S©MR ISSN 1813-3304

СИБИРСКИЕ ЭЛЕКТРОННЫЕ
МАТЕМАТИЧЕСКИЕ ИЗВЕСТИЯ

Siberian Electronic Mathematical Reports

http://semr.math.nsc.ru

Том 17, стр. 585–589 (2020) УДК 512.54

DOI 10.33048/semi.2020.17.037 MSC 20D06, 20D60, 20C20

ON ELEMENT ORDERS IN COVERS OF $L_4(q)$ AND $U_4(q)$

M.A. GRECHKOSEEVA, S.V. SKRESANOV

Abstract. Suppose that L is one of the finite simple groups $\mathrm{PSL}_4(q)$ or $\mathrm{PSU}_4(q)$ and L acts on a vector space W over a field whose characteristic divides q. We prove that the natural semidirect product of W and L contains an element whose order differs from the order of any element of L, thus answering questions 14.60 and 17.73 (a) of the Kourovka Notebook.

Keywords: simple linear group, simple unitary group, orders of elements, modular representation, defining characteristic.

1. Introduction

Problem 14.60 of the Kourovka Notebook [1] asks whether a finite group H having a nontrivial normal subgroup K such that the factor group H/K is isomorphic to one of the simple groups $\mathrm{PSL}_n(q)$ with $n \geqslant 3$ always contains an element whose order is distinct from the order of any element of H/K. Zavarnitsine [2] proved that this is true if $n \neq 4$ or q is composite. Later he [3] constructed an example showing that this is not true if $n = 4$ and $q = 13^{24}$. It turned out that the proof in [3] was incorrect, and the main goal of the present paper is to show that the answer is affirmative for all $n \geqslant 3$, including $n = 4$.

Before stating the main result, let us put the question into a wider context of recognition by spectrum (see the introduction in [4] for a survey on this subject). The spectrum $\omega(G)$ of a finite group G is the set of the orders of elements of G. We say that G is recognizable by spectrum if for every finite group H, the equality $\omega(H) = \omega(G)$ implies $H \simeq G$. If the implication holds for all finite groups H having a normal subgroup K such that $H/K \simeq G$, then we say that G is recognizable by

Grechkoseeva, M.A., Skresanov, S.V., On element orders in covers of $L_4(q)$ and $U_4(q)$.

The reported study was funded by RFBR, project number 18-31-20011.

Received February, 2, 2020, published April, 16, 2020.

spectrum among covers. In this language, Problem 14.60 asks whether the simple groups $\mathrm{PSL}_n(q)$ with $n \geqslant 3$ are recognizable by spectrum among covers.

It is not hard to see that a finite group G is recognizable among covers if and only if $\omega(G) \neq \omega(K:G)$, where $K \neq 1$ is an elementary abelian group and $K:G$ is a split extension of G by K (see, for example, [5, Lemma 12]), and so representations of G come into play. If G is a simple group of Lie type in characteristic p, it is natural to distinguish two cases, depending on whether p divides K or not (cf. Problems 17.73 and 17.74 of [1]). At the present time, the only open question related to recognizability of simple groups among covers is whether $\omega(G) \neq \omega(K:G)$ in the case when $G = \mathrm{PSL}_4(q)$ or $\mathrm{PSU}_4(q)$, $q = p^m$ is odd and composite, and K is an elementary abelian p-group (see the proof of Corollary 1 below for references). We answer this question in the affirmative, thus solving Problems 14.60 and 17.73 (a) of [1].

Theorem 1. *Let L be $\mathrm{PSL}_4(q)$ or $\mathrm{PSU}_4(q)$, where q is a power of an odd prime p. If L acts on a vector space W over a field of characteristic p then $\omega(W \rtimes L) \neq \omega(L)$.*

Corollary 1. *A finite nonabelian simple group L is recognizable by spectrum among covers if and only if L is neither ${}^3D_4(2)$, nor $\mathrm{PSU}_5(2)$, nor $\mathrm{PSU}_3(q)$, where q is a Mersenne prime such that $q^2 - q + 1$ is a prime.*

2. Proof of the main result

We start with some definitions and preliminary results.

If a is a nonzero integer, then the highest power of 2 dividing a is called the 2-part of a and is denoted by $(a)_2$. The following lemma is an easy consequence of the definition.

