S©MR ISSN 1813-3304

СИБИРСКИЕ ЭЛЕКТРОННЫЕ
МАТЕМАТИЧЕСКИЕ ИЗВЕСТИЯ

Siberian Electronic Mathematical Reports
http://semr.math.nsc.ru

Том 4, стр. 345–360 (2007) УДК 512.5
MSC 20D10, 20D20

REGULAR ORBITS OF SOLVABLE LINEAR p'-GROUPS

E. P. VDOVIN

Abstract. In this paper we prove that a solvable linear p'-group $G \leq GL(V)$, where p is the characteristic of the underlying field of V, has a regular orbit on $V \times V$.

1. Introduction

In 1966 D.S. Passman has proved that for a Sylow r-subgroup R of $GL(V) = GL_n(p^k)$ with $r \neq p$ there exist $v, u \in V$ such that $C_R(v) \cap C_R(u) = \{e\}$. As a corollary D.S. Passman proved that for a p-solvable finite group G there exist three Sylow p-subgroups P_1, P_2, P_3 such that $P_1 \cap P_2 \cap P_3 = O_p(G)$. Later in [16] V.I. Zenkov proved by using of the classification of finite simple groups that in each finite group there exist three Sylow p-subgroups P_1, P_2, P_3 such that $P_1 \cap P_2 \cap P_3 = O_p(G)$. In 2005 S. Dolfi [2, Theorem 1.3] has proved that if G is a solvable completely reducible subgroup of odd order of $GL(V)$, then there exist $v, u \in V$ such that $C_G(v) \cap C_G(u) = \{e\}$. As a corollary it was proved [2, Theorem 1.1] that if π is a set of odd primes, G is a finite π-solvable group and H is a Hall π-subgroup of G, then there exist $x, y \in G$ such that $H \cap H^x \cap H^y = O_\pi(G)$.

The main result of the present paper is the following theorem.

Theorem 1.1. *Let G be a solvable subgroup of $GL_n(p^k) = GL_n(q) = GL(V)$ such that $(|G|, p) = 1$. Then there exist $u, v \in V$ such that $C_G(v) \cap C_G(u) = \{e\}$.*

Known examples (see [15], for instance) show that we cannot substitute condition $(|G|, p) = 1$ by a weaker condition of complete reducibility of G.

Vdovin E.P. Regular orbits of solvable linear p'-groups.

The work is supported by Russian Fund of Basic Research (project 05–01–00797), grant of President (MK–3036.2007.1) and SB RAS (grant N 29 for young researchers and Integration Project 2006.1.2).

Received August, 23, 2007, published August, 31, 2007.

Assume that G acts on a set Ω. Then G acts naturally on Ω^k by $g:(x_1,\ldots,x_k)\mapsto (x_1^g,\ldots,x_k^g)$. An element $x=(x_1,\ldots,x_k)\in\Omega^k$ is called *regular under* G if $C_G(x)=\{e\}$, that is x^G is a regular orbit. So Theorem 1.1 states that there exists a regular element $(v,u)\in V^2$. In particular, there exists and element $v\in V$ such that $|v^G|\geqslant |G|^{1/2}$, which solves the problem posed by Isaacs in [6]. Elements $x=(x_1,\ldots,x_k)$ and $y=(y_1,\ldots,y_k)$ of Ω^k are called *equivalent under* G if there exists $g\in G$ such that $x^g=y$ that is $x^G=y^G$.

As corollaries of Theorem 1.1 we prove the following results.

Theorem 1.2. *Let G be a solvable π-subgroup of* $\mathrm{Aut}(H)$*, where H is a finite π'-group. Then there exist $h_1,h_2\in H$ such that $C_G(h_1)\cap C_G(h_2)=\{e\}$.*

Theorem 1.3. *Let G be a π-solvable group, H be a Hall π-subgroup of G. Then there exist $x,y\in G$ such that $H\cap H^x\cap H^y=O_\pi(G)$.*

Note that Theorem 1.3 is not true without the assumption on π-solvability of G. Indeed, consider the symmetric group Sym_5 of degree 5. It has a Hall $\{2,3\}$-subgroup $H=\mathrm{Sym}_4$, but for every $x,y\in\mathrm{Sym}_5$ the intersection $H\cap H^x\cap H^y$ is nontrivial.

By $\mathbb{1}_n$, $\mathbb{0}_n$ we denote the identity and the zero matrices of size $n\times n$, by $\mathbb{0}_{(n,m)}$ we denote the zero matrix of size $n\times m$. By $A\otimes B$ we denote the Kronecker product of matrices A and B. By $\mathrm{diag}(a_1,\ldots,a_n)$ we denote the diagonal matrix with entries $a_1,\ldots,a_n$ on the diagonal, and by $\mathrm{perm}(\tau_1\cdot\ldots\cdot\tau_k;n)$ we denote the permutation matrix of degree n, where $\tau_1,\ldots,\tau_k\in\mathrm{Sym}_n$ are independent cycles. For a group A and a subgroup B of Sym_n by $A\wr B$ we denote the permutation wreath product of A and B.

Some parts of the proof of Theorem 3.1 use GAP [17]. It is not difficult to avoid computer calculations and to make all calculations "by hands" (and the author has done all these calculation "by hands"), but this would enlarge the paper very much. Generators of primitive solvable groups, mentioned in the proof of Theorem 3.1, can be found in

`http://www.math.nsc.ru/~vdovin/generators_primitive.html`

Note also, that the first draft of the paper with the same results obtained by different methods was appeared on the Internet just recently, see [5].

2. Preliminary results

Lemma 2.1. *The following statements are known.*

(a) *$GF(q^n)^*$ is isomorphic to a subgroup (which we shall also denote $GF(q^n)^*$) of $GL_n(q)$ and this subgroup is unique up to conjugation in $GL_n(q)$;*
(b) *there exists $\varphi\in GL_n(q)$ generating $Gal(GF(q^n):GF(q))$, i. e., for every $A\in GF(q^n)^*$ we have that $A^\varphi=A^q$.*

Lemma 2.2. *Let $G\leq GL_n(q)$ be a maximal primitive solvable group. Then the following statements hold:*

(a) *there exists a unique maximal normal Abelian subgroup A of G* [13, § 20, Theorem 9]*;*
(b) *A is isomorphic to a multiplicative subgroup of an extension $GF(q^k)$ of $GF(q)$, in particular, A is a cyclic group of order q^k-1 for some $k\geqslant 1$*

[13, § 19, Lemma 1] *(note that by* [13, § 21, Lemma 2] *for given k the subgroup A is uniquely determined up to conjugation in $GL_n(q)$);*

(c) $n = k \cdot m$ *for some* m [13, § 19, Lemma 1]*;*

(d) denoting by $C = C_G(A)$*, the factor group* G/C *is isomorphic to a subgroup of the Galois group* $Gal(GF(q^k) : GF(q))$*, in particular,* G/C *is cyclic and* $|G/C| \leqslant k$ [13, § 19, Theorem 1]*;*

(e) C *is an absolutely irreducible subgroup of* $GL_m(q^k)$ [13, § 20, Theorem 1]*;*

(f) denoting by B *a maximal subgroup of* C *such that* B/A *is a maximal normal Abelian subgroup of* G/A*, the index* $|B : A| = m^2$ [13, § 20, Theorem 11]*;*

(g) if $m = \prod_{i=1}^{l} r_i^{\alpha_i}$ *is the prime decomposition of* m*, then each* r_i *divides* $|A| = q^k - 1$ [13, § 20, Corollary 1]*;*

(h) $B/A = F(C/A)$ *and* $B = F(C)$ *(*[9, Proposition 2.1]*;*

(i) C/B *is isomorphic to a completely reducible subgroup of* $Sp_{2\alpha_1}(r_1) \times \ldots \times Sp_{2\alpha_l}(r_l)$ [9, Proposition 2.1(13)]*, in particular, if* $l = 1$*, then* C/B *is completely reducible.*

Lemma 2.3 is proved in the first part of the proof of [4, Proposition 4].

