ANNALES DE L'INSTITUT FOURIER

EHUD DE SHALIT
EYAL Z. GOREN

On special values of theta functions of genus two

Annales de l'institut Fourier, tome 47, nº 3 (1997), p. 775-799
<http://www.numdam.org/item?id=AIF_1997__47_3_775_0>

Ann. Inst. Fourier, Grenoble
47, 3 (1997), 775–799

ON SPECIAL VALUES OF THETA FUNCTIONS OF GENUS TWO

by E. DE SHALIT and E.Z. GOREN

1. INTRODUCTION

1.1. Background.

Let K be a quadratic imaginary field and H its Hilbert class field. Let

$$\Delta(\tau) = (2\pi i)^{12} q \prod_{n\geqslant 1} (1-q^n)^{24} \tag{1.1}$$

($q = \exp(2\pi i\tau)$, $\mathrm{Im}(\tau) > 0$) be Ramanujan's Δ-function. For any lattice $L = (\omega_1, \omega_2)\mathbb{Z}^2 \subset \mathbb{C}$, where $\mathrm{Im}(\omega_2^{-1}\omega_1) > 0$, let

$$\Delta(L) = \omega_2^{-12}\Delta(\omega_2^{-1}\omega_1) \tag{1.2}$$

(this only depends on the lattice). For any fractional ideal $\mathfrak{a} \subset K$ of the full ring of integers $\mathcal{O}_K$ let

$$u(\mathfrak{a}) = \frac{\Delta(\mathfrak{a}^{-1})}{\Delta(\mathcal{O}_K)}. \tag{1.3}$$

Then the $u(\mathfrak{a})$ have the following nice properties:

- $u(\mathfrak{a}) \in H^\times$ and the fractional ideal it generates $(u(\mathfrak{a})) = \mathfrak{a}^{12}\mathcal{O}_H$ (so it realizes the Hauptidealsatz in H, up to twelfth powers).
- $u(\mathfrak{a}\mathfrak{b}) = u(\mathfrak{a})u(\mathfrak{b})^{(\mathfrak{a},H/K)}$ where $(\mathfrak{a}, H/K)$ denotes the Artin symbol of $\mathfrak{a}$.

Key words: Theta functions – Complex multiplication – Units.
Math. classification: 11G15.

- $u(\mathfrak{a},\mathfrak{b}) = u(\mathfrak{a}\mathfrak{b})/u(\mathfrak{a})u(\mathfrak{b}) \in \mathcal{O}_H^\times$, and depends only on the classes $[\mathfrak{a}]$ and $[\mathfrak{b}]$ in the ideal class group C_K of K.

The group generated by the units $u(\mathfrak{a},\mathfrak{b})$ is the group of *Siegel units* in H. Its index in $\mathcal{O}_H^\times$ is finite. In fact this index is equal, up to a "trivial" factor (involving 2, 3, and the class number h_K of K), to the class number h_H of H, as follows from the analytic class number formula and Kronecker's limit formula. See [Sie] and [L]. Similar units in arbitrary ray class fields of K, the *elliptic units*, were constructed by Ramachandra [Ra] and Robert [Ro]; see also the book by Kubert and Lang [KL]. They are given as special values of elliptic theta functions, and exhibit the same general behaviour. Kronecker's limit formula gives a relation between the logarithms of these units and values of Artin L-series of K at $s = 0$, a relation which can be used to verify the abelian Stark conjecture in H (or in general in abelian extensions of K). See [Ta], IV.3.9.

Thus it became a major problem in number theory to construct "abelian units" in abelian extensions of CM fields of higher degree, using transcendental functions and the theory of complex multiplication as developed by Shimura and Taniyama. It was hoped that such units would yield new cases of Stark's conjecture. However, even without the link with L-series, it will be very pleasing to have a general construction of "abelian units" similar to the elliptic units of Siegel and Ramachandra.

The purpose of this work is to study certain invariants similar to the $u(\mathfrak{a},\mathfrak{b})$ above, in the Hilbert class field of a *quartic* CM field. These invariants are constructed from theta functions of genus 2, evaluated at CM points, and depend only on the classes of $\mathfrak{a}$ and $\mathfrak{b}$. Certain features of abelian varieties and the theory of complex multiplication that are absent in the case of elliptic curves complicate the situation. For example, one has to take into account the polarization of the abelian surfaces that intervene in the construction, and theta functions with complex multiplication by K give rise to numbers in abelian extensions of the *reflex* field K'. But while these are of technical nature, there is one substantial difference. What eventually makes the Siegel units *units* is the fact that the divisor of Δ is supported at the cusps, and that a similar statement holds on the arithmetic moduli scheme, over $\mathbb{Z}$. On the contrary, the divisor of Siegel modular forms of higher genus can not be supported at infinity (as can be seen from the fact that the Satake compactification of the Siegel moduli space is normal, but the components at infinity are of codimension 2). This makes it difficult to decide whether our invariants are indeed units. Partial results are discussed in section 4 below.

1.2. Set-up.

Let $e(x) = e^{2\pi i x}$, and denote by $\mathfrak{H}_g$ the Siegel space of symmetric $g \times g$ complex matrices τ, with $\operatorname{Im}(\tau)$ positive definite. For $\tau \in \mathfrak{H}_g$, $u \in \mathbb{C}^g$, $r, s \in \mathbb{Q}^g$ define

$$\theta \begin{bmatrix} r \\ s \end{bmatrix} (u, \tau) = \sum_{n \in \mathbb{Z}^g} e\left\{ \frac{1}{2}\, {}^t(n+r)\tau(n+r) + {}^t(n+r)(u+s) \right\}. \tag{1.4}$$

This is the classical theta function with characteristics r and s. One calls the characteristics *integral* if $r, s \in \frac{1}{2}\mathbb{Z}^g$, and *even* if they are integral and ${}^t r \cdot s \in \frac{1}{2}\mathbb{Z}$. Theta functions with integral characteristics depend, up to ± 1, only on r, s mod $\mathbb{Z}^g$. We shall therefore consider integral characteristics modulo $\mathbb{Z}^g$, with the understanding that the resulting theta functions are well defined only up to a sign. When $g = 1$ three out of the four integral characteristics are even, and when $g = 2$ ten out of the 16 are even. Let

$$\theta_{\mathrm{ev}}(u, \tau) = \prod_{\text{even}} \theta \begin{bmatrix} r \\ s \end{bmatrix} (u, \tau) \tag{1.5}$$

where the product runs over all the even characteristics (this is defined up to a sign). Write $\theta_{\mathrm{ev}}(\tau) = \theta_{\mathrm{ev}}(0, \tau)$. When $g = 1$, Ramanujan's $\Delta(\tau) = 16\pi^{12}\theta_{\mathrm{ev}}^8(\tau)$. When $g = 2$ Igusa proved [Ig] that $\theta_{\mathrm{ev}}^2(\tau)$ (denoted by him $\chi_{10}(\tau)$) is a Siegel modular form of level 1 and weight 10 (θ_{ev} itself is of level 2). This function will be our basic transcendental function, which will play the role of Δ. Using Riemann's vanishing theorem and the fact that every principally polarized abelian surface is the Picard variety of a (possibly reducible) curve, one shows that $\theta_{\mathrm{ev}}(\tau)$ vanishes precisely at the set of τ where the abelian surface $A_\tau = \mathbb{C}^2/(\tau, I)\mathbb{Z}^4$ with the associated principal polarization (given over $\mathbb{C}$ by the Riemann form $E_\tau((\tau, I)x, (\tau, I)y) = {}^t x J y$, where $J = \begin{pmatrix} 0 & -I \\ I & 0 \end{pmatrix}$, and $x, y \in \mathbb{Z}^4$) splits up as the product of two elliptic curves with their canonical polarizations.

Let L be a lattice in $\mathbb{C}^2$, and E a Riemann form on L inducing a principal polarization on $\mathbb{C}^2/L$ (so L is its own $\mathbb{Z}$-dual in the $\mathbb{R}$-linear extension of E to a pairing $\mathbb{C}^2 \times \mathbb{C}^2 \to \mathbb{R}$). Let $\Omega = (\omega_1, \omega_2)$ be a symplectic basis of L (meaning $E(\Omega x, \Omega y) = {}^t x J y$). Then

$$\Delta(L, E) = \det(\omega_2)^{-10} \theta_{\mathrm{ev}}^2(\omega_2^{-1}\omega_1) \tag{1.6}$$

depends only on L and E. Note that the primes 2 and 5 play the same role as the primes 2 and 3 for elliptic curves. Note also that 10 (resp. 12) is the least common multiple of the number of roots of unity in cyclic CM fields of degree 4 (resp. 2).

To explain our results, and to avoid technical complications, assume throughout the introduction, that K is a *cyclic* CM field, $[K : \mathbb{Q}\,] = 4$. Let F be its real quadratic subfield. Assume in addition that the class number h_K of K is odd, that the class number of F, $h_F = 1$, and that the absolute different of K, $\mathcal{D}_K = (\delta)$ is generated by an element δ such that $\overline{\delta} = -\delta$ (the bar denotes complex conjugation). The fundamental unit of F must have then norm -1, because if σ is a generator of $\mathrm{Gal}(K/\mathbb{Q})$, the quotient $\sigma(\delta)/\delta$ is a real unit of norm -1. Most of these assumptions will be relaxed later on. Let H be the Hilbert class field of K.

Fix a CM type Φ of K. $\Phi = \{\phi_1, \phi_2\}$ defines an embedding of K in $\mathbb{C}^2$ via $\Phi(u) = (\phi_1(u), \phi_2(u))$. Changing δ, the generator of $\mathcal{D}_K$, if necessary, we may assume that $\mathrm{Im}(\varphi(\delta)) > 0$ for $\varphi \in \Phi$. For any fractional ideal $\mathfrak{a}$ of the full ring of integers $\mathcal{O}_K$ pick a totally positive a such that

$$\mathfrak{a}\bar{\mathfrak{a}} = (a), \quad 0 \ll a \in F \tag{1.7}$$

and consider the lattice $\Phi(\mathfrak{a})$ with the Riemann form

$$E_{a\delta}(\Phi(u), \Phi(v)) = Tr_{K/\mathbb{Q}}(a^{-1}\delta^{-1}\bar{u}v). \tag{1.8}$$

The induced polarization on $\mathbb{C}^2/\Phi(\mathfrak{a})$ is principal, and compatible with complex multiplication in the sense that the associated Rosati involution induces on K complex conjugation. It is now easy to check that, under our simplifying assumptions on K, the number $\Delta(\Phi(\mathfrak{a}), E_{a\delta})$ in fact depends only on Φ and $\mathfrak{a}$, but not on the polarization. We denote it by $\Delta(\Phi(\mathfrak{a}))$ and define

$$u(\Phi; \mathfrak{a}) = \frac{\Delta(\Phi(\mathfrak{a}^{-1}))}{\Delta(\Phi(\mathcal{O}_K))}. \tag{1.9}$$

When Φ is fixed we simply write $u(\mathfrak{a})$ for $u(\Phi; \mathfrak{a})$. In Section 2 we give the details of this construction, in the more general set-up.

