EPFL

Thèse n° 7524

Computing Cyclic Isogenies between Principally Polarized Abelian Varieties over Finite Fields

Présentée le 17 janvier 2020

à la Faculté des sciences de base
Groupe Jetchev
Programme doctoral en mathématiques

pour l'obtention du grade de Docteur ès Sciences

par

Marius Lorenz VUILLE

Acceptée sur proposition du jury

Prof. K. Hess Bellwald, présidente du jury
Prof. D. P. Jetchev, directeur de thèse
Prof. C. Ritzenthaler, rapporteur
Dr Ph. Lebacque, rapporteur
Prof. M. Viazovska, rapporteuse

École
polytechnique
fédérale
de Lausanne

2020

Abstract

Abelian varieties are fascinating objects, combining the fields of geometry and arithmetic. While the interest in abelian varieties has long time been of purely theoretic nature, they saw their first real-world application in cryptography in the mid 1980's, and have ever since lead to broad research on the computational and the arithmetic side. The most instructive examples of abelian varieties are elliptic curves and Jacobian varieties of hyperelliptic curves, and they come naturally equipped with some additional structure, called a principal polarization. Morphisms between abelian varieties that respect both the geometric and the arithmetic structure are called isogenies. In this thesis we focus on the computation of isogenies with cyclic kernel between principally polarized abelian varieties over finite fields.

Keywords: abelian varieties, isogenies, polarizations, Mumford's theory of theta functions, public key cryptography, discrete logarithm problem

Résumé

Les variétés abéliennes sont des objets fascinants, combinant les domaines de géométrie et d'arithmétique. Tandis que pendant longtemps les mathématiciens s'intéressaient aux aspects purement théoriques des variétés abéliennes, leur apparition dans des domaines pratiques tel que la cryptographie à clé publique dans les années 1980 a mené à de vastes recherches du côté computationnel et arithmétique. Les exemples de variétés abéliennes les plus instructives sont les courbes elliptiques et les variétés Jacobiennes de courbes hyperelliptiques. Les deux sont naturellement dotées d'une structure supplémentaire, appelée une polarisation principale. Les morphismes entre variétés abéliennes qui préservent les structures géométriques et arithmétiques sont appelés isogénies. Nous nous intéressons dans cette thèse au calcul d'isogénies de noyau cyclique entre des variétés abéliennes principalement polarisées sur des corps finis.

Mots-clés : variétés abéliennes, isogénies, polarisations, théorie de Mumford sur les fonctions thêta, cryptographie à clé publique, problème du logarithme discret

The author was supported by the Swiss National Science Foundation Grant 162999.

Remerciements

Tout d'abord j'aimerais remercier Dimitar de m'avoir encadré pendant ma thèse et de m'avoir fait découvrir le monde académique. Tes compétences à voir des liens entre différents domaines de mathématiques m'a impressionné dès le premier jour. Mon projet de recherche n'aurait évidemment pas été possible sans le soutien généreux du Fonds National Suisse de la Recherche Scientifique, que j'aimerais remercier également à cette occasion. Je remercie beaucoup les membres du jury, Maryna, Christophe, Philippe et Kathryn, pour l'effort que vous avez mis à soigneusement lire ma thèse et pour le détour au lac Léman. Partager mon bureau avec Hunter, Réda et Enea a été d'une grande inspiration pour moi, non seulement du côté mathématique, et je garderai en mémoire de ce temps partagé avec vous les nombreuses conversations très enrichissantes. Lors de ma thèse j'ai également eu l'occasion de travailler avec Ben, Alina et Chloe et votre enthousiasme et dynamisme m'a beaucoup enchanté. Le bâtiment des maths ne serait pas le même sans les personnes qu'on y rencontre et les amitiés qu'on y fait. Je pense particulièrement à Martino, Mathieu, Adrien, Patelli, David, Thomas, Oli, Louis et Guillaume. Ca fût un énorme plaisir de partager ce chapitre de ma vie avec vous, autour d'une bière à Sat, un barbecue au lac ou lors d'une de ces nombreuses et longues pauses café. Je suis également très reconnaissant de toujours avoir pu compter sur le soutien de Marcia, Anna, Pierrette et Samantha. Vous êtes les meilleures. Meiner Familie und meinen Freunden möchte ich ganz herzlich danken für die enorme Unterstützung während all diesen Jahren. Ich bin nach Lausanne gezogen, um neue Sprachen und Wissenschaften zu entdecken, doch während all dieser Zeit habt ihr dafür gesorgt, dass sich zu Hause immer noch wie zu Hause anfühlt. Dafür bin ich euch unendlich dankbar. Manon, j'aimerais te remercier du fond du cœur pour ton énorme soutien pendant ces trois dernières années.

Contents

Introduction

Secure communication over an insecure channel requires the participants to possess a common secret key. For centuries, a physical key exchange had to take place prior to secure communication. In a world that is getting more and more connected, this barrier became rapidly one of the biggest challenges in 20th century cryptography. The first key exchange protocol over an insecure channel was proposed by Diffie and Hellman in 1976 [DH76]. Two parties that had no prior knowledge of each other were henceforth able to establish a common secret key. This was considered the birth of public-key cryptography. The security of the key exchange protocol is based on the hardness of a certain mathematical problem, commonly referred to as a one-way function. That is, a problem which is computationally easy to establish, but very costly to reverse. The security of the Diffie-Hellman protocol relies on the hardness of computing discrete logarithms in finite cyclic groups. The Discrete Logarithm Problem (DLP) in the group $G = \langle g \rangle$ is: given $h \in G$, find the exponent x such that $h = g^x$. The hardness of the DLP depends on the chosen group, e.g. it becomes trivial in $\mathbb{Z}/n\mathbb{Z}$, but is already much harder in $(\mathbb{Z}/p\mathbb{Z})^\times$. The fastest generic algorithm to solve the discrete logarithm problem is Pollard's rho algorithm [Pol78], which requires $O(\#G^{1/2})$ operations. Generic in the sense that it exploits the group axioms only, and none of the additional structure of the underlying group. If combined with the Pohling-Hellman algorithm [PH78], the complexity is brought down to $O(p^{1/2})$, where p is the largest prime factor of $\#G$. In the multiplicative group of a finite field, the index calculus algorithm and its variants ([Kra22, HR83, Jou13, BGGM15]) is the fastest known algorithm to solve the DLP. From what we have said so far, it becomes clear the importance of being able to construct cyclic groups of large order for which computing discrete logarithms is difficult (i.e. for which no faster algorithm than Pollard's algorithm is known). Koblitz suggested in [Kob87] the use of the group of rational points of an elliptic curve over a finite field. The efficient arithmetic on elliptic curves and the hardness of the DLP make it a popular choice until nowadays. Indeed, apart from certain classes of curves, there is no known attack, faster than the generic one. If E is an elliptic curve over $\mathbb{F}_q$, then by the Hasse-Weil bound the group of $\mathbb{F}_q$-rational points on E is of order $O(q)$. Assuming there exists a prime-order subgroup of small index, Pollard's algorithm solves the discrete logarithm problem on this cyclic subgroup in roughly $O(q^{1/2})$ operations. Working with elliptic curves allows to have relatively small key sizes compared to other popular one-way functions, such as e.g. factorization of integers. The existence of a bilinear pairing, efficient algorithms for point counting and for isogeny computation gave rise to attacks on certain families of elliptic curves (e.g. [MOV91]), however it also opened the door for further cryptographic protocols based on elliptic curves (e.g. [Jou04, BLS01, BF01, DFJP14]). Two years later, Koblitz suggested to consider the use of Jacobian varieties of hyperelliptic curves as well (see [Kob89]). Schemes based on the hyperelliptic curve discrete logarithm problem benefit from smaller key sizes at same security level, compared to their elliptic curve counterpart. Indeed, if H is a genus g hyperelliptic curve over $\mathbb{F}_q$, then the group of $\mathbb{F}_q$-rational points on $\mathrm{Jac}(H)$ is of order $O(q^g)$. Assuming again we dispose of a prime-order subgroup of small index, the generic algorithm solves the DLP in $O(q^{g/2})$ operations. However, there exists an index-calculus algorithm on hyperelliptic Jacobians ([GTTD05]) that has complexity $O(q^{2-2/g})$, making the gain in key size less significant when g increases. For curves of very large genus, there is an algorithm that computes discrete logarithms in subexponential time ([ADH94]). While the arithmetic on hyperelliptic Jacobians is efficient (Mumford coordinates and Cantor

arithmetic, see e.g. [Gal12] and [CFA+12]), point counting and isogeny computation is much harder than for elliptic curves, and there is still a lot to explore.

Jacobian varieties of hyperelliptic curves are abelian varieties, and they come naturally equipped with some additional structure, called a principal polarization. In this thesis we focus on the computation of isogenies between principally polarized abelian varieties over finite fields. Working with the polynomial equations that define the abelian variety is unfeasible in almost any case (except in dimension 1). We rather want to exploit the theory of theta functions and projective embeddings induced by polarizations. The theta functions can thus be considered as projective coordinates on the variety, and it is with respect to these coordinates that we want to compute isogenies. In the particular case of Jacobian varieties of hyperelliptic curves, there exist efficient conversion formulas between the different coordinate systems (Mumford to theta), see [vW98, Cos11, Rob10]. Isogenies allow us to transport the discrete logarithm problem to a potentially weaker variety, hence if the isogeny is efficiently computable, this can decrease the cost of computing discrete logarithms by an important factor. This becomes most relevant in dimension 3. The moduli space of principally polarized abelian varieties of dimension 3 is 6-dimensional, and so is the moduli space of Jacobian varieties of smooth genus 3 curves. A smooth genus 3 curves is either a hyperelliptic curve or a plane quartic. The former case is rather rare, the moduli space of hyperelliptic curves of genus 3 being of dimension 5. In the non-hyperelliptic case, there exists an index-calculus algorithm ([Die06, DT08]) that has complexity $O(q)$, where $\mathbb{F}_q$ is the base field of the underlying curve. As a comparison, the algorithm from [GTTD05] for hyperelliptic curves has complexity $O(q^{4/3})$. Hence, efficiently computable isogenies in dimension 3 (by which we mean with logarithmic dependency in the size of the base field) can drastically weaken the security of cryptographic schemes based on the discrete logarithm problem on hyperelliptic threefolds.

Isogenies that preserve the principal polarizability (and hence, that are expressible in theta coordinates) are deeply linked to the existence of certain endomorphisms of the abelian variety, as explained in Section 3. And the endomorphism determines the degree of the isogeny. For example, if the abelian variety is of dimension g, and if ℓ is a prime number different from the characteristic of the ground field, then isogenies associated to the multiplication-by-ℓ-endomorphism $[\ell]$ are of degree ℓ^g, with kernel isomorphic to $(\mathbb{Z}/\ell\mathbb{Z})^g$. These isogenies are computable (in theta coordinates for any principally polarizable abelian variety, see [Rob10, CR11, LR12], and on Jacobian varieties of hyperelliptic curves using other techniques, see [CE15], [Mil17]). In the present thesis we focus on the computation of isogenies with cyclic kernels that preserve principal polarizability, whenever they exist (i.e. whenever the associated endomorphism exists). This work results from a collaboration with A. Dudeanu, D. Jetchev and D. Robert.

Structure of the thesis. In Section 1 we study holomorphic line bundles on complex tori and the associated global sections, called theta functions. We explain under what condition a basis of theta functions allows to embed the torus into projective space, and how this embedding behaves under isomorphism. In Section 2 we study abelian varieties over fields of positive characteristic. The absence of the characterisation of an abelian variety as the quotient of a vector space by a lattice makes it impossible to study line bundles in the same manner as we do in the complex case. D. Mumford developed the tools for studying theta functions and projective embeddings in the positive characteristic case, and we present his results in Section 2. In Section 3 we study under what condition the polarizability of an abelian variety descends under separable isogenies.

The core of the thesis are Sections 4 and 5. In Section 4 we compute cyclic isogenies that preserve principal polarizability from kernels. That is, given the theta coordinates of an abelian variety and of a cyclic subgroup, we compute the theta coordinates of the quotient abelian variety. The computed modular point allows then to gain information about the target abelian variety, e.g. if it is the Jacobian variety of a hyperelliptic curve or not, and if so, to compute a plane model of the curve. In Section 5 we evaluate the isogeny on points, i.e. given the theta coordinates of a point on the variety, we compute the theta coordinates of the image of the point. Again, in the case of a hyperelliptic Jacobian, we can use the conversion formulas between Mumford and theta coordinates, making this algorithm practical. In Section 6 we analyse the complexities of the algorithms from the previous sections. In Section 7 we give an example of a cyclic isogeny computed with `Magma`. In Section 8 we present recent theoretical results about isogeny graphs from [BJW17] (graphs whose vertices are isomorphism classes of abelian varieties and whose edges are isogenies of a certain type) and say where and how the explicit computation of cyclic isogenies comes to hand, making these results practical.

Contributions. When I started my PhD thesis, the problem of computing cyclic isogenies in theta coordinates was an ongoing research project by A. Dudeanu, D. Jetchev and D. Robert. My contribution was to generalise the algorithm for the evaluation of the isogeny on points (Section 5) to arbitrary dimension, while before they could handle genus 2 only. Also, these new ideas allowed to remove quite restrictive assumptions (linked to the real multiplication algebra) and had a very beneficial effect on the complexity of the evaluation algorithm.

1 Complex abelian varieties

An abelian variety is a connected and complete algebraic group. Abelian varieties are projective and the group law is commutative. If the variety is defined over the complex numbers, then the group of points on the variety is a complex torus. However, not every complex torus admits the structure of an algebraic variety. In this section we will study holomorphic line bundles on complex tori, associated maps into projective space and give a criterion for a complex torus to be algebraic. In a second step, we will study isomorphisms of complex abelian varieties.

1.1 Line bundles on complex tori

1.1.1 Complex tori

A *complex torus* $X = \mathbb{C}^g/\Lambda$ of dimension g is by definition a quotient of $\mathbb{C}^g$ by a lattice $\Lambda \subset \mathbb{C}^g$, where Λ acts on $\mathbb{C}^g$ by translation. We denote by π the projection map $\pi\colon \mathbb{C}^g \to X$. A complex torus of dimension one is called an *elliptic curve*. A choice of a $\mathbb{Z}$-basis $\lambda_1, \ldots, \lambda_{2g}$ of Λ leads to a complex $g \times 2g$ matrix

$$\Pi = \begin{pmatrix} \lambda_{1,1} & \ldots & \lambda_{1,2g} \\ \vdots & \ddots & \vdots \\ \lambda_{g,1} & \ldots & \lambda_{g,2g} \end{pmatrix},$$

where the jth column of Π is the vector of coefficients of λ_j with respect to the standard basis of $\mathbb{C}^g$. The matrix Π is called a *period matrix* for X. Note that one could define the period matrix with respect to any $\mathbb{C}$-basis of $\mathbb{C}^g$. Two different choices of $\mathbb{Z}$-bases for Λ lead to two different period matrices Π_1 and Π_2, and one can pass from Π_1 to Π_2 by right-multiplication by an element of $\mathbf{GL}_{2g}(\mathbb{Z})$.

A *homomorphism* of complex tori is a group homomorphism that is also a holomorphic map. An over-lattice $\Lambda' \supset \Lambda$ yields a homomorphism

$$\mathbb{C}^g/\Lambda \to \mathbb{C}^g/\Lambda',$$

and if Π' is a period matrix for Λ' then the containment $\Lambda \subset \Lambda'$ means that a period matrix Π for Λ is given by

$$\Pi = \Pi' R,$$

where R is a $2g \times 2g$ matrix with integer coefficients. That is, if $\lambda'_1, \ldots, \lambda'_{2g}$ span the lattice Λ', then the elements of Λ can be expressed as $\mathbb{Z}$-linear combinations of $\lambda'_1, \ldots, \lambda'_{2g}$. This observation has an interesting generalization to any homomorphism of complex tori. Therefore, we first consider the following proposition from [BL04, Prop. 1.2.1].

Proposition 1.1. *Let $X = \mathbb{C}^g/\Lambda$ and $X' = \mathbb{C}^{g'}/\Lambda'$ be complex tori, and let $f\colon X \to X'$ be a homomorphism. Then there exists a unique $\mathbb{C}$-linear map $F\colon \mathbb{C}^g \to \mathbb{C}^{g'}$ satisfying $F(\Lambda) \subset \Lambda'$ and making the following diagram commutative*

$$\begin{array}{ccc} \mathbb{C}^g & \xrightarrow{F} & \mathbb{C}^{g'} \\ {\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle\pi'} \\ X & \xrightarrow[f]{} & X'. \end{array}$$

The above proposition gives rise to an injective group homomorphism

$$\rho_a \colon \mathrm{Hom}(X, X') \hookrightarrow \mathrm{Hom}_{\mathbb{C}}(\mathbb{C}^g, \mathbb{C}^{g'}),\ f \mapsto \rho_a(f) = F,$$

called the *analytic representation* of $\mathrm{Hom}(X, X')$. The inclusion $F(\Lambda) \subset \Lambda'$ implies that F restricts to a $\mathbb{Z}$-linear map on Λ with values in Λ', yielding the *rational representation* of $\mathrm{Hom}(X, X')$,

$$\rho_r \colon \mathrm{Hom}(X, X') \hookrightarrow \mathrm{Hom}_{\mathbb{Z}}(\Lambda, \Lambda'),\ f \mapsto \rho_r(f) = \rho_a(f)|_{\Lambda}\,.$$

In the case $X = X'$, the maps ρ_a and ρ_r are representations of the ring $\mathrm{End}(X)$.

Let $X = \mathbb{C}^g/\Lambda$ and $X' = \mathbb{C}^{g'}/\Lambda'$ be complex tori, and let $f \colon X \to X'$ be a homomorphism. The $\mathbb{C}$-linear map $\rho_a(f)$ can be expressed as a matrix $A \in \mathbf{Mat}_{g' \times g}(\mathbb{C})$ with respect to the standard bases of $\mathbb{C}^g$ and $\mathbb{C}^{g'}$. Let $\Pi \in \mathbf{Mat}_{g \times 2g}(\mathbb{C})$ and $\Pi' \in \mathbf{Mat}_{g' \times 2g'}(\mathbb{C})$ be some period matrices for X and X' respectively. The discrete subgroup $\rho_a(f)(\Lambda)$ of $\mathbb{C}^{g'}$ is spanned by the columns of the matrix $A\Pi$. But $\rho_a(f)(\Lambda)$ is a subgroup of Λ' and hence, we can express each column vector of $A\Pi$ as a $\mathbb{Z}$-linear combination of the columns of Π', yielding a relation

$$A\Pi = \Pi' R.$$

Here, $R \in \mathbf{Mat}_{2g' \times 2g}(\mathbb{Z})$ is the matrix of the rational representation $\rho_r(f)$ with respect to the $\mathbb{Z}$-bases determining Π and Π' respectively. This generalises the relation between the period matrices Π and Π' of the above example of the over-lattice. Moreover, if we are in the case where $g = g'$ and $\rho_a(f)$ is an automorphism of the vector space $\mathbb{C}^g$, then writing the period matrix Π' with respect to the $\mathbb{C}$-basis given by the column vectors of A, we obtain a relation

$$\Pi = \Pi' R.$$

A homomorphism f satisfying the above conditions ($g = g'$ and $\rho_a(f)$ bijective) is called an *isogeny*. A more common, equivalent definition of an isogeny is a surjective homomorphism of complex tori $f \colon X \to X'$ with finite kernel. We may always assume that the matrix A of the analytic representation of an isogeny is the identity. Isogenies always arise as quotients, i.e. if X is a complex torus and $\Gamma \subset X$ is a finite subgroup, then up to isomorphism of the target, the isogeny is given by $X \to X/\Gamma$. The *degree* of an isogeny is the order of its kernel. If $n \neq 0$ is an integer, then $n_X \colon X \to X$, $x \mapsto nx$ is an isogeny of degree n^{2g}, since the kernel equals $\frac{1}{n}\Lambda/\Lambda$. An interesting property of isogenies is that they define a symmetric (hence an equivalence) relation on the set of complex tori. To be more precise, if $f \colon X \to X'$ is an isogeny and if e is the exponent of $\ker f$, then there exists a unique isogeny $g \colon X' \to X$ such that $g \circ f = e_X$ and $f \circ g = e_{X'}$.

1.1.2 Holomorphic line bundles

Let $X = \mathbb{C}^g/\Lambda$ be a complex torus. The aim of this section is to describe the group $(\mathrm{Pic}(X), \otimes)$ of holomorphic line bundles on X. We first make an observation on the trivial line bundle $X \times \mathbb{C} \to X$, and try to mimic this idea to construct new line bundles. The total space of the trivial line bundle is $(\mathbb{C}^g/\Lambda) \times \mathbb{C}$. Hence, the first factor is a quotient by Λ. By considering the trivial action of Λ on $\mathbb{C}$ (i.e. $\lambda \cdot t = t$ for all $\lambda \in \Lambda$ and $t \in \mathbb{C}$), we may view the whole total space as a quotient by Λ. That is, $X \times \mathbb{C} = (\mathbb{C}^g \times \mathbb{C})/\Lambda$, where $\lambda \cdot (v, t) = (v + \lambda, t)$. Now, suppose that Λ acts on $\mathbb{C}^g \times \mathbb{C}$ in a fancier way, e.g. as $\lambda \cdot (v, t) = (v + \lambda, a_{(\lambda,v)}t)$, where $a_{(\lambda,v)} \in \mathbb{C}^\times$ is a non-zero

complex number. This determines a function $a\colon \Lambda \times \mathbb{C}^g \to \mathbb{C}^\times$, and in order for the above to be a group action, which means that the associativity must be guaranteed, the function $a(\lambda, v)$ must satisfy

$$a(\lambda_1 + \lambda_2, v) = a(\lambda_1, v + \lambda_2)a(\lambda_2, v), \tag{1.1}$$

for all $\lambda_1, \lambda_2 \in \Lambda$ and $v \in \mathbb{C}^g$. Relation (1.1) is called the *cocycle relation*. We restrict ourselves from now on to functions $a\colon \Lambda \times \mathbb{C}^g \to \mathbb{C}^\times$ satisfying the cocycle relation (1.1) and that are holomorphic in $\mathbb{C}^g$. These functions are called *factors of automorphy*. Under multiplication, the factors of automorphy form an abelian group, which is denoted by $Z^1(\Lambda, H^0(\mathcal{O}^\times_{\mathbb{C}^g}))$. Here, $H^0(\mathcal{O}^\times_{\mathbb{C}^g})$ is the multiplicative group of nonvanishing holomorphic functions on $\mathbb{C}^g$. Let us fix a factor of automorphy $a \in Z^1(\Lambda, H^0(\mathcal{O}^\times_{\mathbb{C}^g}))$. The action of Λ on $\mathbb{C}^g \times \mathbb{C}$ given by

$$\lambda \cdot (v, t) = (v + \lambda, a(\lambda, v)t) \tag{1.2}$$

is free and properly discontinuous, so that the quotient

$$\mathcal{L}_a = (\mathbb{C}^g \times \mathbb{C})/\Lambda$$

is a complex manifold. The projection on the first factor $p\colon \mathcal{L}_a \to X$ turns $\mathcal{L}_a$ into a holomorphic line bundle on X.

Let $h \in H^0(\mathcal{O}^\times_{\mathbb{C}^g})$ be a nonvanishing holomorphic function on $\mathbb{C}^g$, and let $a\colon \Lambda \times \mathbb{C}^g \to \mathbb{C}^\times$, $a(\lambda, v) = h(v+\lambda)/h(v)$ be the associated factor of automorphy. Then,

$$[(v, t)] \mapsto [(v, h(v)t)]$$

induces an isomorphism between the trivial line bundle and the line bundle $\mathcal{L}_a$ determined by a, where the first equivalence class lives in $\mathbb{C}^g \times \mathbb{C}$ modulo the trivial action of Λ, and the second equivalence class lives in $\mathbb{C}^g \times \mathbb{C}$ modulo Λ acting via the factor a. Factors of automorphy of this form are called *boundaries*, and form the multiplicative subgroup $B^1(\Lambda, H^0(\mathcal{O}^\times_{\mathbb{C}^g}))$ of $Z^1(\Lambda, H^0(\mathcal{O}^\times_{\mathbb{C}^g}))$. The first cohomology group of Λ with values in $H^0(\mathcal{O}^\times_{\mathbb{C}^g})$ is the quotient

$$H^1(\Lambda, H^0(\mathcal{O}^\times_{\mathbb{C}^g})) = Z^1(\Lambda, H^0(\mathcal{O}^\times_{\mathbb{C}^g}))/B^1(\Lambda, H^0(\mathcal{O}^\times_{\mathbb{C}^g})),$$

and its elements define isomorphism classes of holomorphic line bundles on X. As a consequence of [BL04, Prop. B.1] and [BL04, Lem. 2.1.1], *any* holomorphic line bundle on X can be described by a factor of automorphy.

Now that we have an explicit way to describe holomorphic line bundles on X via factors of automorphy, we will turn our attention to the study of these factors. The goal is to distinguish one canonical factor of automorphy in each class of factors, i.e. in each isomorphism class of holomorphic line bundles. Using the exact sequence

$$0 \to \mathbb{Z} \to \mathcal{O}_X \to \mathcal{O}_X^\times \to 0,$$

where the arrow $\mathcal{O}_X \to \mathcal{O}_X^\times$ sends the holomorphic function g to the nonvanishing holomorphic function $e(2\pi i g)$, and the associated long cohomology sequence, one can associate to the holomorphic line bundle $\mathcal{L}$ on X a unique alternating $\mathbb{Z}$-valued form on Λ, called the *first Chern class of* $\mathcal{L}$, and denoted by $c_1(\mathcal{L})$. If $a\colon \Lambda \times \mathbb{C}^g \to \mathbb{C}^\times$ is a factor of automorphy for $\mathcal{L}$, which can always be written as $a = e(2\pi i g)$ with $g\colon \Lambda \times \mathbb{C}^g \to \mathbb{C}$ holomorphic in $\mathbb{C}^g$, then the first Chern class of $\mathcal{L}$ determines the form

$$E_{\mathcal{L}}(\lambda_1, \lambda_2) = g(\lambda_2, v + \lambda_1) + g(\lambda_1, v) - g(\lambda_1, v + \lambda_2) - g(\lambda_2, v),$$

with $\lambda_1, \lambda_2 \in \Lambda$ and $v \in \mathbb{C}^g$. Note that if $a \in B^1(\Lambda, H^0(\mathcal{O}_{\mathbb{C}^g}^\times))$ is a boundary, then the associated form on Λ is trivial. One can $\mathbb{R}$-linearly extend the form $E_\mathcal{L}$ to obtain an alternating $\mathbb{R}$-bilinear form $E_\mathcal{L}\colon \mathbb{C}^g \times \mathbb{C}^g \to \mathbb{R}$. The forms arising as the first Chern class of a holomorphic line bundle are characterized, among the alternating $\mathbb{R}$-bilinear forms on $\mathbb{C}^g$, as the forms $E\colon \mathbb{C}^g \times \mathbb{C}^g \to \mathbb{R}$ satisfying

$$E(\Lambda, \Lambda) \subset \mathbb{Z} \text{ and } E(iv_1, iv_2) = E(v_1, v_2) \text{ for all } v_1, v_2 \in \mathbb{C}^g. \tag{1.3}$$

The mappings

$$E \mapsto H(v_1, v_2) := E(iv_1, v_2) + iE(v_1, v_2) \text{ and } H \mapsto E := \operatorname{Im} H, \tag{1.4}$$

with $v_1, v_2 \in \mathbb{C}^g$, set up a 1-1 correspondence between the alternating $\mathbb{R}$-bilinear forms E satisfying (1.3) and the hermitian forms H satisfying $\operatorname{Im} H(\Lambda, \Lambda) \subset \mathbb{Z}$. Recall that a form $H\colon \mathbb{C}^g \times \mathbb{C}^g \to \mathbb{C}$ is hermitian if it is linear in the first variable and satisfies

$$H(v_1, v_2) = \overline{H(v_2, v_1)} \text{ for all } v_1, v_2 \in \mathbb{C}^g.$$

The additive group of hermitian forms H satisfying $\operatorname{Im} H(\Lambda, \Lambda) \subset \mathbb{Z}$ is called the *Néron-Severi group* $\mathrm{NS}(X)$, and we will deliberately switch between the point of view of hermitian forms and alternating $\mathbb{R}$-bilinear forms. Note that sending a holomorphic line bundle to its first Chern class respects group laws, i.e. $\mathrm{Pic}(X) \xrightarrow{c_1} \mathrm{NS}(X)$ is a morphism of groups.

Now that we have seen how to obtain a hermitian form from a factor of automorphy, one might ask what additional information we have to add to a hermitian form (satisfying $\operatorname{Im} H(\Lambda, \Lambda) \subset \mathbb{Z}$) in order to define a factor of automorphy. The answer is a semicharacter. Let $\mathbb{C}_1 = \{z \in \mathbb{C} : |z| = 1\}$ be the circle group, and let $H \in \mathrm{NS}(X)$. A *semicharacter* for H is a map $\chi\colon \Lambda \to \mathbb{C}_1$ that behaves almost like a character, but takes into account the parity of $\operatorname{Im} H$, i.e. that satisfies

$$\chi(\lambda_1 + \lambda_2) = \chi(\lambda_1)\chi(\lambda_2)e(\pi i \operatorname{Im} H(\lambda_1, \lambda_2)) \text{ for all } \lambda_1, \lambda_2 \in \Lambda.$$

The semicharacters for $0 \in \mathrm{NS}(X)$ are precisely the characters on Λ with values in $\mathbb{C}_1$, i.e. $\mathrm{Hom}(\Lambda, \mathbb{C}_1)$. Clearly, if χ_1 and χ_2 are semicharacters for H_1 and H_2 respectively, then $\chi_1\chi_2$ is a semicharacter for $H_1 + H_2$. This turns the set $\mathcal{P}(\Lambda)$ of pairs (H, χ), with $H \in \mathrm{NS}(X)$ and χ a semicharacter for H, into an abelian group. The full description of holomorphic line bundles on X is given by the following theorem [BL04, Thm. 2.2.3].

Theorem 1.2 (Appell-Humbert)**.** *There is an isomorphism*

$$\mathcal{P}(\Lambda) \xrightarrow{\sim} \mathrm{Pic}(X).$$

Let us make the isomorphism from Theorem 1.2 explicit. For this we define a factor of automorphy associated to $(H, \chi) \in \mathcal{P}(\Lambda)$ as follows:

$$a_{(H,\chi)}\colon \Lambda \times \mathbb{C}^g \to \mathbb{C}^\times,\ (\lambda, v) \mapsto \chi(\lambda)e(\pi H(v, \lambda) + \frac{\pi}{2}H(\lambda, \lambda)). \tag{1.5}$$

The map $a_{(H,\chi)}$ satisfies the cocycle relation: for $\lambda_1, \lambda_2 \in \Lambda$ and $v \in \mathbb{C}^g$ we have

$$\begin{aligned}
a_{(H,\chi)}(\lambda_1 + \lambda_2, v) &= \chi(\lambda_1 + \lambda_2)e(\pi H(v, \lambda_1 + \lambda_2) + \frac{\pi}{2}H(\lambda_1 + \lambda_2, \lambda_1 + \lambda_2)) \\
&= \chi(\lambda_1)\chi(\lambda_2)e(\pi i \operatorname{Im} H(\lambda_1, \lambda_2))e(\pi H(v, \lambda_1 + \lambda_2) + \frac{\pi}{2}H(\lambda_1 + \lambda_2, \lambda_1 + \lambda_2)) \\
&= \chi(\lambda_1)e(\pi H(v + \lambda_2, \lambda_1) + \frac{\pi}{2}H(\lambda_1, \lambda_1))\chi(\lambda_2)e(\pi H(v, \lambda_2) + \frac{\pi}{2}H(\lambda_2, \lambda_2)) \\
&= a_{(H,\chi)}(\lambda_1, v + \lambda_2) \cdot a_{(H,\chi)}(\lambda_2, v).
\end{aligned}$$

The action of Λ on $\mathbb{C}^g \times \mathbb{C}$ via $a_{(H,\chi)}$, as described in (1.2), determines a holomorphic line bundle on X, that we denote by $\mathcal{L}(H,\chi)$. Conversely, if $\mathcal{L} \in \mathrm{Pic}(X)$ is a holomorphic line bundle, then $\mathcal{L}$ determines a unique pair (H,χ), and we call $a_{(H,\chi)}$ the *canonical factor of automorphy* for $\mathcal{L}$. Let us denote by $\mathrm{Pic}^0(X)$ the kernel of the homomorphism $\mathrm{Pic}(X) \xrightarrow{c_1} \mathrm{NS}(X)$. Then, the isomorphism from Theorem 1.2 restricts to an isomorphism

$$\mathrm{Hom}(\Lambda, \mathbb{C}_1) \xrightarrow{\sim} \mathrm{Pic}^0(X).$$

We say that two line bundles $\mathcal{L}_1$ and $\mathcal{L}_2$ on X are *algebraically equivalent* if $\mathcal{L}_1 \otimes \mathcal{L}_2^{-1} \in \mathrm{Pic}^0(X)$, i.e. if they determine the same hermitian form on $\mathbb{C}^g$. An algebraic equivalence class of line bundles can thus naturally be identified with an element of $\mathrm{NS}(X)$. Any $v \in \mathbb{C}^g$ determines a holomorphic translation map

$$t_{\bar{v}} \colon X \to X,\ x \mapsto x + \bar{v},$$

where $\bar{v} = v \mod \Lambda \in X$, and we would like to know how the pullback of a holomorphic line bundle on X by $t_{\bar{v}}$ behaves. Therefore, it is most beneficial to consider line bundles of the form $\mathcal{L}(H,\chi)$. The following lemma [BL04, Lem. 2.3.2] implies that pulling back by translations does not change the algebraic equivalence class.

Lemma 1.3. *For all $\mathcal{L} = \mathcal{L}(H,\chi) \in \mathrm{Pic}(X)$ and all $v \in \mathbb{C}^g$ we have*

$$t_{\bar{v}}^* \mathcal{L}(H,\chi) = \mathcal{L}\left(H, \chi e(2\pi i \operatorname{Im} H(v,\cdot))\right).$$

Note that a different choice of representative of $\bar{v}$ yields the same semicharacter. Next, we would like to know how the pullback of a holomorphic line bundle by a homomorphism of complex tori behaves. For the proof of the following lemma, see [BL04, Lem. 2.3.4].

Lemma 1.4. *Let $X = \mathbb{C}^g/\Lambda$ and $X' = \mathbb{C}^{g'}/\Lambda'$ be complex tori and let $f \colon X \to X'$ be a homomorphism. Then, for any $\mathcal{L}(H',\chi') \in \mathrm{Pic}(X')$ we have*

$$f^* \mathcal{L}(H',\chi') = \mathcal{L}(\rho_a(f)^* H', \rho_r(f)^* \chi').$$

1.2 Polarizations, theta functions and projective embeddings

1.2.1 The dual complex torus

Let $X = \mathbb{C}^g/\Lambda$ be a complex torus. The aim of this section is to define duality; a contravariant functor from the category of complex tori to itself. Recall that $\mathrm{Pic}^0(X)$ is isomorphic to $\mathrm{Hom}(\Lambda, \mathbb{C}_1)$ - a real torus of dimension $2g$. The question is if and how one can realize $\mathrm{Pic}^0(X)$ as a complex torus of dimension g. Therefore, consider the space $\overline{\Omega} = \mathrm{Hom}_{\overline{\mathbb{C}}}(\mathbb{C}^g, \mathbb{C})$ of $\mathbb{C}$-antilinear forms $l \colon \mathbb{C}^g \to \mathbb{C}$. This is clearly a g-dimensional complex vector space. The set

$$\widehat{\Lambda} = \{l \in \overline{\Omega} : \operatorname{Im} l(\Lambda) \subset \mathbb{Z}\}$$

is a lattice in $\overline{\Omega}$, and is equal to the kernel of the canonical surjective group morphism

$$\overline{\Omega} \to \mathrm{Hom}(\Lambda, \mathbb{C}_1),\ l \mapsto e(2\pi i \operatorname{Im} l(\cdot)). \tag{1.6}$$

Hence,

$$\overline{\Omega}/\widehat{\Lambda} \xrightarrow{\sim} \mathrm{Pic}^0(X).$$

We call $\mathrm{Pic}^0(X)$, respectively the quotient $\overline{\Omega}/\widehat{\Lambda}$, the *dual complex torus*, and it is denoted by $\widehat{X}$. Given two complex tori $X = \mathbb{C}^g/\Lambda$ and $X' = \mathbb{C}^{g'}/\Lambda'$, and a homomorphism $f\colon X \to X'$, the pullback by f of holomorphic line bundles of $\mathrm{Pic}^0(X')$ gives a homomorphism between the dual tori $\widehat{f}\colon \widehat{X}' \to \widehat{X}$. The analytic representation of $\widehat{f}$ is given by

$$\rho_a(\widehat{f})\colon \overline{\Omega}' \to \overline{\Omega},\ l' \mapsto \rho_a(f)^*(l') = l' \circ \rho_a(f).$$

Clearly, by the properties of the pullback, if $g\colon X' \to X''$ is another morphism, then $\widehat{g \circ f} = \widehat{f} \circ \widehat{g}$. Also, $\widehat{\mathrm{id}_X} = \mathrm{id}_{\widehat{X}}$ and hence, duality is a contravariant functor. The duality also preserves the property of being an isogeny, i.e. if $f\colon X \to X'$ is an isogeny, then $\widehat{f}\colon \widehat{X}' \to \widehat{X}$ is also an isogeny, and moreover $\deg f = \deg \widehat{f}$.

To any line bundle $\mathcal{L} = \mathcal{L}(H, \chi)$ on X we can associate a map $\phi_{\mathcal{L}}\colon X \to \widehat{X}$ from X to its dual $\widehat{X} = \mathrm{Pic}^0(X)$ as follows: for any $x \in X$, according to Lemma 1.3, we have

$$t_x^*\mathcal{L} \otimes \mathcal{L}^{-1} = \mathcal{L}\left(0, e(2\pi i \operatorname{Im} H(v_x, \cdot))\right), \tag{1.7}$$

where $v_x \in \mathbb{C}^g$ is any lift of x. Hence, $x \mapsto t_x^*\mathcal{L} \otimes \mathcal{L}^{-1}$ defines a map $X \xrightarrow{\phi_{\mathcal{L}}} \widehat{X}$. Moreover, observing that $\phi_{\mathcal{L}}(x+y) = \mathcal{L}\left(0, e(2\pi i \operatorname{Im} H(v_x + v_y, \cdot))\right)$, we have that $\phi_{\mathcal{L}}\colon X \to \widehat{X}$ is a homomorphism of complex tori. The homomorphism $\phi_{\mathcal{L}}$ will turn out to be of crucial importance for the construction of isogenies between abelian varieties over finite fields, the main topic of this thesis. Therefore, let us recall some properties of $\phi_{\mathcal{L}}$. With (1.6) and (1.7) in mind, it is easy to see that $\phi_H\colon \mathbb{C}^g \to \overline{\Omega},\ v \mapsto H(v, \cdot)$ is the analytic representation of $\phi_{\mathcal{L}}$. As a direct consequence, $\phi_{\mathcal{L}}$ is an isogeny if and only if H is nondegenerate. Some other properties that are immediate from (1.7) are:

- $\phi_{\mathcal{L}}$ only depends on the algebraic equivalence class of $\mathcal{L}$; the semicharacter χ has disappeared in the definition of $\phi_{\mathcal{L}}(x)$;
- if $\mathcal{L}_1, \mathcal{L}_2 \in \mathrm{Pic}(X)$, then $\phi_{\mathcal{L}_1 \otimes \mathcal{L}_2} = \phi_{\mathcal{L}_1} + \phi_{\mathcal{L}_2}$.

If, as above, $f\colon X \to X'$ is a homomorphism, where $X = \mathbb{C}^g/\Lambda$ and $X' = \mathbb{C}^{g'}/\Lambda'$, and $\mathcal{L}' = \mathcal{L}(H', \chi') \in \mathrm{Pic}(X')$ is a line bundle on X', then the composition

$$\mathbb{C}^g \xrightarrow{\rho_a(f)} \mathbb{C}^{g'} \xrightarrow{\phi_{H'}} \overline{\Omega}' \xrightarrow{\rho_a(f)^*} \overline{\Omega}$$

is equal to the linear map

$$\mathbb{C}^g \xrightarrow{\phi_{\rho_a(f)^* H'}} \overline{\Omega},\ v \mapsto (\rho_a(f)^* H')(v, \cdot).$$

Hence, the following diagram is commutative

$$\begin{array}{ccc} X & \xrightarrow{f} & X' \\ {\scriptstyle \phi_{f^*\mathcal{L}'}}\downarrow & & \downarrow{\scriptstyle \phi_{\mathcal{L}'}} \\ \widehat{X} & \xleftarrow[\widehat{f}]{} & \widehat{X}'. \end{array} \tag{1.8}$$

For $\mathcal{L} = \mathcal{L}(H, \chi) \in \mathrm{Pic}(X)$ we denote by $K(\mathcal{L}) \subset X$ the kernel of $\phi_{\mathcal{L}}$, that is

$$K(\mathcal{L}) = \{x \in X : t_x^*\mathcal{L} \cong \mathcal{L}\}.$$

Those are exactly the $x \in X$ for which $e(2\pi i \operatorname{Im} H(v_x, \cdot)) \equiv 1$ on Λ (no matter the lift $v_x \in \mathbb{C}^g$). In other words, if we denote by

$$\Lambda(\mathcal{L}) := \phi_H^{-1}(\widehat{\Lambda}) = \{v \in \mathbb{C}^g : \operatorname{Im} H(v, \Lambda) \subset \mathbb{Z}\},$$

then we have

$$K(\mathcal{L}) = \Lambda(\mathcal{L})/\Lambda.$$

An important question that will naturally arise in a later part of this thesis (see Section 2.1.1) is, under what condition, given an isogeny of complex tori $f\colon X \to X'$ and a line bundle $\mathcal{L} = \mathcal{L}(H, \chi) \in \operatorname{Pic}(X)$, there exists a line bundle $\mathcal{L}' = \mathcal{L}(H', \chi') \in \operatorname{Pic}(X')$ such that $\mathcal{L} = f^*\mathcal{L}'$. Looking at (1.8), a necessary condition is that $\ker f \subset \ker \phi_{\mathcal{L}} = K(\mathcal{L})$. Moreover, if $x, y \in \ker f$, then $\rho_a(f)(v_x), \rho_a(f)(v_y) \in \Lambda'$ for any lifts v_x and v_y of x and y respectively and thus,

$$\operatorname{Im} H(v_x, v_y) = \operatorname{Im}(\rho_a(f)^* H')(v_x, v_y) = \operatorname{Im} H'(\rho_a(f)(v_x), \rho_a(f)(v_y)) \in \mathbb{Z}.$$

In other words, $\operatorname{Im} H$ takes integer values on $\pi^{-1}(\ker f) = \rho_a(f)^{-1}(\Lambda')$.

Proposition 1.5. *Let the isogeny $f\colon X \to X'$ and $\mathcal{L} = \mathcal{L}(H, \chi) \in \operatorname{Pic}(X)$ be as above. Then the following statements are equivalent:*

i) there exists a line bundle $\mathcal{L}' \in \operatorname{Pic}(X')$ such that $\mathcal{L} = f^*\mathcal{L}'$;

ii) $\operatorname{Im} H(\rho_a(f)^{-1}(\Lambda'), \rho_a(f)^{-1}(\Lambda')) \subset \mathbb{Z}$.

Proof. We have already seen that *i)* implies *ii)*.
Suppose that $\operatorname{Im} H(\rho_a(f)^{-1}(\Lambda'), \rho_a(f)^{-1}(\Lambda')) \subset \mathbb{Z}$. This means that the form $(\rho_a(f)^{-1})^* H$ takes integer values on Λ', hence is an element of $\mathrm{NS}(X')$. Let $\mathcal{M} \in \operatorname{Pic}(X')$ be such that $c_1(\mathcal{M}) = (\rho_a(f)^{-1})^* H$. Then, $c_1(f^*\mathcal{M}) = H$, or equivalently, $\mathcal{L} \otimes f^*\mathcal{M}^{-1} \in \operatorname{Pic}^0(X)$. Since $f\colon X \to X'$ is an isogeny, the dual map $f^*\colon \operatorname{Pic}^0(X') \to \operatorname{Pic}^0(X)$ is an isogeny as well, hence surjective. Let $\mathcal{N} \in \operatorname{Pic}^0(X')$ be such that $\mathcal{L} \otimes f^*\mathcal{M}^{-1} = f^*\mathcal{N}$. Then $\mathcal{M} \otimes \mathcal{N} \in \operatorname{Pic}(X')$ satisfies *i)*. □

Remark 1.6. One should note that in this case, the line bundle $\mathcal{L}'$ is unique up to algebraic equivalence.

When we study abelian varieties over a finite field k, we do not have nice objects such as hermitian forms, lattices, etc. at our disposal. However, we would like to give a criterion similar to *ii)* of Proposition 1.5, in order to have an equivalent condition to the descent of a line bundle under isogeny. As we will see in Section 2.1.1 , the line bundle $\mathcal{L}$ allows us to define an alternating form on $K(\mathcal{L})$ with values in $k^\times$, say $e_{\mathcal{L}}$, and condition *ii)* from the above proposition can be understood as: $\ker f$ is an isotropic subgroup for the pairing $e_{\mathcal{L}}$. As will turn out later, this is the right point of view.

1.2.2 Theta functions and polarizations

The aim of this section is to describe the global sections of a holomorphic line bundle on a complex torus, called *theta functions*. These functions turn out to be paramount for the computations in this thesis. The reason is that, for a well suited line bundle, they allow us to embed complex tori (and later abelian varieties over finite fields) into projective space. Hence, theta functions provide a system of coordinates, and it is

precisely in these coordinates that we will express and manipulate abelian varieties, and most importantly, compute isogenies.

Let $X = \mathbb{C}^g/\Lambda$ be a complex torus and let $\mathcal{L}$ be a holomorphic line bundle on X. Let $\pi\colon \mathbb{C}^g \to X$ be the natural projection. Let $a\colon \Lambda \times \mathbb{C}^g \to \mathbb{C}^\times$ be a factor of automorphy for $\mathcal{L}$, i.e. $\mathcal{L}$ is isomorphic to the line bundle $(\mathbb{C}^g \times \mathbb{C})/\Lambda$, where Λ acts on $\mathbb{C}^g \times \mathbb{C}$ by $\lambda \cdot (v,t) = (v+\lambda, a(\lambda,v)t)$. According to [BL04, Lem. 2.1.1], any holomorphic line bundle on $\mathbb{C}^g$ is trivial. Hence, we might replace $\pi^*\mathcal{L}$ by $\mathbb{C}^g \times \mathbb{C}$ in the following commutative diagram

$$\begin{array}{ccc} \mathbb{C}^g \times \mathbb{C} & \longrightarrow & \mathcal{L} = (\mathbb{C}^g \times \mathbb{C})/\Lambda \\ \downarrow & & \downarrow \\ \mathbb{C}^g & \longrightarrow & X. \end{array}$$

(Note that the trivialization $\pi^*\mathcal{L} \xrightarrow{\sim} \mathbb{C}^g \times \mathbb{C}$ depends on the choice of the factor of automorphy for $\mathcal{L}$.) A global section $s \in \Gamma(X, \mathcal{L})$ (provided it exists) pulls back to a section $\pi^*s\colon \mathbb{C}^g \to \mathbb{C}^g \times \mathbb{C}$, that we might just see as a map $\pi^*s\colon \mathbb{C}^g \to \mathbb{C}$. In order for π^*s to make the above diagram commutative, it must satisfy

$$\pi^*s(v+\lambda) = a(\lambda, v)\pi^*s(v), \text{ for all } v \in \mathbb{C}^g \text{ and } \lambda \in \Lambda.$$

Thus it makes sense to identify $\Gamma(X, \mathcal{L})$ with the set of holomorphic functions $\theta\colon \mathbb{C}^g \to \mathbb{C}$ that satisfy

$$\theta(v+\lambda) = a(\lambda, v)\theta(v),$$

for all $v \in \mathbb{C}^g$ and $\lambda \in \Lambda$. We call such functions *theta functions* for the factor a. On the other side, this identification heavily depends on the choice of the factor of automorphy for $\mathcal{L}$. Another choice of factor is necessarily of the form $a' = a \cdot b$, where $b \in B^1(\Lambda, H^0(\mathcal{O}^\times_{\mathbb{C}^g}))$ is a boundary. If $b(\lambda, v) = h(v+\lambda)/h(v)$ with $h \in H^0(\mathcal{O}^\times_{\mathbb{C}^g})$, then

$$\theta \mapsto \theta' = \theta \cdot h$$

sets up a bijection between the theta functions for the factor a and the theta functions for the factor a'.

A theta function cannot be considered as a function on the torus X, since it is not invariant under translates by the lattice Λ (only constant functions are Λ-invariant). However, if $\theta_0, \ldots, \theta_{N-1}$ are theta functions for the factor a, then

$$x \mapsto (\theta_0(v_x) : \cdots : \theta_{N-1}(v_x)) \in \mathbb{P}^{N-1}_{\mathbb{C}},$$

where $v_x \in \mathbb{C}^g$ is any lift of x, determines a meromorphic map $X \to \mathbb{P}^{N-1}_{\mathbb{C}}$. This map is defined at all points x where not all θ_i vanish simultaneously (observe that the vanishing property of θ_i is identical on the whole coset $v_x + \Lambda$). It is also clear that this map does not depend on the choice of the factor of automorphy. In the next sections we will see under what conditions the torus X can be embedded into projective space by means of theta functions, and how to choose such an embedding in a canonical way. But first we need to study theta functions more thoroughly.

Symplectic Spaces. Recall that a real symplectic vector space consists of a pair (V, e), where V is a $\mathbb{R}$-vector space and $e\colon V \times V \to \mathbb{R}$ is a symplectic pairing, i.e. e is bilinear, alternating and nondegenerate. If V is finite-dimensional, it follows immediately

that $\dim V$ is even, say $2n$. One can always find a basis $v_1, \ldots, v_n, w_1, \ldots, w_n$ of V with respect to which the matrix of e is given by

$$J = \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix}.$$

Such a basis is called a symplectic basis. A linear map $f\colon (V, e) \to (V, e)$ that preserves the symplectic pairing, in the sense that $f^*e = e$, is called a symplectic map. It is easy to see that f is necessarily injective, hence an automorphism. The group of symplectic automorphisms of (V, e) is denoted by $\mathbf{Sp}(V, e)$. If F is the matrix of f with respect to the above symplectic basis, then $f^*e = e$ means that

$$^t(Fv)J(Fw) = J, \text{ for all } v, w \in V,$$

and by the nondegeneracy of e we have that

$$^tFJF = J.$$

Define the symplectic group

$$\mathbf{Sp}_{2n}(\mathbb{R}) = \{M \in \mathbf{Mat}_{2n}(\mathbb{R}) : {}^tMJM = J\}.$$

The group $\mathbf{Sp}_{2n}(\mathbb{R})$ is closed under transposition and we have the following characterization of its elements: if $M \in \mathbf{Mat}_{2n}(\mathbb{R})$ is given as $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$, with $A, B, C, D \in \mathbf{Mat}_n(\mathbb{R})$, then

$$M \in \mathbf{Sp}_{2n}(\mathbb{R}) \Leftrightarrow \begin{cases} {}^tAC, {}^tBD \text{ symmetric and } {}^tAD - {}^tCB = I_n \\ A\,{}^tB, C\,{}^tD \text{ symmetric and } A\,{}^tD - B\,{}^tC = I_n. \end{cases}$$

The inverse of $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathbf{Sp}_{2g}(\mathbb{R})$ is given by

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

Decompositions. Let $X = \mathbb{C}^g/\Lambda$ be a complex torus and let $\mathcal{L} \in \mathrm{Pic}(X)$ be a holomorphic line bundle on X, with first Chern class $H = c_1(\mathcal{L})$ nondegenerate. Then, $\operatorname{Im} H$ is nondegenerate too. We call such a line bundle a *nondegenerate line bundle*. The free $\mathbb{Z}$-module Λ equipped with $\operatorname{Im} H$ forms a symplectic space. One can always find a basis $\lambda_1, \ldots, \lambda_g, \mu_1, \ldots, \mu_g$, called a *symplectic basis* of Λ for $\operatorname{Im} H$, so that the matrix of $\operatorname{Im} H$ with respect to this basis is given by

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

where $\Delta = \operatorname{diag}(\delta_1, \ldots, \delta_g)$ is a diagonal matrix. The vector $\delta = (\delta_1, \ldots, \delta_g)$ is called the *type* of $\mathcal{L}$ or of $\operatorname{Im} H$, and does not depend on the choice of the symplectic basis of Λ. Moreover, we have $\delta_1 | \cdots | \delta_g$. Since $\operatorname{Im} H$ is nondegenerate, $\delta_i \neq 0$ for $i = 1, \ldots, g$, and by an eventual change of sign of the corresponding base vector, we may assume that $\delta_i > 0$ for all $i = 1, \ldots, g$. The *degree* of $\mathcal{L}$ is defined to be $\deg \mathcal{L} = \det \Delta = \prod_{i=1}^g \delta_i$. The set of symplectic bases of Λ for $\operatorname{Im} H$ forms a torsor under the group

$$\mathbf{Sp}_{2g}^{\Delta}(\mathbb{Z}) := \left\{ M \in \mathbf{Mat}_{2g}(\mathbb{Z}) : {}^tM \begin{pmatrix} 0 & \Delta \\ -\Delta & 0 \end{pmatrix} M = \begin{pmatrix} 0 & \Delta \\ -\Delta & 0 \end{pmatrix} \right\}.$$

The basis $\lambda_1, \ldots, \lambda_g, \mu_1, \ldots, \mu_g$ induces a decomposition of the $\mathbb{Z}$-module Λ as

$$\Lambda = \Lambda_1 \oplus \Lambda_2,$$

where Λ_1 and Λ_2 are the isotropic (for $\operatorname{Im} H$) free submodules $\Lambda_1 = \langle \lambda_1, \ldots, \lambda_g \rangle$ and $\Lambda_2 = \langle \mu_1, \ldots, \mu_g \rangle$ respectively.

The real subvector spaces $V_1 = \Lambda_1 \otimes_{\mathbb{Z}} \mathbb{R}$ and $V_2 = \Lambda_2 \otimes_{\mathbb{Z}} \mathbb{R}$ of $\mathbb{C}^g$ are isotropic for the form $\operatorname{Im} H$, and form a direct sum decomposition

$$\mathbb{C}^g = V_1 \oplus V_2$$

of $\mathbb{C}^g$, seen as $\mathbb{R}$-vector space. Also, V_1 and V_2 are of maximal dimension among the isotropic subspaces of $\mathbb{C}^g$. Furthermore, the decomposition $\mathbb{C}^g = V_1 \oplus V_2$ induces a decomposition

$$\Lambda(\mathcal{L}) = \Lambda(\mathcal{L})_1 \oplus \Lambda(\mathcal{L})_2,$$

where $\Lambda(\mathcal{L})_i = \Lambda(\mathcal{L}) \cap V_i$ for $i = 1, 2$. It is easy to see that $\frac{1}{\delta_1}\lambda_1, \ldots, \frac{1}{\delta_g}\lambda_g$ forms a $\mathbb{Z}$-basis of $\Lambda(\mathcal{L})_1$ and that $\frac{1}{\delta_1}\mu_1, \ldots, \frac{1}{\delta_g}\mu_g$ forms a $\mathbb{Z}$-basis of $\Lambda(\mathcal{L})_2$. From the decomposition of $\Lambda(\mathcal{L})$ we obtain a decomposition

$$K(\mathcal{L}) = K(\mathcal{L})_1 \oplus K(\mathcal{L})_2,$$

where $K(\mathcal{L})_i = \Lambda(\mathcal{L})_i / \Lambda_i$, for $i = 1, 2$. If we let $\mathbb{Z}(\delta) := \bigoplus_{i=1}^g \mathbb{Z}/\delta_i\mathbb{Z}$, then it is clear that

$$K(\mathcal{L})_1 \cong K(\mathcal{L})_2 \cong \mathbb{Z}(\delta).$$

Observe that

$$\deg \phi_{\mathcal{L}} = \#K(\mathcal{L}) = (\deg \mathcal{L})^2.$$

Polarizations. Let $X = \mathbb{C}^g/\Lambda$ be a complex torus. Let $\mathcal{L} \in \operatorname{Pic}(X)$ be a holomorphic line bundle on X and suppose that $H = c_1(\mathcal{L})$ is positive definite. We call the algebraic equivalence class of $\mathcal{L}$, or equivalently the positive definite hermitian form $H \in \operatorname{NS}(X)$, a *polarization* on X. By abuse of notation we sometimes call $\mathcal{L}$ itself a polarization. The *type* of a polarization is the type of any representative. A polarization of type $(1, \ldots, 1)$ is called a *principal polarization*. As will turn out later (see Theorem 1.11), a polarization of a certain type is the right information we need to get an analytic embedding of the torus X into projective space. By Chow's theorem [Har77, Appendix B, Thm. 2.2], any closed analytic subvariety of $\mathbb{P}^N_{\mathbb{C}}$ is an algebraic variety, hence X is algebraic. This is the reason why we call a complex torus X that admits a polarization $H = c_1(\mathcal{L})$ an *abelian variety*. The pair (X, H), or equivalently $(X, \mathcal{L})$, is called a *polarized abelian variety*. A *homomorphism of polarized abelian varieties* $f\colon (X, H) \to (X', H')$ is a homomorphism of complex tori such that $\rho_a(f)^* H' = H$. If $\mathcal{L}$ is a polarization, then $\phi_{\mathcal{L}}\colon X \to \widehat{X}$ is an isogeny, called the *polarization isogeny*. Polarizations are of fundamental interest for this thesis. As a first observation, we will see that in the polarized case, up to isomorphism, one can always choose a decomposition of the lattice in a nice way.

Suppose that H is a polarization on $X = \mathbb{C}^g/\Lambda$ of type $\delta = (\delta_1, \ldots, \delta_g)$, and that $\lambda_1, \ldots, \lambda_g, \mu_1, \ldots, \mu_g$ is a symplectic basis of Λ for $\operatorname{Im} H$, inducing the decompositions $\Lambda = \Lambda_1 \oplus \Lambda_2$ and $\mathbb{C}^g = V_1 \oplus V_2$ as in the previous paragraph. Clearly, V_2 is of real dimension g. But we have more.

Proposition 1.7. *Every $v \in \mathbb{C}^g$ is of the form $v = v_2 + iv_2'$, for $v_2, v_2' \in V_2$.*

Proof. Clearly, $V_2 \cap iV_2$ is a complex subvector space of $\mathbb{C}^g$ on which $\operatorname{Im} H$ vanishes (since V_2 isotropic for $\operatorname{Im} H$). By the correspondence (1.4), we also have that H vanishes on $V_2 \cap iV_2$. But H is positive definite, and thus $V_2 \cap iV_2 = \{0\}$. Hence, the real subvector space $V_2 + iV_2 \subset \mathbb{C}^g$ is of real dimension $2g$. □

By the above proposition, any $\mathbb{R}$-basis of V_2 spans $\mathbb{C}^g$ as a $\mathbb{C}$-vector space and hence, is a $\mathbb{C}$-basis by dimension reason. In particular, $\frac{1}{\delta_1}\mu_1, \ldots, \frac{1}{\delta_g}\mu_g$ is a $\mathbb{C}$-basis of $\mathbb{C}^g$. If we denote by $e_1, \ldots, e_g$ the standard basis of $\mathbb{C}^g$, then the isomorphism $F\colon \frac{1}{\delta_i}\mu_i \mapsto e_i$ induces an isomorphism of polarized abelian varieties

$$(X, H) \xrightarrow{\sim} (X', H'), \tag{1.9}$$

where $X' = \mathbb{C}^g/\Lambda'$ and $H' = (F^{-1})^* H$. The lattice $\Lambda' = F(\Lambda)$ is given by $\Omega\mathbb{Z}^g \oplus \Delta\mathbb{Z}^g$, where Ω is a complex $g \times g$ matrix and $\Delta = \operatorname{diag}(\delta_1, \ldots, \delta_g)$. Moreover, this is a decomposition into isotropic submodules for $\operatorname{Im} H'$. It is well known that the matrix Ω satisfies

$$^t\Omega = \Omega \text{ and } \operatorname{Im}\Omega \text{ positive definite.} \tag{1.10}$$

The set of such matrices is called the *Siegel upper half-space*

$$\mathcal{H}_g := \{\Omega \in \mathbf{Mat}_g(\mathbb{C}) : {}^t\Omega = \Omega \text{ and } \operatorname{Im}\Omega \text{ positive definite}\}.$$

For obvious reasons, we often call $\Omega \in \mathcal{H}_g$ a *period matrix*. The form H' is given by

$$H'(v, w) = {}^t v(\operatorname{Im}\Omega)^{-1}\bar{w}. \tag{1.11}$$

Example 1.8. Let $X = \mathbb{C}/\Lambda$ be an elliptic curve and let H be a principal polarization on X. A choice of a symplectic basis of Λ for $\operatorname{Im} H$ induces an isomorphism $(X, H) \xrightarrow{\sim} (X', H')$, where the elliptic curve X' is of the form

$$X' = \mathbb{C}/\tau\mathbb{Z} \oplus \mathbb{Z},$$

with $\tau \in \mathbb{H}$, the Poincaré upper half-space. Writing $\tau = \tau_1 + i\tau_2$, the form H' is given by

$$H'(v, w) = \frac{v\bar{w}}{\tau_2}.$$

For $v = v_1 + iv_2$ and $w = w_1 + iw_2$ we have

$$H'(v, w) = \frac{v_1 w_1 + v_2 w_2}{\tau_2} + i\frac{v_2 w_1 - v_1 w_2}{\tau_2}.$$

In particular, for the basis $\{\tau, 1\}$ of the lattice $\tau\mathbb{Z} \oplus \mathbb{Z}$ we have

$$\operatorname{Im} H'(\tau, 1) = \frac{\tau_2}{\tau_2} = 1.$$

At this point we do not worry too much about the choice of the symplectic basis of Λ for $\operatorname{Im} H$, but it is worth mentioning that Ω heavily relies on that choice. We will study the consequences of distinct choices more thoroughly in Section 1.4.1.

Characteristics. A decomposition of Λ or $\mathbb{C}^g$ only depends on the algebraic equivalence class of $\mathcal{L}$, and not on $\mathcal{L}$ itself. The advantage is that, once a decomposition is fixed, we obtain an explicit description of *all* line bundles with first Chern class $H = c_1(\mathcal{L})$ in terms of characteristics (elements $c \in \mathbb{C}^g$ modulo $\Lambda(\mathcal{L})$). Furthermore, if $\mathcal{L}$ is a polarization, we can describe theta functions for $\mathcal{L}$ in terms of a decomposition plus a characteristic, and obtain in a canonical way a system of theta functions that will allow us (under certain circumstances) to embed the torus $X = \mathbb{C}^g/\Lambda$ into projective space. Hence, we could think of a decomposition plus a characteristic as the sufficient data to obtain projective coordinates on X. And most importantly, these notions have an algebraic analogue, extensively studied in Section 2. We can then talk about canonical coordinates on an abelian variety, and we refer to them as *theta coordinates*. A compatibility notion for the algebraic analogue of "decomposition plus characteristic" for isogenous abelian varieties will lead to the key tool for the computation of isogenies in theta coordinates.

Let $X = \mathbb{C}^g/\Lambda$ be a complex torus and let $H \in \mathrm{NS}(X)$ be a nondegenerate form. Suppose that we have fixed a decomposition $\mathbb{C}^g = V_1 \oplus V_2$, where V_1 and V_2 are isotropic (for $\operatorname{Im} H$) $\mathbb{R}$-vector subspaces of dimension g. We define a map $\chi_0 \colon \mathbb{C}^g \to \mathbb{C}_1$ by

$$\chi_0(v) = e(\pi i \operatorname{Im} H(v_1, v_2)),$$

where $v = v_1 + v_2$ with $v_i \in V_i$. Denote again by χ_0 the restriction of χ_0 to $\Lambda = \Lambda_1 \oplus \Lambda_2$, where $\Lambda_i = V_i \cap \Lambda$. It is not hard to see that χ_0 is a semicharacter for H and hence, $\mathcal{L}_0 = \mathcal{L}(H, \chi_0)$ is a holomorphic line bundle on X. By Lemma 1.3, for each $v \in \mathbb{C}^g$ the pullback by $t_{\bar{v}}$ of $\mathcal{L}_0$ is algebraically equivalent to $\mathcal{L}_0$. In terms of semicharacters, this means that $\chi_0 e(2\pi i \operatorname{Im} H(v, \cdot))$ is a semicharacter for $t_{\bar{v}}^* \mathcal{L}_0$. The following proposition shows that all line bundles algebraically equivalent to $\mathcal{L}_0$ are of this form.

Proposition 1.9. *Let $\mathcal{L}$ and $\mathcal{L}'$ be algebraically equivalent, nondegenerate line bundles on X. Then there exists $x \in X$ such that*

$$\mathcal{L}' = t_x^* \mathcal{L}.$$

Proof. The line bundle $\mathcal{L}' \otimes \mathcal{L}^{-1}$ is in $\mathrm{Pic}^0(X)$. Since $\mathcal{L}$ is nondegenerate, the map $\phi_{\mathcal{L}} \colon X \to \widehat{X} = \mathrm{Pic}^0(X)$, $x \mapsto t_x^* \mathcal{L} \otimes \mathcal{L}^{-1}$ is an isogeny, hence surjective. Let $x \in X$ be such that $\mathcal{L}' \otimes \mathcal{L}^{-1} = \phi_{\mathcal{L}}(x)$. Multiplying both sides by $\mathcal{L}$ we obtain the desired result. □

Moreover, it becomes clear from the above proof that translates of x by $K(\mathcal{L}) = \ker \phi_{\mathcal{L}}$ lead to the same result. In summary we have: for all line bundle $\mathcal{L}$, algebraically equivalent to $\mathcal{L}_0$, there exists a $c \in \mathbb{C}^g$, uniquely determined up to translates by $\Lambda(\mathcal{L}_0)$, such that $\mathcal{L} = t_c^* \mathcal{L}_0$. We call c a *characteristic* of $\mathcal{L}$ with respect to the decomposition $\mathbb{C}^g = V_1 \oplus V_2$. A decomposition plus a characteristic are thus sufficient to describe all holomorphic line bundles on X in the same algebraic equivalence class.

Theta functions. Let us now turn our attention to the explicit construction of theta functions. Let $X = \mathbb{C}^g/\Lambda$ be a complex torus and let $\mathcal{L}$ be a polarization on X of type $\delta = (\delta_1, \ldots, \delta_g)$. Let $H = c_1(\mathcal{L})$ be the first Chern class of $\mathcal{L}$, and suppose $\mathbb{C}^g = V_1 \oplus V_2$ is a decomposition (into isotropic subspaces for $\operatorname{Im} H$), induced by a decomposition $\Lambda = \Lambda_1 \oplus \Lambda_2$. By Proposition 1.7, V_2 generates $\mathbb{C}^g$ as a $\mathbb{C}$-vector space. Since $\operatorname{Im} H$ vanishes on V_2, the form H is symmetric on V_2. We can $\mathbb{C}$-bilinearly extend the form $H|_{V_2 \times V_2}$ to a symmetric bilinear form $B \colon \mathbb{C}^g \times \mathbb{C}^g \to \mathbb{C}$. We will first define theta

functions for the line bundle $\mathcal{L}_0 = \mathcal{L}(H, \chi_0)$ of characteristic 0 with respect to the fixed decomposition of $\mathbb{C}^g$. Let $a_{(H,\chi_0)}(\lambda, v) = \chi_0(\lambda)e(\pi H(v,\lambda) + \frac{\pi}{2}H(\lambda,\lambda))$ be the canonical factor of automorphy for $\mathcal{L}_0$ as in (1.5). Define a function $\theta^0\colon \mathbb{C}^g \to \mathbb{C}$ as

$$\theta^0(v) = e\left(\frac{\pi}{2}B(v,v)\right)\sum_{\lambda\in\Lambda_1} e\left(-\frac{\pi}{2}(H-B)(\lambda,\lambda) + \pi(H-B)(v,\lambda)\right). \tag{1.12}$$

By [BL04, Lem. 3.2.4], the function θ^0 is holomorphic on $\mathbb{C}^g$ and satisfies

$$\theta^0(v+\lambda) = a_{(H,\chi_0)}(\lambda, v)\theta^0(v),$$

for all $v \in \mathbb{C}^g$ and $\lambda \in \Lambda$. We call θ^0 a *canonical theta function for* $\mathcal{L}_0$. Here, the word canonical is to indicate that θ^0 is a theta function for the canonical factor of automorphy $a_{(H,\chi_0)}$ of $\mathcal{L}_0$.

If we let $c \in \mathbb{C}^g$ be the characteristic of $\mathcal{L}$ (defined up to $\Lambda(\mathcal{L}_0)$-translates) with respect to the decomposition $\mathbb{C}^g = V_1 \oplus V_2$, then $\mathcal{L}$ is given by $\mathcal{L} = t_c^*\mathcal{L}_0$. Recall that $\chi = \chi_0 e(2\pi i \operatorname{Im} H(c,\cdot))$ is a semicharacter for $\mathcal{L}$, which in terms of factors of automorphy means

$$a_{(H,\chi)}(\lambda, v) = a_{(H,\chi_0)}(\lambda, v)e(2\pi i \operatorname{Im} H(c,\lambda)). \tag{1.13}$$

A simple pullback of θ^0 by t_c will not be a theta function for the factor $a_{(H,\chi)}$, but only for a $B^1(\Lambda, H^0(\mathcal{O}_{\mathbb{C}^g}^\times))$-equivalent one. However, we can solve this issue by multiplying the theta function $t_c^*\theta^0$ by the corresponding nonvanishing holomorphic function (the one determining the boundary). Let $\theta^c\colon \mathbb{C}^g \to \mathbb{C}$ be the function

$$\theta^c(v) = e\left(-\pi H(v,c) - \frac{\pi}{2}H(c,c)\right)\theta^0(v+c). \tag{1.14}$$

Then, for $v \in \mathbb{C}^g$ and $\lambda \in \Lambda$ we have

$$\begin{aligned}
\theta^c(v+\lambda) &= e\left(-\pi H(v+\lambda,c) - \frac{\pi}{2}H(c,c)\right)\theta^0(v+c+\lambda)\\
&= a_{(H,\chi_0)}(\lambda, v+c)e(-\pi H(\lambda,c))e\left(-\pi H(v,c) - \frac{\pi}{2}H(c,c)\right)\theta^0(v+c)\\
&= a_{(H,\chi_0)}(\lambda, v)e(\pi H(c,\lambda) - \pi H(\lambda,c))\theta^c(v) \qquad (1.15)\\
&= a_{(H,\chi_0)}(\lambda, v)e(2\pi i \operatorname{Im} H(c,\lambda))\theta^c(v)\\
&= a_{(H,\chi)}(\lambda, v)\theta^c(v).
\end{aligned}$$

We call θ^c a *canonical theta function for* $\mathcal{L}$. At line (1.15) we used the trivial computation $a_{(H,\chi_0)}(\lambda, v+c) = a_{(H,\chi_0)}(\lambda, v)e(\pi H(c,\lambda))$.

