K-vector space $L \otimes_R K$ and fractional ideals $\mathfrak{a}_1, \dots, \mathfrak{a}_g$ of R. The couple $(\mathfrak{a}_i, x_i)$ is called a *pseudo-basis* of L and the *Steinitz class* $\mathrm{st}(L)$ of L is defined by the class of the product $\mathfrak{a}_1 \cdots \mathfrak{a}_g$ in $\mathrm{Cl}(R)$. The Steinitz class of a lattice togeither with its rank determines its R-isomorphism class [Con16, Theorem 13].
For a R-ideal $\mathfrak{a}$ of R the norm of $\mathfrak{a}$ is defined by $N(\mathfrak{a}) = \#(R/\mathfrak{a})$. We can extend the definition of the norm to any fractional ideal by the relation $N(\lambda\mathfrak{a}) = |\lambda|^2 N(\mathfrak{a})$ for any $\lambda \in K$.

We will denote the $\mathbb{Z}$-lattices coming from the quotient of a polarizable torus by the letter Γ and we denote R-lattices by L. According to the following theorem, we could call them the same way when the torus is isomorphic to the complex points of an object of $\boldsymbol{\mathcal{A}}_R$. However, when we will consider polarizations in Section 2.3 the lattices Γ and L will lie in different ambient hermitian spaces which justifies the difference of notations. For the same reasons we will write h for the hermitian forms coming from polarizable tori and H for R-lattices.

Theorem 1. *Let R be an order in a quadratic imaginary field K. There is an equivalence of categories between $\boldsymbol{\mathcal{A}}_R$, abelian varieties isomorphic to a product of elliptic curves with CM by R, and $\boldsymbol{\mathcal{L}}_R$, R-lattices given by*

$$\begin{array}{rccc} \mathbf{F}\colon & \boldsymbol{\mathcal{A}}_R & \to & \boldsymbol{\mathcal{L}}_R \\ & A \text{ s.t. } A(\mathbb{C}) \simeq V/\Gamma & \mapsto & \Gamma \\ & (\mathbb{C}\otimes L)/L & \leftarrow\!\shortmid & L. \end{array}$$

on objects and for $f\colon A(\mathbb{C}) \simeq V/\Gamma \to A'(\mathbb{C}) \simeq V'/\Gamma', \mathbf{F}(f) = f_{rat}$.

Proof. Let $A \in \boldsymbol{\mathcal{A}}_R$ such that $\mathbf{T}(A) = A(\mathbb{C}) = V/\Gamma$. There is an isomorphism $\varphi\colon V/\Gamma \to \mathbb{C}^g/\bigoplus \Lambda_i$. The $\mathbb{Z}$-lattices Λ_i have a natural structure of $R = \mathrm{End}(\Lambda_i)$-module. The lattice Γ is stable by multiplication by R, indeed,

$$\varphi_{\mathrm{an}}(R\Gamma) = R\varphi_{\mathrm{an}}(\Gamma) = R\bigoplus_i \Lambda_i = \bigoplus_i \Lambda_i = \varphi_{\mathrm{an}}(\Gamma)$$

so, $R\Gamma = \Gamma$. Moreover, the isomorphism φ endows Γ with a structure of R-module in a natural way

$$r.\gamma = \varphi_{\mathrm{an}}^{-1}(r\varphi_{\mathrm{an}}(\gamma)) = r\gamma, \text{ for } r \in R, \gamma \in \Gamma. \tag{1}$$

Hence, Γ has a structure of R-module and we can see in (1) that this structure does not depend on the isomorphism φ we chose.

Reciprocally, let L be a R-lattice and $(\mathfrak{a}_i, x_i)$ a pseudo-basis of it. Since, the $\mathfrak{a}_i$ are fractional ideals there exists an integer n such that $n\mathfrak{a}_i \subseteq R$, for all i, so the multiplication by n map defines an isogeny $\mathrm{Hom}_{\mathbb{C}}(L, R^g)$. If we endow R^g with the canonical hermitian form $h_0(x,y) = {}^t x\overline{y}$, we have $h_0(R^g, R^g) = R$, hence,

$$\mathrm{im}\, h_0(R^g, R^g) = (\mathrm{im}\,\omega)\mathbb{Z} = \alpha_R\mathbb{Z}.$$

Thus, $\left(R^g, \frac{1}{\alpha_R}h_0\right)$ defines a polarized torus and so does $\left(\Gamma, \frac{n^2}{\alpha_R}h_0\right)$. This proves that the underlying $\mathbb{Z}$-lattice of a R-lattice Γ is polarizable.

Finally, given a morphism $f\colon V/\Gamma \to V'/\Gamma', \mathbf{F}(f) = f_{\mathrm{rat}}\colon \Gamma \to \Gamma'$ and since $f_{\mathrm{rat}} = f_{\mathrm{an}|\Gamma}$ and f_{an} is $\mathbb{C}$-linear, and then R-linear, it is clear that $\mathbf{F}$ maps arrows in a full and faithful way.

Hence, there is an equivalence of categories between R-lattices and polarizable tori X such that there exists an isomorphism $X \to \mathbb{C}/\bigoplus \Lambda_i$. The later being in equivalence with the category of abelian varieties isomorphic to a power of elliptic curves with CM by R. This proves the first equivalence of categories we want to show between $\boldsymbol{\mathcal{A}}_R$ and $\boldsymbol{\mathcal{L}}_R$. □

It may be interesting to enhance why the CM case is so specific. If we consider the functor $\mathbf{F}$ from abelian varieties over $\mathbb{C}$ without restriction to the category of sub $\mathbb{Z}$-lattices of a finite dimensional $\mathbb{C}$-vector space $\mathbf{F}$ is not essentially surjective. Indeed, some $\mathbb{Z}$-lattices Γ of V of dimension greater than 2 are not polarizable. Even if we restrict $\mathbf{F}$ on its essential image it is not full. Indeed, even in dimension 1 there are morphisms of polarizable $\mathbb{Z}$-lattices (i.e., morphisms of groups) which are not the restriction of a $\mathbb{C}$-linear map.

Hence, the structure of $\mathbb{Z}$-module is not enough. Fortunately, considering the R-module structure given by the complex multiplication makes $\mathbf{F}$ an equivalence.

2.3 Polarizable tori and integral lattices

A *hermitian R-lattice* is defined as a couple (L, H) with L a R-lattice and H a positive definite hermitian form on the ambient space KL. The *scale* of a hermitian lattice (L, H) is defined as the fractional ideal $\mathfrak{s}(L) = H(L, L) \subseteq K$. The *dual lattice* $L^{\#}$ of a hermitian lattice is the lattice defined by $L^{\#} = \{v \in V, H(v, L) \subseteq R\}$. We say that (L, H) is $\mathfrak{a}$-*modular* if $\mathfrak{a}L^{\#} = L$. If (L, H) is $\mathfrak{a}$-modular then its scale satisfies $\mathfrak{s}(L) = \mathfrak{a}$. A hermitian R-lattice (L, H) is said to be *integral* if

$$H(L, L) \subseteq R,$$

i.e., it is integral if its scale is an integral ideal and it is also equivalent to $L \subseteq L^{\#}$. A hermitian lattice (L, H) which is R-modular is called *unimodular*, it is equivalent to the conditions (L, H) is integral and its scale is $\mathfrak{s}(L) = (1) = R$. One also defines the *volume* of a hermitian lattice (L, H) as the fractional ideal

$$\mathfrak{v}(L) = \left(\bigoplus_{i=1}^{g} N(\mathfrak{a}_i)\right) \det(G(x_1, \ldots, x_g))R$$

where $G(b)$ denotes the Gram matrix of a family b, namely, $G(b) = (H(x, y))_{x,y\in b}$. A hermitian lattice (L, H) is $\mathfrak{a}$-modular if, and only if,

$$\mathfrak{v}(L) = \mathfrak{a}^g \text{ and } \mathfrak{s}(L) = \mathfrak{a}.$$

(see [Hof91, Section 2]).

In this section we want to explain the link between polarized tori and integral lattices.

Let (V, H) be a hermitian $\mathbb{C}$-vector space and let $\alpha \in \mathbb{R}_{>0}$. We denote by V^{α} the vector space V provided with the hermitian form $H^{\alpha}(x, y) = \alpha H(x, y)$. For a lattice L in (V, H) we denote by L^{α} the hermitian lattice L regarded in the hermitian space (V^{α}, H^{α}) like in [O'M00, Section 82J.].

Lemma 1. *Let $\mathfrak{a}$ be a sub $R = \mathbb{Z}[\omega]$-module of $\mathbb{C}$. Then $\mathfrak{a}$ is an integral ideal of R if, and only if,* $\operatorname{im}\mathfrak{a} \subseteq \alpha_R\mathbb{Z}$*, with* $\alpha_R = \operatorname{im}\omega$.

Proof. The direct sense is straightforward.

Let $a = x + y\omega \in \mathfrak{a}$ with $x, y \in \mathbb{R}$. Since, $\operatorname{im} a = y \operatorname{im}(\omega) \in (\operatorname{im}\omega)\mathbb{Z}$ we have $y \in \mathbb{Z}$. Moreover, $\overline{\omega} \in R$ so $a\overline{\omega} \in \mathfrak{a}$ and $\operatorname{im} a\overline{\omega} = -x \operatorname{im}\omega$ so $x \in \mathbb{Z}$. Hence, $a \in \mathbb{Z}[\omega] = R$ and then $\mathfrak{a} \subseteq R$. □

Proposition 1. *Let $(V/\Gamma, \rho_h)$ be a polarized torus such that $\Gamma \simeq \bigoplus_{i=1}^{g} \Lambda_i$ with $\mathrm{End}_{\mathbb{C}}(\Lambda_i) \simeq R$ with $R = \mathbb{Z}[\omega]$. Then $\mathfrak{s}(\Gamma^{\alpha_R})$ is an integral ideal of R. Moreover, we have the relation*

$$\deg \rho_h = ((\Gamma^{\alpha_R})^{\#} \colon \Gamma^{\alpha_R}).$$

Proof. We know that $h(\Gamma, \Gamma)$ is a sub R-module of $\mathbb{C}$ and since (Γ, h) is a polarizable torus we must have $\operatorname{im} h(\Gamma, \Gamma) \subseteq \mathbb{Z}$. Hence, by Lemma 1, $\mathfrak{s}(\Gamma^{\alpha_R}) = \alpha_R h(\Gamma, \Gamma) \subseteq R$. Moreover,

$$\begin{aligned}
\deg \rho_h &= (\widehat{\Gamma} \colon \rho_h(\Gamma)) \\
&= (\rho_h^{-1}(\widehat{\Gamma}) \colon \Gamma) \\
&= \#\{v \in V, \operatorname{im} h(v, \Gamma) \subseteq \mathbb{Z}\}/\Gamma \\
&= \#\{v \in V, (\operatorname{im}\omega)h(v, \Gamma) \subseteq R\}/\Gamma \text{ (by Lemma 1)} \\
&= \#((\Gamma^{\alpha_R})^{\#}/\Gamma) \\
&= ((\Gamma^{\alpha_R})^{\#} \colon \Gamma^{\alpha_R}).
\end{aligned}$$

□

Remark 1. *If moreover the lattice $(\Gamma^{\alpha_R}, h^{\alpha_R})$ is $\mathfrak{s}(\Gamma^{\alpha_R})$-modular then*

$$\deg \rho_h = ((\Gamma^{\alpha_R})^{\#} \colon \mathfrak{s}(\Gamma^{\alpha_R}).(\Gamma^{\alpha_R})^{\#}) = N(\mathfrak{s}(\Gamma^{\alpha_R}))^g.$$

Hence, classes of principally polarized tori (Γ, h), i.e., with $\deg \rho_h = 1$ correspond to isometry classes of integral lattices whose scale has norm 1 and it is an integral ideal by Proposition 1. So it corresponds to unimodular lattices.

Let $\Lambda \subseteq \mathbb{C}$ be a lattice such that $\mathrm{End}(\Lambda) = R$. We define $\boldsymbol{\mathcal{T}}_R^g$ the subcategory of polarized torus $(X = V/\Gamma, \rho_h)$, with $\Gamma \simeq \bigoplus \Lambda_i$ with $\mathrm{End}(\Lambda_i) \simeq R$. We can conclude with the following theorem.

Theorem 2. *With the notations above there is an equivalence of categories given on objects by*

$$\begin{array}{rl} \boldsymbol{\mathcal{T}}_R^p & \to \boldsymbol{\mathcal{L}}_R^{h,int} \\ (X = V/\Gamma, \rho_h) & \mapsto (\Gamma^{\alpha_R}, h^{\alpha_R}) \\ ((L \otimes \mathbb{C})/L, H^{1/\alpha_R}) & \leftarrow\!\shortmid (L, H). \end{array}$$

Since, $\boldsymbol{\mathcal{T}}_R^p$ is equivalent to the category $\boldsymbol{\mathcal{A}}_R^p$ by the functor $\mathbf{T}$, we have the second equivalence we wanted between $\boldsymbol{\mathcal{A}}_R^p$ and $\boldsymbol{\mathcal{L}}_R^{h,int}$. We call this functor $\mathbf{F}_h$ and it satisfies

$$\begin{array}{rccl} \mathbf{F}_h\colon & \boldsymbol{\mathcal{A}}_R^p & \to \boldsymbol{\mathcal{L}}_R^{h,int} \\ & (A, a) & \mapsto (\mathbf{F}(A)^{\alpha_R}, \mathbf{F}(a)^{\alpha_R}). \end{array}$$

Since every elliptic curve over $\mathbb{C}$ with CM by R has a model over $\overline{\mathbb{Q}}$, the category of polarized abelian varieties over $\overline{\mathbb{Q}}$ isomorphic to a product of E_i with CM by R is equivalent to $\boldsymbol{\mathcal{A}}_R^p$ by the base change functor

$$A \mapsto A_{\mathbb{C}}.$$

Note that morphisms over $\mathbb{C}$ of abelian varieties over $\overline{\mathbb{Q}}$ isomorphic to a product of CM elliptic curves are actually defined over $\overline{\mathbb{Q}}$ by [Sil94, Theorem 2.2.(c)].

3 Action of $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$

The *field of moduli* of a polarized abelian variety (A, a) over $\overline{\mathbb{Q}}$ is the fixed field by the subgroup

$$\{\sigma \in \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right), (A^\sigma, a^\sigma) \simeq (A, a)\}.$$

Given a maximal order in an imaginary quadratic field K we would like to elaborate an algorithm to enumerate all the isomorphism classes of $\boldsymbol{\mathcal{A}}_R^p$ which have field of moduli $\mathbb{Q}$. In order to do this we want to understand the action of $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$ on the hermitian lattices through the functor $\mathbf{F}_h$ we developed in Section 2. In other words given $(A, a) \in \boldsymbol{\mathcal{A}}_R^p$ and $\sigma \in \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$ we want to understand the isometry class of $\mathbf{F}_h(A^\sigma, a^\sigma)$ in terms of $\mathbf{F}_h(A, a)$ and σ.

In order to do so we need to understand the action of $\mathrm{Gal}\left(\overline{\mathbb{Q}}/K\right)$ and the one of the complex conjugation $\mathrm{Gal}(K/\mathbb{Q})$ separately to recover the action of $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) \simeq \mathrm{Gal}\left(\overline{\mathbb{Q}}/K\right) \rtimes \mathrm{Gal}(K/\mathbb{Q})$. We describe the action of $\mathrm{Gal}(K/\mathbb{Q})$ and $\mathrm{Gal}\left(\overline{\mathbb{Q}}/K\right)$ in Theorem 3 and Theorem 4 respectively. The end of this section will be devoted to their proof.

Let us introduce the necessary notations to state the results we aim to show in this section.

Let (L, H) be a hermitian lattice. Let $\iota\colon (KL, H) \to (K^g, H')$ be an isometry. We define $(\overline{L}, \overline{H})$ by $\overline{L} = \iota^{-1}\overline{\iota(L)}$ and

$$\overline{H}(x, y) = \overline{H(\iota^{-1}\overline{\iota(x)}, \iota^{-1}\overline{\iota(y)})} = \overline{H'(\overline{\iota(x)}, \overline{\iota(y)})}$$

where $\bar{\cdot}$ refers to the complex conjugation which is the unique non-trivial automorphism of $\mathrm{Gal}(K/\mathbb{Q})$. The isometry class of $(\overline{L}, \overline{H})$ is independent of the choice of ι. We can now state the description of the action of the complex conjugation.

Theorem 3 (Description of the action of $\mathrm{Gal}(K/\mathbb{Q})$)**.** *Let $(A, a) \in \boldsymbol{\mathcal{A}}_R^p$ over $\overline{\mathbb{Q}}$. Let $\mathbf{F}_h(A, a) = (L, H)$ then there is an isometry*

$$\mathbf{F}_h\left(\overline{A}, \overline{a}\right) \simeq \left(\overline{L}, \overline{H}\right).$$

Let E be an elliptic curve defined over $\overline{\mathbb{Q}}$ with CM by R. Let $\Lambda \subseteq \mathbb{C}$ be a lattice such that $E_{\mathbb{C}} = E_\Lambda$. In the future we will often confuse E and its base change by $E_{\mathbb{C}}$ to avoid heavy notations such as $E_{\mathbb{C}}(\mathbb{C})$ and we will write $E(\mathbb{C})$ instead. Recall that for $\dot{\mathfrak{a}} \in \mathrm{Cl}(R)$, the elliptic curve $\dot{\mathfrak{a}} \star E_\Lambda$ is defined by $E_{\mathfrak{a}^{-1}\Lambda}$. By [Sil94, Proposition 2.4], there is a surjective group morphism

$$F\colon \mathrm{Gal}\left(\overline{\mathbb{Q}}/K\right) \to \mathrm{Cl}(R) \tag{2}$$

such that the elliptic curves E^σ and $F(\sigma) \star E$ are isomorphic. We can now state the description of the action of $\mathrm{Gal}\left(\overline{\mathbb{Q}}/K\right)$.

Theorem 4 (Description of the action of $\mathrm{Gal}\left(\overline{\mathbb{Q}}/K\right)$)**.** *Let* $(A,a) \in \mathcal{A}_R^p$ *over* $\overline{\mathbb{Q}}$*. Let* $\mathbf{F}_h(A,a) = (L,H), \sigma \in \mathrm{Gal}\left(\overline{\mathbb{Q}}/K\right)$ *and* $F(\sigma) = \dot{\mathfrak{a}}^{-1} \in \mathrm{Cl}(R)$*. Then there is an isometry*

$$\mathbf{F}_h(A^\sigma, a^\sigma) \simeq \left(\mathfrak{a}L, \frac{1}{N(\mathfrak{a})}H\right)$$

where $N(\mathfrak{a})$ *is the norm of* $\mathfrak{a}$*.*

The proof of Theorem 3 is made easier by the Lemma 2 which uses the fact that the complex conjugation in $\mathrm{Aut}(\mathbb{C})$ is a continuous map of $\mathbb{C}$. With the identity they are the only automorphisms in $\mathrm{Aut}(\mathbb{C})$ with this property.

3.1 Positioning of the problem

Let us recall from Figure 1 that for every elliptic curve with CM by R and any isomorphism $\eta\colon \mathbb{C}/\Lambda \to E(\mathbb{C})$ there is a unique isomorphism $[\cdot]_E\colon R \to \mathrm{End}(E)$ such that the following diagram commutes

$$\begin{array}{ccc} \mathbb{C}/\Lambda & \xrightarrow{\alpha} & \mathbb{C}/\Lambda \\ {\scriptstyle\eta}\downarrow & & \downarrow{\scriptstyle\eta} \\ E_\Lambda(\mathbb{C}) & \xrightarrow{[\alpha]} & E_\Lambda(\mathbb{C}). \end{array}$$

By, [Sil94, Theorem 2.2] the bracket isomorphism satisfies

$$\text{for all } \sigma \in \mathrm{Aut}(\mathbb{C}), \alpha \in R, ([\alpha]_E)^\sigma = [\alpha^\sigma]_{E^\sigma}.$$

This is true with whatever Λ and $\eta\colon \mathbb{C}/\Lambda \xrightarrow{\sim} E(\mathbb{C})$ we chose and whatever lattice identification $\eta_\sigma\colon \mathbb{C}/\Lambda_\sigma \xrightarrow{\sim} E^\sigma(\mathbb{C})$ of E^σ as soon as we again chose the same on left and right hand sides of the diagram. Of course if we don't take the same isomorphisms on the right and on the left hand sides, for instance we chose η and $-\eta$, those properties do not hold anymore. The main difficulty we will encounter is that we want to deal with isogenies $f\colon E \to E'$ between possibly non-isomorphic elliptic curves. If we expect diagrams like

$$\begin{array}{ccc} \mathbb{C}/\Lambda & \xrightarrow{\alpha} & \mathbb{C}/\Lambda' \\ {\scriptstyle\eta}\downarrow & & \downarrow{\scriptstyle\eta'} \\ E(\mathbb{C}) & \xrightarrow{f} & E'(\mathbb{C}). \end{array}$$

to have nice behaviour with $\mathrm{Aut}(\mathbb{C})$ or just $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$ we need a kind of canonical way to describe the action of $\mathrm{Aut}(\mathbb{C})$ (or $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$) on lattices, and a canonical way to chose the isomorphisms η (to avoid the $-\eta$ issue for instance). We will show that the $\wp$-functions of Weierstrass will do the job.

