Journal of Mathematical Sciences, Vol. 130, No. 3, 2005

PRIVATE LIFE OF GL(5,$\mathbb{Z}$)

A. Yu. Luzgarev* and I. M. Pevzner* UDC 512.5

In the paper, the $(2, 3)$*-generation of* $\mathrm{GL}\,(S, \mathbb{Z})$ *is investigated. We reduce the problem to five specific pairs of matrices. Bibliography:* 4 *titles.*

1. Definitions

A group G that can be generated by an element of order 2 and an element of order 3 is said to be $(2, 3)$-generated, or equivalently, if it is a nontrivial epimorphic image of $\mathrm{PSL}(2, \mathbb{Z})$.

It was shown in [1, 2] that the group $\mathrm{SL}(n, q)$ is $(2, 3)$-generated for $n \geq 5$ and odd $q \neq 9$. Moreover, Di Martino and Vavilov conjecture that all finite simple groups of Lie type are $(2, 3)$-generated, except for some groups of low rank in characteristics 2 and 3.

It is proved in [3] that the groups $\mathrm{SL}(n, \mathbb{Z})$ for $n \geq 13$ and $\mathrm{GL}(n, \mathbb{Z})$ for $n \geq 19$ are $(2, 3)$-generated. On the other hand, if $n = 2$, 4, the groups $\mathrm{SL}(n, \mathbb{Z})$ and $\mathrm{GL}(n, \mathbb{Z})$ are not $(2, 3)$-generated. Recently, it has been shown (see [4]) that the groups $\mathrm{SL}(3, \mathbb{Z})$ and $\mathrm{GL}(3, \mathbb{Z})$ are *not* $(2, 3)$-generated. That paper had a major influence upon our work. Our aim is to prove that $\mathrm{GL}(5, \mathbb{Z})$ and $\mathrm{SL}(5, \mathbb{Z})$ are not $(2, 3)$-generated either. In this paper we reduce the question to a finite number of cases. More precisely, we prove the following theorem.

Theorem 1. *Suppose the group* $\mathrm{GL}(5, \mathbb{Z})$ *is* $(2, 3)$*-generated. Let* A *be a matrix of order* 2 *and* B *be a matrix of order* 3 *that generate this group. Then we may assume that*

$$A = \begin{pmatrix} -1 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}, \qquad B = \begin{pmatrix} 0 & 1 & 0 & 0 & a \\ -1 & -1 & 0 & 0 & b \\ 0 & 0 & 0 & 1 & c \\ 0 & 0 & -1 & -1 & d \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \tag{1}$$

where (a, b, c, d) *is one of the following quadruples:*

$$\begin{array}{ll} (1, -1, -2, -2), & (0, -1, -2, -2), \\ (1, -1, -2, 4), & (0, -1, 4, -8), \\ (-1, 1, -2, -2), & (0, 1, -2, -2), \\ (-1, 1, -2, 4), & (0, 1, 4, -8), \\ (1, -1, 1, -3), & (0, -1, 0, -1). \end{array}$$

We let $\mathrm{GL}(5, \mathbb{Z})$ act from the right on the free Abelian group $\mathbb{Z}^5$ consisting of row vectors. Let p be a prime number, $f_p : \mathrm{GL}(5, \mathbb{Z}) \to \mathrm{GL}(5, p)$ the obvious homomorphism. We will use the fact that $\mathrm{Im}\, f_p$ contains $\mathrm{SL}(5, p)$. In particular, $\mathrm{Im}\, f_p$ is absolutely irreducible in both actions on the row and column vectors.

Assume that $\mathrm{GL}(5, \mathbb{Z}) = \langle A, B \rangle$, where $A^2 = B^3 = I$. It is obvious that $\det A = -1$ and $\det B = 1$. Take a nonzero vector $x \in \mathbb{Z}^5$. Consider the vector $x + xB + xB^2 = x(I + B + B^2)$. Note that $(I - B)^2 = I - 2B + B^2 = (I + B + B^2) - 3B$, and if $I + B + B^2 = 0$ then $(I - B)^2 = -3B$. But $\det(-3B) = -3^5$, while $\det(I - B)^2 \geq 0$, a contradiction. Hence, $I + B + B^2 \neq 0$ and there exists x such that $x + xB + xB^2 \neq 0$. Therefore, $(x + xB + xB^2)B = x(I + B + B^2)B = x + xB + xB^2$. This shows that we found a nonzero vector $\omega = x + xB + xB^2 \in \mathbb{Z}^5$ such that $\omega B = \omega$.

