Elliptic Subcovers of a Curve of Genus 2 I. The Isogeny Defect

Ernst Kani

1 Introduction

Let C be a curve of genus 2 over an arbitrary field K. An *elliptic subcover* is a finite morphism $f : C \to E$ to an elliptic curve E/K which does not factor over a non-trivial isogeny of E. If $f' : C \to E'$ is another elliptic subcover, then f' is said to be *equivalent* to f if there is an isomorphism $\varphi : E \xrightarrow{\sim} E'$ such that $f' = \varphi \circ f$.

The purpose of this paper is to study the set $\mathcal{E}(C)$ of all equivalence classes of elliptic subcovers of a given genus 2 curve C. This is equivalent to studying the set of maximal elliptic subfields of the function field $F = \kappa(C)$ of C. It is well-known that $\mathcal{E}(C)$ has either 0 or 2 or infinitely many elements; this fact (for $K = \mathbb{C}$) was first noticed by Picard and Bolza; cf. Krazer[12], pp. 487-489.

Here we want to study the case that C has infinitely many elliptic subcovers. This happens precisely when the Jacobian J_C of C is K-isogenous to $E \times E$, for some elliptic curve E/K.

A first step towards the problem of understanding $\mathcal{E}(C)$ was taken in [4] in the case that $K = \overline{K}$ is algebraically closed. In that paper it was explained that a certain positive quadratic form q_C, called the *refined Humbert invariant* in [8], gives a (theoretical) description of $\mathcal{E}(C)$, for it establishes a bijection between the set $\mathcal{E}_n(C)$ of elliptic subcovers of degree n and the set of primitive solutions $\mathbf{x}$ of $q_C(\mathbf{x}) = n^2$, for $n \in \mathbb{N}$; cf. [4], Theorem 4.5. Here we extend this result to an arbitrary base field; cf. Theorem 20. In particular, we have

Theorem 1 *The curve C/K has an elliptic subcover of degree n if and only if the refined Humbert invariant q_C primitively represents n^2.*

However, in order to be able to apply this theorem to concrete situations, it is necessary to be able to compute the refined Humbert invariant q_C explicitly. The main objective of this paper and of its sequel [10] is to present a method for computing q_C. As a first step, we compute here the discriminant of the quadratic form q_C and then use this formula in [10] to compute q_C itself.

The method presented here depends on the knowledge of a "presentation (E, E', ψ) of degree N" of C/K which arises from a given elliptic subcover $f : C \to E$ of degree N. This triple consists of E, another (isogenous) elliptic curve E'/K and an

isomorphism $\psi : E[N] \to E'[N]$ which is an anti-isometry with respect to the e_N-pairings; cf. Section 2. Attached to ψ is an important invariant called the *isogeny defect* m_ψ which is defined as follows:

$$m_\psi := \min\{m \geq 1 : m\psi = h_{|E[N]}, \text{ for some } h \in \mathrm{Hom}(E, E')\}.$$

The results are most complete (and easiest to state) when $\mathrm{rank}(\mathrm{Hom}(E, E')) = 1$. In this case we have:

Theorem 2 *Suppose that C/K is a curve which has a presentation (E, E', ψ) of degree N with $\mathrm{char}(K) \nmid N$, and let $m = m_\psi$ be its isogeny defect. If $\mathrm{Hom}(E, E') = \mathbb{Z}h$, where $d := \deg(h) \geq 1$, then the refined Humbert invariant q_C is a positive definite binary quadratic form which has the following properties:*

(i) $\mathrm{disc}(q_C) = -16m^2d$, *and* $m|N$ *with* $(N/m, d) = 1$.

(ii) q_C *primitively represents* N^2;

(iii) $q_C(X, Y) \equiv 0, 1 \pmod 4$, *for all* $X, Y \in \mathbb{Z}$;

(iv) $q_C(X, Y) \neq 1$, *for all* $X, Y \in \mathbb{Z}$.

This theorem is proved at the end of Section 5, using the important Index Formula of Theorem 27 which is proved in Section 6.

In the second part[10] of this paper, Theorem 2 is made more precise by giving an explicit formula for m_ψ and for q_C in terms of an N-presentation (E, E, ψ) of C/K. In addition, we use this to prove that every binary quadratic form q satisfying properties (i)–(iv) is equivalent to) the refined Humbert invariant q_C of some curve C/K, when K is algebraically closed.

In the general case when $r = \mathrm{Hom}(E, E') \geq 1$, there is a result which is similar to Theorem 2. To state it, let $q_{E,E'}$ denote the degree quadratic form of $\mathrm{Hom}(E, E')$ which is defined by $q_{E,E'}(h) = \deg(h)$, for $h \in \mathrm{Hom}(E, E')$, and let $d_{E,E'}$ denote its determinant.

Theorem 3 *If C/K has a presentation (E, E', ψ) of degree N with $\mathrm{char}(K) \nmid N$ and isogeny defect $m = m_\psi$, and if $r = \mathrm{rank}(\mathrm{Hom}(E, E')) \geq 1$, then the refined Humbert invariant q_C is a positive definite quadratic form of rank $r + 1$ which satisfies (the analogues of) properties* (ii)-(iv) *of* Theorem 2*, as well as the following property:*

(i′) $\det(q_C) = 2^{2r+1}m^2d_{E,E'}$.

It is interesting to note that (the proof of) Theorem 3 allows us to prove the following (partial) characterization of Jacobians which are isomorphic to a product $E \times E'$. Such Jacobians were studied in [8], [7] and also indirectly in [6]. One direction of this characterization was proven by Diem and Frey[1].

Theorem 4 *If (E, E', ψ) is a presentation of degree N of a curve C/K of genus 2 with $\mathrm{char}(K) \nmid N$, then $m_\psi = 1$ if and only if $J_C \simeq E \times E'$.*

Corollary 5 *If C/K has an elliptic subcover $f : C \to E$ with $\mathrm{char}(K) \nmid \deg(f)$, if the Picard number $\rho = \mathrm{rk}(\mathrm{NS}(J_C)) \geq 3$, and if $\det(q_C)/2^{2\rho-3}$ is squarefree, then $J_C \simeq E \times E'$, for some elliptic curve E'/K.*

This paper is organized as follows. In Section 2 we first recall from [9] the basic relation between elliptic subcovers of C/K and elliptic subgroups of J_C/K; cf. Theorem 7. Next we introduce and study the notion of an N-presentation (E, E', ψ); cf. Proposition 10. Note that this notion is closely related to the "basic construction" of [2], [3] and [5].

In Section 3 we extend the definition of the refined Humbert invariant q_C for a genus 2 curve $C/\overline{K}$ over an algebraically closed field $\overline{K}$ (cf. [4], [7], [8]) to a curve C/K over an arbitrary base field K. To do this, one has to replace the usual Néron-Severi group $\mathrm{NS}(J_C)$ by a slightly larger group $\mathrm{NS}'(J_C)$ which is isomorphic to a certain additive subgroup $\mathrm{End}_\lambda(J_C)$ of $\mathrm{End}(J_C)$; cf. Proposition 14. One then obtains the above-mentioned bijection of elliptic subcovers and (certain) primitive solutions of q_C; cf. Theorem 20.

In Section 4 we introduce and study the *isogeny defect* of an anti-isometry ψ in a slightly more general setting than above. For use in the next sections, we also define and derive some properties of the *trace* $\mathrm{tr}(g)$ of an endomorphism $g \in \mathrm{End}(E[N])$.

The main structure theorems (Theorems 2 and 3) are proved in Sections 5 and 6. More precisely, in Section 5 we show how these results follow from the Index Theorem 27, which is then proved in Section 6. In the proof of the Index Theorem, we exploit the connection between the (extended) Néron-Severi group $\mathrm{NS}'(J_C)$ and the group $\mathrm{End}_\lambda(J_C)$ of symmetric endomorphisms.

Acknowledgment. I would like to thank the referee for his/her useful comments and suggestions. In addition, I gratefully acknowledge receipt of funding from the Natural Sciences and Engineering Research Council of Canada (NSERC).

2 Elliptic subcovers

Let C/K be a (smooth, projective, geometrically connected) curve of genus 2 over an arbitrary field K. In this section we briefly review some of the basic properties of elliptic subcover $f : C \to E$ of C/K; cf. [4], [5] and [9].

An *elliptic subcover* of C/K is a finite K-morphism $f : C \to E$ to an elliptic curve E/K which does not factor over a non-trivial isogeny of E/K. If f has the property that its base-change $f_{\overline{K}} : C_{\overline{K}} \to E_{\overline{K}}$ to the algebraic closure $\overline{K}$ of K is an elliptic subcover, then we call f a *geometric elliptic subcover*. Clearly, each geometric elliptic

subcover is an elliptic subcover, but the converse assertion is more subtle. However, it turns out that these two concepts are indeed equivalent, as was shown in [9]; cf. Corollary 8 below.

For much of what follows, it is important to note that this condition on f is equivalent to the condition that the induced map $f^* : J_E \to J_C$ on the Jacobians is a closed immersion. Here and below, we use the notations and basic facts about Jacobians as summarized the appendix of [5].

Proposition 6 *If $f : C \to E$ be a finite morphism to an elliptic curve E/K, then f is a geometric elliptic subcover if and only $f^* : J_E \to J_C$ is a closed immersion. If this is the case, then f is separable.*

Proof. The first assertion follows immediately from [4], Proposition 4.2, because $(f_{\overline{K}})^* = (f^*)_{\overline{K}}$ is a closed immersion if and only if f^* is a closed immersion. The second assertion follows from the fact that if f is inseparable, then $f_{\overline{K}}$ factors over an inseparable isogeny of $E_{\overline{K}}$; cf. [9], Proposition 2.2, for the details. □

As in the introduction (or as in [4]), two (geometric) elliptic subcovers $f_i : C \to E_i$ are said to be *equivalent* if there exists an isomorphism (of curves) $\varphi : E_1 \xrightarrow{\sim} E_2$ such that $f_2 = \varphi \circ f_1$. We then have the following general fact which generalizes Corollary 4.3 of [4].

Theorem 7 *The rule $f \mapsto f^* J_E$ defines a bijection*

$$\Phi_C : \mathcal{E}(C) \quad \xrightarrow{\sim} \quad \mathcal{S}(J_C)$$

between the set $\mathcal{E}(C)$ of equivalence classes of geometric elliptic subcovers of C and the set $\mathcal{S}(J_C)$ of elliptic subgroups $E \leq J_C$ of J_C.

Proof. (Sketch; details in [9]). The injectivity of Φ_C follows easily from Lemma 7.2 of [5]; cf. [9]. However, to prove that Φ_C is surjective is much harder, except in special cases. (For example, if C/K has a divisor of degree 1, then a variant of the proof of [4], Corollary 4.3, shows that the map is surjective.) The general case follows from [9], Theorem 1.1, which uses a descent argument based on the existence of normalized covers. Note that if $\mathrm{char}(K) \neq 2$, then this was already proven in [5]. □

Corollary 8 *If $f : C \to E$ is a finite morphism to an elliptic curve E/K, then f factors over a geometric elliptic subcover $f' : C \to E'$ which is unique up to equivalence. In particular, each elliptic subcover $f : C \to E$ is a geometric elliptic subcover.*

Proof. (Sketch; details in [9]). Put $H = \mathrm{Im}(f^*) \leq J_C$. By Theorem 7 there is a geometric elliptic cover $f' : C \to E'$ such that $(f')^* J_E = H$, and it is easy to see that $f = \nu \circ f'$, for some isogeny $\nu : E' \to E$; cf. [9], Corollary 1.2. □

Remark 9 It follows from Theorem 3.2(f) of [5] that the above bijection Φ_C takes elliptic subcovers $f : C \to E$ of degree N to elliptic subgroups of degree N with respect to the canonical polarization $\lambda_C : J_C \to \hat{J}_C$ in the sense of [5]; cf. equation (2) below.

We now explain how an elliptic subcover $f : C \to E$ gives rise to a "presentation" $(E, E_f^{\perp}, \psi_f)$ of C/K which will be used in the sequel. In view of the bijection of Theorem 7, this is a special case of a "presentation" attached to an elliptic subgroup $E \leq J$ of a principally polarized abelian surface (J, λ), so we will give the definition in this generality. For this, recall from [8] that if (A, λ) is any principally polarized abelian variety, then for every integer $N \geq 2$ we have the pairing (of K-group schemes)

$$e_N^{\lambda} \ := e^{N\lambda} : A[N] \times A[N] \to \mu_N.$$

Note that when $\mathrm{char}(K) \nmid N$, then we have by formula (5) on p. 232 of [16] that $e_N^{\lambda} = \overline{e}_N \circ (1 \times \lambda)$, where $\overline{e}_N : A[N] \times \hat{A}[N] \to \mu_N$ is the usual canonical pairing.

Definition. If $N \geq 2$, then an *N-presentation over K* is a triple (E, E', ψ) where E/K and E'/K are elliptic curves and $\psi : E[N] \to E'[N]$ is a K-isomorphism of finite group schemes which is an anti-isometry with respect to the e_N-pairings.

Moreover, if (J, λ) is a principally polarized abelian surface over K, then a *presentation of (J, λ) of degree N over K* is a 4-tuple (E, E', ψ, π) such that (E, E', ψ) is an N-presentation over K and $\pi : E \times E' \to J$ is an isogeny such that

$$\mathrm{Ker}(\pi) \ = \ \mathrm{Graph}(-\psi) \quad \text{and} \quad \hat{\pi} \circ \lambda \circ \pi \ = \ N(\lambda_E \otimes \lambda_{E'}), \tag{1}$$

where $\lambda_E : E \to \hat{E}$ is the canonical principal polarization of E/K and $\lambda_E \otimes \lambda_{E'}$ denotes the product polarization on $E \times E'$, i.e., $\lambda_E \otimes \lambda_{E'} = \phi_{\theta_E + \theta_{E'}}$, where $\theta_E = \theta_E^{E \times E'} = \mathrm{pr}_E^*(0_E)$ and $\theta_{E'} = \theta_{E'}^{E \times E'} = \mathrm{pr}_{E'}^*(0_{E'})$, and $\mathrm{pr}_E = \mathrm{pr}_E^{E \times E'} : E \times E' \to E$ and $\mathrm{pr}_{E'} = \mathrm{pr}_{E'}^{E \times E'} : E \times E' \to E'$ are the projections.

We also say that (E, E', ψ) is an *N-presentation of (J, λ)* over K if there is some isogeny π such that (E', E', ψ, π) is an N-presentation of (J, λ) over K.

In addition, two N-presentations $(E_1, E_1', \psi_1, \pi_1)$ and $(E_2, E_2', \psi_2, \pi_2)$ of (J, λ) are said to be *isomorphic* if there exist isomorphisms $\alpha : E_1 \xrightarrow{\sim} E_2$ and $\alpha' : E_1' \xrightarrow{\sim} E_2'$ of elliptic curves such that $\pi_1 = \pi_2 \circ (\alpha \times \alpha')$.

