SUBGROUPS OF FINITE INDEX OF A CLASS OF ABELIAN VARIETIES

BY HORACIO TAPIA-RECILLAS*

Let k be a field complete with respect to a (non-trivial) non-archimedean valuation with order function ord: $k \to \boldsymbol{R}$. Let $\mathcal{O}$ be the valuation ring, U the group of units, $\mathcal{M}$ the maximal ideal and $\bar{k} = \mathcal{O}/\mathcal{M}$ be the residue field.

Let $A = \text{Proj}\ (R)$ be an abelian variety of dimension $g \geq 1$ over k, where R is a graded ring of theta functions (cf. § 1 below) such that the group $A(k)$ of its k-rational points is isomorphic to $(k^*)^g/\Gamma$ for some multiplicative subgroup Γ of $(k^*)^g$.

The reduction $\bar{R}$ modulo the ideal $\mathcal{M}$ of the ring of theta functions R is a graded ring and $\bar{A} = \text{Proj}(\bar{R})$ is an abelian variety over $\bar{k}$. Taking an appropriate basis for R, one can assume that the projective coordinates of the points of $A(k)$ are in $\mathcal{O}$ but not all of them in $\mathcal{M}$. By reducing the projective coordinates of each $P \in A(k)$ modulo $\mathcal{M}$, one gets a map $\rho: A(k) \to \bar{A}(\bar{k})$, where $\bar{A}(\bar{k})$ denotes the group of $\bar{k}$-rational points of $\bar{A}$.

The purpose of this note is to prove the following result which is a generalization of a theorem for elliptic curves to the case of abelian varieties which have the above uniformization property for special Γ. The result for elliptic curves was obtained by J. Tate, cf. [1], [2].

THEOREM. *If $\bar{A}_{n.s.}$ denotes the non-singular part of $\bar{A}$ and $U(k) = \rho^{-1}(\bar{A}_{n.s}(\bar{k}))$, then:*

i) *$U(k)$ is a subgroup of $A(k)$ of finite index. A set of generators for the group $A(k)/U(k)$ is given.*
ii) *the reduction map $\rho: U(k) \to \bar{A}_{n.s.}(\bar{k})$ is a group homomorphism with kernel $U_1 = \{P \in A(k): \rho(P) = \rho(0)\}$.*
iii) *there is an isomorphism between the groups $(1 + \mathcal{M})^g$ and $U_1(k)$.*
iv) *there is a bijection between $\bar{A}_{n.s.}(\bar{k})$ and $(\bar{k}^*)^g$.*

In §1 we recall some general facts about ultrametric theta functions and the uniformization of abelian varieties over k. In §2 we consider a special type of those abelian varieties described in §1 and give the proof of the results stated above. For more details of the results mentioned in §1 see [4]. I thank Zenaida E. Ramos for many helpful conversations.

§1 Generalities

Let k, $\mathcal{O}$, U, $\mathcal{M}$, and $\bar{k}$ be as described above. For any integer $g \geq 1$ let (a_{ij}) be a $g \times g$ matrix with entries in k satisfying the following Riemann conditions: (a_{ij}) is symmetric and $(\text{ord}\ a_{ij})$ is positive definite.

Let $v_j = (a_{j1}, \cdots, a_{jg})$ and $q_j = a_{jj}$ for $j = 1, 2, \cdots, g$. Note that each $q_j \in \mathcal{M}$.

* This work was partially supported by CONACYT grant No. 000070.

For $m \geq 0$ let R_m be the set of Laurent power series $\theta(x) = \Sigma a_I x^I$ in the g variables $x_1, \cdots, x_g$ with coefficients in $\mathcal{O}$ which converge for every element and which satisfy the following functional equation:

$$\theta(v_j x) = q_j^{-2m} x_j^{-4m}\, \theta(x) \qquad j = 1, 2, \cdots, g.$$

(we use the vector notation *i.e.* $I = (i_1, \cdots, i_g) \in \boldsymbol{Z}^g$, $x = (x_1, \cdots, x_g)$ and if $y = (y_1, \cdots, y_g)$, $xy = (x_1 y_1, \cdots, x_g y_g)$.

