Vol. 96, No. 2 DUKE MATHEMATICAL JOURNAL

THETA IDENTITIES WITH COMPLEX MULTIPLICATION

A. POLISHCHUK

Introduction. This paper grew out from the attempt to refine the notion of a symmetric line bundle on an abelian variety in the case of complex multiplication. Recall that a line bundle L on an abelian variety A is called *symmetric* if $(-\mathrm{id}_A)^*L \simeq L$. It is known that in this case one has an isomophism

$$(n\,\mathrm{id}_A)^*L \simeq L^{n^2}$$

for any $n \in \mathbb{Z}$. Now assume that A admits a complex multiplication by a ring R, that is, we have a ring homomorphism $R \to \mathrm{End}(A) : r \mapsto [r]_A$. If L is nondegenerate, then the corresponding polarization $\phi_L : A \to \hat{A}$ (where $\hat{A}$ is the dual abelian variety to A) defines the Rosati involution on $\mathrm{End}(A) \otimes \mathbb{Q}$ (see [5]). Assume that this involution is compatible with some involution ε on R. Let $R^+ \subset R$ be the subring of ε-invariant elements. Then for every $r \in R^+$, the homomorphism $\phi_L \circ [r]_A : A \to \hat{A}$ is self-dual; hence, one can ask whether it comes from some "natural" line bundle $L(r)$ on A. The word "natural" should mean in particular that the map $r \mapsto L(r)$ from R^+ to the group of symmetric line bundles on A is a homomorphism, resembling the usual homomorphism $n \mapsto L^n$. By analogy with the above isomorphism, we would like to impose the following condition on such a homomorphism

$$[r]_A^* L(r_0) \simeq L(\varepsilon(r) r_0 r)$$

for any $r \in R$, $r_0 \in R^+$. We call such data a $\Sigma_{R,\varepsilon}$-structure (since a suitable generalization of this notion to group schemes with complex multiplication is a refinement of the notion of Σ-structure defined by L. Breen in [2]).

In the first part of the paper we describe an obstruction to the existence of a $\Sigma_{R,\varepsilon}$-structure for a given polarization of A. It turns out that when R is commutative, one can prove the existence of a $\Sigma_{R,\varepsilon}$-structure, assuming that R is unramified at all ε-stable places above 2 (in noncommutative cases, one also needs some additional assumptions at archimedian places). In the case of an elliptic curve E with its standard principal polarization and $R = \mathrm{End}(E)$ this result is sharp: a $\Sigma_{R,\varepsilon}$-structure exists if and only if R is unramified at 2. In the case of commutative real multiplication, one needs only that R is normal above 2 to ensure the existence of a $\Sigma_{R,\varepsilon}$-structure.

Received 31 March 1997. Revision received 16 September 1997.
1991 *Mathematics Subject Classification.* Primary 14K25.

In the second part of the paper, we establish an analogue of generalized Riemann's theta relations (see, e.g., [6]) for theta functions with complex multiplication. Instead of an integer-valued matrix B such that $B^t \cdot B = n \cdot \mathrm{Id}$, where $n \in \mathbb{Z}_{>0}$, our identity uses a matrix A with elements in R (where the abelian variety in question has a complex multiplication by R) such that $B^\varepsilon \cdot B = n \cdot \mathrm{Id}$, where B^ε is obtained by applying ε to all entries of B^t. The existence of a $\Sigma_{R,\varepsilon}$-structure is reflected in the simplification of the expression for theta-characteristics in the right-hand side of this identity (see (2.3.6)).

In [7] we interpret the notion of a symmetric cube structure (Σ-structure in the terminology of [2]) as a monoidal functor from the category of integer-valued symmetric forms to the category of abelian varieties equipped with line bundles. The notion of $\Sigma_{R,\varepsilon}$-structure arises when one tries to find a similar picture in the case of complex multiplication. In the present paper we show (Theorem 1.3.2) that a $\Sigma_{R,\varepsilon}$-structure indeed leads to a monoidal functor from the category of ε-hermitian, projective R-modules. The results of Section 1.5 on the existence of $\Sigma_{R,\varepsilon}$-structure and the simplest example of theta-identity with complex multiplication can also be found in [7].

Acknowledgment. I am grateful to B. Gross for helpful discussions.

1. Line bundles on abelian varieties with complex multiplication

1.1. Basic operations on abelian varieties with complex multiplication. Let R be a ring and A be an abelian variety with complex multiplication by R; that is, a homomorphism $R \to \mathrm{End}(A)$ is given. For an element $r \in R$ we denote by $[r]_A$ the corresponding endomorphism of A.

Given a finitely generated, projective right R-module P, one can define the tensor product $P \otimes_R A$ (which is an abelian variety) based on the property

$$\mathrm{Hom}(P \otimes_R A, A') \simeq \mathrm{Hom}_R(P, \mathrm{Hom}(A, A')) \tag{1.1.1}$$

for any abelian variety A', where the left R-action on A induces the right R-action on $\mathrm{Hom}(A, A')$. Notice that when the ring R is commutative, there is a natural R-action on the tensor product $P \otimes_R A$ defined above. In particular, when R is commutative, tensoring with rank-1 projective R-modules P gives the well-known action of the group $\mathrm{Pic}(R)$ on the set of abelian varieties with complex multiplication by R.

Similarly, if Q is a finitely generated, projective left R-module and A has complex multiplication by R, then one can define an abelian variety $\mathrm{Hom}_R(Q, A)$ such that

$$\mathrm{Hom}(A', \mathrm{Hom}_R(Q, A)) \simeq \mathrm{Hom}_R(Q, \mathrm{Hom}(A', A)) \tag{1.1.2}$$

for any abelian variety A', where $\mathrm{Hom}(A', A)$ is equipped with the natural left

R-action. It is easy to see that

$$\mathrm{Hom}_R(Q, A) \simeq \mathrm{Hom}_R(Q, R) \otimes_R A,$$

where $\mathrm{Hom}_R(Q, R)$ is considered as a right R-module in the natural way.

For an abelian variety B, we denote by $\hat{B}$ the dual abelian variety. If A has complex multiplication by R, then the dual variety $\hat{A}$ has the induced complex multiplication by the opposite ring R^{op}, such that $\widehat{[r]_A} = [r]_{\hat{A}}$. For any finitely generated, projective right R-module P, one has a canonical isomorphism

$$\widehat{P \otimes_R A} \simeq \mathrm{Hom}_{R^{\mathrm{op}}}(P, \hat{A}), \tag{1.1.3}$$

where in the right-hand side P is considered as a left R^{op}-module.

Now assume that R is equipped with an involution $\varepsilon : R \to R$; that is, ε is an antiautomorphism of R such that $\varepsilon^2 = \mathrm{id}$. Then we can convert the complex multiplication by R^{op} on $\hat{A}$ into a complex multiplication by R using ε. Hence, the isomorphism (1.1.3) can be rewritten as

$$\widehat{P \otimes_R A} \simeq \mathrm{Hom}_R(P^{\varepsilon}, \hat{A}) \simeq \mathrm{Hom}_R(P^{\varepsilon}, R) \otimes_R \hat{A}, \tag{1.1.4}$$

where P^{ε} is the left R-module obtained from P using the involution ε.

1.2. Sesquilinear forms and biextensions. There is a bijective correspondence between homomorphisms of abelian varieties $A_2 \to \hat{A}_1$ and biextensions of $A_1 \times A_2$ by $\mathbb{G}_m$. Recall that the latter are given by line bundles $\mathscr{B}$ on $A_1 \times A_2$ together with isomorphisms

$$(p_1 + p_2, p_3)^* \mathscr{B} \simeq p_{13}^* \mathscr{B} \otimes p_{23}^* \mathscr{B},$$

$$(p_1, p_2 + p_3)^* \mathscr{B} \simeq p_{12}^* \mathscr{B} \otimes p_{13}^* \mathscr{B}$$

on $A_1 \times A_1 \times A_2$ and $A_1 \times A_2 \times A_2$, satisfying some natural compatibility conditions (see [2]). For a homomorphism $\phi : A_2 \to \hat{A}_1$, the corresponding biextension $\mathscr{B}_\phi$ is given by a line bundle $(\mathrm{id}, \phi)^* \mathscr{P}$ on $A_1 \times A_2$, where $\mathscr{P}$ is the Poincaré line bundle on $A_1 \times \hat{A}_1$.

If A_1 and A_2 have complex multiplications by R^{op} and R, respectively, then the condition that a homormorphism $A_2 \to \hat{A}_1$ is compatible with R-action is equivalent to the condition that the corresponding biextension $\mathscr{B}$ of $A_1 \times A_2$ is equipped with natural isomorphisms

$$a_r : (r \times \mathrm{id})^* \mathscr{B} \xrightarrow{\sim} (\mathrm{id} \times r)^* \mathscr{B}$$

for every $r \in R$. If we write the R^{op}-action on A_1 as the right R-action, then isomorphisms a_r can be written symbolically as $\mathscr{B}_{xr,y} \simeq \mathscr{B}_{x,ry}$. These isomorphisms are compatible with the structure of biextension on $\mathcal{B}$ and with the R-module structure on A as explained in the following definition (cf. [4, VII 2.10.3], where the case of the commutative ring R is considered).

Definition 1.2.1. An *R-biextension* of $A_1 \times A_2$ is a biextension $\mathcal{B}$ of $A_1 \times A_2$ together with a system of isomorphisms of biextensions a_r as above, such that

(1) the composition

$$\mathcal{B}_{x(r+r'),y} = \mathcal{B}_{xr+xr',y} \xrightarrow{c} \mathcal{B}_{xr,y} \otimes \mathcal{B}_{xr',y} \xrightarrow{a_r \otimes a'_r} \mathcal{B}_{x,ry} \otimes \mathcal{B}_{x,r'y} \xrightarrow{c^{-1}} \mathcal{B}_{x,ry+r'y}$$
$$= \mathcal{B}_{x,(r+r')y},$$

where c is the isomorphism giving a structure of biextension on $\mathcal{B}$, coincides with $a_{r+r'}$;

(2) the composition

$$\mathcal{B}_{xr'r,y} \xrightarrow{a_r} \mathcal{B}_{xr',ry} \xrightarrow{a_{r'}} \mathcal{B}_{x,r'ry}$$

coincides with $a_{r'r}$.

It is easy to see that R-biextensions of $A_1 \times A_2$ correspond bijectively to homomorphisms $A_2 \to \hat{A}_1$ compatible with R-action. However, the definition above has an advantage in that it can be given for arbitrary group schemes.

Now if R is equipped with involution ε, and if A_1, A_2 are abelian varieties with complex multiplication by R, then we can define an (R, ε)-*biextension* of $A_1 \times A_2$ to be an R-biextension of $A_1^{\varepsilon} \times A_2$, where A_1^{ε} is A_1 with a complex multiplication by R^{op} induced by ε. In other words, an (R, ε)-biextension is a biextension $\mathcal{B}$ of $A_1 \times A_2$ together with isomorphisms $\mathcal{B}_{\varepsilon(r)x,y} \simeq \mathcal{B}_{x,ry}$ for $r \in R$, satisfying the compatibility conditions analogous to the conditions (1) and (2) in Definition 1.2.1. The corresponding homomorphism $\phi : A_2 \to \hat{A}_1$ satisfies $\phi \circ [r]_{A_2} = \widehat{[\varepsilon(r)]_{A_1}} \circ \phi$ for all $r \in R$. If ϕ is an isogeny, then this is equivalent to the following equality in $\mathrm{End}(A_2) \otimes \mathbb{Q}$:

$$[\varepsilon(r)]_{A_2} = \phi^{-1} \circ \widehat{[r]_{A_1}} \circ \phi.$$

For example, if $A_1 = A_2 = A$ and $\phi = \phi_M$ for some ample line bundle M on A, then the right-hand side of this equality is the Rosati involution associated with M evaluated at r. Hence, ϕ_M corresponds to an (R, ε)-biextension if and only if ε is compatible with the Rosati involution.