The following result clarifies the relation between N-presentations of (J, λ) and elliptic subgroups of J of degree N.

Proposition 10 (a) *Let (J, λ) be a principally polarized abelian surface and let $E \leq J$ be an elliptic subgroup of J with inclusion morphism $i_E : E \hookrightarrow J$. If E has λ-degree N, i.e., if*

$$\hat{i}_E \circ \lambda \circ i_E \ = \ N\lambda_E, \tag{2}$$

then there is unique elliptic subgroup $E^\perp = E^\perp_\lambda \leq J$ *of* λ*-degree* N *such that*

$$\phi_{E+E^\perp} \;=\; N\lambda, \tag{3}$$

and there is a unique anti-isometry $\psi_E = \psi_{J,\lambda,E} : E[N] \xrightarrow{\sim} E^\perp[N]$ *such that*

$$i_{E^\perp} \circ \psi_E \;=\; (i_E)_{|E[N]}. \tag{4}$$

In addition, $\pi_E = \pi_{J,\lambda,E} := i_E \circ \mathrm{pr}_E + i_{E^\perp} \circ \mathrm{pr}_{E^\perp} : E \times E^\perp \to J$ *is an isogeny such that* $(E, E^\perp, \psi_E, \pi_E)$ *is an* N*-presentation of* (J, λ) *over* K *such that* $\pi_E(\theta_{E^\perp}) = E$.

(b) *Let* (E, E', ψ) *be an* N*-presentation over* K*, and let* $\pi_\psi : A := E \times E' \to A_\psi := A/\mathrm{Graph}(-\psi)$ *be the quotient map. Then* A_ψ *has a unique principal polarization* λ_ψ *such that* (E, E', ψ, π_ψ) *is an* N*-presentation of* (A_ψ, λ_ψ).

In addition, $\bar{E} := \pi_\psi(\theta_{E'}) \simeq E$ *and* $\bar{E}' = \pi_\psi(\theta_E) \simeq E'$ *are elliptic subgroups of* A_ψ *of* λ_ψ*-degree* N*, and* $\bar{E}' = \bar{E}^\perp$.

(c) *If* (E, E', ψ) *is an* N*-presentation of* (J, λ)*, then there is an isomorphism (of polarized abelian surfaces)* $(J, \lambda) \simeq (A_\psi, \lambda_\psi)$*, where the latter pair is as in part* (b).

(d) *If* (E, E', ψ, π) *is an* N*-presentation of* (J, λ)*, then* $\overline{E} := \pi(\theta_{E'}^{E \times E'})$ *is an elliptic subgroup of* J *of* λ*-degree* N*, and the* N*-presentation* $(\overline{E}, \overline{E}^\perp, \psi_{\overline{E}}, \pi_{\overline{E}})$ *of part* (a) *is isomorphic to* (E, E', ψ, π).

(e) *The rule* $(E, E', \psi, \pi) \mapsto \pi(\theta_{E'}^{E \times E'})$ *defines a bijection between the set* $\mathbf{P}_N(J, \lambda)$ *of isomorphism classes of* N*-presentations of* (J, λ) *and the set* $\mathcal{S}_N(J, \lambda)$ *of elliptic subgroups of* J *of* λ*-degree* N.

Remark 11 (a) If $\lambda = \phi_\theta$, for some theta-divisor $\theta \in \mathrm{Div}(J)$, then the left hand side of (2) equals $\phi_{i_E^* \theta}$, so (2) is equivalent to the condition that $(E.\theta) = N$.

Similarly, condition (3) is equivalent to the condition that $E + E^\perp \equiv N\theta$, where $\equiv$ denotes numerical equivalence, and the second condition of (1) is equivalent to the condition that $\pi^*\theta \equiv \theta_E + \theta_{E'}$.

(b) As the above result shows, the concept of a presentation (E, E', ψ) is closely related to the "basic construction" of [2] and [5], §5.

(c) If (E, E', ψ, π) is an N-presentation of (J, λ), and if $\tau : E' \times E \to E \times E'$ denote the isomorphism defined by $\tau(x, y) = (y, x)$, then $(E', E, \psi^{-1}, \pi \circ \tau)$ is also an N-presentation of (J, λ) because $\tau^*(\theta_E^{E' \times E} + \theta_{E'}^{E' \times E}) = \theta_E^{E \times E'} + \theta_{E'}^{E \times E}$ and $\mathrm{Ker}(\pi \circ \tau) = \mathrm{Graph}(-\psi^{-1})$, as is easy to see.

Proof of Proposition 10. (a) Put $E^\perp = \mathrm{Ker}(\hat{i}_E \circ \lambda)$. Then by [5], Proposition 5.2 and Corollary 5.3, $E^\perp$ is an elliptic subgroup of J of λ-degree N, and there is a unique isomorphism ψ such that (3) holds. Moreover, ψ is an anti-isometry by [5], Corollary 5.6. By [5], Proposition 5.5 and Corollary 5.6, the morphism π is an isogeny which satisfies (1), so $(E, E^\perp, \psi, \pi)$ is an N-presentation of (A, λ).

It remains to show that $\pi_E(\theta_{E^\perp}) = E$, that $E^\perp$ satisfies (3) and that this uniquely characterizes $E^\perp$. To prove the latter, suppose that E' is another elliptic subgroup of J such that $\phi_{E+E'} = N\lambda$. Then $E + E^\perp \equiv E + E'$, so $E^\perp \equiv E'$. Then by [4], Theorem 2.8, it follows that their base changes $E^\perp_{\overline{K}}$ and $E'_{\overline{K}}$ to $\overline{K}$ are equal, and hence $E^\perp = E'$. This proves that $E^\perp$ is uniquely determined by (3).

To prove that (3) holds for $E^\perp$ as defined above, write $A = E \times E^\perp$ and let $i_E^A : E \hookrightarrow A$ and $i_{E^\perp}^A : E^\perp \hookrightarrow A$ be the canonical inclusions. Then by the definition of π_E we have

$$\pi_E \circ i_E^A \;=\; i_E \quad \text{and} \quad \pi_E \circ i_{E^\perp}^A \;=\; i_{E^\perp}, \tag{5}$$

and so $\pi(\theta_{E^\perp}^A) = i_E(E) = E$ because $\theta_{E^\perp}^A = \mathrm{pr}_{E^\perp}^*(0) = E \times \{0\} = i_E^A(E)$. Moreover, $\pi_{|\theta_{E^\perp}^A} : \theta_{E^\perp}^A \to E$ is an isomorphism because $\theta_{E^\perp}^A \cap \mathrm{Graph}(-\psi) = \{0\}$ (as subschemes). Thus, $\pi_*\theta_{E^\perp}^A = E$ (equality as divisors). Similarly, since $\theta_E^A = i_{E^\perp}^A(E^\perp)$, we see that also $\pi_*\theta_E = E^\perp$. Thus, since π is an isogeny of degree N^2, it follows that

$$\pi^*E \;\equiv\; N^2\theta_{E^\perp} \quad \text{and} \quad \pi^*E^\perp \;\equiv\; N^2\theta_E. \tag{6}$$

From this we see that $\hat{\pi}_E \circ \phi_{E+E^\perp} \circ \pi_E = \phi_{\pi_E^*(E+E^\perp)} = N^2\phi_{\theta_E+\theta_{E^\perp}} = N^2(\lambda_E \otimes \lambda_{E^\perp}) = N\hat{\pi}_E \circ \lambda \circ \pi$, where the latter equality follows from (1). Thus, since π_E and $\hat{\pi}_E$ are isogenies, we see that (3) holds. Moreover, as was shown above, we have that $\pi_E(\theta_{E^\perp}) = E$.

(b) The existence of the quotient A_ψ and of λ_ψ satisfying (1) follows from [5], Proposition 5.7, so (E, E', ψ, π_ψ) is an N-presentation of (A_ψ, λ_ψ).

To prove the second statement, note that by Corollary 5.9 of [5] there exist elliptic subgroups $\overline{E}$, $\overline{E}' \in \mathcal{S}_N(A_\psi, \lambda_\psi)$ such that

$$\pi_\psi \circ i_E^A \;=\; i_{\overline{E}} \quad \text{and} \quad \pi_\psi \circ i_{E'}^A \;=\; i_{\overline{E}'}.$$

Thus, by a similar argument as in part (a) we see that $\pi_{|\theta_E} : \theta_E \to \bar{E}'$ and $\pi_{|\theta_{E'}} : \theta_{E'} \to \bar{E}$ are isomorphisms, where $\pi = \pi_\psi$, so $E' \simeq \theta_E \simeq \bar{E}'$, and $E \simeq \theta_{E'} \simeq \bar{E}$ and $\pi_*\theta_E = \bar{E}'$ and $\pi_*\theta_E = \bar{E}'$. Thus, as in part (a), it follows that (the analogue of) (3) holds and so $\bar{E}' = \bar{E}^\perp$.

(c) By hypothesis, there exists π such that (E, E', ψ, π) is an N-presentation of (J, λ). By (1) and the universal property of quotients there is a unique isomorphism $\alpha : A_\psi \xrightarrow{\sim} J$ such that $\pi = \alpha \circ \pi_\psi$. Moreover, since $\hat{\alpha} \circ \lambda \circ \alpha$ and λ_ψ both satisfy the second identity of (1), it follows that $\hat{\alpha} \circ \lambda \circ \alpha = \lambda_\psi$. This proves the assertion.

(d) Put $A = E \times E'$. By (1) we know that $\pi : A \to J$ is a quotient of A by $\mathrm{Graph}(-\psi)$, so we can identify J with A_ψ, and then $\lambda_\psi = \lambda$. Thus, by the proof of part (b) we see that $\overline{E} := \pi(\theta_{E'}^A) \in \mathcal{S}_N(J, \lambda)$. Moreover, we know that $\overline{E}' := \pi(\theta_E^A) \in \mathcal{S}_N(J, \lambda)$ and that $\overline{E}^\perp = \overline{E}'$. In addition, we have seen that there exist

isomorphisms $\alpha : E \to \overline{E}$ and $\alpha' : E' \to \overline{E}' = \overline{E}^{\perp}$ such that $i_{\overline{E}} \circ \alpha = \pi \circ i_E^A$ and $\alpha' \circ i_{\overline{E}'} = \pi \circ i_{E'}$.

To show that $\pi_{\overline{E}} \circ (\alpha \times \alpha') = \pi$, put $\overline{A} = \overline{E} \times \overline{E}' = \overline{E} \times \overline{E}^{\perp}$. Then by (5) we have that $\pi_{\overline{E}} \circ (\alpha \times \alpha') \circ i_E^A = \pi_{\overline{E}} \circ i_{\overline{E}}^{\overline{A}} \circ \alpha = i_{\overline{E}} \circ \alpha = \pi \circ i_E^A$, and similarly $\pi_{\overline{E}} \circ (\alpha \times \alpha') \circ i_{E'}^A = \pi \circ i_{E'}^A$, and so it follows that $\pi_{\overline{E}} \circ (\alpha \times \alpha') = \pi$, which proves the assertion.

(e) If $P_1 = (E_1, E_1', \psi_1, \pi_1)$ is an N-presentation of (J, λ), then by part (d) we see that $\varphi(P_1) := \pi_1(\theta_{E_1'}^{E_1 \times E_1'}) \in \mathcal{S}_N(J, \lambda)$. Moreover, if $(E_2, E_2', \psi_2, \pi_2)$ is an N-presentation of (J, λ) which is isomorphic to P_1 via isomorphisms $\alpha : E_1 \to E_2$ and $\alpha' : E_1' \to E_2'$, then $\varphi(P_2) = \varphi(P_1)$ because $(\alpha \times \alpha')(\theta_{E_1}^{E_1 \times E_1'}) = \theta_{E_2}^{E_2 \times E_2'}$, and so the given rule defines a map $\varphi : \mathbf{P}_N(J, \lambda) \to \mathcal{S}_N(J, \lambda)$.

On the other hand, the rule $E \mapsto (E, E^{\perp}, \psi_E, \pi_E)$ defines by part (a) a map $\varphi' : \mathcal{S}_N(J, \lambda) \to \mathbf{P}_N(J, \lambda)$ such that $\varphi(\varphi'(E)) = E$. Since $\varphi' \circ \varphi = 1_{\mathbf{P}_N(J,\lambda)}$ by part(d), it follows that φ and φ' are inverses of each other, and so both are bijections. □

Corollary 12 *If $f : C \to E$ be an elliptic subcover of C/K of degree N, then $(f^* J_E)^{\perp} = \mathrm{Ker}(f_*)$, and there exists an elliptic subcover $f^{\perp} : C \to E^{\perp}$ of degree N such that $(f^{\perp})^* J_{E^{\perp}} = (f^* J_E)^{\perp}$, and a unique anti-isometry*

$$\psi_f : E[N] \xrightarrow{\sim} E_f^{\perp}[N] \quad \textit{such that} \quad (f^{\perp})^* \circ \lambda_{E_f^{\perp}} \psi_f = (f^* \circ \lambda_E)_{|E[N]},$$

where $\lambda_E : E \to J_E = \hat{E}$ is the canonical isomorphism. Moreover, if $A_f = E \times E_f^{\perp}$ denotes the product surface, and if

$$\pi_f := (f^* \circ \lambda_E \circ \mathrm{pr}_E) + ((f^{\perp})^* \circ \lambda_{E_f^{\perp}} \mathrm{pr}_{E_f^{\perp}}) : A_f = E \times E_f^{\perp} \to J_C,$$

then $(E, E_f^{\perp}, \psi_f, \pi_f)$ is an N-presentation of (J_C, λ_C) over K. In addition, if

$$\pi_f' := (\lambda_E^{-1} \circ f_*,\ \lambda_{E_f^{\perp}}^{-1} \circ (f^{\perp})_*) : J_C \ \to \ E \times E_f^{\perp},$$

then $\pi_f' \circ \pi_f = [N]_{E \times E_f^{\perp}}$.

Proof. Since $f_* = \lambda_E^{-1} \circ (f^*)^{\wedge} \circ \lambda$, it follows from the proof of Proposition 10 that $(f^* J_E)^{\perp} = \mathrm{Ker}(f_*)$, and so this has degree N. By Theorem 7 and Remark 9 there exists an elliptic subcover $f^{\perp} : C \to E_f^{\perp}$ of degree N such that $(f^{\perp})^* J_{E^{\perp}} = (f^* J_E)^{\perp}$. Thus Proposition 10 shows that $(E, E_f^{\perp}, \psi_f, \pi_f)$ is an N-presentation of (J_C, λ_C).

