COMPOSITIO MATHEMATICA

F. OORT
M. VAN DER PUT

A construction of an abelian variety with a given endomorphism algebra

Compositio Mathematica, tome 67, n° 1 (1988), p. 103-120
<http://www.numdam.org/item?id=CM_1988__67_1_103_0>

Compositio Mathematica 67: 103–120 (1988)

A construction of an abelian variety with a given endomorphism algebra

F. OORT[1] & M. van der PUT[2]
[1]*Mathematisch Instituut, Rijksuniversiteit Utrecht, Budapestlaan 6, 3508 TA Utrecht, The Netherlands*
[2]*Mathematisch Instituut, Rijksuniversiteit Groningen, Postbus 800, 9700 AV Groningen, The Netherlands*

Received 13 March, 1987; accepted in revised form 21 January 1988

1. Introduction

Suppose given an algebra D. Does there exist an abelian variety Y over some field K such that

$$D \;=\; \mathrm{End}_K(Y) \otimes_{\mathbf{Z}} \mathbf{Q}?$$

This question can be made more precise by fixing the characteristic of K and the dimension of Y.

Just to mention one example (cf. 1.5.1): let D be a quaternion algebra over $\mathbf{Q}$, and let Y be an abelian variety over a field K with

$$D \subset \mathrm{End}_K(Y) \otimes_{\mathbf{Z}} \mathbf{Q}.$$

If $\mathrm{char}(K) = 0$ this implies that $\dim(Y)$ is *even*. However this situation can appear in case $\mathrm{char}(K) = p > 0$, and $\dim(Y)$ is odd.

In order to study such type of questions we look for methods of constructing abelian varieties. It is clear that reduction modulo p of examples constructed in characteristic zero does not always lead to satisfactory answers. A method introduced by Gerritzen, cf. [G], also is not sufficient. However a generalization of this method using the Mumford–Faltings construction of degenerating abelian varieties will provide a satisfactory answer, as will be shown in this paper.

In the construction in [G] we find an abelian variety over a field K, where K is the field of fractions of a complete valuation ring R such that the reduction of the abelian variety is stable and totally degenerated: the connected component of the special fibre of the Néron minimal model over R is a (split) torus over the residue class field k of R. A construction of such degenerations was given by Mumford, cf. [M2]. This was extended by Faltings to the case of a construction of an abelian variety with a given stable reduction. This applied to the idea underlying Gerritzen's construction provides us with the methods we are looking for.

1. The results, some notations and survey of the proof

For an abelian variety Z over a field K, we denote by Z^t the dual abelian variety. Its endomorphism algebra is denoted by

$$\mathrm{End}^0(Z) = \mathrm{End}^0_K(Z) = \mathrm{End}_K(Z) \otimes_{\mathbf{Z}} \mathbf{Q}.$$

If moreover μ is a polarization of Z over K we obtain an involution

$$\mathrm{End}^0(Z) \to \mathrm{End}^0(Z), \quad \alpha \mapsto \alpha',$$

the Rosati involution, which is determined by

$$\mu\alpha' = \alpha^t\mu.$$

Our main result is the following:

(1.1) THEOREM. *Let (Z, μ) be a polarized abelian variety over a field k. Let*

$$D \subset \mathrm{End}^0_k(Z)$$

be a $\mathbf{Q}$-subalgebra stable under the Rosati involution $\alpha \mapsto \alpha'$ induced by μ. Put $n = [D:\mathbf{Q}]$ and let m be a positive integer. There exists an abelian variety Y over $k((t))$ with a polarization λ such that:

(1) $D = \mathrm{End}^0_{k((t))}(Y) = \mathrm{End}^0_K(Y \otimes K)$, where $K = k((t))^a$ denotes an algebraic closure of $k((t))$;

(2) $\dim(Y) = \dim(Z) + m.n$;

(3) the Rosati involution with respect to λ on D coincides with $\delta \mapsto \delta'$;

(4) the formal group $\hat{Y}$ of Y over $k((t))$ is isomorphic to the product of $\hat{Z} \otimes_k k((t))$ with mn copies of the formal group of $\mathbf{G}_{m,k((t))}$.

The theorem has interesting consequences:

(1.2) COROLLARY. *For every $\mathbf{Q}$-algebra D, free of finite rank over $\mathbf{Q}$, provided with a positive definite involution, for every integer $m \geqslant 1$, and every integer* *p that is zero or prime, there exists an abelian variety Y over an algebraically closed field of characteristic p such that*

$$D = \mathrm{End}^0(Y) \quad \text{and} \quad \dim(Y) = (m+1).[D:\mathbb{Q}].$$

(1.3) In (1.8) we prove that (1.1) implies (1.2). The result (1.2) is in [G]; in case $(D, *)$ is not "symmetrically generated" (in the terminology of [G, p. 113]) it is the best possible general result (cf. [O2, Th. (3.4)]).

If $\mathrm{char}(K) = p > 0$, and Y is an abelian variety over K, we write

$$p\text{-rank}(Y) = f$$

in case

$$Y[p](K^a) = (\mathbb{Z}/p)^f;$$

here $Y[p]$ is the scheme-theoretic kernel of multiplication by p on Y, and K^a is an algebraic closure of K. The p-divisible group (scheme) of Y is over K^a isogenous with

$$F = \sum (G_{n_i,m_i} \oplus G_{m_i,n_i}) \oplus s\,.\,G_{1,1} \oplus f.(G_{1,0} \oplus G_{0,1})$$

(Dieudonné–Manin theory). The sequences of pairs of integers

$$\sum ((n_i, m_i) + (m_i, n_i)) + s(1,1) + f((1,0) + (0,1))$$

is called a *symmetrical formal isogeny type* (cf. [02]), and the number f is called the p-rank of this type.

