H. Tapia-Recillas
Nagoya Math. J.
Vol. 69 (1978), 65-96

ULTRAMETRIC THETA FUNCTIONS AND ABELIAN VARIETIES

HORACIO TAPIA-RECILLAS(*)

Let k be a field complete with respect to a non-trivial, non-archimedean valuation and let g be a positive integer. Consider the following question: if Γ is a multiplicative subgroup of $G_g = (k^*)^g$ satisfying certain "Riemann conditions", can one construct in a natural way an abelian variety defined over k having G_g/Γ as its set of k-rational points? This problem was first considered by Morikawa [3]. J. Tate provided a complete solution for $g = 1$ (cf. for example [6]). J. McCabe [2] gave a partial solution for $g > 1$. He showed how to attach to Γ a graded ring R of theta functions such that $A = \mathrm{Proj}.\, R$ is a g-dimensional abelian variety over k. He further constructed a homomorphism $\varphi: G_g/\Gamma \to A_k$ and showed that it is injective. But he could only prove that φ is surjective under restrictive hypotheses, assuming that k is locally compact of characteristic zero. Recently Raynaud [5], Gerritzen [1] and Mumford [4] have generalized and completely solved the problem we are considering. But their techniques are non-elementary and it is still perhaps interesting to show that the map φ is surjective within the context of Tate-McCabe theory, using only simple calculations with Laurent power series.

That is the goal of this paper.

Let $\mathrm{ord.}: k^* \to \mathrm{Reals}$ denote the order function associated to our valuation. In part 1 we start with a $g \times g$ matrix $(\mathscr{A}_{ij})$ with entries in k^* satisfying the following Riemann conditions: $\mathscr{A}_{ij} = \mathscr{A}_{ji}$ and the associated matrix $(\mathrm{ord.}\, \mathscr{A}_{ij})$ is positive definite. Following McCabe we construct the ring R of theta functions associated to $(\mathscr{A}_{ij})$, the abelian variety A and the map $\varphi: G_g/\Gamma \to A_k$ where Γ is the multiplicative sub-

Received July 2, 1976.

(*) This paper includes parts of the author's Ph. D. dissertation at Brandeis University. I would like to thank Professor Paul Monsky for his suggestions during the writing of the thesis and the preparation of this paper. This work was supported by CONACYT PNCB 000070 and the Centro de Investigación del I.P.N., México.

group of G_g generated by the column vectors of $(\mathscr{A}_{ij})$.

Part II is the heart of the paper. In it we assume that the off-diagonal elements of $(\mathscr{A}_{ij})$ have order 0. We call this case the "diagonal case". Here the reduction $\bar{A}$ of A plays an important role. For $g=1$ $\bar{A}$ is a rational curve with an ordinary double point; in general $\bar{A}$ is a rational variety which looks very much like a product of such curves. We attach to each $P \in A_k$ a certain subset $S(P)$ of $\{1, 2, \cdots, g\}$; $S(P)$ describes how singular $\bar{P}$ is on $\bar{A}$. We say that P is a unit point if $S(P) = \varnothing$; this means that $\bar{P}$ is non-singular on $\bar{A}$. In § II. 3 we use an implicit function type argument to show that φ is 1-1 and that all unit points are in the image of φ. The proof that any $P \in A_k$ is in $\varphi(G_g)$ is by induction on the cardinality of $S(P)$. The key steps in the induction are an *addition formula* on A, (Theorem II. 4.6), and the "*decomposition theorem*", (Theorem II. 6.6), whose proof depends on the study of the zeroes of a certain Laurent series θ_P.

We return to the general case in part III. Using the diagonal case and an isogeny argument we show that φ is bijective, assuming only that each ord. $\mathscr{A}_{ij}$ is rational. This mild restriction is unnecessary as Gerritzen's result show, but we have been unable to avoid it.

Throughout this paper we use the following notation: k is a field complete with respect to a non-trivial, non-archimedean valuation, ord: $k^* \to$ Reals is the associated order function, $\mathcal{O}$, $\mathscr{M}$ and $\bar{k}$ are the valuation ring, maximal ideal and residue class field of the valuation. U is the unit group of $\mathcal{O}$ and G_g is the product of g copies of k^*.

I

Part I is concerned with the definition and basic properties of the ring of theta functions R. It contains a proof that $A = \text{Proj.}\, R$ is an abelian variety of dimension g over k.

Most of this material can be found in the first three chapters of McCabe [2], but our arguments are somewhat simpler.

§ I.1. The ring of theta-functions

A Laurent series over k is a formal sum $\sum_{I \in Z^g} \mathscr{A}_I X^I$, $\mathscr{A}_I \in k$, which converges for all $(x_1, \cdots, x_g) \in G_g$. (we shall use standard multivariable notation throughout. If $I = (i_1, \cdots, i_g)$ then X^I means $\prod_j X_j^{i_j}$). The Laurent series form a k-algebra $\mathscr{L}$. The subring of $\mathscr{L}$ consisting of series with $\mathscr{A}_I \in \mathcal{O}$ is called $\mathscr{L}_{\mathcal{O}}$. $\mathscr{L}$ is a domain, and if an element of $\mathscr{L}$ vanishes on all of G_g, each $\mathscr{A}_I = 0$. Suppose $n > 1$ and $(r) = (r_1, \cdots, r_g) \in (\boldsymbol{Z}/n\boldsymbol{Z})^g$. An element $\sum \mathscr{A}_I X^I$ of $\mathscr{L}$ is said to have n-parity (r) if $\mathscr{A}_I = 0$ unless each i_j reduces to r_j mod. n. Let $\mathscr{L}^{(r)}$ denote the subspace of elements of $\mathscr{L}$ having n-parity (r). Then we get a decomposition $\mathscr{L} = \oplus_{(r)} \mathscr{L}^{(r)}$; the "$n$-parity decomposition of $\mathscr{L}$".

Let $(\mathscr{A}_{ij})$ be a $g \times g$ symmetric matrix with entries in k^* such that the associated matrix (ord. $\mathscr{A}_{ij}$) is positive definite.

Let $V_j = (\mathscr{A}_{j1}, \cdots, \mathscr{A}_{jg})$, $q_j = \mathscr{A}_{jj}$. If $m > 0$, $R_m(\mathscr{A}_{ij})$ (or just R_m) will denote the set of elements $\theta \in \mathscr{L}$ which satisfy the following functional relation:

$$(P) \qquad \theta(V_j X) = q_j^{-m} X_j^{-2m} \theta(X) \qquad j = 1, 2, \cdots, g\,.$$

Note that if $\theta(X) = \sum b_I X^I \in R_m$ and $V_j^I = \prod_{t=1}^{g} \mathscr{A}_{jt}^{i_t}$ it follows from the relation (P) that the b_I's satisfy:

$$(P') \qquad b_I V_j^I q_j^m = b_{I+2m\delta_j} \qquad j = 1, 2, \cdots, g$$

where $\delta_j = (0, \cdots, 0, \underset{(j)}{1}, 0, \cdots, 0)$

THEOREM I.1.1. *Let $m > 0$ and $\mathscr{L} = \oplus_{(r)} \mathscr{L}^{(r)}$ be the $2m$-parity decomposition of $\mathscr{L}$. If $R_m^{(r)} = R_m \cap \mathscr{L}^{(r)}$, then:*

1) *$R_m^{(r)}$ is a 1-dimensional k-vector space.*
2) *$R_m = \oplus_{(r)} R_m^{(r)}$ and $\dim_k R_m = (2m)^g$*
3) *$R = \oplus_0^\infty R_m$ is a graded k-algebra with $R_0 = k$.*

Proof. Suppose $\sum b_I X^I \in R_m^{(r)}$. Using the relation (P') we see that b_I determines $b_{I'}$ for $I \equiv I'$ mod. $2m$. Thus dim. $R_m^{(r)} \leq 1$. To complete the proof of 1) we exhibit a generator of $R_m^{(r)}$. Take representatives of r_j in $\boldsymbol{Z}$ and by abuse of language call them r_j too. If $i_j = 2mt_j + r_j$, set

$$b_I = \prod_{j=1}^{g} q_j^{t_j(mt_j + r_j)} \prod_{j>\ell} \mathscr{A}_{j\ell}^{i_j t_\ell + r_\ell t_j}$$

and let $b_I = 0$ if $I \not\equiv (r)$ mod. $2m$. Set $\varphi(X) = \sum b_I X^I$.

A calculation shows that the b_I satisfy (P'). Also

$$\begin{aligned} \text{ord. } b_I &= \sum_j t_j(mt_j + r_j) \text{ ord. } q_j + \sum_{j>\ell} (r_j t_\ell + r_\ell t_j + 2mt_j t_\ell) \text{ ord. } \mathscr{A}_{j\ell} \\ &= m \sum_{j,\ell} t_j t_\ell \text{ ord. } \mathscr{A}_{j\ell} + \sum_{j,\ell} r_j t_\ell \text{ ord. } \mathscr{A}_{j\ell} \end{aligned}$$

Since the matrix (ord. $\mathscr{A}_{ij}$) is positive definite, $\varphi \in \mathscr{L}$ and 1) is proved. 2) and 3) are obvious.

The decomposition of R_m in the Theorem is called the $2m$-parity decomposition of R_m and R is called the graded ring of Theta functions associated to the matrix $(\mathscr{A}_{ij})$.

There is a relation between the graded rings $R(\mathscr{A}_{ij})$ and $R(\mathscr{A}_{ij}^n)$, $n > 0$, that we shall make constant use of. Namely:

$$\text{(a)} \qquad \theta \in R_m(\mathscr{A}_{ij}) \Rightarrow \theta \in R_{mn}(\mathscr{A}_{ij}^n)$$
$$\text{(b)} \qquad \theta \in R_m(\mathscr{A}_{ij}^n) \Rightarrow \theta(X^n) \in R_{mn}(\mathscr{A}_{ij}) \; .$$

These are easily verified. Using (a) together with Theorem I. 1.1. we get:

PROPOSITION I.1.2. *If n is a fixed positive integer, $S_m = R_{mn}(\mathscr{A}_{ij}^n)$ is a k-vector space of dimension $(2mn)^g$, $S = \oplus_0^\infty S_m$ is a graded k-algebra, $R_m \subseteq S_m$ and R is a subring of S.*

Next using (b) with m replaced by mn we see that $\theta(X) \to \theta(X^n)$ defines a graded homomorphism $S \to R$ of degree n^2. The restriction of this map to R is a graded endomorphism of R of degree n^2. Both of these maps will be denoted by α_n. A dimension count shows that $\alpha_n(S)$ consists precisely of those elements of R that can be written as Laurent series in X_j^n, $j = 1, 2, \cdots, g$.

THEOREM I.1.3. *R is integral over $\alpha_n(R)$.*

Proof. We first show that S is integral over R. Let $\theta \in S_m$. For $1 \leq i \leq g$ let $T_i(\theta) = q_i^m X_i^{2m} \theta(V_i X)$. Then:

$$\begin{aligned} T_i(\theta)(V_i^n X) &= q_i^m (q_i^n X_i)^{2m} \theta(V_i^n(V_i X)) \\ &= (q_i^m X_i^{2m} q_i^{2mn})(q_i^{-mn^2}(q_i X_i)^{-2mn})\theta(V_i X) = q_i^{-mn^2} X_i^{-2mn}) T_i(\theta) \; . \end{aligned}$$

Thus $T_i(\theta) \in S_m$ for $i = 1, 2, \cdots, g$ and we have defined operators $T_i : S_m \to S_m$. An easy induction shows that $T_i^\ell(\theta)(X) = q_i^{m\ell^2} X_i^{2m\ell} \theta(V_i^\ell X)$, for all ℓ. Thus T_i^n is the identity map on S_m. Also

$$(T_i \circ T_j)(\theta) = T_i(q_j^m X_j^{2m} \theta(V_j X)) = q_i^m X_i^{2m} q_j^m \mathscr{A}_{ij}^{2m} X_j^{2m} \theta(V_j V_i X) \; .$$

Since this is symmetric in i and j, the T_i commute.

For each i, the various $T_i : S_m \to S_m$ fit together to give a graded automorphism of S which we also denote by T_i. Let T be the finite group generated by the automorphisms T_i. By the definition of T_i, R is the subring of invariants of S under T. So, S is integral over R and $\alpha_n(S)$ over $\alpha_n(R)$. It remains to show that every $\theta \in R$ is integral over $\alpha_n(S)$. We may assume that θ is in some R_{mn} and has a definite n-parity. But then θ^n is a Laurent series in the X_i^n, lies in $\alpha_n(S)$, and the theorem is proved.

Now let E be the $g \times g$ matrix all of whose entries are 1. Then the $2g \times 2g$ matrix $\begin{pmatrix} \mathscr{A}_{ij} & E \\ E & \mathscr{A}_{ij} \end{pmatrix}$ clearly satisfies the Riemann conditions. Let R' be the graded ring of theta-functions attached to this matrix. We shall label the Laurent series variables by $X_1, \cdots, X_g, Y_1, \cdots, Y_g$ instead of $X_1, \cdots, X_{2g}$. Then a Laurent series $\theta(X, Y)$ is in R'_m if and only if:

$$(1) \qquad \theta(V_jX, Y) = q_j^{-m} X_j^{-2m} \theta(X, Y)$$

$$(2) \qquad \theta(X, V_jY) = q_j^{-m} Y_j^{-2m} \theta(X, Y) .$$

In particular, if θ and φ are elements of R_m, then $\theta(X)\varphi(Y)$ is in R'_m and we get a map $R_m \otimes_k R_m \to R'_m$.

