ELSEVIER

Journal of Pure and Applied Algebra 111 (1996) 285–302

JOURNAL OF
PURE AND
APPLIED ALGEBRA

Variations on a theme of Minkowski and Serre

A. Silverberg[a,*], Yu. G. Zarhin[b,c]

[a] *Mathematics Department, Ohio State University, Columbus, OH 43210-1174, USA*
[b] *Mathematics Department, Pennsylvania State University, University Park, PA 16802, USA*
[c] *Institute for Mathematical Problems in Biology, Russian Academy of Sciences, Pushchino, Moscow Region, 142292, Russia*

Communicated by E.M. Friedlander; received 6 November 1994

Abstract

If α is a root of unity in an integral domain $\mathcal{O}$ of characteristic zero, $(\alpha - 1)^k \in n\mathcal{O}$, and no prime divisor of n is a unit in $\mathcal{O}$, then $\alpha = 1$ if n is a positive integer outside a finite set determined by k. We prove this result and generalizations of it, and give results when n is an element of the finite exceptional set. We give applications to endomorphisms of semi-abelian varieties, compatible systems of ℓ-adic representations, and the cohomology of projective varieties.

1991 Math. Subj. Class.: 08A35, 11G10, 14F20

1. Introduction

A result of Serre (see [6, Lemma 4.7.1] and [9, Theorem on p. 17–19]) says 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 $n = 2$. This result is useful in the study of moduli spaces of abelian varieties with full level $n \geq 3$ structure. Serre's Lemma relies on the fact that if $n \geq 3$ then every root of unity which is congruent to 1 modulo n is 1. This idea dates back to Minkowski (see [8]), who proved that an integral matrix of finite order, which is congruent to the identity modulo n, is the identity if $n \geq 3$.

In this paper we give generalizations and variations of the Serre–Minkowski results. For example (see Corollary 3.3), if k and n are positive integers, α is a root of unity in an integral domain $\mathcal{O}$ of characteristic zero, $(\alpha - 1)^k$ is divisible by n, and no prime divisor of n is a unit in $\mathcal{O}$, then $\alpha = 1$ if n is outside of a certain finite set of

[*] Corresponding author. E-mail: silver @ math.ohio-state-edu.

SSDI 0022-4049(95)00113-1

prime powers determined by k. (The case $k = 1$ is the Serre–Minkowski case.) The proof relies on the arithmetic of cyclotomic integers. Although the ideas are simple, the result is useful and does not seem to have been noticed before. We give best-possible restrictions on α when n is in the finite exceptional set. We have results for rings that are not necessarily integral domains (Section 4), and we have applications to matrix rings, eigenvalues, projective modules, and quasi-unipotent elements (see Sections 6 and 7). We provide additional information when n is in the exceptional finite set (see Theorems 5.1, 6.8, 7.4, 8.2 and 8.3), and give examples which show that our results are sharp. In Section 8 we give applications to endomorphisms of semi-abelian varieties, which generalize Serre's result. In Section 9 we give applications to compatible systems of ℓ-adic representations and the cohomology of projective varieties.

We believe these results have independent interest. We also expect that they will have additional applications. For some applications of special cases of these results to abelian varieties, see [13–15].

A different variation on Minkowski's theorem, due to Selberg, says that if K is a field of characteristic zero and H is a finitely generated subgroup of $GL_m(K)$, then H has a net (and therefore torsionfree) subgroup of finite index (see 17.7 on p. 119 of [1]). For other variations on Minkowski's theorem see also Chapter 3 of [16], which deals with n an indecomposable element in a unique factorization domain or a prime ideal of a Dedekind ring in characteristic zero.

Serre pointed out to us another generalization of Minkowski's theorem (see p. 223 of [2], for example). If G is a formal group over a discrete valuation ring $\mathcal{O}$ of residue characteristic p, and π is a uniformizing parameter, then $G(\mathcal{O})$ has trivial prime-to-p torsion, and has trivial p-torsion if $\mathrm{ord}_\pi(p) < p - 1$. Minkowski's theorem follows by taking G to be the formal group of the general linear group. The result can also be applied to the formal group of an elliptic curve with good reduction.

2. Notation

All rings in this paper are rings with identity. However, we do not assume $0 \neq 1$; that is, we do not exclude the zero ring. We denote the mth cyclotomic polynomial by Φ_m, and the integers and rational numbers by $\mathbb{Z}$ and $\mathbb{Q}$, respectively. We use the convention that anything raised to the power 0 is 1. We write $M_g(\mathcal{O})$ for the ring of $g \times g$ matrices over $\mathcal{O}$, and write I_g (or I when it is unambiguous) for the $g \times g$ identity matrix.

Definition 2.1. If k is a positive integer, define a finite set $N(k)$ by

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

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

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

For example,

$$N(1) = \{1,2\}, \qquad N(2) = \{1,2,3,4\}, \qquad N(3) = \{1,2,3,4,8\},$$

$$N(4) = \{1,2,3,4,5,8,9,16\};$$

$$R(1,2) = 2, \qquad R(1,n) = 1 \text{ if } n \geq 3,$$

$$R(2,2) = 4, \qquad R(2,3) = 3, \qquad R(2,4) = 2, \qquad \text{and} \qquad R(2,n) = 1 \text{ if } n \geq 5.$$

3. Integral domains of characteristic zero

Theorem 3.1. *Suppose n, k, and M are positive integers, $\mathcal{O}$ is an integral domain of characteristic zero such that no rational prime which divides n is a unit in $\mathcal{O}$, $b(1),\dots,b(k)$ are integers relatively prime to M, $\alpha \in \mathcal{O}$, $\alpha^M = 1$, and*

$$\prod_{j=1}^{k}(\alpha^{b(j)} - 1) \in n\mathcal{O}.$$

Then $\alpha^{R(k,n)} = 1$.

Proof. Without loss of generality we may assume M is the exact multiplicative order of α. If $M = 1$, then $\alpha = 1$ and there is nothing to show. Suppose $M \neq 1$ and let ℓ^r be a prime power which exactly divides M, with $r \geq 1$. Let $\zeta = \alpha^{M/\ell^r}$. For all integers i, $\zeta^i - 1 \in (\alpha^i - 1)\mathcal{O}$, so

$$\prod_{j=1}^{k}(\zeta^{b(j)} - 1) \in n\mathcal{O}.$$

If i is a positive integer less than ℓ^r and not divisible by ℓ, then the elements $\zeta^i - 1$ each generate the same ideal in $\mathbb{Z}[\zeta] \subseteq \mathcal{O}$, and therefore,

$$\ell^k = (\Phi_{\ell^r}(1))^k = \prod_{i \in (\mathbb{Z}/\ell^r\mathbb{Z})^\times} (1 - \zeta^i)^k \in n^{\varphi(\ell^r)}\mathcal{O},$$

where φ is the Euler φ-function. Thus, $\ell^k n^{-\varphi(\ell^r)} \in \mathcal{O}$.

We will now show that $\mathbb{Z}[1/n] \cap \mathcal{O} = \mathbb{Z}$. Suppose $\beta \in \mathbb{Z}[1/n] \cap \mathcal{O}$. If $\beta \notin \mathbb{Z}$, then we can write $\beta = \frac{a}{pb}$ where a, $b \in \mathbb{Z}$ and p is a prime dividing n but not dividing a. Since p does not divide a, we have $\frac{1}{p} \in \mathbb{Z} + \mathbb{Z}\frac{a}{p} = \mathbb{Z} + \mathbb{Z}b\beta \subseteq \mathcal{O}$, contradicting the assumption that no rational prime which divides n is a unit in $\mathcal{O}$. Therefore, $\beta \in \mathbb{Z}$.

Therefore, $\ell^k n^{-\varphi(\ell^r)} \in \mathbb{Z}$. Thus, $n^{\varphi(\ell^r)}$ divides ℓ^k, so n is a prime power of the form ℓ^m with

$$k \geq m\varphi(\ell^r) = m(\ell - 1)\ell^{r-1} \geq m(\ell - 1).$$

Therefore, $n \in N(k)$. Further, n is a power of every prime which divides the order of α, so the order of α is a prime power ℓ^r, with $m(\ell - 1)\ell^{r-1} \leq k$. □

Remark 3.2. By taking $\mathcal{O}$ to be the ring of integers in an algebraic closure of $\mathbb{Q}$, fixing $n = \ell^m \in N(k)$, and letting α be a primitive $R(k,n)$th root of unity, we see that the upper bound of $R(k,n)$ on the order of α in Theorem 3.1 is sharp.

The most interesting case of Theorem 3.1 is when $b(1) = \cdots = b(k) = 1$, i.e., when $(\alpha - 1)^k \in n\mathcal{O}$. For ease of exposition and notation, we will restrict ourselves to that case from now on, although our results could all be stated in the generality of Theorem 3.1.