1.3. Main properties of the invariants.

In Section 3 we study the properties of the $u(\mathfrak{a})$'s. Here is what we get under our assumptions on K:

1. $u(\mathfrak{a})$ is well defined and $u(\mathfrak{a}) \neq 0, \infty$.

2. $u(\mathfrak{a}) \in H$, $\sqrt{u(\mathfrak{a})} \in K^{ab}$ (in fact, the square root lies in the 2-ray class field of K).

3. Let Φ' be the reflex CM-type of Φ, and $\mathrm{N}_{\Phi'}$ the half-norm corresponding to the embeddings in Φ': $\mathrm{N}_{\Phi'}(x) = \prod_{\sigma \in \Phi'} \sigma(x)$. Then if $\mathcal{C}$ is any ideal of K and $\mathfrak{c} = \mathrm{N}_{\Phi'}(\mathcal{C})$, $u(\mathfrak{a}\mathfrak{c}) = u(\mathfrak{c})u(\mathfrak{a})^{(\mathcal{C},H/K)}$. Every class in C_K, the ideal class group of K, contains an ideal of the form $\mathrm{N}_{\Phi'}(\mathcal{C})$.

4. If $\lambda \in K^{\times}$ then $u(\lambda\mathfrak{a}) = \mathrm{N}_{\Phi}(\lambda)^{10}u(\mathfrak{a})$.

5. $u(\Phi; \mathfrak{a},\mathfrak{b}) = u(\mathfrak{a},\mathfrak{b}) = u(\mathfrak{a}\mathfrak{b})/u(\mathfrak{a})u(\mathfrak{b})$ depends only on the classes of $\mathfrak{a}$ and $\mathfrak{b}$. Its norm from H to K is 1.

6. $u(\Phi\sigma; \sigma^{-1}\mathfrak{a}) = u(\Phi; \mathfrak{a})$ for any $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$. The Galois group acts transitively on the four CM types of K.

7. Assume $(h_K, 5) = 1$. Then the $u(\mathfrak{a})$ generate H. In particular, if $h_K > 1$ they are non-trivial.

8. Assume h_K is prime and different from 5 (and 2). Then the group generated by the $u(\mathfrak{a},\mathfrak{b})$ in $H^{\times}$ has rank $h_K - 1$.

1.4.

Section 4 is devoted to some results on the moduli space of principally polarized abelian surfaces, and questions of integrality. We get the following results concerning integrality of the $u(\mathfrak{a})$'s:

1. The following are equivalent:

(i) If $\mathfrak{a}$ is integral, $u(\mathfrak{a})$ is integral (note that this is true for principal $\mathfrak{a}$ because of property 4 above)

(ii) For every $\mathfrak{a}$, $(u(\mathfrak{a})) = \mathrm{N}_{\Phi}(\mathfrak{a})^{10}$

(iii) For every $\mathfrak{a}$, $(u(\mathfrak{a}))$ is $\mathrm{Gal}(H/K)$-invariant

(iv) The $u(\mathfrak{a},\mathfrak{b})$ are units.

2. If p is a rational prime that splits completely *or* remains inert in K and $(p, \mathfrak{a}) = 1$ then $u(\mathfrak{a})$ is a unit at all the primes of H above p.

While point 1 is a formal consequence of the properties of the $u(\mathfrak{a})$ listed above, point 2 lies deeper, in particular in the inert case. Its proof depends on the following geometric interpretation. Let Z be the divisor of θ_{ev} in the moduli space of principally polarized abelian surfaces with level-n structure (some n). Let $\overline{Z}$ be the Zariski closure of Z in the arithmetic moduli scheme parametrizing the same structures over $\mathbb{Z}[\zeta_n, 1/n]$. Let P be a point in the moduli space representing a principally polarized abelian surface X with potentially good reduction, e.g. the point representing $\mathbb{C}^2/\Phi(\mathfrak{a})$ with the polarization (1.8). Let $\overline{P}$ be its Zariski closure in the arithmetic moduli scheme. Then $\overline{Z}$ and $\overline{P}$ meet at the fiber above a finite place v if and only if the reduction modulo v of X is isomorphic, with the polarization, to a product of two elliptic curves. If P corresponds to an abelian surface with complex multiplication by K as above, then the elliptic curves are supersingular. All this is explained in detail in Section 4.2. In Theorem 15 we analyze the question of how the decomposition of p (the rational prime below v) in K affects the reduction type of an abelian surface with CM by K. The case where p is inert in K relies on results of Oort and Ekedhal [Ek].

Question. Are the $u(\Phi; \mathfrak{a},\mathfrak{b})$ units?

The behavior of the $u(\mathfrak{a}, \mathfrak{b})$ above rational primes p which decompose as a product of two primes in K is the most difficult, and remains unsettled (as do the cases of the finitely many primes which ramify in K). Note that the kernel of the norm map from $\mathcal{O}_H^\times$ to $\mathcal{O}_K^\times$ has rank $2h_K - 2$, so even if the answer to our question is positive, we are left with the task of explaining which "half" of the unit group we get this way. On the other hand, if not units, what are the (finitely many) primes that appear in the ideal decomposition of these invariants?

1.5.

Our approach exploits the fact that the abelian surfaces in question, with their principal polarization, are Jacobians of curves of genus 2, only to the extent of interpreting the divisor of θ_{ev} over the arithmetical moduli scheme. The zero locus of θ_{ev} is precisely the locus of non-Jacobians, or more precisely the locus of abelian surfaces which are Pic^0 of a reducible curve consisting of two curves of genus 1 intersecting transversally at one point. Since the same interpretation persists in characteristic p, the geometric question lying behind the question whether the $u(\mathfrak{a},\mathfrak{b})$ are units is the following. Here we let C be the curve whose (principally polarized) Jacobian is $(\mathbb{C}^2/\Phi(\mathcal{O}_K), E_\delta)$, and $\mathcal{C}_\mathfrak{a}$ the curve whose Jacobian is $(\mathbb{C}^2/\Phi(\mathfrak{a}), E_{a\delta})$.

Question. Suppose the curve $\mathcal{C}$, which is defined over $\overline{\mathbb{Q}}$, has bad reduction modulo π, for some prime π of a (large enough) field of definition. Is the same true of the curve $\mathcal{C}_\mathfrak{a}$? More precisely, suppose that a stable model of $\mathcal{C}$ reduces mod π^n to the union of two elliptic curves intersecting at a point. Is the same true of $\mathcal{C}_\mathfrak{a}$?

Further exploitation of the theory of Jacobians runs into difficulties. For one thing, the relation between the curve $\mathcal{C}$ and the curve $\mathcal{C}_\mathfrak{a}$ is pretty mysterious (although algorithms of G. Frey allow one to compute equations for these curves). In addition, such a relation is missing when one makes the obvious generalization to non-principally polarized surfaces, i.e. dropping the hypothesis on the different of K.

2. THE CONSTRUCTION

2.1. Abelian surfaces with complex multiplication.

The purpose of this section is to formulate conditions for an abelian surface with complex multiplication by the full ring of integers of a quartic CM field, to admit a principal polarization. Let K be a quartic CM field, let Φ be a CM type, and let (K', Φ') be the reflex CM type. Then ([ShTa], II.8.4, example (2)) there are three possibilities: (a) K is biquadratic, Φ is non-primitive, and K' is quadratic imaginary, (b) $K = K'$ is cyclic, or (c) K is non-Galois, its Galois closure $\tilde{K}$ is of degree 8 over $\mathbb{Q}$, and $\mathrm{Gal}(\tilde{K}/\mathbb{Q}) = D_4$. In this case K' is another quartic CM field contained in $\tilde{K}$, and $K \cap K' = \mathbb{Q}$. Let H' be the Hilbert class field of K'. We shall construct a special finitely generated subgroup of $H'^\times$. The construction which we are about to describe may fail in case (a) (the function θ_{ev}^2 may vanish at the corresponding points in $\mathfrak{H}_2$ so we get "0/0"). On the other hand K' is *quadratic* and we have at hand the Siegel units of H', employing theta functions of genus 1, rather than theta functions of genus 2 (see the introduction). We therefore regard case (a) as a degenerate case and exclude it from now on. The remaining cases we call the *cyclic case* (b) and the *non-Galois case* (c).

Let $\mathfrak{c}$ be a fractional ideal of K, and $\Phi(\mathfrak{c}) \subset \mathbb{C}^2$ the lattice obtained by embedding $\mathfrak{c}$ in $\mathbb{C}^2$ via the two embeddings of Φ. We let $\mathcal{O}_K$ act on $\Phi(\mathfrak{c})$ via $\Phi : a\Phi(u) = \Phi(au)$. A Riemann form E on $\Phi(\mathfrak{c})$ is *compatible* with the complex multiplication if

$$E(au,v)=E(u,\bar{a}v) \tag{2.1}$$

for every u,v in $\Phi(\mathfrak{c})$ and every $a\in\mathcal{O}_K$. Since in our case Φ is a simple CM type, *every* Riemann form E on $\Phi(\mathfrak{c})$ turns out to be compatible with the complex multiplication ([ShTa], II.6.2, theorem 4). Furthermore (loc.cit.), there exists a $\delta\in K$, $\bar{\delta}=-\delta$, $\mathrm{Im}(\varphi(\delta))>0$ for $\varphi\in\Phi$, such that $E=E_\delta$, where for $u,v\in\mathfrak{c}$

$$E_\delta(\Phi(u),\Phi(v))=Tr_{K/\mathbb{Q}}(\delta^{-1}\bar{u}v). \tag{2.2}$$

The polarization induced by E_δ on $\mathbb{C}^2/\Phi(\mathfrak{c})$ is *principal* if and only if $\mathcal{D}_K\mathfrak{c}\bar{\mathfrak{c}}=(\delta)$. Thus

$$P_K(\Phi,\delta;\mathfrak{c})\ :\ \mathcal{D}_K\mathfrak{c}\bar{\mathfrak{c}}=(\delta),\ \bar{\delta}=-\delta,\ \text{and } \mathrm{Im}(\varphi(\delta))>0 \text{ for } \varphi\in\Phi \tag{2.3}$$

is the condition for E_δ to induce a principal polarization on $\mathbb{C}^2/\Phi(\mathfrak{c})$, and

$$P_K(\Phi;\mathfrak{c}):\exists\delta\in K \text{ s.t. } P_K(\Phi,\delta;\ \mathfrak{c}) \text{ holds} \tag{2.4}$$

is the condition for the abelian surface $\mathbb{C}^2/\Phi(\mathfrak{c})$ to admit a principal polarization.

Let us consider two cases: (i) if the fundamental unit of $F=K\cap\mathbb{R}$ has norm -1, then multiplying by a real unit we can arrange δ to have any sign distribution at the embeddings of K, so the condition $P_K(\Phi,\mathfrak{c})$ is independent of Φ, and is equivalent to

$$P_K(\mathfrak{c})\ :\ \exists\delta\in K \text{ s.t. } \mathcal{D}_K\mathfrak{c}\bar{\mathfrak{c}}=(\delta) \text{ and } \bar{\delta}=-\delta. \tag{2.5}$$

(ii) If, on the other hand, the fundamental unit of F has norm $+1$, then $P_K(\mathfrak{c})$ implies $P_K(\Phi;\mathfrak{c})$ for two out of the four CM types of K, complex conjugates of each other, but not for the other two.