An example of an (R, ε)-biextension is the canonical biextension of $\mathrm{Jac}(C)^2$ for a curve C with automorphisms. Namely, let $R = \mathbb{Z}[\mathrm{Aut}(C)]$ be the group ring of the group $\mathrm{Aut}(C)$ and $\varepsilon : R \to R$ be the involution such that $\varepsilon(g) = g^{-1}$ for $g \in \mathrm{Aut}(C)$. Then for line bundles L_1, L_2 on C, and for an automorphism g of C, we have a natural isomorphism $\langle g^*L_1, L_2\rangle \simeq \langle L_1, (g^{-1})^*L_2\rangle$, where $\langle\cdot,\cdot\rangle$ denotes the symbol defined in [3].

Let P_1 be a left R-module and P_2 a right R-module. A *sesquilinear form* $b : P_1 \times P_2 \to R$ is a $\mathbb{Z}$-bilinear map such that $b(rx, y) = rb(x, y)$, $b(x, yr) = b(x, y)r$. This is the same as a morphism of left R-modules $P_1 \to \mathrm{Hom}_R(P_2, R)$ or a morphism of right R-modules $P_2 \to \mathrm{Hom}_R(P_1, R)$. Note that if R is equipped with an involution ε, then we can convert right R-modules into left ones, and vice versa. Thus, if P_1' and P_2 are right R-modules, then $b : P_1' \times P_2 \to R$ is a sesquilinear form if b is $\mathbb{Z}$-bilinear, and $b(xr, y) = \varepsilon(r)b(x, y)$, $b(x, yr) = b(x, y)r$ for every $r \in R$.

Let A_1 be an abelian variety with complex multiplication by R^{op}, and let A_2 be an abelian variety with complex multiplication by R. Assume we are given a homomorphism $\phi : A_2 \to \hat{A}_1$ compatible with R-action. Then for every sesquilinear form $b : P_1 \times P_2 \to R$, one can construct a canonical homomorphism of abelian varieties

$$\phi(b) : (P_2 \otimes_R A_2) \to P_1 \widehat{\otimes_{R^{\mathrm{op}}}} A_1.$$

Namely, using (1.1.3), (1.1.2), and (1.1.1), we can write

$$\begin{aligned}\mathrm{Hom}(P_2 \otimes_R A_2, P_1 \widehat{\otimes_{R^{\mathrm{op}}}} A_1) &\simeq \mathrm{Hom}(P_2 \otimes_R A_2, \mathrm{Hom}_R(P_1, \hat{A}_1))\\ &\simeq \mathrm{Hom}_R(P_1, \mathrm{Hom}(P_2 \otimes_R A_2, \hat{A}_1))\\ &\simeq \mathrm{Hom}_R(P_1, \mathrm{Hom}_R(P_2, \mathrm{Hom}(A_2, \hat{A}_1))).\end{aligned}$$

Now we can produce an element in the latter group, that is, a homomorphism of left R-modules $P_1 \to \mathrm{Hom}_R(P_2, \mathrm{Hom}(A_2, \hat{A}_1))$ by the formula $x \mapsto (y \mapsto \phi \circ [b(x, y)]_{A_2})$.

Thus, every R-biextension $\mathscr{B}$ of $A_1 \times A_2$ induces a map $b \mapsto \mathscr{B}(b)$ from the set of sesquilinear forms $b : P_1 \times P_2 \to R$ to biextensions of $(P_1 \otimes_{R^{\mathrm{op}}} A_1) \times (P_2 \otimes_R A_2)$. The original biextension $\mathscr{B}$ is obtained as $\mathscr{B}(b_1)$ for $P_1 = R$ as a left R-module, and for $P_2 = R$ as a right R-module, $b_1(r_1, r_2) = r_1 r_2$. One can easily see that

$$\mathscr{B}(b_1 + b_2) \simeq \mathscr{B}(b_1) \otimes \mathscr{B}(b_2). \tag{1.2.1}$$

Also if $f_1 : P_1 \to P_1'$ and $P_2 \to P_2'$ are morphisms of R-modules and $b' : P_1' \times P_2' \to R$ is a sesquilinear form, then $b = (f_1, f_2)^* b' : P_1 \times P_2 \to R$ is sesquilinear and $\mathscr{B}(b) \simeq (f_1 \otimes_R A \times f_2 \otimes_R A)^* \mathscr{B}(b')$. For example, for every $r \in R$ we have a morphism of right R-modules $l(r) : R \to R : r' \mapsto rr'$. Then the pull-back of the form b_1 by $(\mathrm{id}, l(r))$ is the sesquilinear form $b_r(r_1, r_2) = r_1 r r_2$. The above functoriality implies that

$$\mathscr{B}(b_r) \simeq (\mathrm{id} \times [r]_{A_2})^* \mathscr{B}. \tag{1.2.2}$$

Note that we can consider P_2 as a left R^{op}-module and P_1 as a right R^{op}-module. Then b induces a sesquilinear form $b^{\mathrm{op}} : P_2 \times P_1 \to R^{\mathrm{op}}$ on these R^{op}-modules. Now the biextension $\mathscr{B}(b^{\mathrm{op}})$ of $A_2 \times A_1$ is obtained from $\mathscr{B}(b)$ by permutation of factors.

When R is equipped with an involution ε, one can identify R^{op} with R and rewrite the above constructions using only right R-modules.

1.3. Hermitian forms and line bundles. Let A be an abelian variety with complex multiplication by R and ε be an involution on R. Recall that every (rigidified) line bundle M on A defines a symmetric biextension $\Lambda(M)$ of A^2 by the formula

$$\Lambda(M) = m^*M \otimes p_1^*M^{-1} \otimes p_2^*M^{-1},$$

which corresponds to a symmetric morphism $\phi_M : A \to \hat{A}$. Now assume that $\Lambda(M)$ is an (R, ε)-biextension. Then for every finitely generated, projective right R-module P and a sesquilinear form $b : P \times P \to R$, the construction of the previous section gives a biextension $\mathscr{B}(b)$ of $(P \otimes_R A)^2$. It is easy to see that this biextension is symmetric provided that b is a *hermitian* form; that is, b, in addition to being sesquilinear, satisfies the identity $b(y, x) = \varepsilon(b(x, y))$. We are going to study the following question: When for every hermitian form b can one find a "natural" line bundle $L(b)$ on $P \otimes_R A$ such that $\mathscr{B}(b) \simeq \Lambda(L(b))$? "Natural" means that if $b = f^*b'$ for some morphism of R-modules $f : P \to P'$, then $L(b) = (f \otimes_R A)^* L(b')$, and if $(P, b) = (P_1, b_1) \oplus (P_2, b_2)$ is a direct sum in the category of hermitian modules, then $L(b)$ is the external tensor product of $L(b_1)$ and $L(b_2)$. To see what this means, note that for any $r \in R^+ = \{r_1 \in R \mid \varepsilon(r_1) = r_1\}$, we have the hermitian form h_r on R defined by $h_r(1, 1) = r$; that is, $h_r(x, y) = \varepsilon(x) r y$. Thus, we should have the set of line bundles $L(r)$ on A corresponding to the forms h_r. The "naturality" imposes certain restrictions on $L(r)$, which are described in the following definition.

Definition 1.3.1. Let A be an abelian variety, $R \to \mathrm{End}(A) : r \mapsto [r] = [r]_A$ a ring homomorphism, and $\phi : A \to \hat{A}$ a symmetric homomorphism (that is, $\hat{\phi} = \phi$) such that $\phi \circ [\varepsilon(r)]_A = [r]_{\hat{A}} \circ \phi$ for any $r \in R$, where $[r]_{\hat{A}} = \widehat{[r]_A}$. Then a $\Sigma_{R,\varepsilon}$*-structure* for ϕ is a homomorphism $R^+ \to \mathrm{Pic}^+(A) : r_0 \mapsto L(r_0)$, where $\mathrm{Pic}^+(A)$ is the group of symmetric line bundles on A such that

$$\phi_{L(r_0)} = \phi \circ [r_0]_A \tag{1.3.1}$$

for any $r_0 \in R^+$ and

$$r^* L(r_0) \simeq L(\varepsilon(r) r_0 r) \tag{1.3.2}$$

for any $r \in R$, $r_0 \in R^+$.

Note that (1.3.1) and (1.3.2) lead to the isomorphism

$$L(\varepsilon(r)+r) \simeq ([r],\phi)^*\mathscr{P} \tag{1.3.3}$$

for any $r \in R$. (Apply (1.3.2) to r and $r+1$ and use an isomorphism $\Lambda(L(1)) \simeq (\mathrm{id}\times\phi)^*\mathscr{P}$ on $A\times A$.) If $L(r)$ is a $\Sigma_{R,\varepsilon}$-structure for ϕ, then any other $\Sigma_{R,\varepsilon}$-structure for ϕ has the form

$$L'(r) = L(r)\otimes\eta(r),$$

where $\eta : R^+ \to \mathrm{Pic}_2(A)$ is a homomorphism such that $r^*\eta(r_0) \simeq \eta(\varepsilon(r)r_0 r)$ for any $r\in R$, $r_0 \in R^+$. It follows from (1.3.3) that for such η we also have $\eta(\varepsilon(r)+r)=0$.

There is a trivial example of $\Sigma_{R,\varepsilon}$-structure for 2ϕ: $L(r) = (\mathrm{id}, \phi\circ[r]_A)^*\mathscr{P}$, where $\mathscr{P}$ is the Poincaré line bundle on $A\times\hat{A}$. In particular, if $\phi=\phi_M$ for a symmetric line bundle M on A, then $L(1)\simeq M^2$ in this example. The natural question is under what condition on M there exists a $\Sigma_{R,\varepsilon}$-structure with $L(1)=M$. Below we consider this question for symmetric line bundles of degree 1 on elliptic curves. Now we are going to show that a $\Sigma_{R,\varepsilon}$-structure induces a monoidal functor from the category of hermitian forms to the category of line bundles over abelian varieties.

