Jacobians isomorphic to a product of two elliptic curves

Ernst Kani

1 Introduction

In 1965 Hayashida and Nishi initiated the study of genus 2 curves C whose Jacobian J_C is isomorphic to a product $A = E_1 \times E_2$ of two elliptic curves. In their papers [12], [14] and [13], they determined the number of curves C with $J_C \simeq A$ for a fixed A in many cases, thereby exhibiting the existence of such curves. A similar count was done for supersingular curves by Ibukiyama, Katsura and Oort[16].

Recently there has been renewed interest in such curves, particularly in connection with moduli problems; cf. Earle[6], Lange[26], and McMullen[28], [29].

The purpose of this article is determine how such curves are distributed in the moduli space M_2 of genus 2 curves over an algebraically closed field K. By a result of Lange[25] it is known that these lie on infinitely many curves in M_2; see also [6]. Here we want to make the nature of these curves precise.

To this end, let us say that a curve C *has type* d if $J_C \simeq E_1 \times E_2$, where E_1 and E_2 are connected by a cyclic isogeny of degree d. (If E_1 has CM or is supersingular, then this definition has to slightly modified; see §4 below.) Since every curve C with $J_C \simeq E_1 \times E_2$ has some type $d \geq 1$ (cf. Proposition 25), the following result describes the set of all such curves in M_2:

Theorem 1 *The set $T(d) \subset M_2$ of curves of type d is a closed subset of M_2. If $T(d)$ is non-empty, then $T(d)$ is a finite union of irreducible curves. Moreover, if $\mathrm{char}(K) \nmid d$, then each such component is birationally isomorphic either to the modular curve $X_0(d)^+$ or to a degree 2 quotient thereof.*

Here $X_0(d)^+ = X_0(d)/\langle w_d \rangle$ is (as in [27], p. 145) the quotient of the usual modular curve $X_0(d)$ by the Fricke involution w_d.

The key tool for proving this and other related results is the concept of a "generalized Humbert variety" which is introduced here. This generalizes the *Humbert surfaces* of Humbert and is based on a *refinement* of the usual Humbert invariant (cf. [35]) that was suggested in [19]. There it was observed that each curve C comes equipped with a canonically defined positive definite quadratic form q_C which can be used to define the Humbert invariant (and hence Humbert surfaces).

It turns out that the curves C of type d can be characterized by a property of their associated *refined Humbert invariant* q_C as defined in §2. To formulate this property in a convenient manner, let us say that a positive definite binary quadratic form q

has type d if it has discriminant $-16d$ and is either primitive and lies in the principal genus (but q is not equivalent to the principal (norm) form) or else $q = 4q_1$, where q_1 is primitive (of discriminant $-d$) and lies in the principal genus. (Such quadratic forms are studied in detail in §5.) We then have:

Theorem 2 *If C is a curve of genus 2, then C has type d if and only if its refined Humbert invariant q_C primitively represents a form of type d.*

In view of this, we might expect the various forms q of type d to give us the components of the curve $T(d)$, and this is indeed the case. To make this precise, let $H(q)$ denote the set of isomorphism classes of curves C in the moduli space M_2 such that q_C represents q primitively; we call $H(q)$ the *generalized Humbert variety* associated to q; cf. §3. Thus, Theorem 2 can be restated in terms of the $H(q)$'s; cf. Theorem 13 (which is a refinement of Theorem 2). If $\bar{Q}_d^*$ denotes the set of $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes of forms of type d, then we prove in §8:

Theorem 3 *If $\mathrm{char}(K) \nmid d$, then the $H(q)$, where $q \in \bar{Q}_d^*$, are precisely the irreducible components of $T(d)$. Thus $T(d)$ has precisely $t^*(d) := \#\bar{Q}_d^*$ irreducible components.*

The precise birational structure of the curves $H(q)$ depends on whether or not q is an *ambiguous form*, i.e. on whether or not q has order 2 in the group $\bar{Q}_{-16d}$ of equivalence classes of primitive forms of discriminant $-16d$. (In the case that $q' = \frac{1}{4}q$ is primitive of discriminant $-d$, then this means that q' has order 2 in $\bar{Q}_{-d}$.)

Theorem 4 *Let $q \in \bar{Q}_d^*$. If q is not an ambiguous class, then $H(q) \sim X_0(d)^+$; otherwise $H(q) \sim X_0(d)^+/\langle\alpha_q\rangle$, where α_q is a suitable Atkin-Lehner involution.*

This result is made more precise in §10, where an explicit recipe for the Atkin-Lehner involution α_q is given; cf. Proposition 53 and Theorem 55. Note that it can happen in certain cases that α_q acts trivially on $X_0(d)^+$; these cases are analyzed there as well.

An interesting but difficult question is to characterize the $d's$ for which there is no curve of type d, i.e. to determine the d's for which $T(d)$ is empty or, equivalently, for which $t^*(d) = 0$. Now from its definition one might expect that $t^*(d)$ could be expressed in terms of suitable class numbers of binary quadratic forms, or more precisely, in terms of the number $\bar{h}(D) = h(D)/g(D)$ of (proper) equivalence classes of forms in the principal genus of discriminate $D = -16d$. This is essentially correct, but the formula is complicated by the fact that we need to count forms up to $\mathrm{GL}_2(\mathbb{Z})$-equivalence instead of the more usual $\mathrm{SL}_2(\mathbb{Z})$-equivalence, and so one also needs to know the number of *spinor genera* of discriminant $-16d$; cf. Remark 35.

Nevertheless, one has that the condition $t^*(d) = 0$ is essentially equivalent to the condition that $\bar{h}(-16d) = 1$ (cf. Corollary 34), and hence the precise determination of the exceptional d's hinges on the solution of a classical problem in number theory which was first raised by Gauss. Indeed, Gauss[10], Art. 303, conjectured not only that there are only finitely many d's with $h(-4d) = 1$ but also that the same is true for $\bar{h}(-4d) = 1$, and this was later proven by Chowla[3] in 1934. Moreover, Gauss also conjectured that such d's satisfy $d \leq 1848$, but this does not seem to have been proved unconditionally yet (even though his class-number 1 conjecture has been settled). Nevertheless, Weinberger[37] has shown that Gauss's conjecture follows from the Generalized Riemann Hypothesis (GRH). We thus prove in §7:

Corollary 5 *$T(d)$ is empty for the following* 21 *values of* $d \geq 1$*:*

(1) $d = 1, 2, 4, 6, 10, 12, 18, 22, 28, 30, 42, 58, 60, 70, 78, 102, 130, 190, 210, 330, 462.$

If Gauss's Conjecture is true, then these are all the d's for which $T(d) = \emptyset$. In particular, there are only finitely many d's for which $T(d) = \emptyset$, and these are all given by (1) *if* (GRH) *holds.*

Note that the above result can also be viewed as an *existence theorem*, and hence as a refinement of the work of Hayashida[12]; cf. Remark 42.

Finally, it should be mentioned that there is a close connection between the results obtained here and the study of elliptic subcovers $f : C \to E$ of genus 2 curves, as is explained in [8], §6.

Acknowledgements. I would like to thank Gerd Frey for the many stimulating discussions which we had about this work. In addition, I would like to gratefully acknowledge receipt of funding from the from the Natural Sciences and Engineering Research Council of Canada (NSERC).

2 The refined Humbert invariant

Let A be an abelian surface over an algebraically closed field K of arbitrary characteristic, and assume that A has a principal polarization $\theta \in \mathrm{NS}(A) = \mathrm{Div}(A)/\equiv$, where $\equiv$ denotes numerical equivalence. Thus, $\theta = cl(D)$, where $D \in \mathrm{Div}(A)$ is an ample divisor with self-intersection number $(D.D) = 2$. Put

(2) $$q_{(A,\theta)}(D) = (D.\theta)^2 - 2(D.D), \quad \text{for } D \in \mathrm{NS}(A),$$

where (.) denotes the intersection number of divisors. From the Hodge index theorem it follows easily that $q_{(A,\theta)}$ defines a positive definite quadratic form on the quotient group $\mathrm{NS}(A, \theta) = \mathrm{NS}(A)/\mathbb{Z}\theta$; cf. [19], §3. Since $\mathrm{NS}(A, \theta) \simeq \mathbb{Z}^{\rho-1}$, where $\rho = \mathrm{rk}(\mathrm{NS})$ is the Picard number, we see that $q_{(A,\theta)}$ defines an (equivalence class of) integral, positive definite quadratic form(s) in $\rho - 1$ variables, which will be called the *refined Humbert invariant* of the principally polarized abelian variety (A, θ).

As was explained in [19], §5, $q_{(A,\theta)}$ is closely related to the classical *Humbert invariant* attached to an abelian surface $A/\mathbb{C}$: indeed, any number Δ which is *primitively represented* by $q_{(A,\theta)}$ is a (classical) Humbert invariant of the principally polarized abelian surface (A, θ). It thus follows that the subset

$$H_\Delta = \{\langle A, \theta\rangle \in A_2(K) : q_{(A,\theta)} \text{ primitively represents } \Delta\}$$

of the moduli space A_2 (which classifies isomorphism classes $\langle A, \theta\rangle$ of principally polarized abelian surfaces) is precisely the *Humbert surface* of *discriminant* (or invariant) Δ as defined by Humbert[15] or [35], §IX.2. By Humbert, this defines an irreducible surface in $A_2(\mathbb{C})$ whenever $\Delta \equiv 0, 1 \pmod 4$, and is empty otherwise.

As was indicated in the introduction, we are primarily interested in the principally polarized abelian varieties that arise as Jacobians of (irreducible) genus 2 curves. Now if M_2 denotes the moduli space of smooth, irreducible genus 2 curves, then we have Jacobi morphism $j_2 : M_2 \to A_2$ which takes a curve C to its principally polarized Jacobian (J_C, θ_C) in $A_2(K)$. (Note that θ_C is the class of a curve isomorphic to C.)

Over $\mathbb{C}$, it is a classical fact (cf. Humbert[15], §17, or Krazer[23], p. 485) that the complement $A_2 \setminus j_2(M_2)$ is the Humbert surface H_1 of invariant 1. By a result of Weil[36], this is true over an arbitrary field, as we now show:

Proposition 6 *Let $\langle A, \theta\rangle \in A_2(K)$. Then $\langle A, \theta\rangle \notin j_2(M_2(K))$ if and only if $q_{(A,\theta)}$ represents* 1, *i.e. $q_{(A,\theta)}(D) = 1$, for some $D \in \mathrm{NS}(A)$. Thus*

$$A_2 \setminus j_2(M_2) = H_1.$$

Proof. By Weil[36], Satz 2, we have that $\langle A, \theta\rangle \notin j_2(M_2)$ if and only if $(A, \theta) \simeq (E_1 \times E_2, \theta_1 + \theta_2)$ is a product of two elliptic curves and $\theta = \theta_1 + \theta_2$ is the product polarization (where $\theta_i = cl(pr_i^*(0_{E_i}))$, for $i = 1, 2$).

Now if $(A, \theta) \simeq (E_1 \times E_2, \theta_1 + \theta_2)$, then $(\theta.\theta_i) = 1$, $(\theta_i.\theta_i) = 0$ and so $q_{(A,\theta)}(\theta_i) = 1$.

Conversely, suppose $q_{(A,\theta)}(D) = 1$ for some D. Then D is necessarily primitive, for if $D = mD'$ with $D' \in \mathrm{NS}(A)$, then $1 = q_\theta(D) = m^2 q_\theta(D')$, and so $m = \pm 1$, i.e. D is primitive. Thus, by [19], Theorem 3.1, there exists an elliptic curve E on A with $(E.\theta) = 1$. Put $\theta_1 = \theta - cl(E)$. Then $\theta_1^2 = \theta^2 - 2(\theta.E) + E^2 = 0$, and so $\theta_1 = cl(mE')$, for some elliptic curve E' on A and some $m \in \mathbb{Z}$; cf. [19], Prop. 2.3. But since $\theta = cl(E + mE')$, we have $2 = \theta^2 = 2m(E.E')$, so $m = 1$. Thus $\theta = cl(E + E')$. By Weil[36], Satz 2, we have that $(A, \theta) \simeq (E_1 \times E_2, \theta_1 + \theta_2)$ with $\theta_i = pr_i^*(0_{E_i})$, $i = 1, 2$, and so the assertion follows.

Remark 7 The above shows that the rule $(E_1, E_2) \mapsto \langle E_1 \times E_2, pr_1^* 0_{E_1} + pr_2^* 0_{E_2}\rangle$ defines a surjection $A_1 \times A_1 \to H_1$, where A_1 denotes the moduli space of elliptic curves. It not difficult to see (by an argument similar to that of the proof of Proposition 43) that this map is a *proper* morphism, and so $j_2(A_2)$ is an open subset of A_2. Since j_2 is birational, it thus follows (by Zariski's Main Theorem) that j_2 is an open immersion. Note that by Oort/Steenbrink[34], the Torelli map $j_g : M_g \to A_g$ need not be an immersion if $g \geq 5$ and $\mathrm{char}(K) \neq 0$.

3 Generalized Humbert varieties

The definition of a Humbert surface can be generalized as follows. Given any integral positive definite quadratic form q, let

$$H(q) = \{\langle A, \theta\rangle \in A_2(K) : q_{(A,\theta)} \text{ primitively represents } q\}.$$

Since clearly $H(\Delta x^2) = H_\Delta$ and since it can be shown (cf. [21]) that $H(q)$ is always an algebraic subset of M_2, we shall call $H(q)$ a *generalized Humbert variety* of A_2.

The $H(q)$'s can be used to describe intersections of Humbert surfaces:

Proposition 8 *If m and n are distinct positive integers, then*

$$H_m \cap H_n = \bigcup_q H(q), \tag{3}$$

where the union runs over all equivalence classes of positive definite binary quadratic forms q which primitively represent both m and n.

Proof. Let q be such a form, and let $\langle A, \theta\rangle \in H(q)$. Then $q_{(A,\theta)}$ primitively represents q. Since m is primitively represented by q, it follows that m also primitively represented by $q_{(A,\theta)}$, so $\langle A, \theta\rangle \in H_m$. Thus $H(q) \subset H_m$, and similarly, $H(q) \subset H_n$, so $H(q) \subset H_n \cap H_m$. This shows that the right side of (3) is contained in the left side.

Conversely, suppose $\langle A, \theta\rangle \in H_m \cap H_n$. Then there exist primitive vectors $v, w \in M := \mathrm{NS}(A, \theta)$ such that $q_{(A,\theta)}(v) = m$ and $q_{(A,\theta)}(w) = n$. If v and w were linearly dependent, then $v = \pm w$ and hence $q_{(A,\theta)}(v) = q_{(A,\theta)}(w)$, contrary to the hypothesis. Thus, v and w are linearly independent and hence $M_0 := \mathbb{Z}v + \mathbb{Z}w$ has rank 2. Let M_1 be the saturation of M_0 in M. Then the restriction q of $q_{(A,\theta)}$ to M_1 is a positive definite, binary quadratic form which is primitively represented by $q_{(A,\theta)}$, and so $\langle A, \theta\rangle \in H(q)$. Moreover, $m = q(v)$ is primitively represented by q (because v is primitive in M, hence also in M_1. Similarly, $n = q(w)$ is primitively represented by q. Thus q is one of the forms of the right side of (3), so $\langle A, \theta\rangle \in \cup H(q)$.

Remark 9 (a) Note that there are only finitely many equivalence classes of forms q satisfying the conditions of Proposition 8 because their discriminants are bounded: $|\mathrm{disc}(q)| \leq 4mn$.

(b) The above proposition and Humbert's results imply that $\dim \overline{H(q)} \leq 1$, for all *binary* positive-definite quadratic forms q.

(c) The above proposition can be viewed as giving a partial answer to a question raised by McMullen[28], p. 96.

In the sequel we shall need to work out the refined Humbert invariant in many cases, and for this it is useful to know its discriminant/determinant. (Here, as usual, the determinant $\det(M,\beta)$ of a bilinear module (M,β) is the determinant of any Gram matrix $(\beta(x_i,x_j))$ associated to a basis $\{x_i\}$ of M, and the determinant $\det(M,q)$ of a quadratic module (M,q) is the determinant of the associated bilinear module (M,β_q), where β_q is the bilinear form associated to q.) It turns out that it is closely related to that of the Néron-Severi group, viewed as bilinear module via the intersection pairing:

Proposition 10 *Let* $\rho = \mathrm{rank}(\mathrm{NS}(A))$*. Then the determinant of the quadratic module* $(\mathrm{NS}(A,\theta), q_{(A,\theta)})$ *is related to that of the Néron-Severi group by the formula*

$$\det(\mathrm{NS}(A,\theta), q_{(A,\theta)}) = \tfrac{1}{2}(-4)^{\rho-1}\det(\mathrm{NS}(A),(.)).$$

Proof. Let $\beta = \beta_A$ denote the intersection pairing on $\mathrm{NS}(A)$, and let $M_0 = \{(x.\theta)\theta - 2x : x \in \mathrm{NS}(A)\}$. Clearly, $(y.\theta) = 0$, if $y \in M_0$, i.e. $M_0 \perp \mathbb{Z}\theta$. Thus, if we put $M = M_0 + \mathbb{Z}\theta$, then $\det(\beta_{|M}) = 2\det(\beta_{|M_0})$, where $\beta_{|M} = \beta_{|M\times M}$ (and $\beta_{|M_0} = \beta_{|M_0\times M_0}$). Moreover, since $M \supset 2\mathrm{NS}(A)$, we see that M has finite index in $\mathrm{NS}(A)$, and so $\det(\beta_{|M}) = n^2\det(\beta)$, where $n = [\mathrm{NS}(A) : M]$. Similarly, if we put $\bar{M} = M/\mathbb{Z}\theta$, then $[\mathrm{NS}(A,\theta) : \bar{M}] = [\mathrm{NS}(A) : M] = n$, and so $\det((\beta_{\bar{q}})_{|\bar{M}}) = n^2\det(\beta_{\bar{q}})$, where $\bar{q} = q_\theta$. Now for $y_i \in M_0$ we have $\beta_{\bar{q}}(y_1,y_1) = -4\beta(y_1,y_2)$, and hence $\det((\beta_{\bar{q}})_{|\bar{M}}) = (-4)^s\det(\beta_{|M_0})$, where $s = \mathrm{rank}(M_0)$. (Note that if $x_1,\ldots,x_s$ form a basis of M_0, then their images in $\bar{M}$ form a basis of $\bar{M}$.) Since $s = \rho - 1$, we thus obtain

$$\det(\beta_{\bar{q}}) = \frac{1}{n^2}\det((\beta_{\bar{q}})_{|\bar{M}}) = \frac{(-4)^{\rho-1}}{n^2}\det(\beta_{|M_0}) = \frac{(-4)^{\rho-1}}{2n^2}\det(\beta_{|M}) = \frac{(-4)^{\rho-1}}{2}\det(\beta).$$

4 Curves of type d

We now focus our attention to those curves C of genus 2 whose Jacobian J_C is isomorphic to a product of two elliptic curves. As we shall see below (cf. Proposition 25), these can be classified by an integer d called its *type*, which is defined as follows.

Definition. Let $d \geq 1$ be an integer. A curve C is said to have *type d* if there exist two elliptic curves E_1, E_2, a cyclic isogeny $h : E_1 \to E_2$ of degree $d = \deg(h)$ and an isomorphism $\alpha : J_C \xrightarrow{\sim} E_1 \times E_2$ such that

$$\theta_C \equiv \alpha^*(a\theta_1 + b\theta_2 + c\Gamma_h), \quad \text{for some } a,b,c \in \mathbb{Z}, \tag{4}$$

where $\theta_i = pr_i^*(0_{E_i})$, for $i = 1,2$, and $\Gamma_h \subset E_1 \times E_2$ denotes the graph of h. We denote the set of isomorphism classes $\langle C\rangle$ of curves C of type d by $T(d) \subset M_2(K)$.

