UDC 512.542

Recognizability of groups $G_2(q)$ by spectrum[1]

Vasil'ev A.V., Staroletov A.M.

Let G be a finite group, $\pi(G)$ be the set of prime divisors of the order of G, $\omega(G)$ be the *spectrum* of group G, that is the set of its element orders. The *prime graph* (*Gruenberg — Kegel graph*) of G is defined as follows: its vertices are elements of $\pi(G)$, and two distinct vertices r and s are adjacent if and only if $rs \in \omega(G)$. It is clear that $GK(G)$ is uniquely determined by spectrum $\omega(G)$, and the spectrum in turn is restored by the set $\mu(G)$ of maximal with respect to divisibility elements of $\omega(G)$.

We call groups G and H *isospectral* if $\omega(G) = \omega(H)$. Let $h(G)$ be the number of pairwise nonisomorphic groups isospectral to G. Group G is called *recognizable* (by spectrum) if $h(G) = 1$, *almost recognizable* if $h(G) < \infty$, and *non-recognizable* if $h(G) = \infty$. Since every finite group containing nontrivial normal solube subgroup is non-recognizable [1, Lemma 1], a recognizability of nonabelain simple groups is of prime interest. It turns out that many of these groups are recognized or almost recognized by spectrum. The surveys of results in this area may be found in [1, 2]. Observe that best achievements were obtained here in case when the prime graph of L is disconnect.

The goal of the present paper is to investigate the recognizability of groups $G_2(q)$. It was proved earlier that groups $G_2(3^n)$ are recongizable for every n [3]. Recognizability of the group $G_2(4)$ was set in [4]. It is showed in [5] that the group $G_2(7)$ is restored up to isomorpishm by its prime graph in the class of finite groups, in particular, it is recongizable by spectrum. In this paper we prove recognizablity of $G_2(q)$ in the remain cases.

Theorem. *Let $L = G_2(q)$ be a finite simple group over the field of order $q > 2$ and G be a finite group with $\omega(G) = \omega(L)$. Then groups L and G are isomorphic.*

Note that for $q = 2$ the group $G_2(q)$ is not simple. Its commutant $G_2(2)'$ is isomorphic to the simple unitary group ${}^2A_2(3)$ for which $h({}^2A_2(3)) = \infty$ [6].

[1]The authors were supported by the Russian Foundation for Basic Research(Grants 11-01-91158, 12-01-90006 — the first author, 12-01-31221 — the second author) and the Target program of SB RAS for 2012-2014 (integration project No. 14)

§ 1. Preliminaries

For nonzero integers $n_1, n_2, \ldots, n_k$ denote by $(n_1, n_2, \ldots, n_k)$ their greatest common divisor, by $n_1 \mid n_2$ denote the fact that n_1 divides n_2, and denote by $n_k \vdots n_{k-1} \ldots n_2 \vdots n_1$ the chain of divisibilities $n_1 \mid n_2$, $n_2 \mid n_3$, …, $n_{k-1} \mid n_k$. For nonzero integer n and prime r by n_r we denote r-part of n, i.e., the largest power of r that divides n, while $n_{r'}$ denotes the r'-part of n, i.e., the ratio $|n|/n_r$; moreover, if a prime r is odd and coprime to n, then by $e(r, n)$ is denoted the multiplicative order of n modulo r. For an odd number n put $e(2, n) = 1$, if $n \equiv 1 \pmod 4$, and $e(2, n) = 2$ if $n \equiv 3 \pmod 4$.

Let n be an integer, $|n| > 1$. A prime r is called a *primitive prime divisor* of $n^i - 1$ if $e(r, n) = i$. The existence of primitive divisors for almost all pairs of n and i was established by Zsigmondy.

Lemma 1.1 (Zsigmondy [7]). *Let n be an integer number and $|n| > 1$. Then for every natural number i, there is a prime r with $e(r, n) = i$, except when $(n, i) \in \{(2, 1), (2, 6), (-2, 2), (-2, 3), (3, 1), (-3, 2)\}$.*

The set of all primitive divisors of $n^i - 1$ is denoted by $R_i(n)$, an element of this set is denoted by $r_i(n)$, moreover, if n is foregone then notation r_i is used. For $i \neq 2$ the product of all primitive divisors of $n^i - 1$ taken with multiplicities is called the greatest primitive divisor and denoted by $k_i(n)$. In turn the number $k_2(n)$ is defined as the product of all primitive divisors of $n + 1$ taken with multiplicities. It is easy to check that for fixed n numbers $k_i(n)$ are pairwise coprime for different i. Moreover, when i is odd we have $k_i(n) = k_{2i}(-n)$, in particular, $k_1(n) = k_2(-n) = |n - 1|/2$ if $n \equiv 3 \pmod 4$, and $k_1(n) = k_2(-n) = |n - 1|$ otherwise. It follows from [8] that for $i > 2$

$$k_i(n) = \frac{|\Phi_i(n)|}{(r, \Phi_{i_{r'}}(n))}, \tag{1}$$

where $\Phi_i(x)$ is the ith cyclomatic polynomial, r is the largest prime divisor of i, and if $i_{r'}$ does not divide $r - 1$ then $(r, \Phi_{i_{r'}}(n)) = 1$. In particular, $k_3(n) = k_6(-n) = (n^2 + n + 1)/(3, n - 1)$.

In notations of nonabelain simple groups we keep the following agreements. Groups of Lie type are denoted according to Lie notation. Moreover, we use the short form $A_n^{\varepsilon}(q)$ where $\varepsilon \in \{+, -\}$, setting $A_n^+(q) = A_n(q)$ for the linear group, and $A_n^-(q) = {}^2A_n(q)$ for the

unitary group. The alternating (symmetric) group of degree n is denoted by Alt_n (Sym_n respectively). For convenience we consider the Tits group ${}^2F_4(2)'$ as one of sporadic groups which are denoted according to [9].

Let G be a finite group. Denote by $s(G)$ the number of connected components of the graph $GK(G)$. For every $1 \leq i \leq s(G)$ denote by $\pi_i(G)$ i-th connected component of the graph, by $\omega_i(G)$ subset in $\omega(G)$ of numbers whose prime divisors lie in $\pi_i(G)$. If the order of group G is even then assume that $2 \in \pi_1(G)$.

Lemma 1.2 (Gruenberg, Kegel [10])**.** *If G is a finite group with $s(G) > 1$, then one of the following holds:*

(1) *$s(G) = 2$, G is a Frobenius group;*

(2) *$s(G) = 2$, $G = ABC$, where A, AB are normal subgroup of G, B is a normal subgroup of BC, and AB and BC are Frobenius groups;*

(3) *there is a nonabelain simple group S such that $S \leq \overline{G} = G/K \leq \operatorname{Aut} S$ for some nilpotent normal $\pi_1(G)$-subgroup K of G; moreover, $s(S) \geq s(G)$, and for every $1 < i \leq s(G)$ there is $1 < j \leq s(S)$ such that $\omega_i(G) = \omega_j(S)$.*

Recall that a subset of vertices of graph is called a coclique, if every two vertices of this subset are non-adjacent. Denote by $t(G)$ the maximal size of a coclique in $GK(G)$. If $2 \in \pi(G)$ then denote by $t(2, G)$ the maximal size of a coclique containing 2 and denote by $\rho(2, G)$ a set of vertices in such coclique.