PROPOSITION I.1.4. *The above map is bijective; thus R' is the 2-fold Segré product of R with itself over k.*

Proof. Injectivity is clear. To prove ontoness it suffices to construct elements of pre-assigned $2m$-parity in the image of $R_m \otimes R_m$. This may be done by taking $\theta(X)\varphi(Y)$ where θ and φ have the desired $2m$-parities.

The following proposition is the key to the construction of a group law on $A = \mathrm{Proj.}\,(R)$.

PROPOSITION I.1.5. *If $\theta \in R'_m$ then $\theta'(X, Y) = \theta(XY, XY^{-1}) \in R'_{2m}$. $\theta \to \theta'$ defines a graded endomorphism β of R' of degree 2. $\beta \circ \beta$ maps θ to $\theta(X^2, Y^2)$ and R' is integral over $\beta(R')$.*

Remark. $\theta(XY, XY^{-1})$ is shorthand for

$$\theta(X_1Y_1, \cdots, X_gY_g, X_1Y_1^{-1}, \cdots, X_gY_g^{-1}) .$$

Proof.

$$\theta'(V_jX, Y) = \theta(V_jXY, V_jXY^{-1}) = q_j^{-m}(X_jY_j)^{-2m} q_j^{-m}(X_jY_j^{-1})^{-2m}\theta .$$

Since $(X_jY_j)(X_jY_j^{-1}) = X_j^2$ we get the first functional equation for θ'. Similarly, using the fact that $(XY)(X^{-1}Y) = Y^2$ we get the second, and $\theta' \in R'_{2m}$. We see at once that β is a degree 2 endomorphism and that $\beta \circ \beta = \alpha_2$. By Theorem I.1.3, with R replaced by R', R' is integral over $\beta(R')$.

For technical reasons connected with characteristic 2 we shall also need a 4-fold Segré product. The $4g \times 4g$ matrix which has 4 copies of $(\mathscr{A}_{ij})$ down its diagonal and all 1's elsewhere satisfies the Riemann conditions. Let R'' be the corresponding graded ring of theta-functions. Label the Laurent series variables by $X_1, \cdots, X_g, Y_1, \cdots, Y_g, Z_1, \cdots, Z_g, T_1, \cdots, T_g$. The proof of Proposition I.1.4, gives:

PROPOSITION I.1.6. *The natural map* $R_m \otimes R_m \otimes R_m \otimes R_m \to R''_m$ *is bijective and* R'' *is the* 4*-fold Segré product of* R *with itself over* k.

PROPOSITION I.1.7. *If* $\theta \in R''_m$ *then*

$$\theta''(X, Y, Z, T) = \theta(XYZ, XZ^{-1}T, XY^{-1}T^{-1}, YZ^{-1}T^{-1}) \in R''_{3m} .$$

$\theta \to \theta''$ *defines a degree* 3 *graded endomorphism* η *of* R''. $\eta \circ \eta = \alpha_3$ *and* R'' *is integral over* $\eta(R'')$.

Proof. Similar to that of Proposition I.1.5 and based on the identities:

$$\begin{aligned}
(XYZ)(XZ^{-1}T)(XY^{-1}T^{-1}) &= X^3 \\
(XYZ)(X^{-1}YT)(YZ^{-1}T^{-1}) &= Y^3 \\
(XYZ)(X^{-1}ZT^{-1})(Y^{-1}ZT) &= Z^3 \\
(XZ^{-1}T)(X^{-1}YT)(Y^{-1}ZT) &= T^3 .
\end{aligned}$$

Remark. The proof of Proposition I.1.5 essentially rests on the fact that $A \circ A^t = 2I$ where A is the matrix $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. Similarly, Proposition I.1.7 uses the fact that $B \circ B^t = 3I$ where

$$B = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & -1 & 1 \\ 1 & -1 & 0 & -1 \\ 0 & 1 & -1 & -1 \end{bmatrix} .$$

§ I.2. Finite generation of R

In this section we show that the graded ring of theta functions is a finitely generated algebra over k. In the course of the proof stronger results are obtained, namely:

(1) if char. $k \neq 2$, R_2 generates R_{2m} for large m.

(2) if char. $k \neq 3$, R_3 generates R_{3m} for large m.

LEMMA I.2.1. *The elements of R_1 have no common zero in G_g.*

Proof. Let $q_j = \mathscr{A}_{jj}$; by extending k we may assume $q_j = b_j^2$ with $b_j \in k^*$. If $I = (i_1, \cdots, i_g)$, $i_j = 2mt_j + r_j$, let

$$C_I = \prod_{j=1}^{g} b_j^{i_j^2} \cdot \prod_{r>s} \mathscr{A}_{rs}^{i_r i_s} .$$

and set $\varphi(X) = \sum C_I X^I$.

Since $\operatorname{ord.} C_I = \frac{1}{2} \sum_j i_j^2 \operatorname{ord.} q_j + \sum_{r>s} i_r i_s \operatorname{ord.} \mathscr{A}_{rs}$ and the matrix $(\operatorname{ord.} \mathscr{A}_{ij})$ is positive definite, $\varphi \in \mathscr{L}$. Clearly we have:

$$C_{I+\delta_j} = C_I \cdot b_j^{2i_j+1} \prod_{s \neq j} \mathscr{A}_{sj}^{i_s} .$$

Thus

$$\left(\prod_{s=1}^{g} \mathscr{A}_{js}^{i_s}\right) C_I = b_j^{-1} C_{I+\delta_j} ,$$

and

$$\varphi(V_j X) = b_j^{-1} X_j^{-1} \varphi(X) \qquad j = 1, 2, \cdots, g .$$

Let $\theta(X, Y) = \varphi(XY)\varphi(XY^{-1})$. The proof of Proposition I.1.5 shows that $\theta \in R_1'$. So θ is in the image of $R_1 \otimes R_1$. Now suppose all the elements of R_1 vanish at some point $x \in G_g$. Then $\theta(x, Y) = 0$, so $\varphi(xY) \cdot \varphi(xY^{-1}) = 0$. But $\mathscr{L}$ is an integral domain and $\varphi \neq 0$, so the lemma follows.

THEOREM I.2.2. *Let $m > 0$. Then the elements of R_m which are power series in X_i^m have no common zero in G_g.*

Proof. Let x be any element of G_g. By Lemma I.2.1 there is a $\theta \in R_1(\mathscr{A}_{ij}^m)$ such that $\theta(x^m) \neq 0$. Then by the remark preceding Proposition I.1.2. $\theta(X^m) \in R_m(\mathscr{A}_{ij})$ and does not vanish at x.

Let $n > 0$. We assume for now that char. k does not divide n and the group U_n of n-th roots of unity is contained in k. Recall that $S_m = R_{mn}(\mathscr{A}_{ij}^n)$.

For $m > 0$ and $u = (u_1, \cdots, u_g) \in U_n^g$ let $R_{m,u}$ denote the set of elements $\theta \in \mathscr{L}$ satisfying the following functional relation:

$$\theta(V_j X) = u_j q_j^{-m} X_j^{-2m} \theta(X) \qquad j = 1, 2, \cdots, g$$

PROPOSITION I.2.3. *Let n, U_n and S_m be as above. Then each $R_{m,u}$ is a subspace of S_m of dimension $(2m)^g$ and $S_m = \bigoplus_{(u)} R_{m,u}$, $(u) \in U_n^g$.*

Proof. Let $T_i : \mathscr{L} \to \mathscr{L}$ be the operators of Theorem I.1.3. If $\theta \in R_{m,u}$ then $T_i(\theta) = u_i \theta$ and $T_i^n(\theta) = \theta$. By the proof of Theorem I.1.3, S_m is the subspace of $\mathscr{L}$ fixed by the T_i^n, so $R_{m,u} \subset S_m$. Also the $R_{m,u}$ are just the subspaces of S_m corresponding to the various irreducible representations of the group T. So $S_m = \bigoplus_{(u)} R_{m,u}$. The proof that $\dim R_{m,u} = (2m)^g$ is similar to that of Theorem I.1.1. We omit it.

PROPOSITION I.2.4. *With the same notation as above, the elements of $R_{m,u}$ of pre-assigned n-parity have no common zero in G_g.*

Proof. Let $(r) = (r_1, \cdots, r_g)$ be a given n-parity. Suppose $\theta \in R_n$ with trivial n-parity. By extending k we can get $C_j \in k^*$ such that

$$C_j^{2n} = \left(\prod_{t=1}^{g} \mathscr{A}_{jt}^{r_t}\right) \cdot u_j^{-1} \qquad j = 1, 2, \cdots, g\ .$$

If $(C) = (C_1, \cdots, C_g)$, set $\varphi(X) = (\prod_{j=1}^{g} X_j^{r_j}) \cdot \theta(CX)$. Then $\varphi(V_j X) = (\prod_{t=1}^{g} \mathscr{A}_{jt}^{r_t} X_t^{r_t}) q_j^{-n} (C_j X_j)^{-2n} \theta(CX)$ and it follows that $\varphi \in R_{n,u}$ with n-parity (r).

The zeroes of φ are just translates of the zeroes of θ by C^{-1}. But, by Theorem I.2.2, the $\theta \in R_m$ with trivial n-parity have no common zero.

COROLLARY I.2.5. *If m is a multiple of n, the elements of $R_{m,u}$ of pre-assigned n-parity have no common zero in G_g.*

Proof. If (r) is the given n-parity and $x \in G_g$, choose $\theta_1 \in R_n$ with trivial n-parity such that $\theta_1(x) \neq 0$ and $\theta_2 \in R_{n,u}$ with n-parity (r) such that $\theta_2(x) \neq 0$. If $m = np$, $\theta_1^{p-1} \theta_2 \in R_{m,u}$ and has n-parity (r).

The following simple lemma will be used to prove the finite generation of R.

LEMMA I.2.6. *Let M be a graded algebra over a field k. Assume: $M_m = 0$ for all negative m, M_m is finite dimensional over k for all m and there is a polynomial P such that* $\dim M_m = P(m)$ *for all large m. Then, if M_1 generates M_m for infinitely many m, it generates M_m for all large m.*

Proof. Let $\tilde{M}$ be the subalgebra of M generated by M_1 and $\tilde{P}$ be the Hilbert polynomial of $\tilde{M}_m$. By assumption, $M_m = \tilde{M}_m$ for infinitely many m. Thus P and $\tilde{P}$ are equal at infinitely many m, $P = \tilde{P}$ and $\dim M_m = \dim \tilde{M}_m$ for large m.

Suppose now that we are in the situation of Proposition I.2.3 with $n = 2$. In other words, we assume that char. $k \neq 2$.

PROPOSITION I.2.7. *If* char. $k \neq 2$ *and* $n = 2$, *then* S_1 *generates* S_m *for all large* m.

Proof. It suffices to show that each $\theta \in S_{2t}$ is in $S_t \cdot S_t$. For then S_1 generates S_{2r} for all r and we can use Lemma I.2.6.

By Proposition I.2.3 we may assume $\theta \in R_{2t,u}$ for some $u \in U_2^g$, and that θ has a definite 2-parity. Choose $\theta_1 \in R_{2t,u}$ with the same 2-parity as θ so that $\theta_1(1) \neq 0$. (see Cor. I.2.5). Let $\varphi(X, Y) = \theta(XY)\theta_1(XY^{-1})$. It is easy to see that $\varphi \in R'_{4t}$. Since θ and θ_1 have the same 2-parity, φ is a power series in X_i^2, Y_i^2 and therefore is in $\alpha_2(S_t) \otimes \alpha_2(S_t)$, (cf. remark after Proposition I.1.2). Thus,

$$\varphi(X, X) = \theta_1(1)\theta(X^2) = \theta_1(1)\alpha_2(\theta) \in \alpha_2(S_t)\cdot\alpha_2(S_t)\,; \qquad \theta \in S_t \cdot S_t$$

and we are done.

THEOREM I.2.8. *If* char. $k \neq 2$, $R_2(\mathscr{A}_{ij})$ *generates* $R_{2m}(\mathscr{A}_{ij})$ *for all large* m, *and the graded subring* $R_{(2)} = \bigoplus_0^\infty R_{2m}$ *of the ring of theta functions is a finitely generated* k*-algebra.*

Proof. By extending k we may assume $\mathscr{A}_{ij} = b_{ij}^2$ with $b_{ij} \in k^*$ and $b_{ij} = b_{ji}$. Since $S_m(b_{ij}) = R_{2m}(\mathscr{A}_{ij})$, the first part comes from Prop. I.2.7, and the second part follows.

THEOREM I.2.9. *If* char. $k \neq 2$, *the ring* R *of theta functions is a finitely generated* k*-algebra.*

Proof. Since multiplication by a non-zero element of R_1 gives an isomorphism of the $R_{(2)}$-module $\bigoplus_0^\infty R_{2m+1}$ with an ideal in $R_{(2)}$, $\bigoplus_0^\infty R_{2m+1}$ is a finite $R_{(2)}$-module. So R is a finite $R_{(2)}$-module and a finitely generated k-algebra.