We have seen in (1.9) that the polarized abelian variety (X, H) is isomorphic to $(X' = \mathbb{C}^g/\Lambda', H')$, where the lattice Λ' is of "nice" form. We want to describe theta functions on X', since they are easier to handle. Let $f\colon (X,H) \xrightarrow{\sim} (X' = \mathbb{C}^g/\Lambda', H')$ be the isomorphism of polarized abelian varieties from (1.9), induced by a choice of a symplectic basis for Λ. The lattice $\Lambda' = \rho_a(f)(\Lambda)$ is of the form $\Lambda' = \Omega\mathbb{Z}^g \oplus \Delta\mathbb{Z}^g$, where $\Omega \in \mathcal{H}_g$ is symmetric and with positive definite imaginary part, and $\Delta = \operatorname{diag}(\delta_1, \dots, \delta_g)$. Let $H' = \rho_a(f^{-1})^*H$ be the induced form on X', and let $\chi_0' = \rho_r(f^{-1})^*\chi_0$ and $\chi' = \rho_r(f^{-1})^*\chi$. If we let $\mathcal{L}_0' = \mathcal{L}(H', \chi_0')$ and $\mathcal{L}' = \mathcal{L}(H', \chi')$, then it is clear that $\mathcal{L}_0 = f^*\mathcal{L}_0'$ and $\mathcal{L} = f^*\mathcal{L}'$. The decomposition of Λ' induces a decomposition $\mathbb{C}^g = \Omega\mathbb{R}^g \oplus \mathbb{R}^g$ of $\mathbb{C}^g$ into maximal isotropic subspaces for $\operatorname{Im} H'$, and $c' = \rho_a(f)(c)$ is a characteristic for $\mathcal{L}'$ with respect to this decomposition. Since $\rho_r(f)$ is the restriction of $\rho_a(f)$ to Λ, we have that $a_{(H,\chi_0)} = (\rho_r(f) \times \rho_a(f))^* a_{(H',\chi_0')}$. Then,

$$\rho_a(f^{-1})^*\colon \Gamma(X, \mathcal{L}_0) \xrightarrow{\sim} \Gamma(X', \mathcal{L}_0')$$

is an isomorphism between the theta functions on X for the factor $a_{(H,\chi_0)}$ and the theta functions on X' for the factor $a_{(H',\chi_0')}$. The same holds if we replace $\mathcal{L}_0$ by $\mathcal{L}$, $\mathcal{L}_0'$ by $\mathcal{L}'$, $a_{(H,\chi_0)}$ by $a_{(H,\chi)}$ and $a_{(H',\chi_0')}$ by $a_{(H',\chi')}$.

If we let $B' = \rho_a(f^{-1})^* B$, then it follows immediately from (1.11) that

$$B'(v,w) = {}^t v(\operatorname{Im}\Omega)^{-1} w.$$

Since $\mathbb{C}^g = \Omega\mathbb{R}^g \oplus \mathbb{R}^g$, every $w \in \mathbb{C}^g$ can be written in a unique way as $w = \Omega w_1 + w_2$ with $w_1, w_2 \in \mathbb{R}^g$ and hence, $\operatorname{Re} w = (\operatorname{Re}\Omega)w_1 + w_2$ and $\operatorname{Im} w = (\operatorname{Im}\Omega)w_1$. It is easy to see that

$$(H' - B')(v,w) = {}^t v(\operatorname{Im}\Omega)^{-1}(\bar{w} - w) = -2i\,{}^t v(\operatorname{Im}\Omega)^{-1}\operatorname{Im} w = -2i\,{}^t v w_1.$$

We can now deduce a more familiar description of theta functions, first the characteristic 0 case and then for arbitrary characteristic:

$$\begin{aligned}
(\rho_a(f^{-1})^*\theta^0)(v) &= e\left(\frac{\pi}{2}B(\rho_a(f^{-1})(v), \rho_a(f^{-1})(v))\right) \\
&\qquad \cdot \sum_{\lambda\in\Lambda_1} e\left(-\frac{\pi}{2}(H-B)(\lambda,\lambda) + \pi(H-B)(\rho_a(f^{-1})(v),\lambda)\right) \\
&= e\left(\frac{\pi}{2}B'(v,v)\right) \sum_{\lambda'\in\Lambda_1'} e\left(-\frac{\pi}{2}(H'-B')(\lambda',\lambda') + \pi(H'-B')(v,\lambda')\right) \\
&= e\left(\frac{\pi}{2}B'(v,v)\right) \sum_{\Omega n\in\Omega\mathbb{Z}^g} e\left(-\frac{\pi}{2}(H'-B')(\Omega n,\Omega n) + \pi(H'-B')(v,\Omega n)\right) \\
&= e\left(\frac{\pi}{2}B'(v,v)\right) \sum_{n\in\mathbb{Z}^g} e\left(\pi i\,{}^t n\Omega n + 2\pi i\,{}^t v n\right) \text{ (changing } n \leftrightarrow -n). \qquad (1.16)
\end{aligned}$$

The function

$$\theta(v,\Omega) := \sum_{n\in\mathbb{Z}^g} e\left(\pi i\,{}^t n\Omega n + 2\pi i\,{}^t v n\right) \qquad (1.17)$$

is called the *Riemann theta function*. Since Ω is determined by the isomorphism f, which in turn is determined by a choice of a symplectic basis for Λ, it does not seem to make sense at first to consider Ω as a variable. Yet, when we will study the consequences of different choices of symplectic bases, it is preferable to consider θ as a function on $\mathbb{C}^g \times \mathcal{H}_g$. From the relation $\rho_a(f^{-1})^*\theta^0 = e\left(\frac{\pi}{2}B'(\cdot,\cdot)\right)\theta(\cdot,\Omega)$ it follows that

$$e\left(\frac{\pi}{2}B'(v+\lambda,v+\lambda)\right)\theta(v+\lambda,\Omega) = a_{(H',\chi_0')}(\lambda,v)e\left(\frac{\pi}{2}B'(v,v)\right)\theta(v,\Omega),$$

for all $v \in \mathbb{C}^g$ and $\lambda \in \Lambda'$. The function

$$(\lambda,v) \mapsto e\left(\frac{\pi}{2}B'(v,v)\right) e\left(\frac{\pi}{2}B'(v+\lambda,v+\lambda)\right)^{-1}$$

is a boundary, hence $\theta(v,\Omega) \in \Gamma(X', \mathcal{L}_0')$ for the factor

$$e_{\mathcal{L}_0'}(\lambda,v) := a_{(H',\chi_0')}(\lambda,v)e\left(\frac{\pi}{2}B'(v,v)\right) e\left(\frac{\pi}{2}B'(v+\lambda,v+\lambda)\right)^{-1}.$$

Writing $\lambda = \lambda_1 + \lambda_2 = \Omega n + \Delta m$ with $n, m \in \mathbb{Z}^g$, we have

$$\begin{aligned}
e_{\mathcal{L}_0'}(\lambda,v) &= e\left(\pi i \operatorname{Im} H'(\lambda_1,\lambda_2) + \pi(H'-B')(v,\lambda) + \frac{\pi}{2}(H'-B')(\lambda,\lambda)\right) \\
&= e\left(\pi i\,{}^t n\Delta m - 2\pi i\,{}^t v n - \pi i\,{}^t(\Omega n + \Delta m)n\right) \\
&= e\left(-\pi i\,{}^t n\Omega n - 2\pi i\,{}^t v n\right).
\end{aligned}$$

In summary, the Riemann theta function $\theta(v,\Omega)$ satisfies

$$\theta(v+\Omega n+\Delta m,\Omega)=e\left(-\pi i\,{}^t n\Omega n-2\pi i\,{}^t vn\right)\theta(v,\Omega),$$

for all $v\in\mathbb{C}^g$ and $n,m\in\mathbb{Z}^g$. We see that $\theta(\cdot,\Omega)$ is periodic with respect to $\Lambda_2'=\Delta\mathbb{Z}^g$. This property holds as well if the polarization is principal, i.e. of type $\delta=(1,\dots,1)$.

Let us now study the image of θ^c under $\rho_a(f^{-1})^*$. Recall that

$$\theta^c(v)=e\left(-\pi H(v,c)-\frac{\pi}{2}H(c,c)\right)\theta^0(v+c).$$

For $c'=\rho_a(f)(c)$ there exist unique $a,b\in\mathbb{R}^g$ such that $c'=\Omega a+b$. We have

$$\begin{aligned}
(\rho_a(f^{-1})^*\theta^c)(v)&=e\left(-\pi H(\rho_a(f^{-1})(v),c)-\frac{\pi}{2}H(c,c)\right)\theta^0(\rho_a(f^{-1})(v)+c)\\
&=e\left(-\pi H'(v,c')-\frac{\pi}{2}H'(c',c')\right)\rho_a(f^{-1})^*\theta^0(v+c')\\
&=e\left(-\pi H'(v,c')-\frac{\pi}{2}H'(c',c')\right)e\left(\frac{\pi}{2}B'(v+c',v+c')\right)\\
&\qquad\cdot\sum_{n\in\mathbb{Z}^g}e\left(\pi i\,{}^t n\Omega n+2\pi i\,{}^t(v+c')n\right)\\
&=e\left(-\pi(H'-B')(v,c')-\frac{\pi}{2}(H'-B')(c',c')+\frac{\pi}{2}B'(v,v)\right)\\
&\qquad\cdot\sum_{n\in\mathbb{Z}^g}e\left(\pi i\,{}^t n\Omega n+2\pi i\,{}^t vn+2\pi i\,{}^t c'n\right)\\
&=e\left(2\pi i\,{}^t va+\pi i\,{}^t(\Omega a+b)a+\frac{\pi}{2}B'(v,v)\right)\\
&\qquad\cdot\sum_{n\in\mathbb{Z}^g}e\left(\pi i\,{}^t n\Omega n+2\pi i\,{}^t vn+2\pi i\,{}^t(\Omega a+b)n\right)\\
&=e\left(\frac{\pi}{2}B'(v,v)-\pi i\,{}^t ba\right)\\
&\qquad\cdot\sum_{n\in\mathbb{Z}^g}e\left(\pi i\,{}^t(n+a)\Omega(n+a)+2\pi i\,{}^t(v+b)(n+a)\right).
\end{aligned}$$

We call

$$\theta\begin{bmatrix}a\\b\end{bmatrix}(v,\Omega):=\sum_{n\in\mathbb{Z}^g}e\left(\pi i\,{}^t(n+a)\Omega(n+a)+2\pi i\,{}^t(v+b)(n+a)\right)\tag{1.18}$$

the *Riemann theta function with characteristic* $\begin{bmatrix}a\\b\end{bmatrix}$. The theta functions $\rho_a(f^{-1})^*\theta^c$ and $\theta\begin{bmatrix}a\\b\end{bmatrix}(\cdot,\Omega)$ are related by

$$\rho_a(f^{-1})^*\theta^c=e\left(\frac{\pi}{2}B'(\cdot,\cdot)-\pi i\,{}^t ba\right)\theta\begin{bmatrix}a\\b\end{bmatrix}(\cdot,\Omega),$$

and

$$e_{\mathcal{L}'}(\lambda,v):=a_{(H',\chi')}(\lambda,v)e\left(\frac{\pi}{2}B'(v,v)\right)e\left(\frac{\pi}{2}B'(v+\lambda,v+\lambda)\right)^{-1}$$

is a factor of automorphy for $\theta\begin{bmatrix}a\\b\end{bmatrix}(\cdot,\Omega)$, equivalent to $a_{(H',\chi')}$. We therefore have $\theta\begin{bmatrix}a\\b\end{bmatrix}(v,\Omega)\in\Gamma(X',\mathcal{L}')$. Writing $\lambda=\Omega n+\Delta m$ and $c'=\Omega a+b$, with $n,m\in\mathbb{Z}^g$ and $a,b\in\mathbb{R}^g$, it is easy to see that

$$\begin{aligned}
e_{\mathcal{L}'}(\lambda,v)&=e_{\mathcal{L}_0'}(\lambda,v)e(2\pi i\,\mathrm{Im}\,H'(c',\lambda))\\
&=e\left(-\pi i\,{}^t n\Omega n-2\pi i\,{}^t vn+2\pi i({}^t a\Delta m-{}^t bn)\right).
\end{aligned}$$

The Riemann theta function with characteristic $\begin{bmatrix} a \\ b \end{bmatrix}$ satisfies

$$\theta \begin{bmatrix} a \\ b \end{bmatrix} (v + \Omega n + \Delta m, \Omega) = e\left(-\pi i\, {}^t n \Omega n - 2\pi i\, {}^t v n + 2\pi i({}^t a \Delta m - {}^t b n)\right) \theta \begin{bmatrix} a \\ b \end{bmatrix} (v, \Omega), \tag{1.19}$$

for all $v \in \mathbb{C}^g$ and $n, m \in \mathbb{Z}^g$. The function $\theta \begin{bmatrix} 0 \\ 0 \end{bmatrix} (\cdot, \Omega)$ is just the standard Riemann theta function $\theta(\cdot, \Omega)$. Analogous to the relation between θ^c and θ^0, see (1.14), the theta functions $\theta \begin{bmatrix} a \\ b \end{bmatrix} (\cdot, \Omega)$ and $\theta \begin{bmatrix} 0 \\ 0 \end{bmatrix} (\cdot, \Omega)$ are related by

$$\theta \begin{bmatrix} a \\ b \end{bmatrix} (v, \Omega) = e(\pi i\, {}^t a \Omega a + 2\pi i\, {}^t a (v + b)) \theta \begin{bmatrix} 0 \\ 0 \end{bmatrix} (v + \Omega a + b, \Omega). \tag{1.20}$$

From (1.20) we can carefully verify that for $a', b' \in \mathbb{Z}^g$ we have

$$\theta \begin{bmatrix} a + a' \\ b + b' \end{bmatrix} (v, \Omega) = e(2\pi i\, {}^t a b') \theta \begin{bmatrix} a \\ b \end{bmatrix} (v, \Omega). \tag{1.21}$$

More generally, for $a', b' \in \mathbb{R}^g$, it follows from [BL04, Cor. 3.2.9] that

$$\theta \begin{bmatrix} a + a' \\ b + b' \end{bmatrix} (v, \Omega) = e(\pi i\, {}^t a' \Omega a' + 2\pi i\, {}^t a' (v + b' + b)) \theta \begin{bmatrix} a \\ b \end{bmatrix} (v + \Omega a' + b', \Omega). \tag{1.22}$$

As a direct consequence of (1.18) we have

$$\theta \begin{bmatrix} a \\ b \end{bmatrix} (-v, \Omega) = \theta \begin{bmatrix} -a \\ -b \end{bmatrix} (v, \Omega). \tag{1.23}$$

In particular, if $a, b \in \mathbb{Z}^g$, we have

$$\theta \begin{bmatrix} a/2 \\ b/2 \end{bmatrix} (-v, \Omega) = e(\pi i\, {}^t a b) \theta \begin{bmatrix} a/2 \\ b/2 \end{bmatrix} (v, \Omega). \tag{1.24}$$

Hence, theta functions of half-integer characteristics are either even or odd functions. Depending on the parity of ${}^t ab$, we call $\theta \begin{bmatrix} a/2 \\ b/2 \end{bmatrix}$ an *even theta function* or an *odd theta function* respectively.

Bases of theta functions and projective embeddings. Given a polarization $\mathcal{L} = \mathcal{L}(H, \chi)$ on $X = \mathbb{C}^g/\Lambda$ of type $\delta = (\delta_1, \ldots, \delta_g)$, we have seen how to construct one canonical theta function for $\mathcal{L}$. But there are more. For a fixed decomposition $\mathbb{C}^g = V_1 \oplus V_2$, where V_1 and V_2 are isotropic for $\operatorname{Im} H$, and given a characteristic $c \in \mathbb{C}^g$ for $\mathcal{L}$, we have seen in (1.14) that θ^c is a canonical theta function for $\mathcal{L}$. Let us define $a_{\mathcal{L}} \colon \mathbb{C}^g \times \mathbb{C}^g \to \mathbb{C}^\times$ as

$$a_{\mathcal{L}}(u, v) = \chi_0(u) e\left(2\pi i \operatorname{Im} H(c, u) + \pi H(v, u) + \frac{\pi}{2} H(u, u)\right).$$

It follows that $a_{\mathcal{L}}|_{\Lambda \times \mathbb{C}^g} = a_{(H,\chi)}$ is the canonical factor of automorphy for $\mathcal{L}$. Recall that $K(\mathcal{L}) = \Lambda(\mathcal{L})/\Lambda \subset X$, where $\Lambda(\mathcal{L}) = \{v \in \mathbb{C}^g : \operatorname{Im} H(v, \Lambda) \subset \mathbb{Z}\}$. For $\bar{w} \in K(\mathcal{L})$, define the function

$$\theta^c_{\bar{w}} \colon \mathbb{C}^g \to \mathbb{C},\ v \mapsto a_{\mathcal{L}}(w, v)^{-1} \theta^c(v + w), \tag{1.25}$$

where $w \in \Lambda(\mathcal{L})$ is an arbitrary lift of $\bar{w}$. Using [BL04, Lem. 3.1.3 b)], it is easy to see that the definition of $\theta^c_{\bar{w}}$ does not depend on the choice of the lift of $\bar{w}$.

For $v \in \mathbb{C}^g$ and $\lambda \in \Lambda$ we have

$$\begin{aligned}\theta^c_{\bar{w}}(v+\lambda) &= a_{\mathcal{L}}(w, v+\lambda)^{-1}\theta^c(v+\lambda+w)\\ &= a_{\mathcal{L}}(w,v)^{-1}e(\pi H(\lambda,w))^{-1}a_{(H,\chi)}(\lambda, v+w)\theta^c(v+w)\\ &= a_{(H,\chi)}(\lambda,v)e(\pi(H(w,\lambda)-H(\lambda,w)))a_{\mathcal{L}}(w,v)^{-1}\theta^c(v+w)\\ &= a_{(H,\chi)}(\lambda,v)e(2\pi i \operatorname{Im} H(w,\lambda))\theta^c_{\bar{w}}(v)\\ &= a_{(H,\chi)}(\lambda,v)\theta^c_{\bar{w}}(v).\end{aligned}$$

This shows that $\theta^c_{\bar{w}}$ is a canonical theta function for $\mathcal{L}$. We can use this construction to determine a basis of $\Gamma(X,\mathcal{L})$ of canonical theta functions for $\mathcal{L}$. Recall that with $\Lambda_i = V_i \cap \Lambda$ and $\Lambda(\mathcal{L})_i = V_i \cap \Lambda(\mathcal{L})$, for $i = 1, 2$, we get a decomposition of $K(\mathcal{L})$ as $K(\mathcal{L}) = K(\mathcal{L})_1 \oplus K(\mathcal{L})_2$, where $K(\mathcal{L})_i = \Lambda(\mathcal{L})_i/\Lambda_i$.

Theorem 1.10. *The set $\{\theta^c_{\bar{w}} : \bar{w} \in K(\mathcal{L})_1\}$ is a $\mathbb{C}$-basis of the vector space $\Gamma(X,\mathcal{L})$ of canonical theta functions for $\mathcal{L}$.*

For a proof we refer to [BL04, Thm. 3.2.7]. A decomposition of $\mathbb{C}^g$ plus a characteristic of $\mathcal{L}$ with respect to this decomposition are thus sufficient to obtain a basis of $\Gamma(X,\mathcal{L})$. Fixing an ordering of $K(\mathcal{L})_1$, say $K(\mathcal{L})_1 = \{\bar{w}_0, \dots, \bar{w}_{N-1}\}$, where $N = \#K(\mathcal{L})_1 = \delta_1 \cdots \delta_g$, determines a meromorphic map

$$\Phi_{\mathcal{L}} \colon X \to \mathbb{P}^{N-1}_{\mathbb{C}},\ x \mapsto (\theta^c_{\bar{w}_0}(v_x) : \cdots : \theta^c_{\bar{w}_{N-1}}(v_x)),$$

where $v_x \in \mathbb{C}^g$ is any lift of x. We promised earlier to give a sufficient condition for $\Phi_{\mathcal{L}}$ to be an embedding.

Theorem 1.11 (Lefschetz)**.** *Let $\mathcal{L}$ be a polarization on X of type $\delta = (\delta_1, \dots, \delta_g)$. If $\delta_1 \geq 2$ then $\Phi_{\mathcal{L}}$ is defined on the whole of X, i.e. $\Phi_{\mathcal{L}}$ is a holomorphic map. If $\delta_1 \geq 3$ then $\Phi_{\mathcal{L}} \colon X \hookrightarrow \mathbb{P}^{N-1}_{\mathbb{C}}$ is an embedding.*

See [Lan82, Ch. VI, Thm. 6.1] or [Mum83, Ch. II, Thm. 1.3] for the proof. Of course, the embedding $\Phi_{\mathcal{L}}$ depends on the choice of a basis of $\Gamma(X,\mathcal{L})$. Two different choices of bases are related by an automorphism of $\mathbb{P}^{N-1}_{\mathbb{C}}$. A line bundle $\mathcal{L}$ is called *very ample* if the associated map $\Phi_{\mathcal{L}}$ is an embedding. A line bundle $\mathcal{L}$ is called *ample* if $\mathcal{L}^{\otimes r}$ is very ample for some $r \geq 1$. As a consequence of Theorem 1.11, if $\mathcal{L}$ is a polarization then $\mathcal{L}^{\otimes 3}$ is very ample. In particular, if $\mathcal{L}$ is a principal polarization on X we can embed X into $\mathbb{P}^{3^g-1}_{\mathbb{C}}$. If $\mathcal{L}$ is very ample then $\Phi_{\mathcal{L}}(X)$ is a closed analytic subvariety of $\mathbb{P}^{N-1}_{\mathbb{C}}$ and by Chow's theorem [Har77, Appendix B, Thm. 2.2], X is homeomorphic to an algebraic subvariety of $\mathbb{P}^{N-1}_{\mathbb{C}}$. The functions $\theta^c_{\bar{w}_0}, \dots, \theta^c_{\bar{w}_{N-1}}$ are called *theta coordinates* on X. In summary, if $\mathcal{L}$ is a polarization on X of type $\delta = (\delta_1, \dots, \delta_g)$ with $\delta_1 \geq 3$, then fixing a decomposition of $\mathbb{C}^g$ and a characteristic c of $\mathcal{L}$ with respect to this decomposition determines theta coordinates on the algebraic variety X in a canonical way.

We would like to know how the basis of Theorem 1.10 for the line bundle $\mathcal{L}_0$ of characteristic 0 behaves under the isomorphism $\rho_a(f^{-1})^* \colon \Gamma(X,\mathcal{L}_0) \xrightarrow{\sim} \Gamma(X',\mathcal{L}'_0)$. As before, we have $\Lambda' = \Omega\mathbb{Z}^g \oplus \Delta\mathbb{Z}^g$ and hence, $\Lambda(\mathcal{L}'_0) = \Omega\Delta^{-1}\mathbb{Z}^g \oplus \mathbb{Z}^g$. It follows that $K(\mathcal{L}'_0)_1 = \Omega\Delta^{-1}\mathbb{Z}^g/\Omega\mathbb{Z}^g$. We might identify $K(\mathcal{L}'_0)_1$ with $\{\Omega\Delta^{-1}d\}$, where d runs over a set of representatives of $\mathbb{Z}^g/\Delta\mathbb{Z}^g$. Let us fix $w \in \Lambda(\mathcal{L}_0)_1$ inducing $\bar{w} \in K(\mathcal{L}_0)_1$, and

let $w' = \Omega\Delta^{-1}d = \rho_a(f)(w)$. We have

$$\begin{aligned}
(\rho_a(f^{-1})^*\theta^0_{\bar{w}})(v) &= a_{\mathcal{L}}(w, \rho_a(f^{-1})(v))^{-1}\theta^0(\rho_a(f^{-1})(v) + w) \\
&= (\rho_a(f^{-1})^* a_{\mathcal{L}}(w', v))^{-1}(\rho_a(f^{-1})^*\theta^0(v + w')) \\
&= \chi_0'(w')^{-1} e\left(-\pi H'(v, w') - \frac{\pi}{2}H'(w', w')\right) \\
&\qquad \cdot e\left(\frac{\pi}{2}B'(v + w', v + w')\right)\theta\begin{bmatrix}0\\0\end{bmatrix}(v + \Omega\Delta^{-1}d, \Omega) \\
&= e\left(-\pi(H' - B')(v, w') - \frac{\pi}{2}(H' - B')(w', w')\right) e\left(\frac{\pi}{2}B'(v, v)\right) \\
&\qquad \cdot e(-\pi i\, {}^t(\Delta^{-1}d)\Omega(\Delta^{-1}d) - 2\pi i\, {}^t v\Delta^{-1}d)\theta\begin{bmatrix}\Delta^{-1}d\\0\end{bmatrix}(v, \Omega) \text{ (by (1.20))} \\
&= e\left(\frac{\pi}{2}B'(v, v)\right)\theta\begin{bmatrix}\Delta^{-1}d\\0\end{bmatrix}(v, \Omega).
\end{aligned}$$

Moreover, using (1.19) and the fact that $e(2\pi i\, {}^t(\Delta^{-1}d)\Delta m) = 1$, the theta function $\theta\begin{bmatrix}\Delta^{-1}d\\0\end{bmatrix}(v, \Omega)$ satisfies

$$\theta\begin{bmatrix}\Delta^{-1}d\\0\end{bmatrix}(v + \Omega n + \Delta m, \Omega) = e\left(-\pi i\, {}^t n\Omega n - 2\pi i\, {}^t vn\right)\theta\begin{bmatrix}\Delta^{-1}d\\0\end{bmatrix}(v, \Omega), \tag{1.26}$$

for all $n, m \in \mathbb{Z}^g$. Hence,

$$\left\{\theta\begin{bmatrix}\Delta^{-1}d\\0\end{bmatrix}(v, \Omega) : d \in Repr(\mathbb{Z}^g/\Delta\mathbb{Z}^g)\right\} \tag{1.27}$$

is a basis of $\Gamma(X', \mathcal{L}_0')$ for the factor $e_{\mathcal{L}_0'}(\Omega n + \Delta m, v) = e\left(-\pi i\, {}^t n\Omega n - 2\pi i\, {}^t vn\right)$.

Let $N = \det\Delta = \delta_1 \cdots \delta_g$ and suppose that $\delta_1 \geq 3$. Then, fixing an ordering $\{d_0, \ldots, d_{N-1}\}$ of the representatives of $\mathbb{Z}^g/\Delta\mathbb{Z}^g$ yields an embedding

$$\Phi_{\mathcal{L}_0'} \colon X' \hookrightarrow \mathbb{P}^{N-1}_{\mathbb{C}},\ x \mapsto \left(\theta\begin{bmatrix}\Delta^{-1}d_0\\0\end{bmatrix}(v_x, \Omega) : \cdots : \theta\begin{bmatrix}\Delta^{-1}d_{N-1}\\0\end{bmatrix}(v_x, \Omega)\right),$$

where $v_x \in \mathbb{C}^g$ is any lift of x.

Example 1.12. Let $X = \mathbb{C}^g/\Omega\mathbb{Z}^g \oplus \mathbb{Z}^g$ be a complex torus, where $\Omega \in \mathcal{H}_g$ is in the Siegel upper half-space. Let $H_\Omega(v, w) = {}^t v(\operatorname{Im}\Omega)^{-1}\bar{w}$ be a principal polarization on X and let $\mathcal{L}_\Omega$ be an ample line bundle on X with first Chern class H_Ω and of characteristic 0 with respect to the decomposition $\mathbb{C}^g = \Omega\mathbb{R}^g \oplus \mathbb{R}^g$. By Lefschetz's theorem (Theorem 1.11), we can embed X into projective space by means of global sections of $\mathcal{L}_\Omega^{\otimes r}$, for $r \geq 3$. Let us compute a basis of $\Gamma(X, \mathcal{L}_\Omega^{\otimes r})$, following (1.12) and Theorem 1.10. The first Chern class of $\mathcal{L}_\Omega^{\otimes r}$ is rH_Ω, and the $\mathbb{C}$-bilinear extension $B\colon \mathbb{C}^g \times \mathbb{C}^g \to \mathbb{C}$ of $rH_\Omega|_{\mathbb{R}^g \times \mathbb{R}^g}$ is given by $B(v, w) = r\, {}^t v(\operatorname{Im}\Omega)^{-1}w$. Also, $(rH_\Omega - B)(v, w) = -2ri\, {}^t vw_1$, where $w = \Omega w_1 + w_2$. Applying (1.12), we have that

$$\begin{aligned}
\theta^0(v) &= e\left(\frac{\pi}{2}B(v, v)\right)\sum_{\Omega n \in \Omega\mathbb{Z}^g} e\left(r\pi i\, {}^t(\Omega n)n + 2r\pi i\, {}^t vn\right) \text{ (changing } n \leftrightarrow -n) \\
&= e\left(\frac{\pi}{2}B(v, v)\right)\theta\begin{bmatrix}0\\0\end{bmatrix}(rv, r\Omega)
\end{aligned}$$

is a canonical theta function for $\mathcal{L}_\Omega^{\otimes r}$. The function $v \mapsto e\left(\frac{\pi}{2}B(v, v)\right)$ determines a boundary, so that $\theta\begin{bmatrix}0\\0\end{bmatrix}(rv, r\Omega) \in \Gamma(X, \mathcal{L}_\Omega^{\otimes r})$ for the factor

$$e_{\mathcal{L}_\Omega^{\otimes r}}(\Omega n + m, v) = e(-r\pi i\, {}^t n\Omega n - 2r\pi i\, {}^t vn), \text{ for all } n, m \in \mathbb{Z}^g.$$

Translates of $\theta \begin{bmatrix} 0 \\ 0 \end{bmatrix} (rv, r\Omega)$ by $\Omega a/r + b/r$ (with $a, b \in \mathbb{Z}^g$) adjusted by some factor yield new elements of $\Gamma(X, \mathcal{L}_\Omega^{\otimes r})$. Using (1.20) and Theorem 1.10 we can show that

$$\left\{ \theta \begin{bmatrix} a/r \\ 0 \end{bmatrix} (rv, r\Omega) \right\}_{a \in Repr(\mathbb{Z}^g / r\mathbb{Z}^g)}$$

forms a basis of $\Gamma(X, \mathcal{L}_\Omega^{\otimes r})$ for the factor $e_{\mathcal{L}_\Omega^{\otimes r}}$.

1.3 Why do we care about theta functions?

A complex torus X is a complex manifold, but it need not be algebraic, i.e. it need not be given as the locus of polynomial equations. However, if X admits a polarization $\mathcal{L} \in \mathrm{Pic}(X)$, then by Lefschetz's Theorem 1.11, a suitable power of $\mathcal{L}$ induces an embedding $\Phi_\mathcal{L}$ of X into projective space, and by Chow's theorem [Har77, Appendix B, Thm. 2.2], the torus X is an algebraic variety. But being an algebraic variety, how can we find equations defining X? The embedding $\Phi_\mathcal{L}$ is given by a basis of theta functions, and we can think of these functions as projective coordinates on the variety X. As such, equations defining X can be expressed as relations among the theta functions. These relations are called *Riemman equations*. We will not give the equations here. They can be found in various books such as e.g. [BL04, Thm. 7.5.2] or [Mum66].

But there is more we can deduce from the Riemann equations. Since X is a group, one can ask whether it is possible to perform group arithmetic in theta coordinates. To be more precise, given $x, y \in X$, can we compute the projective coordinates $\Phi_\mathcal{L}(x+y)$ of $x+y$ out of the coordinates $\Phi_\mathcal{L}(x)$ and $\Phi_\mathcal{L}(y)$ of x and y respectively? This will clearly require to manipulate the coordinates of the projective points $\Phi_\mathcal{L}(x)$ and $\Phi_\mathcal{L}(y)$. This, however, is very delicate, since a single coordinate is not a well-defined function (only defined up to a scalar). Consider the affine cone $\widetilde{X} \subset \mathbb{A}^N \setminus \{0\}$ above $\Phi_\mathcal{L}(X) \subset \mathbb{P}^{N-1}$, i.e. the set of affine points $p^{-1}(\Phi_\mathcal{L}(X))$, where $p\colon \mathbb{A}^N \setminus \{0\} \to \mathbb{P}^{N-1}$ is the projection. For $x \in X$, denote by $\widetilde{x} \in \widetilde{X}$ a fixed affine lift of $\Phi_\mathcal{L}(x)$. We will talk more thoroughly about affine cones in Section 2.2.2. Robert in [Rob10, §4.4] gives an algorithm

$$\widetilde{x+y} := \texttt{chain\_add}(\widetilde{x}, \widetilde{y}, \widetilde{x-y}, \widetilde{0}),$$

that computes an affine lift $\widetilde{x+y} \in \widetilde{X}$ of $x+y$, given affine lifts $\widetilde{x}, \widetilde{y}, \widetilde{x-y}, \widetilde{0} \in \widetilde{X}$ of $x, y, x-y$ and 0 respectively. The lift $\widetilde{x+y}$ is computed in a way that $\widetilde{x+y}, \widetilde{x-y}, \widetilde{x}, \widetilde{y}, \widetilde{0}$ satisfy the Riemann relations. So we can think of `chain_add` as "solving" the Riemann equations for $\widetilde{x+y}$. Using recursive calls to `chain_add`, Robert defines an algorithm

$$\widetilde{mx+y} := \texttt{chain\_multadd}(m, \widetilde{x+y}, \widetilde{x}, \widetilde{y}, \widetilde{0}),$$

that computes an affine lift of $mx+y$ for $m > 0$, and it can easily be adapted to the case $m < 0$ as

$$\texttt{chain\_multadd}(m, \widetilde{x+y}, \widetilde{x}, \widetilde{y}, \widetilde{0}) := \texttt{chain\_multadd}(-m, -\widetilde{x+y}, -\widetilde{x}, -\widetilde{y}, \widetilde{0}).$$

Here, $-\widetilde{x}$ denotes a certain affine lift of $-x$. See Proposition 2.35 for more details. Finally, Robert defines the algorithm

$$\widetilde{mx} := \texttt{chain\_mult}(m, \widetilde{x}, \widetilde{0}) = \texttt{chain\_multadd}(m, \widetilde{x}, \widetilde{x}, \widetilde{0}, \widetilde{0}),$$

that computes an affine lift of mx.

We conclude that working with theta coordinates allows us to deduce equations for the abelian variety, as well as to perform arithmetic.

1.3.1 Theta functions on Jacobian varieties

Let C be a smooth projective curve of genus g over $\mathbb{C}$. Let $\big(\mathrm{Jac}(C), \mathcal{O}_{\mathrm{Jac}(C)}(\Theta)\big)$ be the Jacobian variety of C. We know that $\mathrm{Jac}(C)$ is isomorphic to the torus $\mathbb{C}^g/\Lambda$, where the period matrix of the lattice Λ is obtained by integrating g linearly independent holomorphic 1-forms on $2g$ closed loops of C. Let $\mathcal{L} \in \mathrm{Pic}(\mathbb{C}^g/\Lambda)$ be the type $(1,\dots,1)$-line bundle (defining a principal polarization) corresponding to $\mathcal{O}_{\mathrm{Jac}(C)}(\Theta)$. Fixing a symplectic basis of Λ for $c_1(\mathcal{L})$ yields a period matrix $\Omega \in \mathcal{H}_g$ and a line bundle $\mathcal{L}_\Omega \in \mathrm{Pic}(\mathbb{C}^g/\Omega\mathbb{Z}^g \oplus \mathbb{Z}^g)$ such that $\big(\mathrm{Jac}(C), \mathcal{O}_{\mathrm{Jac}(C)}(\Theta)\big) \cong (\mathbb{C}^g/\Omega\mathbb{Z}^g \oplus \mathbb{Z}^g, \mathcal{L}_\Omega)$. Note that the matrix of $c_1(\mathcal{L}_\Omega)$ with respect to the standard basis of $\mathbb{C}^g$ is given by $(\operatorname{Im}\Omega)^{-1}$. The 1-dimensional $\mathbb{C}$-vector space $\Gamma(\mathbb{C}^g/\Omega\mathbb{Z}^g \oplus \mathbb{Z}^g, \mathcal{L}_\Omega)$ is generated by $\theta\begin{bmatrix}0\\0\end{bmatrix}(v,\Omega)$. Fixing a basis of $\Gamma(\mathbb{C}^g/\Omega\mathbb{Z}^g \oplus \mathbb{Z}^g, \mathcal{L}_\Omega^{\otimes 4})$, we can embed the torus $\mathbb{C}^g/\Omega\mathbb{Z}^g \oplus \mathbb{Z}^g$ into $\mathbb{P}^{4^g-1}_{\mathbb{C}}$. Similar to the construction in Example 1.12, a basis of $\Gamma(\mathbb{C}^g/\Omega\mathbb{Z}^g \oplus \mathbb{Z}^g, \mathcal{L}_\Omega^{\otimes 4})$ is given by

$$\left\{\theta\begin{bmatrix}d/4\\0\end{bmatrix}(4v,4\Omega) : d \in \mathit{Repr}(\mathbb{Z}^g/4\mathbb{Z}^g)\right\}.$$

We call them *level-4 theta functions*. The function $\theta\begin{bmatrix}d/4\\0\end{bmatrix}(4v,4\Omega)$ satisfies

$$\theta\begin{bmatrix}d/4\\0\end{bmatrix}(4(v+\Omega n+m),4\Omega) = e\left(-4\pi i\,{}^t n\Omega n - 8\pi i\,{}^t vn\right)\theta\begin{bmatrix}d/4\\0\end{bmatrix}(4v,4\Omega),$$

for all $n, m \in \mathbb{Z}^g$. There exist different bases of $\Gamma(\mathbb{C}^g/\Omega\mathbb{Z}^g \oplus \mathbb{Z}^g, \mathcal{L}_\Omega^{\otimes 4})$ that are of great importance to us. For $d_1, d_2 \in \mathit{Repr}(\mathbb{Z}^g/2\mathbb{Z}^g)$, consider the function $\theta\begin{bmatrix}d_1/2\\d_2/2\end{bmatrix}(2v,\Omega)$ on $\mathbb{C}^g$. Using (1.19), we have that

$$\theta\begin{bmatrix}d_1/2\\d_2/2\end{bmatrix}(2(v+\Omega n+m),\Omega) = e\left(-4\pi i\,{}^t n\Omega n - 8\pi i\,{}^t vn\right)\theta\begin{bmatrix}d_1/2\\d_2/2\end{bmatrix}(2v,\Omega),$$

for all $n, m \in \mathbb{Z}^g$. The functions $\theta\begin{bmatrix}d_1/2\\d_2/2\end{bmatrix}(2v,\Omega)$, for $d_1, d_2 \in \mathit{Repr}(\mathbb{Z}^g/2\mathbb{Z}^g)$, are called *level-(2,...,2) theta functions*. They are related to the level-4 theta functions as follows: for $d_1, d_2 \in \mathit{Repr}(\mathbb{Z}^g/2\mathbb{Z}^g)$ and $v \in \mathbb{C}^g$ we have

$$\theta\begin{bmatrix}d_1/2\\d_2/2\end{bmatrix}(2v,\Omega) = \sum_{\substack{d\in \mathit{Repr}(\mathbb{Z}^g/4\mathbb{Z}^g)\\ d\equiv d_1 \bmod 2}} e(\pi i\,{}^t dd_2)\theta\begin{bmatrix}d/4\\0\end{bmatrix}(4v,4\Omega). \tag{1.28}$$

This shows that

$$\left\{\theta\begin{bmatrix}d_1/2\\d_2/2\end{bmatrix}(2v,\Omega) : d_1, d_2 \in \mathit{Repr}(\mathbb{Z}^g/2\mathbb{Z}^g)\right\}$$

forms another basis of $\Gamma(\mathbb{C}^g/\Omega\mathbb{Z}^g \oplus \mathbb{Z}^g, \mathcal{L}_\Omega^{\otimes 4})$, and we can thus embed $\mathrm{Jac}(C)$ into $\mathbb{P}^{4^g-1}_{\mathbb{C}}$ with level-$(2,\dots,2)$ theta functions. We call

$$\left\{\theta\begin{bmatrix}d_1/2\\d_2/2\end{bmatrix}(0,\Omega) : d_1, d_2 \in \mathit{Repr}(\mathbb{Z}^g/2\mathbb{Z}^g)\right\}$$

the *theta constants of level (2,...,2)* associated to Ω (sometimes also called the *theta null values of level (2,...,2)*). Working with level-$(2,\dots,2)$ theta functions comes with the following advantages:

i) there exists a criterion on the level-$(2,\dots,2)$ theta constants to detect whether the underlying abelian variety is the Jacobian variety of a hyperelliptic curve or not. See Theorem 1.13 below.

ii) in the case of a hyperelliptic Jacobian $\mathrm{Jac}(C)$, we can compute the 4th powers of the level-$(2,\dots,2)$ theta constants directly from the Weierstrass points of the curve. Moreover, this construction has a reciprocal construction, allowing us to compute the Weierstrass points of C from the level-$(2,\dots,2)$ theta constants. See Theorems 1.14 and 1.15 below.

iii) in the non-hyperelliptic genus 3 case (the variety is the Jacobian variety of a smooth plane quartic C), we can compute the 4th powers of the level-$(2,2,2)$ theta constants from the bitangents of the curve. Conversely, given the level-$(2,2,2)$ theta constants, we can compute the bitangents of the curve C and hence, a plane model of the curve. These are called Weber's formula, dating back to 1876 from his work [Web76]. For a more modern treatment of the subject we refer to [Gua11, Rit04, NR17, Fio16].

To address i) and ii) we need to introduce some notations. We follow [Mum84, Ch. IIIa]. Let $B = \{1, 2, \dots, 2g+1, \infty\}$ be an index set. For $i = 1, \dots, g$ define:

$$\begin{aligned}
\eta'_{2i-1} &= {}^t(0,\dots,0,\underset{\substack{i\text{th position}\\\downarrow}}{\tfrac{1}{2}},0,\dots,0) \in \tfrac{1}{2}\mathbb{Z}^g,\\
\eta''_{2i-1} &= {}^t(\tfrac{1}{2},\dots,\tfrac{1}{2},0,0,\dots,0) \in \tfrac{1}{2}\mathbb{Z}^g,\\
\eta'_{2i} &= {}^t(0,\dots,0,\tfrac{1}{2},0,\dots,0) \in \tfrac{1}{2}\mathbb{Z}^g,\\
\eta''_{2i} &= {}^t(\tfrac{1}{2},\dots,\tfrac{1}{2},\tfrac{1}{2},0,\dots,0) \in \tfrac{1}{2}\mathbb{Z}^g,
\end{aligned}$$

and

$$\begin{aligned}
\eta'_{2g+1} &= {}^t(0,\dots,0) \in \tfrac{1}{2}\mathbb{Z}^g,\\
\eta''_{2g+1} &= {}^t(\tfrac{1}{2},\dots,\tfrac{1}{2}) \in \tfrac{1}{2}\mathbb{Z}^g,\\
\eta'_{\infty} &= {}^t(0,\dots,0) \in \tfrac{1}{2}\mathbb{Z}^g,\\
\eta''_{\infty} &= {}^t(0,\dots,0) \in \tfrac{1}{2}\mathbb{Z}^g.
\end{aligned}$$

For $j \in B$ let

$$\eta_j = {}^t(\eta'_j, \eta''_j) \in \frac{1}{2}\mathbb{Z}^{2g},$$

and more generally for $T \subset B$ let

$$\eta_T = \sum_{j\in T} \eta_j \in \frac{1}{2}\mathbb{Z}^{2g}.$$

Note that $\eta_B \in \mathbb{Z}^{2g}$, so that if we denote by T^c the complement of T in B, we have $\eta_T = \eta_{T^c}$ when considered in $\frac{1}{2}\mathbb{Z}^{2g}/\mathbb{Z}^{2g}$. The power set of B is a group under the symmetric difference $T \circ S = (T \cup S) \setminus (T \cap S)$, and η induces a group isomorphism

$$\eta\colon \{T \subset B : \#T \text{ even}\}/T \sim T^c \xrightarrow{\sim} \frac{1}{2}\mathbb{Z}^{2g}/\mathbb{Z}^{2g}. \tag{1.29}$$

Let us fix a period matrix $\Omega \in \mathcal{H}_g$. For $T \subset B$ of even cardinality, denote by

$$\theta[\eta_T](2v, \Omega)$$

the level-$(2,\dots,2)$ theta function of characteristic (the representative of) η_T. By (1.24), the parity of $4\,{}^t\eta'_T\cdot\eta''_T$ determines the parity of $\theta[\eta_T](2v,\Omega)$ (recall that a theta function with half-integer characteristics is either even or odd). Accordingly, we call a characteristic η_T *even* or *odd*. Odd theta functions vanish at 0, and there are precisely 6 odd theta functions in genus 2 and 28 odd theta functions in genus 3. As the next theorem shows, a crucial geometric property of the abelian variety $\mathbb{C}^g/\Omega\mathbb{Z}^g\oplus\mathbb{Z}^g$ can be deduced from the vanishing of the level-(2,...2) theta functions at 0.

Let $U=\{1,3,\dots,2g+1\}\subset B$ be the subset of odd indices. Combining [Mum84, Cor. 6.7] and [Mum84, Thm. 9.1] we obtain the following key result.

Theorem 1.13. *For $\Omega\in\mathcal{H}_g$, the following are equivalent:*

- *$\mathbb{C}^g/\Omega\mathbb{Z}^g\oplus\mathbb{Z}^g$ is isomorphic as a principally polarized abelian variety to the Jacobian variety of a hyperelliptic curve C over $\mathbb{C}$ of genus g;*
- *for all $T\subset B$ of even cardinality,*

$$\theta[\eta_T](0,\Omega)=0 \text{ if and only if } \#(U\circ T)\neq g+1.$$

According to (1.20), the functions $\theta[\eta_T](2v,\Omega)$ and $\theta\begin{bmatrix}0\\0\end{bmatrix}(2v+\Omega\eta'_T+\eta''_T,\Omega)$ differ by a nonvanishing function. The property of being the Jacobian variety of a hyperelliptic curve can thus be deduced from the vanishing of $\theta\begin{bmatrix}0\\0\end{bmatrix}(v,\Omega)$ at certain 2-torsion points. In the genus 2 case, the $T\subset B$, $\#T$ even, corresponding to odd characteristics η_T are precisely the subsets of B satisfying $\#(U\circ T)\neq 3$. That is, $\theta\begin{bmatrix}0\\0\end{bmatrix}(v,\Omega)$ vanishes precisely at the 2-torsion points $\Omega\eta'_T+\eta''_T$ for odd η_T's. In genus 3, however, besides the 28 odd characteristics,

$$\eta_{\{1,3,5,7\}}={}^t\left(\frac12,\frac12,\frac12,\frac12,0,\frac12\right)$$

is the only even characteristic for which $\#(U\circ T)\neq 4$. Hence, we have

$$\Omega\in\mathcal{H}_3 \text{ corresponds to a hyperelliptic Jacobian if and only if}$$
$$\theta\begin{bmatrix}0\\0\end{bmatrix}(\frac12\Omega(e_1+e_2+e_3)+\frac12(e_1+e_3),\Omega)=0.$$

Let now C be a hyperelliptic curve of genus g over $\mathbb{C}$, given by an affine plane model $y^2=f(x)$, where f is a polynomial of degree $2g+2$ without repeated roots. We know that an automorphism of the projective line $\mathbb{P}^1_{\mathbb{C}}$ induces an isomorphism of hyperelliptic curves, so that after sending one root of $f(x)$ to ∞, we can suppose that C is given by an equation $y^2=\prod_{i=1}^{2g+1}(x-a_i)$. The points $P_1=(a_1:0:1),\dots,P_{2g+1}=(a_{2g+1}:0:1)$ are the Weierstrass points of C. Let $\Omega\in\mathcal{H}_g$ be a period matrix such that $\mathrm{Jac}(C)$ is isomorphic to $\mathbb{C}^g/\Omega\mathbb{Z}^g\oplus\mathbb{Z}^g$ as a principally polarized abelian variety. By Theorem 1.13, for all $T\subset B$ of even cardinality, satisfying $\#(U\circ T)=g+1$, we have

$$\theta[\eta_T](0,\Omega)\neq 0.$$

Thomae's formulae allow us to compute the 4th powers of the theta constants of level $(2,\dots,2)$ from the Weierstrass points of the curve.

Theorem 1.14 (Thomae)**.** *There exists a constant c such that for all $T \subset B \setminus \{\infty\}$ of even cardinality,*

$$\theta[\eta_T](0,\Omega)^4 = \begin{cases} c \cdot (-1)^{\#(U\cap T)} \cdot \prod_{\substack{i\in U\circ T \\ j\in (U\circ T)^c - \{\infty\}}} (a_i - a_j)^{-1} & \text{if } \#(U\circ T) = g+1 \\ 0 & \text{if } \#(U\circ T) \neq g+1. \end{cases}$$

The theorem was proven by Thomae in [Tho70]. In fact, Thomae evaluated the constant as well (see [Mum84, §8]). Note that $T \subset B \setminus \{\infty\}$ is not an obstruction to (1.29) being an isomorphism, since either T or T^c is contained in $B \setminus \{\infty\}$ and $\eta_T = \eta_{T^c}$. There exists a reciprocal construction to Thomae's formulae.

Theorem 1.15. *Let $i,j,k \in B \setminus \{\infty\}$ be three distinct indices. Let $V \subset B \setminus \{\infty\}$ of cardinality $g+1$ be such that $i,j \in V$ and $k \notin V$. We have*

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

For a proof we refer to [vW98]. Note that $U \circ (U \circ V \circ \{j,\infty\}) = V \circ \{j,\infty\}$ is of cardinality $g+1$, so that the corresponding theta constant is non-zero. The same holds for $V \circ \{i,k\}, V \circ \{i,\infty\}$ and $V \circ \{j,k\}$.

Remark 1.16. By Torelli's theorem, the principally polarized abelian variety $\big(\mathrm{Jac}(C), \mathcal{O}_{\mathrm{Jac}(C)}(\Theta)\big)$ uniquely determines the curve C (up to isomorphism). From Theorem 1.15 we see that in order to recover an equation of the underlying curve in the hyperelliptic case, it suffices to know the squares of the level-$(2,\ldots,2)$ theta constants. It is a well known fact (see e.g. [Cos11]) that the squares of the level-$(2,\ldots,2)$ theta functions form a generating family for the space $\Gamma(\mathbb{C}^g/\Omega\mathbb{Z}^g \oplus \mathbb{Z}^g, \mathcal{L}_\Omega^{\otimes 2})$ of level-2 theta functions. The squares of the level-$(2,\ldots,2)$ theta null values and the level-2 theta null values thus contain the same geometric information about Ω. However, as Lefschetz's theorem suggests, we should require level at least 3 in order to embed the Jacobian variety of the curve into projective space. Indeed, the level-$(2,\ldots,2)$ theta functions embed $\mathrm{Jac}(C)$ into $\mathbb{P}^{4^g-1}_{\mathbb{C}}$, but the level-2 theta functions (or equivalently, the squares of the level-$(2,\ldots,2)$ theta functions) only embed the Kummer variety $K_{\mathrm{Jac}(C)} = \mathrm{Jac}(C)/\pm 1$ into projective space, and not the Jacobian variety itself. We deduce the surprising fact that, for hyperelliptic Jacobians, we can determine the curve from the Kummer variety only. This fact is highly non-general, but can be explained by the following observation: the inversion $[-1]$ on $\mathrm{Jac}(C)$ is induced by the hyperelliptic involution of the curve. And $K_{\mathrm{Jac}(C)}$ is precisely $\mathrm{Jac}(C)$ modulo $[-1]$, so somehow we can see the Kummer variety as the curve modulo the hyperelliptic involution. But the hyperelliptic involution of C leaves the Weierstrass points (and hence the equation of the curve) invariant, so it does not surprise that the Kummer variety determines the curve.

Thomae's formulae and its reciprocal formulae are implemented in the `Magma` package AVIsogenies (`http://avisogenies.gforge.inria.fr`) for genus 2 and over finite fields. Moreover, if working on the Jacobian variety of a hyperelliptic curve, one can convert between Mumford and theta coordinates (implemented in AVIsogenies for genus 2). For more details we refer to [vW98, Cos11, Rob10].

1.4 Moduli spaces

1.4.1 Polarized abelian varieties of type Δ

Let $X = \mathbb{C}^g/\Lambda$ be a complex torus and let $\mathcal{L} \in \mathrm{Pic}(X)$ be a polarization on X of type $\delta = (\delta_1, \ldots, \delta_g)$. Let $H = c_1(\mathcal{L})$ be the first Chern class of $\mathcal{L}$ and let $\Delta = \mathrm{diag}(\delta_1, \ldots, \delta_g)$. We call $(X, \mathcal{L})$, or equivalently (X, H), a *polarized abelian variety of type Δ (or of type δ)*. We have seen in (1.9) how a choice of a symplectic basis $\lambda_1, \ldots, \lambda_g, \mu_1, \ldots, \mu_g$ of Λ for $\mathrm{Im}\, H$ determines a matrix $\Omega \in \mathcal{H}_g$ and an isomorphism $(X, H) \xrightarrow{\sim} (\mathbb{C}^g/\Omega\mathbb{Z}^g \oplus \Delta\mathbb{Z}^g, H_\Omega)$ of polarized abelian varieties of type Δ, where $(\mathrm{Im}\,\Omega)^{-1}$ is the matrix of H_Ω with respect to the standard basis of $\mathbb{C}^g$. In this section we want to study the impact on Ω of the choice of the symplectic basis of Λ. Let $\lambda'_1, \ldots, \lambda'_g, \mu'_1, \ldots, \mu'_g$ be another symplectic basis of Λ for $\mathrm{Im}\, H$. Let $(\lambda_1, \ldots, \lambda_g, \mu_1, \ldots, \mu_g)$ and $(\lambda'_1, \ldots, \lambda'_g, \mu'_1, \ldots, \mu'_g)$ in $\mathbf{Mat}_{g\times 2g}(\mathbb{C})$ be the period matrices associated to those bases. There exists a matrix $R \in \mathbf{GL}_{2g}(\mathbb{Z})$ such that

$$(\lambda_1, \ldots, \lambda_g, \mu_1, \ldots, \mu_g) = (\lambda'_1, \ldots, \lambda'_g, \mu'_1, \ldots, \mu'_g) \cdot R.$$

Moreover, both bases being symplectic, it follows that ${}^tR \begin{pmatrix} 0 & \Delta \\ -\Delta & 0 \end{pmatrix} R = \begin{pmatrix} 0 & \Delta \\ -\Delta & 0 \end{pmatrix}$, i.e. $R \in \mathbf{Sp}_{2g}^{\Delta}(\mathbb{Z})$. For convenience we may write

$$R = {}^t\begin{pmatrix} A & B \\ C & D \end{pmatrix},$$

with $g \times g$ blocks A, B, C and D in $\mathbf{Mat}_g(\mathbb{Z})$. The basis $\lambda'_1, \ldots, \lambda'_g, \mu'_1, \ldots, \mu'_g$ induces an isomorphism $(X, H) \xrightarrow{\sim} (\mathbb{C}^g/\Omega'\mathbb{Z}^g \oplus \Delta\mathbb{Z}^g, H_{\Omega'})$ of polarized abelian varieties of type Δ, for some $\Omega' \in \mathcal{H}_g$. Consider the composite isomorphism

$$\begin{array}{ccc} & X & \\ \swarrow & & \searrow \\ \mathbb{C}^g/\Omega\mathbb{Z}^g \oplus \Delta\mathbb{Z}^g & \xrightarrow[f]{\cong} & \mathbb{C}^g/\Omega'\mathbb{Z}^g \oplus \Delta\mathbb{Z}^g. \end{array}$$

It is not hard to see that R is the rational representation of f. The isomorphism f is characterized by the relation

$$\rho_a(f) \cdot (\Omega, \Delta) = (\Omega', \Delta) \cdot R,$$

or equivalently

$$\begin{cases} \rho_a(f)\Omega = \Omega' {}^tA + \Delta\, {}^tB \\ \rho_a(f)\Delta = \Omega' {}^tC + \Delta\, {}^tD. \end{cases}$$

It follows that

$$\Omega = {}^t\Omega = (A\Omega' + B\Delta)(\Delta^{-1}C\Omega' + \Delta^{-1}D\Delta)^{-1}.$$

Define the subgroup

$$G_\Delta := \left\{ \begin{pmatrix} \mathbf{1}_g & \\ & \Delta \end{pmatrix}^{-1} {}^tR \begin{pmatrix} \mathbf{1}_g & \\ & \Delta \end{pmatrix} : R \in \mathbf{Sp}_{2g}^{\Delta}(\mathbb{Z}) \right\} \subset \mathbf{GL}_{2g}(\mathbb{Q}).$$

For $M \in G_\Delta$ it follows directly from the definition that ${}^tM \in \mathbf{Sp}_{2g}(\mathbb{Q})$ and since $\mathbf{Sp}_{2g}(\mathbb{Q})$ is closed under transposition, we have $G_\Delta \subset \mathbf{Sp}_{2g}(\mathbb{Q})$. Again, if for $R \in \mathbf{Sp}_{2g}^{\Delta}(\mathbb{Z})$ we use the more convenient notation $R = {}^t\begin{pmatrix} A & B \\ C & D \end{pmatrix}$, then we have

$$G_\Delta = \left\{ \begin{pmatrix} A & B\Delta \\ \Delta^{-1}C & \Delta^{-1}D\Delta \end{pmatrix} : {}^t\begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathbf{Sp}_{2g}^{\Delta}(\mathbb{Z}) \right\} \subset \mathbf{Sp}_{2g}(\mathbb{Q}).$$

Let

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

denote the usual action of $\mathbf{Sp}_{2g}(\mathbb{R})$ on $\mathcal{H}_g$. From the above it becomes clear that a different choice of symplectic basis of Λ for $\operatorname{Im} H$ results in a G_Δ-action on the associated period matrix $\Omega \in \mathcal{H}_g$. To be more precise:

Proposition 1.17. *Let $\lambda_1, \ldots, \lambda_g, \mu_1, \ldots, \mu_g$ and $\lambda'_1, \ldots, \lambda'_g, \mu'_1, \ldots, \mu'_g$ be symplectic bases of Λ for $\operatorname{Im} H$ and let $\Omega, \Omega' \in \mathcal{H}_g$ be the corresponding induced period matrices. Let $R = {}^t\begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathbf{Sp}^{\Delta}_{2g}(\mathbb{Z})$ be such that*

$$(\lambda_1, \ldots, \lambda_g, \mu_1, \ldots, \mu_g) = (\lambda'_1, \ldots, \lambda'_g, \mu'_1, \ldots, \mu'_g) \cdot R.$$

Then, the matrices Ω and Ω' are related by

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

Next, we want to study under what condition two polarized abelian varieties of type Δ are isomorphic. Since any polarized abelian variety of type Δ is isomorphic to a variety $(\mathbb{C}^g/\Omega\mathbb{Z}^g \oplus \Delta\mathbb{Z}^g, H_\Omega)$ for some $\Omega \in \mathcal{H}_g$, it suffices to study the condition on two period matrices $\Omega, \Omega' \in \mathcal{H}_g$ for the existence of an isomorphism of polarized abelian varieties of type Δ

$$f\colon (\mathbb{C}^g/\Omega\mathbb{Z}^g \oplus \Delta\mathbb{Z}^g, H_\Omega) \xrightarrow{\sim} (\mathbb{C}^g/\Omega'\mathbb{Z}^g \oplus \Delta\mathbb{Z}^g, H_{\Omega'}).$$

Symplectic bases of the lattices $\Omega\mathbb{Z}^g \oplus \Delta\mathbb{Z}^g$ and $\Omega'\mathbb{Z}^g \oplus \Delta\mathbb{Z}^g$ for $\operatorname{Im} H_\Omega$ and $\operatorname{Im} H_{\Omega'}$ are given by $\Omega e_1, \ldots, \Omega e_g, \delta_1 e_1, \ldots, \delta_g e_g$ and $\Omega' e_1, \ldots, \Omega' e_g, \delta_1 e_1, \ldots, \delta_g e_g$ respectively. Since $H_\Omega = \rho_a(f)^* H_{\Omega'}$, it follows that

$$\rho_a(f)(\Omega e_1), \ldots, \rho_a(f)(\Omega e_g), \rho_a(f)(\delta_1 e_1), \ldots, \rho_a(f)(\delta_g e_g)$$

is another symplectic basis of $\Omega'\mathbb{Z}^g \oplus \Delta\mathbb{Z}^g$ for $\operatorname{Im} H_{\Omega'}$. The rational representation of f relates the two period matrices for $\mathbb{C}^g/\Omega'\mathbb{Z}^g \oplus \Delta\mathbb{Z}^g$ by

$$(\rho_a(f)(\Omega e_1), \ldots, \rho_a(f)(\delta_g e_g)) = (\Omega' e_1, \ldots, \delta_g e_g) \cdot \rho_r(f)$$

and hence, $\rho_r(f) \in \mathbf{Sp}^{\Delta}_{2g}(\mathbb{Z})$. We can thus apply Proposition 1.17. In summary we have:

Proposition 1.18. *Let $\Omega, \Omega' \in \mathcal{H}_g$ define the polarized abelian varieties of type Δ $(\mathbb{C}^g/\Omega\mathbb{Z}^g \oplus \Delta\mathbb{Z}^g, H_\Omega)$ and $(\mathbb{C}^g/\Omega'\mathbb{Z}^g \oplus \Delta\mathbb{Z}^g, H_{\Omega'})$ respectively, and suppose that there exists an isomorphism of polarized abelian varieties*

$$f\colon (\mathbb{C}^g/\Omega\mathbb{Z}^g \oplus \Delta\mathbb{Z}^g, H_\Omega) \xrightarrow{\sim} (\mathbb{C}^g/\Omega'\mathbb{Z}^g \oplus \Delta\mathbb{Z}^g, H_{\Omega'}).$$

Then:

- *the rational representation $\rho_r(f)$ is in $\mathbf{Sp}^{\Delta}_{2g}(\mathbb{Z})$;*
- *if for convenience we write $\rho_r(f) = {}^t\begin{pmatrix} A & B \\ C & D \end{pmatrix}$, we have*

$$\Omega = (A\Omega' + B\Delta)(\Delta^{-1}C\Omega' + \Delta^{-1}D\Delta)^{-1}.$$

Moreover, the analytic representation of f is given by

$$\rho_a(f) = {}^t(\Delta^{-1}C\Omega' + \Delta^{-1}D\Delta).$$

Example 1.19. Consider the case of elliptic curves. Let $\tau, \tau' \in \mathbb{H}$ be such that there exists an isomorphism of elliptic curves

$$f\colon \mathbb{C}/\tau\mathbb{Z} \oplus \mathbb{Z} \xrightarrow{\sim} \mathbb{C}/\tau'\mathbb{Z} \oplus \mathbb{Z}.$$

(We omit writing the principal polarizations in this picture, but they are there and f respects them.) The analytic representation of f is given by scalar multiplication, say m_λ with $\lambda \in \mathbb{C}^\times$, and we have the relations

$$\begin{cases} \lambda \cdot \tau = a\tau' + b \\ \lambda \cdot 1 = c\tau' + d. \end{cases}$$

Written differently:

$$\lambda \cdot (\tau, 1) = (\tau', 1) \cdot \begin{pmatrix} a & c \\ b & d \end{pmatrix},$$

and $\begin{pmatrix} a & c \\ b & d \end{pmatrix} \in \mathbf{SL}_2(\mathbb{Z}) = \mathbf{Sp}_2(\mathbb{Z})$ since f is supposed to preserve the polarizations. It follows that

$$\tau = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \tau' = \frac{a\tau' + b}{c\tau' + d}$$

and $m_{c\tau'+d}$ is the analytic representation of f.

Discrete subgroups of $\mathbf{Sp}_{2g}(\mathbb{R})$ act properly and discontinuously on $\mathcal{H}_g$ and hence, the quotient

$$\mathcal{A}_\Delta := \mathcal{H}_g/G_\Delta$$

is a complex analytic space of dimension $\frac{g(g+1)}{2}$. But we have just shown that isomorphism classes of polarized abelian varieties of type Δ are in one to one correspondence with G_Δ-orbits of the action $\mathbf{Sp}_{2g}(\mathbb{R}) \curvearrowright \mathcal{H}_g$ and therefore:

Proposition 1.20. *$\mathcal{A}_\Delta$ is a moduli space for polarized abelian varieties of type Δ.*

1.4.2 Polarized abelian varieties of type Δ with invariant theta null values

Fix a type $\Delta = \mathrm{diag}(\delta_1, \ldots, \delta_g)$, and suppose $\delta_1 \geq 3$. Any $\Omega \in \mathcal{H}_g$ determines a polarized abelian variety $(X_\Omega := \mathbb{C}^g/\Omega\mathbb{Z}^g \oplus \Delta\mathbb{Z}^g, H_\Omega)$ of type Δ, where the form H_Ω is given by the matrix $(\mathrm{Im}\,\Omega)^{-1}$ with respect to the standard basis $e_1, \ldots, e_g$ of $\mathbb{C}^g$. Conversely, any polarized abelian variety of type Δ is, up to isomorphism, of this form. Consider the decomposition $\mathbb{C}^g = \Omega\mathbb{R}^g \oplus \mathbb{R}^g$ and let $\mathcal{L}_\Omega$ be the line bundle with first Chern class H_Ω and of characteristic 0 with respect to this decomposition. By (1.27),

$$\left\{\theta \begin{bmatrix} \Delta^{-1}d \\ 0 \end{bmatrix}(v, \Omega) : d \in Repr(\mathbb{Z}^g/\Delta\mathbb{Z}^g)\right\}$$

is a basis of $\Gamma(X_\Omega, \mathcal{L}_\Omega)$ for the factor $e_{\mathcal{L}_\Omega}(\Omega n + \Delta m, v) = e\left(-\pi i\, {}^t n\Omega n - 2\pi i\, {}^t vn\right)$, for all $n, m \in \mathbb{Z}^g$. An ordering $\{d_0, \ldots, d_{\det\Delta - 1}\}$ of $Repr(\mathbb{Z}^g/\Delta\mathbb{Z}^g)$ determines an embedding

$$\Phi_{\mathcal{L}_\Omega}\colon X_\Omega \hookrightarrow \mathbb{P}^{\det\Delta - 1}_{\mathbb{C}},\ x \mapsto \left(\theta \begin{bmatrix} \Delta^{-1}d_0 \\ 0 \end{bmatrix}(v_x, \Omega) : \cdots : \theta \begin{bmatrix} \Delta^{-1}d_{\det\Delta-1} \\ 0 \end{bmatrix}(v_x, \Omega)\right),$$

where $v_x \in \mathbb{C}^g$ is any lift of x.

In the preceding section we have seen that G_Δ-orbits of $\mathcal{H}_g$ characterize isomorphism classes of polarized abelian varieties of type Δ. As Theorems 1.14 and 1.15 suggest, the theta functions of certain level evaluated at 0_{X_Ω} (called the *theta constants* or the *theta null values*) contain important geometric information about the abelian variety X_Ω. However, within a G_Δ-orbit, the theta coordinates can appear in completely different fashion. We would like to find a subgroup of G_Δ with the property that the theta null values remain (projectively) unchanged within its orbits.

Let $R = {}^t\begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathbf{Sp}_{2g}^\Delta(\mathbb{Z})$ with associated $M = \begin{pmatrix} A & B\Delta \\ \Delta^{-1}C & \Delta^{-1}D\Delta \end{pmatrix} \in G_\Delta$. For simplicity write $\Omega_M := M \cdot \Omega = (A\Omega + B\Delta)(\Delta^{-1}C\Omega + \Delta^{-1}D\Delta)^{-1}$, and consider the isomorphism

$$f\colon X_{\Omega_M} = \mathbb{C}^g/\Omega_M\mathbb{Z}^g \oplus \Delta\mathbb{Z}^g \xrightarrow{\sim} X_\Omega = \mathbb{C}^g/\Omega\mathbb{Z}^g \oplus \Delta\mathbb{Z}^g$$

of polarized abelian varieties of type Δ. The rational representation of f is R, and the analytic representation of f is $\rho_a(f) = {}^t(\Delta^{-1}C\Omega + \Delta^{-1}D\Delta)$. First, let us observe that the symplectic basis $\Omega_M e_1, \ldots, \Omega_M e_g, \Delta e_1, \ldots, \Delta e_g$ of $\Omega_M\mathbb{Z}^g \oplus \Delta\mathbb{Z}^g$ for $\operatorname{Im} H_{\Omega_M}$ is sent to

$$\begin{aligned}
\rho_a(f)(\Omega_M e_i) &= {}^t(\Delta^{-1}C\Omega + \Delta^{-1}D\Delta)\,{}^t\Omega_M e_i = (\Omega\,{}^tA + \Delta\,{}^tB)e_i \\
\rho_a(f)(\Delta e_i) &= {}^t(\Delta^{-1}C\Omega + \Delta^{-1}D\Delta)\Delta e_j = (\Omega\,{}^tC + \Delta\,{}^tD)e_i,
\end{aligned}$$

for $i = 1, \ldots, g$, using the fact that ${}^t\Omega_M = \Omega_M$ and ${}^t\Omega = \Omega$. The labelling of the theta functions in $\Gamma(X_{\Omega_M}, \mathcal{L}_{\Omega_M})$ arises from the bijection of $Repr(\mathbb{Z}^g/\Delta\mathbb{Z}^g)$ with $K(\mathcal{L}_{\Omega_M})_1 = \Omega_M\Delta^{-1}\mathbb{Z}^g/\Omega_M\mathbb{Z}^g$, and for the theta functions in $\Gamma(X_\Omega, \mathcal{L}_\Omega)$ the labelling arises from the bijection of $Repr(\mathbb{Z}^g/\Delta\mathbb{Z}^g)$ with $K(\mathcal{L}_\Omega)_1 = \Omega\Delta^{-1}\mathbb{Z}^g/\Omega\mathbb{Z}^g$. Both the decompositions of $K(\mathcal{L}_{\Omega_M})$ and of $K(\mathcal{L}_\Omega)$ are induced by the decompositions of $\mathbb{C}^g$ as $\mathbb{C}^g = \Omega_M\mathbb{R}^g \oplus \mathbb{R}^g$ and $\mathbb{C}^g = \Omega\mathbb{R}^g \oplus \mathbb{R}^g$ respectively. But the isomorphism f does not preserve these decompositions, unless $B = C = 0_g \in \mathbf{Mat}_g(\mathbb{Z})$ and $R = {}^t\begin{pmatrix} A & \\ & \Delta\,{}^tA^{-1}\Delta^{-1} \end{pmatrix} \in \mathbf{Sp}_{2g}^\Delta(\mathbb{Z})$ with $A \in \mathbf{GL}_g(\mathbb{Z})$. However, since the labelling of the theta functions depends on the decompositions of $K(\mathcal{L}_{\Omega_M})$ and of $K(\mathcal{L}_\Omega)$ respectively and not on the ones of $\mathbb{C}^g$, we can require the weaker condition on f to preserve the decompositions of $K(\mathcal{L}_{\Omega_M})$ and $K(\mathcal{L}_\Omega)$. Moreover, to determine an embedding of X_{Ω_M} and X_Ω into projective space by means of theta functions, one must also specify an ordering of the theta functions. Hence, we would like f to respect this ordering. In other words, we require that

$$f(\overline{\tfrac{1}{\delta_i}\Omega_M e_i}) = \overline{\tfrac{1}{\delta_i}\Omega e_i} \text{ and } f(\overline{\tfrac{1}{\delta_i}\Delta e_i}) = \overline{\tfrac{1}{\delta_i}\Delta e_i}, \text{ for } i = 1, \ldots, g. \tag{1.30}$$

Here, $\bar{\cdot}$ denotes an element on the quotient X_{Ω_M} and X_Ω respectively. A necessary and sufficient condition for (1.30) to be satisfied is that

$$A - I_g, B, C, D - I_g \in \Delta \cdot \mathbf{Mat}_g(\mathbb{Z}).$$

For if $A = I_g + \Delta N_A, B = \Delta N_B, C = \Delta N_C$ and $D = I_g + \Delta N_D$ with N_A, N_B, N_C, $N_D \in \mathbf{Mat}_g(\mathbb{Z})$, then

$$\rho_a(f)(\tfrac{1}{\delta_i}\Omega_M e_i) = \tfrac{1}{\delta_i}\Omega e_i + \underbrace{\tfrac{1}{\delta_i}(\Omega\,{}^tN_A\Delta e_i + \Delta\,{}^tN_B\Delta e_i)}_{\in \Omega\mathbb{Z}^g \oplus \Delta\mathbb{Z}^g}$$

and

$$\rho_a(f)(\frac{1}{\delta_i}\Delta e_i) = \frac{1}{\delta_i}\Delta e_i + \underbrace{\frac{1}{\delta_i}(\Omega\, {}^t N_C \Delta e_i + \Delta\, {}^t N_D \Delta e_i)}_{\in \Omega\mathbb{Z}^g \oplus \Delta\mathbb{Z}^g},$$

for all $i = 1, \ldots, g$.