THEOREM 1.3.2. *Assume that a $\Sigma_{R,\varepsilon}$-structure $L(\cdot) : R^+ \to \mathrm{Pic}^+(A)$ for ϕ is given. Then for every finitely generated, projective right R-module P and a hermitian form h on P, there is a canonical symmetric line bundle $L(h)$ on $P\otimes_R A$ such that $\Lambda(L(h)) \simeq \mathscr{B}_\phi(h)$. Furthermore, if $f : P\to P'$ is a morphism of such modules and $h = f^*h'$, then $L(h)\simeq (f\otimes_R A)^*L(h')$. Also, if $(P,h)\simeq(P_1,h_1)\oplus(P_2,h_2)$, then $L(h)$ is isomorphic to the external tensor product of $L(h_1)$ and $L(h_2)$.*

Proof. For every collection of elements $x_1,\ldots,x_n\in P$, we denote by $i_{x_1,\ldots,x_n} : R^n \to P$ the corresponding morphism of right R-modules: $i_{x_1,\ldots,x_n}(r_1,\ldots,r_n) = x_1r_1+\cdots+x_nr_n$. We define $L(h)$ as a unique rigidified line bundle on $P\otimes_R A$ such that for every element $x\in P$, one has

$$(i_x\otimes_R A)^*L(h)\simeq L(h(x,x)),$$

and for every pair of elements $x_1,x_2\in P$, one has

$$(i_{x_1,x_2}\otimes_R A)^*L(h)\simeq p_1^*L(h(x_1,x_1))\otimes p_2^*L(h(x_2,x_2))\otimes(\mathrm{id}\times\phi\circ[h(x,y)]_A)^*\mathscr{P},$$

where we identify $R^2\otimes_R A$ with A^2, p_i, $i=1,2$ are the projections of A^2 on A, and $\mathscr{P}$ is the Poincaré bundle. First, let us check the uniqueness. When $P=R^n$ the uniqueness follows immediately from the theorem of cube. For arbitrary P we can choose a surjective morphism $f : R^n\to P$. Then it follows by definition that $(f\otimes_R A)^*L(h) = L(f^*h)$, where f^*h is the induced form on R^n. Since f is a projection onto a direct summand this implies the uniqueness of $L(h)$. As for existence, let us begin with the case $P = R^n$. Then if $\{e_1, \ldots, e_n\}$ is the standard base of R^n, let us denote $h_{ij} = h(e_i, e_j)$ and set

$$L(h) = \bigotimes_i p_i^* L(h_{ii}) \otimes \bigotimes_{i<j} p_{ij}^*([h_{ij}]_A, \phi)^* \mathscr{P}.$$

One can check easily that the required isomorphisms hold. Now to prove the existence of $L(h)$ in general, choose a surjection $f : R^n \to P$. Then it is sufficient to check that $L(f^*h)$ is in fact a pull-back of some line bundle on $P \otimes_R A$ by $f \otimes_R A : A^n \to P \otimes_R A$. In other words, we have to check that two pull-backs of $L(f^*h)$ to the fiber product $A^n \times_{P \otimes_R A} A^n$ are the same. But this fiber product is of the form $Q \otimes_R A$, where $Q = \ker(R^n \oplus R^n \xrightarrow{(f,-f)} P)$ and two projections to A^n are induced by the natural projections $g_1, g_2 : Q \to R^n$. Now the required isomorphism of two pull-backs of $L(f^*h)$ follows from the equality $g_1^* f^* h = g_2^* f^* h$ of hermitian forms on Q. This proves the existence of $L(h)$. In the case $P = R^n$, using (1.2.1) and (1.2.2) one easily shows that $\Lambda(L(h)) \simeq \mathscr{B}_\phi(h)$. The case of general P follows by considering a surjection $R^n \to P$ as before. The functoriality of $L(h)$ in h follows from its construction. □

1.4. Case of elliptic curve. Let us consider the case when $A = E$ is an elliptic curve, $\phi_0 : E \simeq \hat{E}$ is the standard principal polarization induced by the line bundle $\mathcal{O}(e)$, where $e \in E$ is the neutral element and $R \subset \operatorname{End}(E)$ is a subring closed under the Rosati involution. We assume that the ground field k is algebraically closed and $\operatorname{char}(k) \neq 2$. It is known that $R^+ \subset \mathbb{Z}$; hence, a $\Sigma_{R,\varepsilon}$-structure for ϕ_0 is determined uniquely by the line bundle $L(1)$, which should be of the form $\mathcal{O}(p)$ where $p \in E_2$ is a point of order 2 on E.

PROPOSITION 1.4.1. *Fix a point $p \in E_2$. The following conditions are equivalent:*

(1) *there exists a $\Sigma_{R,\varepsilon}$-structure for ϕ_0 with $L(1) = \mathcal{O}(p)$;*
(2) *for every $r \in R$ such that $r|_{E_2} \neq 0$, one has either $p \notin r(E_2)$, or $r(E_2) = E_2$ and $r(p) = p$.*

Proof. The line bundle $L(1) = \mathcal{O}(p)$ defines a $\Sigma_{R,\varepsilon}$-structure if and only if for every $r \in R$, $r \neq 0$ there is an isomorphism

$$\mathcal{O}(N(r)p) \simeq r^* L(1) = \mathcal{O}(r^{-1}(p)),$$

where $N(r) = \varepsilon(r) r \in \mathbb{Z}$. Since the divisor $r^{-1}(p) \subset E$ is symmetric, this is equivalent to the following equality in E:

$$\sum_{x \in r^{-1}(p) \cap E_2} x = N(r)p. \tag{1.4.1}$$

Note that $N(r) = \deg(r) \equiv |\ker(r|_{E_2})| \bmod(2)$. Thus, $N(r)p = 0$ if and only if $\ker(r|_{E_2}) \neq 0$, otherwise $N(r)p = p$. In particular, both parts of (1.4.1) are equal to zero when $p \notin r(E_2)$. Now assume that $p = r(x_0)$. If, in addition, $r|_{E_2}$ is invertible, then (1.4.1) becomes $x_0 = p$; that is, $r(p) = p$. Otherwise, $|\ker(r|_{E_2})| = 2$ and (1.4.1) becomes $\sum_{x \in \ker(r|_{E_2})} x = 0$, which is impossible. □

In the case $p = e$, the above proposition implies that a $\Sigma_{R,\varepsilon}$-structure with $L(1) = \mathcal{O}(e)$ exists if and only if for every $r \in R$ the restriction $r|_{E_2}$ is either zero or invertible; that is, the image of R under the natural homomorphism $\mathrm{End}(E) \to \mathrm{End}(E_2)$ is a field. Note that there is a maximal subfield $\mathbb{F}_4$ in the matrix algebra $\mathrm{M}_2(\mathbb{F}_2)$. Namely, $\mathbb{F}_4 = \{0, I, A, A^2 = A + I\}$, where I is the identity matrix $A = \left(\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. This means that the maximal subalgebra R_0 of $\mathrm{End}(E)$, for which there exists a $\Sigma_{R_0,\varepsilon}$-structure with $L(1) = \mathcal{O}(e)$, is the preimage of $\mathbb{F}_4$ under the homomorphism $\mathrm{End}(E) \to \mathrm{M}(2, \mathbb{F}_2)$. For example, if $\mathrm{End}(E)$ is commutative, then $R_0 = \mathrm{End}(E)$ if and only if 2 remains prime in $\mathrm{End}(E)$. When $\mathrm{End}(E)$ is an order in an imaginary quadratic extension of $\mathbb{Q}$ so that $\mathrm{End}(E) = \mathbb{Z} + \mathbb{Z}((D + \sqrt{D})/2) \subset \mathbb{C}$, where $D < 0$, this happens if and only if $D \equiv 5 \bmod (8)$. Otherwise, $R_0 = \{r \in \mathrm{End}(E) \mid r \equiv \lambda\, \mathrm{id} (\bmod 2\, \mathrm{End}(E)), \lambda \in \mathbb{Z}/2\mathbb{Z}\}$.

In the case when $p \in E_2$ is nonzero, we can choose a basis $\{e_1, e_2\}$ in E_2 with $e_1 = p$ and use the corresponding identification of $\mathrm{End}(E_2)$ with $\mathrm{M}(2, \mathbb{F}_2)$. Then the above proposition implies that $\Sigma_{R,\varepsilon}$-structure with $L(1) = \mathcal{O}(p)$ exists if and only if the image of R in $\mathrm{M}(2, \mathbb{F}_2)$ is a subalgebra $\bar{R} \subset \mathrm{M}(2, \mathbb{F}_2)$ such that for every $T \in \bar{R} \backslash \{0, 1\}$ one has either $e_1 \notin \mathrm{im}(T)$ or $e_1 = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. One can easily show that besides $\mathbb{F}_2 \subset \mathrm{M}(2, \mathbb{F}_2)$ there are only two more subalgebras in $\mathrm{M}(2, \mathbb{F}_2)$ having this property (both isomorphic to $\mathbb{F}_2 \times \mathbb{F}_2$): one is generated over $\mathbb{F}_2$ by the matrix $\left(\begin{smallmatrix} 0 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, and the other is generated by $\left(\begin{smallmatrix} 1 & 0 \\ 1 & 0 \end{smallmatrix}\right)$. In particular, $\bar{R}$ has no nilpotents. This proves the "only if" part of the following theorem.

Theorem 1.4.2. *A $\Sigma_{R,\varepsilon}$-structure for ϕ_0 exists if and only if the image of R in* $\mathrm{End}(E_2)$ *is a ring without nilpotents.*

Proof. Let $\bar{R} \subset \mathrm{End}(E_2)$ be a ring without nilpotents. Then either $\bar{R}$ is a field, or it contains a nontrivial idempotent. In the former case, $\bar{R}$ is contained in $\mathbb{F}_4 \subset \mathrm{End}(E_2)$. Otherwise, we can choose a base in E_2 in such a way that $\bar{R}$ contains $E_{11} = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$, and hence it contains the subalgebra $D \subset \mathrm{M}(2, \mathbb{F}_2)$ of diagonal matrices. Since $\bar{R}$ is without nilpotents, this implies that $\bar{R} = D$.

If $\bar{R}$ is a field, then $L(1) = \mathcal{O}(e)$ defines a $\Sigma_{R,\varepsilon}$-structure as we have seen above. Otherwise, for some basis $\{e_1, e_2\}$ of E_2, the subalgebra $\bar{R}$ coincides with $D \subset \mathrm{M}(2, \mathbb{F}_2) \simeq \mathrm{End}(E_2)$. Now the conditions of Proposition 1.4.1 are satisfied for $p = e_1 + e_2$; hence, $L(1) = \mathcal{O}(p)$ defines a $\Sigma_{R,\varepsilon}$-structure in this case. □

1.5. Existence of $\Sigma_{R,\varepsilon}$-structure. Consider first the case when R is a commutative integral domain finite over $\mathbb{Z}$ and $\varepsilon = \mathrm{id}$, that is, $R = R^+$ (the case of real multiplication). Then the homomorphism $\phi : A \to \hat{A}$ above should be just R-linear. We say that R is unramified at 2 if $R/2R$ has no nilpotents.