Lemma 1.3. ([11, Proposition 2], [12, Theorem 2]) *Let L be a finite nonabelain simple group with $t(L) \geq 3$ and $t(2, G) \geq 2$, and let G be a finite group isospectral to L. Then the following hold.*

(1) *There exists a nonabelain simple group S such that $S \leq \overline{G} = G/K \leq \operatorname{Aut} S$ for the maximal normal soluble subgroup K in G.*

(2) *For every coclique ρ of $GK(G)$ containing at least 3 elements at most one prime from ρ divides the product $|K| \cdot |\overline{G}/S|$. In particular, $t(S) \geq t(L) - 1$.*

(3) *Every prime $r \in \pi(G)$ non-adjacent to 2 in $GK(G)$ does not divide $|K| \cdot |\overline{G}/S|$. In particular, $t(2, S) \geq t(2, L)$.*

Finite simple groups with disconnected prime graph were described by Williams [10] and Kondrat′ev [13]. The complete list of these groups with corrected inaccuracies can

be found in [4, Tables 1a-1c]. In the present article the short version of this list is used (see Tables 1 and 2). The tables contain all simple groups S (excepting sporadic) with disconnected prime graph satisfying $t(2, S) \geq 3$ (values of $t(2, S)$ for all simple groups were found in [14]). It is inferred from results of Williams and Kondrat′ev that if S is a simple group and $s(S) > 1$, then for every $1 < i \leq s(S)$ the set $\omega_i(S)$ has the unique maximal element with respect to divisibility. In the tables these maximal elements are denoted by $n_i = n_i(S)$ where $1 < i \leq s(S)$. Moreover, in Table 1 for every group S from the list a set $\rho(2, S)$ is given. If S a group of Lie type over the field of order u then an element from $\rho(2, S)$ denoted by r_i is a primitive prime divisor $r_i(u)$ of $u^i - 1$. It follows from [14, Propositions 6.4 and 6.7] that for every group S of Lie type given in Table 1, the set $\rho(2, S)$ is defined uniquely up to choice of primitive divisors of $R_i(u)$. The set $\rho(2, S)$ is defined uniquely for alternating group S from Tables 1 and 2.

T a b l e 1. **Finite simple group S with $s(S) = 2$ and $t(2, S) \geq 3$.**

Throughout the table s is an odd prime number.

S	Conditions on S	$\rho(2, S)$	$n_2(S)$
Alt_{s+1}	$s, s-2$ are primes	$\{2, s, s-2\}$	s
$A_2(u)$	u is even, $u > 4$, $(u-1)_3 = 3$	$\{2, 3, r_2, r_3\}$	$(u^2+u+1)/(3, u-1)$
$A_2(u)$	u is even, $u > 4$, $(u-1)_3 \neq 3$	$\{2, r_2, r_3\}$	$(u^2+u+1)/(3, u-1)$
$A_{s-1}(u)$	u is even, $s > 3$, $(s, u) \neq (7, 2)$	$\{2, r_{s-1}, r_s\}$	$(u^s-1)/(u-1)(s, u-1)$
$A_s(u)$	u is even, $(u-1) \mid (s+1)$, $(s, u) \neq (5, 2)$	$\{2, r_s, r_{s+1}\}$	$(u^s-1)/(u-1)$
$A_s(u)$	$(u-1)_2 = (s+1)_2 > 2$, $(u-1) \mid (s+1)$	$\{2, r_s, r_{s+1}\}$	$(u^s-1)/(u-1)$
${}^2A_2(u)$	u is even, $(u-1)_3 = 3$	$\{2, 3, r_2(-u), r_3(-u)\}$	$(u^2-u+1)/(3, u+1)$
${}^2A_2(u)$	u is even, $u > 2$, $(u-1)_3 \neq 3$	$\{2, r_2(-u), r_3(-u)\}$	$(u^2-u+1)/(3, u+1)$
${}^2A_{s-1}(u)$	u is even, $s > 3$	$\{2, r_{s-1}(-u), r_s(-u)\}$	$(u^s+1)/(u+1)(s, u+1)$
${}^2A_s(u)$	u is even, $(u+1) \mid (s+1)$, $(s, u) \neq (5, 2)$	$\{2, r_s(-u), r_{s+1}(-u)\}$	$(u^s+1)/(u+1)$
${}^2A_s(u)$	$(u+1)_2 = (s+1)_2 > 2$, $(u+1) \mid (s+1)$, and $(s, u) \neq (3, 3)$	$\{2, r_s(-u), r_{s+1}(-u)\}$	$(u^s+1)/(u+1)$
$C_s(2)$	$s > 3$	$\{2, r_s, r_{2s}\}$	$2^s - 1$
$D_s(u)$	$u = 2$ or $u = 5$, $s > 3$	$\{2, r_s, r_{2s-2}\}$	$(u^s-1)/(u-1)$
$D_{s+1}(2)$	$s > 3$	$\{2, r_{s-1}, r_{2s-2}\}$	$2^s - 1$
${}^2D_4(2)$		$\{2, 7, 17\}$	17
${}^2D_n(u)$	u is even, $4 \leq n = 2^m$, $(n, u) \neq (4, 2)$	$\{2, r_{n-1}, r_{2n-2}, r_{2n}\}$	$u^n + 1$
${}^2D_n(2)$	$5 \leq n = 2^m + 1$	$\{2, r_{2n-2}, r_{2n}\}$	$2^{n-1} + 1$
${}^2D_s(3)$	$s \neq 2^m + 1$	$\{2, r_{2s-2}, r_{2s}\}$	$(3^s+1)/4$
${}^2D_n(3)$	$n = 2^m + 1 \neq s$	$\{2, r_{2n-2}, r_{2n}\}$	$(3^{n-1}+1)/2$
$G_2(u)$	$2 < u \equiv \varepsilon 1 \pmod 3$, $\varepsilon = \pm$	$\{2, r_3, r_6\}$	$u^2 - \varepsilon u + 1$
$E_6(u)$	u is even	$\{2, r_8, r_9, r_{12}\}$	$(u^6+u^3+1)/(3, u-1)$
$E_6(u)$	u is odd	$\{2, r_9, r_{12}\}$	$(u^6+u^3+1)/(3, u-1)$
${}^2E_6(u)$	u is even, $u > 2$	$\{2, r_8, r_{12}, r_{18}\}$	$(u^6-u^3+1)/(3, u+1)$
${}^2E_6(u)$	u is odd	$\{2, r_{12}, r_{18}\}$	$(u^6-u^3+1)/(3, u+1)$

T a b l e 2. **Finite simple groups S with $s(S) \geq 3$.**

Throughout the table s is an odd prime, u is a power of a prime v.