For $N, N' \in \mathbf{Mat}_g(\mathbb{Z})$ we write $N \equiv N' \mod \Delta$ if $N - N' \in \Delta \cdot \mathbf{Mat}_g(\mathbb{Z})$. Define

$$\Gamma(\Delta) := \left\{ R = {}^t\begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathbf{Sp}_{2g}^{\Delta}(\mathbb{Z}) : A, D \equiv I_g \mod \Delta, \text{ and } B, C \equiv 0_g \mod \Delta \right\},$$

which is a subgroup of $\mathbf{Sp}_{2g}^{\Delta}(\mathbb{Z})$. Then we have:

Proposition 1.21. *The isomorphism f with rational representation $R = {}^t\begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathbf{Sp}_{2g}^{\Delta}(\mathbb{Z})$ preserves the decompositions of $K(\mathcal{L}_{\Omega_M})$ and $K(\mathcal{L}_\Omega)$ and respects the ordering of their elements if and only if $R \in \Gamma(\Delta)$.*

Define by

$$G_\Delta(\Delta) := \left\{ \begin{pmatrix} \mathbf{1}_g & \\ & \Delta \end{pmatrix}^{-1} {}^t R \begin{pmatrix} \mathbf{1}_g & \\ & \Delta \end{pmatrix} : R \in \Gamma(\Delta) \right\}$$

the corresponding subgroup of G_Δ. Another way to state Proposition 1.21 is:

Proposition 1.22. *The $G_\Delta(\Delta)$-orbits of the $\mathbf{Sp}_{2g}(\mathbb{R}) \curvearrowright \mathcal{H}_g$-action are characterized by the isomorphism classes of polarized abelian varieties of type Δ, where the induced decomposition of $K(\mathcal{L}_\Omega)$ and the ordering of its elements is preserved.*

So far, we know that isomorphisms that come from the $G_\Delta(\Delta)$-action on $\mathcal{H}_g$ preserve certain decompositions and orderings. But there is one major obstruction to having invariant theta null values within such an orbit that we have not discussed yet. The theta functions $\theta \begin{bmatrix} \Delta^{-1}d \\ 0 \end{bmatrix} (\cdot, \Omega) \in \Gamma(X_\Omega, \mathcal{L}_\Omega)$ do not behave nicely under isomorphisms arising from the $G_\Delta(\Delta)$-action. To be more precise, given $M = \begin{pmatrix} A & B\Delta \\ \Delta^{-1}C & \Delta^{-1}D\Delta \end{pmatrix} \in G_\Delta(\Delta)$, a period matrix $\Omega \in \mathcal{H}_g$ and the isomorphism $f\colon X_{\Omega_M} \xrightarrow{\sim} X_\Omega$, where we again write $\Omega_M = M \cdot \Omega$, the pullback $\rho_a(f^{-1})^*\colon \Gamma(X_{\Omega_M}, \mathcal{L}_{\Omega_M}) \xrightarrow{\sim} \Gamma(X_\Omega, \mathcal{L}_\Omega)$ does not behave the way we might think it does. In other words,

$$\rho_a(f^{-1})^* \theta \begin{bmatrix} \Delta^{-1}d \\ 0 \end{bmatrix} (v, \Omega_M) = \theta \begin{bmatrix} \Delta^{-1}d \\ 0 \end{bmatrix} ({}^t(\Delta^{-1}C\Omega + \Delta^{-1}D\Delta)^{-1}v, \Omega_M) \neq \theta \begin{bmatrix} \Delta^{-1}d \\ 0 \end{bmatrix} (v, \Omega),$$

even though f sends $\overline{\frac{1}{\delta_i}\Omega_M e_i} \mapsto \overline{\frac{1}{\delta_i}\Omega e_i}$, for all $i = 1, \ldots, g$, and hence, sends $\overline{\Omega_M \Delta^{-1} d} \mapsto \overline{\Omega\Delta^{-1}d}$. The reason is that

$$f^*\mathcal{L}_\Omega \ncong \mathcal{L}_{\Omega_M},$$

the former line bundle being of characteristic 0 with respect to the decomposition $\mathbb{C}^g = \rho_a(f^{-1})(\Omega\mathbb{R}^g) \oplus \rho_a(f^{-1})(\mathbb{R}^g)$ and the latter being of characteristic 0 with respect to the decomposition $\mathbb{C}^g = \Omega_M\mathbb{R}^g \oplus \mathbb{R}^g$. The following technical Lemma (see [BL04, Lem. 8.4.1]) tells us how to fix this issue. For a matrix $N \in \mathbf{Mat}_g(\mathbb{R})$, denote by $(N)_0 \in \mathbb{R}^g$ the vector of diagonal elements of N.

Lemma 1.23. *Let $\mathcal{L} \in \mathrm{Pic}(X_\Omega)$ be a line bundle with first Chern class H_Ω. Suppose $\mathcal{L}$ is of characteristic $c \in \mathbb{C}^g$ with respect to the decomposition $\mathbb{C}^g = \Omega\mathbb{R}^g \oplus \mathbb{R}^g$. Let $M = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in G_\Delta$ induce the isomorphism $f\colon X_{\Omega_M} \xrightarrow{\sim} X_\Omega$. Then, $f^*\mathcal{L}$ is of characteristic*

$$c' = \rho_a(f^{-1})c + \frac{1}{2}\Omega_M\Delta(C\,{}^tD)_0 + \frac{1}{2}(A\,{}^tB)_0$$

with respect to the decomposition $\mathbb{C}^g = \Omega_M\mathbb{R}^g \oplus \mathbb{R}^g$.
More precisely, if we write $c = \Omega c_1 + c_2$ with $c_1, c_2 \in \mathbb{R}^g$, then

$$c' = \Omega_M c_1' + c_2'$$

with

$$\begin{aligned} c_1' &= Dc_1 - Cc_2 + \frac{1}{2}\Delta(C\,{}^tD)_0 \\ c_2' &= -Bc_1 + Ac_2 + \frac{1}{2}(A\,{}^tB)_0. \end{aligned}$$

According to Lemma 1.23, the characteristic of the line bundle $f^*\mathcal{L}_\Omega$ with respect to the decomposition $\mathbb{C}^g = \Omega_M\mathbb{R}^g \oplus \mathbb{R}^g$ is given by $\frac{1}{2}\Omega_M\Delta(\Delta^{-1}C\Delta\,{}^tD\Delta^{-1})_0 + \frac{1}{2}(A\Delta\,{}^tB)_0$. The next theorem, called the *symplectic transformation formula*, allows us to describe the pullback $\rho_a(f^{-1})^*\colon \Gamma(X_{\Omega_M}, \mathcal{L}_{\Omega_M}) \xrightarrow{\sim} \Gamma(X_\Omega, \mathcal{L}_\Omega)$. It was first given by Igusa in [Igu72, Ch. 5, Thm. 2]. A proof can also be found in [Mum83, Ch. II.5] and [BL04, Thm. 8.6.1].

Theorem 1.24. *Let $M = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \mathbf{Sp}_{2g}(\mathbb{Z})$ and let $\Omega \in \mathcal{H}_g$. For all $c = \Omega c_1 + c_2 \in \mathbb{C}^g$ and $v \in \mathbb{C}^g$ we have*

$$\begin{aligned} \theta\begin{bmatrix} c_1' \\ c_2' \end{bmatrix}({}^t(C\Omega + D)^{-1}v, \Omega_M) &= \kappa(M)\det(C\Omega + D)^{\frac{1}{2}} e(\pi i\,{}^tv(C\Omega + D)^{-1}Cv) \\ &\quad \cdot e(\pi i({}^t(Dc_1 - Cc_2)(-Bc_1 + Ac_2 + (A\,{}^tB)_0) - {}^tc_1c_2))\theta\begin{bmatrix} c_1 \\ c_2 \end{bmatrix}(v, \Omega), \end{aligned}$$

where $\kappa(M) \in \mathbb{C}_1$ is a constant depending only on M, and c_1', c_2' are as in Lemma 1.23.

Back to our initial problem, which is to find a subgroup of G_Δ with the property that the theta null values remain unchanged within its orbits. Let $\Omega \in \mathcal{H}_g$, $M \in G_\Delta$ and write $\Omega_M := M \cdot \Omega$. The theta null values associated to $X_{\Omega_M} = \mathbb{C}^g/\Omega_M\mathbb{Z}^g \oplus \Delta\mathbb{Z}^g$ are

$$\left\{\theta\begin{bmatrix} \Delta^{-1}d \\ 0 \end{bmatrix}(0, \Omega_M) : d \in \mathit{Repr}(\mathbb{Z}^g/\Delta\mathbb{Z}^g)\right\}$$

and the theta null values associated to $X_\Omega = \mathbb{C}^g/\Omega\mathbb{Z}^g \oplus \Delta\mathbb{Z}^g$ are

$$\left\{\theta\begin{bmatrix} \Delta^{-1}d \\ 0 \end{bmatrix}(0, \Omega) : d \in \mathit{Repr}(\mathbb{Z}^g/\Delta\mathbb{Z}^g)\right\}.$$

Let us consider $M = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) = \left(\begin{smallmatrix} I_g + \Delta N_A & \Delta N_B\Delta \\ N_C & I_g + N_D\Delta \end{smallmatrix}\right) \in G_\Delta(\Delta)$ with N_A, N_B, N_C, $N_D \in \mathbf{Mat}_g(\mathbb{Z})$. The isomorphism $f\colon X_{\Omega_M} \xrightarrow{\sim} X_\Omega$ sends $K(\mathcal{L}_{\Omega_M})_1$ to $K(\mathcal{L}_\Omega)_1$ and preserves the ordering of their elements. But as mentioned earlier, the theta null values behave badly under the pullback $\rho_a(f^{-1})^*$. We have

$$G_\Delta(\Delta) \subset \mathbf{Sp}_{2g}(\mathbb{Z}),$$

and therefore we can apply the transformation formula from Theorem 1.24.

For $c = \Omega\Delta^{-1}d$ we have

$$\begin{aligned}
&\theta\begin{bmatrix} D\Delta^{-1}d + \frac{1}{2}\Delta(C\,{}^tD)_0 \\ -B\Delta^{-1}d + \frac{1}{2}(A\,{}^tB)_0 \end{bmatrix}(0,\Omega_M) = \theta\begin{bmatrix} \Delta^{-1}d + N_Dd + \frac{1}{2}\Delta(N_C(I_g + \Delta\,{}^tN_D))_0 \\ -\Delta N_Bd + \frac{1}{2}(\Delta(I_g + N_A\Delta)\,{}^tN_B\Delta)_0 \end{bmatrix}(0,\Omega_M) \\
&= \kappa(M)\det(C\Omega + D)^{\frac{1}{2}} e(\pi i(-\underbrace{{}^td(I_g + {}^tN_D\Delta)N_Bd}_{={}^t(D\Delta^{-1}d)(B\Delta^{-1}d)})) \\
&\cdot e(\pi i\underbrace{{}^td\Delta^{-1}(I_g + \Delta\,{}^tN_D)(\Delta(I_g + N_A\Delta)\,{}^tN_B\Delta)_0}_{={}^t(D\Delta^{-1}d)(A\,{}^tB)_0})\theta\begin{bmatrix} \Delta^{-1}d \\ 0 \end{bmatrix}(0,\Omega). \qquad (1.31)
\end{aligned}$$

We would like to get to the situation where

$$\theta\begin{bmatrix} \Delta^{-1}d \\ 0 \end{bmatrix}(0,\Omega_M) = \lambda(\Omega,M)\cdot\theta\begin{bmatrix} \Delta^{-1}d \\ 0 \end{bmatrix}(0,\Omega), \qquad (1.32)$$

for $\lambda(\Omega,M) \in \mathbb{C}^\times$ a constant that does only depend on Ω and M, and not on d. Let us first address the left-hand side of (1.31). Recall that for $a, b \in \mathbb{R}^g$, $a', b' \in \mathbb{Z}^g$ and $\Omega \in \mathcal{H}_g$ we have

$$\theta\begin{bmatrix} a + a' \\ b + b' \end{bmatrix}(\cdot,\Omega) = e(2\pi i\,{}^tab')\theta\begin{bmatrix} a \\ b \end{bmatrix}(\cdot,\Omega). \qquad (1.33)$$

For $\theta\begin{bmatrix} \Delta^{-1}d + N_Dd + \frac{1}{2}\Delta(N_C(I_g + \Delta\,{}^tN_D))_0 \\ -\Delta N_Bd + \frac{1}{2}(\Delta(I_g + N_A\Delta)\,{}^tN_B\Delta)_0 \end{bmatrix}(0,\Omega_M)$ to be equal to $\theta\begin{bmatrix} \Delta^{-1}d \\ 0 \end{bmatrix}(0,\Omega_M)$ we impose

i) $N_Dd + \frac{1}{2}\Delta(N_C(I_g + \Delta\,{}^tN_D))_0 \in \mathbb{Z}^g$,

ii) $-\Delta N_Bd + \frac{1}{2}(\Delta(I_g + N_A\Delta)\,{}^tN_B\Delta)_0 \in \mathbb{Z}^g$ and

iii) ${}^td\Delta^{-1}(-\Delta N_Bd + \frac{1}{2}(\Delta(I_g + N_A\Delta)\,{}^tN_B\Delta)_0) \in \mathbb{Z}$ (this is the term ${}^tab'$ from (1.33)).

For i) it suffices that

$$(C\,{}^tD)_0 = (N_C(I_g + \Delta\,{}^tN_D))_0 \equiv 0 \mod 2,$$

where the congruence means that $(C\,{}^tD)_0 \in 2\mathbb{Z}^g$. For ii) it suffices that

$$(A\,{}^tB)_0 = (\Delta(I_g + N_A\Delta)\,{}^tN_B\Delta)_0 \equiv 0 \mod 2.$$

But as will turn out soon, for (1.32) to hold we need the stricter condition

$$(\Delta^{-1}A\,{}^tB\Delta^{-1})_0 = ((I_g + N_A\Delta)\,{}^tN_B)_0 \equiv 0 \mod 2.$$

And iii) follows from ii), observing that

$$(\Delta(I_g + N_A\Delta)\,{}^tN_B\Delta)_0 = \Delta^2((I_g + N_A\Delta)\,{}^tN_B)_0.$$

Denote by

$$G_\Delta(\Delta)_0 := \left\{ \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in G_\Delta(\Delta) : (\Delta^{-1}A\,{}^tB\Delta^{-1})_0 \equiv (C\,{}^tD)_0 \equiv 0 \mod 2 \right\}.$$

It is not hard to verify that $G_\Delta(\Delta)_0$ is a subgroup of $G_\Delta(\Delta)$, and for $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in G_\Delta(\Delta)_0$ we have

$$\theta\begin{bmatrix} D\Delta^{-1}d + \frac{1}{2}\Delta(C\,{}^tD)_0 \\ -B\Delta^{-1}d + \frac{1}{2}(A\,{}^tB)_0 \end{bmatrix}(0,\Omega_M) = \theta\begin{bmatrix} \Delta^{-1}d \\ 0 \end{bmatrix}(0,\Omega_M).$$

Addressing the right-hand side of (1.31), the term

$$\begin{aligned} {}^t(D\Delta^{-1}d)(A\,{}^tB)_0 &= {}^td\Delta^{-1}(I_g + \Delta\,{}^tN_D)(\Delta(I_g + N_A\Delta)\,{}^tN_B\Delta)_0 \\ &= {}^td(\Delta^{-1} + {}^tN_D)\Delta^2((I_g + N_A\Delta)\,{}^tN_B)_0 \end{aligned}$$

is in $2\mathbb{Z}$, provided $M \in G_\Delta(\Delta)_0$. It remains to show that ${}^t(D\Delta^{-1}d)(B\Delta^{-1}d) = {}^td(I_g + {}^tN_D\Delta)N_Bd$ is in $2\mathbb{Z}$. Recall that for $M = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \mathbf{Sp}_{2g}(\mathbb{Z})$ we have

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

If $M \in G_\Delta(\Delta)_0$, then so is M^{-1}, and therefore $(I_g + {}^tN_D\Delta)N_B = \Delta^{-1}\,{}^tDB\Delta^{-1}$ is a matrix with even diagonal entries. Moreover, ${}^tDB$ and $\Delta^{-1}\,{}^tDB\Delta^{-1}$ are symmetric matrices. One can easily show that for a symmetric matrix $S \in \mathbf{Mat}_g(\mathbb{Z})$ and $d \in \mathbb{Z}^g$, the integers ${}^tdSd$ and ${}^t(S)_0d$ are of same parity. It follows that ${}^td(I_g + {}^tN_D\Delta)N_Bd$ is even. In summary we have shown:

Theorem 1.25. *For any $\Omega \in \mathcal{H}_g$, $M = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in G_\Delta(\Delta)_0$ and $d \in Repr(\mathbb{Z}^g/\Delta\mathbb{Z}^g)$, the following equality holds:*

$$\theta\begin{bmatrix} \Delta^{-1}d \\ 0 \end{bmatrix}(0, \Omega_M) = \kappa(M)\det(C\Omega + D)^{\frac{1}{2}}\theta\begin{bmatrix} \Delta^{-1}d \\ 0 \end{bmatrix}(0, \Omega).$$

Here, we write $\Omega_M = M \cdot \Omega$, and κ is a constant depending only on M.

Since $G_\Delta(\Delta)_0$ is a subgroup of G_Δ, its action on $\mathcal{H}_g$ is also properly discontinuous and hence, the quotient

$$\mathcal{A}_\Delta(\Delta)_0 := \mathcal{H}_g/G_\Delta(\Delta)_0$$

is a complex analytic space. Moreover, $G_\Delta(\Delta)_0$ contains the group

$$\begin{pmatrix} \mathbf{1}_g & \\ & \Delta \end{pmatrix}^{-1} {}^t\Gamma(2\delta_g)\begin{pmatrix} \mathbf{1}_g & \\ & \Delta \end{pmatrix},$$

where $\Gamma(2\delta_g) = \{R \in \mathbf{Sp}_{2g}^\Delta(\mathbb{Z}) : R \equiv I_{2g} \mod 2\delta_g\}$ is a principal congruence subgroup of $\mathbf{Sp}_{2g}^\Delta(\mathbb{Z})$. This shows that $G_\Delta(\Delta)_0$ is of finite index in G_Δ.

Proposition 1.26. *$\mathcal{A}_\Delta(\Delta)_0$ is a moduli space for polarized abelian varieties of type Δ with invariant (projective) theta null values. Moreover, the embedding $G_\Delta(\Delta)_0 \hookrightarrow G_\Delta$ induces a finite cover $\mathcal{A}_\Delta(\Delta)_0 \to \mathcal{A}_\Delta$ of the moduli space of polarized abelian varieties of type Δ.*

1.4.3 Embedding moduli spaces into projective space

Fix a type $\Delta = \mathrm{diag}(\delta_1, \ldots, \delta_g)$, and suppose $\delta_1 \geq 2$. Fix once and for all an ordering $\{d_0, \ldots, d_{\det\Delta-1}\}$ of $Repr(\mathbb{Z}^g/\Delta\mathbb{Z}^g)$. According to Theorem 1.11 (Lefschetz),

$$\psi_\Delta \colon \mathcal{H}_g \to \mathbb{P}_{\mathbb{C}}^{\det\Delta-1},\ \Omega \mapsto \left(\theta\begin{bmatrix} \Delta^{-1}d_0 \\ 0 \end{bmatrix}(0,\Omega) : \cdots : \theta\begin{bmatrix} \Delta^{-1}d_{\det\Delta-1} \\ 0 \end{bmatrix}(0,\Omega)\right)$$

is a well defined map. Moreover, ψ_Δ is holomorphic by [BL04, §8.7]. Theorem 1.25 implies that ψ_Δ is constant on $G_\Delta(\Delta)_0$-orbits of $\Omega \in \mathcal{H}_g$. Hence, ψ_Δ factors via $\mathcal{H}_g \to \mathcal{A}_\Delta(\Delta)_0$. Let us denote by

$$\overline{\psi}_\Delta \colon \mathcal{A}_\Delta(\Delta)_0 \to \mathbb{P}_{\mathbb{C}}^{\det\Delta-1}$$

the induced holomorphic map. [BL04, Thm. 8.10.1] gives a criterion for $\overline{\psi}_\Delta$ to be an embedding.

Theorem 1.27. *If $\delta_1 \geq 4$ and $2|\delta_1$ or $3|\delta_1$, then*

$$\overline{\psi}_\Delta \colon \mathcal{A}_\Delta(\Delta)_0 \hookrightarrow \mathbb{P}^{\det\Delta-1}_{\mathbb{C}}$$

is an analytic embedding.

In particular, if the hypotheses of Theorem 1.27 are satisfied, then any $M \in G_\Delta$ that preserves the theta null values, in the sense that

$$\theta\begin{bmatrix}\Delta^{-1}d\\0\end{bmatrix}(0,\Omega_M) = \lambda(\Omega,M)\cdot\theta\begin{bmatrix}\Delta^{-1}d\\0\end{bmatrix}(0,\Omega)$$

for all $\Omega \in \mathcal{H}_g$ and $d \in Repr(\mathbb{Z}^g/\Delta\mathbb{Z}^g)$, where $\lambda(\Omega,M)$ is a constant that does not depend on d, is necessarily an element of $G_\Delta(\Delta)_0$.

An important consequence of Theorem 1.27 is that $\mathcal{A}_\Delta(\Delta)_0$, as well as $\mathcal{A}_\Delta$, are quasi-projective algebraic varieties of dimension $\frac{g(g+1)}{2}$ over $\mathbb{C}$, see [BL04, Rem. 8.10.4]. The most important case where Theorem 1.27 applies is that of $\Delta = 4\cdot I_g$. Since $4\cdot I_g$ is a scalar matrix, we have $\mathbf{Sp}_{2g}^{4\cdot I_g}(\mathbb{Z}) = \mathbf{Sp}_{2g}(\mathbb{Z})$ and

$$G_{4\cdot I_g} = \left\{ \begin{pmatrix} A & 4B \\ C/4 & D \end{pmatrix} : {}^t\begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathbf{Sp}_{2g}(\mathbb{Z}) \right\}.$$

Note that for non-scalar Δ's, the group $\mathbf{Sp}_{2g}^{\Delta}(\mathbb{Z})$ need not be closed under transposition and hence, $\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)$ need not be in $\mathbf{Sp}_{2g}^{\Delta}(\mathbb{Z})$. In the case $\Delta = 4\cdot I_g$ however, we can omit the transpose sign, and write

$$G_{4\cdot I_g} = \left\{ \begin{pmatrix} A & 4B \\ C/4 & D \end{pmatrix} : \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathbf{Sp}_{2g}(\mathbb{Z}) \right\}.$$

In the sequel, let us write 4 instead of $4\cdot I_g$. We have

$$G_4(4) = \left\{ \begin{pmatrix} A & 4B \\ C/4 & D \end{pmatrix} \in G_4 : \begin{pmatrix} A & B \\ C & D \end{pmatrix} \equiv I_{2g} \mod 4 \right\}$$

and

$$G_4(4)_0 = \left\{ \begin{pmatrix} A & 4B \\ C/4 & D \end{pmatrix} \in G_4(4) : (\frac{1}{4}A\,{}^tB)_0 \equiv (\frac{1}{4}C\,{}^tD)_0 \equiv 0 \mod 2 \right\},$$

or equivalently

$$G_4(4)_0 = \left\{ \begin{pmatrix} A & 4B \\ C/4 & D \end{pmatrix} \in G_4(4) : (A\,{}^tB)_0 \equiv (C\,{}^tD)_0 \equiv 0 \mod 8 \right\}.$$

Note that matrices $M \in G_4(4)$ induce isomorphisms

$$\mathbb{C}^g/\Omega_M\mathbb{Z}^g \oplus 4\mathbb{Z}^g \xrightarrow{\sim} \mathbb{C}^g/\Omega\mathbb{Z}^g \oplus 4\mathbb{Z}^g$$

that restrict to the identity on the 4-torsion.

To any $\Omega \in \mathcal{H}_g$ we associate the polarized abelian variety $(X_\Omega = \mathbb{C}^g/\Omega\mathbb{Z}^g \oplus 4\mathbb{Z}^g, H_\Omega)$, where $H_\Omega(v,w) = {}^tv(\operatorname{Im}\Omega)^{-1}\bar{w}$. Let $\mathcal{L}_\Omega$ be the line bundle with first Chern class H_Ω and of characteristic 0 with respect to the decomposition $\mathbb{C}^g = \Omega\mathbb{R}^g \oplus \mathbb{R}^g$. A basis of $\Gamma(X_\Omega, \mathcal{L}_\Omega)$ is given by the theta functions

$$\left\{ \theta\begin{bmatrix}d/4\\0\end{bmatrix}(v,\Omega) : d \in Repr(\mathbb{Z}^g/4\mathbb{Z}^g) \right\}.$$

David Mumford (in [Mum83]) and other authors associate to Ω the polarized abelian variety $(\mathbb{C}^g/\Omega\mathbb{Z}^g \oplus \mathbb{Z}^g, 4H_\Omega)$ instead, and as we have seen in Section 1.3.1,

$$\left\{\theta \begin{bmatrix} d/4 \\ 0 \end{bmatrix}(4v, 4\Omega) : d \in Repr(\mathbb{Z}^g/4\mathbb{Z}^g)\right\}$$

is a basis of $\Gamma(\mathbb{C}^g/\Omega\mathbb{Z}^g \oplus \mathbb{Z}^g, \mathcal{L}_\Omega^{\otimes 4})$. The only difference is that in our setup we "put the information of the type $4 \cdot I_g$ in the lattice", i.e. consider the lattice $\Omega\mathbb{Z}^g \oplus 4\mathbb{Z}^g$ with polarization H_Ω, while Mumford "puts the information of the type $4 \cdot I_g$ in the polarization", i.e. considers the lattice $\Omega\mathbb{Z}^g \oplus \mathbb{Z}^g$ with polarization $4H_\Omega$. But those constructions are essentially equivalent, and it is merely a matter of taste. Let $\Omega' := \frac{\Omega}{4}$ and let

$$f\colon X_\Omega = \mathbb{C}^g/\Omega\mathbb{Z}^g \oplus 4\mathbb{Z}^g \xrightarrow{\sim} \mathbb{C}^g/\Omega'\mathbb{Z}^g \oplus \mathbb{Z}^g$$

be the isomorphism induced by the linear isomorphism $\mathbb{C}^g \xrightarrow{\cdot\frac{1}{4}} \mathbb{C}^g$. The isomorphism $\rho_a(f^{-1})^*\colon \Gamma(X_\Omega, \mathcal{L}_\Omega) \xrightarrow{\sim} \Gamma(\mathbb{C}^g/\Omega'\mathbb{Z}^g \oplus \mathbb{Z}^g, \mathcal{L}_{\Omega'}^{\otimes 4})$ is given by

$$\rho_a(f^{-1})^*\theta \begin{bmatrix} d/4 \\ 0 \end{bmatrix}(v, \Omega) = \theta \begin{bmatrix} d/4 \\ 0 \end{bmatrix}(4v, \Omega) = \theta \begin{bmatrix} d/4 \\ 0 \end{bmatrix}(4v, 4\Omega').$$

We know that the theta null values $\left\{\theta \begin{bmatrix} d/4 \\ 0 \end{bmatrix}(0, \Omega)\right\}$ for $(X_\Omega, \mathcal{L}_\Omega)$ are invariant under the $G_4(4)_0$-action (up to a projective factor), hence so are the theta null values $\left\{\theta \begin{bmatrix} d/4 \\ 0 \end{bmatrix}(0, 4\Omega')\right\}$ for $(\mathbb{C}^g/\Omega'\mathbb{Z}^g \oplus \mathbb{Z}^g, \mathcal{L}_{\Omega'}^{\otimes 4})$. But for $M = \begin{pmatrix} A & 4B \\ C/4 & D \end{pmatrix} \in G_4(4)_0$, we have

$$M \cdot 4\Omega' = (A(4\Omega') + 4B)(C/4(4\Omega') + D)^{-1} = 4(A\Omega' + B)(C\Omega' + D)^{-1}.$$

Let us define

$$\Gamma_n := \left\{M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathbf{Sp}_{2g}(\mathbb{Z}) : M \equiv I_{2g} \mod n\right\}$$

and

$$\Gamma_{n,2n} := \left\{\begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \Gamma_n : (A\,{}^tB)_0 \equiv (C\,{}^tD)_0 \equiv 0 \mod 2n\right\}.$$

Then, Γ_n is a principal congruence subgroup of $\mathbf{Sp}_{2g}(\mathbb{Z})$ and $\Gamma_{n,2n}$ is a congruence subgroup, since it contains Γ_{2n}. Also, note that isomorphisms of the form $\mathbb{C}^g/\Omega_M\mathbb{Z}^g \oplus \mathbb{Z}^g \xrightarrow{\sim} \mathbb{C}^g/\Omega\mathbb{Z}^g \oplus \mathbb{Z}^g$, induced by some $M \in \Gamma_n$, restrict to the identity on the n-torsion.

Proposition 1.28. *Let $\Omega \in \mathcal{H}_g$ and let $(\mathbb{C}^g/\Omega\mathbb{Z}^g \oplus \mathbb{Z}^g, \mathcal{L}_\Omega^{\otimes 4})$ be a polarized abelian variety of type $4 \cdot I_g$. Fix an ordering $\{d_0, \ldots, d_{4^g-1}\}$ of $Repr(\mathbb{Z}^g/4\mathbb{Z}^g)$. Then, the projective point*

$$\left(\theta \begin{bmatrix} d_0/4 \\ 0 \end{bmatrix}(0, 4\Omega) : \cdots : \theta \begin{bmatrix} d_{4^g-1}/4 \\ 0 \end{bmatrix}(0, 4\Omega)\right) \in \mathbb{P}_{\mathbb{C}}^{4^g-1}$$

remains unchanged in the $\Gamma_{4,8}$-orbit of Ω.

Combining Proposition 1.28 and Theorem 1.27 gives the important result:

Theorem 1.29. *Fix an ordering $\{d_0, \ldots, d_{4^g-1}\}$ of $Repr(\mathbb{Z}^g/4\mathbb{Z}^g)$. Then,*

$$\psi'_{4\cdot I_g}\colon \mathcal{H}_g \to \mathbb{P}_{\mathbb{C}}^{4^g-1},\ \Omega \mapsto \left(\theta \begin{bmatrix} d_0/4 \\ 0 \end{bmatrix}(0, 4\Omega) : \cdots : \theta \begin{bmatrix} d_{4^g-1}/4 \\ 0 \end{bmatrix}(0, 4\Omega)\right)$$

induces an analytic embedding of the moduli space $\mathcal{H}_g/\Gamma_{4,8}$ into $\mathbb{P}_{\mathbb{C}}^{4^g-1}$.

Recall from Section 1.3.1 the level-(2,...,2) theta functions

$$\left\{\theta \begin{bmatrix} d_1/2 \\ d_2/2 \end{bmatrix} (2v, \Omega) : d_1, d_2 \in Repr(\mathbb{Z}^g/2\mathbb{Z}^g)\right\}.$$

They form another basis of $\Gamma(\mathbb{C}^g/\Omega\mathbb{Z}^g \oplus \mathbb{Z}^g, \mathcal{L}_\Omega^{\otimes 4})$ and hence, the projective point

$$\left(\theta \begin{bmatrix} d_1/2 \\ d_2/2 \end{bmatrix} (0, \Omega)\right)_{d_1,d_2 \in Repr(\mathbb{Z}^g/2\mathbb{Z}^g)} \in \mathbb{P}_{\mathbb{C}}^{4^g-1}$$

remains invariant under the $\Gamma_{4,8}$-action on $\mathcal{H}_g$ as well. Here, we suppose that an ordering of $Repr(\mathbb{Z}^g/2\mathbb{Z}^g) \times Repr(\mathbb{Z}^g/2\mathbb{Z}^g)$ is fixed. The resulting projective factor (i.e. the one that appears when replacing Ω by a $\Gamma_{4,8}$-equivalent Ω') is the same as for the projective point from Proposition 1.28. Applying Theorem 1.24 to the second and the fourth powers of the level-(2,...,2) theta functions, one can show that

$$\left(\theta \begin{bmatrix} d_1/2 \\ d_2/2 \end{bmatrix} (0, \Omega)^2\right)_{d_1,d_2 \in Repr(\mathbb{Z}^g/2\mathbb{Z}^g)}$$

remains invariant under the $\Gamma_{2,4}$-action on $\mathcal{H}_g$ and

$$\left(\theta \begin{bmatrix} d_1/2 \\ d_2/2 \end{bmatrix} (0, \Omega)^4\right)_{d_1,d_2 \in Repr(\mathbb{Z}^g/2\mathbb{Z}^g)}$$

remains invariant under the Γ_2-action on $\mathcal{H}_g$.

We can give a more concrete description/interpretation of this invariance in the case of a hyperelliptic curve C over $\mathbb{C}$. Let g be the genus of C, and suppose C is given by an affine plane model $y^2 = f(x)$, where f is a polynomial of degree $2g+1$. The 2-torsion subgroup of the Jacobian variety $\mathrm{Jac}(C)$ of C is entirely characterized by the Weierstrass points of the curve C. Hence, an ordering $\{a_1, \ldots, a_{2g+1}\}$ of the roots of f determines an ordering of $\mathrm{Jac}(C)[2]$. If $\mathrm{Jac}(C) = \mathbb{C}^g/\Lambda$, then any choice of a symplectic basis of Λ determines a period matrix $\Omega \in \mathcal{H}_g$ and an isomorphism (of principally polarized abelian varieties) $\mathrm{Jac}(C) \cong \mathbb{C}^g/\Omega\mathbb{Z}^g \oplus \mathbb{Z}^g =: X_\Omega$. The 2-torsion points of X_Ω can thus be expressed by the Weierstrass points of C, but the way to do so depends on the choice of the symplectic basis of Λ. How can we handle this ambiguity? A Γ_2-isomorphism $X_{\Omega_M} \xrightarrow{\sim} X_\Omega$, for some $M \in \Gamma_2$ (coming from a different choice of symplectic basis of Λ), restricts to the identity on the 2-torsion. Hence, our way to express the 2-torsion points of X_Ω in terms of the roots of f remains unchanged under such an isomorphism. On the other side, Thomae's formulae (Theorem 1.14) allow us to compute the fourth powers of the theta constants of X_Ω directly from the roots of f, i.e. directly from the 2-torsion points of X_Ω. By what we have said earlier, the fourth powers of the theta constants are invariant (up to a projective factor) under the Γ_2-action on $\mathcal{H}_g$. So, both the way of expressing the 2-torsion points in terms of the roots of f and the way of computing the theta constants from the roots of f are "Γ_2-invariant".

Conversely, for the reciprocal formulae (Theorem 1.15), we see that the right-hand side is $\Gamma_{2,4}$-invariant, whereas the left-hand side is computed from the 2-torsion of X_Ω. But $\Gamma_{2,4} \subset \Gamma_2$ leaves the 2-torsion invariant.

2 Abelian varieties over fields of positive characteristic

The goal of this section is to study embeddings of polarized abelian varieties over arbitrary fields into projective space by means of theta functions. As we have seen in the complex case, a decomposition of $\mathbb{C}^g$ plus a characteristic are sufficient to determine a basis of theta functions in a canonical way. The algebraic analogue to this data is called a *theta structure* and was first introduced by Mumford in [Mum66]. Fixing a polarized abelian variety together with a theta structure yields a basis of theta functions in a canonical way. Hence, if the line bundle is very ample, these canonical theta functions allow us to embed the abelian variety into projective space.

For this section we consider k a fixed algebraically closed field of positive characteristic p. For a further treatment of the subject we refer to [Mum66] and [Rob10].

2.1 The theta group and theta structures

Let X be an abelian variety of dimension g over the field k. The Picard group $\mathrm{Pic}(X)$ is the group of isomorphism classes of line bundles $\mathcal{L}$ on X equipped with the tensor product $\otimes$. The set of (isomorphism classes of) line bundles $\mathcal{L}$ on X such that $t_x^*\mathcal{L} \cong \mathcal{L}$ for all point $x \in X(k)$ is a subgroup of $\mathrm{Pic}(X)$ and is denoted by $\mathrm{Pic}^0(X)$.

Remark 2.1. In the complex case, Lemma 1.3 tells us that $t_x^*\mathcal{L} \cong \mathcal{L}$ for all $x \in X$ if and only if $H = c_1(\mathcal{L}) = 0$, so that our algebraic definition of $\mathrm{Pic}^0(X)$ coincides with the definition of $\mathrm{Pic}^0(X)$ being the kernel of $\mathrm{Pic}(X) \xrightarrow{c_1} \mathrm{NS}(X)$.

Two line bundles $\mathcal{L}_1$ and $\mathcal{L}_2$ on X are said to be *algebraically equivalent* if $\mathcal{L}_1 \otimes \mathcal{L}_2^{-1} \in \mathrm{Pic}^0(X)$. The tensor product respects algebraic equivalences and we define the *Néron-Severi group* $\mathrm{NS}(X)$ as the group of algebraic equivalence classes of line bundles on X. A *polarization* on X is an algebraic equivalence class of an ample line bundle $\mathcal{L}$ on X (see Section 1.2.2 for the definition of ample). By abuse of notation we will often call $\mathcal{L}$ itself a polarization.

Analogous to the complex case there exists an abelian variety $\widehat{X}$ over k, called the *dual abelian variety of* X, with the property that $\widehat{X}(k) \cong \mathrm{Pic}^0(X)$ (see [Mum70, §8]). To any $\mathcal{L} \in \mathrm{Pic}(X)$ we can associate a morphism

$$\phi_{\mathcal{L}} \colon X \to \widehat{X} \tag{2.1}$$

via the map

$$X(k) \to \mathrm{Pic}^0(X),\ x \mapsto t_x^*\mathcal{L} \otimes \mathcal{L}^{-1},$$

and $\phi_{\mathcal{L}}$ is a homomorphism by the Theorem of the Square (see [Mum70, §6, Cor. 4]). Define

$$K(\mathcal{L}) := \ker \phi_{\mathcal{L}} = \{x \in X(k) : t_x^*\mathcal{L} \cong \mathcal{L}\}.$$

It is easy to see that algebraically equivalent line bundles yield the same morphism $X \to \widehat{X}$ and hence, the same subgroup $K(\mathcal{L})$. It is well known that $\mathcal{L}$ is ample if and only if $K(\mathcal{L})$ is finite and $\dim_k \Gamma(X, \mathcal{L}^{\otimes n}) > 0$ for all $n \geq 1$. An ample line bundle $\mathcal{L}$ on X is called a *principal polarization* if the induced isogeny $\phi_{\mathcal{L}} \colon X \to \widehat{X}$ is an isomorphism.

From now on we will always suppose that $\mathcal{L}$ is ample. We call $\deg \mathcal{L} := \dim_k \Gamma(X, \mathcal{L})$ the *degree* of $\mathcal{L}$, and for all $n \geq 1$ we have $\dim_k \Gamma(X, \mathcal{L}^{\otimes n}) = \deg \mathcal{L} \cdot n^g$. Moreover, the morphism $\phi_{\mathcal{L}}$ is an isogeny of degree $\deg \phi_{\mathcal{L}} = (\deg \mathcal{L})^2$, and we will call it the *polarization isogeny associated to* $\mathcal{L}$. We call $\mathcal{L}$ an *ample line bundle of separable type* if $p = char(k) \not| \deg \mathcal{L}$. In this case $\phi_{\mathcal{L}}$ is a separable morphism, and thus we have

$$\#K(\mathcal{L}) = (\deg \mathcal{L})^2.$$

2.1.1 Mumford's theta group

From here on, we will always suppose that $\mathcal{L} \in \mathrm{Pic}(X)$ is an ample line bundle of separable type. We have seen that $K(\mathcal{L})$ is precisely the set of points $x \in X(k)$ for which the line bundles $t_x^*\mathcal{L}$ and $\mathcal{L}$ are isomorphic. But this isomorphism is not unique. As an example, composing it with an automorphism of $\mathcal{L}$ yields a different isomorphism. It was Mumford's great idea (in a series of papers [Mum66, Mum67a, Mum67b]) to study not only $K(\mathcal{L})$, but pairs of elements of $K(\mathcal{L})$ together with isomorphisms.

Definition 2.2. The Mumford theta group is

$$\mathcal{G}(\mathcal{L}) = \{(x, \phi_x) : x \in K(\mathcal{L}), \phi_x \colon \mathcal{L} \xrightarrow{\sim} t_x^*\mathcal{L}\},$$

under the group law: for $(x, \phi_x), (y, \phi_y) \in \mathcal{G}(\mathcal{L})$,

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

is an isomorphism $\mathcal{L} \xrightarrow{\sim} t_{x+y}^*\mathcal{L}$. Hence, we define

$$(x, \phi_x) \cdot (y, \phi_y) = (x + y, t_x^*\phi_y \circ \phi_x).$$

The neutral element is $(0, \mathrm{id}_{\mathcal{L}})$ and the inverse of (x, ϕ_x) under this group law is $(-x, t_{-x}^*\phi_x^{-1})$. The forgetful map $\mathcal{G}(\mathcal{L}) \xrightarrow{\rho_{\mathcal{G}(\mathcal{L})}} K(\mathcal{L})$, $(x, \phi_x) \mapsto x$ is surjective, with kernel the automorphisms of $\mathcal{L}$, i.e. multiplication by non-zero scalars. Hence, we have an exact sequence

$$0 \to k^\times \to \mathcal{G}(\mathcal{L}) \to K(\mathcal{L}) \to 0,$$

where $k^\times \to \mathcal{G}(\mathcal{L})$ is given by $a \mapsto (0, m_a)$, where m_a is the multiplication-by-a automorphism of $\mathcal{L}$.

If $\mathcal{L}$ and $\mathcal{L}'$ define the same polarization on X then by [Mum70, §8, Thm. 1] there exists $c \in X(k)$ such that $\mathcal{L}' \cong t_c^*\mathcal{L}$. Let $\psi \colon \mathcal{L}' \xrightarrow{\sim} t_c^*\mathcal{L}$ denote one such isomorphism. Then

$$\mathcal{G}(\mathcal{L}) \xrightarrow{\sim} \mathcal{G}(\mathcal{L}'),\ (x, \phi_x) \mapsto (x, t_x^*\psi^{-1} \circ t_c^*\phi_x \circ \psi),$$

where

$$\mathcal{L}' \xrightarrow{\psi} t_c^*\mathcal{L} \xrightarrow{t_c^*\phi_x} t_c^*(t_x^*\mathcal{L}) = t_x^*(t_c^*\mathcal{L}) \xrightarrow{t_x^*\psi^{-1}} t_x^*\mathcal{L}',$$

defines an isomorphism between the corresponding theta groups. Hence, we have isomorphic exact sequences

$$\begin{array}{ccccccccc}
0 & \longrightarrow & k^\times & \longrightarrow & \mathcal{G}(\mathcal{L}) & \longrightarrow & K(\mathcal{L}) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow & & \downarrow{\scriptstyle \mathrm{id}} & & \\
0 & \longrightarrow & k^\times & \longrightarrow & \mathcal{G}(\mathcal{L}') & \longrightarrow & K(\mathcal{L}') = K(\mathcal{L}) & \longrightarrow & 0.
\end{array}$$

The central exact sequence $0 \to k^\times \to \mathcal{G}(\mathcal{L}) \to K(\mathcal{L}) \to 0$ is non-split, since $\mathcal{G}(\mathcal{L})$ is a non-commutative group. Nevertheless, a central question when studying Mumford's theta group is: for what subgroups $K \subset K(\mathcal{L})$ does the projection $\rho_{\mathcal{G}(\mathcal{L})} \colon \mathcal{G}(\mathcal{L}) \to K(\mathcal{L})$ admit a section above K. Let us give an example where the splitting occurs, before addressing the general case in Lemma 2.8. Let $f \colon X \to Y$ be a separable isogeny between two abelian varieties, and let $\mathcal{M} \in \mathrm{Pic}(Y)$ be a line bundle on Y. By [Mum70,

§7, Thm. 4] you might want to replace Y by the isomorphic variety $X/\ker f$. Suppose moreover that there exists an isomorphism $\alpha\colon f^*\mathcal{M} \xrightarrow{\sim} \mathcal{L}$. Then for $x \in \ker f$ we have

$$\mathcal{L} \xrightarrow{\alpha^{-1}} f^*\mathcal{M} = (f \circ t_x)^*\mathcal{M} = t_x^*(f^*\mathcal{M}) \xrightarrow{t_x^*\alpha} t_x^*\mathcal{L},$$

which shows that

$$\ker f \subset K(\mathcal{L}).$$

But we can say more in this situation. Consider the map

$$\ker f \to \mathcal{G}(\mathcal{L}),\ x \mapsto (x, t_x^*\alpha \circ \alpha^{-1}), \tag{2.2}$$

which is injective, and it is not hard to see that this map does not depend on the choice of the isomorphism α. A quick verification shows that

$$t_{x+y}^*\alpha \circ \alpha^{-1} = t_x^*(t_y^*\alpha \circ \alpha^{-1}) \circ (t_x^*\alpha \circ \alpha^{-1}),$$

which means $\ker f \hookrightarrow \mathcal{G}(\mathcal{L})$ is a group morphism. Hence, we have a section of $\mathcal{G}(\mathcal{L}) \to K(\mathcal{L})$ above $\ker f$, or equivalently a subgroup $\widetilde{\ker f} \subset \mathcal{G}(\mathcal{L})$ isomorphic to $\ker f$ via $\rho_{\mathcal{G}(\mathcal{L})}$. Be aware that for arbitrary $K \subset K(\mathcal{L})$ there need not exist a lifting $\widetilde{K} \subset \mathcal{G}(\mathcal{L})$ of K into $\mathcal{G}(\mathcal{L})$ and hence, there need not exist a line bundle $\mathcal{M}$ on $Y = X/K$ such that $f^*\mathcal{M} \cong \mathcal{L}$, where $f\colon X \to X/K$ is the projection isogeny. As Grothendieck's descent theory tells us, the splitting of $\mathcal{G}(\mathcal{L}) \to K(\mathcal{L})$ above K is equivalent to the descent of the line bundle $\mathcal{L}$ under the projection $X \to X/K$. Before stating the result, let us define the following.

Definition 2.3. A level subgroup $\widetilde{K}$ of $\mathcal{G}(\mathcal{L})$ is a subgroup that is isomorphic to its image $K = \rho_{\mathcal{G}(\mathcal{L})}(\widetilde{K}) \subset K(\mathcal{L})$. Equivalently, $\widetilde{K}$ is a level subgroup if $k^\times \cap \widetilde{K} = \{0\}$.

A level subgroup $\widetilde{K}$ determines the subgroup $K \subset K(\mathcal{L})$, and we sometimes say that $\widetilde{K}$ is a level subgroup above K. Also, note that level subgroups are commutative. The main theorem about the descent of line bundles under isogenies is due to Grothendieck.

Theorem 2.4. *Let X be an abelian variety and let $\mathcal{L}$ be an ample line bundle of separable type on X. Let K be a (necessarily finite) subgroup of $K(\mathcal{L})$, and let $f\colon X \to Y = X/K$ be the associated separable isogeny. Then there is a 1-1 correspondence between pairs $(\mathcal{M}, \alpha)$, where $\mathcal{M}$ is a line bundle on Y and $\alpha\colon f^*\mathcal{M} \xrightarrow{\sim} \mathcal{L}$ an isomorphism, and level subgroups $\widetilde{K}$ above K. Moreover, the line bundle $\mathcal{M}$ is ample and of separable type.*

Proof. For the equivalence between the existence of pairs $(\mathcal{M}, \alpha)$ and level subgroups $\widetilde{K}$, we refer to [Gro60, §8, Thm. 1.1]. The fact that $\mathcal{M}$ is ample is proven in [Gro61, §3, Thm. 2.6.2]. We know that the following diagram is commutative

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ {\scriptstyle \phi_{\mathcal{L}}}\downarrow & & \downarrow{\scriptstyle \phi_{\mathcal{M}}} \\ \widehat{X} & \xleftarrow[\widehat{f}]{} & \widehat{Y}, \end{array}$$

and hence,

$$\deg \phi_{\mathcal{L}} = (\deg f)^2 \cdot \deg \phi_{\mathcal{M}}.$$

It follows that

$$\deg \mathcal{L} = \underbrace{\deg f}_{\#K} \cdot \deg \mathcal{M}. \tag{2.3}$$

But $\mathcal{L}$ is of separable type and hence, $p = char(k) \nmid \deg \mathcal{M}$. □

A simplified version in the complex case is taken care of by Proposition 1.5.

Let us see if we can relate $\mathcal{G}(\mathcal{M})$ and $\mathcal{G}(\mathcal{L})$ in the above situation. The first observation is that f does not send $K(\mathcal{L})$ to $K(\mathcal{M})$, simply by cardinality reason. Yet, the inverse image behaves nicer in this situation.

Proposition 2.5. *We have $f^{-1}(K(\mathcal{M})) \subset K(\mathcal{L})$.*

Proof. Let α as above be the isomorphism $\alpha\colon f^*\mathcal{M} \xrightarrow{\sim} \mathcal{L}$. Let $y \in K(\mathcal{M})$, so that there exists an isomorphism $\psi_y\colon \mathcal{M} \xrightarrow{\sim} t_y^*\mathcal{M}$, and let $x \in X(k)$ be such that $f(x) = y$. Then we have

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

hence $x \in K(\mathcal{L})$ and $t_x^*\alpha \circ f^*\psi_y \circ \alpha^{-1}$ is an isomorphism $\mathcal{L} \xrightarrow{\sim} t_x^*\mathcal{L}$. □

Denote by

$$\mathcal{G}(\mathcal{L})^* := \{(x, \phi_x) \in \mathcal{G}(\mathcal{L}) : f(x) \in K(\mathcal{M})\}$$

the elements of $\mathcal{G}(\mathcal{L})$ above $f^{-1}(K(\mathcal{M}))$. Then there exists a map

$$\alpha_f\colon \mathcal{G}(\mathcal{L})^* \to \mathcal{G}(\mathcal{M}), \tag{2.4}$$

given as follows : let $(x, \phi_x) \in \mathcal{G}(\mathcal{L})^*$, where $x \in f^{-1}(K(\mathcal{M}))$ and $\phi_x\colon \mathcal{L} \xrightarrow{\sim} t_x^*\mathcal{L}$. Let $y = f(x)$ and let $\psi_y\colon \mathcal{M} \xrightarrow{\sim} t_y^*\mathcal{M}$ be any isomorphism from $\mathcal{M}$ to $t_y^*\mathcal{M}$. Then ϕ_x and $t_x^*\alpha \circ f^*\psi_y \circ \alpha^{-1}$ differ by an automorphism of $\mathcal{L}$, which is the multiplication-by-a map m_a, for some $a \in k^\times$. Sending

$$\alpha_f\colon (x, \phi_x) \in \mathcal{G}(\mathcal{L})^* \mapsto (y, \psi_y \circ m_a) \in \mathcal{G}(\mathcal{M}),$$

where now m_a denotes the multiplication-by-a map on $\mathcal{M}$, is a well defined map. It is not hard to see that α_f is a surjective group homomorphism, and we have the following commutative diagram

$$\begin{array}{ccc} \mathcal{G}(\mathcal{L})^* & \xrightarrow{\alpha_f} & \mathcal{G}(\mathcal{M}) \\ {\scriptstyle \rho_{\mathcal{G}(\mathcal{L})}}\downarrow & & \downarrow{\scriptstyle \rho_{\mathcal{G}(\mathcal{M})}} \\ f^{-1}(K(\mathcal{M})) & \xrightarrow[f]{} & K(\mathcal{M}). \end{array}$$

Proposition 2.6. *Given the descent datum $(\mathcal{M}, \alpha)$, or equivalently the corresponding level subgroup $\widetilde{K}$ above $K := \ker f$, the surjection α_f induces an isomorphism*

$$\mathcal{G}(\mathcal{L})^*/\widetilde{K} \xrightarrow{\sim} \mathcal{G}(\mathcal{M}).$$

Proof. We only need to show that $\ker \alpha_f = \widetilde{K}$. The isomorphism $\alpha\colon f^*\mathcal{M} \xrightarrow{\sim} \mathcal{L}$ is determined by the property to make

$$\begin{array}{ccc} \mathcal{L} & \xrightarrow{\phi_w} & t_w^*\mathcal{L} \\ & {\scriptstyle \alpha^{-1}}\searrow \quad \nearrow{\scriptstyle t_w^*\alpha} & \\ & f^*\mathcal{M} = t_w^*(f^*\mathcal{M}) & \end{array}$$

a commutative diagram for all $(w, \phi_w) \in \widetilde{K}$. But $(x, \phi_x) \in \mathcal{G}(\mathcal{L})^*$ is in the kernel of α_f if and only if $x \in \ker f$ and ϕ_x arises as the composite $t_x^*\alpha \circ f^* \mathrm{id}_{\mathcal{M}} \circ \alpha^{-1} = t_x^*\alpha \circ \alpha^{-1}$, which means that $(x, \phi_x) \in \widetilde{K}$. □

Moreover, see [Mum66, §1, Prop. 2], the subgroup $\mathcal{G}(\mathcal{L})^*$ equals the centralizer $\mathcal{Z}(\widetilde{K})$ of $\widetilde{K}$ in $\mathcal{G}(\mathcal{L})$, where $K = \ker f$. Hence, we have an isomorphism

$$\mathcal{Z}(\widetilde{K})/\widetilde{K} \xrightarrow{\sim} \mathcal{G}(\mathcal{M}),$$

induced by α_f.

As mentioned earlier, the property of admitting a level subgroup need not be true for all subgroups $K \subset K(\mathcal{L})$. In fact, we would like to give a criterion for the existence of a level subgroup without involving any descent theory of line bundles. It turns out that $K(\mathcal{L})$ admits a symplectic pairing and that the subgroups $K \subset K(\mathcal{L})$ that do admit a level subgroup are precisely the isotropic subgroups of $K(\mathcal{L})$.

For $x, y \in K(\mathcal{L})$, let $\widetilde{x}, \widetilde{y} \in \mathcal{G}(\mathcal{L})$ be arbitrary lifts of x and y respectively. Define the commutator pairing

$$e_{\mathcal{L}}(x, y) := \widetilde{x}\widetilde{y}\widetilde{x}^{-1}\widetilde{y}^{-1}.$$

Lifts of elements of $K(\mathcal{L})$ are only defined up to scalars (i.e. up to elements of the form $(0, m_a)$ for $a \in k^\times$), but since $k^\times$ is contained in the center of $\mathcal{G}(\mathcal{L})$ the form $e_{\mathcal{L}}$ is well defined. Moreover, $\widetilde{x}\widetilde{y}\widetilde{x}^{-1}\widetilde{y}^{-1}$ being in the kernel of $\mathcal{G}(\mathcal{L}) \xrightarrow{\rho_{\mathcal{G}(\mathcal{L})}} K(\mathcal{L})$, we can see $e_{\mathcal{L}}(x, y)$ as an element of $k^\times$. It is immediate that $e_{\mathcal{L}}$ is an alternating bilinear pairing on $K(\mathcal{L})$. According to [Mum66, §1, Thm. 1], the center of $\mathcal{G}(\mathcal{L})$ is actually equal to $k^\times$, or equivalently the form $e_{\mathcal{L}}$ is non-degenerate. We have:

Proposition 2.7. *$(K(\mathcal{L}), e_{\mathcal{L}})$ is a symplectic space.*

As for any group admitting a symplectic form, there exist subgroups $K(\mathcal{L})_1$ and $K(\mathcal{L})_2$ of $K(\mathcal{L})$, both isotropic for $e_{\mathcal{L}}$, forming a *symplectic decomposition*

$$K(\mathcal{L}) = K(\mathcal{L})_1 \oplus K(\mathcal{L})_2$$

of $K(\mathcal{L})$. Via $e_{\mathcal{L}}$ we have the identification $K(\mathcal{L})_2 \cong \mathrm{Hom}(K(\mathcal{L})_1, k^\times)$, and we call $K(\mathcal{L})_i$ for $i = 1, 2$ a *maximal isotropic subgroup* of $K(\mathcal{L})$. Now the existence result for level subgroups can be rephrased as follows.

Lemma 2.8. *A subgroup $K \subset K(\mathcal{L})$ admits a level subgroup if and only if it is isotropic for $e_{\mathcal{L}}$.*

Proof. Let $\widetilde{K}$ be a level subgroup above K. For $x, y \in K$ we can choose lifts $\widetilde{x}, \widetilde{y}$ in $\widetilde{K}$. But $\widetilde{K}$ is commutative, hence $e_{\mathcal{L}}(x, y) = 1$. Conversely, let us see how to determine a level subgroup above an isotropic subgroup K. Let $x \in K$ and suppose x is of order l. Let $\widetilde{x} \in \mathcal{G}(\mathcal{L})$ be any lift of x. Then $\widetilde{x}^l$ is in the kernel of $\rho_{\mathcal{G}(\mathcal{L})}$ and is therefore a scalar. Let a be an lth root of $\widetilde{x}^l$, so that the element $\widetilde{x}/a$ above x is of order l. Decompose K as a product of cyclic groups and repeat this lifting procedure for each of the generators. Since $e_{\mathcal{L}}$ is trivial on K, the lifts of these generators commute with each other and hence, generate a subgroup of $\mathcal{G}(\mathcal{L})$ isomorphic to K. □

Hence, if $(X, \mathcal{L})$ is a polarized abelian variety and $K \subset K(\mathcal{L})$ is an isotropic subgroup for $e_{\mathcal{L}}$, then there exists an ample line bundle $\mathcal{M}$ on $Y = X/K$ that satisfies $f^*\mathcal{M} \cong \mathcal{L}$, where $f\colon X \to Y$ is the projection isogeny. Moreover, the line bundle $\mathcal{M}$ is unique up to algebraic equivalence.

2.1.2 The Heisenberg group and theta structures

Let $\mathcal{L}$ be an ample line bundle of separable type on X. If $K(\mathcal{L}) = K(\mathcal{L})_1 \oplus K(\mathcal{L})_2$ is a symplectic decomposition of $K(\mathcal{L})$ with respect to the commutator pairing $e_{\mathcal{L}}$, and if $\delta_1 \mid \delta_2 \mid \cdots \mid \delta_g$ are the elementary divisors of $K(\mathcal{L})_i$ for $i = 1, 2$, then as abstract groups we have the isomorphisms

$$K(\mathcal{L})_1 \cong K(\mathcal{L})_2 \cong \mathbb{Z}(\delta),$$

where $\delta = (\delta_1, \ldots, \delta_g)$ and where we write $\mathbb{Z}(\delta) := \bigoplus_{i=1}^{g} \mathbb{Z}/\delta_i\mathbb{Z}$. We say that $\mathcal{L}$ (or the polarization it defines) is of *type* $\delta = (\delta_1, \ldots, \delta_g)$. Note that $\mathcal{L}$ is a principal polarization if and only if it is of type $(1, \ldots, 1)$.

Given a tuple $\delta = (\delta_1, \ldots, \delta_g) \in \mathbb{Z}^g$ with $\delta_1 \mid \cdots \mid \delta_g$, let

$$K(\delta) := \mathbb{Z}(\delta) \oplus \widehat{\mathbb{Z}}(\delta),$$

where $\widehat{\mathbb{Z}}(\delta) = \mathrm{Hom}(\mathbb{Z}(\delta), k^\times)$. Then $K(\delta)$ is equipped with the standard symplectic pairing e_δ coming from duality, i.e.

$$e_\delta((x_1, y_1), (x_2, y_2)) = \frac{y_2(x_1)}{y_1(x_2)} \in k^\times.$$

Definition 2.9. The Heisenberg group $\mathcal{H}(\delta)$ is the group with underlying set $k^\times \times K(\delta)$ and with group law

$$(a_1, x_1, y_1) \cdot (a_2, x_2, y_2) = (a_1 a_2 y_2(x_1), x_1 + x_2, y_1 + y_2),$$

for all $a_1, a_2 \in k^\times, x_1, x_2 \in \mathbb{Z}(\delta)$ and $y_1, y_2 \in \widehat{\mathbb{Z}}(\delta)$.

The Heisenberg group is a central extension of $K(\delta)$ by $k^\times$, i.e. it fits into the central exact sequence

$$0 \to k^\times \to \mathcal{H}(\delta) \to K(\delta) \to 0,$$

where $a \in k^\times \mapsto (a, 0, 0) \in \mathcal{H}(\delta)$ and $\mathcal{H}(\delta) \to K(\delta)$ is the projection onto $K(\delta)$. The inverse of $(a, x, y) \in \mathcal{H}(\delta)$ is given by

$$(a, x, y)^{-1} = (a^{-1} y(x), -x, -y),$$

and a quick computation shows that $e_\delta((x_1, y_1), (x_2, y_2))$ is the commutator of any lifts of (x_1, y_1) and (x_2, y_2) to $\mathcal{H}(\delta)$ respectively. The elements of $\mathrm{Aut}_{k^\times}(\mathcal{H}(\delta))$, i.e. the automorphisms of $\mathcal{H}(\delta)$ that restrict to the identity on $k^\times$, are called *metaplectic* automorphisms.

The most important concept Mumford introduced in [Mum66] is the link between the somehow hard to interpret theta group associated to an ample line bundle and the more abstract and canonical Heisenberg group.

Definition 2.10. A *theta structure* $\Theta_{\mathcal{L}}$ of type δ is an isomorphism of central extensions

$$\Theta_{\mathcal{L}} \colon \mathcal{H}(\delta) \xrightarrow{\sim} \mathcal{G}(\mathcal{L}),$$

which is the identity on $k^\times$.

When a line bundle $\mathcal{L}$ is fixed and hence, when there is no ambiguity about the type, we will call $\Theta_{\mathcal{L}}$ simply a theta structure. A theta structure $\Theta_{\mathcal{L}}\colon \mathcal{H}(\delta) \xrightarrow{\sim} \mathcal{G}(\mathcal{L})$ induces an isomorphism $\overline{\Theta}_{\mathcal{L}}\colon K(\delta) \xrightarrow{\sim} K(\mathcal{L})$, and the following diagram commutes

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

Since both the pairings on $K(\delta)$ and on $K(\mathcal{L})$ are given by the respective commutators, and since $\Theta_{\mathcal{L}}$ pulls back commutators, $\overline{\Theta}_{\mathcal{L}}$ is actually a symplectic isomorphism.

Once a theta structure $\Theta_{\mathcal{L}}\colon \mathcal{H}(\delta) \xrightarrow{\sim} \mathcal{G}(\mathcal{L})$ is fixed we obtain a symplectic decomposition of $K(\mathcal{L})$ as

$$K(\mathcal{L}) = \overline{\Theta}_{\mathcal{L}}(\mathbb{Z}(\delta)) \oplus \overline{\Theta}_{\mathcal{L}}(\widehat{\mathbb{Z}}(\delta)),$$

and we call it the *induced symplectic decomposition*. Denote by

$$K(\mathcal{L})_1 := \overline{\Theta}_{\mathcal{L}}(\mathbb{Z}(\delta)) \text{ and } K(\mathcal{L})_2 := \overline{\Theta}_{\mathcal{L}}(\widehat{\mathbb{Z}}(\delta))$$

the induced maximal isotropic subgroups of $K(\mathcal{L})$. But there is actually more information contained in a theta structure. There is a canonical map (of sets) $s_\delta\colon K(\delta) \to \mathcal{H}(\delta)$ given by $(x, y) \mapsto (1, x, y)$, and it becomes a morphism of groups when restricted to any isotropic subgroup of $K(\delta)$. Then, via the theta structure $\Theta_{\mathcal{L}}$, the section s_δ induces a section

$$s_{K(\mathcal{L})}\colon K(\mathcal{L}) \to \mathcal{G}(\mathcal{L}) \tag{2.5}$$

of $\rho_{\mathcal{G}(\mathcal{L})}$. The two subgroups $\mathbb{Z}(\delta)$ and $\widehat{\mathbb{Z}}(\delta)$ of $K(\delta)$ are isotropic, hence restricting the section $s_{K(\mathcal{L})}$ to $K(\mathcal{L})_1$ and $K(\mathcal{L})_2$ yields two group sections

$$s_{K(\mathcal{L})_1}\colon K(\mathcal{L})_1 \to \mathcal{G}(\mathcal{L}) \text{ and } s_{K(\mathcal{L})_2}\colon K(\mathcal{L})_2 \to \mathcal{G}(\mathcal{L}).$$

We denote by

$$\widetilde{K}(\mathcal{L})_i := s_{K(\mathcal{L})_i}(K(\mathcal{L})_i)$$

the corresponding level subgroup, for $i = 1, 2$. Note that the sections $s_{K(\mathcal{L})_1}$ and $s_{K(\mathcal{L})_2}$ determine the section $s_{K(\mathcal{L})}$, since for any $z \in K(\mathcal{L})$, written $z = z_1 + z_2$ with $z_i \in K(\mathcal{L})_i$, we have

$$s_{K(\mathcal{L})}(z) = s_{K(\mathcal{L})_2}(z_2) \cdot s_{K(\mathcal{L})_1}(z_1).$$

Proposition 2.11. *A theta structure $\Theta_{\mathcal{L}}\colon \mathcal{H}(\delta) \xrightarrow{\sim} \mathcal{G}(\mathcal{L})$ induces a symplectic isomorphism $\overline{\Theta}_{\mathcal{L}}\colon K(\delta) \xrightarrow{\sim} K(\mathcal{L})$ and level subgroups above the induced maximal isotropic subgroups of $K(\mathcal{L})$. Conversely, any symplectic isomorphism $\overline{\Theta}_{\mathcal{L}}\colon K(\delta) \xrightarrow{\sim} K(\mathcal{L})$ together with group sections of $\rho_{\mathcal{G}(\mathcal{L})}$ above $\overline{\Theta}_{\mathcal{L}}(\mathbb{Z}(\delta))$ and $\overline{\Theta}_{\mathcal{L}}(\widehat{\mathbb{Z}}(\delta))$ induces a theta structure $\Theta_{\mathcal{L}}\colon \mathcal{H}(\delta) \xrightarrow{\sim} \mathcal{G}(\mathcal{L})$ in a unique way.*

We have seen that in the complex case, a decomposition of $\mathbb{C}^g$ into maximal isotropic subspaces and a characteristic c of $\mathcal{L}$ with respect to this decomposition are sufficient to obtain a basis of theta functions in a canonical way. And, provided $\mathcal{L}$ satisfies the condition of Lefschetz's Theorem 1.11, the theta functions can be considered as projective coordinates on the abelian variety. We will show in the next section that, given a polarized abelian variety $(X, \mathcal{L})$, a theta structure $\Theta_{\mathcal{L}}$ is the right information to add in order to obtain theta functions on X in a canonical way.

2.2 Theta functions

For this section we assume that $\mathcal{L}$ is a very ample line bundle of separable type δ on X, so that there exists a canonical embedding $X \hookrightarrow \mathbb{P}(\Gamma(X,\mathcal{L}))$. A choice of a k-basis of $\Gamma(X,\mathcal{L})$ then induces an isomorphism $\mathbb{P}(\Gamma(X,\mathcal{L})) \xrightarrow{\sim} \mathbb{P}_k^{d-1}$, where $d = \deg \mathcal{L}$, and we obtain an embedding

$$X \hookrightarrow \mathbb{P}_k^{d-1}.$$

A different choice of basis results in a $\mathbf{PGL}_d(k)$-action on $\mathbb{P}_k^{d-1}$. In order to fix one embedding we need to fix canonical coordinates on X (i.e. a canonical basis for $\Gamma(X,\mathcal{L})$). This choice will come precisely from the choice of a theta structure. Once we have fixed a theta structure $\Theta_{\mathcal{L}}$ on $(X,\mathcal{L})$, we get canonical theta functions $\{\theta_i^{\Theta_{\mathcal{L}}} : i \in \mathbb{Z}(\delta)\}$ forming a basis for the space of global sections $\Gamma(X,\mathcal{L})$. We will get this canonical basis via the representation theory of the Heisenberg group $\mathcal{H}(\delta)$.

2.2.1 The Schrödinger representation

Let $V(\delta)$ be the vector space of k-valued functions on $\mathbb{Z}(\delta)$. It is well known that the $\mathcal{H}(\delta)$-action on $V(\delta)$ given by

$$((a,x,y)\cdot f)(u) = ae_\delta((u,0),(0,y))f(u+x) = ay(u)f(u+x), \tag{2.6}$$

for $(a,x,y) \in \mathcal{H}(\delta)$, $f \in V(\delta)$ and $u \in \mathbb{Z}(\delta)$, is an irreducible representation, called the *Schrödinger representation*. We can easily see that $k^\times \hookrightarrow \mathcal{H}(\delta)$ acts by its natural character. As the next result shows, this representation is unique.

Theorem 2.12. *$V(\delta)$ is the unique irreducible representation of $\mathcal{H}(\delta)$ where $k^\times$ acts by its natural character. Let V be any representation of $\mathcal{H}(\delta)$ where $k^\times$ acts in this way. Let $\widetilde{K} \subset \mathcal{H}(\delta)$ be any maximal level subgroup (a level subgroup above a maximal isotropic subgroup of $K(\delta)$), and let $r = \dim_k V^{\widetilde{K}}$, where $V^{\widetilde{K}}$ is the subspace of $\widetilde{K}$-invariants. Then,*

$$V \cong \bigoplus_{i=1}^{r} V(\delta).$$

For a proof we refer to [Mum66, Prop.2]. The Mumford theta group $\mathcal{G}(\mathcal{L})$ acts on the space $\Gamma(X,\mathcal{L})$, where the action is given by

$$(x,\phi_x)\cdot s = t_{-x}^*(\phi_x \circ s).$$

Note that $t_{-x}^*(\phi_x \circ s)$ is indeed an element of $\Gamma(X,\mathcal{L})$, since the following diagram commutes

$$\begin{array}{ccc} t_{-x}^*(t_x^*\mathcal{L}) = \mathcal{L} & \longrightarrow & t_x^*\mathcal{L} \\ {\scriptstyle t_{-x}^*(\phi_x\circ s)}\uparrow & & \uparrow{\scriptstyle \phi_x\circ s} \\ X & \xrightarrow[t_{-x}]{} & X. \end{array}$$

Roughly speaking, we can say that the element (x,ϕ_x) acts on s by the translate t_{-x} plus some correcting factor. A scalar $a \in k^\times$ acts by $(0,m_a)\cdot s = m_a \circ s$, and as the following result shows, this representation is irreducible.