First we need to specify the isomorphisms we refer to when we consider the analytic representation of a morphism between abelian varieties. Let A and A' be abelian varieties over $\mathbb{C}$. Consider isomorphisms $\eta\colon V/\Gamma \xrightarrow{\sim} A(\mathbb{C})$ and $\eta'\colon V'/\Lambda' \xrightarrow{\sim} A'(\mathbb{C})$. Every morphism $f\colon A \to A'$ induces a commutative diagram as in Figure 2.

$$\begin{array}{ccc} V/\Gamma & \xrightarrow{\varphi} & V'/\Gamma' \\ {\scriptstyle\eta}\downarrow & & \downarrow{\scriptstyle\eta'} \\ A(\mathbb{C}) & \xrightarrow{f} & A'(\mathbb{C}). \end{array}$$

Figure 2: Analytic representation of an isogeny

The morphism of tori φ can be lifted to a linear map $\alpha\colon V \to V'$ such that $\alpha(\Gamma) \subseteq \Gamma'$. We call α the analytic representation of f associated to the isomorphisms η and η' or simply the analytic representation of (f,η,η').

We will use the Weierstrass $\wp$-functions and Eisenstein series as in [Sil09] as a canonical way to identify an elliptic curve over $\mathbb{C}$ with a complex torus and we will study the rationality of the induced analytic representation for CM elliptic curves in Section 3.2. Then we will extend the results for elliptic curves on product of elliptic curves component by component in Section 3.3 to prove Theorem 3 and 4.

3.2 Action of $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$ on CM elliptic curves

3.2.1 Fixing isomorphisms with Weierstrass $\wp$-functions

By [Sil09, Therorem 5.1], for any $A, B \in \mathbb{C}$ such that $4A^3 - 27B^2 \neq 0$ there exists a unique lattice $\Lambda \subset \mathbb{C}$ such that

$$A = g_2(\Lambda) = 60 \sum_{\omega \in \Lambda \setminus \{0\}} \frac{1}{\omega^4} \text{ and } B = g_3(\Lambda) = 140 \sum_{\omega \in \Lambda \setminus \{0\}} \frac{1}{\omega^6}$$

where $g_2(\Lambda)$ and $g_3(\Lambda)$ are the Eisenstein series of index 4 and 6 of Λ. Moreover, denoting Weierstrass $\wp$-functions by $\wp$, by [Sil09, Proposition 3.6] the map

$$\begin{array}{rccc} \phi_\Lambda \colon & \mathbb{C}/\Lambda & \to & \mathbb{P}^2(\mathbb{C}) \\ & z & \mapsto & [\wp(z,\Lambda) \colon \wp'(z,\Lambda) \colon 1] \end{array}$$

defines an isomorphism of Lie groups on its image $E(\mathbb{C})$ with $E/\mathbb{C}$ with Weierstrass model

$$E \colon y^2 = 4x^3 - Ax - B.$$

We will also call ϕ_Λ the induced isomorphism $\mathbb{C}/\Lambda \xrightarrow{\sim} E(\mathbb{C})$.

From now on, the notation E_Λ means that $E(\mathbb{C}) \simeq \mathbb{C}/\Lambda$ with the isomorphism given by ϕ_Λ.

Let $\kappa \to \mathbb{C}$ be a field extension and $E \colon y^2 = 4x^3 - Ax - B$ with $A, B \in \kappa$ and let Λ be a lattice such that $g_2(\Lambda) = A$ and $g_3(\Lambda) = B$. For any $\sigma \in \mathrm{Aut}(\kappa)$ we define Λ_σ as the unique lattice such that $g_2(\Lambda_\sigma) = A^\sigma$ and $g_3(\Lambda_\sigma) = B^\sigma$.

By definition of Λ_σ we have an isomorphism $\phi_{\Lambda_\sigma} \colon \mathbb{C}/\Lambda_\sigma \to E^\sigma(\mathbb{C})$ with $E^\sigma \colon y^2 = 4x^3 - A^\sigma x - B^\sigma$.

Lemma 2. *For any lattice $\Lambda \subset \mathbb{C}$,*

$$\Lambda_{\bar{\cdot}} = \overline{\Lambda}.$$

Proof. The Eisenstein series $g_2(\Lambda)$ and $g_3(\Lambda)$ are absolutely convergent and the complex conjugation is a continuous map so

$$g_k(\overline{\Lambda}) = \overline{g_k(\Lambda)}.$$

□

3.2.2 Rationality of analytic representations for CM elliptic curves

By [Sil94, Theorem 2.2.(c)] an isogeny $f \colon E \to E'$ between two elliptic curves defined over $\overline{\mathbb{Q}}$ is also defined over $\overline{\mathbb{Q}}$. In this section we want to study the analytic representation α of $(f, \phi_\Lambda, \phi_{\Lambda'})$ when E and E' have Weierstrass model over $\overline{\mathbb{Q}}$, with $\mathbb{C}/\Lambda \underset{\phi_\Lambda}{\simeq} E(\mathbb{C})$ and $\mathbb{C}/\Lambda' \underset{\phi_{\Lambda'}}{\simeq} E'(\mathbb{C})$.

- Is α in $\overline{\mathbb{Q}}$?
- If $\alpha \in \overline{\mathbb{Q}}$, does α behave well with $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$, i.e., is α^σ the analytic representation of $(f^\sigma, \phi_{\Lambda_\sigma}, \phi_{\Lambda'_\sigma})$?

We will positively answer these questions in Proposition 2.

Lemma 3. *Let $\Lambda \subseteq \mathbb{C}$ be a lattice and $E \colon y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)$ be the elliptic curve over $\mathbb{C}$ associated to Λ by ϕ_Λ. Let $r \in \mathbb{C}$, let E' be the elliptic curve associated to $r\Lambda$ and let ν_r be the map defined by.*

$$\begin{array}{rccc} \nu_r & \mathbb{P}^2(\mathbb{C}) & \longrightarrow & \mathbb{P}^2(\mathbb{C}) \\ & [x \colon y \colon 1] & \longmapsto & [\frac{1}{r^2}x \colon \frac{1}{r^3}y \colon 1] \end{array}$$

Then the restriction of ν_r to $E(\mathbb{C}) \subseteq \mathbb{P}^2(\mathbb{C})$ defines an isomorphism on its image $E'(\mathbb{C})$. Moreover, r is the analytic representation of $(\nu_{r|E(\mathbb{C})}, \phi_\Lambda, \phi_{r\Lambda})$.

Proof. For all $z \in \mathbb{C} \setminus r\Lambda, r \in \mathbb{C} \setminus \{0\}$, $\wp(z, r\Lambda) = \frac{1}{r^2}\wp(\frac{z}{r}, \Lambda)$ and $\wp'(z, r\Lambda) = \frac{1}{r^3}\wp'(\frac{z}{r}, \Lambda)$. Hence,

$$\begin{aligned} \phi_{r\Lambda}(z) &= [\wp(z, r\Lambda) \colon \wp'(z, r\Lambda) \colon 1] \\ &= [\frac{1}{r^2}\wp\left(\frac{z}{r}, \Lambda\right) : \frac{1}{r^3}\wp'\left(\frac{z}{r}, \Lambda\right) : 1] \\ &= \nu_r\left(\phi_\Lambda\left(\frac{z}{r}\right)\right). \end{aligned}$$

This proves that the following diagram commutes

$$\begin{array}{ccc} \mathbb{C}/\Lambda & \xrightarrow{r} & \mathbb{C}/r\Lambda \\ {\scriptstyle \phi_\Lambda}\downarrow & & \downarrow{\scriptstyle \phi_{r\Lambda}} \\ E(\mathbb{C}) & \xrightarrow{\nu_{r\,|\,E(\mathbb{C})}} & E'(\mathbb{C}). \end{array}$$

which shows that $(\nu_{r\,|\,E(\mathbb{C})}, \phi_\Lambda, \phi_{r\Lambda})$ has analytic representation r □

Let $\mathfrak{a}$ be any fractional ideal of R, Λ a lattice and $E = E_\Lambda \in \boldsymbol{\mathcal{A}}_R$. We defined $\mathfrak{a} \star E$ earlier as the isomorphism class of $E_{\mathfrak{a}^{-1}\Lambda}$.

From now on we will refer to $\mathfrak{a} \star E$ as the elliptic curve defined by the Weierstrass equation

$$\mathfrak{a} \star E \colon y^2 = 4x^3 - g_2(\mathfrak{a}^{-1}\Lambda)x - g_3(\mathfrak{a}^{-1}\Lambda).$$

Let $f \colon E \to E'$ be an isogeny between elliptic curves with $E' = E_{\Lambda'}$. Let $\mathfrak{a}$ be an integral ideal of R such that $\ker f = E[\mathfrak{a}] = \cap_{a \in \mathfrak{a}} \ker[a]_E$. According to [Sil94, Proposition 1.4], $\mathfrak{a} \star E \simeq E/E[\mathfrak{a}]$ and we can factor $f \colon E \to E'$ and $\alpha \colon \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ as in Figure 3 where $\pi \colon \mathbb{C}/\Lambda \to \mathbb{C}/\mathfrak{a}^{-1}\Lambda$ is the natural projections and $p \colon E \to \mathfrak{a} \star E$ induced by π.

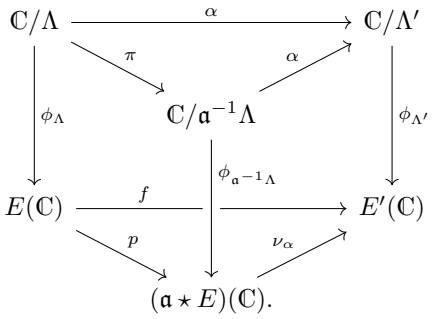


Figure 3: Factorization of isogenies

Lemma 4. *Let Λ be a lattice with complex multiplication such that $g_k(\Lambda) \in \overline{\mathbb{Q}}$ for $k = 2, 3$. Then for any fractional ideal $\mathfrak{a} \subseteq K$, $g_k(\mathfrak{a}^{-1}\Lambda) \in \overline{\mathbb{Q}}$.*

Proof. Let $E \colon y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)$ over $\overline{\mathbb{Q}}$. Since all CM elliptic curve have a model over $\overline{\mathbb{Q}}$ we consider $E' \colon y^2 = 4x^3 - A'x - B'$ a model of $\mathfrak{a} \star E$ over $\overline{\mathbb{Q}}$ and Λ' such that $g_2(\Lambda') = A' \in \overline{\mathbb{Q}}$ and $g_3(\Lambda') = B' \in \overline{\mathbb{Q}}$, i.e., $E' = E_{\Lambda'}$. Consider any isogeny $f \colon E \to E'$ over $\overline{\mathbb{Q}}$ and $\alpha \in \mathbb{C}$ the analytic representation of $(f, \phi_\Lambda, \phi_{\Lambda'})$. Let $r \in \overline{\mathbb{Q}}$ be the coefficient of the induced map on differentials $f^* \frac{dx'}{y'} = r\frac{dx}{y}$. By the proof of [Sil09, Proposition 3.6.(b)] we have $\phi_\Lambda^* \left(\frac{dx}{y}\right) = dz$ for any $E = E_\Lambda$. Thus,

$$(f \circ \phi_\Lambda)^* \left(\frac{dx'}{y'}\right) = \phi_\Lambda^* \circ f^* \left(\frac{dx'}{y'}\right) = \phi_\Lambda^* \left(r\frac{dx}{y}\right) = rdz$$

and

$$(\phi_{\Lambda'} \circ \alpha)^* \left(\frac{dx'}{y'}\right) = \alpha dz' = \alpha dz$$

Since the following diagram commutes

$$\begin{array}{ccc} \mathbb{C}/\Lambda & \xrightarrow{\alpha} & \mathbb{C}/\Lambda' \\ {\scriptstyle \phi_\Lambda}\downarrow & & \downarrow{\scriptstyle \phi_{\Lambda'}} \\ E(\mathbb{C}) & \xrightarrow{f} & E'(\mathbb{C}) \end{array}$$

and we have equality of the differentials $rdz = \alpha dz$. Hence, $r = \alpha \in \overline{\mathbb{Q}}$. Let $\mathfrak{b}$ be an integral ideal such that $\ker f = E[\mathfrak{b}]$. By Figure 3, $\Lambda' = \alpha\mathfrak{b}^{-1}\Lambda$ so $g_k(\mathfrak{b}^{-1}\Lambda) = \alpha^{2k} g_k(\Lambda') \in \overline{\mathbb{Q}}$. Finally, $\mathfrak{b}^{-1}\Lambda$ and $\mathfrak{a}^{-1}\Lambda$ give isomorphic elliptic curves so they must be homothetic by some $\lambda \in \mathrm{Hom}_{\mathbb{C}}(\mathfrak{b}^{-1}\Lambda, \mathfrak{a}^{-1}\Lambda) = \{\mu \in \mathbb{C}, \mu\mathfrak{b}^{-1}\Lambda \subseteq \mathfrak{a}^{-1}\Lambda\} \subseteq K$. Hence,

$$g_k(\mathfrak{a}^{-1}\Lambda) = \lambda^{-2k} g_k(\mathfrak{b}^{-1}\Lambda) \in \overline{\mathbb{Q}}.$$

□

Proposition 2. *Let $E\colon y^2 = 4x^3 - Ax - B$ over $\overline{\mathbb{Q}}$ and $E'\colon y^2 = 4x^3 - A'x - B'$ over $\mathbb{C}$ be elliptic curves both with CM by R. Let Λ and Λ' be lattices with $g_2(\Lambda) = A, g_3(\Lambda) = B, g_2(\Lambda') = A'$ and $g_3(\Lambda') = B'$. Let $f\colon E \to E'$ be an isogeny over $\mathbb{C}$. Consider $\alpha \in \mathbb{C}$ the analytic representation of $(f, \phi_\Lambda, \phi_{\Lambda'})$. Then*

1. *$\alpha \in \overline{\mathbb{Q}}$ if, and only if, $g_i(\Lambda') \in \overline{\mathbb{Q}}$.*
2. *If 1. is satisfied then for every $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), \alpha^\sigma$ is the analytic representation of $(f^\sigma, \phi_{\Lambda_\sigma}, \phi_{\Lambda'_\sigma})$ with f identified with the induced map over $\overline{\mathbb{Q}}$.*
3. *For every fractional ideal $\mathfrak{a}$ we have $(\mathfrak{a}\Lambda)_\sigma = \mathfrak{a}^\sigma \Lambda_\sigma$.*

Proof.

1. Since $\Lambda' = \alpha\mathfrak{a}^{-1}\Lambda$ we have $g_k(\Lambda') = \alpha^{-2k} g_k(\mathfrak{a}^{-1}\Lambda)$. By Lemma 4, $g_k(\mathfrak{a}^{-1}\Lambda) \in \overline{\mathbb{Q}}$ so $\alpha \in \overline{\mathbb{Q}}$ if, and only if, $g_k(\Lambda') \in \overline{\mathbb{Q}}$.

2. We define α_σ the analytic representation of $(f^\sigma, \phi_{\Lambda_\sigma}, \phi_{\Lambda'_\sigma})$. We want to show that $\alpha_\sigma = \alpha^\sigma$. Since Λ_σ and Λ'_σ are such that $g_i(\Lambda_\sigma) \in \overline{\mathbb{Q}}$ and $g_i(\Lambda'_\sigma) \in \overline{\mathbb{Q}}$, by 1. $\alpha_\sigma \in \overline{\mathbb{Q}}$. According to [Sil94, Theorem 2.2],

$$\ker(f^\sigma) = (\ker f)^\sigma = \cap_{a\in\mathfrak{a}} (\ker[a]_E)^\sigma = \cap_{a\in\mathfrak{a}} \ker[a^\sigma]_{E^\sigma} = E^\sigma[\mathfrak{a}^\sigma]. \tag{3}$$

Since, $f^\sigma = \left(\nu_{\alpha|(\mathfrak{a}\star E)(\overline{\mathbb{Q}})}\right)^\sigma \circ p^\sigma$ and $\left(\nu_{\alpha|(\mathfrak{a}\star E)(\overline{\mathbb{Q}})}\right)^\sigma$ is an isomorphism, $\ker f^\sigma = \ker p^\sigma$. By definition of $E[\mathfrak{a}]$ we have

$$[\wp(z,\Lambda)\colon \wp'(z,\Lambda)\colon 1] \in E[\mathfrak{a}] \text{ if, and only if, } z \in \mathfrak{a}^{-1}\Lambda. \tag{4}$$

Moreover, $[\wp(z,\Lambda_\sigma)\colon \wp(z,\Lambda_\sigma)\colon 1] \in \ker p^\sigma$ if, and only if, $z \in (\mathfrak{a}^{-1}\Lambda)_\sigma$ by definition of p^σ but, $z \in (\mathfrak{a}^\sigma)^{-1}\Lambda_\sigma$ because $\ker p^\sigma = E^\sigma[\mathfrak{a}^\sigma]$. Thus, by the relations (3) and (4), we have $(\mathfrak{a}^{-1}\Lambda)_\sigma = (\mathfrak{a}^\sigma)^{-1}\Lambda_\sigma$ (this proves the point 3 of the proposition).

This proves that $(\mathfrak{a}\star E)^\sigma = \mathfrak{a}^\sigma \star E^\sigma$. We also have the factorization

$$f^\sigma = \left(\nu_{\alpha|(\mathfrak{a}\star E)(\overline{\mathbb{Q}})}\right)^\sigma \circ p^\sigma = \nu_{\alpha_\sigma|(\mathfrak{a}^\sigma\star E^\sigma)(\overline{\mathbb{Q}})} \circ p^\sigma.$$

Since p^σ is an isogeny it is surjective. So, the maps $(\nu_{\alpha|\mathbb{P}^2(\overline{\mathbb{Q}})})^\sigma$ and $\nu_{\alpha_\sigma|\mathbb{P}^2(\overline{\mathbb{Q}})}$ coincide and then

$$\frac{1}{\alpha_\sigma^2} = \frac{1}{(\alpha^\sigma)^2} \text{ so } \alpha_\sigma = \pm\alpha^\sigma \text{ and } \frac{1}{\alpha_\sigma^3} = \frac{1}{(\alpha^\sigma)^3} \text{ so } \alpha_\sigma = j\alpha^\sigma$$

for some $j^3 = 1$. Hence, $\alpha_\sigma = \alpha^\sigma$.

□

A nice consequence is that if we take E_Λ with $g_i(\Lambda) \in \overline{\mathbb{Q}}$ then $E_{\mathfrak{a}^{-1}\Lambda}$ has also its Weierstrass model over $\overline{\mathbb{Q}}$ and $\mathrm{Hom}_{\mathbb{C}}(E_\Lambda, E_{\mathfrak{a}^{-1}\Lambda}) = \mathrm{Hom}_{\overline{\mathbb{Q}}}(E_\Lambda, E_{\mathfrak{a}^{-1}\Lambda})$ so the analytic representation of this isogenies associated to the isomorphisms ϕ_Λ and $\phi_{\mathfrak{a}^{-1}\Lambda}$ are in $\mathrm{Hom}_{\mathbb{C}}(\Lambda, \mathfrak{a}^{-1}\Lambda) \subseteq K$. We recall from [Sil94, Proposition 1.2] that $\mathrm{Cl}(R)$ acts simply transitively on the elliptic curves with CM by R. Thus, given two elliptic curves E and E' over $\overline{\mathbb{Q}}$ we can always find a model E'' of E' such that the analytic representations of isogenies from E to E'' are in K.