Lemma 1. *Let a and b be nonzero integers.*

(1) *If $(a)_2 \geqslant (b)_2$, then $(a+b)_2 \neq (a)_2$.*
(2) *If $(a)_2 = (b)_2$, then $(a+b)_2 > (a)_2$.*

The next lemma was proved by Bang [6]. Also it is a special case of Zsigmondy's theorem [7].

Lemma 2. *Suppose that $\varepsilon \in \{+,-\}$ and $a, n \geqslant 2$ are integers. Then either there is a prime r such that r divides $a^n - (\varepsilon 1)^n$ and does not divide $a^i - (\varepsilon 1)^i$ for all $1 \leqslant i < n$, or one of the following holds:*

(1) *$\varepsilon = +$, $n = 6$, $a = 2$;*
(2) *$\varepsilon = -$, $n = 3$, $a = 2$;*
(3) *$n = 2$ and $a + \varepsilon 1$ is a power of 2.*

We refer to the prime r in Lemma 2 as a primitive prime divisor of $a^n - (\varepsilon 1)^n$ and denote some primitive divisor, if any, by $r_n(\varepsilon a)$.

Let F be the algebraic closure of a field of prime order p and let $G = \mathrm{SL}_n(F)$. We will need some information about weights of rational finite dimensional FG-modules, which will be called simply G-modules for brevity. All unexplained terminology can be found, for example, in [8]. We can choose the group D of diagonal matrices in G as a maximal torus of G. If M is a G-module, then $\Omega(M)$ is the set of weights of M (relative to D). The irreducible G-module with the highest weight λ is denoted by $M(\lambda)$. If $V = F^n$ is the natural G-module with a canonical basis $e_1, \dots, e_n$, then e_i is a weight vector for each $i \in \{1, \dots, n\}$, and we denote the corresponding weight by ε_i. The Frobenius map on G is the map defined by $(a_{ij}) \mapsto (a_{ij}^p)$. If M is a G-module, then the composition of the corresponding representation and the ith power of the Frobenius map is also a representation of G on M, and we denote the corresponding module by $M^{(p^i)}$.

Lemma 3. *Let $G = \mathrm{SL}_n(F)$ and let M be an irreducible G-module with p-restricted highest weight. Then either $0 \in \Omega(M)$ or there is a uniquely determined number $k \in \{1, \dots, n-1\}$ such that $\Omega(M)$ contains the set*

$$\{\varepsilon_{i_1} + \varepsilon_{i_2} + \dots + \varepsilon_{i_k} \mid 1 \leqslant i_1 < i_2 < \dots < i_k \leqslant n\}.$$

Proof. See Lemmas 13 and 14 in [2]. □

We proceed now to prove Theorem 1. It is convenient to write $\mathrm{PSL}_4^{\pm}(q)$, and related notation such as $\mathrm{SL}_4^{\pm}(q)$, to denote linear and unitary groups with $+$ corresponding to linear groups and $-$ to the unitary groups. So let $L = \mathrm{PSL}_4^{\varepsilon}(q)$, where $\varepsilon \in \{+,-\}$ and $q = p^m$. Observe that by [2, Lemma 11], we may assume that L acts on W faithfully. Let $S = \mathrm{SL}_4^{\varepsilon}(q)$ and let $G = \mathrm{SL}_4(F)$, where F is the algebraic closure of a field of order p, as above. We may regard W as an S-module and by [2, Lemma 10], we may assume that S acts on W absolutely irreducibly. By Steinberg's theorem [9, Theorem 43], we may also assume that W is the restriction to S of an irreducible G-module $M(\lambda)$ for some q-restricted weight λ. By Steinberg's tensor product theorem [9, Theorem 41], we have

$$M(\lambda) \simeq M(\lambda_0) \otimes M(\lambda_1)^{(p)} \otimes \dots \otimes M(\lambda_{m-1})^{(p^{m-1})},$$

where λ_i are p-restricted. By Lemma 3, for each $i \in \{0, 1, \dots, m-1\}$, there is $k_i \in \{0, 1, 2, 3\}$ such that $\Omega(M(\lambda))$ contains all the weights of the form

$$\mu_0 + p\mu_1 + \dots + p^{m-1}\mu_{m-1},$$

where μ_i is the zero weight if $k_i = 0$, and μ_i is a sum of distinct k_i elements of $\{\varepsilon_1, \dots, \varepsilon_4\}$ if $k_i > 0$.