Next we want to determine the extent to which $(K,\Phi,\mathfrak{c})$ determine δ. Clearly δ may be changed by a totally positive unit of F, and only by such, without affecting $P_K(\Phi,\delta;\mathfrak{c})$. Let $\mathcal{O}_{F,+}^\times$ denote the (infinite cyclic) group of totally positive units of F. The abelian surfaces $\mathbb{C}^2/\Phi(\mathfrak{c})$ with the polarizations corresponding to δ and $\epsilon\delta$ ($\epsilon\in\mathcal{O}_{F,+}^\times$) are isomorphic if and only if $\epsilon\in\mathbb{N}_{K/F}(\mathcal{O}_K^\times)$. Thus the number of isomorphism types of principal polarizations on $\mathbb{C}^2/\Phi(\mathfrak{c})$ (if one exists!) is the index $[\mathcal{O}_{F,+}^\times:\mathbb{N}_{K/F}(\mathcal{O}_K^\times)]$.

Consider again the two cases: (i) If the fundamental unit of F has norm -1, then every totally positive unit of F is already a square in F, so this index is 1. (ii) If on the other hand the fundamental unit of F has norm $+1$, then the groups $\mathcal{O}_{F,+}^{\times} \cong \mathcal{O}_F^{\times}/\mu_F \hookrightarrow \mathcal{O}_K^{\times}/\mu_K$ are both infinite cyclic and the index $Q = [\mathcal{O}_K^{\times}/\mu_K : \mathcal{O}_F^{\times}/\mu_F]$ is 1 or 2 ([Wa], Theorem 4.12). Therefore, if $Q = 1$, $[\mathcal{O}_{F,+}^{\times} : \mathbb{N}_{K/F}(\mathcal{O}_K^{\times})] = 2$, and if $Q = 2$, $[\mathcal{O}_{F,+}^{\times} : \mathbb{N}_{K/F}(\mathcal{O}_K^{\times})] = 1$. Still in case (ii), suppose $K/\mathbb{Q}$ is cyclic. Then $\mu_K = \pm 1$ ($K \neq \mathbb{Q}(\zeta_5)$ because the fundamental unit of $\mathbb{Q}(\sqrt{5})$ has norm -1), and therefore if there is a unit ϵ in K which is not real, its square must be real, so ϵ should be purely imaginary. The same is true of $\sigma(\epsilon)$, so $\sigma(\epsilon)/\epsilon$ is a real unit of norm $\sigma(\sigma(\epsilon)/\epsilon) \cdot \sigma(\epsilon)/\epsilon = \bar{\epsilon}/\epsilon = -1$. This contradiction shows that $Q = 1$. We have proven the following.

Proposition 1. — *Assume that $\mathbb{C}^2/\Phi(\mathfrak{c})$ carries a principal polarization. Then $P_K(\mathfrak{c})$ holds. Conversely, suppose that $P_K(\mathfrak{c})$ holds.*

(i) *If the norm of the fundamental unit of F is -1 then for any CM type Φ the abelian surface $\mathbb{C}^2/\Phi(\mathfrak{c})$ admits a principal polarization, which is unique up to isomorphism.*

(ii) *If the norm of the fundamental unit of F is $+1$ then the abelian surface $\mathbb{C}^2/\Phi(\mathfrak{c})$ admits a principal polarization for two out of the four CM types, and there are $2/Q$ such polarizations, up to isomorphism, where $Q = [\mathcal{O}_K^{\times} : \mathcal{O}_F^{\times}\mu_K]$ is 1 or 2. If $K/\mathbb{Q}$ is cyclic, $Q = 1$.* □

About the condition $P_K(\mathfrak{c})$ we make two remarks. The first is that for certain CM fields K it is *never* satisfied. For example, suppose $K/\mathbb{Q}$ is cyclic, $h_F = 1$ and the fundamental unit of F has norm $+1$. Let σ be a generator of $\mathrm{Gal}(K/\mathbb{Q})$. Since $\mathfrak{c}\bar{\mathfrak{c}}$ is a principal ideal of F, if $P_K(\mathfrak{c})$ holds, then $P_K(\mathcal{O}_K)$ holds too. Let δ be a purely imaginary generator of the different. Since the different is Galois invariant, $\epsilon = \sigma(\delta)/\delta$ is a unit, which must be real ($\sigma(\delta)$ is purely imaginary too). Its norm from F to $\mathbb{Q}$ is $\sigma(\epsilon)\epsilon = \sigma^2(\delta)/\delta = \bar{\delta}/\delta = -1$, contradicting our assumption on the fundamental unit of F. For such a K there do not exist *principally* polarized abelian surfaces admitting complex multiplication by the *full* $\mathcal{O}_K$. On the positive side, $P_K(\mathcal{O}_K)$ will hold for example if $\mathcal{O}_K = \mathcal{O}_F[\sqrt{d}]$ for a totally negative element $d \in F$. Indeed, the relative different $\mathcal{D}_{K/F} = (2\sqrt{d})$ then, and $\mathcal{D}_F$ is principal (as the different of a quadratic field), so the multiplicativity of differents in towers, $\mathcal{D}_K = \mathcal{D}_F\mathcal{D}_{K/F}$ implies that $\mathcal{D}_K$ is generated by a purely imaginary element.

2.2. Definition of the invariants.

Consider the following groups:

$$\tilde{I}_K^\flat = \left\{(\mathfrak{a}, a)\,|\,\mathfrak{a} \text{ is a fractional ideal of } K,\ \mathfrak{a}\bar{\mathfrak{a}} = (a),\ 0 \ll a \in F^\times\right\} \tag{2.6}$$

$$\tilde{C}_K^\flat = \tilde{I}_K^\flat / \left\{((\lambda), \lambda\bar{\lambda})\,|\,\lambda \in K^\times\right\}. \tag{2.7}$$

Let C'_F be the extended class group of F (ideal classes modulo principal ideals generated by totally positive elements of F; this group is equal to C_F if the norm of the fundamental unit is -1 and is an extension of C_F by ± 1 otherwise), and $C_K^\flat = \operatorname{Ker}(\mathbb{N}_{K/F} : C_K \to C'_F)$. Note that if ρ denotes complex conjugation, and if we define $C_{K-} = (1-\rho)C_K$ and $C_K^- = C_K[1+\rho]$ (the kernel of $1+\rho$) then $C_{K-} \subset C_K^\flat \subset C_K^-$, and when h_K is *odd* all three groups are equal. Now we have a short exact sequence

$$0 \to \mathcal{O}_{F,+}^\times / \mathbb{N}_{K/F}(\mathcal{O}_K^\times) \to \tilde{C}_K^\flat \to C_K^\flat \to 0. \tag{2.8}$$

The collection of pairs $(\mathfrak{c}, \delta)$ such that $P_K(\Phi, \delta; \mathfrak{c})$ holds, if non-empty, is a principal homogenous space for $\tilde{I}_K^\flat$, in the action

$$(\mathfrak{a}, a) \cdot (\mathfrak{c}, \delta) = (\mathfrak{a}^{-1}\mathfrak{c}, a^{-1}\delta) \tag{2.9}$$

(the reason for the inverse is simply to make some formulae below look cleaner). We denote this space by $P_{K,\Phi}$, and assume from now on that it is *not empty.*

Definition 1. — *Let $z \in \mathbb{Z}[P_{K,\Phi}]_0 = \{\sum n_i(\mathfrak{c}_i, \delta_i)\,|\,\sum n_i = 0\}$. Define*

$$u(\Phi, z) = \prod \Delta(\Phi(\mathfrak{c}_i), E_{\delta_i})^{n_i} \tag{2.10}$$

where Δ is the function of principally polarized lattices given in the introduction (1.6).

Observe that since Φ is a primitive CM type, the abelian surface $\mathbb{C}^2/\Phi(\mathfrak{c}_i)$ is simple, so its moduli point $\tau = \omega_2^{-1}\omega_1$ corresponding to $(\Phi(\mathfrak{c}_i), E_{\delta_i})$ does not lie on the divisor of θ_{ev}, and therefore $u(\Phi, z)$ is finite and non-zero.

Lemma 2. — (i) *We have*

$$\Delta(\Phi(\lambda\mathfrak{c}), E_{\lambda\bar{\lambda}\delta}) = \mathbb{N}_\Phi(\lambda)^{-10}\Delta(\Phi(\mathfrak{c}), E_\delta).$$

In particular $\Delta(\Phi(\mathfrak{c}), E_{\lambda\bar{\lambda}\delta}) = \Delta(\Phi(\mathfrak{c}), E_\delta)$ if $\lambda \in \mathcal{O}_K^\times$.

(ii) *If $\alpha \in \tilde{I}^{\flat}_K$, then $u(\Phi, \alpha z)$ depends only on the image of α in $\tilde{C}^{\flat}_K$.*

Proof. — If $\Omega = (\omega_1, \omega_2)$ is a symplectic basis for $(\Phi(\mathfrak{c}), E_\delta)$ then $\Phi(\lambda)\Omega$ is a symplectic basis for $(\Phi(\lambda\mathfrak{c}), E_{\lambda\overline{\lambda}\delta})$ so

$$\Delta(\Phi(\lambda\mathfrak{c}), E_{\lambda\overline{\lambda}\delta}) = \det(\Phi(\lambda)\omega_2)^{-10}\theta_{\mathrm{ev}}^2(\omega_2^{-1}\omega_1) = \mathbb{N}_\Phi(\lambda)^{-10}\Delta(\Phi(\mathfrak{c}), E_\delta).$$

When λ is a unit, $\epsilon = \mathbb{N}_\Phi(\lambda)$ is a unit of K' satisfying $\epsilon\overline{\epsilon} = 1$, hence is a root of unity. But 10 is just the least common multiple of orders of roots of unity in quartic CM fields which are cyclic or non-Galois (K' can not be biquadratic). This proves (i), and (ii) follows from it immediately. □

Part (i) of the lemma allows us to make the following construction-definition. Let

$$\mathbb{Z}[P_{K,\Phi}]_{00} = \Big\{\sum n_i(\mathfrak{c}_i, \delta_i) \mid \sum n_i = 0, \qquad \prod(\mathfrak{c}_i, \delta_i)^{n_i} = ((\lambda), \lambda\overline{\lambda}) \text{ for some } \lambda \in K^\times\Big\} \tag{2.11}$$

where $\prod(\mathfrak{c}_i, \delta_i)^{n_i} = (\prod \mathfrak{c}_i^{n_i}, \prod \delta_i^{n_i}) \in \tilde{I}^{\flat}_K$ because $\sum n_i = 0$. Thus $\mathbb{Z}[P_{K,\Phi}]_0/\mathbb{Z}[P_{K,\Phi}]_{00} \cong \tilde{C}^{\flat}_K$ is a finite group. For $z = \sum n_i(\mathfrak{c}_i, \delta_i) \in \mathbb{Z}[P_{K,\Phi}]_{00}$ put

$$v(\Phi, z) = u(\Phi, z)\mathbb{N}_\Phi(\lambda)^{10} \tag{2.12}$$

if $\prod(\mathfrak{c}_i, \delta_i)^{n_i} = ((\lambda), \lambda\overline{\lambda})$. Denoting by $[\mathfrak{c}, \delta]$ the orbit of $(\mathfrak{c}, \delta)$ under the subgroup of $\tilde{I}^{\flat}_K$ of elements of the form $((\lambda), \lambda\overline{\lambda})$, and by $\overline{P}_{K,\Phi}$ the space of these orbits, we have the following.