Lemma 2.3. *Let* $G \leq GL_n(q)$ *be a maximal primitive solvable group and subgroups* A, B, C *of* G *are defined as in Lemma 2.2. Then*

(a) if $g \in A \setminus \{e\}$*, then* $|C_V(g)| = 1$*;*

(b) if $g \in B \setminus A$*, then* $|C_V(g)| \leqslant q^{n/2}$*;*

(c) if $g \in C \setminus B$*, then* $|C_V(g)| \leqslant q^{3n/4}$*.*

Lemma 2.4. *Let* $G \leq GL_n(q)$ *be such that* $|G| < q$*. Then there exists* $v \in V = GF(q)^n$ *such that* $C_G(v) = \{e\}$*.*

Proof. Let $v_1, \ldots, v_n$ be a basis of V. Consider $X = \{v_1 + \lambda v_i \mid \lambda \in GF(q)^*, 2 \leqslant i \leqslant n\}$. Then $|X| = (q-1)^{n-1}$ and, if Y is a subset of X such that $|Y| > (q-1)^{n-2}$, then Y contains a basis of V. So, for every $g \in GL_n(q)$, we have that $|C_X(g)| = |\{x \in X \mid x^g = x\}| \leqslant (q-1)^{n-2}$. Let $Z = \{x \in X \mid C_G(x) \neq \{e\}\}$. Then $|Z| \leqslant \sum_{g \in G \setminus \{e\}} |C_X(g)| \leqslant (q-1)^{n-2}(|G|-1) < |X|$, so there exists $x \in X$ such that $C_G(x) = \{e\}$. □

Lemma 2.5. *Let* G *be a subgroup of* $GL_n(q)$ *with* $(|G|, p) = 1$ *such that there exists a regular element* $(v, u) \in V \times V$ *under* G*. Then for every distinct* $\lambda, \mu \in GF(q)$ *there does not exist an element* $g \in G$ *such that* $(v, \lambda v + u)^g = (v, \mu v + u)$*.*

Proof. Clearly it is enough to prove that for every $\lambda \neq 0$ there does not exist $g \in G$ such that $(v, u)^g = (v, \lambda v + u)$. Assume by contradiction, that such an element g exists. Then we have that $v^g = v$ and $u^g = \lambda v + u$. So $u^{g^p} = p \cdot \lambda v + u = u$. Therefore $g^p \in C_G((v, u)) = \{e\}$, i. e., $g^p = e$. But $(|g|, p) = 1$, so $g = e$. □

Lemma 2.6. [15] *Let* G *be a completely reducible solvable subgroup of* $GL_n(q)$*. Then* $|G| < q^{9n/4} = |V|^{9/4}$*.*

Lemma 2.7. *The structure of maximal completely reducible solvable subgroups of* $Sp_{2n}(q)$ *for small values of* n *and* q *is given below.*

(a) If $q \equiv \pm 1 \pmod 8$*,* $q > 3$ *then there are four nonconjugate maximal completely reducible solvable subgroups* G_1, G_2, G_3, G_4 *of* $Sp_2(q)$*; where* G_1 *is the normalizer in* $Sp_2(q)$ *of a (unique up to conjugation) cyclic subgroup of order* $q-1$ *and* $|G_1| = 2(q-1)$*;* G_2 *is the normalizer in* $Sp_2(q)$ *of a (unique*

up to conjugation) cyclic subgroup of order $q+1$ and $|G_2| = 2(q+1)$; G_3 and G_4 are conjugate in $GL_2(q)$, $Z(G_3) \simeq \mathbb{Z}_2$ and $G_3/Z(G_3) \simeq \mathrm{Sym}_4$.

(b) *If $q \equiv \pm 3 \pmod 8$, $q > 3$ then there are three nonconjugate maximal completely reducible solvable subgroups G_1, G_2, G_3 of $Sp_2(q)$; where G_1 and G_2 can be chosen as in* (a)*; $Z(G_3) \simeq \mathbb{Z}_2$ and $G_3/Z(G_3) \simeq \mathrm{Alt}_4$.*

(c) *There are 2 nonconjugate maximal completely reducible solvable subgroups G_1, G_2 of $Sp_4(2)$; where $G_1 \simeq Sp_2(2) \wr \mathrm{Sym}_2$, $|G_1| = 72$; and $G_2 \simeq \mathbb{Z}_5 \rtimes \mathbb{Z}_4$, $|G_2| = 20$.*

(d) *If G is a completely reducible solvable subgroup of $Sp_4(3)$, then $|G| \leqslant 1152$.*

(f) *If G is a completely reducible subgroup of $Sp_6(q)$ ($q = 2, 3$), then $|G| \leqslant |Sp_2(q)|^3 \cdot |\mathrm{Sym}_3|$; $|G| \leqslant 20$ if $(|G|, 3) = 1$ and $q = 2$.*

(g) *If G is a completely reducible subgroup of $Sp_8(2)$ or $Sp_{10}(2)$, then $|G| \leqslant 6^4 \cdot 24$; $|G| \leqslant 800$ if $(|G|, 3) = 1$.*

Proof. (a) and (b) follows from [13, §21.3]

(c) If G is a maximal completely reducible solvable subgroup of $Sp_4(2)$ and G is not primitive, then G is contained in $Sp_2(2) \wr \mathrm{Sym}_2$. If G is primitive, then it is contained in a maximal primitive solvable subgroup H of $GL_4(2)$. So $A \leq H$ is a cyclic subgroup of order $2^4 - 1$ (other cases from Lemma 2.2 cannot occur, because 2 is the only prime divisor of 4 and it is coprime with $2^t - 1$ for every t). Hence $G = G_2$ in the notations of point (c) of the lemma.

Bounds in points (d)–(g) of the lemma can be obtained in a similar way, by using Lemma 2.2 and [8, Table 3.5.C]. □

3. Primitive solvable groups

In this section we shall prove Theorem 1.1 for primitive solvable subgroups of $GL_n(q)$.

Theorem 3.1. *Let G be a primitive solvable subgroup of $GL_n(q)$ such that $(|G|, q) = 1$. Then there exist $u, v \in V$ such that $C_G(v) \cap C_G(u) = \{e\}$.*

Proof. In view of [2, Theorem 1.3] we may assume that q is odd and 2 divides $|G|$. Assume by contradiction that the statement of Theorem 3.1 is false and $G \leq GL_n(q)$ is a counterexample. It is clear that for $n = 2$, taking v_1, v_2 to be a basis of V, we have that $C_{GL_2(q)}((v_1, v_2)) = \{e\}$, so $n \geqslant 3$. Now G is contained in a maximal primitive solvable subgroup G_1 of $GL_n(q)$. Consider subgroups A_1, B_1, and C_1 of G_1 defined in Lemma 2.2; let $A = G \cap A_1$, $B = G \cap B_1$, $C = G \cap C_1$. Until the end of the proof we fix A_1, B_1, C_1, G_1. Note that $|A_1| = q^k - 1$, so $(|A_1|, q) = 1$. Thus we may assume that $G = GA_1$, i. e., $A_1 = A$. By Lemma 2.2(g) we also have that $(|B_1|, q) = 1$, so we may assume that $B_1 = B$. Note also that we may assume $G \leq C_1$. Indeed, let $(v, u) \in V \times V$ be a regular under $G \cap C_1$ element. Consider $g \in G \setminus C_1$. Let λ be a generating element of $GF(q^k)^* = A$ (see Lemma 2.2(b)). Assume that g centralizes $(v, \lambda v + u)$. Then $(\lambda v + u)^g = \lambda^g v + u^g = \lambda v + u$, so $u^g = u + (\lambda - \lambda^g)v$. Since $v^g = v$ and by Lemma 2.2(d), we obtain that the map $g : \lambda \mapsto \lambda^g$ defined by $(\lambda v)^g = \lambda^g v$ is an automorphism of $GF(q^k)$ fixing $GF(q)$. If $r = |g|$, then $u^{(g^k)} = u = u + k(\lambda - \lambda^g)v$. So $k(\lambda - \lambda^g) = 0$. The condition $(|G|, p) = 1$ implies that $k \neq 0$, hence $\lambda = \lambda^g$, i. e., $g \in C_1$. Lemma 2.5 implies that $g = e$, hence $(v, \lambda v + u)$ is a regular element of G.

Since G is a counterexample, we obtain that for every non-zero element (v_1, v_2) of $V \times V$ there exists a nonidentity element g of G, centralizing (v_1, v_2). Thus we obtain the following inequality

$$(1)\qquad \sum_{g\in A\setminus\{e\}} |C_{V\times V}(g)| + \sum_{g\in B\setminus A} |C_{V\times V}(g)| + \sum_{g\in G\setminus B} |C_{V\times V}(g)| \geqslant |V|^2 - 1 = q^{2n} - 1.$$

In view of Lemma 2.2(b) and Lemma 2.3(a) we have that

$$\sum_{g\in A\setminus\{e\}} |C_{V\times V}(g)| \leqslant |A| - 1 = q^k - 2.$$

Lemma 2.2(f) and Lemma 2.3(b) imply that

$$\sum_{g\in B\setminus A} |C_{V\times V}(g)| < ((n/k)^2 - 1)(q^k - 1)q^n.$$

Denoting by t the maximum of orders of completely reducible subgroups of

$$Sp_{2\alpha_1}(r_1) \times \ldots \times Sp_{2\alpha_l}(r_l)$$

(in the notations of Lemma 2.2(i)) and using Lemma 2.3(c) we obtain that

$$\sum_{g\in G\setminus B} |C_{V\times V}(g)| \leqslant (t-1)(n/k)^2(q^k - 1)q^{3n/2}.$$

By Lemma 2.6 we obtain that $t < (n/k)^{9/2}$. If $n/k \geqslant 5$, q is a power of a prime, and $t(n/k)^2(q^k - 1)q^{3n/2} < q^{2n}$, then the left part of inequality (1) is less than $t(n/k)^2(q^k - 1)q^{3n/2}$. Thus if

$$(2)\qquad t(n/k)^2(q^k - 1) < q^{n/2},$$

then the left part of inequality (1) is less than $|V|^2 - 1$. It is clear that if $k \leqslant n/5$ and n is large enough, then the number $n^{13/2}(q^k - 1)q^{3n/2}$ (here we take for t its upper bound $n^{9/2}$) is less than q^{2n} for every odd q. So we prove the theorem in several steps. First we consider some special cases, with small values of n and n/k, then we turn to the general case.

