Products of CM elliptic curves

Ernst Kani

1 Introduction

Let K be an arbitrary field, and let $E_1, \ldots, E_n$ be isogenous CM elliptic curves over K. The basic problem considered in this paper is to find suitable criteria for determining whether or not a given abelian variety A' is isomorphic to the product variety $A = E_1 \times \ldots \times E_n$. A special case of this problem is to determine this in the case that $A' = E_1' \times \ldots \times E_n'$ is also a product variety.

In the case that $K = \mathbb{C}$ and $n = 2$, Shioda and Mitani[24] presented a solution of this subproblem in terms of the period lattices L_i and L_i' of the elliptic curves $E_i = \mathbb{C}/L_i$ and $E_i' = \mathbb{C}/L_i'$, and a similar criterion is implicit in the work of Schoen[22] for arbitrary n.

In this paper we present a criterion that is partially similar to the complex-analytic approach but has the advantage that it works over an arbitrary ground field. Here the role of the (isomorphism class) of the lattice L_i is replaced by the ideal class

$$I_E(E_i) := \mathrm{Hom}(E_i, E)\pi_i,$$

where E is a fixed suitable elliptic curve which is isogenous to E_i and $\pi_i : E \to E_i$ is any isogeny. It is immediate that $I_E(E_i)$ is an $\mathrm{End}(E)$-ideal whose ideal class does not depend on the choice of the isogeny π_i. Here, "suitable" means that the conductor $f_E = f_{\mathrm{End}(E)}$ of E is a multiple of those of E_i and E_i' for all i. We then have:

Theorem 1 *Let E/K be a CM-elliptic curve and let $E_1, \ldots, E_n, E_1', \ldots, E_n'$ be elliptic curves isogenous to E with $f_{E_i} | f_E$ and $f_{E_i'} | f_E$, for $1 \le i \le n$. Then*

$$E_1 \times \ldots \times E_n \;\simeq\; E_1' \times \ldots \times E_n' \;\Leftrightarrow\; I_E(E_1) \oplus \ldots \oplus I_E(E_n) \;\simeq\; I_E(E_1') \oplus \ldots \oplus I_E(E_n')$$

as $\mathrm{End}(E)$*-modules.*

Note that this result is actually a special case of a very general result about isomorphisms of product abelian varieties; cf. Theorem 43.

At first sight the criterion of Theorem 1 does not seem to specialize to that of [24], Proposition 4.5. However, by using results due to Steinitz[25] and Borevich/Fadeev[1] on the struture of R-modules when R is a quadratic order, one can easily deduce their result from that of Theorem 1; cf. subsection 4.4.

It turns out that general isomorphism problem can be reduced to the previously considered subproblem in many cases, for we have the following result.

Theorem 2 *Let E/K be a CM elliptic curve, where K is either algebraically closed or finite. If A/K is an abelian variety which is isogenous to E^n, for some $n \geq 1$, then there exist CM elliptic curves $E_1, \ldots, E_n/K$ such that $A \simeq E_1 \times \ldots \times E_n$.*

In the case that $K = \mathbb{C}$, this theorem was proved by Shioda and Mitani[24] when $n = 2$ (see also Ruppert[21]), and their work was extended to the general case by Lange[19]. Moreover, Schoen[22] gave a beautiful analysis of this theorem; cf. Remark 59 below.

Over a general ground field K, the analogue of Theorem 2 seems to be more subtle. The following generalization of Theorem 2 uses the concept of the *central conductor* $f_A = f_{\mathrm{End}(A)}$ which is the conductor of the centre $Z(\mathrm{End}(A))$ as an order in $F = Z(\mathrm{End}^0(A))$; cf. §4.3 below.

Theorem 3 *Let E/K be a CM elliptic curve, where K is an arbitrary field, and let A/K be an abelian variety which is isogenous to E^n, for some $n \geq 1$. Then there exist CM elliptic curves $E_1, \ldots, E_n/K$ such that $A \simeq E_1 \times \ldots \times E_n$ if and only if $f_A | f_{E_0}$, for some elliptic curve E_0/K with $E_0 \sim E$.*

Note that if we combine Theorem 3 with Theorem 1, then we get an indirect solution of the isomorphism problem mentioned at the beginning. A more intrinsic solution (similar to Theorem 1) is given below; cf. Corollary 56.

In the case that $n = 2$ and $K = \mathbb{C}$, Shioda and Mitani[24] also showed that one can classify the abelian surfaces A with $A \sim E^2$ by equivalence classes of binary quadratic forms. While their theorem does not directly carry over to an arbitrary ground field, the following refinement is true in general. To state it, it is useful to employ the following terminology. If E/K is a CM elliptic curve, then its *discriminant* is the discriminant $\Delta_E = \Delta(\mathrm{End}(E))$ of the order $\mathrm{End}(E)$; thus $\Delta_E = f_E^2 \Delta_F$, where Δ_F is the discriminant of the imaginary quadratic field $F = \mathrm{End}^0(E)$. Moreover, if A/K is an abelian surface, then its *discriminant* $\Delta(A/K)$ is the discriminant of its Néron-Severi group $\mathrm{NS}(A)$ (with respect to the intersection pairing). We then have the following result:

Theorem 4 *Let E/K be a CM elliptic curve of discriminant $\Delta = \Delta_E$. Then there is a bijection between:*

(i) *the set of proper equivalence classes of positive definite binary quadratic forms q with discriminant $\Delta(q) = \Delta$;*

(ii) *the set of isomorphism classes of abelian surfaces A/K with $A \sim E^2$ and discriminant $\Delta(A/K) = -\Delta$.*

Note that in the above bijection, the binary quadratic forms q need not be primitive, i.e. their *content* $\mathrm{cont}(q)$ need not be equal to 1.

The above Theorem 4 will be deduced in §4.4 from the following generalization to abelian varieties of arbitrary dimension n.

Theorem 5 *Let E/K be a CM elliptic curve with discriminant $\Delta_E = f_E^2 \Delta_F$. If $n \geq 2$, then there are natural bijections between the following sets:*

(i) *The set of sequences $(E'; f_1, \ldots, f_{n-2})$ where $E' \sim E$ is an isomorphism class of elliptic curves with $f_{E'} | f_E$ and the f_i's are positive integers with $f_{E'} | f_1 | \ldots | f_{n-2} | f_E$.*

(ii) *the set of sequences $(I; f_1, \ldots, f_{n-2})$ where I is an isomorphism class of non-zero $\mathrm{End}(E)$-ideals whose associated order $R(I)$ has conductor $f_{R(I)} | f_1 | \ldots | f_{n-2} | f_E$.*

(iii) *the set of sequences $(q; c_1, \ldots, c_{n-2})$ where q is a proper equivalence class of positive binary quadratic forms of discriminant Δ and $c_1 | \ldots | c_{n-2} | \mathrm{cont}(q)$.*

(iv) *the set of isomorphism classes of $\mathrm{End}(E)$-submodules M of $\mathrm{End}(E)^n$ of rank n with $(M : M)_F := \{f \in F : fM \subset M\} = \mathrm{End}(E)$;*

(v) *the set of isomorphism classes of abelian varieties $A \sim E^n$ with central conductor $f_A = f_E$.*

Note that the above theorem can easily be extended to classify the isomorphism classes of abelian varieties $A \sim E^n$ with $f_A | f_E$; cf. Remark 62(b) below.

The basic technique for proving these theorems is the method of Deuring[10], Shimura and Taniyama[23], and Waterhouse[26] of constructing isogenies: for a given left ideal I of $\mathrm{End}(A)$, this method defines a finite subgroup scheme $H(I)$ of A and hence an isogeny $\pi_I : A \to A/H(I)$. This theory, together with some extensions, is presented in some detail in §2.

In order to be able to apply this theory, it is useful to know which finite subgroup schemes H of A are of the form $H = H(I)$ for some ideal I of $\mathrm{End}(A)$; such subgroup schemes are called *ideal subgroups* in this paper. A key result here is the following theorem (see also Theorem 54 below) which classifies the ideal subgroups of $A = E^n$.

Theorem 6 *Let E/K is a CM elliptic curve, and let H be a finite subgroup scheme of E^n. Then $H = H(I)$ for some left ideal I of $\mathrm{End}(E^n)$ if and only if the central conductor $f_{E^n/H}$ of the quotient E^n/H divides the conductor f_E of E.*

This paper is organized as follows. In §2 we review and extend the theory of Deuring, Shimura/Taniyama and Waterhouse. This is then worked out in detail in §3 for the case of a CM elliptic curve. Here Theorem 18, Corollary 19 and Proposition 36 are basic tools for the rest of paper. In §4 we study products of abelian varieties: the general case is analyzed in §4.1 and then applied to products of CM elliptic curves in §4.3. To this end we also review and extend the results of Steinitz and of Borevich/Faddeev[1] in §4.2. Finally, in §4.4 we consider the case of abelian surfaces and show how the present results are related to those of Shioda and Mitani[24].

This research was partially supported by a Discovery Grant from the Natural Sciences and Engineering Research Council of Canada (NSERC), and also by the Graduiertenkolleg of the Institute of Experimental Mathematics (IEM) of the University of Duisburg/Essen. I would like to express my appreciation to Gerd Frey and to the IEM for their hospitality, and to thank him for helpful comments on this paper.

2 Isogenies, subgroups and ideals

2.1 Kernel ideals and ideal subgroups

In this section we review and augment the method of constructing isogenies of via ideals; cf. Waterhouse[26], §3.2. This method is due to Deuring[10] in the case of elliptic curves, and was generalized to abelian varieties by Shimura and Taniyama[23], §7.

Throughout this paper, K is an arbitrary field, and A/K is an abelian variety. All morphisms are tacitly K-morphisms, and all subvarieties are K-subvarieties.

We first review some basic facts about finite subgroup schemes. If H is finite subgroup scheme of A, then the quotient variety $A_H = A/H$ with quotient morphism

$$\pi_H : A \to A_H := A/H$$

exists by [20], p. 111, and is again an abelian variety. Thus, (A_H, π_H) is characterized by the universal property that for any H-invariant morphism $f : A \to X$ there is a unique morphism $f_H : A_H \to X$ such that $f = f_H \circ \pi_H$. Note that π_H is an isogeny of degree $\deg(\pi_H) = |H|$, where $|H|$ denotes the rank of the finite subgroup scheme H.

Conversely, if $\pi : A \to A'$ is an isogeny of abelian varieties, then $\mathrm{Ker}(\pi)$ is a finite subgroup scheme of rank $|\mathrm{Ker}(\pi)| = \deg(\pi)$. Since π is faithfully flat (use [11], Ex.III.9.3(a) or [4], 7.3/1), it follows that $\pi : A \to A'$ is a quotient of A, i.e. there is an isomorphism $\varphi : A' \xrightarrow{\sim} A_{\mathrm{Ker}(\pi)}$ such that $\pi_{\mathrm{Ker}(\pi)} = \varphi \circ \pi$. Thus, we have a bijection between finite subgroup schemes H of A and isogenies $\pi : A \to A'$, modulo isomorphisms.

If H_1 and H_2 are any two (not necessarily finite) subgroup schemes of A, then we write $H_1 \leq H_2$ if the canonical inclusion morphism $j_{H_1} : H_1 \hookrightarrow A$ of H_1 factors over that of H_2, i.e. if $j_{H_1} = j_{H_2} \circ h$, for some $h : H_1 \to H_2$ (necessarily an immersion). Since a homomorphism $h : A \to A'$ of abelian varieties is H_1-invariant if and only if $\mathrm{Ker}(h_1) \leq \mathrm{Ker}(h)$, it follows from the universal property of quotients that if H_1 and H_2 are finite, then the condition $H_1 \leq H_2$ is equivalent to the existence of a morphism (necessarily an isogeny) $\pi_{H_1,H_2} := (\pi_{H_2})_{H_1} : A_{H_1} \to A_{H_2}$ such that $\pi_{H_2} = \pi_{H_1,H_2} \circ \pi_{H_1}$. In particular, we see that $|H_1| = \deg(\pi_{H_1}) \mid \deg(\pi_{H_2}) = |H_2|$ in this case. From this it follows that the relation $\leq$ is a partial order on the set of finite subgroup schemes of A; in particular, $H_1 \leq H_2$ and $H_2 \leq H_1 \Rightarrow H_1 = H_2$ (because π_{H_1,H_2} is an isomorphism if $|H_1| = |H_2|$).

For any finite collection $H_1, \ldots, H_n$ of subgroup schemes of A, their *intersection* $H_1 \cap \ldots \cap H_n := H_1 \times_A \ldots \times_A H_n$ is a subgroup scheme of A, which is the greatest lower bound of $H_1, \ldots, H_n$ with respect to the partial order $\leq$. Note that $\cap H_i$ is finite if at least one of the H_i is finite. We can thus extend the definition of to an infinite collection $\{H_i\}_{i \in I}$ of subgroup schemes provided that at least one of the H_i is finite, because then the definition reduces to a finite subcollection (because the finite subgroup schemes satisfy d.c.c.).

We now present the Deuring/Shimura/Taniyama/Waterhouse method of constructing finite subgroup schemes via left ideals. However, instead of fixing an identification of $\mathrm{End}(A)$ with an abstract ring R (as in [23] and [26]), we shall work directly with

$$R = R_A := \mathrm{End}(A) \quad \text{and} \quad \tilde{R} = \tilde{R}_A := \mathrm{End}^0(A) = \mathrm{End}(A) \otimes \mathbb{Q}$$

because A is usually fixed. Note that R is canonically embedded in $\tilde{R}$. Later in §2.3 we shall study what happens when we replace A by an isogenous variety A'.

Let I be a regular left ideal I of $R = \mathrm{End}(A)$, i.e. I is a left R-ideal which contains an isogeny. Then as in [26], §3.2, we put

$$H(I) = \bigcap_{f \in I} \mathrm{Ker}(f)$$

which is finite subgroup scheme of A. Note that I is finitely generated and that

$$H(I) \;=\; \mathrm{Ker}(h_1) \cap \ldots \cap \mathrm{Ker}(h_r), \quad \text{if } I = \sum_{i=1}^{r} Rh_i, \tag{1}$$

because for all $f, g \in R$ we have

$$\mathrm{Ker}(g) \;\leq\; g^{-1}(\mathrm{Ker}(f)) \;=\; \mathrm{Ker}(fg) \quad \text{and} \quad \mathrm{Ker}(f) \cap \mathrm{Ker}(g) \;\leq\; \mathrm{Ker}(f+g). \tag{2}$$

From (1) it follows immediately that for any two regular left R-ideals I_1, I_2 we have

$$H(I_1 + I_2) \;=\; H(I_1) \cap H(I_2) \tag{3}$$

because $I_1 + I_2$ is generated by $I_1 \cup I_2$.

Here we complement this construction by the following "dual construction". Given a finite subgroup scheme H of A, put

$$I(H) \;=\; \mathrm{Hom}(A_H, A)\pi_H \;=\; \{f \in R : H \leq \mathrm{Ker}(f)\},$$

where the second equality follows from the universal property of (A_H, π_H). It is immediate that $I(H)$ is a left ideal of R. Moreover, $I(H)$ is a regular ideal because $H \leq \mathrm{Ker}([n_H]_A)$, where $n_H = |H|$ (and $[n]_A = n \cdot 1_A$ denotes the multiplication-by-n map), and so $[n_H]_A \in I(H)$. For later reference we observe that it thus follows from the above equality that there exists a unique $\pi'_H \in \mathrm{Hom}(A_H, A)$ such that

$$\pi'_H \circ \pi_H = [n_H]_A \quad \text{and that hence also} \quad \pi_H \circ \pi'_H = [n_H]_{A_H}. \tag{4}$$

If I_1, I_2 and I are regular left R-ideals and H_1, H_2 and H are finite subgroup schemes of A, then we have

$$I_1 \subset I_2 \;\Rightarrow\; H(I_2) \leq H(I_1), \tag{5}$$

$$H_1 \leq H_2 \;\Rightarrow\; I(H_2) \subset I(H_1), \tag{6}$$

$$I \;\subset\; I(H(I)), \tag{7}$$

$$H \;\leq\; H(I(H)). \tag{8}$$

Indeed, (5) and (6) are clear from the definitions. Moreover, if $f \in I$, then $\mathrm{Ker}(f) \geq H(I) = \cap_{g \in I}\mathrm{Ker}(g)$, so $f \in I(H(I))$ and hence $I \subset I(H(I))$, which proves (7). Similarly, since $H \leq \mathrm{Ker}(f)$, for all $f \in I(H)$, we have $H \leq \cap_{f \in I(H)}\mathrm{Ker}(f) = H(I(H))$, which yields (8).

From the above properties we see immediately that

$$H(I) = H(I(H(I))) \quad \text{and} \quad I(H) = I(H(I(H))). \tag{9}$$

Indeed, by (8) (applied to $H = H(I)$) we have $H(I) \leq H(I(H(I))$. On the other hand, since $I \subset I(H(I))$ by (7), it follows from (5) that $H(I) \geq H(I(H(I))$, and so the first equation of (9) follows. The second is proved similarly.

Definition. A regular left R-ideal I is called a *kernel ideal* if we have that $I = I(H(I))$. A finite subgroup scheme H of A is called an *ideal subgroup* (scheme) if we have $H = H(I(H))$.

Remark 7 (a) Waterhouse[26], p. 533, calls an ideal I a kernel ideal if we have $I = \{f \in R : fH(I) = 0\}$. Since $fH(I) = 0 \Leftrightarrow H(I) \leq \mathrm{Ker}(f)$, it is clear that $\{f \in R : fH(I) = 0\} = I(H(I))$, and so his definition agrees with the one above. (He does not define "ideal subgroups".)

(b) It follows from the definition and (9) that I is a kernel ideal if and only if $I = I(H)$, for some finite subgroup scheme H of A. Similarly, we see that H is an ideal subgroup if and only if $H = H(I)$ for some regular left R-ideal I.

(c) If $f \in R$ is an isogeny, then it clear that

$$H(Rf) = \mathrm{Ker}(f) \quad \text{and} \quad I(\mathrm{Ker}(f)) = Rf \tag{10}$$

(the latter by the universal property), and so Rf is a kernel ideal and $\mathrm{Ker}(f)$ is an ideal subgroup. More generally, we have for any regular left R-ideal I, any finite subgroup scheme H of A and isogeny $f \in R$ that

$$H(If) = f^{-1}(H(I)) \quad \text{and} \quad I(f^{-1}(H)) = I(H)f. \tag{11}$$

Indeed, the first equality follows from the fact that intersections commute with inverse images, and the second follows because the faithful flatness of f implies that

$$H \leq \mathrm{Ker}(g) \Leftrightarrow f^{-1}(H) \leq f^{-1}(\mathrm{Ker}(g)) = \mathrm{Ker}(gf), \quad \forall g \in R. \tag{12}$$

From (11) it thus follows that

$$I(H(If)) = I(H(I))f \quad \text{and} \quad H(I(f^{-1}(H))) = f^{-1}(H(I(H))), \tag{13}$$

and so we see that if I is a kernel ideal, then so is If. Similarly, if H is an ideal subgroup, then so is $f^{-1}(H)$. In fact, the converses of these assertions are also true:

$$I \text{ is a kernel ideal} \Leftrightarrow If \text{ is a kernel ideal;} \tag{14}$$

$$H \text{ is an ideal subgroup} \Leftrightarrow f^{-1}(H) \text{ is an ideal subgroup.} \tag{15}$$

Indeed, if If is a kernel ideal, then by the first part of (13) we have $I(H(I))f = I(H(If)) = If$, and so $I(H(I)) = I$ because f is a unit in $\tilde{R} \supset R$. Thus I is a kernel ideal, which proves (14). Similarly, if $f^{-1}(H)$ is an ideal subgroup, then by the second part of (13) we have $f^{-1}(H(I(H))) = H(I(f^{-1}(H))) = f^{-1}(H)$, and so $H(I(H)) = H$ by the faithful flatness of f. Thus H is an ideal subgroup, which proves (15).

(d) For any regular left R-ideal we have

$$I(H(I)) \ \subset \ I^* \ := \ \bigcap_{R\tilde{f} \supset I} R\tilde{f}, \tag{16}$$

where the intersection runs over all $\tilde{f} \in \tilde{R}$ such that $R\tilde{f} \supset I$. Indeed, if $\tilde{f} = f/n$ with $f \in R$ and $n \in \mathbb{N}$, then $I \subset R\tilde{f}$ implies that $In \subset Rf$ and so by (11), (5), (6) and (10) we have that $I(H(I))n = I(H(In)) \subset I(H(Rf)) = Rf$, and hence $I(H(I)) \subset R\tilde{f}$. This verifies (16).

In particular, if $I = I^*$, i.e. if I is a *divisorial ideal* (cf. [5], p. 476), then it follows from (8) and (16) that $I = I(H(I))$. Thus every divisorial ideal is a kernel ideal. In particular, if R is commutative, then every invertible R-ideal I is a kernel ideal by [5], p. 118, 476. Thus, if R is a Dedekind domain, then all non-zero ideals are kernel ideals.

(e) If K'/K is any field extension, then we have an injective ring homomorphism

$$\beta_{K'/K} : \mathrm{End}(A) \ \to \ \mathrm{End}(A \otimes K')$$

given by base-change $f \mapsto f \otimes K'$. *If this is surjective* (hence an isomorphism), then it is clear from the definitions that for a finite subgroup scheme H of A and R-ideal I we have

$$H(I) \otimes K' \ = \ H(\beta_{K'/K}(I)) \quad \text{and} \quad I(H \otimes K') \ = \ \beta_{K'/K}(I(H))$$

because $\mathrm{Ker}(f \otimes K') = \mathrm{Ker}(f) \otimes K'$, for all $f \in \mathrm{End}(A)$. Note, however, that in general $A' := A \otimes K'$ has more finite subgroup schemes than A, i.e. A' may have finite subgroup schemes which are not of the form $H \otimes K'$.

2.2 The invariant $I_A(B)$

Given an abelian variety B which is isogenous to A (notation: $B \sim A$), we shall define an "invariant" $I_A(B)$ which is an isomorphism class of left R-ideals, where, as before, $R = R_A = \mathrm{End}(A)$. This invariant is defined by the rule

$$I_A(B) \ = \ \mathrm{Hom}(B, A)\pi \ = \ I(\mathrm{Ker}(\pi)) \quad \text{where } \pi : A \to B \text{ is any isogeny.}$$

As we shall see presently, the R-module isomorphism class of the right hand side does not depend on the choice of the isogeny $\pi : A \to B$. For this, we first observe the following.

As before, let H_1 and H_2 be two finite subgroup schemes of A and let I_1 and I_2 two regular left R-ideals. It is then easy to see (cf. [26], p. 532) that we have

(17) $A_{H_1} \simeq A_{H_2} \;\Leftrightarrow\; f^{-1}(H_1) = [n]^{-1}(H_2)$, for some $f \in R \cap \tilde{R}^\times$ and $n \in \mathbb{Z}$,

(18) $I_1 \simeq I_2 \;\Leftrightarrow\; I_1 = I_2\tilde{f}$, for some $\tilde{f} \in \tilde{R}^\times$.

From this we see that

(19) $$I_1 \simeq I_2 \;\Rightarrow\; A_{H(I_1)} \simeq A_{H(I_2)}$$

because the hypothesis implies by (18) that $I_1 = I_2\tilde{f}$, where $\tilde{f} = f/n$ with $f \in R \cap \tilde{R}$ an isogeny, and so $I_1 n = I_2 f$. Thus, by (12) we have $[n]^{-1}(H(I_1)) = H(I_1 n) = H(I_2 f) = f^{-1}(H_2)$, and hence $A_{H(I_1)} \simeq A_{H(I_2)}$ by (17). This proves (19).

Similarly, we have

(20) $$A_{H_1} \simeq A_{H_2} \;\Rightarrow\; I(H_1) \simeq I(H_2).$$

Indeed, by (17) the hypothesis implies that there exist f, n such that $f^{-1}(H_1) = [n]^{-1}(H_2)$, and so by (11) we have $I(H_1)f = I(f^{-1}(H_1)) = I([n]^{-1}(H_2)) = I(H_2)n$, so $I(H_2) = I(H_1)\tilde{f}$ with $\tilde{f} = \frac{f}{n}$, and hence $I(H_1) \simeq I(H_2)$, which proves (20).

While in general the converses of (19) and (20) are false, we note that if I_1 and I_2 are kernel ideals, then it follows from (19) and (20) that the converse of (19) holds. Similarly:

(21) $A_{H_1} \simeq A_{H_2} \;\Leftrightarrow\; I(H_1) \simeq I(H_2)$, if H_1 and H_2 are ideal subgroups.

We now apply this to the invariant $I_A(B)$. It follows from (20) that the isomorphism class of $I_A(B)$ does not depend on the choice of the isogeny $\pi : A \to B$, for if $\pi_1 : A \to B$ is another, then $A_{\mathrm{Ker}(\pi)} \simeq B \simeq A_{\mathrm{Ker}(\pi_1)}$, and so by (20) we have $I(\mathrm{Ker}(\pi)) \simeq I(\mathrm{Ker}(\pi_1))$, as asserted.

As was mentioned above, it can happen that $I_A(B_1) \simeq I_A(B_1)$ yet $B_1 \not\simeq B_2$. However, if B_1 and B_2 have the "ideal property" that there exist isogenies $\pi_i : A \to B_i$ such that $\mathrm{Ker}(\pi_i)$ is an ideal subgroup, then we have by the above discussion that

$$I_A(B_1) \simeq I_A(B_2) \;\Leftrightarrow\; B_1 \simeq B_2, \quad \text{provided that } B_1, B_2 \text{ have the ideal property.}$$

Remark 8 It is useful to observe that the "ideal property" of B can be decided by considering a single isogeny $\pi : A \to B$ because if H_1 and H_2 are two finite subgroup schemes, then we have:

(22) If $A_{H_1} \simeq A_{H_2}$, then H_1 is an ideal subgroup $\Leftrightarrow$ H_2 is an ideal subgroup.

Indeed, by (17) the hypothesis means that $f^{-1}(H_1) = [n]^{-1}(H_2)$, for some isogeny $f \in R$ and $n \in \mathbb{N}$ and so the conclusion follows from (15).

