Journal de Théorie des Nombres de Bordeaux

anciennement Séminaire de Théorie des Nombres de Bordeaux

Marco ILLENGO

**Cohomology of integer matrices and local-global divisibility on the torus**

Tome 20, nº 2 (2008), p. 327-334.

<http://jtnb.cedram.org/item?id=JTNB_2008__20_2_327_0>

*Journal de Théorie des Nombres de Bordeaux* **20** (2008), 327-334

# Cohomology of integer matrices and local-global divisibility on the torus

par Marco ILLENGO

Résumé. Soient $p \neq 2$ un nombre premier et $G$ un $p$-groupe de matrices dans $\mathrm{SL}_n(\mathbb{Z})$, pour un nombre entier $n$. Dans cet article nous montrons que, pour $n < 3(p-1)$, un certain sous-groupe du groupe de cohomologie $H^1(G, \mathbb{F}_p^n)$ est trivial. Nous montrons aussi que cette affirmation peut être fausse pour $n \geqslant 3(p-1)$. Avec un résultat de Dvornicich et Zannier (voir [2]), nous obtenons que le principe local-global de divisibilité pour $p$ vaut pour tout tore algébrique de dimension $n < 3(p-1)$.

Abstract. Let $p \neq 2$ be a prime and let $G$ be a $p$-group of matrices in $\mathrm{SL}_n(\mathbb{Z})$, for some integer $n$. In this paper we show that, when $n < 3(p-1)$, a certain subgroup of the cohomology group $H^1(G, \mathbb{F}_p^n)$ is trivial. We also show that this statement can be false when $n \geqslant 3(p-1)$. Together with a result of Dvornicich and Zannier (see [2]), we obtain that any algebraic torus of dimension $n < 3(p-1)$ enjoys a local-global principle on divisibility by $p$.

## 1. Introduction

Let $G$ be a subgroup of $\mathrm{SL}_n(\mathbb{Z})$, for some $n$. Then $G$ acts on $\mathbb{Z}^n$ and, by projection, on $\mathbb{F}_p^n$, for some prime $p$. Consider the group cohomology of the couple $(G, \mathbb{F}_p^n)$ and note that, for every subgroup $C$ of $G$, there is a well-defined restriction map $H^1(G, \mathbb{F}_p^n) \to H^1(C, \mathbb{F}_p^n)$. In this paper we prove the following theorem.

**Theorem 1.** *Let $p \neq 2$ be a prime and let $n < 3(p-1)$. For every $p$-group $G$ in $\mathrm{SL}_n(\mathbb{Z})$ the projection $H^1(G, \mathbb{F}_p^n) \xrightarrow{\varphi} \prod H^1(C, \mathbb{F}_p^n)$, the product being taken on all cyclic subgroups $C$ of $G$, is injective.*

We also prove that this statement is 'best possible' on $n$.

**Proposition 2.** *Let $p \neq 2$ be a prime and let $n \geqslant 3(p-1)$. There exists a $p$-group $G$ in $\mathrm{SL}_n(\mathbb{Z})$ such that the map $H^1(G, \mathbb{F}_p^n) \xrightarrow{\varphi} \prod H^1(C, \mathbb{F}_p^n)$, the product being taken on all cyclic subgroups $C$ of $G$, is not injective.*

---

Manuscrit reçu le 21 janvier 2008.

Our Theorem 1 is motivated by a paper of Dvornicich and Zannier on local-global divisibility for algebraic groups. In [2, Sections 4-5] they proved that local-global divisibility by a prime $p$ holds on every algebraic torus of dimension $n \leqslant \max\{3, 2(p-1)\}$, but fails for at least one torus of dimension $n = p^4 - p^2 + 1$. (We are using the additive notation for the torus: division by $p$ corresponds to taking $p$-th roots in the multiplicative group $\mathbb{G}_m$.)

The authors also suggested that their proof of the condition $n \leqslant 2(p-1)$ in the case $p \neq 2$ could be adapted to prove local-global divisibility by $p$ under a weaker condition, so to reduce the gap of uncertainty for $n$. In particular, in the first part of their proof they show that, for $p \neq 2$ and $n$ fixed, the injectivity of $\varphi$ for any $p$-group $G < \mathrm{SL}_n(\mathbb{Z})$ implies local-global divisibility by $p$ for every algebraic torus of dimension $n$.

