

СИБИРСКИЕ ЭЛЕКТРОННЫЕ
МАТЕМАТИЧЕСКИЕ ИЗВЕСТИЯ

Siberian Electronic Mathematical Reports

<http://semr.math.nsc.ru>

Том 5, стр. 68–74 (2008)

УДК 512.54

MSC 20C20, 20D06, 20D60

EXCEPTIONAL ACTION OF THE SIMPLE GROUPS $L_4(q)$
IN THE DEFINING CHARACTERISTIC

A. V. ZAVARNITSINE

ABSTRACT. We find a counterexample to Problem 14.60 from the Kourovka notebook by giving an example of a group $\mathrm{PSL}_4(q)$ which is not recognizable among its covers from spectrum. Namely, we show that such a group has a module in the defining characteristic with the property that the element order set of the corresponding semidirect product equals that of the group itself.

1. INTRODUCTION

If a group H is a homomorphic image of a finite group G then we call G a *cover* for H , or say that G *covers* H . The Kourovka notebook includes the following [1, Problem 14.60]:

Problem 1. *Suppose that G is a proper cover for the finite simple group $L = L_n(q)$, $n \geq 3$. Is it true that G contains an element whose order is distinct from the order of every element of L ?*

This problem is related to the recognition of finite groups by spectrum. Recall that the *spectrum* $\omega(H)$ of a finite group H is the set of its elements orders. We say that H is *recognizable (by spectrum) among its covers* if, for every finite group G covering H , the equality of the spectra $\omega(G) = \omega(H)$ implies the isomorphism $G \cong H$. Thus, Problem 1 asks if every simple group $L_n(q)$, $n \geq 3$, is recognizable among its covers.

ZAVARNITSINE, A.V., EXCEPTIONAL ACTION OF THE SIMPLE GROUPS $L_4(q)$ IN THE DEFINING CHARACTERISTIC.

© 2008 ZAVARNITSINE A.V.

Supported by RFBR, grants 05-01-00797, 06-01-39001, and 08-01-00322; SB RAS, grant N29 for junior scientists and Integration Project 2006.1.2.

Received March, 13, 2008, published March, 25, 2008.

If follows from [2] that the question in Problem 1 is answered in the affirmative, unless $n = 4$ and q is an odd nonprime. It turns out that the groups $L_4(q)$ exhibit a certain exceptional behavior when acting in the defining characteristic. Our main result is as follows:

Theorem 1. *The group $L = L_4(13^{24})$ has an absolutely irreducible 96-dimensional module W over a field of characteristic 13 such that $\omega(W \rtimes L) = \omega(L)$. In particular, L is not recognizable by spectrum among its covers.*

Observe that so far there have been only two known examples of nonabelian simple groups that are not recognizable among their covers, viz. $U_3(3)$ and $U_3(7)$. Theorem 1 gives a new example of this kind. We conjecture that there are infinitely many groups $L_4(q)$ which are not recognizable among their covers. We do not know if there is such a group of the form $U_4(q)$.

2. AUXILIARY RESULTS

In what follows, we denote $L_n^+(q) = \text{PSL}_n(q)$ and $L_n^-(q) = \text{PSU}_n(q)$. A similar convention is used for $\text{SL}_n^\varepsilon(q)$, where $\varepsilon \in \{+, -\}$. Given a finite group G , denote by $Z(G)$ the center of G and by $\mu(G)$ the numbers in $\omega(G)$ that are maximal with respect to divisibility. Observe that $\omega(G)$ is uniquely restored from $\mu(G)$.

Lemma 1. *Let q be a power of an odd prime p and let $\varepsilon \in \{+, -\}$. Denote $d = \gcd(4, q - \varepsilon 1)$. Then $\mu(L_4^\varepsilon(q))$ contains the following (and only the following) numbers:*

- (i) $\frac{q^4 - 1}{d(q - \varepsilon 1)}, \frac{q^3 - \varepsilon 1}{d}, \frac{p(q^2 - 1)}{d}, q^2 - 1$;
- (ii) $p(q - \varepsilon 1)$, if and only if $d = 4$;
- (iii) 9 , if and only if $p = 3$.