Corollary 3.3. *Suppose n and k are positive integers, $\mathcal{O}$ 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 $(\alpha - 1)^k \in n\mathcal{O}$. Then $\alpha^{R(k,n)} = 1$; in particular, $\alpha = 1$ if $n \notin N(k)$.*

4. Rings in characteristic zero

Remark 4.1. If $\mathcal{O}$ is a non-zero ring, then the natural map $\mathcal{O} \to \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Q}$ is injective if and only if

- the natural map $\mathbb{Z} \to \mathcal{O}$ is injective, and
- no non-zero rational integer is a zero-divisor in $\mathcal{O}$.

Definition 4.2. 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 $0 \neq y \in \mathcal{O}$ such that $xy = 0 = yx$. In particular, if Δ has no $\mathcal{O}$-zero-divisors then $0 \notin \Delta$.

Lemma 4.3. *Suppose $\mathcal{O}$ is a non-zero ring and ℓ is a rational prime. Then:*

(a) *If $1 + \ell\mathcal{O}$ has no $\mathcal{O}$-zero-divisors, then ℓ is not a unit in $\mathcal{O}$.*

(b) *If $\mathcal{O}$ has no non-zero infinitely ℓ-divisible elements, then $1 + \ell\mathcal{O}$ has no $\mathcal{O}$-zero-divisors.*

Proof. (a) If ℓ were a unit in $\mathcal{O}$, then we would have $0 \in 1 + \ell\mathcal{O}$, contradicting the assumption that $1 + \ell\mathcal{O}$ has no $\mathcal{O}$-zero-divisors.

(b) If $(1 + \ell x)y = 0$ with $x, y \in \mathcal{O}$ and $y \neq 0$, then $y = -\ell xy = \ell^2 x^2 y = \cdots = (-1)^i \ell^i x^i y$ for all positive integers i, contradicting the assumption that $\mathcal{O}$ has no non-zero infinitely ℓ-divisible elements. □

Theorem 4.4. *Suppose $\mathcal{O}$ is a ring such that the natural map $\mathcal{O} \to \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Q}$ 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 $\alpha^{R(k,n)} = 1$.*

Proof. Since α has finite multiplicative order and the natural map $\mathcal{O} \to \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Q}$ is injective, $\mathbb{Q}[\alpha]$ is a finite dimensional semisimple commutative $\mathbb{Q}$-algebra and therefore is a direct sum of number fields $\bigoplus_{i=1}^{t} K_i$. Let $\mathcal{O}' = \mathcal{O} \cap \mathbb{Q}[\alpha]$. Then $\mathcal{O}' \otimes \mathbb{Q} = \mathbb{Q}[\alpha] = \bigoplus_{i=1}^{t} K_i$. Let π_i be the projection of $\mathbb{Q}[\alpha]$ onto the ith factor, and let $\mathcal{O}_i = \pi_i(\mathcal{O}')$. Then $K_i = \mathcal{O}_i \otimes \mathbb{Q}$, and $\mathcal{O}'$ is a subring of $\bigoplus_{i=1}^{t} \mathcal{O}_i$.

We will show that no rational prime divisor of n is a unit in any of the integral domains $\mathcal{O}_i$. If this were not the case, then some prime divisor ℓ of n would be a unit in some $\mathcal{O}_i$, say $\mathcal{O}_1$. An inverse of ℓ in $\mathcal{O}_1$ is of the form $\pi_1(x)$ for some $x \in \mathcal{O}' \subseteq \mathcal{O}$. We therefore have $1 - \ell x \in \bigoplus_{i=2}^{t} \mathcal{O}_i$. Since $\mathcal{O}' \subseteq \mathcal{O}' \otimes \mathbb{Q} = \bigoplus_{i=1}^{t} K_i$, we have $\mathcal{O}' \cap K_1 \neq \{0\}$. Let y be a non-zero element of $\mathcal{O}' \cap K_1$. Then $(1 - \ell x)y = 0$, contradicting the assumption that $1 + \ell\mathcal{O}$ has no $\mathcal{O}$-zero-divisors. Therefore no rational prime divisor of n is a unit in any $\mathcal{O}_i$.

Let $\alpha_i = \pi_i(\alpha) \in \mathcal{O}_i$. Then $\alpha = \sum_{i=1}^{t} \alpha_i$, and $\alpha_i\alpha_j = 0$ if $i \neq j$. Since $(\alpha - 1)^k \in n\mathcal{O}$, we have $(\alpha_i - 1)^k \in n\mathcal{O}_i$ for every i. Since α has finite multiplicative order, so do all the α_i. By Theorem 3.1, $\alpha_i^{R(k,n)}$ is the identity in the ring $\mathcal{O}_i$, for every i. But $\alpha^{R(k,n)} = (\sum_{i=1}^{t} \alpha_i)^{R(k,n)} = \sum_{i=1}^{t} \alpha_i^{R(k,n)} = 1$. □

5. Extremal exceptional cases

We provide additional information in the extremal exceptional case $k = m\varphi(\ell^r)$. This case includes all the cases with $k = 1$ or 2 and $1 \neq n \in N(k)$. The direct summands in the following theorem are not necessarily non-zero.

Theorem 5.1. *Suppose ℓ is a prime, m and r are positive integers, $\mathcal{O}$ is a commutative ring, the natural map $\mathcal{O} \to \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Q}$ is injective, $1 + \ell\mathcal{O}$ has no $\mathcal{O}$-zero-divisors, $\alpha \in \mathcal{O}$ is an element of finite multiplicative order, and*

$$(\alpha - 1)^{m(\ell-1)\ell^{r-1}} \in \ell^m\mathcal{O}.$$

Then $\alpha^{\ell^r} = 1$ and there are rings Δ and $\mathcal{O}_r$ in $\mathcal{O}$ and elements $\delta \in \Delta$ and $\alpha_r \in \mathcal{O}_r$ such that $\mathcal{O} = \Delta \oplus \mathcal{O}_r$, $\alpha = \delta + \alpha_r$, δ is an ℓ^{r-1}th root of unity in Δ, and α_r satisfies the ℓ^rth cyclotomic polynomial in $\mathcal{O}_r$.

Proof. If G is a finite abelian group, let $\hat{G}$ be the group of characters of G. Let $\bar{\mathbb{Q}}$ denote an algebraic closure of $\mathbb{Q}$. Then the group ring $\bar{\mathbb{Q}}[G]$ is the direct sum of the one-dimensional subspaces $e_\chi\bar{\mathbb{Q}}[G] = \bar{\mathbb{Q}}e_\chi$, where for $\chi \in \hat{G}$, the idempotent e_χ is defined by

$$e_\chi = \frac{1}{|G|}\sum_{\sigma \in G} \chi^{-1}(\sigma)\sigma \in \bar{\mathbb{Q}}[G].$$

From now on take G to be a cyclic group of order ℓ^r. Then

$$\mathbb{Q}[G] \quad \cong \quad \mathbb{Q}[x]/(x^{\ell^r} - 1).$$

For $0 \leq i \leq r$, let $X_i = \{\chi \in \hat{G}\colon\ \chi$ surjects onto the group of ℓ^ith roots of unity$\}$ and let $P_i = \sum_{\chi \in X_i} e_\chi$. Then X_i is stable under $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, $P_i \in \mathbb{Q}[G]$, P_i is an idempotent,

$\mathbb{Q}[G] \cong \bigoplus_{i=0}^{r} P_i\mathbb{Q}[G]$, and $P_i\mathbb{Q}[G] \cong \mathbb{Q}[x]/\Phi_{\ell^i}(x) \cong \mathbb{Q}(\zeta_i)$ where ζ_i is a primitive ℓ^ith root of unity. For $\chi \in \hat{G}$, the values of χ on G are ℓ^rth roots of unity, so in particular are algebraic integers. Viewing P_i as a polynomial $P_i(x) \in \mathbb{Q}[x]$ (modulo $\Phi_{\ell^i}(x)$), the definitions of e_χ and P_i show that $P_i(x) \in \ell^{-r}\mathbb{Z}[x]$. For $1 \leq i \leq r$ we have

$$\prod_{j\in(\mathbb{Z}/\ell^r\mathbb{Z})^\times} (1-\zeta_i^j) = (N_{\mathbb{Q}(\zeta_i)/\mathbb{Q}}(1-\zeta_i))^{\ell^{r-i}} = \ell^{\ell^{r-i}}, \qquad (1)$$

where $N_{\mathbb{Q}(\zeta_i)/\mathbb{Q}}$ denotes the norm from $\mathbb{Q}(\zeta_i)$ to $\mathbb{Q}$.