Step 1, $k = n$. This means that $A = B = C = G$. By Lemma 2.3(a), for every $v \in V \setminus \{0\}$, we have that $C_G(v) = \{e\}$.

Step 2, $k = n/2$. By Lemma 2.2(e) we have that G is an absolutely irreducible subgroup of $GL_2(q^k)$. Taking v, u to be any base of $V = GF(q^k)^2$ we obtain that $C_G(v) \cap C_G(u) = \{e\}$.

Step 3, $k = n/3$. By Lemma 2.2(e) we have that C is an absolutely irreducible subgroup of $GL_3(q^k)$. Since for every nontrivial element g of $GL_3(q^k)$ the inequality $\dim(C_{GF(q^k)^3}(g)) \leqslant 2$ holds, then for every $g \in C$ we have that $\dim(C_V(g)) \leqslant q^{2n/3}$. By Lemma 2.2(g), G_1 exists only if $q^k - 1$ is divisible by 3, so we may suppose that $q^k \equiv 1 \pmod 3$. If $(q^k, 3) = 1$, then the left part of inequality (1) is not greater than

$$(3)\qquad (q^{n/3} - 2) + 8(q^{n/3} - 1)q^n + 23 \cdot 9 \cdot (q^{n/3} - 1)q^{4n/3}.$$

Number (3) is not greater than $q^{2n} - 1$ in the following cases: $n = 3$ and $q \leqslant 199$, $n = 6$ and $q \leqslant 13$, $n = 9$ and $q = 5$. Now assume that G is a solvable subgroup of $GL_3(q^k)$ and, in the notations of Lemma 2.2, $A = Z(GL_3(q^k))$ is a cyclic subgroup of order $q^k - 1$, B/A is elementary Abelian of order 3^2, and $G/B \simeq Sp_2(3) \simeq SL_2(3)$. By [13, § 21.3, Theorem 6] it follows that G is unique up to conjugation in $GL_3(q^k)$. Let $\lambda \in GF(q^k)^*$ be such that $\langle\lambda\rangle = GF(q^k)^*$ and $\eta = \lambda^{(q^k-1)/3}$. Then A is generated by $f = \lambda \mathbb{1}_3$. By [13, § 21.2, Theorem 4] it follows that B modulo A is generated by matrices

$$a = \mathrm{diag}(1, \eta, \eta^2), b = \mathrm{perm}((1,2,3);3).$$

Thus $B = \langle f, a\rangle \leftthreetimes \langle b\rangle$. Now let $v = (0,0,1)$. Then

$$C_{GL_3(q^k)}(v) = \begin{pmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & a_{2,3} \\ 0 & 0 & 1 \end{pmatrix}.$$

As we noted above $G/B \simeq Sp_2(3) = SL_2(3)$. The group $SL_2(3)$ is known to be generated by

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

Thus we need to find matrices c, d such that $a^c = b^{-1}$, $b^c = a$, $a^d = a$, $b^d = ab$. Direct calculations show that c, d can be chosen in the following way

$$c = \begin{pmatrix} 1 & 1 & 1 \\ 1 & \eta^2 & \eta \\ 1 & \eta & \eta^2 \end{pmatrix}, d = \mathrm{diag}(1,1,\eta).$$

From the structure of B given above we obtain that

$$C_B(v) = B \cap C_{GL_3(q)}(v) = \left\langle \mathrm{diag}(\eta, \eta^2, 1)\right\rangle,$$

in particular $|C_B(v)| = 3$. Moreover, for every $x \in c^G$ we have that $x \notin C_G(v)$. Thus $C_G(v)B/B$ is isomorphic to a proper subgroup of $C/B \simeq SL_2(3)$. In particular, $|C_G(v)B/B| \leqslant 6$, hence $|C_G(v)| \leqslant 18$. Since $(|G|, q) = 1$, then $C_G(v)$ is completely reducible, so $C_G(v) \leq L \simeq GL_2(q^k)$. Let U be the 2-dimensional irreducible module for L. By Lemma 2.4 we obtain that if $q^k \geqslant 19$, then there exists $u \in U$ such that $C_{C_G(v)}(u) = \{e\}$. Therefore, if $q^k \geqslant 19$, then we obtain that there exist $v, u \in V$ such that $C_G(v) \cap C_G(u) = \{e\}$. If $q = 7, 13$, then direct computations (by using [17], for example) show that for $u = (\lambda, \eta, 0)$ we have that $C_G(v) \cap C_G(u) = \{e\}$.

Step 4, $k = n/4$. Then $B/A \simeq 2^4$ and G/B is isomorphic to a completely reducible solvable subgroup of $Sp_4(2)$. By Lemma 2.7(c) it follows that there are two non-conjugate maximal completely reducible solvable subgroups of $Sp_4(2)$, namely either $S_1 \simeq SL_2(2) \wr \mathrm{Sym}_2$ of order 72, or $S_2 \simeq \mathbb{Z}_5 \leftthreetimes \mathbb{Z}_4$ of order 20. If $q = 3^t$, then the conditions $(|G|, q) = 1$ and G/B is a completely reducible subgroup of $Sp_4(2)$ implies that G/B is isomorphic to a subgroup of S_2. So the left part of inequality (1) is not greater than

$$(q^{n/4} - 2) + 15(q^{n/4} - 1)q^n + 19 \cdot 16 \cdot (q^{n/4} - 1)q^{3n/2}. \tag{4}$$

If $(q, 3) = 1$, then the left part of inequality (1) is not greater than

$$(q^{n/4} - 2) + 15(q^{n/4} - 1)q^n + 71 \cdot 16 \cdot (q^{n/4} - 1)q^{3n/2}. \tag{5}$$

If $q = 3^t$, then the number (4) is greater than $q^{2n} - 1$ only for the following values of n and q: $n = 4$, $q = 3, 9, 27, 81, 243$; $n = 8$, $q = 3, 9$; $n = 12, 16$, $q = 3$. If $(q, 3) = 1$, then the number (5) is greater than $q^{2n} - 1$ only for the following values of n and q: $n = 4$, $q < 1136$; $n = 8$, $q \leqslant 31$; $n = 12$, $q = 5, 7$; $n = 16$, $q = 5$.

Let λ be a generating element of $GF(q^k)^*$. Then A is generated by $f = \lambda \mathbb{1}_4$. Assume that $q^k \equiv 1 \pmod 4$. Then by [13, § 21.2, Theorem 5(i)] we obtain that B

modulo A is generated by the following matrices

$$a_1 = \mathbb{1}_2 \otimes \mathrm{diag}(1,-1), a_2 = \mathrm{diag}(1,-1) \otimes \mathbb{1}_2,$$

$$b_1 = \mathbb{1}_2 \otimes \mathrm{perm}((1,2);2), b_2 = \mathrm{perm}((1,2);2) \otimes \mathbb{1}_2.$$

If $q^k \equiv 3 \pmod 4$, let $\gamma, \delta \in GF(q^k)$ be such that $\gamma^2 + \delta^2 + 1 = 0$. Then by [13, § 21.2, Theorem 5(ii)] the subgroup B modulo A is generated either by the above matrices a_1, a_2, b_1, b_2, or by the matrices a_1, b_1,

$$a_2' = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \otimes \mathbb{1}_2, b_2' = \begin{pmatrix} \gamma & \delta \\ \delta & -\gamma \end{pmatrix} \otimes \mathbb{1}_2.$$

Step 4(a), $q^k \equiv 1 \pmod 4$. Let $\iota = \lambda^{(q^k-1)/4}$ be a square root of -1. Then B is generated by f, a_1, a_2, b_1, b_2. As we noted above, G/B is isomorphic to either a subgroup of S_1, or a subgroup of S_2.