It can be shown that R_m is a k-vector space of dimension $(4m)^g$, and $R = \oplus_0^\infty R_m$ is a finitely generated k-algebra (independently of the characteristic of k). We call R the graded ring of ultrametric theta functions associated with the matrix (a_{ij}). It can also be shown that the scheme $A = \mathrm{Proj}(R)$ is an abelian variety of dimension g over k, and if $A(k)$ denotes the group of k-rational points of A there is a canonical homomorphism $\Phi:(k^*)^g/\Gamma \to A(k)$ where Γ is the subgroup generated by the elements $v_j = (a_{j1}, \cdots, a_{jg})$, $j = 1, 2, \cdots, g$ (for details cf. [4]).

Now we take the case when the matrix (a_{ij}) is such that each a_{ij} $i \neq j$ is a unit in the ring $\mathcal{O}$. We call this case the "diagonal" case. In this case, it can be shown that the k-algebra R of theta functions is generated by R_1. A canonical basis for R_1 is given by the 4^g theta functions $\theta_\alpha(x) = \Sigma a_I x^I$ where $\alpha = (\alpha_1, \cdots, \alpha_g)$ is such that $\alpha_i \in \{-1, 0, 1, 2\}$ and $a_I = [\prod_{j=1}^g q_j^{t_j(2t_j+\alpha_j)}] \cdot u_I$ with $I = (i_1, \cdots, i_g)$, $i_j = 4t_j + \alpha_j$ (*i.e.* $i_j \equiv \alpha_j$ mod. 4) and u_I being a unit in $\boldsymbol{U}$ (u_I is given explicitly by

$$\textstyle\prod_{j>k} a_{jk}^{i_k t_j + \alpha_j t_k}, \text{ cf. [4]).}$$

Let $\overline{R}_m$ denote the set of elements $\bar{\theta}(x) = \Sigma \bar{a}_I x^I$ which are reductions, modulo the maximal ideal $\mathcal{M}$, of the elements $\theta(x) = \Sigma a_I x^I$ in R_m (the bar means reduction modulo $\mathcal{M}$). $\overline{R}_m$ is a $\bar{k}$-vector space of dimension $(4m)^g$. In particular, a basis for $\overline{R}_1$ is given by the reductions $\bar{\theta}_\alpha(x)$ of the canonical basis $\{\theta_\alpha(x)\}$ of R_1 described above. The monomials x^I which appear in $\bar{\theta}_\alpha(x)$ are just those for which: $i_j = \alpha_j$ if $\alpha_j = -1, 0, 1$ and $i_j = \pm 2$ if $\alpha_j = 2$.

It can be shown that $\overline{R} = \oplus_0^\infty \overline{R}_m$ is a graded $\bar{k}$-algebra generated by $\overline{R}_1$ and $\overline{A} = \mathrm{Proj}(\overline{R})$ is an abelian variety over $\bar{k}$.

If $P \in A(k)$ has projective coordinates $(x_\alpha(P))$, we may normalize them such that each $x_\alpha(P) \in \mathcal{O}$ but not all of them are in $\mathcal{M}$. Then if $P = (x_\alpha(P))$ is an element of $A(k)$, by reducing each $x_\alpha(P)$ modulo $\mathcal{M}$ one gets an element $\overline{P}$ in the group $\overline{A}(\bar{k})$ of $\bar{k}$-rational points of $\overline{A}$ whose coordinates are $x_\alpha(\overline{P}) = \overline{x_\alpha(P)}$. Thus we have a reduction map $\rho: A(k) \to \overline{A}(\bar{k}), \rho(P) = \overline{P}$.