Together with this result, Theorem 1 allows to replace the condition $n \leqslant 2(p-1)$ with the weaker condition $n < 3(p-1)$.

**Theorem 3.** *Let $p \neq 2$ be a prime, $k$ be a number field, and $\mathcal{T}$ be an algebraic $k$-torus of dimension $n < 3(p-1)$. Fix any point $P \in \mathcal{T}(k)$; if for all but a finite number of completions $k_\nu$ of $k$ there exists a point $D_\nu \in \mathcal{T}(k_v)$ with $pD_\nu = P$, then there exists a $D \in \mathcal{T}(k)$ such that $pD = P$.*

Using the terminology of [2], we say that a cocycle $Z$ on $(G, \mathbb{F}_p^n)$ *satisfies the local conditions* if for every $g \in G$ there exists a $W_g \in \mathbb{F}_p^n$ such that $Z_g = gW_g - W_g$. Note that the set of cocycles that satisfy the local conditions is precisely the kernel of $\varphi$.

For $p \neq 2$ and $n \geqslant 3(p-1)$ the example in Proposition 2 allows, as Dvornicich and Zannier pointed out in [2, Section 4] and [3, Section 3], to build an algebraic torus of dimension $n$ defined over some number field $k$ and, possibly extending the field $k$, a $k$-rational point on the torus for which the local-global divisibility by $p$ fails.

In Section 2 we shall prove Theorem 1, using some elementary results of the geometry of numbers and of the theory of representations.

In Section 3 we shall prove Proposition 2 for the case $n = 3(p-1)$; the general case can be obtained by means of a direct sum with the trivial representation of dimension $n - 3(p-1)$.

Throughout this paper, whenever their orders are known, we shall denote by $I$ the identity matrix and by $O$ the null matrix.

## 2. Proof of theorem

We begin the proof of Theorem 1 by an inspection of the $p$-group $G$. The following result is slightly more general than needed.

**Lemma 4.** *Let $p$ be a prime and let $G$ be a $p$-group of matrices in $\mathrm{SL}_n(\mathbb{Q})$. If $n < p(p-1)$ then $G$ is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^b$, for some $b \leqslant n/(p-1)$.*

*Proof.* Note that any non-trivial element $g$ of $G$ is a matrix of multiplicative order $p^m$, for some positive integer $m$. Then at least one of the eigenvalues of $g$ is a $p^m$-th primitive root of unity; since $g$ is defined over $\mathbb{Q}$, every $p^m$-th primitive root of unity must be an eigenvalue of $g$. This implies that the number of eigenvalues of $g$, bounded by its order $n < p(p-1)$, is at least $\phi(p^m) = p^{m-1}(p-1)$. It follows that $m = 1$, i.e. that $g$ has order $p$. Thus $G$ has exponent $p$.

Let now $K$ be $(\mathbb{Z}/p\mathbb{Z})^*$; we say that two elements, $g$ and $h$, of $G$ are *$K$-conjugate* if there exists a $k \in K$ such that $g^k$ and $h$ are conjugate by an element of $G$. By the theory of characters for finite representations (see [4, Section 12.3]), the number of representations of $G$ which are irreducible over $\mathbb{Q}$ is equal to the number of $K$-conjugation classes of $G$. Now, let $g$ be a non-trivial element of $G$ and assume that it is conjugate to $g^k$, for some $k \in K$. This means that there exists an element $h$ in $G$ such that conjugation by $h$ maps $g$ to $g^k$. This implies that conjugation by $h^p$ maps $g$ to $g^{k^p} = g^k$; on the other hand $h^p$ is the neuter element, thus $g^k = g$. This shows that any two distinct powers of a same element are not conjugate, and that every $K$-conjugation class of $G$ - except the class of the identity element - is the union of $p-1$ distinct conjugation classes of $G$. In other words, every $\mathbb{Q}$-irreducible representation of $G$ is equivalent to the direct sum of the distinct conjugates of some $\mathbb{C}$-irreducible representation of $G$.

Now, if the group $G$ was non-commutative, its faithful representation $G$ would contain an irreducible representation of degree $d \geqslant p$, thus also a $\mathbb{Q}$-irreducible representation of degree $(p-1)d \geqslant (p-1)p > n$, which is not possible. This implies that $G$ is an abelian group.