Remark 11 Suppose that $J_C \simeq E_1 \times E_2$. If E_1 has no complex multiplication (i.e. if $\mathrm{End}(E_1) = \mathbb{Z}$), then its type d is uniquely determined by C by the formula $\det(\mathrm{NS}(J_C)) = 2d$, as we shall see below (cf. Corollary 26). In the other cases, however, C may have several types associated to it.

The first main result is that curves of type d can be characterized by a property of the refined Humbert invariant $q_C := q_{(J_C,\theta_C)}$ associated to C. To formulate this in a simple manner, we first introduce the following class of binary quadratic forms.

Definition. Let $d \geq 1$ be an integer. An integral quadratic form q is said to be of *type* d if it is binary, positive-definite of discriminant $-16d$, and if:

• either q is primitive and in the principal genus (i.e. $q \sim q_1^2$, for some primitive form q_1 of discriminant $-16d$) but not principal (i.e $q \not\sim x^2 + 4dy^2$),

• or $q = 4q_1$, for some primitive form q_1 of discriminant $-d \equiv 1 \pmod 4$ which is in the principal genus.

Remark 12 Since $\mathrm{NS}(J_C, \theta_C)$ does not come with an explicit basis, the quadratic form q_C is only defined up to $\mathrm{GL}_n(\mathbb{Z})$-equivalence, where $n = \mathrm{rk}(\mathrm{NS}(J_C, \theta_C))$. However, when dealing with binary quadratic forms, it is better to use *proper* (or $\mathrm{SL}_2(\mathbb{Z})$)-equivalence since the proper equivalence classes (of fixed discriminant) form a group. We shall denote proper equivalence throughout by the symbol $\sim$, and use $\approx$ for $\mathrm{GL}_n(\mathbb{Z})$-equivalence. Note that for primitive binary quadratic forms we have $q_1 \approx q_2 \Leftrightarrow q_1 \sim q_2$ or $q_1 \sim q_2^{-1}$, and so the above conditions do not depend on the choice of the representative q of the $\mathrm{GL}_2(\mathbb{Z})$-equivalence class.

The following basic result is a restatement of Theorem 2 of the introduction; it relates *curves* of type d to *forms* of type d.

Theorem 13 *A curve C has type d if and only $\langle C \rangle \in H(q)$, for some quadratic form q of type d. Thus*

$$T(d) = \bigcup_{q \in \bar{Q}_d^*} H(q),$$

where $\bar{Q}_d^*$ denotes the set of $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes of forms of type d.

The proof of this theorem will be deferred until section 6 since it requires some basic facts about forms of type d which will be presented in the next section. In section 7 we shall also prove an *existence theorem* which shows that $H(q)$ is non-empty whenever q is a form of type d; cf. Theorem 30.

5 Quadratic forms of type d

This section is devoted to a detailed study of the (binary) quadratic forms of type d which were introduced in the previous section. In particular, it will be shown that each proper equivalence class of such forms can be represented by a "standard prototype" q_s which is associated to a solution $s = (n_1, n_2, k)$ of the equation

$$n_1 n_2 - k^2 d = 1. \tag{5}$$

To define these prototypes, we first introduce some notation.

Notation. Fix an integer $d \geq 1$, and let

$$P(d) = \{(n_1, n_2, k) \in \mathbb{Z}^3 : n_1 > 0,\ n_2 > 0,\ n_1 n_2 - k^2 d = 1\}$$

denote the set of solutions of (5) with positive n_i's. It is convenient to split $P(d)$ into two parts: $P(d) = P(d)^{odd} \,\dot\cup\, P(d)^{even}$, where $P(d)^{even} = \{(n_1, n_2, k) \in P(d) : 2|n_1, 2|n_2\}$.

For a given discriminant $D \equiv 0, 1 \pmod 4$ and an integer n, let

$$Q_D^{(n)} = \{[a, b, c] \in \mathbb{Z}^3 : a > 0, b^2 - 4ac = D,\ \gcd(a, b, c)|n\}$$

denote the set of binary quadratic forms of discriminant D whose *content* $\gcd(a, b, c)$ divides n. Here, as usual, we identify $[a, b, c]$ with the quadratic form $ax^2 + bxy + cy^2$.

We first note that the set $P(d)$ of solutions of (5) can be identified with a suitable set of quadratic forms of discriminant $-4d$:

Lemma 14 *The assignment $(n_1, n_2, k) \mapsto [n_1 d, 2kd, n_2]$ induces a bijection*

$$f_d : P(d) \xrightarrow{\sim} Q_{-4d}^{(2)}(d) := \{[a, b, c] \in Q_{-4d}^{(2)} : d|a,\ 2d|b\}.$$

Moreover, $f_d(n_1, n_2, k)$ is primitive if and only if $\gcd(n_1, n_2, 2) = 1$.

Proof. If $s = (n_1, n_2, k) \in P(d)$, then $\operatorname{disc}(f_d(s)) = (2dk)^2 - 4(n_1 d)n_2 = 4d(dk^2 - n_1 n_2) = -4d$. Furthermore, since $\gcd(n_1 n_2, k^2 d) = 1$ by (5), we have $\gcd(n_1 d, 2kd, n_2) = \gcd(n_1, n_2, 2)|2$, so $f_d(s) \in Q_{-4d}^{(2)}(d)$. (In particular, $f_d(s)$ is primitive if and only if $\gcd(n_1, n_2, 2) = 1$.) Conversely, if $\operatorname{disc}([n_1 d, 2dk, n_2]) = -4d$, then $n_1 n_2 - k^2 d = 1$, so $(n_1, n_2, k) \in P(d)$.

We now study quadratic forms of the following type. For $s = (n_1, n_2, k) \in P(d)$, put

$$q_s(x, y) = n_2^2 x^2 - 2k(t - d)xy + n_1^2 t y^2, \quad \text{where } t = d(n_1 n_2 + 3). \tag{6}$$

Using (5) and the definition of t, we see that

$$k^2 (t - d)^2 + 4d = n_1^2 n_2^2 t, \tag{7}$$

and so $\mathrm{disc}(q_s) = -16d$. As we shall see presently, q_s is always a form of type d, provided that q_s is not in the principal class. The converse is also true (up to proper equivalence), but is harder to prove:

Proposition 15 *If $s = (n_1, n_2, k) \in P(d)$, then q_s has type d, provided that q_s is not equivalent to the principal form. Conversely, if q is any form of type d, then there exists $s \in P(d)$ such that q is properly equivalent to q_s.*

The easy direction of this result is contained in the following more precise assertion.

Lemma 16 *Let $s = (n_1, n_2, k) \in P(d)$ and put $t = d(n_1 n_2 + 3)$.*

(a) If n_2 is odd, then $\tilde{q}_s := [n_2, 2k(t-d), n_2 n_1^2 t] \in Q^{(1)}_{-16d}$ and

$$q_s \sim \tilde{q}_s \circ \tilde{q}_s \quad \text{and} \quad \tilde{q}_s \circ 1_{-4d} \sim f_d(s). \tag{8}$$

Here $1_{-4d} = [1, 0, d]$ denotes the principal form of discriminant $-4d$, $\circ$ denotes the composition of binary forms, and $\sim$ denotes proper equivalence.

(b) If n_1 and n_2 are even, then $q_s = 4q'(s)$ with $q'_s \in Q^{(1)}_{-d}$. Moreover, $f_d(s) = 2f'_d(s)$ with $f'_d(s) \in Q^{(1)}_{-d}$ and we have

$$q'_s \sim f'_d(s) \circ f'_d(s). \tag{9}$$

Proof. (a) From (7) we see that $\mathrm{disc}(\tilde{q}_s) = -16d$, and so $\tilde{q}_s \in Q^{(1)}_{-16d}$ because $\gcd(n_2, -16d) = \gcd(n_2, 2) = 1$. By the proof of [7], Lemma 1, it thus follows that $\tilde{q}_s \circ \tilde{q}_s \sim q_s$. The second formula of (8) follows directly from the composition formula of Arndt applied to $\tilde{q}_s$ and $[d, 0, 1] \sim 1_{-4d}$; cf. [2], p. 129. (Note that $B = 2kd$ satisfies the required congruences.)

(b) Here k, d and hence t are odd, so $t - d = 2t_1$ is even; More precisely, $t_1 = d(2ab+1)$, where $a = \frac{n_2}{2}$ and $b = \frac{n_1}{2}$. Thus $q_s = 4q'_s$ where $q'_s = [a^2, -kt_1, tb^2]$. Clearly, $\mathrm{disc}(q'_s) = \frac{1}{16}\mathrm{disc}(q_s) = -d$, so in particular $-d \equiv 1 \pmod 4$. Since $\gcd(a, -d) = 1$, we see that $q'_s \in \mathbb{Q}^{(1)}_{-d}$. Similarly, $f_d(s) = 2f'_d(s)$ with $f'_d(s) = [bd, kd, a] \in Q^{(1)}_{-d}$ (because $\gcd(a, -d) = 1$).

To prove (9), put $\tilde{q}'_s = [a, -kt_1, abt] \in Q^{(1)}_{-d}$. Since $\gcd(a, d) = 1$, we have again by [7], Lemma 1, that $\tilde{q}'_s \circ \tilde{q}'_s \sim q'_s$. Now $\tilde{q}'_s \sim f'_d(s)$ because if we let $y = -kdb$, then the matrix $g = \left(\begin{smallmatrix} 1 & y \\ 0 & 1 \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ transforms $f'_d(s)$ into $\tilde{q}'_s$; cf. formula (15) below. Thus, $f'_d(s) \circ f'_d(s) \sim \tilde{q}'_s \circ \tilde{q}'_s \sim q'_s$, which proves (9).

In order to prove the converse, we shall first interpret the relation (8) in terms of a natural map π'_d. To construct this map, recall that for any discriminant D, the set $\bar{Q}_D = Q^{(1)}_D/\mathrm{SL}_2(\mathbb{Z})$ of proper equivalence classes of primitive forms of discriminant D form an abelian group under the composition of forms; cf. e.g. [2], p. 61. In addition, for any $n \geq 1$ we have a natural group homomorphism $\pi_{D,n} : \bar{Q}_{n^2 D} \to \bar{Q}_D$ given by $q \mapsto q \circ 1_D$; cf. [2], p. 132. We now prove:

Lemma 17 *If $d > 1$, then there is a unique homomorphism $\pi'_d : \bar{Q}_{-4d} \to \bar{Q}_{-16d}$ such that*

(10) $$\pi'_d(\pi_{-4d,2}(q)) \sim q \circ q, \quad \textit{for all } q \in \bar{Q}_{-16d}.$$

Furthermore, the image of π_d is $(\bar{Q}_{-16d})^2$, the principal genus of discriminant $-16d$.

Proof. First note that $\pi_{D,n}$ is always surjective. Indeed, by using the well-known identification of $\bar{Q}_D$ with $\mathrm{Pic}(\mathfrak{O}_D)$, where $\mathfrak{O}_D = \mathbb{Z} + \frac{1}{2}(1+\sqrt{D})\mathbb{Z}$ is the order of discriminant D, the map $\pi_{D,n}$ corresponds to the canonical map $\mathrm{Pic}(\mathfrak{O}_D) \to \mathrm{Pic}(\mathfrak{O}_{n^2D})$ induced by the inclusion $\mathfrak{O}_{n^2D} \subset \mathfrak{O}_D$, which is known to be surjective; cf. Lang[24], p. 94.

From the explicit formula for $h(D) := |\bar{Q}_D| = |\mathrm{Pic}(\mathfrak{O}_D)|$ (cf. [24], p. 95), we see that $|\mathrm{Ker}(\pi_{D,2})| = 2$, if $D = -4d$ and $d > 1$; in fact, we have

(11) $$\mathrm{Ker}(\pi_{-4d,2}) = \{1_{-16d}, q_d\},$$

where $q_d = [4, 0, d]$, if $d \equiv 1\,(2)$, and $q_d = [4, 4, d+1]$, if $d \equiv 0\,(2)$, as is easy to verify. Thus, if $S(q) = q \circ q$ denotes the squaring homomorphism on $\bar{Q}_D$, then $\mathrm{Ker}(\pi_{D,2}) \le \mathrm{Ker}(S)$, and so by the universal property of quotients, there is a unique homomorphism $\pi'_d : \bar{Q}_{4D} \to \bar{Q}_D$ such that $S = \pi'_d \circ \pi_{D,2}$. This proves the first assertion, and the second follows because $(\bar{Q}_{4D})^2$ is the image of S.

Corollary 18 *If $s = (n_1, n_2, k) \in P(d)^{odd}$, i.e. if $\gcd(n_1, n_2, 2) = 1$, then $q_s \sim \pi'_d(f_d(s))$, and if $s \in P(d)^{even}$, then $q'_s \sim f'_d(s)^2$.*

Proof. If n_2 is odd, then this follows directly from (8) and (10), and if n_1 and n_2 are both even, then $q'_s \sim f'_d(s)^2$ by (9).

There remains the case that n_1 is odd (and n_2 even). Here we observe that

$$f_d(n_1, n_2, k) \sim f_d(n_2, n_1, -k), \quad \text{for all } s = (n_1, n_2, k) \in P(d),$$

because the matrix $g = \left(\begin{smallmatrix} n_2 & -k \\ -kd & n_1 \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ transforms $f_d(s)$ into $f_d(s')$, where $s' = (n_2, n_1, -k)$. Similarly, we have

$$q_s \sim q_{s'},$$

because the matrix $g' = \left(\begin{smallmatrix} n_1 & y \\ k & n_2 \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$, where $y = (n_1 n_2 + 1)kd$, transforms q_s into $q_{s'}$. Thus, since n_1 is odd, we have by (8) that $q_{s'} \sim \pi'_d(f_d(s'))$, and so $q_s \sim q_{s'} \sim \pi'_d(f_d(s')) \sim \pi'_d(f_d(s))$, as claimed.

Corollary 19 *For $d > 1$ we have*

(12) $$|\mathrm{Ker}(\pi'_d)| \;=\; \tfrac{1}{2} g(-16d) \;=\; 2^{\omega(d)-1},$$

where $g(D) = |\bar{Q}_D/\bar{Q}_D^2|$ denotes the number of genera of discriminant D and $\omega(d)$ the number of distinct prime divisors of d. Thus

(13) $$q \in \mathrm{Ker}(\pi'_d) \;\Leftrightarrow\; q \sim [d_1, 0, d_2], \textit{ where } d_1 d_2 = d,\ d_1 \le d_2, \textit{ and } \gcd(d_1, d_2) = 1.$$

Proof. Since $\pi'_d \circ \pi_{D,2} = S$ by (10), and $|\mathrm{Ker}(\pi_{D,2})| = 2$ (cf. the proof of Lemma 17), we see that $|\mathrm{Ker}(\pi'_d)| = \frac{1}{2}|\mathrm{Ker}(S)| = \frac{1}{2}|\mathrm{Coker}(S)| = \frac{1}{2}g(4D)$. This proves the first equality of (12). To prove the second, recall that Gauss's genus theory yields

$$g(D) = 2^{\omega(D)-1+\varepsilon(D)}, \tag{14}$$

where $\varepsilon(D) = 1$ if $D \equiv 0 \,(\mathrm{mod}\ 32)$, $\varepsilon = -1$ if $D \equiv 4 \,(\mathrm{mod}\ 16)$ and $\varepsilon(D) = 0$ otherwise; cf. [18], p. 170. From this, the formula (12) follows easily.

Let d_1, d_2 be as indicated. If d_1 is odd, then $[d_1, 0, 4d_2] \in \mathrm{Ker}(S)$ and so $[d_1, 0, d_2] \sim [d_1, 0, 4d_2] \circ 1_D \sim \pi_{D,2}([d_1, 0, 4d_2]) \in \mathrm{Ker}(\pi'_d)$. Similarly, if d_1 is even, then d_2 is odd, and then $[d_1, 0, d_2] \sim \pi_{D,2}([4d_1, 0, d_2]) \in \mathrm{Ker}(\pi'_d)$. Since the forms $[d_1, 0, d_2]$ are all reduced, they yield $2^{\omega(d)-1}$ distinct equivalence classes in $\mathrm{Ker}(\pi'_d)$. By (12) we have thus found all the classes in $\mathrm{Ker}(\pi'_d)$ and so (13) follows.

Lemma 20 *The inclusion $Q^{(2)}_{-4d}(d) \subset Q^{(2)}_{-4d}$ induces a bijection*

$$Q^{(2)}_{-4d}(d)/\Gamma_0(d) \xrightarrow{\sim} Q^{(2)}_{-4d}/\mathrm{SL}_2(\mathbb{Z}),$$

where $\Gamma_0(d) = \{g = \left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) : d|z\}$.

Proof. Recall that the action of $g = \left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ on $Q^{(n)}_D$ is given by

$$[a, b, c]g = [ax^2 + bxz + cz^2, b(xw + yz) + 2(axy + czw), ay^2 + byw + cw^2]; \tag{15}$$

cf. [2], p. 4. In other words, we have $M(qg) = g^t M(q) q$, where $M(q) = \left(\begin{smallmatrix} a & b \\ b & c \end{smallmatrix}\right)$ denotes the matrix associated to $q = [a, 2b, c]$. From this we see easily that $\Gamma_0(d)$ acts on $Q^{(2)}_D(d)$, where $D = -4d$, and so we have a map $j : Q^{(2)}_D(d)/\Gamma_0(d) \to Q^{(2)}_D/\mathrm{SL}_2(\mathbb{Z})$.

To see that j is injective, suppose that $q_i = [a_i d, 2b_i d, c_i] \in Q^{(2)}_D(d)$, are such that $j(q_1) = j(q_2)$. Then there is a $g = \left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z})$ such that $m_2 = m_1^g := g^t m_1 g$. Then $a_2 d = a_1 d x^2 + 2b_1 d x z + c_1 z^2$ and $b_2 d = b_1 d(xw + yz) + (a_1 dxy + c_1 zw)$, so $d | \gcd(c_1 z^2, c_1 zw) = c_1 z$, and hence $d|z$ because $\gcd(c_1, d) = 1$. (Recall that $(a_i, c_i, b_i) \in P(d)$; cf. Lemma 14.) Thus, $g \in \Gamma_0(d)$, and so j is injective.

We now prove that j is surjective. Let $q = [a, 2b, c] \in Q^{(2)}_{-4d}$. We first note that by replacing q by qg with a suitable $g \in \mathrm{SL}_2(\mathbb{Z})$ we may assume $\gcd(a, d) = 1$. Indeed, if $q \in Q^{(1)}_{-4d}$, then this is well-known; cf. [2], pp. 49-50. In the other case we have $q = 2q_1$, where $q_1 \in Q^{(1)}_{-d}$ and $-d \equiv 1 \,(\mathrm{mod}\ 4)$, and so the assertion follows by same argument applied to q_1. Thus, $\gcd(a, d) = 1$ and hence also $\gcd(a, b) = 1$ because $ac - b^2 = d$. Thus, there exist $x, y \in \mathbb{Z}$ such that $g = \left(\begin{smallmatrix} -b & x \\ a & y \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. Then $qg = [ad, 2yd, *]$, and so we see that $q \in \mathrm{Im}(j)$. This proves that j is bijective.

Proof of Proposition 15. Let $s \in P(d)$. If $s \in P(d)^{odd}$, then $f_d(s)$ is primitive of discriminant $-4d$ and hence by Corollary 18 and Lemma 17 we see that $q_s \sim \pi'_d(f_d(s))$

is in the principal genus of discriminant $-16d$ (and is primitive). Thus, q_s is of type d, provided that q_s is not in the principal class.

On the other hand, if $s \in P(d)^{even}$, then by Lemma 16(b) we know that $q_s = 4q_s'$, where q_s' is primitive of discriminant $-d$. Moreover, (9) shows that q_s' is in the principal genus, so q_s has type d also in this case.

