# RECOGNIZING GROUPS $G_{2}\left(3^{n}\right)$ BY THEIR ELEMENT ORDERS 

## A. V. Vasilyev*

UDC 512.542

Key words: finite group, simple non-Abelian group, recognizability of groups by their element orders.

It is proved that a finite group that is isomorphic to a simple non-Abelian group $G=G_{2}\left(3^{n}\right)$ is, up to isomorphism, recognized by a set $\omega(G)$ of its element orders, that is, $H \simeq G$ if $\omega(H)=$ $\omega(G)$ for some finite group $H$.

For a finite group $G$, we denote by $\omega(G)$ a set of its element orders. If $\omega$ is a subset of the set of natural numbers then $h(\omega)$ denotes the number of pairwise non-isomorphic groups $G$ such that $\omega(G)=w$. We say that $G$ is recognizable by $\omega(G)$, or, briefly, recognizable, if $h(\omega(G))=1$. $G$ is almost recognizable (resp., non-recognizable) if the number $h(\omega(G))$ is finite (resp., infinite).

Since every finite group possessing a non-trivial soluble normal subgroup is non-recognizable (see, e.g., [1, Lemma 1]), each recognizable group is an extension of a direct product $M$ of non-Abelian simple groups by some subgroup of Out $(M)$. Of particular interest is the recognition problem for simple and almost simple groups. (Recall that $G$ is almost simple if $L \leq G \leq \operatorname{Aut}(L)$ for some non-Abelian simple group $L$.) At present, of the many almost simple groups, in particular, of all sporadic groups and of all simple groups whose prime divisors do not exceed 11, we have a knowledge as to their recognizability (for a detailed list, see [1]). Also, recognizable are the following series of simple groups: $L_{2}(q)$ for $q>3, q \neq 9$ (cf. [2-6]), $L_{3}\left(2^{m}\right)$ and $U_{3}\left(2^{m}\right)(c f .[7]), S z(q)={ }^{2} B_{2}(q)(c f .[8]), \operatorname{Re}(q)={ }^{2} G_{2}(q)(c f .[9]),{ }^{2} F_{4}(q)(c f .[10])$, and $A_{n}$, where $n=p, p+1, p+2$ for some prime $p \geqslant 5$ (cf. [11, 12]); non-recognizable are simple groups $S_{4}\left(2^{m}\right)$ (cf. [7]) as well as almost simple groups $P G L_{n}(q)$ for some infinite system of pairs $(n, q)$ (cf. [1]). Note that the recognition problem has not thus far been solved for any simple exceptional Chevalley group (exceptional untwisted group) but $G_{2}(3)$ (cf. [13]). The objective of the present article is to point out an infinite series of simple exceptional Chevalley groups that are recognizable by their element orders. Namely, we prove the following:

THEOREM. For every natural $n, G=G_{2}\left(3^{n}\right)$ is recognizable by the set of its element orders.
Remark. [13], in which $G_{2}(3)$ is proved recognizable, is a fairly recent paper; in the few places in which this group is being spoken of, our proofs are independent and so not omitted.
*Supported by RFFR grant No. 99-01-00550, by RF Ministry of Education (Fundamental Research in Natural Sciences) grant No. E00-1.0.-77, and by a SO RAN grant for Young Scientists under Presidium Decree No. 83 of 10/03/2000.

Translated from Algebra i Logika, Vol. 41, No. 2, pp. 130-142, March-April, 2002. Original article submitted July $31,2000$.

## 1. GROUPS WITH DISCONNECTED PRIME GRAPH AND OTHER PRELIMINARY INFORMATION

Note that the set $\omega(H)$ of a finite group $H$ is closed and is partially ordered under divisibility, and so is uniquely determined by a subset $\mu(H)$ consisting of elements that are maximal under the divisibility relation. The set $\omega(H)$ of $H$ defines the prime graph (Gruenberg-Kegel graph) $G K(H)$ whose vertices are prime divisors of the order of $H$, and two primes $p$ and $q$ are joined by an edge if $H$ contains an element of order $p q$. Denote by $s(H)$ the number of connected components in $G K(H)$, and by $\pi_{i}=\pi_{i}(H)$, $i=1, \ldots, s(H)$, an $i$ th connected component. For a group $H$ of even order, put $2 \in \pi_{1}$. Let $\mu_{i}=\mu_{i}(H)$ be a set of those $n \in \mu(H)$ for which every prime divisor of $n$ belongs to $\pi_{i}$.