LEMMA 3. — (i) *$\overline{P}_{K,\Phi}$ is a principal homogeneous space over $\tilde{C}^{\flat}_K$.*

(ii) *$\mathbb{Z}[\overline{P}_{K,\Phi}]_{00}$ is a free abelian group of rank $|\tilde{C}^{\flat}_K| - 1$.*

(iii) *$v(\Phi, z)$ depends only on the image $\overline{z}$ of z in $\mathbb{Z}[\overline{P}_{K,\Phi}]_{00}$. In particular the group $V(\Phi)$ of all these elements is finitely generated, of rank at most $|\tilde{C}^{\flat}_K| - 1$.* □

3. MAIN PROPERTIES OF THE INVARIANTS

3.1. The action of the symplectic group on θ_{ev}.

To study the properties of the $u(\Phi, z)$ we shall consider the subgroup

$$\tilde{I}^{\sharp}_K = \{(\mathfrak{a}, a) \mid \mathfrak{a}\overline{\mathfrak{a}} = (a) \text{ and } 0 < a \in \mathbb{Q}^\times\} \tag{3.1}$$

of $\tilde{I}^{\flat}_K$, let $\tilde{C}^{\sharp}_K$ be the image of this group in $\tilde{C}^{\flat}_K$, and let $C^{\sharp}_K$ be the image of $\tilde{C}^{\sharp}_K$ in C_K. We shall only consider z of the form $\sum n_i(\mathfrak{c}_i, \delta_i)$, $\sum n_i = 0$, where all the $(\mathfrak{c}_i, \delta_i)$ are in the *same orbit* of $I^{\sharp}_K$. For lack of a better terminology let us call such z's *restricted.* The restriction on z is forced upon us because we chose to work with the symplectic group $\mathrm{Sp}(4)$ and the Siegel space of genus 2, rather than the group $GL(2, F)$ and an associated Hilbert-Blumenthal surface.

Let $G = G\mathrm{Sp}(4)$, viewed as an algebraic group over $\mathbb{Q}$. Thus

$$(3.2) \qquad G(\mathbb{Q}) = \left\{\alpha \in GL(4, \mathbb{Q}) \mid {}^t\alpha J \alpha = \nu(\alpha) J \text{ for some } \nu(\alpha) \in \mathbb{Q}^\times\right\}.$$

As usual, $\alpha \in G(\mathbb{R})$ acts on $\tau \in \mathfrak{H}_2$, sending it to $\alpha(\tau) = (a\tau + b)(c\tau + d)^{-1}$ if $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in block form. Following Shimura [Sh1], [Sh2] we denote by $\mathfrak{M}_k(\mathbb{Q})$ the $\mathbb{Q}$-vector space of complex modular forms f on $\mathfrak{H}_2$ for which

$$(3.3) \qquad f(\alpha(\tau)) = \det(c\tau + d)^k f(\tau)$$

for every $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in *some* congruence group $\Gamma_N \subset \mathrm{Sp}(4, \mathbb{Z})$, and which have a q-expansion with Fourier coefficients in $\mathbb{Q}$. It is easily verified that $\theta^2_{\mathrm{ev}} \in \mathfrak{M}_{10}(\mathbb{Q})$, and as mentioned in the introduction, Igusa proved that it is of level 1.

Fix a pair $(\mathfrak{c}, \delta) \in P_{K,\Phi}$ and $(\mathfrak{a}, a) \in \tilde{I}^{\sharp}_K$. Let $\Omega = (\omega_1, \omega_2)$ be a symplectic basis of $\Phi(\mathfrak{c})$ with respect to the polarization E_δ, and $\tau = \omega_2^{-1}\omega_1$. Then there is an $\alpha \in G(\mathbb{Q})$, $\nu(\alpha) = a$, such that $\Omega\, {}^t\alpha = \Omega' = (\omega'_1, \omega'_2)$ is a symplectic basis of $\Phi(\mathfrak{a}\mathfrak{c})$ with respect to the polarization $E_{a\delta}$. We have $\alpha(\tau) = \omega_2'^{-1}\omega'_1$. Note that since $a \in \mathbb{Q}$ the Riemann form $E_{a\delta}$ is proportional to E_δ, so (assuming $\mathfrak{a}$ is integral) the natural isogeny $\mathbb{C}^2/\Phi(\mathfrak{c}) \to \mathbb{C}^2/\Phi(\mathfrak{a}\mathfrak{c})$ respects the (homogeneous) polarizations. Now let

$$(3.4) \qquad T_K = \left\{\lambda \in K^\times \mid \lambda\bar{\lambda} \in \mathbb{Q}^\times\right\}.$$

These are the rational points of a torus over $\mathbb{Z}$ whose points in any commutative ring R are defined to be $T_K(R) = \left\{\lambda \in (R \otimes \mathcal{O}_K)^\times | \lambda\bar{\lambda} \in R^\times\right\}$. Then there exists a homomorphism $\xi : T_K \to G$ such that

$$(3.5) \qquad \Phi(\lambda) \cdot \Omega = \Omega\, {}^t\xi(\lambda).$$

It is known that the image of ξ is the stabilizer in G of the CM point τ. Now the map ξ can be adelized. Since it takes integers into matrices with integral entries, it also takes the units $T_K(\hat{\mathbb{Z}})$ of $T_K(\mathbb{A}_f)$ (the finite adelic points) into $G(\hat{\mathbb{Z}})$. The same thing can be said about the homomorphism ξ' associated with the period matrix $\Omega\,{}^t\alpha = \Omega'$. Naturally, $\xi'(\lambda) = \alpha\xi(\lambda)\alpha^{-1}$. It follows that for a unit idele $\lambda \in T_K(\hat{\mathbb{Z}})$,

$$\xi(\lambda) \in G(\hat{\mathbb{Z}}) \cap \alpha^{-1}G(\hat{\mathbb{Z}})\alpha. \tag{3.6}$$

3.2.

In [Sh2], Theorem 1.2, Shimura defines g^x for every modular form whose Fourier coefficients lie in $\mathbb{Q}^{ab}$ and every $x \in G(\mathbb{A})_+$. In particular $\theta_{\mathrm{ev}}^{\alpha}(\tau) = \det(c_\alpha\tau + d_\alpha)^{-5}\theta_{\mathrm{ev}}(\alpha(\tau))$ (loc. cit. Theorem 1.2(v)), and $f_\alpha = \theta_{\mathrm{ev}}^{\alpha}/\theta_{\mathrm{ev}}$ is a modular function of some level and Fourier coefficients in $\mathbb{Q}^{ab}$. According to [Sh2], Proposition 1.4, and the fact that θ_{ev}^2 is of level 1, and has rational Fourier coefficients, $(\theta_{\mathrm{ev}}^2)^y = \theta_{\mathrm{ev}}^2$ for every $y \in S = G_{\infty+}G(\hat{\mathbb{Z}})$, where $G_{\infty+}$ is the connected component of the identity of $G(\mathbb{R})$. Let $\eta : K'^{\times} \to T_K$ be the Φ'-half-norm (considered as a map of algebraic groups over $\mathbb{Q}$). Then Shimura's reciprocity law says that $f_\alpha(\tau) \in K'^{ab}$, and for every $x \in K_{\mathbb{A}}'^{\times}$, the action of the Artin symbol of x on $f_\alpha(\tau)$ is given by the formula

$$f_\alpha(\tau)^x = f_\alpha^y(\tau) \tag{3.7}$$

where $y = \xi(\eta(x))^{-1}$ ([Sh1], Proposition 2.2). However, if $x \in U(K_{\mathbb{A}}'^{\times})$ is a *unit* idele, then $\eta(x) \in T_K(\hat{\mathbb{Z}})$ and $y \in G(\hat{\mathbb{Z}}) \cap \alpha^{-1}G(\hat{\mathbb{Z}})\alpha$. It follows that $f_\alpha^y(\tau) = \pm f_\alpha(\tau)$. As $f_\alpha(\tau)^2 = \det(c_\alpha\tau + d_\alpha)^{-10}\theta_{\mathrm{ev}}^2(\alpha(\tau))/\theta_{\mathrm{ev}}^2(\tau) = \Delta(\mathfrak{ac}, E_{a\delta})/\Delta(\mathfrak{c}, E_\delta)$, we have the following result.

LEMMA 4. — *Let $z = (\mathfrak{ac}, a\delta) - (\mathfrak{c}, \delta) = ((\mathfrak{a}^{-1}, a^{-1}) - 1)\cdot(\mathfrak{c}, \delta)$ where $(\mathfrak{c}, \delta) \in P_{K,\Phi}$ and $(\mathfrak{a}, a) \in \tilde{I}_K^{\sharp}$. Then $u(\Phi, z) \in H'$, the Hilbert class field of K', and $\sqrt{u(\Phi, z)} \in K'^{ab}$.* □

3.3. The action of the Galois group.

LEMMA 5. — *Let $C_{K,\Phi} = \mathrm{Im}(\mathbb{N}_{\Phi'} : C_{K'} \to C_K)$. Then*

$$2C_K^- \subset C_{K,\Phi} \subset C_K^{\sharp} \subset C_K^{\flat} \subset C_K^-, \tag{3.8}$$

so in particular the odd order parts of these groups coincide.

Proof. — If $\mathcal{A}$ is an ideal of K', $\mathfrak{a} = \mathbb{N}_{\Phi'}\mathcal{A}$, and ρ denotes complex conjugation, then $\mathfrak{a}\bar{\mathfrak{a}} = \mathfrak{a}^{1+\rho} = (\mathbb{N}\mathcal{A})$, so $C_{K,\Phi} \subset C_K^{\sharp}$. To prove $2C_K^- \subset C_{K,\Phi}$

(all the other assertions in the lemma are obvious) let L be the Galois closure of K. Thus $L = K$ in the cyclic case, and L is a quadratic extension of K in the non-Galois case. Let $H = \mathrm{Gal}(L/K)$, and $G = \mathrm{Gal}(L/\mathbb{Q})$. Identifying embeddings of K in $\mathbb{C}$ with cosets of G/H we may assume that $\Phi = \{H, yH\}$, where in the cyclic case $H = \{1\}$ and y is a generator of G, and in the non-Galois case $H = \{1, x\}$, and G is generated by x and y, $x^2 = y^4 = xyxy = 1$. In both cases $y^2 = \rho$. Now let $\mathfrak{a}$ be an ideal of K whose class $[\mathfrak{a}] \in C_K^-$. Then $\mathbb{N}_{\Phi'}\mathbb{N}_{\Phi}[\mathfrak{a}] = (1+y^3)(1+y)[\mathfrak{a}] = (2+y(1+\rho))[\mathfrak{a}] = 2[\mathfrak{a}]$, proving the desired inclusion, since $\mathbb{N}_{\Phi}[\mathfrak{a}] \in C_{K'}$. □

Note that in the cyclic case we have the somewhat stronger inclusion $C_{K^-} \subset C_{K,\Phi}$, since $(1-\rho) = (1+y^3)(1-y^3)$.