Conversely, suppose q is a form of type d. Assume first that q is primitive. Since q lies in the principal genus, we have by Lemma 17 that $q \sim \pi_d'(q_1)$, for some $q_1 \in Q_{-4d}^{(1)}$. By Lemma 20 (and Lemma 14) we have $q_1 \sim f_d(s)$, for some $s \in P(d)^{odd}$. Thus, $q \sim \pi_d'(f_d(s)) \sim q_s$, the latter by Corollary 18.

Next, suppose that q is not primitive, so by definition $q = 4q'$, where $q' \sim q'' \circ q''$ for some $q'' \in Q_{-d}^{(1)}$. Then $2q'' \in Q_{-4d}^{(2)}$, and so by Lemma 20 (and Lemma 14) there is an $s \in P(d)^{even}$ such that $2q'' \sim f_d(s)$. Thus, $q'' \sim f_d'(s)$ and so by (9) we obtain $q_s' \sim f_d'(s) \circ f_d(s) \sim q'' \circ q'' \sim q'$. We therefore have $q_s = 4q_s' \sim 4q' = q$, as claimed.

We now derive some properties of modules endowed with forms of prototype q_s, where $s \in P(d)$. These will be used in the next section.

Lemma 21 *Let (M, q) be a quadratic module of rank 2, and suppose that M has a basis $\{v_1, v_2\}$ such that for some $s = (n_1, n_2, k) \in P(d)$ we have*

$$q(xv_1 + yv_2) = q_s(x, y), \quad \text{for all } x, y \in \mathbb{Z}.$$

Put $w_1 = v_1$ and $w_2 = -n_1^2 v_1 - kv_2$. Then

$$q(xw_1 + yw_2) = n_2^2 x^2 + 2(n_1 n_2 - 2)xy + n_1^2 y^2. \tag{16}$$

Moreover, for $w_3 = n_1 k d v_1 + n_2 v_2$ we have $q(w_3) = 4dn_1 n_2$, provided that $k \neq 0$.

Proof. The relation (16) is a straight-forward computation, using the transformation law (15) applied to $g = \begin{pmatrix} 1 & -n_1^2 \\ 0 & -k \end{pmatrix}$ and the relation (5).

To compute $q(w_3)$, note first that by (5) we have $kw_3 = -(n_1 w_1 + n_2 w_2)$. Thus, by (16) we obtain $k^2 q(w_3) = q(n_1 w_1 + n_2 w_2) = 4n_1 n_2(n_1 n_2 - 1) = 4n_1 n_2 k^2 d$, and so $q(w_3) = 4n_1 n_2 d$ because $k \neq 0$.

6 The product surface $E_1 \times E_2$

The aim of this section is to prove the basic classification Theorem 13. For this, it is useful to use the following "presentation" of the Néron-Severi group $\mathrm{NS}(A)$ of a product surface $A = E_1 \times E_2$ of two elliptic curves E_1 and E_2.

Proposition 22 *For $a, b \in \mathbb{Z}$ and $h \in \mathrm{Hom}(E_1, E_2)$ put*

$$\mathbf{D}(a, b, h) = (a - \deg(h))\theta_1 + (b - 1)\theta_2 + \Gamma_{-h} \in \mathrm{Div}(A), \tag{17}$$

where $\theta_i = p_i^*(0_{E_i})$, and $\Gamma_f \in \mathrm{Div}(A)$ is the graph of $f = -h$. Then the rule $(a,b,h) \mapsto$ $cl(\mathbf{D}(a,b,h))$ defines a group isomorphism

$$\mathbf{D} = \mathbf{D}_{E_1,E_2} : \mathbb{Z} \oplus \mathbb{Z} \oplus \mathrm{Hom}(E_1,E_2) \stackrel{\sim}{\to} \mathrm{NS}(E_1 \times E_2),$$

and we have

$$(18) \qquad (\mathbf{D}(a,b,f).\mathbf{D}(a',b',f')) = ab' + ba' - \beta_d(f,f'),$$

where β_d is the bilinear form associated to the degree quadratic form on $\mathrm{Hom}(E_1,E_2)$, i.e. $\beta_d(f,f') = \deg(f+f') - \deg(f) - \deg(f')$. In addition, the homomorphism $\phi_D : A \to \hat{A}$ associated to $D = \mathbf{D}(a,b,f)$ is given by

$$(19) \qquad \phi_{\mathbf{D}(a,b,f)} = \lambda_1 \otimes \lambda_2 \circ \begin{pmatrix} [a]_{E_1} & f^t \\ f & [b]_{E_2} \end{pmatrix},$$

where $\lambda_1 \otimes \lambda_2$ denotes the product polarization associated the canonical polarizations $\lambda_i : E_i \stackrel{\sim}{\to} \hat{E}_i$, for $i = 1,2$, and $f^t = \lambda_1^{-1}\hat{f}\lambda_2$ is the dual map.

Proof. Most of this is well-known; for example, the fact that $\mathbf{D}$ is an isomorphism is a special case of the basic relation between correspondences of curves and homomorphisms of their Jacobians; cf. [31], p. 185. In the appendix below we derive this in Proposition 61 as a special case of a more general construction (based on (19)) which has the advantage of being more functorial.

Corollary 23 *The determinant of the Néron-Severi group of $E_1 \times E_2$ with respect to the intersection form is given by*

$$(20) \qquad \det(\mathrm{NS}(E_1 \times E_2)) = (-1)^{\rho-1} \det(\mathrm{Hom}(E_1,E_2), \beta_d),$$

where $\rho = \mathrm{rank}(\mathrm{NS}(E_1 \times E_2)) = \mathrm{rank}(\mathrm{Hom}(E_1,E_2)) + 2$.

Proof. Put $\Gamma_f^* = \mathbf{D}(0,0,f)$. If $f_1,\ldots,f_r$ is a basis of $\mathrm{Hom}(E_1,E_2)$, then by Proposition 22 we have that $\theta_1, \theta_2, \Gamma_{f_1}^*, \ldots, \Gamma_{f_r}^*$ is a basis of $\mathrm{NS}(E_1 \times E_2)$ and so by (18) we see that the Gram matrix $G(\theta_1,\theta_2,\Gamma_1^*,\ldots,\Gamma_{f_r}^*)$ of the intersection form with respect to this basis is given by the block diagonal matrix

$$G(\theta_1,\theta_2,\Gamma_{f_1}^*,\ldots,\Gamma_{f_r}^*) = \mathrm{diag}\left(\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right), -G(f_1,\ldots,f_r)\right),$$

where $G(f_1,\ldots,f_r)$ is the Gram matrix of β_d with respect to the basis $f_1,\ldots,f_r$. From this, formula (20) follows by taking the determinant of both sides.

In the sequel we shall be particularly interested in the set $\mathcal{P}(A)$ consisting of those divisors $D \in \mathrm{NS}(A)$ which define principal polarizations on A. These can characterized by using the set $P(d)$ introduced in the previous section.

Corollary 24 *Let $D = \mathbf{D}(a, b, h) \in \mathrm{NS}(A)$. Then D defines a principal polarization (i.e. $D \in \mathcal{P}(A)$) if and only if $a > 0$ and $ab - \deg(h) = 1$. Thus, every principal polarization of A has the form*

$$(21) \quad D_{s,h} = \mathbf{D}(n_1, n_2, kh) \quad \text{with } h \in \mathrm{Hom}(E_1, E_2) \text{ and } s = (n_1, n_2, k) \in P(\deg(h)).$$

Proof. By the Riemann-Roch Theorem (cf. [30], p. 127), $D \in \mathcal{P}(A)$ if and only if D is ample and $D^2 = 2$, and this holds if and only if $D^2 = 2$ and $(D.\theta_2) > 0$; cf. [19], Corollary 2.2b). Thus, the first assertion follows in view of (18). The second follows from this and the fact that $\deg(kh) = k^2 \deg(h)$.

We now turn to the study of curves C of type d. As promised, we first verify that every curve whose Jacobian is isomorphic to a product of two elliptic curves has a type d, for some $d \geq 1$.

Proposition 25 *Let C be a curve such that its Jacobian J_C has an isomorphism $\alpha : J_C \xrightarrow{\sim} E_1 \times E_2$ to a product of two elliptic curves. Then there exists a* cyclic *isogeny $h : E_1 \to E_2$ of some degree $d \geq 1$ such that*

$$(22) \qquad \theta_C \equiv \alpha^*(D_{s,h}), \quad \text{for some } s = (n_1, n_2, k) \in P(d) \text{ with } k \neq 0.$$

In particular, E_1 is isogenous to E_2 and C has type d.

Proof. Put $D \equiv (\alpha^{-1})^*(\theta_C) \in \mathcal{P}(E_1 \times E_2)$. By Proposition 22 and Corollary 24, $D = \mathbf{D}(n_1, n_2, h_1)$, for some integers n_1, n_2 and homomorphism $h_1 \in \mathrm{Hom}(E_1, E_2)$ satisfying $n_1 n_2 - \deg(h_1) = 1$ and $n_1 > 0$. Note that $h_1 \neq 0$, for otherwise $n_1 = n_2 = 1$ which means $D \equiv \theta_1 + \theta_2$. But then $q_C(\alpha^*\theta_1) = 1$, which contradicts Proposition 6.

Thus, we can write $h_1 = kh$, where h is a cyclic isogeny and $k \neq 0$, and so we see that (22) holds with $s = (n_1, n_2, k) \in P(d)$. Note that this means that C has type d because $D \equiv k\mathbf{D}(n_1, n_2, h) = k(n_1 - d)\theta_1 + k(n_2 - 1)\theta_2 + k\Gamma_{-h}$.

Corollary 26 *If $J_C \simeq E_1 \times E_2$, where $\mathrm{End}(E_1) = \mathbb{Z}$, then C is a curve of unique type $d = \frac{1}{2}\det(\mathrm{NS}(J_C))$.*

Proof. Since $E_2 \sim E_1$ by Proposition 25, it follows that $\mathrm{Hom}(E_1, E_2) = \mathbb{Z}h$, and so by (20) we have $\det(\mathrm{NS}(J_C)) = (-1)^2 \det(\mathrm{NS}(E_1 \times E_2)) = \beta_d(h, h) = 2d$, where $d = \deg(h)$.

Note that h is necessarily cyclic, and that the only cyclic isogenies in $\mathrm{Hom}(E_1, E_2)$ are $\pm h$. Thus, if $\alpha : J_C \xrightarrow{\sim} E_1 \times E_2$ is any isomorphism, then $\theta_C \equiv \alpha^*(D_{s,h})$, for some $s \in P(d)$, and so C has (unique) type $d = \frac{1}{2}\det(\mathrm{NS}(J_C))$.

Remark 27 (a) Although the type d is uniquely determined by the curve C in the above situation, the elliptic curves E_1 and E_2 are not unique (up to isomorphism).

Indeed, if d has more than one prime factor, then we can have an isomorphism $E_1 \times E_2 \simeq E'_1 \times E'_2$ with $E'_1 \not\simeq E_1, E_2$; cf. Proposition 49 below.

(b) If C is any curve of type d satisfying (22) with $(n_1, n_2, k) \in P(d)$, then $\langle C \rangle \in H_{n_1^2} \cap H_{n_2^2}$ because $q_C(\alpha^*(\theta_1)) = n_2^2$ and $q_C(\alpha^*(\theta_1)) = n_1^2$ by (18) (and (2)). (Note that since $\alpha^*(\theta_i)$ is an elliptic curve, its image in $\mathrm{NS}(J_C, \theta_C)$ is primitive by [19], Theorem 2.8.) Thus, if $n_1 \neq n_2$, then we see by Proposition 8 that $\langle C \rangle \in H(q)$, for some binary quadratic form q.

We now turn to the proof of Theorem 13. One direction is contained in the following more precise result.

Proposition 28 *Let $A = E_1 \times E_2$ and $\theta = D_{s,h} \in \mathcal{P}(A)$, where h is a cyclic isogeny of degree d and $s = (n_1, n_2, k) \in P(d)$. Let $\bar{\theta}_1$, $\bar{\theta}_2$ and $\bar{\Gamma}_h^*$ denote the images of θ_1, θ_2, and $\Gamma_h^* = \mathbf{D}(0, 0, h)$ in $\mathrm{NS}(A, \theta)$, respectively.*

(a) $\bar{M} := \langle \bar{\theta}_1, \bar{\theta}_2, \bar{\Gamma}_h^* \rangle$ is a primitive submodule of $\mathrm{NS}(A, \theta)$, and so $\langle A, \theta \rangle \in H(q_{\bar{M}})$, where $q_{|M}$ denotes the restriction of $q_\theta = q_{(A,\theta)}$ to $\bar{M}$.

(b) Let $\bar{D} = kd\bar{\theta}_2 + n_1\bar{\Gamma}_h^*$. Then $\{\bar{\theta}_1, \bar{D}\}$ is a basis of $\bar{M}$, and we have

(23) $$q_\theta(x\bar{\theta}_1 + y\bar{D}) = q_s(x, y) \quad \forall x, y, \in \mathbb{Z}, \quad \textit{where } q_s \textit{ is defined by } (6).$$

Proof. (a) Since h is a cyclic isogeny, it is a primitive element in $\mathrm{Hom}(E_1, E_2)$, and so we can extend h to a basis $h_1 = h, h_2, \ldots, h_r$ of $\mathrm{Hom}(E_1, E_2)$. Then $\{cl(\theta_1), cl(\theta_2), cl(\Gamma_{h_1}^*), \ldots, cl(\Gamma_{h_r}^*)\}$ is a basis of $\mathrm{NS}(E_1 \times E_2)$; cf. Corollary 23. Thus, $M := \langle cl(\theta_1), cl(\theta_2), cl(\Gamma_h^*)\rangle$ is a primitive submodule of $\mathrm{NS}(E_1 \times E_2)$, and so we see that $\bar{M} = M/(\mathbb{Z}\theta)$ is a primitive submodule of $\mathrm{NS}(A, \theta)$. This means that q_θ primitively represents $q_{\bar{M}}$, and so $\langle A, \theta \rangle \in H(q_{\bar{M}})$.

(b) Put $D = \mathbf{D}(0, kd, n_1 h) \in \mathrm{NS}(A)$; thus, $\bar{D}$ is the image of D in $\mathrm{NS}(A, \theta)$. Using (5), we see that $cl(\theta_2) = n_1\theta - kD - n_1^2 cl(\theta_1)$, and $cl(\Gamma_h^*) = n_2 D - kd\theta + n_1 kd\theta_1$, so $\{\theta, cl(\theta_1), D\}$ is a basis of M, and hence $\{\bar{\theta}_1, \bar{D}\}$ is a basis of $\bar{M}$.

Put $D_1 = x\theta_1 + yD$. Then by computing intersection numbers we find that $(\theta.D_1) = n_2 x - n_1 kdy$ and $D_1^2 = 2(kdxy - n_1^2 dy^2)$, and so $q_\theta(D_1) = (\theta.D_1)^2 - 2D_1^2 = n_2^2 x^2 - 2kd(n_1 n_2 + 2)xy + n_1^2 d(k^2 d + 4)y^2 = q_s(x, y)$; here we used the fact that $k^2 d + 4 = n_1 n_2 + 3$ by (5).

For the other direction we shall use the following elementary fact.

Lemma 29 *Let $\overline{cl} : \mathrm{NS}(A) \to \mathrm{NS}(A, \theta) = \mathrm{NS}(A)/\mathbb{Z}\theta$ denote the quotient map, and let $\bar{D} \in \mathrm{NS}(A, \theta)$. If $n \in \mathbb{Z}$, then there exists $D \in \mathrm{NS}(A)$ with*

(24) $$(D.\theta) = n \quad \textit{and} \quad \overline{cl}(D) = \bar{D}$$

if and only if $n \equiv q_{(A,\theta)}(\bar{D}) \pmod 2$.

Proof. If D exists, then $q_\theta(\bar{D}) = q_\theta(D) = n^2 - 2D^2 \equiv n^2 \equiv n \pmod 2$. Conversely, suppose that $n \equiv q_C(\bar{D}) \pmod 2$, and let $D_0 \in \mathrm{NS}(A)$ be any class with $\overline{cl}(D_0) = \bar{D}$. Put $n_0 = (D.\theta)$. Then, by what was just shown, $n_0 \equiv q_C(\bar{D}) \equiv n \pmod 2$, and so $D = \frac{1}{2}(n - n_0)\theta + D_0$ satisfies (24).

Proof of Theorem 13. If C is a curve of type d, then (22) holds for some $s = (n_1, n_2, k) \in P(d)$ by Proposition 25, and so Proposition 28 shows that the form q_s is primitively represented by q_C. Note that q_s cannot represent 1 by Proposition 6, so q_s cannot be in the principal class. Thus, q_s is a form of type d by Proposition 15.

Conversely, suppose that $\langle C \rangle \in H(q)$, where q is a form of type d. Then by Proposition 15 we know $q \sim q_s$ for some $s = (n_1, n_2, k) \in P(d)$. (Note that $k \neq 0$ for otherwise q_s represents $1 = n_2^2$.) Thus, there exist $\bar{D}_1', \bar{D}_2' \in \mathrm{NS}(J_C, \theta_C)$ (which generate a primitive submodule $\bar{M}$ of $\mathrm{NS}(J_C, \theta_C)$) such that

$$q_C(x\bar{D}_1' + y\bar{D}_2') = q_s(x, y), \quad \text{for all } x, y \in \mathbb{Z}.$$

Put $\bar{D}_1 = \bar{D}_1'$ and $\bar{D}_2 = -n_1^2\bar{D}_1' - k\bar{D}_2'$; note that $\bar{D}_1$ and $\bar{D}_2$ are primitive in $\bar{M}$ and hence in $\mathrm{NS}(J_C, \theta_C)$ because $\gcd(-n_1^2, k) = 1$. Applying Lemma 21 to $M = \bar{M}$ and $v_i = \bar{D}_i'$, we see from (16) that $q_C(\bar{D}_1) = n_2^2$ and $q_C(\bar{D}_2) = n_1^2$. Thus, by Theorem 3.2 of [19] we know that there are unique elliptic subgroups $E_i \leq J_C$ such that $\overline{cl}(E_i) = \bar{D}_i$, for $i = 1, 2$, and that we have $(E_1.\theta_C) = n_2$ and $(E_2.\theta_C) = n_1$. Furthermore, since $E_i^2 = 0$, we have $4(E_1.E_2) = 2(E_1 + E_2)^2 = ((E_1 + E_2).\theta_C)^2 - q_C(E_1 + E_2) = (n_1 + n_2)^2 - q_C(\bar{D}_1 + \bar{D}_2)$. By (16) we know that $q_C(\bar{D}_1 + \bar{D}_2) = n_2^2 + 2(n_1n_2 - 2) + n_1^2$, and so $(E_1.E_2) = 1$. Thus, there is an isomorphism $\alpha : J_C \xrightarrow{\sim} E_1 \times E_2$ such that $\alpha^*\theta_1 = E_2$ and $\alpha^*\theta_2 = E_1$.

It remains to show that C has type $d = -\frac{1}{16}\mathrm{disc}(q)$. For this, put $D = \alpha_*\theta_C \in \mathcal{P}(E_1 \times E_2)$, and write $D = \mathbf{D}(a, b, ch)$, where $a, b, c \in \mathbb{Z}$ and $h \in \mathrm{Hom}(E_1, E_2)$ is cyclic. Then $n_1 = (\theta_C.E_2) = (D.\theta_2) = a$, so $a = n_1$ and similarly $b = n_2$.