The last assertion follows immediately from the identities $f_* \circ f^* = [N]_{J_E}$, $(f^{\perp})_* \circ (f^{\perp})^* = [N]_{J_{E_f^{\perp}}}$, $f_* \circ (f^{\perp})^* = 0$ (by construction) and $(f^{\perp})_* \circ f^* = 0$ (by duality). □

Remark 13 If $f_i : C \to E_i$, $i = 1, 2$, are two elliptic subcovers of C/K, then the above proof shows that $f_2^* J_{E_2} = (f_1^*(J_{E_1}))^{\perp}$ if and only if $(f_1)_* f_2^* = 0$. (Use the fact that a containment of elliptic subgroups implies equality.)

3 The refined Humbert invariant

As was mentioned in the introduction, the refined Humbert invariant q_C of C (cf. [4], [8]) can be used to give a description of the set $\mathcal{E}(C)$) elliptic subcovers of C. Unfortunately, the definition of q_C given in [4] and [8] depends on the existence of a theta-divisor $\theta_C \in \mathrm{Div}(J_C)$ and hence cannot readily be used over an arbitrary ground field. In particular, the Néron-Severi group $\mathrm{NS}(J_C)$ of J_C, which played an important role in the definition of q_C, is too small for our purpose.

The simplest way to remedy this problem is to replace $\mathrm{NS}(J_C)$ by a slightly larger group $\mathrm{NS}'(J_C)$ which is a subgroup of $\mathrm{NS}(J_C \otimes \overline{K})$, where $\overline{K}$ is an algebraic closure of K. Another method consists of replacing $\mathrm{NS}(J_C)$ by the much more intrinsic group $\mathrm{End}_\lambda(J_C) \leq \mathrm{End}(J_C)$. This leads to the same results because these two groups are naturally isomorphic; cf. Proposition 14 below. However, the second group is more useful in proofs.

To define these groups, let A/K be an arbitrary abelian variety. For any field extension L/K we have an injective homomorphism $\delta_{L/K} : \mathrm{Div}(A) \hookrightarrow \mathrm{Div}(A_L)$ of the divisor groups, where $A_L = A \otimes L$ is the base-change of A by L, and this induces an injection

$$\overline{\delta}_{L/K} : \mathrm{NS}(A) \ \hookrightarrow \ \mathrm{NS}(A_L),$$

where, as usual, $\mathrm{NS}(A) = \mathrm{Div}(A)/\equiv$ denotes the group of divisors on A modulo numerical equivalence. Fix an algebraic closure $\overline{K}$ of K, and let

$$\mathrm{NS}'(A) \ = \ \{D \in \mathrm{NS}(A_{\overline{K}}) : nD \in \overline{\delta}_{\overline{K}/K}(\mathrm{NS}(A)), \text{ for some } n \geq 1\}$$

denote the saturation of $\overline{\delta}_{\overline{K}/K}(\mathrm{NS}(A))$ in $\mathrm{NS}(A_{\overline{K}})$.

On the other hand, if A has a principal polarization $\lambda : A \xrightarrow{\sim} \hat{A}$ (defined over K), then we can define the additive subgroup $\mathrm{End}_\lambda(A)$ of the ring $\mathrm{End}(A) = \mathrm{End}_K(A)$ of K-endomorphisms of A by:

$$\mathrm{End}_\lambda(A) \ = \ \{\alpha \in \mathrm{End}(A) : \hat{\alpha} \circ \lambda = \lambda \circ \alpha\} \ = \ \{\alpha \in \mathrm{End}(A) : \alpha' = \alpha\},$$

where $\alpha' = r_\lambda(\alpha) := \lambda^{-1} \circ \hat{\alpha} \circ \lambda$. Thus, $\mathrm{End}_\lambda(A)$ consists of those endomorphisms which are symmetric with respect to the *Rosati involution* r_λ defined by λ.

To see that these two groups are isomorphic, recall that there is a natural injective group homomorphism

$$\Phi_\lambda : \mathrm{NS}(A) \quad \hookrightarrow \quad \mathrm{End}_\lambda(A)$$

which is given by the rule $\Phi_\lambda(D) = \lambda^{-1} \circ \phi_{\mathcal{L}(D)}$; cf. Mumford[16] or §11 of [8]. Note that this isomorphism is clearly compatible with base-change, i.e., if L/K is an extension field, then we have

$$\Phi_{\lambda_L}(\overline{\delta}_{L/K}(D)) \ = \ \beta_{L/K}(\Phi_\lambda(D)), \quad \text{for all } D \in \mathrm{NS}(A), \tag{7}$$

where $\beta_{L/K}(h) = h_L \in \mathrm{End}(A_L)$ is the base-change of the endomorphism $h \in \mathrm{End}(A)$.

We now show:

Proposition 14 (a) *If L/K is an extension field, then the base-change homomorphism $\beta_{L/K} : \mathrm{End}_\lambda(A) \hookrightarrow \mathrm{End}_{\lambda_L}(A_L)$ is injective and its cokernel is torsionfree.*

(b) *There is a unique isomorphism*

$$\Phi'_\lambda : \mathrm{NS}'(A) \ \stackrel{\sim}{\to} \ \mathrm{End}_\lambda(A)$$

such that the restriction of $\Phi_{\lambda_{\overline{K}}}$ to $\mathrm{NS}'(A)$ equals $\beta_{\overline{K}/K} \circ \Phi'_\lambda$. Moreover, the quotient $\mathrm{NS}'(A)/\overline{\delta}_{\overline{K}'/K}(\mathrm{NS}(A))$ is a finite 2-group.

Proof. (a) The fact that $\beta_{L/K}$ is injective is clear. Next, recall from [6], Lemma 14(b), that $\beta_{L/K}(\mathrm{End}(A))$ is a primitive submodule of $\mathrm{End}(A_L)$, i.e., the quotient $\mathrm{End}(A_L)/\beta_{L/K}(\mathrm{End}(A))$ is torsionfree. Thus, since $\mathrm{End}_\lambda(A)$ is primitive in $\mathrm{End}(A)$, it follows that $\beta_{L/K}(\mathrm{End}_\lambda(A))$ is primitive in $\mathrm{End}(A_L)$ and hence a fortiori in $\mathrm{End}_{\lambda_L}(A_L)$. This proves the second assertion.

(b) It clearly suffices to show that $\Phi_{\lambda_{\overline{K}}}(\mathrm{NS}'(A)) = \beta_{\overline{K}/K}(\mathrm{End}_\lambda(A))$ because $\Phi_{\lambda_{\overline{K}}}$ and $\beta_{\overline{K}/K}$ are both injective. Now since $\overline{\delta}_{\overline{K}/K}(\mathrm{NS}(A)) \subset \beta_{\overline{K}/K}(\mathrm{End}_\lambda(A))$ by (7) and since the latter subgroup is primitive in $\mathrm{End}_{\lambda_{\overline{K}}}(A)$ by part (a), it follows that that $\Phi_{\lambda_{\overline{K}}}(\mathrm{NS}'(A)) \subset \beta_{\overline{K}/K}(\mathrm{End}_\lambda(A))$.

To prove the opposite inclusion, note first that that there exists $\theta \in \mathrm{NS}'(A)$ such that $\Phi_{\lambda_{\overline{K}}}(\theta) = 1_{A_{\overline{K}}}$. Indeed, since λ is a polarization, there exists $\theta \in \mathrm{NS}(A_{\overline{K}})$ such that $\phi_\theta = \lambda_{\overline{K}}$, and so $\Phi_{\lambda_{\overline{K}}}(\theta) = 1_{A_{\overline{K}}}$. Now by Proposition 6.10 of [15] we know that there exists $D \in \mathrm{NS}(A)$ such that $\phi_D = 2\lambda$. Thus $\overline{\delta}_{\overline{K}/K}(D) = 2\theta$, and so $\theta \in \mathrm{NS}'(A)$.

Now suppose that $h \in \mathrm{End}_\lambda(A)$. Since $\Phi_{\lambda_{\overline{K}}}$ is an isomorphism (cf. [16] or [8]), there exists $D' \in \mathrm{NS}(A_{\overline{K}})$ such that $\Phi_{\lambda_{\overline{K}}}(D') = h_{\overline{K}}$. Thus $\phi_{D'} = \lambda'_{\overline{K}}$, where $\lambda' = \lambda \circ h$. We now show that $D' \in \mathrm{NS}'(A)$. For this, note first that since θ is ample, there is an $n \geq 1$ such that $D'' := n\theta + D'$ is ample. Put $\lambda'' = n\lambda + \lambda'$. Then $\lambda''_{\overline{K}'} = n\phi_\theta + \phi_{D'} = \phi_{D''}$, so λ'' is a polarization of A. Applying Proposition 6.10 of [15] again, we obtain that $2\lambda'' = \phi_{D_1}$, for some $D_1 \in \mathrm{NS}(A)$. Thus $\overline{\delta}_{\overline{K}/K}(D_1) = 2D'' = 2n\theta + 2D'$, so $D' \in \mathrm{NS}(A)$, as desired.

Finally, since the above proof shows that $2\mathrm{NS}'(A) \subset \overline{\delta}_{\overline{K}/K}(\mathrm{NS}(A))$, it follows that the quotient is a finite elementary 2-group because $\mathrm{NS}(A_{\overline{K}})$ is finitely generated. $\square$

Remark 15 For any homomorphism $h : A_1 \to A_2$ of abelian varieties, the pullback of divisors induces a homomorphism $h^* : \mathrm{NS}(A_2) \to \mathrm{NS}(A_1)$ of the Néron-Severi groups. Since this map is compatible with the respective base-change maps, it follows that $h^*_{\overline{K}}\overline{\delta}_{\overline{K}/K}(\mathrm{NS}(A_2)) \subset \overline{\delta}_{\overline{K}/K}(\mathrm{NS}(A_1))$, and so the restriction of $h^*_{\overline{K}}$ to $\mathrm{NS}'(A_2)$ induces a functorial homomorphism

$$h^* : \mathrm{NS}'(A_2) \ \to \ \mathrm{NS}'(A_1).$$

Similarly, the groups $\mathrm{End}_\lambda(A)$ have a functorial property which mirrors that of the Néron-Severi groups, as was explained in the appendix of [8], More precisely, if (A_i, λ_i) are two principally polarized abelian varieties, and if $h : A_1 \to A_2$ is a homomorphism, then we put $h' = r_{\lambda_1,\lambda_2}(h) := \lambda_1^{-1} \circ \hat{h} \circ \lambda_2 : A_2 \to A_1$ and define

$$h^\flat = h^\flat_{\lambda_1,\lambda_2} : \mathrm{End}(A_2) \ \to \ \mathrm{End}(A_1)$$

by $h^\flat(\alpha) = h' \circ \alpha \circ h$. Since $h^\flat$ is compatible with the Rosati involutions, i.e.,

$$h^\flat(r_{\lambda_2}(\alpha)) \ = \ r_{\lambda_1}(h^\flat(\alpha)), \quad \text{for all } \alpha \in \mathrm{End}(A_2), \tag{8}$$

we see that $h^\flat$ restricts to a homomorphism $h^\flat : \mathrm{End}_{\lambda_2}(A_2) \to \mathrm{End}_{\lambda_1}(A_1)$. Moreover, we have by [5], equation (61), that

$$h^\flat(\Phi_{\lambda_2}(D)) \ = \Phi_{\lambda_1}(h^*D), \quad \text{for all } D \in \mathrm{NS}(A_2), \tag{9}$$

and so it also follows that

$$h^\flat_{\overline{K}}(\Phi'_{\lambda_2}(D)) \ = \Phi'_{\lambda_1}(h^*D), \quad \text{for all } D \in \mathrm{NS}'(A_2), \tag{10}$$

For later use, we observe that $h' := r_{\lambda_1,\lambda_2}(h)$ and h are duals of each other in the sense that if $h'' := r_{\lambda_2,\lambda_1}(h')$, then we have that

$$h'' \ = \ h. \tag{11}$$

This follows immediately from properties of the duality isomorphism $\kappa_{A_i} : A_i \xrightarrow{\sim} \hat{\hat{A}}_i$ (cf. [5], p. 42-3). Indeed, $h'' = \lambda_2^{-1} \circ (\lambda_1^{-1} \circ \hat{h} \circ \lambda_2)^\wedge \circ \lambda_1 = \lambda_2^{-1} \circ \hat{\lambda}_2 \circ \hat{\hat{h}} \circ \hat{\lambda}_1^{-1} \circ \lambda_1 = \kappa_{A_2}^{-1} \circ \hat{\hat{h}} \circ \kappa_{A_1} = h$.

We now specialize to the case that A/K is a *surface* and define the *refined Humbert invariant* $\tilde{q}_{(A,\lambda)}$ on $\mathrm{NS}'(A)$ as the restriction of $\tilde{q}_{(A_{\overline{K}},\lambda_{\overline{K}})}$ to $\mathrm{NS}'(A)$, where $\tilde{q}_{(A_{\overline{K}},\lambda_{\overline{K}})}$ denotes the refined Humbert invariant on $\mathrm{NS}(A_{\overline{K}})$ as defined in [4] and [8]. Thus:

$$\tilde{q}_{(A,\lambda)} \ = \ (D.\theta)^2 - 2(D.D), \quad \text{for } D \in \mathrm{NS}'(A), \tag{12}$$

where $\theta \in \mathrm{NS}(A_{\overline{K}})$ is such that $\phi_\theta = \lambda_{\overline{K}}$ and $(D_1.D_2)$ denotes the intersection number of $D_1, D_2 \in \mathrm{NS}(A_{\overline{K}})$. By [4], (3.3) we thus have that

$$\tilde{q}(D) \ \geq \ 0, \ \forall\, D \in \mathrm{NS}'(A), \quad \text{and} \quad \tilde{q}(D) \ = \ 0 \ \Leftrightarrow \ D \in \mathbb{Z}\theta. \tag{13}$$

Since $\tilde{q}(D + n\theta) = \tilde{q}(D)$, for all $n \in \mathbb{Z}$, and since $\theta \in \mathrm{NS}'(A)$, as was shown in the proof of Proposition 14, it follows that $\tilde{q}$ induces a positive-definite quadratic form on

$$\mathrm{NS}(A, \lambda) \ := \ \mathrm{NS}'(A)/\mathbb{Z}\theta.$$

Remark 16 If we transport $\tilde{q}_{(A,\lambda)}$ to $\mathrm{End}_\lambda(A)$ by using the isomorphism Φ'_λ of Proposition 14, then the resulting quadratic form $\tilde{Q}_{(A,\lambda)}$ has a simple direct formula:

$$\tilde{Q}_{(A,\lambda)} \;=\; \mathrm{tr}(\alpha^2) - \tfrac{1}{4}(\mathrm{tr}(\alpha)^2), \quad \text{for } \alpha \in \mathrm{End}_\lambda(A).$$

Here, tr is the usual trace of an endomorphism as defined in Mumford[16], p. 182.