Proposition 2.13. *If $\mathcal{L}$ is an ample line bundle of separable type, then $\Gamma(X,\mathcal{L})$ is an irreducible $\mathcal{G}(\mathcal{L})$-representation.*

Proof. Let $K \subset K(\mathcal{L})$ be a maximal isotropic subgroup for $e_{\mathcal{L}}$, and let $\widetilde{K} \subset \mathcal{G}(\mathcal{L})$ be any level subgroup above K. Consider the isogeny $f\colon X \to X/K$, and let $(\mathcal{M}, \alpha)$ be the descent datum associated to $\widetilde{K}$, i.e. $\mathcal{M}$ is an ample line bundle on X/K and α is an isomorphism $\alpha\colon f^*\mathcal{M} \xrightarrow{\sim} \mathcal{L}$. By maximality of K we have that $\#K = \deg \mathcal{L}$. Thus, $\mathcal{M}$ is of degree 1, which means $\dim_k \Gamma(X/K, \mathcal{M}) = 1$. But f^* maps the sections of $\mathcal{M}$ onto the $\widetilde{K}$-invariant sections of $\mathcal{L}$, i.e. $\dim_k \Gamma(X, \mathcal{L})^{\widetilde{K}} = 1$. □

Let $\Theta_{\mathcal{L}}\colon \mathcal{H}(\delta) \xrightarrow{\sim} \mathcal{G}(\mathcal{L})$ be a fixed theta structure. We can see $\Gamma(X, \mathcal{L})$ as a $\mathcal{H}(\delta)$-representation via $\Theta_{\mathcal{L}}$, and by Theorem 2.12 and Proposition 2.13, the representations $V(\delta)$ and $\Gamma(X, \mathcal{L})$ are isomorphic. Thus there exists a unique (up to a scalar multiple) $\mathcal{H}(\delta)$-equivariant isomorphism $\varphi\colon V(\delta) \to \Gamma(X, \mathcal{L})$. The space $V(\delta)$ has a canonical basis given by the Kronecker delta functions $\{\delta_i : i \in \mathbb{Z}(\delta)\}$,

$$j \in \mathbb{Z}(\delta) \mapsto \delta_i(j) = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{otherwise.} \end{cases}$$

Composing with the isomorphism φ yields a basis for $\Gamma(X, \mathcal{L})$

$$\left\{\theta_i^{\Theta_{\mathcal{L}}} := \varphi(\delta_i) \mid i \in \mathbb{Z}(\delta)\right\}. \tag{2.7}$$

Hence, fixing a theta structure on $(X, \mathcal{L})$ yields a unique (up to a scalar multiple) basis for $\Gamma(X, \mathcal{L})$. Fixing once and for all an ordering $\{i_0, \ldots, i_{d-1}\}$ of $\mathbb{Z}(\delta)$, where $d = \deg \mathcal{L} = \#\mathbb{Z}(\delta)$, we get a projective embedding

$$X \hookrightarrow \mathbb{P}_k^{d-1},\ x \mapsto (\theta_{i_0}^{\Theta_{\mathcal{L}}}(x) : \cdots : \theta_{i_{d-1}}^{\Theta_{\mathcal{L}}}(x)).$$

Notation 2.14. Since we will keep the ordering of the elements of $\mathbb{Z}(\delta)$ fixed, we will subsequently write the embedding as $x \mapsto (\theta_i^{\Theta_{\mathcal{L}}}(x))_{i \in \mathbb{Z}(\delta)}$. Moreover, via the symplectic isomorphism $\overline{\Theta}_{\mathcal{L}}$, we may consider indexing the theta functions by $K(\mathcal{L})_1$, i.e. consider the embedding

$$x \mapsto (\theta_i^{\Theta_{\mathcal{L}}}(x))_{i \in K(\mathcal{L})_1}.$$

Definition 2.15. The functions $\{\theta_i^{\Theta_{\mathcal{L}}} : i \in K(\mathcal{L})_1\}$ are called theta coordinates. Moreover, we call

$$(\theta_i^{\Theta_{\mathcal{L}}}(0))_{i \in K(\mathcal{L})_1}$$

the (projective) theta null point associated to $(X, \mathcal{L}, \Theta_{\mathcal{L}})$.

Let us describe the action of the theta group $\mathcal{G}(\mathcal{L})$ on the theta coordinates explicitly, using the Schrödinger representation (2.6). Let $(z, \phi_z) \in \mathcal{G}(\mathcal{L})$ and let $(a, x, y) = \Theta_{\mathcal{L}}^{-1}((z, \phi_z)) \in \mathcal{H}(\delta)$. For $i \in \mathbb{Z}(\delta)$ we will denote the corresponding $\overline{\Theta}_{\mathcal{L}}(i) \in K(\mathcal{L})_1$ by i as well, and it will be clear from the context if we talk about an element of $\mathbb{Z}(\delta)$ or an element of $K(\mathcal{L})_1$. First, observe that

$$((a, x, y) \cdot \delta_i)(u) = ay(u)\delta_i(u + x) = ay(u)\delta_{i-x}(u) = ay(i - x)\delta_{i-x}(u).$$

Moreover,

$$y(i - x) = e_\delta((i - x, 0), (0, y)) = e_{\mathcal{L}}(i - z_1, z_2),$$

where $z = z_1 + z_2$ with respect to the decomposition $K(\mathcal{L}) = K(\mathcal{L})_1 \oplus K(\mathcal{L})_2$ induced by the theta structure $\Theta_{\mathcal{L}}$. Finally, the action of the Mumford theta group on the theta coordinates is given by

$$(z,\phi_z)\cdot\theta_i^{\Theta_{\mathcal{L}}} = \varphi((a,x,y)\cdot\delta_i) = \varphi(ay(i-x)\delta_{i-x})$$
$$= ae_{\mathcal{L}}(i-z_1,z_2)\theta_{i-z_1}^{\Theta_{\mathcal{L}}}.$$

As we have said before, the action of (z,ϕ_z) on $\Gamma(X,\mathcal{L})$ can roughly be seen as an action above translation by $-z$. To be more precise, for any point $x\in X(k)$ with projective coordinates $(\theta_i^{\Theta_{\mathcal{L}}}(x))_{i\in K(\mathcal{L})_1}$, the point $x-z$ has projective coordinates

$$x-z\mapsto(e_{\mathcal{L}}(i-z_1,z_2)\theta_{i-z_1}^{\Theta_{\mathcal{L}}}(x))_{i\in K(\mathcal{L})_1}.$$

To make sense of this, the ith coordinate of $x-z$ is given by the $(i-z_1)$th coordinate of x times some factor. In particular, translates of x by $K(\mathcal{L})_1$ result in permutations of the theta coordinates, while translates of x by $K(\mathcal{L})_2$ result in dilatations of the theta coordinates.

Remark 2.16. From the above it becomes clear that, given the projective theta coordinates of some point $x\in X(k)$, and given any $z\in K(\mathcal{L})$, we can compute the projective theta coordinates of the point $x-z$ using the (z,ϕ_z)-action on the coordinates of x, where $(z,\phi_z)\in\mathcal{G}(\mathcal{L})$ is any lift of z.

2.2.2 Affine theta coordinates

Theta functions are global sections of ample line bundles, and as such they are not well defined functions with values in k. This is why they yield projective coordinates only. Yet, when we want to compute isogenies, we will have to evaluate and manipulate theta functions individually, and we can only do this by considering them as functions taking values in k. Instead of working with a projective point of theta functions evaluated at $x\in X(k)$, we will have to fix an affine lift of it and work with the "affine theta coordinates". This, however, will turn out to be very delicate since in many applications we need those affine lifts to be "compatible" in a certain sense, and it is not easy to fix compatible affine lifts.

Let $(X,\mathcal{L},\Theta_{\mathcal{L}})$ be a polarized abelian variety with theta structure. Suppose that $\mathcal{L}$ is very ample and of separable type δ. Let

$$\left\{\theta_i^{\Theta_{\mathcal{L}}} : i\in K(\mathcal{L})_1\right\}$$

be a basis of theta functions as in (2.7), and suppose an ordering of $\mathbb{Z}(\delta)$ (which determines an ordering of $K(\mathcal{L})_1$ via $\overline{\Theta}_{\mathcal{L}}$) is fixed. This yields the embedding

$$X\hookrightarrow\mathbb{P}_k^{d-1},\ x\mapsto(\theta_i^{\Theta_{\mathcal{L}}}(x))_{i\in K(\mathcal{L})_1},$$

where $d=\deg\mathcal{L}$. Let $p\colon\mathbb{A}_k^d\setminus\{0\}\to\mathbb{P}_k^{d-1}$ be the natural projection map and consider the affine cone

$$\widetilde{X}:=p^{-1}(X),$$

where we view X as a subset of $\mathbb{P}_k^{d-1}$ via the above embedding.

Definition 2.17. For $x\in X(k)$ we denote by $\widetilde{x}\in\widetilde{X}$ an affine lift of $(\theta_i^{\Theta_{\mathcal{L}}}(x))_{i\in K(\mathcal{L})_1}$. We denote by $\theta_i^{\Theta_{\mathcal{L}}}(\widetilde{x})$ the ith coordinate of $\widetilde{x}$ and we call

$$\left\{\theta_i^{\Theta_{\mathcal{L}}}(\widetilde{x}) : i\in K(\mathcal{L})_1\right\}$$

the affine theta coordinates of x (for the fixed lift).

The main difficulty when working with affine coordinates is that there is no natural way to define a section of $\widetilde{X} \to X$. Even when fixing a lift $\widetilde{x}$ of some $x \in X(k)$, there is no general way this would determine a lift of an arbitrary $y \in X(k)$. However, it is true that for some subsets of X, fixing one affine lift determines lifts for the whole subset. This is closely related to Remark 2.16 of the previous section.

Proposition 2.18. *Let $x \in X(k)$ with fixed affine lift $\widetilde{x} = (\theta_i^{\Theta_\mathcal{L}}(\widetilde{x}))_{i \in K(\mathcal{L})_1}$. Then, for every $z \in K(\mathcal{L})$, the coordinates*

$$\theta_i^{\Theta_\mathcal{L}}(\widetilde{x+z}) := e_\mathcal{L}(i+z_1, -z_2)\theta_{i+z_1}^{\Theta_\mathcal{L}}(\widetilde{x}), \text{ for all } i \in K(\mathcal{L})_1,$$

are affine theta coordinates for an affine lift of $x+z$, that we denote by $\widetilde{x+z}$. Here, $z = z_1 + z_2$ with respect to the decomposition $K(\mathcal{L}) = K(\mathcal{L})_1 \oplus K(\mathcal{L})_2$ induced by $\Theta_\mathcal{L}$.

Proof. This can be seen when acting on $\theta_i^{\Theta_\mathcal{L}}$ by $s_{K(\mathcal{L})}(-z)$, where $s_{K(\mathcal{L})}$ is the section from (2.5). □

Notation 2.19. Let $\widetilde{x}$ be an affine lift of a point $x \in X(k)$, and let $z \in K(\mathcal{L})$. Then we will denote by

$$z \boxplus \widetilde{x} := \widetilde{x+z}$$

the affine lift $\widetilde{x+z}$ of $x+z$ from Proposition 2.18. Be careful, this is not an action! The lift $(z+z') \boxplus \widetilde{x}$ is not equal to $z \boxplus (z' \boxplus \widetilde{x})$ in general. The reason being that the section $s_{K(\mathcal{L})}$ is not a group morphism. However, it determines an action above isotropic subgroups of $K(\mathcal{L})$.

Notation 2.20. For an affine point $\widetilde{x} \in \widetilde{X}$ and for $\xi \in k^\times$, we will denote by $\xi \cdot \widetilde{x}$ the coordinate-wise multiplication by ξ, i.e.

$$\theta_i^{\Theta_\mathcal{L}}(\xi \cdot \widetilde{x}) = \xi \cdot \theta_i^{\Theta_\mathcal{L}}(\widetilde{x}), \text{ for all } i \in K(\mathcal{L})_1.$$

2.2.3 The isogeny theorem

The main tool we will use for computing isogenies is the isogeny theorem, relating the theta coordinates of the source variety to the theta coordinates of the target variety. But this is only possible in a very precise setup.

Let $f\colon (X, \mathcal{L}) \to (Y, \mathcal{M})$ be a separable isogeny of polarized abelian varieties with kernel $K = \ker f$. Let $\delta_\mathcal{L}$ and $\delta_\mathcal{M}$ be the separable types of the line bundles $\mathcal{L}$ and $\mathcal{M}$ respectively. Suppose $f^*\mathcal{M}$ and $\mathcal{L}$ are isomorphic, and let $\alpha\colon f^*\mathcal{M} \xrightarrow{\sim} \mathcal{L}$ be one such isomorphism. We then have a map between the spaces of global sections

$$\alpha \circ f^*\colon \Gamma(Y, \mathcal{M}) \to \Gamma(X, \mathcal{L}).$$

We have seen that theta structures induce bases for the above vector spaces, and we would like to express $\alpha \circ f^*$ in terms of these bases. For this we need to define the notion of compatibility of theta structures with respect to the isogeny f. Let $\Theta_\mathcal{L}$ and $\Theta_\mathcal{M}$ be theta structures on $(X, \mathcal{L})$ and $(Y, \mathcal{M})$ respectively. Recall that a theta structure $\Theta_\mathcal{L}\colon \mathcal{H}(\delta_\mathcal{L}) \xrightarrow{\sim} \mathcal{G}(\mathcal{L})$ contains the information of

- a symplectic isomorphism $\overline{\Theta}_\mathcal{L}\colon K(\delta_\mathcal{L}) \xrightarrow{\sim} K(\mathcal{L})$, yielding the maximal isotropic subgroups $K(\mathcal{L})_1 = \overline{\Theta}_\mathcal{L}(\mathbb{Z}(\delta_\mathcal{L}))$ and $K(\mathcal{L})_2 = \overline{\Theta}_\mathcal{L}(\widehat{\mathbb{Z}}(\delta_\mathcal{L}))$;

- a section of sets $s_{K(\mathcal{L})}\colon K(\mathcal{L}) \to \mathcal{G}(\mathcal{L})$ that is a group morphism when restricted to any isotropic subgroup. Knowing $s_{K(\mathcal{L})}$ is actually equivalent to knowing two group sections $s_{K(\mathcal{L})_i}\colon K(\mathcal{L})_i \to \mathcal{G}(\mathcal{L})$, for $i = 1, 2$ (or equivalently two level subgroups $\widetilde{K}(\mathcal{L})_i = s_{K(\mathcal{L})_i}(K(\mathcal{L})_i) \subset \mathcal{G}(\mathcal{L})$).

The same holds for $\Theta_{\mathcal{M}}\colon \mathcal{H}(\delta_{\mathcal{M}}) \xrightarrow{\sim} \mathcal{G}(\mathcal{M})$. Let $\widetilde{K} \subset \mathcal{G}(\mathcal{L})$ be the level subgroup corresponding to the descent datum $(\mathcal{M}, \alpha)$. Then, for $\Theta_{\mathcal{L}}$ and $\Theta_{\mathcal{M}}$ to be *f-compatible*, they need to satisfy the following conditions:

i) the kernel K of f is compatible with the symplectic decomposition of $K(\mathcal{L})$;

ii) the symplectic decompositions of $K(\mathcal{L})$ and $K(\mathcal{M})$ are f-compatible;

iii) the descent datum is compatible with the theta structure $\Theta_{\mathcal{L}}$;

iv) the sections $s_{K(\mathcal{L})_i}\colon K(\mathcal{L})_i \to \mathcal{G}(\mathcal{L})$ and $s_{K(\mathcal{M})_i}\colon K(\mathcal{M})_i \to \mathcal{G}(\mathcal{M})$ are compatible for $i = 1, 2$.

Let us make the above points more precise. Recall the morphism $\alpha_f\colon \mathcal{Z}(\widetilde{K}) \to \mathcal{G}(\mathcal{M})$ from Section 2.1.1, where $\mathcal{Z}(\widetilde{K})$ is the centralizer of $\widetilde{K}$ in $\mathcal{G}(\mathcal{L})$, inducing an isomorphism

$$\mathcal{Z}(\widetilde{K})/\widetilde{K} \xrightarrow{\sim} \mathcal{G}(\mathcal{M}).$$

Definition 2.21. i) We say that $K = \ker f$ is compatible with the decomposition $K(\mathcal{L}) = K(\mathcal{L})_1 \oplus K(\mathcal{L})_2$ if

$$K = (K(\mathcal{L})_1 \cap K) \oplus (K(\mathcal{L})_2 \cap K).$$

ii) In this case, we say that the decompositions $K(\mathcal{L}) = K(\mathcal{L})_1 \oplus K(\mathcal{L})_2$ and $K(\mathcal{M}) = K(\mathcal{M})_1 \oplus K(\mathcal{M})_2$ are f-compatible if

$$K(\mathcal{M})_i = f(K(\mathcal{L})_i) \cap K(\mathcal{M}), \text{ for } i = 1, 2.$$

iii) We say that the descent datum $(\mathcal{M}, \alpha)$ is compatible with the theta structure $\Theta_{\mathcal{L}}$ if the level subgroups $\widetilde{K}$ and $s_{K(\mathcal{L})}(K)$ above K agree, i.e. if

$$\widetilde{K} = s_{K(\mathcal{L})}(K).$$

iv) If the above compatibilities are satisfied, we say that the sections $s_{K(\mathcal{L})_i}$ and $s_{K(\mathcal{M})_i}$ for $i = 1, 2$ (or equivalently the corresponding level subgroups $\widetilde{K}(\mathcal{L})_i$ and $\widetilde{K}(\mathcal{M})_i$) are f-compatible if

$$\alpha_f(\widetilde{K}(\mathcal{L})_i \cap \mathcal{Z}(\widetilde{K})) = \widetilde{K}(\mathcal{M})_i, \text{ for } i = 1, 2.$$

The compatibility of the sections can be seen as commutative diagrams of group morphisms

$$\begin{array}{ccc} \mathcal{Z}(\widetilde{K}) & \xrightarrow{\alpha_f} & \mathcal{G}(\mathcal{M}) \\ {\scriptstyle s_{K(\mathcal{L})_i}}\uparrow & & \uparrow{\scriptstyle s_{K(\mathcal{M})_i}} \\ K(\mathcal{L})_i \cap f^{-1}(K(\mathcal{M})) & \xrightarrow[f]{} & K(\mathcal{M})_i \end{array}$$

for $i = 1, 2$. Note that these diagrams only make sense if conditions i) - iii) are satisfied, i.e. if $z \in K = \ker f$ can be written as $z = z_1 + z_2$, with $z_i \in K(\mathcal{L})_i \cap K$, and

$$z_i \mapsto s_{K(\mathcal{L})_i}(z_i) \in \widetilde{K} = \ker \alpha_f$$

for $i = 1, 2$.

An element $z \in f^{-1}(K(\mathcal{M}))$ can be written in a unique way as $z = z_1 + z_2$ with $z_i \in K(\mathcal{L})_i \cap f^{-1}(K(\mathcal{M}))$, for $i = 1, 2$, and $f(z) \in K(\mathcal{M})$ can be written in a unique way as $f(z) = f(z)_1 + f(z)_2$ with $f(z)_i \in K(\mathcal{M})_i$, for $i = 1, 2$. By condition ii) we have

$$f(z_i) = f(z)_i.$$

The sections $s_{K(\mathcal{L})}$ and $s_{K(\mathcal{M})}$ satisfy

$$s_{K(\mathcal{L})}(z) = s_{K(\mathcal{L})_2}(z_2) \cdot s_{K(\mathcal{L})_1}(z_1) \in \mathcal{Z}(\widetilde{K})$$

and

$$s_{K(\mathcal{M})}(f(z)) = s_{K(\mathcal{M})_2}(f(z)_2) \cdot s_{K(\mathcal{M})_1}(f(z)_1) \in \mathcal{G}(\mathcal{M}),$$

and since α_f is a group morphism, the compatibility condition of the sections is equivalent to the commutative diagram of sets

$$\begin{array}{ccc} \mathcal{Z}(\widetilde{K}) & \xrightarrow{\alpha_f} & \mathcal{G}(\mathcal{M}) \\ {\scriptstyle s_{K(\mathcal{L})}}\uparrow & & \uparrow{\scriptstyle s_{K(\mathcal{M})}} \\ f^{-1}(K(\mathcal{M})) & \xrightarrow[f]{} & K(\mathcal{M}). \end{array}$$

Be careful, the vertical arrows are not group morphisms.

Definition 2.22. We call

$$f\colon (X, \mathcal{L}, \Theta_{\mathcal{L}}) \to (Y, \mathcal{M}, \Theta_{\mathcal{M}})$$

an isogeny of polarized abelian varieties with theta structure if $f\colon X \to Y$ is a separable isogeny, $f^*\mathcal{M} \cong \mathcal{L}$ and if $\Theta_{\mathcal{L}}$ and $\Theta_{\mathcal{M}}$ are f-compatible theta structures.

The polarized abelian varieties with theta structure $(X, \mathcal{L}, \Theta_{\mathcal{L}})$ and $(Y, \mathcal{M}, \Theta_{\mathcal{M}})$ are endowed with canonical projective coordinates. Provided the theta structures are compatible, the following theorem, called the *isogeny theorem*, tells us how to compute the isogeny $X \to Y$ in theta coordinates.

Theorem 2.23 (Isogeny theorem)**.** *Let $f\colon (X, \mathcal{L}, \Theta_{\mathcal{L}}) \to (Y, \mathcal{M}, \Theta_{\mathcal{M}})$ be an isogeny of polarized abelian varieties with theta structure. There exists a scalar $\lambda \in k^\times$, such that for all $x \in X(k)$ and $i \in K(\mathcal{M})_1$ we have*

$$\theta_i^{\Theta_{\mathcal{M}}}(f(x)) = \lambda \cdot \sum_{\substack{j \in K(\mathcal{L})_1 \\ f(j) = i}} \theta_j^{\Theta_{\mathcal{L}}}(x). \tag{2.8}$$

Proof. We refer to [BL04, Thm. 6.5.1] for the complex case and for arbitrary fields we refer to [Mum66, §1, Thm. 4]. □

In addition, we can state an affine version of the isogeny theorem. Suppose that we have an isogeny of polarized abelian varieties with theta structure

$$f\colon (X,\mathcal{L},\Theta_{\mathcal{L}}) \to (Y,\mathcal{M},\Theta_{\mathcal{M}}).$$

We know that $\Theta_{\mathcal{L}}$ and $\Theta_{\mathcal{M}}$ define affine coordinates on $\widetilde{X}$ and $\widetilde{Y}$ above X and Y respectively. Theorem 2.23 tells us that an affine lift

$$\widetilde{f}\colon \widetilde{X} \to \widetilde{Y}$$

of f can be given as follows: for $\widetilde{x} \in \widetilde{X}$ with coordinates $\widetilde{x} = (\theta_i^{\Theta_{\mathcal{L}}}(\widetilde{x}))_{i\in K(\mathcal{L})_1}$ we define $\widetilde{f}(\widetilde{x}) \in \widetilde{Y}$ to be the affine point with coordinates

$$\theta_i^{\Theta_{\mathcal{M}}}(\widetilde{f}(\widetilde{x})) = \sum_{\substack{j\in K(\mathcal{L})_1 \\ f(j)=i}} \theta_j^{\Theta_{\mathcal{L}}}(\widetilde{x}) \tag{2.9}$$

for all $i \in K(\mathcal{M})_1$. Then $\widetilde{f}(\widetilde{x})$ is indeed above the image of $f(x)$ under the projective embedding of Y.

Proposition 2.24. *Given a polarized abelian variety with theta structure $(X,\mathcal{L},\Theta_{\mathcal{L}})$ and $K \subset K(\mathcal{L})$ isotropic and compatible with the decomposition of $K(\mathcal{L})$ induced by $\overline{\Theta}_{\mathcal{L}}$, there exists an induced polarized abelian variety with theta structure $(Y = X/K,\mathcal{M},\Theta_{\mathcal{M}})$. Moreover, $\Theta_{\mathcal{L}}$ and $\Theta_{\mathcal{M}}$ are f-compatible, where $f\colon X \to Y$ is the projection isogeny.*

Proof. The level subgroup $\widetilde{K} := s_{K(\mathcal{L})}(K) \subset \mathcal{G}(\mathcal{L})$ determines a line bundle $\mathcal{M}$ on Y and an isomorphism $\alpha\colon f^*\mathcal{M} \xrightarrow{\sim} \mathcal{L}$. To define a theta structure $\Theta_{\mathcal{M}}\colon \mathcal{H}(\delta_{\mathcal{M}}) \to \mathcal{G}(\mathcal{M})$, it suffices by Proposition 2.11 to define a symplectic isomorphism $\overline{\Theta}_{\mathcal{M}}\colon K(\delta_{\mathcal{M}}) \to K(\mathcal{M})$ and group sections of $\rho_{\mathcal{G}(\mathcal{M})}$ above $K(\mathcal{M})_1 := \overline{\Theta}_{\mathcal{M}}(\mathbb{Z}(\delta_{\mathcal{M}}))$ and $K(\mathcal{M})_2 := \overline{\Theta}_{\mathcal{M}}(\widehat{\mathbb{Z}}(\delta_{\mathcal{M}}))$. We define the symplectic isomorphism $\overline{\Theta}_{\mathcal{M}}\colon K(\delta_{\mathcal{M}}) \to K(\mathcal{M})$ as follows: for each $x \in K(\delta_{\mathcal{M}}) \subset K(\delta_{\mathcal{L}})$ set

$$\overline{\Theta}_{\mathcal{M}}(x) := f(\overline{\Theta}_{\mathcal{L}}(x)) \in K(\mathcal{M}).$$

Then, the symplectic decomposition $K(\mathcal{M}) = K(\mathcal{M})_1 \oplus K(\mathcal{M})_2$ induced by $\overline{\Theta}_{\mathcal{M}}$ is f-compatible with the symplectic decomposition of $K(\mathcal{L})$ induced by $\overline{\Theta}_{\mathcal{L}}$.
For $i = 1, 2$, and $z \in K(\mathcal{M})_i$, let $z' \in f^{-1}(z)$ be any point in the inverse image. Define the group section $s_{K(\mathcal{M})_i}\colon K(\mathcal{M})_i \to \mathcal{G}(\mathcal{M})$ as

$$s_{K(\mathcal{M})_i}(z) = \alpha_f(s_{K(\mathcal{L})_i}(z')) \in \mathcal{G}(\mathcal{M}).$$

The following diagram can be helpful

$$\begin{array}{ccc} \mathcal{Z}(\widetilde{K}) & \xrightarrow{\alpha_f} & \mathcal{G}(\mathcal{M}) \\ {\scriptstyle s_{K(\mathcal{L})_i}}\uparrow & & \uparrow{\scriptstyle s_{K(\mathcal{M})_i}} \\ f^{-1}(K(\mathcal{M})_i) & \xrightarrow[f]{} & K(\mathcal{M})_i. \end{array}$$

Since $\ker \alpha_f$ is precisely the level subgroup $\widetilde{K} = s_{K(\mathcal{L})}(K)$, the definition of $s_{K(\mathcal{M})_i}$ does not depend on the choice of z'. This defines a theta structure $\Theta_{\mathcal{M}}$ on $(Y,\mathcal{M})$, f-compatible with $\Theta_{\mathcal{L}}$ and hence, an isogeny of polarized abelian varieties with theta structure

$$f\colon (X,\mathcal{L},\Theta_{\mathcal{L}}) \to (Y,\mathcal{M},\Theta_{\mathcal{M}}).$$

□

2.2.4 Product line bundles and product theta structures

Let $(X, \mathcal{L}, \Theta_{\mathcal{L}})$ be a polarized abelian variety of separable type $\delta = (\delta_1, \ldots, \delta_g)$ with theta structure, and let $r \geq 1$ be a nonnegative integer . There is a natural polarization $\mathcal{L}^{\star r}$ on X^r defined as

$$\mathcal{L}^{\star r} = p_1^*\mathcal{L} \otimes \cdots \otimes p_r^*\mathcal{L},$$

where $p_i \colon X^r \to X$ is the projection of the ith factor, for $i = 1, \ldots, r$. A polarization (or ample line bundle) $\mathcal{L}'$ on the variety X^r is called a *product polarization* if $\mathcal{L}'$ is isomorphic to $\mathcal{L}^{\star r}$ for some polarization $\mathcal{L}$ on X. According to [Mum66, §3, Lem.1], we have

$$\mathcal{G}(\mathcal{L}^{\star r}) \cong \mathcal{G}(\mathcal{L})^r / \{(a_1, \ldots, a_r) : a_i \in k^\times \hookrightarrow \mathcal{G}(\mathcal{L}), a_1 \cdots a_r = 1\}.$$

The isomorphism is induced by the map $\mathcal{G}(\mathcal{L})^r \to \mathcal{G}(\mathcal{L}^{\star r})$ sending

$$((x_1, \mathcal{L} \xrightarrow{\phi_{x_1}} t_{x_1}^*\mathcal{L}), \ldots, (x_r, \mathcal{L} \xrightarrow{\phi_{x_r}} t_{x_r}^*\mathcal{L})) \mapsto ((x_1, \ldots, x_r), \mathcal{L}^{\star r} \xrightarrow{p_1^*\phi_{x_1} \otimes \cdots \otimes p_r^*\phi_{x_r}} t_{(x_1,\ldots,x_r)}^*\mathcal{L}^{\star r}).$$

The type $\delta^{\star r}$ of $\mathcal{L}^{\star r}$ is

$$\delta^{\star r} = \left(\underbrace{\delta_1, \ldots, \delta_1}_{r}, \underbrace{\delta_2, \ldots, \delta_2}_{r}, \ldots, \underbrace{\delta_g, \ldots, \delta_g}_{r} \right) \in \mathbb{Z}^{gr},$$

since $\mathbb{Z}(\delta^{\star r}) \cong \mathbb{Z}(\delta)^r$. The group $K(\delta^{\star r}) \cong K(\delta)^r$ is equipped with the symplectic pairing

$$e_{\delta^{\star r}}((z_1, \ldots, z_r), (z_1', \ldots, z_r')) = e_\delta(z_1, z_1') \cdots e_\delta(z_r, z_r') \in k^\times,$$

and the Heisenberg group $\mathcal{H}(\delta^{\star r})$ is defined in the same way as in Definition 2.9. The theta structure $\Theta_{\mathcal{L}} \colon \mathcal{H}(\delta) \to \mathcal{G}(\mathcal{L})$ induces in a natural way a $k^\times$-isomorphism

$$(\Theta_{\mathcal{L}})^{\star r} \colon \mathcal{H}(\delta^{\star r}) \to \mathcal{G}(\mathcal{L}^{\star r}),$$

given by

$$(a, (x_1, y_1), \ldots, (x_r, y_r)) \mapsto (a \cdot \Theta_{\mathcal{L}}(1, x_1, y_1), \ldots, \Theta_{\mathcal{L}}(1, x_r, y_r)).$$

Note that we can actually put the scalar a in any coordinate, not necessarily the first. The canonical coordinates for $(X^r, \mathcal{L}^{\star r}, (\Theta_{\mathcal{L}})^{\star r})$ are then given by

$$\theta_{\mathbf{i}}^{(\Theta_{\mathcal{L}})^{\star r}}(\mathbf{x}) = \theta_{i_1}^{\Theta_{\mathcal{L}}}(x_1) \otimes \cdots \otimes \theta_{i_r}^{\Theta_{\mathcal{L}}}(x_r), \tag{2.10}$$

where $\mathbf{i} = (i_1, \ldots, i_r) \in K(\mathcal{L})_1^r = K(\mathcal{L}^{\star r})_1$ and $\mathbf{x} = (x_1, \ldots, x_r) \in X^r(k)$. A theta structure on $(X^r, \mathcal{L}^{\star r})$ is called an *r-fold product theta structure* if it arises via the above construction, for some polarized abelian variety with theta structure $(X, \mathcal{L}, \Theta_{\mathcal{L}})$, and we will commonly denote it by $(\Theta_{\mathcal{L}})^{\star r}$. The notion of r-fold product theta structures will turn out to be very important for our algorithm of isogeny computation. The following lemma will be useful in the sequel.

Lemma 2.25. *A theta structure $\Theta \colon \mathcal{H}(\delta^{\star r}) \to \mathcal{G}(\mathcal{L}^{\star r})$ is of product form if and only if the induced symplectic isomorphism $\overline{\Theta} \colon K(\delta^{\star r}) \to K(\mathcal{L}^{\star r})$ is of product form.*

Proof. Let $\Theta \colon \mathcal{H}(\delta^{\star r}) \to \mathcal{G}(\mathcal{L}^{\star r})$ be a theta structure and suppose that the induced symplectic isomorphism $\overline{\Theta} \colon K(\delta^{\star r}) \to K(\mathcal{L}^{\star r})$ is of product form. Denote by $\overline{\vartheta} \colon K(\delta) \to$

$K(\mathcal{L})$ the restriction of $\overline{\Theta}$ to a single factor, i.e. $\overline{\Theta} = \overline{\vartheta} \times \cdots \times \overline{\vartheta}$. Let $(x, y) \in K(\delta)$ and $z = \overline{\vartheta}(x, y) \in K(\mathcal{L})$. Then Θ sends

$$(1, (x, y), \ldots, (x, y)) \mapsto ((z, \phi_1), \ldots, (z, \phi_r)),$$

where $\phi_1, \ldots, \phi_r$ are isomorphisms $\mathcal{L} \xrightarrow{\sim} t_z^*\mathcal{L}$. There exist scalars $a_2, \ldots, a_r \in k^\times$ such that $\phi_2 = a_2 \cdot \phi_1, \ldots, \phi_r = a_r \cdot \phi_1$. Define $\vartheta \colon \mathcal{H}(\delta) \to \mathcal{G}(\mathcal{L})$ pointwise by

$$(1, x, y) \mapsto (z, \sqrt[r]{a_2} \cdots \sqrt[r]{a_r} \cdot \phi_1).$$

One carefully checks that ϑ is well defined, is a $k^\times$-isomorphism and that Θ is equal to the r-fold product $\vartheta^{\star r}$ of ϑ. □

2.3 Totally symmetric line bundles and symmetric theta structures

We assume in this section that $char(k) \neq 2$. Let $(X, \mathcal{L})$ be a polarized abelian variety of separable type $\delta = (\delta_1, \ldots, \delta_g)$. A priori, there is no way to fix a particular choice of a representative in the algebraic equivalence class of $\mathcal{L}$. One way to overcome this is to introduce the notions of symmetric and totally symmetric line bundles.

Definition 2.26. A line bundle $\mathcal{L}$ on X is called symmetric if $[-1]^*\mathcal{L} \cong \mathcal{L}$.

As the next proposition shows, symmetric line bundles are quite frequent.

Proposition 2.27. *In every algebraic equivalence class of ample line bundles there exits a symmetric line bundle.*

Proof. Let $\mathcal{L}$ be an ample line bundle on X. It is easy to see that $\mathcal{L}^{-1} \otimes [-1]^*\mathcal{L} \in \mathrm{Pic}^0(X)$, i.e. $\mathcal{L}^{-1} \otimes [-1]^*\mathcal{L} \cong \mathcal{L}_0$ for some $\mathcal{L}_0 \in \mathrm{Pic}^0(X)$. But $\widehat{X}(k)$ is a divisible group, see [EvdGM, Cor. 5.10], hence there exists $\mathcal{L}_0' \in \mathrm{Pic}^0(X)$ such that $(\mathcal{L}_0')^{\otimes 2} = \mathcal{L}_0$. We then have $[-1]^*\mathcal{L} \otimes (\mathcal{L}_0')^{-1} \cong \mathcal{L} \otimes \mathcal{L}_0'$. Since $\mathcal{L}_0' \in \mathrm{Pic}^0(X)$, it satisfies $(\mathcal{L}_0')^{-1} = [-1]^*\mathcal{L}_0'$, and therefore $\mathcal{L} \otimes \mathcal{L}_0'$ is symmetric. □

Suppose that $\mathcal{L}$ is symmetric and fix an isomorphism $\psi \colon \mathcal{L} \xrightarrow{\sim} [-1]^*\mathcal{L}$. For all $x \in X(k)$ we have isomorphisms on the fibers

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

In particular, ψ induces an automorphism $\psi(0) \colon \mathcal{L}(0) \xrightarrow{\sim} \mathcal{L}(0)$, which is given by multiplication by a constant. Up to rescaling ψ, we can assume that $\psi(0)$ is the identity. We then call ψ a *normalized* isomorphism.

Let $\mathcal{L}$ be a symmetric line bundle on X and let $\psi \colon \mathcal{L} \xrightarrow{\sim} [-1]^*\mathcal{L}$ be the normalized isomorphism. If $x \in X[2]$ then $\mathcal{L}(x) \xrightarrow{\psi(x)} \mathcal{L}(-x) = \mathcal{L}(x)$ is an automorphism and hence, $\psi(x)$ is given by multiplication by a scalar. This defines a map

$$e_*^{\mathcal{L}} \colon X[2] \to k^\times.$$

Proposition 2.28. *We have the following properties:*

- $e_*^{\mathcal{L}}(x) \in \{\pm 1\}$;
- $e_*^{\mathcal{L} \otimes \mathcal{L}'} = e_*^{\mathcal{L}} \cdot e_*^{\mathcal{L}'}$ *for all symmetric line bundles* $\mathcal{L}$ *and* $\mathcal{L}'$ *on* X;

- *If $f\colon X \to Y$ is a homomorphism and if $\mathcal{M}$ is a symmetric line bundle on Y, then $f^*\mathcal{M}$ is symmetric and*

$$e_*^{f^*\mathcal{M}}(x) = e_*^{\mathcal{M}}(f(x)), \text{ for all } x \in X[2].$$

- *Let us denote by e_2 the Weil-pairing on $X[2] \times \widehat{X}[2]$. Let $y_0 \in \widehat{X}[2]$ correspond to the line bundle $\mathcal{L}_0 \in \mathrm{Pic}^0(X)$. Then $\mathcal{L}_0$ is symmetric and*

$$e_*^{\mathcal{L}_0}(x) = e_2(x, y_0)$$

for all $x \in X[2]$.

Proof. For a proof see [Mum66, p. 304-305]. □

Definition 2.29. A symmetric line bundle $\mathcal{L}$ is called *totally symmetric* if $e_*^{\mathcal{L}}(x) = 1$ for all $x \in X[2]$.

The notion of totally symmetric line bundles is useful for making a canonical choice of a line bundle within an algebraic equivalence class.

Proposition 2.30. *Let $\mathcal{L}$ be an ample line bundle on X of separable type δ and suppose $2 \mid \delta_1$, or equivalently $X[2] \subset K(\mathcal{L})$. Then there exists a unique totally symmetric line bundle in the algebraic equivalence class of $\mathcal{L}$.*

Proof. It is a well known fact that $X[2] \subset K(\mathcal{L})$ implies that the line bundle $\mathcal{L}$ is the square of a line bundle $\mathcal{L}' \in \mathrm{Pic}(X)$. See [BL04, Lem. 2.5.6] for the complex case and [Rob10, Cor. 3.2.3] for arbitrary characteristic. Then $\mathcal{L}' \otimes [-1]^*\mathcal{L}'$ is algebraically equivalent to $\mathcal{L}$ and is totally symmetric, since for all $x \in X[2]$ we have

$$e_*^{\mathcal{L}' \otimes [-1]^*\mathcal{L}'}(x) = e_*^{\mathcal{L}'}(x) \cdot e_*^{[-1]^*\mathcal{L}'}(x) = e_*^{\mathcal{L}'}(x) \cdot e_*^{\mathcal{L}'}(-x) = \left(e_*^{\mathcal{L}'}(x)\right)^2 = 1.$$

Let $\mathcal{M}$ be another totally symmetric line bundle in the same equivalence class, and let $\mathcal{L}_0 \in \mathrm{Pic}^0(X)$ be such that $\mathcal{M} = \mathcal{L}' \otimes [-1]^*\mathcal{L}' \otimes \mathcal{L}_0$. Then $\mathcal{L}_0$ is necessarily symmetric (i.e. if $y_0 \in \widehat{X}(k)$ corresponds to $\mathcal{L}_0$, then $y_0 \in \widehat{X}[2]$), and $\mathcal{L}_0$ must satisfy

$$1 = e_*^{\mathcal{L}_0}(x) = e_2(x, y_0), \text{ for all } x \in X[2].$$

But e_2 is non degenerate and hence, $y_0 = 0$. □

Corollary 2.31. *If $f\colon (X, \mathcal{L}) \to (Y, \mathcal{M})$ is an isogeny of polarized abelian varieties (i.e. $f^*\mathcal{M}$ is algebraically equivalent to $\mathcal{L}$) and if $\mathcal{L}$ and $\mathcal{M}$ are totally symmetric, then $f^*\mathcal{M} \cong \mathcal{L}$.*

Proof. The line bundle $f^*\mathcal{M}$ is totally symmetric by Proposition 2.28, and by Proposition 2.30 it is isomorphic to $\mathcal{L}$. □

Totally symmetric line bundles also appear as pullbacks of line bundles of certain quotients of X.

Definition 2.32. The quotient $K_X := X/\pm 1$ of X by the involution $[-1]$ is called the Kummer variety of X. We denote by $\pi\colon X \to K_X$ the natural projection.

Then we can show (see [Mum66, §2, Prop. 1]) that the line bundle $\mathcal{L}$ on X is totally symmetric if and only if it is of the from $\pi^*\mathcal{M}$ for some line bundle $\mathcal{M}$ on K_X.

Symmetric theta structures. Suppose that $\mathcal{L}$ is symmetric, of type δ, and let $\psi\colon \mathcal{L} \xrightarrow{\sim} [-1]^*\mathcal{L}$ be the normalized isomorphism. For $(z, \phi_z) \in \mathcal{G}(\mathcal{L})$ consider the composite

$$\mathcal{L} \xrightarrow{\psi} [-1]^*\mathcal{L} \xrightarrow{[-1]^*\phi_z} [-1]^*(t_z^*\mathcal{L}) = t_{-z}^*([-1]^*\mathcal{L}) \xrightarrow{t_{-z}^*\psi^{-1}} t_{-z}^*\mathcal{L}.$$

This determines an automorphism of order 2

$$\gamma_{-1}\colon \mathcal{G}(\mathcal{L}) \to \mathcal{G}(\mathcal{L}),\ (z, \phi_z) \mapsto \left(-z, (t_{-z}^*\psi^{-1}) \circ ([-1]^*\phi_z) \circ \psi\right).$$

Consider the following automorphism of the Heisenberg group

$$\gamma_{-1}\colon \mathcal{H}(\delta) \to \mathcal{H}(\delta),\ (\alpha, x, y) \mapsto (\alpha, -x, -y),$$

which is also of order 2.

Definition 2.33. A theta structure $\Theta_{\mathcal{L}}\colon \mathcal{H}(\delta) \xrightarrow{\sim} \mathcal{G}(\mathcal{L})$ on $(X, \mathcal{L})$ is called symmetric if

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

The reason why symmetric theta structures are of importance to us is that, in case $\mathcal{L}$ is totally symmetric, a symmetric theta structure on $(X, \mathcal{L})$ can be seen as something intermediate between a symplectic isomorphism $K(2\delta) \xrightarrow{\sim} K(\mathcal{L}^{\otimes 2})$ and a symplectic isomorphism $K(\delta) \xrightarrow{\sim} K(\mathcal{L})$. We already know that a theta structure $\mathcal{H}(\delta) \xrightarrow{\sim} \mathcal{G}(\mathcal{L})$ induces a symplectic isomorphism $K(\delta) \xrightarrow{\sim} K(\mathcal{L})$. On the other hand, a particularity of symmetric theta structures is that a symplectic isomorphism $K(2\delta) \xrightarrow{\sim} K(\mathcal{L}^{\otimes 2})$ induces in a unique way a symmetric theta structure $\mathcal{H}(\delta) \xrightarrow{\sim} \mathcal{G}(\mathcal{L})$. Moreover, these correspondences are onto, meaning that every symplectic isomorphism $K(\delta) \xrightarrow{\sim} K(\mathcal{L})$ is induced by a symmetric theta structure $\mathcal{H}(\delta) \xrightarrow{\sim} \mathcal{G}(\mathcal{L})$, and every such theta structure is induced by a symplectic isomorphism $K(2\delta) \xrightarrow{\sim} K(\mathcal{L}^{\otimes 2})$. These are Remarks 2 - 4 of [Mum66, p. 318 - 319]. Stated a little different we have:

Proposition 2.34. *Let $\mathcal{L}$ be a totally symmetric line bundle on X of type δ. Let $\overline{\Theta}\colon K(\delta) \xrightarrow{\sim} K(\mathcal{L})$ be a symplectic isomorphism. In order to fix a symmetric theta structure on $(X, \mathcal{L})$ that induces $\overline{\Theta}$ it suffices to fix a symplectic isomorphism $K(2\delta) \xrightarrow{\sim} K(\mathcal{L}^{\otimes 2})$ that restricts to $\overline{\Theta}$ on $K(\delta)$.*

For the above proposition we identify $K(\delta)$ with a subgroup of $K(2\delta)$ in the following way: the element $(x_1, \ldots, x_g) \in \mathbb{Z}(\delta)$ is sent to $(2x_1, \ldots, 2x_g) \in \mathbb{Z}(2\delta)$, whereas for each $y \in \widehat{\mathbb{Z}}(\delta)$ there exists a unique $y' \in \widehat{\mathbb{Z}}(2\delta)$ such that $y'(x) = y(2x)$ for all $x \in \mathbb{Z}(2\delta)$, and we send y to y'.

Symmetric theta structures are also very handy when it comes to computing the pullback $[-1]^*$ on the theta coordinates. One can carefully verify that, if $\mathcal{L}$ is a totally symmetric line bundle on X and if $\Theta_{\mathcal{L}}$ is a symmetric theta structure, then

$$[-1]\colon (X, \mathcal{L}, \Theta_{\mathcal{L}}) \to (X, \mathcal{L}, \Theta_{\mathcal{L}})$$

is an isogeny of polarized abelian varieties with theta structure. Hence, we can apply the isogeny theorem 2.23 to $[-1]$, and by [Mum66, p. 331] we obtain

$$[-1]^*\theta_i^{\Theta_{\mathcal{L}}} = \theta_{-i}^{\Theta_{\mathcal{L}}}, \tag{2.11}$$

for all $i \in K(\mathcal{L})_1$.

Proposition/Definition 2.35. *Let $\mathcal{L}$ be a totally symmetric line bundle on X and let $\Theta_{\mathcal{L}}$ be a symmetric theta structure. Let $x \in X(k)$ with fixed affine lift $\widetilde{x} = (\theta_i^{\Theta_{\mathcal{L}}}(\widetilde{x}))_{i \in K(\mathcal{L})_1}$. Then, a lift $-\widetilde{x}$ of $-x$ is given by*

$$\theta_i^{\Theta_{\mathcal{L}}}(-\widetilde{x}) = \theta_{-i}^{\Theta_{\mathcal{L}}}(\widetilde{x}), \text{ for all } i \in K(\mathcal{L})_1.$$

3 Polarizability of the quotient of an abelian variety by a finite subgroup

Starting from a principally polarized abelian variety $(X, \mathcal{L}_0)$, we want to give a criterion on the finite subgroups of X to decide whether the quotient variety admits a principal polarization "compatible" with the natural projection isogeny or not. As we have seen in Theorem 2.4, if $\mathcal{L}$ is an ample line bundle of arbitrary type on X, then the finite subgroups $K \subset K(\mathcal{L})$ for which the quotient admits a polarization compatible with the projection isogeny are precisely those subgroups admitting a level subgroup $\widetilde{K} \subset \mathcal{G}(\mathcal{L})$. And by Lemma 2.8, this can be rephrased as K being an isotropic subgroup of $K(\mathcal{L})$ for the commutator pairing $e_{\mathcal{L}}$. But this criterion cannot be applied to the principal polarization $\mathcal{L}_0$ since the group $K(\mathcal{L}_0)$ is trivial. Yet, we will see how to create new polarizations on X from totally positive real endomorphisms of X. For this section we let k be a fixed algebraically closed field that is either $\mathbb{C}$ or of positive characteristic p.

3.1 Recalls

Let us recall some well known notions and results. For any prime number ℓ, the ring of *ℓ-adic integers* $\mathbb{Z}_\ell$ is the ring

$$\mathbb{Z}_\ell = \varprojlim \mathbb{Z}/\ell^n\mathbb{Z},$$

where the inverse limit is over the positive integers n and the transition maps are given by the natural projections $\mathbb{Z}/\ell^{n+1}\mathbb{Z} \to \mathbb{Z}/\ell^n\mathbb{Z}$.

Let X be an abelian variety of dimension g over k. Suppose that the prime number ℓ is different from $char(k)$. The *ℓ-adic Tate module* of X is

$$T_\ell X = \varprojlim X[\ell^n],$$

where the inverse limit is again over the positive integers n and the transition maps are given by $X[\ell^{n+1}] \xrightarrow{[\ell]} X[\ell^n]$. One can show that $T_\ell X$ is a free $\mathbb{Z}_\ell$-module of rank $2g$. Let Y be another abelian variety over k and denote by $\mathrm{Hom}(X, Y)$ the additive group of all maps $X \to Y$ that are at the same time morphisms of algebraic varieties and group morphisms. Any $\alpha \in \mathrm{Hom}(X, Y)$ induces in a natural way a $\mathbb{Z}_\ell$-linear map

$$T_\ell\, \alpha \colon T_\ell X \to T_\ell Y,$$

and this defines an injective homomorphism of groups

$$\mathrm{Hom}(X, Y) \to \mathrm{Hom}_{\mathbb{Z}_\ell}(T_\ell X, T_\ell Y).$$

Moreover, it is even true that

$$\mathrm{Hom}(X, Y) \otimes \mathbb{Z}_\ell \to \mathrm{Hom}_{\mathbb{Z}_\ell}(T_\ell X, T_\ell Y) \tag{3.1}$$

is injective for any prime $\ell \neq char(k)$.

For an integer m not divisible by $char(k)$, there is a nondegenerate pairing, called the *Weil pairing*,

$$e_m \colon X[m] \times \widehat{X}[m] \to \mu_m(k),$$

where $\mu_m(k)$ is the cyclic group of mth roots of unity in k. Combined with any homomorphism $\lambda \colon X \to \widehat{X}$, this becomes a pairing

$$e_m^\lambda \colon X[m] \times X[m] \to \mu_m(k), \;\; e_m^\lambda(x, x') = e_m(x, \lambda(x')).$$

If ℓ is a prime number different from $char(k)$, then we can define a pairing

$$e_\ell \colon T_\ell X \times T_\ell \widehat{X} \to \mathbb{Z}_\ell(1), \;\; e_\ell((x_n),(x'_n)) = (e_{\ell^n}(x_n, x'_n)),$$

where $\mathbb{Z}_\ell(1) = \varprojlim \mu_{\ell^n}(k)$ with transition maps $\mu_{\ell^{n+1}}(k) \xrightarrow{(\cdot)^\ell} \mu_{\ell^n}(k)$. Combined with a homomorphism $\lambda \colon X \to \widehat{X}$, we obtain a pairing

$$e_\ell^\lambda \colon T_\ell X \times T_\ell X \to \mathbb{Z}_\ell(1), \;\; e_\ell^\lambda(x, x') = e_\ell(x, \lambda(x'))$$

(λ seen as an element of $\mathrm{Hom}_{\mathbb{Z}_\ell}(T_\ell X, T_\ell \widehat{X})$). It is not hard to show that if $\mathcal{L} \in \mathrm{Pic}(X)$, then $e_\ell^{\phi_\mathcal{L}}$ is skew-symmetric, where $\phi_\mathcal{L} \colon X \to \widehat{X}$ is the homomorphism associated to $\mathcal{L}$ from (2.1). By [Mil86, Prop. 16.6] the converse is true as well.

Proposition 3.1. *Suppose $char(k) \neq 2$, and let ℓ be a prime number different from $char(k)$. A homomorphism $\lambda \colon X \to \widehat{X}$ is of the form $\phi_\mathcal{L}$ for some $\mathcal{L} \in \mathrm{Pic}(X)$ if and only if $e_\ell^\lambda \colon T_\ell X \times T_\ell X \to \mathbb{Z}_\ell(1)$ is skew-symmetric.*

Note that in this case, $\mathcal{L}^{\otimes 2}$ is algebraically equivalent to the pullback of the Poincaré sheaf $\mathcal{P}$ by $(1, \lambda) \colon X \to X \times \widehat{X}$.

3.2 Real endomorphisms

Let $(X, \mathcal{L}_0)$ be a principally polarized abelian variety of dimension g over k. Composition of endomorphisms turns $\mathrm{End}(X)$ into a ring. It is well known that $\mathrm{End}(X)$ has no zero divisors and is a free abelian group of finite rank (follows from (3.1)). The ring $\mathrm{End}(X)$ possesses an anti-involution, called the *Rosati involution*

$$(\cdot)^\dagger \colon \mathrm{End}(X) \to \mathrm{End}(X),$$

defined as

$$\alpha \mapsto \alpha^\dagger = \phi_{\mathcal{L}_0}^{-1} \circ \widehat{\alpha} \circ \phi_{\mathcal{L}_0}.$$

Here, $\phi_{\mathcal{L}_0} \colon X \to \widehat{X}$ is an isomorphism since $\mathcal{L}_0$ is a principal polarization. We have the following properties: for all $\alpha, \beta \in \mathrm{End}(X)$ and $m \in \mathbb{Z}$,

$$(\alpha + \beta)^\dagger = \alpha^\dagger + \beta^\dagger, \quad (\alpha \circ \beta)^\dagger = \beta^\dagger \circ \alpha^\dagger, \quad (\alpha^\dagger)^\dagger = \alpha, \quad [m]^\dagger = [m].$$

The Rosati involution naturally appears when pulling back $\mathcal{L}_0$ by an endomorphism of X.

Lemma 3.2. *For any endomorphism $\alpha \in \mathrm{End}(X)$ we have*

$$\phi_{\alpha^* \mathcal{L}_0} = \phi_{\mathcal{L}_0} \circ \alpha^\dagger \circ \alpha.$$

Proof. We have already seen that

$$\phi_{\alpha^* \mathcal{L}_0} = \widehat{\alpha} \circ \phi_{\mathcal{L}_0} \circ \alpha.$$

But then

$$\phi_{\alpha^* \mathcal{L}_0} = \phi_{\mathcal{L}_0} \circ \underbrace{\phi_{\mathcal{L}_0}^{-1} \circ \widehat{\alpha} \circ \phi_{\mathcal{L}_0}}_{= \alpha^\dagger} \circ \alpha.$$

□

An endomorphism $\alpha \in \mathrm{End}(X)$ is called a *real endomorphism* (sometimes also called a *symmetric endomorphism*) if it satisfies $\alpha = \alpha^\dagger$. The set of real endomorphisms is denoted by $\mathrm{End}^+(X)$ and forms an additive subgroup of $\mathrm{End}(X)$. For every endomorphism $\alpha \in \mathrm{End}(X)$ there exists a monic polynomial $P_\alpha(t) \in \mathbb{Z}[t]$ of degree $2g$ satisfying $P_\alpha(n) = \deg([n]_X - \alpha)$, for all $n \in \mathbb{Z}$. The polynomial P_α is called the *characteristic polynomial* of α. An element $\alpha \in \mathrm{End}^+(X)$ is called *totally positive* if the roots of P_α are positive, and we denote by $\mathrm{End}^{++}(X) \subset \mathrm{End}^+(X)$ the subset of totally positive real endomorphisms.

If $\mathcal{L}$ is any line bundle on X, then $\phi_{\mathcal{L}_0}^{-1} \circ \phi_{\mathcal{L}}$ is an endomorphism of X, depending only on the algebraic equivalence class of $\mathcal{L}$. This defines an injective homomorphism of abelian groups

$$\mathrm{NS}(X) \to \mathrm{End}(X), \ \ [\mathcal{L}] \mapsto \phi_{\mathcal{L}_0}^{-1} \circ \phi_{\mathcal{L}}.$$

Indeed, if $\phi_{\mathcal{L}_0}^{-1} \circ \phi_{\mathcal{L}} = [0]$, then $K(\mathcal{L}) = \ker \phi_{\mathcal{L}} = X$, which means $\mathcal{L} \in \mathrm{Pic}^0(X)$.

Proposition 3.3. *Suppose $char(k) \neq 2$. An endomorphism $\alpha \in \mathrm{End}(X)$ is of the form $\phi_{\mathcal{L}_0}^{-1} \circ \phi_{\mathcal{L}}$ for some $\mathcal{L} \in \mathrm{Pic}(X)$ if and only if α is symmetric (with respect to $\mathcal{L}_0$). In other words, we have an isomorphism of abelian groups*

$$\mathrm{NS}(X) \xrightarrow{\sim} \mathrm{End}^+(X).$$

Proof. We know by Proposition 3.1 that the homomorphism $\lambda = \phi_{\mathcal{L}_0} \circ \alpha \colon X \to \widehat{X}$ is of the form $\phi_{\mathcal{L}}$ for some $\mathcal{L} \in \mathrm{Pic}(X)$ if and only if e_ℓ^λ is skew-symmetric, where ℓ is a prime number different from $char(k)$. For $x, x' \in T_\ell X$ we have

$$\begin{aligned} e_\ell^\lambda(x, x') &= e_\ell(x, \phi_{\mathcal{L}_0} \circ \alpha(x')) \\ &= e_\ell^{\phi_{\mathcal{L}_0}}(x, \alpha(x')) \\ &= e_\ell^{\phi_{\mathcal{L}_0}}(\alpha(x'), x)^{-1} \quad \text{by Proposition 3.1} \\ &= e_\ell(\alpha(x'), \phi_{\mathcal{L}_0}(x))^{-1} \\ &= e_\ell(x', \widehat{\alpha} \circ \phi_{\mathcal{L}_0}(x))^{-1} \quad \text{by [Mil86, Lem. 16.2 b)].} \end{aligned}$$

If α is symmetric, i.e. $\alpha = \alpha^\dagger = \phi_{\mathcal{L}_0}^{-1} \circ \widehat{\alpha} \circ \phi_{\mathcal{L}_0}$, then

$$e_\ell(x', \widehat{\alpha} \circ \phi_{\mathcal{L}_0}(x))^{-1} = e_\ell(x', \phi_{\mathcal{L}_0} \circ \alpha(x))^{-1} = e_\ell^\lambda(x', x)^{-1}$$

and e_ℓ^λ is skew-symmetric. Conversely, if e_ℓ^λ is skew-symmetric, then

$$e_\ell(x, \phi_{\mathcal{L}_0} \circ \alpha(x')) = e_\ell(x, \widehat{\alpha} \circ \phi_{\mathcal{L}_0}(x'))$$

for all $x, x' \in T_\ell X$, and by the nondegeneracy of e_ℓ we deduce that $\phi_{\mathcal{L}_0} \circ \alpha = \widehat{\alpha} \circ \phi_{\mathcal{L}_0}$. □

One might ask how the isomorphism from Proposition 3.3 behaves when restricted to polarizations.

Proposition 3.4. *Suppose $char(k) \neq 2$. Let X be a principally polarized abelian variety over k. The isomorphism $\mathrm{NS}(X) \xrightarrow{\sim} \mathrm{End}^+(X)$ induces a bijection between the polarizations on X and the set $\mathrm{End}^{++}(X)$ of totally positive real endomorphisms. Moreover, a polarization of degree d is sent to a totally positive real endomorphism of degree d^2. In particular, principal polarizations correspond to totally positive symmetric units of $\mathrm{End}(X)$.*

Proof. We refer to [BL04, Prop. 5.2.4] for the complex case and to [Mum70, §21] for positive characteristic. □

3.3 Principal polarizability of quotients of abelian varieties

Suppose now either $k = \mathbb{C}$ or k is an algebraically closed field of characteristic $p \neq 2$. Let $(X, \mathcal{L}_0)$ be a principally polarized abelian variety of dimension g over k. Let $\beta \in \mathrm{End}^{++}(X)$ be a totally positive real endomorphism. We know from Proposition 3.4 that $\phi_{\mathcal{L}_0} \circ \beta \colon X \to \widehat{X}$ is the polarization isogeny of some ample line bundle $\mathcal{L}_0^\beta$ on X. Furthermore we have $\ker \beta = K(\mathcal{L}_0^\beta)$ and hence, for isotropic subgroups $K \subset \ker \beta$ (for the commutator pairing $e_{\mathcal{L}_0^\beta}$) we can descend the ample line bundle $\mathcal{L}_0^\beta$ to an ample line bundle on $Y = X/K$. Motivated by this observation we can now give the criterion for the principal polarizability of quotients of X by finite subgroups.

Proposition 3.5. *Let $(X, \mathcal{L}_0)$ be a principally polarized abelian variety over k. Let $K \subset X(k)$ be a finite subgroup-scheme, and let $f \colon X \to Y = X/K$ be the corresponding separable isogeny. Then, Y admits a principal polarization if and only if there exists a totally positive real endomorphism $\beta \in \mathrm{End}^{++}(X)$ such that K is a maximal isotropic subgroup of $\ker \beta$ for the commutator pairing $e_{\mathcal{L}_0^\beta}$ (see above).*

Proof. By the above discussion and Grothendieck's descent theory (Theorem 2.4) we know that if β is a totally positive real endomorphism of X, and $K \subset \ker \beta$ is isotropic for $e_{\mathcal{L}_0^\beta}$, then $\mathcal{L}_0^\beta$ descends under f to an ample line bundle $\mathcal{M}_0$ on Y. The maximality of K means that

$$\#K(\mathcal{L}_0^\beta) = \#\ker \beta = (\#K)^2,$$

i.e.

$$\deg f = \#K = \deg \mathcal{L}_0^\beta.$$

By (2.3) it follows that $\deg \mathcal{M}_0 = 1$, hence $\mathcal{M}_0$ is a principal polarization.

Conversely, suppose that $\mathcal{M}_0$ is a principal polarization on Y. Consider the following diagram:

$$\begin{array}{ccccc} X & \xleftarrow{\beta} & X & \xrightarrow{f} & Y \\ & \searrow^{\phi_{\mathcal{L}_0}} & \downarrow & & \downarrow{\scriptstyle \phi_{\mathcal{M}_0}} \\ & & \widehat{X} & \xleftarrow[\widehat{f}]{} & \widehat{Y}. \end{array}$$

Then the composite

$$\beta := \phi_{\mathcal{L}_0}^{-1} \circ \underbrace{\widehat{f} \circ \phi_{\mathcal{M}_0} \circ f}_{= \phi_{f^*\mathcal{M}_0}}$$

is an endomorphism of X. From Proposition 3.4 it follows that β is a totally positive real endomorphism (the pullback of a polarization by an isogeny is again a polarization). If we set $\mathcal{L}_0^\beta = f^*\mathcal{M}_0$, then by (2.2) and Lemma 2.8, the group K is isotropic inside $K(\mathcal{L}_0^\beta) = \ker \beta$ for the commutator pairing $e_{\mathcal{L}_0^\beta}$. Comparing degrees, we see that

$$\deg \beta = \deg \widehat{f} \cdot \deg f = (\#K)^2,$$

i.e. K is maximal isotropic inside $\ker \beta$. □

3.4 Ordinary and simple abelian varieties over finite fields

We present some facts about abelian varieties over finite fields, following [Wat69] and [Oor07]. For this section we fix k a finite field of size $q = p^n$. Let X be an abelian variety of dimension g over k (not necessarily polarized). Let $\mathrm{End}_k(X)$ be the ring of endomorphisms of X that are defined over k, and denote by $\mathrm{End}^0(X) = \mathrm{End}_k(X) \otimes_{\mathbb{Z}} \mathbb{Q}$ the endomorphism algebra of X. It is well-known that $\mathrm{End}^0(X)$ is a semisimple $\mathbb{Q}$-algebra. We say that X is *k-simple* if it does not admit a proper abelian subvariety over k. In the sequel we will say "simple" when we mean "k-simple" (note that the property of not admitting proper subvarieties could get lost over an extension of k, as opposed to "absolutely simple" where the property is preserved under base change). Denote by $\pi_X \in \mathrm{End}_k(X)$ the k-Frobenius endomorphism of X. If X is simple then π_X is a *Weil q-number*, i.e. π_X is an algebraic integer and for every embedding $\psi\colon \mathbb{Q}(\pi_X) \to \mathbb{C}$ we have $|\psi(\pi_X)| = \sqrt{q}$. By the Honda-Serre-Tate theory, Weil q-numbers (up to conjugacy) are in bijection with k-isogeny classes of simple abelian varieties over k. Also, $\mathrm{End}^0(X)$ is a division ring, hence a simple $\mathbb{Q}$-algebra, and its center equals $\mathbb{Q}(\pi_X)$. When it comes to degrees we have

$$2g = [\mathrm{End}^0(X) : \mathbb{Q}(\pi_X)]^{\frac{1}{2}} \cdot [\mathbb{Q}(\pi_X) : \mathbb{Q}]. \tag{3.2}$$

We say that X is *ordinary* if $X[p](\bar{k}) \cong (\mathbb{Z}/p\mathbb{Z})^g$. If X is ordinary and simple then $\mathrm{End}_k(X)$ is commutative. Hence, $\mathrm{End}^0(X)$ is a field of degree $2g$ over $\mathbb{Q}$. If $\pi \in \overline{\mathbb{Q}}$ is any Weil q-number conjugate to π_X, then $\mathrm{End}^0(X)$ is isomorphic to $\mathbb{Q}(\pi)$. The field $K = \mathbb{Q}(\pi)$ is a *CM-field*, i.e. it admits a totally real subfield $K_0 \subset K$ of degree g over $\mathbb{Q}$ (every embedding $\psi_0\colon K_0 \to \mathbb{C}$ satisfies $\psi_0(K_0) \subset \mathbb{R}$) and K/K_0 is quadratic and totally imaginary (for every $\psi\colon K \to \mathbb{C}$ we have $\psi(K) \not\subset \mathbb{R}$). The totally real subfield K_0 is generated by $\pi + \frac{q}{\pi}$ over $\mathbb{Q}$ and the minimal polynomial of π over K_0 is $t^2 - (\pi + \frac{q}{\pi})t + q \in K_0[t]$. If X admits a principal polarization, then $\pi \cdot \pi^\dagger = q$ and hence,

$$K_0 = \mathbb{Q}(\pi + \pi^\dagger).$$

4 Computing cyclic isogenies in theta coordinates

In this section we compute the theta coordinates of the quotient of a principally polarized abelian variety by a rational cyclic subgroup from the theta coordinates of the original variety and of a generator of the subgroup.

Let $k = \mathbb{F}_q$ be a finite field of characteristic $p > 2$, and let $\bar{k}$ be a fixed algebraic closure of k. Let $(X, \mathcal{L}_0)$ be an ordinary and simple principally polarized abelian variety of dimension g over k. By Proposition 2.27, we can suppose without loss of generality that $\mathcal{L}_0$ is symmetric. The endomorphism algebra $\mathrm{End}_k(X) \otimes_{\mathbb{Z}} \mathbb{Q}$ is isomorphic to the CM-field $K = \mathbb{Q}(\pi)$ of degree $2g$ over $\mathbb{Q}$, where π is a Weil q-number whose conjugacy class represents the k-isogeny class of X. Let $K_0 = \mathbb{Q}(\pi+\pi^\dagger)$ be the totally real subfield of K of degree g over $\mathbb{Q}$, and assume that the conductor gap $[\mathcal{O}_{K_0} : \mathbb{Z}[\pi + \pi^\dagger]]$ is odd. Let $\ell \geq 3$ be an odd integer coprime to $p \cdot [\mathcal{O}_{K_0} : \mathbb{Z}[\pi + \pi^\dagger]]$. Suppose we are given a totally positive real endomorphism $\beta \in \mathrm{End}^{++}(X)$ of degree ℓ^2, whose kernel $\ker \beta$ is isomorphic to a product of two cyclic groups of order ℓ. By Proposition 3.4, the isogeny $\phi_{\mathcal{L}_0} \circ \beta \colon X \to \widehat{X}$ is the polarization isogeny of some ample line bundle $\mathcal{L}_0^\beta$ on X, and we can assume $\mathcal{L}_0^\beta$ symmetric (again by Proposition 2.27). Let $G \subset K(\mathcal{L}_0^\beta) = \ker \beta$ be a $\mathrm{Gal}(\bar{k}/k)$-stable cyclic subgroup-scheme of order ℓ. Let $t \in G(\bar{k})$ be a fixed generator of G. Let $Y := X/G$ be the quotient abelian variety and let

$$f \colon X \to Y$$

be the associated separable isogeny of kernel G. Since G is $\mathrm{Gal}(\bar{k}/k)$-stable, both the abelian variety Y and the isogeny f are rational. By [Rob10, Prop. 4.2.12] there exists a level subgroup $\widetilde{G} \subset \mathcal{G}(\mathcal{L}_0^\beta)$ of G such that $\mathcal{L}_0^\beta$ descends to a symmetric ample line bundle $\mathcal{M}_0$ on Y. Moreover, $\mathcal{M}_0$ is of degree 1 and hence, $(Y, \mathcal{M}_0)$ is a principally polarized abelian variety.

For this section we fix $n = 2$ or $n = 4$ and define the totally symmetric ample line bundles $\mathcal{L} := \mathcal{L}_0^{\otimes n}$ and $\mathcal{M} := \mathcal{M}_0^{\otimes n}$. Let $\Theta_{\mathcal{L}}$ be a symmetric theta structure on $(X, \mathcal{L})$, and let

$$\left\{\theta_i^{\Theta_{\mathcal{L}}} : i \in K(\mathcal{L})_1\right\}$$

be the induced basis of theta functions of $\Gamma(X, \mathcal{L})$. We have to suppose furthermore that we know the scalar by which π acts on t and that we know how to evaluate endomorphisms on the $2n$-torsion. This is the case if either of the following holds:

- we know an affine lift $\widetilde{\pi} \colon \widetilde{X} \to \widetilde{X}$ of the Frobenius π and we know how to lift $\mathrm{End}(X[2n])$ to $\mathrm{End}(\widetilde{X[2n]})$, i.e. given an endomorphism $\alpha : X[2n] \to X[2n]$, we know how to compute an affine lift $\widetilde{\alpha} \colon \widetilde{X[2n]} \to \widetilde{X[2n]}$ of α, where the coordinates on the affine cone $\widetilde{X}$ are with respect to $(X, \mathcal{L}, \Theta_{\mathcal{L}})$, or

- we work on the Jacobian variety of a hyperelliptic curve. If this is the case we can use the formulas of [vW98] and [Cos11] to convert between theta and Mumford coordinates. This works because $\mathcal{L} = \mathcal{L}_0^{\otimes n}$, for $n = 2$ or $n = 4$.

In this section we want to describe an algorithm that, given

i) an affine lift $\widetilde{0}_X = (\theta_i^{\Theta_{\mathcal{L}}}(\widetilde{0}_X))_{i \in K(\mathcal{L})_1}$ of 0_X (that we will call an *affine theta null point* for $(X, \mathcal{L}, \Theta_{\mathcal{L}})$),

ii) an affine lift $\widetilde{t} = (\theta_i^{\Theta_{\mathcal{L}}}(\widetilde{t}))_{i \in K(\mathcal{L})_1}$ of a generator t of G,

computes an affine theta null point

$$\widetilde{0}_Y = (\theta_j^{\Theta_{\mathcal{M}}}(\widetilde{0}_Y))_{j\in K(\mathcal{M})_1}$$

for $(Y, \mathcal{M}, \Theta_{\mathcal{M}})$, where $\Theta_{\mathcal{M}}$ is a symmetric theta structure on $(Y, \mathcal{M})$ as defined in Section 4.5.1.

Remark 4.1. According to Remark 1.16, if $(Y, \mathcal{M}_0)$ is isomorphic to the Jacobian variety of a hyperelliptic curve, then $n = 2$ is enough for recovering an equation of the curve from the coordinates of $\widetilde{0}_Y$. Hence, for dimension 2 we can set $n = 2$. However, in the non-hyperelliptic genus 3 case, we need $n = 4$ to compute an affine model of the plane quartic from the coordinates of $\widetilde{0}_Y$ (see e.g. [NR17]).

In Section 5 we will suppose that, in addition, we are given

iii) an affine lift $\widetilde{x} = (\theta_i^{\Theta_{\mathcal{L}}}(\widetilde{x}))_{i\in K(\mathcal{L})_1}$ of a point $x \in X(k)$ of order N coprime to $\ell \cdot [\mathcal{O}_{K_0} : \mathbb{Z}[\pi + \pi^\dagger]]$,

and compute an affine lift

$$\widetilde{f(x)} = (\theta_j^{\Theta_{\mathcal{M}}}(\widetilde{f(x)}))_{j\in K(\mathcal{M})_1}$$

of $f(x)$. We can say that we compute the isogeny f in theta coordinates, i.e. compute

$$\widetilde{f}\colon \widetilde{X} \setminus \{\text{points of order not coprime to } \ell \cdot [\mathcal{O}_{K_0} : \mathbb{Z}[\pi + \pi^\dagger]]\} \to \widetilde{Y},$$

where the affine coordinates on the cones $\widetilde{X}$ and $\widetilde{Y}$ are given by $\Theta_{\mathcal{L}}$ and $\Theta_{\mathcal{M}}$ respectively.