Given an automorphism $\sigma \in \mathrm{Gal}\left(\overline{\mathbb{Q}}/K\right)$ for $F(\sigma) = \dot{\mathfrak{a}}$, with F defined in (1), by [Sil94, Proposition 2.4] we know that E^σ and $\mathfrak{a}\star E$ are isomorphic. This means that their corresponding lattices Λ_σ and $\mathfrak{a}^{-1}\Lambda$ (via the $\wp$-functions) are homothetic by some constant $r_\sigma \in \mathbb{C}$ which depends, a priori, on Λ, σ and the choice of the representative $\mathfrak{a}$ of $F(\sigma)$ we chose. An immediate consequence of Proposition 2 is that r_σ is in $\overline{\mathbb{Q}}$. The issue is that chosing another lattice Λ' would lead to another $r'_\sigma \in \overline{\mathbb{Q}}$. The next proposition shows that, under some condition, we can chose the same r_σ for different lattices.

Proposition 3 (Action of $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ on elliptic curves)**.** *Let $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/K)$ be an automorphism and $\mathfrak{a}$ be a fractional ideal with $F(\sigma) = \dot{\mathfrak{a}} \in \mathrm{Cl}(R)$. Consider an elliptic curve E_Λ over $\overline{\mathbb{Q}}$. Then there exists $r_\sigma \in \overline{\mathbb{Q}}$ and a commutative diagram*

$$\begin{array}{ccc} E^\sigma(\mathbb{C}) & \xrightarrow{f^\sigma} & E'^\sigma(\mathbb{C}) \\ {\scriptstyle \phi_{\Lambda_\sigma}}\uparrow & & \uparrow{\scriptstyle \phi_{\Lambda'_\sigma}} \\ \mathbb{C}/\Lambda_\sigma & \xrightarrow{\alpha} & \mathbb{C}/\Lambda'_\sigma \\ {\scriptstyle r_\sigma}\downarrow & & \downarrow{\scriptstyle r_\sigma} \\ \mathbb{C}/\mathfrak{a}^{-1}\Lambda & \xrightarrow{\alpha} & \mathbb{C}/\mathfrak{a}^{-1}\Lambda'. \end{array}$$

for all $E'(\mathbb{C}) \underset{\phi_{\Lambda'}}{\simeq} \mathbb{C}/\Lambda'$ such that $\mathrm{Hom}_{\mathbb{C}}(\Lambda, \Lambda') \subseteq K$ and all isogenies $f\colon E_\Lambda \to E_{\Lambda'}$ over $\overline{\mathbb{Q}}$ where $\alpha \in K$ is the analytic representation of $(f, \phi_\Lambda, \phi_{\Lambda'})$.

Proof. Since the group of fractional ideals acts transitively on CM elliptic curves over $\overline{\mathbb{Q}}$ there exists an isomorphism $E^\sigma \to \mathfrak{a} \star E$ which induces an isomorphism on associated tori $r_\sigma\colon \mathbb{C}/\Lambda_\sigma \to \mathbb{C}/\mathfrak{a}^{-1}\Lambda$. Let $\alpha \in K$ be the analytic representation of $(f, \phi_\Lambda, \phi_{\Lambda'})$. There exists an ideal $\mathfrak{b} \subseteq R$ such that $\alpha\Lambda = \mathfrak{b}^{-1}\Lambda'$ and Proposition 2.3 implies that $\alpha^\sigma\Lambda_\sigma = (\mathfrak{b}^{-1})^\sigma\Lambda'_\sigma$. Since $\alpha \in K$ and $\mathfrak{b} \subseteq K$ they are invariant by σ. To prove the proposition, we need to show that $r_\sigma\Lambda'_\sigma = \mathfrak{a}^{-1}\Lambda'$.
On one hand we have

$$\alpha\Lambda_\sigma = \mathfrak{b}^{-1}\Lambda'_\sigma, \tag{5}$$

on the other hand

$$\alpha\mathfrak{a}^{-1}\Lambda = \mathfrak{a}^{-1}\mathfrak{b}^{-1}\Lambda'. \tag{6}$$

Combined with $r_\sigma\Lambda_\sigma = \mathfrak{a}^{-1}\Lambda$, (5) and (6), it gives

$$\begin{aligned} r_\sigma\Lambda'_\sigma &= \mathfrak{b}\alpha\mathfrak{a}^{-1}\Lambda \\ &= \mathfrak{b}\mathfrak{a}^{-1}\mathfrak{b}^{-1}\Lambda' \\ &= \mathfrak{a}^{-1}\Lambda' \end{aligned}$$

which concludes the proof. □

3.2.3 Galois action on polarizations of CM elliptic curves

The canonical polarization on an elliptic curve E is defined by

$$\begin{array}{rccc} a_{0,E}\colon & E & \longrightarrow & \widehat{E} \\ & P & \longmapsto & [P] - [O] \end{array}$$

with O the neutral element of the group E. We use this isomorphism to identify any polarization a of E with an element of End(E) by $a_{0,E}^{-1} \circ a$.

Lemma 5. *Let $E(\mathbb{C}) \underset{\phi_\Lambda}{\simeq} \mathbb{C}/\Lambda$ be an elliptic curve with $\Lambda = \mathfrak{a}x$ with $\mathfrak{a} \subseteq K$ a fractional ideal. The principal polarization $a_{0,E}$ induces the hermitian form*

$$\begin{array}{rccc} h_{0,\Lambda}\colon & \mathbb{C} \times \mathbb{C} & \longrightarrow & \mathbb{C} \\ & (z, w) & \longmapsto & \frac{z\overline{w}}{\alpha_R N(\mathfrak{a}) N(x)} \end{array}$$

with $\alpha_R = \mathrm{im}\,\omega > 0$ and $R = \mathbb{Z}[\omega]$.

Proof. The induced hermitian form is necessarily of the form $h_{0,\Lambda} = \mu h_0$ with $\mu \in \mathbb{R}_{>0}$ and $h_0(z, w) = z\overline{w}$ because the conjugacy classes of hermitian forms on $\mathbb{C}$-vector spaces are determined by their rank and signature. Moreover, since $h_{0,\Lambda}$ is a principal polarization $\mathrm{im}\, h_{0,\Lambda}(\Lambda, \Lambda) = \deg a_{0,E}\mathbb{Z} = \mathbb{Z}$. Hence,

$$\begin{aligned} \mathrm{im}\, h_{0,\Lambda}(\Lambda, \Lambda) &= \mathrm{im}\, h_{0,\Lambda}(\mathfrak{a}x, \mathfrak{a}x) \\ &= \mathrm{im}\, \mu N(\mathfrak{a}) N(x) R \\ &= \mu N(\mathfrak{a}) N(x)\, \mathrm{im}\, R \\ &= \mu N(\mathfrak{a}) N(x) \alpha_R \mathbb{Z} = \mathbb{Z}. \end{aligned}$$

Hence, $\mu = \frac{1}{N(\mathfrak{a})N(x)\alpha_R}$. □

We want to investigate first how does $\mathrm{Gal}\left(\overline{\mathbb{Q}}/K\right)$ act on polarizations.

Let $\phi_\Lambda\colon \mathbb{C}/\Lambda \to E(\mathbb{C})$ with $\Lambda = \mathfrak{b}x$. We write $\mathbf{F}_h(E_\Lambda, a_{0,E}) = (\Lambda, H_{0,\Lambda})$ with $H_{0,\Lambda} = h_{0,\Lambda}^{\alpha_R}$ and, by Lemma 5, we can write the Gram matrix of $H_{0,\Lambda}$ in the K basis x of $K\Lambda$, by $G_\Lambda(x) = \frac{1}{N(\mathfrak{b})}$. It is then clear that for all fractional ideal $\mathfrak{a}$, we have $\mathfrak{a}\Lambda = \mathfrak{a}\mathfrak{b}x$ and thus, the Gram matrix of the analytic representation of the canonical polarization of $E_{\mathfrak{a}\Lambda}$ in the basis x is $G_{\mathfrak{a}\Lambda}(x) = \frac{1}{\mathfrak{a}\mathfrak{b}} = \frac{1}{N(\mathfrak{a})}G_\Lambda(x)$.

Moreover, $a_{0,E}^\sigma$ is the canonical polarization a_{0,E^σ} of E^σ for any E and $\sigma \in \mathrm{Aut}(\mathbb{C})$ and every polarization on elliptic curves is of the form $na_{0,E}$ for some $n \in \mathbb{N}^*$. What we did can easily be generalized for any polarization of elliptic curves.

We can conclude with this proposition.

Proposition 4. *Let $E = E_\Lambda \in \boldsymbol{\mathcal{A}}_R, a_{0,E}$ the canonical polarization on E and $\mathbf{F}_h(E, a_{0,E}) = (\Lambda, H_{0,\Lambda})$. Then for any $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/K)$ and $\dot{\mathfrak{a}}^{-1} = F(\sigma)$ there is an isometry*

$$\mathbf{F}_h(E^\sigma, a_{0,E}) \simeq \left(\mathfrak{a}\Lambda, \frac{1}{N(\mathfrak{a})}H_{0,\Lambda}\right).$$

Proof. Let $\mathbf{F}_h(E^\sigma, a_{0,E^\sigma}) = (\Lambda_\sigma, H_{0,\Lambda_\sigma})$. By Proposition 3 and Lemma 3 we have an isomorphism

$$\nu_{r_\sigma}\colon E^\sigma \longrightarrow \mathfrak{a}^{-1} \star E$$

and $(\mathfrak{a}^{-1} \star E)(\mathbb{C}) \simeq \mathbb{C}/\mathfrak{a}\Lambda$. We have $\mathbf{F}_h(\mathfrak{a}^{-1} \star E, a_{0,\mathfrak{a}^{-1}E}) = \left(\mathfrak{a}\Lambda, \frac{1}{N(\mathfrak{a})}H_{0,\Lambda}\right)$. Since every isogeny between elliptic curves is a polarized isogeny for the canonical polarizations, the isomorphism ν_{r_σ} is a polarized isogeny and then its analytic representation $r_\sigma\colon (\Lambda_\sigma, H_{0,\Lambda_\sigma}) \longrightarrow \left(\mathfrak{a}\Lambda, \frac{1}{N(\mathfrak{a})}H_{0,\Lambda}\right)$ defines an isometry on the induced hermitian lattices. □

3.3 Product of CM elliptic curves

Let $A = \bigoplus_{i=1}^g E_i$ be the product of g elliptic curves with CM by R over $\overline{\mathbb{Q}}$. Let $\Lambda_i \subseteq \mathbb{C}$ be lattices such that $\phi_{\Lambda_i}\colon \mathbb{C}/\Lambda_i \to E_i(\mathbb{C})$ is the canonical isomorphism with $g_k(\Lambda_i) \in \overline{\mathbb{Q}}$. Then there is a canonical isomorphism $\phi_\Gamma\colon \mathbb{C}^g/\Gamma \to A(\mathbb{C})$ with $\Gamma = \bigoplus \Lambda_i$ and $\phi_\Gamma = (\phi_{\Lambda_i})_{i=1\dots g}$. In this section we show how the results of Section 3.2 apply to products of elliptic curves and we conclude with the proofs of Theorem 3 and 4.

3.3.1 Isogenies between products of elliptic curves

Proposition 5. *Let $A, A' \in \boldsymbol{\mathcal{A}}_R$ over $\overline{\mathbb{Q}}$ with $A = E_{\Lambda_1} \times \cdots \times E_{\Lambda_g}$ and $A' = E_{\Lambda'_1} \times \cdots \times E_{\Lambda'_g}$. Let $\Gamma = \bigoplus_i \Lambda_i$ and $\Gamma' = \bigoplus_j \Lambda'_j$. Then the matrix M_f of the analytic representation in the canonical basis of $\mathbb{C}\Gamma$ and $\mathbb{C}\Gamma'$ of any map $(f\colon A \to A', \phi_\Gamma, \phi_{\Gamma'})$ has coefficients in $\overline{\mathbb{Q}}$ and for any $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), M_{f^\sigma} = M_f^\sigma$.*

Proof. Consider the following diagram for all k, l

$$\begin{array}{ccccccc}
\mathbb{C}/\Lambda_k & \xhookrightarrow{j_k} & \mathbb{C}^g/\Gamma & \xrightarrow{M_f} & \mathbb{C}^g/\Gamma' & \xrightarrow{p'_l} & \mathbb{C}/\Lambda'_l \\
\downarrow{\scriptstyle \phi_{\Lambda_k}} & & \downarrow{\scriptstyle \phi_\Gamma} & & \downarrow{\scriptstyle \phi_{\Gamma'}} & & \downarrow{\scriptstyle \phi_{\Lambda'_l}} \\
E_{\Lambda_k}(\mathbb{C}) & \xhookrightarrow{\iota_k} & A(\mathbb{C}) & \xrightarrow{f} & A'(\mathbb{C}) & \xrightarrow{\pi'_l} & E_{\Lambda'_l}(\mathbb{C})
\end{array}$$

with j_k, ι_k and p'_l, π'_l the k-th component inclusion and l-th component projection respectively.

Through those morphisms, we can see the k, l coefficient $m_{l,k}$ of M_f as a map

$$m_{l,k}\colon \mathbb{C}/\Lambda_k \to \mathbb{C}/\Lambda'_l$$

which is in $\overline{\mathbb{Q}}$ and, by Proposition 2, $m_{l,k}^\sigma$ is the analytic representation of $((p'_l \circ f \circ \iota_k)^\sigma, \phi_{\Lambda_k}, \phi_{\Lambda_l})$. □

Let $(A, a) \in \boldsymbol{\mathcal{A}}_R^p$ with $A \simeq E_{\Lambda_1} \times \cdots \times E_{\Lambda_g}$. Let $\Gamma = \bigoplus_i \Lambda_i$. We denote by h the hermitian form on $\mathbb{C}^g$ and $\rho_h \in \mathrm{Hom}_{\mathbb{C}}(\Gamma, \widehat{\Gamma})$ the map induced by the polarization a. Consider a_0 the product polarization of the canonical

polarizations on each elliptic curve $a_{0,E_i}\colon E_i \to \widehat{E_i}$. It is an isomorphism

$$a_0\colon \bigoplus_{i=1}^{g} E_i \to \bigoplus_{i=1}^{g} \widehat{E_i}$$

which induces

$$\rho_{h_0} = (\rho_{h_{0,\Lambda_i}})\colon \mathbb{C}^g/\bigoplus_i \Lambda_i \to (\mathbb{C}^g)^*/\bigoplus_i \widehat{\Lambda_i}$$

with each $\rho_{h_{0,\Lambda_i}}$ induced by the canonical polarization on E_{Λ_i}. We can now consider the analytic representation ρ of $(a_0^{-1}\circ a, \phi_\Gamma, \phi_\Gamma)$. By definition, the diagram of Figure 4 commutes.

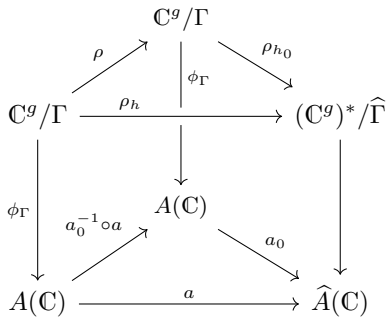


Figure 4: Analytic representation of polarizations

Recall that we denoted $\alpha_R = \operatorname{im}\omega > 0$ with $R = \mathbb{Z}[\omega]$. Let $\Lambda_i = \mathfrak{a}_i x_i$ then $\Gamma = \bigoplus \mathfrak{a}_i x_i$ and, with Lemma 1 we can show that

$$\widehat{\Gamma} = \{\ell \in (\mathbb{C}^g)^*, \operatorname{im}\ell(\Gamma) \subseteq \mathbb{Z}\} = \{\ell \in (\mathbb{C}^g)^*, \alpha_R\ell(\Gamma) \subseteq R\} = \bigoplus \frac{1}{\alpha_R}\overline{\mathfrak{a}_j}^{-1}x_j^*$$

with $x_j^* \in (\mathbb{C}^g)^*$ defined by $x_j^*(x_i) = \delta_{i,j}$ with $\delta_{i,j} = 1$ for $i = j$ and 0 otherwise.

Proposition 6. *With the notation above let $b = (x_i)_{i=1,\dots,g}$. Let $M_{b,b}(\rho)$ be the matrix of ρ in the basis b and $G_\Gamma(b) = (h^{\alpha_R}(x_i, x_j))_{i,j}$ the Gram matrix of the hermitian form $h^{\alpha_R} = \alpha_R h$ in the basis b. Then*

$$M_{b,b}(\rho) = G_\Gamma(b)\cdot D$$

with $D = \operatorname{diag}(N(\mathfrak{a}_1), \dots, N(\mathfrak{a}_g))$ the diagonal matrix with coefficients $d_{i,i} = N(\mathfrak{a}_i)$.

Proof. By definition of $\rho_{h_{0,\Lambda_i}} \in \operatorname{Hom}_{\mathbb{C}}(\Lambda_i, \widehat{\Lambda_i})$ and Lemma 5,

$$\begin{aligned}\rho_{h_{0,\Lambda_i}}\colon \quad \mathbb{C}/\Lambda_i &\longrightarrow \mathbb{C}^*/\widehat{\Lambda_i}\\ z &\longmapsto \left(\ell_z\colon w \mapsto \tfrac{z\overline{w}}{\alpha_R N(\mathfrak{a})N(x_i)}\right).\end{aligned}$$

Hence, $\rho_{h_0}(x_i) = \ell_{x_i} = \frac{1}{N(\mathfrak{a}_i)\alpha_R}x_i^*$ so $\rho_{h_0}^{-1}(x_i^*) = N(\mathfrak{a}_i)\alpha_R x_i$. Thus, for any $\ell = \sum_i u_i x_i^* \in (\mathbb{C}^g)^*$,

$$\rho_{h_0}^{-1}(\ell) = \sum_i u_i N(\mathfrak{a}_i)\alpha_R x_i \tag{7}$$

and then its j-th component is

$$(\rho_{h_0}^{-1}(\ell))_j = u_j N(\mathfrak{a}_j)\alpha_R = \alpha_R \ell(x_j) \tag{8}$$

Now, since $\rho = \rho_{h_0}^{-1}\circ\rho_h$ we have

$$\begin{aligned}\rho_{ij} &= (\rho(x_i))_j\\ &= (\rho_{h_0}^{-1}\circ\rho_h(x_i))_j\\ &= N(\mathfrak{a}_j)\alpha_R\rho_h(x_i)(x_j) \text{ by (7) and (8)}\\ &= N(\mathfrak{a}_j)\alpha_R h(x_i, x_j)\\ &= N(\mathfrak{a}_j)h^{\alpha_R}(x_i, x_j)\\ &= (G_\Gamma(b)\cdot D)_{i,j}.\end{aligned}$$

□

Proposition 7. *Let $A, A' \in \mathcal{A}_R$ with $A = E_{\Lambda_1} \times \cdots \times E_{\Lambda_g}$ and $A' = E_{\Lambda'_1} \times \cdots \times E_{\Lambda_{g'}}$. Assume that for all $i, j, \mathrm{Hom}_{\mathbb{C}}(\Lambda_i, \Lambda'_j) \subseteq K$. Then there exists $r_\sigma \in \overline{\mathbb{Q}}$ such that for any $f\colon A \to A'$, any $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/K)$ and $\mathfrak{a}$ with $F(\sigma) = \dot{\mathfrak{a}} \in \mathrm{Cl}(R)$ there is a commutative diagram*

$$\begin{array}{ccc} A^\sigma(\mathbb{C}) & \xrightarrow{f^\sigma} & A'^\sigma(\mathbb{C}) \\ \uparrow{\scriptstyle \phi_\Gamma} & & \uparrow{\scriptstyle \phi_{\Gamma'_\sigma}} \\ \mathbb{C}^g/\Gamma_\sigma & \xrightarrow{M} & \mathbb{C}^{g'}/\Gamma'_\sigma \\ \downarrow{\scriptstyle r_\sigma I_g} & & \downarrow{\scriptstyle r_\sigma I_{g'}} \\ \mathbb{C}^g/\mathfrak{a}^{-1}\Gamma & \xrightarrow{M} & \mathbb{C}/\mathfrak{a}^{-1}\Gamma'. \end{array}$$

with $\Gamma = \bigoplus_i \Lambda_i$ and $\Gamma' = \bigoplus_j \Lambda'_j$.