The next result, obtained by Gruenberg and Kegel in 1975 and published in [14], will play a crucial part in our further reasoning.

LEMMA 1.1. If a finite group $H$ has a disconnected prime graph $G K(H)$ then one of the following statements holds:
(a) $H=B C$ is a Frobenius group with kernel $B$ and complement $C$;
(b) $H=A B C$, where $A$ and $A B$ are normal subgroups of $H ; A B$ and $B C$ are Frobenius groups with kernels $A$ and $B$ and complements $B$ and $C$, respectively;
(c) $H$ is an extension of a $\pi_{1}(H)$-group $N$ by a group $H_{1}$, where $L \leq H_{1} \leq \operatorname{Aut}(L), L$ is a non-Abelian group with disconnected graph $G K(L)$, with $s(L) \geqslant s(H)$, and $M \simeq H_{1} / L$ is a $\pi_{1}(H)$-group.

Finite simple non-Abelian groups with disconnected prime graph are described by the following:
LEMMA 1.2. Let $L$ be a finite simple group for which $s(L) \geqslant 2$. Then $\left|\mu_{i}(L)\right|=1$ for $2 \leqslant i \leqslant s(L)$. Let $n_{i}(L)$ be a unique element of $\mu_{i}(L)$ for $i \geqslant 2$. Then values for $L, \pi_{1}(L)$, and $n_{i}(L)$ are as in [11, Tables 1-3].

Proof. The groups $L$ and the sets $\pi_{i}(L)$ are described in $[14,15]$; the rest is proved in Lemma 4 of [11]. The latter also contains revised values of the quantities in question, and of the number $n_{i}$ (cf. [11, Tables 1-2]).

Remark. Table 2 in [11] (as well as the corresponding table in [14]) contain an error: for a group $L={ }^{2} G_{2}(q)$ with $q=3^{2 m+1}>3$, the set $\pi_{1}(L)$ is equal to $\pi\left(q\left(q^{2}-1\right)\right)$, not to $\pi\left(q\left(q^{4}-1\right)\right)$, as was pointed out - this can be easily verified by direct computations.

In conclusion of this section, we formulate two versions of the widely known result concerning the faithful action of a Frobenius group.

LEMMA 1.3. If a Frobenius group $F C$ with kernel $F$ and cyclic complement $C=\langle c\rangle$ of order $n$ acts faithfully on a vector space $V$ of non-zero characteristic $p$, which is coprime to the order of the group $F$, then the minimal polynomial of an element $c$ on $V$ is equal to $x^{n}-1$. In particular, the natural semidirect product $V C$ contains an element of order $p \cdot n$, and $\operatorname{dim} C_{V}(c)>0$.

The proof follows the line of Lemma 1 in [16].
LEMMA 1.4. Let $X$ be a finite group, $N \triangleleft X$, and $X / N$ be a Frobenius group with kernel $F$ and cyclic complement $C=\langle c\rangle$ of order $n$. If the preimage of $F$ in $X$ is a Frobenius group, then

$$
n \cdot \prod_{p \in \pi(N)} p \in \omega(X)
$$

The proof follows the line of Lemma 4 in [1].

## 2. PROPERTIES OF THE GROUP $G_{2}(q)$

Under this section, unless specified otherwise, we denote by $G$ the group $G_{2}(q)$, where $q=p^{n}, p$ is an odd prime, and $n \in \mathbf{N}$.

Let $\Phi$ be a root system, $\Phi^{+}$be a positive and $\Pi=\left\{\alpha_{1}, \alpha_{2}\right\}$ a fundamental root systems of an algebra $G_{2}$, where the root $\alpha_{2}$ is longer than $\alpha_{1}$, that is, $\left(\alpha_{2}, \alpha_{2}\right)=3\left(\alpha_{1}, \alpha_{1}\right)$. Denote by $x_{\alpha}(t)$, where $\alpha \in \Phi$ and $t \in \mathbf{F}_{q}$, a root element of $G$, and by $X_{\alpha}$ the corresponding root subgroup. As is known, a simple exceptional Chevalley group $G=G_{2}(q)$ is generated by its root elements. (For details, see [17, 18].) Following them, we denote by $H=\left\langle h_{a_{i}}(u) \mid i=1,2, u \in \mathbf{F}_{q}^{*}\right\rangle$ a Cartan subgroup of $G$, and by $U=\left\langle X_{\alpha} \mid \alpha \in \Phi^{+}\right\rangle$a maximal unipotent subgroup corresponding to $\Phi^{+}$, which is a Sylow $p$-subgroup of $G$. Recall that $p$-elements of $G$ are said to be unipotent and $p^{\prime}$-elements are said to be semisimple.