By the classification of abelian groups, we obtain that $G$ is isomorphic to the direct product of $b$ copies of $\mathbb{Z}/p\mathbb{Z}$, for some integer $b$. Note that any faithful representation of $G$ over $\mathbb{C}$ has order at least $b$, and that any faithful representation of $G$ over $\mathbb{Q}$ has order at least $b(p-1)$. Then $b \leqslant n/(p-1)$. □

For the rest of this section, we shall assume the hypotesis of Theorem 1, that is, we have a prime number $p \neq 2$, an integer $n < 3(p-1)$, and a $p$-group $G < \mathrm{SL}_n(\mathbb{Z})$.

We remark that, when $G$ is a cyclic group, the theorem is trivially true. Applying Lemma 4, we obtain that $G$ is cyclic (and the theorem is proved), except for the case $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$, where $2(p-1) \leqslant n < 3(p-1)$. Let us put ourselves in this case.

Note that the proof of Lemma 4 shows that the representation $G$ is the direct sum of two distinct $\mathbb{Q}$-irreducible representations of order $p-1$ and $(n-2(p-1))$ copies of the trivial representation.

We remark that, after a base-change to the $p$-th cyclotomic field $\mathbb{Q}(\zeta_p)$, the representation $G$ could be written in diagonal form, as a direct sum of its irreducible subrepresentations. Also, after a base-change to $\mathbb{Q}$, the representation $G$ could be written as a direct sum of its $\mathbb{Q}$-irreducible subrepresentations. Since we are dealing with the action of $G$ on $\mathbb{F}_p^n$, though, we shall restrict to base-changes to $\mathbb{Z}$, which are preserved under reduction modulo $p$.

Consider the lattice $\mathsf{N} := \mathbb{Z}^n$; it contains a sublattice $\mathsf{M}$ that is fixed by $G$: it is the intersection of $\mathsf{N}$ with the subspace $(\mathbb{Q}^n)^G$ of vectors which are invariant by $G$. We fix a $\mathbb{Z}$-basis for $\mathsf{M}$ and we apply a result on lattices (see [1, Cor. 3 to Thm. 1, Ch. 1]) to extend it to a basis of $\mathsf{N}$: this splits the lattice as $\mathsf{N} = \mathsf{M} \oplus \mathsf{L}$. Now, let $\rho$ be one of the two non-trivial, $\mathbb{Q}$-irreducible subrepresentations of $G$, and let $H$ be its kernel. Repeating the above argument on the restriction of $H$ to $\mathsf{L}$, we determine a basis for $\mathbb{Z}^n$ that allows us to write $\mathsf{N}$ in the form $\mathsf{N}^{(1)} \oplus \mathsf{N}^{(2)} \oplus \mathsf{N}^{(3)}$. Using this new basis, we can assume that every element $g$ of $G$ is of the form

$$g = \begin{pmatrix} I & A_g & B_g \\ O & M_g & C_g \\ O & O & N_g \end{pmatrix},$$

where $M$ and $N$ are the two $\mathbb{Q}$-irreducible representations of $G$ of order $p-1$. In particular, we can choose generators $\sigma$ and $\tau$ for $G$ of the forms

$$\sigma = \begin{pmatrix} I & A_\sigma & B_\sigma \\ O & M & C_\sigma \\ O & O & I \end{pmatrix}; \qquad \tau = \begin{pmatrix} I & A_\tau & B_\tau \\ O & I & C_\tau \\ O & O & N \end{pmatrix}.$$

Note that the eigenvalues of $M$ are the $p-1$ distinct $p$-th roots of unity. This implies that the minimal polynomial of $M$ is $(x^p-1)/(x-1)$ and that the determinant of $M-I$ is $p$.

Over $\mathbb{F}_p$, the matrix $M$ solves the polynomial $(x-1)^{p-1}$. Its minimal polynomial is thus of the form $(x-1)^s$, for some $s<p$. This implies that $(M-I)^s$ has all entries in $p\mathbb{Z}$, so that $p$ divides every column of $(M-I)^s$. Then $p^{p-1}$ divides its determinant, $\det(M-I)^s = p^s$; it follows that, over $\mathbb{F}_p$, the minimal polynomial of $M$ is $(x-1)^{p-1}$ and $M$ is a Jordan block. In particular we deduce the following proposition.