Step 4(a1), $C_1/B \simeq S_1$. By using generating matrices from case $C_1/B \simeq Sp_2(2)$ (see [13, § 21.3]) it is easy to see that the subgroup H_1 of C_1 such that $H_1/B \simeq Sp_2(2) \times Sp_2(2)$ is generated modulo B by the following matrices

$$g_1 = \mathbb{1}_2 \otimes \mathrm{diag}(1,-\iota), g_2 = \mathrm{diag}(1,-\iota) \otimes \mathbb{1}_2,$$

$$h_1 = \mathbb{1}_2 \otimes \begin{pmatrix} 1 & \iota \\ 1 & -\iota \end{pmatrix}, h_2 = \begin{pmatrix} 1 & \iota \\ 1 & -\iota \end{pmatrix} \otimes \mathbb{1}_2.$$

An element σ, generating C_1 modulo H_1 such that $g_1^\sigma = g_2$ and $h_1^\sigma = h_2$ can be chosen to be equal to $\sigma = \mathrm{perm}((2,3);4)$.

Direct computations show that for $v = (1,1,1,0)$ the order of $C_{H_1}(v)$ divides 6. So $|C_G(v)|$ divides 12 if $(q,3) = 1$ and $|C_G(v)|$ divides 4 if $q = 3^t$. Since $(|G|, q) = 1$, then $C_G(v)$ is completely reducible, so as above we may assume that $C_G(v) \leq GL_3(q^k)$. By Lemma 2.4, for $q^k \geqslant 12$ ($q^k \geqslant 4$ if $q = 3^t$) there exists $u \in GF(q^k)^3 \leq GF(q^k)^4$ such that $C_{C_G(v)}(u) = \{e\}$. So we may assume that $q^k = 5$ (recall that we are assuming $q^k \equiv 1 \pmod 4$). In this case direct computations (by using [17], for example) show that for $u = (0,1,2,1)$ we have $C_G(v) \cap C_G(u) = \{e\}$.

Step 4(a2), $C_1/B \simeq S_2$, in particular $|C_1/B|$ divides 20. Then we have that $|G/B|$ divides 20 and condition $(|G|, q) = 1$ implies that if $q^k = 5^t$, then $|G/B|$ divides 4. Now for $v = (1,1,1,0)$ we have that $C_B(v) = \{e\}$, hence $|C_G(v)|$ divides 20 (if $q^k = 5^t$, then $|C_G(v)|$ divides 4). Lemma 2.4 implies that for $q^k \geqslant 20$ ($q^k \geqslant 4$ if $q^k = 5^t$) there exists u such that $C_G(v) \cap C_G(u) = \{e\}$. Thus we need to consider $q^k = 9, 13, 17$ only (recall that we are still assuming $q^k \equiv 1 \pmod 4$). For $q^k = 13, 17$ we have that the minimal α such that $q^\alpha \equiv 1 \pmod 5$ is equal to 4. So, for every element x of order 5 in $GL_4(q)$, we have that $C_V(x) = \{0\}$. Hence $|C_G(v)|$ divides 4 and Lemma 2.4 implies that there exists u such that $C_G(v) \cap C_G(u) = \{e\}$. For $q^k = 9$ we can take an element x of order 5 to be equal to

$$x = \begin{pmatrix} 0 & 1 & -1 & 0 \\ 0 & 1 & 1 & 0 \\ \iota & 0 & 0 & \iota \\ -\iota & 0 & 0 & \iota \end{pmatrix},$$

where $\iota^2 = -1$. Now direct computations (by using [17], for example) show that $C_{\langle B,x\rangle}(v) = \{e\}$, where $v = (1,1,1,0)$. Since $\langle B, x\rangle \trianglelefteq G$, then $|C_G(v)| \leqslant 4$ and by Lemma 2.4 we have that $C_G(v) \cap C_G(u) = \{e\}$ for some u.

Step 4(b), $q^k \equiv -1 \pmod 4$. Let

$$R = \langle f, a_1, a_2, b_1, b_2 \rangle$$

and

$$R' = \langle f, a_1, a_2', b_1, b_2' \rangle.$$

By [13, § 21.2, Theorem 5] we obtain that, up to conjugation in $GL_4(q^k)$, either $B = R$, or $B = R'$. In view of [7, (1C)] we have that $N_{GL_4(q^k)}(R)/R \simeq O_4^+(2) \simeq SL_2(2) \wr \mathrm{Sym}_2$ and $N_{GL_4(q^k)}(R')/R' \simeq O_4^-(2) \simeq \mathrm{Sym}_5$.

Step 4(b1), $B = R$ and $C_1 = N_{GL_4(q^k)}(R)$ (since $N_{GL_4(q^k)}(R)$ is solvable). Let Q be a Sylow 3-subgroup of C_1. Then BQ is a normal subgroup of C_1 of index 8. We state that the following matrices generate BQ modulo B

$$g_1 = \mathrm{perm}((1,2,3);4), g_2 = \begin{pmatrix} -1 & 1 & -1 & -1 \\ -1 & -1 & 1 & -1 \\ 1 & -1 & -1 & -1 \\ 1 & 1 & 1 & -1 \end{pmatrix}.$$

Indeed, g_1 clearly normalizes B. Direct computations show that the following equalities hold: $a_1 g_2 = g_2 a_2 b_2 f^{(q^k-1)/2}$, $a_2 g_2 = g_2 a_1 a_2 b_1 b_2$, $b_1 g_2 = g_2 a_1 a_2$, and $b_2 g_2 = g_2 a_2 f^{(q^k-1)/2}$, so $g_1, g_2 \in N_{GL_4(q^k)}(B) = C_1$. Now $|g_1| = |g_2| = 3$ and $g_1 \cdot g_2 = g_2 \cdot g_1$, so we may assume that $g_1, g_2 \in Q$. Since $|QB/B| = 9$ we obtain that $\langle g_1, g_2 \rangle B_1 = QB_1$. Again direct computations show that for $v = (1, \lambda, 1, 0)$ we have $C_{QB}(v) = \{e\}$. Since $|C_1/QB| = 8$, we obtain that $|C_G(v)|$ divides 8. Like above, Lemma 2.4 implies that for $q^k \geqslant 8$ there exists u such that $C_G(v) \cap C_G(u) = \{e\}$. If $q^k = 3$ then condition $(|G|, q) = 1$ implies that G is a 2-group and Theorem 3.1 follows from [10]. If $q^k = 7$ then direct computations (by using [17], for example), show that C_1 modulo QB can be generated by the following matrices

$$d_1 = \mathrm{diag}(-1, 1, 1, 1), d_2 = \begin{pmatrix} 0 & -1 & 1 & 0 \\ -1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}.$$

Direct computations (by using [17], for example) show that for $v = (1, 3, 1, 0)$ and $u = (0, 0, 1, 1)$ we have that $C_G(v) \cap C_G(u) = \{e\}$.

Step 4(b2), $B = R'$. By Lemma 2.2(i) it follows that G/B is isomorphic to a completely reducible subgroup of $O_4^-(2) \leq Sp_4(2)$. If G/B is a completely reducible subgroup of $O_4^-(2)$, then $O_2(G/B) = \{e\}$. There are (up to conjugation) two maximal solvable subgroups of $O_4^-(2) \simeq \mathrm{Sym}_6$ with a trivial normal 2-subgroup: $\mathbb{Z}_3 \leftthreetimes \mathbb{Z}_2$ of order 6 and $\mathbb{Z}_5 \leftthreetimes \mathbb{Z}_4$ of order 20. Note that for $q^k > 3$ and $v = (1, \lambda, 1, 0)$ we have that $C_{R_1'}(v) = \{e\}$. So if $|G/B|$ divides 6, then Lemma 2.4 implies that there exist u such that $C_G(v) \cap C_G(u) = \{e\}$ (if $q^k = 3$ then G is a 2-group and Theorem 3.1 follows from [10, Theorem 1.1]). Assume that G/B divides 20. Then Lemma 2.4 implies that for $q^k \geqslant 20$ there exists u such that $C_G(v) \cap C_G(u) = \{e\}$. Thus we may assume that $q^k = 3, 7, 11, 19$ (recall that we are assuming $q^k \equiv -1 \pmod 4$). If $q^k = 7$, then the minimal d such that $q^d \equiv 1 \pmod 5$ is equal to 4. So for every element x of $GL_4(q^k)$ of order 5 we have that $C_V(x) = \{0\}$. Therefore $|C_G(v)|$ divides 4, and Lemma 2.4 again implies that there exists u such that $C_G(v) \cap C_G(u) = \{e\}$. If $q^k = 3$ then we can take $\gamma = \delta = 1$ and direct computations (by using [17], for example) show that C_1 modulo B is generated by

$$x = \begin{pmatrix} 0 & 1 & 0 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 \\ 0 & -1 & 0 & -1 \end{pmatrix}, y = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & -1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix},$$