Let $U(k)$ denote the set of elements $P \in A(k)$ whose coordinate $x_{0,\ldots,0}(P)$ is in the group $\boldsymbol{U}$ of units of $\mathcal{O}$ (each $\alpha_i = 0$, $i = 1, 2, \cdots, g$). In [4, § II] it is shown that if $P \in U(k)$ then each coordinate $x_i(P) = x_{0,\ldots,\underset{(i)}{1},\ldots,0}(P)$ is in $\boldsymbol{U}$, $i = 1, 2, \cdots, g$, and that the canonical homomorphism $\Phi:(k^*)^g/\Gamma \to A(k)$ induces an **isomorphism** between $\boldsymbol{U}^g$ and $U(k)$.

If $\overline{A}_{n.s.}$ denotes the non-singular part of $\overline{A}$, it is readily seen that $U(k) = \rho^{-1}(\overline{A}_{n.s.}(\bar{k}))$, and by the above isomorphism it follows that $U(k)$ is a subgroup of $A(k)$.

Remark. In [4] the following results are proved:
i) using the isomorphism between U^g and $U(k)$ it is shown that the canonical homomorphism $\Phi:(k^*)^g/\Gamma \to A(k)$ is injective in general, and that in the diagonal case this homomorphism is **surjective**.
ii) we have a stronger result: if the valuation group of the valuation of k is contained in the field of rational numbers and if (a_{ij}) is a $g \times g$ matrix satisfying the Riemann conditions such that a_{ij} $i \neq j$ is not necessarily a unit in the valuation ring, then the canonical homomorphism $\Phi:(k^*)^g/\Gamma \to A(k)$ is **bijective**.

The main step in the proof of this result is to reduce this case, by an isogeny argument, to the diagonal case of i).

§2 The Proof of the Theorem

In this section we deal only with the "diagonal" case.

Recall that Γ is the subgroup of $(k^*)^g$ generated by the vectors $v_j = (a_{j1}, \cdots, a_{jg})$, $j = 1, 2, \cdots, g$ of the matrix (a_{ij}) satisfying the Riemann conditions, and that $q_j = a_{jj}$ is in the maximal ideal $\mathscr{M}$ for all $j = 1, 2, \cdots, g$.

Let q be a generator of the maximal ideal $\mathscr{M}$. Since $q_j \in \mathscr{M}$, $q_j = w_j q^{n_j}$ with $w_j \in U$, $n_j > 0$ for all $j = 1, 2, \cdots, g$. Then if $x = (x_1, \cdots, x_g) \in \mathscr{O}^g$ $x_i = u_i q^{s_i}$ with $u_i \in U$, $s_i \geq 0$, it follows that $x \equiv (u_1' q^{r_1}, \cdots, u_g' q^{r_g})$ mod Γ, where $0 \leq r_i \leq n_i - 1$ and each $u_i' \in U$.

If P is any point of $A(k)$, since we are assuming that the canonical map $\Phi:(k^*)^g/\Gamma \to A(k)$ is bijective, multiplying by elements of Γ if necessary, we may assume that there is an element $x = (x_1, \cdots, x_g) \in \mathscr{O}^g$ such that $\Phi(x\Gamma) = P$, and $x_i = u_i q^{m_i}$, $u_i \in U$, $m_i \geq 0$.

By the remark above, it follows that

$$x \equiv (u_1', \cdots, u_g')\,(q^{r_1}, 1, \cdots, 1) \cdots (1, \cdots, 1, q^{r_g}) \bmod \Gamma$$

with $0 \leq r_i \leq n_i - 1$, $u_i' \in U$ and if P_i denotes the point $\Phi((1, \cdots, \underset{(i)}{q}, \cdots, 1)\Gamma)$ of $A(k)$ then

$$P = \Phi((u_1', \cdots, u_g')\Gamma) \cdot P_1^{r_1} \cdots P_g^{r_g}$$

i.e., $P \equiv P_1^{r_1} \cdots P_g^{r_g}$ mod $U(k)$.

Note that the set $\{(q_1^{r_1}, \cdots, q_g^{r_g})\, U^g, 0 \leq r_i \leq n^i - 1\}$ is finite, and so $\mathscr{O}^g/U^g$ is also finite. Since Φ is bijective, it follows that $A(k)/U(k)$ is finite too.

In order to prove assertion (ii) of the theorem it is enough to show that $x_\alpha(\overline{PQ}) = x_\alpha(\overline{P}\,\overline{Q})$ for all α.