Note that A fixes a certain subspace $W \subset \mathbb{Q}^5$ pointwise and $\dim W = 4$ or 2.

2. The first case ($\dim W = 4$)

Let $\{e_1, e_2, e_3, e_4\}$ be a basis for $W \cap \mathbb{Z}^5$ and consider a vector e_5 such that $\{e_1, e_2, e_3, e_4, e_5\}$ is a basis for $\mathbb{Z}^5$. Let $(\lambda_1, \lambda_2, \lambda_3, \lambda_4, \lambda_5)$ be the coordinates of ω with respect to this basis. Since $\mathrm{Im}\, f_5$ is irreducible, it follows

*St.Petersburg State University, St.Petersburg, Russia.

Translated from *Zapiski Nauchnykh Seminarov POMI*, Vol. 305, 2003, pp. 153–162. Original article submitted November 10, 2003.

that $\lambda_5 = \pm 1$. Therefore, $\{e_1, e_2, e_3, e_4, \omega\}$ is a basis for $\mathbb{Z}^5$. Now it follows that in this basis our matrices are of the form

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ a & b & c & d & -1 \end{pmatrix}, \qquad B = \begin{pmatrix} * & * & * & * & * \\ * & * & * & * & * \\ * & * & * & * & * \\ * & * & * & * & * \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$

and $\mathrm{GCD}\,(a,b,c,d) = 1$. Let π be the projection of $\mathbb{Z}^5$ into $\langle e_1, e_2, e_3, e_4\rangle$ along ω. Consider the vectors $f_1 = (a,b,c,d,0)$ and $\pi(f_1B)$. If they are collinear, then the subspace $\langle f_1, \omega\rangle$ is invariant under the action of A and B, because $\omega A = f_1 - \omega$, $\omega B = \omega$, $f_1 A = f_1$, and $f_1 B - \pi(f_1 B) \parallel \omega$. Hence f_1 and $\pi(f_1B)$ span a two-dimensional subspace of $\mathbb{Z}^5$, and we can choose a vector f_2 to obtain a basis for this subspace. We get $\pi(f_1B) \in \langle f_1, f_2\rangle$ and $f_1B \in \langle f_1, f_2, \omega\rangle$.

Furthermore, consider $\pi(f_2B)$. If $\pi(f_2B) \in \langle f_1, f_2\rangle$, then $\langle f_1, f_2, \omega\rangle$ is invariant, and we can choose a vector f_3 such that $\{f_1, f_2, f_3\}$ is a basis for $\langle f_1, f_2, \pi(f_2B)\rangle$. We conclude that $f_2B \in \langle f_1, f_2, f_3, \omega\rangle$. Similarly, consider $\pi(f_3B)$. If $\pi(f_2B) \in \langle f_1, f_2, f_3\rangle$, then $\langle f_1, f_2, f_3, \omega\rangle$ is an invariant subspace, and we can choose f_4 such that $\{f_1, f_2, f_3, f_4\}$ is a basis for $\langle f_1, f_2, f_3, \pi(f_2B)\rangle$. Now we have $\langle f_1, f_2, f_3, f_4\rangle = \langle e_1, e_2, e_3, e_4\rangle$. Hence, $\langle f_1, f_2, f_3, f_4, \omega\rangle$ is a basis for $\mathbb{Z}^5$. In this basis our matrices are of the form

$$A' = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & -1 \end{pmatrix}, \qquad B' = \begin{pmatrix} * & r & 0 & 0 & * \\ * & * & s & 0 & * \\ * & * & * & t & * \\ * & * & * & * & * \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Let us note that ${B'}^3 = I$. A direct calculation shows that

$${B'}^3 = \begin{pmatrix} * & * & * & rst & * \\ * & * & * & * & * \\ * & * & * & * & * \\ * & * & * & * & * \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Therefore, $rst = 0$. But if $r = 0$, then $\pi(f_1B) \parallel f_1$, a contradiction with our construction. Similarly, if $s = 0$, then $\pi(f_2B) \in \langle f_1, f_2\rangle$, and if $t = 0$, then $\pi(f_3B) \in \langle f_1, f_2, f_3\rangle$. All these cases lead to a contradiction.