To prove that $d = \deg(h)$, consider $\bar{D}_3 := n_1kd\bar{D}_1' + n_2\bar{D}_2'$. Since $q_C(\bar{D}_3) = 4dn_1n_2$ by Lemma 21, we know by Lemma 29 that there exists $D_3 \in \mathrm{NS}(J_C)$ such that $(D_3.\theta_C) = -2kd$ and $\overline{cl}(D_3) = \bar{D}_3$. We now observe that

$$\theta_C \equiv n_1E_1 + n_2E_2 + kD_3. \tag{25}$$

Indeed, since $k\bar{D}_3 = -(n_1\bar{D}_1 + n_2\bar{D}_2)$ (cf. the proof of Lemma 21), it follows that $\theta' := n_1E_1 + n_2E_2 + kD_3 = m\theta_C$, for some $m \in \mathbb{Z}$. But then $2m = m\theta_C^2 = (\theta'.\theta_C) = n_1n_2 + n_2n_1 + k(-2kd) = 2$, so $m = 1$. Thus (25) holds, and so we obtain $k\alpha_*D_3 = c\Gamma_h^*$. Since Γ_h^* is primitive in $\mathrm{NS}(E_1 \times E_2)$, it follows that $\alpha_*D_3 = c'\Gamma_h^*$, where $c' = \frac{c}{k} \in \mathbb{Z}$. Thus, $D_3 = c'D_3'$, where $D_3' := \alpha^*(\Gamma_h^*)$, and so $\bar{D}_3' = \overline{cl}(D_3') \in \bar{M} = \mathbb{Z}D_1' + \mathbb{Z}D_2'$ because $\bar{M}$ is a primitive submodule of $\mathrm{NS}(J_C, \theta_C)$. Now $c'\bar{D}_3' = \bar{D}_3 = n_1kd\bar{D}_1' + n_2\bar{D}_2'$, so $c' \mid \gcd(n_1kd, n_2) = \gcd(n_1, n_2)$. But $\gcd(c', n_1n_2) = 1$ because $n_1n_2 - c^2\deg(h) = 1$ (since $D \in \mathcal{P}(E_1 \times E_2)$), and so $c' = \pm 1$, i.e. $\deg(h) = d$. Thus C has type d.

7 The existence theorem

We now show that $H(q)$ is non-empty, whenever q is a form of type d. This follows from the following more precise assertion:

Theorem 30 *Suppose that q is a binary quadratic form of type d. Let E_1 be any elliptic curve with $\mathrm{End}(E_1) = \mathbb{Z}$, and let $E_2 = E_1/H$, where $H \leq E_1$ is any cyclic subgroup (scheme) of degree d. Then there exists a curve C with $J_C \simeq E_1 \times E_2$ such that q_C is equivalent to q, i.e. $q_C \approx q$; in particular, $\langle C \rangle \in H(q)$.*

To prove this, we shall use the following refinement of Corollary 24.

Proposition 31 *Suppose $\mathrm{Hom}(E_1, E_2) = \mathbb{Z}h$, and let $d = \deg(h)$. Then the map $s \mapsto D_{s,h}$ defines a bijection between the set $P(d)$ and the set $\mathcal{P}(A)$ of principal polarizations on $A := E_1 \times E_2$. Furthermore, $\theta \in \mathcal{P}(A)$ is represented by a smooth curve C of genus 2 if and only if $q_{(A,\theta)}$ is not in the principal class.*

Proof. The first assertion follows immediately from Corollary 24 since here every $D \in \mathrm{NS}(E_1 \times E_2)$ has the form $D(a, b, ch)$, and since $\deg(ch) = c^2 \deg(h)$. The second follows immediately from Proposition 6 because a binary quadratic form represents 1 if and only if it is in the principal class.

Proof of Theorem 30. By Proposition 15 there exists $s \in P(d)$ such that $q \sim q_s$. Put $\theta = D_{s,h} \in \mathrm{NS}(E_1 \times E_2)$, where $h : E_1 \to E_2 = E_1/H_1$ denotes the quotient map. (Note that h is cyclic, and so $\mathrm{Hom}(E_1, E_2) = \mathbb{Z}h$.) By Proposition 31 we see that $\theta \in \mathcal{P}(A)$, and Proposition 28 shows that $q_{(A,\theta)} \approx q_s \sim q$. (Note that $\bar{M} = \mathrm{NS}(A, \theta)$ because $\bar{M}$ is primitive in $\mathrm{NS}(A, \theta)$ and $\mathrm{rk}(\mathrm{NS}(A, \theta)) = 2$.) Since q is not in the principal class by hypothesis, Proposition 31 shows that $(A, \theta) \simeq (J_C, \theta_C)$, for some curve C of genus 2. By construction, $q_C \approx q$.

We now consider some applications of the Existence Theorem 30. The first is the following useful fact.

Corollary 32 *If q_i is a quadratic form of type d_i, for $i = 1, 2$, then $H(q_1) = H(q_2)$ if and only if $q_1 \approx q_2$.*

Proof. If $q_1 \approx q_2$, then $H(q_1) = H(q_2)$ by definition. Conversely, suppose $H(q_1) = H(q_2)$. By Theorem 30 there exists $\langle C \rangle \in H(q_1)$ such that $q_C \approx q_1$. Since $\langle C \rangle \in H(q_2)$, this means that q_C primitively represents q_2, and so $q_2 \approx q_C$ because both have rank 2. Thus $q_1 \approx q_2$, as asserted.

Remark 33 The above proof also shows that if $q_1 \not\approx q_2$, then $H(q_1) \cap H(q_2)$ consists only of *CM-points*, i.e. of points $\langle A, \theta \rangle$ such that $A \simeq E_1 \times E_2$, where $E_1 \sim E_2$ are elliptic curves which have complex multiplication (or are supersingular).

Corollary 34 *We have for $d \geq 1$ that $T(d) = \emptyset \Leftrightarrow \bar{Q}_d^* = \emptyset$, and hence*

(26) $T(d) = \emptyset \Leftrightarrow \bar{h}(-16d) = 1$ *and* $d \not\equiv 3\,(4) \Leftrightarrow \bar{h}(-16d) = 1$ *and* $d \neq 3, 7, 15.$

where $\bar{h}(D) = h(D)/g(D)$ denotes the number of forms in the principal genus of primitive binary quadratic forms of discriminant $D = -16d$.

Proof. The first assertion follows directly from Theorems 13 and 30. To prove the first equivalence of (26), note first that it follows from the definitions that the number $t(d)$ of $\mathrm{SL}_2(\mathbb{Z})$-equivalence classes of forms of type d is given by

$$t(d) = \begin{cases} \bar{h}(-16d) - 1, & \text{if } d \not\equiv 3 \,(\mathrm{mod}\ 4) \\ \bar{h}(-16d) - 1 + \bar{h}(-d), & \text{if } d \equiv 3 \,(\mathrm{mod}\ 4). \end{cases} \tag{27}$$

In view of Remark 12 we see that $\bar{Q}_d^* = \emptyset \Leftrightarrow t(d) = 0$, and so the first equivalence follows. To prove the second, it is enough to show that if $d \equiv 3(4)$, then $\bar{h}(-16d) > 1$ when $d \neq 3, 7, 15$. For this we observe that (14) implies that $g(-16d) = 2g(-4d)$, when $d \equiv 3(4)$ and that hence $\bar{h}(-16d) = \bar{h}(-4d)$ because $h(-16d) = 2h(-4d)$ (cf. Lemma 17). Now by Hall[11], Theorem I, we have $\bar{h}(-4d) > 1$ when $d \equiv 3(4)$ and $d \neq 3, 7, 15$, and so the second equivalence follows.

Remark 35 It is clear that the above number $t(d)$ is closely connected to the number $t^*(d) = \#\bar{Q}_d^*$ of $\mathrm{GL}_2(\mathbb{Z})$-equivalence classes of forms of type d. To make this connection precise, however, we require another invariant of forms of discriminant D: the number $\bar{s}(D) = |\bar{Q}_D^2[2]|$ of ambiguous classes in the principal genus. This number is closely related to the number $s(D) = [\bar{Q}_D : \bar{Q}_D^4]$ of *spinor genera* of (primitive) forms of discriminant D as defined by Estes/Pall [7], for we have $\bar{s}(D) = s(D)/g(D)$. Now by Remark 12 we have

$$\bar{h}^*(D) := \#(\bar{Q}_D^2/\mathrm{GL}_2(\mathbb{Z})) = \frac{1}{2}(\bar{h}(D) + \bar{s}(D)), \tag{28}$$

and so we see that

$$t^*(d) := \#\bar{Q}_d^* = \begin{cases} \bar{h}^*(-16d) - 1, & \text{if } d \not\equiv 3 \,(\mathrm{mod}\ 4) \\ \bar{h}^*(-16d) - 1 + \bar{h}^*(-d), & \text{if } d \equiv 3 \,(\mathrm{mod}\ 4). \end{cases} \tag{29}$$

Proof of Corollary 5: From Gauss[10], Art. 303, we know that $\bar{h}(-16d) = 1$ when d is one of the values of (1); cf. also Dickson[5], p. 89. Thus, by Corollary 34 we see that $T(d) = \emptyset$ for those values of d. Moreover, if we look at the list of exceptional discriminants which are of the form $-16d$ with $d \neq 3, 7, 15$, then we obtain the list (1). Finally, the finiteness assertion follows from Chowla[3], and the fact that (GRH) implies Gauss's Conjecture was proved by Weinberger[37].

For later applications it is useful to refine the above existence theorem by determining the number of isomorphism classes of curves C on $E_1 \times E_2$ such that $q_C \approx q$.

Theorem 36 *Let $A = E_1 \times E_2$, where $\mathrm{Hom}(E_1, E_2) = \mathbb{Z}h$, and let q be a quadratic form of type $d := \deg(h)$. Then the number $N_A(q)$ of isomorphism classes of smooth genus 2 curves C on A with $q_C \approx q$ is given by:*

$$N_A(q) = \begin{cases} 2^{\omega(d)-2} & \text{if } q \in \bar{Q}^2_{-16d}[2] \setminus \{q_d\} \text{ or if } \frac{1}{4}q \in \bar{Q}^2_{-d}[2] \setminus \{1_{-d}\}, \\ 2^{\omega(d)-1} & \text{otherwise,} \end{cases} \tag{30}$$

where $q_d = 4x^2 + dy^2$, if $d \equiv 0(2)$, and $q_d = 4x^2 + 4xy + (d+1)y^2$, if $d \equiv 1(2)$.

Remark 37 Note that q_d is not necessarily in $\bar{Q}^2_{-16d}[2]$. In fact, this is the case if and only if $d \equiv 0, 1, 5\,(8)$, as can be verified by checking the generic characters of q_d.

As we shall see presently, the above theorem follows easily from the following fact which is interesting in itself.

Proposition 38 *Let $A = E_1 \times E_2$, where $\mathrm{Hom}(E_1, E_2) = \mathbb{Z}h$, and let $d = \deg(h)$. If C is a smooth genus 2 curve on A, then $C \equiv D_{s,h}$, for some $s \in P(d)$ with $f_d(s) \notin \mathrm{Ker}(\pi'_d)$, and the isomorphism class of C is uniquely determined by the $\mathrm{GL}_2(\mathbb{Z})$-equivalence class of the binary quadratic form $f_d(s)$. Furthermore, $q_C \approx q_s$.*

Before proving this, let us see how Theorem 36 follows from it.

Proof of Theorem 36: Suppose first that q is primitive, so $q \approx q_1^2$, where $q_1 \in \bar{Q}_{-16d}$. If C is any curve on A, then by Proposition 38 we have that $C \equiv D_{s,h}$ with $s \in P(d)$, and that $q_C \approx q_s$. We thus see from Corollary 18 and Proposition 38 that

$$N_A(q) = \#({\pi'_d}^{-1}(q) \,\cup\, {\pi'_d}^{-1}(q^{-1}))/\mathrm{GL}_2(\mathbb{Z}).$$

Now if $q \not\sim q^{-1}$, then the sets ${\pi'_d}^{-1}(q)$ and ${\pi'_d}^{-1}(q^{-1})$ are interchanged under the $\mathrm{GL}_2(\mathbb{Z})$-action, and so $N_A(q) = \#({\pi'_d}^{-1}(q)) = |\mathrm{Ker}(\pi'_d)| = 2^{\omega(d)-1}$ by Corollary 19. (Note that we can assume $d > 1$ for otherwise $\bar{Q}^*_d$ is empty by (26).) This proves (30) in this case. Next, suppose $q \sim q^{-1}$, i.e. $q \in \bar{Q}^2_{-16d}[2]$. Now if $q \in \mathrm{Ker}(\pi_{-4d,2})$, i.e. if $q \sim q_d$ by (11), then ${\pi'_d}^{-1}(q) \subset \bar{Q}_{-4d}[2]$ (cf. Lemma 17), and so $N_A(q) = \#({\pi'_d}^{-1}(q)) = |\mathrm{Ker}(\pi'_d)| = 2^{\omega(d)-1}$ again. On the other hand, if $q \in \bar{Q}^2_{-16d}[2] \setminus \{q_d\}$, then ${\pi'_d}^{-1}(q) \cap \bar{Q}_{-4d}[2] = \emptyset$, and so the $\mathrm{GL}_2(\mathbb{Z})$-action has no fixed points on ${\pi'_d}^{-1}(q)$, and hence $N_A(q) = \frac{1}{2}\#({\pi'_d}^{-1}(q)) = \frac{1}{2}|\mathrm{Ker}(\pi'_d)| = 2^{\omega(d)-2}$ by Corollary 19.

Finally, suppose that q is not primitive. Then $q \approx 4q_1$ with $q_1 \in \bar{Q}^2_{-d}$ and $d \equiv 3 \pmod 4$. In this case we have by the same reasoning as above that

$$N_A(q) = \#({S_d}^{-1}(q_1) \,\cup\, {S_d}^{-1}(q_1^{-1}))/\mathrm{GL}_2(\mathbb{Z}),$$

where $S_d : \bar{Q}_{-d} \to \bar{Q}^2_{-d}$ is the squaring map. Since $|\mathrm{Ker}(S_d)| = g(-d) = 2^{\omega(d)-1}$ (cf. (14)), a similar analysis as above yields (30).

We now turn to the proof of Proposition 38. For this, we require the following information about the functorial behaviour of the divisor $D_{s,f}$.

Proposition 39 *If* $g = \left(\begin{smallmatrix} a & b \\ cd & e \end{smallmatrix}\right) \in \Gamma_0^{\pm}(d) := \Gamma_0(d) \cup \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)\Gamma_0(d)$*, and if* $f \in \mathrm{Hom}(E_1, E_2)$ *has degree* d*, then*

$$\alpha_{g,f} = \begin{pmatrix} [a]_{E_1} & bf^t \\ cf & [e]_{E_2} \end{pmatrix} \in \mathrm{Aut}(E_1 \times E_2),$$

and we have

(31) $$\alpha_{g,f}^*(D_{s,f}) := D_{sg,f}, \quad \textit{for all } s \in P(d),$$

where $sg \in P(d)$ *is defined by the rule* $f_d(sg) = f_d(s)g$.

Proof. We first observe that if $[g]_{E_2} \in \mathrm{End}(E_2 \times E_2)$ denotes the endomorphism induced by the matrix $g \in M_2(\mathbb{Z})$, then we have

(32) $$\alpha_{g,f} = (f^t \times 1_{E_2})^{-1} \circ [g]_{E_2} \circ (f^t \times 1_{E_2}),$$

and so $\alpha_{g,f} \in \mathrm{Aut}(A)$ as $\deg(\alpha_{g,f}) = \deg([g]_{E_2}) = (\det(g))^2 = 1$; cf. Corollary 63.

Although we could deduce (31) directly from the pullback formula (70) by a tedious calculation, it is easier to apply formula (60) to the map $\Psi_f := \Phi_{\lambda_1 \otimes \lambda_2, f^t \times 1} : \mathrm{NS}(A) \to \mathrm{End}(E_2 \times E_2)$ which is introduced in Proposition 56 of the appendix. In our situation (60) becomes

(33) $$\Psi_f(\alpha_{g,f}^* D) = [g^t]_{E_2} \Psi_f(D)[g]_{E_2}, \quad \text{for all } D \in \mathrm{NS}(A),$$

because by (32) and (63) we have

(34) $$c_{f^t \times 1}(\alpha_{g,f}) = [g]_{E_2} \quad \text{and} \quad r_{\lambda_2 \otimes \lambda_2}(c_h(\alpha_{g,f})) = [g^t]_{E_2}.$$

Next we observe that by (19) we have

(35) $$\Psi_f(\mathbf{D}(a, b, cf)) = \begin{pmatrix} f & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} [a] & cf^t \\ cf & [b] \end{pmatrix} \begin{pmatrix} f^t & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} [ad] & [cd] \\ [cd] & [b] \end{pmatrix}, \ \forall a, b, c \in \mathbb{Z},$$

and so $\Psi_f(D_{s,f}) = [M(f_d(s))]_{E_2}$, where (as before) $M(q) = \left(\begin{smallmatrix} a & b \\ b & c \end{smallmatrix}\right) \in M_2(\mathbb{Z})$ denotes the matrix associated to the quadratic form $q = [a, 2b, c]$.

Since the action of g on quadratic forms is given by the formula $M(f_d(gs)) := M(f_d(s)g) = g^t M(f_d(s))g$, we thus obtain from (33) that

$$\Psi_f(\alpha_{g,f}^* D_{s,f}) = [g^t]_{E_2} \Psi_f(D_{s,f})[g]_{E_2} = [g^t M(f_d(s))g]_{E_2} = [M(f_d(sg))]_{E_2} = \Psi_f(D_{sg,f}),$$

and so (31) follows because Ψ_f is injective (cf. Corollary 58).

Corollary 40 *If* $A = E_1 \times E_2$ *and* $\mathrm{Hom}(E_1, E_2) = \mathbb{Z}h$*, where* $\deg(h) = d$*, then the map* $g \mapsto \alpha_{g,h}$ *defines a group isomorphism* $\Gamma_0^{\pm}(d) \xrightarrow{\sim} \mathrm{Aut}(A)$*, and hence the rule* $D_{s,f} \mapsto f_d(s)$ *induces bijections*

(36) $$\bar{f}_A : \mathcal{P}(A)/\mathrm{Aut}(A) \xrightarrow{\sim} Q_{-4d}^{(2)}(d)/\Gamma_0^{\pm}(d) \xrightarrow{\sim} Q_{-4d}^{(2)}/\mathrm{GL}_2(\mathbb{Z}).$$

Proof. By Proposition 39 we know that $g \mapsto \alpha_{g,h}$ defines an (injective) map $\Gamma_0^{\pm}(d) \to \mathrm{Aut}(A)$. Now since $\mathrm{Hom}(E_1, E_2) = \mathbb{Z}h$ and hence $\mathrm{Hom}(E_2, E_1) = \mathbb{Z}h^t$, we see that every $\alpha \in \mathrm{Aut}(A)$ has the form $\alpha = \left(\begin{smallmatrix} a & bh^t \\ ch & e \end{smallmatrix}\right)$, for some $a, b, c, e \in \mathbb{Z}$. But since $1 = \deg(\alpha) = (ae - bcd)^2$ by (69) (cf. proof of Proposition 39), we see that $g := \left(\begin{smallmatrix} a & b \\ cd & e \end{smallmatrix}\right) \in \Gamma_0^{\pm}(d)$ and so $\alpha = \alpha_{g,h}$. Thus, the map $g \mapsto \alpha_{g,h}$ is bijective. Moreover, since $c_{h^t \times 1}$ is a ring homomorphism, it follows from (34) that this bijection is an isomorphism of groups.

By combining Proposition 31 with Lemma 14 we see that the map $D_{s,h} \mapsto s \mapsto f_d(s)$ defines a bijection $f_A : \mathcal{P}(A) \xrightarrow{\sim} Q^{(2)}_{-4d}(d)$. By (31) this is $\Gamma_0^{\pm}(d)$-equivariant, and so the first bijection of (36) follows. The second follows from Lemma 20.

Proof of Proposition 38. If C is a smooth curve of genus 2 on A, then it defines a principal polarization on A (cf. Weil[36] or [19]), and so $C \equiv D_{s,h}$ with $s \in P(d)$ by Proposition 31. Moreover, $q_C \approx q_s$ by (the proof of) Theorem 30, so $f_d(s) \notin \mathrm{Ker}(\pi'_d)$ by Corollary 18 because $q_C \not\approx 1_{-16d}$ by Proposition 31.