4.1 Applying the isogeny theorem to f

Suppose we are given an affine theta null point $\widetilde{0}_X$ for $(X, \mathcal{L}, \Theta_{\mathcal{L}})$ and an affine lift $\widetilde{t}$ of a fixed generator t of G. We want to explain how to compute an affine theta null point $\widetilde{0}_Y$ for $(Y, \mathcal{M}, \Theta_{\mathcal{M}})$, for a certain theta structure $\Theta_{\mathcal{M}}$ on $(Y, \mathcal{M})$. The only tool we have at our disposal to relate theta coordinates of isogenous varieties is the isogeny theorem (Theorem 2.23, or its affine version (2.9)). The isogeny f does not pull back the polarization $\mathcal{M}$ to $\mathcal{L}$, since $\deg f^*\mathcal{M} = \deg f \cdot \deg \mathcal{M} \neq \deg \mathcal{L}$, so there is no straightforward way to apply the isogeny theorem. However, if we let $\mathcal{L}^\beta := (\mathcal{L}_0^\beta)^{\otimes n}$, then

$$f\colon (X, \mathcal{L}^\beta) \to (Y, \mathcal{M})$$

is an isogeny of polarized abelian varieties that satisfies $f^*\mathcal{M} \cong \mathcal{L}^\beta$. In order to apply the isogeny theorem, we have to endow the polarized abelian varieties with f-compatible theta structures. We explain in Section 4.2 what it means to extend $\Theta_{\mathcal{L}}$ to a symmetric theta structure $\Theta_{\mathcal{L}^\beta}$ on $(X, \mathcal{L}^\beta)$, compatible with the descent datum $\widetilde{G} \subset \mathcal{G}(\mathcal{L}^\beta)$, and how to do so. By Proposition 2.24, the theta structure $\Theta_{\mathcal{L}^\beta}$ determines a symmetric f-compatible theta structure $\Theta'_{\mathcal{M}}$ on $(Y, \mathcal{M})$. We could then try to apply the isogeny theorem to the isogeny of polarized abelian varieties with theta structure

$$f\colon (X, \mathcal{L}^\beta, \Theta_{\mathcal{L}^\beta}) \to (Y, \mathcal{M}, \Theta'_{\mathcal{M}}).$$

The problem is that this requires one to know an affine theta null point for $(X, \mathcal{L}^\beta, \Theta_{\mathcal{L}^\beta})$, which we do not. For a comparison, the affine point $\widetilde{0}_X$ has n^g coordinates, whereas a theta null point for $(X, \mathcal{L}^\beta, \Theta_{\mathcal{L}^\beta})$ has $n^g\ell$ coordinates. There is no obvious way to obtain

the remaining coordinates. One idea is to search for an endomorphism $u \in \mathrm{End}(X)$ that satisfies $\bar{u}u = \beta$ and then apply the isogeny theorem to

$$u\colon (X, \mathcal{L}^\beta, \Theta_{\mathcal{L}^\beta}) \to (X, \mathcal{L}, \Theta_{\mathcal{L}}).$$

But there is no reason such a u exists, and even if it does, the isogeny theorem applied to u allows us to compute the theta coordinates for $(X, \mathcal{L}, \Theta_{\mathcal{L}})$ from the theta coordinates for $(X, \mathcal{L}^\beta, \Theta_{\mathcal{L}^\beta})$. We could try to invert this, but it is hopeless since the isogeny theorem yields n^g linear equations that we would have to solve for $n^g\ell$ unknowns. We will follow a different approach for computing an affine theta null point for $(Y, \mathcal{M}, \Theta_{\mathcal{M}})$, that we will explain in the forthcoming sections.

4.2 The β-contragredient isogeny

An idea to overcome the obstruction encountered in the previous section is to apply the isogeny theorem to the β-contragredient isogeny f' instead. Since $\ker f \subset \ker \beta$, there exists a unique rational isogeny $f'\colon Y \to X$, called the *β-contragredient isogeny*, such that $f' \circ f = \beta$ (the proof is similar to that of [EvdGM, Prop. 5.12]). Denote again by $\beta := f \circ f'$ the corresponding endomorphism of Y.

Proposition 4.2.

$$\phi_{(f')^*\mathcal{L}_0} = \phi_{\mathcal{M}_0} \circ \beta.$$

Proof. Let $\gamma \in \mathrm{End}(Y)$ be the endomorphism $\gamma := \phi_{\mathcal{M}_0}^{-1} \circ \phi_{(f')^*\mathcal{L}_0}$, so that we have

$$\phi_{(f')^*\mathcal{L}_0} = \phi_{\mathcal{M}_0} \circ \gamma.$$

By Lemma 3.2 and the fact that β is a real endomorphism, we have

$$\phi_{\beta^*\mathcal{L}_0} = \phi_{\mathcal{L}_0} \circ \beta^2.$$

On the other hand,

$$\begin{aligned}\phi_{\beta^*\mathcal{L}_0} &= \phi_{f^*((f')^*\mathcal{L}_0)} = \widehat{f} \circ \phi_{(f')^*\mathcal{L}_0} \circ f = \widehat{f} \circ \phi_{\mathcal{M}_0} \circ \gamma \circ f = \widehat{f} \circ \phi_{\mathcal{M}_0} \circ f \circ \gamma \\ &= \phi_{f^*\mathcal{M}_0} \circ \gamma = \phi_{\mathcal{L}_0} \circ \beta \circ \gamma.\end{aligned}$$

But $\phi_{\mathcal{L}_0}$ is an isomorphism and $\mathrm{End}(X)$ has no zero divisors, and therefore $\gamma = \beta$. □

Let $\mathcal{M}_0^\beta$ be a symmetric ample line bundle in the algebraic equivalence class determined by $\phi_{\mathcal{M}_0} \circ \beta$ (exists by Proposition 3.4), and let $\mathcal{M}^\beta := (\mathcal{M}_0^\beta)^{\otimes n}$. The line bundle $\mathcal{M}^\beta$ is totally symmetric and algebraically equivalent to the totally symmetric line bundle $(f')^*\mathcal{L}$, hence they are isomorphic. We have an isogeny of polarized abelian varieties

$$f'\colon (Y, \mathcal{M}^\beta) \to (X, \mathcal{L})$$

and an isomorphism $\alpha\colon (f')^*\mathcal{L} \xrightarrow{\sim} \mathcal{M}^\beta$. Let $\Theta_{\mathcal{L}}$ be the fixed symmetric theta structure on $(X, \mathcal{L})$ from above. We want to define a symmetric theta structure $\Theta_{\mathcal{M}^\beta}$ on $(Y, \mathcal{M}^\beta)$ that is f'-compatible with $\Theta_{\mathcal{L}}$. We will do so by first defining a symmetric theta structure Θ on $(Y, \mathcal{M})$, and then extend it (in the sense of Definition 4.3) to a symmetric theta structure $\Theta_{\mathcal{M}^\beta}$ on $(Y, \mathcal{M}^\beta)$.

Note that the theta group $\mathcal{G}(\mathcal{M})$ is isomorphic to the subgroup $\rho_{\mathcal{G}(\mathcal{M}^\beta)}^{-1}(K(\mathcal{M}))$ of $\mathcal{G}(\mathcal{M}^\beta)$, where $\rho_{\mathcal{G}(\mathcal{M}^\beta)}\colon \mathcal{G}(\mathcal{M}^\beta) \to K(\mathcal{M}^\beta)$ is the forgetful map (indeed, both are isomorphic to the abstract group $\mathcal{H}(\delta_{\mathcal{M}})$). Fix $\psi\colon \mathcal{G}(\mathcal{M}) \xrightarrow{\sim} \rho_{\mathcal{G}(\mathcal{M}^\beta)}^{-1}(K(\mathcal{M}))$ one such isomorphism.

Definition 4.3. Let $\Theta\colon \mathcal{H}(\delta_{\mathcal{M}}) \to \mathcal{G}(\mathcal{M})$ be a theta structure and let ψ be as above. An extension of Θ is a theta structure $\Theta_{\mathcal{M}^\beta}\colon \mathcal{H}(\delta_{\mathcal{M}^\beta}) \to \mathcal{G}(\mathcal{M}^\beta)$ that satisfies

$$\Theta_{\mathcal{M}^\beta}|_{\mathcal{H}(\delta_{\mathcal{M}})} = \psi \circ \Theta.$$

The theta structure Θ. We present an ad-hoc construction of the theta structure Θ. Since in a second step we would like to extend Θ to a theta structure on $(Y, \mathcal{M}^\beta)$ that is f'-compatible with $\Theta_{\mathcal{L}}$, some care has to be taken.

The isogeny f' restricts to an isomorphism $K(\mathcal{M}) = Y[n] \xrightarrow{\sim} K(\mathcal{L}) = X[n]$, and we define

$$K(\mathcal{M})_i := (f')^{-1}(K(\mathcal{L})_i) \cap K(\mathcal{M}), \text{ for } i = 1, 2.$$

The subgroups $K(\mathcal{M})_1$ and $K(\mathcal{M})_2$ are isotropic for $e_{\mathcal{M}}$ and form a symplectic decomposition $K(\mathcal{M}) = K(\mathcal{M})_1 \oplus K(\mathcal{M})_2$. Indeed, we have $e_{\mathcal{M}^\beta} = (f')^* e_{\mathcal{L}}$, and it follows that $K(\mathcal{M})_i$ is isotropic for $e_{\mathcal{M}^\beta}$, for $i = 1, 2$. But the symplectic pairings $e_{\mathcal{M}}$ and $e_{\mathcal{M}^\beta}$ come from the commutators in the respective theta groups, and $e_{\mathcal{M}}$ can be seen as the restriction of $e_{\mathcal{M}^\beta}$ to $\rho^{-1}_{\mathcal{G}(\mathcal{M}^\beta)}(K(\mathcal{M}))$ (the commutator pairing is independent of the lift to the theta group).

The types $\delta_{\mathcal{M}}$ and $\delta_{\mathcal{L}}$ are the same, hence $\overline{\Theta}_{\mathcal{L}}$ induces a symplectic isomorphism

$$\overline{\Theta}\colon K(\delta_{\mathcal{M}}) \xrightarrow{\sim} K(\mathcal{M})$$

via f'. By Proposition 2.11, in order to define Θ it suffices to define group sections $s_{K(\mathcal{M})_i}\colon K(\mathcal{M})_i \to \mathcal{G}(\mathcal{M})$, for $i = 1, 2$. We have to be careful in the way we define these sections.

Let us denote by G' the kernel of f'. The isomorphism $\alpha\colon (f')^*\mathcal{L} \xrightarrow{\sim} \mathcal{M}^\beta$ determines a level subgroup $\widetilde{G'} \subset \mathcal{G}(\mathcal{M}^\beta)$. Recall the morphism $\alpha_{f'}\colon \mathcal{G}(\mathcal{M}^\beta)^* \to \mathcal{G}(\mathcal{L})$ from (2.4), where $\mathcal{G}(\mathcal{M}^\beta)^*$ is the subgroup of $\mathcal{G}(\mathcal{M}^\beta)$ above $(f')^{-1}(K(\mathcal{L}))$. By Proposition 2.6, $\alpha_{f'}$ induces an isomorphism $\mathcal{G}(\mathcal{M}^\beta)^*/\widetilde{G'} \xrightarrow{\sim} \mathcal{G}(\mathcal{L})$. To define the sections $s_{K(\mathcal{M})_1}$ and $s_{K(\mathcal{M})_2}$, we need the following proposition.

Proposition 4.4. *We have an isomorphism $\mathcal{G}(\mathcal{M}^\beta)^*/\widetilde{G'} \cong \rho^{-1}_{\mathcal{G}(\mathcal{M}^\beta)}(K(\mathcal{M}))$.*

Proof. It suffices to show that $\mathcal{G}(\mathcal{M}^\beta)^*$ is isomorphic to $\rho^{-1}_{\mathcal{G}(\mathcal{M}^\beta)}(K(\mathcal{M})) \times \widetilde{G'}$. Since $(f')^{-1}(K(\mathcal{L})) = K(\mathcal{M}) \cup G'$, we have $\rho^{-1}_{\mathcal{G}(\mathcal{M}^\beta)}(K(\mathcal{M})) \subset \mathcal{G}(\mathcal{M}^\beta)^*$ by definition. The group $\mathcal{G}(\mathcal{M}^\beta)^*$ is the centralizer of $\widetilde{G'}$ in $\mathcal{G}(\mathcal{M}^\beta)$, and it is easy to see that it is generated by the subgroups $\rho^{-1}_{\mathcal{G}(\mathcal{M}^\beta)}(K(\mathcal{M}))$ and $\widetilde{G'}$. The intersection $\rho^{-1}_{\mathcal{G}(\mathcal{M}^\beta)}(K(\mathcal{M})) \cap \widetilde{G'}$ is trivial (the elements are above n-torsion points and ℓ-torsion points respectively), and $\mathcal{G}(\mathcal{M}^\beta)^*$ is therefore isomorphic to the direct product $\rho^{-1}_{\mathcal{G}(\mathcal{M}^\beta)}(K(\mathcal{M})) \times \widetilde{G'}$. □

The horizontal arrows in the following diagram (for $i = 1, 2$) are isomorphisms, so we define $s_{K(\mathcal{M})_i}\colon K(\mathcal{M})_i \to \mathcal{G}(\mathcal{M})$ to be the vertical dotted arrow

$$\begin{array}{ccccc}
\mathcal{G}(\mathcal{M}) & \xrightarrow{\quad\psi\quad} & \rho^{-1}_{\mathcal{G}(\mathcal{M}^\beta)}(K(\mathcal{M})) \cong \mathcal{G}(\mathcal{M}^\beta)^*/\widetilde{G'} & \longrightarrow & \mathcal{G}(\mathcal{L}) \\
\uparrow{\scriptstyle s_{K(\mathcal{M})_i}} & & & & \uparrow{\scriptstyle s_{K(\mathcal{L})_i}} \\
K(\mathcal{M})_i = (f')^{-1}(K(\mathcal{L})_i) & & \xrightarrow[f']{\qquad\qquad\qquad\qquad} & & K(\mathcal{L})_i.
\end{array}$$

The symplectic isomorphism $\overline{\Theta}$ plus the sections $s_{K(\mathcal{M})_1}, s_{K(\mathcal{M})_2}$ yield a symmetric theta structure

$$\Theta\colon \mathcal{H}(\delta_{\mathcal{M}}) \xrightarrow{\sim} \mathcal{G}(\mathcal{M}).$$

Extending Θ. Given $(Y, \mathcal{M}, \Theta)$ as above, we want to extend Θ to a symmetric theta structure on $(Y, \mathcal{M}^\beta)$. In a second step, we will say how to do so while remaining compatible with the descent datum $\widetilde{G'}$, and therefore being f'-compatible with $\Theta_{\mathcal{L}}$.

Lemma 4.5. *There exists a symmetric theta structure $\Theta_{\mathcal{M}^\beta}$ on $(X, \mathcal{M}^\beta)$ that extends Θ.*

Proof. Observe that $\mathcal{M}$ and $\mathcal{M}^\beta$ are of type $\delta_{\mathcal{M}} = (n, \dots, n) \in \mathbb{Z}^g$ and $\delta_{\mathcal{M}^\beta} = (n, \dots, n, \ell n) \in \mathbb{Z}^g$ respectively. Also,

$$K(\mathcal{M}) = Y[n]$$

and

$$K(\mathcal{M}^\beta) = K(\mathcal{M}^\beta)[n] \oplus K(\mathcal{M}^\beta)[\ell] = Y[n] \oplus K(\mathcal{M}^\beta)[\ell].$$

Hence, we have $K(\delta_{\mathcal{M}}) \subset K(\delta_{\mathcal{M}^\beta})$ and $K(\mathcal{M}) \subset K(\mathcal{M}^\beta)$ and the symplectic isomorphism $\overline{\Theta}\colon K(\delta_{\mathcal{M}}) \xrightarrow{\sim} K(\mathcal{M})$ can be extended to a symplectic isomorphism

$$\overline{\Theta}_{\mathcal{M}^\beta}\colon K(\delta_{\mathcal{M}^\beta}) \xrightarrow{\sim} K(\mathcal{M}^\beta).$$

Let

$$s_{K(\mathcal{M})_i}\colon K(\mathcal{M})_i \to \mathcal{G}(\mathcal{M}) \xrightarrow{\psi} \mathcal{G}(\mathcal{M}^\beta), \text{ for } i = 1, 2,$$

be the two group sections induced by Θ, where $K(\mathcal{M})_1 = \overline{\Theta}(\mathbb{Z}(\delta_{\mathcal{M}}))$ and $K(\mathcal{M})_2 = \overline{\Theta}(\widehat{\mathbb{Z}}(\delta_{\mathcal{M}}))$. The n-torsion part of $K(\mathcal{M}^\beta)_1 = \overline{\Theta}_{\mathcal{M}^\beta}(\mathbb{Z}(\delta_{\mathcal{M}^\beta}))$ and $K(\mathcal{M}^\beta)_2 = \overline{\Theta}_{\mathcal{M}^\beta}(\widehat{\mathbb{Z}}(\delta_{\mathcal{M}^\beta}))$ equals $K(\mathcal{M})_1$ and $K(\mathcal{M})_2$ respectively. Hence, in order to define group sections

$$s_{K(\mathcal{M}^\beta)_i}\colon K(\mathcal{M}^\beta)_i \to \mathcal{G}(\mathcal{M}^\beta), \text{ for } i = 1, 2,$$

it remains to show how to lift the ℓ-torsion part of $K(\mathcal{M}^\beta)_1$ and $K(\mathcal{M}^\beta)_2$. But this can be done in the same way as in Lemma 2.8. By Proposition 2.11, the symplectic isomorphism $\overline{\Theta}_{\mathcal{M}^\beta}$ plus the two group sections $s_{K(\mathcal{M}^\beta)_1}, s_{K(\mathcal{M}^\beta)_2}$ determine a theta structure $\Theta_{\mathcal{M}^\beta}$ on $(Y, \mathcal{M}^\beta)$. By [Mum66, §2, Rem. 2], we can suppose that $\Theta_{\mathcal{M}^\beta}$ is symmetric. □

Henceforth, we will work with the following convention: when extending $\overline{\Theta}$ to a symplectic isomorphism $\overline{\Theta}_{\mathcal{M}^\beta}\colon K(\delta_{\mathcal{M}^\beta}) \xrightarrow{\sim} K(\mathcal{M}^\beta)$, we extend the ℓ-torsion part in such a way that

$$K(\mathcal{M}^\beta)_2[\ell] = G' = \ker f'.$$

And we can extend the section $s_{K(\mathcal{M})_2}$ to a section $s_{K(\mathcal{M}^\beta)_2}\colon K(\mathcal{M}^\beta)_2 \to \mathcal{G}(\mathcal{M}^\beta)$, i.e., lifting the ℓ-torsion part of $K(\mathcal{M}^\beta)_2$, in such a way that

$$s_{K(\mathcal{M}^\beta)_2}(G') = \widetilde{G'} \subset \mathcal{G}(\mathcal{M}^\beta).$$

Simply choose a generator $t' \in G'$ and define $s_{K(\mathcal{M}^\beta)_2}(t')$ as the unique element of $\widetilde{G'}$ above t'. Imposing this choice on $s_{K(\mathcal{M}^\beta)_2}$ does not change the fact that $\Theta_{\mathcal{M}^\beta}$ is a symmetric theta structure. Indeed, $\mathcal{M}^\beta$ is totally symmetric and by [Rob10, Prop. 4.2.12], the level subgroup $\widetilde{G'}$ is what Mumford (in [Mum66]) calls a symmetric level subgroup. Finally, since $\widetilde{G'} = s_{K(\mathcal{M}^\beta)}(G')$, the theta structures $\Theta_{\mathcal{M}^\beta}$ and $\Theta_{\mathcal{L}}$ are f'-compatible and

$$f'\colon (Y, \mathcal{M}^\beta, \Theta_{\mathcal{M}^\beta}) \to (X, \mathcal{L}, \Theta_{\mathcal{L}})$$

is an isogeny of polarized abelian varieties with theta structure.

4.2.1 Applying the isogeny theorem to f'

Recall that we have as an input of the algorithm the polarized abelian variety with symmetric theta structure $(X, \mathcal{L}, \Theta_{\mathcal{L}})$, a theta null point $\widetilde{0}_X$ and an affine lift $\widetilde{t}$ of a fixed generator $t \in G(\bar{k})$, both in theta coordinates determined by $\Theta_{\mathcal{L}}$. Moreover, we have defined a f'-compatible symmetric theta structure $\Theta_{\mathcal{M}^\beta}$ on $(Y, \mathcal{M}^\beta)$ that satisfies $G' = \ker f' \subset K(\mathcal{M}^\beta)_2$. We can apply the isogeny theorem to

$$f' \colon (Y, \mathcal{M}^\beta, \Theta_{\mathcal{M}^\beta}) \to (X, \mathcal{L}, \Theta_{\mathcal{L}}),$$

stating that there exists a constant $\lambda \in \bar{k}^\times$, such that for all $y \in Y(\bar{k})$ and $i \in K(\mathcal{L})_1$ we have

$$\theta_i^{\Theta_{\mathcal{L}}}(f'(y)) = \lambda \cdot \sum_{\substack{j \in K(\mathcal{M}^\beta)_1 \\ f'(j) = i}} \theta_j^{\Theta_{\mathcal{M}^\beta}}(y).$$

The isogeny f' in affine coordinates

$$\widetilde{f'} \colon \widetilde{Y} \to \widetilde{X} \tag{4.1}$$

sends an affine lift $\widetilde{y}$ of y to the affine lift $\widetilde{f'}(\widetilde{y})$ of $f'(y)$, given by

$$\theta_i^{\Theta_{\mathcal{L}}}(\widetilde{f'}(\widetilde{y})) = \sum_{\substack{j \in K(\mathcal{M}^\beta)_1 \\ f'(j) = i}} \theta_j^{\Theta_{\mathcal{M}^\beta}}(\widetilde{y}),$$

for all $i \in K(\mathcal{L})_1$. But f' is injective on $K(\mathcal{M}^\beta)_1$, since $\ker f' \subset K(\mathcal{M}^\beta)_2$. Hence,

$$\theta_i^{\Theta_{\mathcal{L}}}(\widetilde{f'}(\widetilde{y})) = \theta_j^{\Theta_{\mathcal{M}^\beta}}(\widetilde{y}), \tag{4.2}$$

where $j \in K(\mathcal{M}^\beta)_1[n]$ is the unique element of $K(\mathcal{M}^\beta)_1$ that satisfies $f'(j) = i$.

Remark 4.6. This allows us to "partially invert" the isogeny theorem in the sense that: knowing the affine theta null point $\widetilde{0}_X$ for $(X, \mathcal{L}, \Theta_{\mathcal{L}})$, Equation (4.2) fixes an affine theta null point $\widetilde{0}_Y$ for $(Y, \mathcal{M}^\beta, \Theta_{\mathcal{M}^\beta})$ and gives n^g out of the $n^g \ell$ affine coordinates of $\widetilde{0}_Y$. Writing each $j \in K(\mathcal{M}^\beta)_1$ as $j = j_n + j_\ell$, with $j_n \in K(\mathcal{M}^\beta)_1[n]$ and $j_\ell \in K(\mathcal{M}^\beta)_1[\ell]$, we obtain precisely the n^g affine coordinates $\theta_j^{\Theta_{\mathcal{M}^\beta}}(\widetilde{0}_Y)$ for which $j_\ell = 0$.

However, there is no obvious way we could obtain the remaining $n^g(\ell - 1)$ affine coordinates of $\widetilde{0}_Y$.

Wish scenario. Suppose for a moment we were in the situation where we knew the affine theta null point $\widetilde{0}_Y$ for $(Y, \mathcal{M}^\beta, \Theta_{\mathcal{M}^\beta})$ induced by $\widetilde{0}_X$ and $\widetilde{f'}$ as in Remark 4.6 (i.e. we knew all the $n^g \ell$ affine coordinates). This would then determine affine lifts for every element in $G = \ker f$. For a comparison, there are ℓ elements in G, each admitting n^g affine theta coordinates for $(X, \mathcal{L}, \Theta_{\mathcal{L}})$.

The symplectic decomposition of $K(\mathcal{M}^\beta)[\ell] = \ker \beta$ induced by $\overline{\Theta}_{\mathcal{M}^\beta}$ is

$$K(\mathcal{M}^\beta)[\ell] = K(\mathcal{M}^\beta)_1[\ell] \oplus G',$$

and since $f \circ f' = \beta$, the isogeny f' restricts to an isomorphism

$$K(\mathcal{M}^\beta)_1[\ell] \xrightarrow{\sim} G.$$

Let t be the fixed generator of G and let $\tau := (f')^{-1}(t) \in K(\mathcal{M}^\beta)_1[\ell]$. We can use the action of the theta group $\mathcal{G}(\mathcal{M}^\beta)$ on the affine theta coordinates for $(Y, \mathcal{M}^\beta, \Theta_{\mathcal{M}^\beta})$ to obtain affine lifts of $t, 2t, \ldots, (\ell-1)t$ for $(X, \mathcal{L}, \Theta_{\mathcal{L}})$. By Proposition 2.18,

$$\widetilde{\tau} := \tau \boxplus \widetilde{0}_Y$$

(see Notation 2.19) is an affine lift of τ for $(Y, \mathcal{M}^\beta, \Theta_{\mathcal{M}^\beta})$ with jth coordinate given by

$$\theta_j^{\Theta_{\mathcal{M}^\beta}}(\widetilde{\tau}) = \theta_{j+\tau}^{\Theta_{\mathcal{M}^\beta}}(\widetilde{0}_Y),$$

for all $j \in K(\mathcal{M}^\beta)_1$. By (4.2), the n^g coordinates $\theta_j^{\Theta_{\mathcal{M}^\beta}}(\widetilde{\tau})$ with $j \in K(\mathcal{M}^\beta)_1[n]$ determine an affine lift $\widetilde{t} = \widetilde{f'}(\widetilde{\tau})$ of t, with ith affine coordinate (for $i \in K(\mathcal{L})_1$) given by

$$\theta_i^{\Theta_{\mathcal{L}}}(\widetilde{t}) = \theta_j^{\Theta_{\mathcal{M}^\beta}}(\widetilde{\tau}) = \theta_{j+\tau}^{\Theta_{\mathcal{M}^\beta}}(\widetilde{0}_Y), \tag{4.3}$$

where j is the unique element of $K(\mathcal{M}^\beta)_1[n]$ that satisfies $f'(j) = i$. Continuing this way, we obtain affine lifts $\widetilde{2t}, \ldots, \widetilde{(\ell-1)t}$ of $2t, \ldots, (\ell-1)t$ respectively, with affine coordinates

$$\begin{aligned} \theta_i^{\Theta_{\mathcal{L}}}(\widetilde{2t}) &= \theta_{j+2\tau}^{\Theta_{\mathcal{M}^\beta}}(\widetilde{0}_Y), \\ &\vdots \\ \theta_i^{\Theta_{\mathcal{L}}}(\widetilde{(\ell-1)t}) &= \theta_{j+(\ell-1)\tau}^{\Theta_{\mathcal{M}^\beta}}(\widetilde{0}_Y), \end{aligned} \tag{4.4}$$

for all $i \in K(\mathcal{L})_1$. Again, for $i \in K(\mathcal{L})_1$ we write $j \in K(\mathcal{M}^\beta)_1[n]$ for the unique element of $K(\mathcal{M}^\beta)_1$ that satisfies $f'(j) = i$. Written more compactly, we have

$$\widetilde{t} = \widetilde{f'}(\tau \boxplus \widetilde{0}_Y),\ \widetilde{2t} = \widetilde{f'}(2\tau \boxplus \widetilde{0}_Y), \ldots, \widetilde{(\ell-1)t} = \widetilde{f'}((\ell-1)\tau \boxplus \widetilde{0}_Y).$$

Back to reality. Unfortunately we are not given the theta null point $\widetilde{0}_Y$ for $(Y, \mathcal{M}^\beta, \Theta_{\mathcal{M}^\beta})$, but only the theta null point $\widetilde{0}_X$ for $(X, \mathcal{L}, \Theta_{\mathcal{L}})$. Yet, we have seen that $\widetilde{0}_X$ fixes a theta null point $\widetilde{0}_Y$, which in return fixes affine lifts $\widetilde{t}, \ldots, \widetilde{(\ell-1)t}$ of $t, \ldots, (\ell-1)t$ respectively. This motivates the following definition.

Definition 4.7. Let $\widetilde{0}_X$ be a fixed theta null point for $(X, \mathcal{L}, \Theta_{\mathcal{L}})$ (e.g. the input of the algorithm). Let $\widetilde{0}_Y$ be the corresponding theta null point for $(Y, \mathcal{M}^\beta, \Theta_{\mathcal{M}^\beta})$ from Remark 4.6, i.e. the unique lift $\widetilde{0}_Y$ of 0_Y that satisfies $\widetilde{0}_X = \widetilde{f'}(\widetilde{0}_Y)$. For $1 \leq u \leq \ell - 1$, the affine lift $\widetilde{f'}(u\tau \boxplus \widetilde{0}_Y)$ of ut is called the compatible lift and is denoted by

$$\widetilde{ut}_c = \widetilde{f'}(u\tau \boxplus \widetilde{0}_Y).$$

The advantage of knowing the compatible lifts is that if we were given $\widetilde{0}_X$ and $\widetilde{t}_c, \ldots, \widetilde{(\ell-1)t}_c$, we could "patch" the coordinates together (in the sense of (4.3) and (4.4)) and obtain the theta null point $\widetilde{0}_Y$. In our case, the input of the algorithm provides us with an (arbitrary) affine lift $\widetilde{t}$ of the generator t of G. There is absolutely no reason this lift should be equal to the compatible lift $\widetilde{t}_c$. We can compute lifts of $2t, \ldots, (\ell-1)t$ using `chain_mult` from Section 1.3, but again, there is no reason these lifts should be equal to the compatible lifts $\widetilde{2t}_c, \ldots, \widetilde{(\ell-1)t}_c$. Hence, we cannot simply patch together the ℓ-times n^g affine coordinates and hope to get the theta null point $\widetilde{0}_Y$.

The fact of not knowing $\widetilde{0}_Y$ seems to be a serious problem for the further steps of the algorithm. Yet, we will see that the compatible lifts satisfy a certain property (they are excellent lifts, in the sense of [Rob10]) and that we can compute them up to ℓth roots of unity. To be more precise, for all $1 \leq u \leq \ell - 1$, we can compute the lift

$$\zeta_t^{u^2} \cdot \widetilde{ut}_c,$$

where ζ_t is some unknown ℓth root of unity. This still does not allow us to obtain a theta null point for $(Y, \mathcal{M}^\beta, \Theta_{\mathcal{M}^\beta})$, but as will turn out in Section 4.4.2, we will not need to know the exact value of ζ_t to be able to compute a theta null point for $(Y, \mathcal{M})$, the desired output of the algorithm.

4.3 Endomorphisms of Y^r

So far, we have considered the isogeny $f' \colon (Y, \mathcal{M}^\beta, \Theta_{\mathcal{M}^\beta}) \to (X, \mathcal{L}, \Theta_{\mathcal{L}})$. This did not allow us to obtain a theta null point $\widetilde{0}_Y$ for $(Y, \mathcal{M}^\beta, \Theta_{\mathcal{M}^\beta})$. However, as we will explain in Section 4.4.1, we can compute the ℓ-times n^g affine coordinates

$$\begin{aligned}
\theta_j^{\Theta_{\mathcal{M}^\beta}}(\widetilde{0}_Y) &= \theta_i^{\Theta_{\mathcal{L}}}(\widetilde{0}_X), \\
\zeta_t \cdot \theta_{j+\tau}^{\Theta_{\mathcal{M}^\beta}}(\widetilde{0}_Y) &= \theta_i^{\Theta_{\mathcal{L}}}(\zeta_t \cdot \widetilde{t}_c), \\
&\vdots \\
\zeta_t^{(\ell-1)^2} \cdot \theta_{j+(\ell-1)\tau}^{\Theta_{\mathcal{M}^\beta}}(\widetilde{0}_Y) &= \theta_i^{\Theta_{\mathcal{L}}}(\zeta_t^{(\ell-1)^2} \cdot \widetilde{(\ell-1)t}_c),
\end{aligned} \tag{4.5}$$

where $\widetilde{0}_Y$ is the affine lift of 0_Y from Definition 4.7, ζ_t is an unknown ℓth root of unity, j runs over $K(\mathcal{M}^\beta)_1[n]$ and $i = f'(j)$ runs over $K(\mathcal{L})_1$. We will show in Section 4.4.2 how to get rid of the ambiguity due to ζ_t.

For the rest of this section, let us suppose we knew a theta null point $\widetilde{0}_Y$ for $(Y, \mathcal{M}^\beta, \Theta_{\mathcal{M}^\beta})$. We could then, similar to the idea in Section 4.1, try to apply the isogeny theorem to an endomorphism $u \in \mathrm{End}(Y)$ that satisfies $\bar{u}u = \beta$. Indeed, we then have $u^*\mathcal{M} \cong \mathcal{M}^\beta$. But such an endomorphism need not exist, so we cannot rely on it. Instead, we use an idea appearing in [CR11] and motivated by Zarhin's trick [Mil86, Rem. 16.12], used to show that for any abelian variety X, the abelian variety $(X \times \widehat{X})^4$ is principally polarizable. Note that for any integer $r \geq 1$, the endomorphism β induces an endomorphism $\beta^{\times r} \colon Y^r \to Y^r$ of the r-fold product Y^r. Choosing $r > 1$ allows to search for an endomorphism $F \in \mathrm{End}(Y^r)$ that satisfies $\bar{F}F = \beta^{\times r}$. If for example $r = 4$, we know by [Sie21] that any totally positive element of $\mathcal{O}_{K_0}$ is the sum of four squares of algebraic numbers in the same field, i.e. there exist $\alpha_1, \ldots, \alpha_4 \in K_0$ that satisfy $\beta = \alpha_1^2 + \cdots + \alpha_4^2$ (see Algorithm 1). In general, the α_i's need not be integral and hence, need not be in $\mathrm{End}^+(Y)$. Yet, assuming they yield endomorphisms of the ℓ-torsion and the n-torsion subgroups (which is the case since $[\mathcal{O}_{K_0} : \mathbb{Z}[\pi + \pi^\dagger]]$ is assumed coprime to ℓn, i.e. the denominators of the α_i's are coprime to ℓn), one can take F to be the endomorphism whose matrix $M_F \in \mathbf{Mat}_4(\mathrm{End}^+(Y))$ corresponds to left multiplication by $\alpha_1 + \alpha_2 i + \alpha_3 j + \alpha_4 k$ on the Hamilton quaternions over K_0, i.e.

$$M_F = \begin{pmatrix} \alpha_1 & -\alpha_2 & -\alpha_3 & -\alpha_4 \\ \alpha_2 & \alpha_1 & -\alpha_4 & \alpha_3 \\ \alpha_3 & \alpha_4 & \alpha_1 & -\alpha_2 \\ \alpha_4 & -\alpha_3 & \alpha_2 & \alpha_1 \end{pmatrix}.$$

We then have $\bar{F}F = \beta^{\times 4}$, since $M_{\bar{F}} = {}^tM_F$ and ${}^tM_F \cdot M_F = \beta I_4$.

In case β can be written as the sum of two squares of algebraic numbers, $\beta = \alpha_1^2 + \alpha_2^2$, we take $F \in \mathrm{End}(Y^2)$ to be the endomorphism whose matrix is

$$M_F = \begin{pmatrix} \alpha_1 & -\alpha_2 \\ \alpha_2 & \alpha_1 \end{pmatrix}.$$

Let $r = 2$ or $r = 4$ and let $F \in \mathrm{End}(Y^r)$ be such that $\bar{F}F = \beta^{\times r}$. It is easy to see that $F^*\mathcal{M}_0^{\star r}$ has polarization isogeny $\phi_{F^*\mathcal{M}_0^{\star r}} = \phi_{\mathcal{M}_0^{\star r}} \circ \beta^{\times r} = \phi_{(\mathcal{M}_0^{\beta})^{\star r}}$ and hence,

$$F^*\mathcal{M}^{\star r} \cong (\mathcal{M}^{\beta})^{\star r},$$

both being totally symmetric. Consider the r-fold product theta structure $\Theta_{(\mathcal{M}^{\beta})^{\star r}}$ on $(Y^r, (\mathcal{M}^{\beta})^{\star r})$ determined by $\Theta_{\mathcal{M}^{\beta}}$ as in Section 2.2.4. Then, $\Theta_{(\mathcal{M}^{\beta})^{\star r}}$ is easily seen to be symmetric and by [Rob10, Rem. 4.2.15], it is also compatible with the descent datum associated to $\mathcal{M}^{\star r}$ and the isomorphism $F^*\mathcal{M}^{\star r} \cong (\mathcal{M}^{\beta})^{\star r}$. Let $\Theta'_{\mathcal{M}^{\star r}}$ be the induced F-compatible theta structure on $(Y^r, \mathcal{M}^{\star r})$ as in Proposition 2.24. By [Rob10, Rem. 4.2.15], the theta structure $\Theta'_{\mathcal{M}^{\star r}}$ is symmetric as well. We have an isogeny of polarized abelian varieties with theta structure

$$F\colon (Y^r, (\mathcal{M}^{\beta})^{\star r}, \Theta_{(\mathcal{M}^{\beta})^{\star r}}) \to (Y^r, \mathcal{M}^{\star r}, \Theta'_{\mathcal{M}^{\star r}}).$$

The isogeny theorem applied to F states that there exists $\lambda \in \overline{k}^{\times}$, such that for all $\mathbf{y} = (y_1, \ldots, y_r) \in Y^r(\overline{k})$ and $\mathbf{k} \in K(\mathcal{M}^{\star r})_1$ we have

$$\theta^{\Theta'_{\mathcal{M}^{\star r}}}_{\mathbf{k}}(F(\mathbf{y})) = \lambda \cdot \sum_{\substack{\boldsymbol{\tau} \in K((\mathcal{M}^{\beta})^{\star r})_1[\ell] \\ F(\boldsymbol{\tau})=0}} \theta^{\Theta_{(\mathcal{M}^{\beta})^{\star r}}}_{\mathbf{j}+\boldsymbol{\tau}}(\mathbf{y}) = \lambda \cdot \sum_{\substack{\boldsymbol{\tau} \in K((\mathcal{M}^{\beta})^{\star r})_1[\ell] \\ F(\boldsymbol{\tau})=0}} \prod_{s=1}^{r} \theta^{\Theta_{\mathcal{M}^{\beta}}}_{j_s+\tau_s}(y_s),$$

where $\mathbf{j} = (j_1, \ldots, j_r) \in K((\mathcal{M}^{\beta})^{\star r})_1[n]$ is the unique element of $K((\mathcal{M}^{\beta})^{\star r})_1$ that satisfies $F(\mathbf{j}) = \mathbf{k}$. Here, we have used the fact that $K((\mathcal{M}^{\beta})^{\star r})_1 = K((\mathcal{M}^{\beta})^{\star r})_1[n] \oplus K((\mathcal{M}^{\beta})^{\star r})_1[\ell]$, that $\mathbf{k} \in X^r[n]$ and that $\ker F \subset Y^r[\ell]$. Specializing to $\mathbf{y} = 0_{Y^r}$, we obtain

$$\theta^{\Theta'_{\mathcal{M}^{\star r}}}_{\mathbf{k}}(0_{Y^r}) = \lambda \cdot \sum_{\substack{\boldsymbol{\tau} \in K((\mathcal{M}^{\beta})^{\star r})_1[\ell] \\ F(\boldsymbol{\tau})=0}} \prod_{s=1}^{r} \theta^{\Theta_{\mathcal{M}^{\beta}}}_{j_s+\tau_s}(0_Y).$$

The affine version of F

$$\widetilde{F}\colon \widetilde{Y}^r \to \widetilde{Y}^r$$

is given by

$$\theta^{\Theta'_{\mathcal{M}^{\star r}}}_{\mathbf{k}}(\widetilde{F}(\widetilde{\mathbf{y}})) = \sum_{\substack{\boldsymbol{\tau} \in K((\mathcal{M}^{\beta})^{\star r})_1[\ell] \\ F(\boldsymbol{\tau})=0}} \prod_{s=1}^{r} \theta^{\Theta_{\mathcal{M}^{\beta}}}_{j_s+\tau_s}(\widetilde{y}_s), \tag{4.6}$$

and in particular

$$\theta^{\Theta'_{\mathcal{M}^{\star r}}}_{\mathbf{k}}(\widetilde{0}_{Y^r}) = \sum_{\substack{\boldsymbol{\tau} \in K((\mathcal{M}^{\beta})^{\star r})_1[\ell] \\ F(\boldsymbol{\tau})=0}} \prod_{s=1}^{r} \theta^{\Theta_{\mathcal{M}^{\beta}}}_{j_s+\tau_s}(\widetilde{0}_Y). \tag{4.7}$$

Hence, (4.7) allows us to compute a theta null point $\widetilde{0}_{Y^r}$ for $(Y^r, \mathcal{M}^{\star r}, \Theta'_{\mathcal{M}^{\star r}})$. Yet, there are two major obstacles that we have to overcome:

i) As mentioned at the beginning of this section, we do not know the theta null point $\widetilde{0}_Y$ for $(Y, \mathcal{M}^\beta, \Theta_{\mathcal{M}^\beta})$. We know ℓ "parts" of it, each up to an unknown root of unity, see (4.5). Hence, when trying to evaluate the right-hand side of (4.7), what we substitute for $\theta^{\Theta_{\mathcal{M}^\beta}}_{j_s+\tau_s}(\widetilde{0}_Y)$ is the $(j_s+\tau_s)$th coordinate we have at our disposal, which differs from the correct value by an ℓth root of unity. We will show in Section 4.4.2 that we can still correctly compute $\widetilde{0}_{Y^r}$ this way.

ii) There is no reason the theta structure $\Theta'_{\mathcal{M}^{\star r}}$ is of product form, i.e. an r-fold product theta structure. If it were the product of say $\Theta'_{\mathcal{M}}$ (a theta structure on $(Y, \mathcal{M})$), then the coordinates for $\Theta'_{\mathcal{M}^{\star r}}$ would be given by

$$\theta^{\Theta'_{\mathcal{M}^{\star r}}}_{\mathbf{k}} = \theta^{\Theta'_{\mathcal{M}}}_{k_1} \otimes \cdots \otimes \theta^{\Theta'_{\mathcal{M}}}_{k_r},$$

for all $\mathbf{k} = (k_1, \ldots, k_r) \in K(\mathcal{M}^{\star r})_1$, and one could easily obtain the (projective) theta coordinates for a single factor $(Y, \mathcal{M}, \Theta'_{\mathcal{M}})$. What we do in Section 4.5 is to seek for a metaplectic automorphism of $\mathcal{H}(\delta_{\mathcal{M}^{\star r}})$ that turns $\Theta'_{\mathcal{M}^{\star r}}$ into product form and then apply the symplectic transformation formula to the theta coordinates for $(Y^r, \mathcal{M}^{\star r}, \Theta'_{\mathcal{M}^{\star r}})$. If the new theta structure on $(Y^r, \mathcal{M}^{\star r})$ is the r-fold product of say $\Theta_{\mathcal{M}}$, then we can obtain the (projective) theta coordinates of 0_Y for $(Y, \mathcal{M}, \Theta_{\mathcal{M}})$.

4.3.1 Computing $\alpha_1, \ldots, \alpha_r$

We give an algorithm for the case $g = 2$ and $r = 4$. In this case, β is a totally positive element in the real quadratic number field K_0, and $N_{K_0/\mathbb{Q}}(\beta) = \ell$. Let $T = T_{K_0/\mathbb{Q}}(\beta) \in \mathbb{Z}$ be the trace of β. Then β is a root of the polynomial $x^2 - Tx + \ell \in \mathbb{Z}[x]$. Let $a_1, \ldots, a_4 \in \mathbb{Z}_{\geq 0}$ be integers satisfying $a_1^2 + \cdots + a_4^2 = \ell$. Since β is real, we have $T^2 > 4\ell$, and thus $|T| > 2\sqrt{\ell} \geq 2a_1$. Moreover, β is totally positive and hence, we have $T > 0$. Let $b_1, \cdots, b_4 \in \mathbb{Z}_{\geq 0}$ be such that $b_1^2 + \cdots + b_4^2 = T - 2a_1$. We have

$$\begin{aligned}(a_1 - \beta)^2 + a_2^2 + a_3^2 + a_4^2 &= \ell - 2a_1\beta + \beta^2 \\ &= \ell - T\beta + \beta^2 + (b_1^2 + \cdots + b_4^2)\beta \\ &= (b_1^2 + \cdots + b_4^2)\beta.\end{aligned}$$

If we let

$$M = \begin{pmatrix} a_1 - \beta & -a_2 & -a_3 & -a_4 \\ a_2 & a_1 - \beta & -a_4 & a_3 \\ a_3 & a_4 & a_1 - \beta & -a_2 \\ a_4 & -a_3 & a_2 & a_1 - \beta \end{pmatrix} \in \mathbf{Mat}_4(K_0), \tag{4.8}$$

then the linear isomorphism

$$K_0^4 \to K_0^4,\ c \mapsto Mc$$

sends an element of squared norm $\|c\|^2$ to an element of squared norm

$$\|Mc\|^2 = ((a_1 - \beta)^2 + a_2^2 + a_3^2 + a_4^2)\|c\|^2 = (b_1^2 + \cdots + b_4^2)\beta\|c\|^2.$$

Here, the word squared norm is used for the sum of the squares of a vector in K_0^4, and should not be confused with the norm $N_{K_0/\mathbb{Q}}$ on K_0. It suffices then to find a vector $c \in K_0^4$ of squared norm $\|c\|^2 = \frac{1}{b_1^2 + \cdots + b_4^2}$. The columns of the matrix

$$N = \begin{pmatrix} b_1 & -b_2 & -b_3 & -b_4 \\ b_2 & b_1 & -b_4 & b_3 \\ b_3 & b_4 & b_1 & -b_2 \\ b_4 & -b_3 & b_2 & b_1 \end{pmatrix} \in \mathbf{Mat}_4(K_0) \tag{4.9}$$

are pairwise orthogonal, and of squared norm $b_1^2 + \cdots + b_4^2$. Hence, the columns of N^{-1} are pairwise orthogonal too and of squared norm $\frac{1}{b_1^2+\cdots+b_4^2}$. Taking c to be the first column of N^{-1}, we have $Mc \in K_0^4$ and $\|Mc\|^2 = \beta$. That is, β is a sum of four squares.

Algorithm 1 Computing $\alpha_1, \ldots, \alpha_4$ in case $[K_0 : \mathbb{Q}] = 2$

Require: $\beta \in \mathcal{O}_{K_0}$ totally positive
Ensure: $\alpha_1, \ldots, \alpha_4 \in K_0$ satisfying $\beta = \alpha_1^2 + \cdots + \alpha_4^2$
1: compute $a_1, \ldots, a_4 \in \mathbb{Z}_{\geq 0}$ such that $a_1^2 + \cdots + a_4^2 = N_{K_0/\mathbb{Q}}(\beta)$
2: compute $b_1, \ldots, b_4 \in \mathbb{Z}_{\geq 0}$ such that $b_1^2 + \cdots + b_4^2 = T_{K_0/\mathbb{Q}}(\beta) - 2a_1$
3: compute $N^{-1} \in \mathbf{Mat}_4(K_0)$, where N is as in (4.9)
4: **return** Mc, where M is as in (4.8) and c is the first column of N^{-1}

4.4 Computing the theta null point $\widetilde{0}_{Y^r}$ for $(Y^r, \mathcal{M}^{\star r}, \Theta'_{\mathcal{M}^{\star r}})$

This section is about how to correctly compute the right-hand side of (4.7). Let $\widetilde{0}_X$ and $\widetilde{t}$ be the affine lifts given as input of the algorithm, both in theta coordinates for $(X, \mathcal{L}, \Theta_{\mathcal{L}})$. Here, t is a fixed generator of the kernel G of f, $\mathcal{L}$ is a totally symmetric line bundle of type $\delta_{\mathcal{L}} = (n, \ldots, n)$ on X, for $n = 2$ or $n = 4$, and $\Theta_{\mathcal{L}}$ is a symmetric theta structure on $(X, \mathcal{L})$. Let $(Y, \mathcal{M}^\beta, \Theta_{\mathcal{M}^\beta})$ be the polarized abelian variety with theta structure from Section 4.2.1, and let

$$f' \colon (Y, \mathcal{M}^\beta, \Theta_{\mathcal{M}^\beta}) \to (X, \mathcal{L}, \Theta_{\mathcal{L}})$$

be the β-contragredient isogeny of polarized abelian varieties with theta structure.

Recall the algorithm $\texttt{chain\_mult}(m, \widetilde{x}, \widetilde{0}_X)$ from [Rob10, §4.4] and Section 1.3 that, given $m \in \mathbb{Z}$, an affine lift $\widetilde{x}$ and a theta null point $\widetilde{0}_X$ for $(X, \mathcal{L}, \Theta_{\mathcal{L}})$, computes an affine lift of mx. The compatible lift $\widetilde{t}_c$ of t, as defined in Definition 4.7, satisfies a certain property, following [Rob10, §7.4].

Definition 4.8. A lift $\widetilde{x}$ of $x \in X[\ell]$ is called excellent with respect to $(X, \mathcal{L}, \Theta_{\mathcal{L}}, \widetilde{0}_X)$ if

$$\texttt{chain\_mult}(m+1, \widetilde{x}, \widetilde{0}_X) = -\texttt{chain\_mult}(m, \widetilde{x}, \widetilde{0}_X),$$

where $\ell = 2m + 1$ and the lift $-\texttt{chain\_mult}(m, \widetilde{x}, \widetilde{0}_X)$ is as in Proposition 2.35.

By [LR12, Lem. 3.10], for any $u \in \mathbb{Z}$ and $\lambda \in \bar{k}^\times$ we have

$$\texttt{chain\_mult}(u, \lambda \cdot \widetilde{x}, \widetilde{0}_X) = \lambda^{u^2} \cdot \texttt{chain\_mult}(u, \widetilde{x}, \widetilde{0}_X).$$

To compute an excellent lift of t, we look for a scalar $\lambda_t \in \bar{k}^\times$ such that $\lambda_t \cdot \widetilde{t}$ is excellent. Using that

$$\texttt{chain\_mult}(m+1, \lambda_t \cdot \widetilde{t}, \widetilde{0}_X) = \lambda_t^{(m+1)^2} \cdot \texttt{chain\_mult}(m+1, \widetilde{t}, \widetilde{0}_X)$$

and

$$\texttt{chain\_mult}(m, \lambda_t \cdot \widetilde{t}, \widetilde{0}_X) = \lambda_t^{m^2} \cdot \texttt{chain\_mult}(m, \widetilde{t}, \widetilde{0}_X),$$

the lift $\lambda_t \cdot \widetilde{t}$ is excellent if

$$\lambda_t^\ell \cdot \texttt{chain\_mult}(m+1, \widetilde{t}, \widetilde{0}_X) = -\texttt{chain\_mult}(m, \widetilde{t}, \widetilde{0}_X).$$

This determines λ_t^ℓ uniquely. Hence, for any ℓth root λ_t of λ_t^ℓ, the lift $\lambda_t \cdot \widetilde{t}$ is excellent.

Algorithm 2 Computing an excellent lift of t

Require: lifts $\widetilde{t}$ and $\widetilde{0}_X$ of t and 0_X for $(X, \mathcal{L}, \Theta_{\mathcal{L}})$ respectively
Ensure: an excellent lift $\widetilde{t}_e$ with respect to $(X, \mathcal{L}, \Theta_{\mathcal{L}}, \widetilde{0}_X)$
1: compute $\texttt{chain\_mult}(m, \widetilde{t}, \widetilde{0}_X)$ and $\texttt{chain\_mult}(m+1, \widetilde{t}, \widetilde{0}_X)$, where $\ell = 2m+1$
2: compute the scalar $\kappa \in \bar{k}^\times$ such that

$$\kappa \cdot \texttt{chain\_mult}(m+1, \widetilde{t}, \widetilde{0}_X) = -\texttt{chain\_mult}(m, \widetilde{t}, \widetilde{0}_X),$$

where $-\texttt{chain\_mult}(m, \widetilde{t}, \widetilde{0}_X)$ is as in Proposition 2.35
3: compute $\lambda_t \in \bar{k}^\times$ such that $\lambda_t^\ell = \kappa$
4: **return** $\lambda_t \cdot \widetilde{t}$

We will analyse the complexity of Algorithm 2 in Section 6.

4.4.1 The compatible lifts are excellent lifts

We will show that the compatible lift $\widetilde{t}_c = \widetilde{f}'(\tau \boxplus \widetilde{0}_Y)$ is an excellent lift with respect to $(X, \mathcal{L}, \Theta_{\mathcal{L}}, \widetilde{0}_X)$, and that for all $2 \le u \le \ell - 1$, we have

$$\widetilde{ut}_c = \texttt{chain\_mult}(u, \widetilde{t}_c, \widetilde{0}_X).$$

Hence, when computing an excellent lift $\widetilde{t}_e$ of t, it will differ from $\widetilde{t}_c$ by some ℓth root of unity ζ_t, i.e.

$$\widetilde{t}_e = \zeta_t \cdot \widetilde{t}_c.$$

Let us recall Lemma 3.9 and Corollaries 3.16 and 3.17 from [LR12].

Lemma 4.9. *Let $\widetilde{f}' \colon \widetilde{Y} \to \widetilde{X}$ be the affine version of $f' \colon (Y, \mathcal{M}^\beta, \Theta_{\mathcal{M}^\beta}) \to (X, \mathcal{L}, \Theta_{\mathcal{L}})$ as in (4.1). Let $\widetilde{0}_X$ be a fixed theta null point for $(X, \mathcal{L}, \Theta_{\mathcal{L}})$ and let $\widetilde{0}_Y$ be the unique theta null point for $(Y, \mathcal{M}^\beta, \Theta_{\mathcal{M}^\beta})$ that satisfies $\widetilde{f}'(\widetilde{0}_Y) = \widetilde{0}_X$. For all $z, z' \in K(\mathcal{M}^\beta)$ and $\widetilde{y}, \widetilde{y}', \widetilde{y - y'} \in \widetilde{Y}$, we have*

i) $-(z \boxplus \widetilde{0}_Y) = (-z) \boxplus \widetilde{0}_Y$;

ii) $(z+z') \boxplus \texttt{chain\_add}(\widetilde{y}, \widetilde{y}', \widetilde{y - y'}, \widetilde{0}_Y) = \texttt{chain\_add}(z \boxplus \widetilde{y}, z' \boxplus \widetilde{y}', (z-z') \boxplus \widetilde{y - y'}, \widetilde{0}_Y)$;

iii) $\widetilde{f}'(\texttt{chain\_add}(\widetilde{y}, \widetilde{y}', \widetilde{y - y'}, \widetilde{0}_Y)) = \texttt{chain\_add}(\widetilde{f}'(\widetilde{y}), \widetilde{f}'(\widetilde{y}'), \widetilde{f}'(\widetilde{y - y'}), \widetilde{0}_X)$.

We can show:

Lemma 4.10. *Let $z \in K(\mathcal{M}^\beta)$ and let $u \in \mathbb{Z}_{\ge 0}$. Then, for any $\widetilde{y}, \widetilde{y}', \widetilde{y + y'} \in \widetilde{Y}$, we have*

$$\texttt{chain\_mult}(u, z \boxplus \widetilde{y}, \widetilde{0}_Y) = uz \boxplus \texttt{chain\_mult}(u, \widetilde{y}, \widetilde{0}_Y)$$

and

$$\texttt{chain\_multtadd}(u, z \boxplus \widetilde{y + y'}, z \boxplus \widetilde{y}, \widetilde{y}', \widetilde{0}_Y) = uz \boxplus \texttt{chain\_multtadd}(u, \widetilde{y + y'}, \widetilde{y}, \widetilde{y}', \widetilde{0}_Y).$$

Proof. Let us first recall that $\texttt{chain\_mult}(u, \widetilde{y}, \widetilde{0}_Y)$ is defined as

$$\texttt{chain\_mult}(u, \widetilde{y}, \widetilde{0}_Y) = \texttt{chain\_multadd}(u, \widetilde{y}, \widetilde{y}, \widetilde{0}_Y, \widetilde{0}_Y),$$

and that we compute $\texttt{chain\_multadd}(u, \widetilde{y}, \widetilde{y}, \widetilde{0}_Y, \widetilde{0}_Y)$ recursively as

$$\begin{aligned}&\texttt{chain\_multadd}(u, \widetilde{y}, \widetilde{y}, \widetilde{0}_Y, \widetilde{0}_Y) \qquad (4.10)\\ &= \texttt{chain\_add}(\texttt{chain\_multadd}(u-1, \widetilde{y}, \widetilde{y}, \widetilde{0}_Y, \widetilde{0}_Y), \widetilde{y}, \texttt{chain\_multadd}(u-2, \widetilde{y}, \widetilde{y}, \widetilde{0}_Y, \widetilde{0}_Y), \widetilde{0}_Y).\end{aligned}$$

Hence, we can write $\texttt{chain\_mult}(u, \widetilde{y}, \widetilde{0}_Y)$ recursively as

$$\texttt{chain\_mult}(u, \widetilde{y}, \widetilde{0}_Y) = \texttt{chain\_add}(\texttt{chain\_mult}(u-1, \widetilde{y}, \widetilde{0}_Y), \widetilde{y}, \texttt{chain\_mult}(u-2, \widetilde{y}, \widetilde{0}_Y), \widetilde{0}_Y).$$

Note that we have

$$\begin{aligned}&\texttt{chain\_mult}(0, \widetilde{y}, \widetilde{0}_Y) = \widetilde{0}_Y,\\ &\texttt{chain\_mult}(1, \widetilde{y}, \widetilde{0}_Y) = \widetilde{y},\\ &\texttt{chain\_mult}(2, \widetilde{y}, \widetilde{0}_Y) = \texttt{chain\_add}(\widetilde{y}, \widetilde{y}, \widetilde{0}_Y, \widetilde{0}_Y).\end{aligned}$$

We prove the first claim by induction on u. For $u = 1$ we have

$$\texttt{chain\_mult}(1, z \boxplus \widetilde{y}, \widetilde{0}_Y) = z \boxplus \widetilde{y} = z \boxplus \texttt{chain\_mult}(1, \widetilde{y}, \widetilde{0}_Y).$$

Assume that the statement is true for all $v \leq u$, and write

$$\begin{aligned}&\texttt{chain\_mult}(u+1, z \boxplus \widetilde{y}, \widetilde{0}_Y)\\ &= \texttt{chain\_add}(\texttt{chain\_mult}(u, z \boxplus \widetilde{y}, \widetilde{0}_Y), z \boxplus \widetilde{y}, \texttt{chain\_mult}(u-1, z \boxplus \widetilde{y}, \widetilde{0}_Y), \widetilde{0}_Y)\\ &= \texttt{chain\_add}(uz \boxplus \texttt{chain\_mult}(u, \widetilde{y}, \widetilde{0}_Y), z \boxplus \widetilde{y}, (u-1)z \boxplus \texttt{chain\_mult}(u-1, \widetilde{y}, \widetilde{0}_Y), \widetilde{0}_Y)\\ &= (u+1)z \boxplus \texttt{chain\_add}(\texttt{chain\_mult}(u, \widetilde{y}, \widetilde{0}_Y), \widetilde{y}, \texttt{chain\_mult}(u-1, \widetilde{y}, \widetilde{0}_Y), \widetilde{0}_Y)\\ &= (u+1)z \boxplus \texttt{chain\_mult}(u+1, \widetilde{y}, \widetilde{0}_Y).\end{aligned}$$

This proves the induction hypothesis. The proof for `chain_multadd` is similar, except that we use (4.10). □

We are now able to prove the key result:

Proposition 4.11. *The compatible lift $\widetilde{t}_c$ of t is an excellent lift with respect to $(X, \mathcal{L}, \Theta_{\mathcal{L}}, \widetilde{0}_X)$, and for all $2 \leq u \leq \ell - 1$, we have*

$$\widetilde{ut}_c = \texttt{\textit{chain\_mult}}(u, \widetilde{t}_c, \widetilde{0}_X).$$

It follows that $\widetilde{2t}_c, \ldots, \widetilde{(\ell-1)t}_c$ are excellent lifts too.

Proof. Let $\widetilde{0}_Y$ be the unique theta null point for $(Y, \mathcal{M}^\beta, \Theta_{\mathcal{M}^\beta})$ that satisfies $\widetilde{f'}(\widetilde{0}_Y) = \widetilde{0}_X$. Then, for $1 \leq u \leq \ell - 1$, the compatible lift $\widetilde{ut}_c$ of ut is defined as

$$\widetilde{ut}_c = \widetilde{f'}(u\tau \boxplus \widetilde{0}_Y),$$

where $\tau \in K(\mathcal{M}^\beta)_1[\ell]$ is the unique element of $K(\mathcal{M}^\beta)_1$ that satisfies $f'(\tau) = t$ (recall that $\ker f' \subset K(\mathcal{M}^\beta)_2$). Write $\ell = 2m+1$ and observe that $(m+1)\tau \boxplus \widetilde{0}_Y = (-m\tau) \boxplus \widetilde{0}_Y$. This follows from $\ell\tau = 0$ and the fact that $\tau \boxplus \widetilde{0}_Y$ is an action when restricted to an $e_{\mathcal{M}^\beta}$-

isotropic subgroup of $K(\mathcal{M}^\beta)$. We have

$$\begin{aligned}
\texttt{chain_mult}(m+1,\widetilde{t}_c,\widetilde{0}_X) &= \texttt{chain_mult}(m+1,\widetilde{f}'(\tau\boxplus\widetilde{0}_Y),\widetilde{0}_X)\\
&= \widetilde{f}'(\texttt{chain_mult}(m+1,\tau\boxplus\widetilde{0}_Y,\widetilde{0}_Y)) \quad \text{by Lemma 4.9 } iii)\\
&= \widetilde{f}'((m+1)\tau\boxplus \texttt{chain_mult}(m+1,\widetilde{0}_Y,\widetilde{0}_Y)) \quad \text{by Lemma 4.10}\\
&= \widetilde{f}'((-m\tau)\boxplus\widetilde{0}_Y)\\
&= \widetilde{f}'(-(m\tau\boxplus \texttt{chain_mult}(m,\widetilde{0}_Y,\widetilde{0}_Y))) \quad \text{by Lemma 4.9 } i)\\
&= \widetilde{f}'(-\texttt{chain_mult}(m,\tau\boxplus\widetilde{0}_Y,\widetilde{0}_Y)) \quad \text{by Lemma 4.10}\\
&= -\texttt{chain_mult}(m,\widetilde{f}'(\tau\boxplus\widetilde{0}_Y),\widetilde{0}_X) \quad \text{by Lemma 4.9 } iii)\\
&= -\texttt{chain_mult}(m,\widetilde{t}_c,\widetilde{0}_X),
\end{aligned}$$

and therefore $\widetilde{t}_c$ is an excellent lift for $(X,\mathcal{L},\Theta_{\mathcal{L}},\widetilde{0}_X)$. Moreover, for $2\leq u\leq \ell-1$, we have

$$\begin{aligned}
\widetilde{ut}_c &= \widetilde{f}'(u\tau\boxplus\widetilde{0}_Y)\\
&= \widetilde{f}'(u\tau\boxplus \texttt{chain_mult}(u,\widetilde{0}_Y,\widetilde{0}_Y))\\
&= \widetilde{f}'(\texttt{chain_mult}(u,\tau\boxplus\widetilde{0}_Y,\widetilde{0}_Y)) \quad \text{by Lemma 4.10}\\
&= \texttt{chain_mult}(u,\widetilde{f}'(\tau\boxplus\widetilde{0}_Y),\widetilde{0}_X) \quad \text{by Lemma 4.9 } iii)\\
&= \texttt{chain_mult}(u,\widetilde{t}_c,\widetilde{0}_X).
\end{aligned}$$

The last assertion follows from the fact that for all $v\in\mathbb{Z}_{\geq 0}$,

$$\texttt{chain\_mult}(v,\texttt{chain\_mult}(u,\widetilde{t}_c,\widetilde{0}_X),\widetilde{0}_X) = \texttt{chain\_mult}(u,\texttt{chain\_mult}(v,\widetilde{t}_c,\widetilde{0}_X),\widetilde{0}_X).$$

□

4.4.2 Independence of the choice of excellent lifts

Recall that so far we have applied the isogeny theorem to the isogenies of polarized abelian varieties with theta structure

$$f'\colon (Y,\mathcal{M}^\beta,\Theta_{\mathcal{M}^\beta})\to(X,\mathcal{L},\Theta_{\mathcal{L}})$$

and

$$F\colon (Y^r,(\mathcal{M}^\beta)^{\star r},\Theta_{(\mathcal{M}^\beta)^{\star r}})\to(Y^r,\mathcal{M}^{\star r},\Theta'_{\mathcal{M}^{\star r}}),$$

and that we want to compute a theta null point $\widetilde{0}_{Y^r}$ for $(Y^r,\mathcal{M}^{\star r},\Theta'_{\mathcal{M}^{\star r}})$, following (4.7) as

$$\theta^{\Theta'_{\mathcal{M}^{\star r}}}_{\mathbf{k}}(\widetilde{0}_{Y^r}) = \sum_{\substack{\boldsymbol{\tau}\in K((\mathcal{M}^\beta)^{\star r})_1[\ell]\\ F(\boldsymbol{\tau})=0}}\prod_{s=1}^{r}\theta^{\Theta_{\mathcal{M}^\beta}}_{j_s+\tau_s}(\widetilde{0}_Y),$$

for all $\mathbf{k}\in K(\mathcal{M}^{\star r})_1$, where $\mathbf{j}=(j_1,\dots,j_r)\in K((\mathcal{M}^\beta)^{\star r})_1[n]$ is the unique element of $K((\mathcal{M}^\beta)^{\star r})_1$ that satisfies $F(\mathbf{j})=\mathbf{k}$. Knowing the theta null point $\widetilde{0}_Y$ for $(Y,\mathcal{M}^\beta,\Theta_{\mathcal{M}^\beta})$ would require us to know the compatible lifts $\widetilde{t}_c,\widetilde{2t}_c,\dots,\widetilde{(\ell-1)t}_c$ of $t,2t,\dots,(\ell-1)t$

respectively, which we do not. However, if we compute an excellent lift $\widetilde{t}_e$ of t with respect to $(X, \mathcal{L}, \Theta_{\mathcal{L}}, \widetilde{0}_X)$, then it will differ from $\widetilde{t}_c$ by an unknown ℓth root of unity ζ_t,

$$\begin{aligned}
\widetilde{t}_e &= \zeta_t \cdot \widetilde{t}_c \\
\texttt{chain_mult}(2, \widetilde{t}_e, \widetilde{0}_X) &= \zeta_t^{2^2} \cdot \widetilde{2t}_c \\
&\vdots \\
\texttt{chain_mult}(\ell-1, \widetilde{t}_e, \widetilde{0}_X) &= \zeta_t^{(\ell-1)^2} \cdot \widetilde{(\ell-1)t}_c.
\end{aligned}$$

In theta coordinates this reads as

$$\begin{aligned}
\theta^{\Theta_{\mathcal{L}}}_{f'(j)}(\widetilde{t}_e) &= \zeta_t \cdot \theta^{\Theta_{\mathcal{M}^\beta}}_{j+\tau}(\widetilde{0}_Y) \\
\theta^{\Theta_{\mathcal{L}}}_{f'(j)}(\texttt{chain_mult}(2, \widetilde{t}_e, \widetilde{0}_X)) &= \zeta_t^{2^2} \cdot \theta^{\Theta_{\mathcal{M}^\beta}}_{j+2\tau}(\widetilde{0}_Y) \\
&\vdots \\
\theta^{\Theta_{\mathcal{L}}}_{f'(j)}(\texttt{chain_mult}(\ell-1, \widetilde{t}_e, \widetilde{0}_X)) &= \zeta_t^{(\ell-1)^2} \cdot \theta^{\Theta_{\mathcal{M}^\beta}}_{j+(\ell-1)\tau}(\widetilde{0}_Y),
\end{aligned}$$

where j runs through $K(\mathcal{M}^\beta)_1[n]$. Writing $\boldsymbol{\tau} = (\tau_1, \ldots, \tau_r) \in K((\mathcal{M}^\beta)^{\star r})_1[\ell]$ as $\boldsymbol{\tau} = (u_1\tau, \ldots, u_r\tau)$, with $0 \le u_1, \ldots, u_r \le \ell - 1$, we compute the sum

$$\sum_{\substack{\boldsymbol{\tau} \in K((\mathcal{M}^\beta)^{\star r})_1[\ell] \\ F(\boldsymbol{\tau}) = 0}} \prod_{s=1}^{r} \theta^{\Theta_{\mathcal{M}^\beta}}_{j_s+\tau_s}(\widetilde{0}_Y)$$

by substituting $\theta^{\Theta_{\mathcal{L}}}_{f'(j_s)}(\texttt{chain\_mult}(u_s, \widetilde{t}_e, \widetilde{0}_X))$ for $\theta^{\Theta_{\mathcal{M}^\beta}}_{j_s+\tau_s}(\widetilde{0}_Y)$. In particular, what we compute is the sum

$$\sum_{\substack{\boldsymbol{\tau} \in K((\mathcal{M}^\beta)^{\star r})_1[\ell] \\ F(\boldsymbol{\tau}) = 0}} \zeta_t^{u_1^2 + \cdots + u_r^2} \cdot \theta^{\Theta_{\mathcal{M}^\beta}}_{j_1+u_1\tau}(\widetilde{0}_Y) \cdots \theta^{\Theta_{\mathcal{M}^\beta}}_{j_r+u_r\tau}(\widetilde{0}_Y).$$

It remains to show that

$$u_1^2 + \cdots + u_r^2 \equiv 0 \mod \ell,$$

for all $(u_1, \ldots, u_r)$ coming from a $\boldsymbol{\tau} = (u_1\tau, \ldots, u_r\tau) \in K((\mathcal{M}^\beta)^{\star r})_1[\ell] \cap \ker F$. We prove the case $r = 4$. The case $r = 2$ can be proven in a similar way.