3. The second case ($\dim W = 2$)

Consider the eigenspace $V \subset \mathbb{Q}^5$ associated with the eigenvalue -1 of the operator A. It is obvious that -1 is a thrice-repeated root of A, that is, $\dim V = 3$ and $\mathbb{Q}^5 = V \oplus W$.

If the operator B has 5, 4, or 3 linearly independent eigenvectors associated with the eigenvalue 1, then the corresponding eigenspace must have a nonempty intersection with V. The operator A takes any vector with integer coordinates from this intersection to the opposite one, while B takes it to itself, a contradiction. If the operator B has two linearly independent eigenvectors ω_1 and ω_2 associated with the eigenvalue 1, then let y be any noneigenvector. Since yB and y are not collinear, it follows that $y+yB+yB^2 \in \langle \omega_1, \omega_2\rangle$ and $yB^2 \in \langle y, yB, \omega_1, \omega_2\rangle$.

Consider any vector $z \notin \langle y, yB, \omega_1, \omega_2\rangle$. Let αz be the projection of zB into $\langle z\rangle$. Therefore, $\alpha^2 z$ is the projection of zB^2 into $\langle z\rangle$ and $\alpha^3 z$ is the projection of zB^3 into $\langle z\rangle$. But $zB^3 = z$, and $\alpha^3 = 1$. This means that $\alpha = 1$ and the projection of $z + zB + zB^2$ into $\langle z\rangle$ is equal to $3z$. However $z + zB + zB^2$ is B-invariant, whence it belongs to $\langle \omega_1, \omega_2\rangle$ and its projection into $\langle z\rangle$ is equal to 0. Thus we have $z = 0$, a contradiction. This proves that B has only one eigenvector associated with the eigenvalue 1 (up to multiplication by a constant).

By the way we have proved that for any y we have $y + yB + yB^2 \parallel \omega$, whence $yB^2 \in \langle y, yB, \omega\rangle$.

Let $\{e_1, e_2, e_3\}$ be a basis for $V \cap \mathbb{Z}^5$, e_4' and e_5' be vectors such that $\{e_1, e_2, e_3, e_4', e_5'\}$ is a basis for $\mathbb{Z}^5$. Let $(a_1, a_2, a_3, a_4, a_4)$ be the coordinates of ω with respect to this basis. The irreducibility of $\operatorname{Im} f_p$ for all primes p implies that a_4 and a_5 are coprime integers, whence there exist $u, v \in \mathbb{Z}$ such that $a_4u + a_5v = 1$. It follows that we can replace the vectors $\{e_4', e_5'\}$ by the vectors $e_4 = (0,0,0,v,-u)$ and ω to obtain a new basis $\{e_1, e_2, e_3, e_4, \omega\}$. The matrices of our operators with respect to this basis are of the form

$$A = \begin{pmatrix} -1 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ * & * & * & 1 & 0 \\ * & * & * & 0 & 1 \end{pmatrix}, \qquad B = \begin{pmatrix} * & * & * & * & * \\ * & * & * & * & * \\ * & * & * & * & * \\ * & * & * & * & * \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Consider the three-dimensional subspace of $\mathbb{Q}^5$ spanned by the vectors e_1B, e_2B, and e_3B. Its intersection with V has dimension at least 1. This means that there exists a vector $f_1 \in V \cap \mathbb{Z}^5$ such that the coordinates of f_1 have no common divisor different from 1 and $f_1B \in V \cap \mathbb{Z}^5$. If $f_1 || f_1B$, then the subspace spanned by f_1 is invariant under both operators A and B. It follows that f_1 and f_1B span a two-dimensional subspace. Choose an f_1 such that $\{f_1, f_2\}$ is a basis for this subspace. Now f_2B is a linear combination of f_1B and f_1B^2. At the same time, f_1B^2 is a linear combination of f_1, f_1B, and ω (recall that $f_1 + f_1B + f_1B^2$ is an eigenvector, whence it is parallel to ω). Therefore f_2B is a linear combination of f_1, f_1B, and ω. Take an f_3 such that $\{f_1, f_2, f_3\}$ is a basis for V. It is clear that $\{f_1, f_2, f_3, e_4, \omega\}$ is a basis for $\mathbb{Z}^5$. The matrices of our operators with respect to this basis are of the form