Similarly, the property of being a kernel ideal is a property of the isomorphism class: if I, J are two regular left R-ideals, then we have:

(23) If $I \simeq J$, then I is a kernel ideal $\Leftrightarrow$ J is a kernel ideal.

Indeed, by (18) we have $I_1 f = I_2 n$, for some isogeny $f \in R$ and $n \in \mathbb{N}$, and so the conclusion follows from (14).

2.3 Homomorphisms

The discussion of the previous subsection drew attention to the importance of ideal subgroups, and so it is of interest to classify them. Now while it is frequently the case that all regular left R-ideals are kernel ideals (for example, if R is a Dedekind domain; cf. Remark 7(d)), it rarely happens that all finite subgroups schemes of A are ideal subgroups. The reason for this is that if $H = H(I)$ is an ideal subgroup, then $\mathrm{End}(A_H)$ has additional properties which are not necessarily satisfied by $\mathrm{End}(A_H)$ for an arbitrary finite subgroup scheme H.

To explain this in more detail, let H_1 and H_2 be two finite subgroup schemes of A, and consider the subset $\mathcal{H}(H_1, H_2) := \mathrm{Im}(\Phi_{H_1,H_2}) \subset \tilde{R}$ which is the image of the map

$$\Phi_{H_1,H_2} : \mathrm{Hom}(A_{H_1}, A_{H_2}) \ \rightarrow \ \tilde{R} = \mathrm{End}^0(A)$$

defined by the rule

$$\Phi_{H_1,H_2}(h) \ = \ \frac{1}{n_{H_2}} \pi'_{H_2} \circ h \circ \pi_{H_1}, \quad \text{for } h \in \mathrm{Hom}(A_{H_1}, A_{H_2}). \tag{24}$$

Here, as before $n_{H_2} = \deg(\pi_{H_2}) = |H_2|$ and π'_{H_2} is defined by (4).

Remark 9 (a) Note that $\Phi = \Phi_{H_1,H_2}$ is injective because it follows from (4) that

$$\pi_{H_2} \Phi(h) \pi'_{H_1} \ = \ n_{H_1} h, \quad \text{for all } h \in \mathrm{Hom}(A_{H_1}, A_{H_2}). \tag{25}$$

Thus, Φ defines an isomorphism (of additive groups)

$$\Phi : \mathrm{Hom}(A_{H_1}, A_{H_2}) \ \tilde{\rightarrow} \ \mathcal{H}(H_1, H_2)$$

which extends to an isomorphism

$$\Phi^0 : \mathrm{Hom}^0(A_{H_1}, A_{H_2}) := \mathrm{Hom}(A_{H_1}, A_{H_2}) \otimes \mathbb{Q} \ \tilde{\rightarrow} \ \tilde{R}.$$

(To see that Φ^0 is surjective, note that if $\tilde{f} = \frac{f}{n} \in \tilde{R}$ with $f \in R$, $n \in \mathbb{N}$, then $\tilde{h} = \frac{1}{n n_{H_1}} \pi_{H_2} f \pi'_{H_1} \in \mathrm{Hom}^0(A_{H_1}, A_{H_2})$ and $\Phi^0(\tilde{h}) = \tilde{f}$.) Thus, $\mathcal{H}(H_1, H_2)$ is a *lattice* of $\tilde{R}$, i.e. it is an additive subgroup of $\tilde{R}$ which contains a $\mathbb{Q}$-basis of $\tilde{R}$.

Note that the lattices $\mathcal{H}(H_1, H_2)$ can be viewed as a generalization of $I(H)$-construction. Indeed, if we take $H_2 = 0$, then we have

$$\mathcal{H}(H, 0) \ = \ \mathrm{Hom}(A_H, A) \pi_H \ = \ I(H)$$

because $\Phi_{H,0}(h) = h\pi_H$ as here $n_{H_2} = 1$, $A_{H_2} = A$ and $\pi_{H_2} = \pi'_{H_2} = 1_A$.

(b) The map Φ_{H_1,H_2} is *multiplicative* in the sense that if H_3 is another finite subgroup scheme of A, then for $h_i \in \mathrm{Hom}(A_{H_i}, A_{H_{i+1}})$, $i = 1, 2$, we have that

$$\Phi_{H_2,H_3}(h_2)\Phi_{H_1,H_2}(h_1) \;=\; \Phi_{H_1,H_3}(h_2 \circ h_1). \tag{26}$$

Indeed, writing $\pi_i = \pi_{H_i}$, $\pi'_i = \pi'_{H_i}$, and $n_i = n_{H_i}$, for $i = 1, 2, 3$, we have by using (4) that $\Phi_{H_2,H_3}(h_2)\Phi_{H_1,H_2}(h_1) = \frac{1}{d_3}\pi'_3 h_2 \pi_2 \frac{1}{d_2}\pi'_2 h_1 \pi_1 = \frac{1}{d_3}\pi'_3 h_2 h_1 \pi_1 = \Phi_{H_1,H_3}(h_2 \circ h_1)$.

In particular, if $H_1 = H_2 = H$, then $\Phi_H = \Phi_{H,H}$ defines a ring isomorphism

$$\Phi_H : \mathrm{End}(A_H) \;\tilde{\to}\; \mathcal{E}(H) := \mathcal{H}(H, H),$$

and so $\mathcal{E}(H)$ is a subring of $\tilde{R}$. (Note that $\Phi_H(1_{A_H}) = \frac{1}{n_H}\pi'_H\pi_H = 1_A$.) We observe that since $\Phi_H(\pi_H h \pi'_H) = n_H h$, $\forall h \in R$, we have the inclusions

$$n_H R \;\subset\; \mathcal{E}(H) \;\subset\; \tfrac{1}{n_H} R. \tag{27}$$

(c) If $H \leq H'$, then $\Phi_{H,H'}(\pi_{H,H'}) = 1_A$ because $\Phi_{H,H'}(\pi_{H,H'}) = \frac{1}{n_{H'}}\pi'_{H'}\pi_{H,H'}\pi_H = \frac{1}{n_{H'}}\pi'_{H'}\pi_{H'} = 1_A$. Thus, if $H_1 \geq H'_1$ and $H_2 \leq H'_2$, then it follows from (26) that

$$\Phi_{H_1,H_2}(h) = \Phi_{H_2,H'_2}(\pi_{H_2,H'_2})\Phi_{H_1,H_2}(h)\Phi_{H'_1,H_1}(\pi_{H'_1,H_1}) = \Phi_{H'_1,H'_2}(\pi_{H_2,H'_2} \circ h \circ \pi_{H'_1,H_1}),$$

for all $h \in \mathrm{Hom}(A_{H_1}, A_{H_2})$, and so it follows that

$$H_1 \;\geq\; H'_1, \;\; H_2 \;\leq\; H'_2 \quad\Rightarrow\quad \mathcal{H}(H_1, H_2) \;\subset\; \mathcal{H}(H'_1, H'_2). \tag{28}$$

We now want to describe $\mathcal{H}(H_1, H_2)$ in terms of the ideals $I(H_i)$. For this, it is useful to introduce the following notation. If S, T are subsets of $\tilde{R}$, put

$$(S : T) \;:=\; \{f \in \tilde{R} : Tf \subset S\} \;=\; \{f \in \tilde{R} : tf \in S, \forall t \in T\}.$$

We then have the following description of $\mathcal{H}(H_1, H_2)$.

Proposition 10 *If H_1, H_2 are finite subgroup schemes of A and if I_1, I_2 are regular left R-ideals, then*

$$\mathcal{H}(H_1, H_2) \;\subset\; (I(H_1) : I(H_2)), \tag{29}$$

$$(I_1 : I_2) \;\subset\; \mathcal{H}(H(I_1), H(I_2)). \tag{30}$$

Moreover, if H_2 is an ideal subgroup, then equality holds in (29)*, and if I_1 is a kernel ideal, then equality holds in* (30)*.*

Proof. To prove (29), let $h \in \mathrm{Hom}(A_{H_1}, A_{H_2})$ and $f = f'\pi_{H_2} \in I(H_2)$, where $f' \in \mathrm{Hom}(A_{H_1}, A)$. Then by (4) we have $f\Phi(h) = f'\pi_{H_2}\frac{1}{n_{H_2}}\pi'_{H_2}h\pi_{H_1} = f'h\pi_{H_1} \in I(H_2)$, and so the inclusion (29) follows.

In order to prove (30), we first observe that

$$\mathcal{H}(H_1, H_2) \;=\; \left\{\tfrac{f}{n} : f \in R, n \in \mathbb{N} \text{ and } [n]^{-1}(H_1) \leq f^{-1}(H_2)\right\}. \tag{31}$$

Indeed, if $\tilde{f} \in \mathcal{H}(H_1, H_2)$, then $\tilde{f} = \frac{f}{n}$, where $n = n_{H_2}$ and $f = \pi'_{H_2}h\pi_{H_1}$, for some $h \in \mathrm{Hom}(A_{H_1}, A_{H_2})$. Then $\pi_{H_2}f = nh\pi_{H_1} = h(n\pi_{H_2})$, so $f^{-1}(H_2) = \mathrm{Ker}(\pi_{H_2}f) = \mathrm{Ker}(hn\pi_{H_1}) \geq \mathrm{Ker}(n\pi_{H_1}) = [n]^{-1}(H_1)$. Thus, the left hand side of (31) is contained in the right hand side.

Conversely, suppose that $f \in R$ and $n \in \mathbb{N}$ satisfy $[n]^{-1}(H_2) \leq f^{-1}(H_2)$, i.e. $\mathrm{Ker}(n\pi_{H_1}) \leq \mathrm{Ker}(\pi_{H_2}f)$. Then by the universal property of quotients $\exists h \in \mathrm{Hom}(A_{H_1}, A_{H_2})$ such that $\pi_{H_2}f = hn\pi_{H_1} = nh\pi_{H_1}$. Then $n_{H_2}f = \pi'_{H_2}\pi_{H_2}f = \pi'_{H_2}nh\pi_{H_1}$, so $f = \frac{n}{n_{H_2}}\pi'_{H_2}h\pi_{H_1} = n\Phi_{H_1.H_2}(h)$. Thus $\tilde{f} := \frac{f}{n} = \Phi_{H_1,H_2}(h) \in \mathcal{H}(H_1, H_2)$, and so we have verified that equality holds in (31).

Now we prove (30). For this, let $\tilde{f} = \frac{f}{n} \in (I_1 : I_2)$ with $f \in R$, $n \in \mathbb{N}$, and write $H_i = H(I_i)$ and $\pi_i = \pi_{H_i}$ for $i = 1, 2$. We first claim that

$$\mathrm{Ker}(n\pi_1) \;\leq\; \mathrm{Ker}(\alpha f), \quad \forall \alpha \in I_2.$$

Indeed, since $\frac{\alpha}{n}f = \alpha\tilde{f} =: \beta \in I_1$, we have $\alpha f = n\beta$. Since $H_1 = H(I_1) \leq \mathrm{Ker}(\beta)$, we thus have $\mathrm{Ker}(n\pi_1) \leq \mathrm{Ker}(n\beta) = \mathrm{Ker}(\alpha f)$, which proves the above claim.

Now since $H_2 = H(I_2) = \cap_i \mathrm{Ker}(\alpha_i)$, if $I_2 = \sum_i R\alpha_i$, we see that $\mathrm{Ker}(\pi_2 f) = f^{-1}(H_2) = \cap_i f^{-1}(\mathrm{Ker}(\alpha_i)) = \cap_i \mathrm{Ker}(\alpha_i f)$. It thus follows from the above claim that $\mathrm{Ker}(n\pi_1) \leq \mathrm{Ker}(\pi_2 f)$, and hence $\tilde{f} \in \mathcal{H}(H_1, H_2)$ by (31). This proves (30).

By combining (29) and (30) we obtain

$$\mathcal{H}(H_1, H_2) \subset (I(H_1) : I(H_2)) \subset \mathcal{H}(H(I(H_1)), H(I(H_2))) \subset \mathcal{H}(H_1, H(I(H_2))), \tag{32}$$

where the last inclusion follows from (28) (together with (8)). Thus, if H_2 is an ideal subgroup, i.e. if $H_2 = H(I(H_2))$, then equality holds throughout, and hence equality holds in (29). Similarly, combining (29) and (30) yields

$$(I_1 : I_2) \subset \mathcal{H}(H(I_1), H(I_2)) \subset (I(H(I_1)) : I(H(I_2))) \subset (I(H(I_1)) : I_2) \tag{33}$$

and so equality holds throughout if I_1 is a kernel subgroup.

As an application, we obtain that ideal subgroups H satisfy the extra condition that $Z(R) \subset \mathcal{E}(H)$, where $Z(R) = \{z \in R : xz = zx, \forall x \in R\}$ denotes the *centre* of R. This condition is usually not true for arbitrary subgroup schemes of A, as we shall see in Remark 17(b) below.

Corollary 11 *If H is an ideal subgroup of A, then $Z(R) \subset \mathcal{E}(H)$.*

Proof. By hypothesis, $H = H(I)$, for some regular left R-ideal I, and so $(I : I) \subset \mathcal{E}(H)$ by (30). Now $Z(R) \subset (I : I)$ because I is a left R-ideal (for $z \in Z(R) \Rightarrow Iz = zI \subset I$), and so the assertion follows.

The following result, which is a variant of a result of [26], p. 534, shows that the subgroup scheme associated to a product of ideals has a natural interpretation in terms of composition of maps.

Proposition 12 *Let I be a regular left R-ideal and let J be a regular left R'-ideal, where $R' = \mathcal{E}(H(I))$. Then IJ is a regular left R-ideal and*

$$H(IJ) \;=\; \mathrm{Ker}(\pi_{H(\Phi_I^{-1}(J))} \circ \pi_{H(I)}), \tag{34}$$

where $\Phi_I = \Phi_{H(I)} : \mathrm{End}(A_{H(I)}) \xrightarrow{\sim} R'$ and $\pi_{H(\Phi_I^{-1}(J))} : A_{H(I)} \to (A_{H(I)})_{H(\Phi_I^{-1}(J))}$ is the canonical quotient map.

Proof. Put $H = H(I)$. Since $J \subset \mathcal{E}(H) \subset (I(H) : I(H))$ by (29), we have $IJ \subset I(H)J \subset I(H) \subset R$, and hence IJ is an R-ideal. Moreover, IJ is regular because by hypothesis $\exists \alpha \in I \cap \tilde{R}^\times$ and $\beta \in J \cap \tilde{R}^\times$, and so $\alpha\beta \in IJ \cap \tilde{R}^\times$, which means that IJ is regular.

To prove (34), note first that it follows from (25) that $n\Phi_I^{-1}(J) = \pi J \pi'$, where $n = n_H$, $\pi = \pi_H$, and $\pi' = \pi'_H$, and so $\Phi_I^{-1}(J)\pi = \pi J$. From this it follows that

$$\mathrm{Ker}(\pi f) \;=\; \cap_{g \in I} \mathrm{Ker}(gf), \quad \forall f \in J, \tag{35}$$

where we view $\pi f \in \mathrm{Hom}(A, A_H)$ since $\pi f = f_1 \pi$ for some $f_1 \in \Phi_I^{-1}(J) \subset \mathrm{End}(A_H)$. To verify (35), write $f = f_2/n$ with $f_2 \in R$ and $n \in \mathbb{N}$. Then

$$\begin{aligned} [n]^{-1}(\mathrm{Ker}(\pi f)) \;&=\; \mathrm{Ker}(\pi f_2) \;=\; f_2^{-1}(\mathrm{Ker}(\pi)) = f_2^{-1}(\cap_{g \in I} \mathrm{Ker}(g)) \\ &=\; \cap_{g \in I} f_2^{-1}(\mathrm{Ker}(g)) = \cap_{g \in I} \mathrm{Ker}(gf_2) = [n]^{-1}(\cap_{g \in I} \mathrm{Ker}(gf)), \end{aligned}$$

the latter because $gf_2 = gfn$ and $gf \in R$, for all $g \in I$. From this, equation (35) follows because $[n]$ is faithfully flat.

Using (35), we therefore obtain that

$$\begin{aligned} \mathrm{Ker}(\pi_{H(\Phi_I^{-1}(J))}\pi) \;&=\; \pi^{-1}(\mathrm{Ker}(\pi_{H(\Phi_I^{-1}(J))})) \;=\; \pi^{-1}(\cap_{f \in \Phi_I^{-1}(J)} \mathrm{Ker}(f)) \\ &= \cap_{f \in \Phi_I^{-1}(J)} \mathrm{Ker}(f\pi)) \;=\; \cap_{f' \in \Phi_I^{-1}(J)\pi} \mathrm{Ker}(f')) \;=\; \cap_{f' \in \pi J} \mathrm{Ker}(f')) \\ &= \cap_{f \in J} \mathrm{Ker}(\pi f)) \;=\; \cap_{f \in J} f^{-1}(\mathrm{Ker}(\pi)) \;=\; \cap_{f \in J} f^{-1}(\cap_{g \in I} \mathrm{Ker}(g)) \\ &= \cap_{f \in J} \cap_{g \in I} \mathrm{Ker}(gf) \;=\; H(IJ), \end{aligned}$$

which proves (34).

2.4 The quadratic case

We now specialize the discussion to the case that $\tilde{R}$ is a quadratic field $F \supset \mathbb{Q}$. Since R is finitely generated (as a $\mathbb{Z}$-module), it follows that R is an order of $F = \tilde{R}$, i.e. R is a subring of F which is lattice. We first recall some basic facts about such orders and lattices (cf. [3], §II.7 or [6], ch. 7).

Every order R of F is contained in the maximal order $\mathfrak{O}_F$, the ring of integers of F, and is uniquely determined by its *conductor* $f_R := [\mathfrak{O}_F : R]$. Indeed, if $\Delta(R) := f_R^2 \Delta_F$, where $\Delta_F = \Delta(\mathfrak{O}_F)$ is the discriminant of F (or, more correctly, of $\mathfrak{O}_F$), then we have

$$R \;=\; R_\Delta \;:=\; \mathbb{Z} + \mathbb{Z}\omega_\Delta, \quad \text{where } \omega_\Delta \;=\; \frac{1}{2}(\Delta + \sqrt{\Delta}). \tag{36}$$

Thus, R is also uniquely determined by its *discriminant* $\Delta(R)$. Conversely, for each integer f there is unique order of conductor f. Moreover, if R_1, R_2 are orders in F then we have

$$R_1 \subset R_2 \;\Leftrightarrow\; f_{R_2} | f_{R_1} \text{ and hence } f_{R_1 R_2} = (f_{R_1}, f_{R_2}),\; f_{R_1 \cap R_2} = \mathrm{lcm}(f_{R_1}, f_{R_2}). \tag{37}$$

Let Lat_F denote the set of lattices of F, i.e. the set of finitely generated subgroups L of F such that $LF = F$. If $L \in \mathrm{Lat}_F$, then $R(L) := (L : L)$ is an order of F, and for a given order R, the set

$$\mathrm{Lat}(R) = \{L \in \mathrm{Lat}_F : R(L) = R\}$$

is the set of invertible R-submodules of F, and hence forms an abelian group under the multiplication of lattices. Here the identity is R and the inverse of L is

$$L^{-1} \;=\; (R(L) : L) \;=\; \sigma(L) N(L)^{-1}, \tag{38}$$

where $\sigma \in \mathrm{Gal}(F/\mathbb{Q})$ is the unique nontrivial automorphism of F and $N(L) \in \mathbb{Q}^\times$ is the *norm* of L. Moreover, the group

$$\mathrm{Pic}(R) \;=\; \mathrm{Lat}(R)/\{fR : f \in F^\times\}$$

is a finite abelian group whose order is denoted by $h(R) = h(\Delta(R))$.

For later reference we recall the following useful formulae (cf. [6], p. 151):

$$R(L_1 L_2) \;=\; R(L_1) R(L_2) \quad \text{and} \quad N(L_1 L_2) \;=\; N(L_1) N(L_2). \tag{39}$$

In addition, we have following formulae (40) and (41) will be used several times below. Since there does not seem to be a suitable reference, we provide a proof of these identities. Note that (41) is stated without proof on p. 71 of [12].

Lemma 13 *If $L_1, L_2 \in \mathrm{Lat}_F$ are any two lattices of F, then*

$$(L_1 : L_2)L_2 \;=\; (R(L_1) : R(L_2))L_1. \tag{40}$$

Thus, if $f_i = f_{R(L_i)} = [\mathcal{O}_F : R(L_i)]$, for $i = 1, 2$, and if $f = (f_1, f_2)$, then we have

$$(L_1 : L_2) \;=\; [R(L_1)R(L_1) : R(L_1)]L_1L_2^{-1} \;=\; \frac{f_1}{f}L_1L_2^{-1}. \tag{41}$$

Proof. Put $R_i = R(L_i)$ and $R_0 = R_1R_2 = R(L_1L_2)$. Note that $(L_1 : L_2)$ is an R_0-module, for if $c \in (L_1 : L_2)$ and $r_i \in R(L_i)$, then $cr_1r_2 \in (L_1 : L_2)$ because $r_1cr_2L_2 \subset r_1cL_2 \subset r_1L_1 \subset L_1$. In particular, $(R_1 : R_2)$ is also an R_0-module (because $R(R_i) = R_i$).

Now let $c \in (L_1 : L_2)$. Then $(cL_1^{-1}L_2)R_2 = cL_1^{-1}L_2 = cL_2L_1^{-1} \subset L_1L_1^{-1} = R_1$, so $cL_2L_1^{-1} \subset (R_1 : R_2)$, and hence $(L_1 : L_2)L_2L_1^{-1} \subset (R_1 : R_2)$. Thus $(L_1 : L_2)L_2R_1 = (L_1 : L_2)L_2^{-1}L_1 \subset (R_1 : R_2)L_1$. But since $(L_1 : L_2)$ is an R_1-module (as $R_1 \subset R_0$), we have that $(L_1 : L_2)L_2R_1 = (L_1 : L_2)L_2$, and so the left hand side of (40) is contained in the right hand side.

To prove the other inclusion, let $r \in (R_1 : R_2)$. Then $(rL_1L_2^{-1})L_2 = rL_1R_2 = rR_2L_2 \subset R_1L_1 = L_1$, so $rl_1L_2^{-1} \subset (L_1 : L_2)$, and hence $(R_1 : R_2)L_1L_2^{-1} \subset (L_1 : L_2)$. Thus $(R_1 : R_2)L_1R_2 = (R_1 : R_2)L_1L_2^{-1}L_2 \subset (L_1 : L_2)L_2$, and so the other inclusion of (40) holds because $(R_1 : R_2)L_1R_2 = (R_1 : R_2)L_1$ (since $(R_1 : R_2)$ is an R_2-module). This proves (40).

The formula (41) follows immediately from (40) once we have shown that

$$(R(L_1) : R(L_1)) \;=\; \frac{f_1}{f}R(L_1)R(L_2) \quad \text{and} \quad \frac{f_1}{f} \;=\; [R(L_1)R(L_2) : R(L_1)]. \tag{42}$$

Indeed, multiplying (40) by L_2^{-1}, we obtain with (42) that $(L_1 : L_2) = \frac{f_1}{f}R_1R_2L_1L_2^{-1} = \frac{f_1}{f}L_1L_2^{-1}$, where the last equality follows from the obvious fact that $L_i^{\pm 1}$ is an R_i-module, for $i = 1, 2$.

It thus remains to verify (42). For this, we first note that since $f = f_{R_0}$ by (39), we have that $[R_0 : R_1] = \frac{f_1}{f}$, which is the second equality of (42). Thus, $\frac{f_1}{f}R_0$ is largest R_0-module which is contained in R_1, and hence $(R_1 : R_2) \subset \frac{f_1}{f}R_0$ because $(R_1 : R_2)$ is an R_0-module which is contained in R_1. On the other hand, since $\frac{f_1}{f}R_2 \subset \frac{f_1}{f}R_0 \subset R_1$, we have the opposite inclusion $\frac{f_1}{f}R_0 \subset (R_1 : R_2)$, which proves (42).

Corollary 14 *Every non-zero ideal of an order in F is a divisorial ideal.*

Proof. Let R be an order of F and let I be a nonzero R-ideal. Then $I \in \mathrm{Lat}_F$ and $R \subset R(I)$. Applying (41) to $L_1 = R$ and $L_2 = I$ yields

$$(R : I) \;= [R(I) : R]I^{-1} \tag{43}$$

because here $f_2|f_1$, so $f = f_2$ and $\frac{f_1}{f} = [R(I) : R]$. Next, apply (41) to $L_1 = R$ and $L_2 = (R : I)$. Since $R(L_2) = R(I^{-1}) = R(I)$ by (43), we see that in this case (41) gives

$$(R : (R : I)) = [R(I) : R]((R : I))^{-1} = [R(I) : R][R(I) : R]^{-1}(I^{-1})^{-1} = I$$

Since $I^* = (R : (R : I))$ by [5], p. 476, we thus have that $I = I^*$, and so I is a divisorial ideal in the sense of Remark 7(d).

We now apply the preceding results to abelian varieties.

Proposition 15 *Let A/K be an abelian variety such that $\tilde{R} = \mathrm{End}^0(A)$ is a quadratic field. Then every non-zero ideal of $R = \mathrm{End}(A)$ is a kernel ideal, and hence we have for any two non-zero ideals I, J of R that $\Phi_{I,J} := \Phi_{H(I),H(J)}$ defines an isomorphism*

$$\Phi_{I,J} := \Phi_{H(I),H(J)} : \mathrm{Hom}(A_{H(I)}, A_{H(J)}) \quad \xrightarrow{\sim} \quad (I : J). \tag{44}$$

Moreover, we have that $A_{H(I)} \simeq A_{H(J)} \Leftrightarrow I \simeq J$ (as R-modules).

Proof. Since R is an order of $\tilde{R} = F$, we know by Corollary 14 that every non-zero ideal of R is divisorial and hence a kernel ideal by Remark 7(d). This proves the first assertion, and hence the other assertions follow from Proposition 10 and from the discussion after (20).

