RIGIDITY THEOREMS FOR ABELIAN VARIETIES

YU. G. ZARHIN AND A. SILVERBERG

A theme running through this paper is the fact that a root of unity congruent to 1 modulo n is 1, if $n \geq 3$. This theme can be traced back to Minkowski [4], who proved that an integral matrix of finite multiplicative order which is congruent to the identity modulo n is the identity, if $n \geq 3$. Serre applied this idea to abelian varieties, and showed ([3], 4.7.1) that if an automorphism of finite order of a semi-abelian variety induces the identity on the scheme-theoretic kernel of multiplication by n, then it is the identity if $n \geq 3$, and its square is the identity if $n = 2$.

Using Serre's result, Raynaud augmented Grothendieck's study of Neron models of abelian varieties, by proving a useful criterion of semistable reduction ([3], 4.7). Raynaud's criterion says that if an abelian variety and all its n-torsion points are defined over a field with a discrete valuation of residue characteristic not dividing n, and $n \geq 3$, then the abelian variety has semistable reduction (and acquires semistable reduction in a $(\mathbf{Z}/2\mathbf{Z})^r$-extension, if $n = 2$, the valuation ring is henselian, and the residue field is separably closed). One may prove (compare with [2], [1]; see also 3.6 of [8]) that if an abelian variety and all its n-torsion points are defined over a finitely generated extension of $\mathbf{Q}$, and $n \geq 3$, then the Zariski closure of the image of the absolute Galois group under every ℓ-adic representation is connected. Another consequence of the Minkowski idea (see [5]) is that if two abelian varieties are defined over a field F, then every homomorphism between them is defined over every extension of F over which the n-torsion points of the abelian varieties are defined, as long as n is not divisible by the characteristic of F and is at least 3.

In Theorem 1 below we state a generalization of the Minkowski idea. In this generalization, we replace the assumption that the root of unity α is congruent to 1 modulo n by the assumption that $(\alpha - 1)^k$ is congruent to 0 modulo n. In the remainder of the paper we state generalizations of the above applications of the Minkowski idea.

Definition 1. If k is a positive integer, define a finite set $N(k)$ by

$$N(k) = \{\text{prime powers } \ell^m : 0 \le m(\ell-1) \le k\}.$$

Let $R(k,1) = 0$; if n is a positive integer which is not in $N(k)$, let $R(k,n) = 1$; if $1 \ne n = \ell^m \in N(k)$ with ℓ a prime, let

$$R(k,n) = \ell^{r(k,n)} \quad \text{where} \quad r(k,n) = \max\{r \in \mathbf{Z}^+ : m(\ell-1)\ell^{r-1} \le k\}.$$

For example,

$$N(1) = \{1,2\}, \quad N(2) = \{1,2,3,4\},$$
$$N(3) = \{1,2,3,4,8\}, \quad N(4) = \{1,2,3,4,5,8,9,16\};$$
$$R(1,2) = 2, \quad R(1,n) = 1 \text{ if } n \ge 3,$$
$$R(2,2) = 4, \quad R(2,3) = 3, \quad R(2,4) = 2, \quad \text{and} \quad R(2,n) = 1 \text{ if } n \ge 5.$$

Definition 2. If Δ is a subset of a ring $\mathcal{O}$, we say Δ *has no $\mathcal{O}$-zero divisors* if there do not exist $x \in \Delta$ and $0 \ne y \in \mathcal{O}$ such that $xy = 0 = yx$. In particular, if Δ has no $\mathcal{O}$-zero-divisors then $0 \notin \Delta$.

If F is a field, let F^s denote a separable closure and let $\mathrm{char}(F)$ denote the characteristic of F. Suppose (X, λ) is a polarized abelian variety defined over F. Write X_n for the kernel of multiplication by n in $X(F^s)$. If n is a positive integer not divisible by $\mathrm{char}(F)$, and $\boldsymbol{\mu}_n$ is the $\mathrm{Gal}(F^s/F)$-module of n-th roots of unity in F^s, then define a skew-symmetric Galois-equivariant bilinear map

$$e_{\lambda,n} : X_n \times X_n \to \boldsymbol{\mu}_n, e_{\lambda,n}(x_1, x_2) = e_n(x_1, \lambda(x_2)),$$

where e_n is the Weil pairing. If n is relatively prime to the degree of the polarization λ, then the pairing $e_{\lambda,n}$ is nondegenerate. Suppose ℓ is a prime number not equal to $\mathrm{char}(F)$. Let $T_\ell(X) = \varprojlim X_{\ell^r}$ (the Tate module), let $V_\ell(X) = T_\ell(X) \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell$, let $d = \dim(X)$, and let $\rho_{X,\ell}$ denote the ℓ-adic representation

$$\rho_{X,\ell} : \mathrm{Gal}(F^s/F) \to \mathrm{Aut}(T_\ell(X)) \subseteq \mathrm{Aut}(V_\ell(X)) \cong \mathrm{GL}_{2d}(\mathbf{Q}_\ell).$$

Let $G_{F,X}$ denote the image of $\mathrm{Gal}(F^s/F)$ under $\rho_{X,\ell}$. Let $\mathfrak{G}_\ell(F,X)$ denote the algebraic envelope of the image of $\rho_{X,\ell}$, i.e., the Zariski closure of $G_{F,X}$ in $\mathrm{GL}_{2d}(\mathbf{Q}_\ell)$.