$$A' = \begin{pmatrix} -1 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ * & * & * & 1 & 0 \\ b_1 & b_2 & b_3 & 0 & 1 \end{pmatrix}, \qquad B' = \begin{pmatrix} * & * & 0 & 0 & * \\ * & * & 0 & 0 & * \\ * & * & * & * & * \\ * & * & * & * & * \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Note that $b_3 = \pm 1$, since otherwise for a certain prime p the subspace $f_p(\langle f_1, f_2, \omega\rangle)$ is invariant under the action of the matrices A' and B'. Changing the sign of f_3 if necessary, we may assume that $b_3 = 1$. Suppose $f_3' = f_3 + b_1f_1 + b_2f_2$. The matrices of our operators with respect to the basis $\{f_1, f_2, f_3', e_4, \omega\}$ are of the form

$$A'' = \begin{pmatrix} -1 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ * & * & * & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}, \qquad B'' = \begin{pmatrix} * & * & 0 & 0 & * \\ * & * & 0 & 0 & * \\ k_1 & k_2 & k_3 & k & l \\ * & * & * & * & * \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Let us prove that $k = \pm 1$. Otherwise there exists a prime p such that $f_p(\{f_1, f_2, f_3', \omega\})$ is invariant under the maps A and B, and this is a contradiction. Changing the sign of e_4 if necessary, we may assume that $k = 1$. Suppose $f_4 = e_4 + k_1f_1 + k_2f_2 + k_3f_3'$. We obtain $f_3'B = k_1f_1 + k_2f_2 + k_3f_3' + e_4 + l\omega = f_4 + l\omega$, and f_4B is a linear combination of $f_3'B^2$ and ω, while $f_3'B^2$ is a linear combination of f_3', $f_3'B$, and ω (this follows from the above discussion, which actually applies to any vector y). Therefore f_4B is a linear combination of f_3', $f_3'B$, and ω. Since $f_3'B = f_4 + l\omega$, it follows that $f_4B = \alpha_1f_3' + \alpha_2f_4 + \alpha_3\omega$ for some $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{Q}$. Hence $f_4B^2 = \alpha_1(f_4 + l\omega) + \alpha_2(\alpha_1f_3' + \alpha_2f_4 + \alpha_3\omega) + l\omega$. On the other hand, $f_4 = f_3'B - l\omega$ and $f_4B^2 = f_3' - l\omega$. Combining these representations of f_4B^2, we arrive at the relations $\alpha_2\alpha_1 = 1$, $\alpha_1 + \alpha_2^2 = 0$, and $\alpha_1 l + \alpha_2\alpha_3 + l = -l$. Now it follows that $\alpha_1 = -1$, $\alpha_2 = -1$, and $f_4B = -f_3 - f_4 + \alpha_3\omega$. Therefore the matrices of our operators with respect to the basis $\{f_1, f_2, f_3', f_4, \omega\}$ are of the form

$$A'' = \begin{pmatrix} -1 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ \beta_1 & \beta_2 & * & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}, \qquad B'' = \begin{pmatrix} * & * & 0 & 0 & * \\ * & * & 0 & 0 & * \\ 0 & 0 & 0 & 1 & * \\ 0 & 0 & -1 & -1 & * \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$

where β_1 and β_2 are coprime integers. Let $g_1 = (\beta_1, \beta_2, 0, 0, 0)$ with respect to this basis. Now we can choose a vector g_2 such that $\{g_1, g_2\}$ is a basis for $\langle f_1, f_2\rangle$. We have a new basis $\{g_1, g_2, f_3', f_4, \omega\}$, and the matrices of our operators are of the form

$$A''' = \begin{pmatrix} -1 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ 1 & 0 & * & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}, \qquad B''' = \begin{pmatrix} \gamma_1 & \gamma_2 & 0 & 0 & * \\ \delta_1 & \delta_2 & 0 & 0 & * \\ 0 & 0 & 0 & 1 & * \\ 0 & 0 & -1 & -1 & * \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Note that $\gamma_2 = \pm 1$ (this follows from the irreducibility of $\operatorname{Im} f_p$; otherwise the subspace $\langle g_1, f_3', f_4, \omega\rangle$ would be invariant). Changing the sign of g_2 if necessary, we may assume that $\gamma_2 = 1$. The matrix $\begin{pmatrix} \gamma_1 & 1 \\ \delta_1 & \delta_2 \end{pmatrix}$ has order 3 and trace -1. Let Y be the matrix $\operatorname{diag}\left(\begin{pmatrix} 1 & 0 \\ -\gamma_1 & 1 \end{pmatrix}, 1, 1, 1\right)$. Conjugating B'' by Y, we reduce the matrices of our operators to the form