Proof. The claim can be proved by considering the Jordan canonical form of the matrices in $S = \text{SL}_4^\varepsilon(q)$ and determining the intersection of cyclic subgroups of S with the center $Z(S)$. See also [3]. \square

Let r be a prime, G a finite group, and $g \in G$. We say that g is an element of r -maximal order if $r \mid |g| \notin \omega(G)$. We denote by $\nu_r(G)$ the minimal-by-divisibility r -maximal element orders of G . Clearly, $\nu_r(G) \subseteq \omega(G)$.

Lemma 2. *Suppose that a finite group G acts on a vector space W over a field of characteristic r . Then $\omega(W \rtimes G) = \omega(G)$ if and only if there is no $t \in \nu_r(G)$ such that $W \rtimes G$ contains an element of order rt .*

Proof. If $\omega(W \rtimes G) = \omega(G)$ then $rt \notin \omega(G)$ for any r -maximal order t . Conversely, if $\omega(W \rtimes G) \neq \omega(G)$ then we may choose a minimal-by-divisibility element a of $\omega(W \rtimes G) \setminus \omega(G)$. Then we necessarily have $a = rt$ for some $t \in \omega(G)$. Clearly, t is an r -maximal order and in fact $t \in \nu_r(G)$ by the choice of a . \square

Lemma 2 shows that the element orders in $\nu_r(G)$ are r -critical in the sense that the equality $\omega(W \rtimes G) = \omega(G)$ can be detected by analyzing only the action on W of the elements of G of r -critical orders.

Let $t > 1$ and n be natural numbers and let $\varepsilon \in \{+, -\}$. If there exists a prime that divides $t^n - (\varepsilon 1)^n$ and does not divide $t^i - (\varepsilon 1)^i$ for $1 \leq i < n$, then we denote this prime by $t_{[\varepsilon n]}$ and call it a primitive divisor of $t^n - (\varepsilon 1)^n$. In general, a primitive

divisor need neither exist nor be unique. The following lemma is a generalization of the well-known Zsigmondy's theorem:

Lemma 3. *Let $t, n > 1$ be natural numbers and $\varepsilon \in \{+, -\}$. There exists a primitive divisor $t_{[\varepsilon n]}$ of $t^n - (\varepsilon 1)^n$, except in the following cases:*

- (i) $\varepsilon = +, n = 6, t = 2$;
- (ii) $\varepsilon = +, n = 2$, and $t = 2^l - 1$ for some $l \geq 2$;
- (iii) $\varepsilon = -, n = 3, t = 2$;
- (iv) $\varepsilon = -, n = 2$, and $t = 2^l + 1$ for some $l \geq 0$.

Proof. See [4, Lemma 5]. □

Given a natural number n and a prime r , we denote by n_r the r -part of n , i.e. the largest power of r dividing n , and set $n_{r'} = n/n_r$. Also, we denote by $\pi(n)$ the set of prime divisors of n .

The following lemma describes the p -critical element orders of $L_4^\varepsilon(q)$ in odd characteristic:

Lemma 4. *Let q be a power of an odd prime p . The set $\nu_p(L_4^\varepsilon(q))$ contains the following (and only the following) numbers:*

- (i) $q_{[\varepsilon 4]}, q_{[\varepsilon 3]}, (q^2 - 1)_2$;
- (ii) $q_{[\varepsilon 2]}(q - \varepsilon 1)_2$, if and only if $3 < q \equiv \varepsilon 1 \pmod{4}$;
- (iii) $3(q - \varepsilon 1)_3$, if and only if $q \equiv \varepsilon 1 \pmod{3}$;
- (iv) p , if and only if $p > 3$;
- (v) $3r$, where $r \in \pi(3(q^2 - 1))$, if and only if $p = 3$.

Proof. Denote $L = L_4^\varepsilon(q)$. We will go through the elements a of $\mu(L)$ given in Lemma 1 and determine which divisors t of a belong to $\nu_p(L)$.

Let $a = \frac{q^4 - 1}{d(q - \varepsilon 1)} = a_1 a_2$, where $a_1 = \frac{q^2 + 1}{2}$ and $a_2 = \frac{2(q + \varepsilon 1)}{d}$ are coprime.