We now treat the case of characteristic 2. More generally we suppose that char. $k \neq 3$. We take $n = 3$ and assume temporarily that $U_3 \subset k$.

PROPOSITION I.2.10. *With the assumptions above, S_1 generates S_m for all large m.*

Proof. As in the proof of Prop. I.2.7, it suffices to show that each $\theta \in S_{3t}$ is in $S_t \cdot S_t \cdot S_t$. We may assume that $\theta \in R_{3t,u}$ and has a definite 3-parity. Choose $\theta_1 \in R_{3t,u}$ with the same 3-parity as θ so that $\theta_1(1) \neq 0$. Choose $\theta_2 \in R_{3t}$ with trivial 3-parity so that $\theta_2(1) \neq 0$. Set

$$\varphi(X, Y, Z, T) = \theta(XYZ)\theta_1(XZ^{-1}T)\theta_1(XY^{-1}T^{-1})\theta_2(YZ^{-1}T^{-1}) .$$

It is easily seen that $\varphi \in R''_{9t}$ and is a power series in $X_i^3, Y_i^3, Z_i^3, T_i^3$, so it lies in the image of $\alpha_3(S_t) \otimes \alpha_3(S_t) \otimes \alpha_3(S_t) \otimes \alpha_3(S_t)$. Then $\varphi(X, X, X, 1) = \theta_1^2(1)\theta_2(1)\theta(X^3)$ is in $\alpha_3(S_t) \cdot \alpha_3(S_t) \cdot \alpha_3(S_t)$ and so $\theta \in S_t \cdot S_t \cdot S_t$.

THEOREM I.2.11. *If* char. $k \neq 3$ *then $R_3(\mathscr{A}_{ij})$ generates $R_{3m}(\mathscr{A}_{ij})$ for all large m, and $\oplus_0^\infty R_{3m}$ is a finitely generated k-algebra.*

Proof. By extending k we may assume that $U_3 \subset k$ and that $\mathscr{A}_{ij} = b_{ij}^3$ with $b_{ij} \in k^*$ and $b_{ij} = b_{ji}$. Since $S_m(b_{ij}) = R_{3m}(\mathscr{A}_{ij})$, the result follows from Prop. I.2.10.

Imitating the proof of Theorem I.2.9, we have:

THEOREM I.2.12. *If* char. $k \neq 3$, *the ring R of theta functions is a finitely generated k-algebra.*

Finally, by Theorem I.2.9 and Theorem I.2.12, R is a finitely generated k-algebra no matter what the characteristic of the field k is.

§ I.3. The structure of Proj. (R)

Let R be the graded ring of theta functions associated with the matrix $(\mathscr{A}_{ij})$, let A denote the scheme Proj. (R) and A_k the set of its k-valued points. Let Γ be the multiplicative subgroup of G_g generated by the column vectors of $(\mathscr{A}_{ij})$. In this section we show that A is an abelian variety of dimension g over k and construct a canonical homomorphism $\varphi: G_g/\Gamma \to A_k$.

Let x be any element of G_g. By Lemma I.2.1, there is a $\theta \in R_1$ such that $\theta(x) \neq 0$. Thus we have an evaluation homomorphism $\varphi_x: R_\theta \to k$ which induces a morphism φ_x: Spec. $(k) \to$ Spec. (R_θ). This gives us a k-valued point P_x of A. P_x depends only on the class of x modulo Γ, and we have defined a function:

$$\begin{aligned} \varphi: G_g/\Gamma &\to A_k \\ x &\to P_x \,. \end{aligned}$$

The following standard facts will be needed later on.

LEMMA I.3.1. *Let $N \subset M$ be graded rings with M integral over N. Then the open sets* Spec. (M_n), $n \in N_i$, $i > 0$, *cover* Proj. (M) *and the maps* Spec. $(M_n) \to$ Spec. (N_n) *piece together to give a morphism* Proj. (M) $\to$ Proj. (N).

LEMMA I.3.2. *Let M and N be graded algebras and φ_1, φ_2*: Proj. (M) $\to$ Proj. (N) *morphisms. Suppose further that φ_1 and φ_2 have the same restrictions to* Spec. (M_n) *for some $n \in M_r$, $r > 0$, and M is a domain. Then $\varphi_1 = \varphi_2$.*

We are now ready to interpret the results of the last two sections geometrically.

THEOREM I.3.3. *Let $\beta: R' \to R'$ be the map $\theta(X, Y) \to \theta(XY, XY^{-1})$. Then*:

(1) *R' is integral over $\beta(R')$.*
(2) *$A' =$ Proj. (R') is the scheme theoretic product $A \times A$ of A with itself over k.*
(3) *β induces a morphism $\beta^*: A \times A \to A \times A$.*
(4) *The map $A_k \times A_k \to A_k \times A_k$ induced by β^* takes (P_x, P_y) to $(P_{xy}, P_{xy^{-1}})$.*

Proof. Assertions (1) and (2) come from Propositions I.1.5 and I.1.4. Lemma I.3.1 and (1) give a morphism $A' \to A'$ induced by β. Since A' identifies with $A \times A$ we get the morphism β^* of (3), and (4) follows from the definition of β.

With the notations above let:

1) $m: A \times A \longrightarrow A$ be the morphism $A \times A \xrightarrow{\beta^*} A \times A \xrightarrow{\pi_1} A$ where π_1 is projection on the first factor.
2) $-1_A: A \to A$ be the morphism induced by the automorphism $\theta(X) \to \theta(X^{-1})$ of R.
3) $O_A: A \longrightarrow A$ be the morphism $A \longrightarrow$ Spec. $(k) \xrightarrow{e} A$ where e is the k-valued point $P_{(1,\ldots,1)}$.

THEOREM I.3.4. *With the operations defined above A is a commuta-*

tive group scheme over k. *The map* $\varphi: G_g/\Gamma \to A_k$ *constructed at the beginning of this section is a group homomorphism.*

Proof (In outline). To show that A is a commutative group scheme we must verify the commutativity of certain diagrams expressing the associative and commutative law, and the existence of a unit and inverse. For example, for associativity we must show that the morphisms $m \circ (\mathrm{id}_A \times m)$ and $m \circ (m \times \mathrm{id}_A)$ from $A \times A \times A \to A$ are the same. To do this we choose affine open subsets U and V on $A \times A \times A$ and A such that $m \circ (\mathrm{id} \times m)$ and $m \circ (m \times \mathrm{id})$ take U into V. An obvious but tedious calculation shows that the two induced maps $\Gamma(V) \to \Gamma(U)$ coincide and we apply Lemma I.3.2 (for a more detailed proof of a similar result see Theorem I.3.5). Finally, (4) of Theorem I.3.3 shows that $m: A_k \times A_k \to A_k$ takes (P_x, P_y) to P_{xy}: i.e. that $x \to P_x$ is a homomorphism.

THEOREM I.3.5. *For each* $n > 0$ *the map* $\alpha_n^*: A \to A$ *induced by* α_n *is just group scheme multiplication by* n (*which we will denote by* n_A).

Proof. Since R is integral over $\alpha_n(R)$, we get a morphism of schemes $\alpha_n^*: A \to A$. We show first that if θ and θ' are in R'_m then the pull-back of $\theta'/\theta \in \Gamma((A \times A)_\theta)$ under $\alpha_n^* \times \mathrm{id}$ is $\theta'(X^n, X)/\theta(X^n, X)$, at least on some principal open subset U of $A_{\theta(X^n, X)}$.

To see this, take $\psi \neq 0$ in R_m. Since $R'_m = R_m \otimes R_m$, direct calculation shows that the pull-back of $\theta/\psi(X)\psi(Y)$ under $\alpha_n^* \times$ id. is $\theta(X^n, X)/\psi(X^n)\psi(X)$. Since a similar formula holds for the pull-back of $\theta'/\psi(X)\psi(Y)$, we get our result where U is defined by $\psi(X^n)\psi(X)$.

The theorem can now be proved by induction on n. $n = 1$ is obvious. $(n+1)_A$ is the composite map

$$\pi_1 \circ \beta^* \circ (n_A \times \mathrm{id.}): A \to A \times A \to A \times A \to A\ .$$

Fix $G \neq 0$ in R_1 and suppose $F \in R_m$. Then F/G^m in $\Gamma(A_G)$ pulls back to $F(X)G(Y)^m/G(X)^m G(Y)^m$ under π_1 and this pulls back to $F(XY)G(XY^{-1})^m/G(XY)^m G(XY^{-1})^m$ under β^*. By induction, $(n_A \times \mathrm{id}) = (\alpha_n^* \times \mathrm{id})$. If we apply the result of the paragraph above with $\psi = G^{2m}$, we conclude that the pull-back of F/G^m under $(n+1)_A = \pi_1 \circ \beta^* \circ (\alpha_n^* \times \mathrm{id.})$ is $F(X^{n+1})/G(X^{n+1})^m$ over the affine subset of A defined by $G(X^{n+1})G(X^{n-1})G(X^n)G(X)$. The theorem then follows from Lemma I.3.2 applied to the maps α_{n+1} and $(n+1)_A$.

THEOREM I.3.6. *The scheme $A = \mathrm{Proj.}\,(R)$ is an abelian variety of dimension g over k.*

Proof. From Theorem I.3.4, A has the structure of commutative group scheme over k. Since R is a finitely generated k-algebra and an integral domain, A is of finite type, reduced and irreducible. If L is a finite extension of k, let $R(L)$ be the graded L-algebra corresponding to the matrix $(\mathscr{A}_{ij})$ over the field L. Then $R \otimes_k L \simeq R(L)$ and is a domain. Hence, A remains reduced and irreducible under finite extensions of k, and since it is projective, it is an abelian variety. Since $\dim. R_m = (2m)^g$ for all $m > 0$, A has dimension g.

II

In this part we show that the map $\varphi: G_g/\Gamma \to A_k$ defined in § I.3 is an isomorphism provided the elements off the main diagonal of the matrix $(\mathscr{A}_{ij})$ are units in the valuation ring $\mathcal{O}$. *Throughout part II we make this assumption on the $\mathscr{A}_{ij}$'s.* Note that $q_i = \mathscr{A}_{ii} \in \mathscr{M}$ because of positive definiteness.

§ II.1. The reduction of A

Let $R = \oplus_0^\infty R_m$ be the graded ring of theta functions associated to the matrix $(\mathscr{A}_{ij})$. If m is a positive integer, let $R_{m,\mathcal{O}}$ denote the subspace of R_m consisting of Laurent series with coefficients in $\mathcal{O}$. The $2m$-parity decomposition $R_m = \oplus_{(r)} R_m^{(r)}$, $r_j \in \boldsymbol{Z}/2m\boldsymbol{Z}$, induces a decomposition $R_{m,\mathcal{O}} = \oplus_{(r)} R_{m,\mathcal{O}}^{(r)}$ where $R_{m,\mathcal{O}}^{(r)} = R_m^{(r)} \cap R_{m,\mathcal{O}}$. Let $\bar{R}_m = R_{m,\mathcal{O}}/\mathscr{M}R_{m,\mathcal{O}}$, $\bar{R} = \oplus_0^\infty \bar{R}_m$. Then $\bar{R}_m$ is a direct sum of 1-dimensional subspaces $\bar{R}_m^{(r)} = R_{m,\mathcal{O}}^{(r)}/\mathscr{M}R_{m,\mathcal{O}}^{(r)}$ over $\bar{k}$.

There is an obvious map $R_{m,\mathcal{O}} \to \bar{k}[X_i, X_i^{-1}]$ given by $\sum \mathscr{A}_I X^I \to \sum \bar{\mathscr{A}}_I X^I$. The kernel is evidently $\mathscr{M}\cdot R_{m,\mathcal{O}}$, so $\bar{R}_m$ identifies with a subspace of $\bar{k}[X_i, X_i^{-1}]$. We now calculate what this subspace is. Rather than taking r_j to be elements of $\boldsymbol{Z}/2m\boldsymbol{Z}$ we shall take r_j to be integers with $-m < r_j \leq m$. Then, by Theorem I.1.1, every $\theta \in R_{m,\mathcal{O}}$ may be written as $\sum b_I X^I$ where

$$b_I = \prod_{j=1}^{g} q_j^{t_j(mt_j+r_j)} \prod_{j>\ell} \mathscr{A}_{j\ell}^{i_\ell t_j + r_j t_\ell} \cdot b_{(r)}$$

where $b_{(r)} \in \mathcal{O}$, $I = (i_1, \cdots, i_g)$ and $i_j = 2mt_j + r_j$.