Lemma 4.12. *We have*

$$K((\mathcal{M}^\beta)^{\star 4})_1[\ell] \cap \ker F = \{ {}^tM_F(\tau_1, \tau_2, 0, 0) : \tau_1, \tau_2 \in K(\mathcal{M}^\beta)_1[\ell] \}.$$

Proof. Observe that $K((\mathcal{M}^\beta)^{\star 4})_1[\ell]$ is a rational subgroup, since isomorphic to G^4 via the rational morphism $(f')^{\times 4}$. Then, π preserves $K(\mathcal{M}^\beta)_1[\ell]$ and hence, F and $\bar{F}$ are endomorphisms of $K((\mathcal{M}^\beta)^{\star 4})_1[\ell]$ (since we assumed $[\mathcal{O}_{K_0} : \mathbb{Z}[\pi + \pi^\dagger]]$ coprime to ℓ, the endomorphisms α_i, when written as polynomials in π, have denominators coprime to ℓ). Moreover, one can easily verify that $M_F \cdot {}^tM_F = \beta I_4$. We then have $\bar{F}(K((\mathcal{M}^\beta)^{\star 4})_1[\ell]) \subset \ker F \cap K((\mathcal{M}^\beta)^{\star 4})_1[\ell]$ and we conclude by cardinality reason. □

For $\tau_1, \tau_2 \in K(\mathcal{M}^\beta)_1[\ell]$, we have

$${}^tM_F(\tau_1, \tau_2, 0, 0) = (\alpha_1(\tau_1) + \alpha_2(\tau_2), -\alpha_2(\tau_1) + \alpha_1(\tau_2), -\alpha_3(\tau_1) - \alpha_4(\tau_2), -\alpha_4(\tau_1) + \alpha_3(\tau_2)).$$

Write $\tau_1 = u_1\tau$ and $\tau_2 = u_2\tau$, with $0 \leq u_1, u_2 \leq \ell - 1$, and for $s = 1, \ldots, 4$, let a_s be the integer given by the action of α_s on τ, i.e. $0 \leq a_s \leq \ell - 1$ and a_s satisfies

$$\alpha_s(\tau) = a_s\tau. \tag{4.11}$$

Hence, we can write

$$\begin{aligned} &K((\mathcal{M}^{\beta})^{\star 4})_1[\ell] \cap \ker F \\ &= \{((a_1u_1 + a_2u_2)\tau, (-a_2u_1 + a_1u_2)\tau, (-a_3u_1 - a_4u_2)\tau, (-a_4u_1 + a_3u_2)\tau) : 0 \leq u_1, u_2 \leq \ell - 1\}. \end{aligned}$$

But

$$(a_1u_1+a_2u_2)^2+(-a_2u_1+a_1u_2)^2+(-a_3u_1-a_4u_2)^2+(-a_4u_1+a_3u_2)^2 = (a_1^2+\cdots+a_4^2)(u_1^2+u_2^2)$$

and $a_1^2 + \cdots + a_4^2$ is a multiple of ℓ, since it is given by the scalar of the action of $\beta = \alpha_1^2 + \cdots + \alpha_4^2$ on τ. Summarizing the above we have:

Proposition 4.13. *Let $\widetilde{t}_e$ be an excellent lift of t with respect to $(X, \mathcal{L}, \Theta_{\mathcal{L}}, \widetilde{0}_X)$. We can compute a theta null point $\widetilde{0}_{Y^4}$ for $(Y^4, \mathcal{M}^{\star 4}, \Theta'_{\mathcal{M}^{\star 4}})$ as follows: let $\mathbf{k} \in K(\mathcal{M}^{\star 4})_1$ and let $\mathbf{j} = (j_1, \ldots, j_4) \in K((\mathcal{M}^{\beta})^{\star 4})_1[n]$ be the unique element of $K((\mathcal{M}^{\beta})^{\star 4})_1$ that satisfies $F(\mathbf{j}) = \mathbf{k}$. Then, we have*

$$\begin{aligned} \theta_{\mathbf{k}}^{\Theta'_{\mathcal{M}^{\star 4}}}(\widetilde{0}_{Y^4}) = \sum_{0 \leq u_1, u_2 \leq \ell - 1} &\theta_{f'(j_1)}^{\Theta_{\mathcal{L}}}(\texttt{chain\_mult}(a_1u_1 + a_2u_2, \widetilde{t}_e, \widetilde{0}_X)) \\ &\cdot \theta_{f'(j_2)}^{\Theta_{\mathcal{L}}}(\texttt{chain\_mult}(-a_2u_1 + a_1u_2, \widetilde{t}_e, \widetilde{0}_X)) \\ &\cdot \theta_{f'(j_3)}^{\Theta_{\mathcal{L}}}(\texttt{chain\_mult}(-a_3u_1 - a_4u_2, \widetilde{t}_e, \widetilde{0}_X)) \\ &\cdot \theta_{f'(j_4)}^{\Theta_{\mathcal{L}}}(\texttt{chain\_mult}(-a_4u_1 + a_3u_2, \widetilde{t}_e, \widetilde{0}_X)). \end{aligned}$$

4.5 Modification of $\Theta'_{\mathcal{M}^{\star r}}$ on $(Y^r, \mathcal{M}^{\star r})$ via a metaplectic automorphism

From the theta null point $\widetilde{0}_{Y^r}$ for the symmetric theta structure $\Theta'_{\mathcal{M}^{\star r}}$ on $(Y^r, \mathcal{M}^{\star r})$ from Section 4.4 we cannot automatically recover a theta null point for $(Y, \mathcal{M})$. We could do so if $\Theta'_{\mathcal{M}^{\star r}}$ were of the form $\Theta_{\mathcal{M}} \star \Theta_{\mathcal{M}^{\star(r-1)}}$, for theta structures $\Theta_{\mathcal{M}}$ and $\Theta_{\mathcal{M}^{\star(r-1)}}$ on $(Y, \mathcal{M})$ and $(Y^{r-1}, \mathcal{M}^{\star(r-1)})$ respectively.

In order to obtain information about a single polarized factor $(Y, \mathcal{M})$, we need to modify $\Theta'_{\mathcal{M}^{\star r}}$ via a suitably chosen metaplectic automorphism (an automorphism of the corresponding Heisenberg group) so that it has the above form. In our case we will seek for an automorphism of $\mathcal{H}(\delta_{\mathcal{M}^{\star r}})$ that turns $\Theta'_{\mathcal{M}^{\star r}}$ into a theta structure of the form $(\Theta_{\mathcal{M}})^{\star r}$, where $\Theta_{\mathcal{M}}$ is a symmetric theta structure on $(Y, \mathcal{M})$. We explain how to do that now.

Lemma 4.14. *There exists a metaplectic automorphism $M \in \mathrm{Aut}_{k^\times}(\mathcal{H}(\delta_{\mathcal{M}^{\star r}}))$ such that the theta structure $\Theta'_{\mathcal{M}^{\star r}} \circ M$ is a product theta structure.*

Proof. Since $\mathcal{M}$ is totally symmetric, there exists a symmetric theta structure $\Theta_{\mathcal{M}}$ on $(Y, \mathcal{M})$. We can then form the (r-fold) product theta structure $(\Theta_{\mathcal{M}})^{\star r} = \Theta_{\mathcal{M}} \star \cdots \star \Theta_{\mathcal{M}}$ on $(Y^r, \mathcal{M}^{\star r})$. Define $M := \Theta'^{-1}_{\mathcal{M}^{\star r}} \circ (\Theta_{\mathcal{M}})^{\star r}$, which is clearly an element of $\mathrm{Aut}_{k^\times}(\mathcal{H}(\delta_{\mathcal{M}^{\star r}}))$ and satisfies the above property. □

4.5.1 Explicit computation of a metaplectic automorphism M

For simplifying notation in this section, we will write $\mathcal{M}^2$ for $\mathcal{M}^{\otimes 2}$, $(\mathcal{M}^\beta)^2$ for $(\mathcal{M}^\beta)^{\otimes 2}$, etc. Lemma 4.14 shows that $\Theta'_{\mathcal{M}^{\star r}}$ can be transformed into a product theta structure via an automorphism $M \in \mathrm{Aut}_{k^\times}(\mathcal{H}(\delta_{\mathcal{M}^{\star r}}))$, but does not provide such an M. By Proposition 2.34, to determine a symmetric theta structure $\mathcal{H}(\delta_{\mathcal{M}^{\star r}}) \to \mathcal{G}(\mathcal{M}^{\star r})$ it suffices to provide a symplectic isomorphism $K(2\delta_{\mathcal{M}^{\star r}}) \to K((\mathcal{M}^{\star r})^2)$. Observe that $K(2\delta_{\mathcal{M}^{\star r}}) = K((2\delta_{\mathcal{M}})^{\star r}) = K(2\delta_{\mathcal{M}}) \times \cdots \times K(2\delta_{\mathcal{M}})$ and that $K((\mathcal{M}^{\star r})^2) = K((\mathcal{M}^2)^{\star r}) = K(\mathcal{M}^2) \times \cdots \times K(\mathcal{M}^2)$. We have the following proposition.

Proposition 4.15. *Suppose that a symplectic isomorphism $K(2\delta_{\mathcal{M}^{\star r}}) \to K((\mathcal{M}^{\star r})^2)$ is of product form. Then, the induced symmetric theta structure $\mathcal{H}(\delta_{\mathcal{M}^{\star r}}) \to \mathcal{G}(\mathcal{M}^{\star r})$ is also of product form.*

Proof. Observe that the induced symplectic isomorphism $K(\delta_{\mathcal{M}^{\star r}}) \to K(\mathcal{M}^{\star r})$ is of product form, then use Lemma 2.25. □

We will now explain how to find the symplectic isomorphism $K(2\delta_{\mathcal{M}^{\star r}}) \to K((\mathcal{M}^{\star r})^2)$ that turns $\Theta'_{\mathcal{M}^{\star r}}$ into a product theta structure. Consider the polarization $(\mathcal{M}^\beta)^2$ on Y. It determines a symplectic pairing $e_{(\mathcal{M}^\beta)^2}$ on $K((\mathcal{M}^\beta)^2) \subset Y[2\ell n]$, which equals $e_{\mathcal{M}^\beta}$ when restricted to $K(\mathcal{M}^\beta) \subset Y[\ell n]$. Let $\{x_1, \ldots, x_g, \hat{x}_1, \ldots, \hat{x}_g\}$ be any symplectic basis of $K((\mathcal{M}^\beta)^2)[2n] = Y[2n]$ for $e_{(\mathcal{M}^\beta)^2}$ above the symplectic basis of $K(\mathcal{M}^\beta)[n]$ induced by $\Theta_{\mathcal{M}^\beta}$. By "above" we mean that $\{2x_1, \ldots, 2x_g, 2\hat{x}_1, \ldots, 2\hat{x}_g\}$ is equal to the basis induced by $\Theta_{\mathcal{M}^\beta}$. We can then form an r-fold product symplectic basis on $K(((\mathcal{M}^\beta)^{\star r})^2)[2n] = Y^r[2n]$ for the pairing $e_{((\mathcal{M}^\beta)^{\star r})^2}$, that we will for simplicity denote by $\{x_i, \hat{x}_i\}_{i=1}^{gr}$. Let $y_i = F(x_i)$ and $\hat{y}_i = F(\hat{x}_i)$, for $i = 1, \ldots, gr$. The basis $\{y_i, \hat{y}_i\}_{i=1}^{gr}$ of $K((\mathcal{M}^{\star r})^2) = Y^r[2n]$ is not of product form, but is symplectic for the pairing $e_{(\mathcal{M}^{\star r})^2}$. Also, let $\{e_i, \hat{e}_i\}_{i=1}^{gr}$ be the r-fold product basis on $K((\mathcal{L}^{\star r})^2) = X^r[2n]$ given by $e_i = (f')^{\times r}(x_i)$ and $\hat{e}_i = (f')^{\times r}(\hat{x}_i)$, for $i = 1, \ldots, gr$. The basis $\{e_i, \hat{e}_i\}_{i=1}^{gr}$ is symplectic for the pairing $e_{(\mathcal{L}^{\star r})^2}$. Finally, let $\{d_i, \hat{d}_i\}_{i=1}^{gr}$ be the basis of $K(((\mathcal{L}^\beta)^{\star r})^2)[2n] = X^r[2n]$ determined by the property $f^{\times r}(d_i) = y_i$ and $f^{\times r}(\hat{d}_i) = \hat{y}_i$, for $i = 1, \ldots, gr$ (using the fact that $\ker f \subset X[\ell]$). The basis $\{d_i, \hat{d}_i\}_{i=1}^{gr}$ is symplectic for the pairing $e_{((\mathcal{L}^\beta)^{\star r})^2}$ but is not of product form. The following diagram might be helpful.

$$\begin{array}{ccc}
\{e_i, \hat{e}_i\} : r\text{-fold, symplectic for } e_{(\mathcal{L}^{\star r})^2} & \xleftarrow{(f')^{\times r}} & \{x_i, \hat{x}_i\} : r\text{-fold, symplectic for } e_{((\mathcal{M}^\beta)^{\star r})^2} \\
\Big\downarrow & & \Big\downarrow F \\
\{d_i, \hat{d}_i\} : \text{non } r\text{-fold, symplectic for } e_{((\mathcal{L}^\beta)^{\star r})^2} & \xrightarrow[f^{\times r}]{} & \{y_i, \hat{y}_i\} : \text{non } r\text{-fold, symplectic for } e_{(\mathcal{M}^{\star r})^2}
\end{array}$$

Analogous to the definition of the endomorphism $F \in \mathrm{End}(Y^r)$ of Section 4.3, we can define an endomorphism $F \in \mathrm{End}(X^r)$ via the matrix

$$M_F = \begin{pmatrix} \alpha_1 & -\alpha_2 & -\alpha_3 & -\alpha_4 \\ \alpha_2 & \alpha_1 & -\alpha_4 & \alpha_3 \\ \alpha_3 & \alpha_4 & \alpha_1 & -\alpha_2 \\ \alpha_4 & -\alpha_3 & \alpha_2 & \alpha_1 \end{pmatrix}$$

in case $r = 4$ and via the matrix

$$M_F = \begin{pmatrix} \alpha_1 & -\alpha_2 \\ \alpha_2 & \alpha_1 \end{pmatrix}$$

in case $r = 2$. A simple diagram chasing shows that the dotted vertical arrow is

$$F \circ (\beta^{\times r})^{-1},$$

so the non r-fold basis $\{d_i, \hat{d}_i\}_{i=1}^{gr}$ of $X^r[2n]$ can be computed from the basis $\{e_i, \hat{e}_i\}_{i=1}^{gr}$. Note that the basis $\{x_i, \hat{x}_i\}_{i=1}^{gr}$ is above the symplectic basis of $K((\mathcal{M}^\beta)^{\star r})[n]$ induced by the theta structure $\Theta_{(\mathcal{M}^\beta)^{\star r}}$, and that the basis $\{y_i, \hat{y}_i\}_{i=1}^{gr}$ is above the symplectic basis of $K(\mathcal{M}^{\star r})$ induced by the theta structure $\Theta'_{\mathcal{M}^{\star r}}$. Now, if $S_{(\mathcal{M}^{\star r})^2} \in \mathbf{Sp}(K((\mathcal{M}^{\star r})^2))$ is a symplectic automorphism such that the basis $\{S_{(\mathcal{M}^{\star r})^2}(y_i), S_{(\mathcal{M}^{\star r})^2}(\hat{y}_i)\}_{i=1}^{gr}$ of $K((\mathcal{M}^{\star r})^2)$ is of product form, then the induced symmetric theta structure from Proposition 4.15 is also of product form. That is, there exists a symmetric theta structure $\Theta_{\mathcal{M}}$ on $(Y, \mathcal{M})$ so that the theta structure $\mathcal{H}(\delta_{\mathcal{M}^{\star r}}) \to \mathcal{G}(\mathcal{M}^{\star r})$ determined by the basis $\{S_{(\mathcal{M}^{\star r})^2}(y_i), S_{(\mathcal{M}^{\star r})^2}(\hat{y}_i)\}_{i=1}^{gr}$ is equal to $(\Theta_{\mathcal{M}})^{\star r}$.

To find the symplectic automorphism $S_{(\mathcal{M}^{\star r})^2}$ in practice we have to work on X^r instead, i.e. look for a symplectic automorphism $S_{((\mathcal{L}^\beta)^{\star r})^2} \in \mathbf{Sp}(K(((\mathcal{L}^\beta)^{\star r})^2)[2n])$ that turns the basis $\{d_i, \hat{d}_i\}_{i=1}^{gr}$ into a product basis.

Lemma 4.16. *Suppose that $S_{((\mathcal{L}^\beta)^{\star r})^2} \in \mathbf{Sp}(X^r[2n])$ is a symplectic automorphism (for the pairing $e_{((\mathcal{L}^\beta)^{\star r})^2}$ restricted to $X^r[2n]$) such that the basis $\{S_{((\mathcal{L}^\beta)^{\star r})^2}(d_i), S_{((\mathcal{L}^\beta)^{\star r})^2}(\hat{d}_i)\}_{i=1}^{gr}$ is an r-fold product basis of $X^r[2n]$. Then, the basis $\{S_{(\mathcal{M}^{\star r})^2}(y_i), S_{(\mathcal{M}^{\star r})^2}(\hat{y}_i)\}_{i=1}^{gr}$ is an r-fold product symplectic basis of $K((\mathcal{M}^{\star r})^2) = Y^r[2n]$ for $e_{(\mathcal{M}^{\star r})^2}$, where $S_{(\mathcal{M}^{\star r})^2} = f^{\times r} \circ S_{((\mathcal{L}^\beta)^{\star r})^2} \circ (f^{\times r})^{-1} \in \mathbf{Sp}(K((\mathcal{M}^{\star r})^2))$.*

Proof. Write

$$S_{(\mathcal{M}^{\star r})^2}(y_i) = f^{\times r}(S_{((\mathcal{L}^\beta)^{\star r})^2}(d_i)) \qquad \text{and} \qquad S_{(\mathcal{M}^{\star r})^2}(\hat{y}_i) = f^{\times r}(S_{((\mathcal{L}^\beta)^{\star r})^2}(\hat{d}_i)).$$

Since $\{S_{((\mathcal{L}^\beta)^{\star r})^2}(d_i), S_{((\mathcal{L}^\beta)^{\star r})^2}(\hat{d}_i)\}_{i=1}^{gr}$ is an r-fold product basis, so is $\{S_{(\mathcal{M}^{\star r})^2}(y_i), S_{(\mathcal{M}^{\star r})^2}(\hat{y}_i)\}_{i=1}^{gr}$. □

For $N \in \mathbf{GL}_{2g}(\mathbb{Z}/2n\mathbb{Z})$ we denote by $\Delta(N)$ the image of N under the block-wise diagonal embedding

$$\Delta\colon \mathbf{GL}_{2g}(\mathbb{Z}/2n\mathbb{Z}) \hookrightarrow \mathbf{GL}_{2gr}(\mathbb{Z}/2n\mathbb{Z}).$$

To compute such an $S_{((\mathcal{L}^\beta)^{\star r})^2} \in \mathbf{Sp}(X^r[2n])$ in practice, we do the following:

Algorithm 3 Computing $S_{((\mathcal{L}^\beta)^{\star r})^2} \in \mathbf{Sp}(X^r[2n])$

Require: the r-fold product symplectic basis $\{e_i, \hat{e}_i\}_{i=1}^{gr}$ of $X^r[2n]$ for $e_{(\mathcal{L}^{\star r})^2}$

Ensure: a symplectic automorphism $S_{((\mathcal{L}^\beta)^{\star r})^2} \in \mathbf{Sp}(X^r[2n])$ that turns $\{d_i, \hat{d}_i\}_{i=1}^{gr}$ into a product basis

1: compute $M_{F\circ(\beta^{\times r})^{-1}} \in \mathbf{GL}_{2gr}(\mathbb{Z}/2n\mathbb{Z})$, the matrix corresponding to the action of $F \circ (\beta^{\times r})^{-1}$ on $\{e_i, \hat{e}_i\}_{i=1}^{gr}$, i.e. the one corresponding to the change of basis from $\{e_i, \hat{e}_i\}_{i=1}^{gr}$ to $\{d_i, \hat{d}_i\}_{i=1}^{gr}$
2: **for** $N \in \mathbf{GL}_{2g}(\mathbb{Z}/2n\mathbb{Z})$ **do**
3: **if** $\Delta(N)M^{-1}_{F\circ(\beta^{\times r})^{-1}} \in \mathbf{Sp}_{2gr}(\mathbb{Z}/2n\mathbb{Z})$, where the symplectic group $\mathbf{Sp}_{2gr}(\mathbb{Z}/2n\mathbb{Z}) \subset \mathbf{GL}_{2gr}(\mathbb{Z}/2n\mathbb{Z})$ is defined with respect to the pairing $\begin{pmatrix} & I_{gr} \\ -I_{gr} & \end{pmatrix}$ for the standard basis of $(\mathbb{Z}/2n\mathbb{Z})^{2gr}$ **then**
4: **return** $S_{((\mathcal{L}^\beta)^{\star r})^2} := \Delta(N)M^{-1}_{F\circ(\beta^{\times r})^{-1}}$
5: **end if**
6: **end for**

We will analyse the complexity of Algorithm 3 in Section 6. The symplectic automorphism $S_{((\mathcal{L}^\beta)^{\star r})^2}$ determines a symplectic automorphism $S_{(\mathcal{M}^{\star r})^2}$, which by Proposition 4.15 determines a symmetric r-fold product theta structure

$$(\Theta_{\mathcal{M}})^{\star r} \colon \mathcal{H}(\delta_{\mathcal{M}^{\star r}}) \to \mathcal{G}(\mathcal{M}^{\star r}),$$

where $\Theta_{\mathcal{M}}$ is a symmetric theta structure on $(Y, \mathcal{M})$. As a next step, we have to apply the symplectic transformation formula for the metaplectic automorphism $M := \Theta'^{-1}_{\mathcal{M}^{\star r}} \circ (\Theta_{\mathcal{M}})^{\star r}$ to the basis of theta functions $\{\theta_{\mathbf{k}}^{\Theta'_{\mathcal{M}^{\star r}}}\}_{\mathbf{k} \in K(\mathcal{M}^{\star r})_1}$ to obtain a basis of theta functions

$$\{\theta_{\boldsymbol{\kappa}}^{(\Theta_{\mathcal{M}})^{\star r}} = \theta_{\kappa_1}^{\Theta_{\mathcal{M}}} \otimes \cdots \otimes \theta_{\kappa_r}^{\Theta_{\mathcal{M}}}\}_{\boldsymbol{\kappa} \in K(\mathcal{M}^{\star r})_1}$$

for $(Y^r, \mathcal{M}^{\star r}, (\Theta_{\mathcal{M}})^{\star r})$.

4.5.2 Applying the symplectic transformation formula

By the work of Candelori [Can16] (especially Theorem 4.2.1) the symplectic transformation law for analytic theta functions (Theorem 1.24) holds for algebraic theta functions as well. For simplicity of the exposition, suppose we work on one factor of Y as opposed to Y^r. Recall that $\mathcal{M}$ is an nth power of a symmetric principal polarization on Y, for $n = 2$ or $n = 4$, hence a totally symmetric ample line bundle. Let $\Theta'_{\mathcal{M}}$ be a symmetric theta structure on $(Y, \mathcal{M})$ with induced basis

$$\{\theta_i^{\Theta'_{\mathcal{M}}} : i \in K(\mathcal{M})_1\}.$$

Let $M \in \mathrm{Aut}_{k^\times}(\mathcal{H}(\delta_{\mathcal{M}}))$ be a metaplectic automorphism and let $\Theta_{\mathcal{M}} = \Theta'_{\mathcal{M}} \circ M$ be the resulting symmetric theta structure on $(Y, \mathcal{M})$, with induced basis

$$\{\theta_j^{\Theta_{\mathcal{M}}} : j \in K(\mathcal{M})_1\}.$$

Note that the symplectic decompositions on $K(\mathcal{M})$ induced by $\Theta'_{\mathcal{M}}$ and $\Theta_{\mathcal{M}}$ are not the same. Hence, writing $K(\mathcal{M})_1$ is ambiguous, one has to be clear what decomposition of $K(\mathcal{M})$ is understood (i.e. from what theta structure this decomposition is induced). Unfortunately, the bases $\{\theta_i^{\Theta'_{\mathcal{M}}}\}$ and $\{\theta_j^{\Theta_{\mathcal{M}}}\}$ are not well suited for the transformation law. We treat the case $n = 2$ and $n = 4$ separately.

The case $n = 4$. In Section 1.3.1 we have introduced the notion of level-4 and level-$(2, \ldots, 2)$ theta functions for two particular bases of $\Gamma(\mathbb{C}^g/\Omega\mathbb{Z}^g \oplus \mathbb{Z}^g, \mathcal{L}_\Omega^{\otimes 4})$, where $\mathcal{L}_\Omega$ is a principal polarization on $\mathbb{C}^g/\Omega\mathbb{Z}^g \oplus \mathbb{Z}^g$. The two bases are linked by the linear change of coordinates (1.28). This motivates to define an algebraic analogue of level-$(2, \ldots, 2)$ theta functions for $\Gamma(Y, \mathcal{M})$ with respect to $\Theta'_{\mathcal{M}}$ (and similarly with respect to $\Theta_{\mathcal{M}}$).

Let $Y[4] = K(\mathcal{M})_1 \oplus K(\mathcal{M})_2$ be the symplectic decomposition induced by $\Theta'_{\mathcal{M}}$. Multiplication by 2 gives a surjection on $Y[2]$ and hence, we have a decomposition $Y[2] = K_1 \oplus K_2$, where $K_\nu = [2]K(\mathcal{M})_\nu$, for $\nu = 1, 2$. For $i \in Y[2]$ we can distinguish one particular element $\hat{i} \in Y[4]$ satisfying $[2]\hat{i} = i$ (in general, such an element is defined up to $Y[2]$ only). Namely, if $i = \overline{\Theta}'_{\mathcal{M}}(\iota)$ then $\iota \in 2K(\delta_{\mathcal{M}})$, hence it makes sense to consider $\iota/2 \in K(\delta_{\mathcal{M}})$, and put $\hat{i} = \overline{\Theta}'_{\mathcal{M}}(\iota/2)$. Recall that $K(\delta_{\mathcal{M}}) = \mathbb{Z}(\delta_{\mathcal{M}}) \oplus \widehat{\mathbb{Z}}(\delta_{\mathcal{M}})$, where $\mathbb{Z}(\delta_{\mathcal{M}}) = \bigoplus_{i=1}^g \mathbb{Z}/4\mathbb{Z}$, since the type of $\mathcal{M}$ is $\delta_{\mathcal{M}} = (4, \ldots, 4) \in \mathbb{Z}^g$.

For $i_1 \in K_1$ and $i_2 \in K_2$ we define the *algebraic level-$(2, \ldots, 2)$ theta function with characteristic i_1, i_2* as

$$\theta_{i_1,i_2}^{\Theta'_{\mathcal{M}}} := \sum_{i'_1 \in K_1} e_{\mathcal{M}}(-i'_1, i_2)\theta_{\hat{i}_1+i'_1}^{\Theta'_{\mathcal{M}}}. \tag{4.12}$$

The family

$$\{\theta_{i_1,i_2}^{\Theta'_{\mathcal{M}}} : i_1 \in K_1,\, i_2 \in K_2\}$$

forms a basis of $\Gamma(Y,\mathcal{M})$ for $\Theta'_{\mathcal{M}}$. One can go back from level-$(2,\dots,2)$ to level-4 via

$$\theta_i^{\Theta'_{\mathcal{M}}} = \frac{1}{2^g}\sum_{i_2\in K_2} e_{\mathcal{M}}(i-\widehat{2i}, i_2)\theta_{2i,i_2}^{\Theta'_{\mathcal{M}}} \tag{4.13}$$

for all $i \in K(\mathcal{M})_1$. Recall that the field k is of characteristic $p > 2$.

If M is a metaplectic automorphism of $\mathcal{H}(\delta_{\mathcal{M}})$, denote by $S \in \mathbf{Sp}(K(\mathcal{M}))$ the induced symplectic automorphism of $K(\mathcal{M})$ for $e_{\mathcal{M}}$. Letting $\Theta_{\mathcal{M}} = \Theta'_{\mathcal{M}} \circ M$, the automorphism S converts between the bases of $K(\mathcal{M})$ induced by $\Theta'_{\mathcal{M}}$ and $\Theta_{\mathcal{M}}$ respectively. With respect to the basis of $K(\mathcal{M})$ induced by $\Theta'_{\mathcal{M}}$, we can write $S = {}^t\begin{pmatrix} A & B \\ C & D\end{pmatrix}^{-1} \in \mathbf{Sp}_{2g}(\mathbb{Z}/4\mathbb{Z})$. For $i_1 \in K_1, i_2 \in K_2$, let $j_1, j_2 \in Y[2]$ be given by

$$\begin{aligned} j_1 &= Di_1 - Ci_2 + \overline{\Theta}'_{\mathcal{M}}(2(C\,{}^tD)_0) \\ j_2 &= -Bi_1 + Ai_2 + \overline{\Theta}'_{\mathcal{M}}(2(A\,{}^tB)_0), \end{aligned} \tag{4.14}$$

where $(\cdot)_0$ denotes the vector of diagonal elements. Rephrasing Theorem 1.24 for algebraic level-$(2,\dots,2)$ theta functions:

Theorem 4.17. *Let $\Theta'_{\mathcal{M}}$ and $\Theta_{\mathcal{M}}$ be two symmetric theta structures on $(Y,\mathcal{M})$, and let $M \in \mathrm{Aut}_{k^\times}(\mathcal{H}(\delta_{\mathcal{M}}))$ be the metaplectic automorphism such that $\Theta_{\mathcal{M}} = \Theta'_{\mathcal{M}} \circ M$. Let $S \in \mathbf{Sp}(K(\mathcal{M}))$ be the induced symplectic automorphism, and write $S = {}^t\begin{pmatrix} A & B \\ C & D\end{pmatrix}^{-1} \in \mathbf{Sp}_{2g}(\mathbb{Z}/4\mathbb{Z})$ with respect to the symplectic basis of $K(\mathcal{M})$ induced by $\Theta'_{\mathcal{M}}$.*
Then, for all $y \in Y(\bar{k})$, there exists a constant $\lambda \in \bar{k}^\times$ (depending only on y and S) such that for all $i_1 \in K_1, i_2 \in K_2$,

$$\theta_{j_1,j_2}^{\Theta_{\mathcal{M}}}(y) = \lambda \cdot e_{\mathcal{M}}(Di_1 - Ci_2, -Bi_1 + Ai_2 + \overline{\Theta}'_{\mathcal{M}}((A\,{}^tB)_0))e_{\mathcal{M}}(i_1,i_2)^{-1}\theta_{i_1,i_2}^{\Theta'_{\mathcal{M}}}(y),$$

where j_1 and j_2 are as in (4.14).

Knowing how the level-$(2,\dots,2)$ basis $\{\theta_{j_1,j_2}^{\Theta_{\mathcal{M}}}\}$ is related to the level-$(2,\dots,2)$ basis $\{\theta_{i_1,i_2}^{\Theta'_{\mathcal{M}}}\}$, we can describe the symplectic transformation formula from the basis $\{\theta_i^{\Theta'_{\mathcal{M}}}\}$ to the basis $\{\theta_j^{\Theta_{\mathcal{M}}}\}$ in three steps:

i) Use the level-4 to level-$(2,\dots,2)$ base change formula for algebraic theta functions (4.12).

ii) Apply the symplectic transformation formula for algebraic theta functions (Theorem 4.17).

iii) Use the level-$(2,\dots,2)$ to level-4 base change formula for algebraic theta functions (4.13).

The case $n = 2$. The case $n = 2$ is more subtle since we do not have a convenient basis such as the level-$(2,\dots,2)$ theta functions at hand. However, the squares of the level-$(2,\dots,2)$ theta functions form a generating family for $\Gamma(Y,\mathcal{M})$. So, on one side we have the basis $\{\theta_i^{\Theta'_{\mathcal{M}}} : i \in K(\mathcal{M})_1\}$ (of level-2 theta functions) and on the other side we have

the generating family $\{(\theta^{\Theta'_{\mathcal{M}}}_{i_1,i_2})^2 : i_1 \in K(\mathcal{M})_1,\, i_2 \in K(\mathcal{M})_2\}$. These two families are related, and we refer to [Cos11, (3.12) and (3.13)] for the conversion formulas. Hence, the symplectic transformation from the basis $\{\theta_i^{\Theta'_{\mathcal{M}}}\}$ to the basis $\{\theta_j^{\Theta_{\mathcal{M}}}\}$ is again done in three steps:

i) Use the conversion formula to go from the level-2 basis $\{\theta_i^{\Theta'_{\mathcal{M}}}\}$ to the family of squares of level-$(2,\dots,2)$ theta functions.

ii) Apply the symplectic transformation formula for algebraic theta functions (Theorem 4.17). It is perfectly applicable to the squares of the level-$(2,\dots,2)$ theta functions as well.

iii) Use the reciprocal conversion to go from the squares of level-$(2,\dots,2)$ theta functions to the basis $\{\theta_j^{\Theta_{\mathcal{M}}}\}$.

Algorithm 4 Computing a theta null point of $Y = X/G$ for $(\mathcal{M}, \Theta_{\mathcal{M}})$

Require: $\beta \in \mathrm{End}^{++}(X)$ of degree ℓ^2, and lifts $\widetilde{t}, \widetilde{0}_X$ of t and 0_X for $(X, \mathcal{L}, \Theta_{\mathcal{L}})$ respectively, where $t \in \ker \beta$ is of order ℓ and $G = \langle t \rangle$ is $\mathrm{Gal}(\bar{k}/k)$-stable

Ensure: a lift $\widetilde{0}_Y$ of 0_Y for $(Y, \mathcal{M}, \Theta_{\mathcal{M}})$

1: compute an excellent lift $\widetilde{t}_e$ of t with respect to $(X, \mathcal{L}, \Theta_{\mathcal{L}}, \widetilde{0}_X)$, see Algorithm 2

2: compute $\alpha_1, \ldots, \alpha_r \in K_0$ such that $\beta = \alpha_1^2 + \cdots + \alpha_r^2$, see Algorithm 1

3: compute $0 \leq a_1, \ldots, a_r \leq \ell - 1$ such that for all $s = 1, \ldots, r$,

$$\alpha_s(t) = a_s t$$

(knowing that $\alpha_s \in \mathbb{Q}(\pi)$ with denominators coprime to ℓ, it suffices to know the scalar by which π acts on t)

4: **if** $r = 2$ **then**

5: for each $\mathbf{k} \in K(\mathcal{M}^{\star 2})_1$, let $\mathbf{j} = (j_1, j_2) \in K((\mathcal{M}^{\beta})^{\star 2})_1[n]$ be the unique element of $K((\mathcal{M}^{\beta})^{\star 2})_1$ that satisfies $F(\mathbf{j}) = \mathbf{k}$; compute $\theta_{\mathbf{k}}^{\Theta'_{\mathcal{M}^{\star 2}}}(\widetilde{0}_{Y^2})$ as

$$\begin{aligned}\theta_{\mathbf{k}}^{\Theta'_{\mathcal{M}^{\star 2}}}(\widetilde{0}_{Y^2}) = \sum_{0 \leq u \leq \ell-1} & \theta_{f'(j_1)}^{\Theta_{\mathcal{L}}}(\texttt{chain\_mult}(a_1 u, \widetilde{t}_e, \widetilde{0}_X)) \\ & \cdot \theta_{f'(j_2)}^{\Theta_{\mathcal{L}}}(\texttt{chain\_mult}(-a_2 u, \widetilde{t}_e, \widetilde{0}_X))\end{aligned}$$

6: **else if** $r = 4$ **then**

7: for each $\mathbf{k} \in K(\mathcal{M}^{\star 4})_1$, let $\mathbf{j} = (j_1, \ldots, j_4) \in K((\mathcal{M}^{\beta})^{\star 4})_1[n]$ be the unique element of $K((\mathcal{M}^{\beta})^{\star 4})_1$ that satisfies $F(\mathbf{j}) = \mathbf{k}$; compute $\theta_{\mathbf{k}}^{\Theta'_{\mathcal{M}^{\star 4}}}(\widetilde{0}_{Y^4})$ as

$$\begin{aligned}\theta_{\mathbf{k}}^{\Theta'_{\mathcal{M}^{\star 4}}}(\widetilde{0}_{Y^4}) = \sum_{0 \leq u_1, u_2 \leq \ell-1} & \theta_{f'(j_1)}^{\Theta_{\mathcal{L}}}(\texttt{chain\_mult}(a_1 u_1 + a_2 u_2, \widetilde{t}_e, \widetilde{0}_X)) \\ & \cdot \theta_{f'(j_2)}^{\Theta_{\mathcal{L}}}(\texttt{chain\_mult}(-a_2 u_1 + a_1 u_2, \widetilde{t}_e, \widetilde{0}_X)) \\ & \cdot \theta_{f'(j_3)}^{\Theta_{\mathcal{L}}}(\texttt{chain\_mult}(-a_3 u_1 - a_4 u_2, \widetilde{t}_e, \widetilde{0}_X)) \\ & \cdot \theta_{f'(j_4)}^{\Theta_{\mathcal{L}}}(\texttt{chain\_mult}(-a_4 u_1 + a_3 u_2, \widetilde{t}_e, \widetilde{0}_X))\end{aligned}$$

8: **end if**

9: compute the r-fold product symplectic basis $\{e_i, \hat{e}_i\}_{i=1}^{gr}$ of $X^r[2n]$ for $e_{(\mathcal{L}^{\star r})^2}$ in theta coordinates, using the action of the theta group $\mathcal{G}(\mathcal{L}^{\star r})$ on $\Gamma(X^r, \mathcal{L}^{\star r})$

10: compute $S_{((\mathcal{L}^{\beta})^{\star r})^2} \in \mathbf{Sp}(X^r[2n])$ that turns the basis $\{d_i, \hat{d}_i\}_{i=1}^{gr}$ into a product basis, see Algorithm 3 (either if we know how to lift $\mathrm{End}(X[2n])$ to $\mathrm{End}(\widetilde{X[2n]})$, or using the theta to Mumford conversion when working on the Jacobian variety of a hyperelliptic curve)

11: let $M \in \mathrm{Aut}_{k^\times}(\mathcal{H}(\delta_{\mathcal{M}^{\star r}}))$ be the metaplectic automorphism induced by $S_{((\mathcal{L}^{\beta})^{\star r})^2}$ that turns $\Theta'_{\mathcal{M}^{\star r}}$ into an r-fold product theta structure $(\Theta_{\mathcal{M}})^{\star r}$; apply the symplectic coordinate change from Section 4.5.2 to $\left\{\theta_{\mathbf{k}}^{\Theta'_{\mathcal{M}^{\star r}}}(\widetilde{0}_{Y^r})\right\}_{\mathbf{k} \in K(\mathcal{M}^{\star r})_1}$ to obtain the coordinates $\left\{\theta_{\boldsymbol{\kappa}}^{(\Theta_{\mathcal{M}})^{\star r}}(\widetilde{0}_{Y^r})\right\}_{\boldsymbol{\kappa} \in K(\mathcal{M}^{\star r})_1}$ for $(\Theta_{\mathcal{M}})^{\star r}$

12: **return** fix $(\kappa_1, \ldots, \kappa_r) \in K(\mathcal{M}^{\star r})_1$ such that $\theta_{\boldsymbol{\kappa}}^{(\Theta_{\mathcal{M}})^{\star r}}(\widetilde{0}_{Y^r}) \neq 0$ and return

$$\left(\theta_{\kappa}^{\Theta_{\mathcal{M}}}(\widetilde{0}_Y)\right)_{\kappa \in K(\mathcal{M})_1},$$

where

$$\theta_{\kappa}^{\Theta_{\mathcal{M}}}(\widetilde{0}_Y) := \theta_{\kappa}^{\Theta_{\mathcal{M}}}(\widetilde{0}_Y) \cdot \theta_{\kappa_2}^{\Theta_{\mathcal{M}}}(\widetilde{0}_Y) \cdots \theta_{\kappa_r}^{\Theta_{\mathcal{M}}}(\widetilde{0}_Y)$$

for all $\kappa \in K(\mathcal{M})_1$

We analyse the complexity of Algorithm 4 in Section 6.

Theorem 4.18. *Algorithm 4 computes a theta null point $\widetilde{0}_Y$ for $(Y, \mathcal{M}, \Theta_{\mathcal{M}})$.*

Proof. Observe that the $a_1, \dots, a_r$ computed at step 3. are equal to the $a_1, \dots, a_r$ from (4.11). By Proposition 4.13, step 5. or step 7. correctly computes $\left(\theta_{\mathbf{k}}^{\Theta'_{\mathcal{M}^{\star r}}}(\widetilde{0}_{Y^r})\right)_{\mathbf{k}\in K(\mathcal{M}^{\star r})_1}$. Then, as explained in Section 4.5.2, step 11. computes the coordinates $\left\{\theta_{\boldsymbol{\kappa}}^{(\Theta_{\mathcal{M}})^{\star r}}(\widetilde{0}_{Y^r}) = \theta_{\kappa_1}^{\Theta_{\mathcal{M}}}(\widetilde{0}_Y)\cdots\theta_{\kappa_r}^{\Theta_{\mathcal{M}}}(\widetilde{0}_Y)\right\}_{\boldsymbol{\kappa}\in K(\mathcal{M}^{\star r})_1}$ of 0_{Y^r} for the product theta structure $(\Theta_{\mathcal{M}})^{\star r}$ and hence, step 12. outputs an affine theta null point $\widetilde{0}_Y$ for $(Y, \mathcal{M}, \Theta_{\mathcal{M}})$. □

5 Evaluating the cyclic isogeny on points

In Section 4 we explained how to compute the k-rational principally polarized abelian variety $Y = X/G$. To be more precise, we showed how to compute a theta null point $\widetilde{0}_Y$ for $(Y, \mathcal{M}, \Theta_{\mathcal{M}})$, given a theta null point $\widetilde{0}_X$ and an affine lift $\widetilde{t}$ for $(X, \mathcal{L}, \Theta_{\mathcal{L}})$, where t is a generator of G. Here, the totally symmetric ample line bundles $\mathcal{M}$ and $\mathcal{L}$ are nth tensor powers of the symmetric principal polarizations $\mathcal{M}_0$ and $\mathcal{L}_0$ on Y and X respectively, with $n = 2$ or $n = 4$. Also, $\Theta_{\mathcal{M}}$ and $\Theta_{\mathcal{L}}$ are symmetric theta structures on $(Y, \mathcal{M})$ and $(X, \mathcal{L})$ respectively. In this section we will show how to evaluate the isogeny $f\colon X \to Y$ on points.

Let $x \in X(k)$ be a point of order N and suppose that N is coprime to $\ell \cdot [\mathcal{O}_{K_0} : \mathbb{Z}[\pi + \pi^\dagger]]$. Let $\widetilde{0}_X$ and $\widetilde{t}$ be as above and suppose we are given an affine lift $\widetilde{x}$ of x for $(X, \mathcal{L}, \Theta_{\mathcal{L}})$. We will explain how to compute one affine lift $\widetilde{y}$ of $y = f(x)$ for $(Y, \mathcal{M}, \Theta_{\mathcal{M}})$. This defines a map

$$\widetilde{f}\colon \widetilde{X} \setminus \{\text{points of order not coprime to } \ell \cdot [\mathcal{O}_{K_0} : \mathbb{Z}[\pi + \pi^\dagger]]\} \to \widetilde{Y},$$

where the affine coordinates on the cones $\widetilde{X}$ and $\widetilde{Y}$ are given by $\Theta_{\mathcal{L}}$ and $\Theta_{\mathcal{M}}$ respectively.

5.1 Applying the isogeny theorem to f' and F

Similar to the ideas of Section 4, we will apply the isogeny theorem to the isogenies of polarized abelian varieties with theta structure

$$f'\colon (Y, \mathcal{M}^\beta, \Theta_{\mathcal{M}^\beta}) \to (X, \mathcal{L}, \Theta_{\mathcal{L}})$$

and

$$F\colon (Y^r, (\mathcal{M}^\beta)^{\star r}, \Theta_{(\mathcal{M}^\beta)^{\star r}}) \to (Y^r, \mathcal{M}^{\star r}, \Theta'_{\mathcal{M}^{\star r}}).$$

Setting $y = f(x)$, we want to compute an affine lift $\left(\theta^{\Theta'_{\mathcal{M}^{\star r}}}_{\mathbf{k}}(y, \widetilde{0, \ldots, 0})\right)_{\mathbf{k} \in K(\mathcal{M}^{\star r})_1}$ of $(y, 0, \ldots, 0)$ and then modify $\Theta'_{\mathcal{M}^{\star r}}$ by the same metaplectic automorphism of $\mathcal{H}(\delta_{\mathcal{M}^{\star r}})$ as in Section 4.5 to obtain affine coordinates

$$\theta^{(\Theta_{\mathcal{M}})^{\star r}}_{\boldsymbol{\kappa}}(y, \widetilde{0, \ldots, 0}) = \theta^{\Theta_{\mathcal{M}}}_{\kappa_1}(\widetilde{y}) \cdot \theta^{\Theta_{\mathcal{M}}}_{\kappa_2}(\widetilde{0}_Y) \cdots \theta^{\Theta_{\mathcal{M}}}_{\kappa_r}(\widetilde{0}_Y),$$

where $\Theta_{\mathcal{M}}$ is a symmetric theta structure on $(Y, \mathcal{M})$. The affine version of the isogeny theorem for F states that for all $\mathbf{y} = (y_1, \ldots, y_r) \in Y^r(\bar{k})$ with affine lift $\widetilde{\mathbf{y}}$ for $(Y^r, (\mathcal{M}^\beta)^{\star r}, \Theta_{(\mathcal{M}^\beta)^{\star r}})$, an affine lift $\widetilde{F(\mathbf{y})}$ of $F(\mathbf{y})$ for $(Y^r, \mathcal{M}^{\star r}, \Theta'_{\mathcal{M}^{\star r}})$ is given by

$$\theta^{\Theta'_{\mathcal{M}^{\star r}}}_{\mathbf{k}}(\widetilde{F(\mathbf{y})}) = \sum_{\substack{\boldsymbol{\tau} \in K((\mathcal{M}^\beta)^{\star r})_1[\ell] \\ F(\boldsymbol{\tau}) = 0}} \prod_{s=1}^{r} \theta^{\Theta_{\mathcal{M}^\beta}}_{j_s + \tau_s}(\widetilde{y}_s), \text{ for all } \mathbf{k} \in K(\mathcal{M}^{\star r})_1, \tag{5.1}$$

where $\mathbf{j} = (j_1, \ldots, j_r) \in K((\mathcal{M}^\beta)^{\star r})_1[n]$ is the unique element of $K((\mathcal{M}^\beta)^{\star r})_1$ that satisfies $F(\mathbf{j}) = \mathbf{k}$. In our case, we want to apply (5.1) to a point $(y_1, \ldots, y_r)$ that satisfies $F(y_1, \ldots, y_r) = (y, 0, \ldots, 0)$. To obtain affine lifts $\widetilde{y}_1, \ldots, \widetilde{y}_r$ of $y_1, \ldots, y_r$ for $(Y, \mathcal{M}^\beta, \Theta_{\mathcal{M}^\beta})$, we apply the affine version of the isogeny theorem for f', stating that for all $s = 1, \ldots, r$ and for all $i \in K(\mathcal{L})_1$,

$$\theta^{\Theta_{\mathcal{L}}}_i(\widetilde{f'(y_s)}) = \theta^{\Theta_{\mathcal{M}^\beta}}_j(\widetilde{y}_s), \tag{5.2}$$

where $j \in K(\mathcal{M}^\beta)_1[n]$ is the unique element of $K(\mathcal{M}^\beta)_1$ that satisfies $f'(j) = i$. We encounter the same problem as in Section 4.2.1, that is, the left-hand side of (5.2) provides us with n^g coordinates only, as opposed to the $n^g\ell$ coordinates of $\widetilde{y}_s$ for $(Y, \mathcal{M}^\beta, \Theta_{\mathcal{M}^\beta})$. We will explain in Section 5.1.2 how to deal with this issue.

Let us explain how to find $(y_1, \ldots, y_r)$.

Proposition 5.1. *Let $(x_1, \ldots, x_r) = \bar{F}(x, 0, \ldots, 0) \in X^r(k)$ and let $y_1, \ldots, y_r \in Y(k)$ be such that $x_1 = f'(y_1), \ldots, x_r = f'(y_r)$. Then,*

$$F(y_1, \ldots, y_r) = (y, 0, \ldots, 0).$$

Proof. First observe that $\bar{F}F = F\bar{F} = \beta^{\times r}$. We have

$$F(x_1, \ldots, x_r) = \beta^{\times r}(x, 0, \ldots, 0) = (f')^{\times r}(y, 0, \ldots, 0)$$

and hence,

$$\beta^{\times r}(F(y_1, \ldots, y_r)) = F(f(x_1), \ldots, f(x_r)) = f^{\times r}(F(x_1, \ldots, x_r)) = \beta^{\times r}(y, 0, \ldots, 0).$$

But $\beta^{\times r}$ is injective on points of order coprime to ℓ. □

5.1.1 Compatible lifts and suitable lifts

Following Proposition 5.1, consider $x_1 = \alpha_1(x)$, $x_2 = -\alpha_2(x)$ (in case $r = 2$) and $x_1 = \alpha_1(x)$, $x_2 = -\alpha_2(x)$, $x_3 = -\alpha_3(x)$, $x_4 = -\alpha_4(x)$ (in case $r = 4$). Suppose we know affine lifts $\widetilde{x}_1, \ldots, \widetilde{x}_r$ of $x_1, \ldots, x_r$ for $(X, \mathcal{L}, \Theta_{\mathcal{L}})$ (e.g., since x is rational and $\alpha_1, \ldots, \alpha_r \in \mathbb{Q}(\pi)$ have denominators coprime to N by assumption, $\alpha_1, \ldots, \alpha_r$ act on x by scalar multiplication, so that we can compute $\widetilde{x}_1, \ldots, \widetilde{x}_r$). Let $y_1, \ldots, y_r$ be such that $x_1 = f'(y_1), \ldots, x_r = f'(y_r)$. Similar to Remark 4.6, the isogeny theorem (5.2) fixes affine lifts $\widetilde{y}_1, \ldots, \widetilde{y}_r$ of $y_1, \ldots, y_r$ for $(Y, \mathcal{M}^\beta, \Theta_{\mathcal{M}^\beta})$ and yields n^g out of $n^g\ell$ coordinates for each of the $\widetilde{y}_s$.

Remark 5.2. If $f'(y_s) = x_s$, then $f'(y_s + t') = x_s$ for all $t' \in \ker f' = K(\mathcal{M}^\beta)_2[\ell]$. And if $\widetilde{y}_s$ is an affine lift of y_s for $(Y, \mathcal{M}^\beta, \Theta_{\mathcal{M}^\beta})$, then by Proposition 2.18, an affine lift of $y_s + t'$ is given by $t' \boxplus \widetilde{y}_s$. On the other side, $\theta_j^{\Theta_{\mathcal{M}^\beta}}(\widetilde{y}_s) = \theta_j^{\Theta_{\mathcal{M}^\beta}}(t' \boxplus \widetilde{y}_s)$ for all $j \in K(\mathcal{M}^\beta)_1[n]$. Hence, when choosing y_s, we do not have to worry about $\ker f'$.

If we knew the $n^g\ell$ coordinates for each of the $\widetilde{y}_1, \ldots, \widetilde{y}_r$, we could use (5.1) to compute the affine point $\left(\theta_{\mathbf{k}}^{\Theta'_{\mathcal{M}^{\star r}}}(y, \widetilde{0, \ldots, 0})\right)_{\mathbf{k} \in K(\mathcal{M}^{\star r})_1}$. Unfortunately we are not in this situation, but we do a similar observation to that in Section 4.2.1: if t is the fixed generator of G and if τ is the unique element of $K(\mathcal{M}^\beta)_1[\ell]$ that satisfies $f'(\tau) = t$, then the action of the theta group $\mathcal{G}(\mathcal{M}^\beta)$ on $\widetilde{Y}$ and the affine version of the isogeny theorem for f' yield affine lifts

$$\widetilde{x_s + t} = \widetilde{f'}(\tau \boxplus \widetilde{y}_s),\ \widetilde{x_s + 2t} = \widetilde{f'}(2\tau \boxplus \widetilde{y}_s), \ldots,\ \widetilde{x_s + (\ell - 1)t} = \widetilde{f'}((\ell - 1)\tau \boxplus \widetilde{y}_s)$$

of $x_s + t, \ldots, x_s + (\ell - 1)t$, for each $s = 1, \ldots, r$.

Definition 5.3. Let $x \in X(k)$ and $y \in Y(k)$ be such that $x = f'(y)$ (not necessarily the input of the algorithm). Let $\widetilde{x}$ be a fixed affine lift of x for $(X, \mathcal{L}, \Theta_{\mathcal{L}})$. Let $\widetilde{y}$ be the unique affine lift of y for $(Y, \mathcal{M}^\beta, \Theta_{\mathcal{M}^\beta})$ that satisfies $\widetilde{x} = \widetilde{f'}(\widetilde{y})$. For $1 \leq u \leq \ell - 1$, the affine lift $\widetilde{f'}(u\tau \boxplus \widetilde{y})$ of $x + ut$ is called the compatible lift and is denoted by

$$\widetilde{x + ut}_c = \widetilde{f'}(u\tau \boxplus \widetilde{y}).$$

Knowing the lift $\widetilde{x}_s$ and the compatible lifts $\widetilde{x_s + t_c}, \ldots, \widetilde{x_s + (\ell-1)t_c}$, for all $s = 1, \ldots, r$, is sufficient to compute $\left(\theta^{\Theta'_{\mathcal{M}^{\star r}}}_{\mathbf{k}}(y, \widetilde{0, \ldots, 0})\right)_{\mathbf{k} \in K(\mathcal{M}^{\star r})_1}$, but is not a necessary condition. Similar to Section 4.4.1, where we showed that the compatible lift $\widetilde{t}_c$ is an excellent lift with respect to $(X, \mathcal{L}, \Theta_{\mathcal{L}}, \widetilde{0}_X)$, we will show that the compatible lifts $\widetilde{x_1 + t_c}, \ldots, \widetilde{x_r + t_c}$ satisfy some compatibility condition, and that we can compute them up to ℓth roots of unity.

Definition 5.4. Let $x \in X(k)$ (not necessarily the input of the algorithm) and let $\widetilde{x}$ be a fixed affine lift of x for $(X, \mathcal{L}, \Theta_{\mathcal{L}})$. Let $\widetilde{t}$ and $\widetilde{0}_X$ be affine lifts for $(X, \mathcal{L}, \Theta_{\mathcal{L}})$ (e.g. the input of the algorithm). We call an affine lift $\widetilde{x + t}$ of $x + t$ suitable for $\widetilde{t}$, $\widetilde{x}$ and $\widetilde{0}_X$ if

$$\texttt{chain\_multadd}(\ell, \widetilde{x + t}, \widetilde{t}, \widetilde{x}, \widetilde{0}_X) = \widetilde{x}.$$

The computation of a suitable lift of $x + t$ is similar to the computation of excellent lifts in Section 4.4: we take any lift $\widetilde{x + t}$ and search for a scalar $\lambda_{x+t} \in \bar{k}^\times$ such that $\lambda_{x+t} \cdot \widetilde{x + t}$ is suitable. Using [LR12, Lem. 3.10], we obtain that in order for $\lambda_{x+t} \cdot \widetilde{x + t}$ to be suitable, we need

$$\lambda^\ell_{x+t} \cdot \texttt{chain\_multadd}(\ell, \widetilde{x + t}, \widetilde{t}, \widetilde{x}, \widetilde{0}_X) = \widetilde{x}.$$

This determines λ^ℓ_{x+t} uniquely. Hence, for any ℓth root λ_{x+t} of λ^ℓ_{x+t}, the lift $\lambda_{x+t} \cdot \widetilde{x + t}$ is suitable for $\widetilde{t}$, $\widetilde{x}$ and $\widetilde{0}_X$.

Algorithm 5 Computing a suitable lift of $x + t$

Require: lifts $\widetilde{x}, \widetilde{t}, \widetilde{x + t}$ and $\widetilde{0}_X$ of $x, t, x + t$ and 0_X for $(X, \mathcal{L}, \Theta_{\mathcal{L}})$ respectively
Ensure: a suitable lift $\widetilde{x + t}$ of $x + t$ for $\widetilde{t}, \widetilde{x}$ and $\widetilde{0}_X$

1: compute $\texttt{chain\_multadd}(\ell, \widetilde{x + t}, \widetilde{t}, \widetilde{x}, \widetilde{0}_X)$
2: compute the scalar $\kappa \in \bar{k}^\times$ such that

$$\texttt{chain\_multadd}(\ell, \widetilde{x + t}, \widetilde{t}, \widetilde{x}, \widetilde{0}_X) = \kappa \cdot \widetilde{x}$$

3: compute $\lambda_{x+t} \in \bar{k}^\times$ such that $\lambda^\ell_{x+t} = \kappa$
4: **return** $\lambda_{x+t} \cdot \widetilde{x + t}$

We will analyse the complexity of Algorithm 5 in Section 6. Let us now show that the notion of suitable lift is the correct notion.

Proposition 5.5. *Let $x \in X(k)$ and $y \in Y(k)$ be such that $x = f'(y)$ (not necessarily the input of the algorithm) and let $\widetilde{x}$ be a fixed affine lift of x for $(X, \mathcal{L}, \Theta_{\mathcal{L}})$. Let $\widetilde{0}_X$ be a fixed theta null point for $(X, \mathcal{L}, \Theta_{\mathcal{L}})$ and let $\widetilde{t}_c$ be the compatible lift of t (see Definition 4.7). Then, the compatible lift $\widetilde{x + t_c}$ of $x + t$ is suitable for $\widetilde{t}_c$, $\widetilde{x}$ and $\widetilde{0}_X$, and for all $u = 2, \ldots, \ell - 1$ we have*

$$\widetilde{x + ut_c} = \texttt{chain\_multadd}(u, \widetilde{x + t_c}, \widetilde{t}_c, \widetilde{x}, \widetilde{0}_X).$$

Proof. Let $\widetilde{0}_Y$ and $\widetilde{y}$ be the lifts of 0_Y and y for $(Y, \mathcal{M}^\beta, \Theta_{\mathcal{M}^\beta})$ fixed by $\widetilde{f'}, \widetilde{0}_X$ and $\widetilde{x}$

respectively. Then, for all $2 \leq u \leq \ell$ we have

$$\begin{aligned}
&\texttt{chain_multadd}(u, \widetilde{x+t}_c, \widetilde{t}_c, \widetilde{x}, \widetilde{0}_X) \\
&\qquad = \texttt{chain_multadd}(u, \widetilde{f}'(\tau \boxplus \widetilde{y}), \widetilde{f}'(\tau \boxplus \widetilde{0}_Y), \widetilde{f}'(\widetilde{y}), \widetilde{f}'(\widetilde{0}_Y)) \\
&\qquad = \widetilde{f}'(\texttt{chain_multadd}(u, \tau \boxplus \widetilde{y}, \tau \boxplus \widetilde{0}_Y, \widetilde{y}, \widetilde{0}_Y)) \quad \text{by Lemma 4.9 } iii) \\
&\qquad = \widetilde{f}'(u\tau \boxplus \texttt{chain_multadd}(u, \widetilde{y}, \widetilde{0}_Y, \widetilde{y}, \widetilde{0}_Y)) \quad \text{by Lemma 4.10} \\
&\qquad = \widetilde{f}'(u\tau \boxplus \widetilde{y}).
\end{aligned}$$

In particular, if $u = \ell$ then

$$\widetilde{f}'(\ell\tau \boxplus \widetilde{y}) = \widetilde{f}'(\widetilde{y}) = \widetilde{x},$$

and for all other u we have

$$\widetilde{f}'(u\tau \boxplus \widetilde{y}) = \widetilde{x+ut}_c.$$

□

In general, we do not know the compatible lift of $x + t$. However, we would like to apply a similar idea to the one in Section 4.4.2, i.e. starting with an arbitrary lift $\widetilde{x+t}$ of $x + t$, if we make it suitable for $\widetilde{t}_c, \widetilde{x}$ and $\widetilde{0}_X$, then it will differ from $\widetilde{x+t}_c$ by an ℓth root of unity. The problem is that we do not know the compatible lift $\widetilde{t}_c$ of t either. The following proposition will be helpful.

Proposition 5.6. *Let $\widetilde{t}$ (not necessarily excellent), $\widetilde{x}$ and $\widetilde{0}_X$ be fixed affine lifts of t, x and 0_X for $(X, \mathcal{L}, \Theta_{\mathcal{L}})$ respectively. Let $\widetilde{x+t}$ be an affine lift of $x + t$. Then, $\widetilde{x+t}$ is suitable for $\widetilde{t}, \widetilde{x}$ and $\widetilde{0}_X$ if and only if $\widetilde{x+t}$ is suitable for $\zeta \cdot \widetilde{t}, \widetilde{x}$ and $\widetilde{0}_X$, for any ℓth root of unity ζ.*

Proof. This is a direct consequence of [LR12, Lem. 3.10], saying that

$$\texttt{chain\_multadd}(\ell, \widetilde{x+t}, \zeta \cdot \widetilde{t}, \widetilde{x}, \widetilde{0}_X) = \zeta^{\ell(\ell-1)} \cdot \texttt{chain\_multadd}(\ell, \widetilde{x+t}, \widetilde{t}, \widetilde{x}, \widetilde{0}_X).$$

□

5.1.2 Choice of lifts of $x_s + u_s t$

In this section we explain our choice of lifts of $x_1, \ldots, x_r$. Our idea is based on the Chinese Remainder Theorem. Let $\widetilde{x}, \widetilde{t}$ and $\widetilde{0}_X$ be fixed affine lifts of x, t and 0_X for $(X, \mathcal{L}, \Theta_{\mathcal{L}})$ respectively. Suppose that the lifts $\widetilde{x}$ and $\widetilde{0}_X$ satisfy

$$\texttt{chain\_mult}(N, \widetilde{x}, \widetilde{0}_X) = \widetilde{0}_X.$$

(We can easily modify $\widetilde{x}$ in order to satisfy the above.) Suppose that, in addition, we are given a lift of $x + t$ for $(X, \mathcal{L}, \Theta_{\mathcal{L}})$. For example, if we work on the Jacobian variety of a hyperelliptic curve, then we can use the formulas of [vW98] and [Cos11] to convert between theta and Mumford coordinates. If we have converted the points x and t from theta to Mumford coordinates, we compute $x+t$ and convert back to theta coordinates. This works because $\mathcal{L} = \mathcal{L}_0^{\otimes n}$, for $n = 2$ or $n = 4$.

Let $\widetilde{0}_Y$ and $\widetilde{y}$ be the unique affine lifts of 0_Y and y for $(Y, \mathcal{M}^\beta, \Theta_{\mathcal{M}^\beta})$ that satisfy

$$\widetilde{f}'(\widetilde{0}_Y) = \widetilde{0}_X \text{ and } \widetilde{f}'(\widetilde{y}) = \widetilde{x}.$$

It follows immediately that $\texttt{chain\_mult}(N, \widetilde{y}, \widetilde{0}_Y) = \widetilde{0}_Y$. The lifts $\widetilde{0}_Y$ and $\widetilde{y}$ determine compatible lifts $\widetilde{t}_c = \widetilde{f}'(\tau \boxplus \widetilde{0}_Y)$ and $\widetilde{x+t}_c = \widetilde{f}'(\tau \boxplus \widetilde{y})$ of t and $x+t$ respectively, where τ is the unique element of $K(\mathcal{M}^\beta)_1[\ell]$ that satisfies $f'(\tau) = t$.

Let $\widetilde{t}_e$ be the excellent lift of t with respect to $(X, \mathcal{L}, \Theta_\mathcal{L}, \widetilde{0}_X)$ computed in Section 4.4.2. From our initial lift of $x+t$ we compute a lift $\widetilde{x+t}$ that is suitable for $\widetilde{t}_e$, $\widetilde{x}$ and $\widetilde{0}_X$. By Proposition 5.6, the lift $\widetilde{x+t}$ is suitable for $\widetilde{t}_c$, $\widetilde{x}$ and $\widetilde{0}_X$ as well. Hence, it differs from $\widetilde{x+t}_c$ by an unknown ℓth root of unity ζ_{x+t}, i.e.

$$\widetilde{x+t} = \zeta_{x+t} \cdot \widetilde{x+t}_c.$$

Let $\widetilde{y+\tau}$ be the lift of $y+\tau$ induced by $\widetilde{f}'$ and $\widetilde{x+t}$. It is not hard to see that

$$\widetilde{y+\tau} = \zeta_{x+t} \cdot (\tau \boxplus \widetilde{y}).$$

Let

$$c_{[\cdot,\cdot]} \colon \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/N\ell\mathbb{Z},\ (a,u) \mapsto c_{[a,u]}$$

be the inverse of the projection morphism. For $s = 1, \ldots, r$, let $a_{s,x}$ be the integer (mod N) such that $x_s = \alpha_s(x) = a_{s,x}x$. Define lifts of $x_1, \ldots, x_r$ as

$$\widetilde{x}_s := \texttt{chain\_mult}(c_{[a_{s,x},0]}, \widetilde{x+t}, \widetilde{0}_X), \text{ for } s = 1, \ldots, r. \tag{5.3}$$

Indeed, $x+t$ is a point of order $N\ell$ and $c_{[a_{s,x},0]}$ is congruent to $a_{s,x}$ modulo N and congruent to 0 modulo ℓ. The lifts $\widetilde{x}_1, \ldots, \widetilde{x}_r$ and $\widetilde{f}'$ fix lifts $\widetilde{y}_1, \ldots, \widetilde{y}_r$ of $y_1, \ldots, y_r$, and using the compatibility of the affine isogeny $\widetilde{f}'$ with $\texttt{chain\_mult}$, it is not hard to see that

$$\widetilde{y}_s = \texttt{chain\_mult}(c_{[a_{s,x},0]}, \widetilde{y+\tau}, \widetilde{0}_Y), \text{ for all } s = 1, \ldots, r.$$

Knowing the lifts $\widetilde{y}_1, \ldots, \widetilde{y}_r$, or equivalently knowing the compatible lifts

$$\{\widetilde{x_s + u_s t}_c : s = 1, \ldots, r,\ u_s = 1, \ldots, \ell - 1\},$$

where

$$\widetilde{x_s + u_s t}_c = \widetilde{f}'(u_s\tau \boxplus \widetilde{y}_s) = \widetilde{f}'(u_s\tau \boxplus \texttt{chain\_mult}(c_{[a_{s,x},0]}, \widetilde{y+\tau}, \widetilde{0}_Y)), \tag{5.4}$$

we could substitute their coordinates in the right-hand side of (5.1) and compute the affine point $\left(\theta^{\Theta'_{\mathcal{M}^{\star r}}}_{\mathbf{k}}(y, \widetilde{0, \ldots, 0})\right)_{\mathbf{k} \in K(\mathcal{M}^{\star r})_1}$. But of course we are not in the situation where we know the lifts $\widetilde{y}_1, \ldots, \widetilde{y}_r$. We have the following key result.

Proposition 5.7. *Let $\widetilde{0}_X$ and $\widetilde{x}$ be fixed affine lifts of 0_X and x for $(X, \mathcal{L}, \Theta_\mathcal{L})$ respectively, and suppose $\texttt{chain\_mult}(N, \widetilde{x}, \widetilde{0}_X) = \widetilde{0}_X$. Let $\widetilde{t}_e$ be a fixed excellent lift of t with respect to $(X, \mathcal{L}, \Theta_\mathcal{L}, \widetilde{0}_X)$ and let $\widetilde{x+t}$ be a fixed suitable lift of $x+t$ for $\widetilde{t}_e, \widetilde{x}$ and $\widetilde{0}_X$. It differs from the compatible lift $\widetilde{x+t}_c$ by an ℓth root of unity ζ_{x+t}. Let $\widetilde{x}_1, \ldots, \widetilde{x}_r$ be the lifts of $x_1, \ldots, x_r$ as defined in (5.3). For $s = 1, \ldots, r$ and $u_s = 1, \ldots, \ell - 1$, define a lift of $x_s + u_s t$ as*

$$\widetilde{x_s + u_s t} := \texttt{chain\_mult}(c_{[a_{s,x},u_s]}, \widetilde{x+t}, \widetilde{0}_X). \tag{5.5}$$

Then, we have

$$\widetilde{x_s + u_s t} = \zeta_{x+t}^{u_s^2} \cdot \widetilde{x_s + u_s t}_c,$$

where the compatible lift of $x_s + u_s t$ is as in (5.4).

Proof. Observe that for $s = 1, \dots, r$,

$$\begin{aligned}
\widetilde{y}_s &= \texttt{chain_mult}(c_{[a_{s,x},0]}, \widetilde{y+\tau}, \widetilde{0}_Y) = \texttt{chain_mult}(c_{[a_{s,x},0]}, \zeta_{x+t} \cdot (\tau \boxplus \widetilde{y}), \widetilde{0}_Y) \\
&= \texttt{chain_mult}(c_{[a_{s,x},0]}, \tau \boxplus \widetilde{y}, \widetilde{0}_Y) \quad \text{by [LR12, Lem. 3.10], since } c_{[a_{s,x},0]} \equiv 0 \mod \ell \\
&= \texttt{chain_mult}(c_{[a_{s,x},0]}, \widetilde{y}, \widetilde{0}_Y) \quad \text{by Lemma 4.10, since } c_{[a_{s,x},0]} \equiv 0 \mod \ell.
\end{aligned}$$

Now,

$$\begin{aligned}
\widetilde{x_s + u_s}t &= \texttt{chain_mult}(c_{[a_{s,x},u_s]}, \widetilde{x+t}, \widetilde{0}_X) \\
&= \texttt{chain_mult}(c_{[a_{s,x},u_s]}, \widetilde{f'}(\widetilde{y+\tau}), \widetilde{0}_X) \\
&= \widetilde{f'}(\texttt{chain_mult}(c_{[a_{s,x},u_s]}, \widetilde{y+\tau}, \widetilde{0}_Y)) \\
&= \widetilde{f'}(\texttt{chain_mult}(c_{[a_{s,x},u_s]}, \zeta_{x+t} \cdot (\tau \boxplus \widetilde{y}), \widetilde{0}_Y)) \\
&= \widetilde{f'}(\zeta_{x+t}^{c^2_{[a_{s,x},u_s]}} \cdot \texttt{chain_mult}(c_{[a_{s,x},u_s]}, \tau \boxplus \widetilde{y}, \widetilde{0}_Y)) \\
&= \widetilde{f'}(\zeta_{x+t}^{u_s^2} \cdot (u_s\tau \boxplus \texttt{chain_mult}(c_{[a_{s,x},u_s]}, \widetilde{y}, \widetilde{0}_Y))) \\
&\quad \text{(since } c_{[a_{s,x},u_s]} \equiv u_s \bmod \ell, \text{ and Lemma 4.10)} \\
&= \zeta_{x+t}^{u_s^2} \cdot \widetilde{f'}(u_s\tau \boxplus \texttt{chain_mult}(c_{[a_{s,x},0]}, \widetilde{y}, \widetilde{0}_Y)) \\
&\quad \text{(since } \texttt{chain_mult}(N, \widetilde{y}, \widetilde{0}_Y) = \widetilde{0}_Y) \\
&= \zeta_{x+t}^{u_s^2} \cdot \widetilde{f'}(u_s\tau \boxplus \widetilde{y}_s) \quad \text{(by the above)} \\
&= \zeta_{x+t}^{u_s^2} \cdot \widetilde{x_s + u_s}t_c.
\end{aligned}$$

□

Hence, when substituting $\theta^{\Theta_{\mathcal{L}}}_{f'(j_s)}(\texttt{chain\_mult}(c_{[a_{s,x},u_s]}, \widetilde{x+t}, \widetilde{0}_X))$ for $\theta^{\Theta_{\mathcal{M}^\beta}}_{j_s+\tau_s}(\widetilde{y}_s)$ in

$$\sum_{\substack{\boldsymbol{\tau} \in K((\mathcal{M}^\beta)^{\star r})_1[\ell] \\ F(\boldsymbol{\tau})=0}} \prod_{s=1}^{r} \theta^{\Theta_{\mathcal{M}^\beta}}_{j_s+\tau_s}(\widetilde{y}_s),$$

where $j_1, \dots, j_r \in K(\mathcal{M}^\beta)_1[n]$ and $\boldsymbol{\tau} = (\tau_1, \dots, \tau_r) = (u_1\tau, \dots, u_r\tau)$, with $1 \le u_1, \dots, u_r \le \ell - 1$, we actually compute

$$\sum_{\substack{\boldsymbol{\tau} \in K((\mathcal{M}^\beta)^{\star r})_1[\ell] \\ F(\boldsymbol{\tau})=0}} \zeta_{x+t}^{u_1^2+\cdots+u_r^2} \cdot \theta^{\Theta_{\mathcal{M}^\beta}}_{j_1+u_1\tau}(\widetilde{y}_1) \cdots \theta^{\Theta_{\mathcal{M}^\beta}}_{j_1+u_1\tau}(\widetilde{y}_r). \tag{5.6}$$

Let us consider the case $r = 4$. The case $r = 2$ is easier and can be proven in a similar way. In Lemma 4.12 we have seen that

$$K((\mathcal{M}^\beta)^{\star 4})_1[\ell] \cap \ker F = \{ {}^tM_F(\tau_1, \tau_2, 0, 0) : \tau_1, \tau_2 \in K(\mathcal{M}^\beta)_1[\ell] \}.$$

Write $\tau_1 = u_1\tau$ and $\tau_2 = u_2\tau$ with $0 \le u_1, u_2 \le \ell - 1$, and for $s = 1, \dots, 4$, let $a_{s,\tau}$ be the integer (mod ℓ) given by the action of α_s on τ, i.e. $a_{s,\tau}$ satisfies

$$\alpha_s(\tau) = a_{s,\tau}\tau. \tag{5.7}$$

We then have

$$\begin{aligned}
&K((\mathcal{M}^\beta)^{\star 4})_1[\ell] \cap \ker F \\
&= \{((a_{1,\tau}u_1 + a_{2,\tau}u_2)\tau, (-a_{2,\tau}u_1 + a_{1,\tau}u_2)\tau, (-a_{3,\tau}u_1 - a_{4,\tau}u_2)\tau, (-a_{4,\tau}u_1 + a_{3,\tau}u_2)\tau) : 0 \le u_1, u_2 \le \ell - 1\}.
\end{aligned}$$

Proposition 5.8. *Let $\widetilde{0}_X$ and $\widetilde{x}$ be fixed affine lifts of 0_X and x for $(X, \mathcal{L}, \Theta_{\mathcal{L}})$ respectively, and suppose* $\texttt{chain\_mult}(N, \widetilde{x}, \widetilde{0}_X) = \widetilde{0}_X$. *Let $\widetilde{t}_e$ be a fixed excellent lift of t with respect to $(X, \mathcal{L}, \Theta_{\mathcal{L}}, \widetilde{0}_X)$ and let $\widetilde{x+t}$ be a fixed suitable lift of $x+t$ for $\widetilde{t}_e, \widetilde{x}$ and $\widetilde{0}_X$. We can compute an affine lift $\left(\theta^{\Theta'_{\mathcal{M}^{\star 4}}}_{\mathbf{k}}(\widetilde{y,0,0,0})\right)_{\mathbf{k}\in K(\mathcal{M}^{\star 4})_1}$ of $(y,0,0,0)$ for $(Y^4, \mathcal{M}^{\star 4}, \Theta'_{\mathcal{M}^{\star 4}})$ as follows: let $\mathbf{k} \in K(\mathcal{M}^{\star 4})_1$ and let $\mathbf{j} = (j_1, \dots, j_4) \in K((\mathcal{M}^{\beta})^{\star 4})_1[n]$ be the unique element of $K((\mathcal{M}^{\beta})^{\star 4})_1$ that satisfies $F(\mathbf{j}) = \mathbf{k}$. Then, we have*

$$\begin{aligned}\theta^{\Theta'_{\mathcal{M}^{\star 4}}}_{\mathbf{k}}(\widetilde{y,0,0,0}) = \sum_{0\le u_1,u_2\le \ell-1} & \theta^{\Theta_{\mathcal{L}}}_{f'(j_1)}(\texttt{chain\_mult}(c_{[a_{1,x},a_{1,\tau}u_1+a_{2,\tau}u_2]}, \widetilde{x+t}, \widetilde{0}_X)) \\ & \cdot \theta^{\Theta_{\mathcal{L}}}_{f'(j_2)}(\texttt{chain\_mult}(c_{[a_{2,x},-a_{2,\tau}u_1+a_{1,\tau}u_2]}, \widetilde{x+t}, \widetilde{0}_X)) \\ & \cdot \theta^{\Theta_{\mathcal{L}}}_{f'(j_3)}(\texttt{chain\_mult}(c_{[a_{3,x},-a_{3,\tau}u_1-a_{4,\tau}u_2]}, \widetilde{x+t}, \widetilde{0}_X)) \\ & \cdot \theta^{\Theta_{\mathcal{L}}}_{f'(j_4)}(\texttt{chain\_mult}(c_{[a_{4,x},-a_{4,\tau}u_1+a_{3,\tau}u_2]}, \widetilde{x+t}, \widetilde{0}_X)).\end{aligned}$$

Proof. By (5.6) it suffices to show that $(a_{1,\tau}u_1+a_{2,\tau}u_2)^2+(-a_{2,\tau}u_1+a_{1,\tau}u_2)^2+(-a_{3,\tau}u_1-a_{4,\tau}u_2)^2+(-a_{4,\tau}u_1+a_{3,\tau}u_2)^2 \equiv 0 \mod \ell$. But

$$(a_{1,\tau}u_1+a_{2,\tau}u_2)^2+(-a_{2,\tau}u_1+a_{1,\tau}u_2)^2+(-a_{3,\tau}u_1-a_{4,\tau}u_2)^2+(-a_{4,\tau}u_1+a_{3,\tau}u_2)^2 = (a_{1,\tau}^2+\cdots+a_{4,\tau}^2)(u_1^2+u_2^2)$$

and $a_{1,\tau}^2 + \cdots + a_{4,\tau}^2$ is a multiple of ℓ, since it is given by the scalar of the action of $\beta = \alpha_1^2 + \cdots + \alpha_4^2$ on τ. □

5.2 Modification of $\Theta'_{\mathcal{M}^{\star r}}$ via a metaplectic automorphism

We encounter the same problem than in Section 4.5, that is, the symmetric theta structure $\Theta'_{\mathcal{M}^{\star r}}$ on $(Y^r, \mathcal{M}^{\star r})$ is not of product form and hence, the affine point $\left(\theta^{\Theta'_{\mathcal{M}^{\star r}}}_{\mathbf{k}}(\widetilde{y,0,\dots,0})\right)_{\mathbf{k}\in K(\mathcal{M}^{\star r})_1}$ from Section 5.1.2 does not allow us to recover the theta coordinates of $y = f(x)$ for a single factor $(Y, \mathcal{M})$.