Corollary 16 *In the above situation, let R' be an order of $\tilde{R}$ with $R \subset R'$. Then there exists an abelian variety A'/K which is isogenous to A/K such that $\mathrm{End}(A') \simeq R'$.*

Proof. Take $I = [R' : R]R' \subset R$. Then I is a non-zero R-ideal with $R(I) = R'$. Then $A' := A_{H(I)}$ is isogenous to A and $\mathrm{End}(A') \simeq (I : I) = R(I) = R'$ by (44).

Remark 17 (a) Note that if we drop the hypothesis $R \subset R'$ in Corollary 16, then the corresponding statement is in general no longer true; cf. §3.3 below.

(b) We can use the above Corollary 16 to construct an abelian variety A' with a finite subgroup scheme H' such that $\mathcal{E}(H') \not\subset \mathrm{End}(A')$. In particular, H' is not an ideal subgroup by Corollary 11.

Indeed, suppose there exists an abelian variety A/K such that $R := \mathrm{End}(A) \subset F$ but $R \neq \mathfrak{O}_F$. Then by Corollary 16 there is an R-ideal I such that $A' := A_{H(I)}$ satisfies $\mathrm{End}(A') \simeq \mathfrak{O}_F$. Consider $H' = \mathrm{Ker}(\pi'_{H(I)})$. Since $\pi'_{H(I)} : A' \to A$ is an isogeny, we have $(A')_{H'} \simeq A$, so $\mathcal{E}(H') \simeq \mathrm{End}(A) = R$. Thus $\mathcal{O}_F = \mathrm{End}(A') \not\subset \mathcal{E}(H')$, and so H' is not an ideal subgroup of A'.

3 CM elliptic curves

3.1 Kernel ideals and ideal subgroups

We now apply the theory of the previous section to the case that $A = E$ is elliptic curve over K with complex multiplication. By this we mean that E/K is an elliptic curve such that

$$\mathrm{End}^0(E) \;=\; \mathrm{End}^0(E \otimes \overline{K}) \;= F$$

is an imaginary quadratic field F, where $\overline{K}$ denotes the algebraic closure of K. Note that this definition is slightly more restrictive than that of (say) [18], since we assume here that all $\overline{K}$-endomorphisms are already defined over K.

If E/K is a CM elliptic curve, then $R = \mathrm{End}(E)$ is an order in F. Thus, R is uniquely characterized by its conductor $f_E := [\mathfrak{O}_F : R]$ or by its discriminant $\Delta_E := \Delta(R)$, which we call the *conductor* and *discriminant* of E, respectively.

The main results about kernel ideals and ideal subgroups are summarized in the following theorem which can be viewed as a refinement of results of Deuring[10] and Waterhouse[26].

Theorem 18 *Let E/K be a CM elliptic curve and $R = \mathrm{End}(E)$. Then:*

(a) *Every non-zero R-ideal I is a kernel ideal. Thus*

$$\Phi_{I_1,I_2} := \Phi_{H(I_1),H(I_2)} : \mathrm{Hom}(E_{H(I_1)}, E_{H(I_2)}) \;\xrightarrow{\sim}\; (I_1 : I_2) \tag{45}$$

is an isomorphism for all non-zero ideals I_1, I_2 of R.

(b) *If H be a finite subgroup scheme of E, then*

$$H \text{ is an ideal subgroup} \quad\Leftrightarrow\quad f_{E_H} | f_E. \tag{46}$$

Thus, if H_1, H_2 are finite subgroup schemes of E such that $f_{E_{H_i}} | f_E$, for $i = 1, 2$, then

$$\Phi_{H_1,H_2} : \mathrm{Hom}(E_{H_1}, E_{H_2}) \;\xrightarrow{\sim}\; \mathcal{H}(H_1, H_2) \;=\; (I(H_1) : I(H_2)), \tag{47}$$

and we have

$$E_{H_1} \;\simeq\; E_{H_2} \quad\Leftrightarrow\quad I(H_1) \;\simeq\; I(H_2). \tag{48}$$

Proof. (a) This is a special case of Proposition 15.

(b) We first observe that it is enough to verify (46), for then (47) follows immediately from Proposition 10 and (48) follows from (21).

To prove (46), we first note that since $\mathcal{E}(H) \simeq \mathrm{End}(E_H)$, it follows from (37) that $f_{E_H} | f_E \Leftrightarrow R \subset \mathcal{E}(H)$. Thus, the one direction ($\Rightarrow$) follows directly from Corollary 11.

Conversely, suppose that $f_{E_H} | f_E$ or, equivalently, that $R \subset R' := \mathcal{E}(H)$. By (15) it is enough to show that $H_n := [n]^{-1}(H)$ is an ideal subgroup, for some $n \in \mathbb{N}$.

For this, put $f = [R' : R]$, $I = fR'$, and $E' = E_{H(I)}$. Then by (45) we have $\mathrm{End}(R') \simeq (I : I) = R'$. Moreover, if $\pi := \pi_{H(I)} : E \to E'$ and $n := \deg(\pi)$, then by (4) we have $\pi_H[n] = \pi_H \pi' \pi$, where $\pi' = \pi'_{H(I)}$, and so $[n]^{-1}(H) = \mathrm{Ker}(\pi_H[n]) = \pi^{-1}(H')$, where $H' = \mathrm{Ker}(\pi_H \pi')$ is a finite subgroup scheme of E'.

Since $\pi_H \pi' : E' \to E_H$ is an isogeny, it follows that $(E')_{H'} \simeq E_H$, and hence $\mathrm{End}((E')_{H'}) \simeq \mathrm{End}(E_H) \simeq \mathcal{E}(H) = R' \simeq \mathrm{End}(E')$. Thus, by the abovementioned result of Deuring/Waterhouse (which is proved via ℓ-adic representations; cf. [10] or [26], p. 541), there is an ideal I' of $\mathrm{End}(E')$ such that $H' = H(I')$. If $\tilde{I}' = \Phi_I(I')$ is the corresponding ideal of $\mathcal{E}(H(I)) = R'$, then by Proposition 12 we have that $H(I\tilde{I}') = \mathrm{Ker}(\pi_{H(I')} \circ \pi_{H(I)}) = \pi^{-1}(H') = [n]^{-1}(H)$. Thus, $[n]^{-1}(H)$ is an ideal subgroup of E, and hence so is H (by what was said above).

We can apply the above results to obtain information about the following subset $\mathrm{Isog}^+(E/K)$ of the set $\mathrm{Isog}(E/K)$ of elliptic curves isogenous to E/K.

Notation. Let $\mathrm{Isog}(E/K) = \{E'/K : E' \sim E\}/\simeq$ be the set of isomorphism classes of elliptic curves E'/K which are isogenous to E, and let

$$\mathrm{Isog}^+(E/K) \;=\; \{E' \in \mathrm{Isog}(E/K) : f_{E'} | f_E\}.$$

Corollary 19 *If E/K is a CM elliptic curve, then the map $E' \mapsto I_E(E')$ induces a bijection*

$$I_E^+ : \mathrm{Isog}^+(E/K) \;\tilde{\to}\; Id(R_E))/\simeq,$$

where $Id(R_E)/\simeq$ denotes the set of isomorphism classes of non-zero ideals of $R_E = \mathrm{End}(E)$.

Proof. By the discussion of subsection 2.2 we know that the given rule defines a map $I_E : \mathrm{Isom}(E/K) \to Id(R)/\simeq$. We denote its restriction to $\mathrm{Isom}^+(E/K)$ by I_E^+.

To show that I_E^+ is surjective, let $I \in Id(R)$, and put $E' = E_{H(I)}$. Then by (45) we have that $\mathrm{End}(E') \simeq (I : I) = R(I) \supset R$, This means that $f_{E'} | f_E$, and so $E' \in \mathrm{Isog}^+(E/K)$. Moreover, $I_E(E') \simeq I(H(I)) = I$, and hence I_E^+ is surjective.

To show that I_E^+ is injective, let $E_1, E_2 \in \mathrm{Isog}^+(E/K)$ such that $I_E(E_i) \simeq I_E(E_2)$. Thus, by definition, $I(H_1) \simeq I(H_2)$, where $H_i = \mathrm{Ker}(\pi_i)$ and $\pi_i : E \to E_i$ are any two isogenies, and we have $f_{E_i} | f_E$. Since $E_i = E_{H_i}$, we have by (48) that $I(H_1) \simeq I(H_2)$, and so I_E^+ is injective.

Remark 20 It follows from (45) that for any R-ideal I we have that

$$\mathrm{End}(E_{H(I)}) \simeq (I : I) = R(I) \quad \text{and so} \quad f_{E_{H(I)}} = f_E [R(I) : R_E]^{-1}. \tag{49}$$

Moreover, by (47) we have that

$$\mathrm{End}(E') \simeq R(I_E(E')) \quad \text{and} \quad f_{E'} = f_{R(I_E(E'))}, \quad \text{for all } E' \in \mathrm{Isog}^+(E/K). \tag{50}$$

From this we see that if we restrict the map I_E^+ to the subset

$$\mathrm{Isog}^*(E/K) \;=\; \{E' \in \mathrm{Isog}(E/K) : f_{E'} = f_E\},$$

then we obtain the (well-known) bijection

$$\mathrm{Isog}^*(E/K) \;\stackrel{\sim}{\to}\; \{I \in Id(R_E) : R(I) = R_E\}/\simeq \;\stackrel{\sim}{\to}\; \mathrm{Pic}(R). \tag{51}$$

Thus, $\mathrm{Isog}^*(E/K)$ is a finite set of cardinality $h(\Delta_E) := h(R_{\Delta_E})$. Moreover, since

$$\mathrm{Isog}^+(E/K) \;=\; \dot{\bigcup_{f|f_E}} \{E' \in \mathrm{Isog}(E/K) : f'_E = f\} \;=\; \dot{\bigcup_{f|f_E}} \mathrm{Isog}(E_f/K),$$

where $E_f \sim E$ is an elliptic curve of conductor $f|f_E$ (which exists by Corollary 16), we see that $\mathrm{Isog}^+(E/K)$ is also finite set of cardinality

$$\#(\mathrm{Isog}^+(E/K)) \;=\; \sum_{f|f_E} h(\Delta_E/f^2). \tag{52}$$

On the other hand, the set $\mathrm{Isog}(E/K)$ is often infinite; for example, this is the case when K is algebraically closed.

We can also give a "numerical criterion" to detect ideal subgroups; cf. Corollary 23 below. For this we first prove the following result which is also of independent interest.

Proposition 21 *If I is a non-zero ideal of $R = \mathrm{End}(E)$, then*

$$|H(I)| \;=\; \deg(\pi_{H(I)}) \;= [R : I]. \tag{53}$$

Remark 22 If I is not invertible (i.e. if $R(I) \neq R$), then the above formula (53) contradicts the formula on p. 211 of Deuring[10], who asserts that $|H(I)| = [R(I) : I]$ in place of $|H(I)| = [R : I]$.

In fact, Deuring's proof of his statement contains an error. While his proof in the case that $R(I) = R$ is correct, his proof of the general case is not. To be precise, on p. 218 he uses a result of W. Weber incorrectly because that result only applies to invertible ideals (and is, in fact, false otherwise).

Proof of Proposition 21. We first note that if $f \in R = \mathrm{End}(E)$, then

$$\deg(f) \;=\; |\mathrm{Ker}(f)| \;=\; N(f), \tag{54}$$

where $N = N_{F/\mathbb{Q}}$ denotes the usual field norm. Indeed, by e.g. [20], p. 180, we know that $P_f(f) = 0$ where $P_f(X) = X^2 + tX + \deg(f)$, for some $t \in \mathbb{Z}$, and so (54) follows.

From (54) we can conclude that

$$\deg(\pi_{H(I)}) \mid \gcd(\{N(f) : f \in I\}) \;=\; N(I) \;=\; [R(I) : I] \tag{55}$$

because if $f \in I$, then $H(I) \leq \mathrm{Ker}(f)$ and so $|H(I)| = \deg(\pi_{H(I)})|\deg(f) = N(f)$ by (54). Thus, the indicated divisibility holds. The last equality of (55) is just the definition of $N(I)$, and the first equality is well-known. (It follows from one of the steps needed to verify the bijection between equivalence classes of binary quadratic forms and equivalence classes of invertible R'-modules (where $R' = R(I)$).)

Suppose first that I is invertible (i.e. $R(I) = R$). Then $\sigma(I)$ is also an invertible R-ideal (where $\sigma \in \mathrm{Gal}(F/\mathbb{Q}), \sigma \neq 1$) and $N(\sigma(I)) = N(I)$. Moreover, $I\sigma(I) = N(I)R$ by (38). Since $\mathcal{E}(E_{H(I)}) = (I : I) = R(I) = R$, we can apply Proposition 12 to $J = \sigma(I)$ to obtain $H(I\sigma(I)) = \mathrm{Ker}(\pi_H(I')) \circ \pi_{H(I)})$, where $I' = \Phi_I^{-1}(\sigma(I))$. Thus, $|H(I\sigma(I))| = |H(I')| \cdot |H(I)|$. Since $H(I\sigma(I)) = \mathrm{Ker}([N(I)])$, we thus obtain from (54) and (55) that $N(I)^2 = |H(I')| \cdot |H(I)| \mid N(\sigma(I))N(I) = N(I)^2$, and so it follows that we must have equality throughout, so $|H(I)| = N(I) = [R : I]$. This proves (53) when I is invertible.

In order to prove (53) in the general case, we first verify it in the special case that $I = fR'$, where $R' \supset R$ is an order and $f = [R' : R]$. More precisely, we show that

$$|H(fR')| \;=\; f \;=\; [R : fR'], \quad \text{if } R \subset R' \text{ and } f = [R' : R]. \tag{56}$$

First note that the second equality is clear because $[R' : fR'] = f^2$. To prove the first equality, we shall induct on the number $\nu = \nu(f)$ of primes (counted with multiplicities) which divide f. If $\nu = 1$, then $f = p$ is a prime. Since $p \in pR'$, we have $H(pR') \leq \mathrm{Ker}([p])$, and so by the universal property there exists $g \in \mathrm{Hom}(E', E)$ such that $[p] = g\pi$, where $E' = E_{H(pR')}$ and $\pi = \pi_{H(pR')}$. Thus $\deg(\pi) \mid \deg([p]) = p^2$. Now $\deg(\pi) \neq 1$ because otherwise $E' \simeq E$, which is impossible since $\mathrm{End}(E') \simeq \mathcal{E}(H(pR')) = R' \not\simeq R = \mathrm{End}(E)$. Similarly, $\deg(\pi) \neq p^2$ because otherwise g is an isomorphism and then again $E' \simeq E$, contradiction. Thus $\deg(\pi) = p$, and so (56) holds in this case.

Now suppose $\nu > 1$. Then $f = f'p$, where p is a prime and $\nu(f') \geq 1$. Let R_1 be the unique order such that $R \subset R_1 \subset R'$ and $[R_1 : R] = p$ (and hence $[R' : R_1] = f'$). Put $\pi_1 = \pi_{H(pR_1)} : E \to E_1 := E_{H(pR_1)}$. By what was just shown, $\deg(\pi_1) = p$. Now consider $I' = \Phi_{pR_1}^{-1}(f'R') \subset \mathrm{End}(E_1)$. By the induction hypothesis (applied to E_1 in place of E) we have $\deg(\pi_{I'}) = f'$. Thus, since $pR_1 f' R' = fR'$, we have by Proposition 12 that $H(fR') = \mathrm{Ker}(\pi_{H(I')} \circ \pi_1)$, so $\deg(\pi_{fR'}) = \deg(\pi_{I'})\deg(\pi_1) = f'p = f$, which proves (56).

We can now verify (53) for an arbitrary R-ideal $I \neq 0$. Put $R' = R(I)$ and $f = [R' : R]$. Since I is an R'-ideal contained in R, we have $I \subset fR'$, and so $I' := \frac{1}{f} I \subset R'$. Thus I' is an invertible R'-ideal. Since $\mathcal{E}(H(fR')) = R'$, we see that $I'' = \Phi_{fR'}^{-1}(I')$ is an invertible $\mathrm{End}(E_2)$-ideal, where $E_2 := E_{H(fR')}$, and so, by what

was proved above, $\deg(\pi_{H(I'')}) = [R' : I'] = [fR' : I]$ because $fI' = I$. Now since $(fR')I' = R'I = I$, we have by Proposition 12 that $H(I) = \mathrm{Ker}(\pi_{I''} \circ \pi_{fR'})$, and so $\deg(\pi_{H(I)}) = \deg(\pi_{I''})\deg(\pi_{fR'}) = [fR' : I][R : fR']$ by (56). Thus $\deg(\pi_{H(I)}) = [R : I]$, which proves (53) in general.

Corollary 23 *If H is a finite subgroup scheme, then $|H| \mid [R : I(H)]$, and equality holds if and only if H is an ideal subgroup.*

Proof. Since $H \leq H(I(H))$, we have $|H| \mid |H(I(H))| = [R : I(H)]$ by (53). Moreover, H is an ideal subgroup $\Leftrightarrow H = H(I(H)) \Leftrightarrow |H| = |H(I(H))| \Leftrightarrow |H| = [R : I(H)]$, and so the assertion follows.

Corollary 24 *Let H_1 and H_2 be two ideal subgroups of E and let $f_i = f_{E_{H_i}}$. Then the norms of the ideals $I(H_i)$ and of the lattice $\mathcal{H}(H_1, H_2)$ are given by*

$$N(I(H_i)) \;=\; \frac{f_E}{f_i}|H_i| \quad \textit{and} \quad N(\mathcal{H}(H_1, H_2)) \;=\; \frac{\mathrm{lcm}(f_1, f_1)}{\gcd(f_1, f_2)}\frac{|H_1|}{|H_2|}. \tag{57}$$

Proof. Put $n_i = |H_i|$ and $L_i = I(H_i)$. Since $R(L_i) = \mathcal{E}(H_i) \supset R$ by (46) and (47), we have $[R(L_i) : R] = f_E/f_i$, and so $N(L_i) = [R(L_i) : L_i] = \frac{f_E}{f_i}[R : I(H_i)] = \frac{f_E}{f_i}n_i$ by Corollary 23. This proves the first equality of (57).

Now by (47) and (41) we have $\mathcal{H}(H_1, H_2)) = (L_1 : L_2) = \frac{f_1}{f}L_1L_2^{-1}$, where $f = \gcd(f_1, f_2)$. Thus, using the first equality of (57), we obtain

$$N(\mathcal{H}(H_1, H_2)) = \frac{f_1^2}{f^2}\frac{N(L_1)}{N(L_2)} = \frac{f_1^2}{f^2}\frac{(f_E/f_1)n_1}{(f_E/f_2)n_2} = \frac{f_1f_2}{f^2}\frac{n_1}{n_2},$$

which proves the second equation of (57) because $\mathrm{lcm}(f_1, f_2) = \frac{f_1f_2}{f}$.

For later purposes we briefly consider how the constructions $I(\cdot)$ and $H(\cdot)$ behave under specializations.

Proposition 25 *Let E/K be a CM elliptic curve defined over a number field and $\mathfrak{p}$ be a prime ideal of K with residue field $k = \mathfrak{O}_K/\mathfrak{p}$. Assume that E has good reduction E_k/k at $\mathfrak{p}$. Then:*

(a) *E_k/k is a CM elliptic curve if and only if $p = \mathrm{char}(k)$ splits in $F := \mathrm{End}^0(E)$. If this is the case, then the conductor of E_k is $f_{E_k} = f_E/p^r$, where $p^r || f_E$.*

(b) *Assume that the condition of* (a) *holds, and that $p \nmid f_E$, so that the reduction map defines isomorphisms*

$$r_k : \mathrm{End}(E) \;\xrightarrow{\sim}\; \mathrm{End}(E_k) \quad \textit{and} \quad r_k^0 : \mathrm{End}^0(E) \;\xrightarrow{\sim}\; \mathrm{End}^0(E_k).$$

If H is any finite subgroup scheme of E, then its reduction H_k is a subgroup scheme of the same rank, i.e. $|H_k| = |H|$, and we have

$$r_k(I(H)) \subset I(H_k) \quad \textit{and} \quad r_k^0(\mathcal{E}(H)) \subset \mathcal{E}(H_k). \tag{58}$$

Furthermore, both inclusions are equalities if H is an ideal subgroup or if $(p, |H|) = 1$. In addition, we have

$$H(I)_k = H(r_k(I)), \quad \textit{for all non-zero ideals } I \textit{ of } \mathrm{End}(E). \tag{59}$$

Proof. (a) Lang[18], Theorem 13.12 (p. 182).

(b) We first recall how the reduction map r_k is defined. Let $\mathfrak{O}_\mathfrak{p} = (\mathfrak{O}_K)_\mathfrak{p}$ denote the local ring (valuation ring) at $\mathfrak{p}$, and let $\tilde{E}/\mathfrak{O}_\mathfrak{p}$ denote the minimal (Néron) model of E/K (with respect to $\mathfrak{p}$). Then r_k is defined as the composition of the base-change maps

$$r_k = r_k^E : \mathrm{End}(E) \xleftarrow{\sim} \mathrm{End}(\tilde{E}) \to \mathrm{End}(E_k).$$

Now let H be a finite subgroup scheme of E. To define H_k, we shall use the hypothesis that E/K has good reduction at $\mathfrak{p}$, i.e. that $\tilde{E}/S := \mathrm{Spec}(\mathfrak{O}_\mathfrak{p})$ is an abelian scheme (of relative dimension 1). Then $E_H \sim E$ also has good reduction at $\mathfrak{p}$ (by the criterion of Néron-Ogg-Shafarevich or otherwise), and so π_H extends by the Néron property to a homomorphism $\tilde{\pi}_H : \tilde{E} \to \tilde{E}_H$. By [4], 7.3/6, $\tilde{\pi}_H$ is an isogeny. Moreover, since π_H is proper (because $\tilde{E}_H/S$ is proper), it follows that $\tilde{\pi}_H$ is finite and flat by (the argument of) [4], 7.3/2, and hence $\tilde{H} := \mathrm{Ker}(\tilde{\pi}_H)$ is a subgroup scheme of $\tilde{E}$ which is finite and flat over S and whose generic fibre is H. Thus, its special fibre $H_k = \tilde{H} \times_S \mathrm{Spec}(k)$ is a finite subgroup scheme of E_k of the same rank as H, i.e. $|H| = |H_k|$. Note also that the above shows that $(E_k)_{H_k}$ is the reduction of E_H.

As a special case of this construction we see that

$$\mathrm{Ker}(g)_k = \mathrm{Ker}(\tilde{g}) \times_S \mathrm{Spec}(k) = \mathrm{Ker}(r_k(g)), \quad \text{for all } g \in \mathrm{End}(E). \tag{60}$$

From this, equation (59) follows immediately because intersections (i.e. fibre products) commute with base-change.

To prove the first part of (58), let $h \in I(H)$, so $h = g\pi_H$ with $g \in \mathrm{Hom}(E_H, E)$ and hence $\tilde{h} = \tilde{g}\tilde{\pi}_H$ and $r_k(h) = \tilde{h}_k = \tilde{g}_k(\tilde{\pi}_H)_k = g_k\pi_{H_k} \in I(H_k)$ because $g_k \in \mathrm{Hom}((E_H)_k, E_k)$ (and $(E_H)_k = (E_k)_{H_k}$). This proves the first inclusion of (58).

The second inclusion follows immediately from the fact that

$$r_k^0(\Phi_H(h)) = \Phi_{H_k}(r_k^{E_H}(h)), \quad \text{for all } h \in \mathrm{End}(E_H), \tag{61}$$

which in turn follows from the functoriality of the construction of r_k, for we have that $n_H r_k^0(\Phi_H)(h) = r_k(\pi'_H h \pi_H) = (\pi'_H)_k h_k (\pi_H)_k = \pi'_{H_k} r^{E_H}(h)\pi_{H_k} = n_{H_k}\Phi_{H_k}(r_k^{E_H}(h))$.

Note that it follows from (61) that

$$r_k^0(\mathcal{E}(H)) = \mathcal{E}(H_k) \quad \Leftrightarrow \quad p \nmid f_{\mathcal{E}(H)} = f_{E_H} \tag{62}$$

because by part (a) we know that $r_k^{E_H}$ is surjective if and only if $p \nmid f_{E_H}$.

Now suppose that H is an ideal subgroup scheme. Since $f_{E_H} | f_E$ by (46), it follows from (62) that we have equality in the second part of (58). Moreover, since $H = H(I)$ for some ideal I, we see from (59) that $H_k = H(r_k(I))$ is also an ideal subgroup. Put $R = \mathrm{End}(E)$. Since $r_k(R) = \mathrm{End}(E_k)$, we obtain from Corollary 23 that $[R : I(H)] = |H| = |H_k| = [r_k(R) : I(H_k)]$, and so we must have equality in the first part of (58) as well.

Finally, to prove that equality holds in (58) when $(|H|, p) = 1$, we first observe that although the map $H \mapsto H_k$ is not injective in general, we do have

$$H_1 \leq H_2 \quad \Leftrightarrow \quad (H_1)_k \leq (H_2)_k, \quad \text{if } (|H_1|, p) = 1. \tag{63}$$

To see this, recall first that we also have a reduction map $r_k^{E(K)} : E(K) \to E_k(k)$ on the group of rational points and that by base-change this extends to a map $\overline{r}_k : E(\overline{K}) \to E(\overline{k})$ whose kernel has no non-trivial points of order prime to $p = \mathrm{char}(k)$. We thus have an isomorphism

$$\overline{r}_k^{(p)} : E(\overline{K})_{tor}^{(p)} \xrightarrow{\sim} E_k(\overline{k})_{tor}^{(p)},$$

where $E(\overline{K})_{tor}^{(p)}$ denotes the group of torsion points in $E(\overline{K})$ of order prime to p, and $E_k(\overline{k})_{tor}^{(p)}$ is defined similarly. Now if H is a finite group scheme of E with $(|H|, p) = 1$, then H is an etale group scheme, and so we can identify $H_k \otimes \overline{k}$ and $H \otimes \overline{K}$ with subgroups of $E_k(\overline{k})$ and of $E(\overline{K})$ of the same order and we have $\overline{r}_k^{(p)}(H \otimes \overline{K}) = H_k \otimes \overline{k}$.