Let $n = \ell^m$ and $k = m(\ell-1)\ell^{r-1}$. Then $R(k,n) = \ell^r$, and Theorem 4.4 implies that $\alpha^{\ell^r} = 1$. Sending x to α gives a surjective $\mathbb{Q}$-algebra homomorphism

$$(\mathbb{Q}[G] \cong)\, \mathbb{Q}[x]/(x^{\ell^r}-1) \to \mathbb{Q}[\alpha].$$

For $0 \leq i \leq r$, let p_i be the image of P_i in $\mathbb{Q}[\alpha]$, i.e., $p_i = P_i(\alpha) \in \ell^{-r}\mathbb{Z}[\alpha]$. We can make the following identifications:

$$\mathbb{Q}[\alpha] \quad\cong\quad \bigoplus_{p_i\neq 0} p_i\mathbb{Q}[\alpha] \quad\cong\quad \bigoplus_{p_i\neq 0} \mathbb{Q}(\zeta_i).$$

We will use the hypotheses on α to show that $p_r \in \mathcal{O}$. Let

$$\beta = \prod_{j\in(\mathbb{Z}/\ell^r\mathbb{Z})^\times} (1-\alpha^j).$$

By our hypotheses, $\beta^m \in \ell^m\mathcal{O}$. We have $p_0\beta = 0$, and (1) implies that $p_i\beta = \ell^{\ell^{r-i}}p_i$ for $1 \leq i \leq r$. Therefore,

$$\beta = \sum_{i=1}^{r} \ell^{\ell^{r-i}} p_i \quad\text{and}\quad \beta^m = \sum_{i=1}^{r} \ell^{m\ell^{r-i}} p_i.$$

If $r = 1$, then $\beta^m = \ell^m p_1 \in \ell^m\mathcal{O}$, so $p_1 \in \mathcal{O}$ by the injectivity of the natural map $\mathcal{O} \to \mathcal{O}\otimes_{\mathbb{Z}}\mathbb{Q}$. Suppose $r > 1$. Let

$$B = \beta^m \prod_{i=1}^{r-1}(\beta^m - \ell^{m\ell^{r-i}}), \qquad C = \prod_{i=1}^{r-1}(1-\ell^{m(\ell^{r-i}-1)}).$$

Then $B \in \ell^{mr}\mathcal{O}$, and C is a non-zero integer which is not divisible by the prime ℓ. Since $p_0\beta = 0$ and $p_i(\beta^m - \ell^{m\ell^{r-i}}) = 0$, we easily see that $B = \ell^{mr}Cp_r$. Therefore, $\ell^{mr}Cp_r \in \ell^{mr}\mathcal{O}$. Since the natural map $\mathcal{O} \to \mathcal{O}\otimes_{\mathbb{Z}}\mathbb{Q}$ is injective, $Cp_r \in \mathcal{O}$. But $\ell^r p_r \in \mathbb{Z}[\alpha] \subseteq \mathcal{O}$. Since ℓ and C are relatively prime, we have $p_r \in \mathcal{O}$.

Let $\delta = (1-p_r)\alpha$. Then $\delta^{\ell^{r-1}} = 1 - p_r$ and $p_r\Phi_{\ell^r}(\alpha) = 0$. Letting $\Delta = (1-p_r)\mathcal{O}$, $\mathcal{O}_r = p_r\mathcal{O}$, and $\alpha_r = p_r\alpha$, we obtain the desired result. □

Remark 5.2. Retaining the notation of Theorem 5.1 and its proof, let $\delta' = \delta + p_r \in \mathcal{O}$ and $\gamma_r = (1-p_r)+\alpha_r \in \mathcal{O}$. Then $\alpha = \delta'\gamma_r = \gamma_r\delta'$, $(\delta')^{\ell^{r-1}} = 1$, and $(\gamma_r - 1)\Phi_{\ell^r}(\gamma_r) = 0$. (Of course, this gives no additional information in the case $r = 1$.)

Remark 5.3. A computation shows that a formula for the idempotents $P_i(x) \in \ell^{-r}\mathbb{Z}[x]$ is given by

$$P_i(x) = \ell^{-r}\sum_{j=0}^{\ell^r-1} a_j x^j \quad \text{where } a_j = \begin{cases} \varphi(\ell^i) & \text{if } \ell^i \mid j, \\ -\ell^{i-1} & \text{if } \ell^i \nmid j \text{ but } \ell^{i-1} \mid j, \\ 0 & \text{otherwise.} \end{cases}$$

Example 5.4. The idempotents $p_0, \ldots, p_{r-1}$ in the proof of Theorem 5.1 are not necessarily elements of $\mathcal{O}$. For example, let $\mathcal{O}$ be the commutative ring of integer matrices of the form $\left(\begin{smallmatrix} a & b \\ b & a \end{smallmatrix}\right)$ and let $\alpha = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ $m = 1$, $r = 2$, and $\ell = 2$. Then

$$\alpha^2 = 1 \quad \text{and} \quad (\alpha - 1)^2 = \begin{pmatrix} 2 & -2 \\ -2 & 2 \end{pmatrix} \in 2\mathcal{O}.$$

However,

$$p_0 = \frac{1}{4}(1 + \alpha + \alpha^2 + \alpha^3) = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \notin \mathcal{O},$$

and

$$p_1 = \frac{1}{4}(1 - \alpha + \alpha^2 - \alpha^3) = \frac{1}{2}\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \notin \mathcal{O}.$$

Here, $p_2 = 0$.

6. Matrix rings

Lemma 6.1. *Suppose $\mathcal{O}$ is a commutative ring, the natural map $\mathcal{O} \to \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Q}$ is injective, ℓ is a rational prime, $1 + \ell\mathcal{O}$ has no $\mathcal{O}$-zero-divisors, and g is a positive integer. Then $1 + \ell M_g(\mathcal{O})$ has no $M_g(\mathcal{O})$-zero-divisors.*

Proof. Let $\mathcal{O}_\ell$ be the localization of $\mathcal{O}$ with respect to the multiplicative semigroup $1 + \ell\mathcal{O}$. Our assumptions on $\mathcal{O}$ and ℓ imply that the natural map $\mathcal{O} \to \mathcal{O}_\ell$ is injective. Assume that there are matrices $A, B \in M_g(\mathcal{O})$ such that $(1 + \ell A)B = 0$. We will show $B = 0$. The determinant of $1 + \ell A$ is in $1 + \ell\mathcal{O}$, and therefore is a unit in $\mathcal{O}_\ell$. Therefore $1 + \ell A$ has an inverse, call it Y, in $M_g(\mathcal{O}_\ell)$. Then $B = Y(1 + \ell A)B = 0$. We have shown that $1 + \ell M_g(\mathcal{O})$ has no $M_g(\mathcal{O})$-zero-divisors. □

Theorem 6.2. *Suppose n, k, and g are positive integers, $\mathcal{O}$ is a ring such that the natural map $\mathcal{O} \to \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Q}$ is injective, and either*

(a) *for every rational prime divisor ℓ of n, $\mathcal{O}$ has no non-zero infinitely ℓ-divisible elements, or*

(b) *$\mathcal{O}$ is commutative and for every rational prime divisor ℓ of n, $1 + \ell\mathcal{O}$ has no $\mathcal{O}$-zero-divisors.*

If $A \in M_g(\mathcal{O})$ is a matrix of finite multiplicative order such that $(A - I)^k \in nM_g(\mathcal{O})$, then $A^{R(k,n)} = I$.

Proof. Let ℓ be a prime divisor of n. In case (a), since $\mathcal{O}$ has no non-zero infinitely ℓ-divisible elements, neither does $M_g(\mathcal{O})$. By Lemmas 4.3 and 6.1, in both cases $1 + \ell M_g(\mathcal{O})$ has no $M_g(\mathcal{O})$-zero-divisors. Theorem 6.2 now follows from Theorem 4.4. □

In Theorem 6.3 below, the congruence condition on the $g \times g$ matrix A is that for some $t \in \{1,\dots,k\}$, A modulo 2^k can be viewed as a $t \times t$ matrix

$$\begin{pmatrix} I_{a_1} & & * \\ & \ddots & \\ 0 & & I_{a_t} \end{pmatrix}$$

whose entries b_{ij} are rectangular matrices such that for $i = 1,\dots,t$, the entry b_{ii} is a square identity matrix (not necessarily all of the same size), and such that for $i \geq j$, b_{ij} is a rectangular zero matrix.