Let $M \in \mathrm{Aut}_{k^\times}(\mathcal{H}(\delta_{\mathcal{M}^{\star r}}))$ be the metaplectic automorphism from Section 4.5.1 that transforms the theta structure $\Theta'_{\mathcal{M}^{\star r}}$ on $(Y^r, \mathcal{M}^{\star r})$ into a symmetric product theta structure $(\Theta_{\mathcal{M}})^{\star r}$, where $\Theta_{\mathcal{M}}$ is a symmetric theta structure on $(Y, \mathcal{M})$. Similar to Section 4.5.2, we apply the symplectic transformation formula to $\left\{\theta^{\Theta'_{\mathcal{M}^{\star r}}}_{\mathbf{k}}(\widetilde{y,0,\dots,0})\right\}_{\mathbf{k}\in K(\mathcal{M}^{\star r})_1}$ and obtain

$$\left\{\theta^{(\Theta_{\mathcal{M}})^{\star r}}_{\boldsymbol{\kappa}}(\widetilde{y,0,\dots,0}) = \theta^{\Theta_{\mathcal{M}}}_{\kappa_1}(\widetilde{y}) \cdot \theta^{\Theta_{\mathcal{M}}}_{\kappa_2}(\widetilde{0}_Y) \cdots \theta^{\Theta_{\mathcal{M}}}_{\kappa_r}(\widetilde{0}_Y)\right\}_{\boldsymbol{\kappa}\in K(\mathcal{M}^{\star r})_1}.$$

Algorithm 6 Evaluating the isogeny f on points

Require: lifts $\widetilde{x}, \widetilde{t}$ and $\widetilde{0}_X$ of x, t and 0_X for $(X, \mathcal{L}, \Theta_{\mathcal{L}})$ respectively, where $x \in X(k)$ is a point of order N (coprime to $\ell \cdot [\mathcal{O}_{K_0} : \mathbb{Z}[\pi + \pi^\dagger]]$), and t is a generator of $G = \ker f$

Ensure: a lift $\widetilde{y}$ of $y = f(x)$ for $(Y, \mathcal{M}, \Theta_{\mathcal{M}})$

1: modify $\widetilde{x}$ so that it satisfies $\texttt{chain\_mult}(N, \widetilde{x}, \widetilde{0}_X) = \widetilde{0}_X$

2: compute an excellent lift $\widetilde{t}_e$ of t with respect to $(X, \mathcal{L}, \Theta_{\mathcal{L}}, \widetilde{0}_X)$, see Algorithm 2

3: compute a lift of $x + t$ for $(X, \mathcal{L}, \Theta_{\mathcal{L}})$ (e.g. using the theta to Mumford coordinate conversion when working on the Jacobian variety of a hyperelliptic curve)

4: compute a lift $\widetilde{x+t}$ of $x + t$ that is suitable for $\widetilde{t}_e, \widetilde{x}$ and $\widetilde{0}_X$, see Algorithm 5

5: let $\alpha_1, \ldots, \alpha_r$ be as in step 2. of Algorithm 4; compute $0 \le a_{1,x}, \ldots, a_{r,x} \le N-1$ and $0 \le a_{1,t}, \ldots, a_{r,t} \le \ell - 1$ such that for all $s = 1, \ldots, r$,

$$\alpha_s(x) = a_{s,x} x \text{ and } \alpha_s(t) = a_{s,t} t$$

(knowing that $\alpha_s \in \mathbb{Q}(\pi)$ with denominators coprime to N and ℓ, it suffices to know the scalar by which π acts on t)

6: **if** $r = 2$ **then**

7: for each $\mathbf{k} \in K(\mathcal{M}^{\star 2})_1$, let $\mathbf{j} = (j_1, j_2) \in K((\mathcal{M}^\beta)^{\star 2})_1[n]$ be the unique element of $K((\mathcal{M}^\beta)^{\star 2})_1$ that satisfies $F(\mathbf{j}) = \mathbf{k}$; compute $\theta^{\Theta'_{\mathcal{M}^{\star 2}}}_{\mathbf{k}}(\widetilde{y, 0})$ as

$$\theta^{\Theta'_{\mathcal{M}^{\star 2}}}_{\mathbf{k}}(\widetilde{y,0}) = \sum_{0 \le u \le \ell - 1} \theta^{\Theta_{\mathcal{L}}}_{f'(j_1)}(\texttt{chain\_mult}(c_{[a_{1,x}, a_{1,t}u]}, \widetilde{x+t}, \widetilde{0}_X)) \cdot \theta^{\Theta_{\mathcal{L}}}_{f'(j_2)}(\texttt{chain\_mult}(c_{[a_{2,x}, -a_{2,t}u]}, \widetilde{x+t}, \widetilde{0}_X))$$

8: **else if** $r = 4$ **then**

9: for each $\mathbf{k} \in K(\mathcal{M}^{\star 4})_1$, let $\mathbf{j} = (j_1, \ldots, j_4) \in K((\mathcal{M}^\beta)^{\star 4})_1[n]$ be the unique element of $K((\mathcal{M}^\beta)^{\star 4})_1$ that satisfies $F(\mathbf{j}) = \mathbf{k}$; compute $\theta^{\Theta'_{\mathcal{M}^{\star 4}}}_{\mathbf{k}}(\widetilde{y,0,0,0})$ as

$$\begin{aligned}\theta^{\Theta'_{\mathcal{M}^{\star 4}}}_{\mathbf{k}}(\widetilde{y,0,0,0}) = \sum_{0 \le u_1, u_2 \le \ell - 1} & \theta^{\Theta_{\mathcal{L}}}_{f'(j_1)}(\texttt{chain\_mult}(c_{[a_{1,x}, a_{1,t}u_1 + a_{2,t}u_2]}, \widetilde{x+t}, \widetilde{0}_X)) \\ & \cdot \theta^{\Theta_{\mathcal{L}}}_{f'(j_2)}(\texttt{chain\_mult}(c_{[a_{2,x}, -a_{2,t}u_1 + a_{1,t}u_2]}, \widetilde{x+t}, \widetilde{0}_X)) \\ & \cdot \theta^{\Theta_{\mathcal{L}}}_{f'(j_3)}(\texttt{chain\_mult}(c_{[a_{3,x}, -a_{3,t}u_1 - a_{4,t}u_2]}, \widetilde{x+t}, \widetilde{0}_X)) \\ & \cdot \theta^{\Theta_{\mathcal{L}}}_{f'(j_4)}(\texttt{chain\_mult}(c_{[a_{4,x}, -a_{4,t}u_1 + a_{3,t}u_2]}, \widetilde{x+t}, \widetilde{0}_X))\end{aligned}$$

10: **end if**

11: take the same metaplectic automorphism $M \in \mathrm{Aut}_{k^\times}(\mathcal{H}(\delta_{\mathcal{M}^{\star r}}))$ as in step 11. of Algorithm 4 and apply the symplectic coordinate change to $\left\{\theta^{\Theta'_{\mathcal{M}^{\star r}}}_{\mathbf{k}}(\widetilde{y, 0, \ldots, 0})\right\}_{\mathbf{k} \in K(\mathcal{M}^{\star r})_1}$ to obtain the coordinates $\left\{\theta^{(\Theta_{\mathcal{M}})^{\star r}}_{\boldsymbol{\kappa}}(\widetilde{y, 0, \ldots, 0})\right\}_{\boldsymbol{\kappa} \in K(\mathcal{M}^{\star r})_1}$ for the product theta structure $(\Theta_{\mathcal{M}})^{\star r}$

12: **return** fix $(\kappa_1, \ldots, \kappa_r) \in K(\mathcal{M}^{\star r})_1$ such that $\theta^{(\Theta_{\mathcal{M}})^{\star r}}_{\boldsymbol{\kappa}}(\widetilde{y, 0, \ldots, 0}) \neq 0$ and return

$$\left(\theta^{\Theta_{\mathcal{M}}}_{\kappa}(\widetilde{y})\right)_{\kappa \in K(\mathcal{M})_1},$$

where

$$\theta^{\Theta_{\mathcal{M}}}_{\kappa}(\widetilde{y}) := \theta^{\Theta_{\mathcal{M}}}_{\kappa}(\widetilde{y}) \cdot \theta^{\Theta_{\mathcal{M}}}_{\kappa_2}(\widetilde{0}_Y) \cdots \theta^{\Theta_{\mathcal{M}}}_{\kappa_r}(\widetilde{0}_Y)$$

for all $\kappa \in K(\mathcal{M})_1$

We analyse the complexity of Algorithm 6 in Section 6.

Theorem 5.9. *Algorithm 6 computes an affine lift $\widetilde{y}$ of $y = f(x)$ for $(Y, \mathcal{M}, \Theta_{\mathcal{M}})$.*

Proof. Observe that the $a_{1,t}, \dots, a_{r,t}$ computed at step 5. are equal to the $a_{1,\tau}, \dots, a_{r,\tau}$ from (5.7). By Proposition 5.8, step 7. or step 9. correctly computes $\left(\theta_{\mathbf{k}}^{\Theta'_{\mathcal{M}^{\star r}}}(y, \widetilde{0, \dots, 0})\right)_{\mathbf{k} \in K(\mathcal{M}^{\star r})_1}$. Then, as explained in Section 4.5.2, step 11. computes the coordinates $\left\{\theta_{\boldsymbol{\kappa}}^{(\Theta_{\mathcal{M}})^{\star r}}(y, \widetilde{0, \dots, 0}) = \theta_{\kappa_1}^{\Theta_{\mathcal{M}}}(\widetilde{y}) \cdot \theta_{\kappa_2}^{\Theta_{\mathcal{M}}}(\widetilde{0}_Y) \cdots \theta_{\kappa_r}^{\Theta_{\mathcal{M}}}(\widetilde{0}_Y)\right\}_{\boldsymbol{\kappa} \in K(\mathcal{M}^{\star r})_1}$ of $(y, \dots, 0)$ for the product theta structure $(\Theta_{\mathcal{M}})^{\star r}$ and hence, step 12. outputs an affine lift $\widetilde{y}$ of y for $(Y, \mathcal{M}, \Theta_{\mathcal{M}})$. $\square$

6 Complexity analysis

The algorithms from Sections 4 and 5 depend on the following parameters:

- the degree ℓ of the isogeny $f\colon X \to Y$,
- the level $n = 2$ or $n = 4$ of the theta functions that we use in the computation, i.e. the integer n where $\mathcal{L} = \mathcal{L}_0^{\otimes n}$,
- the dimension g of the abelian variety X,
- the parameter $r = 2$ or $r = 4$,
- the order N of the point $x \in X(k)$,

as well as on the sizes of the fields

- $k = \mathbb{F}_q$, the field of definition of X,
- k_0, the field of definition of the affine theta coordinates of 0_X,
- k_t, the field of definition of the affine theta coordinates of t,
- k_x, the field of definition of the affine theta coordinates of x,
- k_{x+t}, the field of definition of the affine theta coordinates of $x + t$.

Remark 6.1. If $(X, \mathcal{L}_0)$ is the Jacobian variety of a hyperelliptic curve C over $\mathbb{F}_q$, we can explicitly determine the fields k_0, k_t, k_x and k_{x+t}. Suppose that the Weierstrass points of C have coordinates in $\mathbb{F}_{q^d}$. Then k_0 is equal to $\mathbb{F}_{q^{nd}}$. In general, if $x' \in X(\mathbb{F}_{q^{d'}})$ is any $\mathbb{F}_{q^{d'}}$-rational point on the Jacobian variety of C, then the theta coordinates of x' will be elements of the composite field of $\mathbb{F}_{q^{nd}}$ and $\mathbb{F}_{q^{d'}}$. Since x is $\mathbb{F}_q$-rational we have that $k_x = k_0 = \mathbb{F}_{q^{nd}}$, and if l is the smallest integer such that $X[\ell] \subset X(\mathbb{F}_{q^l})$, then k_t is the composite field of $\mathbb{F}_{q^{nd}}$ and $\mathbb{F}_{q^l}$. In this case, the ℓth roots of unity form a subgroup of $\mathbb{F}_{q^l}^\times$, hence an excellent lift $\widetilde{t_e}$ of t will also have coordinates in k_t. Finally, by the same arguments we have that $k_{x+t} = k_t$ and that a suitable lift of $x + t$ will have coordinates in k_{x+t}.

Denote by $\mathbf{M}(k), \mathbf{S}(k), \mathbf{A}(k)$ and $\mathbf{D}(k)$ the costs of multiplication, squaring, addition and division in the field k respectively, and idem for the fields k_0, k_t, k_x and k_{x+t}. Following [Rob10, 4.4.11] and [Rob10, 4.4.13], a chain addition for affine points with coordinates in k_t has complexity

$$(n^g + 2^g)\mathbf{M}(k_t) + (n^g + 2^g)\mathbf{S}(k_t) + n^g\mathbf{D}(k_t) + (4n)^g\mathbf{A}(k_t),$$

and a chain multiplication $\texttt{chain\_mult}(m, \widetilde{t}, \widetilde{0}_X)$ requires at most $2\log(m)$ chain additions, with a slightly different complexity of

$$(n^g + 2^g)\mathbf{M}(k_t) + n^g\mathbf{S}(k_t) + n^g\mathbf{D}(k_t) + (4n)^g\mathbf{A}(k_t)$$

each.

Complexity analysis of Algorithm 1. The complexity of this algorithm is negligible, it depends only on the complexities of writing ℓ as the sum of two or four squares of integers respectively, and inverting a 4×4 rational matrix.

Complexity analysis of Algorithm 2. The complexity is dominated by the chain multiplication, which requires

$$2\log(\ell/2)\cdot((n^g+2^g)\mathbf{M}(k_t)+n^g\mathbf{S}(k_t)+n^g\mathbf{D}(k_t)+(4n)^g\mathbf{A}(k_t))$$

operations, as well as taking an ℓth root of κ.

Complexity analysis of Algorithm 3. First, we need to evaluate the r endomorphisms $\alpha_1,\ldots,\alpha_r$ on the $2n$-torsion basis $\{e_1,\ldots,e_g,\hat{e}_1,\ldots,\hat{e}_g\}$ of $X[2n]$. This computation depends on g, n and $\log q$ and is independent of ℓ. It is very fast, supposing we work on the Jacobian variety of a hyperelliptic curve and use the theta to Mumford coordinate conversion. Then the loop is over a group of order

$$\#\,\mathbf{GL}_{2g}(\mathbb{Z}/2n\mathbb{Z})=\begin{cases}2^{(2g)^2}\cdot\#\,\mathbf{GL}_{2g}(\mathbb{Z}/2\mathbb{Z}) & \text{if } n=2\\ 2^{2(2g)^2}\cdot\#\,\mathbf{GL}_{2g}(\mathbb{Z}/2\mathbb{Z}) & \text{if } n=4\end{cases}$$

see [Han06, Cor. 2.8], but if $N\in\mathbf{GL}_{2g}(\mathbb{Z}/2n\mathbb{Z})$ satisfies $\Delta(N)M^{-1}_{F\circ(\beta^{\times r})^{-1}}\in\mathbf{Sp}_{2gr}(\mathbb{Z}/2n\mathbb{Z})$, then $N'N$ also satisfies $\Delta(N'N)M^{-1}_{F\circ(\beta^{\times r})^{-1}}\in\mathbf{Sp}_{2gr}(\mathbb{Z}/2n\mathbb{Z})$ for all $N'\in\mathbf{Sp}_{2g}(\mathbb{Z}/2n\mathbb{Z})$, so that we can expect the loop to stop after roughly

$$\frac{\#\,\mathbf{GL}_{2g}(\mathbb{Z}/2n\mathbb{Z})}{\#\,\mathbf{Sp}_{2g}(\mathbb{Z}/2n\mathbb{Z})}$$

iterations. Knowing that

$$\#\,\mathbf{Sp}_{2g}(\mathbb{Z}/2n\mathbb{Z})=\begin{cases}2^{2g^2+g}\cdot\#\,\mathbf{Sp}_{2g}(\mathbb{Z}/2\mathbb{Z}) & \text{if } n=2\\ 2^{2(2g^2+g)}\cdot\#\,\mathbf{Sp}_{2g}(\mathbb{Z}/2\mathbb{Z}) & \text{if } n=4\end{cases}$$

and

$$\frac{\#\,\mathbf{GL}_{2g}(\mathbb{Z}/2\mathbb{Z})}{\#\,\mathbf{Sp}_{2g}(\mathbb{Z}/2\mathbb{Z})}=2^{g(2g-1)}\prod_{i=0}^{g-1}\left(1-\frac{1}{2^{2i+1}}\right),$$

we can expect the loop to stop after roughly

$$2^{2g(2g-1)}\prod_{i=0}^{g-1}\left(1-\frac{1}{2^{2i+1}}\right)$$

iterations in case $n=2$, and after roughly

$$2^{3g(2g-1)}\prod_{i=0}^{g-1}\left(1-\frac{1}{2^{2i+1}}\right)$$

iterations in case $n=4$.

Complexity analysis of Algorithm 4. For steps 1. and 2. see the complexities of Algorithms 1 and 2. If we work on the Jacobian variety of a hyperelliptic curve C over k, then the excellent lift $\widetilde{t}_e$ will have coordinates in k_t. For step 3., if we know the scalar by which π acts on t (which is easy to determine when working on the Jacobian variety of a hyperelliptic curve), then this step is brought down to a computation in $\mathbb{Z}/\ell\mathbb{Z}$. For steps 5. and 7., we first precompute

$$\texttt{chain\_mult}(2,\widetilde{t}_e,\widetilde{0}_X),\ldots,\texttt{chain\_mult}(\ell-1,\widetilde{t}_e,\widetilde{0}_X).$$

Since $\widetilde{t}_e$ is excellent, it suffices to compute the lifts $\texttt{chain\_mult}(2, \widetilde{t}_e, \widetilde{0}_X), \ldots, \texttt{chain\_mult}(m+1, \widetilde{t}_e, \widetilde{0}_X)$, the remaining ones being determined by them. Since `chain_mult` is defined recursively using `chain_add`, we can compute $\texttt{chain\_mult}(2, \widetilde{t}_e, \widetilde{0}_X), \ldots, \texttt{chain\_mult}(m+1, \widetilde{t}_e, \widetilde{0}_X)$ with m chain additions, i.e. to a total cost of

$$\ell/2 \cdot ((n^g + 2^g)\mathbf{M}(k_t) + (n^g + 2^g)\mathbf{S}(k_t) + n^g\mathbf{D}(k_t) + (4n)^g\mathbf{A}(k_t)).$$

Next, for each of the n^{gr} elements $\mathbf{k} \in K(\mathcal{M}^{\star r})_1$, computing the right-hand side of the formula requires $\ell^{r/2}$ times $(r-1)$ multiplications and one addition in the field k_t, leading to a total cost of

$$n^{gr}\ell^{r/2}((r-1)\mathbf{M}(k_t) + \mathbf{A}(k_t)). \tag{6.1}$$

For step 9., computing the symplectic basis $\{e_1, \ldots, e_g, \hat{e}_1, \ldots, \hat{e}_g\}$ of $X[2n]$ is rapid, using the action of the theta group $\mathcal{G}(\mathcal{L})$ on $\Gamma(X, \mathcal{L})$. For step 10., see the complexity analysis of Algorithm 3. For step 11., if $n = 2$ we have to do the conversion from level-2 to the squares of level-$(2, \ldots, 2)$, then the symplectic transformation formula and finally the reciprocal conversion from the squares of level-$(2, \ldots, 2)$ to level-2, and if $n = 4$ we have to do the change of basis from level-4 to level-$(2, \ldots, 2)$, then the symplectic transformation formula and finally the change of basis from level-$(2, \ldots, 2)$ to level-4. This, at first sight, seems to require 2^{2gr} multiplications of elements of k_t by nth roots of unity and 2^{5gr} additions in k_t if $n = 2$ and 2^{6gr} additions in k_t if $n = 4$. However, the theta null point $\widetilde{0}_{Y^r}$ for $(\Theta_{\mathcal{M}})^{\star r}$ contains no more information than the theta null point of 0_Y for $\Theta_{\mathcal{M}}$ ($\widetilde{0}_{Y^r}$ is just the theta null point of the r-fold product of $(Y, \mathcal{M}, \Theta_{\mathcal{M}})$). Hence, knowing n^g coordinates of $\widetilde{0}_{Y^r}$ as opposed to knowing all the n^{gr} coordinates is sufficient. And this performs step 12. at the same time. This observation brings down the number of operations of steps 11. and 12. to $n^g 2^{gr}$ multiplications of elements of k_t by nth roots of unity and $n^g 2^{2gr}$ additions in k_t. Overall, the cost of Algorithm 4 is dominated by (6.1) of steps 5. and 7.

Complexity analysis of Algorithm 5. The complexity is dominated by the chain multiplication, which requires

$$2\log(\ell) \cdot ((n^g + 2^g)\mathbf{M}(k_{x+t}) + n^g\mathbf{S}(k_{x+t}) + n^g\mathbf{D}(k_{x+t}) + (4n)^g\mathbf{A}(k_{x+t}))$$

operations, as well as taking an ℓth root of κ.

Complexity analysis of Algorithm 6. The chain multiplication in step 1. requires

$$2\log(N) \cdot ((n^g + 2^g)\mathbf{M}(k_x) + n^g\mathbf{S}(k_x) + n^g\mathbf{D}(k_x) + (4n)^g\mathbf{A}(k_x))$$

operations, followed by the computation of some Nth root. For step 2., see the complexity of Algorithm 2 or take the excellent lift $\widetilde{t}_e$ computed at step 1. of Algorithm 4. Step 3. is not costly when working on the Jacobian variety of a hyperelliptic curve, and requires one chain addition otherwise. For the computation of the suitable lift of $x + t$ in step 4., see the complexity of Algorithm 5 above. For step 5., if we know the scalar by which π acts on t (which is easy to determine when working on the Jacobian variety of a hyperelliptic curve), then this step is brought down to a computation in $\mathbb{Z}/\ell\mathbb{Z}$. For steps 7. and 9., as opposed to steps 5. and 7. of Algorithm 4, we do not precompute all the chain multiplications, since there would be a total of $N\ell$ precomputations to perform, out of which at most $n^{gr}\ell^{r/2}r$ would be needed (which is way less, supposing

that $N \gg n^{gr}\ell^{r/2-1}r$). Hence, for each $\mathbf{k} \in K(\mathcal{M}^{\star r})_1$ we compute $\ell^{r/2}$ times r chain multiplications of size at most $N\ell$, followed by $(r-1)$ multiplications and one addition, resulting in a total cost of

$$n^{gr}\ell^{r/2} \cdot [2r\log(N\ell)((n^g + 2^g)\mathbf{M}(k_{x+t}) + n^g\mathbf{S}(k_{x+t}) + n^g\mathbf{D}(k_{x+t}) + (4n)^g\mathbf{A}(k_{x+t})) \\ + (r-1)\mathbf{M}(k_{x+t}) + \mathbf{A}(k_{x+t})]. \tag{6.2}$$

By the same observation as in the analysis of Algorithm 4, we can perform steps 11. and 12. in $n^g 2^{gr}$ multiplications of elements of k_{x+t} by nth roots of unity and $n^g 2^{2gr}$ additions in k_{x+t}. Overall, the cost of Algorithm 6 is dominated by (6.2) of steps 7. and 9.

7 Implementation

We have implemented the algorithm from Section 4 in `Magma` and have computed the following example: let H be the hyperelliptic genus 2 curve over $\mathbb{F}_{23}$ given by the affine equation

$$H : y^2 = x^5 + x^4 + 3x^3 + 22x^2 + 19x,$$

and let $J = \mathrm{Jac}(H)$ be its Jacobian variety. Then J is ordinary and simple and the (irreducible) characteristic polynomial of the Frobenius endomorphism π_J is given by $\chi_{\pi_J}(z) = z^4+14z^2+529$. The endomorphism algebra $\mathrm{End}^0(J) = \mathrm{End}(J)\otimes_{\mathbb{Z}}\mathbb{Q}$ is isomorphic to the quartic CM-field $K = \mathbb{Q}(\pi) = \mathbb{Q}[z]/(\chi_{\pi_J})$, and the totally real subfield $K_0 \subset K$, corresponding to the Rosati-stable elements of $\mathrm{End}^0(J)$, is generated over $\mathbb{Q}$ by $\pi+\pi^\dagger$ (it is isomorphic to $\mathbb{Q}(\sqrt{2})$). The real endomorphism $\beta = -38(\pi_J + \pi_J^\dagger) + 215$ is totally positive and of $K_0/\mathbb{Q}$-norm 17 (i.e. a degree 17^2-endomorphism). Consider the 17-torsion point $t = (x^2 + u_1x + u_0, v_1x + v_0) \in J(\mathbb{F}_{23^{16}})$, where

$$u_1 = 10a^{15} + 9a^{14} + 17a^{13} + 5a^{12} + 14a^{11} + 19a^{10} + 14a^9 + 14a^8 + 5a^7 + 22a^6 + a^5 + 19a^4 + 13a^3 + 2a^2 + 15a + 7,$$
$$u_0 = 6a^{15} + 11a^{14} + 17a^{13} + 19a^{12} + 10a^{11} + a^{10} + 21a^9 + 15a^8 + 18a^7 + 21a^6 + 5a^5 + 18a^4 + 4a^3 + 6a^2 + 3a + 19,$$
$$v_1 = 19a^{15} + 11a^{14} + 18a^{13} + 3a^{12} + 20a^{11} + 11a^{10} + 8a^9 + a^8 + 19a^7 + 5a^6 + 14a^5 + 3a^4 + 4a^3 + 10a^2 + 22a + 22,$$
$$v_0 = a^{15} + 10a^{14} + 11a^{13} + 22a^{12} + 3a^{11} + 14a^{10} + 21a^9 + 5a^8 + 9a^7 + 17a^5 + 20a^4 + 6a^3 + 8a^2 + 13a + 5$$

and a satisfies $a^{16} + 19a^7 + 19a^6 + 16a^5 + 13a^4 + a^3 + 14a^2 + 17a + 5 = 0$. The subgroup $G = \langle t\rangle$ is Galois-stable, since $\pi_J(t) = [6]t$, and we have $\beta(t) = 0$. We have computed the quotient J/G, which is isomorphic as a principally polarized abelian surface to the Jacobian variety J' of the hyperelliptic curve H' over $\mathbb{F}_{23}$ with affine plane model

$$H' : y^2 = 5x^6 + 18x^5 + 18x^4 + 8x^3 + 20x.$$

Indeed, the characteristic polynomial of the Frobenius endomorphism $\pi_{J'}$ equals χ_{π_J}, but H and H' have Cardona-Quer-Nart-Pujola invariants (c.f. [CNP05] and [CQ05]) given by $[16, 12, 17]$ and $[18, 5, 0]$ respectively and hence, the Jacobians J and J' are non isomorphic (as principally polarized abelian surfaces). The computation took 363.2 seconds on a 2.3 GHz Intel Core i7 CPU with 8 GB memory.

Since $\chi_{\pi_J} = \chi_{\pi_{J'}}$ we know that J and J' are $\mathbb{F}_{23}$-isogenous. But can we be sure the isogeny is the one we computed? It has been verified by E. Milio that indeed, J and J' are isogenous by an isogeny of degree 17. He did so by first computing the Igusa invariants of the curves, from which he did then compute the Gundlach invariants (those are invariants of the $\bar{k}$-isomorphism class of the curve, with Jacobian variety having real multiplication by $\mathbb{Q}(\sqrt{2})$, see [MR17]). The 17-modular polynomial (as defined in [MR17]) vanishes when evaluated at the Gundlach invariants of H an H' and hence, J and J' are 17-isogenous.

You must be warned: on most examples I ran my code I was confronted to a serious problem and the output failed. I managed to locate and identify the problem, but have not yet managed to resolve it. There is, however, a small number of examples (including the above) where the code runs well. I am still trying hard to resolve this issue. For any additional information, please get in touch with me.

8 Isogeny graphs

Let k be a fixed finite field of size $q = p^r$. For abelian varieties X and Y over k, being k-isogenous is an equivalence relation. Tate's isogeny theorem [Tat66] gives a criterion for X and Y to be k-isogenous, and it can be verified by comparing the characteristic polynomials of the k-Frobenius endomorphisms π_X and π_Y on the $\mathbb{Q}_\ell$-vector spaces $V_\ell X = T_\ell X \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ and $V_\ell Y = T_\ell Y \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ respectively, where ℓ is any prime number different from p. Knowing that X and Y are k-isogenous, there are many situations where one would like to find an explicit isogeny between them (e.g. in the area of Isogeny Based Cryptography, see [DFJP14] and [DF17]). Various attempts have been made in dimension 1 [Gal99, DG16, BJS14], yet it remains a very difficult problem. In higher dimension this becomes even less clear, due to our lack of understanding of the "structure" of isogeny classes. To gain better understanding of this structure, isogeny classes are commonly modelled as graphs. Isogenous varieties share the same endomorphism algebra, whereas their endomorphism ring need not be the same (e.g. if the endomorphism algebra is isomorphic to the CM-field $\mathbb{Q}(\pi)$ for some Weil q-number π, then any order containing π and $\frac{q}{\pi}$ occurs as the endomorphism ring of an abelian variety in this isogeny class, see [Wat69, Thm. 7.4]). Hence, one would like to study those graphs with a special focus on the variation of the endomorphism ring under isogeny. A complete description of such graphs for genus 1 has been presented by D. Kohel in his thesis [Koh96], and more recent results on the structure of isogeny graphs in higher dimension have been presented by [IT14, BJW17, Mar18]. We will henceforth focus on the results of [BJW17]. While their results deliver a description of the structure of such graphs, our results from Sections 4 and 5 will come to hand for the explicit computation of the edges in certain isogeny graphs.

8.1 Preliminaries

Let X be an abelian variety of dimension g over k. Let $\bar{k}$ be a fixed algebraic closure of k. We suppose that X is ordinary, i.e. $X[p](\bar{k}) \cong (\mathbb{Z}/p\mathbb{Z})^g$, where $p = char(k)$. For simplicity we will denote the base change $X_{\bar{k}} = X \otimes_k \bar{k}$ by X again. We also suppose that X is absolutely simple, i.e. it does not admit a proper abelian subvariety over $\bar{k}$. According to [Wat69, Thm. 7.2], any (a priori $\bar{k}$-) endomorphism of X is defined over k, that is

$$\mathrm{End}_k(X) = \mathrm{End}_{\bar{k}}(X).$$

For an ordinary and absolutely simple abelian variety X defined over k, we can thus unambiguously write $\mathrm{End}(X)$. Note that the result of [Wat69] has to be understood with care, the way it is stated is misleading: he requires X to be simple, which by [Oor07] (the remark below Exercise 18.11) is not enough. One should require X to be absolutely simple.

Let $\pi \in \overline{\mathbb{Q}}$ be a Weil q-number whose conjugacy class represents the k-isogeny class of X (Honda-Serre-Tate theory). That is, the k-Frobenius endomorphism π_Y of any k-isogenous abelian variety Y/k has the same minimal polynomial over $\mathbb{Q}$ as π, and vice versa, if Y is an abelian variety over k whose k-Frobenius is conjugate to π, then Y is k-isogenous to X. The endomorphism algebra $\mathrm{End}(X) \otimes_{\mathbb{Z}} \mathbb{Q}$ is isomorphic to the CM-field $K = \mathbb{Q}(\pi)$, and we may choose the isomorphism such that $\pi_X \mapsto \pi$.

If Y is an abelian variety defined over $\bar{k}$ that is $\bar{k}$-isogenous to X, then

$$\mathrm{End}(X) \otimes_{\mathbb{Z}} \mathbb{Q} = \mathrm{End}_{\bar{k}}(X) \otimes_{\mathbb{Z}} \mathbb{Q} \cong \mathrm{End}_{\bar{k}}(Y) \otimes_{\mathbb{Z}} \mathbb{Q}$$

and hence, $\mathrm{End}_{\bar{k}}(Y) \otimes_{\mathbb{Z}} \mathbb{Q}$ is again isomorphic to the CM-field K. Clearly, Y is ordinary and $\bar{k}$-simple. If Y is defined over k, then Y is absolutely simple, and we have $\mathrm{End}_k(Y) = \mathrm{End}_{\bar{k}}(Y)$. The k-Frobenius π_X of X and the k-Frobenius π_Y of Y are conjugate (X and Y share the same endomorphism algebra), hence Y is actually k-isogenous to X. In this case we can say even more: if $f\colon X \to Y$ is a k-isogeny, and $g\colon X \to Y$ is any other isogeny, then $f^{-1} \circ g \in \mathrm{End}_{\bar{k}}(X) \otimes_{\mathbb{Z}} \mathbb{Q} = \mathrm{End}_k(X) \otimes_{\mathbb{Z}} \mathbb{Q}$ and hence, g is defined over k. To summarise:

Proposition 8.1. *Let X be an ordinary and absolutely simple abelian variety defined over k. If Y is also defined over k and $\bar{k}$-isogenous to X, then all the isogenies between X and Y are defined over k.*

The isomorphism $\mathrm{End}(X) \otimes_{\mathbb{Z}} \mathbb{Q} \xrightarrow{\sim} K = \mathbb{Q}(\pi)$ induces an embedding $\mathrm{End}_{\bar{k}}(Y) \hookrightarrow K$ of the endomorphism ring of any $\bar{k}$-isogenous abelian variety Y, and the embedding does not depend on the choice of an isogeny $X \to Y$. We can thus unambiguously denote by $\mathcal{O}(Y)$ the order of K corresponding to $\mathrm{End}_{\bar{k}}(Y)$ for any abelian variety Y in the $\bar{k}$-isogeny class of X. If Y is defined over k, then from what we have said above, Y is absolutely simple and $\mathcal{O}(Y)$ corresponds to $\mathrm{End}_k(Y)$. Under this identification we have $\pi_Y \mapsto \pi$. Let K_0 be the totally real subfield of K of degree g over $\mathbb{Q}$. Define the real order $\mathcal{O}_0(X) = \mathcal{O}(X) \cap K_0$. We say that X has *complex multiplication* (CM) by $\mathcal{O}(X)$ and *real multiplication* (RM) by $\mathcal{O}_0(X)$. Tensoring with $\mathbb{Z}_\ell$, for ℓ a prime number different from $char(k)$, we obtain the *local CM order* $\mathcal{O}(X) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ and the *local RM order* $\mathcal{O}_0(X) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ of X at ℓ. This allows us to transfer the study of endomorphisms of X to the study of endomorphisms of the ℓ-adic Tate module $T_\ell X$. If $X \to Y$ is an isogeny of ℓ-power degree, then for any prime number $\ell' \neq \ell$ one has

$$\mathcal{O}(X) \otimes_{\mathbb{Z}} \mathbb{Z}_{\ell'} = \mathcal{O}(Y) \otimes_{\mathbb{Z}} \mathbb{Z}_{\ell'} \tag{8.1}$$

(see [BJW17, Prop. 3.4]). Hence, it makes sense to consider graphs of isogenies of fixed prime-power degree, and study the local variation of the endomorphism ring under such isogenies.

Notation 8.2. Let ℓ be a fixed prime number different from the characteristic of k. Let $K_\ell = K \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ and $K_{0,\ell} = K_0 \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ be the local complex and real multiplication algebras. Denote by $\mathfrak{o}_K = \mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ and $\mathfrak{o}_{K_0} = \mathcal{O}_{K_0} \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ the maximal orders of K_ℓ and $K_{0,\ell}$ respectively. Also, denote by $\mathfrak{o}(X) = \mathcal{O}(X) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ and $\mathfrak{o}_0(X) = \mathcal{O}_0(X) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ the local CM and RM orders of X.

We can give a more explicit description of $K_\ell, K_{0,\ell}, \mathfrak{o}_K, \mathfrak{o}_{K_0}$, etc. For more details, we refer to [Neu99, Ch. II]. Let F be a number field, fix ℓ a prime number and suppose it factors in F as $\ell\mathcal{O}_F = \mathfrak{l}_1^{e_1} \cdots \mathfrak{l}_r^{e_r}$. Each prime ideal $\mathfrak{l}_i$ above ℓ induces a valuation $v_{\mathfrak{l}_i}\colon F \to \mathbb{Z} \cup \{\infty\}$ on F, where for any $x \in F^\times$, $v_{\mathfrak{l}_i}(x)$ is the exponent of $\mathfrak{l}_i$ in the factorization of the fractional ideal $x\mathcal{O}_F$, and $0 \mapsto \infty$. We can then define a non-archimedean absolute value

$$|\cdot|_{\mathfrak{l}_i}\colon F \to \mathbb{R}_{\geq 0},\ x \mapsto q_i^{-v_{\mathfrak{l}_i}(x)},$$

where $q_i = \ell^{f_i}$ with $f_i = [\mathcal{O}_F/\mathfrak{l}_i : \mathbb{Z}/\ell\mathbb{Z}]$ the inertia degree of $\mathfrak{l}_i$. Denote by $F_{\mathfrak{l}_i}$ the completion of the valued field $(F, |\cdot|_{\mathfrak{l}_i})$. It is a finite extension of $\mathbb{Q}_\ell$ and we have $[F_{\mathfrak{l}_i} : \mathbb{Q}_\ell] \leq [F : \mathbb{Q}]$. The absolute value $|\cdot|_{\mathfrak{l}_i}$ extends to an absolute value on $F_{\mathfrak{l}_i}$ (since $\mathbb{R}$ is complete), and we will again denote it by $|\cdot|_{\mathfrak{l}_i}$. There is a second, equivalent definition of $|\cdot|_{\mathfrak{l}_i}$ on $F_{\mathfrak{l}_i}$, involving the norm map $N_{F_{\mathfrak{l}_i}/\mathbb{Q}_\ell}\colon F_{\mathfrak{l}_i} \to \mathbb{Q}_\ell$ and the ℓ-adic

absolute value $|\cdot|_\ell$ on $\mathbb{Q}_\ell$. Namely, for all $x \in F$, one has

$$|x|_{\mathfrak{l}_i} = |N_{F_{\mathfrak{l}_i}/\mathbb{Q}_\ell}(x)|_\ell.$$

The ring of integers of $F_{\mathfrak{l}_i}$ is

$$\mathcal{O}_{F_{\mathfrak{l}_i}} = \{x \in F_{\mathfrak{l}_i} : |x|_{\mathfrak{l}_i} \leq 1\} = \{x \in F_{\mathfrak{l}_i} : N_{F_{\mathfrak{l}_i}/\mathbb{Q}_\ell}(x) \in \mathbb{Z}_\ell\}.$$

It is a DVR with unique maximal ideal

$$\mathfrak{L}_i = \{x \in F_{\mathfrak{l}_i} : |x|_{\mathfrak{l}_i} < 1\},$$

and a generator is any $\varpi \in \mathfrak{L}_i$ of maximal absolute value. In fact, we have

$$\mathfrak{L}_i = \mathfrak{l}_i \mathcal{O}_{F_{\mathfrak{l}_i}}$$

and hence, the ideals of $\mathcal{O}_{F_{\mathfrak{l}_i}}$ are of the form $\mathfrak{l}_i^m \mathcal{O}_{F_{\mathfrak{l}_i}}$, for some $m \geq 0$. It is a well-known result that

$$\mathcal{O}_{F_{\mathfrak{l}_i}}/\mathfrak{L}_i \cong \mathcal{O}_F/\mathfrak{l}_i \cong \mathbb{F}_{\ell^{f_i}}$$

(compatibility of local and global inertia degrees) and that

$$\ell \mathcal{O}_{F_{\mathfrak{l}_i}} = \mathfrak{L}_i^{e_i}$$

(compatibility of local and global ramification indices). One then easily deduces the local fundamental identity

$$[F_{\mathfrak{l}_i} : \mathbb{Q}_\ell] = e_i f_i.$$

Consider the localization $\mathcal{O}_{F,\mathfrak{l}_i} = \{\frac{a}{b} : a, b \in \mathcal{O}_F,\ b \notin \mathfrak{l}_i\} \subset F$ of $\mathcal{O}_F$ at $\mathfrak{l}_i$. We have

$$\mathcal{O}_{F,\mathfrak{l}_i} = \{x \in F : v_{\mathfrak{l}_i}(x) \geq 0\}$$

and one can show that $\mathcal{O}_{F_{\mathfrak{l}_i}}$ is the completion of $\mathcal{O}_{F,\mathfrak{l}_i}$ inside $F_{\mathfrak{l}_i}$ with respect to $|\cdot|_{\mathfrak{l}_i}$. More generally, $\mathfrak{L}_i^m$ is the completion of $\mathfrak{l}_i^m \mathcal{O}_{F,\mathfrak{l}_i}$ inside $F_{\mathfrak{l}_i}$ with respect to $|\cdot|_{\mathfrak{l}_i}$.

The inclusion $F \hookrightarrow F_{\mathfrak{l}_i}$ induces a homomorphism $F \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \to F_{\mathfrak{l}_i}$ via $a \otimes b \mapsto ab$ and hence, we have a canonical homomorphism $F \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \to F_{\mathfrak{l}_1} \oplus \cdots \oplus F_{\mathfrak{l}_r}$. The ever-present Chinese Remainder Theorem ensures that this is an isomorphism, i.e.

$$F_\ell := F \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \xrightarrow{\sim} F_{\mathfrak{l}_1} \oplus \cdots \oplus F_{\mathfrak{l}_r}.$$

Restricting to $\mathcal{O}_F \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$, we have

$$\mathfrak{o}_F := \mathcal{O}_F \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \xrightarrow{\sim} \mathcal{O}_{F_{\mathfrak{l}_1}} \oplus \cdots \oplus \mathcal{O}_{F_{\mathfrak{l}_r}}.$$

For all $j \neq i$, the ideal $\mathfrak{l}_i \mathcal{O}_{F_{\mathfrak{l}_j}}$ is the whole of $\mathcal{O}_{F_{\mathfrak{l}_j}}$, since it is not of the form $\mathfrak{L}_j^m = \mathfrak{l}_j^m \mathcal{O}_{F_{\mathfrak{l}_j}}$ for some $m \geq 0$. We deduce that

$$\mathfrak{o}_F/\mathfrak{l}_i \mathfrak{o}_F = \mathcal{O}_{F_{\mathfrak{l}_i}}/\mathfrak{L}_i \cong \mathcal{O}_F/\mathfrak{l}_i \cong \mathbb{F}_{\ell^{f_i}}. \tag{8.2}$$

Moreover, we have

$$\ell \mathfrak{o}_F = \mathfrak{L}_1^{e_1} \oplus \cdots \oplus \mathfrak{L}_r^{e_r} \tag{8.3}$$

and

$$\mathfrak{o}_F/\ell \mathfrak{o}_F = \mathcal{O}_{F_{\mathfrak{l}_1}}/\mathfrak{L}_1^{e_1} \oplus \cdots \oplus \mathcal{O}_{F_{\mathfrak{l}_r}}/\mathfrak{L}_r^{e_r}.$$

8.2 Applications

What we have encountered in Sections 4 and 5 are isogenies from principally polarized abelian varieties with cyclic kernels which are maximal isotropic inside $\ker \beta$ for the commutator pairing $e_{\mathcal{L}_0^\beta}$, where β is some totally positive real endomorphism. Call these isogenies *β-cyclic isogenies*. In view of Proposition 3.5, β-cyclic isogenies preserve the principal polarizability, in the sense that the target variety of a β-cyclic isogeny is again a principally polarizable abelian variety. The existence of such isogenies is strongly linked to the existence of totally positive real endomorphisms. Multiplication by a positive integer n is a totally positive real endomorphism, hence maximal isotropic subgroups of the n-torsion subgroup of X yield isogenies that preserve principal polarizability. To be more precise, if $\mathcal{L}_0$ is a principal polarization on X and ℓ is a prime number different from $char(k)$, then any isogeny with kernel a maximal isotropic subgroup of $X[\ell]$ for the Weil pairing $e_\ell^{\phi_{\mathcal{L}_0}}$ on $X[\ell]$ induced by $\mathcal{L}_0$ (which in this case coincides with the commutator pairing $e_{\mathcal{L}_0^\ell}$ on $K(\mathcal{L}_0^\ell)$) preserves the principal polarizability.

Definition 8.3. Let $(X, \mathcal{L}_0)$ be a principally polarized abelian variety over k, and let ℓ be a prime number different from $char(k)$. An isogeny $f\colon X \to Y$ is called an $(\ell, \dots, \ell)$-isogeny if $\ker f$ is a maximal isotropic subgroup of $X[\ell]$ for the Weil pairing $e_\ell^{\phi_{\mathcal{L}_0}}$ (or equivalently for the commutator pairing $e_{\mathcal{L}_0^\ell}$).

Richelot in [Ric37a] and [Ric37b] computed $(2,2)$-isogenies between abelian surfaces. More recently, [Smi09] has given a method to compute $(2,2,2)$-isogenies from Jacobian varieties of genus 3 hyperelliptic curves. More generally, $(\ell, \dots, \ell)$-isogenies can be computed in theta coordinates from any principally polarized abelian variety due to [Rob10, CR11, LR12], and from Jacobian varieties of hyperelliptic genus 2 and 3 curves C via the explicit evaluation of some G-invariant functions on $\mathrm{Jac}(C)$, where G is the kernel of the isogeny, see [CE15] and [Mil17].

There are many applications where one would like to find a path of computable isogenies to reach an abelian variety with maximal complex multiplication. And for this it is sufficient to be able to find a path of prime-power degree isogenies to an abelian variety with maximal local complex multiplication (since maximal locally at all prime numbers implies maximal globally, and there are only finitely many prime numbers for which the local CM order is non-maximal). We will see in Section 8.4.3 if and how a principally polarizable abelian surface with maximal local CM is reachable by a path of computable isogenies. Among the applications of reaching isogenous varieties with maximal complex multiplication we can cite:

- Random self-reducibility of the discrete logarithm problem in genus 2. Let X be an ordinary and absolutely simple principally polarizable abelian surface over k. Suppose that the endomorphism algebra of X is isomorphic to the CM-field K, and that the endomorphism ring of X is isomorphic to the maximal order $\mathcal{O}_K$. The ideal class group $\mathrm{Cl}(\mathcal{O}_K)$ acts freely and transitively on the set of isomorphism classes of abelian varieties isogenous to X and with same endomorphism ring, by the so-called CM-action, see [Wat69]. If one wants to restrict to isogenies preserving the principal polarizability, then one has to consider a certain subgroup of $\mathrm{Cl}(\mathcal{O}_K)$, namely the image $\mathcal{P}(\mathcal{O}_K)$ of the natural projection of the Shimura class group on the ideal class group $\mathrm{Cl}(\mathcal{O}_K)$. Recall the Shimura class group

  $$\mathfrak{S} = \{(\mathfrak{a}, \alpha) | \mathfrak{a} \text{ a fractional ideal of } \mathcal{O}_K,\ \alpha \in K_0 \text{ totally positive, and } \mathfrak{a}\bar{\mathfrak{a}} = \alpha\mathcal{O}_K\}/\sim,$$

with component wise multiplication, and the equivalence is modulo the subgroup given by the $(v\mathcal{O}_K, v\bar{v})$ with $v \in K^\times$ and $v\bar{v} \in K_0$ totally positive. The orbit $\mathcal{P}(X)$ of the CM-action of $\mathcal{P}(\mathcal{O}_K)$ on X is a set of of k-isomorphism classes of principally polarizable abelian surfaces isogenous to X and with same endomorphism ring. By [JW19, Thm. 1.1] one can construct expander graphs on $\mathcal{P}(X)$, where the edges are cyclic isogenies of bounded prime degree. Hence, they are β-cyclic isogenies, and computable by the results from Sections 4 and 5. Then by [JW19, Thm. 1.3] we obtain the random self-reducibility of the discrete logarithm in genus 2 under GRH. That is, if there is a polynomial time algorithm (in $\log \#k$) that can solve the DLP for a positive proportion of vertices in $\mathcal{P}(X)$, then there is a probabilistic algorithm of polynomial runtime that can solve the DLP on all vertices of $\mathcal{P}(X)$.

- Computation of an explicit isogeny between two given isogenous principally polarized abelian surfaces. The same expander properties from the previous point can be applied to find an explicit isogeny between two given isogenous principally polarized abelian surfaces. First compute a path to isogenous surfaces with maximal endomorphism ring and then do a random walk, using the CM-action of $\mathcal{P}(\mathcal{O}_K)$. Again, the isogenies to be computed for this random walk are β-cyclic isogenies. For more details we refer to [JW19, §5].

- The CM-method. This method aims to generate hyperelliptic curves of genus 2 over finite fields with good cryptographic security parameters. First compute the Igusa invariants of such a curve, and then use Mestre's algorithm [Mes91] to construct a model of the curve. There are three different approaches for computing the Igusa invariants of such a curve: 1) complex analytic techniques [vW99, Wen03, Str10]; 2) p-adic lifting techniques [CKL08, CL09, GHK$^+$06]; 3) techniques based on the Chinese Remainder Theorem (the *CRT* method) [EL10, FL08, BGL11]. The CRT method requires one to find an ordinary abelian surface whose endomorphism ring is the maximal order. Hence, starting from a random abelian variety, one would like to compute a path of isogenies to reach one with maximal endomorphism ring.

- Computation of endomorphism rings of abelian surfaces over finite fields, see [Bis15] and [Spr19].

8.3 $\mathfrak{l}$-isogeny graphs

Let us now present some results of [BJW17]. Fix a $\bar{k}$-isogeny class of g-dimensional ordinary and simple abelian varieties over $\bar{k}$ that admits at least one abelian variety X_0 defined over k (it is then absolutely simple). Fix an isomorphism $\mathrm{End}(X_0) \otimes_{\mathbb{Z}} \mathbb{Q} \xrightarrow{\sim} K$ to the CM-field $K = \mathbb{Q}(\pi)$, where π is a Weil q-number that represents the k-isogeny class of X_0, in such a way that $\pi_{X_0} \mapsto \pi$. Let K_0 be the totally real subfield of K of degree g over $\mathbb{Q}$. Recall the *conductor* $\mathfrak{f}$ of an order $\mathcal{O}$ in a number field F is defined as $\mathfrak{f} = \{x \in F : x\mathcal{O}_F \subset \mathcal{O}\}$.

Definition 8.4. Let X be an abelian variety in this isogeny class. Let ℓ be a prime number different from $char(k)$ and let $\mathfrak{l}$ be a prime ideal of $\mathcal{O}_{K_0}$ above ℓ. Suppose $\mathfrak{l}$ is coprime to the conductor of $\mathcal{O}_0(X)$. An $\mathfrak{l}$-isogeny from X is an isogeny whose kernel is a proper $\mathcal{O}_0(X)$-stable subgroup of $X[\mathfrak{l} \cap \mathcal{O}(X)]$.

Remark 8.5. An $\mathfrak{l}$-isogeny is a priori defined over $\bar{k}$, and is of degree $N(\mathfrak{l})$.

Let $\mathfrak{l}$ be a prime ideal of $\mathcal{O}_{K_0}$ above the prime number $\ell \neq char(k)$. According to [BJW17, Prop. 3.1 (ii)], if $X \to Y$ is an $\mathfrak{l}$-isogeny, then $\mathfrak{o}_0(X) \subset \mathfrak{o}_0(Y)$. In particular, having maximal local real multiplication is preserved under $\mathfrak{l}$-isogenies.

Definition 8.6. An $\mathfrak{l}$-*isogeny graph* is a graph $\mathscr{W}_\mathfrak{l}$ whose vertices are isomorphism classes of abelian varieties in the fixed $\bar{k}$-isogeny class having maximal local real multiplication (i.e. the local endomorphism rings contain $\mathfrak{o}_{K_0}$). There is a an edge of multiplicity m from a vertex with representative X to a vertex with representative Y if there are m distinct subgroups $G \subset X$ that are kernels of $\mathfrak{l}$-isogenies such that $X/G \cong Y$.

Remark 8.7. If there is an $\mathfrak{l}$-isogeny $X \to Y$, then the contragredient isogeny $Y \to X$ need not be an $\mathfrak{l}$-isogeny. That is, an $\mathfrak{l}$-isogeny graph is a directed graph in general. However, if $\mathfrak{l}$ is principal (generated by a real but not necessarily totally positive endomorphism) then the contragredient isogeny of an $\mathfrak{l}$-isogeny is again an $\mathfrak{l}$-isogeny.

A full description of the connected components of the graph $\mathscr{W}_\mathfrak{l}$, with a precise criterion for these components to be volcanoes, is given by [BJW17, Thm. 4.3]. As we know from [BJW17, Thm. 2.1], every order of K_ℓ that contains $\mathfrak{o}_{K_0}$ is of the form

$$\mathfrak{o}_\mathfrak{f} := \mathfrak{o}_{K_0} + \mathfrak{f}\mathfrak{o}_K,$$

for some unique $\mathfrak{o}_{K_0}$-ideal $\mathfrak{f}$. Moreover, the conductor of $\mathfrak{o}_\mathfrak{f}$ is $\mathfrak{f}\mathfrak{o}_K$.

Let $\mathfrak{l}$ be a prime of K_0 above ℓ. The local CM order of a vertex X in the $\mathfrak{l}$-isogeny graph $\mathscr{W}_\mathfrak{l}$ can thus be identified with an ideal of $\mathfrak{o}_{K_0}$ and hence, one can define the *level* $v_\mathfrak{l}(X)$ of X as the valuation at $\mathfrak{l}$ of the unique $\mathfrak{o}_{K_0}$-ideal $\mathfrak{f}$ such that $\mathfrak{o}(X) = \mathfrak{o}_\mathfrak{f}$. Note that if $\mathfrak{c}$ is the conductor of $\mathfrak{o}(X)$, then $\mathfrak{f} = \mathfrak{c} \cap \mathfrak{o}_{K_0}$.

Definition 8.8. An edge $X \to Y$ in the $\mathfrak{l}$-isogeny graph $\mathscr{W}_\mathfrak{l}$ is called $\mathfrak{l}$-ascending if $v_\mathfrak{l}(Y) = v_\mathfrak{l}(X) - 1$. It is called $\mathfrak{l}$-descending if $v_\mathfrak{l}(Y) = v_\mathfrak{l}(X) + 1$ and $\mathfrak{l}$-horizontal otherwise.

Let us recall [BJW17, Prop. 4.10]:

Proposition 8.9. *Suppose X has local CM order $\mathfrak{o}_\mathfrak{f}$, for some $\mathfrak{o}_{K_0}$-ideal $\mathfrak{f}$. There are $N(\mathfrak{l}) + 1$ kernels of $\mathfrak{l}$-isogenies from X. The target varieties of $\mathfrak{l}$-descending $\mathfrak{l}$-isogenies have local CM order $\mathfrak{o}_{\mathfrak{l}\mathfrak{f}}$, and the $\mathfrak{l}$-descending kernels are permuted simply transitively by the action of $(\mathfrak{o}_\mathfrak{f}/\mathfrak{o}_{\mathfrak{l}\mathfrak{f}})^\times$. The other $\mathfrak{l}$-isogenies are $\mathfrak{l}$-ascending if $v_\mathfrak{l}(X) > 0$, in which case the target varieties have local CM order $\mathfrak{o}_{\mathfrak{l}^{-1}\mathfrak{f}}$, and $\mathfrak{l}$-horizontal otherwise, in which case the target varieties have local CM order $\mathfrak{o}_\mathfrak{f}$. More precisely, if $v_\mathfrak{l}(X) > 0$ there are $N(\mathfrak{l})$ $\mathfrak{l}$-descending $\mathfrak{l}$-kernels from X and a unique $\mathfrak{l}$-ascending $\mathfrak{l}$-kernel. If $v_\mathfrak{l}(X) = 0$, then:*

- *i) If $\mathfrak{l}$ is inert in K, all $N(\mathfrak{l}) + 1$ $\mathfrak{l}$-kernels are $\mathfrak{l}$-descending;*
- *ii) If $\mathfrak{l}$ splits in K into two prime ideals $\mathscr{L}_1$ and $\mathscr{L}_2$, there are two $\mathfrak{l}$-horizontal $\mathfrak{l}$-kernels, namely $X[\mathscr{L}_1]$ and $X[\mathscr{L}_2]$, and $N(\mathfrak{l}) - 1$ $\mathfrak{l}$-descending ones;*
- *iii) If $\mathfrak{l}$ ramifies in K as $\mathscr{L}^2$, there is one $\mathfrak{l}$-horizontal $\mathfrak{l}$-kernel, namely $X[\mathscr{L}]$, and $N(\mathfrak{l})$ $\mathfrak{l}$-descending ones.*

In particular, Proposition 8.9 tells us that an $\mathfrak{l}$-isogeny can not modify the valuation of the local CM order of X (or to be more precise, of the corresponding $\mathfrak{o}_{K_0}$-ideal) at any prime $\mathfrak{l}'$ of K_0 above ℓ different from $\mathfrak{l}$. That is, $v_{\mathfrak{l}'}(X) = v_{\mathfrak{l}'}(Y)$ for any two connected vertices X and Y in the graph $\mathscr{W}_\mathfrak{l}$. This, together with (8.1), we see that all vertices in

a connected component of $\mathscr{W}_\mathfrak{l}$ of the same level share a common global endomorphism ring. We can thus divide a connected component $\mathscr{V}$ of $\mathscr{W}_\mathfrak{l}$ into subgraphs $\mathscr{V}_i$ of vertices with same level $i \geq 0$, or equivalently with same global endomorphism ring. Also, if X is a vertex in $\mathscr{V}_i$, for some $i > 0$, then there is always a path of $\mathfrak{l}$-ascending $\mathfrak{l}$-isogenies to a vertex Y in $\mathscr{V}_0$. That is, one can reach an abelian variety Y whose local CM order is not divisible by $\mathfrak{l}$ (this is again an abuse of notation; we actually mean the $\mathfrak{o}_{K_0}$-ideal corresponding to $\mathfrak{o}(X)$ is not divisible by $\mathfrak{l}$). Repeating this for all primes $\mathfrak{l}'$ of K_0 above ℓ, we can reach an abelian variety with local CM order $\mathfrak{o}_K$.

Definition 8.10. If X is a vertex in $\mathscr{V}_i$, for some $i > 0$, let G be the unique $\mathfrak{l}$-ascending $\mathfrak{l}$-kernel from Proposition 8.9. We call $\mathrm{pr}_\mathfrak{l}(X) = X/G \in \mathscr{V}_{i-1}$ the $\mathfrak{l}$-predecessor of X, and denote by $\mathrm{up}_X^\mathfrak{l} \colon X \to \mathrm{pr}_\mathfrak{l}(X)$ the canonical $\mathfrak{l}$-ascending projection.

Be aware that Proposition 8.9 counts the number of $\mathfrak{l}$-kernels from a given vertex in $\mathscr{W}_\mathfrak{l}$, and not the number of edges in this graph. Two distinct kernels might lead to isomorphic quotients, which can happen for $\mathfrak{l}$-horizontal and for $\mathfrak{l}$-descending isogenies. For the exact number of edges in any connected component of $\mathscr{W}_\mathfrak{l}$, we refer to [BJW17, Thm. 4.3] (this number depends only on the level and not on the vertex itself). We would like to point out that if the units of the global CM order of any vertex in $\mathscr{V}_0$ are real (i.e. are in $\mathcal{O}_{K_0}$), then the number of descending edges is exactly the number of $\mathfrak{l}$-descending kernels from Proposition 8.9. For example, in dimension 2, the field K is a primitive quartic CM-field, and provided $K \neq \mathbb{Q}(\zeta_5)$, we have $\mathcal{O}_K^\times = \mathcal{O}_{K_0}^\times$. It follows that the number of descending edges from each vertex in $\mathscr{W}_\mathfrak{l}$ is given by the number of $\mathfrak{l}$-descending kernels from Proposition 8.9.

This gives us a way to navigate in any fixed connected component $\mathscr{V}$ of the graph $\mathscr{W}_\mathfrak{l}$. In particular, if a vertex X is in $\mathscr{V}_i$, for $i > 0$, then $\mathrm{up}_X^\mathfrak{l}$ is the unique edge connecting to $\mathscr{V}_{i-1}$ and all the other edges connect to $\mathscr{V}_{i+1}$ (no horizontal ones). If X is in $\mathscr{V}_0$, then depending on the splitting of $\mathfrak{l}$ in K there are 0, 1 or 2 horizontal edges from X, the remaining ones connecting to $\mathscr{V}_1$. The horizontal structure of $\mathscr{V}_0$ can be described as the Cayley graph of the subgroup of $\mathrm{Pic}(\mathcal{O}_{\mathscr{V}_0})$ generated by the prime ideals of $\mathcal{O}_{\mathscr{V}_0}$ above $\mathfrak{l}$ (only if $\mathfrak{l}$ not inert), see [BJW17, Thm. 4.3]. Here, the order $\mathcal{O}_{\mathscr{V}_0}$ of K denotes the common global CM order of the vertices in $\mathscr{V}_0$. To be more precise, if $\mathscr{L}$ is a prime ideal of $\mathcal{O}_{\mathscr{V}_0}$ above $\mathfrak{l}$, then the edge $\mathscr{L}$ in the Cayley graph corresponds to the edge $X \to X/X[\mathscr{L}]$ in the $\mathfrak{l}$-isogeny subgraph $\mathscr{V}_0$. It becomes clear that one has to exclude the inert case, since $X \to X/X[\mathfrak{l}]$ is not an $\mathfrak{l}$-isogeny.

Rationality. So far, all the vertices and all the edges we have considered were over $\bar{k}$. Suppose X is defined over k and is in $\mathscr{V}_i$, for some $i \geq 0$. Under the identification of $\mathrm{End}(X)$ with the order $\mathcal{O}(X) \subset K$, the k-Frobenius π_X is sent to π. All vertices in $\mathscr{V}_i$ share $\mathcal{O}(X)$ as a common endomorphism ring. Let Y be another vertex in $\mathscr{V}_i$. Then Y is of the form X/G for some finite subgroup $G \subset X[\ell^\infty]$, and $\mathcal{O}(Y) = \mathcal{O}(X)$. Hence, we have $\pi \in \mathfrak{o}(Y) = \mathfrak{o}(X/G)$, and by [BJW17, Prop. 3.1], the kernel G is defined over k. It follows that Y is defined over k. The same argument works for Y in $\mathscr{V}_j$, for $j \leq i$, observing that $\mathfrak{o}(X) \subset \mathfrak{o}(Y)$ (follows from Proposition 8.9). Hence, all the vertices and all the edges from $\mathscr{V}_i$ upwards are defined over k.

Proposition 8.11. *Starting from an ordinary and absolutely simple abelian variety X defined over k, the path to level 0 consists of k-rational $\mathfrak{l}$-isogenies only.*

8.4 Dimension 2

From an arbitrary principally polarizable abelian surface it is almost always possible to find a path of computable isogenies to reach a principally polarizable surface with maximal local complex multiplication. We will explain this in the forthcoming sections.

8.4.1 (ℓ,ℓ)-isogeny graphs with non-maximal local real multiplication

Let X_0 be an ordinary and absolutely simple abelian surface over k, and fix ℓ a prime number different from $char(k)$. The endomorphism algebra of X_0 is isomorphic to a quartic CM-field K. We are interested in the $\bar{k}$-isogeny class of X_0. Let X be a principally polarizable abelian surface in this class. In this section we suppose that the real endomorphism ring $\mathcal{O}_0(X)$ of X is not maximal locally at ℓ. Since K_0 is a real quadratic number field, its orders are of the form $\mathbb{Z} + f\mathcal{O}_{K_0}$, for some integer f, and the conductor of such an order is $f\mathcal{O}_{K_0}$. The corresponding local order is the order $\mathfrak{o}_n := \mathbb{Z}_\ell + \ell^n \mathfrak{o}_{K_0}$ of $K_{0,\ell}$, where $n = v_\ell(f)$ is the valuation of f at ℓ.

Fix $\mathcal{L}_0$ a principal polarization on X. Any maximal isotropic subgroup $G \subset X[\ell]$ for the commutator pairing $e_{\mathcal{L}_0^\ell}$ (or equivalently for the Weil pairing $e_\ell^{\phi_{\mathcal{L}_0}}$) induces an (ℓ,ℓ)-isogeny $f\colon X \to Y = X/G$ and a unique principal polarization $\mathcal{M}_0$ on Y that satisfies $\phi_{f^*\mathcal{M}_0} = \phi_{\mathcal{L}_0} \circ [\ell]$. Conversely, any (ℓ,ℓ) isogeny for $e_{\mathcal{L}_0^\ell}$ is, up to isomorphism of the target, of this form. It is worth noticing that the kernels $G \subset X[\ell]$ of (ℓ,ℓ)-isogenies from X depend on the choice of the principal polarization. A subgroup G might be isotropic for $e_{\mathcal{L}_0^\ell}$ but need not be so if one changes polarization.

Suppose that $\mathfrak{o}_0(X) = \mathfrak{o}_n$, for some $n > 0$. An (ℓ,ℓ)-isogeny $X \to Y$ is called *RM-ascending* if $\mathfrak{o}_0(X) \subsetneq \mathfrak{o}_0(Y)$. It is called *RM-descending* if $\mathfrak{o}_0(Y) \subsetneq \mathfrak{o}_0(X)$ and it is called *RM-horizontal* if $\mathfrak{o}_0(X) = \mathfrak{o}_0(Y)$. A priori, (ℓ,ℓ)-isogenies are defined over $\bar{k}$, and the number of (ℓ,ℓ)-isogenies from X with respect to $\mathcal{L}_0$ is $\ell^3 + \ell^2 + \ell + 1$. We now state [BJW17, Thm. 6.3]:

Theorem 8.12. *Suppose $\mathfrak{o}_0(X) = \mathfrak{o}_n$ with $n > 0$. The kernels of (ℓ,ℓ)-isogenies from X (for the Weil pairing $e_\ell^{\phi_{\mathcal{L}_0}}$) are:*

i) A unique RM-ascending one, whose target variety has local RM order $\mathfrak{o}_{n-1}$,

ii) $\ell^2 + \ell$ RM-horizontal ones,

iii) ℓ^3 RM-descending ones, whose target varieties have local RM order $\mathfrak{o}_{n+1}$.

In particular, we see that an (ℓ,ℓ)-isogeny can change the local RM level by at most 1. The kernel $G \subset X[\ell]$ of the unique RM-ascending (ℓ,ℓ)-isogeny from Theorem 8.12 does not depend on the choice of a principal polarization on X (it is given in a "canonical" form, see [BJW17, Prop. 7.6]). Moreover, G is defined over the same field as X.

Definition 8.13. The RM-predecessor of X is the abelian surface $\mathrm{pr}_{\mathrm{RM}}(X) = X/G$, where G is the unique RM-ascending kernel from X. We denote by $\mathrm{up}_X^{\mathrm{RM}}\colon X \to \mathrm{pr}_{\mathrm{RM}}(X)$ the canonical projection. If $\mathcal{L}_0$ is a principal polarization on X, denote by $\mathrm{pr}_{\mathrm{RM}}(\mathcal{L}_0)$ the unique principal polarization on $\mathrm{pr}_{\mathrm{RM}}(X)$ induced by $\mathcal{L}_0$ via $\mathrm{up}_X^{\mathrm{RM}}$.

With this being said:

Proposition 8.14. *Starting from a principally polarizable ordinary and simple (absolutely simple if defined over k) abelian surface X, for all prime $\ell \neq char(k)$ where the*

local RM order of X is not maximal, there is a path of (ℓ,ℓ)-isogenies to a principally polarizable abelian surface with maximal real multiplication locally at ℓ. This path does not depend on the choice of a principal polarization on X. Moreover, if X is defined over k, then all the isogenies in the path are defined over k.

8.4.2 (ℓ,ℓ)-isogeny graphs with maximal local real multiplication

Let us again fix the $\bar{k}$-isogeny class of X_0, where X_0 is as in Section 8.4.1. Let X be a principally polarizable abelian surface in this isogeny class, and fix ℓ a prime number different from $char(k)$. By Proposition 8.14, we can suppose without loss of generality that the RM order of X is maximal locally at ℓ. We would like to apply the results from Section 8.3 to study (ℓ,ℓ)-isogenies from X that preserve the maximal local real multiplication (RM-horizontal). Fix $\mathcal{L}_0$ a principal polarization on X. There are a total of $\ell^3+\ell^2+\ell+1$ kernels of (ℓ,ℓ)-isogenies from X with respect to $\mathcal{L}_0$. Fix $\mathfrak{l}$ a prime ideal of $\mathcal{O}_{K_0}$ above ℓ.