If C' is another curve on A which is isomorphic to C, then by Torelli's theorem there exists an automorphism $\alpha \in \mathrm{Aut}(A)$ with $\alpha(C) = C'$, and so it follows from by Corollary 40 that the isomorphism class is uniquely determined by the $\mathrm{GL}_2(\mathbb{Z})$-equivalence class of $f_d(s)$.

Corollary 41 *Let $A = E_1 \times E_2$, where $\mathrm{Hom}(E_1, E_2) = \mathbb{Z}h$, and let $d = \deg(h)$. Then the number N_A of isomorphism classes of smooth genus 2 curves on A is*

$$N_A = \#(Q^{(2)}_{-4d}/\mathrm{GL}_2(\mathbb{Z})) - 2^{\omega(d)-1} = \begin{cases} \frac{1}{2}h(-4d) & \text{if } d \equiv 0, 1, 5 \pmod 8 \\ \frac{1}{2}(h(-4d) - 2^{\omega(d)-1}) & \text{if } d \equiv 2, 4, 6 \pmod 8 \\ \frac{1}{2}(h(-4d) + h(-d)) & \text{if } d \equiv 3, 7 \pmod 8 \end{cases},$$

except when $d = 1$; in that case $N_A = 0$.

Proof. By Corollary 40 the total number of isomorphism classes of principal polarizations on A is $\#(Q^{(2)}_{-4d}/\mathrm{GL}_2(\mathbb{Z}))$. By Proposition 38 we know that $f_d(s) \in Q^{(2)}_{-4d}$ corresponds to a smooth curve if and only if $f_d(s) \notin \mathrm{Ker}(\pi'_d)$, and so the first formula for N_A follows from (12). The second formula follows from this and (14) because $\#(Q^{(1)}_D/\mathrm{GL}_2(\mathbb{Z})) = \frac{1}{2}(h(D) + g(D))$.

Remark 42 The number N_A was also determined by Hayashida [12], §7-8, but his formula for N_A is much more complicated than the one above since he gives the result in terms of the class number h_K of the associated imaginary quadratic field $K = \mathbb{Q}(\sqrt{-d})$. However, by using the well-known relation between $h(-16d)$ and h_K (cf. Lang[24], p. 95), a somewhat tedious calculation shows that the two formulae give the same result.

8 The irreducibility of $H(q)$

The next task is to show that the generalized Humbert variety $H(q)$ is a closed and irreducible subset of A_2 when q is quadratic form of type d. This will be done by exhibiting $H(q)$ as the image of the modular curve $X_0(d)$ by a suitable morphism μ_s.

To define this morphism, recall that $X_0(d)$ classifies *cyclic* isogenies of degree d of elliptic curves, i.e. $X_0(d)(K)$ can be identified with the set of isomorphism classes $\langle f : E \to E'\rangle$, where f is a cyclic isogeny of degree d; cf. [4], p. 283, or [22], p. 100.

Proposition 43 *Let $s \in P(d)$. Then the rule*

$$\langle f : E \to E'\rangle \mapsto \langle E \times E', D_{s,f}\rangle = \langle E \times E', \phi_{D_{s,f}}\rangle$$

defines a proper *morphism $\mu_s : X_0(d) \to A_2$ with image $\mu_s(X_0(N)) = H(q_s)$, where q_s is the quadratic form defined by* (6).

Proof. Recall from Corollary 24 that $D_{s,f} \in \mathcal{P}(E \times E')$, so $\mu_s(f) \in A_2(K)$, i.e. $\mu_s(f)$ is a principally polarized abelian variety. Since this formation is compatible with isomorphisms, we thus see that this rule defines a map $\mu_s : X_0(d)(K) \to A_2(K)$.

To show that μ_s comes from a morphism of varieties, we shall use the fact that both $X_0(d)$ and A_2 are the coarse moduli spaces of functors $\mathcal{X}_0(d)$ and $\mathcal{A}_2 = \mathcal{A}_{2,1,1}$ on $\underline{Sch}_{/K}$, respectively. It is thus enough to construct a morphism of functors $\tilde{\mu}_s = \{\tilde{\mu}_{s,S}\}_S : \mathcal{X}_0(d) \to \mathcal{A}_2$ which extends μ_s (i.e. $\tilde{\mu}_{s,S} = \mu_s$ for $S = \mathrm{Spec}(K)$).

To construct $\tilde{\mu}_s$, we can use almost the same definition as for μ_s. Indeed, given a K-scheme S, then $\mathcal{X}_0(d)(S)$ consists of isomorphism classes $\langle f : E \to E'\rangle$ in which $f : E \to E'$ is an isogeny of elliptic curves $/S$ which is cyclic in the sense of [22], p. 100. Moreover, $\mathcal{A}_2(S)$ consists of isomorphism classes $\langle A, \lambda\rangle$ of principally polarized abelian schemes A/S of dimension 2; cf. [32], p. 129. We now define

$$\tilde{\mu}_{s,S}(\langle f : E \to E'\rangle) = \langle E \times_S E', \lambda_{s,f}\rangle,$$

where $\lambda_{s,f} : A := E \times_S E' \to \hat{A}$ is the principal polarization defined in Lemma 44 below.

It is clear that this definition is compatible with isomorphisms, and so we obtain a map $\tilde{\mu}_{s,S} : \mathcal{X}_0(d) \to \mathcal{A}_2(S)$. Note that for $S = \mathrm{Spec}(K)$ we have $\lambda_{s,f} = \phi_{D_{s,f}}$ (cf. proof of Lemma 44 below) and so $\tilde{\mu}_{s,S} = \mu_s$ agrees with the map μ_s as defined above. Moreover, since this construction is compatible with base change, the collection $\tilde{\mu}_s = \{\tilde{\mu}_{s,S}\}_S$ defines a morphism of functors, which therefore induces a morphism $\mu_s : X_0(d) \to A_2$ between the coarse moduli schemes.

By Proposition 28 we know that $\mu_s(X_0(d)) \subset H(q_s)$. On the other hand, the proof of Theorem 13 in §6 shows that if $\langle A, \theta\rangle \in H(q_s)$, then $(A, \theta) \simeq (E \times E', D_{s,f})$ for some cyclic isogeny $f : E \to E'$ of degree d, and so $\langle A, \theta\rangle = \mu_s(\langle f\rangle)$. Thus $\mu_s(X_0(d)) = H(q_s)$, as claimed.

It remains to show that μ_s is proper. Since $X_0(d)$ and A_2 are of finite type over K, it is enough to check that the functor $\tilde{\mu}_s$ satisfies the valuative criterion of properness. Thus, let $S = \mathrm{Spec}(R)$ be a discrete valuation ring with quotient field $F \supset K$ and let $y = \langle A, \lambda \rangle \in \mathcal{A}_2(S)$ be such that there exists $x_F = \langle E_1 \xrightarrow{h} E_2 \rangle \in \mathcal{X}_0(d)(F)$ with $\tilde{\mu}_{s,F}(x_F) = \langle A_F, \lambda_F \rangle$, where $A_F = A \otimes F$ and $\lambda_F = \lambda \otimes F$. We want to show that x_F extends to $x \in \mathcal{X}_0(d)(S)$ and that $\tilde{\mu}_{s,S}(x) = y$. For this we observe that since $A_F \simeq E_1 \times E_2$, and A_F has good reduction over R by hypothesis, it follows that the same is true for E_i, and so there exist elliptic curves $\tilde{E}_i/R$ with $\tilde{E}_i \otimes F = E_i$. By the Néron property we know that $A \simeq \tilde{E}_1 \times_S \tilde{E}_2$ and that h extends to $\tilde{h} : \tilde{E}_1 \to \tilde{E}_2$. From [22], p. 162, it follows that $\tilde{h}$ is again cyclic, so $x = \langle \tilde{h} \rangle \in \mathcal{X}_0(d)(S)$. We then have $\tilde{\mu}_s(x) = y$ because $\lambda_{s,\tilde{h}}$ and λ agree on the generic fibre, and so $\tilde{\mu}_s$ is proper.

Lemma 44 *Let $f : E_1 \to E_2$ be an isogeny of degree d between two elliptic curves over a scheme S, and let $s = (n_1, n_2, k) \in P(d)$. If $\lambda_i : E_i \xrightarrow{\sim} \hat{E}_i$ denotes the canonical polarization of E_i, and $\lambda_1 \otimes \lambda_2$ the product polarization, then*

$$\lambda_{s,f} = \lambda_1 \otimes \lambda_2 \circ \begin{pmatrix} [n_1]_{E_1} & kf^t \\ kf & [n_2]_{E_2} \end{pmatrix}$$

is a principal polarization on $E_1 \times_S E_2$.

Proof. First note that if $S = \mathrm{Spec}(K)$, then $\lambda_{s,f} = \phi_{D_{s,f}}$ by (19). Thus, since the formation of $\lambda_{s,f}$ clearly commutes with base-change, it follows that $\lambda_{s,f}$ is a principal polarization (in the sense of [32], p. 120) once we have shown that $\lambda_{s,f}$ is an isomorphism. Now since $f^t f = [d]_{E_1}$ and $f f^t = [d]_{E_2}$ (cf. [22], p. 81), it follows from (5) that

$$\begin{pmatrix} [n_1]_{E_1} & kf^t \\ kf & [n_2]_{E_2} \end{pmatrix} \begin{pmatrix} [n_2]_{E_1} & -kf^t \\ -kf & [n_1]_{E_2} \end{pmatrix} = \begin{pmatrix} 1_{E_1} & 0 \\ 0 & 1_{E_2} \end{pmatrix}.$$

Thus, since the product polarization $\lambda_1 \otimes \lambda_2$ (which is defined as in §11) is an isomorphism, we see that $\lambda_{s,f}$ is an isomorphism.

Corollary 45 *If q is a quadratic form of type d, then $H(q)$ is a closed subvariety of A_2 of dimension 1. Moreover, if $\mathrm{char}(K) \nmid d$, then $H(q)$ is an irreducible curve.*

Proof. By Propositions 15 and 43 we have $H(q) = \mu_s(X_0(d))$, for some $s \in P(d)$, and so $H(q)$ is a closed subset since μ_s is proper. Moreover, $\dim H(q) = \dim X_0(d) = 1$ because $H(q)$ is infinite by Theorem 30. Finally, if $\mathrm{char}(K) \nmid d$, then $X_0(d)$ is irreducible (by Igusa), and hence so is its image $H(q)$.

Proof of Theorem 3. By Corollary 45 and Theorem 13 we see that the $H(q)$ for $q \in \bar{Q}_d^*$ are the irreducible components of $T(d)$. Since $H(q_1) \neq H(q_2)$ if $q_1 \not\approx q_2$ (cf. Corollary 32), we see that the number of such components is precisely $\#\bar{Q}_d^*$.

9 The action of Atkin-Lehner involutions

As is well-known, the curve $X_0(d)$ comes equipped with a group of automorphisms called *Atkin-Lehner involutions.* In order to understand the birational structure of $H(q)$, it is important to determine how these involutions act on the maps μ_s which were constructed in the previous section. Before stating the result, we first observe:

Proposition 46 *Let $s, s' \in P(d)$. Then $\mu_s = \mu_{s'}$ if and only if $f_d(s) \approx f_d(s')$.*

Proof. Suppose first that $f_d(s) = f_d(s')g$ with $g \in \mathrm{GL}_2(\mathbb{Z})$. Then by the proof of Lemma 20 we know that $g \in \Gamma_0^{\pm}(d)$, and so $f_d(s) = f_d(s'g)$ in the notation of (31). Thus, if $x = \langle f : E \to E' \rangle \in X_0(d)(K)$, then $\alpha_{g,f}$ defines by Proposition 39 an isomorphism $(E \times E', D_{s',f}) \simeq (E \times E', D_{s,f})$, and so $\mu_{s'}(x) = \mu_s(x)$. This proves that $\mu_s = \mu_{s'}$ provided that $X_0(d)$ is reduced. In the general case (i.e. when $\mathrm{char}(K)|d$), essentially the same argument (by replacing $D_{s,f}$ by $\lambda_{s,f}$ as in the proof of Proposition 43) shows that we actually have an equality $\tilde{\mu}_{s'} = \tilde{\mu}_s$ of morphisms of functors, and so the induced morphisms μ_s and $\mu_{s'}$ on the coarse moduli spaces are equal.

Conversely, suppose $\mu_s = \mu_{s'}$. Then in particular $\mu_s(x) = \mu_{s'}(x)$ for any point $x = \langle E \xrightarrow{f} E' \rangle \in X_0(d)(K)$ which we can take to be a non-CM point, i.e. we have $\mathrm{Hom}(E, E') = \mathbb{Z}f$. Then the equality $\mu_s(x) = \mu_{s'}(x)$ means that there is an $\alpha \in \mathrm{Aut}(E \times E')$ such that $\alpha^* D_{s,f} = D_{s',f}$. Now by Corollary 40 we know that $\alpha = \alpha_{g,f}$ for some $g \in \Gamma_0^{\pm}(d)$ and that $f_d(s)g = f_d(s')$. Thus, $f_d(s) \approx f_d(s')$, as asserted.

We now come to the action on the Atkin-Lehner involutions on the maps μ_s. For this, recall that each Atkin-Lehner involution α on $X_0(d)$ is uniquely defined by a divisor $d_1||d$ of d, i.e. by a divisor $d_1|d$ with the property that $\gcd(d_1, d/d_1) = 1$. We can thus write $\alpha = \alpha_{d_1}$; this will be explained in more detail below.

Theorem 47 *For each $d_1||d$, the Atkin-Lehner involution α_{d_1} permutes the μ_s's. More precisely, if $s \in P(d)$, then*

(37)
$$\mu_s \circ \alpha_{d_1} = \mu_{s'}, \quad \textit{where } f_d(s') \approx f_d(s) \circ a_{d_1}.$$

Here $a_{d_1} = [d_1, 0, d/d_1]$ if $s \in P(d)^{odd}$ and $a_{d_1} = [d_1, d_1, (d_1^2+d)/(4d_1)]$, if $s \in P(d)^{even}$. Moreover, the orbits of the group of Atkin-Lehner automorphisms on $\{\mu_s\}$ are in one-to-one correspondence with the images $H(q_s) = \mathrm{Im}(\mu_s)$; i.e. we have

(38)
$$\mathrm{Im}(\mu_{s_1}) = \mathrm{Im}(\mu_{s_2}) \quad \Leftrightarrow \quad \exists d_1||d \textit{ such that } \mu_{s_1} = \mu_{s_2} \circ \alpha_{d_1}.$$

In order to prove this theorem, we need some auxiliary results concerning Atkin-Lehner involutions. We begin with their (functorial) definition, i.e. with their action on the functor $\mathcal{X}_0(d)$ which was discussed in the previous section.

Fix $d_1||d$ and put $d_2 = d/d_1$. Let $h : E_1 \to E_2$ be a *cyclic* isogeny of degree d and for $i = 1, 2$, consider the quotient maps

$$h_{i1} = h_{i1}^{(h)} : E_1 \to E_i' := E_1/\mathrm{Ker}(h)[d_i], \quad \text{where } \mathrm{Ker}(h)[d_i] = \mathrm{Ker}(h) \cap E_1[d_i].$$

Note that h_{i1} is a cyclic isogeny of degree $\deg(h_{i1}) = d_i$, for $i = 1, 2$. By the universal property of quotients, there is a unique morphism $h_{i2}' = (h_{i2}')^{(h)} : E_i' \to E_2$ such that

$$h = h_{i2}' \circ h_{i1}, \quad \text{for } i = 1, 2. \tag{39}$$

Note that h_{i2}' is cyclic of degree d/d_i, for $i = 1, 2$. Put $h_{i2} = (h_{i2}')^t : E_2 \to E_i'$; thus, $h_{i2}' = h_{i2}^t$. Finally, put

$$h' = (h')^{(h)} := h_{21} \circ h_{11}^t = (h_{11} \circ h_{12}^t)^t : E_1' \to E_2'.$$

Note that h' is a cyclic isogeny of degree $d = d_1 d_2$ because h_{21} and h_{11}^t are cyclic of degree d_2 and degree d_1, respectively, and because $\gcd(d_1, d_2) = 1$. We observe that

$$h' = h_{21} \circ h_{11}^t = h_{22} \circ h_{12}^t. \tag{40}$$

(Indeed, the first equality is just the definition, whereas the second follows from the fact that $h_{21} h_{11}^t h_{11} = h_{21}[d_1] = [d_1] h_{21} = h_{22} h_{22}^t h_{12} \overset{(39)}{=} h_{22} h_{12}^t h_{11}$, because is an isogeny.) We now put

$$\alpha_{d_1}(\langle E_1 \xrightarrow{h} E_2 \rangle) = \langle E_1' \xrightarrow{h'} E_2' \rangle.$$

Note that the above construction works for elliptic curves over an arbitrary base scheme, and that it is compatible with base change. Thus, α_{d_1} defines a morphism of functors $\alpha_{d_1} : \mathcal{X}_0(d) \to \mathcal{X}_0(d)$. In fact, α_{d_1} is an automorphism (and even an involution, i.e. $\alpha_{d_1} \circ \alpha_{d_1} = 1_{\mathcal{X}_0(d)}$) because with the above notation we have

$$\alpha_{d_1}(\langle E_1' \xrightarrow{h'} E_2' \rangle) = \langle E_1 \xrightarrow{h} E_2 \rangle.$$

(To see this, note that first that by (40) we have $\mathrm{Ker}(h')[d_i] = \mathrm{Ker}(h_{1i}^t)$, and so $h_{i1}^{(h')} = h_{1i}^t : E_i' \to E_i$ and $(h_{i2}')^{(h')} = h_{2i}$. Thus $(h')^{(h')} = (h_{11}^{(h')} (h_{21}')^{(h')})^t = (h_{11}^t h_{21})^t = h_{21}^t h_{11} = h$, and the assertion follows.)

Over $\mathbb{C}$, the Atkin-Lehner involutions on $X_0(d)_{\mathbb{C}} = \Gamma_0(d)\backslash\mathfrak{H}$ can be defined by the Atkin-Lehner matrices of [1]. Although we don't need this here, we do need these matrices in order to construct isomorphisms between $E_1 \times E_2$ and $E_1' \times E_2'$.

Notation. Put $\Gamma_0^{\pm}(d_2)_{d_1} = \{g \in \Gamma_0^{\pm}(d_2) : g \equiv \left(\begin{smallmatrix} 0 & * \\ * & * \end{smallmatrix}\right) \pmod{d_1}\}$. Thus, $g \in \Gamma_0^{\pm}(d_2)_{d_1} \Leftrightarrow$

$$g = \begin{pmatrix} a_{11}d_1 & a_{12} \\ a_{21}d_2 & a_{22} \end{pmatrix} \quad \text{where } a_{ij} \in \mathbb{Z} \text{ and } a_{11}a_{22}d_1 - a_{12}a_{21}d_2 = \pm 1. \tag{41}$$

If $g \in \Gamma_0^{\pm}(d_2)_{d_1}$, then the *associated Atkin-Lehner matrix* is

$$\tilde{g} := \begin{pmatrix} 1 & 0 \\ 0 & d_1 \end{pmatrix} g = \begin{pmatrix} a_{11}d_1 & a_{12} \\ a_{21}d & a_{22}d_1 \end{pmatrix}. \tag{42}$$

Proposition 48 *Let* $\alpha_{d_1}(E_1 \xrightarrow{h} E_2) = (E_1' \xrightarrow{h'} E_2')$ *and let* $g \in \Gamma_0^{\pm}(d_2)_{d_1}$. *Put*

$$\alpha_g := \begin{pmatrix} a_{11}h_{11} & a_{12}h_{12} \\ a_{21}h_{21} & a_{22}h_{22} \end{pmatrix} \quad \textit{where} \quad g = \begin{pmatrix} a_{11}d_1 & a_{12} \\ a_{21}d_2 & a_{22} \end{pmatrix}$$

and where the $h_{ij} = h_{ij}^{(h)}$ *are as defined above. Then*

$$(h_{12} \times h_{22}) \circ [g]_{E_2} = \alpha_g \circ (h^t \times 1), \tag{43}$$

and so $\alpha_g : E_1 \times E_2 \xrightarrow{\sim} E_1' \times E_2'$ *is an isomorphism. Moreover,*

$$((h')^t \times 1) \circ [\tilde{g}]_{E_2'} = \alpha_g \circ (h^t \times 1) \circ (h_{22}^t \times h_{22}^t). \tag{44}$$

Proof. By (39) we have $h_{i1}h^t = h_{i1}(h_{ii2}^t h_{11})^t = h_{i1}h_{i1}^t h_{i2} = d_i h_{i2}$, and from this (43) follows immediately. Since $\det(g) = \pm 1$, we see that $\deg([g]_{E_2}) = (\pm 1)^2 = 1$; cf. Corollary 63. Thus, since $\deg(h_{12} \times h_{22}) = d_1 d_2 = d = \deg(h^t \times 1)$, it follows from (43) that $\deg(\alpha_g) = 1$, i.e. that α_g is an isomorphism.