where $|x| = 5$, $|y| = 8$ and $y^4 \in B$. Direct computations (by using [17], for example) imply that for $v = (1, -1, 0, 0)$, $u = (0, 0, 0, 1)$ we have $C_G(v) \cap C_G(u) = \{e\}$. If $q^k = 11$ then we can take $\gamma = 1$, $\delta = 3$ and direct computations (by using [17], for example) show that C_1 modulo B is generated by

$$x = \begin{pmatrix} 1 & 3 & 1 & 3 \\ 0 & -1 & 0 & -1 \\ 3 & -1 & -3 & 1 \\ -1 & 0 & 1 & 0 \end{pmatrix}, y = \begin{pmatrix} 2 & 5 & 6 & 2 \\ 1 & 5 & 6 & 1 \\ 6 & 1 & 1 & 5 \\ 5 & 9 & 9 & 6 \end{pmatrix},$$

where $|x| = 5$, $|y| = 8$ and $y^4 \in B$. Direct computations (by using [17], for example) imply that for $v = (1, 2, 1, 0)$ we have $C_G(v) = \{e\}$. If $q^k = 19$ then we can take $\gamma = \delta = 3$ and direct computations (by using [17], for example) show that an element x of order 5 of $GL_4(19)$ normalizing B can be chosen to be equal to

$$x = \begin{pmatrix} 9 & 9 & 10 & 10 \\ 10 & 9 & 9 & 10 \\ 0 & 3 & 0 & 3 \\ 3 & 0 & 3 & 0 \end{pmatrix}.$$

Then $M = \langle B, x \rangle$ is a normal subgroup of C_1 of index 4 and direct computations (by using [17], for example) show that for $v = (1, 2, 1, 0)$ we have $C_M(v) = \{e\}$. So $|C_G(v)| \leqslant 4$ and Lemma 2.4 imply that there exists u such that $C_G(v) \cap C_G(u) = \{e\}$.

Now we turn to the general case. We may assume that $n/k \geqslant 5$. Direct calculations show that $(n/k)^{13/2} \cdot (q^k - 1) < q^{n/2}$ if $n \geqslant 64$, i. e., inequality (2) is true and inequality (1) is not true. So we may assume that $n \leqslant 63$. Recall that by Lemma 2.2, each prime divisor of $|B/A|$ should divide $|A|$. Calculations by using Lemma 2.6 show that inequality (1) is true only for the following values of q and n:

(1) $q = 3$, $n = 8, 16$;
(2) $q = 5$, $n = 8, 12, 16$;
(3) $q = 7$, $n = 6, 8, 9, 12, 16$;
(4) $q = 9$, $n = 8$;
(5) $q = 11$, $n = 5, 8, 10$;
(6) $q = 13$, $n = 6, 8$;
(7) $q = 17$, $n = 8$;
(8) $q = 19$, $n = 6, 8$.

Step 5. $n = 5$, $q = 11$. In this case we remain to consider $k = 1$. Denote by λ the generating element of $GF(11)$ and let $\eta = \lambda^2$. By [13, §21.3, Theorem 4] we obtain that B is generated by $f = \lambda \mathbb{1}_5$, $a = \mathrm{diag}(1, \eta, \eta^2, \eta^3, \eta^4)$, $b = \mathrm{perm}((1, 2, 3, 4, 5); 5)$.

Consider $x = \mathrm{diag}(\eta, \eta, 1, \eta^3, 1)$ and

$$y = \begin{pmatrix} \eta & 1 & \eta^3 & 1 & \eta \\ \eta & \eta & 1 & \eta^3 & 1 \\ 1 & \eta & \eta & 1 & \eta^3 \\ \eta^3 & 1 & \eta & \eta & 1 \\ 1 & \eta^3 & 1 & \eta & \eta \end{pmatrix}.$$

Direct computations show that $a^x = a$, $b^x = ba$, $a^y = ab$, $b^y = b$, so elements f, a, b, x, y generate $N_{GL_5(11)}(B)$ and $G \leq \langle f, a, b, x, y \rangle = M$. Again by direct calcultion (by using, [17], for example), it is easy to check that for $v = (\lambda, \lambda^2, \lambda^5, 1, 0)$ we have $|C_M(v)| = 10$. Thus $|C_G(v)| \leqslant 10$ and by Lemma 2.4 there exists u such that $C_G(v) \cap C_G(u) = \{e\}$.

Step 6. $n = 6$, $q \in \{7, 13, 19\}$. In this case we remain to consider $k = 1$, so $G = C$. Let λ be a generating element of $GF(q)$ and $\eta = \lambda^{(q-1)/3}$. By Lemma 2.2 we obtain that $B/A = B'/A \times B''/A$ and $C/B \leq C'/B \times C''/B$, where $|B'/A| = 2^2$, $|B''/A| = 3^2$, $C'/B \leq Sp_2(2)$, $C''/B \simeq Sp_2(3)$. Moreover by using [13, §20.2, Theorem 6] and [13, §21.2, Theorems 4,5] we obtain that B' modulo A is generated either by

$$a_1 = \mathrm{diag}(1, -1) \otimes \mathbb{1}_3, b_1 = \mathrm{perm}((1, 2); 2) \otimes \mathbb{1}_3,$$

or by

$$a_1' = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \otimes \mathbb{1}_3, b_1' = \begin{pmatrix} \gamma & \delta \\ \delta & -\gamma \end{pmatrix} \otimes \mathbb{1}_3,$$

(the second possibility occurs only if $q \equiv 3 \pmod 4$; γ, δ satisfy $\gamma^2 + \delta^2 + 1 = 0$); and B'' modulo A is generated by

$$a_2 = \mathbb{1}_2 \otimes \mathrm{diag}(1, \eta, \eta^2), b_2 = \mathbb{1}_2 \otimes \mathrm{perm}((1, 2, 3); 3).$$

We also have that C'' modulo B is generated by $\mathbb{1}_2 \otimes c$ and $\mathbb{1}_2 \otimes d$, where c and d are chosen as in Step 3(a).

Step 6(a). $q \equiv 1 \pmod 4$, i. e., $q = 13$. Then B' modulo A is generated by a_1 and b_1. Let $\iota = \lambda^3$ be a square root of -1 in $GF(13)$. By [13, § 21.3] we have that C' modulo B is generated by

$$g = \mathrm{diag}(1, -\iota) \otimes \mathbb{1}_3, h = \begin{pmatrix} 1 & \iota \\ 1 & -\iota \end{pmatrix} \otimes \mathbb{1}_3.$$

Thus $G = \langle \lambda \mathbb{1}_6, a_1, b_1, a_2, b_2, \mathbb{1}_2 \otimes c, \mathbb{1}_2 \otimes d, g, h \rangle$, and direct calculations (by using [17], for example) show that for $v = (\lambda, \lambda^2, \lambda^4, \lambda^3, 1, \lambda)$ we have $C_G(v) = \{e\}$.

Step 6(b). $q \equiv -1 \pmod 4$, i. e., $q = 7, 19$. Let $R = \langle \lambda \mathbb{1}_6, a_1, b_1, a_2, b_2 \rangle$ and $R' = \langle \lambda \mathbb{1}_6, a_1', b_1', a_2, b_2 \rangle$. Then by [13, §21.2, Theorem 5] we obtain that, up to conjugation in $GL_6(q)$, either $B' = R$, or $B' = R'$. In view of [7, (1C)] we have that $C'/B \simeq O_2^+(2) \simeq \mathbb{Z}_2$ if $B' = R$, and $C'/B \simeq O_2^-(2) \simeq GL_2(2)$ if $B' = R'$.

Step 6(b1). $B' = R$, $C'/B \simeq \mathbb{Z}_2$. In this case C' modulo B is generated by

$$g = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes \mathbb{1}_3,$$

so $G \leq \langle \lambda \mathbb{1}_6, a_1, b_1, a_2, b_2, \mathbb{1}_2 \otimes c, \mathbb{1}_2 \otimes d, g \rangle$. Direct calculations (by using [17], for example) show that for $v = (\lambda, \lambda^2, \lambda^4, \lambda^3, 1, \lambda)$ we have that $|C_G(v)| \leqslant 2$. By Lemma 2.4 we obtain that there exists u such that $C_G(v) \cap C_G(u) = \{e\}$.

Step 6(b2). $B' = R'$, $C'/B \simeq GL_2(2)$. If we take $\lambda = 3$ for $q = 7$ and $\lambda = 2$ for $q = 19$, then we may choose $\gamma = \lambda$, $\delta = \lambda^2$ for $q = 7$; and $\lambda = \delta = 3 = \lambda^{13}$ for $q = 19$. In view of [13, §21.3] we obtain that C' modulo B is generated by

$$g = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \otimes \mathbb{1}_3, h = \begin{pmatrix} \gamma & \delta - 1 \\ \delta + 1 & -\gamma \end{pmatrix} \otimes \mathbb{1}_3.$$

Thus $G \leq \langle \lambda \mathbb{1}_6, a_1', b_1', a_2, b_2, \mathbb{1}_2 \otimes c, \mathbb{1}_2 \otimes d, g, h \rangle$. Direct calculations (by using [17], for example) show that for $v = (\lambda, \lambda^2, \lambda^4, \lambda^3, 1, \lambda)$ we have $C_G(v) = \{e\}$.