**Proposition 5.** *Let $M$ be as above. For every two non-negative integers $i$ and $j$ with $i+j=p-1$, the image of $(M-I)^i$ is the kernel of $(M-I)^j$, i.e. for every vector*[1] *$A \in \mathbb{Z}^{p-1}$*

$$(M-I)^j A \equiv O \pmod{p} \iff \exists B \in \mathbb{Z}^{p-1} \mid A \equiv (M-I)^i B \pmod{p}.$$

*The same holds for $N$.*

[1] This immediately extends to matrices $(p-1)\times m$, for any positive integer $m$.

We remark that a direct computation of $\sigma\tau = \tau\sigma$ provides

$$\sigma\tau = \begin{pmatrix} I & A_\sigma & \star \\ O & M & C_\sigma + C_\tau \\ O & O & N \end{pmatrix}$$

and the relations

$$(1)\quad A_\tau = O, \qquad (M-I)C_\tau = -C_\sigma(N-I), \qquad B_\sigma = A_\sigma(M-I)^{-1}C_\sigma.$$

Let now $\tilde{Z}$ be a $(G, \mathbb{F}_p^n)$-cocycle that satisfies the local conditions. Then for every $g$ in $G$ there exists a $\tilde{W}_g$ in $\mathbb{F}_p^n$ such that $\tilde{Z}_g \equiv g\tilde{W}_g - \tilde{W}_g \pmod p$; we choose representants $W_g$ of $\tilde{W}_g$ in $\mathbb{Z}^n$ and we define $Z_g := gW_g - W_g$ for every $g$ in $G$. Note that $\tilde{Z}_g \equiv Z_g \pmod p$ for every $g$ in $G$.

Modulo a coboundary we can assume $Z_\tau \equiv O \pmod p$. This implies, by the cocycle relation, $Z_{\sigma\tau} \equiv Z_\sigma + \sigma Z_\tau \equiv Z_\sigma \pmod p$. By definition, $Z_\sigma$ and $Z_{\sigma\tau}$ are:

$$\begin{pmatrix} Z_\sigma^{(1)} \\ Z_\sigma^{(2)} \\ Z_\sigma^{(3)} \end{pmatrix} = \begin{pmatrix} A_\sigma W_\sigma^{(2)} + B_\sigma W_\sigma^{(3)} \\ (M-I)W_\sigma^{(2)} + C_\sigma W_\sigma^{(3)} \\ O \end{pmatrix};$$

$$\begin{pmatrix} Z_{\sigma\tau}^{(1)} \\ Z_{\sigma\tau}^{(2)} \\ Z_{\sigma\tau}^{(3)} \end{pmatrix} = \begin{pmatrix} \star \\ (M-I)W_{\sigma\tau}^{(2)} + (C_\sigma + C_\tau)W_{\sigma\tau}^{(3)} \\ (N-I)W_{\sigma\tau}^{(3)} \end{pmatrix}.$$

We remark that $(N-I)W_{\sigma\tau}^{(3)} \equiv O \pmod p$; by Proposition 5, this implies that $W_{\sigma\tau}^{(3)} \equiv (N-I)^{p-2}\tilde{R} \pmod p$, for some $\tilde{R}$ with entries in $\mathbb{F}_p$. It follows that, modulo $p$, $(M-I)^{p-2}Z_{\sigma\tau}^{(2)}$ is of the form

$$(M-I)^{p-1}W_{\sigma\tau}^{(2)} + (M-I)^{p-2}(C_\sigma + C_\tau)(N-I)^{p-2}\tilde{R}.$$

Applying the second relation in (1) and $(M-I)^{p-1} \equiv (N-I)^{p-1} \equiv O$, we obtain $(M-I)^{p-2}Z_{\sigma\tau}^{(2)} \equiv O \pmod p$. Applying Proposition 5 to $Z_\sigma^{(2)}$ (or to $Z_{\sigma\tau}^{(2)}$) we obtain $Z_\sigma^{(2)} \equiv (M-I)\tilde{S} \pmod p$, for some $\tilde{S}$ with entries in $\mathbb{F}_p$. Let $S$ be any representant of $\tilde{S}$ over $\mathbb{Z}$; since the entries of $Z_\sigma^{(2)} - (M-I)S$ are all divisible by $p$ and since $(M-I)$ has determinant $p$, we may assume $Z_\sigma^{(2)} = (M-I)S$. Thus we have

$$Z_\sigma^{(1)} = A_\sigma(M-I)^{-1}Z_\sigma^{(2)} = A_\sigma S.$$

Taking $V = \left(\begin{smallmatrix} O \\ S \\ O \end{smallmatrix}\right)$, we have $Z_\sigma = \sigma V - V$ and $Z_\tau \equiv \tau V - V \pmod p$. This implies that $\tilde{Z}$ is a $(G, \mathbb{F}_p^n)$-coboundary, concluding the proof of Theorem 1.