Now each $\mathscr{A}_{j\ell}$ $(j \neq \ell)$ has order 0. Also $t_j(mt_j + r_j) \geq 0$ and equality holds only when $t_j = 0$ or when $t_j = -1$ and $r_j = m$. Thus the reduction $\sum \bar{b}_I X^I$, of θ only involves monomials with $|i_j| \leq m$. In particular the monomials X^I appearing in a generator of $\bar{R}_m^{(r)}$ are just those for which the following conditions hold:

$$\begin{aligned} i_j &= r_j && \text{whenever} \quad |r_j| < m \\ i_j &= \pm m && \text{whenever} \quad r_j = m \,. \end{aligned}$$

PROPOSITION II.1.1. *$\bar{R}_2$ generates $\bar{R}_{2m}$ for all $m > 0$.*

Proof. It suffices to show that $\bar{R}_1\bar{R}_m = \bar{R}_{m+1}$ for all $m > 1$. If $\bar{R}_{m+1} = \oplus_{(r)} \bar{R}_{m+1}^{(r)}$ is the $2(m+1)$-parity decomposition of $\bar{R}_{m+1}$ it suffices to construct a non-zero element of $\bar{R}_1\bar{R}_m$ of arbitrary $2(m+1)$-parity $(r) = (r_1, \cdots, r_g)$, $-(m+1) < r_j \leq (m+1)$. We argue by induction on $\sum |r_j|$, and define numbers c_j and d_j by:

$$\begin{aligned} &c_j = 0, \quad d_j = r_j && \text{if } |r_j| < m \\ &c_j = 1 && \text{if } r_j = m, \ -m, \ m+1 \\ &d_j = m-1, \ 1-m, \ m && \text{if } r_j = m, \ -m, \ m+1 \,. \end{aligned}$$

Let $\bar{\theta}_c$ generate $\bar{R}_1^{(c)}$ and $\bar{\theta}_d$ generate $\bar{R}_m^{(d)}$. The monomials X^I appearing in $\bar{\theta}_c\bar{\theta}_d$ are just those for which:

$$\begin{aligned} &i_j = r_j && \text{whenever} \quad |r_j| < m \\ &i_j = m \text{ or } m-2 && \text{whenever} \quad r_j = m \\ &i_j = -m \text{ or } 2-m && \text{whenever} \quad r_j = -m \\ &i_j = \pm(m+1) \text{ or } \pm(m-1) && \text{whenever} \quad r_j = m+1 \,. \end{aligned}$$

In particular, a generator $\bar{\theta}_r$ of $\bar{R}_{m+1}^{(r)}$ occurs as a component of $\bar{\theta}_c\bar{\theta}_d$. By induction it will suffice to show that every other $\bar{\theta}_s$ occurring in $\bar{\theta}_c\bar{\theta}_d$ has $\sum |s_j| < \sum |r_j|$. Now X^s must appear in $\bar{\theta}_c\bar{\theta}_d$. So by the above, either $s_j = r_j$, or $|r_j| \geq m$ and $s_j = \pm(m-2)$ or $\pm(m-1)$. If $(s) \neq (r)$, we are in this latter case for at least one index j. Since $m > 1, |m-2| < |m|, |s_j| < |r_j|, \sum |s_j| < \sum |r_j|$ and the proposition is proved.

The above result and Nakayama's Lemma show that $R_{2,\mathscr{O}}$ generates $R_{2m,\mathscr{O}}$ for all m. So the graded ring $R_{(2)} = \oplus_0^\infty R_{2m}$ is generated by R_2. Let $\hat{R}_2$ be the space of linear maps $R_2 \to k$. Then we may identify A_k with a Zariski-closed subset of the projectification of $\hat{R}_2$. The linear maps $i: R_2 \to k$ which correspond to points of A_k are those which can be extended to k-algebra maps $R_{(2)} \to k$. If $x \in G_g$ then P_x corresponds to the evaluation map $\theta \to \theta(x)$.

For $P \in A_k$, the corresponding element of $\hat{R}_2$ will be denoted by i_P. We shall normalize i_P so that $i_P(R_{2,\mathcal{O}}) = \mathcal{O}$. It is still, of course, only determined up to multiplication by a unit of $\mathcal{O}$.

We next define bases θ_α and λ_α, of $R_{2,\mathcal{O}}$ and $R_{1,\mathcal{O}}$, that we shall make constant use of. Namely, if $\alpha_j \in \{-1, 0, 1, 2\}$ let θ_α be a generator of $R_{2,\mathcal{O}}^{(\alpha)}$. If $\alpha_j \in \{0, 1\}$, let λ_α be a generator of $R_{1,\mathcal{O}}^{(\alpha)}$. The monomials X^I appearing in $\bar{\theta}_\alpha$ are just those for which:

$$\begin{array}{lll} i_j = \alpha_j & \text{whenever} & \alpha_j = 0, 1 \quad \text{or} \quad -1 \\ i_j = \pm 2 & \text{whenever} & \alpha_j = 2 \,. \end{array}$$

The monomials X^I appearing in $\bar{\lambda}_\alpha$ are just those for which:

$$\begin{array}{lll} i_j = 0 & \text{whenever} & \alpha_j = 0 \\ i_j = \pm 1 & \text{whenever} & \alpha_j = 1 \,. \end{array}$$

If $P \in A_k$, let $X_\alpha(P) = i_P(\theta_\alpha)$. The $X_\alpha(P)$ are projective coordinates for P. Since the θ_α are a basis for $R_{2,\mathcal{O}}$ and i_P is normalized, the $X_\alpha(P)$ are in $\mathcal{O}$, but not all in $\mathcal{M}$.

Now let $\bar{A} = \text{Proj.}\,(\bar{R})$ and $\bar{A}_{\bar{k}}$ be the set of $\bar{k}$-valued points of $\bar{A}$. Since $\bar{R}_2$ generates $\bar{R}_{(2)}$ we may identify $\bar{A}_{\bar{k}}$ with a Zariski-closed subset of the projectification of $\hat{\bar{R}}_2$. Let $i_{\bar{P}}$ be the map corresponding to $\bar{P}$. For $\bar{P} \in \bar{A}_{\bar{k}}$, $X_\alpha(\bar{P}) = i_{\bar{P}}(\bar{\theta}_\alpha)$ give projective coordinates for $\bar{P}$.

Each normalized $i_p : R_2 \to k$ gives by reduction a non-zero map $\bar{R}_2 \to \bar{k}$. Thus we get a reduction mapping $P \to \bar{P}$ from A_k to $\bar{A}_{\bar{k}}$. If P has projective coordinates $\{X_\alpha(P)\}$, those of $\bar{P}$ are $\{\overline{X_\alpha(P)}\}$.

§ II.2. A stratification on $\bar{A}$

To simplify notation let $\theta_0 = \theta_{0,\cdots,0}$ and $\theta_j = \theta_{0,\cdots,\underset{(j)}{1},\cdots,0}$ for $j = 1, 2, \cdots, g$. We may assume that the reductions of $\theta_0, \theta_1, \theta_2, \cdots, \theta_g$ are $1, X_1, X_2, \cdots, X_g$ respectively. Let x_j denote the rational function $\bar{\theta}_j / \bar{\theta}_0$ $j = 1, 2, \cdots, g$ on $\bar{A}$. Since $\bar{\theta}_\alpha$ is a polynomial in X_i and X_i^{-1} with coefficients in $\bar{k}$, the rational function $\bar{\theta}_\alpha / \bar{\theta}_0$ on $\bar{A}$ is given by $\sum c_I x^I$, $c_I \in \bar{k}^*$ where the sum extends over all $(i_1, \cdots, i_g)$ such that

$$\begin{array}{ll} i_j = \alpha_j & \text{if} \quad \alpha_j = 0, 1, \text{ or } -1 \\ i_j = \pm 2 & \text{if} \quad \alpha_j = 2 \,. \end{array}$$

THEOREM II.2.1. *For each* $\bar{P} \in \bar{A}_{\bar{k}}$ *there is a unique subset* $S = S(\bar{P})$ *of* $\{1, 2, \cdots, g\}$ *such that*:

$$\text{(1)} \qquad \textit{if} \quad \alpha^{-1}(2) = S, \quad \textit{then} \quad X_\alpha(\bar{P}) \neq 0$$

$$\text{(2)} \qquad \textit{if} \quad \alpha^{-1}(2) \not\supset S, \quad \textit{then} \quad X_\alpha(\bar{P}) = 0 \; .$$

Proof. The uniqueness of $S(\bar{P})$ is obvious. To prove the existence, let $(\mathcal{O}_v, \mathcal{M}_v)$ be a valuation ring dominating the local ring $(\mathcal{O}_{\bar{P}}, \mathcal{M}_{\bar{P}})$ of $\bar{P}$ on $\bar{A}$. Let v be the order function attached to the ring $\mathcal{O}_v$.

With $x_j = \bar{\theta}_j/\bar{\theta}_0$, let $S = \{j : v(x_j) \neq 0\}$. Writing $\bar{\theta}_\alpha/\bar{\theta}_0$ as $\sum c_I x^I$ with $c_I \in \bar{k}^*$ we see:

$$(*) \qquad v(c_I x^I) = \sum_{j=1}^{g} i_j v(x_j) \geq \sum_{j \in S} 2 \min . \, (v(x_j), v(x_j^{-1}))$$

$$(**) \qquad v(\bar{\theta}_\alpha/\bar{\theta}_0) \geq \sum_{j \in S} 2 \min . \, (v(x_j), v(x_j^{-1})) \; .$$

If $\alpha^{-1}(2) = S$, there is exactly one term x^I such that the equality in (*) holds, so strict equality holds in (**). Suppose now that for some α with $\alpha^{-1}(2) = S$, $X_\alpha(\bar{P}) = 0$. Let $\beta = (\beta_1, \cdots, \beta_g)$ be such that $X_\beta(\bar{P}) \neq 0$. Then the rational function $\bar{\theta}_\alpha/\bar{\theta}_\beta$ is in $\mathcal{M}_{\bar{P}} \subset \mathcal{M}_v$. Since $\alpha^{-1}(2) = S$, the above calculation shows that:

$$v(\bar{\theta}_\alpha/\bar{\theta}_\beta) = v(\bar{\theta}_\alpha/\bar{\theta}_0) - v(\bar{\theta}_\beta/\bar{\theta}_0) \leq 0$$

which is a contradiction, and (1) follows.

In order to prove (2), note that if $\alpha^{-1}(2) \not\supset S$, we have strict inequality in (**). Now let β be such that $\beta^{-1}(2) = S$. By (1), $X_\beta(\bar{P}) \neq 0$ and so the rational function $\bar{\theta}_\alpha/\bar{\theta}_\beta \in \mathcal{O}_{\bar{P}}$. Since $\alpha^{-1}(2) \not\supset S$, the above calculation shows that $v(\bar{\theta}_\alpha/\bar{\theta}_\beta) > 0$ and so $\bar{\theta}_\alpha/\bar{\theta}_\beta \in \mathcal{M}_v$. Therefore $\bar{\theta}_\alpha/\bar{\theta}_\beta \in \mathcal{M}_{\bar{P}} = \mathcal{M}_v \cap \mathcal{O}_{\bar{P}}$ and (2) follows.

THEOREM II.2.2. *Let* $i_{\bar{P}} : \bar{R}_2 \to \bar{k}$ *be the map associated to* $\bar{P} \in \bar{A}_{\bar{k}}$ *and let* $S = S(\bar{P})$. *Then*:

$$\text{(1)} \qquad \alpha^{-1}(1) = S \Rightarrow i_{\bar{P}}(\bar{\lambda}_\alpha^2) \neq 0$$

$$\text{(2)} \qquad \alpha^{-1}(1) \not\supset S \Rightarrow i_{\bar{P}}(\bar{\lambda}_\alpha^2) = 0 \; .$$

Proof. $\bar{\lambda}_\alpha^2/\bar{\theta}_0 = (\sum d_I x^I)^2$, $d_I \in \bar{k}^*$ with $i_j = 0$ when $\alpha_j = 0$, $i_j = \pm 1$ when $\alpha_j = 1$, and $x_j = \bar{\theta}_j/\bar{\theta}_0$.

It follows that:

$$v(\bar{\lambda}_\alpha^2/\bar{\theta}_0) \geq \sum_{j \in S} 2 \min . \, (v(x_j), v(x_j^{-1}))$$

with equality if $\alpha^{-1}(1) = S$ and strict inequality if $\alpha^{-1}(1) \not\supset S$.

To prove (1) suppose $\alpha_i \in \{0, 1\}$ with $\alpha^{-1}(1) = S$. Choose $\beta_i \in \{-1, 0, 1, 2\}$ so that $\beta^{-1}(2) = S$. By Th. II.2.1, $\bar{\lambda}_\alpha^2/\bar{\theta}_\beta \in \mathcal{O}_{\bar{P}}$. Furthermore:

$$v(\bar{\lambda}_\alpha^2/\bar{\theta}_\beta) = v(\bar{\lambda}_\alpha^2/\bar{\theta}_0) - v(\bar{\theta}_\beta/\bar{\theta}_0) = 0 .$$

Thus $\bar{\lambda}_\alpha^2/\bar{\theta}_\beta$ is a unit in $\mathcal{O}_{\bar{P}}$ and (1) follows.

Similarly, if $\alpha^{-1}(1) \not\supset S$, $\bar{\lambda}_\alpha^2/\bar{\theta}_\beta \in \mathcal{O}_{\bar{P}} \cap \mathcal{M}_v = \mathcal{M}_{\bar{P}}$ and (2) follows.

Suppose now $P \in A_k$ with reduction $\bar{P}$. *By the support $S(P)$ of P we mean the set $S(\bar{P})$ of Theorem* II.2.1. We conclude this section with some remarks which we will use constantly.