The inert case. Suppose first that ℓ is inert in K_0. We can use Proposition 8.9 to describe $\ell\mathcal{O}_{K_0}$-isogenies. There are ℓ^2+1 such $\ell\mathcal{O}_{K_0}$-isogenies. If, moreover, the kernel of an $\ell\mathcal{O}_{K_0}$-isogeny is isotropic for the Weil pairing $e_\ell^{\phi_{\mathcal{L}_0}}$, then it is an (ℓ,ℓ)-isogeny. The following is [BJW17, Thm. 6.4 (i)]:

Theorem 8.15. *Let $\mathcal{L}_0$ be a principal polarization on X, and suppose X has maximal real multiplication locally at ℓ. If ℓ is inert in K_0, then the ℓ^2+1 kernels of $\ell\mathcal{O}_{K_0}$-isogenies are (ℓ,ℓ)-isogenies for the pairing $e_\ell^{\phi_{\mathcal{L}_0}}$. Conversely, among the $\ell^3+\ell^2+\ell+1$ (ℓ,ℓ)-isogenies from X for $e_\ell^{\phi_{\mathcal{L}_0}}$, the only RM-horizontal ones are the ℓ^2+1 $\ell\mathcal{O}_{K_0}$-isogenies, the remaining $\ell^3+\ell$ (ℓ,ℓ)-isogenies are RM-descending with local RM order of the target surface given by $\mathbb{Z}_\ell+\ell\mathfrak{o}_{K_0}$.*

Theorem 8.15 tells us that being the kernel of an (ℓ,ℓ)-isogeny that preserves the local maximal real multiplication is independent of the choice of a polarization, and that Proposition 8.9 applies. In particular, the $\ell\mathcal{O}_{K_0}$-predecessor $\mathrm{pr}_{\ell\mathcal{O}_{K_0}}(X)$ of X is independent of the choice of a principal polarization on X and $\mathrm{up}_X^{\ell\mathcal{O}_{K_0}}: X \to \mathrm{pr}_{\ell\mathcal{O}_{K_0}}(X)$ is an (ℓ,ℓ)-isogeny.

Proposition 8.16. *Starting from a principally polarizable ordinary and simple (absolutely simple if defined over k) abelian surface X, and a prime number $\ell \neq char(k)$ that is inert in K_0 and such that the RM order of X is maximal locally at ℓ, there is a path of (ℓ,ℓ)-isogenies to a principally polarizable abelian surface with maximal complex multiplication locally at ℓ. This path does not depend on the choice of a principal polarization on X. Moreover, if X is defined over k, then all the isogenies in the path are defined over k.*

The split case. Suppose now ℓ splits in K_0 as $\ell\mathcal{O}_{K_0}=\mathfrak{l}_1\mathfrak{l}_2$. The $\mathfrak{l}_i$-isogenies, for $i=1,2$, can be described via Proposition 8.9. If we compose an $\mathfrak{l}_1$-isogeny with an $\mathfrak{l}_2$-isogeny, or vice versa, we obtain an isogeny of degree ℓ^2 with kernel a subgroup of $X[\mathfrak{l}_1\mathfrak{l}_2\cap\mathcal{O}(X)]=X[\ell]$, and there are a total of $\ell^2+2\ell+1$ such isogenies. If the kernel of such a composition is isotropic for the Weil pairing $e_\ell^{\phi_{\mathcal{L}_0}}$, then it is an (ℓ,ℓ)-isogeny. The following is [BJW17, Thm. 6.4 (ii)]:

Theorem 8.17. *Let $\mathcal{L}_0$ be a principal polarization on X, and suppose X has maximal real multiplication locally at ℓ. Suppose ℓ splits in K_0 as $\ell\mathcal{O}_{K_0} = \mathfrak{l}_1\mathfrak{l}_2$. The $\ell^2 + 2\ell + 1$ compositions of an $\mathfrak{l}_1$-isogeny with an $\mathfrak{l}_2$-isogeny, or vice versa, are (ℓ, ℓ)-isogenies for the pairing $e_\ell^{\phi_{\mathcal{L}_0}}$. Conversely, among the $\ell^3 + \ell^2 + \ell + 1$ (ℓ, ℓ)-isogenies from X for $e_\ell^{\phi_{\mathcal{L}_0}}$, the only RM-horizontal ones are the compositions of an $\mathfrak{l}_1$-isogeny with an $\mathfrak{l}_2$-isogeny, or vice versa, the remaining $\ell^3 - \ell$ (ℓ, ℓ)-isogenies are RM-descending with local RM order of the target surface given by $\mathbb{Z}_\ell + \ell\mathfrak{o}_{K_0}$.*

Theorem 8.17 tells us that being the kernel of an (ℓ, ℓ)-isogeny that preserves the local maximal real multiplication is independent of the choice of a polarization. However, it is not immediately clear how to use the structural results from Proposition 8.9 for $\mathfrak{l}_1$-isogenies and $\mathfrak{l}_2$-isogenies to navigate in the isogeny class of X with (ℓ, ℓ)-isogenies only, and hopefully reach a variety with maximal local CM order.

The ramified case. If ℓ ramifies in K_0 as $\ell\mathcal{O}_{K_0} = \mathfrak{l}^2$, then a composition of two $\mathfrak{l}$-isogenies is an isogeny of degree ℓ^2 with kernel a subgroup of $X[\mathfrak{l}^2 \cap \mathcal{O}(X)] = X[\ell]$. There are a total of $\ell^2 + \ell + 1$ such isogenies, some kernels of $\mathfrak{l}$-isogenies being counted multiple times. If the kernel of such a composition is isotropic for the Weil pairing $e_\ell^{\phi_{\mathcal{L}_0}}$, then it is an (ℓ, ℓ)-isogeny. The following is [BJW17, Thm. 6.4 (iii)]:

Theorem 8.18. *Let $\mathcal{L}_0$ be a principal polarization on X, and suppose X has maximal real multiplication locally at ℓ. Suppose ℓ ramifies in K_0 as $\ell\mathcal{O}_{K_0} = \mathfrak{l}^2$. The $\ell^2 + \ell + 1$ compositions of two $\mathfrak{l}$-isogenies are (ℓ, ℓ)-isogenies for the pairing $e_\ell^{\phi_{\mathcal{L}_0}}$. Conversely, among the $\ell^3 + \ell^2 + \ell + 1$ (ℓ, ℓ)-isogenies from X for $e_\ell^{\phi_{\mathcal{L}_0}}$, the only RM-horizontal ones are the compositions of two $\mathfrak{l}$-isogenies, the remaining ℓ^3 (ℓ, ℓ)-isogenies are RM-descending with local RM order of the target surface given by $\mathbb{Z}_\ell + \ell\mathfrak{o}_{K_0}$.*

Theorem 8.18 tells us that being the kernel of an (ℓ, ℓ)-isogeny that preserves the local maximal real multiplication is independent of the choice of a polarization. However, it is not immediately clear how to use the structural results from Proposition 8.9 for $\mathfrak{l}$-isogenies to navigate in the isogeny class of X with (ℓ, ℓ)-isogenies only, and hopefully reach a variety with maximal local CM order.

8.4.3 Going up

Let X be a principally polarizable abelian surface in the previously fixed isogeny class (ordinary and simple). Let ℓ be a prime number different from $char(k)$, and let $\mathcal{L}_0$ be a principal polarization on X. We are interested in finding a path of (ℓ, ℓ)-isogenies (the first one being with respect to the Weil pairing $e_\ell^{\phi_{\mathcal{L}_0}}$) and β-cyclic isogenies to reach the maximal local complex multiplication order whenever possible.

The inert case. If ℓ is inert in K_0, then Propositions 8.14 and 8.16 tell us that there is a path of (ℓ, ℓ)-isogenies to a principally polarizable abelian surface with maximal CM order locally at ℓ. The path does not depend on the choice of a principal polarization on X. Moreover, if X is defined over k, then all the isogenies in the path are defined over k. The split and ramified cases are a bit more subtle.

The split case. Using Proposition 8.14, we can suppose that X has maximal real multiplication locally at ℓ. Suppose ℓ splits in K_0 as $\ell\mathcal{O}_{K_0} = \mathfrak{l}_1\mathfrak{l}_2$. The local CM order

of X is of the form $\mathfrak{o}_{\mathfrak{f}} = \mathfrak{o}_{K_0} + \mathfrak{f}\mathfrak{o}_K$, for some $\mathfrak{o}_{K_0}$-ideal $\mathfrak{f} = \mathfrak{l}_1^n\mathfrak{l}_2^m$, where n, m are nonnegative integers. The target surface $\mathrm{pr}_{\mathfrak{l}_1}(X)$ of the unique $\mathfrak{l}_1$-ascending $\mathfrak{l}_1$-isogeny $\mathrm{up}_X^{\mathfrak{l}_1}$ has local CM order given by $\mathfrak{o}_{\mathfrak{l}_1^{n-1}\mathfrak{l}_2^m}$, and the target surface $\mathrm{pr}_{\mathfrak{l}_2}(\mathrm{pr}_{\mathfrak{l}_1}(X))$ of the unique $\mathfrak{l}_2$-ascending $\mathfrak{l}_2$-isogeny $\mathrm{up}^{\mathfrak{l}_2}_{\mathrm{pr}_{\mathfrak{l}_1}(X)}$ from $\mathrm{pr}_{\mathfrak{l}_1}(X)$ has local CM order given by $\mathfrak{o}_{\mathfrak{l}_1^{n-1}\mathfrak{l}_2^{m-1}}$. But this composition is an (ℓ,ℓ)-isogeny. Assuming without loss of generality that $n \leq m$, continuing this way we have a path of (ℓ,ℓ)-isogenies to a principally polarizable abelian surface with local CM order $\mathfrak{o}_{\mathfrak{l}_2^{m-n}}$ (hence at $\mathfrak{l}_1$-level 0). Set $m' = m-n$. If $\mathfrak{l}_1$ is not inert in K, then there exist $\mathfrak{l}_1$-horizontal $\mathfrak{l}_1$-isogenies. Composing an $\mathfrak{l}_1$-horizontal $\mathfrak{l}_1$-isogeny with the $\mathfrak{l}_2$-ascending $\mathfrak{l}_2$-isogeny $\mathrm{up}^{\mathfrak{l}_2}$, we reach a principally polarizable abelian surface with maximal CM order locally at ℓ with m' additional (ℓ,ℓ)-isogenies. However, if $\mathfrak{l}_1$ is inert in K, then there are no $\mathfrak{l}_1$-horizontal $\mathfrak{l}_1$-isogenies. We can still compose an $\mathfrak{l}_1$-descending $\mathfrak{l}_1$-isogeny with $\mathrm{up}^{\mathfrak{l}_2}$, followed by the composition of $\mathrm{up}^{\mathfrak{l}_1}$ with $\mathrm{up}^{\mathfrak{l}_2}$, and get a path of two (ℓ,ℓ)-isogenies to a principally polarizable abelian surface with local CM order $\mathfrak{o}_{\mathfrak{l}_2^{m'-2}}$. Finally, we observe that if m' is even, or equivalently if $n+m$ is even, then we can reach a principally polarizable abelian surface with maximal CM order locally at ℓ with a path of (ℓ,ℓ)-isogenies. As a conclusion, the only case when we cannot reach a principally polarizable abelian surface with maximal CM order locally at ℓ with a path of (ℓ,ℓ)-isogenies in the split case is when $m+n$ is odd and both $\mathfrak{l}_1$ and $\mathfrak{l}_2$ are inert in K. In this case the largest reachable local CM orders are $\mathfrak{o}_{K_0} + \mathfrak{l}_1\mathfrak{o}_K$ and $\mathfrak{o}_{K_0} + \mathfrak{l}_2\mathfrak{o}_K$. The above described path of (ℓ,ℓ)-isogenies does not depend on the choice of a principal polarization on X. By Proposition 8.11, if X is defined over k, then all $\mathfrak{l}_i$-isogenies are defined over k, for $i = 1, 2$ and hence, all the (ℓ,ℓ)-isogenies are defined over k, except if $\mathfrak{o}(X) = \mathfrak{o}_{\mathfrak{l}_2^m}$, $\mathfrak{l}_1$ is inert in K and none of the $\mathfrak{l}_1$-descending $\mathfrak{l}_1$-isogenies from X is defined over k, or if $\mathfrak{o}(X) = \mathfrak{o}_{\mathfrak{l}_1^n}$, $\mathfrak{l}_2$ is inert in K and none of the $\mathfrak{l}_2$-descending $\mathfrak{l}_2$-isogenies from X is defined over k

The ramified case. Suppose again that X has maximal real multiplication locally at ℓ. If ℓ ramifies in K_0 as $\ell\mathcal{O}_{K_0} = \mathfrak{l}^2$, then the local CM order of X is of the form $\mathfrak{o}_{\mathfrak{f}} = \mathfrak{o}_{K_0} + \mathfrak{f}\mathfrak{o}_K$, for some $\mathfrak{o}_{K_0}$-ideal $\mathfrak{f} = \mathfrak{l}^n$, where n is some nonnegative integer. The composition $\mathrm{up}^{\mathfrak{l}}_{\mathrm{pr}_{\mathfrak{l}}(X)} \circ \mathrm{up}^{\mathfrak{l}}_X$ is an (ℓ,ℓ)-isogeny to a principally polarizable abelian surface with local CM order $\mathfrak{o}_{\mathfrak{l}^{n-2}}$. Continuing this way, provided n is even, we reach a principally polarizable abelian surface with maximal CM order locally at ℓ with a path of (ℓ,ℓ)-isogenies. If n is odd and we are at a principally polarizable abelian surface with local CM order $\mathfrak{o}_{\mathfrak{l}}$, and if $\mathfrak{l}$ is not inert in K, then $\mathfrak{l}$-horizontal $\mathfrak{l}$-isogenies exist and a composition of such an isogeny with $\mathrm{up}^{\mathfrak{l}}$ is an (ℓ,ℓ)-isogeny to a principally polarizable abelian surface with maximal CM order locally at ℓ. As a conclusion, the only case when we cannot reach a principally polarizable abelian surface with maximal CM order locally at ℓ with a path of (ℓ,ℓ)-isogenies in the ramified case is when n is odd and $\mathfrak{l}$ is inert in K. In this case the largest reachable local CM order is $\mathfrak{o}_{K_0} + \mathfrak{l}\mathfrak{o}_K$. The above described path of (ℓ,ℓ)-isogenies does not depend on the choice of a principal polarization on X. By Proposition 8.11, if X is defined over k, then all $\mathfrak{l}$-isogenies are defined over k and hence, all the (ℓ,ℓ)-isogenies are defined over k.

Going to the maximal local CM order with (ℓ,ℓ) and β-cyclic isogenies. Using the results from the previous paragraphs, suppose we have computed a path of (ℓ,ℓ)-isogenies to a principally polarizable abelian surface X with maximal local RM order and with local CM order $\mathfrak{o}_{K_0} + \mathfrak{l}\mathfrak{o}_K$, where $\mathfrak{l}$ is a prime of K_0 above ℓ (in the split or in the ramified case), and that there is no path of (ℓ,ℓ)-isogenies to a principally

polarizable abelian surface with local CM order $\mathfrak{o}_K$. There is, however, the $\mathfrak{l}$-ascending $\mathfrak{l}$-isogeny $\mathrm{up}_X^{\mathfrak{l}} : X \to \mathrm{pr}_{\mathfrak{l}}(X)$, and $\mathrm{pr}_{\mathfrak{l}}(X)$ has maximal local complex multiplication $\mathfrak{o}_K$. If $\mathfrak{l}$ is principal, generated by a totally positive element $\beta \in \mathcal{O}_{K_0}$ of $K_0/\mathbb{Q}$-norm ℓ (corresponds to a degree ℓ^2-endomorphism of X), we may consider the (β)-ascending (β)-isogeny $\mathrm{up}_X^{(\beta)}$. Let $\mathcal{L}_0$ be a principal polarization on X. The kernel of $\mathrm{up}_X^{(\beta)}$ is cyclic of order ℓ, hence maximal isotropic inside $\ker \beta$ for the commutator pairing $e_{\mathcal{L}_0^\beta}$, and $\mathrm{up}_X^{(\beta)}$ is a β-cyclic isogeny. Moreover, we see that this isogeny does not depend on the choice of a principal polarization on X. By the results from Sections 4 and 5, we can compute $\mathrm{up}_X^{(\beta)}$.

Proposition 8.19. *Let X be an ordinary and simple (absolutely simple if defined over k) principally polarizable abelian surface. Let ℓ be a prime number different from $\mathrm{char}(k)$. Suppose that ℓ is inert in K_0 or that at least one prime ideal of K_0 above ℓ is generated by a totally positive element $\beta \in \mathcal{O}_{K_0}$. Let $\mathcal{L}_0$ be a principal polarization on X. Then, there is a path of (ℓ,ℓ)-isogenies (the first one being with respect to the Weil pairing $e_\ell^{\phi_{\mathcal{L}_0}}$) from X, followed by at most one β-cyclic isogeny to a principally polarizable abelian surface with maximal complex multiplication locally at ℓ. This path does not depend on the choice of a principal polarization on X. Moreover, if X is defined over k, then all the isogenies are defined over k.*

Suppose now X has local CM order $\mathfrak{o}_{K_0} + \mathfrak{l}\mathfrak{o}_K$ and $\mathfrak{l}$ is not generated by a totally positive element of $\mathcal{O}_{K_0}$. Suppose however that there exists an ideal $\mathfrak{m} \lhd \mathcal{O}_{K_0}$, coprime to $\mathfrak{l}$, such that $\mathfrak{l}\mathfrak{m}$ is generated by a totally positive element $\beta \in \mathcal{O}_{K_0}$. Let $\mathcal{L}_0$ be a principal polarization on X. Subject to the following conditions, we can still reach an abelian surface with maximal local complex multiplication with a computable β-cyclic isogeny:

i) the maximal isotropic subgroups of $\ker \beta$ for $e_{\mathcal{L}_0^\beta}$ are cyclic;

ii) for all $\mathfrak{p} \mid \mathfrak{m}$, the surface X is at $\mathfrak{p}$-level 0 in the $\mathfrak{p}$-isogeny graph, and the prime $\mathfrak{p}$ is not inert in K.

Namely, if $\mathfrak{m}$ factors in K_0 as $\mathfrak{m} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$, then the $\mathfrak{l}$-ascending $\mathfrak{l}$-isogeny $\mathrm{up}_X^{\mathfrak{l}}$, composed with e_1 $\mathfrak{p}_1$-horizontal $\mathfrak{p}_1$-isogenies, e_2 $\mathfrak{p}_2$-horizontal $\mathfrak{p}_2$-isogenies, and so on, is a β-cyclic isogeny $X \to Y$ for the commutator pairing $e_{\mathcal{L}_0^\beta}$, and Y has maximal complex multiplication locally at ℓ. Condition ii) only ensures that we do not decrease the $\mathfrak{p}$-level of X at any prime $\mathfrak{p} \neq \mathfrak{l}$, and can safely be weakened. Condition i) is verified if for example all the prime factors of $\mathfrak{m}$ are above distinct prime numbers (and different from ℓ), have inertia degree 1 and exponent 1 in the factorization of $\mathfrak{m}$. If condition i) cannot be fulfilled, e.g. if a maximal isotropic subgroup of $\ker \beta$ contains a subgroup isomorphic to $\mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/r\mathbb{Z}$, for some prime number $r \neq \ell$, then the computation of a cyclic isogeny has to be preceded by an (r,r)-isogeny.

8.5 Perspectives in dimension 3

In dimension 3 the situation is more delicate. While the theory of $\mathfrak{l}$-isogenies can still be applied when the abelian threefold has maximal local real multiplication, it is not known if one can always reach such a variety with (ℓ,ℓ,ℓ)-isogenies only, starting from an arbitrary principally polarizable abelian threefold. The latter problem is the subject of an ongoing research project of the author with D. Jetchev, C. Martindale, E. Milio and

B. Wesolowski. Among the applications of an algorithm that finds a computable path of isogenies to reach an abelian variety with maximal complex multiplication presented in Section 8.2, the random self-reducibility of the discrete logarithm problem in dimension 3 becomes particularly interesting. Namely, using the transitive action of $\mathcal{P}(\mathcal{O}_K)$ (the projection of the Shimura class group on $\mathrm{Cl}(\mathcal{O}_K)$) on the set of k-isomorphism classes of principally polarizable ordinary and absolutely simple abelian threefolds with maximal endomorphism ring, one can combine a random walk on this horizontal graph (using β-cyclic isogenies of prime degree only) with descending (ℓ,ℓ,ℓ)-isogenies to reach a uniformly random principally polarizable abelian threefold. With reasonable heuristic assumptions on the proportion of quartic Jacobians in the fixed isogeny class, this path has a high probability to end at a non-hyperelliptic Jacobian. Note that it is important to compute the β-cyclic isogenies at maximal endomorphism level, otherwise a non-negligible proportion of varieties in the isogeny class would not be reachable via the above described random path.

8.5.1 (ℓ,ℓ,ℓ)-isogeny graphs with maximal local real multiplication

Let k be a finite field of size q and consider a $\bar{k}$-isogeny class of ordinary and simple abelian threefolds that admits some variety X_0 defined over k. Fix an isomorphism $\mathrm{End}(X_0)\otimes_{\mathbb{Z}}\mathbb{Q} \xrightarrow{\sim} K$ to the sextic CM-field $K=\mathbb{Q}(\pi)$, where π is a Weil q-number that represents the k-isogeny class of X_0, and let K_0 be the totally real cubic subfield of K.

Let ℓ be a prime number different from the characteristic of k, and suppose it factors in K_0 as $\ell\mathcal{O}_{K_0} = \mathfrak{l}_1^{e_1}\cdots\mathfrak{l}_r^{e_r}$. Starting from a principally polarizable threefold X with maximal real multiplication locally at ℓ in this isogeny class, one would like to know that a certain combination of $\mathfrak{l}_i$-isogenies is an (ℓ,ℓ,ℓ)-isogeny, similar to the case of dimension 2 described in Section 8.4.2 (as you might guess, it will be a combination of e_1 $\mathfrak{l}_1$-isogenies, with e_2 $\mathfrak{l}_2$-isogenies, etc). This, applied to the $\mathfrak{l}_i$-ascending $\mathfrak{l}_i$-isogenies $\mathrm{up}^{\mathfrak{l}_i}$, as defined in Definition 8.10, is then a computable (ℓ,ℓ,ℓ)-isogeny. And similarly, a combination of $\mathfrak{l}_i$-descending $\mathfrak{l}_i$-isogenies is a computable (ℓ,ℓ,ℓ)-isogeny.

We can prove this, similar to [BJW17] for dimension 2, using ℓ-adic techniques. Let $V_\ell := T_\ell X\otimes_{\mathbb{Z}_\ell}\mathbb{Q}_\ell$, where $T_\ell X$ is the ℓ-adic Tate module of X. We know that V_ℓ is a $\mathbb{Q}_\ell$-vector space of dimension 6, and $T_\ell X$ is a $\mathbb{Z}_\ell$-lattice in V_ℓ. Also, V_ℓ is a $K_\ell = K\otimes_{\mathbb{Q}}\mathbb{Q}_\ell$-module of rank one (this is Tate's theorem). The bridge between the study of ℓ-power degree isogenies from X and the ℓ-adic vector space V_ℓ is that neighbor lattices of $T_\ell X$ in V_ℓ (for the containment "$\subset$") can naturally be identified with finite subgroups of $X[\ell^\infty]$, yielding the isogenies. Elements of $T_\ell X$ are sequences $(P_n)_{n\geq 1}$ with $P_n\in X[\ell^n]$ and $\ell P_{n+1}=P_n$ for all $n\geq 1$, and elements of V_ℓ are of the form $(P_n)_{n\geq 1}\otimes\ell^{-m}$, with $m\in\mathbb{Z}_{\geq 0}$. Via

$$(P_n)_{n\geq 1}\otimes\ell^{-m}\mapsto(P_{n+m})_{n\geq 1},$$

we obtain an identification of V_ℓ with the set of sequences $(Q_n)_{n\geq 1}$ with $Q_n\in X[\ell^\infty]$ and $\ell Q_{n+1}=Q_n$ for all $n\geq 1$. Under this identification, $T_\ell X$ corresponds to the sequences satisfying $Q_1\in X[\ell]$. The projection

$$(Q_n)_{n\geq 1}\mapsto \ell Q_1$$

induces an isomorphism

$$V_\ell/T_\ell X \xrightarrow{\sim} X[\ell^\infty](\bar{k})$$

and hence,

$$\{\text{finite subgroups of } X[\ell^\infty](\bar{k})\}\leftrightarrow\{\mathbb{Z}_\ell\text{-lattices in } V_\ell \text{ containing } T_\ell X\}.$$

Fix $\mathfrak{l}$ a prime of K_0 above ℓ. We want to define $\mathfrak{l}$-isogenies (as in Definition 8.4) in the ℓ-adic setting, for abelian threefolds with maximal local real multiplication. Let $\Lambda \subset V_\ell$ be a $\mathbb{Z}_\ell$-lattice and denote by

$$\mathfrak{o}(\Lambda) = \{\alpha \in K_\ell : \alpha\Lambda \subset \Lambda\}$$

the stabiliser of Λ for the K_ℓ-action. Tate's theorem states that

$$\mathfrak{o}(T_\ell X) = \mathfrak{o}(X) = \mathcal{O}(X) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell,$$

where $\mathcal{O}(X) \subset K$ is the CM-order of X corresponding to $\mathrm{End}_{\bar{k}}(X)$. Suppose now throughout that the stabiliser of Λ contains $\mathfrak{o}_{K_0}$, i.e. Λ is an $\mathfrak{o}_{K_0}$-module. It is not hard to show that Λ is an $\mathfrak{o}(\Lambda)$-module of rank one (the proof is similar to that of [BJW17, Lem. 7.7]). From this it follows that Λ is a free $\mathfrak{o}_{K_0}$-module of rank 2.

Since Λ is $\mathfrak{o}_{K_0}$-stable, we have $\mathfrak{l}\Lambda \subset \Lambda$ and hence, $\Lambda/\mathfrak{l}\Lambda$ is an $\mathfrak{o}_{K_0}/\mathfrak{l}\mathfrak{o}_{K_0}$-module, i.e. an $\mathfrak{o}_{K_0}/\mathfrak{l}\mathfrak{o}_{K_0} \cong \mathcal{O}_{K_0}/\mathfrak{l}$-vector space of dimension 2. The $\mathfrak{o}_{K_0}/\mathfrak{l}\mathfrak{o}_{K_0}$-vector subspaces of $\Lambda/\mathfrak{l}\Lambda$ can naturally be identified with $\mathfrak{o}_{K_0}$-stable lattices Γ satisfying $\mathfrak{l}\Lambda \subset \Gamma \subset \Lambda$.

Definition 8.20. The set of $\mathfrak{l}$-neighbors of Λ is

$$\mathscr{L}_\mathfrak{l}(\Lambda) = \{\mathfrak{l}\Lambda \subset \Gamma \subset \Lambda : \Gamma \text{ an } \mathfrak{o}_{K_0}\text{-stable } \mathbb{Z}_\ell\text{-lattice and } \Gamma/\mathfrak{l}\Lambda \text{ of } \mathfrak{o}_{K_0}/\mathfrak{l}\mathfrak{o}_{K_0}\text{-dimension one}\}.$$

Next, we want to define (ℓ, ℓ, ℓ)-neighbors in the ℓ-adic setting (for a comparison, see Definition 8.3). Let $\mathcal{L}_0$ be a principal polarization on X. The symplectic pairing $e_\ell^{\phi_{\mathcal{L}_0}} : T_\ell X \times T_\ell X \to \mathbb{Z}_\ell$ from Section 3.1 (here, the target group is written additively) extends to a symplectic pairing on V_ℓ, that we will denote by

$$\langle \cdot, \cdot \rangle \colon V_\ell \times V_\ell \to \mathbb{Q}_\ell.$$

For $\alpha \in K_\ell$ and $x, y \in V_\ell$ we have $\langle \alpha x, y\rangle = \langle x, \alpha^\dagger y\rangle$. In particular, for $\alpha \in K_{0,\ell}$ we have $\langle \alpha x, y\rangle = \langle x, \alpha y\rangle$.

Lemma 8.21. *For all $\alpha, \beta \in K_{0,\ell}$ and all $x \in V_\ell$ we have*

$$\langle \alpha x, \beta x\rangle = 0.$$

Proof. This follows from $\langle \alpha x, \beta x\rangle = \langle x, \alpha\beta x\rangle = \langle x, \beta\alpha x\rangle = \langle \beta x, \alpha x\rangle = -\langle \alpha x, \beta x\rangle$. □

Recall that for a $\mathbb{Z}_\ell$-lattice Λ in V_ℓ, the *dual lattice* of Λ is defined as

$$\Lambda^* = \{x \in V_\ell : \langle x, \Lambda\rangle \subset \mathbb{Z}_\ell\}.$$

The lattice $T_\ell X$ is self-dual, i.e. $(T_\ell X)^* = T_\ell X$, following from the fact that $V_\ell = T_\ell X \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ and that $\mathcal{L}_0$ is a principal polarization.

Lemma 8.22. *For any self-dual $\mathbb{Z}_\ell$-lattice $\Lambda \subset V_\ell$, the quotient $\Lambda/\ell\Lambda$ is a symplectic $\mathbb{Z}_\ell/\ell\mathbb{Z}_\ell \cong \mathbb{Z}/\ell\mathbb{Z}$-vector space of dimension 6 for the pairing*

$$\langle x + \ell\Lambda, y + \ell\Lambda\rangle = \langle x, y\rangle \mod \ell\mathbb{Z}_\ell.$$

Proof. The containment $\Lambda \subset \Lambda^*$ ensures that indeed, $\langle \Lambda, \Lambda\rangle \subset \mathbb{Z}_\ell$. For the nondegeneracy, suppose that $x \in \Lambda$ is such that $\langle x, y\rangle \in \ell\mathbb{Z}_\ell$ for all $y \in \Lambda$. It follows that $\ell^{-1}x \in \Lambda^* = \Lambda$ and hence, $x \in \ell\Lambda$. □

Definition 8.23. The set of (ℓ,ℓ,ℓ)-neighbors of a self-dual $\mathbb{Z}_\ell$-lattice $\Lambda \subset V_\ell$ is

$$\mathscr{L}(\Lambda) = \{\ell\Lambda \subset \Gamma \subset \Lambda : \Gamma \text{ a } \mathbb{Z}_\ell\text{-lattice and } \Gamma/\ell\Lambda \text{ maximal isotropic in } \Lambda/\ell\Lambda\}.$$

We can give a formula for the number of (ℓ,ℓ,ℓ)-neighbors of Λ.

Proposition 8.24. *The number of maximal isotropic subspaces of a symplectic $\mathbb{Z}/\ell\mathbb{Z}$-vector space of dimension 6 is*

$$\prod_{i=1}^{3}(\ell^i+1) = \ell^6+\ell^5+\ell^4+2\ell^3+\ell^2+\ell+1.$$

Proof. Let $(V,\langle\cdot,\cdot\rangle)$ be a symplectic $\mathbb{Z}/\ell\mathbb{Z}$-vector space of dimension 6, and let $\{\lambda_1,\lambda_2,\lambda_3,\mu_1,\mu_2,\mu_3\}$ be a symplectic basis of V for $\langle\cdot,\cdot\rangle$. The set of symplectic bases of V for $\langle\cdot,\cdot\rangle$ is a principal homogenous space under the action of $\mathbf{Sp}(V,\langle\cdot,\cdot\rangle)$, and via $\{\lambda_1,\dots,\mu_3\}$ we might identify $\mathbf{Sp}(V,\langle\cdot,\cdot\rangle)$ with $\mathbf{Sp}_6(\mathbb{Z}/\ell\mathbb{Z})$. We have a decomposition $V = \langle\lambda_1,\lambda_2,\lambda_3\rangle \oplus \langle\mu_1,\mu_2,\mu_3\rangle$ into maximal isotropic subspaces. Given any maximal isotropic subspace M of V, a basis of M can be completed to a symplectic basis of V, see e.g. [dG06, Thm. 1.15]. Hence, $\mathbf{Sp}_6(\mathbb{Z}/\ell\mathbb{Z})$ acts transitively on the set of maximal isotropic subspaces. In order to compute the number of maximal isotropic subspaces, it suffices to identify the stabilizer of $\langle\lambda_1,\lambda_2,\lambda_3\rangle$. A symplectic matrix $\gamma = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathbf{Sp}_6(\mathbb{Z}/\ell\mathbb{Z})$ stabilizes $\langle\lambda_1,\lambda_2,\lambda_3\rangle$ if and only if $C=0$. And $\gamma = \begin{pmatrix} A & B \\ 0 & D \end{pmatrix}$ is symplectic if and only if $A \in \mathbf{GL}_3(\mathbb{Z}/\ell\mathbb{Z})$, $D = ({}^tA)^{-1}$ and $A\,{}^tB$ is symmetric. Let us count the number of such matrices. The matrix A is in $\mathbf{GL}_3(\mathbb{Z}/\ell\mathbb{Z})$, so there are $\ell^3\prod_{i=1}^3(\ell^i-1)$ possible choices. For each choice of A we can choose $B \in \mathbf{Mat}_3(\mathbb{Z}/\ell\mathbb{Z})$ with the only constraint that $A\,{}^tB$ is symmetric. We carefully verify that this leaves us with the freedom of choosing $\frac{3\cdot4}{2}$ coefficients of B, as if we would require B itself to be symmetric. Hence, there are total of ℓ^6 choices for B. Since $\#\,\mathbf{Sp}_6(\mathbb{Z}/\ell\mathbb{Z}) = \ell^{3^2}\prod_{i=1}^3(\ell^{2i}-1)$, the number of maximal isotropic subspaces of V is given by

$$\frac{\prod_{i=1}^3(\ell^{2i}-1)}{\prod_{i=1}^3(\ell^i-1)} = \prod_{i=1}^{3}(\ell^i+1).$$

□

We now show that a combination of $\mathfrak{l}$-isogenies from $T_\ell X$ (depending on the splitting of ℓ in K_0) is an (ℓ,ℓ,ℓ)-isogeny. We will only treat the cases ℓ inert in K_0, ℓ totally split and $\ell\mathcal{O}_{K_0} = \mathfrak{l}_1\mathfrak{l}_2$, the remaining cases being similar. Suppose throughout that $\Lambda \subset V_\ell$ is a self-dual $\mathbb{Z}_\ell$-lattice with maximal local real multiplication, i.e. $\mathfrak{o}_{K_0} \subset \mathfrak{o}(\Lambda)$.

The inert case. The local real multiplication algebra $K_{0,\ell}$ is the completion of K_0 with respect to the absolute value $|\cdot|_{\ell\mathcal{O}_{K_0}}$ induced by the prime ideal $\ell\mathcal{O}_{K_0}$. Moreover, by (8.2) we have that $\mathfrak{o}_{K_0}/\ell\mathfrak{o}_{K_0} \cong \mathcal{O}_{K_0}/\ell\mathcal{O}_{K_0} \cong \mathbb{F}_{\ell^3}$.

Proposition 8.25. *The set of (ℓ,ℓ,ℓ)-neighbors of Λ with maximal local real multiplication is equal to the set of $\ell\mathfrak{o}_{K_0}$-neighbors of Λ.*

Proof. Since $\Lambda/\ell\Lambda$ is a symplectic $\mathbb{F}_\ell$-vector space of dimension 6, it is of cardinality ℓ^6. But it is also an $\mathfrak{o}_{K_0}/\ell\mathfrak{o}_{K_0} \cong \mathbb{F}_{\ell^3}$-module and by cardinality reason, it is an $\mathbb{F}_{\ell^3}$-vector

space of dimension 2. The lattices $\ell\Lambda \subset \Gamma \subset \Lambda$ that are $\mathfrak{o}_{K_0}$-stable are naturally identified with $\mathbb{F}_{\ell^3}$-vector subspaces of $\Lambda/\ell\Lambda$. An isotropic $\mathbb{F}_{\ell^3}$-subspace of $\Lambda/\ell\Lambda$ must be of dimension 0 or 1 and hence, maximal isotropic subspaces are $\mathbb{F}_{\ell^3}$-lines. Conversely, all $\mathbb{F}_{\ell^3}$-lines are isotropic by Lemma 8.21 (hence maximal isotropic).

□

The totally split case. Suppose that $\ell\mathcal{O}_{K_0} = \mathfrak{l}_1\mathfrak{l}_2\mathfrak{l}_3$. The local real endomorphism algebra $K_{0,\ell}$ is the direct sum of the completions of K_0 with respect to the absolute values $|\cdot|_{\mathfrak{l}_1}$, $|\cdot|_{\mathfrak{l}_2}$ and $|\cdot|_{\mathfrak{l}_3}$ respectively. Moreover, for $i = 1, 2, 3$, we have $\mathfrak{o}_{K_0}/\mathfrak{l}_i\mathfrak{o}_{K_0} \cong \mathbb{Z}/\ell\mathbb{Z}$.

Proposition 8.26. *For any $\{i, j, k\} = \{1, 2, 3\}$, an element of $\mathscr{L}_{\mathfrak{l}_i}(\mathscr{L}_{\mathfrak{l}_j}(\mathscr{L}_{\mathfrak{l}_k}(\Lambda)))$ is an (ℓ, ℓ, ℓ)-neighbor of Λ with maximal local real multiplication.*

Proof. Let $\Gamma \in \mathscr{L}_{\mathfrak{l}_3}(\mathscr{L}_{\mathfrak{l}_2}(\mathscr{L}_{\mathfrak{l}_1}(\Lambda)))$ (as will become clear from the proof, the order of the indices is not relevant). By definition, Γ is $\mathfrak{o}_{K_0}$-stable. Let us show that Γ is an (ℓ, ℓ, ℓ)-neighbor of Λ. There exist $\mathfrak{o}_{K_0}$-stable lattices Γ_1, Γ_2 such that

$$\begin{array}{ll} \mathfrak{l}_1\Lambda \subset \Gamma_1 \subset \Lambda & \text{and } \Gamma_1/\mathfrak{l}_1\Lambda \text{ is an } \mathbb{F}_\ell\text{-line} \\ \mathfrak{l}_2\Gamma_1 \subset \Gamma_2 \subset \Gamma_1 & \text{and } \Gamma_2/\mathfrak{l}_2\Gamma_1 \text{ is an } \mathbb{F}_\ell\text{-line} \\ \mathfrak{l}_3\Gamma_2 \subset \Gamma \subset \Gamma_2 & \text{and } \Gamma/\mathfrak{l}_3\Gamma_2 \text{ is an } \mathbb{F}_\ell\text{-line.} \end{array}$$

We deduce that

$$\begin{aligned} \Gamma_1 &= \mathbb{Z}_\ell\gamma_1 + \mathfrak{l}_1\Lambda \text{ for some } \gamma_1 \in \Gamma_1 \\ \Gamma_2 &= \mathbb{Z}_\ell\gamma_2 + \mathfrak{l}_2\Gamma_1 \text{ for some } \gamma_2 \in \Gamma_2 \\ \Gamma &= \mathbb{Z}_\ell\gamma + \mathfrak{l}_3\Gamma_2 \text{ for some } \gamma \in \Gamma. \end{aligned}$$

Let ϖ_1 be a generator of the principal ideal $\mathfrak{l}_1\mathfrak{o}_{K_0}$ (to be more rigorous, we should write $(\varpi_1, 1, 1)$ for a generator of $\mathfrak{l}_1\mathfrak{o}_{K_0}$). Let ϖ_2 and ϖ_3 be generators of $\mathfrak{l}_2\mathfrak{o}_{K_0}$ and $\mathfrak{l}_3\mathfrak{o}_{K_0}$ respectively, and observe that $(\varpi_1\varpi_2\varpi_3) = \ell\mathfrak{o}_{K_0}$ by (8.3). We may suppose without loss of generality that $\varpi_1\varpi_2\varpi_3 = \ell$. We have

$$\Gamma = \mathbb{Z}_\ell\gamma + \mathbb{Z}_\ell\varpi_3\gamma_2 + \mathbb{Z}_\ell\varpi_2\varpi_3\gamma_1 + \ell\Lambda.$$

In order for $\Gamma/\ell\Lambda$ to be isotropic, it suffices to show that

$$\langle\gamma, \varpi_3\gamma_2\rangle \equiv \langle\gamma, \varpi_2\varpi_3\gamma_1\rangle \equiv \langle\varpi_3\gamma_2, \varpi_2\varpi_3\gamma_1\rangle \equiv 0 \mod \ell\mathbb{Z}_\ell.$$

For this, let us first show that

$$\langle\gamma_2, \varpi_2\varpi_3\gamma_1\rangle \equiv 0 \mod \ell\mathbb{Z}_\ell. \tag{8.4}$$

Since $\gamma_2 \in \Gamma_2 \subset \Gamma_1$, there exist $a \in \mathbb{Z}_\ell$ and $z \in \Lambda$ such that $\gamma_2 = a\gamma_1 + \varpi_1 z$. Then

$$\langle\gamma_2, \varpi_2\varpi_3\gamma_1\rangle = \langle a\gamma_1, \varpi_2\varpi_3\gamma_1\rangle + \langle\varpi_1 z, \varpi_2\varpi_3\gamma_1\rangle = 0 + \langle z, \ell\gamma_1\rangle \equiv 0 \mod \ell\mathbb{Z}_\ell.$$

With the same argument one shows that

$$\langle\varpi_3\gamma_2, \varpi_2\varpi_3\gamma_1\rangle \equiv 0 \mod \ell\mathbb{Z}_\ell.$$

To show that $\langle\gamma, \varpi_2\varpi_3\gamma_1\rangle \equiv 0 \mod \ell\mathbb{Z}_\ell$, we observe that $\gamma \in \Gamma \subset \Gamma_2$ and hence, there exist $b, c \in \mathbb{Z}_\ell$ and $z' \in \Lambda$ such that

$$\gamma = b\gamma_2 + c\varpi_2\gamma_1 + \varpi_1\varpi_2 z'.$$

But $\langle c\varpi_2\gamma_1, \varpi_2\varpi_3\gamma_1\rangle = 0$, and by (8.4) we know that $\langle b\gamma_2, \varpi_2\varpi_3\gamma_1\rangle \equiv 0 \mod \ell\mathbb{Z}_\ell$. Moreover, since $\varpi_1\varpi_2\varpi_3 = \ell$, we have $\langle \varpi_1\varpi_2 z', \varpi_2\varpi_3\gamma_1\rangle \equiv 0 \mod \ell\mathbb{Z}_\ell$. Finally, to show that $\langle \gamma, \varpi_3\gamma_2\rangle \equiv 0 \mod \ell\mathbb{Z}_\ell$ it suffices to show that $\langle c\varpi_2\gamma_1, \varpi_3\gamma_2\rangle \equiv 0 \mod \ell\mathbb{Z}_\ell$. But $\gamma_2 = a\gamma_1 + \varpi_1 z$ and hence,

$$\langle c\varpi_2\gamma_1, \varpi_3\gamma_2\rangle = \langle c\varpi_2\gamma_1, a\varpi_3\gamma_1\rangle + \langle c\varpi_2\gamma_1, \varpi_1\varpi_3 z\rangle \equiv 0 \mod \ell\mathbb{Z}_\ell.$$

□

The case $\ell\mathcal{O}_{K_0} = \mathfrak{l}_1\mathfrak{l}_2$. Suppose without loss of generality that $\mathfrak{l}_1$ is of inertia degree 1 and that $\mathfrak{l}_2$ is of inertia degree 2. The local real endomorphism algebra $K_{0,\ell}$ is the direct sum of the completions of K_0 with respect to the absolute values $|\cdot|_{\mathfrak{l}_1}$ and $|\cdot|_{\mathfrak{l}_2}$ respectively. By (8.2) we have $\mathfrak{o}_{K_0}/\mathfrak{l}_1\mathfrak{o}_{K_0} \cong \mathbb{Z}/\ell\mathbb{Z}$ and $\mathfrak{o}_{K_0}/\mathfrak{l}_2\mathfrak{o}_{K_0} \cong \mathbb{F}_{\ell^2}$. We deduce that $\mathfrak{o}_{K_0}$ can be written as $\mathfrak{o}_{K_0} = \mathbb{Z}_\ell + \mathbb{Z}_\ell\alpha + \mathfrak{l}_2\mathfrak{o}_{K_0}$, for some $\alpha \in \mathfrak{o}_{K_0}$.

Proposition 8.27. *For any $\{i,j\} = \{1,2\}$, an element of $\mathscr{L}_{\mathfrak{l}_i}(\mathscr{L}_{\mathfrak{l}_j}(\Lambda))$ is an (ℓ,ℓ,ℓ)-neighbor of Λ with maximal local real multiplication.*

Proof. Let $\Gamma \in \mathscr{L}_{\mathfrak{l}_2}(\mathscr{L}_{\mathfrak{l}_1}(\Lambda))$ (the second case is similar). By definition, Γ is $\mathfrak{o}_{K_0}$-stable. There exists a $\mathfrak{o}_{K_0}$-stable lattice Γ_1 such that

$$\begin{array}{ll} \mathfrak{l}_1\Lambda \subset \Gamma_1 \subset \Lambda & \text{and } \Gamma_1/\mathfrak{l}_1\Lambda \text{ is an } \mathbb{F}_\ell\text{-line} \\ \mathfrak{l}_2\Gamma_1 \subset \Gamma \subset \Gamma_1 & \text{and } \Gamma/\mathfrak{l}_2\Gamma_1 \text{ is an } \mathbb{F}_{\ell^2}\text{-line.} \end{array}$$

We deduce that

$$\begin{aligned} \Gamma_1 &= \mathbb{Z}_\ell\gamma_1 + \mathfrak{l}_1\Lambda \text{ for some } \gamma_1 \in \Gamma_1 \\ \Gamma &= (\mathbb{Z}_\ell + \mathbb{Z}_\ell\alpha)\gamma + \mathfrak{l}_2\Gamma_1 \text{ for some } \gamma \in \Gamma. \end{aligned}$$

As before, we let ϖ_1 and ϖ_2 be generators of the principal ideals $\mathfrak{l}_1\mathfrak{o}_{K_0}$ and $\mathfrak{l}_2\mathfrak{o}_{K_0}$ respectively. They satisfy $(\varpi_1\varpi_2) = \ell\mathfrak{o}_{K_0}$ and we may choose ϖ_1 and ϖ_2 such that $\varpi_1\varpi_2 = \ell$. We can write

$$\Gamma = \mathbb{Z}_\ell\gamma + \mathbb{Z}_\ell\alpha\gamma + \mathbb{Z}_\ell\varpi_2\gamma_1 + \ell\Lambda.$$

Let us show that $\langle \gamma, \varpi_2\gamma_1\rangle \equiv 0 \mod \ell\mathbb{Z}_\ell$, the proof for $\langle \alpha\gamma, \varpi_2\gamma_1\rangle$ being similar. Since $\gamma \in \Gamma \subset \Gamma_1$, we can write $\gamma = a\gamma_1 + \varpi_1 z$ for some $a \in \mathbb{Z}_\ell$ and $z \in \Lambda$. But then

$$\langle \gamma, \varpi_2\gamma_1\rangle = \langle a\gamma_1, \varpi_2\gamma_1\rangle + \langle \varpi_1 z, \varpi_2\gamma_1\rangle = 0 + \langle z, \ell\gamma_1\rangle \equiv 0 \mod \ell\mathbb{Z}_\ell.$$

□

8.5.2 Going up

Let $(X, \mathcal{L}_0)$ be a principally polarized abelian threefold in the previously fixed isogeny class (ordinary and simple), and suppose it has maximal real multiplication locally ℓ. Suppose ℓ factors in K_0 as $\ell\mathcal{O}_{K_0} = \mathfrak{l}_1^{e_1}\cdots\mathfrak{l}_r^{e_r}$. From the previous section we know that a composition of e_1 $\mathfrak{l}_1$-isogenies with e_2 $\mathfrak{l}_2$-isogenies, etc., is an (ℓ,ℓ,ℓ)-isogeny from X for the Weil pairing $e_\ell^{\phi_{\mathcal{L}_0}}$, preserving the maximality of the local real multiplication order. In particular, this can be applied to the isogenies $\mathrm{up}^{\mathfrak{l}_1}, \ldots, \mathrm{up}^{\mathfrak{l}_r}$. With the exact same reasoning as in Section 8.4.3, we can show that using (ℓ,ℓ,ℓ)-isogenies only, we can reach a principally polarized abelian threefold X' with local complex multiplication $\mathfrak{o}_K$ or $\mathfrak{o}_{K_0} + \mathfrak{l}_i\mathfrak{o}_K$, for some $1 \le i \le r$. Let $\mathcal{L}_0'$ be the principal polarization on X' induced

by $\mathcal{L}_0$ and this ascending path. Provided $\mathfrak{l}_i$ is principal and of norm ℓ, generated by a totally positive real endomorphism β, the (β)-isogeny $\mathrm{up}^{(\beta)}$ has a cyclic, maximal isotropic kernel inside $\ker\beta$ for the commutator pairing $e_{(\mathcal{L}_0')^\beta}$, hence is a β-cyclic isogeny. That is, the path of isogenies to a principally polarized abelian threefold with maximal local complex multiplication is computable.

If $\mathfrak{l}_i$ is not generated by a totally positive real endomorphism, there is still a situation where we are able to reach a principally polarized abelian threefold with maximal local complex multiplication with a computable isogeny, analogous to dimension 2. Namely, if there exists an ideal $\mathfrak{m} \triangleleft \mathcal{O}_{K_0}$, coprime to $\mathfrak{l}_i$, such that $\mathfrak{l}_i\mathfrak{m}$ is generated by a totally positive element $\beta \in \mathcal{O}_{K_0}$, and such that the following conditions hold:

i) the maximal isotropic subgroups of $\ker\beta$ for $e_{(\mathcal{L}_0')^\beta}$ are cyclic;

ii) for all $\mathfrak{p} \mid \mathfrak{m}$, the threefold X' is at $\mathfrak{p}$-level 0 in the $\mathfrak{p}$-isogeny graph, and the prime $\mathfrak{p}$ is not inert in K.

The $\mathfrak{l}_i$-ascending isogeny $\mathrm{up}^{\mathfrak{l}_i}$, composed with $\mathfrak{p}$-horizontal $\mathfrak{p}$-isogenies (for $\mathfrak{p}$ the prime factors of $\mathfrak{m}$), is a computable β-cyclic isogeny. Hence, we can reach a principally polarized abelian threefold with maximal complex multiplication locally at ℓ. As in dimension 2, condition ii) only ensures that we do not decrease the $\mathfrak{p}$-level of X' at any prime $\mathfrak{p} \neq \mathfrak{l}_i$, and can be weakened. Condition i) is verified if for example all the prime factors of $\mathfrak{m}$ are above distinct prime numbers (and different from ℓ), have inertia degree 1 and exponent 1 in the factorization of $\mathfrak{m}$. If condition i) cannot be fulfilled, e.g. if a maximal isotropic subgroup of $\ker\beta$ contains a subgroup isomorphic to $\mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/r\mathbb{Z}$, for some prime number $r \neq \ell$, then the computation of a cyclic isogeny has to be preceded by an (r, r, r)-isogeny.

8.5.3 Application to the discrete logarithm problem in dimension 3

Until nowadays, little is known about the proportion of hyperelliptic and non-hyperelliptic Jacobians in a randomly chosen $\bar{k}$-isogeny class of ordinary and simple abelian threefolds. And even if one would make reasonable assumptions on the proportions (e.g. based on the dimensions of the moduli spaces of hyperelliptic and non-hyperelliptic genus 3 curves), the distribution of the hyperelliptic and quartic Jacobians inside the isogeny class is not known. This makes it practically impossible to construct an explicit isogeny path from a hyperelliptic Jacobian over k to a quartic Jacobian over k in a deterministic way, which would decrease the complexity for the computation of a discrete logarithm from $O(\#k^{4/3})$ to $O(\#k)$, see [Die06, DT08] and [GTTD05]. Yet, one can follow a random path and try to estimate the probability of reaching a quartic Jacobian. Let X be a principally polarized abelian threefold in the isogeny class. Let K be a fixed sextic CM-field, isomorphic to the endomorphism algebra of X. Up to isomorphism, the endomorphism ring of any variety isogenous to X is contained in $\mathcal{O}_K$. We want the endpoint of a random path of computable isogenies starting from X to be uniform among the isogeny class. To achieve this, we cannot simply compute random isogenies. The reason being that the orders of $\mathcal{O}_K$ corresponding to the endomorphism rings of two (ℓ, ℓ, ℓ)-isogenous or β-isogenous varieties satisfy some "neighbor relation". To get rid of this restrictive neighbor relation, we first need to compute a deterministic path to a variety with maximal endomorphism ring $\mathcal{O}_K$. Only after this has been achieved, we can start randomizing the path. There are only finitely many prime numbers at which the local endomorphism ring of X is not maximal. If for all these prime numbers

we are in the situation described in Section 8.5.2, i.e. we are able to compute a path of (ℓ, ℓ, ℓ)-isogenies and β-cyclic isogenies to a principally polarized abelian threefold with maximal local complex multiplication, then we have a path of computable isogenies to a principally polarized abelian threefold X' with maximal global endomorphism ring. If we denote by $\mathcal{P}(\mathcal{O}_K)$ the projection of the Shimura class group on $\mathrm{Cl}(\mathcal{O}_K)$, then the $\mathcal{P}(\mathcal{O}_K)$-orbit of X' under the CM-action is the set of all isomorphism classes of principally polarizable abelian threefolds with maximal endomorphism ring. By [JW19, Thm. 1.1], one can construct expander graphs on the $\mathcal{P}(\mathcal{O}_K)$-orbit of X', where the edges are $\mathfrak{l}$-isogenies of bounded prime degree. Hence, they are β-cyclic isogenies. To obtain a uniform endpoint of a random path starting from X, one first computes the deterministic path to X', then does a random walk on the set of isomorphism classes of principally polarized abelian threefolds with endomorphism ring $\mathcal{O}_K$ using the transitive CM-action, and finally computes random descending (ℓ, ℓ, ℓ)-isogenies.

References

[ADH94] Leonard M. Adleman, Jonathan DeMarrais, and Ming-Deh Huang, *A subexponential algorithm for discrete logarithms over the rational subgroup of the Jacobians of large genus hyperelliptic curves over finite fields*, Algorithmic number theory (Ithaca, NY, 1994), Lecture Notes in Comput. Sci., vol. 877, Springer, Berlin, 1994, pp. 28–40. MR 1322708

[BF01] Dan Boneh and Matthew K. Franklin, *Identity-based encryption from the weil pairing*, Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology (London, UK, UK), CRYPTO '01, Springer-Verlag, 2001, pp. 213–229.

[BGGM15] Razvan Barbulescu, Pierrick Gaudry, Aurore Guillevic, and François Morain, *Improving NFS for the discrete logarithm problem in non-prime finite fields*, Advances in cryptology—EUROCRYPT 2015. Part I, Lecture Notes in Comput. Sci., vol. 9056, Springer, Heidelberg, 2015, pp. 129–155. MR 3344923

[BGL11] Reinier Bröker, David Gruenewald, and Kristin Lauter, *Explicit CM theory for level 2-structures on abelian surfaces*, Algebra Number Theory **5** (2011), no. 4, 495–528. MR 2870099

[Bis15] Gaetan Bisson, *Computing endomorphism rings of abelian varieties of dimension two*, Math. Comp. **84** (2015), no. 294, 1977–1989. MR 3335900

[BJS14] Jean-François Biasse, David Jao, and Anirudh Sankar, *A quantum algorithm for computing isogenies between supersingular elliptic curves*, Progress in Cryptology - INDOCRYPT 2014 - 15th International Conference on Cryptology in India, New Delhi, India, December 14-17, 2014, Proceedings, 2014, pp. 428–442.

[BJW17] Ernest Hunter Brooks, Dimitar Jetchev, and Benjamin Wesolowski, *Isogeny graphs of ordinary abelian varieties*, Res. Number Theory **3** (2017), Art. 28, 38. MR 3718564

[BL04] C. Birkenhake and H. Lange, *Complex abelian varieties*, second ed., Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 302, Springer Verlag, Berlin, 2004.

[BLS01] Dan Boneh, Ben Lynn, and Hovav Shacham, *Short signatures from the weil pairing*, Proceedings of the 7th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology (Berlin, Heidelberg), ASIACRYPT '01, Springer-Verlag, 2001, pp. 514–532.

[Can16] Luca Candelori, *The transformation laws of algebraic theta functions*, arXiv:1609.04486.

[CE15] Jean-Marc Couveignes and Tony Ezome, *Computing functions on Jacobians and their quotients*, LMS J. Comput. Math. **18** (2015), no. 1, 555–577. MR 3389883

[CFA+12] Henri Cohen, Gerhard Frey, Roberto Avanzi, Christophe Doche, Tanja Lange, Kim Nguyen, and Frederik Vercauteren, *Handbook of elliptic and hyperelliptic curve cryptography, second edition*, 2nd ed., Chapman & Hall/CRC, 2012.

[CKL08] Robert Carls, David Kohel, and David Lubicz, *Higher-dimensional 3-adic CM construction*, J. Algebra **319** (2008), no. 3, 971–1006. MR 2379090

[CL09] Robert Carls and David Lubicz, *A p-adic quasi-quadratic time point counting algorithm*, Int. Math. Res. Not. IMRN (2009), no. 4, 698–735. MR 2480098

[CNP05] G. Cardona, E. Nart, and J. Pujolas, *Curves of genus two over fields of even characteristic*, Mathematische Zeitschrift, 250:177–201 (2005).

[Cos11] R. Cosset, *Applications des fonctions theta a la cryptographie sur courbes hyperelliptiques*, Ph.D. thesis, Loria, Nancy, 2011.

[CQ05] G. Cardona and J. Quer, *Field of moduli and field of definition for curves of genus 2*, Lecture Notes Ser. Comput., 13:71–83 (2005).

[CR11] R. Cosset and D. Robert, *Computing (ℓ, ℓ)-isogenies in polynomial time on jacobians of genus 2 curves*, `http://eprint.iacr.org/2011/143`, 2011.

[DF17] L. De Feo, *Mathematics of isogeny based cryptography*, arXiv:1711.04062 (2017).

[DFJP14] Luca De Feo, David Jao, and Jérôme Plût, *Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies*, J. Math. Cryptol. **8** (2014), no. 3, 209–247. MR 3259113

[dG06] Maurice de Gosson, *Symplectic geometry and quantum mechanics*, Operator Theory: Advances and Applications, vol. 166, Birkhäuser Verlag, Basel, 2006, Advances in Partial Differential Equations (Basel). MR 2241188

[DG16] Christina Delfs and Steven D. Galbraith, *Computing isogenies between supersingular elliptic curves over $\mathbb{F}_p$*, Des. Codes Cryptogr. **78** (2016), no. 2, 425–440. MR 3451433

[DH76] Whitfield Diffie and Martin E. Hellman, *New directions in cryptography*, IEEE Trans. Information Theory **IT-22** (1976), no. 6, 644–654. MR 0437208

[Die06] Claus Diem, *An index calculus algorithm for plane curves of small degree*, Algorithmic Number Theory, 7th International Symposium, ANTS-VII, Berlin, Germany, July 23-28, 2006, Proceedings, 2006, pp. 543–557.

[DT08] Claus Diem and Emmanuel Thomé, *Index calculus in class groups of non-hyperelliptic curves of genus three*, J. Cryptology **21** (2008), no. 4, 593–611.

[EL10] Kirsten Eisenträger and Kristin Lauter, *A CRT algorithm for constructing genus 2 curves over finite fields*, Arithmetics, geometry, and coding theory (AGCT 2005), Sémin. Congr., vol. 21, Soc. Math. France, Paris, 2010, pp. 161–176. MR 2856565

[EvdGM] B. Edixhoven, G. van der Geer, and B. Moonen, *Abelian varieties*, Draft.

[Fio16] A. Fiorentino, *Weber's formula for the bitangents of a smooth plane quartic*, arXiv:1612.02049v1 (2016).

[FL08] David Freeman and Kristin Lauter, *Computing endomorphism rings of Jacobians of genus 2 curves over finite fields*, Algebraic geometry and its applications, Ser. Number Theory Appl., vol. 5, World Sci. Publ., Hackensack, NJ, 2008, pp. 29–66. MR 2484047

[Gal99] Steven D. Galbraith, *Constructing isogenies between elliptic curves over finite fields*, LMS J. Comput. Math. **2** (1999), 118–138. MR 1728955

[Gal12] ———, *Mathematics of public key cryptography*, 1st ed., Cambridge University Press, New York, NY, USA, 2012.

[GHK+06] P. Gaudry, T. Houtmann, D. Kohel, C. Ritzenthaler, and A. Weng, *The 2-adic CM method for genus 2 curves with application to cryptography*, Advances in cryptology—ASIACRYPT 2006, Lecture Notes in Comput. Sci., vol. 4284, Springer, Berlin, 2006, pp. 114–129. MR 2444631

[Gro60] A. Grothendieck, *Séminaire de géométrie algébrique*, Institut des Hautes Études Scientifiques, Paris, 1960/61, 1960. MR 0217088

[Gro61] ———, *Éléments de géométrie algébrique. III. Étude cohomologique des faisceaux cohérents. I*, Inst. Hautes Études Sci. Publ. Math. (1961), no. 11, 167.

[GTTD05] Pierrick Gaudry, Emmanuel Thomé, Nicolas Thériault, and Claus Diem, *A double large prime variation for small genus hyperelliptic index calculus*, Research Report RR-5764, INRIA, 2005.

[Gua11] J. Guardia, *On the Torelli problem and Jacobian Nullwerte in genus three*, Michigan Math. J. **60** (2011), no. 1, 51–65. MR 2785863

[Han06] Juncheol Han, *The general linear group over a ring*, Bull. Korean Math. Soc. **43** (2006), no. 3, 619–626. MR 2264921

[Har77] Robin Hartshorne, *Algebraic geometry*, Springer-Verlag, New York-Heidelberg, 1977, Graduate Texts in Mathematics, No. 52. MR 0463157

[HR83] Martin E. Hellman and Justin M. Reyneri, *Fast computation of discrete logarithms in $GF(q)$*, Springer US, 1983.

[Igu72] J.-I. Igusa, *Theta functions*, Grundlehren der mathematischen Wissenschaften, vol. 194, Springer, 1972.

[IT14] Sorina Ionica and Emmanuel Thomé, *Isogeny graphs with maximal real multiplication*, Cryptology ePrint Archive, Report 2014/230, 2014, `https://eprint.iacr.org/2014/230`.

[Jou04] Antoine Joux, *A one round protocol for tripartite Diffie-Hellman*, J. Cryptology **17** (2004), no. 4, 263–276. MR 2090557

[Jou13] Antoine Joux, *A new index calculus algorithm with complexity $l(1/4+o(1))$ in very small characteristic*, Cryptology ePrint Archive, Report 2013/095, 2013, `https://eprint.iacr.org/2013/095`.

[JW19] Dimitar Jetchev and Benjamin Wesolowski, *Horizontal isogeny graphs of ordinary abelian varieties and the discrete logarithm problem*, Acta Arith. **187** (2019), no. 4, 381–404. MR 3911698

[Kob87] Neal Koblitz, *Elliptic curve cryptosystems*, Math. Comp. **48** (1987), no. 177, 203–209. MR 866109

[Kob89] ———, *Hyperelliptic cryptosystems*, J. Cryptology **1** (1989), no. 3, 139–150. MR 1007215

[Koh96] David Russell Kohel, *Endomorphism rings of elliptic curves over finite fields*, ProQuest LLC, Ann Arbor, MI, 1996, Thesis (Ph.D.)–University of California, Berkeley. MR 2695524

[Kra22] Maurice Kraitchik, *Théorie des nombres*, Gauthier-Villars (1922).

[Lan82] S. Lang, *Introduction to algebraic and abelian functions*, Springer Verlag, New York NY, 1982.

[LR12] D. Lubicz and D. Robert, *Computing isogenies between abelian varieties*, Compos. Math. **148** (2012), no. 5, 1483–1515.

[Mar18] Chloe Martindale, *Isogeny graphs, modular polynomials, and applications*, 2018, Thesis (Ph.D.).

[Mes91] Jean-François Mestre, *Construction de courbes de genre* 2 *à partir de leurs modules*, Effective methods in algebraic geometry (Castiglioncello, 1990), Progr. Math., vol. 94, Birkhäuser Boston, Boston, MA, 1991, pp. 313–334. MR 1106431

[Mil86] J. S. Milne, *Abelian varieties*, Arithmetic geometry (Storrs, Conn., 1984), Springer, New York, 1986, pp. 103–150.

[Mil17] Enea Milio, *Computing isogenies between jacobian of curves of genus 2 and 3*, arXiv:1709.06063.

[MOV91] Alfred Menezes, Tatsuaki Okamoto, and Scott Vanstone, *Reducing elliptic curve logarithms to logarithms in a finite field*, Proceedings of the Twenty-third Annual ACM Symposium on Theory of Computing (New York, NY, USA), STOC '91, ACM, 1991, pp. 80–89.

[MR17] Enea Milio and Damien Robert, *Modular polynomials on Hilbert surfaces*, working paper or preprint, September 2017.

[Mum66] D. Mumford, *On the equations defining abelian varieties. I*, Invent. Math. **1** (1966), 287–354.

[Mum67a] ———, *On the equations defining abelian varieties. II*, Invent. Math. **3** (1967), 75–135.

[Mum67b] ———, *On the equations defining abelian varieties. III*, Invent. Math. **3** (1967), 215–244.

[Mum70] David Mumford, *Abelian varieties*, Tata Institute of Fundamental Research Studies in Mathematics, vol. 5, Published for the Tata Institute of Fundamental Research, Bombay, 1970.

[Mum83] ———, *Tata lectures on theta. I*, Modern Birkhäuser Classics, Birkhäuser Boston, Inc., Boston, MA, 1983, With the collaboration of C. Musili, M. Nori, E. Previato and M. Stillman, Reprint of the 1983 edition.

[Mum84] ———, *Tata lectures on theta. II*, Modern Birkhäuser Classics, Birkhäuser Boston, Inc., Boston, MA, 1984, 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 original.

[Neu99] Jürgen Neukirch, *Algebraic number theory*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 322, Springer-Verlag, Berlin, 1999, Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder. MR 1697859

[NR17] Enric Nart and Christophe Ritzenthaler, *A new proof of a Thomae-like formula for non hyperelliptic genus 3 curves*, Arithmetic, geometry, cryptography and coding theory, Contemp. Math., vol. 686, Amer. Math. Soc., Providence, RI, 2017, pp. 137–155. MR 3630613

[Oor07] F. Oort, *Abelian varieties over finite fields*, Higher-dimensional varieties over finite fields, Summer school in Goettingen (2007).

[PH78] Stephen C. Pohlig and Martin E. Hellman, *An improved algorithm for computing logarithms over* GF(p) *and its cryptographic significance*, IEEE Trans. Information Theory **IT-24** (1978), no. 1, 106–110. MR 0484737

[Pol78] J. M. Pollard, *Monte Carlo methods for index computation* (mod p), Math. Comp. **32** (1978), no. 143, 918–924. MR 0491431

[Ric37a] Fried. Jul. Richelot, *De transformatione integralium Abelianorum primi ordinis commentatio*, J. Reine Angew. Math. **16** (1837), 221–284. MR 1578134

[Ric37b] ———, *De transformatione integralium Abelianorum primi ordinis commentatio. Caput secundum. De computatione integralium Abelianorum primi ordinis*, J. Reine Angew. Math. **16** (1837), 285–341. MR 1578135

[Rit04] Christophe Ritzenthaler, *Point counting on genus 3 non hyperelliptic curves*, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 3076, Springer, Berlin, 2004, pp. 379–394. MR 2138009

[Rob10] D. Robert, *Fonctions thêta et applications à la cryptologie*, Ph.D. thesis, Nancy, 2010.

[Sie21] Carl Siegel, *Darstellung total positiver Zahlen durch Quadrate*, Math. Z. **11** (1921), no. 3-4, 246–275. MR 1544496

[Smi09] Benjamin Smith, *Isogenies and the discrete logarithm problem in Jacobians of genus 3 hyperelliptic curves*, J. Cryptology **22** (2009), no. 4, 505–529. MR 2525710

[Spr19] Caleb Springer, *Computing the endomorphism ring of an ordinary abelian surface over a finite field*, Journal of Number Theory (2019).

[Str10] M. Streng, *Complex multiplication of abelian surfaces*, Ph.D. thesis, Universiteit Leiden, 2010.

[Tat66] John Tate, *Endomorphisms of abelian varieties over finite fields*, Invent. Math. **2** (1966), 134–144. MR 0206004

[Tho70] J. Thomae, *Beitrag zur Bestimmung von θ(0,...,0) durch die Klassenmoduln algebraischer Funktionen*, Journal fur die Reine und Angewandte Mathematik (1870), 70:201–222.

[vW98] Paul van Wamelen, *Equations for the Jacobian of a hyperelliptic curve*, Trans. Amer. Math. Soc. **350** (1998), 3083–3106.

[vW99] ———, *Examples of genus two CM curves defined over the rationals*, Math. Comp. **68** (1999), no. 225, 307–320. MR 1609658

[Wat69] William C. Waterhouse, *Abelian varieties over finite fields*, Ann. Sci. École Norm. Sup. (4) **2** (1969), 521–560. MR 0265369

[Web76] H. M. Weber, *Theorie der Abelschen Functionen vom Geschlecht 3*, Berlin: Druck und Verlag von Georg Reimer (1876).

[Wen03] Annegret Weng, *Constructing hyperelliptic curves of genus 2 suitable for cryptography*, Math. Comp. **72** (2003), no. 241, 435–458. MR 1933830

Marius Vuille

Bergluftweg 11,
2505 Biel, Switzerland,
marius_vuille@hotmail.com,
+41 78 861 27 29

Personal Profile

I am a PhD candidate in mathematics at EPFL in Lausanne, Switzerland. My research focuses on cryptography and arithmetic geometry, and more precisely on computing isogenies between abelian varieties over finite fields, and the associated isogeny graphs.

Education

10/2014-present	**PhD candidate in mathematics**, EPFL, under the supervision of Prof. Dimitar Jetchev
2012-2014	**MSc in mathematics**, EPFL and University of Amsterdam
2009-2012	**BSc in mathematics,** EPFL
2005-2008	**High school**, Gymnasium Alpenstrasse, Biel, bilingual studies (german/french)

Professional experiences

2011-present — **EPFL,** teaching assistant

- Various undergraduate classes such as Geometry, Linear Algebra, Calculus, Group and Ring theory
- MSc class in Number theory and cryptanalysis, including theoretical and programming assignments
- MSc class in Algebraic curves for cryptography, including theoretical and programming assignments

08/2013-01/2014 — **Ecole Sofia**, Lausanne

- Teaching mathematics on high school level, 10 lessons per week
- Teaching german for secondary level students, 2 lessons per week

Languages

German : native
French : professional level
English : professional level

Programming skills

Advanced knowledge in SageMath (Python) and Magma, programming is part of my PhD project
Good knowledge in C++ (class at EPFL)
Daily use of LaTeX

Publications

Cyclic Isogenies for Abelian Varieties with Real Multiplication (joint with A. Dudeanu, D. Jetchev and D.Robert)
https://arxiv.org/abs/1710.05147

Invited Talks

- Graduate Colloquium (Uni Fribourg), 09/2016, *Towards Hyperelliptic Curve Cryptography*
- PhD Seminar (Uni Basel), 03/2017, *Using Hyperelliptic Curves in Cryptography*
- Arithmetic, Geometry, Cryptography and Coding Theory (CIRM, Marseille), 06/2017, *Computing Cyclic Isogenies between Abelian Varieties over Finite Fields*
- Séminaire de géométrie et d'algèbre effectives (Uni Rennes), 02/2017, *Computing Cyclic Isogenies between Principally Polarized Abelian Varieties over Finite Fields*