From this, the assertion (63) follows immediately, provided that also $(p, |H_2|) = 1$. To prove it without this hypothesis, note that we can reduce the assertion to this case as follows. Put $n_1 = |H_1| = |(H_1)_k|$. Since $H_1 \leq \mathrm{Ker}([n_1])$, we see that $H_1 \leq H_2 \Leftrightarrow H_1 \leq H_2[n_1] := H_2 \cap \mathrm{Ker}([n_1]))$, and similarly, $(H_1)_k \leq (H_2)_k \Leftrightarrow (H_1)_k \leq (H_2)_k[n_1] = (H_2[n_1])_k$. Thus, since $p \nmid |H_2[n_1]|$, it follows that (63) is true.

We are now ready to prove that equality holds in (58) when $p \nmid |H|$. Indeed, since $f_{\mathcal{E}(H)} | n^2 f_E$ by (27), it follows from (62) that equality holds in the second part of (58). To prove this also for the first part, let $g \in I(H_k)$, so $H_k \leq \mathrm{Ker}(g)$. Since $r_k : \mathrm{End}(E) \to \mathrm{End}(E_k)$ is an isomorphism, there exists a unique $g_1 \in \mathrm{End}(E)$ such that $r_k(g_1) = g$. By (60) we know that $\mathrm{Ker}(g_1)_k = \mathrm{Ker}(g)$, and so it follows from (63) that $H \leq \mathrm{Ker}(g_1)$. Thus $g_1 \in I(H)$ and so $g = r_k(g_1) \in r_k(I(H))$. This shows that equality holds in the first part of (58) as well.

3.2 The case $K = \mathbb{C}$

In the case that $K = \mathbb{C}$, every elliptic curve $E/\mathbb{C}$ has an analytic description, i.e. there exists a lattice $L \subset \mathbb{C}$ and an isomorphism of compact Riemann surfaces $E_{\mathbb{C}} \simeq \mathbb{C}/L$, where $E_{\mathbb{C}}$ denotes the compact Riemann surface associated to the (algebraic) curve

E. As we shall see, it is very illuminating to relate the previous constructions to the lattices appearing in the complex theory.

To make this analytic description more precise, recall first that if $L \subset \mathbb{C}$ is any lattice, then the existence of the Weierstrass $\wp$-function $\wp_L$ shows that the Riemann surface $\mathbb{C}/L$ can be identified with a unique elliptic curve $E_L \subset \mathbb{P}^2(\mathbb{C})$ (given by the Weierstrass equation $y^2 = 4x^3 - g_2(L)x - g_2(L)$) and that we have an isomorphism

$$\rho_L : \mathbb{C}/L \xrightarrow{\sim} E_L(\mathbb{C}) \quad \text{given by } z + L \mapsto (\wp_L(z) : \wp_L'(z) : 1) \in \mathbb{P}^2(\mathbb{C}).$$

Conversely, given any $E/\mathbb{C}$, then E is isomorphic to a Weierstrass curve $E' \subset \mathbb{P}^2(\mathbb{C})$, and for each such $E' : y^2 = 4x^3 - ax - b$ there is a unique lattice L such that $g_2(L) = a$ and $g_2(L) = b$; cf. Cox[7], p. 224. In particular, $E_L = E' \simeq E$.

Via this isomorphism we have a natural identification

$$\Psi_L : (L : L)_{\mathbb{C}} = \{\lambda \in \mathbb{C} : \lambda L \subset L\} \xrightarrow{\sim} \mathrm{End}(E_L) \tag{64}$$

given by $\lambda \mapsto \pi_\lambda$, where $\pi_\lambda = \pi_\lambda^L \in \mathrm{End}(E_L)$ is defined by $\pi_\lambda(\rho_L(z+L)) = \rho_L(\lambda z + L)$; cf. [18], §1.4.

From this one sees easily that E_L is a CM elliptic curve if and only if $(L : L)_{\mathbb{C}} \neq \mathbb{Z}$. If this is the case, then $(L : L)_{\mathbb{C}}$ is an order in some (unique) imaginary quadratic field $F \subset \mathbb{C}$ and $L = \lambda L_0$, for some lattice $L_0 \subset F$ and $\lambda \in \mathbb{C}^\times$. Since $E_L \simeq E_{L_0}$, we can and will henceforth assume that $L = L_0 \in \mathrm{Lat}_F$.

If E_L is CM elliptic curve with $L \in \mathrm{Lat}_F$, then its finite subgroup schemes H can be identified with lattices $L_H \supset L$, as we shall now see. Via this identification we can determine $I(H)$ and $H(I)$ as follows.

Proposition 26 *Let $L \in \mathrm{Lat}_F$, where F is an imaginary quadratic field. For every lattice $L' \in \mathrm{Lat}_F$ with $L \subset L'$, the group $H_{L'} = \rho_L(L'/L)$ is a finite subgroup scheme of E_L, and conversely every finite subgroups scheme H of E_L is of the form $H = H_{L_H}$, for a unique lattice $L_H \in \mathrm{Lat}_F$ with $L \subset L_H$. Moreover,*

$$(E_L)_H \simeq E_{L_H}, \quad \mathcal{E}(H) \simeq R(L_H) \quad \textit{and} \quad |H| = [L_H : L]. \tag{65}$$

In addition, if I is a non-zero ideal of $\mathrm{End}(E_L)$*, then we have*

$$I(H) = \Psi_L((L : L_H)), \tag{66}$$

$$H(I) = \rho_L((L : \Psi_L(I))/L). \tag{67}$$

Proof. Since every finite subgroup scheme of E_L is reduced (and etale), we can identify them with the (abstract) finite subgroups of $E_L(\mathbb{C}) \simeq \mathbb{C}/L$. Thus, if $L' \in \mathrm{Lat}_F$ with $L \leq L'$, then $[L' : L] < \infty$ and so L'/L is a finite subgroup of $\mathbb{C}/L$. Clearly, every finite subgroup H of $\mathbb{C}/L$ has the form $H = L_H/L$, for a unique subgroup L_H with $L \leq L_H \leq \mathbb{C}$. Since $L_H \subset \frac{1}{n}L$, where $n = |H|$, it follows that $L_H \in \mathrm{Lat}_F$.

Since the inclusion $L \subset L_H$ defines a surjective analytic homomorphism $\pi : \mathbb{C}/L \to \mathbb{C}/L_H$ with kernel L_H/L, it follows that $(E_L)_H \simeq E_{L_H}$ and $|H| = |L_H/L| = [L_H : L]$. Thus $\mathcal{E}(H) = \Phi_H(\mathrm{End}((E_L)_H)) \simeq \mathrm{End}((E_L)_H) \simeq \mathrm{End}(E_{L_H}) = \Psi_{L_H}(R(L_H)) \simeq R(L_H)$, which proves (65).

Let $0 \neq \lambda \in R(L)$. Since $\mathrm{Ker}(\pi_\lambda) = \rho_L((\frac{1}{\lambda}L)/L)$, we see that $\lambda \in \Psi_L^{-1}(I(H)) \Leftrightarrow \rho_L(L_H/L) \leq \mathrm{Ker}(\pi_\lambda) \Leftrightarrow L_H \leq \frac{1}{\lambda}L \Leftrightarrow L_H\lambda \leq L \Leftrightarrow \lambda \in (L : L_H)$, which proves (66).

To prove (67), put $I' = \Psi_L^{-1}(I)$. Then by definition

$$H(I) = \bigcap_{\lambda \in I'} \mathrm{Ker}(\pi_\lambda) = \bigcap_{0 \neq \lambda \in I'} \rho_L((\lambda^{-1}L)/L) = \rho_L(\tilde{H}(I')/L), \text{ where } \tilde{H}(I') = \bigcap_{0 \neq \lambda \in I'} \lambda^{-1}L.$$

Now $\tilde{H}(I') = (L : I')$ because $x \in (L : I') \Leftrightarrow x\lambda \in L, \forall \lambda \in I', \lambda \neq 0 \Leftrightarrow x \in \cap_{0 \neq \lambda \in I'} \lambda^{-1}L$, and so (67) follows.

Corollary 27 *If $L, L' \in \mathrm{Lat}_F$ are two lattices, then $I_{E_L}(E_{L'}) \simeq L(L')^{-1}$.*

Proof. Since $E_L \simeq E_{nL}$ and $L(L')^{-1} \simeq nL(L')^{-1}$, for any $n \in \mathbb{N}$, we may assume without loss of generality that $L \subset L'$. Put $H = \rho_L(L'/L)$. Since $(E_L)_H \simeq E_{L'}$, we have $I_{E_L}(E_{L'}) \simeq I(H) = \psi_L((L : L')) \simeq (L : L')$ by (66). This proves the assertion because $(L : L') \simeq L(L')^{-1}$ by (41).

We can use the above proposition to give not only a quick proof of Proposition 21 and of its Corollary 23 in the case that $K = \mathbb{C}$ but also an important *refinement* of these results.

Proposition 28 *Let E/K be a CM elliptic curve, where K is an arbitrary field. If $R = \mathrm{End}(E)$, then for any finite subgroup scheme H of E with $\mathrm{char}(K) \nmid |H|$*

$$R(I(H)) = \mathcal{E}(H)R, \tag{68}$$

$$[R : I(H)] = [\mathcal{E}(H)R : \mathcal{E}(H)] \cdot |H|. \tag{69}$$

Proof. By base-change (cf. Remark 7(e)), it is enough to consider the case that $K = \overline{K}$ is algebraically closed. Moreover, since $E \simeq E_0 \otimes K$ for some $E_0/\overline{P}$, where $P \subset K$ is the prime subfield (and since all finite subgroups schemes are defined of $\overline{P}$), we can assume that either $K = \overline{\mathbb{Q}}$ or $K = \overline{\mathbb{F}}_p$.

Case 1: $K = \overline{\mathbb{Q}}$.

By base-change again, we can assume here that $K = \mathbb{C}$. Then $E \simeq E_L$, for some lattice $L \in \mathrm{Lat}_F$ and some imaginary quadratic field F, and $H = \rho_L(L_H/L)$, for some $L_H \in \mathrm{Lat}_F$ with $L \subset L_H$.

Put $L_1 = L$ and $L_2 = L_H$, and $R_i = R(L_i)$ and $R' = R_1R_2$. Then $R_1 = \Psi_L^{-1}(R) \simeq R$ and $R_2 \simeq \mathcal{E}(H)$ by (65). Thus $[\mathcal{E}(H)R : \mathcal{E}(H)] = [R' : R_2] = \frac{f_2}{f}$, where $f_i = f_{R_i}$ and $f = f_{R'} = (f_1, f_2)$. Now by (66) and (41) we have $\Psi_L^{-1}(I(H)) = (L_1 : L_2) = \frac{f_1}{f}L_1L_2^{-1}$.

From this we see on the one hand that $R((L_1 : L_2)) = R(L_1)R(L_2^{-1}) = R'$ by (39), which proves (68). On the other hand we obtain

$$\frac{f_1}{f}[R : I(H)] = [R' : (L_1 : L_2)] = N(\tfrac{f_1}{f}L_1L_2^{-1}) = \frac{f_1^2}{f^2}N(L_1)N(L_2)^{-1}.$$

But since $L_1 \subset L_2$ we have $N(L_1)N(L_2)^{-1} = \frac{f_2}{f_1}[L_2 : L_1]$ because if we choose $n \in \mathbb{N}$ such that $nL_2 \subset \mathfrak{O}_F$, then $\frac{f_1}{f_2}N(L_1)N(L_2)^{-1} = \frac{f_1}{f_2}N(nL_1)N(nL_2)^{-1} = [\mathfrak{O}_F : nL_1][\mathfrak{O}_F : nL_2]^{-1} = [nL_2 : nL_1] = [L_2 : L_1]$. Thus $\frac{f_1}{f}[R : I(H)] = \frac{f_1f_2}{f^2}[L_2 : L_1]$, and so (69) follows because $|H| = [L_2 : L_1]$ by (65).

Case 2: $K = \overline{\mathbb{F}}_p$

By the Deuring Lifting Theorem ([18], p. 184) there is a number field $K'/\mathbb{Q}$ and a CM elliptic curve E'/K' and a prime $\mathfrak{p}|p$ of K' such that E' has good reduction E'_k at $\mathfrak{p}$ and $E'_k \otimes \overline{\mathbb{F}}_p \simeq E$ and such that the reduction map induces an isomorphism $r_k : \mathrm{End}(E') \xrightarrow{\sim} \mathrm{End}(E'_k) \simeq \mathrm{End}(E)$, where $k = \mathfrak{O}_{K'}/\mathfrak{p}$ is the residue field. Note that we have that $p \nmid f_{E'}$; cf. Proposition 25(a).

By enlarging the ground field K' if necessary, we may assume without of loss of generality that the n-torsion points of E are K'-rational, where $n = |H|$. Then the n-torsion points of E'_k are k-rational, and so we can identify H with a subgroup of $E'_k(k)$ of order n, which therefore lifts uniquely to a subgroup H' of $E'(K')$ which we view as a subgroup scheme of E' of rank n. Thus $(H')_k = H$ in the notation of Proposition 25(b), and so by Proposition 25 we have

$$I(H) = r_k(I(H')) \quad \text{and} \quad r_k^0(\mathcal{E}(H')) \;=\; \mathcal{E}(H).$$

Since (68) is true for H' by Case 1, it follows from the above that

$$R(I(H)) = r_k^0(R(I(H'))) = r_k^0(\mathcal{E}(H')R') = \mathcal{E}(H)R,$$

where $R' := \mathrm{End}(E')$ and $R := r_k(R') = \mathrm{End}(E'_k)$. Thus (68) holds for H.

Similarly, from the above we obtain that $[R' : I(H')] = [R : I(H)]$ and also that $[\mathcal{E}(H')R' : \mathcal{E}(H')] = [\mathcal{E}(H)R : \mathcal{E}(H)]$. Thus, since (69) is true for H' by Case 1, it follows that (69) also holds for H because

$$[R : I(H)] = [R' : I(H')] = [\mathcal{E}(H')R' : \mathcal{E}(H')]|H'| = [\mathcal{E}(H)R : \mathcal{E}(H)]|H|.$$

The above formulae (68) and (69) allow us to prove the following useful fact.

Proposition 29 *In the situation of* Proposition 28*, let H_1 and H_2 be two finite subgroups of E with $(|H_1|, |H_2|) = 1$ and $\mathcal{E}(H_i) \subset R$, for $i = 1, 2$. If $\mathrm{char}(K)) \nmid |H_i|$, for $i = 1, 2$, then*

$$\mathcal{E}(H_1 + H_2) \;=\; \mathcal{E}(H_1) \cap \mathcal{E}(H_2).$$

Proof. First note that for any two finite subgroups H_1, H_2 of E we have

$$I(H_1)I(H_2) \ \subset \ I(H_1+H_2) \ \subset \ I(H_1) \cap I(H_2). \tag{70}$$

Indeed, since $H_i \leq H_1+H_2$, we have $I(H_1+H_2) \subset I(H_i)$ by (6) and so the second inclusion of (70) follows. To prove the first inclusion, let $f_i \in I(H_i)$, so $H_i \leq \mathrm{Ker}(f_i)$. Since $f_1 f_2 = f_2 f_1$, we have $H_i \leq \mathrm{Ker}(f_i) \leq \mathrm{Ker}(f_1 f_2)$ and so $H_1 + H_2 \leq \mathrm{Ker}(f_1 f_2)$. Thus $f_1 f_2 \in I(H_1+H_2)$, and so the first inclusion of (70) holds.

Put $n_i = |H_i|$, $e_i = [R : \mathcal{E}(H_i)]$ and $N_i = [R : I(H_i)]$, so $N_i = e_i n_i$ by (69) (together with the hypothesis that $\mathcal{E}(H_i) \subset R$). Since $H_i \leq \mathrm{Ker}([n_i])$, we have $n_i \in I(H_i)$, and so $Rn_i \subset I(H_i)$, which implies that $N_i = [R : I(H_i)]|[R : Rn_i] = n_i^2$. Thus, since $(n_1, n_2) = 1$, we see that also $(N_1, N_2) = 1$ and hence that $(e_1, e_2) = 1$.

In addition we have that $I(H_1) + I(H_2) = R$ because $n_i \in I(H_i)$ and $(n_1, n_2) = 1$. Thus, by elementary ideal theory we have that $I(H_1)I(H_2) = I(H_1) \cap I(H_2)$, and so equality holds throughout in (70). Using (68) and (39), we obtain for $H = H_1 + H_2$ that

$$\mathcal{E}(H)R = R(I(H)) = R(I(H_1)I(H_2)) = R(I(H_1))R(I(H_2)) = R \cdot R = R,$$

because $R(I(H_i)) = R\mathcal{E}(H_i) = R$ by (68) and the hypothesis. Thus $\mathcal{E}(H_1+H_2) \subset R$.

Next we note that $H_1 \cap H_2 = 0$ (because $|H_1 \cap H_2| \mid (n_1, n_2) = 1$), and so $|H_1 + H_2| = n_1 n_2$. Moreover, since $I(H_1+H_2) = I(H_1) \cap I(H_2)$, we see that $[R : I(H_1+H_2)] = [R : I(H_1) + I(H_2)] = N_1 N_2$, the latter because $I(H_1) + I(H_2) = R$. Thus, by (69) (applied to $H = H_1 + H_2$) we obtain $n_1 e_1 n_2 e_2 = N_1 N_2 = [R\mathcal{E}(H) : \mathcal{E}(H)] n_1 n_2$, and so $[R : \mathcal{E}(H)] = e_1 e_2$. Thus, if $f = f_R$, then $\mathcal{E}(H)$ has conductor $f e_1 e_2 = \mathrm{lcm}(f e_1, f e_2)$ because $(e_1, e_2) = 1$. Since $f_{\mathcal{E}(H_i)} = f e_i$, it thus follows from (37) that $\mathcal{E}(H) = \mathcal{E}(H_1) \cap \mathcal{E}(H_2)$, as claimed.

Coming back to the case that $E = E_L$, we now generalize the above formula (66) for $I(H)$ by giving a similar interpretation of the lattice $\mathcal{H}(H_1, H_2)$.

For this, we first observe that the identification map Ψ_L of (64) can be generalized as follows. If $L_1, L_2 \in \mathbb{C}$ are any two lattices, then by [18], §1.4, we have a bijection

$$\Psi_{L_1,L_2} : (L_2 : L_1)_{\mathbb{C}} \quad \tilde{\to} \quad \mathrm{Hom}(E_{L_1}, E_{L_2}) \tag{71}$$

which is given by the rule $\lambda \mapsto \pi_\lambda = \pi_\lambda^{L_1,L_2} \in \mathrm{Hom}(E_{L_1}, E_{L_2})$, where π_λ is defined by

$$\pi_\lambda(\rho_{L_1}(z + L_1)) \ = \ \rho_{L_2}(\lambda z + L_2), \quad \text{for } \lambda \in (L_2 : L_1)_{\mathbb{C}} = \{\lambda \in \mathbb{C} : \lambda L_1 \subset L_2\}.$$

Note that these maps Ψ are multiplicative in the sense that if L_3 is a third lattice, then we have

$$\pi_{\lambda_2\lambda_1}^{L_1,L_3} \ = \ \pi_{\lambda_2}^{L_2,L_3} \circ \pi_{\lambda_1}^{L_1,L_2}, \quad \text{if } \lambda_1 \in (L_2 : L_1)_{\mathbb{C}} \text{ and } \lambda_2 \in (L_3 : L_2)_{\mathbb{C}}. \tag{72}$$

We now prove the following generalization of (66).

Proposition 30 *Let $L \in \mathrm{Lat}_F$, where F is an imaginary quadratic field, and let $H_i = \rho_L(L_{H_i}/L)$ be two finite subgroups of E_L. Then we have*

$$\mathcal{H}(H_1, H_2) \;=\; \Psi_L^0((L_{H_2} : L_{H_1})), \tag{73}$$

where $\Psi_L^0 : F \xrightarrow{\sim} \mathrm{End}^0(E_L)$ is the canonical extension of Ψ_L to F.

Proof. First note that if $H = \rho_L(L_H/L)$, then we have

$$\pi_H = \pi_1^{L,L_H} \quad \text{and} \quad \pi'_H = \pi_{n_H}^{L_H,L}, \quad \text{where } n_H = |H|. \tag{74}$$

Indeed, since $\pi_1^{L,L_H} : E_L \to E_{L_H}$ is surjective and has kernel $H = \rho_L(L_H/L)$, we see that $(E_{L_H}, \pi_1^{L,L_H}) \simeq ((E_L)_H, \pi_H)$ is a quotient of E_L by H. Thus, the first equality of (74) holds. Moreover, since $n_H = [L_H : L]$ by (65), we have $n_H L_H \subset L$ and so $n_H \in (L : L_H)$. Thus, $\pi_{n_H}^{L_H,L}$ exists, and by (72) we have $\pi_{n_H}^{L_H,L} \circ \pi_H = \pi_{n_H}^{L,L} = [n_H]_{E_L}$, and so $\pi'_H = \pi_{n_H}^{L_H,L}$; cf. (4).

We next observe that

$$\Phi_{H_1,H_2}(\Psi_{L_{H_1},L_{H_2}}(\lambda)) \;= \Psi_L^0(\lambda), \quad \text{for all } \lambda \in (L_{H_2} : L_{H_1})_{\mathbb{C}}. \tag{75}$$

Indeed, from the definitions and (74) and (72) we obtain

$$\Phi_{H_1,H_2}(\Psi_{L_{H_1},L_{H_2}}(\lambda)) = \frac{1}{n_H}\pi'_H \pi_\lambda^{L_{H_1},L_{H_2}} \pi_H = \frac{1}{n_H}\pi_{n_H\lambda}^{L,L} = \frac{1}{n_H}\Psi_L(n_H\lambda) = \Psi_L^0(\lambda),$$

which proves (75). From this, equation (73) follows immediately because $\Phi_{H_1,H_2} \circ \Psi_{L_{H_1},L_{H_2}}$ is an isomorphism from $(L_{H_2} : L_{H_2})$ to $\mathcal{H}(H_1, H_2)$; cf. (71) and Remark 9(a).

Remark 31 (a) It follows from (73), (41) and (65) that

$$(\psi_L^0)^{-1}(\mathcal{H}(0, H)) \;=\; (L_H : L) \;=\; [R\mathcal{E}(H) : \mathcal{E}(H)]L_H L^{-1},$$

where $R = \mathrm{End}(E_L) \simeq R(L)$. Thus, we can partially recover the lattice L_H (which defines the analytic curve $\mathbb{C}/L_H \simeq (E_L)_H$) from the "algebraic lattice" $\mathcal{H}(0, H)$.

(b) If E/K is any CM curve over $K \subset \mathbb{C}$, then it follows from (73) that for any two finite subgroup schemes H_1, H_2 of E we have that

$$(I(H_1) : I(H_2)) \;=\; \frac{[RR_1R_2 : RR_2]}{[R_1R_2 : R_2]} R\mathcal{H}(H_1, H_2), \tag{76}$$

where $R = \mathrm{End}(E)$ and $R_i = \mathcal{E}(H_i)$. Indeed, as in the proof of Corollary we can assume that $K = \mathbb{C}$, $E = E_L$ and $H_i = \rho_L(L_i/L)$. Then in view of (73), (67) and (65), the formula (76) follows from the following formula (which is easily deduced from (41)):

$$((L : L_2) : (L : L_1)) \;=\; [RR_1R_2 : RR_2]RL_1L_2^{-1} \;=\; \frac{[RR_1R_2 : RR_2]}{[R_1R_2 : R_2]}(L_1 : L_2)R, \tag{77}$$

in which $R = R(L)$ and $R_i = R(L_i)$.

3.3 Endomorphism rings

In the sequel it is sometimes useful to know which orders of an imaginary quadratic field F can be endomorphism rings of CM elliptic curves E/K or, more precisely, to describe the set of conductors $f_{E'}$ for $E' \in \mathrm{Isog}(E/K)$. Note that the answer for the corresponding question for the subset $\mathrm{Isog}^+(E/K)$ follows from Corollary 19: an order R of $F = \mathrm{End}^0(E)$ is the endomorphism ring of some $E' \in \mathrm{Isog}^+(E/K)$ if and only if we have $f_R | f_E$. However, the characterization of the set of conductors in $\mathrm{Isog}(E/K)$ is more delicate and depends on the nature of the ground field K.

We begin with the case that K is algebraically closed. Here the set of CM curves in $\mathrm{Isog}(E/K)$ can be characterized as follows.

Proposition 32 *Let K be an algebraically closed field, and let E_1/K and E_2/K be two CM curves. Then $E_1 \sim E_2$ if and only if $\mathrm{End}^0(E_1) \simeq \mathrm{End}^0(E_2)$.*

Proof. Clearly, if $E_1 \sim E_2$, then $\mathrm{End}^0(E_1) \simeq \mathrm{End}^0(E_2)$. To prove the converse, suppose first that $K = \mathbb{C}$. If $\mathrm{End}^0(E_1) \simeq \mathrm{End}^0(E_2) =: F$, then by the discussion of the previous section we know that $E_i \simeq E_{L_i}$, for some $L_i \in \mathrm{Lat}_F$, and then $\mathrm{Hom}(E_1, E_2) \simeq (L_2 : L_1) \neq 0$. Thus $E_1 \sim E_2$.

From this, the assertion follows for an arbitrary field K of characteristic 0. Indeed, any two CM curves over K are defined over $\overline{\mathbb{Q}}$ (cf. [18], p. 40), i.e. $E_i = E_i^0 \otimes K$ for some $E_i^0/\overline{\mathbb{Q}}$. Since $F = \mathrm{End}(E_i) = \mathrm{End}(E_i^0) = \mathrm{End}(E_i^0 \otimes \mathbb{C})$, and $\mathrm{Hom}(E_1^0, E_2^0) = \mathrm{Hom}(E_1^0 \otimes \mathbb{C}, E_2^0 \otimes \mathbb{C})$, we conclude from what was just proved that $E_1^0 \sim E_2^0$ and hence also $E_1 \sim E_2$.