Step 7. $n = 8$, $q \in \{3, 5, 7, 9, 11, 13, 17, 19\}$. In this case we remain to consider $k = 1$, so $G = C$. Let λ be a generating element of $GF(q)$, then A is generated by $\lambda \mathbb{1}_8$. The structure of $N_{GL_8(q)}(B)$ is different for $q \equiv 1 \pmod 4$ and for $q \equiv -1 \pmod 4$.

Step 7(a). $q \equiv 1 \pmod 4$, i. e., $q \in \{5, 9, 13, 17\}$. Denoting $a = \mathrm{diag}(1, -1)$ and $b = \mathrm{perm}((1, 2); 2)$, by [13, §21.2, Theorem 5(i)] it follows that B modulo A is generated by $a_1 = a \otimes \mathbb{1}_4$, $a_2 = \mathbb{1}_2 \otimes a \otimes \mathbb{1}_2$, $a_3 = \mathbb{1}_4 \otimes a$, and $b_1 = b \otimes \mathbb{1}_4$, $b_2 = \mathbb{1}_2 \otimes b \otimes \mathbb{1}_2$, $b_3 = \mathbb{1}_4 \otimes b$. By [7, (1B)] we obtain that $N_{GL_8(q)}(B)/B \simeq Sp_6(2)$. Direct calculations show that $N_{GL_8(q)}(B)$ modulo B is generated by the following matrices:

$$x = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}, y = \begin{pmatrix} 0 & 0 & 0 & -1 & -1 & 0 & 0 & 0 \\ 0 & 0 & -\iota & 0 & 0 & \iota & 0 & 0 \\ 0 & 0 & 0 & \iota & -\iota & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & \iota & 0 & 0 & 0 & 0 & -\iota & 0 \\ \iota & 0 & 0 & 0 & 0 & 0 & 0 & -\iota \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix},$$

where $\iota^2 = -1$, $|x| = 2$, $|yB| = 30$. Direct calculations (by using [17], for example) show that for $v = (\lambda, \lambda^2, \lambda^3, 1, 0, \lambda^{-1}, 0, \lambda^{-2})$ and $u = (0, 0, 0, 1, 0, 0, 1, 1)$ we have $C_{N_{GL_8(q)}(B)}(v) \cap C_{N_{GL_8(q)}(B)}(u) = \{e\}$.

Step 7(b). $q \equiv -1 \pmod 4$, i. e., $q \in \{3, 7, 11, 19\}$. By [13, §21.2, Theorem 5(ii)] it follows that, up to conjugation in $GL_8(q)$, either $B = R$, or $B = R'$, where R is generated by $\lambda \mathbb{1}_8, a_1, a_2, a_3, b_1, b_2, b_3$; R' is generated by $\lambda \mathbb{1}_8, a_1, a_2, a_3', b_1, b_2, b_3'$; $a_1, a_2, a_3, b_1, b_2, b_3$ are taken as in Step 7(a), and

$$a_3' = \mathbb{1}_4 \otimes \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, b_3' = \mathbb{1}_4 \otimes \begin{pmatrix} \gamma & \delta \\ \delta & -\gamma \end{pmatrix},$$

with $\gamma^2 + \delta^2 + 1 = 0$. By [7, (1C)] we obtain that $N_{GL_8(q)}(R)/R \simeq O_6^+(2)$ and $N_{GL_8(q)}(R')/R' \simeq O_6^-(2)$.

Step 7(b1). $B = R$, $N_{GL_8(q)}(B)/B \simeq O_6^+(2)$. Direct calculations show that $N_{GL_8(q)}(B)$ modulo B is generated by

$$x = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}, y = \begin{pmatrix} -1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & -1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

If $q = 3$ then computations by using [17] show that for

$$v = (-1, 1, 0, -1, -1, 0, 1, -1)$$

we have $|C_{N_{GL_8(3)}(B)}(v)| = 2304 = 2^8 \cdot 3^2$. Condition $(|G|, q) = 1$ implies that $C_G(v)$ is contained in a Sylow 2-subgroup Q of $C_{N_{GL_8(3)}(B)}(v)$. Again by using [17] it is easy to check that there exists u such that $C_Q(u) = \{e\}$. If $q \geqslant 7$, then direct calculations (by using [17], for example) show that for $v = (\lambda, \lambda^2, \lambda^3, 1, 0, \lambda^{-1}, 0, \lambda^{-2})$ and $u = (0, 0, 0, 1, 0, 0, 1, 1)$ we have $C_{N_{GL_8(q)}(B)}(v) \cap C_{N_{GL_8(q)}(B)}(u) = \{e\}$.

Step 7(b2). $B = R'$, $N_{GL_8(q)}(B)/B \simeq O_6^-(2)$. Direct calculations show that $N_{GL_8(q)}(B)$ modulo B is generated by

$$x_1 = x \otimes \mathbb{1}_4, x_2 = \mathbb{1}_2 \otimes x \otimes \mathbb{1}_2, x_3 = \mathbb{1}_4 \otimes x, x_4 = \mathbb{1}_4 \otimes y,$$

$$x_5 = \mathrm{diag}(-1, -1, 1, 1, 1, 1, 1, 1), x_6 = \mathrm{perm}((2, 3); 4) \otimes \mathbb{1}_2, x_7 = \mathbb{1}_2 \otimes z,$$

where

$$x = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}, y = \begin{pmatrix} \gamma & \delta - 1 \\ \delta + 1 & -\gamma \end{pmatrix},$$

z is a 4×4 matrix of order 5, that is given in Step 4(b2) for $q \in \{3, 11, 19\}$ (γ and δ are also defined there), and

$$z = \begin{pmatrix} -3 & -1 & -3 & -3 \\ -1 & 3 & 3 & -3 \\ -3 & -1 & 3 & 3 \\ -1 & 3 & -3 & 3 \end{pmatrix}$$

if $q = 7$ (γ and δ for $q = 7$ are chosen as in Step 6(b2)). If $q = 3$, then calculations by using [17] show that for $v = (0, 0, 0, 1, 0, 1, 0, 1)$ we have $|C_{N_{GL_8(3)}(B)}(v)| = 1296 = 16 * 81$. The condition $(|G|, q) = 1$ implies that $C_G(v)$ is contained in a Sylow 2-subgroup of $C_{N_{GL_8(3)}(B)}(v)$. Calculations by using [17] show that for a Sylow 2-subgroup Q of $C_{N_{GL_8(3)}(B)}(v)$ there exists u such that $C_Q(u) = \{e\}$. If $q \geqslant 7$, then direct calculations (by using [17], for example) show that for $v = (\lambda, \lambda^2, \lambda^3, 1, 0, \lambda^{-1}, 0, \lambda^{-2})$ and $u = (0, 0, 0, 1, 0, 0, 1, 1)$ we have $C_{N_{GL_8(q)}(B)}(v) \cap C_{N_{GL_8(q)}(B)}(u) = \{e\}$.

Step 8. $n = 9$, $q = 7$. In this case we remain to consider $k = 1$, so $G = C$. Let λ be a generating element of $GF(7)$, then A is generated by $\lambda \mathbb{1}_8$. Denote by $\eta = \lambda^2$. Then [13, § 21.2, Theorem 4] implies that B modulo A is generated by $a_1 = \mathrm{diag}(1, \eta, \eta^2) \otimes \mathbb{1}_3$, $a_2 = \mathbb{1}_3 \otimes \mathrm{diag}(1, \eta, \eta^2)$, $b_1 = \mathrm{perm}((1, 2, 3); 3) \otimes \mathbb{1}_3$, $b_2 = \mathbb{1}_3 \otimes \mathrm{perm}((1, 2, 3); 3)$. Direct calculations (by using [17], for example) show that $N_{GL_9(7)}(B)$ modulo B is generated by $c_1 = c \otimes \mathbb{1}_3$, $c_2 = \mathbb{1}_3 \otimes c$, $d_1 = d \otimes \mathbb{1}_3$, $d_2 = \mathbb{1}_3 \otimes d$, $x_1 = \mathrm{perm}((2, 4)(3, 7)(6, 8); 9)$, $x_2 = \mathrm{diag}(\eta, \eta, \eta^2, 1, \eta, 1, \eta, 1, 1)$, where matrices c and d are defined in Step 3. Then for $v = (\lambda, \lambda^2, \lambda^3, 1, 0, \lambda^{-1}, 0, \lambda^{-2}, \lambda]$, $u = (0, 0, 0, 1, 0, 0, 1, 1, 1)$ we have that $C_{N_{GL_9(7)}(B)}(v) \cap C_{N_{GL_9(7)}(B)}(u) = \{e\}$.