To prove (44), note first that (40) shows that $(h_{12} \times h_{22}) \circ (h_{22}^t \times h_{22}^t) = (h')^t \times [d_1]$ (because $\deg(h_{22}) = d/d_2 = d_1$), and so by (43) we obtain $\alpha_g \circ (h^t \times 1) \circ (h_{22}^t \times h_{22}^t) = (h_{12} \times h_{22}) \circ [g]_{E_2} \circ (h_{22}^t \times h_{22}^t) = (h_{12} \times h_{22}) \circ (h_{22}^t \times h_{22}^t) \circ [g]_{E_2'} = ((h')^t \times [d_1]) \circ [g]_{E_2'} = ((h')^t \times 1) \circ [\tilde{g}]_{E_2'}$, which is (44).

In passing, we observe the following interesting fact concerning isomorphisms of product surfaces in the non-CM case; this will be used in the next section.

Proposition 49 *Let* (E_1, E_2) *and* (E_1', E_2') *be two pairs of elliptic curves, and assume that* $\mathrm{Hom}(E_1, E_2) = \mathbb{Z}h$ *and* $\mathrm{Hom}(E_1, E_2) = \mathbb{Z}h'$. *If* $d = \deg(h)$, *then*

$$E_1 \times E_2 \simeq E_1' \times E_2' \Leftrightarrow \exists\, d_1 || d \textit{ such that } \langle E_1' \xrightarrow{h'} E_2' \rangle = \alpha_{d_1}(\langle E_1 \xrightarrow{h} E_2 \rangle). \tag{45}$$

Proof. The one direction follows from Proposition 48. Conversely, suppose that there exists an isomorphism $f : E_1 \times E_2 \xrightarrow{\sim} E_1' \times E_2'$. Then $E_i' \sim E_1 \sim E_2$, and so $\mathrm{Hom}(E_i, E_j') = \mathbb{Z}h_{ji}$, for some (cyclic) $h_{ji} \in \mathrm{Hom}(E_i, E_j')$, for all $i, j = 1, 2$. We can thus write $f = (a_{ij}h_{ij})$ with $a_{ij} \in \mathbb{Z}$. Similarly, since $\mathrm{Hom}(E_j', E_i) = \mathbb{Z}h_{ji}^t$, we can write $g := f^{-1} = (b_{ij}h_{ji}^t)$ with $b_{ij} \in \mathbb{Z}$. Since $1_{E_1' \times E_2'} = fg = \left(\begin{smallmatrix} [c_{11}] & * \\ * & [c_{22}] \end{smallmatrix}\right)$, we obtain the relations

$$c_{11} = a_{11}b_{11}d_{11} + a_{12}b_{21}d_{12} = 1 \quad \text{and} \quad c_{22} = a_{21}b_{12}d_{21} + a_{22}b_{22}d_{22} = 1,$$

where $d_{ij} = \deg(h_{ij})$. From these we see that $\gcd(d_{11}, d_{12}) = 1 = \gcd(d_{21}, d_{22})$. Thus, $h_{12}^t h_{11} \in \mathrm{Hom}(E_1, E_2)$ is a composition of isogenies with cyclic kernels of relatively prime order, and hence also has cyclic kernel. This means that $h_{12}^t h_{11}$ is a generator of $\mathrm{Hom}(E_1, E_2)$ and hence $h_{12}^t h_{11} = \pm h$. By replacing h_{11} by $-h_{11}$ if necessary, we thus have $h = h_{12}^t h_{11}$. Similarly, $h_{22}^t h_{21} = h$, (replacing h_{21} by $-h_{21}$, if necessary). Thus (39) holds with $h'_{i2} = h_{i2}^t$.

Next, using the fact that $gf = 1_{E_1\times E_2}$, we obtain in a similar way the relations

$$a_{11}b_{11}d_{11} + a_{21}b_{12}d_{21} = 1 \quad \text{and} \quad a_{12}b_{21}d_{12} + a_{22}b_{22}d_{22} = 1,$$

and hence $\gcd(d_{11}, d_{21}) = 1 = \gcd(d_{12}, d_{22})$. Thus, since by (39) we have $d_{12}d_{11} = d_{22}d_{21}$, we see that $d_{11}|d_{22}$ and $d_{22}|d_{11}$, and hence $d_{11} = d_{22}$ and also $d_{12} = d_{21}$. Thus, if we put $d_i = d_{i1}$, then $d = d_1d_2$ and $(d_1, d_2) = 1$, so $d_1||d$ and $\mathrm{Ker}(h_{i1}) = \mathrm{Ker}(h)[d_i]$, for $i = 1, 2$. Now $h'^{(h)} = h_{21}\circ h_{11}^t \in \mathrm{Hom}(E'_1, E'_2)$ has cyclic kernel because $h_{12} = (h'_{12})^t$ and h_{11}^t both have cyclic kernels of orders $d_{12} = d_2$, and $d_{11} = d_1$, respectively, and $(d_1, d_2) = 1$. Thus, $h'^{(h)} = \pm h'$, and so $\alpha_{d_1}(\langle E_1 \xrightarrow{h} E_2\rangle) = \langle E'_1 \xrightarrow{h'} E'_2\rangle$, as claimed.

Remark 50 In terms of the terminology of [20], p. 99, condition (39) means that $(h, h_{11}, h'_{12}, h_{21}, h'_{22})$ is an *isogeny factor set* representing the *diamond configuration* $(h, \mathrm{Ker}(h)[d_1], \mathrm{Ker}(h)[d_2])$. Thus, Proposition 49 gives a (partial) explanation of why such factor sets arise in the study of product surfaces.

We now want to compute the pullback of divisors with respect the isomorphism α_g defined in Proposition 48. For this, we shall use the embedding $\Psi_h = \Phi_{\lambda_1\otimes\lambda_2, h^t\times 1}$ which was defined in the proof of Proposition 39.

Proposition 51 *In the situation of* Proposition 48 *we have*

(46) $$(h_{22}\times h_{22})\Psi_h(\alpha_g^*D')(h_{22}^t\times h_{22}^t) = [\tilde{g}^t]_{E'_2}\Psi_{h'}(D')[\tilde{g}]_{E'_2}, \quad \forall D' \in \mathrm{NS}(E'_1\times E'_2).$$

In particular, if $a', b', c' \in \mathbb{Z}$, then

(47) $$\alpha_g^*\mathbf{D}(a', b', c'h') = \mathbf{D}(a, b, ch),$$

where $a, b, c \in \mathbb{Z}$ are given by the matrix equation

(48) $$\begin{pmatrix} ad & cd \\ cd & b \end{pmatrix} = g^t \begin{pmatrix} a'd_2 & c'd \\ c'd & b'd_1 \end{pmatrix} g = \frac{1}{d_1}\tilde{g}^t \begin{pmatrix} a'd & c'd \\ c'd & b' \end{pmatrix} \tilde{g}.$$

Thus, if $s' \in P(d)$, then we have an isomorphism of principally polarized abelian surfaces

(49) $$\alpha_g : (E_1\times E_2, D_{s'\tilde{g},h}) \xrightarrow{\sim} (E'_1\times E'_2, D_{s',h'}),$$

where $s'\tilde{g} \in P(d)$ is defined by the rule $M(f_d(s'\tilde{g})) = \frac{1}{d_1}\tilde{g}^tM(f_d(s'))\tilde{g}$.

Proof. Since $r_{\lambda'_2\otimes\lambda'_2,\lambda_2\otimes\lambda_2}(h_{22}^t\times h_{22}^t) = h_{22}\times h_{22}$ (cf. (63)), it follows from the definitions and formula (55) of the appendix that the left hand side of (46) equals $(h_{22}^t\times h_{22}^t)^\flat(h^t\times 1)^\flat\Phi_{\lambda_1\otimes\lambda_2}(\alpha_g^*D') = (h_{22}^t\times h_{22}^t)^\flat(h^t\times 1)^\flat(\alpha_g)^\flat\Phi_{\lambda'_1\otimes\lambda'_2}(D') = (\alpha_g(h^t\times$

$1)(h_{22}^t \times h_{22}^t))^\flat \Phi_{\lambda_1' \otimes \lambda_2'}(D') = (((h')^t \times 1)[\tilde{g}]_{E_2'})^\flat \Phi_{\lambda_1' \otimes \lambda_2'}(D') = ([\tilde{g}]_{E_2'})^\flat \Psi_{h'}(D')$, where we have used (57) and (44) in the last three equalities. Since $r_{\lambda_2 \otimes \lambda_2'}([\tilde{g}]_{E_2'}) = [\tilde{g}^t]_{E_2'}$ by (63), we obtain $([\tilde{g}]_{E_2'})^\flat \Psi_{h'}(D') = [\tilde{g}^t]_{E_2'} \Psi_{h'}(D')[\tilde{g}]_{E_2'}$, which proves (46).

To prove (47), first note that the second equality of (48) follows immediately from the fact that $\tilde{g} = \mathrm{diag}(1, d_1)g$. Furthermore, by multiplying out the right hand side of (48), we see that if g has the form (41), then $a = a'd_1a_{11}^2 + 2dc'a_{11}a_{21} + b'd_2a_{21}^2, b = a'd_2a_{12}^2 + 2c'da_{12}a_{22} + b'd_1a_{22}^2, c = a'a_{11}a_{12} + c'(d_2a_{12}a_{21} + d_1a_{11}a_{22}) + b'a_{21}a_{22}$, and so $a, b, c \in \mathbb{Z}$. Now by (35) we have $\Psi_h(\mathbf{D}(a, b, ch)) = [g_1]_{E_2}$, where $g_1 = \left(\begin{smallmatrix} ad & cd \\ cd & b \end{smallmatrix}\right)$, and similarly $\Psi_{h'}(\mathbf{D}(a', b', c'h')) = [g_1']_{E_2'}$ with $g_1' = \left(\begin{smallmatrix} a'd & c'd \\ c'd & b' \end{smallmatrix}\right)$. Thus, if $D' = \mathbf{D}(a', b', c'h')$, then by (48) the right hand side of (46) equals $[d_1g_1]_{E_2'} = (h_{22} \times h_{22})(h_{22}^t \times h_{22}^t)[g_1]_{E_2'} = (h_{22} \times h_{22})[g_1]_{E_2}(h_{22}^t \times h_{22}^t) = (h_{22} \times h_{22})\Psi_h(D)(h_{22}^t \times h_{22}^t)$, where $D = \mathbf{D}(a, b, ch)$. Comparing this to the left hand side of (46) yields $\Psi_h(\alpha_g^*(D')) = \Psi_h(D)$ (because $h_{22} \times h_{22}$ and $h_{22}^t \times h_{22}^t$ are isogenies), and so (47) follows because Ψ_h is injective; cf. Corollary 58 of the appendix.

Finally, to prove (49), recall from Proposition 48 that $\alpha_g : E_1 \times E_2 \xrightarrow{\sim} E_1' \times E_2'$ is an isomorphism. Now by (47) we have $\alpha_g^* D_{s',h'} = D_{s'\tilde{g},h}$, and so (49) follows.

Proof of Theorem 47. Fix $s = (n_1, n_2, k) \in P(d)$ and let $g \in \Gamma_0^{\pm}(d_2)_{d_1}$. If $\tilde{g}$ is defined by (42), then a short computation shows that $\frac{1}{d_1}\tilde{g}^t M(f_d(s))\tilde{g} = M(f_d(s'))$, for some $s' \in P(d)$ and that $M(f_d(s')) = g^t M(q) g$, where $q = [n_1d_2, 2k, n_2d_1]$. Since $g \in \mathrm{GL}_2(\mathbb{Z})$, this implies that $f_d(s') \approx q$, and so Lemma 52 below shows that $f_d(s') \approx q \sim f_d(s) \circ a_{d_1}$. Thus, (37) follows once we have shown that $\mu_s \circ \alpha_{d_1} = \mu_{s'}$.

For this, let $x = \langle E_1 \xrightarrow{h} E_2 \rangle \in \mathcal{X}_0(d)$ and put $x' = \alpha_{d_1}(x) = \langle E_1' \xrightarrow{h'} E_2' \rangle$. Then $\mu_s(\alpha_{d_1}(x)) = \mu_s(x') = \langle E_1' \times E_2', D_{s,h'} \rangle$. Now by (49) we have $\alpha_g : (E_1 \times E_2, D_{s',h}) \xrightarrow{\sim} (E_1' \times E_2', D_{s,h})$, and so $\mu_s(\alpha_{d_1}(x)) = \mu_{s'}(x)$. This proves that $\mu_s \circ \alpha_{d_1} = \mu_{s'}$ when $X_0(d)$ is reduced. In the general case a similar argument (generalized to elliptic curves over K-schemes) shows that we have an equality $\tilde{\mu}_s \circ \alpha_{d_1} = \tilde{\mu}_{s'}$ of morphisms of functors, and so (37) holds in general.

It remains to prove (38). For this, let $s_1, s_2 \in P(d)$ be such that $\mathrm{Im}(\mu_{s_1}) = \mathrm{Im}(\mu_{s_2})$. Then Proposition 43 shows that $H(q_{s_1}) = H(q_{s_2})$ and so by Corollary 32 we have $q_{s_1} \approx q_{s_2}$. We now distinguish two cases.

If $s_1 \in P(d)^{odd}$, then q_{s_1} is primitive by Lemma 16 and hence so is q_{s_2}. Thus, also $s_2 \in P(d)^{odd}$. By Corollary 18 (and Remark 12) we thus have that $f_d(s_1) \sim f_d(s_1) \circ a$, where $a \in \mathrm{Ker}(\pi_d')$. By Corollary 19 we have $a \sim a_{d_1}$, for some $d_1||d$, and so (37) shows that $\mu_{s_1} \circ \alpha_{d_1} = \mu_{s_2}$, as desired.

Now suppose that $s_1 \in P(d)^{even}$; then also $s_2 \in P(d)^{even}$. Here $f_d(s_i) = 2f_d'(s_i)$, where $f_d'(s_i) \in Q_{-d}^{(1)}$, and by Corollary 18 we thus have $f_d'(s_1) \sim f_d'(s_2) \circ a$ with $a \in \bar{Q}_{-d}[2]$. By genus theory, it follows that $a \sim a_{d_1} = [d_1, d_1, (d_1 + d_2)/4]$, for some $d_1||d$, and so (37) shows again that $\mu_{s_1} \circ \alpha_{d_1} = \mu_{s_2}$. This proves one direction of (38), and so (38) follows since the other direction is trivial.

Lemma 52 *Let* $s = [n_1, n_2, k] \in P(d)$*, and put* $q = [d_2 n_1, 2k, d_1 n_2]$*, where* $d = d_1 d_2$ *with* $\gcd(d_1, d_2) = 1$*. Then* $f_d(s) \circ a_{d_1} \sim q$*, where* $a_{d_1} = [d_1, 0, d_2]$ *if* $s \in P(d)^{odd}$*, and* $a_{d_1} = [d_1, d_1, (d_1 + d_2)/4]$ *if* $s \in P(d)^{even}$*.*

Proof. If $s \in P(d)^{odd}$, then $f_d(s) = [dn_1, 2kd, n_2]$ is primitive of discriminant $-4d$, and the composition algorithm of Shanks (cf. [2], p. 64) shows that $a_{d_1} \circ f_d(s) \sim q$. Indeed, if $2 \nmid n_1$, apply [2], Th. 4.12, to $f_1 = [d_1, 2d_1, d_1 + d_2] \sim [d_1, 0, d_2]$ and $f_2 = f_d(s)$. Then (with the notation there) $m = n = d_1$, and so we can take $x = 1, y = 0$ and $z = dn_1 - d_1$, and so $f_1 \circ f_2 \sim [d_1 n_1 d/d_1^2, 2d_1 + 2z, *] = q$. On the other hand, if $2|n_1$, then $f_s(s) \sim [n_2 d, -2kd, n_1]$, where $2 \nmid n_2$, and then by the same argument $[d_2, 0, d_1] \circ [n_2 d, -2kd, n_1] \sim [n_2 d_1, -2kd, n_1 d_2] \sim q$. Thus $a_{d_1} \circ f_d(s) \sim q$ because $a_{d_1} \sim [d_2, 0, d_1]$.

Now suppose $s \in P(d)^{even}$. Then $f_d(s) = 2f'_d(s)$ where $f'_d(s) = [n'_1 d, kd, n'_2]$ is primitive of discriminant $-d$. Applying [2], Th. 4.12, to $f_1 = [d_1, d_1, (d_1 + d_2)/4]$ and $f_2 = f'_d(s)$ shows that $f_1 \circ f_2 \sim [n'_1 d_2, kd, n'_2 d_1]$ because here again $m = n = d_1$, and so we can take $x = 1$, $y = 0$, and $z = (kd - d_1)/2$. Thus $f_d(s) \circ a_{d_1} := 2(f'_d(s) \circ a_{d_1}) \sim 2[n'_1 d_2, kd, n'_2 d_1] = q$.

10 The birational structure of $H(q)$

In order to determine the birational structure of $H(q)$, we shall first calculate the automorphism group $\mathrm{Aut}(\mu_s)$ of the morphism $\mu_s : X_0(d) \to H(q_s)$. As we shall see, the *Fricke involution* $w_d = \alpha_d$ on $X_0(d)$ always lies in $\mathrm{Aut}(\mu_s)$. However, if q_s is an ambiguous form, then there is another Atkin-Lehner involution α_s in $\mathrm{Aut}(\mu_s)$, as the following result shows.

Proposition 53 *(a) If* $s \in P(d)^{odd}$*, then* $q_s \in \bar{Q}^2_{-16d}[2]$ *(i.e.,* q_s *is ambiguous) if and only if* $f_d(s)^2 \in \mathrm{Ker}(\pi'_d)$*. If this is the case, then there is a unique* $d_1 || d$ *with* $d_1 \le d_2 := d/d_1$ *such that* $[d_1, 0, d_2] \sim \pi_{-4d,2}(q_s) \sim f_d^2(s)$*.*

(b) If $s \in P(d)^{even}$*, then* $q'_s := \frac{1}{4} q_s \in \bar{Q}^2_{-d}[2]$ *(i.e.,* q_s *is ambiguous) if and only if* $f'_d(s)^2 \in \bar{Q}^2_{-d}[2]$*. If this is the case, then there is a unique* $d_1 || d$ *with* $d_1 \le d_2 := d/d_1$ *such that* $[d_1, d_1, (d_1 + d_2)/4] \sim q'_s \sim f'_d(s)^2$*.*

(c) Let $s \in P(d)$ *and put* $\alpha_s = \alpha_{d_1}$*, where* d_1 *is as above, if* q_s *is ambiguous, and* $d_1 = 1$ *otherwise. Then* $G(q_s) := \langle w_d, \alpha_s \rangle \le \mathrm{Aut}(\mu_s)$*, and hence* μ_s *factors over the quotient map* $\pi_{q_s} : X_0(d) \to X_0(d)^+_{q_s} := X_0(d)/G(q_s)$*.*

(d) We have $G(q_s) = \langle w_d \rangle$ *if and only if either* q_s *is not ambiguous or if* $\frac{1}{4} q_s \sim 1_{-d}$ *or if* $q_s \sim q_d$*, where* q_d *is as in* Theorem 36*.*

Proof. (a) By (8) we have $f_d(s)^2 \sim \pi_{-4d,2}(q_s)$ and by (10) we have $\pi'_d(\pi_{-4d,2}(q_s)) \sim q_s^2$. Thus, $f_d(s)^2 \in \mathrm{Ker}(\pi'_d) \Leftrightarrow q_s^2 \sim 1 \Leftrightarrow q_s \in \bar{Q}^2_{-16d}[2]$. This proves the first assertion, and the second follows from (13).