(1.4) Corollary. *Let p be a prime number and let F be a symmetrical formal isogeny type with positive p-rank. There exists an algebraically closed field K with char(K) = p, and an abelian variety Y over K such that the p-divisible group of Y has formal isogeny type F and such that* $\mathrm{End}(Y) = \mathbb{Z}$.

This gives a partial answer to Question (12.7) of [O1]. The implication (1.1) ⇒ (1.4) is proven in (1.9).

(1.5) *Examples*

(1.5.1.) Let $\mathrm{char}(k) = p > 0$ and let E be a supersingular elliptic curve over an algebraically closed field k. Then $\mathrm{End}^0(E) = D$ is the quaternion algebra over $\mathbf{Q}$ ramified at p and at ∞. The theorem shows that for any $g \geqslant 5$ there exists an abelian variety Y over a field extension of k with $\dim(Y) = g$, and $\mathrm{End}^0(Y) = D$.

Indeed, apply the theorem with $Z = E^{g-4}$, with diagonal action of D, and with $m = 1$.

This was the motivating example which led us to the theorem. Note that if an algebra of Type III acts on an abelian variety Z in *characteristic zero* then $\dim(Z)$ is even (for the definition of types cf. [M1, §21], and also see [M1, pag. 202]). We see that this is not true in positive characteristic (and cf. [O2, Th. 4.8] for all possible $\mathrm{End}^0(X) = D$ of Type III(1)).

(1.5.2) Let D be a definite quaternion division algebra over $\mathbf{Q}$. Choose a maximal subfield L of D. Then L is imaginary quadratic over $\mathbf{Q}$ and

$$D \otimes_{\mathbf{Q}} L \cong M(2 \times 2; L).$$

There exists an elliptic curve E over a field $k \supset \mathbf{F}_p$ such that

$$L \subset \mathrm{End}^0(E).$$

Then

$$D \subset \mathrm{End}^0(E \times E),$$

and for a polarization λ on E the polarization $\left(\begin{smallmatrix} \lambda & 0 \\ 0 & \lambda \end{smallmatrix}\right)$ induces the involution on D. Thus the theorem gives for any integer $m \geqslant 1$ the existence of an abelian variety Y over $k((t))$ with

$$\dim(Y) = 2 + 4m, \quad \text{and} \quad D = \mathrm{End}^0(Y)$$

(for details, cf. [O2, Lemma 4.4]).

(1.5.3) Let $d \geqslant 3$ be an integer, and let a and b be integers with $0 < a < b$, such that $a + b = d$ and $(a, b) = 1$. We choose an abelian variety Z over a finite field with formal group (over an algebraically closed field) equal to $G_{a,b} \times G_{b,a}$ as in [T, pag. 352–04, “Problème de Manin”]. Then $D = \mathrm{End}^0(Z)$ has centre F, which is a quadratic imaginary extension of $\mathbf{Q}$, and p is split in $F \supset \mathbf{Q}$. Further $[D{:}\ F] = d^2$ and $\dim(Z) = d$. By the theorem we can construct for any $m \geqslant 0$ an abelian variety Y with $\dim(Y) = d + 2md^2$ and $D = \mathrm{End}^0(Y)$. We note that d^2 does not divide $\dim(Y)$. According to [M1, pag. 202] such examples do not exist in characteristic zero.

(1.6) REMARK. For a more systematic description which algebras can occur as $\mathrm{End}^0(T)$ for some abelian variety Y over an algebraically closed field we refer to [O2].

We note that the method of construction in (1.1) basically concerns deformation of a (partially) degenerated abelian variety. Choose a point on the boundary of the moduli space such that $D \subset \mathrm{End}^0(Y_0)$ and such that the "quasi-polarization" on Y_0 induces a given involution on D. Then a deformation is found which preserves the action of D, such that the generic fibre Z has exactly $D = \mathrm{End}^0(Z)$.

Another method is to take an appropriate abelian variety Y_0 with $D \subset \mathrm{End}^0(Y_0)$ (this time it corresponds with an interior point of the moduli scheme), and apply deformation theory. See [O2] for some details.

(1.7) *The idea of the proof of Theorem* (1.1). The construction of the abelian variety Z in the theorem is inspired by [G, Th. 12]. We use furthermore the construction of semi-abelian varieties as initiated by Mumford and completed by Faltings, cf. [M2], and [F, §3].

We make a slight change in notation: instead of (Z, μ) we now write (Z_0, μ_0). We write

$$Z = Z_0 \otimes_k k[[t]]$$

for the "constant" abelian scheme over this complete discrete valuation ring. Let

$$D_0 = D \cap \mathrm{End}_k(Z_0).$$

Let T denote a split torus over $k[[t]]$ with character group $(D_0)^m$, viewed as a right-D_0-module. Then T has dimension mn and T is provided with a left-action of D_0. It is shown in Lemma (3.1) that there exists an extension

$$0 \to T \to G \to Z \to 0$$

given by a D_0-equivariant homomorphism

$$\tau\colon X(T) \to Z^t(k[[t]])$$

where $X(T)$ is the character group of T, such that

$$D = \mathrm{End}(G) \otimes \mathbf{Q}.$$

The next step is to find a free subgroup Λ of $G(k((t)))$ of rank mn such that:

(i) all data in Faltings' construction [F, §3] are available for Λ and G,
(ii) Λ is D_0-invariant.