Proposition 1.5.1. *Let A be an abelian variety with multiplication by R, and let M be a symmetric line bundle on A such that $\phi = \phi_M$ is R-linear. Assume that R is unramified at 2. Then there exists a unique $\Sigma_{R,\mathrm{id}}$-structure for ϕ with $L(1) = M$.*

Proof. Since $R/2R$ is a product of fields, the Frobenius homomorphism $F : R/2R \to R/2R : x \to x^2$ is bijective. Hence, any element $r \in R$ can be represented in the form $r = a^2 + 2b$ with $a, b \in R$, and if $a_1^2 + 2b_1 = a_2^2 + 2b_2$, then $a_2 - a_1 \in 2R$. Now we define the $\Sigma_{R,\mathrm{id}}$-structure

$$L(r) := a^* M \otimes ([b], \phi)^* \mathscr{P},$$

where $r = a^2 + 2b$. It is easy to check that $L(r)$ is well defined and satisfies the required properties. The uniqueness follows from (1.3.2) and (1.3.3). □

Returning to the general case, let us describe an obstruction to the existence of a $\Sigma_{R,\varepsilon}$-structure for a given ϕ. For this we need to assume that the ground field is algebraically closed of characteristic $\neq 2$. Consider the group

$$\tilde{K}(\phi) = \{(L, r_0) \mid L \in \mathrm{Pic}^+(A), r_0 \in R^+, \phi_L = \phi \circ [r_0]_A\}$$

with the group law $(L, r_0)(L', r_0') = (L \otimes L', r_0 + r_0')$. We have an exact sequence of abelian groups

$$0 \to \mathrm{Pic}_2(A) \to \tilde{K}(\phi) \xrightarrow{\pi} R^+ \to 0, \tag{1.5.1}$$

where the the first embedding is $\eta \mapsto (\eta, 0)$, $\eta \in \mathrm{Pic}_2(A)$, and π is the projection $(L, r_0) \mapsto r_0$. Moreover, we have a canonical splitting σ of the pull-back of this extension by the homomorphism $\mathrm{tr} : R \to R^+ : r \mapsto \varepsilon(r) + r$:

$$\sigma(r) = (([r], \phi)^* \mathscr{P}, \varepsilon(r) + r).$$

Note that if a $\Sigma_{R,\varepsilon}$-structure for ϕ exists, then for $r \in R^- = \{r \in R : \varepsilon(r) = -r\}$ from (1.3.3) we get that the line bundle $([r], \phi)^* \mathscr{P} \simeq L(0)$ is trivial. Thus, the first obstacle to existence of such a structure is given by a homomorphism

$$\delta(\phi) : R^- \to \mathrm{Pic}_2(A) : r \mapsto ([r], \phi)^* \mathscr{P}.$$

The inclusion $([r], \phi)^* \mathscr{P} \in \mathrm{Pic}_2(A)$ follows from the isomorphism

$$([r], \phi)^* \mathscr{P} \simeq (\mathrm{id}, \phi \circ [r])^* \mathscr{P} \simeq ([\varepsilon(r)], \phi)^* \mathscr{P}.$$

This isomorphism implies also that $\delta(\phi)$ factors through a homomorphism $\bar{\delta}(\phi) : R^-/\mathrm{tr}^-(R) \to \mathrm{Pic}_2(A)$, where $\mathrm{tr}^-(r) = r - \varepsilon(r)$. Notice that $\bar{\delta}$ can be considered as a morphism of right $R/2R$-modules, where the action of $R/2R$ on $\mathrm{Pic}_2(A)$ is given by $r(\eta) = r^*(\eta)$, while its action on $R^-/\mathrm{tr}^-(R)$ is given by $r(r') = \varepsilon(r)r'r \bmod(\mathrm{tr}^-(R))$, where $r \in R$, $r' \in R^-/\mathrm{tr}^-(R)$.

Assume that $\delta(\phi) = 0$. Then σ descends to a splitting $\bar{\sigma} : \mathrm{tr}(R) \to \tilde{K}(\phi)$ of π over the subgroup $\mathrm{tr}(R) \subset R^+$. Hence, we can define the reduced group $K(\phi) = \tilde{K}(\phi)/\sigma(\mathrm{tr}(R))$, which is an extension of $R/\mathrm{tr}(R)$ by $\mathrm{Pic}_2(A)$. It is easy to see that the group $K(\phi)$ has a natural structure of right $R/2R$-module induced by the action $r(L, r') = (r^*L, \varepsilon(r)r'r)$, so we can consider the exact sequence

$$0 \to \mathrm{Pic}_2(A) \to K(\phi) \to R^+/\mathrm{tr}(R) \to 0 \tag{1.5.2}$$

as an extension of $R/2R$-modules, where $R^+/\mathrm{tr}(R)$ is equipped with the following (right) $R/2R$-module structure: $r(r_0) = \varepsilon(r)r_0 r \bmod(\mathrm{tr}(R))$ for $r \in R$, $r_0 \in R^+$.

PROPOSITION 1.5.2. *Assume that the ground field is algebraically closed of characteristic $\neq 2$. Then a $\Sigma_{R,\mathrm{id}}$-structure for ϕ exists if and only if $\bar{\delta}(\phi) = 0$ and the class $e(\phi) \in \mathrm{Ext}^1_{R/2R}((R^+/\mathrm{tr}(R), \mathrm{Pic}_2(A))$ of the extension (1.5.2) is trivial.*

Proof. We have seen that the condition $\bar{\delta}(\phi) = 0$ is necessary for existence of a $\Sigma_{R,\varepsilon}$-structure for ϕ. Also, such a structure gives a splitting $r_0 \mapsto (L(r_0), r_0)$ of the extension (1.5.1), which induces an $R/2R$-linear splitting of (1.5.2). Since all the steps in the argument are invertible, the "if" part follows easily. □

Remark. Notice that in the case of the standard polarization ϕ_0 of an elliptic curve the homomorphism $\bar{\delta}(\phi_0)$ can be nontrivial. Indeed, the triviality of this homomorphism is equivalent to the triviality of the line bundle $\mathcal{O}(E_{r-1} - E_r - e)$ for any $r \in R^-$ where we denote $E_r = r^{-1}(e)$. In the case of characteristic zero, this is equivalent to the following identity for the group law on E:

$$\sum_{(r-1)x=0} x = \sum_{rx=0} x$$

for any $r \in R^-$. One can see easily that this can happen only when both sides are zero. In particular, if $\ker(r|_{E_2})$ has order 2, but $\ker((r-1)|_{E_2}) = 0$, then $\bar{\delta}(\phi_0) \neq 0$. For example, this is so when R contains $r = \sqrt{-2}$, which acts nontrivially on E_2.

Let R be an order in a finite-dimensional division algebra D over $\mathbb{Q}$, and let ε be an involution of R, such that the corresponding involution of D is positive, that is, $\mathrm{Tr}_{D/\mathbb{Q}}(\varepsilon(x)x) > 0$ for any $x \in D^*$. Let K be the center of D, so that $\mathfrak{o} = R \cap K$ is an order in K. Recall (see, e.g., [5]) that if $\varepsilon|_{\mathfrak{o}}$ is trivial, then either $D = K$ or D is a quaternion algebra over K, which is either totally indefinite (unramified at every infinite place) or totally definite.

THEOREM 1.5.3. *Assume that $\mathfrak{o}$ is unramified at every ε-stable prime ideal $\mathfrak{p}$ of $\mathfrak{o}$ above 2 and that $R/\mathfrak{p}R$ is semisimple. If $\varepsilon|_{\mathfrak{o}}$ is trivial, then assume, in addition,* *that either $D = K$ or that D is an indefinite quaternion algebra over K and for every prime $\mathfrak{p} \subset \mathfrak{o}$ over 2, the completion $\hat{R}_{\mathfrak{p}}$ is isomorphic to the matrix algebra $\mathrm{M}_2(\hat{\mathfrak{o}}_{\mathfrak{p}})$, where $\hat{\mathfrak{o}}_{\mathfrak{p}}$ is the completion of $\mathfrak{o}$ at $\mathfrak{p}$. Let A be an abelian variety over an algebraically closed field k such that $\mathrm{char}(k) \neq 2$. Then for any symmetric homomorphism $\phi : A \to \hat{A}$, such that $\phi \circ [\varepsilon(r)]_A = [r]_{\hat{A}} \circ \phi$ for any $r \in R$, there exists a $\Sigma_{R,\varepsilon}$-structure for ϕ.*

Remark. Let $\mathfrak{o}$ be the ring of integers in K and R be the maximal $\mathfrak{o}$-order in D. Then the conditions of the above theorem are that $K/\mathbb{Q}$ and D/K are unramified at every ε-stable place of K above 2 and D is not a definite quaternion algebra over K when $\varepsilon|_K$ is trivial (is not of Type III in the classification list of [5, IV, 21, Thm. 2]).

We need two lemmas for the proof.

LEMMA 1.5.4. *Let $\mathbb{F}_{2^l}$ be a finite field with 2^l elements and let $M = \mathrm{M}_n(\mathbb{F}_{2^l})$ be the matrix algebra over $\mathbb{F}_{2^l}$. Let σ be an involution of M such that $\sigma|_{\mathbb{F}_{2^l}}$ is nontrivial. Then for every element $m_0 \in M$ stable under σ, there exists $m \in M$ such that $m_0 = \sigma(m) + m$.*

Proof. Since $\sigma^2 = \mathrm{id}$, we should have necessarily $l = 2d$ and $\sigma|_{\mathbb{F}_{2^l}}(x) = x^{2^d}$, so for $m_0 \in \mathbb{F}_{2^l} \subset M$ the assertion follows. Let σ_0 be the following involution of M:

$$\sigma_0((a_{ij})) = (\sigma|_{\mathbb{F}_{2^l}}(a_{ji})).$$

Then $\sigma \circ \sigma_0$ is an automorphism of M that should be inner, and hence, we get $\sigma(x) = u\sigma_0(x)u^{-1}$ for some $u \in M^* = \mathrm{GL}_n(\mathbb{F}_{2^l})$ such that $\sigma_0(u) = \lambda u$ for $\lambda \in \mathbb{F}_{2^l}^*$. It follows that $\lambda^{2^d} = \lambda^{-1}$; that is, $\lambda = \mu^{2^d-1}$ for some $\mu \in \mathbb{F}_{2^l}^*$. Thus, changing u by $\mu^{-1}u$ we may assume that $\sigma_0(u) = u$. Note that for σ_0 the assertion follows from the case $m_0 \in \mathbb{F}_{2^l}$ considered above. Now if $\sigma(m_0) = u\sigma_0(m_0)u^{-1} = m_0$, then $\sigma_0(m_0u) = m_0u$; therefore, $m_0u = \sigma_0(m) + m$ for some $m \in M$, and hence, $m_0 = \sigma(mu^{-1}) + mu^{-1}$. □

LEMMA 1.5.5. *Let B be a discrete valuation ring. Then any automorphism of the matrix algebra $\mathrm{M}_n(B)$ is inner.*

Proof. Let L be the field of fraction for B. Then any automorphism of $\mathrm{M}_n(L)$ is inner; hence, any automorphism of $\mathrm{M}_n(B)$ has form $\alpha(a) = uau^{-1}$, where $u \in \mathrm{GL}_n(L)$ is such that $u\mathrm{M}_n(B)u^{-1} = \mathrm{M}_n(B)$. Considering the standard left action of $\mathrm{M}_n(L)$ on L^n, we derive the inclusion $a(uB^n) \subset uB^n$ for any $a \in \mathrm{M}_n(B)$. Let $\pi \subset B$ be a uniformizing element. Changing u by a scalar, we may assume that $uB^n \subset B^n$, but $uB^n \not\subset \pi B^n$. Then the image of uB^n in $(B/\pi B)^n$ is invariant under the standard action of $\mathrm{M}_n(B/\pi B)$, which implies that $uB^n = B^n$, that is, $u \in \mathrm{GL}_n(B)$. □