(b) By (9) we have $f'_d(s)^2 \sim q'_s$, so the first assertion is trivial. The second follows immediately from the fact that the forms $[d_1, d_1, (d_1+d_2)/2]$ represent all ambiguous classes in $\bar{Q}_{-d}$; cf. proof of Theorem 47.

(c) It is enough to show that $\mu_s \circ \alpha'_d = \mu_s$ for $d' = d$ and $d' = d_1$, and this follows from Theorem 47 once we have shown that $f_d(s) \approx f_d(s) \circ a_{d'}$. This is clear if $d' = d$ (or $d' = d_1 = 1$) because then $a_{d'} \sim 1$. (Indeed, if $s \in P(d)^{odd}$, then $a_d = [d, 0, 1] \sim 1_{-4d} = a_1$, and if $s \in P(d)^{even}$, then $a_d = [d, d, \frac{d+1}{4}] \sim 1_{-d} = a_1$.) On the other hand, if $d' = d_1$ and we are in the situation of (a), then $f_d(s)^2 \sim a_{d_1} \sim a_{d_1}^{-1}$ and then $f_d(s) \approx f_d(s)^{-1} \sim f_d(s) \circ a_{d_1}$. Similarly, if we are in the situation of (b), then $f'_d(s)^2 \sim a_{d_1} \sim a_{d_1}^{-1}$ and then $f'_d(s) \approx f'_d(s)^{-1} \sim f'_d(s) \circ a_{d_1}$, so again $f_d(s) \approx f_d(s) \circ a_{d_1}$.

(d) Since $\langle w_d \rangle = \{\alpha_1, \alpha_d\}$, we see that $G(s) = \langle w_d \rangle \Leftrightarrow d_1 = 1$ (because $d_1 \leq d/d_1$). Thus, if q_s is not ambiguous, then the assertion is clear, so assume q_s is ambiguous. If q_s is not primitive, then by part (b) we see that $d_1 = 1 \Leftrightarrow a_{d_1} \sim 1_{-d} \Leftrightarrow q'_s \sim 1_{-d}$, and if q_s is primitive, then by part (a) we have $d_1 = 1 \Leftrightarrow a_{d_1} \sim 1_{-4d} \Leftrightarrow q_s \in \mathrm{Ker}(\pi_{-4d,2}) \Leftrightarrow q_s \sim q_d$, the latter by (11).

We now show that $\mathrm{Aut}(\mu_s) = G(q_s)$ by examining the fibres of μ_s at non-CM points.

Proposition 54 *Let $s \in P(d)$ and let $x \in X_0(d)(K)$ be a non-CM point. Then*

$$\mu_s^{-1}(\mu_s(x)) = G(q_s)x = \{x, w_d(x), \alpha_s(x), w_d\alpha_s(x)\}, \tag{50}$$

and so $\mathrm{Aut}(\mu_s) = G(q_s)$, *provided that* $\mathrm{char}(K) \nmid d$.

Proof. Write $x = \langle E_1 \xrightarrow{h} E_2 \rangle$ and let $y = \langle E'_1 \xrightarrow{h'} E'_2 \rangle \in X_0(d)(K)$. Then we have:

$$\mu_s(x) = \mu_s(y) \ \Leftrightarrow \ y = \alpha_{d_1}(x), \text{ for some } d_1 || d \text{ with } f_d(s) \approx f_d(s) \circ a_{d_1}. \tag{51}$$

Indeed, if $y = \alpha_{d_1}(x)$ and $f_d(s) \approx f_d(s) \circ a_{d_1}$, then $\mu_s(y) = \mu_s(\alpha_{d_1}(x)) = \mu_s(x)$ by (37). Conversely, if $\mu_s(x) = \mu_s(y)$, then $\exists \alpha : E_1 \times E_2 \xrightarrow{\sim} E'_2 \times E'_2$ such that $\alpha^* D_{s,h'} = D_{s,h}$. Then by Proposition 49 we know that $\exists d_1 || d = \deg(h)$ such that $y = \alpha_{d_1}(x)$, and so by Theorem 47 we have $\mu_s(y) = \mu_{s'}(x)$, where $s' \in P(d)$ is such that $f_d(s') \sim f_d(s) \circ a_{d_1}$. Thus, $\mu_s(x) = \mu_{s'}(x)$, which means that $(E_1 \times E_2, D_{s,h}) \simeq (E_1 \times E_2, D_{s',h})$. From Corollary 40 it follows that $f_d(s) \approx f_d(s') \sim f_d(s) \circ a_{d_1}$, and so (51) holds.

We now analyze the condition that $f_d(s) \approx f_d(s) \circ a_{d_1}$. For this, assume first that $f_d(s)$ is primitive, i.e. that $s \in P(d)^{odd}$. Then we have

$$f_d(s) \approx f_d(s) \circ a_{d_1} \ \Leftrightarrow \ a_{d_1} \sim 1 \text{ or } a_{d_1} \sim f_d(s)^2 \sim \pi_{-4d,2}(q_s). \tag{52}$$

Indeed, by Remark 12 we see that this condition holds if and only if either $f_d(s) \sim f_d(s) \circ a_{d_1}$ or $f_d(s)^{-1} \sim f_d(s) \circ a_{d_1}$. In the first case this means that a_{d_1} is principal, and the second case we have $a_{d_1} \sim a_{d_1}^{-1} \sim f_d(s)^2 \sim \pi_{-4d,2}(q_s)$, the latter by (8).

This proves (52). Note that the second condition implies by Proposition 53 that $q_s \in \bar{Q}^2_{-16d}[2]$ because $a_{d_1} \in \mathrm{Ker}(\pi'_d)$ by (13).

Thus, if $q_s \notin \bar{Q}^2_{-16d}[2]$, or if $q_s \sim q_d$, then the right hand side of (52) reduces to the condition $a_{d_1} \sim 1$ (because $\mathrm{Ker}(\pi_{-4d,2}) = \langle q_d \rangle$ by (11)), and so by reduction theory we see that this is the case if and only $d_1 = 1$ or $d_1 = d$. Thus, in this case it follows from (51) and (52) that $\mu_s(x) = \mu_s(y) \Leftrightarrow y \in \{x, w_d(x)\} = G(q_s)x$.

Next, suppose that $q_s \in \bar{Q}^2_{-16d}[2]$ but $q_s \not\sim q_d$. Then by Proposition 53(a) we have $a = a_{d_1}$, for some $d_1 || d$ with $d_1 \le d_2 = d/d_1$. Since $a_{d_2} \sim a_{d_1}$ and $\alpha_{d_2} = w_d \alpha_{d_1}$, it thus follows from (51)and (52) that (50) holds.

Now suppose that $f_d(s)$ is not primitive, i.e. $s \in P(d)^{even}$. Then $f_d(s) = 2f'_d(s)$ with $f'_d(s) \in \bar{Q}_{-d}$ and $q_s = 4q'$ with $q' \sim f'_d(s)^2$; cf. Lemma 16(b). In this case a similar argument to the one above shows that

$$(53) \qquad f_d(s) \approx f_d(s) \circ a_{d_1} \;\Leftrightarrow\; a_{d_1} \sim 1 \text{ or } a_{d_1} \sim f'_d(s)^2 \sim q'.$$

Thus, if $q' \notin \bar{Q}_{-d}[2]$ or if $q' \sim 1_{-d}$, then the right hand side of (53) reduces to the condition $a_{d_1} \sim 1$ and so as before we see that $\mu_s^{-1}(\mu_s(x)) = \{x, w_d(x)\} = G(q_s)x$ in this case. On the other hand, if $q' \in \bar{Q}_{-d}[2] \setminus \{1_{-d}\}$, then one concludes by a similar argument as above that (50) holds.

To verify the last assertion, assume $\mathrm{char}(K) \nmid d$. Then $\mu_s : X_0(d) \to H(q_s)$ is finite because it is a proper, surjective morphism between irreducible curves; cf. EGA (II, 7.4.4) and EGA (III, 4.4.2). Thus, from (50) we see that the separable degree $\deg_s(\mu)$ of μ_s equals $|G(q_s)|$ because there are infinitely many non-CM points on $X_0(d)$. We thus have $|G(q_s)| \le |\mathrm{Aut}(\mu_s)| \le \deg_s(\mu_s) = |G(q_s)|$, and so we have equality throughout. In particular, $G(q_s) = \mathrm{Aut}(\mu_s)$, as claimed.

Theorem 55 *Let $q \in \bar{Q}^*_d$, and suppose that* $\mathrm{char}(K) \nmid d$. *Then $X_0(q)^+_q$ is the normalization of $H(q)$. In particular, $X_0(q)^+$ is the normalization of $H(q)$ if and only if either q is not ambiguous or if $\frac{1}{4}q \sim 1_{-d}$ or if $q_s \sim q_d$, where q_d is as in* Theorem 36.

Proof. Since $q \sim q_s$, for some $s \in P(d)$ by Proposition 15, we see that the last assertion follows from the first assertion together with Proposition 53(d).

To prove the first assertion, recall that by Proposition 53(c) we have that $\mu_s = \bar{\mu}_s \circ \pi_q$, for some morphism $\bar{\mu}_s : X_0(q)^+_q \to H(q)$. Note that $X_0(q)^+_q$ is affine and that hence $\bar{\mu}_s$ is again finite (use EGA (II, 5.4.3)). Since $X_0(q)^+_q$ is normal, we see that $\bar{\mu}_s = \nu \circ \tilde{\mu}_s$ factors over the normalization $\nu : \tilde{H}(q) \to H(q)$. By the proof of Proposition 54 we know that $\deg_s(\mu_s) = \deg(\pi_q)$, and so we see that $\deg_s(\tilde{\mu}_s) = 1$, i.e. that μ_s is purely inseparable. Thus, the assertion follows once we have shown that $\tilde{\mu}_s$ or, equivalently, that μ_s is separable. Since this is automatic if $\mathrm{char}(K) = 0$, it remains to verify this assertion if $p = \mathrm{char}(K) \neq 0$.

For this, we shall use a specialization argument. Let $R = \mathbb{Z}_{(p)} \subset \mathbb{Q}$ denote the discrete valuation ring with residue field $\mathbb{F}_p$, and let $X_0(d)/R$ and A_2/R be the coarse moduli schemes of the functors $\mathcal{X}_0(d)$ and $\mathcal{A}_2$ on $\underline{Sch}_{/R}$, respectively. Since $p \nmid d$, we know that $X_0(R)/R$ is smooth and that hence its fibres are the coarse moduli schemes of the corresponding fibre functors; cf. [22], p. 510. In addition, one has that the fibres of A_2 are the coarse moduli schemes its fibre functors; cf. Igusa[17], for M_2 in place of A_2 (which suffices for our purposes). Now the method of proof of Proposition 43 extends to construct an R-morphism $\mu_s : X_0(d) \to A_2$, and the same proof shows that μ_s is again proper. Thus, by Fulton [9], Proposition 20.3(a), we have $\deg(\mu_s^\circ) = \deg(\mu_s^s)$, where μ_s° and μ_s^s are the restrictions of μ_s to the generic and special fibres of $X_0(d)$, respectively. Since these can be identified with the previously constructed morphisms μ_s (over $K = \mathbb{Q}$ and over $K = \mathbb{F}_p$, respectively), we have by (the proof of) Proposition 54 that $\deg_s(\mu_s^\circ) = |G(q_s)| = \deg_s(\mu_s^s)$. But since $\deg_s(\mu_s^\circ) = \deg(\mu_s^\circ)$, it follows that also $\deg_s(\mu_s^s) = \deg(\mu_s^s)$, and so μ_s^s is separable.

Proof of Theorems 1 and 4. From the definition of $G(q_s)$, it clear that Theorem 4 and the last part of Theorem 1 are special cases of Theorem 55. Moreover, the fact that $T(d)$ is a closed subset (and that it is a finite union of curves) follows from Theorem 13 and Proposition 43.

11 Appendix: The Néron-Severi group

The purpose of this appendix is to present some basic facts about the Néron-Severi groups of abelian varieties which were used throughout the paper.

Let A be an abelian variety over an algebraically closed field K, and let $\mathrm{NS}(A) = \mathrm{Pic}(A)/\mathrm{Pic}^0(A)$ denote the Néron-Severi group of A. If A has a principal polarization $\lambda = \phi_\theta : A \xrightarrow{\sim} \hat{A}$ (cf. Milne[30], p. 126), then $\mathrm{NS}(A)$ can be interpreted as a subgroup of $\mathrm{End}(A)$. More precisely, if r_λ denotes the Rosati involution on $\mathrm{End}(A)$ (which is defined by the rule $r_\lambda(\alpha) = \lambda^{-1}\hat{\alpha}\lambda$), then by Mumford[33], p. 190, 209, the map $D \mapsto \lambda^{-1}\phi_D$ defines an isomorphism

$$\Phi_\lambda : \mathrm{NS}(A) \xrightarrow{\sim} \mathrm{End}_\lambda(A) := \{\alpha \in \mathrm{End}(A) : r_\lambda(\alpha) = \alpha\}. \tag{54}$$

The isomorphism Φ_λ satisfies the following functorial property.

Proposition 56 *If (A_i, λ_i), $i = 1, 2$, are two principally polarized abelian varieties, and $h \in \mathrm{Hom}(A_1, A_2)$,*

$$\Phi_{\lambda_1}(h^*D) = r_{\lambda_1,\lambda_2}(h)\Phi_{\lambda_2}(D)h, \quad \forall D \in \mathrm{NS}(A_2), \tag{55}$$

where $r_{\lambda_1,\lambda_2}(h) = \lambda_1^{-1}\hat{h}\lambda_2 \in \mathrm{Hom}(A_2, A_1)$. In other words, $\Phi_{\lambda_1} \circ h^* = h^\flat \circ \Phi_{\lambda_2}$, where $h^\flat : \mathrm{End}(A_2) \to \mathrm{End}(A_1)$ is defined by $h^\flat(\alpha) = r_{\lambda_1,\lambda_2}(h)\alpha h$. Moreover,

$$r_{\lambda_1} \circ h^\flat = h^\flat \circ r_{\lambda_2}, \tag{56}$$

and hence $\Phi_{\lambda_1} \circ h^*$ defines a homomorphism $\Phi_{\lambda_1,h} : \mathrm{NS}(A_2) \to \mathrm{End}_{\lambda_1}(A_1)$.

Proof. The first formula follows immediately from the definitions and the fact that $\phi_{h^*D} = \hat{h} \circ \phi_D \circ h$, for $D \in \mathrm{Pic}(A)$. Similarly, (56) follows from the definitions together with the fact that $r_{\lambda_1,\lambda_2}(h)\widehat{} \circ \lambda_1 = \lambda_2 \circ h$.

Remark 57 For later reference, let us observe here that the assignment $h \mapsto h^\flat = h^\flat_{\lambda_1,\lambda_2}$ is functorial: if (A_i, λ_i), $i = 1, 2, 3$, are three principally polarized abelian varieties, and $h_i \in \mathrm{Hom}(A_i, A_{i+1})$ for $i = 1, 2$, then

$$(h_2 \circ h_1)^\flat_{\lambda_1,\lambda_2} = (h_1)^\flat_{\lambda_1,\lambda_2} \circ (h_2)^\flat_{\lambda_2,\lambda_3}. \tag{57}$$

This follows easily from the definitions and the fact that $r_{\lambda_1,\lambda_3}(h_1 \circ h_2) = r_{\lambda_1,\lambda_2}(h_1) \circ r_{\lambda_2,\lambda_3}(h_2)$.

In the case that h is an isogeny, we can define $h^\flat$ in another way.

Corollary 58 *If $h : A_1 \to A_2$ is an isogeny, then the rule $c_h(\alpha) = h^{-1}\alpha h$ defines a ring isomorphism $c_h : \mathrm{End}^0(A_2) \xrightarrow{\sim} \mathrm{End}^0(A_1)$ which is related to $h^\flat$ by the formula*

$$h^\flat(\alpha) = \beta c_h(\alpha), \quad \textit{where } \beta = h^\flat(1) = r_{\lambda_1,\lambda_2}(h)h, \tag{58}$$

and we have

$$r_{\lambda_1}(c_h(\alpha)) = \beta c_h(r_{\lambda_2}(\alpha))\beta^{-1}, \quad \forall \alpha \in \mathrm{End}^0(A_2). \tag{59}$$

Thus $\Phi_{\lambda_1,h} := \Phi_{\lambda_1} \circ h^* = h^\flat \circ \Phi_{\lambda_2} = \beta(c_h \circ \Phi_{\lambda_2}) : \mathrm{NS}(A_2) \to \mathrm{End}_{\lambda_1}(A_1)$ is an injective group homomorphism which satisfies

$$\Phi_{\lambda_1,h}(\alpha^*D) = r_{\lambda_1}(c_h(\alpha))\Phi_{\lambda_1,h}(D)c_h(\alpha), \quad \forall D \in \mathrm{NS}(A_2),\ \alpha \in \mathrm{End}(A_2). \tag{60}$$

Proof. It is clear that c_h is a ring isomorphism and that (58) holds. Thus, since $r_{\lambda_1}(\beta) = r_{\lambda_1}(h^\flat(1)) = h^\flat(1) = \beta$ by (56), we see that $r_{\lambda_1}(c_h(\alpha))\beta = r_{\lambda_1}(c_h(\alpha))r_{\lambda_1}(\beta) = r_{\lambda_1}(\beta c_h(\alpha)) \overset{(58)}{=} r_{\lambda_1}(h^\flat(\alpha)) \overset{(56)}{=} h^\flat(r_{\lambda_2}(\alpha)) \overset{(58)}{=} \beta c_h(r_{\lambda_2}(\alpha)$, and so (59) follows.

Write $\Phi = \Phi_{\lambda_1,h}$. Then $\Phi = h^\flat \circ \Phi_{\lambda_2}$ by (55) and hence $\Phi = \beta(c_h \circ \Phi_{\lambda_2})$ by (58). From the latter expression it is clear that Φ is an injective group homomorphism. Moreover, since c_h is multiplicative, we have $\Phi(\alpha^*D) = \beta c_h(\Phi_{\lambda_2}(\alpha^*D)) \overset{(55)}{=} \beta c_h(r_{\lambda_2}(\alpha)\Phi_{\lambda_2}(D)\alpha) \overset{(59)}{=} r_{\lambda_1}(c_h(\alpha))\beta c_h(\Phi_{\lambda_2}(D))c_h(\alpha)$, which proves (60).

Let (A_i, λ_i) be two principally polarized abelian varieties, and $A = A_1 \times A_2$ be the product variety with projections $p_i : A \to A_i$ and inclusions $e_i : A_i \to A$. Then $p := \hat{p}_1 + \hat{p}_2 : \hat{A}_1 \times \hat{A}_2 \xrightarrow{\sim} \hat{A}$ is an isomorphism, and $\lambda_1 \times \lambda_2 := p \circ \lambda_1 \times \lambda_2 : A \xrightarrow{\sim} \hat{A}$ is a principal polarization of A, called the product polarization. (Note that if $\lambda_i = \phi_{\theta_i}$, then $\lambda_1 \otimes \lambda_2 = \phi_\theta$, where $\theta = p_1^*\theta_1 + p_2^*\theta_2$.)