Now suppose that $\mathrm{char}(K) = p \neq 0$. Then $E_i = E_i^0 \otimes K$, for some CM curves $E_i^0/\mathbb{F}_p^r$ (and some $r \geq 1$); cf. [18], p. 184. By the Deuring Lifting Theorem ([18], p. 184), there exists a number field L and CM elliptic curves $\tilde{E}_i/L$ whose reduction is E_i^0 and such that $\mathrm{End}^0(\tilde{E}_i) = \mathrm{End}^0(E_i^0)$. By the characteristic 0 result, there is a finite extension L'/L such that $\tilde{E}_1 \otimes L' \sim \tilde{E}_2 \otimes L'$, and hence $E_1^0 \otimes \overline{\mathbb{F}}_p \sim E_2^0 \otimes \overline{\mathbb{F}}_p$, and hence also $E_1 \sim E_2$.

In view of the previous result, the following result classifies the possible conductors of elliptic curves in $\mathrm{Isom}(E/K)$ (when K is algebraically closed).

Proposition 33 *Let K be an algebraically closed field and let $\Delta < 0$ be a discriminant.*

(a) *If $\mathrm{char}(K) = 0$, then there exists a CM elliptic curve E/K with $\Delta_E = \Delta$.*

(b) *If $\mathrm{char}(K) = p \neq 0$, then there exists a CM elliptic curve E/K with $\Delta_E = \Delta$ if and only if $(\frac{\Delta}{p}) = 1$.*

Proof. (a) This follows easily from the complex theory (together with the reduction steps as in the proof of Proposition 32); cf. Deuring[10], p. 263.

(b) Deuring[10], p. 263. Note that the condition $(\frac{\Delta}{p}) = 1$ is equivalent to the following two conditions: (i) p splits in $F = \mathbb{Q}(\sqrt{\Delta})$ and (ii) $p \nmid f_{R_\Delta}$.

If K is a finite field, then the results of Waterhouse[26] furnish a solution to the above question.

Proposition 34 *Let $K = \mathbb{F}_q$ be a finite field and let $E/\mathbb{F}_q$ be a CM elliptic curve. Let*

$$h_{E/K}(X) \;=\; X^2 - a_{E/F}X + q$$

be the characteristic polynomial of the Frobenius endomorphism of E/K, and put $\Delta(h_{E/K}) = a_{E/K}^2 - 4q$. If $\Delta \in \mathbb{Z}$, then there is an elliptic curve $E' \simeq E$ with $\Delta_{E'} = \Delta$ if and only if $\Delta(h_{E/K})/\Delta = n^2$, for some $n \in \mathbb{N}$.

Proof. Let $\phi_{E/K} \in R := \mathrm{End}(E)$ denote the Frobenius endomorphism of E/K, and let $R' \subset \tilde{R} = \mathrm{End}^0(E)$ be an order. Then by [26], Theorem 4.2, there is an elliptic curve E'/K with $E' \sim E$ and $\mathrm{End}(E') \simeq R'$ if and only if $\phi_{E/K} \in R'$. Since $\mathbb{Z}[\phi_{E/K}]$ is a order of discriminant $\Delta(h_{E/K})$, we see that the latter condition is equivalent to $\Delta(h_{E/K}) = \Delta n^2$ (with $n = [R' : \mathbb{Z}[\phi_{E/K}]$).

For fields of characteristic 0, we have the following partial analogue of Proposition 34. Here we shall use the modular function j which is defined on the upper half plane $\mathfrak{H}$ and which can be viewed as a function on the set of lattices of $\mathbb{C}$ by the rule $j(L) = j(\omega_1/\omega_2)$, if $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 \subset \mathbb{C}$ with $\mathrm{Im}(\omega_1/\omega_2) > 0$.

Proposition 35 *Let $K \subset \mathbb{C}$, and let R be a quadratic lattice of discriminant $\Delta = \Delta(R) < 0$. Then there is a CM elliptic curve E/K with $\mathrm{End}(E) \simeq R$ if and only if $\mathbb{Q}(\sqrt{\Delta}, j(R)) \subset K$.*

Proof. Suppose first that E/K is a CM elliptic curve with $\mathrm{End}(E) \simeq R$. Put $F = \mathrm{End}^0(E) = \mathbb{Q}(\sqrt{\Delta})$. Then by §3.2 there is a lattice $L \in \mathrm{Lat}_F$ such that $E \otimes \mathbb{C} \simeq E_L$, and $R(L) \simeq R$. Then $j(L) = j_E \in K$. Moreover, by [18], DIFF 3 (p. 119), we know that $F \subset K$ (because $\mathrm{End}(E) = \mathrm{End}(E_L)$), and so $F(j(L)) \subset K$. But $F(j(L)) = F(j(R))$ by the First Main Theorem of complex multiplication (cf. [7], Theorem 11.1), and so $\mathbb{Q}(\sqrt{\Delta}, j(R)) = F(j(L)) \subset K$.

Conversely, suppose that $\mathbb{Q}(\sqrt{\Delta}, j(R)) \subset K$. Since R is a lattice in $F := \mathbb{Q}(\sqrt{\Delta})$ and since $j(R) \in K$, there is an elliptic curve E/K such that $E \otimes \mathbb{C} = E_R$. Since $\mathrm{End}(E_R) \simeq R \subset F$ and $F \subset K$, it follows from [18], DIFF 3, again that $\mathrm{End}(E) = \mathrm{End}(E_R) \simeq R$. Thus, E/K is a CM curve with $\mathrm{End}(E) \simeq R$.

The following result shows that the set of conductors appearing in $\mathrm{Isog}(E/K)$ forms a sublattice of $\mathbb{N}$ with respect to the partial order $f_E | f_{E'}$.

Proposition 36 *Let E/K be a CM elliptic curve. If $E_1, \ldots, E_n \in \mathrm{Isog}(E/K)$, then there is an elliptic curve $E' \sim E$ such that $f_{E'} = \mathrm{lcm}(f_{E_1}, \ldots, f_{E_n})$.*

Proof. By induction, it is clearly enough to verify the case $n = 2$.

Since $E_i \sim E$, we can view $R_i := \mathrm{End}(E_i)$ as a subring of $F = \mathrm{End}^0(E)$ which is uniquely determined by the condition that $[\mathfrak{O}_F : R_i] = f_{E_i}$. Put $R' = R_1 R_2$ and $f_i = [R' : R_i]$. Since R' has conductor $f = (f_{E_1}, f_{E_2})$ by (37), we see that $(f_1, f_2) = 1$. Note that $\mathrm{char}(K) \nmid f_i = 1$ by Proposition 33(b).

Next, consider the R_i-ideal $I_i = f_i R'$ and put $\pi_i = \pi_{H(I_i)} : E_i \to E_i' = (E_i)_{H(I_i)}$. Since by (45) we have $\mathcal{E}(H(I_i)) \simeq R(I_i) = R(f_i R') = R'$, it follows from Remark 20 that there is an invertible R'-ideal I such that $(E_1')_{H(I)} \simeq E_2'$. Furthermore, by replacing I by cI if necessary (where $c \in F^\times$), we can assume that $(N(I), f_1) = 1$ and that $\mathrm{char}(K) \nmid N(I)$.

Put $H_1 = \mathrm{Ker}(\pi_1')$ and $H_2 = \mathrm{Ker}(\pi_2 \circ \pi_{H(I)})$. Clearly $(E_1')_{H_i} \simeq E_i$, and so $\mathcal{E}(H_i) \simeq R_i \subset R' \simeq \mathrm{End}(E_1')$. Furthermore, $|H_1| = \deg(\pi_1') = \deg(\pi_1) = f_1$, and $|H_2| = \deg(\pi_2') \deg(\pi_{H(I)}) = f_2 N(I)$, so $(|H_1|, |H_2|) = 1$. In addition, we have that $\mathrm{char}(K) \nmid |H_i|$. Thus, by Proposition 29 we have $\mathcal{E}(H_1 + H_2) = \mathcal{E}(H_1) \cap \mathcal{E}(H_2) = R_1 \cap R_2$, which has conductor $\mathrm{lcm}(f_{E_1}, f_{E_2})$ by (37). Thus $(E_1')_{H_1+H_2}$ has conductor $\mathrm{lcm}(f_{E_1}, f_{E_2})$, and so the assertion follows because $E \sim E_1' \sim (E_1')_{H_1+H_2}$.

3.4 The quadratic form q_{E_1,E_2}

Let E_1/K and E_2/K be any two isogenous elliptic curves, and put

$$q_{E_1,E_2}(f) \;=\; \deg(f), \quad \text{for } f \in \mathrm{Hom}(E_1, E_2).$$

Since $\mathrm{Hom}(E_1, E_2) \simeq \mathbb{Z}^r$, where $r = \mathrm{rank}(\mathrm{Hom}(E_1, E_2)) = \dim_{\mathbb{Q}}(\mathrm{End}^0(E_i))$, we see that by fixing a basis of $\mathrm{Hom}(E_1, E_2)$, we obtain an explicit positive definite quadratic form in r variables. Thus, by varying over all bases of $\mathrm{Hom}(E_1, E_2)$, we obtain a $\mathrm{GL}_r(\mathbb{Z})$-equivalence class of quadratic forms in r variables.

In the case that E_i is a CM elliptic curve, we have $r = [F : \mathbb{Q}] = 2$, so q_{E_1,E_2} defines an equivalence class of positive binary quadratic forms, i.e. $q_{E_1,E_2} \sim ax^2 + bxy + cy =: q$, for some $a, b, c \in \mathbb{Z}$ with $\Delta(q) = b^2 - 4ac < 0$. Note that the *discriminant* $\Delta(q)$ and the *content* $\mathrm{cont}(q) = \gcd(a, b, c)$ are invariants of the $\mathrm{GL}_2(\mathbb{Z})$-equivalence class of q.

In order to determine q_{E_1,E_2}, we introduce the following notation. Given a lattice $L \in \mathrm{Lat}_F$, where F is an imaginary quadratic field, put

$$q_L(\lambda) \;=\; \frac{N(\lambda)}{N(L)}, \quad \text{for } \lambda \in L,$$

where, as before, $N(\lambda) = N_{F/\mathbb{Q}}(\lambda)$ denotes the field norm. Note that $q_L(\lambda) \in \mathbb{Z}$; cf. [3], §II.7. Thus, by choosing a basis $\{\alpha, \beta\}$ of $L = \mathbb{Z}\alpha + \mathbb{Z}\beta$, the map q_L defines an

integral quadratic form

$$q_{L,\alpha,\beta}(x,y) = q_L(x\alpha + y\beta), \quad \text{for } x, y \in \mathbb{Z},$$

and hence q_L defines an equivalence class of positive binary quadratic forms. Moreover, we have by [3], §II.7 that

$$\Delta(q_L) \;=\; \Delta(R(L)) \quad \text{and} \quad \mathrm{cont}(q_L) = 1. \tag{78}$$

We now prove:

Proposition 37 *Let E/K be a CM elliptic curve and $E_1, E_2 \in \mathrm{Isog}^+(E)$. If $f_i = f_{E_i}$, then*

$$q_{E_1,E_2} \;\sim\; cq_L, \quad \textit{where } L = I_E(E_1)I_E(E_2)^{-1} \quad \textit{and} \quad c = \frac{\mathrm{lcm}(f_1,f_2)}{\gcd(f_1,f_2)}. \tag{79}$$

In particular, $c = \mathrm{cont}(q_{E_1,E_2})$ and

$$\Delta(q_{E_1,E_2}) \;=\; -\mathrm{lcm}(|\Delta_{E_1}|, |\Delta_{E_2}|) \;=\; \mathrm{lcm}(f_1,f_2)^2\Delta_F, \;\; \textit{where } F = \mathrm{End}^0(E). \tag{80}$$

Proof. Let $\pi_i : E \to E_i$ be an isogeny and put $H_i = \mathrm{Ker}(\pi_i)$ and $n_i = \deg(\pi_i)$. Moreover, put $\Phi = \Phi_{H_1,H_2}$ and $\mathcal{H} = \mathcal{H}(H_1,H_2)$. We first show that

$$q_{E_1,E_2}(h) = cq_{\mathcal{H}}(\Phi(h)), \quad \text{for all } h \in \mathrm{Hom}(E_1,E_2); \tag{81}$$

here we used the identification $E_i = E_{H_i}$.

Since the H_i's are ideal subgroups by (46), we have by (57) that $N(L) = c\frac{n_1}{n_2}$. Moreover, since we have by (54) that $\deg(f) = N(f)$, for all $f \in R = \mathrm{End}(E)$, we see from the definition of Φ that $N(\Phi(h)) = N(\frac{1}{n_2}\pi_2 h \pi_1) = \frac{1}{n_2^2}\deg(\pi_2 h \pi_1) = \frac{1}{n_2^2}\deg(\pi_2)\deg(h)\deg(\pi_1) = \frac{n_1}{n_2}\deg(h)$, and so

$$q_{E_1,E_2}(h) = \deg(h) = \frac{n_2}{n_1}N(\Phi(h)) = c\frac{N(\Phi(h))}{N(\mathcal{H})}, \quad \text{for } h \in \mathrm{Hom}(E_1,E_2).$$

This proves (81) and hence also (79) because by (47) and (41) we have that $\mathcal{H} = (I(H_1) : I(H_2)) = \frac{f_1}{f}I(H_1)I(H_2)^{-1} = \frac{f_1}{f}L$, and so $q_{\mathcal{H}} \sim q_L$.

Since q_L is primitive by (78), we have from (79) that $\mathrm{cont}(q_{E_1,E_2}) = c \cdot \mathrm{cont}(q_L) = c$. Moreover, by (78) we have that $\Delta(q_L) = \Delta(R(L))$. Now since $R(I(H_i)) = \mathcal{E}(H_i) \simeq \mathrm{End}(E_i)$ has conductor f_i, it follows from (39) and (37) that $R(L) = R(I(H_1))R(I(H_2))$ has conductor $f = (f_1,f_2)$, and so $\Delta(q_L) = f^2\Delta_F$. Thus we see that $\Delta(q_{E_1,E_2}) = c^2\Delta(q_L) = (cf)^2\Delta(f) = \mathrm{lcm}(f_1,f_2)^2\Delta_F$, and so (80) follows.

Remark 38 If $L \in \mathrm{Lat}_F$ is any lattice, then we had seen above that q_L naturally defines a $\mathrm{GL}_2(\mathbb{Z})$-equivalence class of positive binary quadratic forms. As is well-known, one can also associate to L an $\mathrm{SL}_2(\mathbb{Z})$-equivalence class of forms by restricting the set $\{q_{L,\alpha,\beta}\}$ to those forms that arise from *oriented* bases $\{\alpha, \beta\}$ of L, i.e. those for which $\mathrm{Im}(\beta/\alpha) > 0$ (where we view $F \subset \mathbb{C}$). Thus, if we write $cq_L^+ = \{cq_{L,\alpha,\beta} : L = \mathbb{Z}\alpha + \mathbb{Z}\beta, \mathrm{Im}(\beta/\alpha) > 0\}$, for $c \in \mathbb{N}$ and $L \in \mathrm{Lat}_F$, then it is well-known that the rule $I \mapsto \tilde{q}_I^+ := [R(I) : R_\Delta]q_I^+$ induces a bijection

$$q_\Delta : \ Id(R_\Delta)/\simeq \ \ \tilde{\to} \ \ Q_\Delta/\mathrm{SL}_2(\mathbb{Z})$$

between the set of isomorphism classes of non-zero ideals of the order R_Δ of discriminant $\Delta < 0$ and the set of proper equivalence classes of positive binary quadratic forms of discriminant Δ.

Now if we combine this bijection with the bijection I_E^+ defined in Corollary 19, then we obtain a bijection

$$q_E^+ : \ \mathrm{Isog}^+(E/K) \ \tilde{\to} \ Id(\mathrm{End}(E))/\simeq \ \tilde{\to} \ Q_{\Delta_E}/\mathrm{SL}_2(\mathbb{Z})$$

which is given by the formula

$$(82) \quad q_{E,E'}^+ \ := \ q_E^+(E') \ = \ q_{\Delta_E}(I_E(E')) \ = \ [R(I_E(E')) : R_E]q^+_{I_E(E')} \ = \ \frac{f_E}{f_{E'}}q^+_{I_E(E')},$$

where the last equality follows from the second equation of (50).

On the other hand, if $f_{E'}|f_E$, then equation (79) tells us that

$$q_{E,E'} \ \sim \ q_{E',E} \ \sim \ \frac{f_E}{f_{E'}}q_{I_E(E')} \quad \text{and} \quad \Delta(q_{E',E}) = \Delta_E.$$

Comparing this with (82), we therefore obtain the important relation that

$$(83) \qquad q_{E,E'} \ \sim \ q^+_{E,E'}, \quad \text{for } E' \in \mathrm{Isog}^+(E/K),$$

where, as before, the symbol $\sim$ (for quadratic forms) means $\mathrm{GL}_2(\mathbb{Z})$-equivalence. Note, however, that $q^+_{E,E'}$ denotes a proper (or $\mathrm{SL}_2(\mathbb{Z})$)-equivalence class of quadratic forms and hence is a finer invariant than the $\mathrm{GL}_2(\mathbb{Z})$-equivalence class $q_{E,E'}$. In fact, it follows from the above that if $E', E'' \in \mathrm{Isog}^+(E/K)$, then we have that

$$q_{E,E'} \ \sim \ q_{E,E''} \quad \Leftrightarrow \quad I_E(E'') \simeq I_E(E') \ \text{ or } \ I_E(E'') \simeq I_E(E')^{-1},$$

and so there are two non-isomorphic elliptic curves in $\mathrm{Isog}^+(E/K)$ which have the same form q, except when q is *ambiguous*, i.e. when $I_E(E') \simeq I_E(E')^{-1}$.

Corollary 39 *Let E_1/K and E_2/K be two isogenous a CM elliptic curves with* $\mathrm{End}^0(E_i) \simeq F$. *If $f_i = f_{E_i}$, then*

$$\Delta(q_{E_1,E_2}) \;=\; \mathrm{lcm}(f_1,f_2)^2\Delta_F \quad \textit{and} \quad \mathrm{cont}(q_{E_1,E_2}) = \frac{\mathrm{lcm}(f_1,f_2)}{\gcd(f_1,f_2)}. \tag{84}$$

Proof. By Proposition 36 there is a CM elliptic curve E such that $E \sim E_i$ and $f_{E_i}|f_E$, for $i = 1, 2$. Thus $E_i \in \mathrm{Isog}^+(E)$, for $i = 1, 2$, and so the assertion follows from Proposition 37.

4 Product abelian varieties

4.1 Kernel ideals and ideal subgroups of A^n

Let $A = A_1 \times A_2 \times \ldots \times A_n$ be the product of the abelian varieties $A_1, \ldots, A_n/K$, and let $p_i^A : A \to A_i$ denote the ith projection and $e_j^A : A_j \to A$ be the jth inclusion map. If $A' = A'_1 \times A'_2 \times \ldots \times A'_m$ is another product abelian variety, then (as is well-known) the group $\mathrm{Hom}(A, A')$ can be identified with a set of $m \times n$ "matrices". More precisely, we have the isomorphism

$$T_{A,A'} : \mathrm{Hom}(A,A') \quad \xrightarrow{\sim} \quad M(A,A') \;:=\; \bigoplus_{i=1}^{m}\bigoplus_{j=1}^{n} \mathrm{Hom}(A_j, A'_i)$$

given by the rule $T_{A,A'}(h) = (h_{ij})$, where $h_{ij} = p_i^{A'} \circ h \circ e_j^A \in \mathrm{Hom}(A_j, A'_i)$. We shall refer to the elements of $M(A, A')$ as "matrices". Note that this identification is multiplicative in the sense that if $A'' = A''_1 \times \ldots \times A''_t$ is another abelian product, then we have the rule

$$T_{A,A''}(h' \circ h) = T_{A',A''}(h') \cdot T_{A,A'}(h), \quad \text{if } h \in \mathrm{Hom}(A,A'),\ h' \in \mathrm{Hom}(A',A''), \tag{85}$$

where the product on the right hand side is the product of "matrices" which is defined by the rule $(h'_{ik})(h_{kj}) = (h''_{ij})$, where $h''_{ij} = \sum_k h'_{ik} \circ h_{kj}$. This follows easily from the identity $\sum_{k=1}^n e_k^{A'} p_k^{A'} = 1_{A'}$. In particular, if $A = A_1^n$, then $T_{A,A}$ defines a ring isomorphism

$$T_{A_1,n} \;=\; T_{A,A} :\; \mathrm{End}(A_1^n) \quad \xrightarrow{\sim} \quad M(A_1^n, A_1^n) \;=\; M_n(\mathrm{End}(A_1))$$

between $\mathrm{End}(A_1^n)$ and the ring of $n \times n$ matrices with coefficients in the ring $\mathrm{End}(A_1)$.

In order to study abelian varieties which are isogenous to $A = A_1^n$, we shall use the theory of kernel ideals and ideal subgroups of section 2. For this, we need to understand the ideals of $M_n(R)$, where $R = \mathrm{End}(A_1)$. To construct such ideals, we shall use the following notation.

Notation. Let R be a ring. If $\alpha = (\alpha_{ij}) \in M_n(R)$ is an $n \times n$ matrix, then we let $\alpha_i = (\alpha_{i1}, \ldots, \alpha_{in}) \in R^n$ denote the ith row of α. Moreover, if M is subset of R^n, then we put

$$\mathcal{I}_n(M) \;=\; \mathcal{I}_{R,n}(M) \;=\; \{\alpha \in M_n(R) : \alpha_i \in M, \text{ for } 1 \leq i \leq n\}.$$

Proposition 40 *The rule $M \mapsto \mathcal{I}_n(M)$ induces an inclusion preserving bijection between the set of left R-submodules of R^n and the set of left ideals of $M_n(R)$. Furthermore, if M_1 and M_2 are two R-submodules of R^n, then*

$$M_1 \;\simeq\; M_2 \text{ as } R\text{-modules} \quad \Leftrightarrow \quad \mathcal{I}_n(M_1) \;\simeq\; \mathcal{I}_n(M_2) \text{ as } M_n(R)\text{-modules.}$$

Proof. This follows almost immediately from the fact that $\{R, M_n(R), R^n, (R^n)^*\}$ is a Morita context; cf. Curtis-Reiner[8], p. 64. Indeed, if $P = R^n$, with standard basis $\underline{x} = \{x_1, \ldots, x_n\}$, then we have (as in [8]) the identification $\tau_{\underline{x}} : \mathrm{End}_R(P)^{op} \xrightarrow{\sim} M_n(R)$ (which is given by $\tau_{\underline{x}}(\alpha) = (a_{ij})$, where $x_i\alpha = \sum_j a_{ij}x_j$). Furthermore, by Morita (or otherwise) we have the canonical identification $\theta : P^* \otimes_R P \xrightarrow{\sim} \mathrm{End}_R(P)^{op}$ which is defined by $\theta(x^* \otimes y)z = x^*(z)y$ for $x^* \in P^* = \mathrm{Hom}_R(P, R)$ and $y, z \in P$. Now if $\{x_i^*\}$ denotes the dual basis of P^* (with respect to the basis $\{x_i\}$), then $\theta(x_i^* \otimes x_j) = \varepsilon_{ij}$, where $\varepsilon_{ij} = (\delta_{ik}\delta_{jl})_{kl}$ denotes the matrix whose (i,j)-th entry is 1 and is 0 otherwise. From this it is immediate that

$$\theta(P^* \otimes_R M) \;=\; \mathcal{I}_n(M),$$

and so all the assertions (and more) follow from the Morita Theorem ([8], p. 60).

We now apply this to study kernel ideals associated to the product abelian variety A^n, where A is a fixed abelian variety. Recall from above that we have a canonical identification

$$T_{A,n} : \mathrm{End}(A^n) \quad \xrightarrow{\sim} \quad M_n(R), \quad \text{where } R := \mathrm{End}(A).$$

For what follows, it is useful to introduce the following abbreviation. If $I_1, \ldots, I_n$ are left $\mathrm{End}(A)$-ideals, then we write

$$(I_1|\ldots|I_n) := T_{A,n}^{-1}(\mathcal{I}_n(I_1 \oplus \ldots \oplus I_n)),$$

which is a left $\mathrm{End}(A^n)$-ideal. Note that we have that

$$T_{A,n}((I_1|I_2|\ldots|I_n)) \;=\; \{(\alpha_{ij}) \in M_n(R) : \alpha_{ij} \in I_j, \text{ for } 1 \leq i, j \leq n\}. \tag{86}$$

Proposition 41 *If $H_1, \ldots, H_n$ are finite subgroup schemes of A, then*

$$I(H_1 \times H_2 \times \ldots \times H_n) \;=\; (I(H_1)|I(H_2)|\ldots|I(H_n)). \tag{87}$$

Thus, if $I_1, \ldots, I_n$ are kernel ideals, then $(I_1|\ldots|I_n)$ is also a kernel ideal.

Proof. Write $\pi_i = \pi_{H_i} : A \to A_i := A_{H_i}$ and $\pi = \pi_1 \times \ldots \times \pi_n : A^n \to A_1 \times \ldots \times A_n$. Since $\mathrm{Ker}(\pi) = H := H_1 \times \ldots \times H_n$, we can identify $\pi_{H_1 \times \ldots \times H_n}$ with π. Thus $I(H) = \mathrm{Hom}(A_H^n, A^n)\pi$.

Write $T = T_{A,n}$, $T' = T_{A^n, A_H^n}$ and $T'' = T_{A_H^n, A^n}$. Since $T'(\pi) = \mathrm{diag}(\pi_1, \ldots, \pi_n)$ is the diagonal "matrix" with entries $\pi_i \in \mathrm{Hom}(A, A_i)$, we see that if $f \in \mathrm{End}(A^n)$, then $f \in I(H) \Leftrightarrow f = f'\pi$, for some $f' \in \mathrm{Hom}(A_H^n, A^n) \Leftrightarrow T(f) = T''(f')T'(\pi)$, for some $T''(f') \in M(A_H^n, A^n)$. Thus, if we write $T(f) = (\alpha_{ij})$ with $\alpha_{ij} \in \mathrm{End}(A)$, then $h \in I(H) \Leftrightarrow (\alpha_{ij}) = (\beta_{ij})\mathrm{diag}(\pi_1, \ldots, \pi_n)$, for some $\beta_{ij} \in \mathrm{Hom}(A_j, A)$. Since the (i,j)-th entry of $(\beta_{ij})\mathrm{diag}(\pi_1, \ldots, \pi_n)$ is $\beta_{ij}\pi_j$, we see that $f \in I(H) \Leftrightarrow T(f) = (\alpha_{ij})$ with $\alpha_{ij} = \beta_{ij}\pi_j \in \mathrm{Hom}(A_j, A)\pi_j = I(H_j)$, and so the first assertion follows; cf. (86).