Up to conjugation, $G$ contains two maximal parabolic subgroups. Following [19], where such groups are described in detail, we denote these groups by $P_{1}$ and $P_{2}$. Of interest to us is the group $P_{1}$. This admits the Levi decomposition (cf. [18, Thm. 8.5.2]): $P_{1}=U_{1}: L_{1}$, where $U_{1}=\left\langle X_{\alpha} \mid \alpha \in \Phi^{+} \backslash\left\{\alpha_{2}\right\}\right\rangle$ is a unipotent subgroup of order $q^{5}$ and $L_{1}=\left\langle H, X_{\alpha_{2}}, X_{-\alpha_{2}}\right\rangle$ is a subgroup of order $q\left(q^{2}-1\right)(q-1)$; moreover, $U_{1} \cap L_{1}=1$ and $P_{1}=N_{G}\left(U_{1}\right)$ is the normalizer of $U_{1}$ in $G$.

LEMMA 2.1. $G$ contains a Frobenius subgroup $F C$ whose kernel $F$ is an elementary Abelian $p$-group of order $q^{2}$ and whose complement $C=\langle c\rangle$ is a cyclic group of order $q^{2}-1$.

Proof. Denote by $F$ a subgroup of $U_{1}$ generated by root subgroups $X_{3 \alpha_{1}+\alpha_{2}}$ and $X_{3 \alpha_{1}+2 \alpha_{2}}$. The subgroup is of order $q^{2}$, and it is an elementary Abelian $p$-group since elements $x_{3 \alpha_{1}+\alpha_{2}}(t)$ and $x_{3 \alpha_{1}+2 \alpha_{2}}(u)$ commute, in view of the Chevalley commutator formula, for any $t, u \in \mathbf{F}_{q}$ (cf. [18, Thm. 5.2.2]).

A Cartan subgroup $H$ normalizes every root subgroup. Furthermore, using the Chevalley commutator formula, it is not hard to verify that $X_{\alpha}^{g} \subseteq F$, where $\alpha=3 \alpha_{1}+\alpha_{2}$ or $3 \alpha_{1}+2 \alpha_{2}$, and $g$ runs through the set of elements like $x_{ \pm \alpha_{2}}(t), t \in \mathbf{F}_{q}$. Therefore the subgroup $L_{1}$ normalizes $F$.

Let $u \in \mathbf{F}_{q}^{*}, u^{2}=1$. An element $z=h_{\alpha_{2}}(u)$, lying in the center of the group $L_{1}$, acts on $F$ regularly. In fact, direct computations show that $z$ inverts all non-trivial elements of $F$. Consequently, $L_{1}$ acts on $F$ faithfully. Therefore if we treat $F$ as a two-dimensional vector space $V$ over a field of order $q$ we obtain a natural embedding of $L_{1}$ in $G L(V)$, a group of non-singular linear transformations of $V$. On the other hand, $|G L(V)|=q\left(q^{2}-1\right)(q-1)=\left|L_{1}\right|$, and so $L_{1} \simeq G L_{2}(q)$.

The vector space $V$ can be identified with an additive group of a field of order $q^{2}$. Then the operator of right multiplication by a primitive element of that field induces a non-singular linear transformation $\varphi$ of a space $V$ of order $q^{2}-1$, which is obviously regular on $V$. Hence its image $c$ in $L_{1}$ shares the same properties. Thus the subgroup $F C$, where $C=\langle c\rangle$, is the desired Frobenius group. The lemma is proved.

We recall that a maximal torus in a finite Chevalley group is a maximal Abelian $p^{\prime}$-subgroup (the converse is not always true).