Since we don't need this, we won't prove the above assertion here, i.e., that $\tilde{Q}_{(A,\lambda)}(\Phi'_\lambda(D)) = \tilde{q}_{(A,\lambda)}(D)$, for $D' \in \mathrm{NS}'(A)$; this is proved in [11].

It is worthwhile to mention that it is shown in [11] that the above definition of $\tilde{Q}_{(A,\lambda)}$ can be generalized to principal polarized abelian varieties (A,λ) of arbitrary dimension, and that one then has that $Q_{(A,\lambda)}$ defines an integral, positive definite quadratic form on the quotient group $\mathbb{E}_\lambda(A) := \mathrm{End}_\lambda(A)/\mathbb{Z}1_A$.

For later reference, we observe the following compatibility relation of $\tilde{q}_{(A,\lambda)}$ with respect to "polarized isogenies".

Proposition 17 *Let (A_i,λ_i), $i=1,2$, be two principally polarized abelian surfaces, and let $\pi : A_1 \to A_2$ be an isogeny such that $\hat{\pi}\lambda_2\pi = N\lambda_1$, for some $N \geq 1$. Then $\pi^* : \mathrm{NS}'(A_2) \to \mathrm{NS}'(A_1)$ is injective with finite cokernel, and we have*

$$\tilde{q}_{(A_1,\lambda_1)}(\pi^* D) \;=\; N^2 \tilde{q}_{(A_2,\lambda_2)}(D), \forall D \in \mathrm{NS}'(A_2). \tag{14}$$

Proof. Since $\pi_{\overline{K}}$ is finite and surjective, it follows that $\pi^*_{\overline{K}} : \mathrm{NS}((A_2)_{\overline{K}}) \to \mathrm{NS}((A_1)_{\overline{K}})$ is injective (by the projection formula). Thus, its restriction to $\mathrm{NS}'(A_2)$ is also injective. Moreover, since $N^2\mathrm{NS}'(A_1) = [N]^*\mathrm{NS}'(A_1) = \pi^*(\pi')^*\mathrm{NS}'(A_1) \subset \pi^*\mathrm{NS}'(A_2)$, where $N = \deg(\pi)$ and $\pi' \circ \pi = [N]_{A_1}$, and since $\mathrm{NS}'(A_1)$ is finitely generated, we see that the cokernel of π^* is finite.

Let $\theta_i \in \mathrm{NS}'(A_i)$ be such that $\phi_{\theta_i} = (\lambda_i)_{\overline{K}}$, for $i = 1,2$. Then the given relation between the λ_i's means that $\pi^*\theta_2 = N\theta_1$; cf. [5], formula (37). Moreover, the relation implies that $\deg(\pi)^2 = \deg([N]_{A_1}) = N^4$, so $\deg(\pi) = N^2$. We thus see that (14) follows directly from the projection formula because with $\tilde{q}_i = \tilde{q}_{(A_i,\lambda_i)}$ we have $\tilde{q}_1(\pi^* D) = (\frac{1}{N}(\pi^*\theta_2.\pi^* D))^2 - 2(\pi^* D.\pi^* D) = (N(\theta_2.D))^2 - 2N^2(D.D) = N^2\tilde{q}_2(D)$. □

We now want to generalize Theorem 3.1 of [4] to principally polarized abelian surfaces (A,λ) which are defined over an arbitrary ground field K. For this, recall from §2 or [5], p. 9, that the λ-*degree* $\deg_\lambda(E)$ of an elliptic subgroup $E \leq A$ is defined by the rule (2). To state the result, we use the notation $\mathrm{cl}(D) \in \mathrm{NS}(A)$ to denote the class of a divisor $D \in \mathrm{Div}(A)$ and let $\mathrm{cl}'(D) = \overline{\delta}_{\overline{K}/K}(\mathrm{cl}(D)) \in \mathrm{NS}'(A)$ be its base-change. We then have:

Theorem 18 *Let (A,λ) is a principally polarized abelian surface over an arbitrary field K, and let $\theta \in \mathrm{NS}(A_{\overline{K}})$ be such that $\phi_\theta = \lambda_{\overline{K}}$. For any $n \geq 1$, the rules*

$$E \mapsto \mathrm{cl}'(E) \quad \textit{and} \quad D \mapsto D + \mathbb{Z}\theta \in \mathrm{NS}(A,\lambda)$$

induce bijections between the following three sets:

(i) *the set* $\mathcal{S}_n(A,\lambda)$ *of elliptic subgroups* $E \in \mathcal{S}(A)$ *of degree* $n = \deg_\lambda(E)$*;*

(ii) *the set* $\mathcal{P}_n(A,\lambda)$ *of primitive elements* $D \in \mathrm{NS}'(A)$ *with* $(D.D) = 0$ *and* $(D.\theta) = n$*;*

(iii) *the set* $\mathcal{P}_{n^2}(q_{(A,\lambda)})$ *of primitive elements* $\overline{D} \in \mathrm{NS}(A,\lambda)$ *with* $q_{(A,\lambda)}(\overline{D}) = n^2$*;*

(iv) *the set* $\mathbf{P}_n(A,\lambda)$ *of isomorphism classes of* n*-presentations of* (A,λ)*.*

Before proving this, we first establish the following technical fact.

Lemma 19 *Let* $E \in \mathcal{S}(A)$ *be an elliptic subgroup of* A *with immersion* $i_E : E \hookrightarrow A$*, and let* $i'_E := r_{\lambda_E,\lambda}(i_E) : A \to E$ *be its "dual". Then* $E^\perp := E^\perp_\lambda = \mathrm{Ker}(i'_E)$ *, and* $(E^\perp)^\perp = E$*. Moreover,*

$$\Phi_\lambda(\mathrm{cl}(E^\perp)) \;=\; e_E := i_E \circ i'_E \quad \textit{and} \quad \Phi_\lambda(\mathrm{cl}(E)) \;=\; e_{E^\perp}, \tag{15}$$

where we view E *and* $E^\perp$ *as divisors on* A*. In particular,*

$$\mathrm{Ker}(\Phi_\lambda(\mathrm{cl}(E))) \;=\; E. \tag{16}$$

Proof. The identity $E^\perp = \mathrm{Ker}(i'_E)$ follows from the proof of Proposition 10(a), and the identity $(E^\perp)^\perp = E$ is clear from (3). To verify (15), note that since $E^\perp = \mathrm{Ker}(i'_E) = (i'_E)^*(0_E)$ by definition, it follows from the functorial formula (61) of [8] (applied to $h = i'_E$) that $\Phi_\lambda(\mathrm{cl}(E^\perp)) = \Phi_\lambda((i'_E)^*(0_E)) = i''_E\Phi_{\lambda_E}(0_E)i'_E = i_E i'_E$ because $i''_E = i_E$ and $\Phi_{\lambda_E}(0_E) = \lambda_E^{-1}\phi_{\mathcal{L}(0_E)} = 1_E$. This proves the first formula of (15), and the second formula follows from this by replacing E by $E^\perp$ and using the identity $E = (E^\perp)^\perp$.

Since $i_{E^\perp}$ is injective, we have $\mathrm{Ker}(e_{E^\perp}) = \mathrm{Ker}(i'_{E^\perp}) = (E^\perp)^\perp = E$. Thus, by (15) we have that $\mathrm{Ker}(\Phi_\lambda(\mathrm{cl}(E))) = \mathrm{Ker}(e_{E^\perp}) = E$, which proves (16). □

Proof of Theorem 18. Since the bijection between the sets $\mathcal{S}_n(A,\lambda)$ and $\mathbf{P}_n(A,\lambda)$ was established in Proposition 10, the assertion clearly follows from the following two claims.

Claim 1. The rule $E \mapsto \mathrm{cl}'(E)$ defines a bijection $\Psi_{\lambda,n} : \mathcal{S}_n(A,\lambda) \xrightarrow{\sim} \mathcal{P}_n(A,\lambda)$.
If $E \in \mathcal{S}_n(A,\lambda)$, then $E_{\overline{K}}$ is an elliptic subgroup of $A_{\overline{K}}$, and clearly $\mathrm{cl}(E_{\overline{K}}) = \mathrm{cl}'(E) \in \mathrm{NS}'(A)$. By Remark 11(a) we have that

$$\deg_\lambda(E) \;=\; (\mathrm{cl}'(E).\theta). \tag{17}$$

Clearly $(E_{\overline{K}}.E_{\overline{K}}) = 0$; cf. [4], Proposition 2.1. Moreover, since $\mathrm{cl}'(E) = \mathrm{cl}(E_{\overline{K}})$ is primitive in $\mathrm{NS}(A_{\overline{K}})$ by Corollary 2.6 of [4], it is also primitive in $\mathrm{NS}'(A)$, and so it follows that $\mathrm{cl}'(E) \in \mathcal{P}_n(A,\lambda)$. Thus, the given rule defines a map $\Psi_{\lambda,n} : \mathcal{S}_n(A,\lambda) \to \mathcal{P}_n(A,\lambda)$.

It is immediate that $\Psi_{\lambda,n}$ is injective because if $\mathrm{cl}'(E) = \mathrm{cl}'(E')$, then by [4], Theorem 2.8, we have that $E_{\overline{K}} = E'_{\overline{K}}$, and so $E = E'$.

To prove that $\Psi_{\lambda,n}$ is surjective, let $D \in \mathcal{P}_n(A,\lambda)$. Since $\mathrm{NS}'(A)$ is a primitive subgroup of $\mathrm{NS}(A_{\overline{K}})$ by construction, it follows that D is primitive in $\mathrm{NS}(A_{\overline{K}})$, and so by Theorem 2.8 of [4] there is an elliptic subgroup E of $A_{\overline{K}}$ such that $\mathrm{cl}(E) = D$. Now since $D \in \mathrm{NS}'(A)$, we have by Proposition 14 that $\Phi_{\lambda_{\overline{K}}}(D) = \alpha_{\overline{K}}$, for some $\alpha \in \mathrm{End}_\lambda(A)$. Then $H = \mathrm{Ker}(\alpha)$ is a subgroup scheme of A, and $H_{\overline{K}} = \mathrm{Ker}(\alpha_{\overline{K}}) = \mathrm{Ker}(\Phi_{\lambda_{\overline{K}}}(D))$. But by Lemma 19 we have that $\mathrm{Ker}(\Phi_{\lambda_{\overline{K}}}(D)) = E$, so $H_{\overline{K}} = E$ is an elliptic subgroup of $A_{\overline{K}}$, and hence H is one of A. By (17) we see that $\deg_\lambda(H) = n$, so $H \in \mathcal{S}_n(A,\lambda)$. This proves Claim 1.

Claim 2. The rule $D \mapsto \overline{D} = D + \mathbb{Z}\theta$ defines a bijection $\Psi'_{\lambda,n} : \mathcal{P}_n(A,\lambda) \xrightarrow{\sim} \mathcal{P}_{n^2}(q_{(A,\lambda)})$. This is proved in exactly the same method as that of the proof of Theorem 3.1 of [4]. □

We now apply this result to the study of elliptic subcovers of a curve C/K of genus 2.

Theorem 20 *Let C/K be a curve of genus 2, and put $q_C = q_{(J_C,\lambda_C)}$. Then the rule $f \mapsto \mathrm{cl}'(f^*J_E) + \mathbb{Z}\theta_C$, where $\phi_{\theta_C} = (\lambda_C)_{\overline{K}}$, induces for each $n \geq 1$ a bijection*

$$\varepsilon_n : \mathcal{E}_n(C) \quad \xrightarrow{\sim} \quad \mathcal{P}_{n^2}(q_C)$$

between the set $\mathcal{E}_n(C)$ of equivalence classes of elliptic subcovers $f : C \to E$ of degree n and the set $\mathcal{P}_{n^2}(q_C)$ of primitive elements $\overline{D} \in \mathrm{NS}'(J_C,\lambda_C)$ with $q_C(\overline{D}) = n^2$.

Proof. Combine the bijections of Theorem 7 and of Theorem 18. □

4 The isogeny defect

We now study the *isogeny defect* m_ψ of an anti-isometry $\psi : E[N] \to E'[N]$. For technical reasons, it is useful to generalize m_ψ (which was defined in the Introduction) as follows.

Definition. Let E/K and E'/K be elliptic curves, and let $\psi \in \mathrm{Hom}(E[N], E'[N])$. Moreover, let $\mathcal{H} \leq \mathcal{H}_{E,E'} := \mathrm{Hom}(E,E')$ be a *primitive subgroup* of $\mathcal{H}_{E,E'}$, i.e., $\mathcal{H}$ is a subgroup of $\mathcal{H}_{E,E'}$ such that $\mathcal{H}_{E,E'}/\mathcal{H}$ is torsionfree. Then the *isogeny defect of ψ with respect to $\mathcal{H}$* is

$$m_\psi(\mathcal{H}) \;:=\; \min\{m \geq 1 : m\psi = h_{|E[N]}, \text{ for some } h \in \mathcal{H}\}.$$

Remark 21 (a) Clearly, $m_\psi(\mathcal{H}) = 1$ if and only if ψ is *induced by an isogeny* in $\mathcal{H}$, i.e., if and only if $\psi = h_{|E[N]}$, for some $h \in \mathcal{H} \leq \mathrm{Hom}(E,E')$. Note also that if $\mathcal{H} = \{0\}$, then $m_\psi(\mathcal{H}) = \mathrm{ord}(\psi)$ by definition.

(b) We can express $m_\psi(\mathcal{H})$ as an index of groups. Indeed, let

$$\rho_N : \mathrm{Hom}(E, E') \ \to \ \mathrm{Hom}(E[N], E'[N])$$

be the restriction map $h \mapsto h_{|E[N]}$, and put $\mathcal{H}_N = \rho_N(\mathcal{H})$, which is a subgroup of $\mathrm{Hom}(E[N], E'[N])$. Then by elementary group theory

$$m_\psi(\mathcal{H}) \ = \ [\langle\psi\rangle + \mathcal{H}_N : \mathcal{H}_N] \ = \ [\langle\psi\rangle : \langle\psi\rangle \cap \mathcal{H}_N]. \tag{18}$$

In particular, we see that $m_\psi(\mathcal{H}) \mid \mathrm{ord}(\psi) \mid N$, and that

$$k\psi = \rho_N(h), \text{ for some } k \in \mathbb{Z}, h \in \mathcal{H} \quad \Rightarrow \quad m_\psi(\mathcal{H}) \mid k. \tag{19}$$

As was mentioned in the introduction, the isogeny defect $m_\psi := m_\psi(\mathrm{Hom}(E, E'))$ determines the determinant of the refined Humbert invariant $q_C = q_{(J_C, \lambda_C)}$ attached to a genus 2 curve C/K with presentation (E, E', ψ); cf. Theorem 3. While the precise formula will be proven in the next two sections, here we first prove some general facts about $m_\psi(\mathcal{H})$ which will be used in the proof of Theorem 3.