S	Conditions on S	n_2	n_3	n_4	n_5
Alt_s	$s, s-2$ are primes	s	$s-2$		
$A_1(u)$	u is even, $u > 2$	$u+1$	$u-1$		
$A_1(u)$	$u \equiv 1 \pmod 4$	v	$(u+1)/2$		
$A_1(u)$	$3 < u \equiv 3 \pmod 4$	v	$(u-1)/2$		
${}^2A_5(2)$		7	11		
${}^2D_s(3)$	$s = 2^m + 1$	$(3^{s-1}+1)/2$	$(3^s+1)/4$		
$G_2(u)$	$u \equiv 0 \pmod 3$	u^2-u+1	u^2+u+1		
$F_4(u)$	u is even	u^4+1	u^4-u^2+1		
${}^2G_2(u)$	$u = 3^{2k+1} > 3$	$u-\sqrt{3u}+1$	$u+\sqrt{3u}+1$		
${}^2F_4(u)$	$u = 2^{2k+1} > 2$	$u^2-\sqrt{2u^3}+u-\sqrt{2u}+1$	$u^2+\sqrt{2u^3}+u+\sqrt{2u}+1$		
$E_7(2)$		73	127		
$E_7(3)$		757	1093		
$A_2(4)$		3	5	7	
${}^2B_2(u)$	$u = 2^{2k+1} > 2$	$u-1$	$u-\sqrt{2u}+1$	$u+\sqrt{2u}+1$	
${}^2E_6(2)$		13	17	19	
$E_8(u)$	$u \equiv 2, 3 \pmod 5$	$\frac{u^{10}-u^5+1}{u^2-u+1}$	$\frac{u^{10}+u^5+1}{u^2+u+1}$	u^8-u^4+1	
$E_8(u)$	$u \not\equiv 2, 3 \pmod 5$	$\frac{u^{10}-u^5+1}{u^2-u+1}$	$\frac{u^{10}+u^5+1}{u^2+u+1}$	u^8-u^4+1	$\frac{u^{10}+1}{u^2+1}$

Lemma 1.4. *Let q be a power of a prime p. Then*

(1) $\mu(G_2(q)) \subseteq \{8, 12, 2(q \pm 1), q^2-1, q^2 \pm q + 1\} \subseteq \omega(G_2(q))$ *for* $p = 2$;

(2) $\mu(G_2(q)) = \{p^2, p(q \pm 1), q^2-1, q^2 \pm q + 1\}$ *for* $p = 3, 5$;

(3) $\mu(G_2(q)) = \{p(q \pm 1), q^2-1, q^2 \pm q + 1\}$ *for* $p > 5$.

Proof. It is a consequence of the results [15, 16].

Lemma 1.5. *Let G be a finite group isospectal to $G_2(q)$, $q > 2$, and $S \leq \overline{G} = G/K \leq \operatorname{Aut} S$, where K is the soluble radical of G. Assume that $S \simeq A^{\varepsilon}_{n-1}(u)$ where either $n \geq 3$, or $n = 2$ and u is even. Then there exist integers i_1, i_2, $m_1(S) \in \mu(S)$ and $m_2(S) \in \mu(S)$ such that $\{i_1, i_2\} = \{n-1, n\}$ and the following chains of divisibilities hold*

$$(q^2+q+1) \vdots m_1(S) \vdots k_{i_1}(\varepsilon u) \vdots k_3(q);$$

$$(q^2 - q + 1) \vdots m_2(S) \vdots k_{i_2}(\varepsilon u) \vdots k_6(q).$$

Proof. Let $p_1 \in R_3(q)$, $p_2 \in R_6(q)$. Then the set $\{2, p_1, p_2\}$ is the maximal coclique of $GK(G)$ containing 2. By Lemma 1.3(3), the primes p_1, p_2 divide the order of S, so the set $\{2, p_1, p_2\}$ is a coclique of $GK(S)$. Since S is not $A_1(u)$ for odd u, the numbers p_1 and p_2 do not equal to characteristic v of S. Hence there are integers i_1, i_2 such that $p_1 \in R_{i_1}(\varepsilon u)$, $p_2 \in R_{i_2}(\varepsilon u)$. Note that p_1 and p_2 are greater than 3. It follows from Tables 1 and 2 that $\{i_1, i_2\} = \{n-1, n\}$, and for every $r \in R_{n-1}(\varepsilon u)$ and $s \in R_n(\varepsilon u)$ the primes r and s are non-adjacent in $GK(S)$. Therefore, $R_3(q) \subseteq R_{i_1}(\varepsilon u)$ and $R_6(q) \subseteq R_{i_2}(\varepsilon u)$. By [17, Theorems 2.1, 2.2], the group S contains cyclic Hall subgroups of orders $k_{n-1}(\varepsilon u)$ and $k_n(\varepsilon u)$. Hence the inclusion $R_3(q) \subseteq R_{i_1}(u)$ implies the divisibility $k_3(q) \mid k_{i_1}(\varepsilon u)$. Similarly, we get $k_6(q) \mid k_{i_2}(\varepsilon u)$. The set $\mu(S)$ contains an element $m_1(S)$ divisible by $k_{i_1}(\varepsilon u)$, and so by $k_3(q)$, and element $m_2(S)$ divisible by $k_{i_2}(\varepsilon u)$, and so by $k_6(q)$. Since $q > 2$, Lemma 1.4 yields that the unique element in $\mu(G)$ divisible by $k_6(q)$ is $q^2 - q + 1$, therefore, $m_2(S)$ divides $q^2 - q + 1$. Similarly, $m_1(S) \mid (q^2 + q + 1)$.

Lemma 1.6. *Let G be a finite group isospectral to $G_2(q)$, $q > 2$, and $S \leq \overline{G} = G/K \leq \operatorname{Aut} S$, where K is soluble radical of G. Assume that $S \simeq A_1(u)$ for odd u, and $t = n_3(S)$, where $n_3(S)$ is taken from Table 2. Then for some $\tau \in \{+, -\}$ we have $v = k_3(\tau q)$ and $t \in \{q^2 - \tau q + 1, k_3(-\tau q)\}$.*

Proof. Let $p_1 \in R_3(q)$, $p_2 \in R_6(q)$. By the same way as in Lemma 1.5, we obtain that $\{2, p_1, p_2\}$ is a coclique containing 2 of $GK(S)$, so one of p_1 and p_2 is equal to v, the other divides t (see Table 2). Repeating the arguments of the proof of Lemma 1.5 we obtain that for some $\tau \in \{+, -\}$ the following chains of divisibilities hold

$$(q^2 + \tau q + 1) \vdots v \vdots k_3(\tau q);$$

$$(q^2 - \tau q + 1) \vdots t \vdots k_3(-\tau q).$$

Now the conclusion holds obviously, since v is a prime and the ratio of $q^2 - \tau q + 1$ and $k_3(-\tau q)$ lies in the set $\{1, 3\}$.

Lemma 1.7. *Suppose n is an integer greater than 2, u is a prime power, $\varepsilon \in \{+, -\}$. Let $a_n^\varepsilon(u) = \left|\frac{(\varepsilon u)^{n/2}-1}{(\varepsilon u-1, n)(\varepsilon u-1)}\right|$ and $b_n^\varepsilon(u) = \left|\frac{(\varepsilon u)^{(n-1)/2}-1}{(\varepsilon u-1, n)}\right|$. Then $a_n^\varepsilon(u) > 3$ for even n, except*

when $(n,u) \in \{(4,2),(4,3),(4,4),(4,5),(4,7),(4,9),(4,11),(6,2)\}$, *and* $b_n^{\varepsilon}(u) > 3$ *for odd* n, *except when* $(n,u) \in \{(3,2),(3,3),(3,4),(3,5),(3,7),(3,8),(5,2),(5,4)\}$.

Proof. Elementary calculations.