LEMMA 2.2. $G$ contains two subgroups $N_{\varepsilon}$, where $\varepsilon= \pm 1$, of respective orders $\left(q^{2}-\varepsilon q+1\right) \cdot 6$. If $q \equiv \varepsilon(\bmod 3)$, then one of these subgroups is a Frobenius group with cyclic kernel of order $q^{2}-\varepsilon q+1$ and cyclic complement of order 6 . If $q=3^{n}$ then both of these subgroups are Frobenius groups.

Proof. The classification of maximal tori for Chevalley groups in [20, Parts E, G] implies that $G$ contains two maximal cyclic tori $T_{\varepsilon}$ of respective orders $q^{2}-\varepsilon q+1$, where $\varepsilon= \pm 1$. By [14, Lemma 5], for every maximal torus $T$ of $G$, the set $\pi(T)$ forms a connected component of $G K(G)$ iff $\left(|T|,\left|C_{G}(i)\right|\right)=1$ for any involution $i \in G$. Note that the description of connected components of the prime graph of simple Lie-type groups is underpinned by just this idea (cf. Lemma 1.2 above). The results of [20, Part F] imply
that all involutions in $G$ are conjugate, and that the centralizer $C_{G}(i)$ of each is of order $q^{2}\left(q^{2}-1\right)^{2}$. It is easy to verify that $\left(\left|T_{\varepsilon}\right|,\left|C_{G}(i)\right|\right)=3$ for $q \equiv \varepsilon(\bmod 3)$ and is equal to 1 in all other cases. Consequently, if $q \not \equiv \varepsilon(\bmod 3)$ then $\pi\left(T_{\varepsilon}\right)$ is a connected component in $G K(G)$. Therefore the normalizer $N_{\varepsilon}=N_{G}\left(T_{\varepsilon}\right)$ of a subgroup $T_{\varepsilon}$ in $G$ is a Frobenius group. It remains to observe that the factor group $N_{\varepsilon} / T_{\varepsilon}$ is isomorphic to a cyclic group of order 6 (cf. [20, Part E, Ch. 2, Sec. 5]). The lemma is proved.

In the next lemma we point out some properties of the set $\mu(G)$, whose proof is based on examining the structure of $G$ and on several arithmetic arguments.

LEMMA 2.3. For $G$, the following statements hold:
(a) $p^{2} \in \mu(G)$;
(b) $\left(q^{2}-1\right) \in \mu(G)$;
(c) if a 2-period of $G$ is equal to $2^{t}$, that is, $t \in \mathbf{N}$ is such that $2^{t} \in \omega(G)$ and $2^{t+1} \notin \omega(G)$, then $p \cdot 2^{t} \notin \omega(G)$;
(d) 2-periods of $G$ and $G_{2}\left(q^{p}\right)$ coincide;
(e) if $q=3^{n}$ then $s(G)=3, \pi_{1}(G)=\pi\left(q\left(q^{2}-1\right)\right), n_{2}=q^{2}-q+1$, and $n_{3}=q^{2}+q+1$; but if $q \equiv \varepsilon(\bmod 3)$ then $s(G)=2, \pi_{1}(G)=\pi\left(q\left(q^{2}-1\right)\left(q^{3}-\varepsilon\right)\right)$, and $n_{2}=q^{2}-\varepsilon q+1$;
(f) if $q=3^{n}$, where $n$ is an odd natural number, then $5 \notin \omega(G)$.