$$A'''' = \begin{pmatrix} -1 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ 1 & 0 & r & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}, \qquad B'''' = \begin{pmatrix} 0 & 1 & 0 & 0 & * \\ -1 & -1 & 0 & 0 & * \\ 0 & 0 & 0 & 1 & * \\ 0 & 0 & -1 & -1 & * \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Now let $Y' = \operatorname{diag}\left(1, 1, 1, \begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix}\right)$. Conjugating B'''' by Y', we derive that the matrices of our operators are of the form (we denote them again by A and B)

$$A = \begin{pmatrix} -1 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}, \qquad B = \begin{pmatrix} 0 & 1 & 0 & 0 & a \\ -1 & -1 & 0 & 0 & b \\ 0 & 0 & 0 & 1 & c \\ 0 & 0 & -1 & -1 & d \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}. \tag{2}$$

4. Further steps

Consider a vector $(k, l, 0, 0, 0) \in \mathbb{Z}^5$. The operator A takes it to the opposite one, and the operator B takes it to the vector $(-l, k-l, 0, 0, ka+lb)$. The latter vector is parallel to the starting one if and only if

$$ka + lb = 0, \quad k(k-l) = l(-l)$$

(as before, in fact we need only equality modulo a prime p). First note that we are interested only in the case where a and b are not both equal to zero (otherwise the first two vectors of the basis span an invariant subspace). Solving these equations, we obtain $k = bt$, $l = -at$, and $a^2 + ab + b^2 = 0$. This means that if $a^2 + ab + b^2 \equiv 0 \pmod p$ for a prime p, then the one-dimensional subspace spanned by $(k, l, 0, 0, 0)$ is invariant. If this is not true for any prime p, then either $a^2 + ab + b^2 = 1$ or $a^2 + ab + b^2 = -1$. Solving these quadratic equations, we have six possibilities for the pair (a, b):

$$(a, b) = (0, 1), (0, -1), (-1, 0), (-1, 1), (1, -1), \text{ or } (1, 0).$$

Consider a vector $P = (x, 0, y, 2x, 2y)$. First note that this is an eigenvector for the matrix A: $PA = P$. It can easily be checked that $PB = (0, x, -2x, y-2x, xa+yc+2xd+2y)$, $PB^2 = (-x, -x, -y+2x, -y, x(b+a) + y(d+c) - 2xc + 2y)$, and $P + PB + PB^2 = (0, 0, 0, 0, 6y + 2xa + 2yc + 2xd + xb + yd - 2xc)$. We want to put $P + PB + PB^2 = (0, 0, 0, 0, 0)$; this yields one equation involving x and y. Now consider the vector $PBA = (y-2x, -x, 2x+xa+yc+2xd+2y, y-2x, xa+yc+2xd+2y)$. Let us try to represent this vector as a linear combination of P and PB. Note that $PBA+PB = (y-2x, 0, xa+yc+2xd+2y, 2y-4x, 2xa+2yc+4xd+4y)$ and there is a hope that this vector is parallel to P. This hope gives us one more equation: $x(xa+yc+2xd+2y) = y(y-2x)$. Therefore, if both equations

$$\begin{cases} 6y + 2xa + 2yc + 2xd + xb + yd - 2xc = 0 \\ x(xa + yc + 2xd + 2y) - y(y - 2x) = 0 \end{cases} \tag{3}$$

hold modulo a prime p, then the vectors P and PB span an invariant subspace (we have just proved that PA, PB^2, and PBA can be expressed as linear combinations of P and PB).

Now we try to solve these equations. The first equation is linear and has the form $yh = -xg$ (where $h = 6 + 2c + d$ and $g = 2a + 2d - 2c + b$). First we prove the following fact.