## 3. A counterexample

In this section we shall prove Proposition 2. Let $p \neq 2$ be a prime and let $n \geqslant 3(p-1)$ be an integer. As we have said in Section 1, we can assume $n = 3(p-1)$. We are going to define a $p$-group $G$ of matrices in $\mathrm{SL}_n(\mathbb{Z})$ and a $(G, \mathbb{F}_p^n)$-cocycle $Z$ that satisfies the local conditions without being a coboundary.

Let $M \in \mathrm{SL}_{p-1}(\mathbb{Z})$ be a matrix with minimal polynomial $(x^p - 1)/(x - 1)$ (for instance, the Frobenius matrix of this polynomial). Note that $M$ satisfies Proposition 5, as in the previous section. Let now $\mathbf{u}$ and $\mathbf{v}$ be vectors in $\mathbb{Z}^{p-1}$ such that

$$\begin{aligned} \mathbf{u} &\not\equiv O \pmod p, & \mathbf{v} &\not\equiv O \pmod p; \\ (M-I)\mathbf{u} &\equiv O \pmod p, & \mathbf{v}^t(M-I) &\equiv O \pmod p. \end{aligned}$$

We define the matrix $X := \frac{1}{p}\mathbf{u} \times \mathbf{v}^t$, with entries in $\mathbb{Q}$; note that its entries are not all in $\mathbb{Z}$. We also define the matrices $A := (M-I)X$ and $B := X(I-M)$, with entries in $\mathbb{Z}$.

Let $G$ be the group generated by the matrices $\sigma$ and $\tau$ defined as

$$\sigma = \begin{pmatrix} M & O & A \\ & M & A \\ & & I \end{pmatrix}, \qquad \tau = \begin{pmatrix} I & O & B \\ & M & A+B \\ & & M \end{pmatrix};$$

it is easily verified that $G$ is a subgroup of $\mathrm{SL}_n(\mathbb{Z})$ and that the map

$$(i,j) \quad \mapsto \quad \sigma^i\tau^j = \begin{pmatrix} M^i & O & M^iX - XM^j \\ & M^{i+j} & M^{i+j}X - XM^j \\ & & M^j \end{pmatrix}$$

provides an isomorphism $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

**Lemma 6.** *There exist vectors* $\mathbf{r}$, $\mathbf{s}$ *and* $\mathbf{t}$ *in* $\mathbb{Z}^{p-1}$ *such that:*

$$\begin{aligned} &B\mathbf{t} \equiv (M-I)\mathbf{r} \not\equiv O && \pmod p, \\ &(M-I)B\mathbf{t} \equiv O && \pmod p, \\ &(A+B)\mathbf{t} \equiv (M-I)\mathbf{s} && \pmod p. \end{aligned}$$

*Proof.* Assume $B(M-I)^{p-2} \equiv O \pmod p$. Then by Proposition 5 there exists an integer matrix $X_0$ with $B \equiv X_0(M-I) \pmod p$; since $(M-I)$ has determinant $p$, this implies that $X = -B(M-I)^{-1}$ is an integer matrix, which is absurd. Thus $B(M-I)^{p-2} \not\equiv O \pmod p$.

We take a vector $\mathbf{t}_0$ in $\mathbb{Z}^{p-1}$ with $B(M-I)^{p-2}\mathbf{t}_0 \not\equiv O \pmod p$ and we define $\mathbf{t} = (M-I)^{p-2}\mathbf{t}_0$; then $B\mathbf{t} \not\equiv O \pmod p$.

By definition of $A$ and $B$ we have $(M-I)B = -A(M-I)$. Together with $(M-I)^{p-1} \equiv O \pmod p$, this implies

$$(M-I)B(M-I)^{p-2} \equiv (M-I)^{p-2}A(M-I) \equiv O \pmod p.$$

Then $(M-I)B\mathbf{t} \equiv O \pmod p$ and $(M-I)^{p-2}(A+B)\mathbf{t} \equiv O \pmod p$; we conclude by Proposition 5. $\square$