Let Y denote the general fibre of the semi-abelian variety "G/Λ". Then Y is an abelian variety over $k((t))$ with $\dim(Y) = \dim(Z) + mn$. Part (4) of the theorem follows at once from the Faltings' construction. It can be seen that

$$\mathrm{End}(Y) \quad = \quad \{\alpha \in \mathrm{End}(G) \,|\, \alpha(\Lambda) \subset \Lambda\}.$$

Using (ii) one obtains part (2) and (3) from the theorem.

In §2 we construct for a given extension $G/T = Z$ of an abelian scheme Z over a complete discrete valuation ring R all "lattices" Λ satisfying (i) above.

In §3 the extension G with $\mathrm{End}(G) \otimes \mathbb{Q} = D$ is constructed and D_0-invariant lattices are derived.

In fact the contents of the Sections 2 and 3 remain valid if R is replaced by a normal, excellent ring which is complete with respect to some non-zero ideal.

We conclude this section by giving the proofs of (1.2) and (1.4) starting from the theorem.

(1.8) *Proof of* (1.2.). Let n be a positive integer, and suppose $s \in GL(n, \mathbb{Q})$ is a symmetric non-singular matrix. We denote by α' the transpose of a matrix α (and s being symmetric we have $s = s'$). Note that

$$\alpha \mapsto s^{-1}\alpha' s$$

is an involution on $GL(n, \mathbb{Q})$.

Suppose $(D, *)$ and m be given as in (1.2). We write $n := [D\colon \mathbb{Q}]$, and we choose a $\mathbb{Q}$-base $D = \mathbb{Q}^n$ for D. This gives an embedding

$$D \subset M(n \times n, \mathbb{Q}).$$

Let (,) denote the standard inner product on $\mathbb{Q}^n$. On D an inner product is given by the formula

$$\langle x, y\rangle \quad = \quad \mathrm{Tr}(xy^* + yx^*).$$

Then there exists an $s \in GL(n, \mathbb{Q})$ such that

$$\langle x, y\rangle \quad = \quad (sx, y) \qquad \text{for all} \quad x, y \in D.$$

Because $\langle x, y\rangle = \langle y, x\rangle$ it follows that s is symmetric. By $\langle \mathrm{d}x, y\rangle = \langle x, \mathrm{d}^*y\rangle$ we conclude that

$$s^{-1}d's = d^* \qquad \text{for all} \quad d \in D.$$

We choose some elliptic curve E over some field $k \supset \mathbb{F}_p$, and a polarization τ on E. With the matrix s constructed above we choose

$$\mu := s\begin{pmatrix} \tau & & 0 \\ & \ddots & \\ 0 & & \tau \end{pmatrix},$$

which is a polarization on $Z := E^n$. For $\beta \in \mathrm{End}^0(Z)$ we have

$$\mu\beta^{\S} = \beta^t\mu,$$

where $\beta \mapsto \beta^{\S}$ is the Rosati involution induced by μ. For

$$\alpha \in M(n \times n, \mathbb{Q}) \subset M(n \times n, \mathrm{End}^0(E)) = \mathrm{End}^0(Z)$$

we have

$$\alpha^{\S} = \mu^{-1}\alpha^t\mu, = s^{-1}\alpha' s.$$

Thus $d^* = d^{\S}$ for all $d \in D \subset \mathrm{End}^0(Z)$. Hence (1.2) follows from (1.1).

(1.9) *Proof of* (1.4). The isogeny type of the p-divisible group has the form $F = F_1 \oplus (G_{1,0} \oplus G_{0,1})$ since F has positive p-rank. According to the Honda–Serre solution of the Manin problem, cf. [T, pp. 352–04] there exists an abelian variety over a finite field of characteristic p with formal isogeny type F_1. Now apply (1.1) with $m = 1$ and $D = \mathbb{Q}$. The statement follows from part (1) and (4) of the theorem.

2. The Faltings–Mumford construction

In this section R denotes a complete discrete valuation ring with maximal ideal $\mathfrak{m}$ and with field of fractions K.

(2.1) The data for the Faltings–Mumford construction [F, §3] can be stated as follows:

(1) *An abelian scheme Z over R together with an ample line bundle M on Z* (and as usual $\varphi_M\colon Z \to Z^t$ denotes the morphism induced by $a \mapsto t_a M \otimes M^{-1}$).

(2) *An extension G of Z by a split torus T over R.* This is an exact sequence

$$0 \longrightarrow F \longrightarrow G \xrightarrow{\pi} Z \longrightarrow 0$$

given by a homomorphism of groups

$$\tau\colon X(T) \to Z^t(R),$$

where $X(T)$ denotes the group of characters of T. We choose further for each $x \in X(T)$ a line bundle $\mathcal{O}_x$ on Z such that $\mathcal{O}_{x_1+x_2} = \mathcal{O}_{x_1} \otimes \mathcal{O}_{x_2}$ for all $x_1, x_2 \in X(T)$ and such that $\tau(x) \in \mathrm{Pic}^0(Z)(R)$ is the class of the line bundle $\mathcal{O}_x$.