Theorem 6.3. *Suppose k and g are positive integers, $k \geq 2$, $\mathcal{O}$ is a commutative ring, and the natural map $\mathcal{O} \to \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Q}$ is injective. Suppose that $1 + 2\mathcal{O}$ has no $\mathcal{O}$-zero-divisors. Suppose $A \in M_g(\mathcal{O})$ is a matrix of finite multiplicative order, and suppose that A modulo $2^k M_g(\mathcal{O})$ has main diagonal consisting of at most k square blocks of identity matrices and is zero below the diagonal blocks. Then $A = I$.*

Proof. The hypotheses imply that $(I - A)^k \in 2^k M_g(\mathcal{O})$. Since $R(k, 2^k) = 2$, by Theorem 6.2 we then have $A^2 = I$. This implies (for example, by induction on k) that $(I - A)^k = 2^{k-1}(I - A)$. Therefore $2^{k-1}(I - A) \in 2^k M_g(\mathcal{O})$, which implies that $I - A \in 2M_g(\mathcal{O})$. Therefore $A = I + 2B$ where $B \in M_g(\mathcal{O})$ and where B modulo $2M_g(\mathcal{O})$ consists of at most k square blocks of zero matrices on the main diagonal (corresponding to the blocks of identity matrices in A modulo $2^k M_g(\mathcal{O})$) and is zero below the diagonal blocks. Then $0 = I - A^2 = (I + A)(I - A) = 2(I + B)(I - A)$, so $0 = (I + B)(I - A)$. Taking the determinant we have $\det(I + B) \in 1 + 2\mathcal{O}$, so $\det(I + B)$ is a unit in the localization of $\mathcal{O}$ with respect to $1 + 2\mathcal{O}$. Thus the map defined by multiplication by $I + B$ is injective, so $I - A = 0$. □

Theorem 6.4. *Suppose n and g are positive integers, $n \geq 4$, $\mathcal{O}$ is a ring such that the natural map $\mathcal{O} \to \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Q}$ is injective, and either*

(a) *for every rational prime divisor ℓ of n, $\mathcal{O}$ has no non-zero infinitely ℓ-divisible elements, or*

(b) *$\mathcal{O}$ is commutative and for every rational prime divisor ℓ of n, $1 + \ell\mathcal{O}$ has no $\mathcal{O}$-zero-divisors.*

If $A \in M_g(\mathcal{O})$ is a matrix of finite multiplicative order, $0 \leq a \leq g$, and b is an $a \times (g - a)$ matrix over $\mathcal{O}$ such that

$$A \in \begin{pmatrix} I_a & b \\ 0 & I_{g-a} \end{pmatrix} + nM_g(\mathcal{O}),$$

then $A = I$.

Proof. The hypotheses imply that $(A-I)^2 \in nM_g(\mathcal{O})$. By Theorem 6.2, we then have $A=I$ if $n \geq 5$. Suppose $n=4$. Under the hypotheses in case (b), Theorem 6.4 follows by taking $k=2$ in Theorem 6.3. Now assume we are under the hypotheses in case (a). Then Theorem 6.2 implies that $A^2=I$. Write

$$A=\begin{pmatrix} I_a+4\alpha & \beta \\ 4\gamma & I_{g-a}+4\delta \end{pmatrix}$$

with matrices α, β, γ, and δ of appropriate sizes. Since $A^2=I$, we have $0=2\alpha+4\alpha^2+\beta\gamma$, $0=\beta+2\alpha\beta+2\beta\delta$, $0=\gamma+2\gamma\alpha+2\delta\gamma$, and $0=\gamma\beta+2\delta+4\delta^2$. By our assumptions, $\mathcal{O}$, and therefore also $M_g(\mathcal{O})$, has no non-zero infinitely 2-divisible elements. Therefore we have directly that $\beta=0$ and $\gamma=0$, from the second and third equations. Then the first and fourth equations similarly imply that $\alpha=0$ and $\delta=0$, so $A=I$. □

Example 6.5. (a) Let

$$A=\begin{pmatrix} 1 & -1 \\ 3 & -2 \end{pmatrix} \in M_2(\mathbb{Z}).$$

Then

$$A \in \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} + 3M_2(\mathbb{Z})$$

and A has multiplicative order 3.

(b) Let

$$A=\begin{pmatrix} -1 & 1 \\ -2 & 1 \end{pmatrix} \in M_2(\mathbb{Z}).$$

Then

$$A \in \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} + 2M_2(\mathbb{Z})$$

and A has multiplicative order 4.

Lemma 6.6. *Suppose $\mathcal{O}$ and $\bar{\mathcal{O}}$ are integral domains of characteristic zero, $\mathcal{O}$ is a subring of $\bar{\mathcal{O}}$, and every element of $\bar{\mathcal{O}}$ is integral over $\mathcal{O}$. If $v \in \mathcal{O}$ and v is not a unit in $\mathcal{O}$, then v is not a unit in $\bar{\mathcal{O}}$.*

Proof. Suppose $v^{-1} \in \bar{\mathcal{O}}$. Then v^{-1} is integral over $\mathcal{O}$, so there exist $m \in \mathbb{Z}^+$ and $a_0,\ldots,a_{m-1} \in \mathcal{O}$ such that $v^{-m}+a_{m-1}v^{1-m}+\cdots+a_1v^{-1}+a_0=0$. Multiplying by v^{m-1} and rearranging the equation gives $v^{-1}=-a_{m-1}-a_{m-2}v-\cdots-a_0v^{m-1}$. Therefore $v^{-1} \in \mathcal{O}$, contradicting the assumption. □

Theorem 6.7. *Suppose $\mathcal{O}$ is an integral domain of characteristic zero, n and k are positive integers such that no rational prime which divides n is a unit in $\mathcal{O}$, $A \in M_g(\mathcal{O})$*

satisfies $(A - I)^k \in nM_g(\mathcal{O})$, *and* λ *is an eigenvalue of* A *which is a root of unity. Then* $\lambda^{R(k,n)} = 1$.

Proof. View the eigenvalues of A as lying in the integral closure $\bar{\mathcal{O}}$ of $\mathcal{O}$ in an algebraically closed field containing $\mathcal{O}$. By Lemma 6.6, no rational prime which divides n is a unit in $\bar{\mathcal{O}}$. Write$(A - I)^k = nB$ with $B \in M_g(\mathcal{O})$. Then we have $(\lambda - 1)^k = n\mu$ where μ is an eigenvalue of B, so $\mu \in \bar{\mathcal{O}}$. Applying Corollary 3.3 to the ring $\bar{\mathcal{O}}$ and the element λ shows that λ is an $R(k,n)$th root of unity. □

Theorem 6.8. *Suppose* ℓ *is a prime,* B *is a ring such that the natural map* $B \to B \otimes_{\mathbb{Z}} \mathbb{Q}$ *is injective, and either*

(a) *B has no non-zero infinitely ℓ-divisible elements, or*

(b) *B is commutative and $1 + \ell B$ has no B-zero-divisors.*

Suppose m *and* r *are positive integers,* P *is a finitely generated projective right* B*-module, and* α *is an automorphism of* P *of finite order such that*

$$(\alpha - 1)^{m(\ell-1)\ell^{r-1}} \in \ell^m \mathit{End}_B(P).$$

Then P *is a direct sum of* α*-invariant right submodules* P_1 *and* P_2 *of* P *such that* $\alpha^{\ell^{r-1}}$ *acts as the identity on* P_1 *and* $\Phi_{\ell^r}(\alpha)$ *acts as the zero map on* P_2.

Proof. Since P is a finitely generated projective right B-module, it is a direct summand of a free right B-module of finite rank, say $B^g = P \oplus Q$. Therefore we can view the ring $\mathrm{End}_B(P)$ of right B-module endomorphisms of P as contained in the ring $M_g(B)$, with $\mathrm{End}_B(P) = \{\gamma \in M_g(B) : \ \gamma(P) \subseteq P, \gamma(Q) = 0\}$. Write 1_P, 1_Q, and I for the identity elements in $\mathrm{End}_B(P)$, $\mathrm{End}_B(Q)$, and $M_g(B)$, respectively. Then $I = 1_P + 1_Q$. Since the natural map $M_g(B) \to M_g(B) \otimes_{\mathbb{Z}} \mathbb{Q}$ is injective, so is the natural map $\mathrm{End}_B(P) \to \mathrm{End}_B(P) \otimes_{\mathbb{Z}} \mathbb{Q}$. In case (a), $M_g(B)$, and therefore $\mathrm{End}_B(P)$, has no non-zero infinitely ℓ-divisible elements, and by Lemma 4.3, $1_P + \ell\,\mathrm{End}_B(P)$ has no $\mathrm{End}_B(P)$-zero-divisors. In case (b), $I + \ell M_g(B)$ has no $M_g(B)$-zero-divisors by Lemma 6.1. If there were elements x, $y \in \mathrm{End}_B(P)$ such that $(1_P + \ell x)y = 0 = y(1_P + \ell x)$, then $(I + \ell x)y = 0 = y(I + \ell x)$ in $M_g(B)$, since $1_Q z = 0 = z 1_Q$ for every $z \in \mathrm{End}_B(P)$. Therefore $1_P + \ell\, \mathrm{End}_B(P)$ has no $\mathrm{End}_B(P)$-zero-divisors. Let $\mathcal{O}' = \mathrm{End}_B(P) \cap \mathbb{Q}[\alpha]$. Then $\mathcal{O}'$ is a commutative ring such that the natural map $\mathcal{O}' \to \mathcal{O}' \otimes_{\mathbb{Z}} \mathbb{Q}$ is injective, $1 + \ell\mathcal{O}'$ has no $\mathcal{O}'$-zero-divisors, and $(\alpha - 1)^{m(\ell-1)\ell^{r-1}} \in \ell^m \mathcal{O}'$. Theorem 5.1 provides an idempotent $p_r \in \mathcal{O}'$ such that, letting $\delta = (1 - p_r)\alpha \in \mathcal{O}'$ and $\alpha_r = p_r\alpha \in \mathcal{O}'$, we have $\delta^{\ell^{r-1}} = 1 - p_r$ and $p_r \Phi_{\ell^r}(\alpha) = 0$. Let $P_1 = \delta(P)$ and $P_2 = \alpha_r(P)$. Then $P = P_1 \oplus P_2$, and P_1 and P_2 satisfy the required conditions. □