Lemma 22 *In the above situation we have the exact sequence*

$$0 \ \to \ N\mathcal{H} \ \to \ \mathcal{H} \ \to \ \mathcal{H}_N \ \to \ 0.$$

Thus, if $r = r_{\mathcal{H}} := \mathrm{rank}(\mathcal{H})$*, then*

$$|\mathcal{H}_N| \ = \ N^r \quad \textit{and hence} \quad |\mathcal{H}_N + \langle\psi\rangle| \ = \ m_\psi(\mathcal{H})N^r. \tag{20}$$

Proof. Clearly, $N\mathcal{H} \leq \mathrm{Ker}(\rho_N) \cap \mathcal{H}$. Conversely, if $h \in \mathrm{Ker}(\rho_N) \cap \mathcal{H}$, then $E[N] = \mathrm{Ker}([N]_E) \leq \mathrm{Ker}(h)$, so $h = h' \circ [N]_E$, for some $h' \in \mathrm{Hom}(E, E')$ (because $(E, [N]_E)$ is a quotient of E by $E[N]$). Thus $h = Nh'$, and so $h' \in \mathcal{H}$ because $\mathcal{H}$ is a primitive subgroup of $\mathrm{Hom}(E, E')$ by hypothesis. Thus, $h \in N\mathcal{H}$, and so $N\mathcal{H} = \mathrm{Ker}(\rho_N) \cap \mathcal{H}$. Since $\rho_N(\mathcal{H}) = \mathcal{H}_N$ by definition, this shows that the above sequence is exact.

Since $\mathcal{H} \simeq \mathbb{Z}^r$, it follows from the above that $\mathcal{H}_N \simeq (\mathbb{Z}/N\mathbb{Z})^r$, and so $|\mathcal{H}_N| = N^r$. Thus, by (18) we obtain that $|\mathcal{H}_N + \langle\psi\rangle| = m_\psi(\mathcal{H})|\mathcal{H}_N| = m_\psi(\mathcal{H})N^r$. □

In order to calculate the discriminant of q_C, we shall make use of the *trace* $\mathrm{tr}(g)$ of an element $g \in \mathrm{End}(E[N])$. Since $\mathrm{tr}(g)$ is closely linked to the *transpose* g^t of g, we first recall the definition of g^t and some of its properties. Although this is not necessary, it will be convenient to *assume henceforth in this section* that $\mathrm{char}(K) \nmid N$.

Proposition 23 *If* $g \in \mathrm{Hom}(E[N], E'[N])$*, then there exists a unique homomorphism* $g^t \in \mathrm{Hom}(E'[N], E[N])$ *such that*

$$e_N^{E'} \circ (g \times 1_{E'[N]}) \ = \ e_N^E \circ (1_{E[N]} \times g^t), \tag{21}$$

where $e_N^E : E[N] \times E[N] \to \mu_N$ *is the usual* e_N*-pairing on* E*. Moreover, we have*

$$(g^t)^t \;=\; g, \tag{22}$$

$$g^t g \;=\; [\det(g)]_{E[N]}, \tag{23}$$

for all $g \in \mathrm{Hom}(E[N], E'[N])$*, where* $\det(g) \in \mathbb{Z}/N\mathbb{Z}$ *is the unique number such that*

$$e_N^{E'} \circ (g \times g) \;=\; [\det(g)]_{\mu_N} \circ e_N^E. \tag{24}$$

Proof. The existence and uniqueness of g^t follows from the non-degeneracy of e_N^E. By skew-symmetry we have $e_N^E \circ ((g^t)^t \times 1) = [-1] \circ e_N^E \circ (1 \times (g^t)^t) = [-1] e^{E'} \circ (g^t \times 1) = e^{E'} \circ (1 \times g^t) = e^{E'} \circ (g \times 1)$, and so $(g^t)^t = g$ by the non-degeneracy of e_N^E.

The existence of a unique $\det(g) \in \mathbb{Z}/N\mathbb{Z}$ satisfying (24) was explained in [5], §4. Thus, since $e_N^E \circ (1 \times g^t g) = e_N^E \circ (1 \times g^t) \circ (1 \times g) = e_N^{E'} \circ (g \times 1) \circ (1 \times g) = [\det(g)] \circ e_N^E = e_N^E \circ (1 \times [\det(g)])$, we see that equation (23) follows from the non-degeneracy of e_N^E. □

Corollary 24 *If* $g \in \mathrm{End}(E[N])$*, then*

$$g^t + g \;=\; [\mathrm{tr}(g)]_{E[N]}, \tag{25}$$

where the trace $\mathrm{tr}(g) \in \mathbb{Z}/N\mathbb{Z}$ *is defined by*

$$\mathrm{tr}(g) \;:=\; \det(1+g) - \det(g) - 1.$$

Proof. Since the transpose is a homomorphism and since $[1]^t = [1]$, we obtain from (23) that $[\mathrm{tr}(g)] = (1+g)^t(1+g) - g^t g - 1 = (1+g^t)(1+g) - g^t g - 1 = g^t + g$, which proves (25). □

Remark 25 (a) If $h \in \mathrm{Hom}(E, E')$ is a homomorphism, then its transpose is defined as $h^t := r_{\lambda_E, \lambda_{E'}}(h) = \lambda_{E'}^{-1} \circ \hat{h} \circ \lambda_E$, where (as before) $\lambda_E = \phi_{0_E} : E \xrightarrow{\sim} \hat{E}$ is the canonical principal polarization of E. By Proposition III.8.2 of [17] we have

$$(h_{|E[N]})^t \;=\; (h^t)_{|E'[N]}, \quad \text{and hence} \quad \det(h_{|E[N]}) \equiv \deg(h) \,(\mathrm{mod}\ N), \tag{26}$$

by (23) because $h^t \circ h = [\deg(h)]_E$. Note also that if $h \in \mathrm{End}(E)$, then if follows from (26) and the definitions that $\mathrm{tr}(h_{|E[N]}) \equiv \mathrm{tr}(h) \,(\mathrm{mod}\ N)$.

(b) If E''/K is another elliptic curve and if $g_2 \in \mathrm{Hom}(E'[N], E''[N])$, then it is easy to see that

$$(g_2 \circ g_1)^t \;=\; g_1^t \circ g_2^t, \quad \text{for all } g_1 \in \mathrm{Hom}(E[N], E'[N]). \tag{27}$$

(c) Since the transpose is a homomorphism and $[1]^t = [1]$, it follows from (25) that the trace $\mathrm{tr} : \mathrm{End}(E[N]) \to \mathbb{Z}/N\mathbb{Z}$ is a homomorphism with

$$\mathrm{tr}([m]_{E[N]}) \;\equiv\; 2m \,(\mathrm{mod}\ N), \quad \text{for all } m \in \mathbb{Z}. \tag{28}$$

Next we observe that the transpose (and hence det and tr) are compatible when we restrict $g \in \mathrm{Hom}(E[N], E'[N])$ to the subgroup $E[M]$, where $M|N$. More precisely, if $\pi^E_{N,M} : E[N] \to E[M]$ is the surjective map induced by multiplication by $\overline{N} := \frac{N}{M}$, then there exists a unique homomorphism $g_M = \rho_{N,M}(g) \in \mathrm{Hom}(E[M], E'[M])$ such that

$$\pi^{E'}_{N,M} \circ g \;=\; g_M \circ \pi^E_{N,M}, \;\text{ and hence }\; g_{|E[M]} = \varepsilon^{E'}_{M,N} \circ g_M, \tag{29}$$

where $\varepsilon^{E'}_{M,N} : E'[M] \hookrightarrow E'[N]$ is the canonical inclusion. In particular, we see that $\rho_{N,M}(\rho_N(h)_M) = \rho_M(h)$, for $h \in \mathrm{Hom}(E, E')$. Since

$$e^E_N \circ (1_{E[N]} \times \varepsilon^E_{M,N}) \;=\; e^E_M \circ (\pi^E_{N,M} \times 1_{E[M]}) \tag{30}$$

by [17], Proposition III.8.1(e), it follows immediately that

$$(g^t)_M \;=\; (g_M)^t, \quad \text{for all } g \in \mathrm{Hom}(E[N], E'[N]). \tag{31}$$

In particular, from (23) we obtain that

$$\det(g_M) \;\equiv\; \det(g) \,(\mathrm{mod}\ M), \quad \text{for all } g \in \mathrm{Hom}(E[N], E'[N]). \tag{32}$$

5 The determinant of q_C

In this section we prove the main structure theorems (Theorems 2 and 3) of the refined Humbert invariant q_C. Thus, let C/K be a curve of genus 2 over an arbitrary ground field K, and suppose that (E, E', ψ) is a presentation of degree N of C/K or, more correctly, of (J_C, λ_C), in the sense of §2.

The most difficult part of Theorem 2 (respectively, of Theorem 3) is the discriminant formula (i) (respectively, the determinant formula (i′)). As we shall see, both formulae follow easily from the following formula (33) for the determinant of the quadratic form $d_C = d_{J_C}$ on $\mathrm{NS}'(J_C)$ which is defined by the intersection pairing, i.e., $d_C(D) = \frac{1}{2}(D.D)$, for $D \in \mathrm{NS}'(J_C)$. Note that $d_C(D) = \chi(\mathcal{O}_{J_C}(D)) \in \mathbb{Z}$ by the Riemann-Roch Theorem; cf. [16], p. 150.

Theorem 26 *Let C/K be curve of genus 2 with presentation (E, E', ψ) of degree N. If $\mathrm{char}(K) \nmid N$, and if $r = \mathrm{rank}(\mathrm{Hom}(E, E')) \geq 1$, then the determinant of intersection form d_C on $\mathrm{NS}'(J_C)$ is given by*

$$\det(d_C) \;=\; (-1)^{r+1} m_\psi^2 \det(q_{E,E'}), \tag{33}$$

where m_ψ is the isogeny defect of ψ, and $q_{E,E'}$ is the degree form on $\mathrm{Hom}(E, E')$.

Here, as in [8], the *determinant* of a quadratic form q on a module $M \simeq \mathbb{Z}^r$ is the determinant of the associated Gram matrix of any basis $x_1, \ldots, x_r$ of M, i.e.,

$$\det(q) \;=\; \det((M,q)) \;=\; \det(G_q(x_1,\ldots,x_r)),$$

where $G_q(x_1,\ldots,x_r) = (b_q(x_i,x_j))_{1\le i,j,\le r}$ is the Gram matrix and b_q is the associated bilinear form which is given by $b_q(x,y) = q(x+y) - q(x) - q(y)$, for all $x, y \in M$.

As we will see presently, Theorem 26 follows almost immediately from the following index formula.

Theorem 27 *Let (E, E', ψ) be an N-presentation over K with associated quotient data $(\pi_\psi, A_\psi, \lambda_\psi)$ as in* Proposition 10(b). *If $A = E \times E'$ and $\mathrm{char}(K) \nmid N$, then*

$$[\mathrm{NS}'(A) : \pi_\psi^* \mathrm{NS}'(A_\psi)] \;=\; m_\psi N^\rho, \tag{34}$$

where $\rho = \mathrm{rank}(\mathrm{NS}'(A_\psi)) = \mathrm{rank}(\mathrm{NS}(A_\psi)) = \mathrm{rank}(\mathrm{NS}(A)) = \mathrm{rank}(\mathrm{Hom}(E,E')) + 2$ is the Picard number of A_ψ and of A, and m_ψ is the isogeny defect of ψ.

We first show how Theorem 26 follows from the Index Theorem 27. For this, we require the following preliminary results.

Lemma 28 *If E/K and E'/K are elliptic curves over an arbitrary field K, then the rule $(a,b,h) \mapsto \alpha(a,b,h) := \begin{pmatrix} [a]_E & h^t \\ h & [b]_{E'} \end{pmatrix}$ defines an isomorphism*

$$\alpha_{E,E'} : \tilde{\mathcal{H}}_{E,E'} := \mathbb{Z} \times \mathbb{Z} \times \mathrm{Hom}(E,E') \;\xrightarrow{\sim}\; \mathrm{End}_\lambda(A),$$

where $\lambda = \lambda_E \otimes \lambda_{E'}$ is the product polarization on $A = E \times E'$. In addition, Φ_λ is surjective, and hence we have isomorphisms

$$\Phi_\lambda : \mathrm{NS}(A) \;\xrightarrow{\sim}\; \mathrm{End}_\lambda(A) \quad \textit{and} \quad \overline{\delta}_{\overline{K}/K} : \mathrm{NS}(A) \;\xrightarrow{\sim}\; \mathrm{NS}'(A).$$

Moreover, if we put $\mathbf{D}(a,b,h) = \Phi_\lambda^{-1}(\alpha_{E,E'}(a,b,h))$, for $(a,b,h) \in \tilde{\mathcal{H}}_{E,E'}$, then

$$d_A(\mathbf{D}(a,b,h)) \;=\; ab - \deg(h) \;=\; ab - q_{E,E'}(h), \tag{35}$$

$$\tilde{q}_{(A,\lambda)}(\mathbf{D}(a,b,h)) \;=\; (a-b)^2 + 4\deg(h). \tag{36}$$

Thus, if $r = \mathrm{rank}(\mathrm{Hom}(E,E')) \ge 1$, then

$$\det(d_A) \;= (-1)^{r+1} \det(q_{E,E'}). \tag{37}$$

Proof. Since $\mathrm{End}_{\lambda_E}(E) = \{[m]_E : m \in \mathbb{Z}\} \simeq \mathbb{Z}$, and similarly $\mathrm{End}_{\lambda_{E'}}(E') \simeq \mathbb{Z}$, the first assertion follows immediately from Proposition 61 of [8]. (Note that this proposition holds for an arbitrary ground field K.)

For $(a,b,h) \in \tilde{\mathcal{H}}_{E,E'}$, put $\tilde{\mathbf{D}}(a,b,h) := (a-d)\theta_E + (b-1)\theta_{E'} + \Gamma_{-h} \in \mathrm{Div}(A)$, where $d = \deg(h)$, $\theta_E = \mathrm{pr}_E^*(0_E)$, $\theta_{E'} = \mathrm{pr}_{E'}^*(0_{E'})$, and Γ_{-h} denotes the graph of $-h$. By formula (23) of [8] we have

$$\Phi_\lambda(\mathrm{cl}(\tilde{\mathbf{D}}(a,b,h))) \;=\; \alpha_{E,E'}(a,b,h), \quad \text{for all } (a,b,h) \in \tilde{\mathcal{H}}_{E,E'}, \tag{38}$$

and so Φ_λ is surjective and hence is an isomorphism because Φ_λ is always injective. We thus have that $\mathbf{D}(a,b,h) = \mathrm{cl}(\tilde{\mathbf{D}}(a,b,h))$ and that $\overline{\delta}_{\overline{K}/K}\mathrm{NS}(A) = \beta_{\overline{K}/K}(\mathrm{End}_\lambda(A)) = \mathrm{NS}'(A)$, and so we obtain the indicated isomorphism.