Proof of Theorem 1.5.3. The first step is to show that under the assumptions of the theorem $R^- = \mathrm{tr}^-(R)$, so that $\bar{\delta}(\phi) = 0$. Since $2R^- \subset \mathrm{tr}^-(R)$, it is sufficient to check the inclusion $R^-/2R^- \subset \mathrm{tr}(R)/2R^+$ of subgroups in $R/2R$. Let $(2) = \bigcap_i \mathfrak{q}_i$ be the primary decomposition of 2 in $\mathfrak{o}$, where $\mathfrak{q}_i$ are $\mathfrak{p}_i$-primary ideals and $\mathfrak{p}_i$ are different prime ideals of $\mathfrak{o}$. Then $R/2R$ contains $\mathfrak{o}/2\mathfrak{o} = \prod_i \mathfrak{o}/\mathfrak{q}_i$ as a central subalgebra, and there is a decomposition $R/2R \simeq \prod_i M_i$, where $M_i = R/\mathfrak{q}_i R$. Note that ε permutes $\mathfrak{p}_i$, so that $\varepsilon(\mathfrak{p}_i) = \mathfrak{p}_{\varepsilon(i)}$; hence,

$$(2) = \bigcap_i \varepsilon(\mathfrak{q}_i) = \bigcap_i \mathfrak{q}_{\varepsilon(i)} = \bigcap_i (\varepsilon(\mathfrak{q}_i) \cap \mathfrak{q}_{\varepsilon(i)}).$$

Changing $\mathfrak{q}_i$ by $\mathfrak{q}_i \cap \varepsilon(\mathfrak{q}_{\varepsilon(i)})$, we may assume that $\varepsilon(\mathfrak{q}_i) = \mathfrak{q}_{\varepsilon(i)}$. Then the induced involution of $R/2R$ maps M_i to $M_{\varepsilon(i)}$. Also, if $\varepsilon(i) = i$, then $\mathfrak{q}_i = \mathfrak{p}_i$, and $M_i = R/\mathfrak{p}_i R$ is semisimple. Let $r \in R^-$; then the image of r in $R/2R$ decomposes as follows: $\bar{r} = \sum_i r_i$, where $r_i \in M_i$, $r_{\varepsilon(i)} = \varepsilon(r_i)$. To prove that $\bar{r} \in \mathrm{tr}(R)/2R^+$, it is sufficient to check that $r_i \in \mathrm{tr}(R)/2R^+$ for every i such that $\varepsilon(i) = i$.

Assume first that $\varepsilon|_{\mathfrak{o}}$ is nontrivial. Since $\mathfrak{o}$ is unramified at every ε-stable place above 2, the induced involution of $\mathfrak{o}/\mathfrak{p}_i$ for $\varepsilon(i) = i$ is nontrivial. For such i, the $\mathfrak{o}/\mathfrak{p}_i$-algebra M_i is a product of matrix algebras over field extensions of $\mathfrak{o}/\mathfrak{p}_i$, and we are done by Lemma 1.5.4.

Now let $\varepsilon|_{\mathfrak{o}}$ be trivial. In the case $D = K$, we have $R^- = 0$, so we may assume that D is an indefinite quaternion algebra over K. Then $M_i = R/\mathfrak{p}_i R \simeq \hat{R}_i/\mathfrak{p}_i\hat{R}_i$ for every i, where $\hat{R}_i \simeq \mathrm{M}_2(\hat{\mathfrak{o}}_i)$ is the $\mathfrak{p}_i$-adic completion of R, $\hat{\mathfrak{o}}_i = \hat{\mathfrak{o}}_{\mathfrak{p}_i}$. By Lemma 1.5.5 the induced involution $\varepsilon : \hat{R}_i \to \hat{R}_i$ has form $\varepsilon(x) = ux^tu^{-1}$ for some $u \in \mathrm{GL}_2(\hat{\mathfrak{o}}_i)$, where x^t denotes the tranposed matrix to x and $u^t = \pm u$. We claim that the case $u^t = -u$ is impossible. Indeed, let $x \mapsto x^* = \mathrm{Tr}_{D/K}(x) - x$ be the canonical involution of D, where $\mathrm{Tr}_{D/K} : D \to K$ is the reduced trace. Then for the involution ε on D, we have $\varepsilon(x) = ax^*a^{-1}$ for some $a \in D^*$ such that $a^* = -a$ (see [5]). It follows that for the induced involution of the $\mathfrak{p}_i$-adic completion $\hat{D}_i \simeq \mathrm{M}_2(\hat{K}_i)$, we have $\varepsilon(x) = ax^*a^{-1} = ux^tu^{-1}$. Note that $x^* = sx^ts^{-1}$, where $s = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$; hence, u is proportional to as, and the condition $a^* = -a$ rewritten as $(as)^t = as$ implies that $u^t = u$. Therefore, if $\varepsilon(x) = -x$ for some $x \in \hat{R}_i$, then $x = y - \varepsilon(y)$ for $y \in \hat{R}_i$, which implies the required inclusion $r_i \in \mathrm{tr}(R)/2R^+$.

By Proposition 1.5.2 it remains to show that the extension of $R/2R$-modules (1.5.2) splits. When $\varepsilon|_{\mathfrak{o}}$ is trivial, this is a consequence of the semisimplicity of $R/2R$. Otherwise, the argument above shows that $R^+/\mathrm{tr}(R) = 0$. □

If $\varepsilon = \mathrm{id}$ and $R = \mathfrak{o}$, we can improve the above theorem as follows.

THEOREM 1.5.6. *Let $\mathfrak{o}$ be an order in the number field. Assume that the localization of $\mathfrak{o}$ at every prime ideal above 2 is normal. Let A be an abelian variety over an algebraically closed field k such that* $\mathrm{char}(k) \neq 2$. *Then for any $\mathfrak{o}$-linear polarization $\phi : A \to \hat{A}$ there exists a $\Sigma_{\mathfrak{o},\mathrm{id}}$-structure for ϕ.*

Proof. Since $R^- = 0$ in this case, it is sufficient to show that $\mathrm{Ext}^1_{R/2R}(M, \hat{A}_2) = 0$ for any finite $R/2R$-module M. Since $(2) = \bigcap_i \mathfrak{p}_i^{e_i}$ for different prime ideals $\mathfrak{p}_i \subset \mathfrak{o}$, it is sufficient to prove that $\mathrm{Ext}^1_{R_i}(k_i, \hat{A}_{\mathfrak{p}_i^{e_i}}) = 0$, where

$R_i = R/\mathfrak{p}_i^{e_i}$, $k_i = R/\mathfrak{p}_i$. Now we use the following general fact: If B is a discrete valuation ring with a uniformizing element π and N is a $B/(\pi^n)$-module such that the natural map $N \to N_{\pi^{n-1}} = \{x \in N \mid \pi^{n-1}x = 0\}$ induced by the action of π is surjective, then $\mathrm{Ext}^1_{B/(\pi^n)}(B/(\pi), N) = 0$. Indeed, this follows easily from the resolution $0 \to B/(\pi^{n-1}) \xrightarrow{\pi} B/(\pi^n) \to B/(\pi) \to 0$ for $B/(\pi)$. Thus, it is sufficient to check the surjectivity of the homomorphism $\hat{A}_{\mathfrak{p}_i^l} \to \hat{A}_{\mathfrak{p}_i^{l-1}}$ induced by the action of the local uniformizer $\pi \in \mathfrak{p}_i$. Note that $(\pi) = \mathfrak{p}_i\mathfrak{q}$ for some nonzero ideal $\mathfrak{q}$ prime to $\mathfrak{p}_i$. Hence, we have a decomposition $\hat{A}_{\pi^n} \simeq \hat{A}_{\mathfrak{p}_i^n} \times \hat{A}_{\mathfrak{q}^n}$. Since $[\pi] : \hat{A} \to \hat{A}$ is an isogeny, the homomorphism $\hat{A}_{\pi^l} \xrightarrow{\pi} \hat{A}_{\pi^{l-1}}$ is surjective, which implies the surjectivity of the induced homomorphism $\hat{A}_{\mathfrak{p}_i^l} \to \hat{A}_{\mathfrak{p}_i^{l-1}}$. □

2. Theta functions

2.1. Canonical theta function. Our notation below is close to [1]. The only substantial difference is that we write the canonical theta series in slightly more invariant form.

Let V be a complex vector space with a positive-definite hermitian form H, and let $L \subset V$ be a $\mathbb{Z}$-lattice such that the restriction of $E = \mathrm{Im}\, H$ to L takes integer values. Let $\chi : L \to \mathbb{C}_1^* = \{z \in \mathbb{C} : |z| = 1\}$ be a map such that

$$\chi(l_1 + l_2) = \chi(l_1)\chi(l_2)\exp(\pi i E(l_1, l_2)). \tag{2.1.1}$$

A *canonical theta function* for (H, χ) is a holomorphic function f on V such that

$$f(v + l) = \chi(l)\exp(\pi H(v, l) + \frac{\pi}{2}H(l, l))f(v).$$

We denote the space of such functions by $T(H, L, \chi)$. One can interpret this condition as invariance of f under the action of some group. Namely, let $\mathrm{Heis}(V)$ be the Heisenberg group corresponding to (V, E). Recall that as a set $\mathrm{Heis}(V) = \mathbb{C}_1^* \times V$ and the group law in $\mathrm{Heis}(V)$ is defined by the formula

$$(t, v) \cdot (t', v') = (tt' \exp(\pi i E(v, v')), v + v'),$$

where $t, t' \in \mathbb{C}_1^*$, $v, v' \in V$. In particular, $\mathrm{Heis}(V)$ is a central extension of V by $\mathbb{C}_1^*$. There is a representation of $\mathrm{Heis}(V)$ on the space of holomorphic functions on V given by the formula

$$U_{(t,v)}f(x) = t^{-1}\exp\Big(-\pi H(x, v) - \frac{\pi}{2}H(v, v)\Big)f(x + v),$$

where $U_{(t,v)}$ is an operator corresponding to $(t, v) \in \mathrm{Heis}(V)$. It is easy to see from (2.1.1) that the map $l \mapsto (\chi(l), l)$ defines a homomorphism $\sigma_\chi : L \to \mathrm{Heis}(V)$. Now the definition of a canonical theta function can be rephrased as the condition that f is invariant under the action of $\sigma_\chi(L)$. In particular, the normalizer

$N_\chi \subset \mathrm{Heis}(V)$ of the subgroup $\sigma_\chi(L) \subset \mathrm{Heis}(V)$ acts on the space $T(H,L,\chi)$ of canonical theta functions for (H,χ). It is easy to see that N_χ consists of elements $(t,v) \in \mathrm{Heis}(V)$ with $v \in L^\perp$, where $L^\perp = \{v \in V : E(v,L) \subset \mathbb{Z}\}$. Furthermore, it is known that $T(H,L,\chi)$ is an irreducible representation of the group $G(H,L,\chi) = N_\chi/\sigma_\chi(L)$ of dimension $\sqrt{[L^\perp : L]}$. Recall also that $T(H,L,\chi)$ is identified with the space of global sections of the line bundle $\mathscr{L}(H,\chi)$ on the complex abelian variety V/L (see, e.g., [5]), and the action of $G(H,L,\chi)$ on it can be defined in purely algebraic terms.

An example of a map χ satisfying (2.1.1) is obtained when we have a decomposition $L = L_1 \oplus L_2$, where L_i are isotropic with respect to E. (Further, we refer to such decomposition as *isotropic decomposition* of L.) Namely, there is a canonical map $\chi_0 = \chi_0(L_1,L_2) : L \to \{\pm 1\}$ satisfying (2.1.1), which is given by the formula

$$\chi_0(l) = \exp(\pi i E(l_1,l_2)), \tag{2.1.2}$$

where $l = l_1 + l_2$, $l_i \in L_i$. Any two maps χ and χ' satisfying (2.1.1) are related by the formula

$$\chi'(l) = \chi(l)\exp(2\pi i E(c,l)) \tag{2.1.3}$$

for some $c \in V$, which is uniquely determined modulo $L^\perp$. It is easy to see that the corresponding homomorphisms $\sigma_{\chi'}$ and σ_χ are related as follows:

$$\sigma_{\chi'}(l) = (1,c)\sigma_\chi(l)(1,c)^{-1}. \tag{2.1.4}$$

Therefore, we can define an isomorphism of the corresponding finite Heisenberg groups

$$\alpha_c : G(H,L,\chi) \to G(H,L,\chi') : g \mapsto (1,c)g(1,c)^{-1}. \tag{2.1.5}$$

Now the operator $U_{(1,c)}$ restricts to an isomorphism between $T(H,L,\chi)$ and $T(H,L,\chi')$ compatible with the actions of $G(H,L,\chi)$ and $G(H,L,\chi')$ via α_c.