Remark 6.9. A ring B satisfies (a) or (b) of Theorem 6.8 if and only if its opposite ring does. Therefore Theorem 6.8 also holds if the word "right" is everywhere replaced by "left".

Theorem 6.10. *Suppose ℓ is a prime, m and r are positive integers, $\mathcal{O}$ is an integral domain of characteristic zero with no non-zero infinitely ℓ-divisible elements, $\ell\mathcal{O}$ is a maximal ideal of $\mathcal{O}$, M is a free $\mathcal{O}$-module of finite rank, and A is an endomorphism of M of finite multiplicative order such that $(A-1)^{m(\ell-1)\ell^{r-1}} \in \ell^m \mathrm{End}(M)$.*

(a) *If $r > 1$, then the torsion subgroup of $M/(A-1)M$ is killed by ℓ^{r-1}.*

(b) *If $r = 1$, then the torsion subgroup of $M/(A-1)M$ is a vector space over $\mathcal{O}/\ell\mathcal{O}$ of dimension $c/(\ell-1)$ where c is the corank of the submodule in M of A-invariant elements.*

Proof. By Theorem 6.2 we have $A^{\ell^r} = 1$. By Theorem 6.8 we have $M \cong P_1 \oplus P_2$, with (torsion-free) A-invariant $\mathcal{O}$-modules P_1 and P_2, such that $A^{\ell^{r-1}}$ acts as the identity on P_1 and $\Phi_{\ell^r}(A)$ acts as zero on P_2. The torsion subgroup of $M/(A-1)M$ is the direct sum of the torsion subgroups of $P_1/(A-1)P_1$ and of $P_2/(A-1)P_2$. Let $f(x) = (x^{\ell^{r-1}} - 1)/(x-1) = 1 + x + x^2 + \cdots + x^{\ell^{r-1}-1} \in \mathbb{Z}[x]$. Then $f(x) - \ell^{r-1} \in (x-1)\mathbb{Z}[x]$. Suppose $m \in P_1$ and t is a positive integer such that $tm \in (A-1)P_1$. Then $f(A)tm \in f(A)(A-1)P_1 = (A^{\ell^{r-1}} - 1)P_1 = 0$. Since P_1 is torsion-free, $f(A)m = 0$. Therefore, $\ell^{r-1}m \in (A-1)P_1$. Thus, ℓ^{r-1} kills the torsion subgroup of $P_1/(A-1)P_1$. Let $\mathcal{O}' = \mathcal{O}[x]/\Phi_{\ell^r}(x)$. Then P_2 is an $\mathcal{O}'$-module. Since $\ell\mathcal{O}$ is a prime ideal in $\mathcal{O}$, $\Phi_{\ell^r}(x+1)$ is an Eisenstein polynomial over $\mathcal{O}$, so $\Phi_{\ell^r}(x)$ is irreducible, $\mathcal{O}'$ is an integral domain, and $\mathcal{O}'/(x-1)\mathcal{O}' \cong \mathcal{O}/\ell\mathcal{O}$. Let $\tilde{\mathcal{O}}$ be the localization of $\mathcal{O}'$ at the maximal ideal $(x-1)\mathcal{O}'$. Since $\mathcal{O}$ has no non-zero infinitely ℓ-divisible elements, and ℓ divides $(x-1)^{(\ell-1)\ell^{r-1}}$ in $\mathcal{O}'$, we have $\bigcap_{j \geq 1}((x-1)\mathcal{O}')^j = 0$. This implies that $\tilde{\mathcal{O}}$ is a principal ideal domain. Since $P_2 \otimes \tilde{\mathcal{O}}$ is a torsion-free $\tilde{\mathcal{O}}$-module, it is free, say of rank d. The torsion subgroup of $P_2/(A-1)P_2$ is isomorphic to the torsion $\mathcal{O}$-module $P_2 \otimes (\mathcal{O}'/(x-1)\mathcal{O}')$, and we have

$$P_2 \otimes (\mathcal{O}'/(x-1)\mathcal{O}') \cong P_2 \otimes (\tilde{\mathcal{O}}/(x-1)\tilde{\mathcal{O}}) \cong (\tilde{\mathcal{O}}/(x-1)\tilde{\mathcal{O}})^d \cong (\mathcal{O}/\ell\mathcal{O})^d.$$

Thus ℓ kills the torsion subgroup of $P_2/(A-1)P_2$. We therefore have (a). Now suppose $r = 1$. Then $P_1/(A-1)P_1 = 0$. Further, the set of A-invariants of M is P_1, so has corank equal to the $\mathcal{O}$-rank of P_2, which is $[\mathcal{O}' : \mathcal{O}]d = (\ell-1)d$. □

7. Quasi-unipotent elements

Definition 7.1. In a ring, an element α is:

(a) *nilpotent* if some positive integral power of α is 0,

(b) *unipotent* if $\alpha - 1$ is nilpotent,

(c) *quasi-unipotent* if some positive integral power of α is unipotent.

Every unipotent element is quasi-unipotent. Every quasi-unipotent element is a unit. If x and α are commuting elements of a ring, x is nilpotent, and α has finite multiplicative order, then $\alpha + x$ is quasi-unipotent.

Theorem 7.2. *Suppose $\mathcal{O}$ is a ring such that the natural map $\mathcal{O} \to \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Q}$ 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 a quasi-unipotent element of $\mathcal{O}$ and $(\alpha - 1)^k \in n\mathcal{O}$. Then $\alpha^{R(k,n)}$ is unipotent.*

Proof. Let $\mathcal{O}' = \mathcal{O} \cap \mathbb{Q}[\alpha]$, a commutative subring of $\mathcal{O}$. Let J be the ideal in $\mathcal{O}'$ consisting of all the nilpotent elements of $\mathcal{O}'$. First we will show that for every rational prime divisor ℓ of n, $1 + \ell(\mathcal{O}'/J)$ has no $\mathcal{O}'/J$-zero-divisors. If not, then there would exist elements x, $y \in \mathcal{O}'$ with $y \notin J$ and with $(1+\ell x)y \in J$. Then $(1+\ell x)^s y^s = 0$ for some positive integer s. Since $(1+\ell x)^s \in 1+\ell\mathcal{O}$, and $1+\ell\mathcal{O}$ has no $\mathcal{O}$-zero-divisors, we must have $y^s = 0$, contradicting that $y \notin J$. Therefore $1 + \ell(\mathcal{O}'/J)$ has no $\mathcal{O}'/J$-zero-divisors. Theorem 7.2 follows by applying Theorem 4.4 to the ring $\mathcal{O}'/J$ and the image of α in $\mathcal{O}'/J$. □

Example 7.3. Let

$$\alpha = \begin{pmatrix} 1 & 1 \\ -4 & -3 \end{pmatrix} \in \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} + 4M_2(\mathbb{Z}).$$

Then $(\alpha - I)^2 \in 4M_2(\mathbb{Z})$ and α is quasi-unipotent (since α^2 is unipotent) but α is not unipotent (its characteristic polynomial is $(x+1)^2$).