Lemma 1.8. *Let* q *be a positive integer. A prime divisor of* q^2+q+1 *or* q^2-q+1 *distinct from* 3 *is of type* $6k+1$ *for some integer* k. *Moreover, for* $q > 2$ *both of these numbers have a prime divisor distinct from* 3.

Proof. Due to the equality $q^2 - q + 1 = (q-1)^2 + (q-1) + 1$, it is sufficient to prove the statement of the lemma for prime divisors of numbers $q^2 + q + 1$. Suppose r is a prime divisor of $q^2 + q + 1$. Then r divides $q^3 - 1$. Moreover, by Fermat's little theorem $r \mid (q^{(r-1)} - 1)$. We have $(q^3 - 1, q^{(r-1)} - 1) = q^{(3,r-1)} - 1$. If $(3, r-1) = 1$ then $r \mid (q-1)$, hence $q^2 + q + 1 \equiv 3 \pmod r$. Hence $r = 3$. Suppose that $(3, r-1) = 3$. Since $q^2 + q + 1$ is odd, we have $r \equiv 1 \pmod 6$. The second part of the statement follows from the fact that $q^2 \pm q + 1$ is not divisible by 9 for all $q > 2$. The lemma is proved.

§ 2. Proof of the theorem: a nonabelain composition factor

Let $L = G_2(q)$ and G be a finite group with $\omega(G) = \omega(L)$. As observed, the recognizability of $G_2(q)$ was proved for $q = 3^k$, $k \geq 1$, and $q = 4, 7$, so we assume that $(3, q) = 1$, $q \geq 5$, and $q \neq 7$. Note that $GK(G) = GK(L)$, so $t(2, G) = 3$, hence, by Lemma 1.3, there is a nonabelain simple group S such that $S \leq G/K \leq \operatorname{Aut} S$ for the maximal normal soluble subgroup K of G, and $s(S) \geq 2$, $t(2, S) \geq 3$. Thus S is either a sporadic group or one of the groups from Tables 1 and 2. We consider every case separately and show that $S \simeq L$. Fix ε from $\{+, -\}$ such that $n_2(L) = q^2 + \varepsilon q + 1$. Lemma 1.2 implies that $q^2 + \varepsilon q + 1 = n_i(S)$ for some $i > 1$. Further we use this fact without a detailed explanation.

Lemma 2.1. *S is neither a sporadic group, nor the Tits group.*

Proof. It is a direct consequence of Lemma 7 in [18].

Lemma 2.2. *$S \not\simeq Alt_m$.*

Proof. Assume the contrary. It follows from Tables 1 and 2 that either m or $m-1$ is prime. Therefore, among prime divisors of the order of S there are exactly two numbers

not-adjacent to 2. These are either m and $m-2$ or $m-1$ and $m-3$. By Lemma 1.3(3), every prime divisor of $k_3(q)$ and $k_6(q)$ should be equal to of one of those numbers. Hence $k_3(q)$ coincides to one of them and $k_6(q)$ does to the other. Therefore, $|k_3(q) - k_6(q)| = 2$. On the other hand,

$$|k_3(q) - k_6(q)| \geq q^2 - q + 1 - \frac{q^2+q+1}{3} = \frac{2}{3}(q-1)^2 > 2$$

for $q > 2$; a contradiction.

Lemma 2.3. *$S \not\simeq {}^2D_4(2), {}^2A_5(2), E_7(2), E_7(3), A_2(4), {}^2E_6(2)$.*

Proof. Assume the contrary. Then $q^2 + \varepsilon q + 1 = n_i(S)$ where $i \in \{2, 3, 4\}$. Since $q \geq 5$, we have $q^2 + \varepsilon q + 1 \geq 21$. Applying Tables 1 and 2 we obtain $S \in \{E_7(2), E_7(3)\}$. If $S = E_7(2)$ then $q^2 + \varepsilon q + 1 = 73$. Hence $(q, \varepsilon) = (8, +)$ and $(q, \varepsilon) = (9, -)$, so $q = 8$ due to $(q, 3) = 1$. Since $127 \in \omega(E_7(2)) \setminus \omega(G_2(8))$, it is impossible. If $S = E_7(3)$ then $q^2 + \varepsilon q + 1 = 757$. Hence $(q, \varepsilon) = (27, +)$ or $(q, \varepsilon) = (28, -)$, and both cases are impossible due to restrictions for q.

Lemma 2.4. *$S \not\simeq A_1(u)$.*

Proof. Let $S \simeq A_1(u)$. Suppose that u is even. It follows from Lemma 1.5 that $q^2+\varepsilon q+1 = u+\tau 1$ where $\tau \in \{+, -\}$. Moreover, by Lemma 1.6, $\frac{q^2-\varepsilon q+1}{u-\tau 1} \in \{1, 3\}$. If $q^2-\varepsilon q+1 = u-\tau 1$, then $\tau 2 = (u + \tau 1) - (u - \tau 1) = (q^2 + \varepsilon q + 1) - (q^2 - \varepsilon q + 1) = 2\varepsilon q$; a contradiction. Therefore $q^2 - \varepsilon q + 1 = 3(u - \tau 1)$. So $\tau 6 = 2q^2 + \varepsilon 4q + 2$, which is impossible for $q > 4$. Thus u is odd. Let $q^2+\varepsilon q+1 = (u+\tau 1)/2$ where $\tau \in \{+, -\}$. Then Lemma 1.6 yields that $q^2 - \varepsilon q + 1 = 3v$. If $q = 5$ then $\varepsilon = +$, $v = 7$ and $u = 62 - \tau 1$, which is impossible. So we may assume that $q \geq 8$ and hence $v \geq 19$. If $u = v$ then $6(q^2 + \varepsilon q + 1) = q^2 - \varepsilon q + 1 + \tau 3$, whence $5q^2 + 7\varepsilon q + (5 - \tau 3) = 0$, which is impossible for $q \geq 8$. Therefore, $u \geq v^2$. Then $2(q^2+\varepsilon q+1) = u+\tau 1 \geq 19v+\tau 1 > 6(q^2-\varepsilon q+1)$, whence $q^2-2\varepsilon q+1 < 0$; a contradiction. Therefore, $q^2 + \varepsilon q + 1 = v$. By Lemma 1.6, we have $a(u + \tau 1) = 2(q^2 - \varepsilon q + 1)$ where $a \in \{1, 3\}$. Let $u = v$. If $a = 1$ then the equality $q^2 - 3\varepsilon q + 1 = 0$ holds, and if $a = 3$ then the equality $q^2 + 5\varepsilon q + 1 = 0$ does. Both equalities are impossible for $q > 4$. Hence $u \geq v^2$. Since $q \geq 5$, the inequality $v \geq 31$ holds. Therefore, $2(q^2 - \varepsilon q + 1) = a(u + \tau 1) \geq 31v + \tau 1 = 31(q^2 + \varepsilon q + 1) + \tau 1$, which is again impossible for $q \geq 5$.