To prove that $\omega(W \rtimes L) \neq \omega(L)$, it is sufficient to find a semisimple element $g \in S$ such that $\langle g \rangle \cap Z(S) = 1$, $p|g| \notin \omega(L)$ and for each $i \in \{0, 1, \dots, m-1\}$ with $k_i > 0$, there are k_i distinct characteristic values $\theta_{i,1}, \dots, \theta_{i,k_i}$ of g such that

$$\prod_{i:\, k_i > 0} (\theta_{i,1} \dots \theta_{i,k_i})^{p^i} = 1. \tag{1}$$

Indeed, there is $x \in G$ such that $h = g^x$ is a diagonal matrix. By (1) and the preceding paragraph, there is $\mu \in \Omega(M(\lambda))$ such that $\mu(h) = 1$. It follows that h has a nontrivial fixed point in W, and so too does g. Hence $p|g| \in \omega(W \rtimes L) \setminus \omega(L)$.

By [3, Lemma 4], if $|g|$ is one of the following numbers, then $p|g| \notin \omega(L)$:

(1) $r_4(\varepsilon q)$, $r_3(\varepsilon q)$, $(q^2-1)_2$;
(2) $r_2(\varepsilon q)(q - \varepsilon 1)_2$ if $3 < q \equiv \varepsilon 1 \pmod 4$.

Observe that all the above primitive divisors exist by Lemma 2. Also observe that S has a semisimple element with characteristic values $\theta_1, \theta_2, \theta_3, \theta_4 \in F$ if and only if $\theta_1\theta_2\theta_3\theta_4 = 1$ and for every $i \in \{1, 2, 3, 4\}$, there is $j \in \{1, 2, 3, 4\}$ such that $\theta_i^{\varepsilon q} = \theta_j$ (see [10, 2.6 (A)] for unitary groups).

Let $\theta \in F^{\times}$ have order $r_4(\varepsilon q)$ and let $g \in S$ be an element whose characteristic values are θ, $\theta^{\varepsilon q}$, θ^{q^2}, $\theta^{\varepsilon q^3}$. It is clear that $\theta^{q^2+1} = 1$, $|g| = r_4(\varepsilon q)$, and $\langle g \rangle \cap Z(S) = 1$. If $k_i \in \{0, 2\}$ for all i and $\theta_{i,1} = \theta$, $\theta_{i,2} = \theta^{q^2}$ for i with $k_i = 2$, then (1) holds.

Let $\theta \in F^\times$ have order $r_3(\varepsilon q)$ and let $g \in S$ be an element whose characteristic values are θ, $\theta^{\varepsilon q}$, θ^{q^2}, 1. If $k_i \neq 2$ for any i then taking $\theta_{i,1} = 1$ for i with $k_i = 1$ and $\theta_{i,1} = \theta$, $\theta_{i,2} = \theta^{\varepsilon q}$, $\theta_{i,3} = \theta^{q^2}$ for i with $k_i = 3$ gives us the desired result.

Thus we may assume that both 2 and 1, or both 2 and 3, occur among the numbers k_i. In particular, $q > p$.

Let $q \equiv -\varepsilon \pmod 4$ and choose $\theta \in F^\times$ of order $(q^2-1)_2$. Observe that $\theta^{q+\varepsilon} = -1$ since $(q^2-1)_2 = 2(q+\varepsilon)_2$. Let $g \in S$ be an element whose characteristic values are θ, $\theta^{\varepsilon q}$, -1, 1. For all i with $k_i > 0$, we set $\theta_{i,1} = 1$. If $k_i = 2$, then $\theta_{i,2} = -1$, and if $k_i = 3$, then $\theta_{i,2} = \theta$, $\theta_{i,3} = \theta^{\varepsilon q}$. Then the left side of (1) is equal to 1 or -1. If it is equal to -1, then we replace $\theta_{i,1} = 1$ by $\theta_{i,1} = -1$ for some i with $k_i \in \{1, 3\}$.