Proposition 6. — *Let $\mathcal{A}$ be an ideal of K', and $(\mathcal{A}, H'/K')$ its Artin symbol. Let $(\mathfrak{a}, a) = (\mathbb{N}_{\Phi'}\mathcal{A}, \mathbb{N}\mathcal{A})$ so that $(\mathfrak{a}, a) \in \tilde{I}_K^{\sharp}$. Then for every restricted $z \in \mathbb{Z}[P_{K,\Phi}]_0$ (see Section 3.1)*

$$u(\Phi, z)^{(\mathcal{A}, H'/K')} = u(\Phi, (\mathfrak{a}, a) \cdot z). \tag{3.9}$$

The invariants $u(\Phi, z)$ (z restricted) lie in the subfield H'_{Φ} of H' which is the fixed field of $C_{K'}^{\Phi'} = \mathrm{Ker}(\mathbb{N}_{\Phi'} : C_{K'} \to C_K)$.

Proof. — Fix $(\mathfrak{c}, \delta) \in P_{K,\Phi}$ and write $u(\mathfrak{b}) = u(\Phi, (\mathfrak{b}^{-1}\mathfrak{c}, b^{-1}\delta) - (\mathfrak{c}, \delta))$ if $(\mathfrak{b}, b) \in \tilde{I}_K^{\sharp}$. Then we have to prove

$$u(\mathfrak{b})^{(\mathcal{A}, H'/K')} = u(\mathfrak{a}\mathfrak{b})/u(\mathfrak{a}). \tag{3.10}$$

Let Ω be a symplectic basis for $(\Phi(\mathfrak{c}), E_{\delta})$ as before. Let $\beta \in G(\mathbb{Q})$, $\nu(\beta) = b^{-1}$ be such that $\Omega' = \Omega\, {}^t\beta$ is a symplectic basis of $\Phi(\mathfrak{b}^{-1}\mathfrak{c})$. Let $x \in K'^{\times}_{\mathbb{A}}$ represent the ideal $\mathcal{A}$. Then $\eta(x)$ is an idele representing $\mathfrak{a}$ (we use the same notation as in Section 3.1). Let $y = \xi(\eta(x))^{-1}$. By strong approximation (and class number 1 for $\mathbb{Q}$), we have $G_{\mathbb{A},+} = (S \cap \beta^{-1}S\beta)G_{\mathbb{Q},+}$ where $S = G_{\infty,+}G(\hat{\mathbb{Z}})$ as before. Write therefore $y = s\gamma$ with $s \in (S \cap \beta^{-1}S\beta)$ and $\gamma \in G_{\mathbb{Q},+}$. Now

$$\Phi(\mathfrak{a}^{-1}\mathfrak{c}) = \Omega\, {}^t y\hat{\mathbb{Z}}^4 \cap \Omega\mathbb{Q}^4 = \Omega\, {}^t\gamma\hat{\mathbb{Z}}^4 \cap \Omega\mathbb{Q}^4 = \Omega\, {}^t\gamma\mathbb{Z}^4. \tag{3.11}$$

The first equality here holds inside $\Omega\mathbb{A}_f^4$, and can be verified by localizing at each rational prime p, using (3.5) above. Similarly,

$$\begin{aligned}\Phi(\mathfrak{b}^{-1}\mathfrak{a}^{-1}\mathfrak{c}) &= \Omega'\, {}^t(\beta y\beta^{-1})\hat{\mathbb{Z}}^4 \cap \Omega'\mathbb{Q}^4 \\ &= \Omega'\, {}^t(\beta\gamma\beta^{-1})\hat{\mathbb{Z}}^4 \cap \Omega'\mathbb{Q}^4 = \Omega'\, {}^t(\beta\gamma\beta^{-1})\mathbb{Z}^4 = \Omega\, {}^t(\beta\gamma)\mathbb{Z}^4\end{aligned}$$

where we have used $\xi'(\lambda) = \beta\xi(\lambda)\beta^{-1}$. Recall that $u(\mathfrak{b}) = f_\beta^2(\tau)$. Shimura's reciprocity law says that

$$f_\beta^2(\tau)^x = (f_\beta^2)^y(\tau) = (f_\beta^2)^\gamma(\tau) = f_\beta^2(\gamma(\tau)) = f_{\beta\gamma}^2(\tau)/f_\gamma^2(\tau),$$

which is the desired relation. We have used in the last formula the fact that f_β^2 is invariant under $s \in (S \cap \beta^{-1}S\beta)$. □

Remark. — The degree $[H'_\Phi : K'] = |C_{K,\Phi}|$. Denote it by $h_{K,\Phi}$. If h_K is *odd*, so that there is a decomposition $C_K = C_K^+ \times C_K^-$, then $h_{K,\Phi} = h_K^-$.

Corollary 7. — *Consider the $u(\mathfrak{b})$ defined in the proof of proposition 6 with $[\mathfrak{b}] \in C_{K,\Phi}$ (cf. Lemma 5 for the definition of $C_{K,\Phi}$). Then, if $(\mathfrak{a}, a) = (\mathbb{N}_{\Phi'}\mathcal{A}, \mathbb{N}\mathcal{A})$ we have*

(i) *$u(\mathfrak{a},\mathfrak{b}) = u(\mathfrak{a}\mathfrak{b})/u(\mathfrak{a})u(\mathfrak{b})$ depends only on $[\mathfrak{a}]$ and $[\mathfrak{b}]$,*

(ii) *$\mathbb{N}_{H'_\Phi/K'}u(\mathfrak{a},\mathfrak{b}) = 1$.*

Proof. — Point (i) is clear; see also Lemma 3(iii) in Section 2.2.

Point (ii) follows from the fact that $u(\mathfrak{a},\mathfrak{b}) = u(\mathfrak{b})^{(\mathcal{A},H'/K')-1}$, if $\mathfrak{a} = \mathbb{N}_{\Phi'}\mathcal{A}$. □

With $(\mathfrak{c}, \delta)$ fixed, the $u(\mathfrak{a},\mathfrak{b})$ are special cases of the invariants $v(\Phi, z)$ defined in (2.12). Sometimes, nothing is lost if we restrict to them.

Lemma 8. — *Suppose that h_K is odd, and that $[\mathcal{O}_{F,+}^\times : \mathbb{N}_{K/F}(\mathcal{O}_K^\times)] = 1$. Then the group $V(\Phi)$ (see Lemma 3, Section 2.2) is generated by the $u(\mathfrak{a},\mathfrak{b})$ as in the corollary.*

Proof. — Under our assumptions, $C_{K,\Phi} = C_K^\flat$, and the map $\tilde{C}_K^\flat \to C_K^\flat$ is an isomorphism. See Lemma 5, Section 3.3 and (2.8). It follows from Lemma 3(i), Section 2.2, that every element $z \in \mathbb{Z}[\overline{P}_{K,\Phi}]_{00}$ may be written as $\sum n_i[\mathfrak{a}_i, a_i] \cdot [\mathfrak{c}, \delta]$ where $\mathfrak{a}_i = \mathbb{N}_{\Phi'}\mathcal{A}_i$, $a_i = \mathbb{N}\mathcal{A}_i$ for ideals $\mathcal{A}_i$ of K', $\sum n_i = 0$ and $\prod \mathfrak{a}_i^{n_i} = (1)$. But then $v(\Phi, z) = \prod u(\mathfrak{a}_i)^{n_i}$ is in the group generated by the $u(\mathfrak{a},\mathfrak{b})$. □

3.4. Non-degeneracy results.

Under the assumptions of the last lemma, the rank of the group of units in H'_Φ is $2h_K^- - 1$, and the rank of the group of units whose norm to K' is 1 is $2h_K^- - 2$. On the other hand the rank of the free abelian group $\mathbb{Z}[\overline{P}_{K,\Phi}]_{00}$ is $h_K^- - 1$. It is reasonable to expect that the group $V(\Phi)$ has the same rank, i.e. that the homomorphism $v(\Phi, \cdot)$ is injective.

Proposition 9. — *Fix $(\mathfrak{c},\delta)\in P_{K,\Phi}$ as above. Suppose that h_K is odd, and that $(h_K^-,5)=1$. Then the invariants $u(\mathfrak{a})$, where $\mathfrak{a}$ runs over ideals of K of the form $\mathbb{N}_{\Phi'}\mathcal{A}$, generate H'_Φ over K'.*

Proof. — Let H'' be the subfield of H'_Φ generated by these invariants. Let $\mathcal{A}$ be an ideal of K' such that $(\mathcal{A},H''/K')=1$. For every other ideal $\mathcal{B}$ of K', letting $\mathfrak{a}=\mathbb{N}_{\Phi'}\mathcal{A}$ and $\mathfrak{b}=\mathbb{N}_{\Phi'}\mathcal{B}$ we have

$$u(\mathfrak{a})^{(\mathcal{B},H'/K')-1}=u(\mathfrak{a}\mathfrak{b})/u(\mathfrak{a})u(\mathfrak{b})=u(\mathfrak{b})^{(\mathcal{A},H'/K')-1}=1 \tag{3.13}$$

so $u(\mathfrak{a})\in K'$. It also follows that $u(\mathfrak{a}^r)=u(\ \mathfrak{a})^r$ for every r. Choosing r so that $\mathfrak{a}^r=(\lambda)$ is principal, and applying Lemma 2 (i), Section 2.2, we deduce that $(u(\mathfrak{a}))^r=(u(\mathfrak{a}^r))=(u((\lambda)))=\mathbb{N}_\Phi((\lambda))^{10}=\mathbb{N}_\Phi\mathfrak{a}^{10r}$. It follows that $\mathbb{N}_\Phi\mathfrak{a}^{10}$ is a *principal* ideal of K'. Now $\mathbb{N}_\Phi$ and $\mathbb{N}_{\Phi'}$ induce isomorphisms of the odd-order parts of $C_{K'}^-$ and C_K^-, as was noted towards the end of the proof of Lemma 5, Section 3.3 (their composition on the minus parts being multiplication by 2). It therefore follows that $(h_{K'}^-,5)=1$ as well, and that $\mathbb{N}_\Phi\mathfrak{a}$ is principal. But then also $\mathfrak{a}=\mathbb{N}_{\Phi'}\mathcal{A}$ is principal, which means that $[\mathcal{A}]\in C_{K'}^{\Phi'}=\mathrm{Ker}(\mathbb{N}_{\Phi'}:C_{K'}\to C_K)$, the subgroup defining H'_Φ. We conclude that $H''=H'_\Phi$. □