By formula (22) of [8] we obtain that $d_A(\mathbf{D}(a,b,h)) = \frac{1}{2}(\mathbf{D}(a,b,h).\mathbf{D}(a,b,h)) = ab - \deg(h)$, which is (35). Moreover, since $\lambda = \phi_\theta$, where $\theta = \mathbf{D}(1,1,0)$, we see that (36) follows from formula (22) of [8] because $(\mathbf{D}(a,b,h).\theta) = a+b$.

The last assertion follows from (35) as in [8], Corollary 24. Thus, if $f_1,\dots,f_r$ is a basis of $\mathcal{H}_{E,E'}$, and if we put $D_i = \mathbf{D}(0,0,f_i)$, for $1 \le i \le r$, then $\theta_E, \theta_{E'}, D_1, \dots, D_r$ is a basis of $\mathrm{NS}(A)$, and so we see from (35) that the Gram matrix $G_{d_A}(\theta_E, \theta_{E'}, D_1, \dots, D_r)$ of the intersection form d_A with respect to this basis is given by the block diagonal matrix

$$G_{d_A}(\theta_E, \theta_{E'}, D_1, \dots, D_r) = \mathrm{diag}\left(\left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right), -G_q(f_1,\dots,f_r)\right),$$

where $G_q(f_1,\dots,f_r)$ is the Gram matrix of $q = q_{E,E'}$ with respect to the basis $f_1,\dots,f_r$. From this, formula (37) follows by taking the determinant of both sides. □

Lemma 29 *Let A_1/K and A_2/K be two abelian surfaces and let $\pi : A_1 \to A_2$ be an isogeny of degree N^2. If $\rho = \mathrm{rank}(\mathrm{NS}'(A_1))$, then*

$$\det(d_{A_2}) = (M/N^\rho)^2 \det(d_{A_1}), \quad \textit{where } M = [\mathrm{NS}'(A_1) : \pi^*(\mathrm{NS}'(A_2))]. \tag{39}$$

Proof. Put $\mathrm{NS}_i = \mathrm{NS}'(A_i)$ and $d_i = d_{A_i}$, for $i = 1, 2$. Viewing $\pi^*\mathrm{NS}_2$ as a quadratic subspace of NS_1 via the intersection form d_1 on NS_1, we see that $\det((\pi^*\mathrm{NS}_2, d_1)) = M^2 \det((\mathrm{NS}_1, d_1))$. On the other hand, by the projection formula we have that $d_1(\pi^*(D)) = N^2 d_2(D)$, for all $D \in \mathrm{NS}_2$, so $\det((\pi^*\mathrm{NS}_2, d_1)) = N^{2\rho}\det((\mathrm{NS}_2, d_2))$, and hence (39) follows. □

Proof of Theorem 26 (using Theorem 27): Since $(J_C, \lambda_C) \simeq (A_\psi, \lambda_\psi)$ by Proposition 10(c) and $\pi = \pi_\psi$ satisfies the hypotheses of Lemma 29, and since $M = m_\psi N^\rho$ by Theorem 27, we see that (33) follows from (39) and (37) because

$$\det(d_C) \;=\; (M/N^\rho)^2 \det(d_A) \;=\; m_\psi^2 \det(d_A) \;=\; (-1)^{r+1} m_\psi^2 \det(q_{E,E'}).$$

□

Before proving the Index Theorem 27, let us see how the main structure theorem (Theorem 3) follows from Theorem 26. For this, we use the following result which is analogous to Proposition 9 of [8] and which is proved in the same way.

Lemma 30 *Let A/K be an abelian surface with principal polarization λ, and let $\rho = \mathrm{rank}(\mathrm{NS}'(A))$. Then the determinant of $q_{(A,\lambda)}$ on $\mathrm{NS}(A,\lambda)$ is given by*

$$\det(q_{(A,\lambda)}) \;=\; \tfrac{1}{2}(-4)^{\rho-1}\det(d_A). \tag{40}$$

Proof of Theorem 3 (using Theorems 26 and 27). By (13) we know that q_C is an integral, positive definite quadratic form in t variables, where $t = \mathrm{rank}(\mathrm{NS}(J_C,\lambda)) = \rho - 1$, and $\rho = \mathrm{rank}(\mathrm{NS}'(J_C))$. By Theorem 27 we know that $\rho = r+2$, where $r = \mathrm{rank}(\mathrm{Hom}(E,E'))$, so $t = r+1$. This proves the first assertion of Theorem 3.

To prove property (i′), note that by Lemma 30 and Theorem 26 we obtain that

$$\det(q_C) = \tfrac{1}{2}(-4)^{r+1}\det(d_C) = \tfrac{1}{2}(-4)^{r+1}(-1)^{r+1}m_\psi^2\det(q_{E,E'}) = 2^{2r+1}m_\psi^2\det(q_{E,E'}).$$

To prove property (ii), we observe that the hypothesis implies by Proposition 10 that J_C has an elliptic subgroup $E \le J_C$ of λ_C-degree N, and so q_C represents N^2 primitively by Theorem 18.

For property (iii) we note that $\tilde{q}_C(D) = (D.\theta)^2 - 4d_C(D) \equiv (D.\theta)^2 \pmod 4$, and so $\tilde{q}_C(D) \equiv 0$ or $1 \pmod 4, \forall D \in \mathrm{End}_{\lambda_C}(J_C)$. Thus, property (iii) holds.

Finally, since $\tilde{q}_{C_{\overline{K}}}$ does not represent 1 by Proposition 6 of [8], the same is true for its restriction $\tilde{q}_C$ to $\mathrm{NS}'(A)$, and so property (iv) holds. □

Proof of Theorem 4 (using Theorem 26). If $m_\psi = 1$, then by definition $\psi = h_{|E[N]}$ for some $h \in \mathrm{End}(E,E')$. Put (as in [1]) $\nu := \left(\begin{smallmatrix}[N] & 0\\ h & [1]\end{smallmatrix}\right) \in \mathrm{End}(E\times E')$. Then $\mathrm{Ker}(\nu) = \mathrm{Graph}(-\psi)$, so $J_C \simeq (E\times E')/\mathrm{Graph}(-\psi) \simeq E\times E'$.

Conversely, suppose that there exists an isomorphism $\alpha : A := E\times E' \xrightarrow{\sim} J_C$. Then $r \ge 1$ by [8], Prop. 26, and $\mathrm{NS}'(A) = \alpha^*\mathrm{NS}'(J_C)$ and $d_A(\alpha^*D) = d_C(D)$, for $D \in \mathrm{NS}'(J_C)$, so by Lemma 28 we obtain that $\det(d_C) = \det(\mathrm{NS}'(J_C), d_C)) = \det(\mathrm{NS}'(A), d_A)) = (-1)^{r+1}\det(q_{E,E'})$. Comparing this to formula (33) for $\det(d_C)$ shows that $m_\psi^2 = 1$, so $m_\psi = 1$, as claimed. □

Proof of Corollary 5 (using Theorems 26 and 27). The first hypothesis implies by Corollary 12 that C/K has an N-presentation (E,E',ψ) over K, where $E' = E_f^\perp$ and $\psi = \psi_f$. By Theorem 27 we have that $r = \rho - 2 \ge 1$, so by Theorem 3 (which was proved above) we have that $\det(q_C)/2^{2\rho-3} = m_\psi^2\det(q_{E,E'})$. Since this is assumed to be squarefree, it follows that $m_\psi = 1$, and so $J_C \simeq E\times E'$ by Theorem 4. □

Proof of Theorem 2 (using Theorem 3). If $q(x,y) = ax^2+bxy+cy^2$ is a binary quadratic form, then $\mathrm{disc}(q) \;=\; b^2-4ac \;=\; -\det\begin{pmatrix} 2a & b\\ b & 2c\end{pmatrix} = -\det(q)$. Since here

$r = 1$ and $\det(q_{E,E'}) = \det((2\deg(h))) = 2d$, we see that the discriminant formula follows immediately from the determinant formula (i′) of Theorem 3.

Thus, to finish the proof of Theorem 2, we only need to verify that $m|N$ and that $\gcd(N/m, d) = 1$. For this, note first that $m = m_\psi | N$ by Remark 21. Next, since here $\mathcal{H}_{E,E'} = \mathbb{Z}h$, we have by definition that $\exists k \in \mathbb{Z}$ such that $m\psi = kh_{|E[N]}$. Since $\mathrm{ord}(h_{|E[N]}) = |(\mathcal{H}_{E,E^n})_N| = N$ by Lemma 22, we see that $\frac{N}{(k,N)} = \mathrm{ord}(kh_{|E[N]}) = \mathrm{ord}(m\psi) = \frac{N}{m}$, and hence $m = (k, N)$. Put $\bar{k} = \frac{k}{m}$ and $\bar{N} = \frac{N}{m}$. Since $mE[N] = E[\bar{N}]$, we see that $\bar{k}h_{|E[\bar{N}]} = \psi_{|E[\bar{N}]}$, so $\rho_{\bar{N}}(\bar{k}h) = \psi_{\bar{N}}$ in the notation of (29). Taking determinants, we obtain by (32) that $\bar{k}^2 d \equiv \det(\bar{k}h_{|E[\bar{N}]}) \equiv \det(\psi_{\bar{N}}) \equiv \det(\psi) \equiv -1 \pmod{\bar{N}}$, and so $(d, \bar{N}) = 1$, as desired. □

6 The index formula

We now turn to the proof of the Index Theorem 27. For technical reasons and for greater generality, it is useful to generalize the theorem as follows.

Theorem 31 *Let E/K and E'/K be elliptic curves and let $\psi \in \mathrm{Hom}(E[N], E'[N])$. Moreover, let $G_\psi = \mathrm{Graph}(-\psi)$ be the graph of $-\psi$ and let*

$$\pi = \pi_\psi : A := E \times E' \to A_\psi := (E \times E')/G_\psi,$$

be the associated quotient isogeny. Assume that A_ψ has a principal polarization λ_ψ. In addition, let $\mathcal{H} \leq \mathrm{Hom}(E, E')$ be a primitive subgroup, and put

$$\tilde{\mathcal{H}} \;=\; \{\mathbf{D}'(a, b, h)) : a, b \in \mathbb{Z},\, h \in \mathcal{H}\} \;\leq\; \mathrm{NS}'(A),$$

where $\mathbf{D}'(a, b, h) = \overline{\delta}_{\overline{K}/K}\mathbf{D}(a, b, h) = \mathbf{D}(a, b, h_{\overline{K}})$. If $\mathrm{char}(K) \nmid m_\psi(\mathcal{H})$, then

$$[\tilde{\mathcal{H}} : \pi_\psi^*(\mathrm{NS}'(A_\psi)) \cap \tilde{\mathcal{H}}] \;=\; m_\psi(\mathcal{H})N^{r_\mathcal{H}+2}, \tag{41}$$

where $r_\mathcal{H} = \mathrm{rank}(\mathcal{H})$ and $m_\psi(\mathcal{H})$ is the isogeny defect of ψ with respect to $\mathcal{H}$.

Proof of Theorem 27 (using Theorem 31). Since ψ is an anti-isometry, we know by Proposition 10(b) that there is principal polarization λ_ψ on A_ψ, and so we can apply Theorem 31 with $\mathcal{H} = \mathrm{Hom}(E, E')$. Then $\tilde{\mathcal{H}} = \overline{\delta}_{\overline{K}/K}(\mathrm{NS}(A)) = \mathrm{NS}'(A)$ by Lemma 28, so (41) implies (34) with $\rho = r_\mathcal{H} + 2 = \mathrm{rank}(\mathrm{NS}'(A)) = \mathrm{rank}(\mathrm{NS}(A))$. Moreover, since π_ψ^* is injective (cf. Proposition 17), we see from (34) that $\mathrm{rank}(\mathrm{NS}'(A)) = \mathrm{rank}(\mathrm{NS}'(A_\psi))$. Finally, since by Proposition 14 we know that $\mathrm{rank}(\mathrm{NS}(A_\psi)) = \mathrm{rank}(\mathrm{NS}'(A_\psi))$, the rank assertions follow. □

We now turn to the proof of Theorem 31. If $m_\psi(\mathcal{H}) = 1$, then (41) follows easily from the following result.

Proposition 32 *In the situation of* Theorem 31 *put* $\nu_{N,h} = \begin{pmatrix} [N] & 0 \\ h & [1] \end{pmatrix} \in \mathrm{End}(A)$, *where* $h \in \mathcal{H}$. *Then*

$$\nu_{N,h}^*(D) \;=\; \mathbf{D}'(aN^2 + bd + Nt, b, fN + bh), \quad \forall D = \mathbf{D}'(a,b,f) \in \tilde{\mathcal{H}}, \tag{42}$$

where $d = \deg(h)$ *and* $t = \mathrm{tr}(h^t f)$, *and hence*

$$D \in \nu_{N,h}^* \mathrm{NS}'(A) \quad \Leftrightarrow \quad \rho_N(f) = \rho_N(bh) \;\; \textit{and} \;\; \varphi_h(D) \equiv 0 \,(\mathrm{mod}\ N^2), \tag{43}$$

where $\varphi_h(\mathbf{D}'(a,b,f)) = a + bd - \mathrm{tr}(h^t f)$. *Thus,*

$$\tilde{\mathcal{H}} \cap \nu_{N,h}^* \mathrm{NS}'(A) \;=\; \nu_{N,h}^*(\tilde{\mathcal{H}}), \tag{44}$$

and hence

$$[\tilde{\mathcal{H}} : \nu_{N,h}^*(\tilde{\mathcal{H}})] \;=\; N^{r_{\mathcal{H}}+2}. \tag{45}$$

Proof. The formula (42) follows immediately from formula (76) of [8]. Thus, if $D = \mathbf{D}'(a,b,f)$ satisfies $\rho_N(f) = \rho_N(bh)$ and $\varphi_h(D) = cN^2$, then $(f - bh)_{E[N]} = 0$, so $f - bh = f_0 N$ with $f_0 \in \mathrm{Hom}(E, E')$, and then $D = \nu_{N,h}^*(\mathbf{D}'(c, b, f_0))$ by (42) because $\varphi_h(D) + bd + N\mathrm{tr}(h^t f_0) = a + 2bd + \mathrm{tr}(h^t(Nf_0 - f)) = a + 2bd - \mathrm{tr}(bh^t h) = a$.

Conversely, if $D = \mathbf{D}'(a,b,f) \in \nu_{N,h}^* \mathrm{NS}'(A)$, then $D = \nu_{N,h}^*(D')$, for some $D' = \mathbf{D}'(a', b', f')$. Thus by (42) we have that $b = b'$, and $f = Nf' + bh$, so $\rho_N(f) = \rho_N(bh)$. Moreover, $a = N^2 a' + bd + N\mathrm{tr}(h^t f')$, so $N^2 a' = a - bd - \mathrm{tr}(h^t(f - bh)) = \varphi_h(D)$, and hence $\varphi_h(D) \equiv 0 \,(\mathrm{mod}\ N^2)$. This proves (43).