Let $x_i(P) = x_{0,\ldots,\underset{(i)}{1},\ldots,0}(P)$ for $i = 1, 2, \cdots, g$. We claim that if $x_i(\overline{PQ}) = x_i(\overline{P}\,\overline{Q})$ for $i = 1, 2, \cdots, g$ then $x_\alpha(\overline{PQ}) = x_\alpha(\overline{P}\,\overline{Q})$ for all α. This is a consequence of the following fact:

An element $\overline{P} \in \overline{A}_{n.s.}(\overline{k})$ is determined by its coordinates

$$x_i(\overline{P}), \quad i = 1, 2, \cdots, g.$$

In order to see this, let $\theta_i(x) = \theta_{0,\ldots,\underset{(i)}{1},\ldots,0}(x)$ and $\theta_{-i}(x) = \theta_{0,\ldots,\underset{(i)}{1},\ldots,0}(x)$ for $i = 1, 2, \cdots, g$. By normalizing these functions we may assume that $\theta_i(x) = x_i + \cdots$, $\theta_{-i}(x) = x_i^{-1} + \cdots$, and have reductions $\bar{\theta}_i(x) = x_i$, $\bar{\theta}_{-i}(x) = x_i^{-1}$.

For any $\beta = (\beta_1, \cdots, \beta_g)$, $\beta_i \in \{-1, 0, 1, 2\}$ we have $\bar{\theta}_0^{2g-1}\bar{\theta}_\beta = \bar{F}_\beta(\bar{\theta}_0, \bar{\theta}_i, \bar{\theta}_{-i})$ where $\bar{F}_\beta$ is a homogeneous polynomial of degree $2g$ with coefficients in $\bar{k}$. Then we have $x_\beta(\bar{P}) = \bar{F}_\beta(x_i(\bar{P}), x_{-i}(\bar{P}))$. We also have $x_i(\bar{P})x_{-i}(\bar{P}) = 1$. Thus the coordinates $x_i(\bar{P})$ determine each $x_\beta(\bar{P})$.

Now, the relation $x_i(\overline{PQ}) = x_i(\bar{P}\,\bar{Q})$, $i = 1, 2, \cdots, g$ follows at once from the following identities for the reductions of theta functions:

$$(*) \qquad \bar{\theta}_0(xy)\bar{\theta}_0(xy^{-1}) = \bar{\theta}_0(x)^2\bar{\theta}_0(y)^2$$

$$\bar{\theta}_i(xy)\bar{\theta}_0(xy^{-1}) = \bar{\theta}_i(x)\bar{\theta}_0(x)\bar{\theta}_i(y)\bar{\theta}_0(y).$$

These identities are obvious from the form of the reductions of the theta functions $\bar{\theta}_\alpha$, cf. §1 above.

Thus the reduction map $\rho: U(k) \to \bar{A}_{n.s.}(\bar{k})$ is a homomorphism whose kernel is obviously $\{P \in A(k) : \bar{P} = \bar{0}\}$.

Remark 1. It can also be proved that an element $P \in U(k)$ is determined by its coordinates $x_i(P)$, $i = 1, 2, \cdots, g$. The idea is as follows: for any $\beta = (\beta_1, \cdots, \beta_g)$, $\beta_i \in \{-1, 0, 1, 2\}$ one has the relation $\bar{\theta}_0^{2g-1}\bar{\theta}_\beta = \bar{F}_\beta(\bar{\theta}_0, \bar{\theta}_i, \bar{\theta}_{-i})$ as above. Lift the homogeneous polynomial $\bar{F}_\beta$ to a polynomial F_β with coefficients in $\mathcal{O}$, so that one has $\theta_0^{2g-1}\theta_\beta = F_\beta(\theta_0, \theta_i, \theta_{-i}) + CG_\beta(\theta_\alpha)$ where $C \in \mathcal{M}$ (independent of β), G_β is a polynomial with coefficients in $\mathcal{O}$ and the θ_α's are the canonical basis for R_1 (recall that R_1 generates R). If $P \in A(k)$, it follows from the above relation that:

$$\text{(a)} \qquad x_\beta(P) = F_\beta(x_i(P), x_{-i}(P)) + CG_\beta(x_\alpha(P)).$$

In a similar way one sees easily that

$$\text{(b)} \qquad x_i(P)x_{-i}(P) = 1 + CG_i(x_\alpha(P)),$$

where $C \in \mathcal{M}$ and G_i is a polynomial with coefficients in $\mathcal{O}$ (the same C may be taken in (a) and (b)).