Step 9. $n = 10$, $q = 11$. In this case we remain to consider $k = 1$ Let λ be a generating element of $GF(11)^*$ and $\eta = \lambda^2$. By Lemma 2.2 we obtain that $B/A = B'/A \times B''/A$ and $C/B \leq C'/B \times C''/B$, where $|B'/A| = 2^2$, $|B''/A| = 5^2$, $C'/B \leq Sp_2(2)$, $C''/B \leq Sp_2(5)$. By [13, §20.2, Theorem 6] and [13, §21.2, Theorems 4,5] it follows that B' modulo A is generated either by

$$a_1 = \mathrm{diag}(1, -1) \otimes \mathbb{1}_5, b_1 = \mathrm{perm}((1, 2), 2) \otimes \mathbb{1}_5,$$

or by

$$a_1' = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \otimes \mathbb{1}_5, b_1' = \begin{pmatrix} \gamma & \delta \\ \delta & -\gamma \end{pmatrix} \otimes \mathbb{1}_5,$$

where $\gamma^2 + \delta^2 + 1 = 0$; and B'' modulo A is generated by

$$a_2 = \mathbb{1}_2 \otimes \operatorname{diag}(1, \eta, \eta^2, \eta^3, \eta^4), b_2 = \mathbb{1}_2 \otimes \operatorname{perm}((1,2,3,4,5);5).$$

We also have that C'' modulo B is generated by $\mathbb{1}_2 \otimes x$ and $\mathbb{1}_2 \otimes y$, where x, y are defined in Step 5.

Let $R = \langle \lambda \mathbb{1}_9, a_1, b_1, a_2, b_2 \rangle$ and $R' = \langle \lambda \mathbb{1}_9, a_1', b_1', a_2, b_2 \rangle$. Then by [13, §21.2, Theorem 5] we obtain that, up to conjugation in $GL_{10}(11)$, either $B' = R$, or $B' = R'$. In view of [7, (1C)] we have that $C'/B \simeq O_2^+(2) \simeq \mathbb{Z}_2$ if $B' = R$ and $C'/B \simeq O_2^-(2) \simeq GL_2(2)$ if $B' = R'$.

Step 9(a). $B' = R$, $C'/B \simeq \mathbb{Z}_2$. In this case C' modulo B is generated by

$$g = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes \mathbb{1}_5,$$

so $G \leq \langle \lambda \mathbb{1}_{10}, a_1, b_1, a_2, b_2, g, \mathbb{1}_2 \otimes x, \mathbb{1}_2 \otimes y \rangle$. Direct calculations (by using [17], for example) show that for

$$v = (\lambda, \lambda^2, \lambda^3, \lambda^4, \lambda^5, \lambda^6, \lambda^7, \lambda^8, \lambda^9, 0),$$

$$u = (1, 0, 0, 0, 0, -1.0, 0, 1, 1)$$

we have $C_{N_{GL_{10}(q)}(B)}(v) \cap C_{N_{GL_{10}(q)}(B)}(u) = \{e\}$.

Step 9(b). $B' = R'$, $C'/B \simeq GL_2(2)$. We may take $\gamma = 1$ and $\delta = 3$, as in Step 4($a2_2$). In view of [13, §21.3] we obtain that C' modulo B is generated by

$$g = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \otimes \mathbb{1}_5, h = \begin{pmatrix} \gamma & \delta - 1 \\ \delta + 1 & -\gamma \end{pmatrix} \otimes \mathbb{1}_5.$$

Thus $G = \langle \lambda \mathbb{1}_{10}, a_1', b_1', a_2, b_2, g, h, \mathbb{1}_2 \otimes x, \mathbb{1}_2 \otimes y \rangle$. Direct calculations (by using [17], for example) show that for

$$v = (\lambda, \lambda^2, \lambda^3, \lambda^4, \lambda^5, \lambda^6, \lambda^7, \lambda^8, \lambda^9, 0),$$

$$u = (1, 0, 0, 0, 0, -1.0, 0, 1, 1)$$

we have $C_{N_{GL_{10}(q)}(B)}(v) \cap C_{N_{GL_{10}(q)}(B)}(u) = \{e\}$.

Step 10. $n = 12$, $q = 7$. In this case we remain to consider cases $k = 1$. We have that $B/A \simeq B'/A \times B''/A$, where B'/A is a 2-group of order 2^4 and B''/A is a group of order 3^2. Moreover $C/B \simeq C'/B \times C''/B$, where $C''/B \simeq Sp_2(3)$ and either $C'/B \simeq O_4^+(2)$, or $C'/B \simeq O_4^-(2)$. Generators were found in the previous steps 6 and 7, and for $v = (\lambda, \lambda^2, \lambda^3, \lambda^4, \lambda^5, 1, 0, \lambda^(-1), 0, \lambda^{-2}, \lambda, 0)$, $u = (0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, -1)$ we have that $C_G(v) \cap C_G(u) = \{e\}$.

Step 11. $n = 16$, $k = 3, 5, 7$. In this case we remain to consider $k = 1$. If $k = 1$, then $N_{GL_{16}(q)}(B)/B$ is isomorphic to either $Sp_8(2)$, or $O_8^+(2)$, or $O_8^-(2)$. We describe how one can obtain generating elements if $N_{GL_{16}(q)}(B)/B \simeq Sp_8(2)$ (in this case $q \equiv 1 \pmod 4$). Denote $a = \operatorname{diag}(1, -1)$, $b = \operatorname{perm}((1,2);2)$. Then B modulo A is generated by a_i, b_i, where $i = 1, \ldots, 4$, $a_i = \mathbb{1}_{2(i-1)} \otimes a \otimes \mathbb{1}_{8-2(i-1)}$, $b_i = \mathbb{1}_{2(i-1)} \otimes b \otimes \mathbb{1}_{8-2(i-1)}$. Consider $B_1 \leq GL_8(q)$ generated by $\lambda \mathbb{1}_8, \bar{a}_1, \bar{a}_2, \bar{a}_3, \bar{b}_1, \bar{b}_2, \bar{b}_3$, where $\bar{a}_i = \mathbb{1}_{2(i-1)} \otimes a \otimes \mathbb{1}_{4-2(i-1)}$ and $\bar{b}_i = \mathbb{1}_{2(i-1)} \otimes b \otimes \mathbb{1}_{4-2(i-1)}$. Then generators x, y of $N_{GL_8(q)}(B_1)$ are found in Step 7(a) and $N_{GL_{16}(q)}(B)$ modulo B is generated by $x \otimes \mathbb{1}_2$, $\mathbb{1}_2 \otimes x$, $y \otimes \mathbb{1}_2$, $\mathbb{1}_2 \otimes y$. In the remaining cases we proceed in the same way. Direct calculations (by using [17], for example) show that in any case for

$$v = (\lambda, \lambda^2, \lambda^3, 1, 0, \lambda^{-1}, 0, \lambda^{-2}, \lambda^{-2}, 0, \lambda^{-1}, 0, 1, \lambda^3, \lambda^2, \lambda),$$

$$u = (0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 0, 0)$$

we have that $C_G(v) \cap C_G(u) = \{e\}$. This completes the proof of Theorem 3.1. $\square$

4. Proof of the main theorem

Lemma 4.1. [12, Theorem 1.2] *Let $G \leq \mathrm{Sym}_n$ be a solvable permutation group. Then there exists a partition P of $\{1, \ldots, n\}$ into at most five parts such that only the identity element of G fixes P.*

From the proof of [12, Theorem 1.2] it is easy to obtain the following corollary.

Corollary 4.2. *Let $G \leq \mathrm{Sym}_n$ be a solvable permutation group of order not divisible by 3. Then there exists a partition P of $\{1, \ldots, n\}$ into at most four parts such that only the identity element of G fixes P.*

Lemma 4.3. *Let G be a primitive solvable subgroup of $GL_n(q)$ with $(|G|, p) = 1$. If $q = 3$ then there exist at least 4 non-equivalent under G regular elements in $V \times V$ and if $q \geqslant 5$, then there exist at least 5 non-equivalent under G regular elements in $V \times V$.*

Proof. If $q \geqslant 5$, then Lemma 4.3 immediately follows from Lemma 2.5 (we have at least q non-equivalent regular elements). If $q = 3$ and (v, u) is a regular element under G, then consider $U = \langle v, u \rangle$. Consider the homomorphism $\varphi : N_G(U) \to GL(U) = GL_2(3)$ given by $\varphi : g \mapsto g|_U$. Since (v, u) is a regular element under G, we obtain that φ is an embedding. The condition $(|G|, 3) = 1$ implies that $N_G(U)^\varphi$ is a 2-subgroup of $GL(U)$. By using [17] it is easy to check that, for a Sylow 2-subgroup Q of $GL_2(3) = GL(U)$, in $U \times U$ there are 4 non-equivalent (under Q) regular (under Q) elements. $\square$

Now we prove Theorem 1.1. In view of [2, Theorem 1.3] we may assume that the order of G is even, so q is odd. Assume by contradiction that $G \leq GL_n(q)$ is a counterexample to the statement of Theorem 1.1 of minimal order. It is evident that G is irreducible. If G is primitive then by Theorem 3.1 it follows that there exist a regular under G element $(v, u) \in V \times V$, so G is irreducible and imprimitive.