Theorem 7.4. *Suppose ℓ is a prime, m and r are positive integers, $\mathcal{O}$ is a commutative ring, the natural map $\mathcal{O} \to \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Q}$ is injective, $1+\ell\mathcal{O}$ has no $\mathcal{O}$-zero-divisors, $\alpha \in \mathcal{O}$ is a quasi-unipotent element, and*

$$(\alpha - 1)^{m(\ell-1)\ell^{r-1}} \in \ell^m \mathcal{O}.$$

Then there are rings Δ and $\mathcal{O}_r$ in $\mathcal{O}$ and elements $\delta \in \Delta$ and $\alpha_r \in \mathcal{O}_r$ such that $\mathcal{O} = \Delta \oplus \mathcal{O}_r$, $\alpha = \delta + \alpha_r$, $\delta^{\ell^{r-1}}$ is a unipotent element in Δ, and $\Phi_{\ell^r}(\alpha_r)$ is a nilpotent element in $\mathcal{O}_r$.

Proof. The proof is similar to the proof of Theorem 5.1. By Theorem 7.2, α^{ℓ^r} is unipotent. Therefore, there is a positive integer s such that $(\alpha^{\ell^r} - 1)^s = 0$, and $\mathbb{Q}[\alpha]$ is a finite dimensional commutative $\mathbb{Q}$-algebra. Sending x to α gives a surjective $\mathbb{Q}$-algebra homomorphism

$$\bigoplus_{i=0}^{r} \mathbb{Q}[x]/\Phi_{\ell^i}(x)^s \cong \mathbb{Q}[x]/(x^{\ell^r} - 1)^s \quad \to \quad \mathbb{Q}[\alpha].$$

This defines idempotents (not necessarily non-zero) $p_0, \dots, p_r$ in $\mathbb{Q}[\alpha]$ such that $p_0 + \cdots + p_r = 1$ and $p_i \Phi_{\ell^i}(\alpha)^s = 0$ for $i = 0, \dots, r$. Let $\delta = 1 - p_r$, $\Delta = \delta\mathcal{O}$, $\mathcal{O}_r = p_r\mathcal{O}$, and $\alpha_r = p_r\alpha$. The theorem will follow once we show δ, $p_r \in \mathcal{O}$. Define β as in the proof of Theorem 5.1; then $\beta^m \in \ell^m\mathcal{O}$. Let J be the ideal of $\mathbb{Q}[\alpha]$ consisting of the nilpotent elements. Then $p_0\beta \in J$, and by (1), $p_i(\beta - \ell^{\ell^{r-i}}) \in J$ for $1 \le i \le r$. Let A be a positive integer such that $p_0\beta^A = 0$ and $p_i(\beta^m - \ell^{m\ell^{r-i}})^A = 0$ for $1 \le$

$i \le r$. First suppose $r = 1$, and take $\gamma \in \mathcal{O}$ such that $\beta^{mA} = \ell^{mA}\gamma$. Then $p_0\gamma = 0$ and $p_1(1-\gamma)^A = 0$. Therefore, $p_0 = (1-\gamma)^A \in \mathcal{O}$, and $p_1 = 1 - p_0 \in \mathcal{O}$. Now suppose $r > 1$, and define B and C as in the proof of Theorem 5.1. Then $B \in \ell^{mr}\mathcal{O}$ and $B^A = p_rB^A \in \ell^{mrA}Cp_r + p_rJ$. Write $B^A = \ell^{mrA}\eta$ with $\eta \in \mathcal{O}$. Then $p_r\eta = \eta$ and $\ell^{mrA}p_r(C-\eta) \in p_rJ$, so $\ell^{mrAt}p_r(C-\eta)^t = 0$ for some positive integer t. Now $C-\eta = \delta C + p_r(C-\eta)$, so $(C-\eta)^t = \delta C^t$. Then $p_rC^t = C^t - \delta C^t = C^t - (C-\eta)^t \in \mathcal{O}$. Since ℓ and C are relatively prime, we will know p_r (and therefore also δ) is in $\mathcal{O}$ once we know that $\ell^d p_r \in \mathbb{Z}[\alpha] \subseteq \mathcal{O}$ for some non-negative integer d. This follows from the fact that the resultant of the polynomials $\Phi_{\ell^r}(x)^s$ and $\prod_{i=0}^{r-1} \Phi_{\ell^i}(x)^s$ is a power of ℓ. □

8. Semi-abelian varieties

Theorem 8.1. *Suppose G is a commutative group scheme over a field, which is an extension of an abelian variety by a torus, n, k, and s are positive integers, s and n are relatively prime, $\alpha \in End(G) \otimes_{\mathbb{Z}} \mathbb{Z}[1/s]$, α has finite multiplicative order, and $(\alpha - 1)^k$ is 0 on the scheme-theoretic kernel of multiplication by n on G. Then $\alpha^{R(k,n)} = 1$. In particular, if $n \notin N(k)$ then $\alpha = 1$.*

Proof. Let $\mathcal{O} = \mathrm{End}(G) \otimes_{\mathbb{Z}} \mathbb{Z}[1/s]$. Since $(\alpha - 1)^k$ is 0 on the scheme-theoretic kernel of multiplication by n, we have $(\alpha - 1)^k \in n\mathcal{O}$. Since $\mathrm{End}(G)$ is a finitely generated free $\mathbb{Z}$-module and s and n are relatively prime, $\mathcal{O}$ has no non-zero infinitely ℓ-divisible elements, if ℓ is a rational prime divisor of n. Thus, $\mathcal{O}$, α, and n satisfy the hypotheses of Theorem 4.4. □

Theorem 8.2. *Suppose G is a commutative group scheme over a field, which is an extension of an abelian variety by a torus, ℓ is a rational prime, m and r are positive integers, α is an automorphism of G of finite multiplicative order, and $(\alpha-1)^{m(\ell-1)\ell^{r-1}}$ is 0 on the scheme-theoretic kernel of multiplication by ℓ^m. Then G is the direct sum of α-invariant connected subschemes G_1 and G_2 such that G_1 is the identity component of $ker(1 - \alpha^{\ell^{r-1}})$ and G_2 is the identity component of $ker(\Phi_{\ell^r}(\alpha))$.*

Proof. Let $\mathcal{O} = \mathrm{End}(G) \cap \mathbb{Q}[\alpha]$. Then $\mathcal{O}$ is a commutative subring of $\mathrm{End}(G)$, and the natural map $\mathcal{O} \to \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Q}$ is injective. There are no non-zero infinitely ℓ-divisible elements in $\mathrm{End}(G)$, and therefore in $\mathcal{O}$, so $1 + \ell\mathcal{O}$ has no $\mathcal{O}$-zero-divisors by Lemma 4.3. Let $p \in \mathcal{O}$ be the idempotent p_r obtained in Theorem 5.1, let $G_1 = (1-p)(G) = \ker(p)$, and let $G_2 = p(G) = \ker(1-p)$. Then $\alpha^{\ell^r} = 1$, G_1 and G_2 are α-invariant subschemes of G, $G = G_1 \oplus G_2$, and G_1 and G_2 are connected. By Remark 5.3 and the identity $\Phi_\ell(x^{\ell^{r-1}}) = \Phi_{\ell^r}(x)$, we have $p = 1 - \ell^{-1}\Phi_\ell(\alpha^{\ell^{r-1}}) = 1 - \ell^{-1}\Phi_{\ell^r}(\alpha)$. Therefore, $\ell(1-p) = \Phi_{\ell^r}(\alpha)$. Note also that $1 - x^{\ell^{r-1}}$ divides $\ell - \Phi_{\ell^r}(x)$. We then have

$$\ell\ker(1 - \alpha^{\ell^{r-1}}) \subseteq \ell\ker(\ell - \Phi_{\ell^r}(\alpha)) = \ell\ker(\ell p) \subseteq G_1 = \ker(p) \subseteq \ker(1 - \alpha^{\ell^{r-1}}),$$

$$\ell\ker(\Phi_{\ell^r}(\alpha)) = \ell\ker(\ell(1-p)) \subseteq G_2 = \ker(1-p) \subseteq \ker(\Phi_{\ell^r}(\alpha)).$$

Therefore, $\ker(1-\alpha^{\ell^{r-1}})/G_1$ and $\ker(\Phi_{\ell^r}(\alpha))/G_2$ are killed by ℓ, and so are finite. Therefore, G_1 is the identity component of $\ker(1-\alpha^{\ell^{r-1}})$ and G_2 is the identity component of $\ker(\Phi_{\ell^r}(\alpha))$. □

In the following result, a quasi-unipotent endomorphism means an endomorphism α such that $(\alpha^s-1)^t=0$ for some positive integers s and t.