Proof. Using the Chevalley commutator formula, it is not hard to determine how a Sylow $p$-subgroup $U$ of $G$ is structured. In particular, the $p$-period of $U$ is equal to $p^{2}$ (which is false for $p=2$ ). On the other hand, it is well known that a subgroup $O^{p^{\prime}}(C)$ of the centralizer $C=C_{G}(g)$ of any semisimple element $g$ in $G$ is structured as follows: $O^{p^{\prime}}(C)=L T$, where $L$ is a central product of Chevalley groups $L_{i}\left(q^{k}\right), i=1,2$, $k=1,2$, whose root systems are subsystems of the root system of $G$, defined over some extension $\mathbf{F}_{q^{k}}$ of the field $\mathbf{F}_{q}$, and $T$ is a torus in $G$. It is not hard to verify that $p^{2} \notin \omega\left(X\left(q^{k}\right)\right)$ for every Chevalley group $X\left(q^{k}\right)$ the root system of which is a subsystem in $\Phi(G)$. Therefore $p^{2} \cdot|g| \notin \omega(G)$.
(b) A cyclic subgroup $T$ of $G$ of order $q^{2}-1$ is a maximal torus. Therefore $r\left(q^{2}-1\right) \notin \omega(G)$ for every prime $r \neq p$. Moreover, if $G$ has an element $x$ of order $p\left(q^{2}-1\right)$ then $x$ lies in the centralizer $C$ of an involution $i \in T$. Analysis of the structure of $C$ (cf. [20, Part F, Sec. 9]) indicates that $p\left(q^{2}-1\right) \notin \omega(C)$.
(c) Let $x$ be a 2-element of maximal order in $G$. Then $x$ lies in the maximal torus $T$ of order $q^{2}-1$, and the result now follows by applying essentially the same argument as in (b).
(d) Elements $x \in G$ and $x^{\prime} \in G^{\prime}=G_{2}\left(q^{p}\right)$ whose orders are 2-periods of the groups $G$ and $G^{\prime}$, respectively, lie in the maximal tori $T \leq G$ and $T^{\prime} \leq G^{\prime}$, which are cyclic subgroups of orders $q^{2}-1$ and $q^{2 p}-1$, respectively. On the other hand, $q^{2 p}-1=\left(q^{2}-1\right)\left(q^{2(p-1)}+\ldots+q^{2}+1\right)$. Since $p$ and $q$ are odd numbers, 2 does not divide $q^{2(p-1)}+\ldots+q^{2}+1$, as desired.
(e) Follows from [11, Lemma 1.2, Tables 1 and 2].
(f) Is verified by direct computations.

## 3. PROOF OF THE MAIN RESULT

We fix some natural $n$ and denote by $G$ the group $G_{2}(q)$, where $q=3^{n}$. Assume that $G$ defies statement of the theorem and that a finite group $H$ is a counterexample. Then $H \not 千 G, \omega(H)=\omega(G)$, and $\mu(H)=$ $\mu(G)$; hence, by Lemma 2.3(e), $s(H)=s(G)=3, \pi_{1}(H)=\pi_{1}(G)=\pi\left(q\left(q^{2}-1\right)\right), n_{2}(H)=n_{2}(G)=q^{2}-q+1$, and $n_{3}(H)=n_{3}(G)=q^{2}+q+1$.

Since $s(H)=3, H$ admits three possibilities, in compliance with items (a)-(c) in Lemma 1.1.
First let $H=B C$ be a Frobenius group. By the Thompson theorem in [21], the kernel $B$ of this group is a nilpotent subgroup. By $[6$, Lemma 3], $H$ is insoluble as is any other group the number of connected
components in the prime graph of which is strictly more than 2 . Consequently, the complement $C$ is an insoluble group. This implies, in particular, that $s(C)=1$ (cf. [6, proof of Lemma 4]). Therefore $s(H)=2$, a contradiction. The case where $H$ is a Frobenius 2-group, that is, $H$ satisfies the conditions of Lemma 1.1(b), can be treated similarly.

Thus we may assume that $H=N \cdot H_{1}$, where $L \leq H_{1} \leq$ Aut $(L)$ for some non-Abelian simple group $L$ such that $s(L) \geqslant 3$, and $N$ and $H_{1} / L$ are $\pi_{1}(G)$-groups.

We claim that $L \simeq G$. By Lemma 1.2, $L$ is one of the groups in [11, Tables 2 and 3]. Analysis of different possibilities for $L$ proceeds along similar lines; so, we only handle some exemplifying cases.

Assume that $L$ does not belong to any infinite series, for instance, $L \simeq M_{22}$. Table 3 in [11] indicates that $s(L)=4, n_{2}(L)=5, n_{3}(L)=7$, and $n_{3}(L)=11$. Since the connected components of the graph $G K(H)$, distinct from $\pi_{1}$, can only be obtained from similar components of $G K(L)$, we have $n_{2}=n_{2}(H)=n_{i}(L)$ and $n_{3}=n_{3}(H)=n_{j}(L)$ for some $i, j \in\{2,3,4\}$ such that $n_{i}<n_{j}$. On the other hand, $n_{2}=n_{2}(G)=q^{2}-q+1$ and $n_{3}=n_{3}(G)=q^{2}+q+1$. Therefore $n_{3}-n_{2}=2 \cdot 3^{n}=2 q$ is equal to one of the numbers $n_{j}(L)-n_{i}(L)$, that is, to 2,4 , or 6 . In the first and second cases, contradiction is obvious. For the last case $q=3$, and by Lemma 2.3(f), $5 \notin \omega(G)$. But $5 \in \omega(L) \subseteq \omega(H)$. Contradiction.