Proof. Apply Lemma 3 and following the same steps as in the proof of Proposition 5. □

Proposition 8. *Let $E_1, \ldots, E_g$ be elliptic curves over $\overline{\mathbb{Q}}$ with CM by R and the isomorphisms $\phi_{\Lambda_i}\colon \mathbb{C}/\Lambda_i \to E_i(\mathbb{C})$ with $\mathrm{Hom}_{\mathbb{C}}(\Lambda_i, \Lambda_j) \subseteq K$. Let a_{0,E_i} be the canonical polarization on E_i, a_0 be the product polarization on $E_1 \times \cdots \times E_g$ and $\mathbf{F}_h(\bigoplus_i E_i, a_0) = (\bigoplus_i \Lambda_i, H_0)$. Then for any $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/K)$ and $\dot{\mathfrak{a}}^{-1} = F(\sigma)$ there is an isometry*

$$\mathbf{F}_h\left(\bigoplus_i E_i^\sigma, a_0^\sigma\right) \underset{r_\sigma}{\simeq} \left(\mathfrak{a}\bigoplus_i \Lambda_i, \frac{1}{N(\mathfrak{a})} H_0\right).$$

Proof. This is just Lemma 4 applied component by component. □

3.3.2 Proof of Theorem 3 and 4

We have now the necessary tools to prove both Theorem 3 and 4. As both theorems aim to describe the isometry class of $\mathbf{F}_h(A^\sigma, a^\sigma)$, for $(A, a) \in \mathcal{A}_R^p$ and $\sigma \in \mathrm{Gal}\left(\overline{\mathbb{Q}}/K\right)$ or $\mathrm{Gal}\left(K/\mathbb{Q}\right)$, it is enough to show there is such an isometry for a particular object in the isomorphism class of (A^σ, a^σ). By definition of $\mathcal{A}_R^p$, each isomorphism class of polarized abelian variety contains an element of the form $(E_1 \times \cdots \times E_g, a)$ so we will show the isometry for this particular case.

Let (L, H) be an integral rank g hermitian R-lattice. Fixing a basis b of KL gives an isomorphism $KL \simeq K^g$ and pushing forward H on K^g gives an isometry $(KL, H) \to (K^g, H)$. We identify (L, H) with its image in (K^g, H). The hermitian form H is determined by the Gram matrix of b given by $G = G(b) = (H(v, w))_{v,w \in b} \in M_{g,g}(K)$. Indeed, with $x, y \in K^g$, colon vectors in the basis b of KL, we have

$$H(x, y) = {}^t x G \overline{y}$$

and then, by definition,

$$\overline{H}(x, y) = \overline{H(\overline{x}, \overline{y})} = \overline{{}^t \overline{x} G \overline{\overline{y}}} = {}^t x \overline{G} \overline{y}.$$

Hence, $(\overline{L}, \overline{H})$ has Gram matrix $\overline{G}$.

Proof of Theorem 3. Let $(A, a) \in \mathcal{A}_R^p$ over $\overline{\mathbb{Q}}$ with $A = E_{\Lambda_1} \times \cdots \times E_{\Lambda_g}$ with $\mathrm{Hom}_{\mathbb{C}}(\Lambda_i, \Lambda_j) \subseteq K$. Let $\mathbf{F}_h(A, a) = (L, H)$ and let $\mathbf{F}_h(\overline{A}, \overline{a}) = (L', H')$. We write $\Lambda_i = \mathfrak{a}_i x_i$ and $b = (x_1, \ldots, x_g)$ such that $(\mathfrak{a}_i, x_i)$ is a pseudo-basis of $L = \bigoplus_i \Lambda_i$. By Lemma 2, $L' = \overline{L}$. Moreover, by Proposition 6, $M_{b,b}(\rho) = G_L(b) \cdot D$ with $D = \mathrm{diag}(N(\mathfrak{a}_1), \ldots, N(\mathfrak{a}_g))$. By Proposition 5 and by applying the complex conjugation to the diagram

$$\begin{array}{ccc} \mathbb{C}^g/L & \xrightarrow{\rho} & \mathbb{C}^g/L \\ \downarrow{\scriptstyle \phi_L} & & \downarrow{\scriptstyle \phi_L} \\ A(\mathbb{C}) & \xrightarrow{a_0^{-1} \circ a} & A(\mathbb{C}) \end{array}$$

the analytic representation of $(\overline{a_0}^{-1} \circ \overline{a}, \phi_{\overline{L}}, \phi_{\overline{L}})$ is $\overline{M_{b,b}(\rho)} = \overline{G_L(b)}$ where ρ is the analytic representation of $(a_0^{-1} \circ a, \phi_L, \phi_L)$. Hence, $(\overline{L}, H')$ has Gram matrix $\overline{G_L(b)}$ so $H' = \overline{H}$. □

Proof of Theorem 4. Let $(A,a) \in \mathcal{A}_R^p$ such that $A = E_{\Lambda_1} \times \cdots \times E_{\Lambda_g}$ such that $\mathrm{End}(\Lambda_i, \Lambda_j) \subseteq K$ for all i,j. We will write $E_i = E_{\Lambda_i}$ for simplicity. Let $\Gamma = \bigoplus \Lambda_i$ and $\mathbf{F}_h(A,a) = (L,H), \sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/K)$ with $L = \Gamma$ and $\dot{\mathfrak{a}}^{-1} = F(\sigma)$.

First step : find a polarized isogeny $(E^n, D\cdot\lambda_0) \to (A,a)$ with D diagonal with integer entries. Let $\Lambda = \Lambda_1$ and $E = E_1$ and λ_0 the product polarization on E^g. There exist $\alpha_i \in K$ such that for all $i, \alpha_i\Lambda \subseteq \Lambda_i$. This gives us an isogeny $q\colon E^g \to A$. We denote by $Q = \mathrm{diag}(\alpha_1, \ldots, \alpha_g)$ the analytic representation of $(q, \phi_{\Lambda^g}, \phi_\Gamma)$. We consider $\lambda\colon E^g \to \widehat{E}^g$ the pullback polarization of a on E^g, i.e., the unique polarization on E^g that makes q a polarized isogeny. We consider $M = \lambda_0^{-1} \circ \lambda \in \mathrm{End}(E^g) \simeq M_g(R)$, and since $\lambda = \widehat{\lambda}$ the matrix M is a hermitian matrix, i.e., ${}^t\overline{M} = M$. Now consider a matrix $P \in M_g(R)$ such that ${}^t\overline{P}MP = D$ with D a diagonal matrix. Since M is positive definite and hermitian, so does D and then it has positive integers entries. So, we have a polarized isogeny $f = q \circ P\colon (E^g, D\cdot\lambda_0) \to (A,a)$.

$$\begin{array}{ccccc} E^g & \xrightarrow{P} & E^g & \xrightarrow{q} & \bigoplus E_i \\ \downarrow{\scriptstyle D} & & \downarrow{\scriptstyle M} & & \downarrow{\scriptstyle a} \\ E^g & \xleftarrow[{}^t\overline{P}]{} & E^g & \xleftarrow[\widehat{q}]{} & \widehat{\bigoplus E_i} \simeq \bigoplus E_i \end{array}$$

We will denote by $S = QP$ the analytic representation of $(f, \phi_{\Lambda^g}, \phi_\Gamma)$. Since f is a polarized isogeny

$$S\colon (K\Lambda^g, D) \to (KL, H) \tag{9}$$

is an isometry.

Second step : conclude. By Proposition 8, $\mathbf{F}_h\left((E^g)^\sigma, D^\sigma\right) \underset{r_\sigma}{\simeq} \left(\mathfrak{a}\Lambda^g, \frac{1}{N(\mathfrak{a})}D\right)$. We now consider $\mathbf{F}_h(A^\sigma, a^\sigma) = (L_\sigma, H_\sigma)$ and $\iota_\sigma = \mathbf{F}_h(f^\sigma)$. By Proposition 3, we have $r_\sigma L_\sigma = \mathfrak{a}L$ and there is a commutative diagram

$$\begin{array}{ccc} (E^g)^\sigma(\mathbb{C}) & \xrightarrow{f^\sigma} & A^\sigma(\mathbb{C}) \\ \uparrow{\scriptstyle \phi_{P_\sigma}} & & \uparrow{\scriptstyle \phi_{L_\sigma}} \\ \mathbb{C}^g/\Lambda_\sigma^g & \xrightarrow{S} & \mathbb{C}^g/L_\sigma \\ \downarrow{\scriptstyle r_\sigma I_g} & & \downarrow{\scriptstyle r_\sigma I_g} \\ \mathbb{C}/\mathfrak{a}\Lambda^g & \xrightarrow{S} & \mathbb{C}^g/\mathfrak{a}L. \end{array}$$

Moreover, we have the isometries of hermitian spaces

$$r_\sigma I_g\colon (KL_\sigma, H_\sigma) \to \left(K\mathfrak{a}L, H' = \frac{1}{N(r_\sigma)}H_\sigma\right) \tag{10}$$

$$S\colon \left(K\mathfrak{a}\Lambda^g, \frac{1}{N(\mathfrak{a})}D\right) \to (K\mathfrak{a}L, H'). \tag{11}$$

By the isometries (9) and (11) we have $H' = \frac{1}{N(\mathfrak{a})}\overline{{}^tS^{-1}}DS^{-1} = \frac{1}{N(\mathfrak{a})}H$. Hence,

$$\mathbf{F}_h(A^\sigma, a^\sigma) = (L_\sigma, H_\sigma) \simeq \left(\mathfrak{a}L, \frac{1}{N(\mathfrak{a})}H\right).$$

This concludes the proof of Theorem 4.

□

4 Application to the field of moduli of varieties in $\mathcal{A}_R^p$

4.1 General results on the field of moduli of principally polarized abelian varieties in $\mathcal{A}_R^p$

We recall that the *field of moduli* of a polarized abelian variety (A,a) over $\overline{\mathbb{Q}}$ is the fixed field by the subgroup

$$\{\sigma \in \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right), (A^\sigma, a^\sigma) \simeq (A,a)\}.$$

In the same way we define the field of moduli of a curve C over $\overline{\mathbb{Q}}$ by the fixed field of $\{\sigma \in \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right), C^\sigma \simeq C\}$.

The Abel-Jacobi map $C \mapsto (\mathrm{Jac}(C), j)$ which associates a curves to its polarized Jacobian variety induces a morphism

$$\begin{array}{rccc}[\mathrm{Jac}]: & M_g & \longrightarrow & A_g \\ & [C] & \longmapsto & [\mathrm{Jac}(C), j]\end{array}$$

between the moduli space of smooth absolutely irreducible projective genus g curves and the moduli space of principally polarized abelian varieties of dimension g. By [CS86, Chapter VII,Corollary 12.2], $[\mathrm{Jac}]$ is injective so C and $(\mathrm{Jac}(C), j)$ have the same field of moduli.

For $g = 2$ and $g = 3$ the moduli spaces M_g and A_g have the same dimension and are irreducible. Thus, the Jacobian map is dominant if the field is algebraically closed. More specifically, every indecomposable principally polarized abelian variety is the Jacobian of a curve (see [Hoy63]).

We give a necessary condition on the class group of R and on $\mathbf{F}_h(A, a)$ for an abelian variety $(A, a) \in \boldsymbol{\mathcal{A}}_R^p$ to have field of moduli $\mathbb{Q}$.

Proposition 9. *Let $(A, a) \in \boldsymbol{\mathcal{A}}_R^p$ and $\mathbf{F}_h(A, a) = (L, H)$ be a hermitian lattice of rank g. If (A, a) has field of moduli $\mathbb{Q}$ then R has exponent dividing g and $\mathrm{st}(L)$ has order at most 2.*

Proof. If (L, H) corresponds to a field of moduli $\mathbb{Q}$ polarized abelian variety then $(L, H) \simeq \left(\mathfrak{a}L, \frac{1}{N(\mathfrak{a})}H\right)$ for all fractional ideal $\mathfrak{a}$. In particular, $L \simeq \mathfrak{a}L$ for all $\mathfrak{a}$ and then, their Steinitz classes are the same

$$\mathrm{st}(L) = \mathrm{st}(\mathfrak{a}L) = \mathfrak{a}^g \,\mathrm{st}(L) \in \mathrm{Cl}(R).$$

Hence, $\dot{\mathfrak{a}}^g = 1 \in \mathrm{Cl}(R)$ so $\mathrm{Cl}(R)$ has exponent dividing g.

The hermitian lattice isometry class must also be invariant by the action of the complex conjugation so

$$\mathrm{st}(L) = \mathrm{st}(\overline{L}) = \overline{\mathrm{st}(L)}.$$

By the formula $\overline{\mathfrak{a}}\mathfrak{a} = N(\mathfrak{a})R$ it means that $\mathrm{st}(L)$ must have order at most 2. □

Corollary 1. *Let $(A, a) \in \boldsymbol{\mathcal{A}}_R^p$ of dimension g odd. Suppose (A, a) has field of moduli $\mathbb{Q}$ then there exists an elliptic curve E with CM by R such that $A \simeq E^g$.*

Proof. Let $(L, H) = \mathbf{F}_h(A, a)$ be the corresponding unimodular hermitian lattice. By Proposition 9, its Steinitz class $\mathrm{st}(L)$ has order dividing g and 2 hence it must be 1. In other words L is free over R, i.e., $L \simeq R^g$ and then $A \simeq E^g$ with $\mathbf{F}(E) \simeq R$. □

4.2 Enumeration of the indecomposable principally polarized abelian varieties in $\boldsymbol{\mathcal{A}}_R^p$ with field of moduli $\mathbb{Q}$

Since we are able to understand the action of $\mathrm{Gal}\left(\overline{\mathbb{Q}}/K\right)$ and $\mathrm{Gal}(K/\mathbb{Q})$ throught the equivalence of categories $\mathbf{F}_h$ developed in Section 2 we are able to check when $(A, a) \simeq (A^\sigma, a^\sigma)$ for all $\sigma \in \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$ when $(A, a) \in \boldsymbol{\mathcal{A}}_R^p$ by looking for isometries between hermitian R-lattices. This is what Algorithm 1 does.

We denote by $\mathscr{A}_R(g)$ the set of all classes of dimension g indecomposable principally polarized abelian varieties $(A, a) \in \boldsymbol{\mathcal{A}}_R^p$ and by $\mathscr{A}_{R,\mathbb{Q}}(g)$ the subset of $\mathscr{A}_R(g)$ corresponding to elements with field of moduli $\mathbb{Q}$.

To compute the list of elements of $\mathscr{A}_{R,\mathbb{Q}}(g)$ for a given maximal order R we need the list of all unimodular indecomposable hermitian R-lattices of rank g. This can be done the classification of these lattices developed by authors in [KNRR21].

We want to run the algorithm over all maximal orders of a given exponent dividing g. By [EKN20], the complete list of the corresponding discriminants is finite for all g and known for g up to 8 under the Extended Riemann Hypothesis.

4.3 Enumeration of dimension 2 and 3 principally polarized abelian varieties of $\boldsymbol{\mathcal{A}}_R^p$ with field of moduli $\mathbb{Q}$

As the computations become quickly time-consuming as the dimension g and the discriminant of the order grows we restricted to $g = 2$ and 3 to be able to have complete tables (up to one discriminant for $g = 3$). We used the Magma library developed in [KNRR21].

Algorithm 1 Enumeration algorithm

Require: An integer g and a maximal order R with exponent dividing g.
Ensure: The list of unimodular indecomposable hermitian lattices (L, H) corresponding to the elements of $\mathscr{A}_{R,\mathbb{Q}}(g)$.

$\mathrm{LList} \leftarrow \{\text{Unimodular indecomposable hermitian lattices of rank } g\}/\simeq$
$\mathrm{LList}_{\mathrm{FM}-\mathbb{Q}} \leftarrow \{\ \}$ { List of abelian varieties with field of moduli $\mathbb{Q}$.}
for $(L, H) \in \mathrm{LList}$ **do**
  $\mathrm{bool} \leftarrow$ **true**
  for $\mathfrak{a} \in \{\text{generators of } \mathrm{Cl}(R)\}$ **do**
    $\mathrm{bool} \leftarrow \mathrm{bool}$ and $(L, H) \simeq \left(\mathfrak{a}L, \frac{1}{N(\mathfrak{a})}H\right)$.
  end for
  if bool and $(L, H) \simeq \left(\overline{L}, \overline{H}\right)$ **then**
    $\mathrm{LList}_{\mathrm{FM}-\mathbb{Q}} \leftarrow \mathrm{LList}_{\mathrm{FM}-\mathbb{Q}} \cup \{(L, H)\}$
  end if
end for
return $\mathrm{LList}_{\mathrm{FM}-\mathbb{Q}}$

h_R	Δ	$\mathscr{P}$	$\#\mathscr{A}_{R,\mathbb{Q}}$	$\#\mathscr{A}_R$	h_R	Δ	$\mathscr{P}$	$\#\mathscr{A}_{R,\mathbb{Q}}$	$\#\mathscr{A}_R$	h_R	Δ	$\mathscr{P}$	$\#\mathscr{A}_{R,\mathbb{Q}}$	$\#\mathscr{A}_R$
1	-3	0	0	0	2	-15	0	1	1	2	-115	0	3	11
	-4	0	0	0		-20	1	1	3		-123	0	4	12
	-7	0	0	0		-24	1	3	3		-148	3	5	13
	-8	1	1	1		-35	0	1	5		-187	0	3	17
	-11	1	1	1		-40	2	4	4		-232	5	10	20
	-19	1	1	1		-51	0	2	6		-235	0	5	21
	-43	2	2	2		-52	2	3	5		-267	0	6	24
	-67	3	3	3		-88	2	6	8		-403	0	3	35
	-163	7	7	7		-91	0	1	9		-427	0	3	37

h_R	Δ	$\mathscr{P}$	$\#\mathscr{A}_{R,\mathbb{Q}}$	$\#\mathscr{A}_R$	h_R	Δ	$\mathscr{P}$	$\#\mathscr{A}_{R,\mathbb{Q}}$	$\#\mathscr{A}_R$	h_R	Δ	$\mathscr{P}$	$\#\mathscr{A}_{R,\mathbb{Q}}$	$\#\mathscr{A}_R$
4	-84	0	2	18	4	-340	0	2	60	4	-595	2	2	106
	-120	3	4	24		-372	0	2	66		-627	0	0	112
	-132	1	2	26		-408	0	4	72		-708	1	2	122
	-168	0	4	32		-435	0	2	80		-715	0	2	126
	-195	0	2	40		-483	0	0	88		-760	1	4	130
	-228	1	2	42		-520	3	4	90		-795	2	2	140
	-280	0	4	50		-532	0	2	92		-1012	0	2	172
	-312	1	4	56		-555	0	2	100		-1435	0	2	246

h_R: Class number of the maximal order R of $\mathbb{Q}(\sqrt{\Delta})$.
$\#\mathscr{A}_R$: Number of elements of $\mathscr{A}_R(2)$ defined in Section 4.2.
$\#\mathscr{A}_{R,\mathbb{Q}}$: Number of elements of $\mathscr{A}_{R,\mathbb{Q}}(2)$.
$\mathscr{P}$: Number of elements (A, a) of $\mathscr{A}_{R,\mathbb{Q}}(2)$ such that $A \simeq E^2$ for some E.

Table 1: Computations for $g = 2$

We use Algorithm 1 to compute the cardinality of $\mathscr{A}_{R,\mathbb{Q}}(2)$ and copy the results in the Table 1. In the column $\mathscr{P}$ we copy the number of $(A, a) \in \boldsymbol{\mathcal{A}}_R^p$ such that A is the square of an elliptic curve with field of moduli $\mathbb{Q}$ to confirm we find the same values as in [GHR19, Table 2].

In fact, for $g = 2$, the following proposition shows that it is not necessary to check if $(L, H) \simeq (\overline{L}, \overline{H})$.