(3) *A bilinear form*

$$b\colon X(T) \times X(T) \to K$$

satisfying

$$b(x_1, x_2) = b(x_2, x_1) \quad \text{for all} \quad x_1, x_2 \in X(T)$$

and

$$b(x, x) \in \mathfrak{m} \quad \text{for all} \quad x \in X(T) \quad \text{with} \quad x \neq 0.$$

(4) *An homomorphism of groups $c\colon X(T) \to Z(R)$ with $\tau = \varphi_M \cdot c$ and a family of isomorphisms*

$$\varphi(x_1, x_2)\colon t^*_{c(x_1)}\mathcal{O}_{x_2} \xrightarrow{\sim} \mathcal{O}_{x_2},$$

additive in x_1 and x_2, i.e.,

$$\varphi(x_1, x_2 + x_3) = \varphi(x_1, x_2) \otimes \varphi(x_1, x_3) \quad \text{and}$$

$$\varphi(x_1 + x_2, x_3) = \varphi(x_1, x_3) \cdot (t^*_{c(x_1)}\varphi(x_2, x_3)).$$

(5) *A family of isomorphisms*

$$\psi(x)\colon t^*_{c(x)}M \to m \otimes \mathcal{O}_x, \quad \text{all } x \in X(T)$$

such that $\psi(x_1 + x_2)$ *equals the composition* (which *is an isomorphism*)

$$t^*_{c(x_1+x_2)}M = t^*_{c(x_1)}t^*_{c(x_2)}M \xrightarrow[t^*_{c(x_1)}(\psi(x_2))]{}$$

$$t^*_{c(x_1)}M \otimes t^*_{c(x_1)}\mathcal{O}_{x_2} \xrightarrow[\psi(x_1)\otimes\varphi(x_1,x_2)]{} M \otimes \mathcal{O}_{x_1} \otimes \mathcal{O}_{x_2}$$

for all $x_1, x_2 \in X(T)$.

(2.2) *Remarks*

(2.2.1) These data differ slightly from those in [F, §3]. We will show however that they are equivalent. First of all we have no need for a subgroup of finite index of $X(T)$ and we will not consider more general rings than complete discrete valuation rings. The bilinear form b in (2.1) part (3) induces a homomorphism ℓ: $X(T) \to T(K)$ given by

$$\langle \ell(x_1), x_2 \rangle = b(x_1, x_2) \qquad \text{for all} \qquad x_1, x_2 \in X(T).$$

Let $a \in Z(R)$ and let an additive family of isomorphisms $\varphi(x)$: $t^*_a\mathcal{O}_x \to \mathcal{O}_x$ be given. The extension π: $G \to Z$ is equal to $\mathcal{S}pec(\oplus\, \mathcal{O}_x)$ and $\pi^*\mathcal{O}_G = \oplus\, \mathcal{O}_x$. There exists a unique element $b \in G(R)$ such that $\pi(b) = a$ and such that the natural isomorphism f: $t^*_b\mathcal{O}_G \to \mathcal{O}_G$ satisfies $\pi^*(f) = \oplus\, \varphi(x)$. Hence part (4) of (2.1) is equivalent to giving a homomorphism c': $X(T) \to G(R)$ with $\pi . c' = c$. The homomorphism $i = \ell . c'$: $X(T) \to G(K)$, given by $i(x) = \ell(x)c'(x)$ is injective because $b(x, x) \in \mathfrak{m}$ for all $x \in X(T)$ with $x \neq 0$. In this way we have obtained the data of [F, §3]. The converse is shown in a similar way.

(2.2.2) Let $\Lambda \subset G(K)$ denote the image of i. The semi-abelian variety over R constructed in [F, §3] will be (abusively) denoted by G/Λ since it is obtained by dividing a certain formal scheme over R, corresponding to G, by the action of Λ. The general fibre $(G/\Lambda) \otimes_R K = Y$ is an abelian variety over K. Let L be any finite field extension of K with ring of integers S. Since S is a discrete valuation ring one has

$$(G/\Lambda)(L) = G(L)/\Lambda \quad \text{and} \quad (G/\Lambda)(S) = G(S).$$

(2.2.3) The family of isomorphisms in (5) can be interpreted as a family of isomorphisms of $\mathcal{O}_G$-modules

$$\tilde{\psi}(x)\colon t^*_{c'(x)}\pi^*M \to \pi^*M$$

satisfying

$$\tilde{\psi}(x_1 + x_2) = \tilde{\psi}(x_1) \cdot (t^*_{c'(x_1)}\tilde{\psi}(x_2))$$

for all $x_1, x_2 \in X(T)$. In particular this defines an action of the group $\Lambda \subset G(K)$ on the line bundle π^*M on $G \otimes_R K$.

The abelian variety $Y = (G/\Lambda) \otimes_R K$ depends only on the extension G and on the lattice $\Lambda \subset G(K)$. In particular one can multiply b with a symmetric bilinear s: $X(T) \times X(T) \to R^*$ and ℓ with the corresponding σ: $X(T) \to T(R)$ and c' with σ^{-1} without changing Y.