Let $L \simeq F_{1}$. Then $s(L)=4$ and $n_{j}-n_{i}$ cannot be equal to 12,18 , or 30 . The only acceptable possibility is the case where $j=3, i=2$, and $n_{j}-n_{i}=18$. Here, we have $q=9$. It follows that $n_{2}=9^{2}-9+1=73$, but $n_{2}=n_{2}(L)=41$, and we arrive at a contradiction again.

The cases treated above contain enough arguments (comparison of $n_{3}-n_{2}=2 q$ and $n_{j}(L)-n_{i}(L)$, expressing $q$ in terms of these values, and application of Lemma 2.3(f)), in order to sort out all other possibilities for $L$ not in infinite series. Moreover, such arguments are sufficient to deny all the infinite series but $A_{1}\left(q^{\prime}\right)=L_{2}\left(q^{\prime}\right)$, where $q^{\prime} \equiv \pm 1(\bmod 4)$, in Tables 2 and 3 of [11]. We handle the latter case.

Let $L \simeq L_{2}\left(q^{\prime}\right)$, where first $q^{\prime} \equiv 1(\bmod 4), q^{\prime}=p^{\prime m}$, and $p^{\prime}$ is a prime. We have $s(L)=3, n_{2}(L)=p^{\prime}$, and $n_{3}(L)=\left(q^{\prime}+1\right) / 2$.

If $q^{\prime}=p^{\prime}$ then $p^{\prime}=n_{2}(L)=n_{3}=q^{2}+q+1$ and $\left(p^{\prime}+1\right) / 2=n_{3}(L)=n_{2}=q^{2}-q+1$. It follows that $2 q=n_{3}-n_{2}=\left(p^{\prime}-1\right) / 2$. Expressing $p^{\prime}$ from the latter equality and substituting it in the former, we obtain $4 q+1=p^{\prime}=q^{2}+q+1$. Hence $q=3$ and $q^{\prime}=13$. Let $L=L_{2}(13)$. This group is described in [22], and so its properties which are made use of in what follows are easily verifiable. The group Aut ( $L$ ) has no elements of order 9. Hence $H_{1}$ also has none. On the other hand, $9 \in \omega(G)$, and so $3 \in \omega(N)$. Denote by $H_{0}$ the preimage of $L$ in $H$. It follows that $N \unlhd H_{0}$ and $C_{H_{0}}(N) \subseteq N$. The group $L$ contains a subgroup $K$, which is a Frobenius group with cyclic kernel $F$ of order 13 and cyclic complement $R$ of order 6. Again, $13=n_{2}(L)=n_{2}(H)$, and hence the preimage of $F$ in $H_{0}$ is a Frobenius group with kernel $N$ and complement $F$. Thus the preimage $X$ of $K$ in $H_{0}$ satisfies all the conditions of Lemma 1.4. Therefore $18=3 \cdot 6 \in \omega(X) \subseteq \omega\left(H_{0}\right) \subseteq \omega(H)=\omega(G)$. By Lemma 2.3(a), $9 \in \mu(G)$, a contradiction.

Let $q^{\prime}=p^{\prime m}, m>1$. Then $p^{\prime}=n_{2}(L)=n_{2}=q^{2}-q+1$ and $\left(q^{\prime}+1\right) / 2=n_{3}(L)=n_{3}=q^{2}+q+1$. This means that $\left(n_{2}^{m}+1\right) / 2=n_{2}+2 q$. Hence $n_{2}^{m}-2 n_{2}+1=4 q$. We have $n_{2}^{m}-2 n_{2}+1 \geqslant n_{2}^{2}-2 n_{2}+1=$ $\left(n_{2}-1\right)^{2}=\left(q^{2}-q\right)^{2}=q^{2}(q-1)^{2}$, which is of course greater than $4 q$ since $q \geqslant 3$.