Suppose that $t|a$ and $t \in \nu_p(L)$. Then $t = t_1 t_2$ for uniquely determined divisors t_1 and t_2 of a_1 and a_2 . Since $pa_2 \in \omega(L)$, it follows that $t_1 \neq 1$ (otherwise, $pt \in \omega(L)$, a contradiction). Hence, $t_2 = 1$ by the minimality of t . But any nontrivial divisor of a_1 is p -maximal; thus, t is a prime divisor of a_1 , i.e. is of the form $q_{[\varepsilon 4]}$.

Let $a = \frac{q^3 - \varepsilon 1}{d} = a_1 a_2$, where $a_1 = \frac{q^2 + \varepsilon q + 1}{\gcd(3, q - \varepsilon 1)}$ and $a_2 = \frac{\gcd(3, q - \varepsilon 1)(q - \varepsilon 1)}{d}$

are coprime. As above, we have $t = t_1 t_2$. If $t_1 \neq 1$ then the minimal-by-divisibility elements of this form are the prime divisors of a_1 , i.e. $t = q_{[\varepsilon 3]}$. Suppose that $t_1 = 1$. If $q \not\equiv \varepsilon 1 \pmod{3}$ then $a_2 = (q - \varepsilon 1)/d$ and $pa_2 \in \omega(L)$, which implies $pt \in \omega(L)$, a contradiction. Let $q \equiv \varepsilon 1 \pmod{3}$. Then $a_2 = a_{2,1} a_{2,2}$, where $a_{2,1} = 3(q - \varepsilon 1)_3$ and $a_{2,2} = (q - \varepsilon 1)_{3'}/d$ are coprime, and we have the corresponding decomposition $t_2 = t_{2,1} t_{2,2}$ with $t_{2,i}|a_{2,i}$, $i = 1, 2$. If $t_{2,1} < a_{2,1}$ then $t|(q - \varepsilon 1)/d$, but $p(q - \varepsilon 1)/d \in \omega(L)$ which yields a contradiction. Therefore, $t_{2,1} = a_{2,1}$. This number, however, is a p -maximal order and so the minimal-by-divisibility number in this case is $3(q - \varepsilon 1)_3$.

Let $a = q^2 - 1 = a_1 a_2$, where $a_1 = (q^2 - 1)_2$ and $a_2 = (q^2 - 1)_{2'}$ are coprime, and let $t = t_1 t_2$ as above. If $t_1 = a_1$ then this number is p -maximal and hence the minimal number in this case is $(q^2 - 1)_2$. If $t_1 \leq a_1/d$ then $pt \in \omega(L)$, a contradiction. Suppose that $t_1 = a_1/2$ and $d = 4$. Then $t_1 = (q - \varepsilon 1)_2$. We write $a_2 = a_{2,1} a_{2,2}$, where $a_{2,1} = (q - \varepsilon 1)_{2'}$ and $a_{2,2} = (q + \varepsilon 1)_{2'}$ are coprime and, correspondingly, $t_2 = t_{2,1} t_{2,2}$. If $t_{2,2} = 1$ then $pt \in \omega(L)$, a contradiction. Otherwise, the number t is

p -maximal it $t_{2,2}$ equal to any prime divisor of $(q + \varepsilon 1)_{2'}$ (which exist unless $q = 3$ and have the form $q_{[\varepsilon 2]}$).

Finally, let $p|a$. Then, clearly, $p|t$. Since p is a p -maximal number if and only if $p^2 \notin \omega(L)$, i.e. if $p > 3$, we have $p \in \nu_p(L)$ in this case. Let $p = 3$. Then 9 is a maximal order and so $3r \in \nu_p(L)$ for every prime divisor r of $3(q^2 - 1)$. \square

Lemma 5. *Let $q = 13^{24}$. All the possible values of $q_{[+n]}$ for $n = 2, 3, 4$ are as follows:*

- (i) $q_{[+2]} \in \{1009, 407865361, 659481276875569\}$;
- (ii) $q_{[+3]} \in \{19, 37, 73, 271, 937, 4177, 181297, 428041, 1471069, 1609669,$
9818892432332713\};
- (iii) $q_{[+4]} \in \{97, 2657, 88993, 441281, 283763713, 127028743393,$
403791981344275297\}.