(a) $P \in A_k$ has empty support if and only if $X_0(P)$ is a unit.
(b) Suppose $y = (y_1, \cdots, y_g) \in G_g$ with $|\text{ord. } y_j| \leq \frac{1}{2} \text{ord. } q_j$. Then $S(\varphi(y)) = \{j : \text{ord. } y_j \neq 0\}$
(c) $\lambda_\alpha(X) = \sum b_I X^I$ where $i_j = 2t_j + \alpha_j$ and $\text{ord. } b_I = \sum_j t_j(t_j + \alpha_j) \text{ ord. } q_j$
(d) $\theta_\alpha(X) = \sum b_I X^I$ where $i_j = 4t_j + \alpha_j$ and $\text{ord. } b_I = \sum_j t_j(2t_j + \alpha_j) \text{ ord. } q_j$.

(a) is immediate from the definitions of $S(P)$. We call such points unit points; in the next section we study them carefully. We get (c) and (d) by specifying m to be 1 or 2 in the remarks before Prop. II.1.1. To prove (b) we use:

LEMMA II.2.3. *Let $0 \neq q \in \mathcal{M}$ and $y \in k^*$ with $|\text{ord. } y| \leq \frac{1}{2} \text{ord. } q$. Let $\alpha \in \{0, 1\}$, $t \in \mathbf{Z}$ and set $s = t(t + \alpha) \text{ ord. } q + (2t + \alpha) \text{ ord. } y$. Then:*
(1) *if $\alpha = 0$, $s \geq 0$*
(2) *if $\alpha = 1$, $s \geq -|\text{ord. } y|$. For ord. $y > 0$ (respectively ord. $y < 0$) equality occurs if and only if $t = -1$ (respectively $t = 0$).*

Proof. (1) is trivial. In order to prove (2) note that if ord. $y \geq 0$ then $s \geq (2(t + 1)^2 - 1) \text{ ord. } y$, and if ord. $y < 0$, $s \geq (2t^2 - 1)|\text{ord. } y|$.

LEMMA II.2.4. *Suppose $y = (y_1, \cdots, y_g) \in G_g$ with $|\text{ord. } y_j| \leq \frac{1}{2} \text{ord. } q_j$. Let $S = \{j : \text{ord. } y_j \neq 0\}$. Suppose $\alpha_j \in \{0, 1\}$. Then:*

$$(*) \qquad \text{ord. } \lambda_\alpha(y) \geq -\sum_{j \in S} |\text{ord. } y_j| .$$

Furthermore, equality holds if $\alpha^{-1}(1) = S$ and inequality holds if $\alpha^{-1}(1) \not\supset S$.

Proof. By (c), $\lambda_\alpha(y) = \sum b_I y^I$ where

$$\text{ord.}\ (b_I y^I) = \sum_{j=1}^{g} s_j = \sum_{j=1}^{g} t_j(t_j + \alpha_j)\ \text{ord.}\ q_j + (2t_j + \alpha_j)\ \text{ord.}\ y_j\ .$$

So by Lemma II.2.3, ord. $(b_I y^I) \geq -\sum_{j\in S} |\text{ord.}\ y_j|$ giving (*). Suppose now that $\alpha^{-1}(1) = S$. Then there is precisely one monomial $b_I y^I$ in $\lambda_\alpha(y)$ such that ord. $(b_I y^I) = -\sum_{j\in S} |\text{ord.}\ y_j|$ (whenever ord. $y_j = 0$, $t_j = 0$. When ord. $y_j > 0$, $t_j = -1$ and when ord. $y_j < 0$, $t_j = 0$). Thus equality holds in (*). Finally, if $\alpha^{-1}(1) \not\supset S$, there is an index j such that $\alpha_j = 0$ and ord. $y_j \neq 0$. Then, $s_j \geq 0 > -|\text{ord.}\ y_j|$ and the last assertion follows.

Remark (b) is an immediate consequence of Lemma II.2.4 and Theorem II.2.2. (note that $i_P(\lambda_\alpha^2) = \lambda_\alpha(y)^2$ up to multiplication by a non-zero constant independent of α).

§ II.3. The unit points of A_k

Let U denote the multiplicative group of units of the ring $\mathcal{O}$ and U_k be the set of unit points of A_k (i.e. points with empty support). In this section we show that φ induces a bijection $U^g \to U_k$. The injectivity of $\varphi: G_g/\Gamma \to A_k$ follows easily.

Let $P \in U_k$. We shall normalize the coordinates of P so that $X_0(P) = 1$. Then $X_\alpha(P) \in \mathcal{O}$ for all $\alpha: \{1, 2, \cdots, g\} \to \{-1, 0, 1, 2\}$. Furthermore, if $P \in A_k$ and α is such that $\alpha^{-1}(2) = \varnothing$, then $X_\alpha(P) \in U$. In particular $X_1(P), \cdots, X_g(P)$ are in U. (here $X_j = X_{0,\ldots,\underset{(j)}{1},\ldots,0}$).

THEOREM II.3.1. *The restriction of the canonical map $\varphi: G_g/\Gamma \to A_k$ to U^g is a bijection of U^g with U_k.*

Proof. If $x \in U^g$, it follows from remark (b) of § II.2. that $\varphi(x) \in U_k$. In order to prove bijectivity, it is enough to show the following:

(1) $\psi: U^g \to U^g$; $x \to (\theta_1(x)/\theta_0(x), \cdots, \theta_g(x)/\theta_0(x))$ is 1-1 and onto.

(2) Two unit points with the same values of $X_1, \cdots, X_g$ must be equal.

We proceed to prove (1) and (2). We may normalize the θ_i so that $\theta_0 = 1 + \cdots$, and $\theta_j = X_j + \cdots$. Then ψ is "close to the identity" so (1) is intuitively clear. To give a rigorous proof, suppose $u = (u_1, \cdots, u_g) \in U^g$. Let $T: U^g \to U^g$ be the map $x \to x - \psi(x) + u$. It suffices to show that T has a unique fixed point.

Let $r = \min.\ (\text{ord.}\ q_j)$. If $x, y \in U^g$ set ord. $(x - y) = \min.\text{ord.}\ (x_j - y_j)$. We know that $\theta_0(X) = \sum C_I X^I$ where $i_j = 4t_j$ and ord. $C_I = \sum 2t_j^2$ ord. q_j. So if $I \neq (0, \cdots, 0)$, ord. $C_I \geq r$. It follows that if $x, y \in U^g$:

(a) $$\text{ord.}\,(\theta_0(x) - \theta_0(y)) \geq \text{ord.}\,(x - y) + r\,.$$

Let $\theta_j^*(X) = \theta_j(X) - X_j\theta_0(X)$. A similar calculation gives:

(b) $$\text{ord.}\,(\theta_j^*(x) - \theta_j^*(y)) \geq \text{ord.}\,(x - y) + r\,.$$

Now the difference between the j'th coordinate of $T(x)$ and of $T(y)$ is $\theta_j^*(x)/\theta_0(x) - \theta_j^*(y)/\theta_0(y)$. Using (a), (b) and the fact that $\theta_0(x)$ and $\theta_0(y)$ are units, we see that this has ord. $\geq$ ord. $(x - y) + r$. So T is a contraction mapping. Since k is complete, so is U^g, and T has a unique fixed point.

To prove (2) note that for any α, $(\bar{\theta}_0)^{2g-1}(\prod_{i=1}^g (\bar{\theta}_i)^2)\bar{\theta}_\alpha$ is an element of $\bar{R}_{8g}$ which only contains terms X^I with $0 \leq i_j \leq 4$. So we may write:

$$(\bar{\theta}_0)^{2g-1}\left(\prod_{i=1}^{g} (\bar{\theta}_i)^2\right)\bar{\theta}_\alpha = \bar{F}_\alpha(\bar{\theta}_0, \bar{\theta}_1, \cdots, \bar{\theta}_g)$$

where $\bar{F}_\alpha$ is a homogeneous polynomial of degree $4g$ with coefficients in $\bar{k}$. Lift $\bar{F}_\alpha$ to a homogeneous F_α with coefficients in $\mathcal{O}$. Then $\theta_\alpha^{2g-1}(\prod_{i=1}^g \theta_i^2)\theta_\alpha$ and $F_\alpha(\theta_0, \theta_1, \cdots, \theta_g)$ differ by an element of $\mathcal{M}R_{8g,\mathcal{O}}$. Since $R_{2,\mathcal{O}}$ generates $R_{8g,\mathcal{O}}$ we have:

$$\theta_0^{2g-1}\left(\prod_{i=1}^{g} \theta_i^2\right)\theta_\alpha = F_\alpha(\theta_0, \theta_1, \cdots, \theta_g) + CG_\alpha(\theta_\beta)$$

where $C \in \mathcal{M}$ and may be taken independent of α, and each G_α has coefficients in $\mathcal{O}$. From this we deduce polynomial identities that hold on all A. Namely suppose $P \in A_k$ with $X_0(P) = 1$. Then:

(*) $$\left(\prod_{i=1}^{g} X_i(P)^2\right)X_\alpha(P) = f_\alpha(X_1(P), \cdots, X_g(P)) + Cg_\alpha(X_\beta(P))$$

where f_α, g_α have coefficients in $\mathcal{O}$. Suppose now that P and Q are unit points with $X_j(P) = X_j(Q)$. Then $X_\alpha(P)$ and $X_\alpha(Q)$ are in $\mathcal{O}$ and each $X_j(P)$ is a unit. (*) and an easy induction show that $X_\alpha(P) \equiv X_\alpha(Q) \bmod C^n$ for all n. So $X_\alpha(P) = X_\alpha(Q)$ and $P = Q$.

THEOREM II.3.2. *$\varphi\colon G_g/\Gamma \to A_k$ is injective.*

Proof. Suppose $\varphi(x) = \varphi(1) = P$. Modifying x by an element of Γ we may assume $x = (x_1, \cdots, x_g)$ with $|\text{ord.}\,x_j| \leq \frac{1}{2}\,\text{ord.}\,q_j$. Now P is a unit point. So by remark (b) of § II.2 each ord. $x_j = 0$ and $x \in U^g$. By the theorem above, $x = 1$.

§ II.4. An addition formula

THEOREM II.4.1. *Suppose $Q, R \in A_k$ with disjoint supports. Then $S(QR) = S(Q) \cup S(R)$.*

The proof of this result will occupy the rest of this section. It is based on an *addition formula*, Theorem II.4.6, which plays a central role in this paper. Recall that A' is the abelian variety attached to the $2g \times 2g$ matrix with two copies of $(\mathscr{A}_{ij})$ down its diagonal and ones elsewhere. We identify $\{1, 2, \cdots, 2g\}$ with the disjoint union of two copies of $\{1, 2, \cdots, g\}$ in the obvious way. Then a map $\alpha: \{1, 2, \cdots, 2g\} \to \{0, 1\}$ may be thought of as a pair of maps β and $\gamma: \{1, 2, \cdots, g\} \to \{0, 1\}$. Under the identification of R_1' with $R_1 \otimes R_1$, $\lambda_\alpha(X, Y)$ corresponds to $\lambda_\beta(X)\lambda_\gamma(Y)$, and similarly for R_2' and $\theta_\alpha(X, Y)$. If $P \in A_k'$, $S(P)$ may be thought of as a subset of the disjoint union of two copies of $\{1, 2, \cdots, g\}$. On the other hand P identifies with some $(Q, R) \in A_k \times A_k$ and we have:

LEMMA II.4.2. *$S(P)$ is the disjoint union of $S(Q)$ in the first copy of $\{1, 2, \cdots, g\}$ and $S(R)$ in the second.*

Proof. $i_P(\lambda_{\beta,\gamma}(X, Y)) = i_Q(\lambda_\beta) i_R(\lambda_\gamma)$. The result follows easily from Theorem II.2.2. applied to A'.

LEMMA II.4.3. *Let $Q, R \in A_k$. Suppose there is a subset S of $\{1, 2, \cdots, g\}$ such that*

$$\text{ord. } i_{(Q,R)}(\lambda_\beta(XY)\lambda_\gamma(XY^{-1})) \geq 0$$

for all $\beta, \gamma: \{1, 2, \cdots, g\} \to \{0, 1\}$, with equality if $\beta^{-1}(1) = \gamma^{-1}(1) = S$ and inequality if $\beta^{-1}(1) \not\supset S$ or $\gamma^{-1}(1) \not\supset S$. Then $S(QR) = S$.

Proof. $i_{(QR, QR^{-1})}(\lambda_\beta(X)\lambda_\gamma(Y)) = i_{(Q,R)}(\lambda_\beta(XY)\lambda_\gamma(XY^{-1}))$. So if the hypotheses of the lemma hold, Theorem II.2.2 applied to A' shows that the support of (QR, QR^{-1}) is the disjoint union of two copies of S. By Lemma II.4.2, $S(QR) = S(QR^{-1}) = S$.

LEMMA II.4.4. *Suppose the monomial $X^\delta Y^\eta$ appears in $\lambda_\beta(XY) \cdot \lambda_\gamma(XY^{-1})$. Then:*

$$(*) \quad \begin{cases} \textit{whenever} \quad \beta_j = \gamma_j \textit{ both } \delta_j \textit{ and } \eta_j \textit{ are even} \\ \textit{whenever} \quad \beta_j \neq \gamma_j \textit{ both } \delta_j \textit{ and } \eta_j \textit{ are odd} \end{cases}$$

$$\begin{cases} \textit{whenever} \quad \gamma_j = 0 \ , \ \delta_j \equiv \eta_j \ \mathrm{mod.}\ 4 \\ \textit{whenever} \quad \gamma_j = 1 \ , \ \delta_j \not\equiv \eta_j \ \mathrm{mod.}\ 4 \end{cases}$$

Proof. $\lambda_\beta(XY)\lambda_\gamma(XY^{-1})$ is a sum of monomials of the form $X^{m+n}Y^{m-n}$ with $m_j \equiv \beta_j$ mod. 2 and $n_j \equiv \gamma_j$ mod. 2. The result follows.