Let $q \equiv \varepsilon \pmod 4$ and let $\theta \in F^\times$ have order $t = r(q-\varepsilon)_2$, where $r = r_2(\varepsilon q)$. Take $g \in S$ to be an element whose characteristic values are θ^a, $\theta^{\varepsilon a q}$, θ^{rb}, $\theta^{-a(1+\varepsilon q)-rb}$, where a and b are integers and a is coprime to r. Since $\theta^{t/2} = -1$, the characteristic values of $g^{t/2}$ are $(-1)^a$, $(-1)^a$, $(-1)^b$, $(-1)^b$. So if a and b have opposite parity, then $|g| = t$ and $\langle g \rangle \cap Z(S) = 1$.

If $k_i = 2$, then set $\theta_{i,1} = \theta^a$ and $\theta_{i,2} = \theta^{a\varepsilon q}$. If $k_i = 1$, then set $\theta_{i,1} = \theta^{rb}$. If $k_i = 3$, then set $\theta_{i,1} = \theta^a$, $\theta_{i,2} = \theta^{\varepsilon a q}$, and $\theta_{i,3} = \theta^{-a(1+\varepsilon q)-rb}$. Then the corresponding factor in the left side of (1) is equal to $\theta^{a(1+\varepsilon q)p^i}$, θ^{rbp^i}, or θ^{-rbp^i} respectively. It follows that the product in the left side of (1) is equal to θ^c, where

$$c = a(1+\varepsilon q)(p^{i_1} + \cdots + p^{i_j}) + rb(\tau_{j+1}p^{i_{j+1}} + \cdots + \tau_l p^{i_l})$$

for some $\tau_{j+1}, \ldots, \tau_l \in \{+, -\}$. Set $A = (1+\varepsilon q)(p^{i_1} + \cdots + p^{i_j})$ and $B = \tau_{j+1}p^{i_{j+1}} + \cdots + \tau_l p^{i_l}$. Observe that A is a nonzero integer since $j > 0$ and $i_1, \ldots, i_j$ are different positive integers. By similar reasons, B is also nonzero.

It is clear that r divides c, and hence $\theta^c = 1$ if and only if

$$aA + rbB \equiv 0 \pmod{(q-\varepsilon)_2}. \tag{2}$$

If $(A)_2 < (B)_2$, then we set $b = 1$ and take a to be a solution of the congruence

$$aA/(A)_2 \equiv -rB/(A)_2 \pmod{(q-\varepsilon)_2}$$

coprime to r (we can choose such a solution because r does not divide $q - \varepsilon$). Since both $B/(A)_2$ and $(q-\varepsilon)_2$ are even, while $A/(A)_2$ is odd, the number a is even, as required. Similarly, if $(A)_2 > (B)_2$, then we set $a = 1$ and take b to be a solution of the congruence

$$rbB/(B)_2 \equiv -A/(B)_2 \pmod{(q-\varepsilon)_2}.$$

Let $(A)_2 = (B)_2$. Suppose that for some i with $k_i = 2$, we replace $\theta_{i,1} = \theta^a$, $\theta_{i,2} = \theta^{\varepsilon aq}$ by $\theta_{i,1} = \theta^{rb}$, $\theta_{i,2} = \theta^{-a(1+\varepsilon q)-rb}$. Then the corresponding factor in the left side of (1) changes from $\theta^{a(1+\varepsilon q)p^i}$ to $\theta^{-a(1+\varepsilon q)p^i}$, and so A is decreased by $2(1+\varepsilon q)p^i$, while B is unchanged. Observe that $A - 2(1+\varepsilon q)p^i$ is still nonzero and divisible by r. If $(A)_2 \geqslant 2(1+\varepsilon q)_2 = 4$, then $(A - 2(1+\varepsilon q)p^i)_2 \neq (A)_2$ by Lemma 1, and we can proceed as in the case $(A)_2 \neq (B)_2$.

We are left with the case $(A)_2 = (B)_2 = 2$. If for some i with $k_i = 1$, we replace $\theta_{i,1} = \theta^{rb}$ by $\theta_{i,1} = \theta^{-a(1+\varepsilon q)-rb}$, this decreases A and B by $(1+\varepsilon q)p^i$ and $2rp^i$ respectively. Similarly, if there is i with $k_i = 3$, then we can increase A and B by the corresponding amounts replacing $\theta_{i,3} = \theta^{-a(1+\varepsilon q)-rb}$ by $\theta_{i,3} = \theta^{rb}$. By Lemma 1, we have $(A \pm (1+\varepsilon q)p^i)_2 > (A)_2$, and so the previous argument goes through. The proof of the theorem is complete.