Now assume that we have data (H,L,χ) as above and assume that $U \subset V$ is a maximal E-isotropic $\mathbb{R}$-subspace such that U is generated by $U \cap L$ over $\mathbb{R}$, and $\chi|_{U\cap L} \equiv 1$. It is easy to see that U generates V as a $\mathbb{C}$-space and since $H|_{U\times U}$ is a symmetric form, it extends to a $\mathbb{C}$-bilinear symmetric form $S : V \times V \to \mathbb{C}$. Now we set

$$\theta^\chi_{H,L,U}(x) = \exp\left(\frac{\pi}{2}S(x,x)\right) \sum_{l\in L/U\cap L} \chi(l)\exp\left(\pi(H-S)(x,l) - \frac{\pi}{2}(H-S)(l,l)\right). \tag{2.1.6}$$

One can easily check that $\theta^{\chi}_{H,L,U} \in T(H,L,\chi)$. Furthermore, notice that $\tilde{L} = L + U \cap L^{\perp}$ is also a lattice in V such that the restriction of E to $\tilde{L}$ is integer-valued. The map χ has a unique extension to a map $\tilde{\chi} : \tilde{L} \to \mathbb{C}_1^*$ satisfying (2.1.1), such that $\tilde{\chi}|_{U \cap L^{\perp}} \equiv 1$. Then one has

$$\theta^{\chi}_{H,L,U} = \theta^{\tilde{\chi}}_{H,\tilde{L},U}.$$

In particular, $\theta^{\chi}_{H,L,U}$ is an element of $T(H,\tilde{L},\tilde{\chi}) \subset T(H,L,\chi)$. In other words, $\theta^{\chi}_{H,L,U} \in T(H,L,\chi)$, and $\theta^{\chi}_{H,L,U}$ is invariant under the action of $(1, U \cap L^{\perp}) \subset G(H,L,\chi)$.

LEMMA 2.1.1. *For any $c \in U$ one has*

$$\theta^{\chi'}_{H,L,U} = U_{(1,c)} \theta^{\chi}_{H,L,U},$$

where χ' and χ are related by (2.1.3).

The proof is straightforward and is left to the reader.

The following simple statement is sometimes referred to as the "Isogeny theorem."

LEMMA 2.1.2. *Let H, L, χ, U be as above and let $L' \subset L$ be a sublattice. Then*

$$\theta^{\chi}_{H,L,U} = \sum_{l \in L/(L' + U \cap L)} \chi(l)^{-1} U_{(1,l)} \theta^{\chi}_{H,L',U}.$$

We also need the following lemma (in which V can be replaced by any real symplectic vector space).

LEMMA 2.1.3. *If $L \subset V$ and U are as above, then the lattice $\tilde{L} = L + U \cap L^{\perp}$ is self-dual.*

Proof. It is sufficient to prove that if L and U are as above and $U \cap L^{\perp} = U \cap L$, then L is self-dual. (To prove the statement of the lemma, apply this to $\tilde{L}$.) We use the induction in the dimension of V. Choose a nonzero element $x \in U \cap L$. Then there exists $N \in \mathbb{Z}$ such that $E(x, L) = N\mathbb{Z} \subset \mathbb{Z}$. In particular, $x/N \in U \cap L^{\perp} = U \cap L$. Replacing x by x/N we can assume that $N = 1$, so that there exists an element $y \in L$ such that $E(x,y) = 1$. Consider the E-orthogonal decomposition $V = (\mathbb{R}x \oplus \mathbb{R}y) \oplus V_0$. Then $L = (\mathbb{Z}x \oplus \mathbb{Z}y) \oplus V_0 \cap L$, $L^{\perp} = (\mathbb{Z}x \oplus \mathbb{Z}y) \oplus V_0 \cap L^{\perp}$ and $U = \mathbb{R}x \oplus V_0 \cap U$. Hence, we can apply the induction assumption to $V_0 \cap L$ and $V_0 \cap U$. □

Remarks. (1) When one has an isotropic decomposition $L = L_1 \oplus L_2$ such that $U \cap L = L_2$ and $\chi = \chi_0(L_1, L_2)$, the function $\theta^{\chi}_{H,L,U}$ we defined coincides with the function ϑ^0 defined in [1, Ch. 3, 2.3].

(2) If $L = L^{\perp}$, then for given H and χ, an isotropic subspace U as above exists if and only if the line bundle $\mathscr{L}(H,\chi)$ on V/L is even (see [6]).

2.2. Classical theta functions and the functional equation. Let Z be an element of the Siegel upper half-plane $\mathfrak{H}_g$; that is, let Z be a $g \times g$ matrix, such that $Z^t = Z$ and $\operatorname{Im} Z > 0$. Then it defines an abelian variety with principal polarization in the standard way. First, $L(Z) = Z\mathbb{Z}^g \oplus \mathbb{Z}^g$ is a lattice in $\mathbb{C}^g$, and the hermitian form H_Z on $\mathbb{C}^g$ is defined by the matrix $(\operatorname{Im} Z)^{-1}$ in the standard basis. Then one has an isotropic decomposition $L(Z) = L(Z)_1 \oplus L(Z)_2$, where $L(Z)_1 = Z\mathbb{Z}^g$, $L(Z)_2 = \mathbb{Z}^g$; hence the corresponding map $\chi_0 : L(Z) \to \{\pm 1\}$, satisfying (2.1.1). One also has the corresponding decomposition $\mathbb{C}^g = Z\mathbb{R}^g \oplus \mathbb{R}^g$ into summands that are lagrangian with respect to the real symplectic form $E_Z = \operatorname{Im} H_Z$. For $v \in \mathbb{C}^g$ we use the notation $v = Zv_1 + v_2$, where $v_1, v_2 \in \mathbb{R}^g$. Now one can compute that for any $c \in \mathbb{C}^g$, one has

$$U_{(1,c)}\theta^{\chi_0}_{H_Z, L(Z), \mathbb{R}^g} = \exp\Big(\frac{\pi}{2} S(\cdot\,,\cdot) - \pi i (c_1)^t \cdot c_2\Big)\theta\begin{bmatrix} c_1 \\ c_2 \end{bmatrix}(\cdot\,, Z),$$

where $S(v,w) = v^t(\operatorname{Im} Z)^{-1}w$, $\theta\left[\begin{smallmatrix} c_1 \\ c_2 \end{smallmatrix}\right](\cdot\,,Z)$ is the classical theta function with characteristics

$$\theta\begin{bmatrix} c_1 \\ c_2 \end{bmatrix}(v, Z) = \sum_{l \in \mathbb{Z}^g} \exp(\pi i (l + c_1)^t Z (l + c_1) + 2\pi i (v + c_2)(l + c_1))$$

for $v \in \mathbb{C}^g$.

We are going to use this comparison and rewrite the classical functional equation in terms of canonical theta functions. Namely, assume that we have a complex vector space V, a lattice $L \subset V$, and a positive hermitian form H on V such that the restriction of $E = \operatorname{Im} H$ to L takes integer values and $L^{\perp} = L$. Then to every pair (χ, U), where $\chi : L \to \mathbb{C}^*_1$ is a map satisfying (2.1.1) and $U \subset V$ is an E-lagrangian subspace generated by $U \cap L$ such that $\chi|_U \equiv 1$, we associated the canonical theta function $\theta^{\chi}_{H,L,U}$ for (H, χ). Now if we consider another such pair (χ', U'), then we get the canonical theta function $\theta^{\chi'}_{H,L,U'}$ for (H, χ'). We can choose $c \in V$ (uniquely up to adding an element of L) such that

$$\chi'(l) = \chi(l)\exp(2\pi i E(c, l)) \tag{2.2.1}$$

for $l \in L$. Then $U_{(1,c)}$ gives an isomorphism of $T(H, L, \chi)$ with $T(H, L, \chi')$. Since $T(H, L, \chi')$ in this case is 1-dimensional, we should have an identity

$$\theta^{\chi'}_{H,L,U'}(v) = q \cdot U_{(1,c)}\theta^{\chi}_{H,L,U}(v), \tag{2.2.2}$$

where $q \in \mathbb{C}^*$ is a constant depending on H, χ, c, U, and U'.

For every pair M_1, M_2 of free $\mathbb{Z}$-modules of rank $g = \dim V$ in V such that M_i generates V over $\mathbb{C}$, we define $\det_{M_1}(M_2) \in \mathbb{C}^*/\{\pm 1\}$ as follows: choose arbitrary bases of M_i and write the transition matrix from the basis in M_1 to that in M_2, then take its determinant. Up to sign, this number does not depend on a choice of bases in M_i.

THEOREM 2.2.1. *Let (χ, U) and (χ', U') be as above. Assume also that $\chi^2 \equiv \chi'^2 \equiv 1$. Then for any $c \in (1/2)L$, such that (2.2.1) holds, one has*

$$\theta^{\chi'}_{H,L,U'}(v) = \zeta \cdot \det_{U\cap L}(U' \cap L)^{1/2} U_{(1,c)} \theta^{\chi}_{H,L,U}(v), \tag{2.2.3}$$

where $\zeta^8 = 1$.