**Proposition 7.** *The vectors $Z_\sigma^{(1)} := O$ and $Z_\tau^{(1)} := B\mathbf{t}$ define a $(G, \mathbb{F}_p^n)$-cocycle $Z \equiv \begin{pmatrix} Z^{(1)} \\ O \\ O \end{pmatrix} \pmod p$ that is not a $(G, \mathbb{F}_p^n)$-coboundary.*

*Proof.* To show that $Z$ is a cocycle we only need to verify, on $Z^{(1)}$, the cocycle conditions derived from the relations $\sigma^p = I$, $\tau^p = I$ and $\sigma\tau = \tau\sigma$:

$$\begin{aligned} Z_{\sigma^p}^{(1)} - Z_I^{(1)} &\equiv (M^{p-1} + \ldots + M + I)Z_\sigma^{(1)} \equiv O && \pmod p; \\ Z_{\tau^p}^{(1)} - Z_I^{(1)} &\equiv pZ_\tau^{(1)} \equiv O && \pmod p; \\ Z_{\sigma\tau}^{(1)} - Z_{\tau\sigma}^{(1)} &\equiv (M-I)Z_\tau^{(1)} \equiv O && \pmod p. \end{aligned}$$

If $Z$ was a coboundary, then there would exist a vector $W$ in $\mathbb{Z}^n$ such that $Z_g \equiv (g-I)W \pmod p$ for every $g$ in $G$; computing $Z_\sigma$ and $Z_\tau$, we would obtain

$$\begin{aligned} Z_\sigma^{(2)} &\equiv (M-I)W^{(2)} + AW^{(3)} && \pmod p, \\ Z_\tau^{(1)} &\equiv BW^{(3)} && \pmod p, \\ Z_\tau^{(2)} &\equiv (M-I)W^{(2)} + AW^{(3)} + BW^{(3)} && \pmod p, \end{aligned}$$

which is absurd, since $Z_\tau^{(2)} \equiv Z_\sigma^{(2)} \equiv O \pmod p$ and $Z_\tau^{(1)} \not\equiv O \pmod p$. $\square$

It now remains to be shown that $Z$ satisfies the local conditions, i.e. that for every $g$ in $G$ there exists a $W_g$ in $\mathbb{F}_p^n$ such that $Z_g \equiv (g-I)W_g \pmod p$.

Over $\tau$ we have

$$(\tau - I)\begin{pmatrix} O \\ -\mathbf{s} \\ \mathbf{t} \end{pmatrix} \equiv \begin{pmatrix} O & O & B \\ O & M-I & A+B \\ O & O & M-I \end{pmatrix} \begin{pmatrix} O \\ -\mathbf{s} \\ \mathbf{t} \end{pmatrix} \equiv \begin{pmatrix} Z_\tau^{(1)} \\ O \\ O \end{pmatrix} \pmod p$$

For every $i \in \mathbb{F}_p^*$ we have $Z_{\tau^i\sigma}^{(1)} \equiv iZ_\tau^{(1)} + Z_\sigma^{(1)} \equiv iB\mathbf{t} \pmod p$; then

$$(\sigma\tau^i - I)\begin{pmatrix} i\mathbf{r} \\ O \\ O \end{pmatrix} \equiv \begin{pmatrix} M-I & \star & \star \\ O & \star & \star \\ O & O & \star \end{pmatrix} \begin{pmatrix} i\mathbf{r} \\ O \\ O \end{pmatrix} \equiv \begin{pmatrix} Z_{\sigma\tau^i}^{(1)} \\ O \\ O \end{pmatrix} \pmod p$$

Since $\tau$ and the $\sigma\tau^i$ with $i \in \mathbb{F}_p$ are the generators of all non-trivial cyclic subgroups of $G$, this shows that $Z$ satisfies the local conditions. This completes the proof of Proposition 2.

## References

[1] J. W. S. Cassels, *An introduction to the Geometry of Numbers*. Springer, 1997.

[2] R. Dvornicich, U. Zannier, Local-global divisibility of rational points in some commutative algebraic groups. *Bull. Soc. Math. France* **129** (2001), no. 3, 317–338.

[3] R. DVORNICICH, U. ZANNIER, On a local-global principle for the divisibility of a rational point by a positive integer. *Bull. London Math. Soc.* **39** (2007), 27–34.
[4] J.-P. SERRE, *Représentations linéaires des groupes finis.* Hermann, 1967.

Marco ILLENGO
Scuola Normale Superiore
Piazza dei Cavalieri 7
56126 Pisa, Italia
*E-mail*: `marco.illengo@sns.it`