To prove (44), note first that $\nu_{N,h}^*(\tilde{\mathcal{H}}) \subset \tilde{\mathcal{H}} \cap \nu_{N,h}^* \mathrm{NS}'(A)$ by (42). Now suppose conversely that $D = \mathbf{D}'(a,b,f) \in \tilde{\mathcal{H}} \cap \nu_{N,h}^* \mathrm{NS}'(A)$. Then by (43) we have that $f = bh + Nf'$, for some $f' \in \mathcal{H}_{E,E'} := \mathrm{Hom}(E, E')$ and $\varphi_h(D) = kN^2$, for some $k \in \mathbb{Z}$. Thus $\mathrm{tr}(h^t f) = 2bd + N\mathrm{tr}(h^t f')$ and so $Nk^2 + bd + N\mathrm{tr}(h^t f') = a$. Thus $D = \nu_{N,h}^* \mathbf{D}'(k, b, f')$ by (42). Now $f' \in \mathcal{H}$ because $Nf' = f - bh \in \mathcal{H}$ and $\mathcal{H}$ is a primitive subgroup of $\mathcal{H}_{E,E'}$. Thus, $\mathbf{D}'(k, b, f') \in \tilde{\mathcal{H}}$, and so $D = \nu_{N,h}^* \mathbf{D}'(k, b, f') \in \nu_{N,h}^* \tilde{\mathcal{H}}$. This proves (44).

Let $\rho_h : \mathrm{NS}'(A) \to \mathrm{Hom}(E[N], E'[N])$ and $\tilde{\varphi}_h : \mathrm{NS}'(A) \to \mathbb{Z}/N^2\mathbb{Z}$ be defined by $\rho_h(\mathbf{D}'(a,b,f)) = \rho_N(f - bh)$ and by $\tilde{\varphi}_h(D) = \varphi_h(D) \,(\mathrm{mod}\ N^2)$, respectively. Then (43) states that

$$\nu_{N,h}^* \mathrm{NS}'(A) \;=\; \mathrm{Ker}(\rho_h) \cap \mathrm{Ker}(\tilde{\varphi}_h). \tag{46}$$

Since $\rho_h(\mathbf{D}'(0,0,f)) = \rho_N(f)$, we see that $\rho_h(\tilde{\mathcal{H}}) = \mathcal{H}_N$, and so

$$[\tilde{\mathcal{H}} : \tilde{\mathcal{H}} \cap \mathrm{Ker}(\rho_h)] \;=\; |\mathcal{H}_N| \;=\; N_{\mathcal{H}}^r,$$

the latter by (20). Moreover, since $\mathbf{D}'(1,0,0) \in \tilde{\mathcal{H}} \cap \mathrm{Ker}(\rho_h)$ and $\varphi_h(\mathbf{D}'(1,0,0)) = 1$, we see that

$$[\tilde{\mathcal{H}} \cap \mathrm{Ker}(\rho_h) : \tilde{\mathcal{H}} \cap \nu_{N,h}^* \mathrm{NS}'(A)] \;=\; |\tilde{\varphi}_h(\tilde{\mathcal{H}} \cap \mathrm{Ker}(\rho_h))| = N^2,$$

and so (45) follows by using (44). □

The main task in working out the index (41) in the general case is to find a useful characterization of the elements of $\mathcal{N}_\psi := \pi_\psi^* \mathrm{NS}'(A_\psi)$ inside $\mathcal{N} = \mathrm{NS}'(A)$. Now by Remark 15 it is clear that this problem is equivalent to the (easier) problem of characterizing the elements of the group $\mathcal{E}_\psi := \pi_\psi^\flat \mathrm{End}_{\lambda_\psi}(A_\psi)$ inside $\mathcal{E} := \mathrm{End}_\lambda(A)$. A first step towards this goal is given by the following general result.

Proposition 33 *Let (A_i, λ_i), $i = 1, 2$ be two principally polarized abelian varieties and let $\pi : A_1 \to A_2$ be an isogeny. Put $\pi' = \lambda_1^{-1} \hat{\pi} \lambda_2 \in \mathrm{Hom}(A_2, A_1)$. If $\alpha \in \mathrm{End}(A_1)$ and $\beta \in \mathrm{Hom}(A_2, A_1)$, then*

(a) *$\alpha = \beta_1 \circ \pi$, for some $\beta_1 \in \mathrm{Hom}(A_2, A_1)$ $\Leftrightarrow$ $\mathrm{Ker}(\pi) \leq \mathrm{Ker}(\alpha)$.*

(b) *$\beta = \pi' \circ \gamma$, for some $\gamma \in \mathrm{End}(A_2)$ $\Leftrightarrow$ $\mathrm{Ker}(\pi) \leq \mathrm{Ker}(\hat{\beta} \circ \lambda_1)$.*

(c) *$\alpha \in \mathrm{Im}(\pi^\flat) \Leftrightarrow \alpha = \beta \circ \pi$, for some $\beta \in \mathrm{Hom}(A_2, A_1)$, and $\mathrm{Ker}(\pi) \leq \mathrm{Ker}(\hat{\beta} \circ \lambda_1)$.*

Proof. (a) This follows from the universal property of quotients, using the fact that (A_2, π) is a quotient of A_1 by the group scheme $\mathrm{Ker}(\pi)$.

(b) We have that $\beta = \pi' \circ \gamma$, for some $\gamma \in \mathrm{End}(A_2) \Leftrightarrow \hat{\beta} = \hat{\gamma} \circ (\pi')^\wedge$, for some $\hat{\gamma} \in \mathrm{End}(\hat{A}_2)$. Since $(\pi')^\wedge = \lambda_2 \circ \pi \circ \lambda_1^{-1}$ by (11), we see that the given condition is equivalent to $\hat{\beta} \circ \lambda_1 = \gamma' \circ \pi$, for some $\gamma' = \hat{\gamma} \circ \lambda_2 \Leftrightarrow \mathrm{Ker}(\pi) \leq \mathrm{Ker}(\hat{\beta} \circ \lambda_1)$, the latter by the same reason as in part (a).

(c) Since $\alpha \in \mathrm{Im}(\pi^\flat) \Leftrightarrow \alpha = \pi' \circ (\gamma \circ \pi)$, for some $\gamma \in \mathrm{End}(A_2)$, this follows immediately from part (b). □

Corollary 34 *Suppose that $\alpha \in \mathrm{End}_{\lambda_1}(A_1)$. Then $\alpha \in \pi^\flat \mathrm{End}_{\lambda_2}(A_2)$ if and only if $\alpha = \beta \circ \pi$, for some $\beta \in \mathrm{Hom}(A_2, A_1)$ with $\mathrm{Ker}(\pi) \leq \mathrm{Ker}(\hat{\beta} \circ \lambda_1)$.*

Proof. This follows immediately from Proposition 33 and the fact that

$$\pi^\flat \mathrm{End}_{\lambda_2}(A_2) \;=\; \pi^\flat \mathrm{End}(A_2) \cap \mathrm{End}_{\lambda_1}(A_1). \tag{47}$$

To verify (47), note first that $\pi^\flat \mathrm{End}_{\lambda_2}(A_2) \leq \pi^\flat \mathrm{End}(A_2) \cap \mathrm{End}_{\lambda_1}(A_1)$ by (8). Conversely, suppose that $\alpha = \pi^\flat(\beta) \in \mathrm{End}_\lambda(A_1)$, where $\beta \in \mathrm{End}(A_2)$. Then by (8) again we have that $\pi^\flat(r_{\lambda_2}(\beta)) = r_{\lambda_1}(\pi^\flat(\beta)) = \pi^\flat(\beta)$, and so $r_{\lambda_2}(\beta) = \beta$ because $\pi^\flat$ is injective (since π and π' are isogenies). Thus $\beta \in \mathrm{End}_{\lambda_2}(A_2)$, and so $\alpha \in \pi^\flat \mathrm{End}_{\lambda_2}(A_2)$. This proves the opposite inclusion and hence (47). □

Corollary 35 *If* $\mathrm{Ker}(\pi) \leq A_1[N]$, *then* $N\mathrm{End}(A_1) \leq \mathrm{Hom}(A_2, A_1)\pi$. *Thus, if* $\mathrm{char}(K) \nmid N$, *and if* $\alpha \in \mathrm{End}(A_1)$, *then*

$$N\alpha \in \pi^\flat \mathrm{End}(A_2) \;\Leftrightarrow\; e_N^{\lambda_1}(\alpha(x), y) = 1,\ \forall x, y \in \mathrm{Ker}(\pi)(\overline{K}). \tag{48}$$

Proof. Since $\mathrm{Ker}(\pi) \leq A_1[N]$, there exists $\pi' : A_2 \to A_1$ such that $\pi' \circ \pi = [N]_A$. Thus $N\alpha = (\alpha \circ \pi') \circ \pi \in \mathrm{Hom}(A_2, A_1)\pi$, which gives the first assertion.

To prove (48), we thus have by Proposition 33(c) that $N\alpha \in \pi^\flat \mathrm{End}(A_2) \Leftrightarrow \mathrm{Ker}(\pi) \leq \mathrm{Ker}(\hat{\beta} \circ \lambda_1) \Leftrightarrow \hat{\beta}(\lambda_1(x)) = 0, \forall x \in \mathrm{Ker}(\pi)(\overline{K})$, where $\beta = \alpha \circ \pi'$. Since $\hat{\beta}(\lambda_1(x)) \in \hat{A}_2[N]$, it follows from the non-degeneracy of $\bar{e}_N$ that

$$\hat{\beta}(\lambda_1(x)) = 0 \;\Leftrightarrow\; \bar{e}_N(y, \hat{\beta}(\lambda_1(x))) = 1, \forall y \in A_2[N].$$

Now since $\bar{e}_N(y, \hat{\beta}(\lambda_1(x))) = \bar{e}_N(\beta(y), \lambda_1(x)) = \bar{e}_N(\alpha(\pi'(y)), \lambda_1(x))$ (cf. [13], Lemma 16.2(c)) and since $\pi'(A_2[N](\overline{K})) = \mathrm{Ker}(\pi)(\overline{K})$, we see that (48) follows. □

Corollary 36 *In the situation of* Theorem 31 *let* $\alpha = \alpha(a, b, f) \in \mathcal{E}$. *Then*

$$\alpha \in \mathrm{Hom}(A_\psi, A)\pi_\psi \quad \Leftrightarrow \quad f^t\psi = [a]_{E[N]} \text{ and } \rho_N(f) = b\psi. \tag{49}$$

In particular, if $m_\psi(\mathcal{H}) = N$, *then for* $\tilde{\mathcal{H}}' := \Phi'_\lambda(\tilde{\mathcal{H}}) \leq \mathrm{End}_\lambda(A)$ *we have that*

$$\tilde{\mathcal{H}}' \;\cap\; \mathrm{Hom}(A_\psi, A)\pi_\psi \;=\; N\tilde{\mathcal{H}}'. \tag{50}$$

Proof. By Proposition 33(a), we know that $\alpha \in \mathrm{Hom}(A_\psi, A)\pi_\psi \Leftrightarrow \mathrm{Graph}(-\psi) \leq \mathrm{Ker}(\alpha) \Leftrightarrow \alpha \circ \gamma_{-\psi} = 0$, where $\gamma_{-\psi} : E[N] \to A[N]$ is the graph homomorphism of $-\psi$. Since $\alpha \circ \gamma_{-\psi} = ([a]_{E[N]} - f^t\psi, \rho_N(f) - b\psi)$, the assertion (49) follows.

To prove (50), note first that $N\tilde{\mathcal{H}}' \subset \tilde{\mathcal{H}}' \cap \mathrm{Hom}(A_\psi, A)\pi_\psi$ by Corollary 35.

Conversely, if $\alpha = \alpha(a, b, f) \in \tilde{\mathcal{H}}' \cap \mathrm{Hom}(A_\psi, A)\pi_\psi$, then by (49) we have that $b\psi = \rho_N(f) \in \rho_N(\mathcal{H})$, so by (19) we have that $N|b$ and hence $\rho_N(f) = 0$. This means that $f = Nf_0$ with $f_0 \in \mathcal{H}$ by Lemma 22. Thus $[a]_{E[N]} = f^t\psi = Nf_0^t\psi = 0$, so $N|a$, and so $\alpha = N\alpha(\frac{a}{N}, \frac{b}{N}, f_0) \in N\tilde{\mathcal{H}}'$. This proves (50). □

We can use the above results to prove Theorem 31 in the case that $m_\psi(\mathcal{H}) = N$. This follows from the following more general result.

Proposition 37 *In the situation of* Theorem 31, *assume also that* $\mathrm{char}(K) \nmid N$. *If* $D = \mathbf{D}'(a, b, f) \in \mathrm{NS}'(A)$, *then*

$$ND \in \pi_\psi^* \mathrm{NS}'(A_\psi) \quad \Leftrightarrow \quad p_\psi(D) := a + b\det(\psi) - \mathrm{tr}(f^t\psi) \equiv 0 \,(\mathrm{mod}\ N). \tag{51}$$

Proof. Put $\alpha = \Phi'_\lambda(D) = \alpha(a,b,f) \in \mathcal{E} = \mathrm{End}_\lambda(A)$ and $p_\psi(\alpha) = p_\psi(D)$. Then by (10) we see that $ND \in \pi_\psi^* \mathrm{NS}'(A_\psi) \Leftrightarrow N\alpha \in \mathcal{E}_\psi := (\pi_\psi)^\flat_{\lambda,\lambda_\psi} \mathrm{End}_{\lambda_\psi}(A_\psi)$. To characterize the latter condition, we first observe that

$$(52) \quad e_N^\lambda(\alpha(k_1), k_2) \;=\; e_N^E(x_1, x_2)^{p_\psi(\alpha)}, \quad \forall k_i = (x_i, -\psi(x_i)) \in \mathrm{Ker}(\pi_\psi)(\overline{K}), i = 1, 2.$$

Indeed, since $\alpha(k_1) = (y_1, y_2)$ with $y_1 = ax_1 - f^t\psi(x_1)$, $y_2 = f(x_1) - b\psi(x_1)$, we have $e_N^\lambda(\alpha(k_1), k_2) = e_N^E(y_1, x_2) e_N^{E'}(y_2 - \psi(x_2)$; cf. the proof of Corollary 5.6 of [5]. Thus $e_N^\lambda(\alpha(k_1), k_2) = e_N(x_1, x_2)^a e_N(-f^t\psi(x_1), x_2) e_N(f(x_1), -\psi(x_2)) e_N(-b\psi(x_1) - \psi(x_2))$. Since $e_N(f(x_1), \psi(x_2)) = e_N(x_1, f^t\psi(x_2))$, and since

$$e_N^E(g(x_1), x_2) e_N^E(x_1, g(x_2)) = e_N^E(x_1, g^t(x_2) + g(x_2)) = e_N^E(x_1, x_2)^{\mathrm{tr}(g)}, \; \forall g \in \mathrm{End}(E[N]),$$

we thus see that $e_N^\lambda(\alpha(k_1), k_2) = e_N(x_1, x_2)^{a + b\det(\psi) - \mathrm{tr}(f^t\psi)}$. This proves (52).