Lemma 1. *If $g \equiv h \equiv 0 \pmod p$ for a prime p, then the matrices A and B do not generate $\mathrm{GL}(5, \mathbb{Z})$.*

Proof. If the assumption holds, then the first equation of (3) has the form $0 = 0$, which is always true, and the other equation is homogeneous and quadratic. This means that we have a quadratic equation for the variable y/x:

$$-\left(\frac{y}{x}\right)^2 + (c+4)\frac{y}{x} + (2d+1) = 0. \tag{4}$$

It may be the case that this equation has no roots in $\mathbb{Z}/p\mathbb{Z}$ at all, but there is nothing wrong with that. Let K be the algebraic closure of $\mathbb{Z}/p\mathbb{Z}$. This equation has a root in K, whence there exists a vector $P \in K^5$ such that the vectors P and PB span a subspace that is invariant under the action of the matrices A and B as elements of $\mathrm{GL}(5, K)$. Consider, for example, a matrix $T \in \mathrm{GL}(5, \mathbb{Z})$ that adds the first coordinate of a vector to the fourth. Of course, this matrix viewed as an element of $\mathrm{GL}(5, K)$ does precisely the same. If the matrices A and B generate $\mathrm{GL}(5, \mathbb{Z})$, then T can be expressed as the product of a number of the matrices A and B, and thus PT belongs to our invariant subspace of K^5. Hence, PT is a linear combination of P and PB. But $PT = (x, 0, y, 3x, 2y)$, where $x \neq 0$, since we solved the quadratic equation for y/x. Therefore, the coefficient of PB in this linear combination is equal to zero (the second coordinate of PT equals 0), and PT is parallel to P. This contradiction proves the lemma.

Consider the expression

$$(a + 2d)h^2 + (c_4)hg - g^2. \tag{5}$$

Assume that it is not equal to ± 1; then there exists a prime p such that this expression modulo p equals 0. If $h \equiv 0 \pmod{p}$, then using (5), we obtain $g \equiv 0 \pmod{p}$, and the assumption of the lemma holds. Thus we may assume that $h \not\equiv 0 \pmod{p}$. Now we take any $x \not\equiv 0 \pmod{p}$ and $y = xg/h$. It is easily shown that the pair (x, y) is a nontrivial solution of (3) modulo p (the first equation holds by our choice of y, and the second holds by the choice of p such that (5) equals 0). Thus our hope for an invariant subspace is satisfied.

It remains to exclude the last case: expression (5) is equal to 1 or -1.

Both cases lead to an equation for a, b, c, d. We should solve it in integers. Note that we have already known all possibilities for a and b. If we introduce a new variable $t = 2c+d$ and substitute $t-2c$ for d in the equation, it becomes quadratic for t. Then we write down a solution of this equation and note that the discriminant, which depends on a, b, and t, should be the square of an integer. Substituting known possible values for a and b, we find the corresponding values of t that satisfy the condition mentioned above and make sure that for these a, b, and t the solutions of the quadratic equaiton for c is also integer. All this stuff leads to ten possibilities for the quadruple (a, b, c, d):

$$\begin{array}{ll} (1, -1, -2, -2), & (0, -1, -2, -2), \\ (1, -1, -2, 4), & (0, -1, 4, -8), \\ (-1, 1, -2, -2), & (0, 1, -2, -2), \\ (-1, 1, -2, 4), & (0, 1, 4, -8), \\ (1, -1, 1, -3), & (0, -1, 0, -1). \end{array}$$

In fact there are only *five* possibilities: for any pair of matrices (A, B) consider the pair (A, B^2), which generates $\mathrm{GL}(5, \mathbb{Z})$ if and only if (A, B) generates $\mathrm{GL}(5, \mathbb{Z})$. If we apply our process to the pair (A, B^2), we obtain another quadruple (a, b, c, d). Thus the quadruples are divided into pairs, and it remains to investigate the generation of $\mathrm{GL}(5, \mathbb{Z})$ for only one quadruple in every pair (we put every pair on a separate line).

Translated by A. Yu. Luzgarev.

REFERENCES

1. L. Di Martino and N. Vavilov, "$(2,3)$-generation of $\mathrm{SL}(n, q)$. I. Cases $n = 5, 6, 7$," *Comm. Algebra*, **22**, 1321–1347 (1994).
2. L. Di Martino and N. Vavilov, "$(2,3)$-generation of $\mathrm{SL}(n, q)$. II. Cases $n \geq 8$," *Comm. Algebra*, **24**, 487–515 (1996).
3. P. Sanchini and M. C. Tamburini, "Constructive $(2,3)$-generation: a permutational approach," *Rend. Sem. Math. Fis. Milano*, **LXIV**, 141–158 (1994).
4. M. C. Tamburini and P. Zucca, "On a question of M. Conder," *Atti Accad. Naz. Lincei Rend.*, **11**, 5–7 (2000).