Further we will assume that b: $X(T) \times X(T) \to K^*$ has the form

$$b(x_1, x_2) = t^{B(x_1, x_2)} \quad \text{where} \quad B\colon X(T) \times X(T) \to \mathbf{Z}$$

is a bilinear, symmetric and positive definite and where $\mathfrak{m} = tR$.

In the next proposition we show that the data Z, M, τ, B can be completed to the full data of (2.1).

(2.3) PROPOSITION. *Let the following be given:*

(*1*) *an abelian scheme Z over R and an ample line bundle M on it;*

(*2*) *an extension*

$$0 \longrightarrow T \longrightarrow G \xrightarrow{\pi} Z \longrightarrow 0$$

corresponding to a homomorphism τ: $X(T) \to Z^t(R)$;

(*3*) *a symmetric bilinear positive definite B: $X(T) \times X(T) \to \mathbf{Z}$.*

Then there exists a homorphism c': $X(T) \to G(R)$ and a family of isomorphisms $\{\psi(x) \mid x \in X(T)\}$ such that:

(*4*) *$\varphi_M \cdot \pi \cdot c' = \tau$, and*

(*5*) *$\psi(x)$: $t^*_{c(x)}M \to M \otimes \mathcal{O}_x$ (with $c = \pi \cdot c'$) has the property*

$$\psi(x_1 + x_2) = (\psi(x_1) \otimes \varphi(x_1, x_2)) \cdot (t^*_{c(x_1)}(x_2))$$

where φ corresponds to c'.

Moreover the ψ is unique up to multiplication by a homomorphism $X(T) \to T(R)$ derived from a bilinear symmetric form $X(T) \times X(T) \to R^*$ and up to torsion coming from Ker φ_M.

In the proof we fix a homomorphism c: $X(T) \to Z(R)$ with $\varphi_M \cdot c = \tau$. This homomorphism is unique up to elements in Ker $\varphi_M(R)$. We need several lemmas.

(2.4) LEMMA. *Let L be a line bundle on Z such that the class of L belongs to* $\mathrm{Pic}^0(Z)$. *Then there exists an additive family of isomorphisms*

$$\varphi(x)\colon\ \mathrm{t}^*_{c(x)}L \to L,$$

i.e.

$$\varphi(x_1 + x_2) \;=\; \varphi(x_1)\,.\,(t^*_{c(x_1)}\varphi(x_2))$$

for all x_1, $x_2 \in X(T)$.

Proof. The notation $M(a)$ for any $\mathcal{O}_X$-module and any point $a \in X$ means $M(a) = \otimes_{\mathcal{O}_{X,a}} \mathcal{O}_{X,a}/\mathfrak{m}_{X,a}$. Since the class of L belongs to $\mathrm{Pic}^0(Z)$ the line bundle

$$m^*L \otimes p_1^*L^{-1} \otimes p_2^*L^{-1} \otimes_R L(0) \;=\; \vartheta_2(L)$$

on $Z \times Z$ is canonically isomorphis to $\mathcal{O}_{Z\times Z}$. This isomorphism induces canonical isomorphisms

$$L(x + y) \otimes_R L(x)^{-1} \otimes_R L(y)^{-1} \otimes_R L(0) \xrightarrow{\sim} R.$$

Further we have canonical isomorphisms

$$t_x^*L \xrightarrow{\sim} L \otimes_R L(x) \otimes_R L(0)^{-1}$$

for every $x \in X(T)$ we fix an isomorphism of R-modules $\varrho(x)\colon L(c(x)) \to R$ and we define $\varphi_0(x)\colon t^*_{c(K)}L \to L$ by

$$t^*_{c(x)}L \xrightarrow{\sim} L \otimes_R (c(x)) \otimes L(0)^{-1} \xrightarrow[\mathrm{id}_L \otimes \varrho(x) \otimes \varrho(0)^{-1}]{} L.$$

Consider the following diagram:

$$\begin{tikzcd}
t^*_{c(x+y)}L \arrow[r, "f"] \arrow[dd, "h"] & t^*_{c(x)}(L \otimes L(c(y)) \otimes L(0)^{-1}) \arrow[d, "g"] \\
& L \otimes L(c(x)) \otimes L(0)^{-1} \otimes L(c(y)) \otimes L(0)^{-1} \arrow[d, "\alpha"] \\
L \otimes L(c(x + y)) \otimes L(0)^{-1} \arrow[ur, "k"] \arrow[r, "\beta"] & L.
\end{tikzcd}$$

The morphisms f, g, h and k are induced by the isomorphism $\vartheta_2(L) \to \mathcal{O}_{Z\times Z}$ and hence the upper triangle is commutative. Further α is the map

$$\alpha = \mathrm{id}_L \otimes \varrho(x) \otimes \varrho(0)^{-1} \otimes \varrho(y) \otimes \varrho(0)^{-1}$$

and

$$\beta = \mathrm{id}_L \otimes \varrho(x + y) \otimes \varrho(0)^{-1}$$

One easily sees that $\beta . h = \varphi_0(x + y)$ and

$$\alpha . g . f = \varphi_0(x) . (t^*_{c(x)} \varphi_0(y)).$$

It follows that

$$\varphi_0(x + y) = a(x, y)\varphi_0(x) . (t^*_{c(x)} \varphi_0(y))$$

where a: $X(T) \times X(T) \to R^*$ is symmetric! Since $X(T)$ is a free $\mathbb{Z}$-module there exists a function b: $X(T) \to R^*$ with $b(x + y) = a(x, y)b(x)b(y)$ for all $x, y \in X(T)$. Then $\varphi(x) = b(x)^{-1}\varphi_0(x)$ for all $x \in X(T)$ satisfies the condition of the lemma.