Proof. The primitive divisors $q_{[+n]}$ can be obtained by analyzing the prime factorization of $q^n - 1$, see [5]. \square

In the following lemmas, we denote

$$J_n = \begin{pmatrix} 1 & 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 & 1 \\ 0 & 0 & 0 & \dots & 0 & 1 \end{pmatrix},$$

where the right-hand side is the unipotent Jordan block of size n over a field of characteristic p .

Lemma 6. *We have*

- (i) $|J_n| = p^m$, where m is the unique integer such that $p^{m-1} < n \leq p^m$;
- (ii) The minimal polynomial of J_n is $(x - 1)^n$.

Proof. Straightforward. \square

Lemma 7. *Suppose that a cyclic group $C = \langle c \mid c^{p^m} = 1 \rangle$ acts on a vector space W over a field of characteristic p . Then $p^{m+1} \in \omega(W \rtimes C)$ if and only if the Jordan canonical form of c on W contains the block J_{p^m} .*

Proof. It is sufficient to consider element orders in the coset cW of $W \rtimes C$ (see Lemma 9 in [8]). An element $cw \in cW$ has order p^{m+1} if and only if

$$1 \neq (cw)^{p^m} = w(1 + c + \dots + c^{p^m-1}),$$

i. e. the polynomial $f(x) = 1 + x + \dots + x^{p^m-1}$ does not annihilate c . However, in characteristic p , we have

$$f(x) = \frac{x^{p^m} - 1}{x - 1} = \frac{(x - 1)^{p^m}}{x - 1} = (x - 1)^{p^m-1}.$$

From Lemma 6 it follows that $f(c) = 0$ if all Jordan blocks of c have size at most $p^m - 1$ and $f(c) \neq 0$ if there is a Jordan block of c of size p^m . The claim follows. \square

For square matrices A and B , we write $A \simeq B$ if A and B are similar. The symbol $\wedge^2 A$ denotes the exterior square of the matrix A . (We are interested in $\wedge^2 A$ to be defined only up to similarity.)

Lemma 8. *Let the ground field have characteristic $p = 13$. Then we have*

- (i) $J_i \otimes J_j \simeq J_{j-i+1} \oplus J_{j-i+3} \oplus J_{j-i+5} \oplus \dots \oplus J_{j+i-1}$ for $i = 2, \dots, 5$, $j = i, i+1, \dots, 7$;
- (ii) $\wedge^2 J_2 \simeq J_1$, $\wedge^2 J_3 \simeq J_3$, $\wedge^2 J_4 \simeq J_1 \oplus J_5$,
- (iii) $\wedge^2(J_i \oplus J_j) \simeq \wedge^2 J_i \oplus (J_i \otimes J_j) \oplus \wedge^2 J_j$ for all i, j .

Proof. Assertions (i) and (ii) follow by a direct calculation. Assertion (iii) is well known and holds for arbitrary matrices. \square

3. PROOF OF MAIN RESULT

We will denote by \mathbb{F}_q a finite field of $q = p^m$ elements. Let $G = \mathrm{SL}_4(q)$, and let W be an FG -module, where F is a field of characteristic p . Denote by W^{ρ^i} , $i = 0, 1, \dots$, the twisting of W by the i th power of the Frobenius map ρ which corresponds to the automorphism $x \mapsto x^p$ of F . The symbol $\wedge^i W$, $i = 0, 1, \dots$, denotes the i th exterior power of W .

Proposition 1. *Let $q = 13^{24}$ and let V be the natural 4-dimensional module for $\mathrm{SL}_4(q)$ over \mathbb{F}_q . Denote*

$$W = V^{\rho^5} \otimes V^{\rho^{11}} \otimes (\wedge^2 V).$$

Then W , when viewed as an (absolutely irreducible 96-dimensional) module for $L = \mathrm{L}_4(q)$, satisfies $\omega(W \searrow L) = \omega(L)$.

Proof. Firstly, observe that V is the restriction to $S = \mathrm{SL}_4(q)$ of the natural module for the linear algebraic group $\mathrm{SL}_4(F)$, where F is the algebraic closure of \mathbb{F}_q , which is a (rational finite dimensional) irreducible module for this group of highest weight ω_1 . Then W is such a restriction of the irreducible module of highest weight $(p^5 + p^{11})\omega_1 + \omega_2$, where $p = 13$, and so is absolutely irreducible as a module for S by the Steinberg Twisted Tensor Product Theorem [6, Theorem 41].