Corollary 10. — *Fix $(\mathfrak{c},\delta)\in P_{K,\Phi}$, assume that h_K is odd, and that h_K^- is a prime $\neq 5$. Then the map $v(\Phi,\cdot)$ is injective, and the rank of the group $V(\Phi)$ is $h_K^- -1$.*

Proof. — Consider $\mathbb{Q}\bigotimes V(\Phi)$ (written additively) as a rational representation of the *cyclic, prime-order* group $\Gamma=\mathrm{Gal}(H'_\Phi/K')$. Γ has two $\mathbb{Q}$ -irreducible representations: the trivial one $\mathbb{Q}$, and $\mathbb{Q}[\Gamma]_0$ which is of dimension $h_K^- -1$. Since the rank of $V(\Phi)$ is at most $h_K^- -1$, if equality does not hold here, the action of Γ on $\mathbb{Q}\bigotimes V(\Phi)$ is trivial. This means that for $v\in V(\Phi)$ and $\gamma\in\Gamma$, $\gamma(v)=\zeta(\gamma)v$ with $\zeta(\gamma)$ a root of unity. But the roots of unity in H'_Φ are just those of K', which are at most of order 10, and therefore, for a fixed v, $\gamma\mapsto\zeta(\gamma)$ is a homomorphism from the cyclic group Γ, whose order h_K^- is prime to 10, to a group of order dividing 10. This shows that in fact Γ fixes $V(\Phi)$. Pick $\mathfrak{a}=\mathbb{N}_{\Phi'}\mathcal{A}$, write $h=h_K^-$ for brevity, let $\lambda\in K^\times$ be a generator of $\mathfrak{a}^h$ and consider $u(\mathfrak{a})^h\mathbb{N}_\Phi(\lambda)^{-10}$. This number belongs to $V(\Phi)$, because it is $v(\Phi,z)$ for $z=h\left((\mathfrak{a},a)-1\right)\cdot(\mathfrak{c},\delta)\in\mathbb{Z}[P_{K,\Phi}]_{00}$. If Γ acts on it trivially, so it does on $u(\mathfrak{a})^h$. It follows that the $u(\mathfrak{a}$,$\mathfrak{b})=u(\mathfrak{a})^{(\mathcal{B},H'/K')-1}$ are h^{th} roots of unity. Since $(h,10)=1$, we deduce that $u(\mathfrak{a}$,$\mathfrak{b})=1$ and that the $u(\mathfrak{a})$ lie in K'. This contradicts the last proposition. □

3.5. Changing the CM type.

LEMMA 11. — *Let σ be an automorphism of $\overline{\mathbb{Q}}$. Then $\Phi\sigma^{-1}$ is a CM type of σK and for every $(\mathfrak{c},\delta) \in P_{K,\Phi}$ we have $(\sigma(\mathfrak{c}),\sigma(\delta)) \in P_{\sigma K,\Phi\sigma^{-1}}$ and $u(\Phi\sigma^{-1},\sigma z) = u(\Phi,z)$.*

Proof. — Clear, by "transport of structure". Note that the lattice $\Phi\sigma^{-1}(\sigma(\mathfrak{c})) = \Phi(\mathfrak{c})$ is just the same lattice, and the polarization $E_{\sigma(\delta)}$ on the "transported" lattice $\Phi\sigma^{-1}(\sigma(\mathfrak{c}))$ coincides with E_δ on the "original" $\Phi(\mathfrak{c})$ (see identity (2.2)). □

COROLLARY 12. — (i) *$u(\overline{\Phi},\overline{z}) = u(\Phi,z)$, and $V(\Phi) = V(\overline{\Phi})$.*

(ii) *If K ic cyclic,* Gal$(K/\mathbb{Q})$ *acts transitively on the four CM types, and the subgroup $V(\Phi)$ is independent of Φ.* □

4. INTEGRALITY QUESTIONS

4.1. Equivalence of integrality conditions.

PROPOSITION 13. — *Fix $(\mathfrak{c},\delta) \in P_{K,\Phi}$ and write, as above, for $(\mathfrak{a},a) = (\mathbb{N}_{\Phi'}\mathcal{A},\mathbb{N}\mathcal{A}) \in \tilde{I}^\sharp_K$,*

$$u(\mathfrak{a}) = \frac{\Delta(\Phi(\mathfrak{a}^{-1}\mathfrak{c}),E_{a^{-1}\delta})}{\Delta(\Phi(\mathfrak{c}),E_\delta)}$$

(compare the proof of Proposition 6, Section 3.3). Then the following are equivalent:

(i) *For every $\mathfrak{a}$, $(u(\mathfrak{a})) = \mathbb{N}_\Phi(\mathfrak{a})^{10}$.*

(ii) *For every $\mathfrak{a}$ the ideal $(u(\mathfrak{a}))$ is* Gal(H'/K')*-invariant.*

(iii) *If $\mathfrak{a}$ is an integral ideal, $u(\mathfrak{a})$ is an algebraic integer.*

(iv) *The $u(\mathfrak{a},\mathfrak{b}) = u(\mathfrak{a}\mathfrak{b})/u(\mathfrak{a})u(\mathfrak{b})$ are units .*

Proof. — Clearly (i) implies (ii), (iii) and (iv). Since $u(\mathfrak{a})^{(\mathcal{B},H'/K')-1} = u(\mathfrak{a},\mathfrak{b})$ for $\mathfrak{b} = \mathbb{N}_{\Phi'}\mathcal{B}$, (iv) implies (ii). Suppose (ii) holds, and choose r such that $\mathfrak{a}^r = (\lambda)$ is principal. Then, if $\mathfrak{a} = \mathbb{N}_{\Phi'}\mathcal{A}$, $\mathbb{N}_\Phi(\lambda)^{10} = u(\mathfrak{a}^r) = u(\mathfrak{a})^{1+\sigma+\sigma^2+\cdots+\sigma^{r-1}}$ where $\sigma = (\mathcal{A},H'/K')$, so $\mathbb{N}_\Phi(\mathfrak{a})^{10r} = (\mathbb{N}_\Phi(\lambda))^{10} = (u(\mathfrak{a}))^r$, from which (i) follows. Finally, suppose that (iii) holds. Then choosing an integral $\mathcal{B}$ such that $\mathcal{A}\mathcal{B}$ is principal, and letting $\mathfrak{b} = \mathbb{N}_{\Phi'}\mathcal{B}$, we have $\mathbb{N}_\Phi(\mathfrak{a}\mathfrak{b})^{10} = (u(\mathfrak{a}\mathfrak{b})) = (u(\mathfrak{a}))(u(\mathfrak{b})^{(\mathcal{A},H'/K')})$. Since the greatest common divisor of all the $\mathbb{N}_\Phi(\mathfrak{ab})$ is $\mathbb{N}_\Phi(\mathfrak{a})$, (iii) implies that $(u(\mathfrak{a}))|\mathbb{N}_\Phi(\mathfrak{a})^{10}$. This holds for every $\mathfrak{a}$ in the image of $\mathbb{N}_{\Phi'}$, and for principal $\mathfrak{a}$'s there is an equality. It follows now from the cocycle condition that (i) must hold for all $\mathfrak{a}$. □

4.2. Preliminaries on the Siegel moduli space.

For $n \geqslant 3$ let $\mathcal{A}_{2,n}$ be the scheme over $\mathbb{Z}\left[\zeta_n, \frac{1}{n}\right]$ which classifies principally polarized abelian surfaces with symplectic principal level-n structure ([FC], chapter IV, definition 6.1 and remark 6.2(c)). It is quasi-projective and smooth over $\mathbb{Z}\left[\zeta_n, \frac{1}{n}\right]$ (but not proper), and $\mathcal{A}_{2,n}(\mathbb{C}) \cong \Gamma_2(n)\backslash\mathfrak{H}_2$, where $\Gamma_2(n)$ is the principal congruence group of level n in $Sp(4,\mathbb{Z})$. In the following we shall consider the base change of $\mathcal{A}_{2,n}$ to $U = \mathrm{Spec}\left(\mathcal{O}_M\left[\frac{1}{n}\right]\right)$ where M is some large number field containing ζ_n. It will not cause any confusion if we continue to denote this base change by $\mathcal{A}_{2,n}$. We shall denote its generic fiber by $A_{2,n} = \mathcal{A}_{2,n} \times_U \mathrm{Spec}(M)$. Let f be a rational function on $\mathcal{A}_{2,n}$ (by definition, "defined over M"). Let $(f)_\eta$ be the divisor of f on $A_{2,n}$ and $\overline{(f)_\eta}$ its Zariski closure in $\mathcal{A}_{2,n}$. If the divisor (f) of f on $\mathcal{A}_{2,n}$ does not contain any vertical components then $(f) = \overline{(f)_\eta}$. Suppose that this is the case, and let $x \in A_{2,n}(M)$ be a point where f is defined, so that $f(x) \in M$. The point x extends to a section $\overline{x}$ from some open $U' \subset U$ to $\mathcal{A}_{2,n}$. Assume that $U' = U$. Let v be a finite prime of M not dividing n, and suppose that $\overline{x}$ and $(f) = \overline{(f)_\eta}$ do not intersect on the reduction $\mathcal{A}_{2,n}(v) = \mathcal{A}_{2,n} \times_U \mathrm{Spec}(k_v)$, where $k_v = \mathcal{O}_M/v$. Then (almost by definition) $f(x)$ is a *unit* at v.

Fix $(\mathfrak{c}, \delta) \in P_{K,\Phi}$, and take $\mathfrak{a} = \mathbb{N}_{\Phi'}\mathcal{A}$ as in the previous section, but integral. Let us apply the above discussion to the function f_α used to construct $u(\mathfrak{a}^{-1})$ (see Section 3.2), and to the point x corresponding to the pair $(\mathbb{C}^2/\Phi(\mathfrak{c}), E_\delta)$ with *some* level-n structure. Thus over $\mathbb{C}$, x is represented by $\tau = \omega_2^{-1}\omega_1$ as in Section 3.1. Here we take n to be a power of $a = \mathbb{N}\mathcal{A}$, so that f_α is of level n.

For M we take a large enough number field, over which $\mathbb{C}^2/\Phi(\mathfrak{c})$, its endomorphisms, the polarization E_δ, and all the n-torsion of $\mathbb{C}^2/\Phi(\mathfrak{c})$ are defined, and over the ring of integers of which there exists a model of $\mathbb{C}^2/\Phi(\mathfrak{c})$ with everywhere good reduction. We denote by X the restriction of this model to the open set U, and by $X(v)$ its reduction modulo v. The polarization λ_η defined by the Riemann form E_δ on the generic fiber X_η

of X, extends to a principal polarization λ on X, and so does the level-n structure, because n is invertible on U. This means that x extends to a section $\overline{x}$ of U whose reduction modulo v, $\overline{x}(v)$, corresponds to the pair $(X(v), \lambda(v))$ with some level-n structure.

4.3.