(2.5) COROLLARY. *There exists a bi-additive family of isomorphisms* $\varphi(x, y)$: $t^*_{c(x)}\mathcal{O}_y \to \mathcal{O}_y$.

REMARK. Corollary (2.5) follows from (2.4). The description $G = \mathcal{S}pec(\oplus\, \mathcal{O}_x)$ implies that π: $G(R) \to Z(R)$ is surjective. Hence there exists a homorphism c': $X(T) \to G(R)$ with $\pi . c' = c$. From c' we obtain a bi-additive family of isomorphisms $t^*_{c(x)}\mathcal{O}_y \to \mathcal{O}_y$.

(2.6) LEMMA. *Let a family of isomorphisms*

$$\varphi(x, y): t^*_{c(x)}\mathcal{O}_y \to \mathcal{O}_y$$

and a family of isomorphisms

$$\psi(x): t^*_{c(x)}M \to M \otimes \mathcal{O}_x$$

be given. The function f: $X(T) \times X(T) \to R^*$ *given by the formula*

$$\psi(x + y) = f(x, y)(\psi(x) \otimes \varphi(x, y)) . (t^*_{c(x)}\psi(y))$$

satisfies the cocycle relation

$$f(x + y, z)f(x, y) = f(x, y + z)f(y, z).$$

Proof. We may assume that $\varphi(x, y)$ is bi-additive. Consider the sequence of isomorphisms induced by ψ and by φ:

$$t^*_{c(x+y+z)}M \xrightarrow{\alpha_4} t^*_{c(x+y)}(M \otimes \mathcal{O}_z) \xrightarrow{\alpha_3}$$

$$t^*_{c(x)}(M \otimes \mathcal{O}_y) \otimes t^*_{c(x)}\mathcal{O}_z \xrightarrow{\alpha_2} t^*_{c(x)}\mathcal{O}_y \otimes \mathcal{O}_z \xrightarrow{\alpha_1} M \otimes \mathcal{O}_{x+y+z}.$$

Then

$$f(x, y) \cdot \alpha_1\alpha_2\alpha_3 = \psi(x + y) \otimes \varphi(x + y, z)$$

and

$$f(x + y, z)f(x, y)\alpha_1\alpha_2\alpha_3\alpha_4$$

$$= f(x + y, z)(\psi(x + y) \otimes \varphi(x + y, z)) \cdot (t^*_{c(x+y)}\psi(z))$$

$$= \psi(x + y + z).$$

Similarly

$$f(y, z)\alpha_3\alpha_4 = t^*_{c(x)}\psi(y + z).$$

Since $\varphi(x, y) \otimes \varphi(x, z) = \varphi(x, y + z)$ we have

$$f(x, y + z)f(y, z)\alpha_1\alpha_2\alpha_3\alpha_4$$

$$= f(x, y + z)(\psi(x) \otimes \varphi(x, y) \otimes \varphi(x, z)) \cdot (t^*_{c(x)}\psi(y + z))$$

$$= \psi(x + y + z).$$

The cocycle relation now follows.

(2.7) *End for the proof of* (2.3). Let $\varphi_0(x, y)$ be bi-additive and let $\psi_0(x)$ (arbitrary) be given. They determine f; $X(T) \times X(T) \to R^*$ as in Lemma (2.6). take q: $X(T) \to R^*$ arbitrarily and take a: $X(T) \times X(T) \to R^*$

bilinear and antisymmetric. Put $\psi(x) = q(x)\psi_0(x)$ and $\varphi(x, y) = a(x, y)\varphi_0(x, y)$. Then φ, ψ satisfies (5) in Lemma (2.3) if and only if

$$(*)\ f(x, y) = \frac{q(x + y)}{q(x)q(y)} a(x, y).$$

Instead of working with R^* we take an arbitrary commutative group A (with additive notation) with trivial $X(T)$-action. By definition we have:

$H^2(X(T), A)$

$$= \frac{\{f: X(T) \times X(T) \to A \mid f(x + y, z) + f(x, y) = f(x, y + z) + f(y, z)\}}{\{dq \mid q: X(T) \to A \text{ arbitrary and } dq(x, y) = q(x + y) - q(x) - q(y)\}}.$$

It is well-known that

$$H^2(X(T), A) = \operatorname{Hom}(\Lambda^2 X(T), A)$$

$$= \{a: X(T) \times X(T) \to A \mid a \text{ is bilinear and antisymmetric}\}.$$

It follows that $(*)$ has a solution. Moreover the bilinear antisymmetric form a in the solution is unique and q is unique up to multiplication by a homomorphism $X(T) \to R^*$. This proves (2.3).

(2.8) Definition. A homomorphim c': $X(T) \to G(R)$ with $\pi . c' = c$ is called M-symmetric if there are isomorphisms

$$\psi(x): t^*_{c(x)}M \to M \otimes \mathcal{O}_x$$

satisfying

$$\psi(x + y) = (\psi(x) \otimes \varphi(x, y) . t^*_{c(x)}\psi(y))$$

for all $x, y \in X(T)$ and where $\varphi(x, y)$ corresponds to c'.