If $\alpha \in \mathrm{End}(A_1 \times A_2)$, then we can identify α with the 2×2 matrix (α_{ij}) by putting $\alpha_{ij} = p_i \alpha e_j \in \mathrm{Hom}(A_j, A_i)$. Thus

$$\mathrm{End}(A_1 \times A_2) = \left\{ \begin{pmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{pmatrix} : \alpha_{ij} \in \mathrm{Hom}(A_j, A_i) \right\}.$$

Proposition 59 *In the above situation we have*

$$(61)\ \mathrm{End}_{\lambda_1\otimes\lambda_2}(A_1\times A_2)=\left\{\begin{pmatrix}\alpha_{11} & \alpha_{21}'\\ \alpha_{21} & \alpha_{22}\end{pmatrix}:\alpha_{ii}\in\mathrm{End}_{\lambda_i}(A_i),\alpha_{21}\in\mathrm{Hom}(A_1,A_2)\right\},$$

where $\alpha_{21}'=r_{\lambda_1,\lambda_2}(\alpha_{21})$. *Thus, the rule* $(\alpha_1,\alpha_2,\beta)\mapsto\left(\begin{smallmatrix}\alpha_1 & \beta'\\ \beta & \alpha_2\end{smallmatrix}\right)$ *defines an isomorphism*

$$\mu=\mu_{\lambda_1,\lambda_2}:\mathrm{End}_{\lambda_1}(A_1)\oplus\mathrm{End}_{\lambda_2}(A_2)\oplus\mathrm{Hom}(A_1,A_2)\ \xrightarrow{\sim}\ \mathrm{End}_{\lambda_1\otimes\lambda_2}(A_1\times A_2)$$

which induces an isomorphism

$$\mathbf{D}=\mathbf{D}_{\lambda_1,\lambda_2}:\mathrm{NS}(A_1)\oplus\mathrm{NS}(A_2)\oplus\mathrm{Hom}(A_1,A_2)\ \xrightarrow{\sim}\ \mathrm{NS}(A_1\times A_2).$$

Moreover, we have

$$\mathbf{D}(D_1,D_2,0)\ =\ p_1^*D_1+p_2^*D_2,\quad\forall D_i\in\mathrm{NS}(A_i).\tag{62}$$

Proof. Since $\hat{e}_i(\lambda_1\otimes\lambda_2)=\lambda_ip_i$ and $(\lambda_1\otimes\lambda_2)e_j=\hat{p}_j\lambda_j$, we see that $p_ir_{\lambda_1\otimes\lambda_2}(\alpha)e_j=r_{\lambda_i,\lambda_j}(p_j\alpha e_i)=r_{\lambda_i,\lambda_j}(\alpha_{ji})$. Thus

$$r_{\lambda_1\otimes\lambda_2}\begin{pmatrix}\alpha_{11} & \alpha_{12}\\ \alpha_{21} & \alpha_{22}\end{pmatrix}=\begin{pmatrix}\alpha_{11}' & \alpha_{21}'\\ \alpha_{12}' & \alpha_{22}'\end{pmatrix},\tag{63}$$

where $\alpha_{ji}'=r_{\lambda_i,\lambda_j}(\alpha_{ji})=\lambda_i^{-1}\hat{\alpha}_{ji}\lambda_j$. From (63) we therefore see that $\alpha=(\alpha_{ij})\in\mathrm{End}_{\lambda_1\otimes\lambda_2}(A)\Leftrightarrow\alpha_{ij}=\alpha_{ji}',\forall i,j=1,2\Leftrightarrow\alpha_{12}=\alpha_{21}',\alpha_{ii}\in\mathrm{End}_{\lambda_i}(A_i),i=1,2$, the latter because the hypothesis $\alpha_{12}=\alpha_{21}'$ implies that $\alpha_{12}'=(\alpha_{21}')'=\alpha_{12}$. This proves (61), and from this the assertion about μ follows immediately. Finally, if we put $\mathbf{D}_{\lambda_1,\lambda_2}=\Phi_{\lambda_1\otimes\lambda_2}^{-1}\circ\mu_{\lambda_1,\lambda_2}\circ(\Phi_{\lambda_1}\oplus\Phi_{\lambda_2}\oplus id)$, then it is clear by (54) that $\mathbf{D}=\mathbf{D}_{\lambda_1,\lambda_2}$ yields the desired isomorphism.

To prove (62), we first note that since $\hat{e}_i(\lambda_1\otimes\lambda_2)=\lambda_ip_i$, we have $r_{\lambda_1\otimes\lambda_2,\lambda_i}(p_i)=e_i$ and hence $\Phi_{\lambda_1\otimes\lambda_2}(p_i^*D_i)=e_i\Phi_{\lambda_i}(D_i)p_i$ by (55). Thus $\Phi_{\lambda_1\otimes\lambda_2}(p_1^*D_1+p_2^*D_2)=\mu(\Phi_{\lambda_1}(D_1),\Phi_{\lambda_2}(D_2),0)$, and so (62) follows.

Another useful formula is the following.

Proposition 60 *Let* (A,λ) *be a principally polarized abelian variety. If* $m_A:A\times A\to A$ *denotes the addition map and* $\delta_A:A\to A\times A$ *the diagonal map, then* $r_{\lambda\otimes\lambda,\lambda}(m_A)=\delta_A$ *and hence*

$$\Phi_{\lambda\otimes\lambda}(m_A^*D)=\delta_A\Phi_\lambda(D)m_A,\quad\forall D\in\mathrm{NS}(A).\tag{64}$$

Proof. Since $\hat{e}_i(\lambda\otimes\lambda)=\lambda p_i$ and $\hat{e}_i\hat{m}_A=id_{\hat{A}}$, we have $p_ir_{\lambda\otimes\lambda,\lambda}(m_A)=p_i(\lambda\otimes\lambda)^{-1}\hat{m}_A\lambda=\lambda^{-1}\hat{e}_i\hat{m}_A\lambda=1_A$, and so $r_{\lambda\otimes\lambda,\lambda}(m_A)=\delta_A$. Thus (64) follows from (55).

We now specialize the above results to the case of products of two elliptic curves.

Proposition 61 *Let $A = E_1 \times E_2$ be a product of two elliptic curves, and let $\lambda_i = \phi_{0_{E_i}}$. Then the isomorphism*

$$\mathbf{D} = \mathbf{D}_{\lambda_1,\lambda_2} : \mathbb{Z} \oplus \mathbb{Z} \oplus \mathrm{Hom}(E_1, E_2) \xrightarrow{\sim} \mathrm{NS}(A)$$

is given by the formula

$$\mathbf{D}(a, b, f) = cl((a - \deg(f))\theta_1 + (b - 1)\theta_2 + \Gamma_{-f}). \tag{65}$$

Here $\theta_i = p_i^*(0_{E_i})$, $\Gamma_f \in \mathrm{Div}(A)$ is the graph of f, and $cl(D) \in \mathrm{NS}(A)$ denotes the class of a divisor $D \in \mathrm{Div}(A)$. Thus

$$(\mathbf{D}(a, b, f).\mathbf{D}(a, b, f)) = 2(ab - \deg(f)), \tag{66}$$

$$(\mathbf{D}(a, b, f).(x\theta_1 + y\theta_2)) = bx + ay. \tag{67}$$

Proof. First note that since $\mathrm{NS}(E_i) = \mathbb{Z}cl(0_{E_i}) \simeq \mathbb{Z}$, the map $\mathbf{D}$ yields the indicated isomorphism. To prove (65), it is in view of (62) enough to verify that

$$\Phi_{\lambda_1\otimes\lambda_2}(\Gamma_{-f}) = \mu([\deg(f)]_{E_1}, 1_{E_2}, f) \tag{68}$$

and this follows from the identities $\Gamma_{-f} = (f \times 1)^* m_{E_2}^*(0_{E_2})$, $r_{\lambda_1\otimes\lambda_2,\lambda_2\otimes\lambda_2}(f \times 1_{E_2}) = f' \times 1_{E_2}$ and $\Phi_{\lambda_2}(0_{E_2}) = 1_{E_2}$ because by (55) and (64) we obtain $\Phi_{\lambda_1\otimes\lambda_2}(\Gamma_{-f}) = (f' \times 1_{E_2})\Phi_{\lambda_2\otimes\lambda_2}(m_{E_2}^* 0_{E_2})(f \times 1_{E_2}) = (f' \times 1_{E_2})\delta_{E_2}\Phi_{\lambda_2}(0_{E_2})m_{E_2}(f \times 1_{E_2}) = (f' \times 1_{E_2})\delta_{E_2} m_{E_2})(f \times 1_{E_2}) = \left(\begin{smallmatrix} f' & 0 \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 1 \\ 1 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} f & 0 \\ 0 & 1 \end{smallmatrix}\right) = \mu(f'f, 1, f) = \mu([\deg(f)], 1, f)$.

From (65), the formulae (66) and (67) follow immediately because $(\theta_1.\theta_2) = (\Gamma_{-f}.\theta_1) = 1$, $(\Gamma_{-f}.\theta_2) = \deg(-f) = \deg(f)$ and $\theta_1^2 = \theta_2^2 = \Gamma_{-f}^2 = 0$, the latter because $\theta_1 = \{0\} \times E_2 \simeq E_2$ and $\theta_2 \simeq \Gamma_{-f} \simeq E_1$ are elliptic curves.

Corollary 62 *Let $A' = E_1' \times E_2'$ be another product surface and let $\alpha = (\alpha_{ij}) \in \mathrm{Hom}(A', A))$, where $\alpha_{ij} \in \mathrm{Hom}(E_j', E_i)$. Then*

$$\deg(\alpha) = |(d_{11} + d_{21})(d_{12} + d_{22}) - \deg(f_\alpha)|, \tag{69}$$

where $d_{ij} = \deg(\alpha_{ij})$ and $f_\alpha = \alpha_{12}^t\alpha_{11} + \alpha_{22}^t\alpha_{21}$. Moreover, for $f \in \mathrm{Hom}(E_1, E_2)$ we have

$$\alpha^*\mathbf{D}(n_1, n_2, f) = \mathbf{D}(n_1', n_2', f') \tag{70}$$

where n_1', n_2', and f' are determined by the matrix equation

$$\begin{pmatrix} [n_1']_{E_1'} & (f')^t \\ f' & [n_2']_{E_2'} \end{pmatrix} = \begin{pmatrix} \alpha_{11}^t & \alpha_{21}^t \\ \alpha_{12}^t & \alpha_{22}^t \end{pmatrix} \begin{pmatrix} [n_1]_{E_1} & f^t \\ f & [n_2]_{E_2} \end{pmatrix} \begin{pmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{pmatrix}. \tag{71}$$

In other words, we have explicitly

$$\begin{aligned} n_1' &= n_1 d_{11} + n_2 d_{21} + \mathrm{tr}(\alpha_{21}^t f \alpha_{11}) \\ n_2' &= n_1 d_{12} + n_2 d_{22} + \mathrm{tr}(\alpha_{12}^t f \alpha_{22}) \\ f' &= n_1 \alpha_{12}^t \alpha_{11} + n_2 \alpha_{22}^t \alpha_{21} + \alpha_{12}^t f^t \alpha_{21} + \alpha_{22}^t f \alpha_{11} \end{aligned}$$

where $\mathrm{tr}(h) \in \mathbb{Z}$ is defined by $[\mathrm{tr}(h)] = h + h^t$, for $h \in \mathrm{End}(E_i')$.

Proof. To prove (69), consider $\tilde{\alpha} := r_{\lambda_1\otimes\lambda_2}(\alpha)\alpha$. Since $\deg(r_{\lambda_1\otimes\lambda_2}(\alpha)) = \deg(\hat{\alpha}) = \deg(\alpha)$, we have $\deg(\alpha)^2 = \deg(\tilde{\alpha})$. Now by (63) we have $\tilde{\alpha} = \left(\begin{smallmatrix}\alpha'_{11} & \alpha'_{21}\\ \alpha'_{12} & \alpha'_{22}\end{smallmatrix}\right)\left(\begin{smallmatrix}\alpha_{11} & \alpha_{12}\\ \alpha_{21} & \alpha_{22}\end{smallmatrix}\right) = \mu([d_1],[d_2],f_\alpha)$, where $d_1 = d_{11}+d_{21}$ and $d_2 = d_{12}+d_{22}$, and so $4\deg(\alpha)^2 = 4\deg(\mu([d_1],[d_2],f_\alpha) = (\mathbf{D}(d_1,d_2,f_\alpha)^2)^2$, where the latter equality follows from the Riemann-Roch Theorem (cf. [33], p. 150) because $\mu([a],[b],f) = \Phi_{\lambda_1\otimes\lambda_1}(\mathbf{D}(a,b,f))$. From this (69) follows immediately by using (66).

To prove (70) and (71), note first that there exist unique n'_1, n'_2 and f' such that (70) holds. Then $\Phi_{\lambda'_1\otimes\lambda'_2}(\mathbf{D}(n'_1,n'_2,f'))$ equals the left hand side of (71), where λ'_i denotes the canonical polarization of E'_i. On the other hand, by (a slight generalization of) formula (63), the right hand side of (71) equals $r_{\lambda'_1\otimes\lambda'_2,\lambda_1\otimes\lambda_2}(\alpha)\Phi_{\lambda_1\otimes\lambda_2}(\mathbf{D}(n_1,n_2,f))\alpha$. Since this equals $\Phi_{\lambda'_1\otimes\lambda'_2}(\alpha^*\mathbf{D}(n_1,n_2,f))$ by (55), we see that (71) holds. The last assertion follows from this by multiplying out the right side of (71).

Corollary 63 *Let $g \in M_2(\mathbb{Z})$ be a 2×2 matrix and let $[g]_E \in \mathrm{End}(E\times E)$ be the endomorphism induced by g. Then $\deg([g]_E) = \det(g)^2$.*

Proof. Write $g = (a_{ij})$, and apply (69) to $\alpha = [g]_E = ([a_{ij}]_E)$. Here $d_{ij} = \deg([a_{ij}]_E) = a_{ij}^2$, and $\deg(f_\alpha) = \deg([a_{12}a_{11}+a_{22}a_{21}]) = (a_{12}a_{11}+a_{22}a_{21})^2$. Thus $\deg(\alpha) = |(a_{11}^2 + a_{21}^2)(a_{12}^2+a_{22}^2) - (a_{12}a_{11}+a_{22}a_{21})^2| = |(a_{11}a_{22}-a_{12}a_{21})^2| = \det(g)^2$.

References

[1] A. Atkin, J. Lehner, Hecke operators on $\Gamma_0(m)$. *Math. Ann.* **185** (1970), 134-160.

[2] D. Buell, *Binary Quadratic Forms.* Springer-Verlag, New York, 1989.

[3] S. Chowla, An extension of Heilbronn's class-number theorem. *Quart. J. Math.* **5** (1934), 304–307.

[4] P. Deligne, M. Rapoport, Les schémas de modules de courbes elliptiques. In: *Modular functions of one variable II*, Lecture Notes in Math. 349, Springer-Verlag, Berlin, 1973, pp. 143–316.

[5] L. Dickson, *Introduction to the Theory of Numbers.* U of Chicago Press, Chicago, 1929.

[6] C. Earle, The genus two Jacobians that are isomorphic to a product of elliptic curves. In: *The Geometry of Riemann Surfaces and Abelian Varieties.* Contemp. Math. 397, AMS, Providence, RI, 2006, pp. 27–36.

[7] D. Estes, G. Pall, Spinor genera of binary quadratic forms. *J. Number Theory* **5** (1973), 421–432.

[8] G. Frey, E. Kani, Curves of genus 2 with elliptic differentials and associated Hurwitz spaces. Preprint, 2008, 70pp.

[9] W. Fulton, *Intersection Theory.* Springer-Verlag, Berlin, 1984.

[10] C.F. Gauss, *Untersuchungen über die höhere Arithmetik.* (Translation of *Disquisitiones Arithmeticae*). Chelsea Reprint, New York, 1981.

[11] N. Hall, Binary quadratic discriminants with a single class in each genus. *Math. Z.* **44** (1938), 85–90.

[12] T. Hayashida, A class number associated with a product of two elliptic curves. *Natur. Sci. Rep. Ochanomizu Univ.* **16** (1965), 9–19.

[13] T. Hayashida, A class number associated with the product of an elliptic curve with itself. *J. Math. Soc. Japan* **20** (1968), 26–43.

[14] T. Hayashida, M. Nishi, Existence of curves of genus two on a product of two elliptic curves. *J. Math. Soc. Japan* **17** (1965), 1–16.

[15] G. Humbert, Sur les fonctions abéliennes singulières. I. *J. de Math.* (ser. 5) **5** (1899), 233–350 = Œuvres, Gauthier-Villars er Cie., Paris, 1929, pp. 297–401.

[16] T. Ibukiyama, T. Katsura, F. Oort, Supersingular curves of genus two and class numbers. *Compositio Math.* **57** (1986), 127–152.

[17] J.-I. Igusa, Arithmetic variety of moduli for genus 2. *Ann. Math.* **72** (1960), 612–649.

[18] B. Jones, *The Arithmetic Theory of Quadratic Forms.* Carus Monographs No. 10, MAA, 1967.

[19] E. Kani, Elliptic curves on abelian surfaces. *Manus. math.* **84** (1994), 199–223.

[20] E. Kani, The number of curves with elliptic differentials. *J. reine angew. Math.* **485** (1997), 93-121.

[21] E. Kani, Generalized Humbert Varieties. In preparation.

[22] N. Katz, B. Mazur, *Arithmetic Moduli of Elliptic Curves.* Princeton University Press, Princeton, NJ, 1985.

[23] A. Krazer, *Lehrbuch der Thetafunktionen.* Leipzig, 1903; Chelsea Reprint, New York, 1970.

[24] S. Lang, *Elliptic Functions.* Addison-Wesley, Reading, MA, 1972.

[25] H. Lange, Produkte elliptischer Kurven. *Nachr. Akad. Wiss. Göttingen* Math.-Phys. Kl. II 1975, no. 8, 95–108.

[26] H. Lange, Principal polarizations on products of elliptic curves. In: *The Geometry of Riemann Surfaces and Abelian Varieties.* Contemp. Math. 397, AMS, Providence, RI, 2006, pp. 153–162.

[27] B. Mazur, Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.* **47** (1977), 33 – 186.

[28] C. McMullen, Teichmüller curves in genus 2: discriminant and spin. *Math. Ann.* **333** (2005), 87–130.

[29] C. McMullen, Dynamics of $\mathrm{SL}_2(\mathbb{R})$ over moduli space in genus two. *Ann. Math.* **165** (2007), 397–456.

[30] J.S. Milne, Abelian varieties. In: *Arithmetic Geometry.* (G. Cornell, J. Siverman, eds.), Springer-Verlag, New York, 1986; pp. 103–150.

[31] J.S. Milne, Jacobian varieties. In: *Arithmetic Geometry.* (G. Cornell, J. Siverman, eds.), Springer-Verlag, New York, 1986; pp. 165–212.

[32] D. Mumford, *Geometric Invariant Theory.* Springer-Verlag, Berlin, 1965.

[33] D. Mumford, *Abelian Varieties.* Oxford U Press, Oxford, 1970.

[34] F. Oort, J. Steenbrink, The local Torelli problem for algebraic curves. *Journées de Géometrie Algébrique d'Angers, Juillet 1979/Algebraic Geometry, Angers, 1979*, Sijthoff & Noordhoff, Alphen aan den Rijn—Germantown, Md., 1980; pp. 157–204.

[35] G. van der Geer, *Hilbert Modular Surfaces.* Springer-Verlag, Berlin, 1988.

[36] A. Weil, Zum Beweis des Torellischen Satzes. *Nachr. Ges. Wiss. Göttingen, Math.-Phys. Klasse* 1957, = Œuvres II, pp. 307–327.

[37] P. Weinberger, Exponents of class groups of complex quadratic fields. *Acta Arith.* **22** (1973), 117–124.