To study the divisor of $f_\alpha = \theta_{\text{ev}}^{\alpha}/\theta_{\text{ev}}$ we shall use the *q-expansion principle* ([FC], Chapter V, Proposition 1.8). Changing the matrices Ω and Ω' giving the symplectic bases of $\Phi(\mathfrak{c})$ and $\Phi(\mathfrak{a}\mathfrak{c})$, we may assume that α is a *diagonal* matrix, because every double coset of $\mathrm{Sp}(4,\mathbb{Z})$ in $GSp(4,\mathbb{Q})$ has a diagonal representative ([Sh3], Proposition 1.6). Such a change will affect τ, but not the invariant $u(\mathfrak{a}^{-1}) = f_\alpha^2(\tau)$. So if $\nu(\alpha) = a \in \mathbb{Z}$, then $\alpha = \begin{pmatrix} aD^{-1} & \\ & D \end{pmatrix}$ with D diagonal, and both D and aD^{-1} integral (since $\mathfrak{a}$ was integral).

The classical q-expansion of θ_{ev} is easily seen to have Fourier coefficients in $\mathbb{Z}$. Indeed, the q -expansion of $\theta\begin{bmatrix} r \\ s \end{bmatrix}$ ($\begin{bmatrix} r \\ s \end{bmatrix}$ integral and even) is given by

$$\theta\begin{bmatrix} r \\ s \end{bmatrix}(\tau) = \sum_{x\in\mathbb{Z}^2} e\left(\frac{1}{8}tr(\xi(x+r)\tau)\right) \cdot e({}^t(x+r)s) \tag{4.2}$$

where $\xi(x+r)$ is the symmetric, semi-definite, integral matrix $\xi(x+r)_{ij} = 4(x_i+r_i)(x_j+r_j)$. Note that $e({}^t(x+r)s) = \pm 1$. Since $\xi(x+r) = \xi(x'+r)$ if and only if $x + r = \pm(x' + r)$, the greatest common divisor of the Fourier coefficients of $\theta\begin{bmatrix} r \\ s \end{bmatrix}$ is 1 if $r = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$ (for which there are 4 possible s's) and 2 if $r \neq \begin{pmatrix} 0 \\ 0 \end{pmatrix}$ (three r's for each of which there are 2 s's), and the g.c.d. of the Fourier coefficients of θ_{ev} is 2^6. On the other hand $tr(\xi(x+r)\cdot\alpha(\tau)) = a\cdot tr(D^{-1}\xi(x+r)D^{-1}\cdot\tau)$. Since also every prime divisor of $\det(D)$ divides a, *away from the prime divisors of* a, the g.c.d. of the Fourier coefficients of $\theta_{\text{ev}}^{\alpha} = \det(D)^{-5}\theta_{\text{ev}}(\alpha(\tau))$ is also 2^6.

From the q-expansion principle (see p. 141 of [FC] for the relation between the "classical" q-expansion and the one appearing in Proposition 1.8 there) it follows that both $2^{-6}\theta_{\text{ev}}$ and $2^{-6}\theta_{\text{ev}}^{\alpha}$ belong to $\Gamma(\mathcal{A}_{2,n}, \omega^{\otimes 10})$ with n some fixed power of a (and where ω is the line bundle which is the determinant of the cotangent space at 0 of the universal abelian surface over $\mathcal{A}_{2,n}$). Furthermore, they do not vanish on the reduction $\mathcal{A}_{2,n}(v)$ for v prime to n. It follows that the divisor of f_α does not have any vertical components, and is therefore equal to the closure of its intersection with the generic fiber. Thus $f_\alpha(\tau)$ will be a unit at v as long as $\overline{(f_\alpha)_\eta}$ will not contain the point $\overline{x}(v)$ in the fiber above v. Clearly this will be the case if the Zariski closures of both (θ_{ev}) and $(\theta^\alpha_{\text{ev}})$ do not contain $\overline{x}(v)$.

4.4.

As mentioned in the introduction, $Z = (\theta_{\text{ev}}) \subset A_{2,n}$ is the locus of all the principally polarized abelian surfaces which are isomorphic to a product of two elliptic curves (with the polarization). We claim that the same interpretation holds for its Zariski closure $\overline{Z}$ in $\mathcal{A}_{2,n}$: $\overline{x}(v)$ lies on $\overline{Z}$ if and only if $X(v)$ is isomorphic (with the polarization $\lambda(v)$) to a product of two elliptic curves. To prove the claim, consider the map $\mu : A_{1,n} \times A_{1,n} \to A_{2,n}$ which over $\mathbb{C}$ is given by $(\Gamma_1(n)\tau_1, \Gamma_1(n)\tau_2) \mapsto \Gamma_2(n)\begin{pmatrix}\tau_1 & \\ & \tau_2\end{pmatrix}$. Its image is closed (since μ extends to a map of the Satake compactifications $\mu^c : A^c_{1,n} \times A^c_{1,n} \to A^c_{2,n}$, and μ^c maps the components at infinity to the components at infinity) and Z is the union of the translates of $\operatorname{Im}(\mu)$ under $\Gamma_2/\Gamma_2(n)$, $\Gamma_2 = \operatorname{Sp}(4,\mathbb{Z})$. Now μ extends to a closed map $\overline{\mu} : \mathcal{A}_{1,n} \times \mathcal{A}_{1,n} \to \mathcal{A}_{2,n}$ over U, and the union of the translates of $\operatorname{Im}(\overline{\mu})$ under $\Gamma_2/\Gamma_2(n)$ is therefore closed, so coincides with $\overline{Z}$ (in fact, $\mathcal{A}_{1,n} \times \mathcal{A}_{1,n}/\sigma \hookrightarrow \mathcal{A}_{2,n}$ is a closed immersion, where σ is the transposition of the two factors [G]). But this union has just the right modular interpretation as given in our claim.

Put $Z' = (\theta^\alpha_{\text{ev}})$, and denote by x' the point in $A_{2,n}(M)$ represented by $\alpha(\tau)$ – a point corresponding to the pair $(\mathbb{C}^2/\Phi(\mathfrak{a}\mathfrak{c}), E_{\mathfrak{a}\delta})$ with some level-n structure. We claim that $\overline{x}(v)$ lies on $\overline{Z}'$ if and only if $\overline{x}'(v)$ lies on $\overline{Z}$. To justify the claim we need to distinguish between the point x' and its image in $A_{2,1}$ which we denote by x'_1. Similarly, we denote by Z_1 the image of Z, which is simply the divisor of θ_{ev} on $A_{2,1}$. (The fact that $\mathcal{A}_{2,1}$ is not a *scheme* but only a stack should not cause any trouble, or can be circumvented by the introduction of an auxiliary level structure, relatively prime to n and v.) Now consider the finite morphism $A_{2,n} \to A_{2,1}$ which over $\mathbb{C}$ is given by $\Gamma_2(n)\tau \mapsto \Gamma_2\alpha(\tau)$ (well defined since $\Gamma_2(n) \subset \Gamma_2 \cap \alpha^{-1}\Gamma_2\alpha$). It is easy to write its moduli-theoretic interpretation, thereby showing that it extends to a finite morphism $\mathcal{A}_{2,n} \to \mathcal{A}_{2,1}$. The preimage of Z_1 under this morphism is Z', hence the preimage of $\overline{Z}_1$ under the extended morphism is $\overline{Z}'$. But the image of $\overline{x}$ is $\overline{x}'_1$, so $\overline{x}'_1(v) \in \overline{Z}_1$ if and only if $\overline{x}(v) \in \overline{Z}'$. Since $\overline{x}'_1(v) \in \overline{Z}_1$ if and only if $\overline{x}'(v) \in \overline{Z}$, the claim follows.

We summarize the discussion in the following proposition.

PROPOSITION 14. — *Notation as in Proposition 13, let X (respectively X') be an abelian surface over U which is a model of $\mathbb{C}^2/\Phi(\mathfrak{c})$ (resp. $\mathbb{C}^2/\Phi(\mathfrak{a}\mathfrak{c})$), and $X(v)$ (resp. $X'(v)$) its reduction modulo v for a finite place v relatively prime to a. Let λ (resp. λ') be the principal polarization on X (resp. X'), which over $\mathbb{C}$ corresponds to the Riemann form E_δ (resp. $E_{a\delta}$) and $\lambda(v)$ (resp. $\lambda'(v)$) its reduction modulo v. If $(X(v), \lambda(v))$ is not isomorphic to a product of elliptic curves with their canonical polarizations, and if the same property holds for $(X'(v), \lambda'(v))$, then $u(\mathfrak{a}^{-1}) = f_\alpha^2(\tau)$ is a unit at v.* □

We remark that $(X(v), \lambda(v))$ can only be isomorphic to a product of two elliptic curves (with the polarizations) for finitely many v's. Indeed, the discussion above shows that these v's are the places where $\overline{x}$ intersects $\overline{Z}$, and this intersection is finite.

4.5. The reduction type of abelian surfaces with CM by $\mathcal{O}_K$.

THEOREM 15. — *Assume that K is a cyclic extension of $\mathbb{Q}$. Let $U = \mathrm{Spec}\mathcal{O}_M\left[\frac{1}{n}\right]$ as before and let v be a finite place of U. Let X be an abelian surface over U with CM by $\mathcal{O}_K$, and $\mathfrak{p} = v \cap \mathcal{O}_K$. Assume that $\mathfrak{p}$ is unramified in K.*

(i) *If $\mathfrak{p}$ is split in K then $X(v)$ is ordinary, and is not isogenous to the product of two elliptic curves.*

(ii) *If $\mathfrak{p}$ is inert in K then $X(v)$ is isogenous, but not isomorphic, to a product of two supersingular elliptic curves.*

(iii) *In the remaining case $X(v)$ is isomorphic to a product of two supersingular elliptic curves.*

We emphasize that this theorem does *not* take polarization into account.

Proof. — Let φ be the Grossencharacter of M associated to X by the theory of complex multiplication. Its conductor is relatively prime to v, and

$$(\varphi(\mathfrak{A})) = \mathbb{N}_{\Phi'}(\mathbb{N}_{M/K}\mathfrak{A}) \tag{4.3}$$

for every ideal $\mathfrak{A}$ of M relatively prime to the conductor. In case (i), if $\mathfrak{p}$ is split, $\varphi(v)$ is divisible precisely by 2 out of the 4 primes above $p = \mathfrak{p} \cap \mathbb{Q}$

in K. Since $\varphi(v)$ lifts Frob_v it follows that $X(v)$ is ordinary. Were $X(v)$ isogenous to a product of two elliptic curves, they would be ordinary, so $\mathrm{End}(X(v)) \otimes \mathbb{Q}$ could only contain a quartic field K if the two elliptic curves were isogenous to each other and had complex multiplication by an imaginary quadratic field k. But then K would contain k, contradicting the assumption that it is cyclic and not biquadratic.