Proposition 10. *Let (A, a) be a dimension 2 principally polarised abelian variety over $\mathbb{C}$ with A isomorphic to the power of elliptic curves E_i with CM by R maximal. Let $\mathbf{F}_h(A, a) = (L, H)$ be a hermitian integral lattice and let $\mathfrak{a}$ be the Steinitz class of L. Then*

$$\mathbf{F}_h\left(\overline{A}, \overline{a}\right) = \left(\overline{L}, \overline{H}\right) \simeq \left(\overline{\mathfrak{a}}L, \frac{1}{N(\mathfrak{a})}H\right).$$

Hence, in this particular case, the action of the complex conjugation corresponds to the action of an automorphism of $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$.

Proof. Let us write $L = Rx \oplus \mathfrak{a}y$. Let $G = \begin{pmatrix} \alpha & \beta \\ \overline{\beta} & \delta \end{pmatrix}$ be the Gram matrix of H in the basis (x, y) of KL. Since (A, a) is principally polarized (L, H) must be unimodular and then its volume $\mathfrak{v}(L) = N(\mathfrak{a}) \det(G)R = R$ so $N(\mathfrak{a}) \det(G)$ is invertible and real in R so $N(\mathfrak{a}) \det(G) = 1$.

Now consider $P = N(\mathfrak{a}) \begin{pmatrix} \overline{\beta} & \delta \\ -\alpha & -\beta \end{pmatrix}$, matrix of a linear map $K\overline{x} + K\overline{y} \to Kx + Ky$. It satisfies the relation

$$ {}^tP \frac{1}{N(\mathfrak{a})} G \overline{P} = N(\mathfrak{a}) \det(G) \overline{G} = \overline{G}. $$

So, P defines an isometry between hermitian spaces.

Moreover, $\alpha = H(x, x) = N(x) \in R \cap \mathbb{R} = \mathbb{Z}$, $\beta = H(x, y)$, so $\overline{\mathfrak{a}}\beta = H(x, \mathfrak{a}y) \subseteq R$ so $\beta \in \overline{\mathfrak{a}}^{-1} = \frac{\mathfrak{a}}{N(\mathfrak{a})}$ and, in the same way, $\delta \in \frac{1}{N(\mathfrak{a})}\mathbb{Z}$. Hence,

$$ \begin{aligned} P\overline{x} &= N(\mathfrak{a})(\overline{\beta}x - ay) \in \overline{\mathfrak{a}}x + N(\mathfrak{a})y = \overline{\mathfrak{a}}L \\ P\overline{\mathfrak{a}y} &= N(\mathfrak{a})\overline{\mathfrak{a}}(\delta x - by) \in \overline{\mathfrak{a}}x + N(\mathfrak{a})y = \overline{\mathfrak{a}}L. \end{aligned} $$

Thus, P defines an isometry $(\overline{L}, \overline{H}) \to \left(\overline{\mathfrak{a}}L, \frac{1}{N(\mathfrak{a})}H\right)$ □

In dimension $g = 3$ computations are more time consuming. Fortunately, by Corollary 1, in odd dimension all isomorphism class of (A, a) in $\mathscr{A}_{R,\mathbb{Q}}(3)$ are actually isomorphic to some a power of an elliptic curve. Hence, we can run the algorithm only on free unimodular hermitian lattices and the latter are easier to enumerate and to work with.

We copy the results of the computations in Table 2. Pay attention that the table is complete up to the discriminant $\Delta = -4027$ with class group isomorphic to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ for which the algorithm is still running.

h_R	Δ	$\#\mathscr{A}_{R,\mathbb{Q}}$	$\#\mathscr{A}_R^{\text{free}}$	h_R	Δ	$\#\mathscr{A}_{R,\mathbb{Q}}$	$\#\mathscr{A}_R^{\text{free}}$
1	-3	0	0	3	-107	2	44
	-4	0	0		-139	1	79
	-7	0	0		-211	0	209
	-8	0	0		-283	1	417
	-11	0	0		-307	0	507
	-19	1	1		-331	2	613
	-43	3	5		-379	0	851
	-67	5	13		-499	1	1665
	-163	13	103		-547	1	2059
					-643	1	3075
3	-23	0	3		-883	0	6703
	-31	0	6		-907	1	7163
	-59	1	10				
	-83	0	24	9	-4027	?	?

h_R: Class number of the maximal order R of $\mathbb{Q}(\sqrt{\Delta})$.
$\#\mathscr{A}_R^{\text{free}}$: Number of classes (A, a) in $\mathscr{A}_R(3)$ with $A \simeq E^3$ for some E.
$\#\mathscr{A}_{R,\mathbb{Q}}$: Number of elements of $\mathscr{A}_{R,\mathbb{Q}}(3)$.

Table 2: Computations for $g = 3$

References

[BL04] Christina Birkenhake and Herbert Lange. *Complex abelian varieties*, volume 302 of *Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, second edition, 2004.

[Con16] K. Conrad. Ideal classes and relative integers, 2016. `https://kconrad.math.uconn.edu/blurbs/gradnumthy/relativeintandidealclasses.pdf`.

[CS86] Gary Cornell and Joseph H. Silverman, editors. *Arithmetic geometry*. Springer-Verlag, New York, 1986. Papers from the conference held at the University of Connecticut, Storrs, Connecticut, July 30–August 10, 1984.

[EKN20] Andreas-Stephan Elsenhans, Jürgen Klüners, and Florin Nicolae. Imaginary quadratic number fields with class groups of small exponent. *Acta Arith.*, 193(3):217–233, 2020.

[FG18] Francesc Fité and Xavier Guitart. Fields of definition of elliptic k-curves and the realizability of all genus 2 Sato-Tate groups over a number field. *Trans. Amer. Math. Soc.*, 370(7):4623–4659, 2018.

[FG20] Francesc Fité and Xavier Guitart. Endomorphism algebras of geometrically split abelian surfaces over $\mathbb{Q}$. *Algebra & Number Theory*, 14(6):1399–1421, jul 2020.

[GHR19] Alexandre Gélin, Everett W. Howe, and Christophe Ritzenthaler. Principally polarized squares of elliptic curves with field of moduli equal to $\mathbb{Q}$. In *Proceedings of the Thirteenth Algorithmic Number Theory Symposium*, volume 2 of *Open Book Ser.*, pages 257–274. Math. Sci. Publ., Berkeley, CA, 2019.

[Hof91] Detlev W. Hoffmann. On positive definite Hermitian forms. *Manuscripta Math.*, 71(4):399–429, 1991.

[Hoy63] W. L. Hoyt. On products and algebraic families of Jacobian varieties. *Ann. Math. (2)*, 77:415–423, 1963.

[JKP+18] Bruce W. Jordan, Allan G. Keeton, Bjorn Poonen, Eric M. Rains, Nicholas Shepherd-Barron, and John T. Tate. Abelian varieties isogenous to a power of an elliptic curve. *Compos. Math.*, 154(5):934–959, 2018.

[Kan11] Ernst Kani. Products of CM elliptic curves. *Collect. Math.*, 62(3):297–339, 2011.

[KNRR21] Markus Kirschmer, Fabien Narbonne, Christophe Ritzenthaler, and Damien Robert. Spanning the isogeny class of a power of an elliptic curve. *Math. Comp.*, 91(333):401–449, 2021.

[Mil08] James S. Milne. Abelian varieties (v2.00), 2008. Available at www.jmilne.org/math/.

[Mum70] David Mumford. *Abelian varieties*. Tata Institute of Fundamental Research Studies in Mathematics, No. 5. Published for the Tata Institute of Fundamental Research, Bombay; Oxford University Press, London, 1970.

[O'M00] O. Timothy O'Meara. *Introduction to quadratic forms*. Classics in Mathematics. Springer-Verlag, Berlin, 2000. Reprint of the 1973 edition.

[Sil94] J.H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics. Springer New York, 1994.

[Sil09] Joseph H Silverman. *The Arithmetic of Elliptic Curves*. Graduate texts in mathematics. Springer, Dordrecht, 2009.

Annexe A

ÉNUMÉRATION HEURISTIQUE DES JACOBIENNES DÉCOMPOSÉES DE DIMENSION 2 AVEC CORPS DE MODULES $\mathbb{Q}$

Comme cela a été démontré dans la Section 2.2.4 il y a une équivalence de catégories entre les variétés abéliennes polarisées sur $\overline{\mathbb{Q}}$ isogènes à un produit de courbes elliptiques à multiplication complexe par un ordre R et les R-réseaux hermitiens entiers. Dans [Nar22] nous nous intéressions au cas maximal exclusivement (donc nous ne considérions pas toute la classe d'isogénie). Dans ce cas nous avons pu traduire l'action de $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$ sur les réseaux hermitiens à travers l'équivalence de catégories énoncée.

Dans cette section nous souhaitons présenter les calculs dans le cas non-maximal **sous réserve que la traduction démontrée dans le cas maximal tient toujours dans le cas non-maximal**, i.e. qu'il existe un morphisme surjectif[1] $F\colon \mathrm{Gal}\left(\overline{\mathbb{Q}}/K\right) \to \mathrm{Cl}(R)$ tel que pour $(A,a) \in \boldsymbol{\mathcal{A}}_R^p, \sigma \in \mathrm{Gal}\left(\overline{\mathbb{Q}}/K\right)$ et $\mathfrak{a}^{-1}$ un représentant de $F(\sigma)$ alors il existe une isométrie

$$\mathbf{F}_h(A^\sigma, a^\sigma) \simeq \left(\mathfrak{a}L, \frac{1}{N(\mathfrak{a})}H\right)$$

où $(L,H) = \mathbf{F}_h(A,a)$.

J'insiste sur le fait que les résultats présentés ici ne sont pas démontrés au moment où j'écris ces lignes. Cependant, étant donné que plusieurs personnes m'ont demandé de leur fournir ces résultats (même heuristiques) j'ai jugé que cette appendice serait peut-être utile à d'autres personnes.

L'algorithme utilisé pour énumérer les réseaux hermitiens unimodulaires sur un ordre quadratique R est [KNRR21, Algorithm 2]. L'algorithme qui teste si un réseau hermitien

1. Il est facile de constater que l'action de la conjugaison complexe est la même que dans le cas maximal.

(L, H) est isomètre à ses conjugués sous l'action de $\mathrm{Cl}(R)$ est rigoureusement le même que celui de [Nar22, Algorithm 1].

Par ailleurs, [Nar22, Proposition 9] est toujours valable pour R non maximal, i.e. si (L, H) est un R-réseau hermitien unimodulaire de rang g correspondant à une variété abélienne principalement polarisée ayant corps des modules $\mathbb{Q}$ alors $\mathrm{Cl}(R)$ est d'exposant au plus g. Pour simplifier nous parlerons d'ordres d'exposant au plus 2 plutôt que d'ordres quadratiques imaginaires dont le groupe des classes est d'exposant au plus 2. Ainsi, une classification des ordres d'exposant au plus 2 est nécessaire si nous souhaitons énumérer toutes les jacobiennes. Nous proposons une telle classification dans la Section A.2 à partir de la classification des ordres maximaux d'exposant au plus 2 faite dans [EKN20]. Puisque les auteurs utilisent l'hypothèse de Riemann généralisée dans [EKN20] la liste des jacobiennes sera complète sous cette hypothèse (et encore une fois sous réserve que la traduction de l'action galoisienne est la bonne).

A.1 Résultats heuristiques

Avant d'expliquer comment nous avons trouvé les ordres d'exposant 2 nous exposons ici les résultats des calculs dans les trois tableaux suivants. Nous expliquons colonne par colonne comment lire les tableaux.

1. La première colonne, Δ, est le discriminant de l'ordre $R = \mathbb{Z}[f\omega]$.
2. La seconde colonne, f, est le conducteur de $R = \mathbb{Z}[f\omega]$ dans l'ordre maximal $\mathscr{O}_K \simeq \mathbb{Z}[\omega]$.
3. La troisième colonne, $\#\,\mathrm{Cl}(\mathbb{Z}[f\omega])$, est le nombre de classes de R, i.e. le cardinal de son groupe des classes (ou groupe de Picard). C'est toujours une puissance de 2 car $\mathrm{Cl}(\mathbb{Z}[f\omega]) \simeq (\mathbb{Z}/2\mathbb{Z})^s$ pour un s.
4. La quatrième colonne indique le nombre de classe d'isomorphisme courbes de genre 2 sur $\overline{\mathbb{Q}}$ telle que $\mathrm{Jac}(C) \simeq E_1 \times E_2$ avec $R \subseteq \mathrm{End}(E_i)$ et C de corps de modules $\mathbb{Q}$.
5. La cinquième colonne indique le nombre de classe d'isomorphismes de courbes décrites ci-dessus telles que $\mathrm{Jac}(C) \simeq E^2$ (i.e. $\mathrm{Hom}(\mathrm{Jac}(C), E) \simeq R^2$ est un R-module libre).
6. La sixième colonne indique le nombre total de classes d'isomorphismes de courbes C sur $\overline{\mathbb{Q}}$ telles que $\mathrm{Jac}(C) \simeq E_1 \times E_2$ avec $R \subseteq \mathrm{End}(E_i)$.

Nous avons fait trois tableaux. Le s-ème reporte les ordres $R \subseteq \mathscr{O}_K$ tels que $\mathrm{Cl}(\mathscr{O}_K) \simeq (\mathbb{Z}/2\mathbb{Z})^s$. Les lignes grisées sont celles correspondant aux ordres non-maximaux, i.e. les lignes pour lesquelles les résultats ne sont pas encore certifiés.

Δ	f	$\#\,\mathrm{Cl}\,(\mathbb{Z}\,[f\omega])$	Corps de modules $\mathbb{Q}$		Total
			Total	Libres	
-3	1	1	0	0	0
-12	2	1	1	1	1
-27	3	1	2	1	2
-48	4	2	5	0	9
-75	5	2	2	1	8
-147	7	2	4	2	10
-192	8	4	9	0	71
-4	1	1	0	0	0
-16	2	1	1	1	1
-36	3	2	1	1	5
-64	4	2	5	1	11
-100	5	2	3	2	7
-7	1	1	0	0	0
-28	2	1	2	2	2
-112	4	2	6	0	12
-448	8	4	6	0	84
-8	1	1	1	1	1
-32	2	2	2	0	6
-72	3	2	4	2	6
-288	6	4	10	0	76
-11	1	1	1	1	1
-99	3	2	3	1	9
-19	1	1	1	1	1
-43	1	1	2	2	2
-67	1	1	3	3	3
-163	1	1	7	7	7

TABLE A.1 – Ordres d'exposant 2 dont l'ordre maximal est principal et le nombre de réseaux hermitiens unimodulaire de rang 2 invariants par le groupe des classes.

Δ	f	$\#\,\mathrm{Cl}\,(\mathbb{Z}\,[f\omega])$	Corps de modules $\mathbb{Q}$		Total
			Total	Libres	
-15	1	2	1	0	1
-60	2	2	3	0	9
-250	4	4	7	0	55
-960	8	8	7	0	387
-20	1	2	1	1	3
-180	3	4	2	1	32
-24	1	2	3	1	3
-216	3	6	3	0	87
-35	1	2	1	0	5
-315	3	4	2	0	58
-40	1	2	4	2	4
-160	2	4	6	0	44
-51	1	2	2	0	6
-52	1	2	3	2	5
-88	1	2	6	2	8
-352	2	4	6	0	92
-91	1	2	1	0	9
-115	1	2	3	0	11
-123	1	2	4	0	12
-148	1	2	5	3	13
-187	1	2	3	0	17
-232	1	2	10	5	20
-928	2	4	12	0	236
-235	1	2	5	0	21
-267	1	2	6	0	24
-403	1	2	3	0	35
-427	1	2	3	0	37

TABLE A.2 – Ordres R d'exposant 2 tels que $\mathrm{Cl}(\mathscr{O}_K) \simeq \mathbb{Z}/2\mathbb{Z}$ et le nombre de réseaux hermitiens unimodulaire de rang 2 invariants par le groupe des classes.

Δ	f	$\#\,\mathrm{Cl}\,(\mathbb{Z}\,[f\omega])$	Corps de modules $\mathbb{Q}$		Total
			Total	Libres	
-84	1	4	2	0	18
-120	1	4	4	3	24
−480	2	8	4	0	260
-132	1	4	2	1	26
-168	1	4	4	0	32
−672	2	8	4	0	356
-195	1	4	2	0	40
-228	1	4	2	1	42
-280	1	4	4	0	50
−1120	2	8	4	0	578
-312	1	4	4	1	56
−1248	2	8	4	0	644
-340	1	4	2	0	60
-372	1	4	2	0	66
-408	1	4	4	0	72
−1632	2	8	4	0	836
-435	1	4	2	0	80
-483	1	4	0	0	88
-520	1	4	4	3	90
−2080	2	8	4	0	1058
-532	1	4	2	0	92
-555	1	4	2	0	100
-595	1	4	2	2	106
-627	1	4	0	0	112
-708	1	4	2	1	122
-715	1	4	2	0	126
-760	1	4	4	1	130
−3040	2	8	4	0	1538
-795	1	4	2	2	140
-1012	1	4	2	0	172
-1435	1	4	2	0	246

TABLE A.3 – Ordres R d'exposant 2 tels que $\mathrm{Cl}(\mathscr{O}_K) \simeq (\mathbb{Z}/2\mathbb{Z})^2$ et le nombre de réseaux hermitiens unimodulaire de rang 2 invariants par le groupe des classes.

A.2 Classification des ordres d'exposant 2

A.2.1 Énoncé du théorème et résultats préliminaires

On énonce directement le résultat que l'on souhaite démontrer. Ce résultat pour $\Delta \neq -3$ et -4 ainsi que les résultats essentiels à sa démonstration ([Cox85, Exercise 7.28] et [Cox85, Equation (7.25) et (7.27)]) m'ont gentiment été suggérés par Marco Streng que je remercie chaleureusement.

Théorème A.2.1. *Soit R un ordre quadratique imaginaire dans K, de conducteur f dans $\mathscr{O}_K$. On suppose que l'exposant de $\mathrm{Cl}(R)$ divise 2. Alors l'exposant de $\mathrm{Cl}(\mathscr{O}_K)$ aussi. De plus si on note Δ le discriminant de $\mathscr{O}_K$ on a alors*

Si $\Delta \notin \{-3,-4\}$ **:** $f \in \left\{2^a 3^b \text{ tels que } a \leq 3, b \leq 1\right\}$.

Si $\Delta \in \{-3,-4\}$ **:** $f \in \left\{2^a 3^b 5^c 7^d \text{ tels que } a \leq 3, b \leq 1, c \leq 1, d \leq 1\right\}$.

Connaissant ce théorème une boucle naïve sur tous les ordres maximaux $\mathscr{O}_K = \mathbb{Z}[\omega]$ en testant pour chaque conducteur f si $\mathrm{Cl}(\mathbb{Z}[f\omega]) \simeq (\mathbb{Z}/2\mathbb{Z})^s$ prend quelques secondes. Donc, même si nous pourrions être plus précis sur quels a, b, c, d sont possibles pour les conducteurs $f = 2^a 3^b 5^c 7^d$ tels que R est d'exposant 2, je me suis contenté du strict nécessaire. Nous avons alors reporté dans la Table A.4 la classification des ordres quadratiques imaginaires dont l'ordre du groupe des classes divise 2. La légende indique comment lire la table. Les cases grisées correspondent aux ordres qui ne sont pas maximaux.