It remains to prove the corollary. If L is neither $\mathrm{PSL}_4(q)$, $\mathrm{PSU}_3(q)$, $\mathrm{PSU}_4(q)$, $\mathrm{PSU}_5(2)$, nor ${}^3D_4(2)$, then L is recognizable among covers by [11, Corollary 1.1]. For $\mathrm{PSU}_3(q)$, $\mathrm{PSU}_5(2)$ and ${}^3D_4(2)$, the result is proved in [12], [13, Proposition 2] and [14] respectively. If q is even then $\mathrm{PSL}_4(q)$ and $\mathrm{PSU}_4(q)$ are recognizable by spectrum [15, Theorem 1]. Thus we may assume that $L = \mathrm{PSL}_4(q)$ or $\mathrm{PSU}_4(q)$ with q odd. As we mentioned in Introduction, it suffices to show that $\omega(L) \neq \omega(K \rtimes L)$ for every elementary abelian group $K \neq 1$ with L-action. If p and $|K|$ are coprime, the result follows from [2, Lemma 11] for linear groups and [13, Theorem 1] for unitary groups. If p divides the order of K, we apply Theorem 1.

References

[1] *Unsolved problems in group theory. The Kourovka notebook*, 19th ed., Inst. of Mathematics, SO RAN, Novosibirsk, 2018.

[2] A.V. Zavarnitsine, *Properties of element orders in covers for $L_n(q)$ and $U_n(q)$*, Siberian Math. J., **49**:2 (2008), 246–256. MR2419657

[3] A.V. Zavarnitsine, *Exceptional action of the simple groups $L_4(q)$ in the defining characteristic*, Siberian Electronic Mathematical Reports, **5** (2008), 65–74. MR2586623

[4] M.A. Grechkoseeva, A.V. Vasil'ev, *On the structure of finite groups isospectral to finite simple groups*, J. Group Theory, **18**:5 (2015), 741–759. MR3393413

[5] A.V. Zavarnitsine, *Recognition of the simple groups $L_3(q)$ by element orders*, J. Group Theory, **7**:1 (2004), 81–97. MR2030231

[6] A.S. Bang, *Taltheoretiske Undersøgelser*, Tidsskrift Math., **4** (1886), 70–80, 130–137.

[7] K. Zsigmondy, *Zur Theorie der Potenzreste*, Monatsh. Math. Phys., **3** (1892), 265–284. MR1546236

[8] J.C. Jantzen, *Representations of algebraic groups. 2nd ed.*, vol. 107, Amer. Math. Soc., Providence, RI, 2003. MR2015057

[9] R. Steinberg, *Lectures on Chevalley groups*, Yale University, New Haven, Conn., 1968. MR0466335

[10] G.E. Wall, *On the conjugacy classes in the unitary, symplectic and orthogonal groups*, J. Aust. Math. Soc., **3** (1963), 1–62. MR0150210

[11] M.A. Grechkoseeva, *On element orders in covers of finite simple groups of Lie type*, J. Algebra Appl., **14** (2015), 1550056 [16 pages]. MR3305303

[12] A.V. Zavarnitsine, *Recognition of the simple groups $U_3(q)$ by element orders*, Algebra Logic, **45**:2 (2006), 106–116. MR2260330

[13] M.A. Grechkoseeva, *On element orders in covers of finite simple classical groups*, J. Algebra, **339** (2011), 304–319. MR2811323

[14] V.D. Mazurov, *Unrecognizability by spectrum for a finite simple group ${}^3D_4(2)$*, Algebra Logic, **52**:5 (2013), 400–403. MR3184663

[15] V.D. Mazurov, G.Y. Chen, *Recognizability of the finite simple groups $L_4(2^m)$ and $U_4(2^m)$ by the spectrum*, Algebra Logic, **47**:1 (2008), 49–55. MR2408572

Mariya Alexandrovna Grechkoseeva
Sobolev Institute of Mathematics,
4, Koptyuga ave.,
Novosibirsk, 630090, Russia
E-mail address: grechkoseeva@gmail.com

Saveliy Vyacheslavovich Skresanov
Sobolev Institute of Mathematics,
4, Koptyuga ave.,
Novosibirsk, 630090, Russia.
Novosibirsk State University,
1, Pirogova str.,
Novosibirsk, 630090, Russia
E-mail address: skresan@math.nsc.ru