Theorem 1. *Suppose $\mathcal{O}$ is a ring such that the natural map $\mathcal{O} \to \mathcal{O} \otimes_{\mathbf{Z}} \mathbf{Q}$ is injective, and suppose k and n are positive integers. Suppose that for every rational prime divisor ℓ of n, $1 + \ell\mathcal{O}$ has no $\mathcal{O}$-zero-divisors. Suppose α is an element of*

$\mathcal{O}$ of finite multiplicative order such that $(\alpha - 1)^k \in n\mathcal{O}$. Then $\alpha^{R(k,n)} = 1$. In particular, if $n \notin N(k)$ then $\alpha = 1$.

Corollary . *Suppose n is a positive integer, $\mathcal{O}$ is an integral domain of characteristic zero such that no rational prime which divides n is a unit in $\mathcal{O}$, $\alpha \in \mathcal{O}$, α has finite multiplicative order, and $(\alpha - 1)^2 \in n\mathcal{O}$. If $n \geq 5$ then $\alpha = 1$, if $n = 4$ then $\alpha^2 = 1$, if $n = 3$ then $\alpha^3 = 1$, and if $n = 2$ then $\alpha^4 = 1$.*

Theorem 2. *Suppose G is a commutative group scheme over a field, which is an extension of an abelian variety by a torus, n and k are positive integers, α is an endomorphism of G of finite multiplicative order, and $(\alpha - 1)^k$ is 0 on the scheme-theoretic kernel of multiplication by n on G. Then $\alpha^{R(k,n)} = 1$.*

The following result is an analogue of the result of Raynaud stated in the introduction, and generalizes to higher dimensional abelian varieties earlier work on elliptic curves due to Frey [7] and to Flexor and Oesterlé [6].

Theorem 3. *Suppose (X, λ) is a polarized abelian variety defined over a field F, v is a discrete valuation on F, n is an integer not divisible by the residue characteristic of v, $\widetilde{X}_n$ is a maximal isotropic subgroup of X_n with respect to the pairing $e_{\lambda,n}$, and the points of $\widetilde{X}_n$ are defined over F. If $n \geq 5$ then X has semistable reduction at v. If $n = 2$, 3, or 4, then X has semistable reduction above v over every totally ramified Galois (necessarily cyclic) extension of F of degree 4, 3, or 2, respectively.*

Theorem 4. *Suppose (X, λ) is a polarized abelian variety defined over a field F which is either a finitely generated extension of $\mathbf{Q}$ or a global field of positive characteristic, and let $p = char(F)$. Suppose ℓ is a prime number, n is an integer, $n \geq 5$, p does not divide ℓn, and $\widetilde{X}_n$ is a maximal isotropic subgroup of X_n with respect to $e_{\lambda,n}$. Suppose the points of $\widetilde{X}_n$ are defined over F, and the roots of unity in $e_{\lambda,n}(X_n, \widetilde{X}_n)$ are contained in F. Then $\mathfrak{G}_\ell(F, X)$ is connected.*

Theorem 5. *Suppose (X, λ) and (Y, μ) are polarized abelian varieties defined over a field F, n is a positive integer which is not divisible by the characteristic of F, and $n \geq 5$. Suppose $\widetilde{X}_n$, respectively $\widetilde{Y}_n$, is a maximal isotropic subgroup of X_n, respectively Y_n, with respect to the pairing $e_{\lambda,n}$, respectively $e_{\mu,n}$. Suppose the points of $\widetilde{X}_n$ and $\widetilde{Y}_n$ are defined over F, and the roots of unity in $e_{\lambda,n}(X_n, \widetilde{X}_n)$ and*

$e_{\mu,n}(Y_n, \widetilde{Y}_n)$ are contained in F. Then every homomorphism between X and Y is defined over F.

Note that the two preceding results are false if one drops the hypothesis that the roots of unity in $e_{\lambda,n}(X_n, \widetilde{X}_n)$ and $e_{\mu,n}(Y_n, \widetilde{Y}_n)$ are contained in F (for example, consider CM elliptic curves defined over $\mathbf{Q}$).

References

[1] M. Borovoi, Mat. Sbornik (N. S.) **94** (136) (1974), 649–652; English transl. in Math. USSR Sbornik **23** (1974), 613–616.
[2] M. Borovoi, Problems of group theory and homological algebra, No. 1 (Russian), pp. 3–53, Yaroslav. Gos. Univ., Yaroslavl', 1977.
[3] A. Grothendieck, Groupes de monodromie en géometrie algébrique, SGA7 I, Lecture Notes in Math. vol. 288, 1972, pp. 313–523.
[4] H. Minkowski, J. reine angew. Math. **101** (1887), 196–202.
[5] A. Silverberg, J. Pure and Applied Algebra **77** (1992), 253-262.
[6] M. Flexor and J. Oesterlé, Astérisque **183** (1990), 25–36.
[7] G. Frey, Ark. Mat. **15** (1977), 1–19.
[8] W. Chi, Amer. J. Math. **114** (1992), 315–353.

Institute for Mathematical Problems in Biology, Russian Academy of Sciences, Pushchino, Moscow Region

Pennsylvania State University

Ohio State University