$h_K = 1$			$h_K = 2$			$h_K = 4$			$h_K = 8$		
Δ	f	s	Δ	f	s	Δ	f	s	Δ	f	s
-3	1	0	-15	1	1	-84	1	2	-420	1	3
-12	2	0	-60	2	1	-120	1	2	-660	1	3
-27	3	0	-240	4	2	-480	2	3	-840	1	3
-48	4	1	-960	8	3	-132	1	2	-3360	2	4
-75	5	1	-20	1	1	-168	1	2	-1092	1	3
-147	7	1	-180	3	2	-672	2	3	-1155	1	3
-192	8	2	-24	1	1	-195	1	2	-1320	1	3
-4	1	0	-96	2	2	-228	1	2	-5280	2	4
-16	2	0	-35	1	1	-280	1	2	-1380	1	3
-36	3	1	-315	3	2	-1120	2	3	-1428	1	3
-64	4	1	-40	1	1	-312	1	2	-1540	1	3
-100	5	1	-160	2	2	-1248	2	3	-1848	1	3
-7	1	0	-51	1	1	-340	1	2	-7392	2	4
-28	2	0	-52	1	1	-372	1	2	-1995	1	3
-112	4	1	-88	1	1	-408	1	2	-3003	1	3
-448	8	2	-352	2	2	-1632	2	3	-3315	1	3
-8	1	0	-91	1	1	-435	1	2			
-72	3	1	-115	1	1	-483	1	2	$h_K = 16$		
-32	2	1	-123	1	1	-520	1	2			
-288	6	2	-148	1	1	-2080	2	3	-5460	1	4
-11	1	0	-187	1	1	-532	1	2			
-99	3	1	-232	1	1	-555	1	2			
-19	1	0	-928	2	2	-595	1	2			
-43	1	0	-235	1	1	-627	1	2			
-67	1	0	-267	1	1	-708	1	2			
-163	1	0	-403	1	1	-715	1	2			
			-427	1	1	-760	1	2			
						-3040	2	3			
						-795	1	2			
						-1012	1	2			
						-1435	1	2			

h_K : nombre de classes de K, i.e. $h_K = \#\operatorname{Cl}(\mathscr{O}_K)$.
Δ : Discriminant de l'ordre R, i.e. $R = \mathbb{Z}\left[\frac{\Delta+\sqrt{\Delta}}{2}\right]$.
f : Conducteur de R dans l'ordre maximal $\mathscr{O}_K$.
s : L'entier s tel que $\operatorname{Cl}(R) \simeq (\mathbb{Z}/2\mathbb{Z})^s$.

TABLE A.4 – Classification des ordres quadratiques imaginaire d'exposant au plus 2 (classification complète sous l'hypothèse de Riemann généralisée).

A.2.2 Démonstration du Théorème A.2.1

L'équation [Cox85, Equation (7.25)] montre qu'il existe une suite exacte

$$1 \to I_K(f) \cap P_K/P_{K,\mathbb{Z}}(f) \to \mathrm{Cl}(R) \to \mathrm{Cl}(\mathscr{O}_K) \to 1 \tag{A.1}$$

où la définition de $G = I_K(f) \cap P_K/P_{K,\mathbb{Z}}(f)$, n'importe pas. La lectrice intéressée pourra se reporter à la référence. Nous n'aurons besoin que du fait que, puisque G s'injecte dans $\mathrm{Cl}(R)$, en particulier son exposant divise 2. Par ailleurs, l'exposant de $\mathrm{Cl}(\mathscr{O}_K)$ divise celui de $\mathrm{Cl}(R)$ car il existe un morphisme surjectif de $\mathrm{Cl}(R)$ dans $\mathrm{Cl}(\mathscr{O}_K)$.

On va alors séparer la preuve en deux partie : on traite d'abord le cas $\Delta \notin \{-3, -4\}$ puis on traite séparément les cas $\Delta = -3$ et $\Delta = -4$.

Cas $\Delta \notin \{-3, -4\}$

L'idée de la preuve est la suivante. D'après [Cox85, Equation (7.27)], pour tout $\mathscr{O}_K$ de discriminant $\Delta \neq -3, -4$ on a une suite exacte

$$1 \longrightarrow (\mathbb{Z}/f\mathbb{Z})^\times \longrightarrow (\mathscr{O}_K/f\mathscr{O}_K)^\times \longrightarrow G \longrightarrow 1 \tag{A.2}$$

(où $G = I_K(f) \cap P_K/P_{K,\mathbb{Z}}(f)$ est le même que dans la suite exacte (A.1) et, on le rappelle, est d'exposant au plus 2). Le premier morphisme de la suite exacte (A.2) est l'application induite par le morphisme d'anneaux universel $\mathbb{Z} \to \mathscr{O}_K$. On pose $f = \prod_{i=1}^r p_i^{\alpha_i}$ la décomposition en facteurs premiers de f. Par le Théorème des restes pour les entiers et les ordres maximaux on a une suite exacte

$$1 \longrightarrow \left(\prod_{i=1}^r \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}\right)^\times \longrightarrow \left(\prod_{i=1}^r \mathscr{O}_K/p_i^{\alpha_i}\mathscr{O}_K\right)^\times \longrightarrow G \longrightarrow 1$$

qui induit des isomorphismes [2]

$$\left(\prod_{i=1}^r \mathscr{O}_K/p_i^{\alpha_i}\mathscr{O}_K\right)^\times / \left(\prod_{i=1}^r \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}\right)^\times \simeq \prod_{i=1}^r (\mathscr{O}_K/p_i^{\alpha_i}\mathscr{O}_K)^\times / (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^\times \simeq G.$$

Ainsi, tous les facteurs $(\mathscr{O}_K/p_i^{\alpha_i}\mathscr{O}_K)^\times / (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^\times$ apparaissent comme sous-groupe de G et donc doivent avoir un exposant 2 au plus.

2. Le premier isomorphisme provient du fait que les anneaux dans le produit sont de caractéristique p_i et qu'il n'existe pas de morphisme d'anneaux entre deux anneaux de caractéristiques positives différentes.

L'objectif est alors de déterminer à quelle condition sur p le groupe $(\mathscr{O}_K/p^\alpha\mathscr{O}_K)^\times / (\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ peut être d'exposant au plus 2. La structure du groupe $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est très bien connue, si p est impair c'est un groupe cyclique d'ordre $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$ (où φ est l'indicatrice d'Euler) et $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ est presque cyclique ; pour $\alpha \geq 2$ on a

$$(\mathbb{Z}/2^\alpha\mathbb{Z})^\times \simeq (\mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}/2^{\alpha-2}\mathbb{Z}.$$

Malheureusement, la structure de groupe de $(\mathscr{O}_K/p^\alpha\mathscr{O}_K)^\times$ n'est pas connue à ma connaissance. Elle semble dépendre fortement de si p est impair et de si l'idéal $\langle p \rangle$ est inerte, se décompose ou ramifie dans $\mathscr{O}_K$. Une fois ces distinctions faites, la structure de $(\mathscr{O}_K/\mathfrak{p}^\alpha)^\times$ semble pouvoir être décrite de manière générale indépendemment de K. Je ne sais pas si c'est vrai ni comment le démontrer, je propose ci-dessous uniquement les résultats sur la structure de $(\mathscr{O}_K/\mathfrak{p}^\alpha)^\times$ nécessaires à la preuve du Théorème A.2.1. Ces résultats ne sont pas suffisants pour en déduire la structure du groupe en général.

On notera souvent $[a]$ ou $[\mathfrak{a}]$ pour la classe d'un élément $a \in \mathscr{O}_K$ ou d'un idéal $\mathfrak{a}$ dans un quotient $\mathscr{O}_K/\mathfrak{b}$.

Lemme A.2.2. *Soit $\mathfrak{p}$ un idéal premier de $\mathscr{O}_K$, $\beta \in \mathscr{O}_K$ et $n \geq 1$ et considérons le morphisme de $\mathscr{O}_K$-modules*

$$\begin{aligned} m_\beta \colon \quad \mathscr{O}_K/\mathfrak{p}^n &\longrightarrow \mathscr{O}_K/\mathfrak{p}^n \\ x &\longmapsto \beta x. \end{aligned}$$

Alors $\ker m_\beta = \mathfrak{p}^{n-d}/\mathfrak{p}^n$ *et* $\operatorname{im} m_\beta = \mathfrak{p}^d/\mathfrak{p}^n$ *avec* $d = v_\mathfrak{p}(\beta)$*, la $\mathfrak{p}$-valuation de β, i.e. le plus grand t tel que* $\mathfrak{p}^t | \beta\mathscr{O}_K$.

Démonstration. Soit $x \in \mathscr{O}_K$ tel que $\pi(x) \in \ker m_\beta$ avec $\pi \colon \mathscr{O}_K \to \mathscr{O}_K/\mathfrak{p}^n$ la projection canonique. Alors $\beta x \in \mathfrak{p}^n$ donc $\mathfrak{p}^n | \beta x\mathscr{O}_K$ mais, par unicité de la décomposition en idéaux premiers $\beta\mathscr{O}_K = \mathfrak{p}^d\mathfrak{a}$ avec $\mathfrak{a}$ premier à $\mathfrak{p}$. Ainsi $\mathfrak{p}^n | x\mathfrak{p}^d\mathfrak{a}$ et $\mathfrak{p}^{n-d} | x\mathfrak{a}$. Puisque $\mathfrak{a}$ est premier à $\mathfrak{p}$, $\mathfrak{p}^{n-d} | x\mathscr{O}_K$, i.e. $x \in \mathfrak{p}^{n-d}$.

Réciproquement, il est clair que $x \in \mathfrak{p}^{n-d}$ implique $x\beta \in \mathfrak{p}^n$. Donc, $\ker m_\beta = \mathfrak{p}^{n-d}/\mathfrak{p}^n = \pi(\mathfrak{p}^{n-d})$. Puisque, $\#(\mathscr{O}_K/\mathfrak{p}^n)/(\mathfrak{p}^{n-d}/\mathfrak{p}^n) = \#\mathscr{O}_K/\mathfrak{p}^{n-d} = N(\mathfrak{p})^{n-d}$ on a $\#\ker m_\beta = N(\mathfrak{p})^d$ et $\#\operatorname{im} m_\beta = N(\mathfrak{p})^{n-d}$.

Il est clair que $\operatorname{im} m_\beta \subseteq \pi(\mathfrak{p}^d) = \mathfrak{p}^d/\mathfrak{p}^n$ de cardinal $N(\mathfrak{p})^{n-d}$ on a une inclusion d'ensembles finis de même cardinaux donc $\operatorname{im} m_\beta = \mathfrak{p}^d/\mathfrak{p}^n$. □

On a une généralisation de [Cox85, Exercise 7.28] (le résultat est énoncé pour $m = 1$

dans le livre).

Proposition A.2.3. *Soit K un corps quadratique imaginaire et $\mathfrak{p} \subseteq \mathscr{O}_K$ un idéal premier. Alors, pour tout n et m tels que $n \geq 2m \geq 2$ on a une suite exacte de groupes*

$$1 \longrightarrow \mathscr{O}_K/\mathfrak{p}^m \longrightarrow (\mathscr{O}_K/\mathfrak{p}^n)^\times \longrightarrow \left(\mathscr{O}_K/\mathfrak{p}^{n-m}\right)^\times \longrightarrow 1$$

où le premier morphisme est $\alpha \mapsto [1+\alpha u]$ pour un $u \in \mathfrak{p}^{n-m} \setminus \mathfrak{p}^{n-m+1}$ et le second est la projection canonique π.

En particulier, en prenant les cardinaux pour $m = 1$, on a

$$\#\left(\mathscr{O}_K/\mathfrak{p}^n\right)^\times = N(\mathfrak{p})^{n-1}(N(\mathfrak{p})-1).$$

Démonstration. On va montrer que π est surjectif. C'est suffisant de ne traiter que le cas $m = 1$, les autres cas suivent par récurrence. Soit $[a] \in (\mathscr{O}_K/\mathfrak{p}^{n-1})^\times$ il existe donc $b \in \mathscr{O}_K$ tel que $[ab] = 1$, i.e. il existe $\gamma \in \mathfrak{p}^{n-1}$ tel que

$$ab = 1 + \gamma.$$

Si $\gamma \in \mathfrak{p}^n$ c'est gagné sinon, $\gamma \in \mathfrak{p}^{n-1} \setminus \mathfrak{p}^n$, c'est-à-dire que $v_\mathfrak{p}(\gamma) = n-1$, et le morphisme $\mathscr{O}_K$-linéaire

$$\begin{array}{rccc} m_{a\gamma}\colon & \mathscr{O}_K/\mathfrak{p}^n & \longrightarrow & \mathscr{O}_K/\mathfrak{p}^n \\ & x & \longmapsto & a\gamma x \end{array}$$

satisfait $\ker m_{a\gamma} = [\mathfrak{p}] \subseteq \mathscr{O}_K/\mathfrak{p}^n$ et $\operatorname{im} m_{a\gamma} = [\mathfrak{p}^{n-1}]$. En particulier, il existe $x \in \mathscr{O}_K$ tel que $a\gamma x = -\gamma = 1 - ab \in \mathscr{O}_K/\mathfrak{p}^n$ donc $a(b + x\gamma) = 1 \in \mathscr{O}_K/\mathfrak{p}^n$ donc la classe de a dans $\mathscr{O}_K/\mathfrak{p}^n$ est aussi inversible et est envoyé sur $[a] \in \mathscr{O}_K/\mathfrak{p}^{n-1}$ par π.

Maintenant, puisque $\mathfrak{p}^{n-m}$ et $\mathfrak{p}^{n-m+1}$ sont distincts par l'unicité de la factorisation en idéaux premiers dans les ordres maximaux, on peut choisir un élément $u \in \mathfrak{p}^{n-m} \setminus \mathfrak{p}^{n-m+1}$, i.e. tel que $v_\mathfrak{p}(u) = n - m$. Pour tout $a \in \mathscr{O}_K, au \in \mathfrak{p}^{n-m}$ et $(au)^2 \in \mathfrak{p}^{2(n-m)} \subseteq \mathfrak{p}^n$ d'après l'hypothèse $n \geq 2m$. Ainsi, la classe de au dans $\mathscr{O}_K/\mathfrak{p}^n$ est nilpotente ce qui implique que $[1+au]$ est inversible dans $\mathscr{O}_K/\mathfrak{p}^n$. De plus,

$$[1+au][1+bu] = [1+au+bu+abu^2] = [1+(a+b)u]$$

ce qui définit clairement un morphisme de groupe

$$\begin{aligned} \mathscr{O}_K &\longrightarrow (\mathscr{O}_K/\mathfrak{p}^n)^\times \\ a &\longmapsto [1+au] \end{aligned}$$

qui a pour noyau $\mathfrak{p}^m$ donc se factorise en un morphisme injectif qu'on note $\phi\colon \mathscr{O}_K/\mathfrak{p}^m \to (\mathscr{O}_K/\mathfrak{p}^n)^\times$. Puisque

$$\ker \pi_{|(\mathscr{O}_K/\mathfrak{p}^n)^\times} = \{[1+v], v \in \mathfrak{p}^{n-m}/\mathfrak{p}^n\} = \{[1+m_u(a)], a \in \mathscr{O}_K/\mathfrak{p}^n\} = \operatorname{im}\phi$$

car $v_\mathfrak{p}(u) = n-m$. La suite est donc bien exacte. □

Remarquons l'analogie entre les ordres quadratiques maximaux $\mathscr{O}_K$ et $\mathbb{Z}$. Pour un idéal premier $\mathfrak{p}$ (resp. $p\mathbb{Z}$) de $\mathscr{O}_K$ (resp. de $\mathbb{Z}$) on a $\#\left(\mathscr{O}_K/\mathfrak{p}^\alpha\right)^\times = N(\mathfrak{p})^{\alpha-1}(N(\mathfrak{p})-1)$ (resp.$\#\left(\mathbb{Z}/p^\alpha\mathbb{Z}\right)^\times = p^{\alpha-1}(p-1)$). Malheureusement, l'analogie semble s'arrêter là. La structure de groupe de $(\mathscr{O}_K/\mathfrak{p}^\alpha)^\times$ semble plus difficile à décrire que celle de $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$.

Remarquons aussi que la structure d'anneau de $\mathscr{O}_K/\mathfrak{p}^\alpha\mathscr{O}_K$ semble difficile à expliciter en général. Par exemple, si 2 ramifie dans $\mathscr{O}_K$, i.e. $2\mathscr{O}_K = \mathfrak{p}^2$ pour un idéal $\mathfrak{p}$. Alors $A = \mathscr{O}_K/2\mathscr{O}_K$ est un anneau à 4 éléments, de caractéristique 2, ce n'est donc pas $\mathbb{Z}/4\mathbb{Z}$. On a $\#A^\times = 2$ donc $A \neq \mathbb{F}_4$ car $\mathbb{F}_4^\times = 3$ et A n'est pas non plus isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$ car ce dernier n'a qu'un seul inversible. Il ne s'agit donc pas d'un des 3 anneaux « classiques » à 4 éléments (il existe 4 classes d'anneaux unitaires commutatifs à 4 éléments).

Proposition A.2.4. *Soit p un premier de $\mathbb{Z}$ qui se décompose dans $\mathscr{O}_K$, i.e. il existe $\mathfrak{p} \neq \overline{\mathfrak{p}}$ un idéal premier de $\mathscr{O}_K$ tel que $\mathfrak{p}\overline{\mathfrak{p}} = p\mathscr{O}_K$. Alors, pour tout $\alpha \geq 1$ on a des isomorphismes d'anneaux*

$$\mathbb{Z}/p^\alpha\mathbb{Z} \simeq \mathscr{O}_K/\mathfrak{p}^\alpha\mathscr{O}_K \text{ et } \mathscr{O}_K/p^\alpha\mathscr{O}_K \simeq (\mathbb{Z}/p^\alpha\mathbb{Z})^2.$$

Démonstration. Puisque l'anneau $\mathscr{O}_K/\mathfrak{p}^\alpha\mathscr{O}_K$ est de cardinal p^α sa caractéristique doit diviser p^α. Soit β tel que $p^\beta \in \mathfrak{p}^\alpha$ alors $\mathfrak{p}^\beta\overline{\mathfrak{p}}^\beta \subseteq \mathfrak{p}^\alpha$, i.e. $\mathfrak{p}^\alpha|\mathfrak{p}^\beta\overline{\mathfrak{p}}^\beta$ donc par unicité de la factorisation $\beta \geq \alpha$. Ainsi, $\mathscr{O}_K/\mathfrak{p}^\alpha\mathscr{O}_K$ est de caractéristique $\geq p^\alpha$. Le morphisme universel $\mathbb{Z} \to \mathscr{O}_K/\mathfrak{p}^\alpha\mathscr{O}_K$ se factorise en un morphisme d'anneaux injectif

$$\mathbb{Z}/p^\alpha\mathbb{Z} \to \mathscr{O}_K/\mathfrak{p}^\alpha\mathscr{O}_K$$

entre anneaux de même cardinal. Il s'agit donc d'un isomorphisme.

C'est valable aussi pour l'idéal premier $\overline{\mathfrak{p}}$ donc par le théorème des restes

$$\mathscr{O}_K/p^\alpha\mathscr{O}_K \simeq \mathscr{O}_K/\mathfrak{p}^\alpha\overline{\mathfrak{p}}^\alpha\mathscr{O}_K \simeq \mathscr{O}_K/\mathfrak{p}^\alpha\mathscr{O}_K \times \mathscr{O}_K/\overline{\mathfrak{p}}^\alpha\mathscr{O}_K \simeq (\mathbb{Z}/p^\alpha\mathbb{Z})^2.$$

□

Le dernier cas qui demandera une attention particulière dans la preuve du Théorème A.2.1 est le cas où 2 ramifie dans $\mathscr{O}_K$. On va donc avoir besoin de quelques résultats sur la structure de $\mathscr{O}_K/2^\alpha\mathscr{O}_K$.

Lemme A.2.5. *Soit $\mathscr{O}_K$ un ordre quadratique maximal tel que 2 ramifie*[3] *dans $\mathscr{O}_K$, i.e. $2\mathscr{O}_K = \mathfrak{p}^2$ pour un idéal $\mathfrak{p} = \langle 2, \beta\rangle$ de norme 2. Alors, pour tout $\alpha \in \mathbb{N}, a \in \mathscr{O}_K$ on a*

$$(1+2\beta a)^{2^{\alpha-1}} = 1 + 2^\alpha\beta a \mod \mathfrak{p}^{2\alpha+2}.$$

Démonstration. On procède par récurrence sur α. Pour $\alpha = 1$ on a $(1+2\beta a)^1 = 1+2^1\beta a$.