(2.9) Remark. For any homomorphism c': $X(T) \to G(R)$ with $\pi . c' = c$ there exists a unique bilinear, antisymmetric a: $X(T) \times X(T) \to R^*$ such that $\alpha . c'$: $X(T) \to G(R)$ is M-symmetric. Here α denotes the homomorphis $X(T) \to T(R)$ induced by a.

3. *D*-invariance

Let R, $\mathfrak{m}$, K be as in §2 and let $k = R/\mathfrak{m}$. Let the abelian scheme Z over R be given and let D_0 be an order in D such that $D_0 \subset \mathrm{End}(Z)$. The action of $\alpha \in \mathrm{End}(Z)$ on Z^t is denoted by $\alpha^t \in \mathrm{End}(Z^t)$. We suppose in the sequel that the right End(Z)-module $Z^t(R)$ has rank $\geqslant m$. In the situation of §1 we choose $R = k[[t]]$) and $Z = Z_0 \otimes_k k[[t]]$. Then $Z^t(k[[t]])$ is uncountable. Thus $Z^t(k[[t]])$ has an infinite rank as End(Z)-module.

The group of characters $X(T)$ of T is identified with $D_0 \times \cdots \times D_0$, i.e., m copies of the right D_0-module D_0.

(3.1) LEMMA. *There exists a homomorphism τ: $X(T) \to Z^t(R)$ such that the corresponding extension $Z = G/T$ has the property that* $\mathrm{End}(G) \otimes \mathbf{Q} = D$.

Proof. Any $\alpha \in \mathrm{End}(G)$ satisfies $\alpha(T) \subset T$. Furthermore $\alpha_1 = \alpha|T$ and $\alpha_2 =$ (the induced endomorphism on $Z = G/T$) are determined by α. The action of α_1 on $X(T)$ is denoted by α_1^* and the action of α_2 on Z^t is denoted by α_2^t. One easily sees that

$$\mathrm{End}(G) = \{(\alpha_1, \alpha_2)|\alpha_1 \in \mathrm{End}(T), \alpha_2 \in \mathrm{End}(Z), \tau\alpha_1^* = \alpha_1^t\tau\}.$$

Let $e_1, \ldots, e_m$ be a basis of the right D_0-module $X(T)$. Take elements $a_1, \ldots, a_m \in Z^t(R)$, linearly independent over $\mathrm{End}^0(Z)$. Define τ: $X(T) \to Z^t(R)$ by

$$\tau\left(\sum_{i=1}^{m} e_i d_i^*\right) = \sum_{i=1}^{m} a_i d_i^t \qquad \text{for} \quad d_1, \ldots, d_m \in D_0.$$

Clearly $D_0 \subset \mathrm{End}(G)$. Choose $\alpha = (\alpha_1, \alpha_2) \in \mathrm{End}(G) \otimes \mathbf{Q}$. Then $e_1\alpha_1^* = \Sigma\, e_i d_i$ for certain $d_i \in D$ and hence $\Sigma\, a_i d_i^t = a_1\alpha_2^t$. Because $a_1, \ldots, a_m$ are linearly independent this implies that $\alpha_2 = d_1$. After subtracting d_1 from $\alpha = (\alpha_1, \alpha_2)$ we may suppose that $\alpha_2 = 0$. Since τ is injective, we conclude that also $\alpha_1 = 0$, and hence $\alpha = 0$. This shows that $D = \mathrm{End}(G) \otimes \mathbf{Q}$.

(3.2) LEMMA. *Let Z, τ, G be as in (3.1) and let M be an ample line bundle on Z such that the Rosati involution R on* $\mathrm{End}^0(Z)$ *satisfies $R(D) = D$. There exists a D_0-invariant homomorphism c': $X(T) \to G(R)$ satisfying*:

(1) $\varphi_M . \pi . c' = \tau$,

(2) c' is symmetric with respect to M.

Proof. There exists a homomorphism c'': $X(T) \to G(R)$ where c'' is D_0-invariant and $\varphi_M . \pi . c'' = \tau$. According to (2.9) there is a unique anti-symmetric bilinear a: $X(T) \times X(T) \to R^*$ such that

$$c' = c''.a\colon X(T) \to G(R)$$

is symmetric with respect to M.

We have to show that a is also D_0-equivariant. The equivariance of c'' can be expressed as $c''(xd^*) = R(d)c''(x)$ for $x \in X(T)$ and $d \in D_0$. Let

$$\varphi(x, yd^*)\colon t^*_{c(x)}\mathcal{O}_y \to \mathcal{O}_y$$

denote the family of isomorphisms corresponding to c''. The equivariance of c'' can be expressed in the φ as: $\varphi(x, d^*) = d^*(\varphi(x(Rd)^*, y))$. Indeed, we note that $\mathcal{O}_{yd^*} = d^*(\mathcal{O}_y)$. The isomorphisms

$$\varphi(x, yd^*)\colon t^*_{c(x)}\mathcal{O}_{yd^*} \to \mathcal{O}_{yd^*}$$

together with

$$t^*_{c(x)}d^* = d^*t^*_{dc(x)} \quad \text{and} \quad dc(x) = c(xR(d)^*)$$

induce an isomorphism

$$d^*t^*_{c(x(Rd)^*}\mathcal{O}_y \to d^*\mathcal{O}_y$$

which coincides with $d^*(\varphi(x(Rd)^*, y))$.