Secondly, the representation that corresponds to W sends the central elements of S to the identity matrix and so W indeed can be viewed as a module for L .

Assume to the contrary that there is $a \in \omega(W \searrow L) \setminus \omega(L)$. By Lemma 2, $a = 13t$ for some $t \in \nu_{13}(L)$. We will go through all values in $\nu_{13}(L)$ which are given in Lemma 4.

Let $t = q_{[+4]}$. Every element $g \in L$ of order t is the image of such an element of S with characteristic values $\theta, \theta^q, \theta^{q^2}, \theta^{q^3}$, where $\theta \in F^\times$ is of order t . Hence, the characteristic values of g in W have the form

$$\theta^{p^5 q^i} \cdot \theta^{p^{11} q^j} \cdot \theta^{q^k + q^l},$$

where $0 \leq i, j, k, l \leq 3$ and $k \neq l$. Therefore, in order to arrive at a contradiction in this case, we need to show that the congruence

$$13^{5+24i} + 13^{11+24j} + 13^{24k} + 13^{24l} \equiv 0 \pmod{t},$$

is not solvable for the indicated i, j, k, l and the values of t as in Lemma 5(iii). This can be verified directly (or using a computer).

Let $t = q_{[+3]}$ or $t = 3(q-1)_3 = 27$. Then $t|(q^3-1)/3$ and the characteristic values of a preimage in S of $g \in L$ of order t are $\theta, \theta^q, \theta^{q^2}, \theta^{-(1+q+q^2)}$, where $\theta \in F^\times$ is of order t . As above this gives the congruence

$$(1) \quad 13^5 a_i + 13^{11} a_j + a_k + a_l \equiv 0 \pmod{t},$$

where $a_i, a_j, a_k, a_l \in \{1, 13^{24}, 13^{48}, -(1+13^{24}+13^{48})\}$, $a_k \neq a_l$, which can be shown to have no solutions for the values of t given in Lemma 5(ii) or for $t = 3(q-1)_3 = 27$.

Let $t = q_{[+2]}(q-1)_2 = 32q_{[+2]}$ or $t = (q^2-1)_2 = 64$, respectively. Note that $t|(q^2-1)$. Since $Z(S) = 4$ and t is a 2-maximal element order in $\omega(S)$ (which follows by considering the orders of the maximal tori of S , see [7, Theorem 2.1]) any preimage in S of an element $g \in L$ of order t has order t . We consider the possible cyclic subgroups $\langle c \rangle$ of S of order t that intersect trivially with $Z(S)$. For some characteristic value $\theta_1 \in \mathbb{F}_{q^2}$ of the generator c of such a subgroup, we have either $q_{[+2]} \mid |\theta_1|$ or $|\theta_1| = 64$, respectively. Hence, there are two possibilities for the set of characteristic values of c :

- (i) $\{\theta_1, \theta_1^q, \theta_2, \theta_2^q\}$, where $\theta_2 \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ and $(\theta_1\theta_2)^{q+1} = 1$;
- (ii) $\{\theta_1, \theta_1^q, \theta_2, (\theta_1^{q+1}\theta_2)^{-1}\}$, where $\theta_2 \in \mathbb{F}_q$.

We show that case (i) is impossible. Indeed, assume to the contrary that (i) holds. Then $q_{[+2]} \mid |\theta_2|$ or $|\theta_2| = 64$, respectively. However, in the latter case, we have $c^{32} = \text{diag}\{-1, -1, -1, -1\} \in Z(S)$, a contradiction, while in the former case we have either $|\theta_2| = t$ or $|\theta_2| < t$. If $|\theta_2| = t$ then again $c^{t/2} = \text{diag}\{-1, -1, -1, -1\} \in Z(S)$, which is impossible. If $|\theta_2| < t$ then $\theta_2 = \theta_1^{2m}$ for some m and we have

$$1 = (\theta_1\theta_2)^{q+1} = \theta_1^{(2m+1)(q+1)}.$$

This contradicts the fact that the 2-part of $|\theta_1|$ is $32 > 2 = ((2m+1)(q+1))_2$.