Now let $P, Q \in U(k)$ be such that $x_i(P) = x_i(Q)$ for $i = 1, 2, \cdots, g$. Since $x_\beta(P)$, $x_\beta(Q)$ are in $\mathcal{O}$ for all β and $x_i(P) \in U$ for all i, it follows from the relation (b) that $x_{-i}(P) \equiv x_{-i}(Q) \bmod C$, and from (a) that $x_\beta(P) \equiv x_\beta(Q) \bmod C$. Repeating the argument one has $x_\beta(P) \equiv x_\beta(Q) \bmod C^n$ for all $n > 0$. Therefore $x_\beta(P) = x_\beta(Q)$ for all β.

Remark 2. The relations (*) above for the reductions of theta functions can be lifted to the following relations in the ring R:

$$\theta_0(xy)\theta_0(xy^{-1}) = \theta_0(x)^2\theta_0(y)^2 + F(\theta_\alpha(x), \theta_\alpha(y))$$

$$\theta_i(xy)\theta_0(xy^{-1}) = \theta_i(x)\theta_0(x)\theta_i(y)\theta_0(y) + G(\theta_\alpha(x), \theta_\alpha(y)),$$

where F and G are homogeneous polynomials with reduction zero. For a more detailed proof of remark 1 and more relations among theta functions cf. [4].

To prove assertion (iii) let $x = (x_1, \cdots, x_g)$, $x_i \in (1 + \mathscr{M})$ and $P = \Phi(x\Gamma)$. Then one sees easily that $x_i(\bar{P}) = x_i(\bar{0}) = 1$ for all $i = 1, 2, \cdots, g$. Since the coordinates $x_i(\bar{P})$ determine $\bar{P}$, it follows that $P \in \ker \rho = U_1(k)$. Conversely, if $P = \Phi(x\Gamma) \in U_1(k)$ with $x = (x_1, \cdots, x_g)$, $x_i \in \mathscr{O}$, then $x_i(\bar{P}) = \bar{x}_i = 1$, *i.e.* $x_i \in (1 + \mathscr{M})$ for all $i = 1, 2, \cdots, g$. Thus the canonical homomorphism Φ induces an isomorphism between $(1 + \mathscr{M})^g$ and $U_1(k)$.

To prove the last assertion (iv), let $\lambda: \bar{A}_{rs.}(\bar{k}) \to (\bar{k}^*)^g$ be defined by $\lambda(\bar{P}) = (x_1(\bar{P}), \cdots, x_g(\bar{P}))$. It follows from the identities (*) above that λ is a homomorphism, which obviously has trivial kernel and is surjective.

CENTRO DE INVESTIGACION DEL IPN, MEXICO, D.F.

REFERENCES

[1] J. T. TATE, *The arithmetic of elliptic curves.* Invent. Math., **23** (1974), 179–205.

[2] ———, *Algorithm for determining the type of a singular fiber in an elliptic pencil,* in Lecture Notes in Mathematics, Springer-Verlag, Berlin-Heidelberg-New York, **476** (1972), 33–53.

[3] D. MUMFORD, *An analytic construction of degenerating abelian varieties over complete rings.* Compositio Math. **24** (1972), 239–272.

[4] H. TAPIA-RECILLAS, *Ultrametric theta functions and abelian varieties. Nagoya Math. J.* **69** (1978), 65–96.

[5] ———, *Subgrupos de índice finito de una clase de curvas elípticas.* En prensa en: Rev. Mat. Hisp. Amer.