LEMMA II.4.5. *Suppose we are given $\beta_j, \gamma_j, \delta_j, \eta_j$ such that β_j and γ_j are in $\{0, 1\}$, δ_j and η_j are in $\{0, \pm 1, 2\}$, and* (*) *of Lemma* II.4.4 *is satisfied. Then the coefficient of $X^\delta Y^\eta$ in $\lambda_\beta(XY)\lambda_\gamma(XY^{-1})$ is (unit) $(\prod_j q_j)$ where j runs over all indices such that $\delta_j = \eta_j = 2$.*

Proof. Let $\lambda_\beta(X) = \sum b_I X^I$ and $\lambda_\gamma(X) = \sum C_J X^J$. The coefficient we are studying is just $b_{(\delta+\eta)/2} C_{(\delta-\eta)/2}$. (*) shows that $(\delta_j + \eta_j)/2 \equiv \beta_j$ mod. 2, and that $(\delta_j - \eta_j)/2 \equiv \gamma_j$ mod. 2. Also $(\delta_j + \eta_j)/2$ and $(\delta_j - \eta_j)/2$ are both in $\{0, \pm 1\}$ except for the single exceptional case $\delta_j = \eta_j = (\delta_j + \eta_j)/2 = 2$. The result now follows from remark (c) of § II.2.

THEOREM II.4.6. $\lambda_\beta(XY)\lambda_\gamma(XY^{-1}) = \sum_{\delta,\eta} C_{\delta,\eta}\theta_\delta(X)\theta_\eta(Y)$. *Here δ and η range over all maps $\{1, \cdots, g\} \to \{0, \pm 1, 2\}$ satisfying* (a) *and* (b) *below, and $C_{\delta,\eta} =$ (unit) $(\prod q_j)$, the product ranging over all j such that $\delta_j = \eta_j = 2$.*

(a) *whenever $\beta_j = \gamma_j$ then δ_j and η_j are in $\{0, 2\}$. They are equal when $\gamma_j = 0$ and unequal when $\gamma_j = 1$.*

(b) *whenever $\beta_j \neq \gamma_j$ then δ_j and η_j are in $\{-1, 1\}$. They are equal when $\gamma_j = 0$ and unequal when $\gamma_j = 1$*

Proof. $\lambda_\beta(XY)\lambda_\gamma(XY^{-1}) \in R_2'$ and so may be written as $\sum_{\delta,\eta} C_{\delta,\eta}\theta_\delta(X) \cdot \theta_\eta(Y)$. Lemma II.4.4 shows that only δ and η satisfying (a) and (b) can occur in this decomposition. Comparing coefficients of $X^\delta Y^\eta$ and using Lemma II.4.5 we get the result.

Taking every β_j and γ_j equal to 1 in Theorem II.4.6 we get:

THEOREM II.4.7.

$$\lambda_{1,\ldots,1}(XY)\lambda_{1,\ldots,1}(XY^{-1}) = \sum_\alpha C_\alpha \theta_{2-\alpha}(X)\theta_\alpha(Y)$$

where α ranges over all maps $\{1, 2, \cdots, g\} \to \{0, 2\}$ and the C_α are units.

We now prove Theorem II.4.1. Suppose $S(Q) \cap S(R) = \varnothing$, and let $S = S(Q) \cup S(R)$. It suffices to show that the hypotheses of Lemma II.4.3 are satisfied. So, by Theorem II.4.6 we must show that $\sum C_{\delta,\eta} X_\delta(Q) X_\eta(R)$

is a unit when $\beta^{-1}(1) = \gamma^{-1}(1) = S$ and is in $\mathscr{M}$ when $\beta^{-1}(1) \not\supset S$ or $\gamma^{-1}(1) \not\supset S$.

Suppose first that $\beta^{-1}(1) = \gamma^{-1}(1) = S$. For $j \in S(Q)$ let $\delta_j = 2$ and $\eta_j = 0$, for $j \in S(R)$ let $\delta_j = 0$ and $\eta_j = 2$ and for $j \notin S$ let $\delta_j = \eta_j = 0$. Then δ, η satisfy the conditions of Theorem II.4.6 and $C_{\delta,\eta}X_\delta(Q)X_\eta(R)$ is a unit. Suppose we have any pair δ, η appearing in the expansion of $\lambda_\beta(XY)\lambda_\gamma(XY^{-1})$. If $X_\delta(Q)$ is to be a unit we must have $\delta_j = 2$ (and $\eta_j = 0$) for $j \in S(Q)$. If $X_\eta(R)$ is a unit, $\eta_j = 2$ (and $\delta_j = 0$) for $j \in S(R)$. Finally if $C_{\delta,\eta}$ is a unit, $\delta_j = \eta_j = 0$ for $j \notin S$. So $C_{\delta,\eta}X_\delta(Q)X_\eta(R)$ is a unit for a single pair and $\sum C_{\delta,\eta}X_\delta(Q)X_\eta(R)$ is a unit.

Suppose next that $\beta^{-1}(1) \not\supset S$. Take an index $j \in S$ such that $\beta_j = 0$. If $\gamma_j = 1$ then δ_j and η_j are in $\{\pm 1\}$ and $X_\delta(Q)X_\eta(R) \in \mathscr{M}$. If $\gamma_j = 0$ then either $\delta_j = \eta_j = 0$ so that $X_\delta(Q)X_\eta(R) \in \mathscr{M}$, or $\delta_j = \eta_j = 2$ so that $C_{\delta,\eta} \in \mathscr{M}$. Thus $\sum C_{\delta,\eta}X_\delta(Q)X_\eta(R) \in \mathscr{M}$. We argue similarly if $\gamma^{-1}(1) \not\supset S$.

§ II.5. The function θ_P

Let $P \in A_k$. Then $i_P : R_2 \to k$ induces a map $i_P \otimes 1 : R_2' = R_2 \otimes R_2 \to R_2$. If $\theta \in R_2'$ its image under $i_P \otimes 1$ is denoted by $(\theta \mid X = P)$. If $P = \varphi(x)$, then $(\theta(X, Y) \mid X = P)$ is just the Laurent series $\theta(x, Y)$.

We abbreviate $\lambda_{1,\dots,1}$ to λ_1 and let ψ be the element $\lambda_1(XY)\lambda_1(XY^{-1})$ of R_2'. *For $P \in A_k$ let $\theta_P = (\psi \mid X = P)$.* θ_P, like i_P, is determined up to multiplication by a unit in $\mathcal{O}$.

If $\theta \in R_2$ and $Q \in A_k$ we say that $\theta(Q) = 0$ if $i_Q(\theta) = 0$. Note that $\theta(\varphi(x)) = 0$ if and only if $\theta(x) = 0$. We shall need a simple result, Proposition II.5.2, concerning the zeroes of θ_P, which follows from:

LEMMA II.5.1. *$\theta_P(Q) = 0$ if and only if either $\lambda_1^2(PQ) = 0$ or $\lambda_1^2(PQ^{-1}) = 0$.*

Proof. (P, Q) and (PQ, PQ^{-1}) are in $A_k' = A_k \times A_k$ and so give homomorphisms $R'_{(2)} \to k$. $i_{(P,Q)} = i_P \otimes i_Q$ and $i_{(PQ,PQ^{-1})}\theta(X, Y) = i_{(P,Q)}\theta(XY, XY^{-1})$.

Thus:

$$\begin{aligned} i_{PQ}(\lambda_1^2)i_{PQ^{-1}}(\lambda_1^2) &= i_{(PQ,PQ^{-1})}(\lambda_1(X)^2\lambda_1(Y)^2) \\ &= i_{(P,Q)}(\psi^2) = (i_P \otimes i_Q)(\psi^2) = i_Q(\theta_P^2) \end{aligned}$$

and the result follows.

PROPOSITION II.5.2. *Suppose* $P, Q, R \in A_k$ *and* $\theta_P(R) = 0$. *Then, either* $\theta_{PQ^{-1}}(QR) = 0$ *or* $\theta_{PQ}((QR)^{-1}) = 0$.

We next study the Laurent expansion of θ_P.

PROPOSITION II.5.3. $\theta_P = \sum C_\alpha X_{2-\alpha}(P)\theta_\alpha$ *where* α *ranges over all maps* $\{1, 2, \cdots, g\} \to \{0, 2\}$ *and each* C_α *is a unit.*

Proof. Apply $i_P \otimes 1$ to both sides of Theorem II.4.7.

PROPOSITION II.5.4. *The reduction of* $\theta_P(Y)$ *is a non-zero polynomial in* Y_j *and* Y_j^{-1} $(1 \leq j \leq g)$, *which does not involve* Y_j *or* Y_j^{-1} *if* $j \in S(P)$.

Proof. If $\alpha: \{1, 2, \cdots, g\} \to \{0, 2\}$ is chosen so that $\alpha^{-1}(0) = S(P)$, then $X_{2-\alpha}(P)$ is a unit. So by Proposition II.5.3 $\bar{\theta}_P \neq 0$. Suppose now $j \in S(P)$. Then, if $\alpha_j = 0$, $\bar{\theta}_\alpha$ does not involve Y_j or Y_j^{-1} while if $\alpha_j = 2$, $X_{2-\alpha}(P) \in \mathscr{M}$. The result follows.

§ II.6. The decomposition theorem

Throughout this section *we assume* k *algebraically closed.* Our goal is the following "decomposition theorem": Suppose $P \in A_k$. Then $P = QR$ where $Q = \varphi(z, 1, \cdots, 1)$ for some $z \in k^*$ and $1 \notin S(R)$. We begin the proof with a criterion which guarantees that $1 \notin S(R)$. Suppose $R \in A_k$ and $(\bar{u}_2, \cdots, \bar{u}_g) \in (\bar{k}^*)^{g-1}$. We say that $(\bar{u}_2, \cdots, \bar{u}_g)$ is in $\bar{N}_R$ if there exists $u = (u_1, \cdots, u_g) \in U^g$ such that u_i lifts $\bar{u}_i$ for $i > 1$, and $\theta_R(u) = 0$.

PROPOSITION II.6.1. *If* $1 \in S(R)$, *then* $\bar{N}_R$ *is contained in a proper Zariski-closed subset of* $(\bar{k}^*)^{g-1}$.

Proof. Let $\bar{\theta}_R$ be the reduction of θ_R. By Proposition II.5.4, $\bar{\theta}_R$ is a non-zero polynomial in Y_j and Y_j^{-1} for $j > 1$. If $(\bar{u}_2, \cdots, \bar{u}_g) \in \bar{N}_R$ then $\bar{\theta}_R(\bar{u}_2, \cdots, \bar{u}_g) = 0$.

We next derive some simple results on the zeroes of power series and Laurent series in one variable.

LEMMA II.6.2. *Suppose* $H(X) = \sum_0^\infty \mathscr{A}_i X^i \in \mathscr{O}[[X]]$ *with* $\bar{H} \neq 0$ *and* $\mathscr{A}_0 \in \mathscr{M}$. *Then there exists an* $x \in \mathscr{M}$ *such that* $H(x) = 0$.

Proof. Let s be the smallest index such that $\mathscr{A}_s$ is a unit. By the Weierstrass Preparation Theorem, $H(X) = G \cdot (X^s - \sum_0^{s-1} C_i X^i)$ where G is a unit in $\mathscr{O}[[X]]$ and each $C_i \in \mathscr{M}$. Now k is algebraically closed and

x may be taken to be any root of $X^s - \sum_0^{s-1} C_i X^i$.

LEMMA II.6.3. *Let $\mathscr{L}_c$ be the ring of everywhere convergent Laurent series, $\sum_{-\infty}^{\infty} \mathscr{A}_i X^i$, with $\mathscr{A}_i \in \mathcal{O}$. Suppose $G \in \mathscr{L}_c$ with $\bar{G} \neq 0$. Then any root $\bar{x}$ of $\bar{G}$ in $\bar{k}^*$ lifts to a root of G in U.*

Proof. Let $x \in U$ be any lifting of $\bar{x}$. Replacing G by $G(xX)$ we may assume $\bar{x} = 1$. Let $\psi: \mathscr{L}_c \to \mathcal{O}[[Y]]$ be the homomorphism mapping X on $1 - Y$, and $H = \psi(G)$. Then $\bar{H} = \bar{G}(1 - Y) \neq 0$, and $\bar{H}(0) = 0$. By the lemma above, $H(y) = 0$ for some $y \in \mathscr{M}$, and $G(1 - y) = 0$.

The next result requires some notation. Suppose G is an everywhere convergent Laurent series in $X_0, X_1, \cdots, X_n$ and $u = (u_1, \cdots, u_n) \in U^n$. Let G_u be the 1-variable Laurent series $G(X, u_1, \cdots, u_g)$. If $g(X) = \sum b_I X^I$ is an everywhere convergent Laurent series let ord. $g = \min.(\text{ord. } b_I)$. Finally if $\bar{g}$ is a polynomial over $\bar{k}$ in X_j and $X_j^{-1} (1 \leq j \leq n)$ let $(U^n)_{\bar{g}} = \{u \in U^n : \bar{g}(\bar{u}) \neq 0\}$.