Proof. First let us assume that $\chi = \chi_0(L_1, L_2)$, $U = \mathbb{R}L_2$ for some isotropic decomposition $L = L_1 \oplus L_2$, and similarly the pair (χ', U') arises from some isotropic decomposition $L = L'_1 \oplus L'_2$. Then we can find an automorphism $T : L \to L$, which preserves $E|_{L\times L}$, such that $L'_i = T(L_i)$, $i = 1, 2$. Choosing bases in L_1 and L_2 in such a way that the matrix of $E|_{L\times L}$ with respect to them is standard, and identifying V with $\mathbb{C}^g$ using the base in L_2, we may assume that $V = \mathbb{C}^g$, $H = H_Z$, $L_1 = Z\mathbb{Z}^g$, and $L_2 = \mathbb{Z}^g$ for some $Z \in \mathfrak{H}_g$. Let $(e_1, \dots, e_g)$ be the standard basis in $\mathbb{Z}^g$; then $(Ze_1, \dots, Ze_g, e_1, \dots, e_g)$ is the basis of L in which E has the standard form. With respect to this base, T is given by a symplectic matrix $[T] \in \mathrm{Sp}_{2g}(\mathbb{Z})$. Let $[T] = \left(\begin{smallmatrix} A & C \\ B & D \end{smallmatrix}\right)$ be the block form of $[T]$, where $A, B, C, D \in \mathrm{M}(g, \mathbb{Z})$. Then $L'_1 = (ZA + B)(\mathbb{Z}^g) \subset \mathbb{C}^g$ and $L'_2 = (ZC + D)(\mathbb{Z}^g) \subset \mathbb{C}^g$. Thus, $(ZC + D)^{-1}(L'_2) = \mathbb{Z}^g$ and $(ZC + D)^{-1}(L'_1) = Z'\mathbb{Z}^g$, where $Z' = (ZC + D)^{-1}(ZA + B) \in \mathfrak{H}_g$. It follows that

$$\theta^{\chi_0(L'_1, L'_2)}_{H_Z, L'_1, L'_2}((ZC + D)v) = \theta^{\chi_0(L(Z')_1, L(Z')_2)}_{H_{Z'}, L(Z')_1, L(Z')_2}(v),$$

so that (2.2.2) with $v = 0$ assumes the form

$$\theta\begin{bmatrix} 0 \\ 0 \end{bmatrix}(0, Z') = q \cdot \exp(-\pi i (c_1)^t \cdot c_2) \cdot \theta\begin{bmatrix} c_1 \\ c_2 \end{bmatrix}(0, Z). \tag{2.2.4}$$

Comparing this with the classical functional equation and using the fact that $c \in (1/2)L$, we conclude that

$$q = \zeta \cdot \det(ZC + D)^{1/2},$$

where $\zeta^8 = 1$. Now by definition $\det(ZC + D)$ represents $\det_{L_2}(L'_2) \in \mathbb{C}^*/\{\pm 1\}$. Hence, we can rewrite (2.2.2) in the form

$$\theta^{\chi_0(L'_1, L'_2)}_{L'_1, L'_2}(v) = \zeta \cdot \det_{L_2}(L'_2)^{1/2} \cdot U_{(1,c)} \theta^{\chi_0(L_1, L_2)}_{L_1, L_2}(v), \tag{2.2.5}$$

where $\det_{L_2}(L'_2)^{1/2}$ is defined up to multiplying by the 4th root of unity and ζ is an 8th root of unity defined with the same ambiguity.

The general case can be deduced as follows. We can always choose isotropic decompositions $L = L_1 \oplus L_2$ and $L = L'_1 \oplus L'_2$ such that $U = \mathbb{R}L_2$ and $U' = \mathbb{R}L'_2$. Then we can find $c_1 \in U \cap (1/2)L$ and $c_2 \in U' \cap (1/2)L$ such that

$$\chi = \chi_0(L_1, L_2)\exp(2\pi i E(c_1, \cdot)),$$

$$\chi' = \chi_0(L'_1, L'_2)\exp(2\pi i E(c_2, \cdot)).$$

Then by Lemma 2.1.1 we have

$$\theta^{\chi}_{H,L,U} = U_{(1,c_1)}\theta^{\chi_0(L_1,L_2)}_{H,L,U},$$

$$\theta^{\chi'}_{H,L,U'} = U_{(1,c_2)}\theta^{\chi_0(L'_1,L'_2)}_{H,L,U'},$$

and the equation is easily deduced from the case considered above. □

2.3. Theta identity. Let V, L, H, χ be as in Section 2.1. Assume that V/L has a complex multiplication by a ring R and that $\varepsilon : R \to R$ is an involution such that

$$H(\varepsilon(r)v, v') = H(v, rv').$$

Let $B = (b_{ij}) \in \mathrm{M}(k, R)$ be a matrix such that $B^{\varepsilon} \cdot B = n \cdot \mathrm{Id}$ for some $n \in \mathbb{Z}_{>0}$. Here $B^{\varepsilon} = \varepsilon(B)^t$, where $\varepsilon(B)$ is obtained by applying ε to all elements of B. In other words, if we consider the morphism of free, right R-modules $B : R^k \to R^k$ and the standard hermitian form $h^k_1(X, Y) = X^{\varepsilon} \cdot Y$ on R^k (here we represent elements of R^k as columns), then one has

$$B^{-1}h^k_1 = nh^k_1. \tag{2.3.1}$$

Then if we consider B as a complex operator on $V^{\oplus k}$, one can easily check that

$$B^{-1}H^{\oplus k} = nH^{\oplus k}. \tag{2.3.2}$$

This implies that we have a map

$$B^* : T(H^{\oplus k}, L^{\oplus k}, \chi^{\oplus k}) \to T(nH^{\oplus k}, L^{\oplus k}, B^{-1}(\chi^{\oplus k})) : f \mapsto f(B(\cdot)),$$

where $\chi^{\oplus k}(l_1, \ldots, l_k) = \prod_i \chi(l_i)$. Furthermore, this map is compatible with the actions of the corresponding Heisenberg groups on these spaces via the homomorphism

$$G(nH^{\oplus k}, L^{\oplus k}, (\chi^n)^{\oplus k}) \to G(H^{\oplus k}, L^{\oplus k}, \chi^{\oplus k}) : (t, v) \mapsto (t, B(v)),$$

where $v \in (n^{-1}L^{\perp})^{\oplus k}$.

Now assume that $\chi^2 \equiv 1$ and that we have an E-lagrangian subspace $U \subset V$ generated by $U \cap L$ such that $\chi|_{U \cap L} = 1$. Let $\tilde{L} = L + U \cap L^{\perp}$ and let $\tilde{\chi} : \tilde{L} \to \{\pm 1\}$ be the unique extension of χ to $\tilde{L}$ satisfying (2.1.1) such that $\tilde{\chi}|_{U \cap L^{\perp}} \equiv 1$. Then, according to Lemma 2.1.3, the lattice $\tilde{L}$ is self-dual with respect to E.

LEMMA 2.3.1. *There exists an element $c \in ((1/2n)L^{\perp})^{\oplus k}$ such that*

$$\chi^{\oplus k}(Bl) = (\chi^n)^{\oplus k}(l) \exp(2\pi i n E^{\oplus k}(c, l))$$

for any $l \in L^{\oplus k}$, and

$$\tilde{\chi}^{\oplus k}(Bv) = \exp(2\pi i n E^{\oplus k}(c, v))$$

for any $v \in U^{\oplus k} \cap B^{-1}(\tilde{L}^{\oplus k})$.

Proof. First choose $c' \in (1/2)B^{-1}(\tilde{L}^{\oplus k})$ such that

$$B^{-1}(\tilde{\chi}^{\oplus k})|_{U^{\oplus k} \cap B^{-1}(\tilde{L}^{\oplus k})} = \exp(2\pi i n E^{\oplus k}(c', \cdot)).$$

Now we define a map $\chi' : B^{-1}(\tilde{L}^{\oplus k}) \to \{\pm 1\}$ by the formula

$$B^{-1}(\tilde{\chi}^{\oplus k}) = \chi' \exp(2\pi i n E^{\oplus k}(c', \cdot)).$$

Then $\chi'|_{U^{\oplus k} \cap L^{\oplus k}} \equiv 1$, so we can choose an element $c'' \in U^{\oplus k} \cap ((1/2n)L^{\perp})^{\oplus k}$ such that

$$\chi'|_{L^{\oplus k}} = (\chi^n)^{\oplus k} \exp(2\pi i n E^{\oplus k}(c'', \cdot)).$$

It remains to set $c = c' + c''$. □

THEOREM 2.3.2. *With the above notation, one has*

$$B^* \theta^{\chi^{\oplus k}}_{H^{\oplus k}, L^{\oplus k}, U^{\oplus k}} = \zeta \cdot \det B^{-1/2} n^{gk/2} d^{-1/2} \cdot \sum_v \chi(Bv) U_{(1,v)} U_{(1,c)} \theta^{(\chi^n)^{\oplus k}}_{nH^{\oplus k}, L^{\oplus k}, U^{\oplus k}}, \tag{2.3.3}$$

where $\det B$ is the determinant of B considered as a complex operator on V^k, the summation is taken over the finite group $v \in B^{-1}(\tilde{L}^{\oplus k})/(L^{\oplus k} + U^{\oplus k} \cap B^{-1}(\tilde{L}^{\oplus k}))$, d is the number of elements in this group, the Heisenberg action on the right-hand side is associated with the hermitian form $nH^{\oplus k}$, and an element c is chosen as in Lemma 2.3.1.

Proof. Notice that $B^{-1}(\tilde{L}^{\oplus k})$ is a self-dual lattice with respect to $B^{-1}E^{\oplus k} = nE^{\oplus k}$, and one has

$$B^* \theta^{\chi^{\oplus k}}_{H^{\oplus k}, L^{\oplus k}, U^{\oplus k}} = \theta^{B^{-1}(\tilde{\chi}^{\oplus k})}_{nH^{\oplus k}, B^{-1}(\tilde{L}^{\oplus k}), B^{-1}(U^{\oplus k})}.$$

Now we want to apply the functional equation (2.2.3) to the self-dual lattice $B^{-1}(\tilde{L}^{\oplus k})$ and a pair of lagrangian subspaces $B^{-1}(U^{\oplus k})$ and $U^{\oplus k}$ in $V^{\oplus k}$. Let us define a map $\chi' : B^{-1}(\tilde{L}^{\oplus k}) \to \{\pm 1\}$ by the formula

$$B^{-1}(\tilde{\chi}^{\oplus k}) = \chi' \exp(2\pi i n E^{\oplus k}(c, \cdot)),$$

where c is chosen as in Lemma 2.3.1. Then $\chi'(v_1 + v_2) = \chi'(v_1)\chi'(v_2) \cdot \exp(2\pi i n E^{\oplus k}(v_1, v_2))$ and $\chi'|_{U^{\oplus k} \cap B^{-1}(\tilde{L}^{\oplus k})} \equiv 1$. Applying (2.2.3) we get

$$\theta^{B^{-1}(\tilde{\chi}^{\oplus k})}_{nH^{\oplus k}, B^{-1}(\tilde{L}^{\oplus k}), B^{-1}(U^{\oplus k})}$$
$$= \zeta \cdot \det_{U^{\oplus k} \cap B^{-1}(\tilde{L}^{\oplus k})}(B^{-1}(U^{\oplus k}) \cap B^{-1}(\tilde{L}^{\oplus k}))^{1/2} U_{(1,c)} \theta^{\chi'}_{nH^{\oplus k}, B^{-1}(\tilde{L}^{\oplus k}), U^{\oplus k}}. \quad (2.3.4)$$

Now we apply Lemma 2.1.2 to the embedding of lattices $L^{\oplus k} \subset B^{-1}(\tilde{L}^{\oplus k})$ and use the fact that $\chi'|_{L^{\oplus k}} = (\chi^n)^{\oplus k}$:

$$\theta^{\chi'}_{nH^{\oplus k}, B^{-1}(\tilde{L}^{\oplus k}), U^{\oplus k}} = \sum_{v \in B^{-1}(\tilde{L}^{\oplus k})/(L^{\oplus k} + U^{\oplus k} \cap B^{-1}(\tilde{L}^{\oplus k}))} \chi'(v) U_{(1,v)} \theta^{(\chi^n)^{\oplus k}}_{nH^{\oplus k}, L^{\oplus k}, U^{\oplus k}}. \quad (2.3.5)$$

Combining (2.3.4) and (2.3.5), we obtain

$$B^* \theta^{\chi^{\oplus k}}_{H^{\oplus k}, L^{\oplus k}, U^{\oplus k}}$$
$$= \zeta \cdot \det_{U^{\oplus k} \cap B^{-1}(\tilde{L}^{\oplus k})}(B^{-1}(U^{\oplus k}) \cap B^{-1}(\tilde{L}^{\oplus k}))^{1/2} \sum_v \chi'(v) U_{(1,c)} U_{(1,v)} \theta^{(\chi^n)^{\oplus k}}_{nH^{\oplus k}, L^{\oplus k}, U^{\oplus k}},$$

where the summation is taken over $v \in B^{-1}(\tilde{L}^{\oplus k})/(L^{\oplus k} + U^{\oplus k} \cap B^{-1}(\tilde{L}^{\oplus k}))$. It remains to use the relation

$$\chi'(v) U_{(1,c)} U_{(1,v)} = \chi'(v) \exp(2\pi i n E^{\oplus k}(c, v)) U_{(1,v)} U_{(1,c)} = \chi^{\oplus k}(v) U_{(1,v)} U_{(1,c)}$$

and the lemma below. □

LEMMA 2.3.3. *In the situation above*

$$\det_{U^{\oplus k} \cap B^{-1}(\tilde{L}^{\oplus k})}(B^{-1}(U^{\oplus k}) \cap B^{-1}(\tilde{L}^{\oplus k})) = \det B^{-1} \cdot \frac{n^{gk}}{d},$$

where $d = [B^{-1}(\widetilde{L^{\oplus k}}) : (L^{\oplus k} + U^{\oplus k} \cap B^{-1}(\widetilde{L^{\oplus k}})]$.