The second assertion is clear: if the I_j's are kernel ideals, then $I_j = I(H_j)$, for some finite group scheme H_j, and so by the first assertion we have that $(I_1|\ldots|I_n) = I(H_1 \times \ldots \times H_n)$ is a kernel ideal; cf. Remark 7(b).

We also have the following result which is partially dual to Proposition 41.

Proposition 42 *If $I_1, \ldots, I_n$ are left ideals of* $\mathrm{End}(A)$*, then*

$$H((I_1|I_2|\ldots|I_n)) \;\leq\; H(I_1) \times H(I_2) \times \ldots \times H(I_n), \tag{88}$$

and equality holds if $I_1, \ldots, I_n$ are kernel subgroups. Thus, if $H_1, \ldots, H_n$ are ideal subgroups of A, then $H_1 \times \ldots \times H_n$ is an ideal subgroup of A^n.

Proof. Let $f_i \in I_i$, where $i = 1, \ldots, n$. Since $T_{A,n}(f_1 \times \ldots \times f_n) = \mathrm{diag}(f_1, \ldots, f_n)$, we see that $f_1 \times \ldots \times f_n \in (I_1|\ldots|I_n)$. Thus

$$H((I_1|I_2|\ldots|I_n)) \leq \bigcap_{1 \leq i \leq n} \bigcap_{f_i \in I_i} \mathrm{Ker}(f_1 \times \ldots \times f_n) = \left(\bigcap_{f_1 \in I_1} \mathrm{Ker}(f_1)\right) \times \ldots \times \left(\bigcap_{f_n \in I_n} \mathrm{Ker}(f_n)\right).$$

Since the right hand side equals $H(I_1) \times \ldots \times H(I_n)$, the first assertion follows.

To prove the second assertion, put $H_i = H(I_i)$, so $I(H_i) = I_i$ by hypothesis. Thus, by (88), (8), and (87) we obtain $H((I_1|\ldots|I_n)) \leq H_1 \times \ldots H_n \leq H(I(H_1 \times \ldots \times H_n)) = H((I(H_1)|\ldots|I(H_n))) = H((I_1|\ldots|I_n))$, and so we must have equality throughout. This proves the second assertion, and from this the last assertion follows immediately. Indeed, since each $I_i := I(H_i)$ is a kernel ideal, we obtain from (87) that $H(I_1|\ldots|I_n) = H(I_1) \times \ldots \times H(I_n) = H_1 \times \ldots \times H_2$, the latter because each H_i is an ideal subgroup. But this means that $H_1 \times \ldots \times H_2$ is an ideal subgroup; cf. Remark 7(b).

We can now put together what we proved so far to conclude the following result which partially generalizes Theorem 1 of the introduction.

Theorem 43 *Let $H_1, \ldots, H_n$ and $H'_1, \ldots, H'_n$ be ideal subgroups of A. Then*

$$A_{H_1} \times \ldots \times A_{H_n} \simeq A_{H'_1} \times \ldots \times A_{H'_n} \Leftrightarrow I(H_1) \oplus \ldots \oplus I(H_n) \simeq I(H'_1) \oplus \ldots \oplus I(H'_n).$$

Proof. Since $H := H_1 \times \ldots \times H_n$ and $H' := H'_1 \times \ldots \times H'_n$ are ideal subgroups of A^n by Proposition 42, we have by (21) that $A^n_H \simeq A^n_{H'} \Leftrightarrow I(H) \simeq I(H')$. Now by (87) we have $I(H) = (I_1|\ldots|I_n)$ and $I(H') = (I'_1|\ldots|I'_n)$, where $I_i = I(H_i)$ and $I'_i = I(H'_i)$. Thus, since $T := T_{A,n}$ is an isomorphism, and since $T(I(H)) = T((I_1|\ldots|I_n)) = \mathcal{I}_n(I_1 \oplus \ldots \oplus I_n)$ and $T(I(H')) = \mathcal{I}_n(I'_1 \oplus \ldots \oplus I'_n)$, we see that $I(H) \simeq I(H')$ (as $\mathrm{End}(A^n)$-modules) $\Leftrightarrow \mathcal{I}_n(I_1 \oplus \ldots \oplus I_n) \simeq \mathcal{I}_n(I'_1 \oplus \ldots \oplus I'_n)$ (as $M_n(\mathrm{End}(A))$-modules) $\Leftrightarrow I_1 \oplus \ldots \oplus I_n \simeq I'_1 \oplus \ldots \oplus I'_n$ (as $\mathrm{End}(A)$-modules), the latter by Proposition 40. This proves the assertion.

Note that Theorem 1 follows easily from this and the results of section 3, as we shall now see.

Proof of Theorem 1. Let $\pi_i : E \to E_i$ and $\pi'_i : E \to E'_i$ be isogenies. Since $f_{E_i}|f_E$ and $f_{E'_i}|f_E$, we know by (46) that $H_i = \mathrm{Ker}(\pi_i)$ and $H'_i = \mathrm{Ker}(\pi_i)$ are ideal subgroups, and so the assertion follows from Theorem 43 because $E_i \simeq E_{H_i}$, $E'_i \simeq E_{H'_i}$ and $I_E(E_i) \simeq I(H_i)$ and $I_E(E'_i) \simeq I(H'_i)$.

4.2 The theorems of Steinitz and of Borevich and Faddeev

In order to derive further properties about abelian varieties which are isogenous to a product A^n, we shall use the results due to Steinitz[25] and to Borevich and Faddev[1] about the R-module structure of the submodules of R^n.

Theorem 44 (Steinitz) *If R be a Dedekind domain, then every submodule of R^n is isomorphic to a direct sum of R-ideals. Moreover, if $I_1, \ldots, I_n$ and $J_1, \ldots J_m$ are R-ideals, then*

$$I_1 \oplus \ldots \oplus I_n \;\simeq\; J_1 \oplus \ldots \oplus J_m \quad \Leftrightarrow \quad m = n \;\; \textit{and} \;\; I_1 \cdots I_n \;\simeq\; J_1 \cdots J_m.$$

Proof. See [8], p. 85.

This theorem does not generalize to arbitrary orders in a number field F, for already the first assertion of theorem may be false. As Borevich and Faddeev[2] observed, one needs the extra condition that the order R be *cyclic* in the sense that $\mathfrak{O}_F/R$ is a cyclic R-module. In their papers, they prove the following generalization of Steinitz's theorem.

Theorem 45 (Borevich/Faddeev) *Let R be an order in a Dedekind domain $\mathfrak{O}$. Then:*

(a) *The order R is cyclic if and only if for all $n \geq 1$ we have that every R-submodule of R^n is isomorphic to a direct sum of R-ideals.*

(b) *Let R be a cyclic order, and let M be an R-submodule of R^n of rank n. Then there exist R-ideals $I_1, \ldots, I_n$ such that*

$$M \simeq I_1 \oplus \ldots \oplus I_n \quad \text{and} \quad R(I_1) \subset R(I_2) \subset \ldots R(I_n), \tag{89}$$

and the orders $R(I_1) \subset \ldots \subset R(I_n)$ and the ideal class of the product $I_1 \cdots I_n$ are uniquely determined by the isomorphism class of M. More precisely, if $J_1, \ldots, J_m$ are R-ideals with $R(J_1) \subset \ldots \subset R(J_m)$, then we have

$$I_1 \oplus \ldots \oplus I_n \simeq J_1 \oplus \ldots \oplus J_m \Leftrightarrow n = m \text{ and } R(I_k) = R(J_k), \text{ for } 1 \leq k \leq n, \text{ and } I_1 \cdots I_n \simeq J_1 \cdots J_m. \tag{90}$$

Proof. (a) This is the main theorem of Borevich/Faddeev[2].

(b) The existence of the $I_1, \ldots, I_n$ satisfying (89) is proven in [1], Theorem 3. The uniqueness of the orders $R(I_1), \ldots, R(I_n)$ and of the product $I_1 \cdots I_n$ is proven in Theorems 5 and 6 of [1], and the assertion (90) is the content of [1], Theorem 7.

Remark 46 (a) Since a Dedekind domain is trivially a cyclic order (in itself), it clear that Theorem 45 generalizes Theorem 44.

(b) Every order $R_\Delta = \mathbb{Z} + \mathbb{Z}\omega_\Delta$ in a quadratic field $F = \mathbb{Q}(\sqrt{\Delta})$ is cyclic because $\mathfrak{O}_F = \mathbb{Z} + \mathbb{Z}\omega_F = R_\Delta + R_\Delta \omega_F$. Thus, Theorem 45(b) applies to all orders in quadratic fields.

(c) It follows from the above Theorem 45 (cf. [1], Theorem 8) that the rule

$$(R_1, \ldots, R_n; I) \mapsto R_1 \oplus \ldots \oplus R_{n-1} \oplus I$$

induces a bijection between the following sets:

(i) the set of lists $(R_1, \ldots, R_n; I)$ where $R \subset R_1 \subset \ldots \subset R_n \subset \mathfrak{O}_F$ are orders containing R and $I \in \mathrm{Pic}(R_n)$ is a class of invertible R_n-ideals;

(ii) the set of isomorphism classes of finitely generated torsion-free R-modules of rank n.

Corollary 47 *Let V be an n-dimensional F-vector space, where $F \supset \mathbb{Q}$ is a quadratic field, and let L be a lattice in V, i.e. $L \subset V$ is a finitely generated subgroup which contains a basis of V. Then $R_F(L) := (L : L)_F = \{x \in F : xL \subset L\}$ is an order of F, and L is an $R_F(L)$-module. Furthermore, there exists a sequence of orders $R_1 = R_F(L) \subset R_2 \subset \ldots \subset R_n$, an invertible R_n-ideal I and a basis $x_1, \ldots, x_n$ of V such that*

$$L = R_1 x_1 + R_2 x_2 + \ldots + R_{n-1} x_{n-1} + I x_n. \tag{91}$$

Proof. Since L is finitely generated, it follows easily that $R_F(L)$ is a subring of $\mathfrak{O}_F$. Thus, $R_F(L)$ is order of F provided that $d\mathfrak{O}_F \subset R_F(L)$, for some d. To see this, fix a basis $\{x_1, \ldots, x_n\}$ of V, and put $L_0 = \sum \mathcal{O}_F x_i$. By the usual argument there is a $n \in \mathbb{N}$ such that $nL \subset L_0$, and $d := [L_0 : nL]$ is finite. Since $R_F(L_0) = \mathfrak{O}_F$, we see that $d\mathfrak{O}_F \subset (nL : nL) = R_F(L)$.

Put $R = R_F(L)$, so clearly L is an R-module. By Remark 46(b), (c) we see that there exist orders $R_1 \subset \ldots \subset R_n$ and an invertible R_n ideal I such that $L \simeq L' := R_1 y_1 + \ldots + R_{n-1} y_{n-1} + I y_n$ (as R-modules), where $\{y_1, \ldots, y_n\}$ is any basis of V. But any such isomorphism extends to an isomorphism of $FL = V$ to $FL' = V$ and hence is given by $g \in \mathrm{Aut}_F(L)$. Thus, L has the form (91) with respect to the basis $x_1 = g^{-1}(y_1), \ldots, x_n = g^{-1}(y_n)$.

Finally, we observe that if L has the form (91), then $R_F(L) = R_1 \cap \ldots \cap R_{n-1} \cap R(I) = R_1$, which proves the assertion that $R_F(L) = R_1$.

For later applications we note the following variant of the bijection mentioned in Remark 46(c).

Corollary 48 *Let R be an order in quadratic field F and assume that $n \geq 2$. If I is a non-zero R-ideal and if $f_1, \ldots f_{n-2}$ are positive integers with $f_{R(I)} | f_1 | \ldots | f_{n-2} | f_R$, and if R_i denotes the unique order of F of conductor f_i, then*

$$M(I; f_1, \ldots, f_{n-2}) \ := \ I \oplus f_R R_1 \oplus \ldots \oplus f_R R_{n-2} \oplus R$$

is an R-submodule of R^n with $R_F(M) = R$. Moreover, the map $\mu_{R,n} : (I; f_1, \ldots, f_{n-2}) \mapsto M(I; f_1, \ldots, f_{n-2})$ induces a bijection between:

(i) *the set of sequences $(I; f_1, \ldots, f_{n-2})$ where I is an isomorphism class of non-zero R-ideals and $f_{R(I)} | f_1 | \ldots | f_{n-2} | f_R$;*

(ii) *the set of isomorphism classes of R-submodules M of R^n of rank n with $R_F(M) = R$.*

Proof. If $(I; f_1, \ldots, f_{n-2})$ is a tuple as in (i), put $I_k = f_R R_i$, for $1 \leq k \leq n-2$. Clearly $R(I_k) = R_k$, for $1 \leq k \leq n-2$, and so $R(I) \supset R(I_1) \supset \ldots \supset R(I_{n-2}) \supset R$. Furthermore, since $[R_i : R] | f_R = [\mathfrak{O}_F : R]$, we see that $I_k \subset R$, and hence each I_k is an R-ideal. Thus $M := M(I; f_1, \ldots, f_{n-2})$ is an R-submodule of R^n. Furthermore, since $(M : M)_F = R(I) \cap R(I_1) \cap \ldots \cap R(I_{n-2}) \cap R = R$, we see that $\mu_{R,n}$ defines a map from the set described in (i) to the set described in (ii).

To see that $\mu_{R,n}$ is injective, suppose that $M(I; f_1, \ldots, f_{n-2}) \simeq M(I'; f'_1, \ldots, f'_{n-2})$, and put $I_0 = I$, $I_k = f_R R_k$, $1 \leq k \leq n-2$ and $I_{n-1} = R$, and define I'_k similarly using $(I'; f'_1, \ldots, f'_{n-2})$. Since $R = R(I_{n-1}) \subset R(I_{n-2}) \subset \ldots \subset R(I_0)$ and $R = R(I'_{n-1}) \subset R(I'_{n-2}) \subset \ldots \subset R(I'_0)$ are linearly ordered, if follows from Theorem 45(b) that $R(_k) = R(I'_k)$ for $0 \leq k \leq n-1$ and that $I_0 \cdots I_{n-1} \simeq I'_0 \cdots I'_{n-1}$. Thus $f_k = f'_k$,

for $k = 1, \ldots, n-2$. Moreover, since $I_0 \cdots I_{n-1} = f_R^{n-2} I$ and $I_0' \cdots I_{n-1}' = f_R^{n-2} I'$, we see that $I \simeq I'$, and so $\mu_{R,n}$ is injective.

To see that $\mu_{R,n}$ is surjective, let M be an R-submodule of R^n of rank n with $(M : M) = R$. Then by Corollary 47 we know that $M \simeq R_1 \oplus \ldots \oplus R_{n-1} \oplus I$, where $R_1 \subset \ldots \subset R_n$ are orders and I is an invertible R_n-ideal and that $R_1 = R$ because $(M : M) = R$ by hypothesis. Put $f_i = f_{R_{n-1-i}}$ for $1 \leq i \leq n-2$ Then clearly $f_R I \subset f_R R_n$, so $f_R I$ is an R-ideal which is isomorphic to I, and so it is clear that $M(f_R I; f_1, \ldots, f_{n-2}) \simeq I \oplus R_{n-2} \oplus \ldots \oplus R_1 \oplus R \simeq M$, and so $\mu_{R,n}$ is surjective.

One of the disadvantages of Theorem 45 is that it does not give a recipe for determining the orders R_k and ideals I_k such that (89) holds when M is given. For this we prove the following result (which is similar to Lemma 8 of [1], but without the restrictive hypothesis that $R_1 \subset R_2$):

Proposition 49 *Let L_1 and $L_2 \in \mathrm{Lat}_F$ be lattices in a quadratic field F, and put $R = R(L_1) \cap R(L_2)$. Then there is an R-module isomorphism*

$$L_1 \oplus L_2 \simeq R \oplus (L_1 L_2). \tag{92}$$

Proof. Put $R_i := R(L_i)$ and $f_i := [R_i : R]$. Then $(f_1, f_2) = 1$ by (37). We first claim:

$$\exists\, \lambda_1, \lambda_2 \in F^\times \quad \text{such that} \quad \lambda_1 L_1 + \lambda_2 L_2 = R. \tag{93}$$

Indeed, by replacing L_i by $m_i L_i$ we may assume that the L_i's are R-ideals, and so $L_i \subset f_i R$. Then $L_i' := \frac{1}{f_i} L_i \subset R_i$ is an invertible R_i-ideal, and so $\exists \lambda_2 \in F^\times$ such that $\lambda_2 L_2' + f_1 R_2 = R_2$ (cf. [18], p. 93) or, equivalently, that $(N(\lambda_2 L_2'), f_1) = 1$; cf. [7], p. 143). Put $(f_1, f_2) = 1$, we thus have $(N(L_2''), f_1) = 1$. Note also that $m_2 := [R : L_2''] = f_2 N(\lambda_2 L_2')$, so $(m_2, f_1) = 1$. Next choose $\lambda_1 \in F^\times$ such that $\lambda_1 L_1' + m_2 R_1 = R_1$ and put $L_1'' = \lambda_1 L_1 = f_1 \lambda_1 L_1' \subset f_1 R_1 \subset R$. Then $m_1 := [R : L_1''] = f_1 N(\lambda_1 L_1')$ and so $(m_1, m_2) = 1$. From this it follows that $L_1'' + L_2'' = R$, which proves (93).

To prove (92), we may assume in view of (93) that $L_1 + L_2 = R$ because $L_1 \oplus L_2 \simeq \lambda_1 L_1 \oplus \lambda L_2$. Thus, there exist $\alpha_i \in L_i$ such that $\alpha_1 - \alpha_2 = 1$. Define the map

$$\beta : L_1 \oplus L_2 \to R \oplus L_1 L_2 \quad \text{by} \quad \beta(\lambda_1, \lambda_2) = (\lambda_1 + \lambda_2, \lambda_1 \alpha_1 + \lambda_2 \alpha_2)$$

Clearly, β is R-module homomorphism with $\beta(L_1 \oplus L_2) \subset R \oplus L_1 L_2$. It is clear that β is injective because $\det(\left(\begin{smallmatrix} 1 & \alpha_1 \\ 1 & \alpha_2 \end{smallmatrix}\right)) = \alpha_2 - \alpha_1 = -1$. Moreover, β is surjective because if $r \in R$, $\lambda \in L_1 L_2 \subset L_1 \cap L_2$, then $\beta(\alpha_1 r - \lambda, \lambda - \alpha_2 r) = (r, \lambda)$. Thus β is an isomorphism, which proves (92).

Remark 50 It follows from the above result by induction that if $L_1, \ldots, L_n \in \mathrm{Lat}_F$ and $R = \cap_i R(L_i)$, then there is an R-module isomorphism

$$L_1 \oplus \ldots \oplus L_n \simeq R_1 \oplus \ldots \oplus R_{n-1} \oplus (L_1 \cdots L_n) \text{ where } R_k = R(L_1 \cdots L_k) \cap R(L_{k+1}) \text{ if } k < n.$$

For later applications we also want to explain the connection between the (conductor of) the order $R_F(L)$ defined above and the so-called *central conductor* of a suitable order in the matrix ring $M_n(F)$. This central conductor is defined as follows.

Definition. Let $\mathcal{R}$ be an order in $M_n(F)$, i.e. $\mathcal{R} \subset M_n(F)$ is a subring which is finitely generated as a $\mathbb{Z}$-module and which contains an F-basis of $M_n(F)$. For convenience, assume that $F \supset \mathbb{Q}$ is a quadratic field. Then the centre $Z(\mathcal{R})$ of $\mathcal{R}$ is an order of $F = Z(M_n(F))$, and hence is uniquely determined by its conductor

$$f_{\mathcal{R}} := f_{Z(\mathcal{R})} = [\mathfrak{O}_F : Z(\mathcal{R})],$$

which we call the *central conductor* of $\mathcal{R}$. Clearly, this is an invariant of the isomorphism class of $\mathcal{R}$. Note that this term is closely related to that of [8], p. 604: there the central conductor is the ideal $f_{\mathcal{R}}\mathfrak{O}_F$.

Proposition 51 *Let R be an order in a quadratic field F and let M be an R-submodule of R^n of rank n. Put*

$$\mathcal{R}(M) \ := \ (\mathcal{I}_n(M) : \mathcal{I}_n(M)) \ = \ \{g \in M_n(F) : \mathcal{I}_n(M)g \subset \mathcal{I}_n(M)\}.$$

Then we have R-ring isomorphisms

$$\text{(94)} \qquad \mathrm{End}(M)^{op} \ \tilde{\to} \ \mathcal{R}(M) \quad \textit{and} \quad R_F(M) \ \tilde{\to} \ Z(\mathcal{R}(M))$$

and hence the central conductor of $\mathcal{R}(M)$ equals the conductor of $R_F(M)$, i.e. $f_{\mathcal{R}(M)} = f_{R_F(M)}$.

Proof. Put $\mathcal{M} := M_n(R)$, and view $\mathcal{M}$ as a left $\mathcal{M}$-module. Then (as for any ring) we have the canonical identification $\rho_{\mathcal{M}} : \mathcal{M} \tilde{\to} \mathrm{End}_{\mathcal{M}}(\mathcal{M})$ given by $g \mapsto \rho_g$, where $\rho_g(g') = g'g$ denotes the right multiplication map. Combining this with the identification $\tau_{\underline{x}} : \mathrm{End}_R(R^n)^{op} \tilde{\to} \mathcal{M}$ defined in the proof of Proposition 40, we thus obtain an isomorphism $\rho := \rho_{\mathcal{M}} \circ \tau_{\underline{x}} : \mathrm{End}_R(R^n)^{op} \tilde{\to} \mathrm{End}_{\mathcal{M}}(\mathcal{M})$, which extends to an isomorphism $\tilde{\rho} : \mathrm{End}_F(F^n)^{op} \tilde{\to} \mathrm{End}_{\tilde{\mathcal{M}}}(\tilde{\mathcal{M}})$, where $\tilde{\mathcal{M}} = M_n(F)$.

Since M is a lattice in F^n, every $f \in \mathrm{End}_R(M)^{op}$ extends uniquely to $\tilde{f} \in \mathcal{E} := \mathrm{End}_F(F^n)^{op}$, and so we can identify $\mathrm{End}_R(M)^{op}$ with the subring $(M : M)_{\mathcal{E}} = \{f \in \mathcal{E} : Mf \subset M\}$ of $\mathcal{E}$. It is then immediate from the definition of $\mathcal{I}_n(M)$ that

$$\tilde{\rho}((M : M)_{\mathcal{E}}) \ = \ (\mathcal{I}_n(M) : \mathcal{I}_n(M)) \ = \ \mathcal{R}(M).$$

This proves this first isomorphism of (94), and from this the second follows because $Z((M : M)_{\mathcal{E}}) = (M : M)_{\mathcal{E}} \cap Z(\mathcal{E}) = (M : M)_F = R_F(M)$.

4.3 Products of CM elliptic curves

We now apply the results of the previous subsections to the case that $A = E$ is a CM elliptic curve (in the sense of §3.1). The first result is the following.

Proposition 52 *Let E/K be a CM elliptic curve and let I be a regular ideal of* $\mathrm{End}(E^n)$*, where $n \geq 1$. Then I is a kernel ideal and there exist non-zero ideals $I_1, \ldots, I_n$ of* $\mathrm{End}(E)$ *such that $I \simeq (I_1 | \ldots | I_n)$. Furthermore,*

$$(95)\quad E^n_{H(I)} \;\simeq\; E_{H(I_1)} \times \ldots \times E_{H(I_n)} \quad \textit{and} \quad \mathcal{E}(H(I)) \;\simeq\; \mathrm{End}_R(I_1 \oplus \ldots \oplus I_n)^{op}.$$

Proof. Let I be an ideal of $\mathrm{End}(E^n)$, and put $R = \mathrm{End}(E)$. Since $T = T_{E,n} : \mathrm{End}(E^n) \xrightarrow{\sim} M_n(R)$ is an isomorphism, it follows from Proposition 40 that $I = \mathcal{I}_n(M)$, for some R-submodule $M \subset R^n$. Moreover, since I is regular, we see that M has finite index in R^n. Since $F = \mathrm{End}^0(E)$ is an (imaginary) quadratic field, we have by Corollary 47 that there exist orders R_i with $R \subset R_1 \subset \ldots \subset R_n$ of R, an ideal I of R_n and a basis $\{x_i\}$ of F^n such that M has the form (91). Put $f = [R_n : R]$. Then $fR_i \subset R$ is an R-ideal for all i, and so

$$I \;=\; I_1 x_1' + I_2 x_2' + \ldots + I_n x_n',$$

where $I_i = fR_i$ for $1 \leq i < n$ and $I_n = fI$ and $x_i' = \frac{1}{f} x_i$. Thus, if $g \in M_n(F)$ is the matrix that takes the standard basis of F^n to the basis $\{x_i'\}$, then we see that

$$(96)\qquad I \;=\; (I_1 | \ldots | I_n)h,$$

where $h = T_{E,n}(g)^{-1} \in \mathrm{End}^0(E^n)$ and $I_1, \ldots, I_n$ are non-zero R-ideals. Thus $I \simeq I' := (I_1 | \ldots | I_n)$. Since each I_k is a kernel ideal of $\mathrm{End}(E)$ by Theorem 18, we have by Proposition 41 that I' is a kernel ideal, and hence so is I by Remark 7(c). This proves the first two assertions.

Since the I_k's are kernel ideals, we have $H((I_1 | \ldots | I_n) = H(I_1) \times \ldots \times H(I_n)$ by Proposition 42. Thus, by (19) we have $E^n_{H(I)} \simeq E^n_{H((I_1|\ldots|I_n))} = E_{H(I_1)\times\ldots\times H(I_n)} \simeq E_{H(I_1)} \times \ldots \times E_{H(I_n)}$, which proves the first isomorphism of (95).