Theorem 8.3. *Suppose G is a commutative group scheme over a field, which is an extension of an abelian variety by a torus, ℓ is a rational prime, m and r are positive integers, α is an automorphism of G which is a quasi-unipotent endomorphism, and $(\alpha-1)^{m(\ell-1)\ell^{r-1}}$ is 0 on the scheme-theoretic kernel of multiplication by ℓ^m. Then G is the direct sum of α-invariant subschemes G_1 and G_2 with the properties that $\alpha^{\ell^{r-1}}$ acts as a unipotent endomorphism on G_1 and $\Phi_{\ell^r}(\alpha)$ acts as a nilpotent endomorphism on G_2.*

Proof. The proof parallels the proof of Theorem 8.2, with Theorem 7.4 invoked in place of Theorem 5.1. □

9. ℓ-adic representations and étale cohomology

Lemma 9.1. *Suppose that b, k, m, and n are positive integers, m and n are relatively prime, and for each prime divisor q of n we have a matrix $A_q\in M_b(\mathbb{Z}_q)$ such that the characteristic polynomials of the A_q have coefficients in $\mathbb{Z}[1/m]$ independent of q, and such that $(A_q-I)^k\in nM_b(\mathbb{Z}_q)$. Suppose ℓ is a prime divisor of n and v is a kth root of n in an algebraic closure of $\mathbb{Q}_\ell$. Then for every eigenvalue α of A_ℓ, $v^{-1}(\alpha-1)$ satisfies a monic polynomial with coefficients in $\mathbb{Z}[1/m]$.*

Proof. Let $v_1,\dots,v_k$ denote the kth roots of n in an algebraic closure of $\mathbb{Q}_\ell$. If α is an eigenvalue of A_ℓ, then $(\alpha-1)^k/n$ is an eigenvalue of $n^{-1}(A_\ell-I)^k\in M_b(\mathbb{Z}_\ell)$. Thus $(\alpha-1)^k/n$, and therefore also the numbers $v_j^{-1}(\alpha-1)$, satisfy monic polynomials with coefficients in $\mathbb{Z}_\ell$. Let $f(x)=\det(A_\ell-Ix)\in\mathbb{Z}[1/m][x]$, the characteristic polynomial of A_ℓ. Let

$$h(x)=n^{-b}\prod_{j=1}^{k}f(1+v_jx)=\prod_{j=1}^{k}\det(v_j^{-1}(A_\ell-I)-Ix)\in\mathbb{Z}[(mn)^{-1}][x].$$

The roots of h are exactly the numbers $v_j^{-1}(\alpha-1)$ for eigenvalues α of A_ℓ and for $j\in\{1,\dots,k\}$. Therefore the coefficients of h satisfy monic polynomials with coefficients in $\mathbb{Z}_\ell$, but are also in $\mathbb{Z}[(mn)^{-1}]$, so lie in $\mathbb{Z}[(mn)^{-1}]\cap\mathbb{Z}_q$ for every prime divisor q of n. Since $\bigcap_{q|n}(\mathbb{Z}[(mn)^{-1}]\cap\mathbb{Z}_q)=\mathbb{Z}[1/m]$, we have $h\in\mathbb{Z}[1/m][x]$. Therefore, $v^{-1}(\alpha-1)$ satisfies the monic polynomial $h\in\mathbb{Z}[1/m][x]$, whenever α is an eigenvalue of A_ℓ and v is a kth root of n. □

Lemma 9.2 (Silverberg and Zarhin [15, Proposition 2.5]). *Suppose φ is an invertible linear operator on a finite-dimensional vector space V over a field of characteristic zero. Then the multiplicative group generated by the eigenvalues of φ contains no non-trivial roots of unity if and only if the smallest algebraic subgroup of $GL(V)$ containing φ is connected.*

If F is a field, let F^s denote a separable closure of F and let G_F denote $\mathrm{Gal}(F^s/F)$. We recall some definitions from Chapter I of [11] relating to ℓ-adic representations. Since these definitions make sense not only for number fields, but also for global fields, we will allow such generality. See [18] for the theory of global fields.

If ℓ is a prime number, an *ℓ-adic representation* of G_F is a continuous homomorphism $\rho_\ell\colon G_F \to \mathrm{Aut}(V_\ell)$, where V_ℓ is a finite dimensional vector space over $\mathbb{Q}_\ell$. A *lattice* of V_ℓ is a sub-$\mathbb{Z}_\ell$-module of V_ℓ which is free of finite rank and generates V_ℓ over $\mathbb{Q}_\ell$.

Suppose from now on that F is a global field. Let Σ_F denote the set of all finite places of F, i.e., the set of all normalized discrete valuations of F. If $v \in \Sigma_F$, let κ_v denote the residue field of v, and let q_v denote the cardinality of the finite field κ_v. If L is a finite Galois extension of F in F^s, and $w \in \Sigma_L$ is a place of L extending v, let I_w and D_w denote, respectively, the inertia and decomposition groups of w. We have $I_w \subseteq D_w \subseteq \mathrm{Gal}(L/F)$. The quotient group D_w/I_w is a finite cyclic group which can be canonically identified with $\mathrm{Gal}(\kappa_w/\kappa_v)$, and has a canonical generator ϕ_w which corresponds to the Frobenius element (raising to the q_vth power) in $\mathrm{Gal}(\kappa_w/\kappa_v)$. If L is an arbitrary Galois extension of F in F^s, let Σ_L denote the projective limit of the sets Σ_M where M ranges over the finite extensions of F in L. If $w \in \Sigma_L$, then D_w, I_w, and ϕ_w can be defined as above.

If $\rho_\ell : G_F \to \mathrm{Aut}(V_\ell)$ is an ℓ-adic representation and $v \in \Sigma_F$, we say ρ_ℓ is *unramified* at v if for every extension w of v to F^s, ρ_ℓ is trivial on the inertia group I_w of w. If ρ_ℓ is unramified at v, then the restriction of ρ_ℓ to D_w factors through D_w/I_w, so $\rho_\ell(\phi_w)$ is defined. We call $\rho_\ell(\phi_w)$ a Frobenius element associated to v, and denote it $Fr_{\ell,w}$. The conjugacy class of $Fr_{\ell,w}$ in $\mathrm{Aut}(V_\ell)$ is independent of w, so the characteristic polynomial $P_{v,\ell}$ of $Fr_{\ell,w}$ is well-defined and depends only on ρ_ℓ and v (see p. I-6 of [11] and p. 108 of [17]).

Definition 9.3. If S is a set of prime numbers which does not contain $\mathrm{char}(F)$, we call a system $\{\rho_\ell\colon \ell \in S\}$ of ℓ-adic representations of G_F an *almost integral compatible system of ℓ-adic representations* if for every pair of prime numbers ℓ and ℓ' in S there is a subset $S_{\ell,\ell'}$ of Σ_F of density zero such that if $v \in \Sigma_F - S_{\ell,\ell'}$, and p is the residue characteristic of v, then

(a) ρ_ℓ and $\rho_{\ell'}$ are unramified at v,

(b) $P_{v,\ell}$ and $P_{v,\ell'}$ have coefficients in $\mathbb{Z}[1/p]$, and

(c) $P_{v,\ell} = P_{v,\ell'}$.

We remark that when F is a number field, every compatible system of integral ℓ-adic representations (I.2 of [11]) is an almost integral compatible system of ℓ-adic representations.

Theorem 9.4. *Suppose k and n are positive integers, and F is a global field of characteristic not dividing n. Suppose that S is a set of prime numbers which contains all the prime divisors of n but does not contain char(F), and suppose $\{\rho_\ell\colon \ell \in S\}$ is an almost integral compatible system of ℓ-adic representations*

$$\rho_\ell : G_F \to Aut(V_\ell).$$

Suppose that for every prime divisor q of n, T_q is a G_F-invariant lattice in V_q such that for every $\sigma \in G_F$,

$$(\rho_q(\sigma) - 1)^k \in n\,End(T_q).$$

Suppose $\ell \in S$, let $\mathcal{Z}_\ell$ be the Zariski closure of the image of G_F under ρ_ℓ, and let Φ_ℓ denote the (finite) group of connected components of $\mathcal{Z}_\ell$. Then the exponent of the group Φ_ℓ divides $R(n,k)$. In particular, if $n \notin N(k)$, then $\mathcal{Z}_\ell$ is connected.