Proof. We can write

$$\det_{U^{\oplus k}\cap B^{-1}(\tilde{L}^{\oplus k})}(B^{-1}(U^{\oplus k})\cap B^{-1}(\tilde{L}^{\oplus k}))=\det_{U^{\oplus k}\cap B^{-1}(\tilde{L}^{\oplus k})}(U^{\oplus k}\cap L^{\oplus k})$$

$$\times\det_{U^{\oplus k}\cap L^{\oplus k}}(B^{-1}(U^{\oplus k}\cap L^{\oplus k}))\cdot\det_{B^{-1}(U^{\oplus k}\cap\mathscr{L}^{\oplus k})}(B^{-1}(U^{\oplus k}\cap\tilde{L}^{\oplus k}))$$

$$=[U^{\oplus k}\cap B^{-1}(\tilde{L}^{\oplus k}):U^{\oplus k}\cap L^{\oplus k}]\cdot\det B^{-1}\cdot[U^{\oplus k}\cap\tilde{L}^{\oplus k}:U^{\oplus k}\cap L^{\oplus k}]^{-1}.$$

Now we use the formula

$$[B^{-1}(\tilde{L}^{\oplus k}):L^{\oplus k}]=[B^{-1}(\tilde{L}^{\oplus k}):(L^{\oplus k}+U^{\oplus k}\cap B^{-1}(\tilde{L}^{\oplus k}))]$$

$$\times[U^{\oplus k}\cap B^{-1}(\tilde{L}^{\oplus k}):U^{\oplus k}\cap L^{\oplus k}]$$

$$=d\cdot[U^{\oplus k}\cap B^{-1}(\tilde{L}^{\oplus k}):U^{\oplus k}\cap L^{\oplus k}].$$

Since the lattice $B^{-1}(\tilde{L}^{\oplus k})$ is self-dual with respect to $nE^{\oplus k}$, it follows that

$$[B^{-1}(\tilde{L}^{\oplus k}):L^{\oplus k}]=\left[\frac{1}{n}L^{\perp}:L\right]^{k/2}=n^{gk}\cdot[L^{\perp}:L]^{k/2}.$$

Together with the previous formula, this leads to

$$[U^{\oplus k}\cap B^{-1}(\tilde{L}^{\oplus k}):U^{\oplus k}\cap L^{\oplus k}]=d^{-1}\cdot n^{gk}\cdot[L^{\perp}:L]^{k/2}.$$

It remains to use the fact that

$$[U^{\oplus k}\cap\tilde{L}^{\oplus k}:U^{\oplus k}\cap L^{\oplus k}]=[U\cap L^{\perp}:U\cap L]^{k}=[L^{\perp}:L]^{k/2}.\qquad\square$$

Corollary 2.3.4. *Assume that $U^{\oplus k}\cap B^{-1}(\tilde{L}^{\oplus k})\subset L^{\oplus k}$ and that the line bundle $\mathscr{L}(H,\chi)$ on V/L is of the form $L(1)$ for some $\Sigma_{R,\varepsilon}$-structure $r\mapsto L(r)$. Then one has*

$$B^{*}\theta^{\chi^{\oplus k}}_{H^{\oplus k},L^{\oplus k},U^{\oplus k}}=\zeta\cdot\det B^{-1/2}[L^{\perp}:L]^{-k/4}\cdot\sum_{v\in B^{-1}(\tilde{L}^{\oplus k})/L^{\oplus k}}\chi(Bv)U_{(1,v)}\theta^{(\chi^{n})^{\oplus k}}_{nH^{\oplus k},L^{\oplus k},U^{\oplus k}}\cdot\tag{2.3.6}$$

Remarks. (1) Following Shimura, let us define

$$f_{*}(x)=\exp\Big(-\frac{\pi}{2}H(x,x)\Big)f(x)$$

for every function f on V. In the case when V/L has many complex multiplications, Shimura [8] defined a subset $T_a(H,L,\chi) \subset T(H,L,\chi)$ consisting of functions f for which $f_*(\mathbb{Q}L) \subset K'_{\mathrm{ab}}$, where K'_{ab} is the maximal abelian extension of K', the *reflex* of the CM-field K associated with V/L (see [9]). It is shown in [8] that, in fact, $T_a(H,L,\chi)$ generates $T(H,L,\chi)$; more precisely, the standard basis of $T(H,L,\chi)$ multiplied by a suitable constant is a basis of $T_a(H,L,\chi)$ over K'_{ab} (see [8, Prop. 2.4]). Now it follows from definition that the map B^* for a matrix B as above sends $T_a(H^{\oplus k},L^{\oplus k},\chi^{\oplus k})$ to $T_a(nH^{\oplus k},L^{\oplus k},B^{-1}\chi^{\oplus k})$. Our theorem gives an explicit formula for this operator in terms of standard bases of these K'_{ab}-linear spaces (note that $\det B \in K'$).

(2) If the line bundle $t_c^*\mathscr{L}(H,\chi)$ extends to a $\Sigma_{R,\varepsilon}$-structure for some $c \in (1/2)L^{\perp}$, then the same simplification of theta characteristics as in the above corollary can be achieved—one just has to replace θ by $U_{(1,c)}\theta$ in formula (2.3.6).

Let us rewrite the formula (2.3.6) of Corollary 2.3.4 in the classical notation. Namely, assume that $V = \mathbb{C}^g$ and $L = Z\mathbb{Z}^g + \mathbb{Z}^g$, where $Z \in \mathfrak{H}_g$, $H = H_Z$ is given by $\operatorname{Im} Z^{-1}$ (so that $L^{\perp} = L$), $U = \mathbb{R}^g \subset \mathbb{C}^g$, and $\chi = \chi_0(Z\mathbb{Z}^g, \mathbb{Z}^g)$. Then the corollary can be restated as follows: if $\mathbb{C}^g/Z\mathbb{Z}^g + \mathbb{Z}^g$ has a complex multiplication by R and $L(1) = \mathscr{L}(H_Z, \chi_0(Z\mathbb{Z}^g, \mathbb{Z}^g))$ extends to a $\Sigma_{R,\varepsilon}$-structure, then for every matrix $B = (b_{ij}) \in \mathrm{M}_k(R)$ such that $B^{\varepsilon} \cdot B = n \cdot \mathrm{Id}$, $n \in \mathbb{Z}_{>0}$, and $(\mathbb{R}^g)^{\oplus k} \cap B^{-1}(L^{\oplus k}) = (\mathbb{Z}^g)^{\oplus k}$, one has

$$\exp\left(\frac{\pi}{2}\sum_{i=1}^{k}(Bx)_i^t \cdot (\operatorname{Im} Z)^{-1} \cdot (Bx)_i - \frac{\pi}{2} n \sum_{i=1}^{k} x_i^t \cdot (\operatorname{Im} Z)^{-1} \cdot x_i\right) \cdot \prod_{i=1}^{k} \theta\left(\sum_{j=1}^{k} b_{ij}x_j, Z\right)$$

$$= \zeta \cdot \det B^{-1/2} \cdot \sum_{v \in B^{-1}(L^{\oplus k})/L^{\oplus k}} \exp\left(\pi i \sum_{i=1}^{k} (Bv)_{i,1}^t \cdot (Bv)_{i,2} - \pi i n \sum_{i=1}^{k} v_{i,1}^t \cdot v_{i,2}\right)$$

$$\cdot \prod_{i=1}^{k} \theta\begin{bmatrix} v_{i,1} \\ v_{i,2} \end{bmatrix}(nx_i, nZ),$$

where $x \in (\mathbb{C}^g)^{\oplus k}$, for every $y \in (\mathbb{C}^g)^{\oplus k}$ we denote by $y_i \in \mathbb{C}^g$, $1 \leqslant i \leqslant k$, the components of y, $y_{i,1}$, $y_{i,2} \in \mathbb{R}^g$ are the corresponding real components: $y_i = Zy_{i,1} + y_{i,2}$.

Here are examples of matrices B in the case $g = 1$ for which the condition $(\mathbb{R})^{\oplus k} \cap B^{-1}(L^{\oplus k}) = (\mathbb{Z})^{\oplus k}$ is satisfied. If $k = 1$, then it simply means that $B = (b)$, where $b \in L$ is a primitive element of the lattice. If $k = 2$, we can take

$$B = \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix},$$

such that $L = a\mathbb{Z} + b\mathbb{Z}$, to satisfy this condition.

REFERENCES

[1] C. BIRKENHAKE AND H. LANGE, *Complex Abelian Varieties*, Grundlehren Math. Wiss. **302**, Springer-Verlag, Berlin, 1992.

[2] L. BREEN, *Fonctions thêta et théorème du cube*, Lecture Notes in Math. **980**, Springer-Verlag, Berlin, 1983.

[3] P. DELIGNE, "La formule de dualite globale" in *Théorie des topos et cohomolgie étale des schémas, Séminaire de Géometrie Algebrique du Bois-Marie (SGA 4)*, Lecture Notes in Math. **305**, Springer-Verlag, Berlin, 1973, exp. XVIII.

[4] A. GROTHENDIECK, M. RAYNAUD, P DELIGNE, AND D. RIM, *Groupes de monodromie en géométrie algébrique, I, Séminaire de Géometrie Algebrique du Bois-Marie (SGA 7I)*, Lecture Notes in Math. **288**, Springer-Verlag, Berlin, 1972.

[5] D. MUMFORD, *Abelian Varieties*, 2d ed., Tata Inst. Fund. Res. Lectures on Math. and Phys. **5**, Oxford Univ. Press, Oxford, 1974.

[6] D. MUMFORD, M. NORI, AND P. NORMAN, *Tata Lectures on Theta, III*, Progr. Math. **97**, Birkhäuser, Boston, 1991.

[7] A. POLISHCHUK, *Biextensions: Weil representation on derived categories and theta-functions*, Ph.D. thesis, Harvard Univ., 1996.

[8] G. SHIMURA, *Introduction to the Arithmetic Theory of Automorphic Functions*, Kanô Memorial Lectures **1**, Publ. Math. Soc. Japan **11**, Princeton Univ. Press, Princeton, 1971.

[9] ———, *Theta functions with complex multiplication*, Duke Math. J. **43** (1976), 673–696.

DEPARTMENT OF MATHEMATICS, HARVARD UNIVERSITY, 1 OXFORD STREET, CAMBRIDGE, MASSACHUSETTS 02138, USA; apolish@math.harvard.edu