Since G is imprimitive, there exists a non-refinable decomposition $V = \oplus_{i=1}^k V_i$ into l-dimensional subspaces with $n = kl$, a primitive solvable group $L \leq GL(V_1) = GL_l(q)$, and a transitive solvable group $T \leq \mathrm{Sym}_k$ such that G permutes the V_i and $G \leq L \wr T$. Note also that condition $(|G|, q) = 1$ implies that $(|L \wr T|, q) = 1$. It is enough to prove that there exist a regular under $L \wr T$ element $(v, u) \in V \times V$. Note that T provides an identification between the V_i.

Assume first that $q \geqslant 5$. By Theorem 3.1 and Corollary 4.3, there exist at least 5 non-equivalent under L regular under L elements

$$(v_{1,1}, u_{1,1}), (v_{1,2}, u_{1,2}), (v_{1,3}, u_{1,3}), (v_{1,4}, u_{1,4}), (v_{1,5}, u_{1,5}) \in V_1 \times V_1.$$

Also by Lemma 4.1 there exists a partition $\{1, 2, \ldots, k\} = P_1 \cup P_2 \cup P_3 \cup P_4 \cup P_5$ which is fixed only by the identity element of T. Clearly we may assume that $v_{1,i}, u_{1,i}$ are nonzero vectors for all i. Let $v_{i,j}, u_{i,j}$ be the T-images of $u_{1,j}, v_{1,j}$ respectively in V_i. Define

$$v = \sum_{i\in P_1} v_{i,1} + \sum_{i\in P_2} v_{i,2} + \sum_{i\in P_3} v_{i,3} + \sum_{i\in P_4} v_{i,4} + \sum_{i\in P_5} v_{i,5},$$
$$u = \sum_{i\in P_1} u_{i,1} + \sum_{i\in P_2} u_{i,2} + \sum_{i\in P_3} u_{i,3} + \sum_{i\in P_4} u_{i,4} + \sum_{i\in P_5} u_{i,5}.$$

We claim that (v, u) is a regular element under G. Consider $g \in C_G((v, u))$. Let $i \leqslant k$ be arbitrary, $V_i^g = V_j$, $i \in P_m$, $j \in P_l$. Then $(v_{i,m}, u_{i,m})^g = (v_{j_l}, u_{j_l})$. Hence $(v_{i,m}, u_{i,m})^g$ and (v_{j_l}, u_{j_l}) cannot be the images of non-equivalent (under L) regular (under L) elements, i. e. $m = l$. So g fixes the partition $P_1 \cup P_2 \cup P_3 \cup P_4 \cup P_5$. Thus g induces the identity permutation of $\{V_1, \dots, V_k\}$, hence $g \in L^k$ and so $g = e$.

If $q = 3$, then by Theorem 3.1 and Corollary 4.3, there exist at least 4 non-equivalent under L regular under L elements, and by Corollary 4.2 there exists a partition $\{1, 2, \dots, k\} = P_1 \cup P_2 \cup P_3 \cup P_4$ which is fixed only by the identity element of T. We construct a regular (under G) element $(v, u) \in V \times V$ like in the previous case.

5. Proofs of Theorems 1.2 and 1.3

Proof of Theorem 1.2. If $2 \notin \pi$ then the theorem is proved in [2, Theorem 1.2]. Assume that $2 \in \pi$ and consider the natural semidirect product $H \rtimes G$. Assume by contradiction that $H \rtimes G$ is a counterexample of minimal order. By Feit-Thompson Odd Order Theorem [3] we obtain that $H \rtimes G$ is solvable. Let $F = F(H \rtimes G)$ be the Fitting subgroup of $H \rtimes G$. Since G acts faithfully and $(|G|, |H|) = 1$ it follows that $F \le H$. Now $C_{H\rtimes G}(F) = Z(F)$, hence, by the minimality of $|H \rtimes G|$ we obtain that $H = F$. Taking $F/\Phi(F)$ and using the fact that $(|G|, |F|) = 1$ we obtain that $F = V_1 \times \ldots \times V_k$, where each V_i is elementary Abelian of order $p_i^{k_i}$. By Theorem 1.1 it follows that for every i there exist v_i, u_i such that $C_G(v_i) \cap C_G(u_i) \le C_G(V_i)$. Hence $C_G(v_1 \cdot \ldots \cdot v_k) \cap C_G(u_1 \cdot \ldots \cdot u_k) \le C_G(V_1) \cap \ldots \cap C_G(V_k) \le C_G(F) = \{e\}$. □

Proof of Theorem 1.3. Assume by contradiction that G is a counterexample of minimal order. By induction we have that $O_\pi(G) = \{e\}$. Let $M \neq \{e\}$ be a minimal normal subgroup of G. Then M is a π'-group. By induction we have that $G = M \rtimes H$. In view of Theorem 1.2 we obtain that there exist $x, y \in M$ such that $C_H(x) \cap C_H(y) = \{e\}$. Now if $h \in H \cap H^x$, then $h = x^{-1} h_1 x$ for some $h_1 \in H$, hence $h_1^{-1} h = h_1^{-1} x^{-1} h_1 x$. Since $h_1^{-1} h \in H$ and $h_1^{-1} x^{-1} h_1 x \in M$, then $h_1^{-1} h = e$ and $h \in C_H(x)$. Thus $H \cap H^x \cap H^y = C_H(x) \cap C_H(y) = \{e\} = O_\pi(G)$. □

References

[1] J.D. Dixon, *The Fitting subgroup of a linear solvable group*, J.Austral.Math.Soc., **7**:4(1967), 417–424.

[2] S. Dolfi, *Intersections of odd order Hall subgroups*, Bull.London Math.Soc., **37**:1 (2005), 61–66.

[3] W. Feit, J. Thompson, *Solvability of groups of odd order*, Pacif. J. Math., **13**:3 (1963), 775–1029.

[4] D. Gluck, O. Manz, *Prime factors of character degrees of solvable groups*, Bull.London Math.Soc., **19**:5 (1987), 431–437.

[5] Z. Halasi, K. Podoski, *On the Orbits of Solvable Linear Groups*, arXiv:0707.2873v1, www.arxiv.org.

[6] I.M. Isaacs, *Large orbits in actions of nilpotent groups*, Proc.Amer.Math.Soc., **127**:1 (1999), 45–50.

[7] A. Jianbei, 2-*Weights for General Linear Groups*, J.Algebra, **149**:2 (1992), 500–527.

[8] P. Kleidman, M. Liebeck, *The Subgroup Structure of the Finite Classical Groups*, London Math.Soc.Lect.Notes, **129** (1990), Cambridge University Press.

[9] P.P. Palfy, *Bounds for linear groups of odd order*, Proc.Second Internat.Group Theory Conf., Bressanone/Brixen, 1989, Suppl.Rend.Circ.Mat.Palermo, **23** (1990), 253–263.

[10] D.S. Passman, *Groups with normal solvable Hall p'-subgroups*, Trans.Amer.Math.Soc., **123**:1 (1966), 99–111.

[11] Y. Segev, *On completely reducible solvable subgroups of $GL(n, \Delta)$*, Israel J.Math., **51**:1-2 (1985), 163–176.

[12] A. Seress, *The minimal base size of primitive solvable permutation groups*, J.London Math.Soc.(2), **53** (1996), 243–255.

[13] D.A. Suprunenko, *Matrix groups*, AMS, Providence, RI, 1976.

[14] D.A. Suprunenko, *Solvable and nilpotent linear groups*, Minsk, 1958 (In Russian).

[15] T.R. Wolf, *Solvable and nilpotent subgroups of $GL_n(q^m)$*, Canad. J. Math., **34**:5 (1982), 1097–1111.

[16] V.I. Zenkov, *Intersections of nilpotent subgroups in finite groups*, Fund.Prikl.Mat., **2**:1 (1996), 1–92.

[17] The GAP Group, GAP — Groups, Algorithms, and Programming, Version 4.4.10 (2007); (http://www.gap-system.org).

Evgeniy Petrovich Vdovin
Sobolev Institute of Mathematics,
pr. Koptyuga, 4,
630090, Novosibirsk, Russia
E-mail address: vdovin@math.nsc.ru