LEMMA II.6.4. *Suppose G is an everywhere convergent Laurent series in $X_0, \cdots, X_n$. Write $G = \sum_{-\infty}^{\infty} g_i(X_1, \cdots, X_n) X_0^i$ and suppose that for at least two indices i, $g_i \neq 0$. Then there exists a real number r and a $\bar{g} \neq 0$ such that whenever $u \in (U^n)_{\bar{g}}$ there exists a $y \in k^*$ with $G_u(y) = 0$ and* ord. $y = r$.

Proof. Let $d_i = \text{ord. } g_i$. We may assume $\min. d_i = 0$. Multiplying G by a power of X_0 and replacing X_0 by X_0^{-1} if necessary we may assume that $d_0 = 0$ and that $d_j \neq \infty$ for some positive j. Suppose first that $d_j = 0$ for some $j > 0$. Take $r = 0$ and $\bar{g} = \bar{g}_0 \bar{g}_j$. Then if $u \in (U^n)_{\bar{g}}$, $g_0(u)$ and $g_j(u)$ are units. So $G_u = \sum g_i(u) X^i$ has at least two unit coefficients, $\bar{G}_u$ has a root in $\bar{k}^*$ and G_u has a root with ord. $= 0$ by Lemma II.6.3. In general note that $d_i / i \to \infty$ with i. Let $r = -\min_{i>0} d_i / i$ and choose $C \in k^*$ with ord. $C = r$. Replacing G by $G(CX_0, X_1, \cdots, X_n)$ we reduce to the previously handled case.

We apply the above result to θ_P, where P is a given element of A_k.

PROPOSITION II.6.5. *There exists a real number r and an $\bar{h} \neq 0$ such that whenever $(u_2, \cdots, u_g) \in U^{g-1}$ with $\bar{h}(\bar{u}_2, \cdots, \bar{u}_g) \neq 0$, then there exists a $y \in k^*$ with $\theta_P(y, u_2, \cdots, u_g) = 0$ and* ord. $y = r$.

Proof. $\theta_P = \sum C_\alpha X_{2-\alpha}(P) \theta_\alpha$ and the $C_\alpha X_{2-\alpha}(P)$ do not all vanish. So if we write $\theta_P(X) = \sum_{-\infty}^{\infty} h_i(X_2, \cdots, X_g)X_1^i$ we find that $h_i \neq 0$ for all i in some congruence class mod. 4. Now apply Lemma II.6.4.

THEOREM II.6.6. *Suppose $P \in A_k$ with $1 \in S(P)$. Then $P = QR$ where $Q = \varphi(z, 1, \cdots, 1)$ for some $z \in k^*$, and $1 \notin S(R)$.*

Proof. Take r and $\bar{h}$ as in Proposition II.6.5. Choose $z \in k^*$ with ord. $z = -r$ and set $Q = \varphi(z, 1, \cdots, 1)$. Suppose that $\bar{u} = (\bar{u}_2, \cdots, \bar{u}_g) \in (\bar{k}^*)^{g-1}$ and $\bar{h}(\bar{u}) \neq 0$. We shall show that $\bar{u}$ is either in $\bar{N}_{PQ^{-1}}$ or in $(\bar{N}_{PQ})^{-1}$. It will follow from this that either $\bar{N}_{PQ^{-1}}$ or $\bar{N}_{PQ}$ is Zariski-dense. Replacing z by z^{-1} if necessary we can assume $\bar{N}_{PQ^{-1}}$ is dense. By Proposition II.6.1, $1 \notin S(PQ^{-1})$. Since $P = Q(PQ^{-1})$, the theorem will follow.

To show that $\bar{u}$ is either in $\bar{N}_{PQ^{-1}}$ or in $(\bar{N}_{PQ})^{-1}$ lift it to $(u_2, \cdots, u_g)$ in U^{g-1} and choose y as in Proposition II.6.5. Set $R = \varphi(y, u_2, \cdots, u_g)$. Then $\theta_P(R) = 0$. Now, since ord. $z = -r$, $(yz, u_2, \cdots, u_g)$ is in U^g and its image under φ is QR. Since $\theta_P(R) = 0$, Proposition II.5.2, shows that $\theta_{PQ^{-1}}(QR) = 0$ or $\theta_{PQ}((QR)^{-1}) = 0$. In the first case $\bar{u} \in \bar{N}_{PQ^{-1}}$, in the second case $(\bar{u})^{-1} \in \bar{N}_{PQ}$.

THEOREM II.6.7. *In the situation of Theorem* II.6.6, $S(Q) = \{1\}$ *and* $S(R) = S(P) - \{1\}$.

Proof. Q and R have disjoint supports so we may apply Theorem II.4.1.

§ II.7. φ is surjective

THEOREM II.7.1. *Suppose k is algebraically closed. Then $\varphi\colon G_g/\Gamma \to A_k$ is surjective.*

Proof. Suppose $P \in A_k$. We show that $P \in \operatorname{Im}(\varphi)$ arguing by induction on the cardinality of $S(P)$. If $S(P) = \varnothing$, Theorem II.3.1 shows that $P \in \varphi(U^g)$. If $S(P) \neq \varnothing$ we may assume $1 \in S(P)$. Since k is algebraically closed we may write $P = QR$ as in Theorem II.6.6. Theorem II.6.7 and induction conclude the proof.

We next show how to eliminate the hypothesis of algebraic closure.

LEMMA II.7.2. *Let $0 \neq q \in \mathcal{M}$ and $y \in k^*$ with $|$ord. $y| \leq \frac{1}{2}$ ord. q. Suppose $\alpha \in \{0, \pm 1, 2\}$, $t \in \boldsymbol{Z}$ and $s = t(2t + \alpha)$ ord. $q + (4t + \alpha)$ ord. y. Then:*

(1) *if $\alpha = 0, s \geq 0$*

(2) *if* $\alpha = \pm 1$, $s \geq -|\text{ord.}\, y|$. *If* $\alpha = -1$ *and* $\text{ord.}\, y > 0$, *or if* $\alpha = 1$ *and* $\text{ord.}\, y < 0$ *equality occurs only when* $t = 0$.

(3) *if* $\alpha = 2$, $s \geq -2\,|\text{ord.}\, y|$. *For* $\text{ord.}\, y > 0$ *equality occurs only when* $t = -1$. *For* $\text{ord.}\, y < 0$, *equality occurs only when* $t = 0$.

Proof. (1) is clear. To prove (2) and (3) note that $t(2t + \alpha) \geq 0$. Thus the results hold if $\text{ord.}\, y = 0$. If $\text{ord.}\, y > 0$, $s \geq (2t(2t + \alpha) + (4t + \alpha))$ $\text{ord.}\, y$, while if $\text{ord.}\, y < 0$, $s \geq (2t(2t + \alpha) - (4t + \alpha))\,|\text{ord.}\, y|$. The calculation is now straightforward.

LEMMA II.7.3. *Suppose* $y = (y_1, \cdots, y_g) \in G_g$ *with* $|\text{ord.}\, y_j| \leq \frac{1}{2}\, \text{ord.}\, q_j$. *Let* $S = \{j : \text{ord.}\, y_j \neq 0\}$. *Let* $\alpha : \{1, 2, \cdots, g\} \to \{0, 2\}$ *be the map such that* $\alpha^{-1}(2) = S$. *Then* $\text{ord.}\, \theta_\alpha(y) = -2 \sum_{j \in S} |\text{ord.}\, y_j|$.

Proof. By (d) of § II.2, $\theta_\alpha(y) = \sum b_I y^I$ where

$$\text{ord.}\, (b_I y^I) = \sum_{j=1}^{g} s_j = \sum_{j=1}^{g} (t_j(2t_j + \alpha_j)\, \text{ord.}\, q_j + (4t_j + \alpha_j)\, \text{ord.}\, y_j)\ .$$

By Lemma II.7.2, $s_j \geq -2\,|\text{ord.}\, y_j|$ for $j \in S$. Thus $\text{ord.}\, (b_I y^I) \geq -2 \sum_{j \in S} |\text{ord.}\, y_j|$. Also if equality is to hold we must have $t_j = 0$ for $j \notin S$, $t_j = -1$ when $\text{ord.}\, y_j > 0$, and $t_j = 0$ when $\text{ord.}\, y_j < 0$. So there is only one monomial for which equality holds, and the lemma follows.

LEMMA II.7.4. *Situation as in Lemma* II.7.3. *Suppose* $\text{ord.}\, y_1 \neq 0$. *Define* $\beta_j \in \{0, \pm 1, 2\}$ *by setting* $\beta_j = \alpha_j$ *if* $j > 1$, $\beta_1 = -1$ *if* $\text{ord.}\, y_1 > 0$ *and* $\beta_1 = 1$ *if* $\text{ord.}\, y_1 < 0$. *Then* $\text{ord.}\, \theta_\beta(y) = |\text{ord.}\, y_1| - 2 \sum_{j \in S} |\text{ord.}\, y_j|$.

Proof. Entirely similar to that of Lemma II.7.3.

THEOREM II.7.5. $\varphi : G_g/\Gamma \to A_k$ *is bijective.*

Proof. Theorem II.3.2 shows that φ is 1:1. To prove ontoness suppose $P \in A_k$. Let L be a complete algebraically closed extension of k. By Theorem II.7.1 there is a $y = (y_1, \cdots, y_g) \in (L^*)^g$ with $\varphi(y) = P$, and we may assume $|\text{ord.}\, y_j| \leq \frac{1}{2}\, \text{ord.}\, q_j$. Suppose $\text{ord.}\, y_1 \neq 0$. Define α and β as in Lemmas II.7.2 and II.7.3. Then

$$|\text{ord.}\, y_1| = \text{ord.}\, \theta_\beta(y) - \text{ord.}\, \theta_\alpha(y) = \text{ord.}\, (X_\beta(P)/X_\alpha(P))\ .$$

In particular there exists an $x_1 \in k^*$ such that $\text{ord.}\, x_1 = \text{ord.}\, y_1$. Similarly choose $x_j \in k^*$ so that $\text{ord.}\, x_j = \text{ord.}\, y_j$ and let $x = (x_1, \cdots, x_g)$. Then

$yx^{-1} \in U_L^q$, so $\varphi(yx^{-1})$ is a unit point. Since $\varphi(yx^{-1}) = P\varphi(x^{-1})$ it is in A_k. Thus $P\varphi(x^{-1}) \in \varphi(U_k^q)$ and $P \in \varphi(G_g)$.

III

In this part we show that the map $\varphi: G_g/\Gamma \to A_k$ is bijective assuming only that the matrix $(\mathscr{A}_{ij})$ is such that each ord. $\mathscr{A}_{ij}$ is rational. We do this by reducing to the diagonal case (cf. § II).

§ III.1. Isogenies

Let $(\mathscr{A}_{ij})$ be a $g \times g$ matrix with entries in k^* satisfying the Riemann conditions (i.e. $(\mathscr{A}_{ij})$ is symmetric and (ord. $\mathscr{A}_{ij}$) is positive definite). Let $S = (s_{ij})$ and $T = (t_{ij})$ be $g \times g$ matrices over $\boldsymbol{Z}$ such that $S \cdot T = nI$, $n \neq 0$ and let

$$b_{ij} = \prod_{k,\ell} \mathscr{A}_{k\ell}^{s_{ik}s_{j\ell}}$$

It is readily seen that the matrix (b_{ij}) also satisfies the Riemann conditions. Attached to the matrix $(\mathscr{A}_{ij})$ are the period vectors V_i, the group Γ, the graded ring $R(\mathscr{A}_{ij})$ of theta functions, the abelian variety A and the map $\varphi: G_g/\Gamma \to A_k$; similarly attached to (b_{ij}) we have W_i, $\Gamma', R(b_{ij}), B$ and $\varphi': G_g/\Gamma' \to B_k$.

The following identities are obvious:

$$\prod_j b_{ij}^{t_{rj}} = \prod_j \mathscr{A}_{rj}^{ns_{ij}} \tag{1}$$

$$\prod_{i,j} b_{ij}^{t_{ri}t_{rj}} = \mathscr{A}_{rr}^{n^2} . \tag{2}$$

Let $\lambda_1, \lambda_2: G_g \to G_g$ be the maps defined by:

$$\lambda_1(x) = (y_1^n, \cdots, y_g^n) \qquad \text{where} \qquad y_i = \prod_j x_j^{s_{ij}}$$

$$\lambda_2(x) = (z_1, \cdots, z_g) \qquad \text{where} \qquad z_i = \prod_j x_j^{t_{ij}} .$$

PROPOSITION III.1.1. *λ_1 maps Γ into Γ', λ_2 maps Γ' into Γ and the composition in either order is the map $x \to x^{n^2}$.*

Proof. The image of V_r under λ_1 is the vector whose i-th component is $\prod_j \mathscr{A}_{rj}^{ns_{ij}} = \prod_j b_{ij}^{t_{rj}}$. But this is just the vector $\prod_j W_j^{t_{rj}}$. Similarly $\lambda_2(W_r) = \prod_j V_j^{ns_{rj}}$. The last assertion is obvious.