Let the cocycle $f(-, -)$ be given by the formula

$$\psi(x + y) = f(x, y)(\psi(x) \otimes \varphi(x, y)).(t^*_{c(x)}\psi(y)).$$

The alternating bilinear a: $X(T) \times X(T) \to R^*$ satisfies

$$a(x, y)^2 = f(x, y)f(y, x)^{-1}.$$

The D_0-equivariance of a can be expressed as

$$a(x(Rd)^*, y) = a(x, yd^*) \quad \text{for all} \quad d \in D_0.$$

The D_0-equivariance of $a(x, y)^2$ follows at once from $\varphi(x, yd^*) = d^*(\varphi(x(Rd)^*, y))$. After changing D_0 into $\mathbb{Z}.1 + 2D_0$ (or similar changes of τ, M, etc.), the equivariance of a follows.

(3.3) LEMMA. *There exists a positive definite symmetric bilinear form* $B\colon X(T) \times X(T) \to \mathbb{Z}$ *satisfying* $B(xd^*, y) = B(x, yR(d)^*)$ for all $x, y \in X(T)$ *and* $d \in D_0$.

Proof. Let $e_1, \ldots, e_m$ be a D_0-basis for $X(T)$. Define

$$B\left(\sum e_i d_i^*, \sum e_i \tilde{d}_i^*\right) := \sum_{i=1}^{m} \mathrm{Tr}\,(d_i R(\tilde{d}_i)),$$

where Tr denotes the reduced trace of $\mathrm{End}^0(Z)$ over $\mathbb{Q}$. According to [M1, §21, Th. 1] we see that B has the required properties.

(3.4) *End of the proof of* (1.1). Let $R = k[[t]]$ and put $Z = Z_0 \otimes_k R$. Then Z, τ, G, M, c', B as in (3.1)–(3.3) determine an abelian variety Y over the field $k((t))$. We still have to show that $\mathrm{End}^0(Y) = \mathrm{End}^0(Y \otimes k((t))^a) = D$.

The inclusion $D \subset \mathrm{End}^0(Y)$ follows at once from the following statement:

"Let for $i = 1$, and $i = 2$ the set of data $(Z_i, M_i, T_i, G_i, b_i, \varphi_i, \psi_i)$ as in (2.1) be given. Let Y_i denote the resulting abelian variety over $K = k((t))$ and let $\Lambda_i \subset G_i(K)$ denote the subgroup introduced in (2.2.2). A morphism of algebraic groups $\alpha\colon G_1 \to G_2$ satisfying $\tilde{\alpha}(\Lambda_1) \subset \Lambda_2$ induces a unique R-morphism of semi-abelian varieties $\alpha\colon G_1/\Lambda_1 \to G_2/\Lambda_2$ such that under the canonical isomorphism of $\mathfrak{m}$-adic completions of G_i and G_i/Λ_i one has that a and $\tilde{\alpha}$ are formally identical".

In the special case $Z_1 = Z_2 = 0$ this statement is contained in [M2, p. 257, Th. 4.6]. The general case is asserted in [F, §3, p. 342].

Let L be a finite field extension of $k((t))$. Let S denote the integral closure of $k[[t]]$ in L and let $\mathfrak{m}_S$ be the maximal ideal of S. Let $\alpha \in \mathrm{End}(Y \otimes_{k((t))} L)$. Then α induces an endomorphism of the Néron minimal model N of $Y \otimes_{k((t))} L$ and also an endomorphism of the unit component M of the $\mathfrak{m}_S$-adic completion of N.

From the construction it follows that M is isomorphic to the $\mathfrak{m}_S$-adic completion of $G \otimes_R S$. Hence $\alpha \in D_0$. It follows that $\mathrm{End}^0(Y \otimes L) \subset D$, and hence

$$\mathrm{End}^0(Y \otimes_{k((t))} k((t))^a) = D.$$

Thus Theorem (1.1) is proved.

References

[F] G. Faltings: Arithmetische Kopaktifizierung des Modulraums der abelsche Varietäten. *Lect. N. Mat.* 1111 (1984) pp. 321–383.

[G] L. Gerritzen: On multiplicative algebras of Riemann matrices. *Math. Ann.* 194 (1971) 109–122.

[M1] D. Mumford: *Abelian Varieties.* Tata Inst. Fund. Research, Bombay, and Oxford Univ. Press (1974).

[M2] D. Mumford: An analytic construction of degenerating abelian varieties over complete rings. *Comp. Math.* 24 (1972) 239–272.

[O1] F. Oort: Lifting algebraic curves, abelian varieties and their endomorphisms to characteristic zero. In: S.J. Bloch (ed.) *Algebraic Geometry*, Bowdoin 1985, *Proceed. Symp. Pure Math.* Vol. 46, Part 2, A.M.S. (1987) pp. 165–195.

[O2] F. Oort: Endomorphism algebras of abelian varieties. To appear: *Algebr. Geom. and Communt. Algebra in Honor of Masayoshi Nagata* (1987) pp. 101–134.

[T] J. Tate: Classes d'isogénie des variétés abéliennes sur un corps fini (d'après T. Honda). Sém. Bourbaki 21 (1968/69), Exp. 352. *Lect. N. Math.* 179, Springer-Verlag (1971).