Therefore, the characteristic values of c are as in (ii). Note that in this case we must have $|\theta_1| = t$ and there is $0 \leq m < 32$ such that $\theta_2 = \theta_1^{mt/32}$. We determine whether $\langle c \rangle$ intersects $Z(S)$ trivially, i. e. whether $c^{t/2} \neq \text{diag}\{-1, -1, -1, -1\}$. We have $(\theta_1)^{t/2} = -1$ and so $c^{t/2} = \text{diag}\{-1, -1, (-1)^{mt/32}, (-1)^{mt/32}\}$. If $t = 64$ then $(-1)^{mt/32} = 1$ for any m . If $t = 32q_{[+2]}$ then $(-1)^{mt/32} = 1$ exactly when m is even.

Summarizing, as above we have to show that the congruence (1) does not hold, where $a_k \neq a_l$, and a_i, a_j, a_k, a_l are taken from the set $\{1, 13^{24}, 2m, -(1+13^{24}+2m)\}$ with a fixed m satisfying $0 \leq m < 32$ if $t = 64$, and from the set $\{1, 13^{24}, q_{[+2]}m, -(1+13^{24}+q_{[+2]}m)\}$ with a fixed *even* m satisfying $0 \leq m < 32$ if $t = 32q_{[+2]}$ and $q_{[+2]}$ is as given in Lemma 5(i). This can be shown by a direct verification.

Observe that we have shown so far that L contains no semisimple element of p -maximal order that centralizes in W a nonzero vector. We now show the same for unipotent elements.

Suppose, finally, that $t = p = 13$. A preimage of order t in S of an element $g \in L$ of order t has (unipotent) Jordan blocks J_i of size $i \leq 4$ in its action on the natural module V . The action of the field automorphism ρ preserves the Jordan structure, hence the Jordan blocks of g have size at most 7 on $V^{\rho^5} \otimes V^{\rho^{11}}$ and at most 5 on $\wedge^2 V$ by Lemma 8. Thus, the Jordan blocks of g on W have size at most 11 again by Lemma 8(i). However, in order for there to exist an element of order p^2 in $W \rtimes L$, some element of L of order p must have a Jordan block of size $p = 13$ by Lemma 7. This contradiction shows that $W \rtimes L$ does not have elements of order 13^2 and the proof is complete. \square

Theorem 1 is now a direct consequence of Proposition 1.

REFERENCES

- [1] Unsolved problems in group theory, *The Kourovka notebook*, 14th ed., Sobolev Inst. Mat. (Novosibirsk), 1999.
- [2] A.V. Zavarnitsine, *Properties of element orders in covers for $L_n(q)$ and $U_n(q)$* , Sib. Math. J., **49**: 2 (2008), 246–256.
- [3] A.A. Buturlakin, *The spectra of the linear and unitary groups*, Algebra and Logic, **47**: 2 (2008), to appear.
- [4] V.D. Mazurov, A.V. Zavarnitsine, *On element orders in coverings of the simple groups $L_n(q)$ and $U_n(q)$* , Proceedings of the Steklov Institute of Mathematics, Suppl. 1 (2007), 145–154.
- [5] R.P. Brent, P.L. Montgomery, H.J.J. te Riele, *Factorizations of Cunningham numbers with bases 13 to 99: Millennium Edition*, Modelling, Analysis and Simulation, MAS-R0107, ISSN 1386-3703, Amsterdam (2001), viii+20 pp.
- [6] R. Steinberg, *Lectures on Chevalley groups*, Yale University, New Haven, 1968.
- [7] A.A. Buturlakin, M. A. Grechkoseeva, *The cyclic structure of maximal tori of the finite classical groups*, Algebra and Logic, **46**: 2 (2007), 73–89.
- [8] A.V. Zavarnitsine, *Recognition of the simple groups $U_3(q)$ by element orders*, Algebra and Logic, **45**: 2(2006), 106–116.

ANDREI V. ZAVARNITSINE
SOBOLEV INSTITUTE OF MATHEMATICS,
PR. KOPTYUGA, 4,
630090, NOVOSIBIRSK, RUSSIA
E-mail address: `zav@math.nsc.ru`