Lemma 2.5. *$S \not\simeq A^{\epsilon}_{n-1}(u)$, where $n \geq 3$ and $\epsilon \in \{+, -\}$.*

Proof. Let $S \simeq A_{n-1}^{\epsilon}(u)$. First we suppose that n is even. Note that in this case $k_n(\epsilon u)$ divides $(\epsilon u)^{n/2}+1$ and, in particular, $k_n(\epsilon u) \leq |(\epsilon u)^{n/2}+1|$. Further, by [17, Theorems 2.1, 2.2], the number $k_n(\epsilon u)$ divides t, where $t = \left|\frac{\epsilon u^n-1}{(\epsilon u-1,n)(\epsilon u-1)}\right| \in \mu(S)$. Therefore, by Lemma 1.5, there is $\tau \in \{+,-\}$ such that the following chain of divisibilities holds

$$(q^2+\tau q+1) \vdots t \vdots k_n(\epsilon u) \vdots k_3(\tau q).$$

Assume that $(n,u) \notin M$ where $M = \{(4,2),(4,3),(4,4),(4,5),(4,7),(4,9),(4,11),(6,2)\}$. Lemma 1.7 implies $a_n^{\epsilon}(u) = \left|\frac{(\epsilon u)^{n/2}-1}{((\epsilon u)-1,n)(\epsilon u-1)}\right| > 3$. On the other hand,

$$q^2+\tau q+1 \leq 3k_3(\tau q) \leq 3k_n(\epsilon u) \leq 3|(\epsilon u)^{n/2}+1| < a_n^{\epsilon}(u)\cdot|(\epsilon u)^{n/2}+1| = t;$$

a contradiction. Hence $(n,u) \in M$. By Lemma 1.8, all prime divisors of $q^2+\tau q+1$ distinct from 3 have form $6k+1$, so the same is true for t. If $n=4$ and $u = 2,3,4,7,9,11$, then we have a contradiction for 5 divides t. If $(n,u) = (4,5)$, then either $t = 39$ and $\epsilon = +$ or $t = 52$ and $\epsilon = -$. The last case is impossible, since number $q^2+\tau q+1$ is odd. Therefore, $k_3(\tau q) \mid 13$, so $q^2+\tau q+1 = 39$, which is impossible for q is a prime power. Let finally $(n,u) = (6,2)$. If $\epsilon = +$ then $t = 63$, which contradicts to Lemma 1.8 because of $9 \mid (q^2+\tau q+1)$. Therefore, $\epsilon = -$ and $t = 7$. We obtain that $(q^2+\tau q+1)$ divides 21, hence $q = 5$. In this case $11 \in \pi(S) \setminus \pi(L)$; a contradiction. Thus n cannot be even.

Let $n-1$ be even. Again $k_{n-1}(\epsilon u)$ divides $(\epsilon u)^{(n-1)/2}+1$ and, in particular, $k_{n-1}(\epsilon u) \leq |(\epsilon u)^{(n-1)/2}+1|$. By [17, Theorems 2.1, 2.2], the number $k_{n-1}(\epsilon u)$ divides t, where $t = \left|\frac{\epsilon u^{n-1}-1}{(\epsilon u-1,n)}\right| \in \mu(S)$. Therefore, Lemma 1.5 implies that there is $\tau \in \{+,-\}$ such that the chain of divisibilities holds

$$(q^2+\tau q+1) \vdots t \vdots k_{n-1}(\epsilon u) \vdots k_3(\tau q).$$

Suppose that $(n,u) \notin M$ where $M = \{(3,2),(3,3),(3,4),(3,5),(3,7),(3,8),(5,2),(5,4)\}$. Lemma 1.7 yields that $b_n^{\epsilon}(u) = \left|\frac{(\epsilon u)^{(n-1)/2}-1}{(\epsilon u-1,n)}\right| > 3$. On the other hand,

$$q^2+\tau q+1 \leq 3k_3(\tau q) \leq 3k_{n-1}(\epsilon u) \leq 3|(\epsilon u)^{(n-1)/2}+1| < b_n^{\epsilon}(u)\cdot|(\epsilon u)^{(n-1)/2}+1| = t;$$

a contradiction. Hence $(n,u) \in M$. If $(n,u) \in (3,3),(3,5),(3,7)$ then t is even; if $(n,u) = (3,4)$ then t is divisible on 5; if $(n,u) = (5,4)$ then t is divisible on 17; in all these cases we obtain a contradiction applying Lemmas 1.5 and 1.8. The case $(n,u) = (3,2)$ is impossible,

since for $\epsilon = -$ group S is not simple, and for $\epsilon = +$ we have $S = A_2(2) \simeq A_1(7)$, which contradicts to Lemma 2.4. If $(n, u) = (3, 8)$, then $t = 21$ or $t = 63$. The last case is impossible for 9 does not divide $q^2 + \tau q + 1$. Hence $\epsilon = -$ and $k_3(\tau q)$ divides 21. So $q = 5$ and $19 \in \pi(S) \setminus \pi(L)$; a contradiction. It remains to treat the case $(n, u) = (5, 2)$, in which either $t = 15$ or $t = 3$. In the former case we get a contradiction by Lemma 1.8, the later case is impossible due to $t \geq 7$.

Lemma 2.6. $S \not\simeq C_s(2)$.

Proof. Let $S \simeq C_s(2)$. It follows from Table 1 that $q^2 + \varepsilon q + 1 = 2^s - 1$, whence $q(q+\varepsilon 1) = 2(2^{(s-1)/2} - 1)(2^{(s-1)/2} + 1)$. If q is even then the equality provides $q = 2$, so we may assume that q is odd. The numbers $2^{(s-1)/2} - 1$ and $2^{(s-1)/2} + 1$ are pairwise coprime, therefore only one of them is divisible by q, hence $2(2^{(n-1)/2} - 1)(2^{(n-1)/2} + 1) \geq 2q(q-2)$. It follows that $q(q+\varepsilon 1) \geq 2q(q-2)$, which is wrong for $q > 5$. Hence $q = 5$. The equality $q^2 + \varepsilon q + 1 = 2^s - 1$ implies that $\varepsilon = +$ and $s = 5$. However, $17 \in \pi(S) \setminus \pi(L)$; a contradiction.

Lemma 2.7. $S \not\simeq D_n(u)$.

Proof. Assume the contrary. Table 1 provides that either $u = 2$, $n \in \{s, s+1\}$ and $q^2 + \varepsilon q + 1 = 2^s - 1$, or $u = 5$, $n = s$ and $q^2 + \varepsilon q + 1 = (5^s - 1)/4$, where s is a prime greater than 3. Treating the former case similarly to Lemma 2.6 we obtain that $s = 5$, $\varepsilon = +$, so $q = 5$. However, $17 \in \pi(D_5(2)) \subseteq \pi(D_6(2))$, but $17 \notin \pi(G_2(5))$; a contradiction. Thus $q^2 + \varepsilon q + 1 = (5^s - 1)/4$, hence $4q(q + \varepsilon 1) = 5(5^{s-1} - 1)$. Since s is an odd prime, the number $s - 1$ is even, so $4q(q + \varepsilon) = 5(5^{(s-1)/2} - 1)(5^{(s-1/2)} + 1)$. If q is divisible by 5, then $q = 5$, so $5^{s-1} - 1 \in \{16, 24\}$. It is possible only if $s = 3$, which contradicts to the choice of s. Therefore $(q, 5) = 1$. Since $(5^{(s-1)/2} + 1, 5^{(s-1)/2} - 1) = 2$, one of these numbers is divisible by q. Hence $4(q + \varepsilon 1) \geq 5(q - 2)$. Since $q > 5$, we have $\varepsilon = +$. Then $q \leq 13$ and $q + 1$ is divisible by 5, which is possible only in if $q = 9$; a contradiction.