To prove the second, note first that since $I \simeq I'$ are kernel ideals of $\mathrm{End}(E^n)$, we have by (19) and Proposition 10 that $\mathcal{E}(H(I)) \simeq \mathcal{E}(H(I')) = (I' : I')$. On the other hand, since $I' = T^{-1}_{E,n}(\mathcal{I}_n(I_1 \oplus \ldots \oplus I_n))$ by definition, it follows from (94) that $(I' : I') \simeq \mathrm{End}_R(I_1 \oplus \ldots \oplus I_n)^{op}$, and so the second isomorphism of (95) follows.

The above result allows us to work out the *central conductor* f_A of the abelian variety $A = A_{H(I)}$. This important invariant is defined as follows.

Definition. If $A \sim E^n$ is any abelian variety which is isogenous to E^n, then its *central conductor* is the central conductor $f_A := f_{\mathrm{End}(A)}$ of the order $\mathrm{End}(A)$ in $\mathrm{End}^0(A) \simeq \mathrm{End}^0(E^n) = M_n(F)$. (Recall that $f_{\mathrm{End}(A)}$ was defined in §4.2).

Corollary 53 *If $A \simeq E_1 \times \ldots \times E_n$, where $E_1, \ldots, E_n \in \mathrm{Isog}(E/K)$, then*

$$f_A = \mathrm{lcm}(f_{E_1}, \ldots, f_{E_n}).$$

Proof. By Proposition 36 there is an $E_0 \in \mathrm{Isog}(E/K)$ such that $f_{E_0} = \mathrm{lcm}(f_{E_1}, \ldots, f_{E_n})$. Thus, if $\pi_i : E_0 \to E_i$ is an isogeny, then $H_i = \mathrm{Ker}(\pi_i)$ is an ideal subgroup of E_0 by (46) (because $f_{E_i} | f_{E_0}$ by construction). Thus, $H_i = H(I_i)$, for some R_0-ideal I_i, where $R_0 = \mathrm{End}(E_0)$. Note that by (45) we have that $\mathrm{End}(E_i) \simeq \mathcal{E}(H_i) = (I_i : I_i) = R(I_i)$, and so $f_{E_i} = f_{R(I_i)}$.

Put $H = H_1 \times \ldots \times H_n$. Then $A_H \simeq E_{H_1} \times \ldots \times E_{H_n} \simeq E_1 \times \ldots \times E_n \simeq A$. By Proposition 41 we have $H = H(I)$, where $I = (I_1 | \ldots | I_n)$. Thus, by (95) we have $\mathrm{End}(A) \simeq \mathrm{End}(A_H) \simeq \mathcal{E}(H) \simeq \mathrm{End}_{R_0}(M)^{op}$, where $M = I_1 \oplus \ldots \oplus I_n \subset R_0^n$, and so $Z(\mathrm{End}(A)) \simeq Z(\mathrm{End}_{R_0}(M))^{op} = (M : M)_F = R_F(M)$ by (94). Now clearly $(M : M)_F = R(I_1) \cap \ldots \cap R(I_n)$. Since the latter has conductor $\mathrm{lcm}(f_{R(I_1)}, \ldots, f_{R(I_n)})$ by (37), the assertion follows.

We next want to characterize the ideal subgroups of E^n. The following characterization shows that the necessary condition of Corollary 11 is also sufficient. Moreover, this result can also be viewed as a generalization of the criterion (46) of Theorem 18.

Theorem 54 *Let E/K is a CM elliptic curve, and let H be a finite subgroup scheme of E^n. Then:*

$$(97) \quad H \text{ is an ideal subgroup of } E^n \;\Leftrightarrow\; Z(\mathrm{End}(E^n)) \subset \mathcal{E}(H) \;\Leftrightarrow\; f_{\mathcal{E}(H)} \mid f_E.$$

Before proving this, we note the following immediate application.

Corollary 55 *If $A \sim E^n$ is an abelian variety which is isogenous to E^n with $f_A | f_E$, then there exist elliptic curves $E_1, \ldots, E_n \in \mathrm{Isog}^+(E/K)$ such that $A \simeq E_1 \times \ldots \times E_n$.*

Proof. Let $\pi : E^n \to A$ be an isogeny, and let $H = \mathrm{Ker}(\pi)$. Then $E_H^n \simeq A$ and $\mathrm{End}(A) \simeq \mathcal{E}(H)$, so $f_A = f_{\mathcal{E}(H)}$. It thus follows from the hypothesis and (97) that H is an ideal subgroup. Thus, $H = H(I)$, for some regular left ideal I of $\mathrm{End}(E^n)$, and hence by (95) we have $A \simeq A_H \simeq E_1 \times \ldots \times E_n$, where $E_i := E_{H(I_i)}$, for suitable ideals I_i of $\mathrm{End}(E)$. Since $H(I_i)$ is an ideal subgroup of E, we have by (46) that $f_{E_i} | f_E$, and so $E_i \in \mathrm{Isog}^+(E/K)$, as claimed.

Another application of Theorem 54 is the following result which can be viewed as a solution of the isomorphism problem which was posed in the introduction of this paper. Note that it applies to an arbitrary tuple $E_1, \ldots, E_n/K$ of isogenous CM curves because by Proposition 36 we can always find an elliptic curve E/K such that $E_1, \ldots, E_n \in \mathrm{Isog}^+(E/K)$.

Corollary 56 *Let E/K be a CM elliptic curve and $E_1, \ldots, E_n \in Isog^+(E/K)$. If $A \sim E^n$ is an abelian variety isogenous to E^n, then the following conditions are equivalent:*

$$A \simeq E_1 \times \ldots \times E_n; \tag{98}$$

$$I_{E^n}(A) \simeq (I_E(E_1) : \ldots : I_E(E_n)) \quad \textit{and} \quad f_A | f_E; \tag{99}$$

$$\mathrm{End}(E)^n \otimes_{\mathrm{End}(E^n)} I_{E^n}(A) \simeq I_E(E_1) \oplus \ldots \oplus I_E(E_n) \quad \textit{and} \quad f_A | f_E. \tag{100}$$

Proof. Fix isogenies $\pi : E^n \to A$ and $\pi_i : E \to E_i$, for $1 \leq i \leq n$, and put $H = \mathrm{Ker}(\pi)$ and $H_i = \mathrm{Ker}(\pi_i)$. Also, put $A' = E_1 \times \ldots \times E_n$. Since $f_{E_i} | f_E$ by hypothesis, we know by (46) that $H_i = H(I(H_i))$ is an ideal subgroup of E, so $H' := H_1 \times \ldots \times H_n$ is an ideal subgroup of E^n by Proposition 42. Furthermore, we have that $I_{E^n}(A') \simeq I(H') = (I(H_1) : \ldots : I(H_n)) \simeq (I_E(E_1) : \ldots : I_E(E_n))$ by (87).

Now suppose that (98) holds. Then by Corollary 53 we have that $f_A = f_{E_1 \times \ldots \times E_n} = \mathrm{lcm}(f_{E_1}, \ldots, f_{E_n}) | f_E$. Moreover, $I_{E^n}(A) \simeq I_{E^n}(A') \simeq (I_E(E_1) : \ldots : I_E(E_n))$, and so (99) holds. Conversely, if (99) holds, then H is an ideal subgroup of E^n by Theorem 54, and so $A \simeq A'$ by (21). Thus, conditions (98) and (99) are equivalent.

To prove the equivalence of conditions (99) and (100), consider the submodules $M_1 := \mathrm{End}(E)^n \otimes_{\mathrm{End}(E^n)} I_{E^n}(A)$ and $M_2 = I_E(E_1) \oplus \ldots \oplus I_E(E_n)$. Then by definition we have $T_{E,n}^{-1}(\mathcal{I}_n(M_2)) = (I_E(E_1) : \ldots : I_E(E_n))$ and by Morita equivalence (cf. the proof of Proposition 40) we have $T_{E,n}^{-1}(\mathcal{I}_n(M_1)) \simeq I_{E^n}(A)$. Thus, since $M_1 \simeq M_2$ (as $\mathrm{End}(E)$-modules) $\Leftrightarrow T_{E,n}^{-1}\mathcal{I}_n(M_1) \simeq T_{E,n}^{-1}\mathcal{I}_n(M_2)$ (as $\mathrm{End}(E^n)$-modules) by Proposition 40, the equivalence of conditions (99) and (100) follows.

As first step towards establishing Theorem 54, we prove the following result.

Proposition 57 *Let H be a finite subgroup scheme of E^n, where E/K is a CM elliptic curve. Then H is an ideal subgroup of E^n if and only if*

$$A_H \simeq E_1 \times \ldots \times E_n, \quad \textit{where } E_i \in \mathrm{Isog}^+(E/K), \ \textit{for } 1 \leq i \leq n. \tag{101}$$

Proof. Suppose first that $H = H(I)$ is an ideal subgroup. Then by (95) we have $E_H^n \simeq E_1 \times \ldots \times E_n$ where $E_i = E_{H(I_i)}$. Since $H(I_i)$ is an ideal subgroup of E, we have by (46) that $f_{E_i} | f_E$, i.e. that $E_i \in \mathrm{Isog}^+(E/K)$.

Conversely, suppose that (101) holds, and fix an isogeny $\pi_i : E \to E_i$ for $1 \leq i \leq n$. Then by (46) we know that $H_i := \mathrm{Ker}(\pi_i)$ is an ideal subgroup of E, so $H' := H_1 \times \ldots \times H_n$ is an ideal subgroup of E^n by Proposition 42. Since $E_i \simeq E_{H_i}$, we have by the hypothesis (101) that $E_H^n \simeq E_{H_1} \times \ldots \times E_{H_n} \simeq E_{H'}^n$, and so it follows from (22) that H is also an ideal subgroup of E^n.

As we shall see presently, Theorem 54 follows easily from the following result.

Theorem 58 *Let E/K be a CM elliptic curve, where K is an algebraically closed field. If $A \sim E^n$ is an abelian variety which is isogenous to E^n, then there exist elliptic curves $E_1, \ldots, E_n \sim E$ such that $A \simeq E_1 \times \ldots \times E_n$.*

Remark 59 In the case that $K = \mathbb{C}$, Theorem 58 was first proven by Lange[19], using the results of Shioda and Mitani[24] (who proved the case $n = 2$). A different proof of this was given by Schoen; cf. [22], Satz 2.4. His proof is based on the above Theorem 45(b) of Borevich and Faddeev[1] and hence is closely related to the one given below (in the case $K = \mathbb{C}$).

In his paper, Schoen[22] also proves the following interesting "converse" to Theorem 58 in the case $K = \mathbb{C}$. Suppose that $A/\mathbb{C}$ is an abelian variety with the property that if $B \sim A$, then $B \simeq A_1 \times \ldots \times A_n$, for some simple abelian varieties A_i. Then either A is simple or $A \sim E^n$, where $E/\mathbb{C}$ is a CM elliptic curve.

Before proving Theorem 58, let us see how Theorem 54 follows from it.

Proof of Theorem 54 (using Theorem 58). First note that the second equivalence of (97) is trivial because we have $\mathrm{End}(E) = Z(\mathrm{End}(E^n)) \subset \mathcal{E}(H) \Leftrightarrow \mathrm{End}(E) \subset Z(\mathcal{E}(H)) \Leftrightarrow f_{\mathcal{E}(H)} | f_E$.

Next we note that the one direction ($\Rightarrow$) of the first equivalence of (97) is true by Corollary 11. It thus remains to prove the other direction.

Thus, suppose that $Z(\mathrm{End}(E^n)) \subset \mathcal{E}(H)$. Since E is a CM elliptic curve, we have that $\mathrm{End}(E^n) = \mathrm{End}(E^n \otimes \overline{K})$, and hence also that $\mathrm{End}(A) = \mathrm{End}(A \otimes \overline{K})$. (To see this, note that $\mathrm{End}^0(E^n) = \mathrm{End}^0(A)$ (because $A \sim E^n$), and that $\mathrm{End}^0(E^n) = \mathrm{End}^0(E^n \otimes \overline{K})$, and so the assertion follows because $\mathrm{End}(A \otimes \overline{K})/\mathrm{End}(A)$ is always torsionfree.) Thus, we have that $\mathcal{E}(H \otimes \overline{K}) \simeq \mathrm{End}(A \otimes \overline{K}) = \mathrm{End}(A) \simeq \mathcal{E}(H)$, and so $Z(\mathrm{End}(E^n \otimes \overline{K})) \subset Z(\mathcal{E}(H \otimes \overline{K}))$. Thus $f_{A_{H \otimes \overline{K}}} = f_{\mathcal{E}(H \otimes \overline{K})} | f_{E \otimes \overline{K}} = f_E$.

By Theorem 58 we have that $A_{H \otimes \overline{K}} \simeq E_1 \times \ldots \times E_n$, for some elliptic curves $E_i/\overline{K}$. By Corollary 53 we have $f_{E_i} | f_{A_{H \otimes \overline{K}}} | f_E$, and so $E_i \in \mathrm{Isog}^+(E \otimes \overline{K}/\overline{K})$. Thus, condition (101) holds for $H \otimes \overline{K}$, and so $H \otimes \overline{K}$ is an ideal subgroup of $(E \otimes \overline{K})^n = E^n \otimes \overline{K}$ by Proposition 57. It thus follows from Remark 7(d) that H is an ideal subgroup of E^n.

Proof of Theorem 58. We shall divide the proof into several cases.

Case 1. $K = \mathbb{C}$.

Here $E \simeq E_L$, where $L \in \mathrm{Lat}_F$ is a lattice in $F = \mathrm{End}^0(E)$; cf. §3.2. Thus $E^n \simeq \mathbb{C}^n/L^n$, where $L^n = L \oplus \ldots \oplus L \subset F^n$. Let $\pi : E^n \to A$ be an isogeny. Then $\mathrm{Ker}(\pi) = L'/L^n$, for some subgroup $L' \subset \mathbb{C}^n$. Since $[L' : L^n] = \deg(\pi) < \infty$, it follows that L' is a lattice in F^n (in particular, $L' \subset F^n$) and hence by Corollary 47 we know that L' has the form (91). Put $L'' = L'_1 \oplus \ldots \oplus L'_n \subset F^n$, where $L'_i = R_i$ for $1 \leq i \leq n-1$ and $L'_n = I$ and the R_i's and I are given by (91). Thus $L' = L''g$, for some $g \in \mathrm{Aut}_F(F^n) \subset \mathrm{Aut}_{\mathbb{C}}(\mathbb{C}^n)$, and so $A \simeq \mathbb{C}^n/L' \simeq \mathbb{C}^n/L'' \simeq \mathbb{C}/L'_1 \times \ldots \times \mathbb{C}/L'_n$, and so the assertion follows because $L'_i \in \mathrm{Lat}_F$ (and hence $\mathbb{C}/L'_i \sim E_L$).

Case 2. $\mathrm{char}(K) = 0$.

As was mentioned in the proof of Proposition 32, there is a CM elliptic curve $E_0/\overline{\mathbb{Q}}$ such that $E_0 \otimes K \simeq E$. Furthermore, if $\pi : E^n \to A$ is an isogeny with kernel H, then there is a subgroup scheme H_0 of E_0^n such that $H_0 \otimes K = H$, and so $A_0 = (E_0^n)_{H_0}$ is an abelian variety over $\overline{\mathbb{Q}}$ with $A_0 \otimes K \simeq A$. It is thus enough to verify the assertion for $K = \overline{\mathbb{Q}}$.

Thus, let $K = \overline{\mathbb{Q}}$. By Case 1 we know that there exist CM elliptic curves $E_1, \ldots, E_n \in \mathrm{Isog}(E \otimes \mathbb{C}/\mathbb{C})$ such that $A \otimes \mathbb{C} \simeq E_1 \times \ldots \times E_n$. As before, there exist CM elliptic curves E_{i0}/K such that $E_{i0} \otimes \mathbb{C} \simeq E_i$. Put $A' = E_{10} \times \ldots \times E_{n0}$. As was just mentioned, every finite group scheme of $A \otimes \mathbb{C}$ is already defined over K, and so it follows that the condition $A \otimes \mathbb{C} \sim A' \otimes \mathbb{C}$ implies that $A \sim A'$. This proves the assertion in this case.

Case 3. $K = \overline{\mathbb{F}}_p$.

Let $K^{\#}$ denote the quotient field of the ring $W(K)$ of Witt-vectors. For any *ordinary* abelian variety A/K, its *Serre-Tate lift* $A^{\#}/K^{\#}$ exists and is uniquely characterized by the property that all endomorphisms of A/K lift to $A^{\#}$; cf. [9], p. 238, or [13], p. 2368, and the references therein. Since E and hence $A \sim E^n$ are ordinary abelian varieties, their Serre-Tate lifts exist; note that $(E^{\#})^n \simeq (E^n)^{\#}$. Since $\mathrm{Hom}((E^n)^{\#}, A^{\#}) = \mathrm{Hom}(E^n, A)$, it thus follows that $A^{\#} \sim (E^{\#})^n$. By Case 2 we know that there is a finite extension $K'/K^{\#}$ and elliptic curves $E_1', \ldots, E_n'/K'$ such that $A^{\#} \otimes K' \simeq E_1' \times \ldots \times E_n'$. Since each $E_i' \sim E^{\#} \otimes K'$ has good reduction E_i/K, we obtain that $A \simeq E_1 \times \ldots \times E_n$ because A is the reduction of $A^{\#} \otimes K'$.

Case 4. $\mathrm{char}(K) = p \neq 0$.

This is partially similar to the proof of Case 2, but extra care has to taken here in descending A. To be precise, note first that there is a CM elliptic curve $E_0/\overline{\mathbb{F}}_p$ such that $E_0 \otimes K \simeq E$; cf. the proof of Proposition 32. Furthermore, if $\pi : E^n \to A$ is an isogeny with kernel H, then by Lemma 60 below, there is a subgroup scheme H_0 of E_0^n such that $H_0 \otimes K = H$, and so $A_0 = (E_0^n)_{H_0}$ is an abelian variety over $\overline{\mathbb{Q}}$ with $A_0 \otimes K \simeq A$. By Case 3 there exist $E_1, \ldots, E_n \sim E_0$ such that $A_0 \simeq E_1 \times \ldots \times E_n$, and then $A \simeq A_0 \otimes K \simeq E_1' \times \ldots \times E_n'$, where $E_i' = E_i \otimes K \sim E$, as desired.

In the above proof we made use of the following fact.

Lemma 60 *Let E/K be a CM elliptic curve where K is an algebraically closed field, and let $n \geq 1$. Then E^n has only finitely many subgroup schemes H of fixed rank N. Thus, if K'/K is any extension field, then every finite subgroup scheme of $E^n \otimes K'$ is of the form $H \otimes K'$, where H is a finite subgroup scheme of E^n.*

Proof. If $\mathrm{char}(K) = 0$, then every finite subgroup scheme is etale and the assertion is trivial. Thus, assume that $\mathrm{char}(K) = p \neq 0$. Since E is ordinary, we have for any $r \geq 1$ that $E[p^r] := \mathrm{Ker}([p^r]_E) \simeq \mathbb{Z}/p^r\mathbb{Z} \times \mu_{p^r}$, and hence that $E^n[p^r] \simeq (\mathbb{Z}/p^r\mathbb{Z})^n \times (\mu_{p^r})^n$.

Thus E^n does not contain any local-local subgroup scheme (in the sense of [20], p. 136), and so by the structure of finite commutative group schemes ([20], p. 137) we have that any finite subgroup scheme H of E^n is isomorphic to $H_{et} \times (\mathbb{Z}/p^{r_1}\mathbb{Z})^{t_1} \times (\mu_{p^{r_2}})^{t_2}$, where H_{et} is an etale subgroup scheme of rank prime to p and $r_i, t_i \geq 0$ are integers. Thus, there are only finitely many (isomorphism classes of) finite subgroup schemes of fixed rank N which are embeddable in E^n.

Now let H/K be a fixed finite subgroup scheme of rank $N = p^r N'$ with $p \nmid N'$ which is embeddable in E^n. Then $\mathrm{Hom}(H, E^n) = \mathrm{Hom}(H, E^n[N])$, and so $\mathrm{Hom}(H, E^n) = \mathrm{Hom}(H_{et}, E[N']) \oplus \mathrm{Hom}((\mathbb{Z}/p^{r_1})^{t_1}, (\mathbb{Z}/p^r\mathbb{Z})^n) \oplus \mathrm{Hom}((\mu_{p^{r_2}})^{t_2}, (\mu_{p^r})^n)$ is finite (since each piece of the decomposition is finite). In particular, there are only finitely many embeddings of H into E^n, and so it follows from the above that there are only finitely many finite subgroup schemes of fixed rank N.

To prove the last assertion, note that since A/K is projective, it follows from the theory of Hilbert schemes that the set of subgroup schemes of fixed rank N is represented by a quasi-projective scheme $\mathcal{H}_N$. By what was just shown, $\mathcal{H}_N(K)$ is finite, and so it follows that $\dim \mathcal{H}_N = 0$. Thus $\mathcal{H}_N(K') = \mathcal{H}_N(K)$, for all K'/K, which yields the last assertion.

Remark 61 As the above proof shows, the assertions of Lemma 60 are true for any ordinary abelian variety A/K (in place of E^n/K). On the other hand, both statements are false for non-ordinary abelian varieties. In particular, if E is a supersingular elliptic curve, then already E^2 has infinitely many subgroup schemes which are isomorphic to α_p, and their cardinality equals the cardinality of K (and hence increases when we enlarge K).

This concludes the proof of Theorem 58 and hence also of Theorem 54, as was proven above. We next prove Theorem 3 of the introduction, which is an easy consequence of Theorem 54.

Proof of Theorem 3. If $A \simeq E_1 \times \ldots \times E_n$ with $E_i \sim E$, then by Corollary 53 we have $f_A = \mathrm{lcm}(f_{E_1}, \ldots, f_{E_n})$. By Proposition 36 there exists an elliptic curve $E_0 \sim E$ with $f_{E_0} = \mathrm{lcm}(f_{E_1}, \ldots, f_{E_n})$, and so $f_A = f_{E_0}$.

Conversely, suppose there exists $E_0 \sim E$ such that $f_A | f_{E_0}$. Then $A \sim E^n \sim E_0^2$, and so there is an isogeny $\pi : E_0^n \to A$. Put $H = \mathrm{Ker}(\pi)$. Then $(E_0^n)_H \simeq A$ and so $f_{\mathcal{E}(H)} = f_A | f_{E_0}$ by hypothesis. By Theorem 54 we therefore know that H is an ideal subgroup of E_0^n and so it follows from Proposition 57 that $A \simeq (E_0^n)_H \simeq E_1 \times \ldots \times E_n$, for some elliptic curves $E_1, \ldots, E_n \sim E_0$.

Next we shall use Theorem 3 to prove Theorem 2 of the introduction.

Proof of Theorem 2. If the field K is algebraically closed, then this is Theorem 58. Thus, assume that K is a finite field.

Let $h_{A/K}(X) \in \mathbb{Z}[X]$ (respectively, $m_{A/K}(X) \in \mathbb{Z}[X]$) denote the characteristic polynomial (respectively, minimal polynomial) of the Frobenius endomorphism ϕ_A of A/K. Since $A \sim E^n$, we have $h_{A/K}(X) = h_{E/K}(X)^n$ and $m_{A/K}(X) = m_{E/K}(X)$. Note that $m_{E/K} = h_{E/K}$ is irreducible over $\mathbb{Q}$ since E/K is a CM elliptic curve.

Since $\phi_A \in Z(\mathrm{End}(A)) \subset Z(\mathrm{End}^0(A)) \simeq F = \mathrm{End}^0(E)$, we see that $\mathbb{Z}[\phi_A]$ is an order in F (because $m_{A/K}$ is irreducible of degree 2). Thus, since $\mathbb{Z}[\phi_A] \subset Z(\mathrm{End}(A))$, it follows that $f_A | f_{\mathbb{Z}[\phi_A]}$. Now by Waterhouse (cf. Proposition 34 above) there is an elliptic curve E_0/K with $E_0 \sim E$ such that $\Delta_{E_0} = \Delta(h_{E/K})$. Thus, since the discriminant of the order $\mathbb{Z}[\phi_A]$ is $\Delta(m_{A/K}) = \Delta(h_{E/K})$, we see that $f_{\mathbb{Z}[\phi_A]} = f_{E_0}$ and that hence $f_A | f_{E_0}$. It therefore follows from Theorem 3 that $A \simeq E_1 \times \ldots \times E_n$, for some elliptic curves $E_1, \ldots, E_n \sim E_0 \sim E$.

We now turn to the proof of Theorem 5 of the introduction.

Proof of Theorem 5. We will construct bijections between the various sets defined by the conditions (i) – (v).

(i) $\leftrightarrow$ (ii): Let $(E'; f_1, \ldots, f_{n-2})$ be a tuple as in (i), and put $\varphi_1(E'; f_1, \ldots, f_n) = (I_E(E'); f_1, \ldots, f_{n-2})$. Since $f_{E'} | f_E$, we know by (46) that if $\pi : E \to E'$ is any isogeny, then $\mathrm{Ker}(\pi) = H(I)$ for some ideal I of $\mathrm{End}(E)$. Thus $I_E(E') \simeq I$ because I is a kernel ideal by Theorem 18(a) and also $\mathrm{End}(E') \simeq \mathrm{End}(E_{H(I)}) \simeq R(I)$ by (49). Thus $f_{E'} = f_{R(I)}$, and so $(I_E(E'); f_1, \ldots, f_{n-2})$ is in the set described by condition (ii). By Corollary 19 we thus see that φ_1 defines a bijection between sets (i) and (ii).

(ii) $\leftrightarrow$ (iii): If $(I; f_1, \ldots, f_{n-2})$ is a tuple as in (ii), and put $\varphi_2(I; f_1, \ldots, f_{n-2}) = (q_\Delta(I); f_1/f_I, \ldots, f_{n-2}/f_I)$, where q_Δ is the bijection constructed in Remark 38 and $f_I = f_{R(I)}$. Here $R_\Delta \simeq \mathrm{End}(E)$ (because E has discriminant Δ). By construction, $q_\Delta(I)$ has content $\mathrm{cont}(q_\Delta(I)) = [R(I) : R_\Delta] = f_E/f_{R(I)}$, and so we see that $(q_\Delta(I); f_1/f_I, \ldots, f_{n-2}/f_I)$ is in the set described by condition (iii) and that φ_2 is a bijection.