In cases (ii) and (iii) $\varphi(v)$ is divisible by p. This implies that $X(v)$ contains no (geometric) points of order p, and for an abelian surface this ensures that it is isogenous to a product of two supersingular elliptic curves [Oo]. Let α_p be the group-scheme kernel of Frobenius on $\mathbb{G}_a$. Oort's a-number $a(X(v)) = \dim \mathrm{Hom}(\alpha_p, X(v)[p])$ is then 2 if $X(v)$ is *isomorphic* to a product of two supersingular elliptic curves, and 1 otherwise (see [Oo]). In case (iii), $(p) = \mathfrak{p}_1\mathfrak{p}_2$ and $X(v)[p] = X(v)[\mathfrak{p}_1] \oplus X(v)[\mathfrak{p}_2]$. Since each $X(v)[\mathfrak{p}_i]$ is a local-local group scheme, it admits non-trivial homomorphisms of α_p into it, and $a(X(v)) = 2$.

Case (ii) is the most interesting, and to deal with it we refer to an argument of Ekedhal [Ek]. Consider $X(v)$ over the algebraic closure $k = \overline{k}_v$ of $k_v = \mathcal{O}_M/v$. Let $W = W(k)$ be the ring of Witt vectors over k and σ the (arithmetic) Frobenius automorphism of W. Then the contravariant Dieudonné module of $X(v)$, D $(= H^1_{crys}(X(v)/W))$ is a $W[F,V]$-module, where the absolute Frobenius F (respectively Verschiebung V) acts σ-linearly (resp. σ^{-1}-linearly). It also carries, by functoriality, an action of the ring $\mathcal{O}_K$. Furthermore, D/pD is canonically identified with the de-Rham cohomology of $X(v)$, so it admits a Hodge filtration

$$0 \to H^0(X(v), \Omega^1) \to D/pD \to H^1(X(v), \mathcal{O}_{X(v)}) \to 0. \tag{4.4}$$

For $\tau \in \mathrm{Gal}(K/\mathbb{Q})$ denote by τ also the character $\mathcal{O}_K \xrightarrow{\tau} \mathcal{O}_K \hookrightarrow \mathcal{O}_M \twoheadrightarrow \mathcal{O}_M/v \hookrightarrow k = \overline{k}_v$. Different τ's in $\mathrm{Gal}(K/\mathbb{Q})$ induce different characters τ of $\mathcal{O}_K$ to k, because p is unramified in K. Then

$$D/pD = \bigoplus_{\tau} (D/pD)_\tau \tag{4.5}$$

where $(D/pD)_\tau$, the τ-eigenspace for the action of $\mathcal{O}_K$, is 1-dimensional. Since F acts σ-linearly on D, but commutes with the action of the endomorphisms from $\mathcal{O}_K$, it maps $(D/pD)_\tau$ to $(D/pD)_{\sigma\tau}$. Clearly

$$H^0(X(v), \Omega^1) = Ker(F : D/pD \to D/pD) = \bigoplus_{\tau \in \Phi} (D/pD)_\tau \tag{4.6}$$

and $\bigoplus_{\tau \in \overline{\Phi}} (D/pD)_\tau$ maps isomorphically onto $H^1(X(v), \mathcal{O}_{X(v)})$.

Now suppose that p is inert in K. Then σ is a generator of $\mathrm{Gal}(k_v/\mathbb{F}_p) \cong \mathrm{Gal}(K/\mathbb{Q})$ and $|\Phi \cap \sigma\overline{\Phi}| = 1$. It follows that F does not annihilate $H^1(X(v), \mathcal{O}_{X(v)})$. From here it follows that $X(v)$ is not a product of two supersingular elliptic curves, because for a supersingular elliptic curve E, F annihilates $H^1(E, \mathcal{O}_E)$. □

Corollary 16. — *Suppose that $K/\mathbb{Q}$ is cyclic, and p is either a split or an inert prime in K. Then the invariants $u(\mathfrak{a})$, $(\mathfrak{a}, p) = 1$, are units at all the primes above p. So are the $u(\mathfrak{a},\mathfrak{b})$ for all $\mathfrak{a}$ and $\mathfrak{b}$.*

Proof. — Combine Proposition 14 and Theorem 15. For the $u(\mathfrak{a},\mathfrak{b})$ note that the restriction $(\mathfrak{a}, p) = 1$ may be dropped because $u(\mathfrak{a},\mathfrak{b})$ depends only on the ideal classes of $\mathfrak{a}$ and $\mathfrak{b}$. □

It is possible to get a similar classification for $X(v)$ when K is *non-Galois*, and get a similar corollary for the $u(\mathfrak{a})$. See [G]. In a different direction, let $\mathcal{C}_{\mathfrak{c}}$ (resp. $\mathcal{C}_{\mathfrak{ac}}$) be the genus 2 curve whose (principally polarized) Jacobian is isomorphic over $\mathbb{C}$ to $(\mathbb{C}^2/\Phi(\mathfrak{c}), E_\delta)$ (resp. $(\mathbb{C}^2/\Phi(\mathfrak{ac}), E_{a\delta})$). They are defined over the field of algebraic numbers.

Corollary 17. — *If both $\mathcal{C}_{\mathfrak{c}}$ and $\mathcal{C}_{\mathfrak{ac}}$ have a model with good reduction at a place v of residual characteristic p, and $(\mathfrak{a}, p) = 1$, then $u(\mathfrak{a})$ is a unit at v.*

Proof. — The Jacobian of a smooth curve of genus 2 is not isomorphic (with the polarization) to a product of two elliptic curves, so this corollary follows from Proposition 14. □

More generally, considering the curves whose Jacobians are the given abelian surfaces, we are led to questions like the one at the end of the introduction.

4.6. Concluding remarks and some examples.

(1) Although this was our initial hope, we found no compelling reason for the invariants studied in this paper to be units. The question raised in the introduction is meant to be an honest question, not a conjecture. Paul van Wamelen has informed us of some examples of curves of genus 2 whose Jacobians have CM by cyclic quartic fields of class number 2 (we also learned that Gerhard Frey has produced examples of the same sort). These examples do not meet the conditions imposed by us. As a result, invariants of the form $u(\mathfrak{a})$ where $\mathfrak{a}$ is *not* of the form $\mathrm{N}_{\Phi'}(\mathcal{A})$ can be

computed, and they turn out to satisfy (ii), *but not* (i) and (iii), of the conditions of Proposition 13. Yet the appearance of primes not dividing $\mathfrak{a}$ in the factorization of $u(\mathfrak{a})$ (always primes of relative degree 2, conforming to Corollary 16) makes one suspect that the $u(\mathfrak{a})$ might not be units even under the conditions imposed in Section 4. Consider for example the cyclic field $K = \mathbb{Q}(\sqrt{-65+26\sqrt{5}})$. It has class number 2, and $F = Q(\sqrt{5})$ has class number 1 and a fundamental unit of norm -1. The two abelian surfaces with CM by $\mathcal{O}_K$ are the Jacobians of

$$(4.7)\quad \mathcal{C} : y^2 = -8x^6 - 64x^5 + 1120x^4 + 4760x^3 - 48400x^2 + 22627x - 91839$$

and

$$(4.8)\quad \mathcal{C}' : y^2 = 79888x^6 + 293172x^5 - 348400x^3 - 29744x + 103259.$$

However, the stable model of $\mathcal{C}$ has bad reduction precisely at 11, and that of $\mathcal{C}'$ precisely at 31 and 41. To compute examples where the class number is odd and where complex conjugation acts like -1, one would have to go to a field which is at least of degree 20 over $\mathbb{Q}$.

(2) One can prove [G] that for any finite set S of rational primes, for any $\dot{g} \geqslant 2$ and for any n, there *does not* exist a single function f on the Siegel modular group of genus g and principal level n such that $f(\tau)$ is an S-unit for every CM point τ.

(3) Let H_Δ be the Humbert surface of invariant Δ in $\Gamma_2(1)\backslash\mathfrak{H}_2$ (see [vdG], Chapter IX). Let F_Δ be a modular form of weight m_Δ and level 1 whose divisor is a multiple of H_Δ (such a form exists and can be chosen to have rational Fourier coefficients). Define the invariants $u_\Delta(\Phi, \mathfrak{a})$ as before, with F_Δ taking the place of $F_1 = \theta_{\mathrm{ev}}^2$. Then the results of Section 3 generalize easily. For example, $u_\Delta(\Phi, \mathfrak{a}\ ) \neq 0, \infty$ if Δ is different from the discriminant of F, and the action of the Galois group is given by the same cocycle condition derived from Shimura's reciprocity law. The integrality results of Section 4 (Corollaries 16 and 17) are not as easy to generalize. However, for $\Delta = 4$ Corollary 16 holds under the further assumption that $p \neq 2$.

BIBLIOGRAPHY

[Ek] T. EKEDHAL, On Supersingular Curves and Abelian Varieties, Math. Scand. 60 (1987), 151-178.

[FC] G. FALTINGS, C.-L. CHAI, Degeneration of Abelian Varieties, Springer-Verlag, Berlin-Heidelberg, 1990.

[G] Eyal Z. GOREN, Ph.D. Thesis, Hebrew University of Jerusalem (1996).

[Ig] J.I. IGUSA, On Siegel Modular Forms of Genus Two (II), Am. J. Math., 86 (1964), 392-412.

[KL] D. KUBERT, S. LANG, Modular Units, Springer-Verlag, Berlin-Heidelberg-New York, 1981.

[L] S. LANG, Elliptic Functions, Addison-Wesley, Reading, 1973.

[Oo] F. OORT, Which Abelian Surfaces are Products of Elliptic Curves? Math. Ann., 214, 1975, 35-47.

[Ra] K. RAMACHANDRA, Some Applications of Kronecker's Limit Formulas, Ann. Math., 80 (1964), 104-148.

[Ro] G. ROBERT, Unités Elliptiques, Bull. Soc. Math. France, Mémoire, 36 (1973).

[ShTa] G. SHIMURA, Y. TANIYAMA, Complex Multiplication of Abelian Varieties and its Applications to Number Theory, Math. Soc. Japan (1991).

[Sh1] G. SHIMURA, Theta Functions with Complex Multiplication, Duke Math. J., 43 (1976), 673-696.

[Sh2] G. SHIMURA, On Certain Reciprocity Laws for Theta Functions and Modular Forms, Acta Math., 141 (1978), 35-71.

[Sh3] G. SHIMURA, Arithmetic of Alternating Forms and Quaternion Hermitian Forms, J. Math. Soc. Japan, 15 (1963).

[Sie] C. L. SIEGEL, Lectures on Advanced Analytic Number Theory, Tata Institute for Fundamental Research (1961).

[Ta] J. TATE, Les Conjectures de Stark sur les Fonctions L d'Artin en s=0, Progress in Math. vol. 47, Birkhauser (1984).

[vdG] G. VAN DER GEER, Hilbert Modular Surfaces, Springer-Verlag, Berlin-Heidelberg-New York, 1988.

[Wa] L. WASHINGTON, Introduction to Cyclotomic Fields, Springer-Verlag, 1982.

Manuscrit reçu le 27 août 1996,
accepté le 24 janvier 1997.

E. DE SHALIT & E.Z. GOREN,
Hebrew University of Jerusalem
Institute of Mathematics
Givat Ram
91904 Jerusalem (Israël).
deshalit@math.huji.ac.il
egoren@abel.harvard.edu