Lemma 2.8. $S \not\simeq {}^2D_n(u)$.

Proof. Assume that $S \simeq {}^2D_n(u)$. It follows from Tables 1 and 2 that there are 3 possible values for $q^2+\varepsilon q+1$: $(3^{n-1}+1)/2$, $(3^n+1)/4$ or 2^k+1 for some k. If $q^2+\varepsilon q+1 = 2^k+1$ then $q(q+\varepsilon 1) = 2^k$. So $q = 2$, which is impossible. Let $q^2+\varepsilon q+1 = (3^{n-1}+1)/2$. In this case n

is odd, so $2q(q+\varepsilon 1) = (3^{(n-1)/2}+1)(3^{(n-1)/2}-1)$. Since $(3^{(n-1)/2}+1, 3^{(n-1)/2}-1) = 2$, one of these two numbers is divisible by q. Suppose firstly that both of them are not equal to q. Then $3^{(n-1)/2}+1 \geq 2q$, which implies $2q(q+\varepsilon 1) \geq 2q(2q-2)$, a contradiction. Therefore, either $3^{(n-1)/2}+1$ or $3^{(n-1)/2}-1$ is equal to q. Therefore $2q(q+\varepsilon 1) = q(q \pm 2)$, which is impossible due to restrictions on q. Let finally $q^2+\varepsilon q+1 = (3^n+1)/4$. Then n is odd, so $4q(q+\varepsilon 1) = 3(3^{(n-1)/2}+1)(3^{(n-1)/2}-1)$. The equality $(3^{(n-1)/2}+1, 3^{(n-1)/2}-1) = 2$ implies that either $3^{(n-1)/2}+1$ or $3^{(n-1)/2}-1$ is divisible by $2q$. Therefore $4q(q+\varepsilon 1) \geq 3 \cdot 2q(2q-2)$; a contradiction.

Lemma 2.9. *S is neither $E_6(u)$ nor ${}^2E_6(u)$.*

Proof. Assume the contrary. Then $q^2+\varepsilon q+1 = n_2(S) = \frac{u^6+\tau u^3+1}{(u-\tau 1,3)}$ where $\tau = +$ for $S \simeq E_6(u)$ and $\tau = -$ for $S \simeq {}^2E_6(u)$. First, suppose that $(u-\tau 1, 3) = 1$. Then $q(q+\varepsilon 1) = u^3(u^3+\tau 1)$. If $q > u^3+1$ then $q+\varepsilon 1 \geq u^3+\tau 1$, so $q(q+\varepsilon 1) > u^3(u^3+\tau 1)$. Similarly, if $q < u^3-1$ then $q(q+\varepsilon 1) < u^3(u^3+\tau 1)$. Hence q is equal to one of the numbers u^3-1, u^3, u^3+1. Assume that $q = u^3+\tau 1 = (u+\tau 1)(u^2-\tau u+1)$. Since q is a prime power and $(u+\tau 1, u^2-\tau u+1)$ divides 3, we have $q \in \{7, 9\}$; a contradiction. Hence $q = u^3$. In this case the definition of primitive prime divisor and Lemma 1.1 imply that $R_{12}(u) \subseteq R_4(q)$ and $R_{12}(u) \neq \varnothing$. Therefore, for $r \in R_{12}(u)$ we have $r \in \pi(S) \setminus \pi(L)$; a contradiction. Suppose that $(u-\tau 1, 3) = 3$. Then $3(q^2+\varepsilon q+1) = u^6+\tau u^3+1$, so $3q(q+\varepsilon 1) = (u^3-\tau 1)(u^3+\tau 2)$. The numbers $u^3-\tau 1$ and $u^3+\tau 2$ are distinct from 3, hence $(u^3-\tau 1, u^3+\tau 2) = 3$. Therefore at least one of them is divisible by $3q$. Hence $3(q^2+\varepsilon q+1) = (u^3-\tau 1)(u^3+\tau 2) \geq 3q(3q-3)$, which is false for $q > 2$.

Lemma 2.10. *$S \not\simeq F_4(u)$*

Proof. Let $S \simeq F_4(u)$. Using Table 2 we find out that $q^2+\varepsilon q+1$ is equal to one of the numbers u^4+1, u^4-u^2+1. In the first case $q(q+\varepsilon 1) = u^4$, which is possible only if $q = 2$; a contradiction. In the second case, we have the equality $q(q+\varepsilon) = u^2(u^2-1)$. Similarly to Lemma 2.9 we obtain that $q \in \{u^2-1, u^2\}$. If $q = u^2$ then $R_8(u) \subseteq R_4(q)$. The set $R_8(u)$ is not empty and lies in $\pi(S) \setminus \pi(L)$; which is impossible. Therefore $q = u^2-1$. Since $u^4+1 \in \omega(S)$, we have $(q+1)^2+1 = u^4+1 \in \omega(L)$, but $(q+1)^2+1$ is greater than any number from $\mu(L)$ for $q > 2$; a contradiction.

Lemma 2.11. *$S \not\simeq {}^2G_2(3^{2m+1})$.*

Proof. In this case Table 2 provides that $q^2+\varepsilon q+1 = 3^{2m+1}+\tau 3^{m+1}+1$, where $\tau \in \{+,-\}$. Hence $q(q+\varepsilon 1) = 3^{m+1}(3^m+\tau 1)$. Since one of the numbers q and $q+\varepsilon 1$ must be divisible by 3^{m+1}, we have $3^{m+1}(3^m+\tau 1) = q(q+\varepsilon 1) \geq 3^{m+1}(3^{m+1}-1)$, which is impossible due to $m \geq 1$.

Lemma 2.12. *$S \not\simeq {}^2B_2(2^{2m+1})$.*

Proof. Assume the contrary. Then $q^2+\varepsilon q+1$ is equal to one of the following numbers: $u-1$, $u \pm \sqrt{2u}+1$, where $u = 2^{2m+1}$. If $q^2+\varepsilon q+1 = 2^{2m+1}-1$, then $q(q+\varepsilon 1) = 2(2^m+1)(2^m-1)$. Either 2^m+1 or 2^m-1 is divisible by q, so $q(q+\varepsilon 1) = 2(2^m+1)(2^m-1) \geq 2q(q-2)$, which is possible only if $q \leq 5$. Hence $q = 5$, $\varepsilon = +$, and $m = 2$. Then $41 \in \omega(S) \setminus \omega(L)$; a contradiction. Therefore $q^2+\varepsilon q+1 = u \pm \sqrt{2u}+1$. Hence $q(q+\varepsilon) = 2^{m+1}(2^m+\tau 1)$. One of the numbers q and $q+\varepsilon 1$ is divisible by 2^{m+1}, so $2^{m+1}(2^m+\tau 1) = q(q+\varepsilon) \geq 2^{m+1}(2^{m+1}-1)$. It is possible only if $m = 1$ and $\tau = +$, hence $q(q+\varepsilon 1) = 4 \cdot 3$, which is false for $q \geq 5$.