Let $L \simeq L_{2}\left(q^{\prime}\right)$ and $q^{\prime} \equiv-1(\bmod 4)$. If $q^{\prime}=p^{\prime}$ is a prime then two distinct expressions of $p^{\prime}$ via $q$ yield a quadratic equation for $q$, whose solutions are 1 and 2 . If $q^{\prime}=p^{\prime m}, m>1$, then a chain of inequalities like in the preceding case leads us to a contradiction again.

Thus we may assume that $L \simeq G$. We claim that the subgroup $N$ of $H$ is trivial. This fact follows from the following:

Proposition 3.1. Let $N$ be a non-trivial normal subgroup of a finite group $X$ and $L=X / N$ be a factor group isomorphic to $G$. Then $\omega(X) \nsubseteq \omega(G)$.

Proof. Assume that the theorem fails, letting $X$ be a counterexample of minimal order. Then every Sylow subgroup $S$ of $N$ is normal in $X$. Assume, to the contrary, that $Y=N_{X}(S)$ is the normalizer of $S$ in $X$, and $Y \neq X$. By the Frattini lemma, $G \simeq X / N=Y N / N \simeq Y /(Y \cap N)$. Since $X$ is a minimal counterexample, the group $Y$ meets the conclusion of the theorem. On the other hand, $\varnothing \neq \omega(Y) \backslash \omega(G) \subseteq$ $\omega(X) \backslash \omega(G)=\varnothing$. Contradiction.

Now we claim that $N$ is an $r$-group for some prime $r$. Indeed, let $S$ be a proper Sylow subgroup of $N$. Then we arrive at a contradiction by applying the theorem to the group $X / S$ and its normal divisor $N / S$. Likewise we can prove that $N$ is an elementary Abelian $r$-group. Since $s(G)>1, L$ acts on $N$ faithfully. Consequently, if we identify $N$ with a vector space $V$ over a field $\mathbf{F}_{r}$, then $L$ and hence $G$ can be thought of as subgroups of $G L(V)$.

First let $r=3$. By Lemma 2.2, $G$ contains a Frobenius group with kernel of order $q^{2}-q+1$ coprime to 3 and cyclic complement of order 6 ; so, by Lemma 1.3, the natural semidirect product $X_{1}=N G$ contains an element of order 18. By [23. Lemma 10], $\omega\left(X_{1}\right) \subseteq \omega(X)$. Hence $X$ also has an element of order 18, which contradicts Lemma 2.3(a).

Next let $r \neq 3$. Apply then Lemma 1.3 to a Frobenius group with kernel of order $q^{2}$ and cyclic complement of order $q^{2}-1$ (such a group exists in view of Lemma 2.1). Then $X_{1}$ and hence $X$ will contain an element of order $r \cdot\left(q^{2}-1\right)$, which contradicts Lemma 2.3(b). The proposition is proved.

The group $H_{0}$, which is the preimage of $L$ in $H$, satisfies the conditions of the proposition. Thus $N=1$. Consequently, $H=H_{1}$ and $L \leq H \leq$ Aut $(L)$. Denote the factor $H / L$ by $M$. Obviously, $M \leq$ Out $(L)$. Therefore every element of $M$ is a product of some field automorphism $f$ and graph automorphism $g$. We claim that $f$ and $g$ are trivial.

Let $f \neq 1$ and $r$ be a prime dividing the order of $f$. There is no loss of generality in assuming that $|f|=r$. Denote by $\tau$ an automorphism of the field $\mathbf{F}_{q}$ inducing $f$. If $q=3^{n}$ then $r$ divides $n$, and we put $q^{\prime}=q^{n / r}$. Since $\tau$ fixes a subfield $\mathbf{F}_{q^{\prime}}$ of $\mathbf{F}_{q}, f$ centralizes a subgroup $L^{\prime}$ of $L$ isomorphic to $G_{2}\left(q^{\prime}\right)$. Hence $r \cdot k \in \omega(H)$ for every number $k \in \omega\left(L^{\prime}\right)$ such that $(r, k)=1$. Let $r \neq 3$. By Lemma 2.3(a), $9 \in \omega\left(L^{\prime}\right)$. But $9 r \in \omega(H)=\omega(G)$, which is a contradiction with Lemma 2.3(a). Let $r=3$. In view of Lemma 2.3(d), the 2-periods of $L^{\prime}$ and $L$ coincide and are equal to $2^{t}$, say. It follows that $3 \cdot 2^{t} \in \omega(H)$, which is a contradiction with Lemma 2.3(c). Thus $f=1$.