(ii) $\leftrightarrow$ (iv): This is Corollary 48.

(iv) $\leftrightarrow$ (v): For an R-module M as in (iv), put $\varphi_4(M) = T_{E,n}^{-1}(\mathcal{I}_n(M))$, which is a regular left $\mathrm{End}(E^n)$-ideal. By Proposition 40 and Proposition 51 we know that φ_4 induces a bijection between the set described by (iv) and the following set:

(iv′) the set of isomorphism classes of regular left ideals I of $\mathrm{End}(E^n) \simeq M_n(R)$ with $Z((I : I)) = R$.

Next, if I is an ideal as in (iv′), then put $\varphi_5(I) = A_I := E^n_{H(I)}$. Since I is a kernel ideal by Proposition 52, we have that $\mathrm{End}(A_I)) \simeq (I : I)$, and so $Z(\mathrm{End}(A_I)) = Z((I : I)) = R = \mathrm{End}(E)$, which means that $f_{A_I} = f_E$. Thus the isomorphism class of A_I is an element of the set described by (v). By (19) and the sentence before (21) we know that φ_5 defines an injection from the set described by (iv′) into the set (v). Finally, this map is surjective. Indeed, if $A \sim E^n$ with $f_A = f_E$, and if $\pi : E^n \to A$ is any isogeny, then by Theorem 54 we know that H is an ideal subgroup, so $\mathrm{Ker}(\pi) = H(I)$

for some regular left ideal I of $\mathrm{End}(E^n)$. Thus $A \simeq E^n_{H(I)}$. Furthermore, by the above computation we have $Z((I:I)) = R$, and so I is in the set defined by condition (iv′).

Remark 62 (a) It is sometimes useful to have a direct description of the bijection between the sets defined by conditions (i) and (v) of Theorem 5. Indeed, if we unravel the bijections constructed in the proof of Theorem 5, then we obtain that this bijection is given by the rule $(E'; f_1, \ldots, f_{n-2}) \mapsto A(E'; f_1, \ldots, f_{n-2}; E)$, where

$$A(E'; f_1, \ldots, f_{n-2}; E) := E' \times E_1 \times \ldots \times E_{n-2} \times E, \tag{102}$$

where $E_i = E_{H(f_E R_i)}$ and $f_{R_i} = f_i$. To verify this, note first that the bijection is given by $\varphi_5 \circ \varphi_4 \circ \mu_{R,n} \circ \varphi_1$ in the notation of the proof of Theorem 5. Thus, if we put $I_1 = I_E(E')$, $I_{i+1} = f_E R_i$ for $i = 1, \ldots, n-2$ and $I_n = R$, then $\mu_{R,n}(\varphi_1\varphi_1(E', f_1, \ldots, f_{n-2}) = I_1 \oplus \ldots \oplus I_n$. On the other hand, $\varphi_5(\varphi_4(I_1 \oplus \ldots \oplus I_n)) = \varphi_5((I_1 : \ldots : I_n)) = E_{H(I_1)} \times \ldots \times E_{H(I_n)}$ by Proposition 41, and so the assertion follows.

(b) The bijections of Theorem 5 yield immediately a classification of all abelian varieties $A \sim E^n$ with $f_A | f_E$. More precisely, we have natural bijections between the follow sets:

(i) *The set of sequences* $(E'; f_1, \ldots, f_{n-1})$ *where* $E' \sim E$ *is an isomorphism class of elliptic curves with* $f_{E'} | f_E$ *and the* f_i*'s are positive integers with* $f_{E'} | f_1 | \ldots | f_{n-1} | f_E$.

(ii) *the set of sequences* $(I; f_1, \ldots, f_{n-1})$ *where* I *is an isomorphism class of non-zero* $\mathrm{End}(E)$*-ideals whose order* $R(I)$ *has conductor* $f_{R(I)} | f_1 | \ldots | f_{n-1} | f_E$.

(iii) *the set of sequences* $(q; c_1, \ldots, c_{n-2})$ *where* q *is a proper equivalence class of positive binary quadratic forms of discriminant* $\Delta(q) = \Delta/m^2$*, for some* $m \in \mathbb{N}$*, and* $c_1 | \ldots | c_{n-2} | \mathrm{cont}(q)$.

(iv) *the set of isomorphism classes of* $\mathrm{End}(E)$*-submodules* M *of* $\mathrm{End}(E)^n$ *of rank* n*;*

(v) *the set of isomorphism classes of abelian varieties* $A \sim E^n$ *with central conductor* $f_A | f_E$.

4.4 Abelian product surfaces

We now specialize the previous results to the case of abelian *surfaces*, i.e. to the case $n = 2$. In particular, we shall prove Theorem 4 and show how the results of Shioda and Mitani[24] follow from the above theorems.

We begin with the following refinement of Theorem 1 (in the case $n = 2$) which is closely related to Proposition 4.5 of [24].

Proposition 63 *Let* $E_1, E_2, E_1', E_2' \in \mathrm{Isog}^+(E/K)$*, where* E/K *is a CM elliptic curve, and put* $f_i = f_{E_i}$ *and* $f_i' = f_{E_i'}$*. Then* $E_1 \times E_2 \simeq E_1' \times E_2'$ *if and only if*

$$\mathrm{lcm}(f_1, f_2) = \mathrm{lcm}(f_1', f_2') \text{ and } I_E(E_1) I_E(E_2) \simeq I_E(E_1') I_E(E_2').$$

Proof. To prove this, we shall use the criterion of Theorem 1. Now by Proposition 49 we have that $I_E(E_1) \oplus I_E(E_2) \simeq I_E(E_1') \oplus I_E(E_2') \Leftrightarrow R \oplus I_E(E_1)I_E(E_2) \simeq R' \oplus I_E(E_1')I_E(E_2')$, where $R = R(I_E(E_1)) \cap R(I_E(E_2))$ and $R' = R(I_E(E_1')) \cap R(I_E(E_2'))$. Moreover, by Theorem (45) these modules are isomorphic if and only $R = R'$ and $I_E(E_1)I_E(E_2) \simeq I_E(E_1')I_E(E_2')$. Since $R(I_E(E_i))$ has conductor f_i by (50), we see that R has conductor $f_R = \mathrm{lcm}(f_1, f_2)$ by (37), and similarly $f_{R'} = \mathrm{lcm}(f_1', f_2')$. Thus $R = R'$ if and only if $\mathrm{lcm}(f_1, f_2) = \mathrm{lcm}(f_1', f_2')$, and so the assertion follows from Theorem 1.

If $K = \mathbb{C}$, then above result can be restated in the following form which is essentially Proposition 4.5 of [24].

Corollary 64 *Let $L_1, L_2, L_1', L_2' \in \mathrm{Lat}_F$ be lattices in a quadratic field F and let $f_i = f_{R(L_i)}$ and $f_i' = f_{R(L_i')}$ be the conductors of their associated orders. Then*

$$E_{L_1} \times E_{L_2} \simeq E_{L_1'} \times E_{L_2'} \quad \Leftrightarrow \quad L_1L_2 \simeq L_1'L_2' \text{ and } \mathrm{lcm}(f_1, f_2) = \mathrm{lcm}(f_1', f_2').$$

Proof. Put $E_i = E_{L_i}$ and $E_i' = E_{L_i'}$. Since $\mathrm{End}(E_{L_i}) \simeq R(L_i)$ by (64), we have $f_{E_i} = f_i$ and similarly $f_{E_i'} = f_i'$. Let $R = R(L_1) \cap R(L_2) \cap R(L_1') \cap R(L_2')$, and choose $n \in \mathbb{N}$ such that $L := nR \subset L_i \cap L_i'$, for $i = 1, 2$. Put $E = E_L$. Since $\mathrm{End}(E) \simeq R \subset R(L_i) \simeq \mathrm{End}(E_{L_i})$, we see that $E_i \in \mathrm{Isog}^+(E/\mathbb{C})$ and similarly $E_i' \in \mathrm{Isog}^+(E/\mathbb{C})$. By Corollary 27 we have $I_E(E_i) \simeq L_i^{-1}L$ and $I_E(E_i') \simeq (L_i')^{-1}L$. Thus $I_E(E_1)I_E(E_2) \simeq I_E(E_1')I_E(E_2') \Leftrightarrow L_1^{-1}L_2^{-1}L \simeq (L_1')^{-1}(L_2')^{-1}L \Leftrightarrow (L_1L_2)^{-1} \simeq (L_1'L_2')^{-1}$, the latter because $R(L) \subset R(L_1^{-1}) \cap R((L_1')^{-1})$. Thus $I_E(E_1)I_E(E_2) \simeq I_E(E_1')I_E(E_2') \Leftrightarrow L_1L_2 \simeq L_1'L_2'$, and hence it is clear that the corollary follows from Proposition 63.

We next prove Theorem 4, which is clearly a special case of the following more precise result.

Theorem 65 *Let E/K be a CM elliptic curve of discriminant $\Delta = \Delta_E$. Then there exist bijections between the following sets:*

(i) *the set* $\mathrm{Isog}^+(E/K)$ *of isomorphism classes of elliptic curves E'/K with $E' \sim E$ and $f_{E'} | f_E$;*

(ii) *the set of non-zero ideal classes of* $\mathrm{End}(E)$*;*

(iii) *the set of proper equivalence classes of positive definite binary quadratic forms q with discriminant $\Delta(q) = \Delta$;*

(iv) *the set of* $\mathrm{End}(R)$*-submodules M of* $\mathrm{End}(E)^2$ *of rank 2 with $R_F(M) = R$;*

(v) *the set of isomorphism classes of abelian surfaces A/K with $A \sim E^2$ and central conductor $f_A = f_E$;*

(vi) *the set of isomorphism classes of abelian surfaces A/K with $A \sim E^2$ and discriminant $\Delta(A/K) = -\Delta$.*

More precisely, the bijection between (i) *and* (ii) *is given by the map* I_E^+ *of* Corollary 19*, the bijection between* (ii) *and* (iii) *is the map* q_Δ *of* Remark 38*, the bijection between* (iv) *and* (v) *is given by the rule* $M \mapsto (E^2)_{H(T_{E,2}^{-1}(\mathcal{I}_n(M)))}$*, and the sets* (v) *and* (vi) *are identical. In addition, the bijection between* (i) *and* (v) *and* (vi) *is induced by the rule* $E' \mapsto E \times E'$*.*

Remark 66 Note that the bijection between the sets described by conditions (iii) and (vi) of Theorem 65 (which is the same as that between the sets (i) and (ii) of Theorem 4) is not given explicitly. However, it can be described as follows: given $q \in Q_{\Delta_E}/\mathrm{SL}_2(\mathbb{Z})$, let $E'_q = E'_{E,q} \in \mathrm{Isog}^+(E/K)$ be such that $q^+_{E,E'_q} = q$, where $q^+_{E,E'}$ is as in Remark 38. Then the map $q \mapsto A_q = E \times E'_q$ induces the bijection between the sets (iii) and (vi).

Proof. The equivalence of conditions (i) – (v) is just a restatement of Theorem 5 in the case $n = 2$. Moreover, by the proof of that theorem and by Remark 62(a) we know that the bijections are as indicated.

It thus remains to show that the sets (v) and (vi) are identical. For this, suppose first that condition (v) holds. Then by what was just said, it follows that $A \simeq E' \times E$, for some $E' \in \mathrm{Isog}^+(E/K)$. Thus $f_A = \mathrm{lcm}(f_{E'}, f_E) = f_E$ by Corollary 53. It thus follows from Proposition 67 below that $\Delta(A/K) = -f_A^2\Delta_F = -f_E^2\Delta_F = -\Delta$, and so condition (vi) holds.

Conversely, suppose that condition (vi) holds. Since $\Delta(A/K) = -\Delta_E$, it follows from Proposition 67 below that $\Delta(A/K) = -f_A^2\Delta_F$, and so $f_A = f_E$ because $\Delta_E = f_E^2\Delta_F$. Thus condition (v) holds.

In the above proof we had used the following fact.

Proposition 67 *Let* A/K *be abelian surface which is isogenous to* $E \times E$*, where* E/K *is a CM elliptic curve. Then there is an integer* m *such that the discriminant of* A/K *is* $\Delta(A/K) = -m^2 f_A^2 \Delta_F$*, where* $F = \mathrm{End}^0(E)$*. Moreover,* $m = 1$ *if there exists an elliptic curve* $E_0 \sim E$ *such that either* $f_A | f_{E_0}$ *or such that* $\Delta(A/K) | \Delta_{E_0}$*.*

Proof. Suppose first that $A \simeq E_1 \times E_2$, for some CM elliptic curves E_i/K which are isogenous. Then by [16], Proposition 22, we have $\mathrm{NS}(A \otimes \overline{K}) \simeq \mathbb{Z}^2 \oplus \mathrm{Hom}(\overline{E}_1, \overline{E}_2)$, where $\overline{E}_i = E_i \otimes \overline{K}$. Moreover, since $\mathrm{Hom}(E_1, E_2) = \mathrm{Hom}(\overline{E}_1, \overline{E}_2)$, the explicit isomorphism shows that $\mathrm{NS}(A) = \mathrm{NS}(A \otimes \overline{K})$; cf. [17], (proof of) Lemma 63. Let q_A be the intersection form on $\mathrm{NS}(A)$, i.e. $q_A(D) = \frac{1}{2}(D.D)$, where $(D.D)$ denotes the self-intersection number of a divisor (class) $D \in \mathrm{NS}(A)$. Then by [16], Proposition 22 (or [17], equation (6)) we have

$$q_A \sim xy \perp q_{E_1,E_2}, \tag{103}$$

where xy denotes the quadratic form associated to the hyperbolic plane and q_{E_1,E_2} is as in §3.4. From (103) it follows immediately that

$$\Delta(q_A) \;=\; -\Delta(q_{E_1,E_2}) \;=\; -\mathrm{lcm}(f_{E_1}, f_{E_2})^2\Delta_F \;=\; -f^2_{E_1\times E_2}\Delta_F, \tag{104}$$

where the last two equations follow from equation (80) and Corollary 53, respectively. Thus, the asserted formula holds in this case (with $m = 1$).

Next, suppose that there exists an elliptic curve E_0 such that $f_A | f_{E_0}$. Then by Corollary 16 there is an elliptic curve $E_1 \sim E_0$ such that $f_A = f_{E_1}$, and then by Theorem 5 there exists $E' \in \mathrm{Isog}^+(E_1/K)$ such that $A \simeq E' \times E_1$. Thus, the assertion follows from the previously discussed case.

Now suppose that A/K is any abelian surface with $A \sim E^2$. Then $\mathrm{NS}(A)\otimes\mathbb{Q} \simeq \mathrm{NS}(E^2)\otimes\mathbb{Q} = \mathrm{NS}(E^2\otimes\overline{K})\otimes\mathbb{Q}$, the latter by the discussion at the beginning of this proof. Thus $\mathrm{NS}(A)\otimes\mathbb{Q} = \mathrm{NS}(\overline{A})\otimes\mathbb{Q}$, where $\overline{A} := A\otimes\overline{K}$, and so $m := [\mathrm{NS}(\overline{A}) : \mathrm{NS}(A)] < \infty$. It thus follows that $\Delta(A/K) = m^2\Delta(\overline{A}/\overline{K})$. Now by Theorem 58 we have that $\overline{A} \simeq \overline{E}_1 \times \overline{E}_2$ for some elliptic curves $\overline{E}_i \sim E\otimes\overline{K}$, and so by the previously discussed case we have $\Delta(\overline{A}/\overline{K}) = -f^2_{\overline{A}}\Delta_F$. Since $f_A = f_{\overline{A}}$ (as was explained in the proof of Theorem 54), we obtain that $\Delta(A/K) = -m^2 f_A^2\Delta_F$, as claimed.

Finally, suppose that $\Delta(A/K)|\Delta_{E_0} = f^2_{E_0}\Delta_F$, for some elliptic curve E_0/K. Since we have that $\Delta(A/K) = -m^2 f_A^2\Delta_F$ by what was just shown, we see that $mf_A = f_{E_0}$ and so $f_A | f_{E_0}$. But in this case we showed above that we must have $m = 1$.

In view of the close relationship (103) that exists between the quadratic form q_A defined by the intersection pairing on $\mathrm{NS}(A)$ and the form $q^+_{E,E'}$ which defines the one of the bijections of Theorem 65 (cf. Remark 66), it might be tempting to try to use q_A in place of $q^+_{E,E'}$ to classify the abelian surfaces A/K with $A \sim E^2$. This, however, does not lead to a bijection, as the following result shows.

Corollary 68 *Let E/K be a CM elliptic curve with discriminant $\Delta = \Delta_E$, and let $q \in Q_\Delta$ be a positive binary quadratic form of discriminant Δ and content c. Then the number*

$$N_q \;:= \#(\{A \sim E\times E : q_A \sim xy \perp (-q)\}/\simeq)$$

of isomorphism classes of abelian surfaces A/K which are isogenous to E^2 and whose intersection form q_A is equivalent to $xy \perp (-q)$ is equal to the number of primitive forms in the principal genus of primtive forms of discriminant $\Delta' = \Delta/c^2$. Thus, if $g(\Delta')$ denotes the number of genera of discriminant Δ', then we have

$$N_q \;=\; \frac{h(\Delta')}{g(D')}, \quad \textit{where } \Delta' = \Delta(q)/\mathrm{cont}(q)^2. \tag{105}$$

Proof. Let q^A denote the (proper) equivalence class of binary forms of discriminant Δ which corresponds to A/K via the bijection of Theorem 65. Then by (103) and (83)

we have $q_A \sim xy \perp (-q^A)$. Thus, $q_A \sim xy \perp (-q) \Leftrightarrow xy \perp (-q^A) \sim xy \perp (-q) \Leftrightarrow q^A$ and q are in the same genus, the latter by Remark 27 of [17]. Since the number of such forms q^A equals the number of forms in the principal genus (and is given by the formula of (105)), the assertion follows.

We also note that the above Proposition 67 allows us to reformulate Theorem 3 in the case of surfaces as follows.

Theorem 69 *Let A/K be an abelian suface which is isogenous to $E \times E$, where E/K is a CM elliptic curve. Then there exist CM elliptic curves $E_1, E_2/K$ such that $A \simeq E_1 \times E_2$ if and only if $\Delta(A/K)|\Delta_{E_0}$, for some elliptic curve E_0/K with $E_0 \sim E$.*

Proof. If $A \simeq E_1 \times E_2$, then by Theorem 3 we know that $f_A | f_{E_0}$, for some $E_0 \sim E$. Thus, by (104) we have that $\Delta(A/K) = -f_A^2 \Delta_F | f_{E_0}^2 \Delta_F = \Delta_{E_0}$, as claimed.

Conversely, suppose that $\Delta(A/K)|\Delta_{E_0}$, for some $E_0 \sim E$. Then by Proposition 67 we have that $\Delta(A/K) = -f_A^2 \Delta_F$, and so it follows that $f_A | f_{E_0}$. By Theorem 3 we thus obtain that $A \simeq E_1 \times E_2$, for some elliptic curves $E_1, E_2/K$.

From the above Theorem 4 (or from Theorem 65) we can deduce the following result which is essentially the same as Theorem 3.1 of [24]:

Theorem 70 *Let K be an algebraically closed field of characteristic 0. Then there is a bijection between the following sets:*

(i) *the set $Q/\mathrm{SL}_2(\mathbb{Z})$ of proper equivalence classes of positive definite binary quadratic forms;*

(ii) *the set of isomorphism classes of abelian surfaces A/K with Picard number $\rho(A) := \mathrm{rank}(\mathrm{NS}(A)) = 4$.*

Remark 71 In the paper [24], the abelian surfaces $A/\mathbb{C}$ with $\rho(A) = 4$ are called *singular abelian surfaces*; cf. [24], p. 459. This terminology unfortunately conflicts with classical terminology of *singular abelian varieties* used in the 19th century: these are abelian varieties with the property that $\mathrm{End}(A) \neq \mathbb{Z}$; cf. Hurwitz[15], p. 167, 187 (and the references therein) and Humbert [14].

Proof of Theorem 70. It follows from the classification theory of endomorphisms of simple abelian surfaces in characteristic 0 (cf. [20], p. 202) that if $\rho(A) = 4$, then A cannot be simple and so one sees easily that $A \sim E^2$, where E/K is a CM elliptic curve. Thus the set (ii) is the same as the set

(ii′) *the set of isomorphism classes of abelian surfaces A/K with $A \sim E^2$, for some CM elliptic curve E/K.*

To describe the bijection, fix for each discriminant $\Delta < 0$ an elliptic curve E_Δ with $\Delta_{E_\Delta} = \Delta$ (which exists by Proposition 33(a)). Let

$$\mathcal{A}(\Delta) \ := \ \{A/K : A \sim E_\Delta^2 \text{ and } \Delta(A/K) = -\Delta\}/\simeq$$

denote the set of isomorphism classes of abelian surfaces A/K which are isogenous to $E_\Delta \times E_\Delta$ and have discriminant $\Delta(A/K) = -\Delta$. Now if $A \sim E^2$, where E/K is some CM curve and if $\Delta(A/K) = -\Delta$, then it follows from Theorem 65 that $E \sim E_\Delta$, and so we see that the set $\mathcal{A}$ described by (ii′) is the disjoint union of the sets $\mathcal{A}(\Delta)$, where Δ runs over all negative discriminants. We thus see from Remark 66 that the rule $q \mapsto E_\Delta \times E'_{E_\Delta, q}$ (notation as in Remark 66) induces the desired bijection

$$Q/\mathrm{SL}_2(\mathbb{Z}) \;=\; \dot{\bigcup_{\Delta<0}} Q_\Delta/\mathrm{SL}_2(\mathbb{Z}) \quad \tilde{\to} \quad \dot{\bigcup_{\Delta<0}} \mathcal{A}(\Delta) \;=\; \mathcal{A}.$$

Remark 72 The same argument as above shows that if K is an algebraically closed field of characteristic $p \neq 0$, then we have a bijection between the following two sets:

(i) the set $Q^{(p)}/\mathrm{SL}_2(\mathbb{Z})$ of proper equivalence classes of positive definite binary quadratic forms whose discriminant Δ satisfies $(\frac{\Delta}{p}) = 1$;

(ii) the set of isomorphism classes of abelian surfaces A/K such that $A \sim E^2$, for some CM elliptic curve E/K.

References

[1] Z. Borevich, D. Faddeev, Representations of orders with cyclic index. *Trudy Mat. Inst. Steklov = Proc. Steklov Inst. Math.* **80** (1965), 51–65.

[2] Z. Borevich, D. Faddeev, A note on orders with cyclic index. *Dokl. Akad. Nauk SSSR* **164** (1965), 727–728 = *Soviet Math. Doklady* **6** (1965), 1273–1274.

[3] Z. Borevich, I. Shafarevich, *Number Theory.* Academic Press, New York, 1966.

[4] S. Bosch, W. Lütkebohmert, M. Raynaud, *Néron Models.* Springer-Verlag, Berlin, 1990.

[5] N. Bourbaki, *Commutative Algebra, Ch. I-VII.* Addison-Wesley, Reading, 1972.

[6] J. Buchmann, U. Vollmer, *Binary Quadratic Forms.* Springer, Berlin, 2007.

[7] D. Cox, *Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory and Complex Multiplication.* Wiley, New York, 1989.

[8] C. Curtis, I. Reiner, *Methods of Representation Theory I.* J. Wiley & Sons, New York, 1981.

[9] P. Deligne, Variétés abéliennes ordinaires sur un corps fini. *Invent. Math.* **6** (1969), 238-243.

[10] M. Deuring, Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. *Abh. Math. Sem. Hamburg* **14** (1941), 197–272.

[11] R. Hartshorne, *Algebraic Geometry.* Springer-Verlag, New York, 1977.

[12] F. Hirzebruch, D. Zagier, Intersection numbers of curves on Hilbert modular surfaces and modular forms of Nebentypus. *Invent. math.* **36** (1976), 57–113 = *Gesammelte Abh./Coll. Papers* II, Springer-Verlag, Berlin, 1987, pp. 409–465.

[13] E. W. Howe, Principally polarized ordinary abelian varieties over finite fields. *Trans. Amer. Math. Soc.* **347** (1995), 2361-2401.

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

[15] A. Hurwitz, Über algebraische Korrespondenzen und das verallgemeinerte Korrespondenzprinzip. *Math. Ann.* **28** (1887), 561–585 = *Math. Werke* I, Birhäuser, Basel, 1932, pp. 163 – 188.

[16] E. Kani, The moduli spaces of Jacobians isomorphic to a product of two elliptic curves. Preprint, 39 pages.

[17] E. Kani, The existence of Jacobians isomorphic to a product of two elliptic curves. *Inst. Exp. Math., Essen*, Universität Duisburg-Essen, IEM Preprint No. 3–2009, 36 pages.

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

[19] H. Lange, Produkte elliptischer Kurven. *Nachr. Akad. Wiss. Göttingen Math.-Phys. Kl. II* (1975), 95–108.

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

[21] W. Ruppert, When is an abelian surface isomorphic or isogenous to a product of elliptic curves? *Math. Z.* **203** (1990), 293–299.

[22] C. Schoen, Produkte abelscher Varietäten und Moduln über Ordnungen. *J. reine angew. Math.* **429** (1992), 115–123.

[23] G. Shimura, Y. Taniyama, *Complex Multiplication of Abelian Varieties*. Math. Soc. Japan, Tokyo, 1961.

[24] T. Shioda, N. Mitani, Singular abelian surfaces and binary quadratic forms. In: *Classification of algebraic varieties and compact complex manifolds*. Lect. Notes Math. **412** (1974), 259–287.

[25] E. Steinitz, Zur Theorie der Moduln. *Math. Ann.* **52** (1899), 1–57.

[26] W.C. Waterhouse, Abelian varieties over finite fields. *Ann. Sci. École Norm. Sup.* (4), **2** (1969), 521-560.