Lemma 2.13. *$S \not\simeq {}^2F_4(2^{2m+1})$.*

Proof. Assume the contrary. Then $q^2+\varepsilon q+1 = u^2+\tau\sqrt{2u^3}+u+\tau\sqrt{2u}+1$, where $u = 2^{2m+1}$ and $\tau \in \{+,-\}$. Therefore, $q(q+\varepsilon 1) = 2^{m+1}(2^{2m+1}+1)(2^m+\tau 1)$. Since $(2^{2m+1}+1, 2^m+\tau 1)$ divides 3, the number q divides only one of the three factors in the right part of the last equality. If q divides 2^{m+1} or $2^m+\tau 1$, the equality obviously does not hold. Hence q divides $2^{2m+1}+1$. If $q = 2^{2m+1}+1$ then the equality is false again, because of $q+\varepsilon 1 = 2^{2m+1}+1+\varepsilon 1 \neq 2^{2m+1}+\tau 2^{m+1}$. Hence $2^{2m+1}+1 \geq 3q$. Then $3q(3q-1)/2 \leq (2^{2m+1}+1)(2^{2m+1}+\tau 2^{m+1}) = q(q+\varepsilon 1)$, which is impossible.

Lemma 2.14. *$S \not\simeq E_8(q)$.*

Proof. Assume that $S \simeq E_8(u)$. Then $q+\varepsilon q+1 \in \{\frac{u^{10}+u^5+1}{u^2+u+1}, \frac{u^{10}-u^5+1}{u^2-u+1}, u^8-u^4+1, \frac{u^{10}+1}{u^2+1}\}$.

If $q+\varepsilon q+1 = u^8-u^4+1$ then $q(q+\varepsilon 1) = u^4(u^4-1)$. Let $(u^4,q) \neq 1$. It follows that $u^4 = q$ and $\varnothing \neq R_{20}(u) \subseteq R_5(q)$. We get a contradiction in view of $r_{20}(u) \in \omega(S) \setminus \omega(L)$. Hence $q \mid (u^4-1)$ and $u^4 \mid (q+\varepsilon 1)$, so $u^4-1 = q$, $\varepsilon = +$. In this case $u-1$ and $u+1$ should be powers of p. This is possible only if $u \in \{2,3\}$. However, $15 = 2^4-1$ and $80 = 3^4-1$ are not prime powers; a contradiction.

Suppose that $q^2+\varepsilon q+1 = \frac{u^{10}+1}{u^2+1}$. Then $q(q+\varepsilon 1) = u^2(u^2-1)(u^4+1)$. If $(q, u^4+1) = 1$, then q divides u^2 or u^2-1. In both cases $q+\varepsilon 1 \geq (u^4+1) > u^2+1$, hence $q > u^2$, which is

impossible. Therefore u^4+1 is divisible by q and $q+\varepsilon 1$ is divisible by $u^2(u^2-1)$. Suppose that $q+\varepsilon 1 > u^2(u^2-1)$. Then $q+\varepsilon 1 \geq 2u^2(u^2-1) > u^4+2 \geq q+1$; a contradiction. Hence $q+\varepsilon 1 = u^2(u^2-1)$ and $q = u^4+1$, which is impossible.

Let $q^2+\varepsilon q+1 = \frac{u^{10}+\tau u^5+1}{u^2+\tau u^2+1}$ for some $\tau \in \{+,-\}$. We have $q(q+\varepsilon 1) = u(u^4-1)(u^3-\tau u^2+\tau 1)$. Direct check shows that an equality of such type is impossible for $u \leq 5$ and arbitrary ε, τ, and q, where q is a prime power. So we may assume that $u > 5$. Moreover, numbers u, u^2-1, u^2+1, $u^3-\tau u^2+\tau 1$ are pairwise coprime except the following cases: $(u^2-1, u^2+1) \in \{1,2\}$ and $(u^2+1, u^3-\tau u^2+\tau 1) \in \{1,5\}$. Therefore, since q is a prime power and q divides $u(u^4-1)(u^3-\tau u^2+\tau 1)$, the following inequality holds $q \leq 5(u^3-\tau u^2+\tau 1)$. Hence $q+\varepsilon 1 \geq u(u^4-1)/5$. But $u > 5$ provides $u(u^4-1)/5 > 5(u^3-\tau u^2+\tau 1)+1$, so $q+\varepsilon 1 > q+1$; a contradiction.

Lemma 2.15. *If $S \simeq G_2(u)$ then $q = u$.*

Proof. Let $S \simeq G_2(u)$. Then $q^2+\varepsilon q+1 = u^2+\tau u+1$ where $\tau \in \{+,-\}$. Hence $q(q+\varepsilon 1) = u(u+\tau 1)$. If $q \neq u$ then $q = u+\tau 1$. Note that $u^2-1 \in \omega(G_2(u))$, so $q(q-\tau 2) \in \omega(G_2(q))$. Since $q \geq 5$, Lemma 1.4 yields that $q(q-\tau 2)$ divides only one number from $p(q+1)$, $p(q-1)$. Hence $q = p$, and $q-2$ divides $q+1$. It is possible only if $q = 5$ and $\varepsilon = -$, which contradicts to the choice of ε, because 5^2-5+1 is divisible by 3, and so is not equal to $n_2(L)$. Therefore $q = u$. The lemma is proved.

Thus, $S \simeq L = G_2(q)$.

§ 3. Completion of the proof

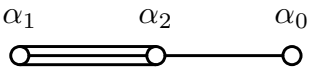
By the preceeding arguments, we may assume that $S = L$ and $L \leq \overline{G} = G/K \leq \operatorname{Aut} L$, where K is the soluble radical of G. Therefore, to complete the proof of the theorem it is sufficient to establish the following two lemmas.

Lemma 3.1. $K = 1$.

Proof. Assume the contrary. By [19, Lemma 12], we may suppose that $G = V \leftthreetimes L$ is a natural simedirect product of an elementary abelian r-group V and the group L, moreover, L acts on V by conjugation faithfully and irreducibly. First, assume that $r \neq p$. Then [20, Lemma 1.4] implies that L includes a Frobenius subgroup with a kernel of order q^2

and a cyclic complement of order q^2-1. Therefore, [21, Lemma 1] yields that G contains an element of order $r(q^2-1)$. Since $\omega(G)=\omega(L)$, this contradicts to Lemma 1.4. Hence $r=p$. By the main result of [22], the group L is unisingular for every odd q, that is every its semisimple element has fixed point in every FL-module, where F is a finite field of characteristic p. In particular, $p(q^2-1)\in\omega(G)\setminus\omega(L)$; a contradiction. Thus we may assume that $q=2^k>4$.