For $\theta \in \mathscr{L}$ let $\psi_1(X) = \theta(Y_1^n, \cdots, Y_g^n)$ where $Y_i = \prod_j X_j^{s_{ij}}$ and $\psi_2(X) = \theta(Z_1, \cdots, Z_g)$ where $Z_i = \prod_j X_j^{t_{ij}}$.

PROPOSITION III.1.2. *If* $\theta \in R_m(b_{ij})$ *then* $\psi_1 \in R_{mn^2}(\mathscr{A}_{ij})$. *If* $\theta \in R_m(\mathscr{A}_{ij})$ *then* $\psi_2 \in R_{mn^2}(b_{ij})$. *Consequently* $\theta \to \psi_1$ (*resp.* $\theta \to \psi_2$) *gives a graded homomorphism of degree* $n^2\mu_1 : R(b_{ij}) \to R(\mathscr{A}_{ij})$ (*resp.* $\mu_2 : R(\mathscr{A}_{ij}) \to R(b_{ij})$), *and the composition* (*in either order*) *is the map* $\alpha_{n^2} : \theta(X) \to \theta(X^{n^2})$.

Proof. $\psi_1(V_rX) = \theta(Z_1^n, \cdots, Z_g^n)$ where $Z_i = \prod_j (\mathscr{A}_{rj}X_j)^{s_{ij}}$. It follows from (1) above that $Z_i^n = (\prod_j b_{ij}^{t_{rj}})Y_i^n$ and thus

$$(Z_1^n, \cdots, Z_g^n) = \Big(\prod_j W_j^{t_{rj}}\Big)(Y_1^n, \cdots, Y_g^n) .$$

Since $\theta \in R_m(b_{ij})$,

$$\psi_1(V_rX) = \Big(\prod_{i,j} b_{ij}^{t_{ri}t_{rj}}\Big)^{-m}\Big(\prod_i Y_i^{-2mnt_{ri}}\Big)\psi_1(X) .$$

By (2) this is just $\mathscr{A}_{rr}^{-mn^2}X_r^{-2mn^2}\psi_1(X)$, and so $\psi_1 \in R_{mn^2}(\mathscr{A}_{ij})$. Similarly for ψ_2. The other statements are obvious.

PROPOSITION III.1.3. *The homomorphisms of Proposition* III.1.2 *are finite and induce morphisms of group varieties* $\mu_1^* : A \to B$ *and* $\mu_2^* : B \to A$.

Proof. Since the composition (in either order) is the map α_{n^2} which is finite (cf. Theorem I.1.3), μ_1 and μ_2 are finite. So we get morphisms of varieties $A \to B$ and $B \to A$ which are readily seen to be group variety morphisms.

From Proposition III.1.3 we get homomorphisms $\mu_1^* : A_k \to B_k$ and $\mu_2^* : B_k \to A_k$. The composite map $A_k \to B_k \to A_k$ is the map induced by $\alpha_{n^2} : R(\mathscr{A}_{ij}) \to R(\mathscr{A}_{ij})$ which by Theorem I.3.5 is multiplication by n^2.

§ III.2. φ is bijective

PROPOSITION III.2.1. *There is a commutative diagram of maps*:

$$\begin{array}{ccccc} G_g/\Gamma & \xrightarrow{\lambda_1} & G_g/\Gamma' & \xrightarrow{\lambda_2} & G_g/\Gamma \\ \downarrow{\scriptstyle\varphi} & & \downarrow{\scriptstyle\varphi'} & & \downarrow{\scriptstyle\varphi} \\ A_k & \xrightarrow{\mu_1^*} & B_k & \xrightarrow{\mu_2^*} & A_k \end{array}$$

where the λ_i *are induced by the maps of Proposition* III.1.1.

Furthermore $(\lambda_2 \circ \lambda_1)(x) = x^{n^2}$ *and* $\mu_2^* \circ \mu_1^*$ *is just multiplication by* n^2.

Proof. The commutativity of the diagram follows in a straightforward way from the definition of the maps. The last assertions follow from Propositions III.1.1 and III.1.3.

Now we proceed to show that φ is bijective.

Let Λ be a subring of the reals, $\boldsymbol{R}$. We say that a $g \times g$ matrix $\mathscr{A}$ over $\boldsymbol{R}$ is Λ-diagonalizable if there exists an invertible matrix S_0 over Λ such that $S_0 \mathscr{A} S_0^t$ is diagonal. Let $\boldsymbol{Z}_\ell$ denote the localization (not the completion) of $\boldsymbol{Z}$ at the prime ℓ.

THEOREM III.2.2. *Let* $\alpha_{ij} = \text{ord.}\, \mathscr{A}_{ij}$ *and* $\mathscr{A}$ *be the matrix* (α_{ij}). *Suppose that* $\mathscr{A}$ *is* $\boldsymbol{Z}_\ell$*-diagonalizable for every prime* ℓ. *Then the map* $\varphi: G_g/\Gamma \to A_k$ *is bijective (for the matrix* $(\mathscr{A}_{ij})$*).*

Proof. Let S_0 be an invertible matrix over $\boldsymbol{Z}_\ell$ diagonalizing $\mathscr{A}$ and let $T_0 = S_0^{-1}$. Replacing S_0 and T_0 by integer multiples prime to ℓ we get matrices S and T over $\boldsymbol{Z}$ with $ST = nI$, $(n, \ell) = 1$ and $S \mathscr{A} S^t$ diagonal. Let b_{ij} be defined as in § III.1. Then the matrix (ord. b_{ij}) which is equal to $S\mathscr{A}S^t$, is diagonal. So by the main result of § II, the map φ' of Proposition III.2.1 is bijective.

Now let $x \in G_g/\Gamma$ be such that $\varphi(x) = 0$. Then by Proposition III.2.1, $\lambda_1(x) = 1$ and so $x^{n^2} = 1$. But n may be taken prime to any ℓ. Since the n^2 obtained in this way generate the unit ideal in $\boldsymbol{Z}$, $x = 1$. Similarly, if $P \in A_k$ let $P' = \mu_1^*(P)$. Then $P' \in \text{Im.}\, \varphi'$ and so $n^2 P \in \text{Im.}\, \varphi$. Since n may be choosen prime to any ℓ, $P \in \text{Im.}\, \varphi$ and the theorem is proved.

The following slight modification of Theorem III.2.2 will be useful later.

THEOREM III.2.3. *Suppose* $\alpha_{ij} = \text{ord.}\, \mathscr{A}_{ij} \in \boldsymbol{Z}$ *and generate the unit ideal. Suppose further there exist positive integers* $m_1, \cdots, m_s$ *such that* $\mathscr{A} \oplus \text{diag.}\, (m_1, \cdots, m_s)$ *is* $\boldsymbol{Z}_\ell$*-diagonalizable for every prime* ℓ. *Then* φ *is bijective (for the matrix* $(\mathscr{A}_{ij})$*).*

Proof. Since the α_{ij} generate the unit ideal, there exist $q \in k^*$ with ord. $q = 1$. Then the matrix

$$\left(\begin{array}{c|ccc} \mathscr{A}_{ij} & & 1 & \\ \hline & q^{m_1} & & 1 \\ 1 & & \ddots & \\ & 1 & & q^{m_s} \end{array}\right)$$

also satisfies the Riemann conditions and the corresponding order matrix is $\mathscr{A} \oplus \mathrm{diag.}\,(m_1, \cdots, m_s)$.

Let Γ_i be the subgroup of k^* generated by q^{m_i}, and E_i the corresponding elliptic curve. Then by Theorem III.2.2 the map

$$G_g/\Gamma \times k^*/\Gamma_1 \times \cdots \times k^*/\Gamma_s \to A_k \times (E_1)_k \times \cdots \times (E_s)_k$$

is bijective. Therefore φ is bijective too.

The following simple result will be proved in the appendix.

LEMMA. *Let (α_{ij}) be a symmetric matrix with entries in $\boldsymbol{Z}_\ell$. Then:*
1) *if $\ell \neq 2$, (α_{ij}) is $\boldsymbol{Z}_\ell$-diagonalizable.*
2) *if $\ell = 2$, there exist integers $m_1, \cdots, m_s$*
which are powers of 2 such that $(\alpha_{ij}) \oplus \mathrm{diag.}\,(m_1, \cdots, m_s)$ is $\boldsymbol{Z}_\ell$-diagonalizable.

Let $(\mathscr{A}_{ij})$ be our matrix satisfying the Riemann conditions. Combining the above lemma with Theorem III.2.3 we have:

COROLLARY 1. *If* $\mathrm{ord.}\,\mathscr{A}_{ij} \in \boldsymbol{Z}$ *and generate the unit ideal, then φ is bijective (for the matrix $(\mathscr{A}_{ij})$).*

COROLLARY 2. *If each* $\mathrm{ord.}\,\mathscr{A}_{ij}$ *is in $\boldsymbol{Q}$, or less generally, if the value group of the valuation is contained in $\boldsymbol{Q}$,then φ is bijective.*

Appendix Quadratic forms over $\boldsymbol{Z}_\ell$

Let R be a discrete valuation ring, M a finite free R-module and $(\ ,\ ): M \times M \to R$ a symmetric bilinear map. The following lemma is easy linear algebra.

LEMMA 1. *Let $n_1, \cdots, n_s \in M$ and N be the R-submodule generated by the n_i's. If* $\mathrm{det.}((n_i, n_j))$ *is a unit in R, then the n_i's are R-linearly independent and $M = N \oplus N^\perp$.*

We say that M is decomposable if $M = N \oplus N'$ with N and N' nonzero submodules of M and orthogonal; M is diagonalizable if it is the orthogonal sum of 1-dimensional submodules; and M is primitive if there exist $m, m' \in M$ with (m, m') a unit in R.

THEOREM 1. *If 2 is a unit in R, then M is diagonalizable.*

Proof. We may assume M primitive. Let $m, m' \in M$ with (m, m') a unit. Then $(m+m', m+m') = (m, m) + (m', m') +$ unit. So there exists $n \in M$ with (n, n) a unit. By Lemma 1, $M = Rn \oplus (Rn)^{\perp}$ and we use induction on the dimension.

COROLLARY 1. *Let $\mathscr{A}$ be a symmetric matrix over $\boldsymbol{Z}_{\ell}$ $(\ell \neq 2)$. Then there exists an invertible matrix S over $\boldsymbol{Z}_{\ell}$ such that $S\mathscr{A}S^t$ is diagonal.*

Suppose now that 2 is not a unit in R.

LEMMA 2. *If M is primitive and indecomposable, then* dim. $M \leq 2$.

Proof. If there exists $m \in M$ with (m, m) a unit then by Lemma 1, $M = Rm \oplus (Rm)^{\perp}$. So $M = Rm$ and dim. $M = 1$. Suppose that (m, m) is in the maximal ideal of R for all m. Choose m_1 and m_2 with (m_1, m_2) a unit. By Lemma 1 and indecomposibility, $M = Rm_1 + Rm_2$.

THEOREM 2. *For any M there exists a diagonalizable R-module N such that the orthogonal direct sum of M and N is diagonalizable.*

Proof. We may assume M primitive and indecomposable. By Lemma 2 we may assume M generated by e_1 and e_2 with (e_1, e_1), (e_2, e_2) in the maximal ideal and (e_1, e_2) a unit. Replacing e_2 by a multiple we may assume $(e_1, e_2) = -1$. Let $N = Re_3$ with $(e_3, e_3) = 1$. Then $(e_1 + e_3, e_2 + e_3) = 0$. Since $(e_1 + e_3, e_1 + e_3)$ and $(e_2 + e_3, e_2 + e_3)$ are units we conclude from Lemma 1 that $M \oplus N$ admits an orthogonal basis consisting of $e_1 + e_3$, $e_2 + e_3$ and one other vector.

Remark. The proof of Theorem 2 shows the following: if π is a generator of the maximal ideal of R, then N can be choosen to have the form $\oplus Ru_i$ with $(u_i, u_j) = \pi^{n_i}\delta_{ij}$.

Taking $R = \boldsymbol{Z}_2$ and $\pi = 2$ we have:

COROLLARY 2. *Let $\mathscr{A}$ be a symmetric matrix over $\boldsymbol{Z}_2$ Then there exist $m_1, \cdots, m_s$ which are powers of 2 such that the matrix $\mathscr{A} \oplus$* diag. $(m_1, \cdots, m_s)$ *is $\boldsymbol{Z}_2$-diagonalizable.*

REFERENCES

[1] Gerritzen, L. On non-archimedean representation of abelian varieties. Math. Ann., vol. **196** (1972), pp. 323–346.

[2] McCabe, J. *P*-adic theta functions. Ph.D. thesis, Harvard University (1968), unpublished.

[3] Morikawa, H. On theta functions and abelian varieties over valuation fields of rank one. I, II Nagoya Math. Jour. vol. **20** (1962), pp. 1–27 and pp. 231–250.

[4] Mumford, D. An analytic construction of degenerating abelian varieties over complete local rings. Composito Math. vol. **24** (1972), pp. 129–174 and pp. 239–272.
[5] Raynaud, M. Variétés abéliennes et géométrie rigide. Actes Congress Intern. Math. **1** (1970), pp. 473–477.
[6] Roquette, P. Analytic theory of elliptic functions over local fields. Vandenhoeck and Ruprecht in Göttingen (1970).

Departamento de Matemáticas
Centro de Investigación, I.P.N.
México, D.F. México