Soit $\alpha \geq 1$ tel qu'il existe $\delta \in \mathfrak{p}^{2\alpha+2}$ tel que $(1+2\beta a)^{2^{\alpha-1}} = 1 + 2^\alpha\beta a + \delta$. Alors

$$(1+2\beta a)^{2^\alpha} = (1+2^\alpha\beta a+\delta)^2 = 1 + 2^{2\alpha}\beta^2a^2 + \delta^2 + 2^{\alpha+1}\beta a + 2\delta + 2^\alpha\beta\delta a.$$

On va montrer que $2^{2\alpha}\beta^2a^2 + \delta^2 + 2\delta + 2^\alpha\beta\delta a \in \mathfrak{p}^{2\alpha+4}$.
Puisque $2\mathscr{O}_K = \mathfrak{p}^2$ on a

$$\begin{aligned} 2^{2\alpha}\beta^2a^2 &\in \mathfrak{p}^{4\alpha+2} \subseteq \mathfrak{p}^{2\alpha+4} \text{ pour } \alpha \geq 1 \\ \delta^2 &\in \mathfrak{p}^{4\alpha+4} \subseteq \mathfrak{p}^{2\alpha+4} \\ 2\delta &\in \mathfrak{p}^{2\alpha+4} \\ 2^\alpha\beta\delta &\in \mathfrak{p}^{2\alpha+1+2\alpha+2} \subseteq \mathfrak{p}^{4\alpha+3} \subseteq \mathfrak{p}^{2\alpha+4} \text{ pour } \alpha \geq 1. \end{aligned}$$

Donc

$$(1+2\beta a)^{2^\alpha} = 1 + 2^{\alpha+1}\beta a \mod \mathfrak{p}^{2\alpha+4}$$

ce qui conclue la preuve. □

Corollaire A.2.6. *En reprenant les mêmes notations que dans le Lemme A.2.5, pour tout $a \in \mathscr{O}_K$ premier à $\mathfrak{p}$ l'image de $u_a = 1 + 2\beta a$ dans $(\mathscr{O}_K/\mathfrak{p}^{2\alpha})^\times$ et dans $(\mathscr{O}_K/\mathfrak{p}^{2\alpha+1})^\times$ est d'ordre exactement $2^{\alpha-1}$ pour $\alpha \geq 2$.*

3. C'est le cas si, et seulement si, $2|\Delta$, i.e. si $\mathscr{O}_K = \mathbb{Z}[\omega]$, avec $\omega = 1 + \sqrt{-d}$. On peut alors choisir $\beta = \omega$ si d est pair et $\beta = 1 + \omega$ sinon. On a toujours $v_\mathfrak{p}(\beta) = 1$.

Démonstration. D'après la Proposition A.2.3, $\#(\mathscr{O}_K/\mathfrak{p}^n)^\times$ est d'ordre 2^n. Ainsi, par le Théorème de Lagrange, tous les éléments sont d'ordre 2^t pour $t \leq n$.

Puisque $2^{\alpha-1}\beta a \in \mathfrak{p}^{2\alpha-1} \setminus \mathfrak{p}^{2\alpha}, 1 + 2^{\alpha-1}\beta a$ est inversible et est différent de 1 dans $(\mathscr{O}_K/\mathfrak{p}^{2\alpha})^\times$ donc, par le Lemme A.2.5 appliqué à $\alpha - 2, (1 + 2\beta a)^{2^{\alpha-2}} \neq 1 \mod \mathfrak{p}^{2\alpha}$ donc $1 + 2\beta a$ est d'ordre 2^t pour $t \geq \alpha - 1$. Encore d'après le même lemme appliqué à $\alpha - 1, (1 + 2\beta a)^{2^{\alpha-1}} = 1 + 2^\alpha \beta a \mod \mathfrak{p}^{2\alpha+2} = 1 \mod \mathfrak{p}^{2\alpha}$. Donc $t \leq \alpha - 1$ donc u_a est d'ordre $2^{\alpha-1}$ dans $(\mathscr{O}_K/\mathfrak{p}^{2\alpha})^\times$.

De plus, par la Proposition A.2.3, la projection $\pi\colon (\mathscr{O}_K/\mathfrak{p}^{2\alpha+1})^\times \to (\mathscr{O}_K/\mathfrak{p}^{2\alpha})^\times$ est surjective et $\pi(1+2\beta a)$ est d'ordre $2^{\alpha-1}$ donc $2^{\alpha-1}$ divise l'ordre de $1+2\beta a \in (\mathscr{O}_K/\mathfrak{p}^{2\alpha+1})^\times$. En appliquant une fois de plus le Lemme A.2.5 à $\alpha - 1, (1 + 2\beta a)^{2^{\alpha-1}} = 1 + 2^\alpha \beta a \mod \mathfrak{p}^{2\alpha+2} = 1 \mod \mathfrak{p}^{2\alpha+1}$. Donc l'image de u_a dans $(\mathscr{O}_K/\mathfrak{p}^{2\alpha+1})^\times$ est aussi d'ordre $2^{\alpha-1}$. □

Proposition A.2.7. *En reprenant les notations du Corollaire A.2.6, pour tout $a \notin \mathfrak{p}$ on a*

$$\left(\mathbb{Z}/2^{\alpha-1}\mathbb{Z}\right)^\times \cap \langle u_a \rangle = \{1\}$$

où $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ est identifié avec le sous-groupe de $(\mathscr{O}_K/2^\alpha\mathscr{O}_K)^\times$ donné par l'injection[4] *$\mathbb{Z}/2^\alpha\mathbb{Z} \to \mathscr{O}_K/2^\alpha\mathscr{O}_K$ induite par le morphisme universel $\mathbb{Z} \to \mathscr{O}_K/2^\alpha\mathscr{O}_K$.*

Démonstration. On considère $(1 + 2\beta a)^n$ pour $n < 2^{\alpha-1}$. Alors

$$(1 + 2\beta a)^n = \sum_{k=0}^{n} \binom{n}{k} (2\beta a)^k = 1 + 2\beta a n + \sum_{k=2}^{n} \binom{n}{k} (2\beta a)^k.$$

On écrit $n = m2^j$ et $k = m_0 2^{j_0}$ avec m et m_0 impairs. On va montrer que pour tout n et $n \geq k \geq 2$ on a $v_\mathfrak{p}\left(\binom{n}{k}(2\beta a)^k\right) > 3 + 2j$.

D'après la relation $k\binom{n}{k} = n\binom{n-1}{k-1}$ on a que si $j \geq j_0$ alors $2^{j-j_0} | \binom{n}{k}$. Nous allons nous appuyer sur l'inégalité

$$v_\mathfrak{p}\left(\binom{n}{k}(2\beta a)^k\right) \geq 2\min(j - j_0, 0) + 3k = 2\min(j - j_0, 0) + 3m_0 2^{j_0}.$$

Cas $j < j_0$: Une récurrence immédiate sur j_0 montre que pour tout $m_0 \geq 1, j_0 \geq 1$, tel que $m_0 2^{j_0} \geq 2$ et tout $0 \leq j < j_0$ on a $3m_0 2^{j_0} > 3 + 2j$. En effet, pour $j_0 = 1, 6m_0 > 3$ et $j_0 \geq 1$ donné tel que pour tout m_0 et $j < j_0, 3m_0 2^{j_0} > 3 + 2j$ on a au rang $j_0 + 1$: $3m_0 2^{j_0+1} = 2 \times 3m_0 2^{j_0} > 6 + 4j \geq 3 + 2(j + 1) = 2j + 5$.

4. Puisque 2 ramifie, l'anneau $\mathscr{O}_K/2^\alpha\mathscr{O}_K$ est de caractéristique 2^α.

Cas $j \geq j_0$: Ici $v_{\mathfrak{p}}\left(\binom{n}{k}(2\beta a)^k\right) \geq 2j - 2j_0 + 3m_0 2^{j_0}$ or $2j - 2j_0 + 3m_0 2^{j_0} > 3 + 2j$ si, et seulement si $3m_0 2^{j_0} > 3 + 2j_0$ ce qui peut aussi être montré par récurrence. Si $j_0 = 0$, alors $m_0 \geq 3$ et ainsi, $3m_0 \geq 9 > 3$, la fin de la récurrence est la même que pour $j < j_0$.

Supposons désormais qu'il existe un entier q dont la classe dans $\mathbb{Z}/2^{\alpha-1}\mathbb{Z}$ est inversible (donc q est impair, disons $q = 2q' + 1$) et tel que $q = (1 + 2\beta a)^n \neq 1 \mod 2^\alpha \mathscr{O}_K$ avec $n = m2^j$. Puisqu'on a supposé que $(1 + 2\beta a)^n \neq 1 \mod 2^\alpha \mathscr{O}_K$ on a $2\beta an \neq 0 \mod 2^\alpha \mathscr{O}_K$. En effet, puisque $v_{\mathfrak{p}}\left(\binom{n}{k}(2\beta a)^k\right) > 3 + 2j = v_{\mathfrak{p}}(2\beta an), 2\beta an = 0 \mod 2^\alpha \mathscr{O}_K$ implique $\binom{n}{k}(2\beta a)^k = 0 \mod 2^\alpha \mathscr{O}_K$ pour tout k donc $(1 + 2\beta a)^n = 1 \mod 2^\alpha \mathscr{O}_K$ ce qui est absurde. Donc, en notant $2\beta an = \mathfrak{p}^{3+2j}\mathfrak{a}$ avec $\mathfrak{a}$ premier à $\mathfrak{p}$ on a

$$q = 2q' + 1 = 1 + 2\beta an + \gamma$$

avec $\gamma \in \mathfrak{p}^r$ et $r > 3 + 2j$. Donc

$$q'\mathscr{O}_K = \mathfrak{p}^{1+2j}(\mathfrak{a} + \mathfrak{p} \times \mathfrak{b})$$

pour un idéal $\mathfrak{b}$. Donc q' est un entier dont la $\mathfrak{p}$-valuation est $2j+1$ ce qui est contradictoire car la $\mathfrak{p}$-valuation de tout entier est paire. □

On peut enfin démontrer le résultat qui nous intéresse.

Démonstration du Théorème A.2.1 pour $\Delta \notin \{-3, -4\}$. On va étudier pour quels p le groupe

$$\left(\mathscr{O}_K/p^\alpha\mathscr{O}_K\right)^\times / \left(\mathbb{Z}/p^\alpha\mathbb{Z}\right)^\times$$

peut être d'exposant 2. Remarquons que si c'est le cas alors son cardinal est une puissance de 2.

p **est inerte :** Si p est inerte, i.e. $p\mathscr{O}_K$ est un idéal premier, par la Proposition A.2.3,

$$\#\left(\mathscr{O}_K/p^\alpha\mathscr{O}_K\right)^\times / \left(\mathbb{Z}/p^\alpha\mathbb{Z}\right)^\times = p^{2(\alpha-1)}(p^2 - 1)/p^{\alpha-1}(p - 1) = p^{\alpha-1}(p + 1).$$

Donc soit $\alpha = 1$, soit $p = 2$ et $p + 1$ doit être pair, ce qui est impossible. Supposons $\alpha = 1$. Alors $\mathscr{O}_K/p\mathscr{O}_K$ est un corps fini isomorphe à $\mathbb{F}_{p^2}$ et donc $(\mathscr{O}_K/p\mathscr{O}_K)^\times = (\mathscr{O}_K/p\mathscr{O}_K) \setminus \{1\}$ est cyclique tout comme le quotient $(\mathscr{O}_K/p\mathscr{O}_K)^\times/(\mathbb{Z}/p\mathbb{Z})^\times$ qui est d'ordre $p + 1$, donc $p + 1 = 2$ ce qui est absurde. Donc, si un ordre quadratique est

d'exposant au plus 2 alors son conducteur n'est pas divisible par un premier inerte dans $\mathscr{O}_K$.

p **est ramifié :** Dans ce cas $p\mathscr{O}_K = \mathfrak{p}^2$ pour un idéal premier $\mathfrak{p}$. Le quotient

$$(\mathscr{O}_K/p^\alpha\mathscr{O}_K)^\times/(\mathbb{Z}/p^\alpha\mathbb{Z})^\times \simeq (\mathscr{O}_K/\mathfrak{p}^{2\alpha})^\times/(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$$

est de cardinal $\frac{p^{2\alpha-1}(p-1)}{p^\alpha(p-1)} = p^{\alpha-1}$ donc, par le théorème de Cauchy, $p = 2$. D'après la Proposition A.2.7 on a $(\mathscr{O}_K/\mathfrak{p}^{2\alpha})^\times/(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ a un sous-groupe isomorphe à $\mathbb{Z}/2^{\alpha-1}\mathbb{Z}$ engendré par la classe de u_a. Ceci implique que $\alpha - 1 \leq 1$, i.e. $\alpha \leq 2$.

p **est décomposé :** Dans ce cas $p\mathscr{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$ pour $\overline{\mathfrak{p}} \neq \mathfrak{p}$. Alors d'après la Proposition A.2.4 on a un isomorphisme d'anneaux

$$\mathscr{O}_K/p^\alpha\mathscr{O}_K \simeq \mathscr{O}_K/\mathfrak{p} \times \mathscr{O}_K/\overline{\mathfrak{p}} \simeq (\mathbb{Z}/p^\alpha\mathbb{Z})^2$$

et, puisque $\mathscr{O}_K/p^\alpha\mathscr{O}_K$ est de caractéristique p^α, $\mathbb{Z}/p^\alpha\mathbb{Z}$ s'injecte dans $\mathscr{O}_K/p^\alpha\mathscr{O}_K$, sa composée par les isomorphismes ci-dessus donne

$$\begin{array}{rcl} \mathbb{Z}/p^\alpha\mathbb{Z} & \longrightarrow & (\mathbb{Z}/p^\alpha\mathbb{Z})^2 \\ a & \longmapsto & (a,a). \end{array}$$

Or pour tout groupe abélien H on a toujours exacte une suite exacte

$$\begin{array}{ccccccccc} 0 \to & H & \to & H \times H & \to & H & \to & 0 \\ & x & \mapsto & (x,x),(x,y) & \mapsto & x-y & & \end{array} \tag{A.3}$$

Donc $(\mathscr{O}_K/p^\alpha\mathscr{O}_K)^\times/(\mathbb{Z}/p^\alpha\mathbb{Z})^\times \simeq (\mathbb{Z}/p^\alpha\mathbb{Z})^\times$. On en déduit que soit p est impair auquel cas $\alpha = 1$ et $p = 3$, soit $p = 2$ auquel cas $\alpha \in \{1,2,3\}$.

On obtient alors que $f = 2^a3^b$, avec $a \leq 3$ et $b \leq 1$. Nous avons en fait montré des résultats beaucoup plus précis et nous pourrions discuter d'avantage de quel cas peut se produire en fonction du discriminant par exemple mais ça n'est pas nécessaire alors nous en resterons là. □

Cas $\Delta = -3$ ou -4

La clé pour les cas $\Delta \notin \{-3,-4\}$ est la suite exacte (A.2) qui dépend du fait que $\mathscr{O}_K$ a pour groupe des inversibles $\mathscr{O}_K^\times = \{\pm 1\}$. Pour les deux cas restants le groupe des

inversibles est plus gros. On a $\mathscr{O}_{\mathbb{Z}[j]}^{\times} = \{\pm 1, \pm j, \pm j^2\}$ pour le discriminant et $\mathscr{O}_{\mathbb{Z}[i]}^{\times} = \{\pm 1, \pm i\}$ pour le discriminant -4. On peut alors s'inspirer de la suite exacte (A.2) pour en déduire ([Cox85, Exercise 7.30])

$$1 \to \{\pm 1\} \to (\mathbb{Z}/f\mathbb{Z})^{\times} \times \mathscr{O}_K^{\times} \xrightarrow{\phi} (\mathscr{O}_K/f\mathscr{O}_K)^{\times} \to G \to 1 \tag{A.4}$$

où $\phi(a,u) = au$ (et $G = I_K(f) \cap P_K/P_{K,\mathbb{Z}}(f)$ qui, on le rappelle est d'exposant au plus 2). Pour chaque p^{α} intervenant dans la décomposition en facteurs premiers de f on a le diagramme commutatif

$$\begin{array}{ccc} \prod_i \left(\left((\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^{\times} \times \mathscr{O}_K^{\times} \right) / \{\pm 1\} \right) & \xrightarrow{\prod_i \phi_{p_i}} & \prod_i (\mathscr{O}_K/p_i^{\alpha_i}\mathscr{O}_K)^{\times} \\ \uparrow & & \uparrow \\ \left((\mathbb{Z}/f\mathbb{Z})^{\times} \times \mathscr{O}_K^{\times} \right) / \{\pm 1\} & \xrightarrow{\phi} & (\mathscr{O}_K/f\mathscr{O}_K)^{\times} \end{array}$$

où la flèche ϕ provient de la suite exacte (A.4), celle du haut est aussi une application composante par composante de la suite exacte (A.4), la flèche de droite est l'isomorphisme du théorème des restes appliqué à $\mathscr{O}_K/f\mathscr{O}_K$ et celle de gauche provient aussi du théorème des restes mais appliqué à $\mathbb{Z}/f\mathbb{Z}$. L'intérêt est de considérer le groupe (et donc chaque composante du produit)

$$\prod_i (\mathscr{O}_K/p_i^{\alpha_i}\mathscr{O}_K)^{\times} / \left(\left((\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^{\times} \times \mathscr{O}_K^{\times} \right) / \{\pm 1\} \right)$$

comme un sous groupe de

$$(\mathscr{O}_K/f\mathscr{O}_K)^{\times} / \left(\left((\mathbb{Z}/f\mathbb{Z})^{\times} \times \mathscr{O}_K^{\times} \right) / \{\pm 1\} \right)$$

qui est isomorphe à G d'exposant au plus 2 et d'en déduire des conditions sur les p encore une fois. La quasi totalité de la fin de la preuve peut être traitée avec les outils déjà développé à l'exception près du cas $p = 2$ dans $\mathbb{Z}[j]$ pour lequel nous avons besoin du Lemme A.2.8 et de la PropositionA.2.9.

Lemme A.2.8. *Soit $\mathscr{O}_K = \mathbb{Z}[j] = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ alors pour $\alpha \geq 3, 1+4j$ est d'ordre $2^{\alpha-2}$ dans $(\mathscr{O}_K/2^{\alpha}\mathscr{O}_K)^{\times}$.*

Démonstration. On prouve que

$$(1+4j)^{2^{\alpha-3}} = 1 + 2^{\alpha-1}j \mod 2^\alpha \mathscr{O}_K.$$

C'est trivial pour $\alpha = 3$. Soit $\alpha \geq 3$ tel que la relation est vraie au rang α, donc on a $b \in \mathscr{O}_K$ tel que $(1+4j)^{2^{\alpha-3}} = 1 + 2^{\alpha-1}j + 2^\alpha b$ donc,

$$(1+4j)^{2^{\alpha-2}} = (1 + 2^{\alpha-1}j + b2^\alpha)^2 = 1 + 2^\alpha j \mod 2^{\alpha+1}\mathscr{O}_K.$$

□

Proposition A.2.9. *En reprenant les notation du Lemme A.2.8 il existe un élément d'ordre $2^{\alpha-2}$ dans le quotient $(\mathscr{O}_K/2^\alpha\mathscr{O}_K)^\times / \operatorname{im}\phi$ avec*

$$\begin{aligned} \phi\colon \ (\mathbb{Z}/2^\alpha\mathbb{Z})^\times \times \mathscr{O}_K^\times &\longrightarrow (\mathscr{O}_K/2^\alpha\mathscr{O}_K)^\times \\ (u,a) &\longmapsto au. \end{aligned}$$

Démonstration. On montre que $\langle 1+4j\rangle$ ne contient aucune classe d'entier autre que 1. D'abord, puisque j est inversible, $\mathscr{O}_K/2^\alpha\mathscr{O}_K$ est un $\mathbb{Z}/2^\alpha\mathbb{Z}$-module libre de base $(1,j)$ donc on peut représenter toutes les classes de la forme $a+bj$ modulo $2^\alpha\mathscr{O}_K$ avec a,b des entiers uniques modulo 2^α. Supposons maintenant qu'il existe $n \in \mathbb{N}$ et $u \in \mathbb{Z}$ impair tels que

$$(1+4j)^n = u \mod 2^\alpha\mathscr{O}_K$$

avec $n = 2^{\alpha_0}m, \alpha_0 < \alpha - 2$ et m impair. On a donc $((1+4j)^n)^{2^{\alpha-2-\alpha_0}} = (1+2^{\alpha-1}j)^m = u^{2^{\alpha-2-\alpha_0}}$ et, puisque $1+2^{\alpha-1}j$ est d'ordre 2, on a $(1+2^{\alpha-1}j)^m = 1+2^{\alpha-1}j$. Cependant, $(1,j)$ est une $\mathbb{Z}/2^\alpha\mathbb{Z}$-base de $\mathscr{O}_K/2^\alpha\mathscr{O}_K$ donc $1+2^{\alpha-1}j$ ne peut être l'image d'un élément de $2^\alpha\mathscr{O}_K$.