Consider extended Dynkin diagram of the algebra G_2:



where α_1,α_2 are simple roots, α_1 is short, α_2 is long, and $\alpha_0=-(3\alpha_1+2\alpha_2)$ is a negative root of the highest weight. Further notation of the lemmas corresponds to [23], in particular, a root subgroup corresponding the root α is denoted by X_α, and its element corresponding to a scalar t from the base field is denoted by $x_\alpha(t)$. Assume that $A=\langle X_{\alpha_0},X_{-\alpha_0}\rangle$. Homomorphism φ from $SL_2(q)$ to A, defined by

$$\begin{pmatrix}1&t\\0&1\end{pmatrix}\to x_{-\alpha_0}(t) \text{ and } \begin{pmatrix}1&0\\t&1\end{pmatrix}\to x_{\alpha_0}(t),$$

is isomorpishm, because q is even. Therefore $A\simeq SL_2(q)$. Let λ is a generator of the multiplicative group of the field F_q of order q. Denote by x the image of diagonal matrix $\mathrm{diag}(\lambda,\lambda^{-1})$ under the isomorpishm φ (this is the element $h_{-\alpha_0}(\lambda)=h_{\alpha_1}(\lambda)h_{\alpha_2}(\lambda^2)$ in terms of [23]). Note that the order of x is equal to $q-1>3$. The subgroup A lies in the following two subgroups of group L: $B=\langle X_{\pm\alpha_2},X_{\pm\alpha_0}\rangle\simeq SL_3(q)$ and $\langle X_{\pm\alpha_1},X_{\pm\alpha_0}\rangle=A\times C$, where $C\simeq A$. If W is a natural B-module then $\dim C_W(x)=1$. Therefore, by [24, consequence 1.6], the element x fixes a point in every B-module over any field of characteristic 2. In particular, considering V as B-module, we obtain that $U=C_V(x)\neq 0$. The subgroup $C\simeq SL_2(q)$ contains dihedral subgroup D of order $2s$, where s is an odd prime divisor of $q+1$. Let z is an involution and y is an element of order s from D. Since D centralizes x, the submodlue U is D-invariant. If $0\neq u\in C_U(y)$ then G contains the element uxy of order $2(q-1)s$, which is impossible due to Lemma 1.4. Hence $C_U(y)=0$. Then [21, Lemma 1] implies that the group $U\leftthreetimes D$ contains an element uz of order 4, and so the element uzx of G has the order $4(q-1)\notin\omega(L)$; a contradiction. The lemma is proved.

Lemma 3.2. *If $L \leq G \leq \operatorname{Aut} L$ then $L = G$.*

Proof. Assume the contrary. Since $p \neq 3$, we may assume that G is a split extension of L by a field automorpishm φ of prime order r. The centralizer $C_L(\varphi)$ of this automorpishm in L is isomorphic to the group $G_2(q_0)$, where $q = q_0^r$. If $p = 2$ and $r > 2$, then $8r \in \omega(G) = \omega(L)$; a contradiction. Taking into account that $q \geq 5$, we obtain $q_0 \geq 4$. Assume that $r \neq 3$. Observe that in this case $q_0^2 + \varepsilon q_0 + 1$ divides $q^2 + \varepsilon q + 1$, where $\varepsilon \in \{+, -\}$, and $((q_0^2 + q_0 + 1)(q_0^2 - q_0 + 1), (q^2 - 1)) = 3$. Choose $\varepsilon \in \{+, -\}$ so that r does not divide $q^2 + \varepsilon q + 1$. Then $r(q_0^2 + \varepsilon q_0 + 1) \in \omega(G) = \omega(L)$, which contradicts to Lemma 1.4. If $r = 3$, choose $\varepsilon \in \{+, -\}$ so that $q_0 \equiv \varepsilon 1 \pmod 3$. Then $3p(q_0 + \varepsilon 1) \in \omega(G) = \omega(L)$, which again contradicts to Lemma 1.4. The lemma and the theorem are proved.

References

1. *V. D. Mazurov*, Groups with prescibed spectrum, Izv. Ural. Gos. Univ., 2005, N 36 (Mat. Mekh., 7), 119–138.

2. *M. A. Grechkoseeva, W. J. Shi , A. V. Vasil′ev*, Recognition by spectrum of finite simple roups of Lie type, Front. Math. China, **3**, N 2 (2008), 275–285.

3. *A. V. Vasil′ev*, Recognizing groups $G_2(3^n)$ by their element orders, Algebra Logika, **41**, N 2 (2002), 130–142.

4. *V. D. Mazurov*, Recognition of finite simple groups $S_4(q)$ by their element orders, Algebra Logika, **41**, N 2 (2002), 166–198.

5. *A. V. Zavarnitsin*, Recognition of finite groups by the prime graph, Algebra Logika, **45**, N 4 (2006), 390–408.

6. *V. D. Mazurov*, Recognition of finite groups by a set of orders of their elements, Algebra Logika, **37**, N 6 (1998), 651—666.

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

8. *M. Roitman*, On Zsigmondy primes, Proc. Amer. Math. Soc., **125**, N 7 (1997), 1913–1919.

9. *J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, R. A. Wilson*, Atlas of finite groups, Oxford: Clarendon Press, 1985.

10. *J. S. Williams*, Prime graph components of finite groups, J. Algebra, **69**, N 2 (1981), 487–513.

11. *A. V. Vasil'ev*, On connection between the structure of a finite group and the properties of its prime graph, Sibirsk. Mat. Zh., **46**, N 3 (2005), 615–624.

12. *A. V. Vasil'ev, I. B. Gorshkov*, On recognition of finite simple groups with connected prime graph, Sibirsk. Mat. Zh., **50**, N 2 (2009), 292–299.

13. *A. S. Kondrat'ev*, Prime graph components of finite simple groups, Mat. Sb., **180**, N 6 (1989), 787–797.

14. *A. V. Vasil'ev, E. P. Vdovin*, An adjacency criterion for the prime graph of a finite simple group, Algebra Logika, **44**, N 6 (2005), 682–725.

15. *W. M. Kantor, A. Seress*, Prime power graphs for groups of Lie type, J. Algebra, **247** (2002), 370–434.

16. *D. Deriziotis*, Conjugacy classes and centralizers of semisimple elements in finite groups of Lie type, Vorlesungen aus dem Fachbereich Mathematik der Universitat GH Essen, 11, Universitat Essen, Fachbereich Mathematik, Essen, 1984.

17. *A. A. Buturlakin, M. A. Grechkoseeva*, The cyclic structure of maximal tori of the finite classical groups, Algebra Logika, **46**, N 2 (2007), 129–156.

18. *A. M. Staroletov*, Sporadic composition factors of finite groups isospectral to simple groups, Sib. Elektron. Mat. Izv., **8** (2011), 268–272.

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

20. *A. V. Vasil'ev, M. A. Grechkoseeva, V. D. Mazurov, Kh. P. Chao, G. Yu. Chen, W. Shi*, Recognition of the finite simple groups $F_4(2^m)$ by spectrum, Sibirsk. Mat. Zh., **45**, N 6 (2004), 1256–1262.

21. *V. D. Mazurov*, Characterization of finite groups by sets of orders of their elements, Algebra Logika, **36**, N 1 (1997), 37–53.

22. *R. M. Guralnick, P. H. Tiep*, Finite simple unisingular groups of Lie type, J. Group Theory, **6**, N 3 (2003), 271–310.

23. *R. W. Carter*, Simple groups of Lie type (Pure and Applied Mathematics, **28**), London etc., John Wiley & Sons, 1972.

24. *I. D. Suprunenko, A. E. Zalesski*, Fixed vectors for elements in modules for algebraic groups, Int. J. Algebra Comput., **17**, No 5–6 (2007), 1249–1261.

Authors' addresses:

Vasil′ev Andrey Victorovich
Sobolev Institute of Mathematics, Acad. Koptyug pr., 4
e-mail: vasand@math.nsc.ru

Staroletov Alexey Mikhailovich
Sobolev Institute of Mathematics, Acad. Koptyug pr., 4
e-mail: astaroletov@gmail.com

Abstract

Two groups are called isospectral if they have equal sets of element orders. We proved that for every finite simple exceptional group $L = G_2(q)$ every finite group G isospectral to L must be isomorphic to it.

Keywords: finite simple group, exceptional group of Lie type, element order, the spectrum of group, recognition by spectrum.