Proof. Let $\mathcal{Z}'$ be a connected component of $\mathcal{Z}_\ell$. It follows easily from the Chebotarev density theorem (Theorem 12 on p. 289 of [18]) that we can find a place $v \in \Sigma_F - \bigcup_{q|n\ell} S_{\ell,q}$, of residue characteristic p not dividing n, and a Frobenius element $Fr_{\ell,w} \in \mathrm{Im}(\rho_\ell)$ associated to v, such that $Fr_{\ell,w} \in \mathcal{Z}'$. Let $\varphi = Fr_{\ell,w}$. Applying Lemma 9.1 to the Frobenius elements $Fr_{q,w}$ for all prime divisors q of n, we conclude that the eigenvalues α of φ satisfy $(\alpha - 1)^k \in n\bar{\mathbb{Z}}[1/p]$, where $\bar{\mathbb{Z}}$ denotes the ring of algebraic integers. Let $D = \det(\varphi)$. Then D is the product of the eigenvalues of φ, and $D \in (1 + n^{1/k}\bar{\mathbb{Z}}[1/p]) \cap \mathbb{Z}[1/p]$. It follows that D can be written as a fraction such that no prime divisor of n divides the numerator or denominator. Let M be the multiplicative group generated by the eigenvalues of φ. Then M is a multiplicative subgroup of the multiplicative semi-group $1 + n^{1/k}\bar{\mathbb{Z}}[1/p, 1/D]$. Applying Corollary 3.3 to $\mathcal{O} = \bar{\mathbb{Z}}[1/p, 1/D]$, we conclude that every root of unity λ in M satisfies $\lambda^{R(n,k)} = 1$. Let M' be the multiplicative group generated by the eigenvalues of $\varphi^{R(n,k)}$. Then $M' = \{\beta^{R(n,k)} : \beta \in M\}$, so M' contains no non-trivial roots of unity. By Lemma 9.2, the smallest algebraic subgroup G of $\mathrm{Aut}(T_\ell)$ containing $\varphi^{R(n,k)}$ is connected. Therefore, $\varphi^{R(n,k)} \in G \subseteq \mathcal{Z}_\ell^0$, the identity connected component of $\mathcal{Z}_\ell$. Since $\mathcal{Z}'$ is a coset of $\mathcal{Z}_\ell^0$, we have $\mathcal{Z}' = \varphi\mathcal{Z}_\ell^0$. Therefore, $y^{R(n,k)} \in \mathcal{Z}_\ell^0$ for every $y \in \mathcal{Z}'$. □

Suppose X is a smooth projective variety over a global field F. Let $\bar{X} = X \times_F F^s$, the variety obtained by extension of scalars. Suppose i and j are integers and $j \geq 0$. Then G_F acts on $H^j(\bar{X}, \mathbb{Z}/m\mathbb{Z})(i)$ for every positive integer m not divisible by char(F), and therefore acts on the twisted étale cohomology groups $H^j(\bar{X}, \mathbb{Z}_\ell)(i)$ for every prime $\ell \neq$ char(F). If ℓ is a prime and $\ell \neq$ char(F), let L_ℓ be the quotient of $H^j(\bar{X}, \mathbb{Z}_\ell)(i)$ by its torsion subgroup. Then L_ℓ is a $\mathbb{Z}_\ell$-lattice, and we can (non-canonically) identify

$\mathrm{Aut}(L_\ell)$ with $GL_b(\mathbb{Z}_\ell)$, where b is the jth Betti number of $\bar{X}$ (note that b is independent of ℓ). Let ρ_ℓ denote the associated ℓ-adic representation (see Section 2 of [10]),

$$\rho_\ell : G_F \to GL_b(\mathbb{Z}_\ell).$$

Corrollary 9.5. *Suppose X is a smooth projective variety over a global field F. Suppose i is an integer, n and k are positive integers, j is a non-negative integer, ℓ is a prime number, and char(F) does not divide $n\ell$. Suppose that for every $\sigma \in G_F$, $(\sigma - 1)^k$ kills $H^j(\bar{X}, \mathbb{Z}/n\mathbb{Z})(i)$. Let $\mathcal{Z}_\ell$ be the Zariski closure of the image of G_F under ρ_ℓ, and let Φ_ℓ denote the (finite) group of connected components of $\mathcal{Z}_\ell$. Then the exponent of the group Φ_ℓ divides $R(n,k)$. In particular, if $n \notin N(k)$, then $\mathcal{Z}_\ell$ is connected.*

Proof. For every prime $q \neq \mathrm{char}(F)$ and positive integer r, there is a natural injection of $H^j(\bar{X}, \mathbb{Z}_q)(i) \otimes \mathbb{Z}/q^r\mathbb{Z}$ into $H^j(\bar{X}, \mathbb{Z}/q^r\mathbb{Z})(i)$ (see Lemma 1.11 in Chapter V of [7]). Suppose that $\sigma \in G_F$. Since $(\sigma - 1)^k$ kills $H^j(\bar{X}, \mathbb{Z}/n\mathbb{Z})(i)$, we have that $(\rho_q(\sigma) - 1)^k \in nM_b(\mathbb{Z}_q)$ for every prime $q \neq \mathrm{char}(F)$ (where b is the jth Betti number of $\bar{X}$). By [3, 4], the representations ρ_ℓ for $\ell \neq \mathrm{char}(F)$ form an almost integral compatible system of ℓ-adic representations. We now apply Theorem 9.4. □

Remark 9.6. Conjecturally, an analogue of Corollary 9.5 holds with the twisted étale cohomology group replaced by the $\mathbb{Z}$-form of a motive (as defined on p. 387 of [12]). In this setting, the Weil conjecture on the independence of the characteristic polynomial of Frobenius is an open question (see Conjecture 12.5 of [12]).

Remark 9.7. Corollary 9.5 remains true for varieties over finitely generated extensions of $\mathbb{Q}$. The proof is based on the Chebotarev density theorem for these extensions (Theorem on p. 206 of [5]) and a variant of Theorem 9.4. This variant is obtained by modifying the notion of almost integral compatible system of ℓ-adic representations to this setting (compare with pp. 108–109 of [17]).

Acknowledgements

The first author would like to thank the NSF for financial support.

References

[1] A. Borel, Introduction aux Groupes Arithmétiques, Actualités Scientifiques et Industrielles, Vol. 1341 (Hermann, Paris, 1969).

[2] N. Bourbaki, Groupes et Algèbres de Lie (Hermann, Paris, 1972) Chap. 3.

[3] P. Deligne, La conjecture de Weil I, Inst. Hautes Études Sci. Publ. Math. 43 (1974) 273–307.

[4] P. Deligne, La conjecture de Weil II, Inst. Hautes Études Sci. Publ. Math. 52 (1980) 137–252.

[5] G. Faltings, Complements to Mordell, in: G. Faltings et al., Rational Points (Third Enlarged Edition), (Friedr. Vieweg & Sohn, Braunschweig/Wiesbaden, 1992) Chap. VI.

[6] A. Grothendieck, Modèles de Néron et monodromie, in: A. Grothendieck, ed., Groupes de Monodromie en Géometrie Algébrique, SGA7 I, Lecture Notes in Math. 288 (Springer, Berlin, 1972) 313–523.

[7] J. S. Milne, Étale Cohomology (Princeton Univ. Press, Princeton, 1980).

[8] H. Minkowski, Gesammelte Abhandlungen, Bd. I, Leipzig, 1911, pp. 212-218 (Zur Theorie der positiven quadratischen Formen, J. reine angew. Math. 101 (1887) 196–202).

[9] J-P. Serre, Rigidité du foncteur de Jacobi d'echelon $n \geq 3$, Appendix to A. Grothendieck, Techniques de construction en géométrie analytique, X. Construction de l'espace de Teichmüller, Séminaire Henri Cartan, 1960/61, no. 17.

[10] J-P. Serre, Représentations ℓ-adiques, in: Kyoto Int. Symp. on Algebraic Number Theory, Japan Soc. for Promotion of Sci. (1977) 177–193.

[11] J-P. Serre, Abelian ℓ-adic Representations and Elliptic Curves, 2nd ed. (Addison-Wesley, Redwood City, CA, 1989).

[12] J-P. Serre, Propriétés conjecturales des groupes de Galois motiviques et des représentations ℓ-adiques, in: U. Jannsen, S. Kleiman, J-P. Serre, eds., Motives, Proc. Symp. Pure Math. 55 (1994) Part 1, 377–400.

[13] A. Silverberg and Yu. G. Zarhin, Isogenies of abelian varieties, J. Pure Appl. Algebra 90 (1993) 23–37.

[14] A. Silverberg and Yu. G. Zarhin, Semistable reduction and torsion subgroups of abelian varieties, Ann. Inst. Fourier 45 (1995) 403–420.

[15] A. Silverberg and Yu. G. Zarhin, Connectedness results for ℓ-adic representations associated to abelian varieties, Comp. Math. 97 (1995) 273–284.

[16] D. A. Suprunenko, Matrix groups, Translations of Mathematical Monographs 45 (Amer. Math. Soc., Providence, 1976) (translation of Gruppy Matrits, Moscow, 1972).

[17] J. Tate, Algebraic cycles and poles of zeta functions, in: O. F. G. Schilling, ed., Arithmetical Algebraic Geometry, Proc. Conf. Purdue Univ., 1963 (Harper and Row, New York, 1965) 93–110.

[18] A. Weil, Basic Number Theory (Springer, Berlin, 1967).