Supposons que $(1+4j)^n = au \in (\mathscr{O}_K/2^\alpha\mathscr{O}_K)^\times$ avec $a \in \mathbb{Z}$ et $u \in \mathscr{O}_K^\times$ alors $(1+4j)^{3n} = \pm a^3$, donc $a \in \{\pm 1\}$ et $2^{\alpha-2}|3n$ donc $2^{\alpha-2}|n$ et $au = 1$. On en conclue que $1+4j$ est d'ordre $2^{\alpha-2}$ dans le quotient. □

Fin de la démonstration du Théorème A.2.1. On veut étudier à quelles conditions sur p le groupe

$$H = (\mathscr{O}_K/p^\alpha\mathscr{O}_K)^\times \,/\, \Big(\big((\mathbb{Z}/p^\alpha\mathbb{Z})^\times \times \mathscr{O}_K^\times\big)/\{\pm 1\}\Big)$$

peut être d'exposant au plus 2. On sépare encore les cas p inerte, ramifié et décomposé. On pose $\delta = \#\mathscr{O}_K^\times/2$. On a $\delta = 3$ pour $\Delta = -3$ et $\delta = 2$ pour $\Delta = -4$.

p **inerte :** On a $\#H = \frac{p^{2\alpha-2}(p^2-1)}{p^{\alpha-1}(p-1)\delta} = \frac{p^{\alpha-1}(p+1)}{\delta}$.

Cas $\Delta = -4$: On a $\delta = 2$ donc $p \neq 2$ sinon $p+1$ impair. Donc p est impair et donc $\alpha = 1$ mais alors $\mathscr{O}_K/p\mathscr{O}_K$ est un corps donc H est cyclique d'ordre $\frac{p+1}{2}$ et d'exposant au plus 2 donc $p = 3$.

Cas $\Delta = -3$: Si p est impair, on a forcément $p = 3$ et $\alpha \leq 2$ (absurde car 3 est ramifié dans $\mathbb{Z}[j]$) ou alors $\alpha = 1$ auquel cas, encore une fois $(\mathscr{O}_K/p\mathscr{O}_K)^\times$ est cyclique d'ordre $\frac{p+1}{3}$ ce qui impose $p = 5$ (on a effectivement 5 inerte dans $\mathbb{Z}[j]$).

Si $p = 2$, d'après la Proposition A.2.9, $1 + 4j$ est d'ordre $2^{\alpha-2}$ dans H. Donc $\alpha \leq 3$.

p **ramifié :** On a $\#H = \frac{p^{2\alpha-1}(p-1)}{p^{\alpha-1}(p-1)\delta} = \frac{p^\alpha}{\delta}$. Donc

Cas $\Delta = -4$: On a alors $\delta = 2$ donc $p = 2$ et, par la Proposition A.2.7, on a un élément $u_a \in (\mathscr{O}_K/2^\alpha\mathscr{O}_K)^\times$ d'ordre $2^{\alpha-1}$ dans $(\mathscr{O}_K/2^\alpha\mathscr{O}_K)^\times/(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$. On considère n tel que $\phi_p(u_a)^n = 1$ (on étudie l'ordre de son image dans H). On a alors $(a, u) \in (\mathbb{Z}/2^\alpha\mathbb{Z})^\times \times \mathscr{O}_K^\times, u_a^n = au$ donc $u_a^{2n} = a^2$ car $u^2 = 1$ dans $\mathscr{O}_K^\times$. Donc $u_a^{2n} \in \langle u_a \rangle \cap (\mathbb{Z}/2^\alpha\mathbb{Z})^\times = \{1\}$ autrement dit $2^{\alpha-1} | 2n$ donc l'ordre de l'image de u_a dans H est divisible par $2^{\alpha-2}$. On en déduit que $\alpha \leq 3$.

Cas $\Delta = -3$: On a $\delta = 3$ donc $p = 3$ et $\alpha = 1$.

En conclusion, on a forcément 2 qui ramifie dans $\mathscr{O}_K = \mathbb{Z}[i]$ qui impose $\alpha \leq 3$ et 3 qui ramifie dans $\mathscr{O}_K = \mathbb{Z}[j]$ qui impose $\alpha = 1$.

p **est décomposé :** On a $\#H = \frac{\left(p^{\alpha-1}(p-1)\right)^2}{p^{\alpha-1}(p-1)\delta} = \frac{p^{\alpha-1}(p-1)}{\delta}$. Puisque 2 ramifie dans $\mathbb{Z}[i]$ et est inerte dans $\mathbb{Z}[j]$ on a forcément p impair. De plus, 3 est ramifié dans $\mathbb{Z}[j]$. On en déduit qu'on a nécessairement $\alpha = 1$ et H de cardinal $\frac{p-1}{\delta}$. Par ailleurs, la Proposition A.2.4 et la suite exacte (A.3) montre que

$$(\mathscr{O}_K/p\mathscr{O}_K)^\times \simeq \langle a \rangle \times \langle u \rangle$$

où a est un générateur de l'image de $(\mathbb{Z}/p\mathbb{Z})^\times$ et u un élément d'ordre $p-1$. Un argument similaire à celui utilisé pour montrer que l'image de u_a dans H est d'ordre $\geq 2^{\alpha-2}$ dans le cas $\Delta = -4$ ramifié montre que l'image de u dans H est d'ordre $\geq \frac{p-1}{\delta}$. Ce qui impose $p = 5$ pour $\Delta = -4$ et $p = 7$ pour $\Delta = -3$.

□

BIBLIOGRAPHIE

[AK17] Zavosh Amir-Khosravi. Serre's tensor construction and moduli of abelian schemes. *manuscripta mathematica*, 156(3-4) :409–456, oct 2017.

[Bai62] Walter L. Baily, Jr. On the theory of θ-functions, the moduli of abelian varieties, and the moduli of curves. *Ann. of Math. (2)*, 75 :342–381, 1962.

[BF60] Z. I. Borevič and D. K. Faddeev. Integral representations of quadratic rings. *Vestnik Leningrad. Univ.*, 15(19) :52–64, 1960.

[BFGR06] Nils Bruin, E. Victor Flynn, Josep González, and Victor Rotger. On finiteness conjectures for endomorphism algebras of abelian surfaces. *Math. Proc. Cambridge Philos. Soc.*, 141(3) :383–408, 2006.

[BL94] J. A. Buchmann and H. W. Lenstra, Jr. Approximating rings of integers in number fields. *J. Théor. Nombres Bordeaux*, 6(2) :221–260, 1994.

[BS66] A. I. Borevich and I. R. Shafarevich. *Number theory*. Pure and Applied Mathematics, Vol. 20. Academic Press, New York-London, 1966. Translated from the Russian by Newcomb Greenleaf.

[Cona] K. Conrad. Ideal classes and relative integers. https ://kconrad.math.uconn.edu/blurbs/gradnumthy/relativeintandidealclasses.pdf.

[Conb] K. Conrad. Ideal factorization. https ://kconrad.math.uconn.edu/blurbs/gradnumthy/idealfactor.pdf.

[Cox85] D. A. Cox. *Primes of the form x^2+ny^2, Fermat, class field theory, and complex multiplication*. Wiley Interscience, 1985.

[CR15] Romain Cosset and Damien Robert. An algorithm for computing (ℓ, ℓ)-isogenies in polynomial time on jacobians of hyperelliptic curves of genus 2. *Mathematics of Computation*, 84(294) :1953–1975, 11 2015.

[CS15] Tommaso Giorgio Centeleghe and Jakob Stix. Categories of abelian varieties over finite fields, I : Abelian varieties over $\mathbb{F}_p$. *Algebra Number Theory*, 9(1) :225–265, 2015.

[CS21] Tommaso Giorgio Centeleghe and Jakob Stix. Categories of abelian varieties over finite fields ii : Abelian varieties over finite fields and morita equivalence, 2021.

[Deb95] Olivier Debarre. The Schottky problem : an update. In *Current topics in complex algebraic geometry (Berkeley, CA, 1992/93)*, volume 28 of *Math. Sci. Res. Inst. Publ.*, pages 57–64. Cambridge Univ. Press, Cambridge, 1995.

[Deb05] O. Debarre. *Tores et variétés abéliennes complexes*. Société Mathématique de France, 2005.

[Del69] Pierre Deligne. Variétés abéliennes ordinaires sur un corps fini. *Invent. Math.*, 8 :238–243, 1969.

[EKN20] Andreas-Stephan Elsenhans, Jürgen Klüners, and Florin Nicolae. Imaginary quadratic number fields with class groups of small exponent. *Acta Arith.*, 193(3) :217–233, 2020.

[Fei78] Walter Feit. Some lattices over $\mathbf{Q}(\sqrt{-3})$. *J. Algebra*, 52(1) :248–263, 1978.

[FG20] Francesc Fité and Xavier Guitart. Endomorphism algebras of geometrically split abelian surfaces over $\mathbb{Q}$. *Algebra & Number Theory*, 14(6) :1399–1421, jul 2020.

[Fio16] A. Fiorentino. Weber's formula for the bitangents of a smooth plane quartic, 2016.

[GHR19] Alexandre Gélin, Everett W. Howe, and Christophe Ritzenthaler. Principally polarized squares of elliptic curves with field of moduli equal to $\mathbb{Q}$. In *Proceedings of the Thirteenth Algorithmic Number Theory Symposium*, volume 2 of *Open Book Ser.*, pages 257–274. Math. Sci. Publ., Berkeley, CA, 2019.

[Gru12] Samuel Grushevsky. The Schottky problem. In *Current developments in algebraic geometry*, volume 59 of *Math. Sci. Res. Inst. Publ.*, pages 129–164. Cambridge Univ. Press, Cambridge, 2012.

[Har77] Robin Hartshorne. *Algebraic geometry*. Graduate Texts in Mathematics, No. 52. Springer-Verlag, New York-Heidelberg, 1977.

[HN65] Tsuyoshi Hayashida and Mieo Nishi. Existence of curves of genus two on a product of two elliptic curves. *J. Math. Soc. Japan*, 17 :1–16, 1965.

[Hof91] D.W. Hoffmann. On positive definite hermitian forms. *Manuscripta mathematica, Springer-Vertag*, 1991.

[Hug06] Bonnie Huggins. Fields of moduli and fields of definition of curves, 2006.

[IKY22] Tomoyoshi Ibukiyama, Valentijn Karemaker, and Chia-Fu Yu. The gauss problem for central leaves, 2022.

[Iya69] Kenichi Iyanaga. Class numbers of definite Hermitian forms. *J. Math. Soc. Japan*, 21 :359–374, 1969.

[Jac62] R. Jacobowitz. Hermitian forms over local fields. *Amer. J. Math.*, 84 :441–465, 1962.

[JKP+18] Bruce W. Jordan, Allan G. Keeton, Bjorn Poonen, Eric M. Rains, Nicholas Shepherd-Barron, and John T. Tate. Abelian varieties isogenous to a power of an elliptic curve. *Compos. Math.*, 154(5) :934–959, 2018.

[Kan11] Ernst Kani. Products of CM elliptic curves. *Collect. Math.*, 62(3) :297–339, 2011.

[Kir16] M. Kirschmer. *Definite quadratic and hermitian forms with small class number*. Habilitation à diriger des recherches en mathématiques et en informatique, 2016.

[Kir19] Markus Kirschmer. Determinant groups of Hermitian lattices over local fields. *Arch. Math. (Basel)*, 113(4) :337–347, 2019.

[Kne57] Martin Kneser. Klassenzahlen definiter quadratischer Formen. *Arch. Math.*, 8 :241–250, 1957.

[KNRR21] Markus Kirschmer, Fabien Narbonne, Christophe Ritzenthaler, and Damien Robert. Spanning the isogeny class of a power of an elliptic curve. *Math. Comp.*, 91(333) :401–449, 2021.

[Lan87] Serge Lang. *Elliptic functions*, volume 112 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1987. With an appendix by J. Tate.

[Lan94] Serge Lang. *Algebraic number theory*, volume 110 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1994.

[Lau01] Kristin Lauter. Geometric methods for improving the upper bounds on the number of rational points on algebraic curves over finite fields. *J. Algebraic Geom.*, 10(1) :19–36, 2001. With an appendix in French by J.-P. Serre.

[Lei14] Tom Leinster. *Basic category theory*, volume 143 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2014.

[Liu02] Qing Liu. *Algebraic geometry and arithmetic curves*, volume 6 of *Oxford Graduate Texts in Mathematics*. Oxford University Press, Oxford, 2002. Translated from the French by Reinie Erné, Oxford Science Publications.

[LR12] Reynald Lercier and Christophe Ritzenthaler. Hyperelliptic curves and their invariants : geometric, arithmetic and algorithmic aspects. *J. Algebra*, 372 :595–636, 2012.

[LRRS14] Reynald Lercier, Christophe Ritzenthaler, Florent Rovetta, and Jeroen Sijsling. Parametrizing the moduli space of curves and applications to smooth plane quartics over finite fields. *LMS J. Comput. Math.*, 17(suppl. A) :128–147, 2014.

[LW85] Lawrence S. Levy and Roger Wiegand. Dedekind-like behavior of rings with 2-generated ideals. *J. Pure Appl. Algebra*, 37(1) :41–58, 1985.

[Mar20a] Stefano Marseglia. Computing the ideal class monoid of an order. *J. Lond. Math. Soc. (2)*, 101(3) :984–1007, 2020.

[Mar20b] Stefano Marseglia. Super-multiplicativity of ideal norms in number fields. *Acta Arith.*, 193(1) :75–93, 2020.

[Mil08] James S. Milne. Abelian varieties (v2.00), 2008. Available at www.jmilne.org/math/.

[Mil20] James S. Milne. Algebraic number theory (v3.08), 2020. Available at www.jmilne.org/math/.

[Mum66] D. Mumford. On the equations defining abelian varieties. I. *Invent. Math.*, 1 :287–354, 1966.

[Mum67a] D. Mumford. On the equations defining abelian varieties. II. *Invent. Math.*, 3 :75–135, 1967.

[Mum67b] D. Mumford. On the equations defining abelian varieties. III. *Invent. Math.*, 3 :215–244, 1967.

[Mum70] David Mumford. *Abelian varieties*. Tata Institute of Fundamental Research Studies in Mathematics, No. 5. Published for the Tata Institute of Fundamental Research, Bombay ; Oxford University Press, London, 1970.

[MWZ96] A. J. Menezes, Y. H. Wu, and R. J. Zuccherato. An elementary introduction to hyperelliptic curves, 1996.

[Nar22] Fabien Narbonne. Polarized products of elliptic curves with complex multiplication and field of moduli $\mathbb{Q}$, 2022.

[O'M63] O.T. O'Meara. *Introduction to quadratic forms*. Springer-Verlag, 1963.

[OU73] Frans Oort and Kenji Ueno. Principally polarized abelian varieties of dimension two or three are Jacobian varieties. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.*, 20 :377–381, 1973.

[Rit10] Christophe Ritzenthaler. Explicit computations of Serre's obstruction for genus-3 curves and application to optimal curves. *LMS J. Comput. Math.*, 13 :192–207, 2010.

[Rit17] C. Ritzenthaler. Effective geometry and arithmetic of curves : an introduction, 2017.

[SC86] J.H. Silverman and G. Cornell. *Arithmetic geometry*. Springer, 1986.

[Sch85] Winfried Scharlau. *Quadratic and Hermitian forms*, volume 270 of *Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1985.

[Sch98] A. Schiemann. Classification of hermitian forms with the neighbour method. *Academic Press*, 1998.

[Ser20] Jean-Pierre Serre. *Rational points on curves over finite fields*, volume 18 of *Documents Mathématiques (Paris) [Mathematical Documents (Paris)]*. Société Mathématique de France, Paris, [2020] ©2020. With contributions by Everett Howe, Joseph Oesterlé and Christophe Ritzenthaler, Edited by Alp Bassa, Elisa Lorenzo García, Christophe Ritzenthaler and René Schoof.

[Shi64] G. Shimura. Arithmetic of the unitary group. *Annals of Mathematics Second Series, Vol. 79, No. 2, pp. 369-409 (41 pages)*, 1964.

[Sil94] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[Sil09] Joseph H Silverman. *The Arithmetic of Elliptic Curves*. Graduate texts in mathematics. Springer, Dordrecht, 2009.

[Tat66] John Tate. Endomorphisms of abelian varieties over finite fields. *Invent. Math.*, 2 :134–144, 1966.

[Vak] R Vakil. Foundations of algebraic geometry classes 28 and 29. `https://math.stanford.edu/~vakil/0708-216/216class2829.pdf`.

[VDd83] S. G. Vlèduts and V. G. Drinfel' d. The number of points of an algebraic curve. *Funktsional. Anal. i Prilozhen.*, 17(1) :68–69, 1983.

[Web76] H. Weber. Theory of abelian functions of genus 3. (Theorie der Abelschen Functionen vom Geschlecht 3.), 1876.

[Wen01] Annegret Weng. A class of hyperelliptic CM-curves of genus three. *J. Ramanujan Math. Soc.*, 16(4) :339–372, 2001.

[Zay16] Alexey Zaytsev. Optimal curves of low genus over finite fields. *Finite Fields Appl.*, 37 :203–224, 2016.

DOCTORAT BRETAGNE LOIRE / MATHSTIC

UNIVERSITÉ DE RENNES 1

Titre : Produits polarisés de courbes elliptiques à multiplication complexe et applications aux courbes de petit genre

Mot clés : Variétés abéliennes, réseaux hermitiens, courbes optimales, corps de modules, multiplication complexe

Résumé : Dans cette thèse je souhaite présenter certaines équivalences de catégories reliant les variétés abéliennes polarisées isogènes à un produit de courbes elliptiques à multiplication complexe et les réseaux hermitiens sur un ordre quadratique imaginaire. Une de ces équivalences concerne ces variétés sur les corps finis tandis que l'autre se place sur le corps des nombres complexes. Pour chacune d'elles nous présentons des applications à l'existence de certaines courbes algébriques de petit genre ($g = 2, 3$ et 4). Dans le cas des corps finis nous nous servons de la théorie des fonctions thêta algébriques développée par David Mumford pour reconstruire des courbes optimales de genre 2 et 3 en calculant notamment l'obstruction de Serre en genre $g = 3$. En genre 4 nous nous servons du calcul de la forme modulaire d'Igusa algébrique pour caractériser le lieu des jacobiennes, ce qui fournit une réponse partielle au problème de Schottky dans ce cas particulier. Nous nous en servons pour déterminer l'inexistence de certaines courbes optimales. Sur $\mathbb{C}$ nous nous servons d'une équivalence similaire pour classifier les classes d'isomorphisme des courbes algébriques de genre 2 et 3 ayant pour corps de module $\mathbb{Q}$ et dont la jacobienne est isomorphe au produit de courbes elliptiques à multiplication complexe par un ordre maximal.

Title: Polarized products of elliptic curves with complex multiplication and applications to the curves of small genus

Keywords: Abelian varieties, hermitian lattices, optimal curves, field of moduli, complex multiplication

Abstract: In the PhD thesis I study two equivalences of categories connecting polarized abelian varieties isogenous to a product of elliptic curves with complex mutliplication and hermitian lattices over a quadratic imaginary order. One of these equivalences concerns abelian varieties over finite fields whereas the other one is over $\mathbb{C}$. For each of them we propose applications to the existence of some curves of small genus ($g = 2, 3$ or 4). In the finite fields case we use the theory of algebraic theta functions developped by David Mumford to compute equations of optimal curves of genus 2 and 3 by computing the Serre's obstruction for $g = 3$. In genus 4 we use the algebraic version of the Igusa modular form to determine the Jacobian locus which gives a partial answer to the Schottky problem in this case. We then use it to determine the non existence of some optimal curves. Over $\mathbb{C}$ we use a similar equivalence of categories to classify the set servons d'une équivalence similaire pour classifier isomorphism classes of algebraic curves of genus 2 and 3 with field of moduli $\mathbb{Q}$ and whose Jacobian is isomorphic to the product of elliptic curves with complex multiplication by a maximal order.