Thus, by (48) and (52) we obtain that $N\alpha \in \mathcal{E}_\psi \Leftrightarrow e_N^\lambda(\alpha(k_1), k_2) = 1, \forall k_i \in G_\psi(\overline{K}) \Leftrightarrow e_N^E(x_1, x_2)^{p_\psi(\alpha)} = 1, \forall x_i \in E[N](\overline{K}) \Leftrightarrow p_\psi(\alpha) \equiv 0 \,(\mathrm{mod}\ N)$ by the non-degeneracy of e_N^E. This proves (51). □

Corollary 38 *If $m_\psi(\mathcal{H}) = N$ and $\mathrm{char}(K) \nmid N$, then*

$$(53) \qquad \tilde{\mathcal{H}} \cap \pi_\psi^* \mathrm{NS}'(A_\psi) \;=\; N(\tilde{\mathcal{H}} \cap \mathrm{Ker}(p_\psi)),$$

where $p_\psi : \mathrm{NS}'(A) \to \mathbb{Z}/N\mathbb{Z}$ is as in (51)*. Thus,*

$$(54) \qquad [\tilde{\mathcal{H}} : \tilde{\mathcal{H}} \cap \pi_\psi^* \mathrm{NS}'(A_\psi)] \;=\; N^{r_\mathcal{H}+3}.$$

Proof. Put $\mathcal{N}_\psi := \pi_\psi^* \mathrm{NS}'(A_\psi)$. Then by (51) we have that $N(\tilde{\mathcal{H}} \cap \mathrm{Ker}(p_\psi)) \leq \tilde{\mathcal{H}} \cap \mathcal{N}_\psi$. On the other hand, if $D \in \tilde{\mathcal{H}} \cap \mathcal{N}_\psi$, then $\alpha := \Phi'_\lambda(D) \in \tilde{\mathcal{H}}' \cap \mathcal{E}_\psi$, where as before $\mathcal{E}_\psi = (\pi_\psi)^\flat \mathrm{End}_{\lambda_\psi}(A_\psi)$. Since $\mathcal{E}_\psi \subset \mathrm{Hom}(A_\psi, A)\pi_\psi$, it follows from (50) that $\alpha = N\alpha'$ with $\alpha' \in \tilde{\mathcal{H}}'$, and so $D = ND'$ with $D' \in \tilde{\mathcal{H}}$. Thus, by (51) we obtain that $D' \in \mathrm{Ker}(p_\psi)$, and so $D \in N(\tilde{\mathcal{H}} \cap \mathrm{Ker}(p_\psi))$. This proves (53).

Since $[\tilde{\mathcal{H}} : \tilde{\mathcal{H}} \cap \mathrm{Ker}(p_\psi)] = |p_\psi(\tilde{\mathcal{H}})| = N$ (because $p_\psi(\mathbf{D}'(1,0,0)) \equiv 1 \,(\mathrm{mod}\ N)$), we have by (53) that $[\tilde{\mathcal{H}} : \tilde{\mathcal{H}} \cap \mathcal{N}_\psi] = [\tilde{\mathcal{H}} : N\tilde{\mathcal{H}}][N\tilde{\mathcal{H}} : N(\tilde{\mathcal{H}} \cap \mathrm{Ker}(p_\psi))] = N^{r_\mathcal{H}+2}N = N^{r_\mathcal{H}+3}$, which proves (54). □

By using the following result, we can combine the results of Proposition 32 and of Corollary 38 to deduce Theorem 31.

Proposition 39 *In the situation of* Theorem 31*, put $m = m_\psi(\mathcal{H})$. Then there exists an $h \in \mathcal{H}$ such that $m\psi = m\rho_N(h)$ and we have*

$$(55) \qquad \varepsilon_{N,m}^{E'} \circ \bar{\psi} \circ \pi_{N,m}^E \;=\; \psi - \rho_N(h),$$

for a unique $\bar{\psi} \in \mathrm{Hom}(E[m], E'[m])$. *Moreover, if* $\nu := \nu_{\frac{N}{m},h} \in \mathrm{End}(A)$, *then* $\nu^{-1}G_{\bar{\psi}} = G_\psi$, *and hence there a unique isomorphism* $\alpha_\psi : A_\psi \xrightarrow{\sim} A_{\bar{\psi}}$ *such that*

$$\alpha_\psi \circ \pi_\psi = \pi_{\bar{\psi}} \circ \nu. \tag{56}$$

In addition, $m_{\bar{\psi}}(\mathcal{H}) = m_\psi(\mathcal{H})$.

Proof. By definition there exists $h' \in \mathcal{H}$ such that $m\psi = \rho_N(h')$. Thus, if we put $\bar{N} = \frac{N}{m}$, then this implies that $\rho_N(\bar{N}h') = \bar{N}m\psi = 0$, so $\bar{N}h' = Nh$, for some $h \in \mathcal{H}$ by Lemma 22, and hence $h' = mh$. This proves the first assertion.

The identity $m\psi = m\rho_N(h)$ implies that $\psi_{\bar{N}} = \rho_{\bar{N}}(h)$, where $\psi_{\bar{N}}$ is as in (29), so $E[\bar{N}] \leq \mathrm{Ker}(\psi - \rho_N(h))$. Since $(E[m], \pi^E_{N,m})$ is the quotient of $E[N]$ by $E[\bar{N}]$, it follows that there exists a unique $\bar{\psi} \in \mathrm{Hom}(E[m], E'[N]) = \mathrm{Hom}(E[m], E'[m])$ such that (55) holds.

Next, let $\nu = \nu_{\bar{N},h} = \left(\begin{smallmatrix} [\bar{N}] & 0 \\ h & [1] \end{smallmatrix}\right) \in \mathrm{End}(A)$, and let $\gamma_{-\psi}$ be as in the proof of Corollary 36. Then $\nu \circ \gamma_{-\psi} = \gamma_{-\bar{\psi}} \circ \pi_{N,m}$ because $\nu((x, -\psi(x)) = (\bar{N}x, h(x) - \psi(x)) = (\bar{N}x, -\bar{\psi}(\bar{N}x))$ by (55), and so $\nu(G_\psi) \leq G_{\bar{\psi}}$, or equivalently, $G_\psi \leq \nu^{-1}G_{\bar{\psi}}$. But since $\deg(\nu) = \bar{N}^2$, we have that $|\nu^{-1}G_{\bar{\psi}}| = \bar{N}^2|G_{\bar{\psi}}| = \bar{N}^2m^2 = N^2 = |G_\psi|$, and so $G_\psi = \nu^{-1}G_{\bar{\psi}}$, as claimed.

Since $\mathrm{Ker}(\pi_{\bar{\psi}} \circ \nu) = \nu^{-1}(G_{\bar{\psi}}) = \mathrm{Ker}(\pi_\psi)$ by what was just proved, it follows from the universal property of quotients that there is a unique isomorphism $\alpha_\psi : A_\psi \xrightarrow{\sim} A_{\bar{\psi}}$ such that (56) holds.

It remains to prove that $\bar{m} := m_{\bar{\psi}}(\mathcal{H}) = m$. Since $\bar{\psi} \in \mathrm{Hom}(E[m], E'[m])$, it is clear that $\bar{m}|m$. Now by definition there exists a $g \in \mathcal{H}$ such that $\bar{m}\bar{\psi} = \rho_m(g)$. Then by (55) we have that $\bar{m}(\psi - \rho_N(h)) = \bar{m}\bar{\psi} \circ \pi_{N,m} = \rho_m(g) \circ \pi_{N,m} = \bar{N}\rho_N(g)$, so $\bar{m}\psi = \rho_N(\bar{N}g + \bar{m}h)$. Since $\bar{N}g + \bar{m}h \in \mathcal{H}$, this means that $m|\bar{m}$ by (19), and so $\bar{m} = m$, as desired. □

Corollary 40 *In the situation of* Proposition 39, *let* $D \in \mathcal{H} \cap \pi^*_\psi \mathrm{NS}'(A_\psi)$ *and put* $\bar{N} = \frac{N}{m}$. *Then* $D = mD'$, *where* $D' = \mathbf{D}'(a, b, f) \in \tilde{\mathcal{H}}$ *satisfies*

$$\rho_{\bar{N}}(f) \;=\; \rho_{\bar{N}}(bh) \quad \textit{and} \quad \varphi_h(D') \;\equiv\; 0 \,(\mathrm{mod}\ \bar{N}^2). \tag{57}$$

Proof. By (56), $\exists D'' \in \mathrm{NS}'(A_{\bar{\psi}})$ such that $D' = \nu^*\pi^*_{\bar{\psi}}(D'')$. By (44) we see that $\pi^*_{\bar{\psi}}(D'') \in \tilde{\mathcal{H}}$. Then (53) (applied to $\bar{\psi}$) shows that $\pi^*_{\bar{\psi}}(D'') = m\tilde{D}'$, for some $\tilde{D}' \in \tilde{\mathcal{H}}$. Thus $D = mD'$, where $D' = \nu^*\tilde{D}' \in \tilde{\mathcal{H}} \cap \nu^*\mathrm{NS}'(A)$, and (57) holds by (43). □

Proof of Theorem 31. Let h, $\bar{\psi}$, ν and $\alpha := \alpha_\psi$ be as in Proposition 39. Put $m = m_\psi(\mathcal{H}) = m_{\bar{\psi}}(\mathcal{H})$ and $\bar{N} = \frac{N}{m}$. Since $\nu = \nu_{\bar{N},h}$ by Proposition 39, we are in the situation of Proposition 32 and so $\tilde{\mathcal{H}} \cap \nu^*\mathcal{N} = \nu^*\tilde{\mathcal{H}}$ by (44), where $\mathcal{N} = \mathrm{NS}'(A)$.

Since $\mathcal{N}_{\bar{\psi}} := \pi_{\bar{\psi}}^* \mathrm{NS}'(A_{\bar{\psi}}) \leq \mathcal{N}$, we have that $\tilde{\mathcal{H}} \cap \nu^* \mathcal{N}_{\bar{\psi}} = \tilde{\mathcal{H}} \cap \nu^* \mathcal{N} \cap \nu^* \mathcal{N}_{\bar{\psi}} = \nu^* \tilde{\mathcal{H}} \cap \nu^* \mathcal{N}_{\bar{\psi}} = \nu^*(\tilde{\mathcal{H}} \cap \mathcal{N}_{\bar{\psi}})$, the latter because ν^* is injective. Since $\mathcal{N}_{\psi} := \pi_{\psi}^* \mathrm{NS}'(A_{\psi}) = \nu^* \pi_{\bar{\psi}}^*(A_{\bar{\psi}})$ by (56), we thus obtain that $\tilde{\mathcal{H}} \cap \mathcal{N}_{\psi} = \tilde{\mathcal{H}} \cap \nu^* \mathcal{N}_{\bar{\psi}} = \nu^*(\tilde{\mathcal{H}} \cap \mathcal{N}_{\bar{\psi}})$, and so

$$[\tilde{\mathcal{H}} : \tilde{\mathcal{H}} \cap \mathcal{N}_{\psi}] = [\tilde{\mathcal{H}} : \nu^* \tilde{\mathcal{H}}][\nu^* \tilde{\mathcal{H}} : \nu^*(\tilde{\mathcal{H}} \cap \mathcal{N}_{\bar{\psi}})] = [\tilde{\mathcal{H}} : \nu^* \tilde{\mathcal{H}}][\tilde{\mathcal{H}} : \tilde{\mathcal{H}} \cap \mathcal{N}_{\bar{\psi}}].$$

Now by (45) we have that $[\tilde{\mathcal{H}} : \nu^* \tilde{\mathcal{H}}] = \bar{N}^{\tilde{r}}$, where $\tilde{r} = \mathrm{rank}(\tilde{\mathcal{H}}) = r_{\mathcal{H}} + 2$. Moreover, since $\bar{\psi} \in \mathrm{Hom}(E[m], E'[m])$ and $m_{\bar{\psi}} = m$, we are in the situation of Corollary 38 (with N replaced by m), and so $[\tilde{\mathcal{H}} : \tilde{\mathcal{H}} \cap \mathcal{N}_{\bar{\psi}})] = m^{\tilde{r}+1}$ by (54). Thus, $[\tilde{\mathcal{H}} : \tilde{\mathcal{H}} \cap \mathcal{N}_{\psi}] = \bar{N}^{\tilde{r}+1} m^{\tilde{r}+1} = m N^{\tilde{r}}$, which proves (41) and hence Theorem 31. □

References

[1] C. Diem, G. Frey, Non-constant curves of genus 2 with infinite pro-Galois covers. *Israel Journal of Mathematics* **164** (2008), 193–220.

[2] G. Frey, E. Kani, Curves of genus 2 covering elliptic curves and an arithmetical application. In: *Arithmetic Algebraic Geometry* (G. van der Geer, F. Oort, J. Steenbrink, eds.), Progress In Math. vol. 89, Birkhäuser, Boston, 1991, pp. 153-176.

[3] G. Frey, E. Kani, Curves of genus 2 with elliptic differentials and associated Hurwitz spaces. *Contemporary Math.* **487** (2009), 33–81.

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

[5] E. Kani, The Hurwitz space of genus 2 covers of an elliptic curve. *Collect. Math.* **54** (2003), 1–51.

[6] E. Kani, Products of CM elliptic curves. *Collect. Math.* **62** (2011), 297-339.

[7] E. Kani, Jacobians isomorphic to a product of two elliptic curves and ternary quadratic forms. *J. Number Theory* **139** (2014), 138–174.

[8] E. Kani, The moduli spaces of Jacobians isomorphic to a product of two elliptic curves. *Collect. Math.* **67** (2016), 21–54.

[9] E. Kani, Elliptic subcovers of hyperelliptic curves. *Math. Nachr.* **290** (1917), 2890–2900.

[10] E. Kani, Elliptic subcovers of a curve of genus 2. II. The refined Humbert invariant. *J. Number Theory* **193** (2018), 302–335.

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

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

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

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

[15] D. Mumford, *Geometric Invariant Theory*. Springer-Verlag, Berlin, 1966.

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

[17] J. H. Silverman, *The Arithmetic of Elliptic Curves*. GTM 106, Springer-Verlag, New York, 1986.