Let $g \neq 1$. Then, as is known, the order of $\mathbf{F}_{q}$ is an odd power of 3 , and $|g|=2$. The centralizer $C$ of $g$ in $L$ is isomorphic to a Ree group $\operatorname{Re}(q)={ }^{2} G_{2}(q)$. On the other hand, $\operatorname{Re}(q)$ contains an element of order $q^{2}-q+1$. Therefore $2\left(q^{2}-q+1\right) \in \omega(H)=\omega(G)$, which clashes with Lemma 2.3(e). The theorem is proved.

## REFERENCES

1. V. D. Mazurov, "The set of orders of elements in a finite group," Algebra Logika, 33, No. 1, 81-89 (1994).
2. W. J. Shi, "A characteristic property of $A_{5}$," J. Southwest-China Teach. Univ., Ser. B., No. 3, 11-14 (1986).
3. W. J. Shi, "A characteristic property of $P S L_{2}(7)$," J. Austr. Math. Soc., Ser. A, 36, No. 3, 354-356 (1984).
4. W. J. Shi, "A characterization of some projective special linear groups," J. Southwest-China Teach. Univ., Ser. B., No. 2, 2-10 (1985).
5. W. J. Shi, "A characteristic property of $J_{1}$ and $P S L_{2}\left(2^{n}\right)$," Adv. Math. Beijing, 16, No. 4, 397-401 (1987).
6. R. Brandl and W. J. Shi, "The characterization of $P S L(2, q)$ by its element orders," J. Alg., 163, No. 1, 109-114 (1994).
7. V. D. Mazurov, M. C. Xu, and H. P. Cao, "Recognition of finite simple groups $L_{3}\left(2^{m}\right)$ and $U_{3}\left(2^{m}\right)$ by their element orders," Algebra Logika, 39, No. 5, 567-585 (2000).
8. W. J. Shi, "A characterization of Suzuki simple groups," Proc. Am. Math. Soc., 114, No. 3, 589-591 (1992).
9. R. Brandl and W. J. Shi, "A characterization of finite simple groups with Abelian Sylow 2-subgroups," Ric. Mat., 42, No. 1, 193-198 (1993).
10. H. W. Deng and W. J. Shi, "The characterization of Ree groups ${ }^{2} F_{4}(q)$ by their element orders," J. Alg., 217, No. 1, 180-187 (1999).
11. A. S. Kondratiev and V. D. Mazurov, "Recognition of alternating groups of prime degree from their element orders," Sib. Mat. Zh., 41, No. 2, 360-371 (2000).
12. A. V. Zavarnitsin, "Recognition by the element order set of alternating groups of degree $r+1$ and $r+2$ for prime $r, "$ Preprint No. 47, Institute of Discrete Mathematics and Informatics, Novosibirsk (2000).
13. S. Lipschutz and W. J. Shi, "Finite groups whose element orders do not exceed twenty," Progr. Nat. Sc., 10, No. 1, 11-21 (2000).
14. J. S. Williams, "Prime graph components of finite groups," J. Alg., 69, No. 2, 487-513 (1981).
15. A. S. Kondratiev, "On prime graph components for finite simple groups," Mat. Sb., 180, No. 6, 787-797 (1989).
16. V. D. Mazurov, "Recognition of finite groups by a set of orders of their elements," Algebra Logika, 37, No. 6, 651-666 (1998).
17. R. Steinberg, Lectures on Chevalley Groups, Yale University (1967).
18. R. W. Carter, Simple Groups of Lie Type, Pure Appl. Math., 28, Wiley, London (1972).
19. A. V. Vasilyev, "Minimal permutation representations of finite simple exceptional groups of types $G_{2}$ and $F_{4}$," Algebra Logika, 35, No. 6, 663-684 (1996).
20. Seminar on Algebraic Groups and Related Finite Groups, Springer, Berlin (1970).
21. J. G. Thompson, "Normal p-complements for finite groups," Math. Z., 72, No. 2, 332-354 (1960).
22. J. Conway, R. Curtis, S. Norton, et al., Atlas of Finite Groups, Clarendon, Oxford (1985).
23. A. V. Zavarnitsin and V. D. Mazurov, "Element orders in coverings of the symmetric and alternating groups," Algebra Logika, 38, No. 3, 296-315 (1999).
