Serdica
Mathematical Journal
Сердика
Математическо списание

Serdica Math. J. **37** (2011), 365–370

Serdica
Mathematical Journal

Bulgarian Academy of Sciences
Institute of Mathematics and Informatics

(2, 3)-GENERATION OF THE GROUPS $PSL_6(q)$

K. Tabakov, K. Tchakerian

Communicated by V. Drensky

Abstract. We prove that the group $PSL_6(q)$ is $(2,3)$-generated for any q. In fact, we provide explicit generators x and y of orders 2 and 3, respectively, for the group $SL_6(q)$.

1. Introduction. A group G is called $(2,3)$-generated if $G = \langle x, y\rangle$ for some elements x and y of orders 2 and 3, respectively. Such groups attract attention mostly by the fact that a group is $(2,3)$-generated if and only if it is a homomorphic image of the famous modular group $PSL_2(\mathbb{Z})$. This generation property is known to hold for a number of series of finite simple groups. The most powerful result in this direction is the theorem of Liebeck-Shalev and Lübeck-Malle which states that all finite simple groups, except the symplectic groups $PSp_4(2^m)$, $PSp_4(3^m)$, the Suzuki groups $Sz(2^m)$ (m odd), and finitely many other groups, are $(2,3)$-generated (see [11]). Concerning the projective special

2010 *Mathematics Subject Classification:* 20F05, 20D06.
Key words: (2,3)-generated group.
This work is partially supported by the Scientific Research Fund of the "St. Kl. Ohridski" University of Sofia under Contract No 027, 2012.

linear groups $PSL_n(q)$, $(2,3)$-generation has been proved in the cases $n = 2, q \neq 9$ [8], $n = 3, q \neq 4$ [4], [1], $n = 4, q \neq 2$ [12], [13], [9], $n = 5$, any q [14], $n \geq 5$, odd $q \neq 9$ [2],[3], and $n \geq 13$, any q [10]. The present paper is another contribution to the problem. We prove the following:

Theorem. *The group $PSL_6(q)$ is $(2,3)$-generated for any q.*

We note that our approach is quite different from that of the authors of [2]. Their approach is based on the classification of finite irreducible linear groups generated by root subgroups, while we make use of the known list of maximal subgroups of $PSL_6(q)$.

2. Proof of the Theorem.

Let $G = SL_6(q)$ and $\overline{G} = G/Z(G) = PSL_6(q)$, where $q = p^m$ and p is a prime. Set $d = (6, q-1)$, also $Q = q^5 - 1$ if $q \neq 3, 7$ and $Q = (q^5 - 1)/2$ if $q = 3$ or 7. The group G acts naturally on a six-dimensional vector space V over the field $F = GF(q)$ and $\overline{G}$ acts on the corresponding projective space $P(V)$. Fix a basis $e_1, e_2, e_3, e_4, e_5, e_6$ of V.

We shall need the following result.

Lemma 1. *Let $\overline{M}$ be a maximal subgroup of the group $\overline{G}$. Then either $\overline{M}$ is reducible on the space $P(V)$ or $\overline{M}$ has no element of order $Q/(d,Q)$.*

Proof. The maximal subgroups of $PSL_6(q)$ are determined (up to conjugacy) in [5]. In particular, this implies that one of the following holds:

(i) $\overline{M}$ belongs to the family C_1 of reducible subgroups of $\overline{G}$;

(ii) $\overline{M}$ is a member of one of the remaining families C_2, C_3, C_4, C_5, C_8 of (irreducible) geometric subgroups of $\overline{G}$;

(iii) $\overline{M} \cong PSL_3(q)$ if q is odd or $\overline{M} \cong PSL_2(11)$, A_7, M_{12}, $PSL_3(4) \cdot \mathbb{Z}_2$, $PSU_4(3)$, or $PSU_4(3) \cdot \mathbb{Z}_2$ for specific values of p and q.

Zsigmondy's well-known theorem provides a primitive prime divisor of $p^{5m} - 1$, i.e., a prime r which divides $p^{5m} - 1$ but does not divide $p^i - 1$ for $0 < i < 5m$. We have $r \geq 11$ (as $r - 1$ is a multiple of $5m$) and hence r divides $Q/(d,Q)$. Now it is easy to verify that in case (ii) the only subgroup of order divisible by r is $\overline{M} \cong PSU_6(q_0) \cdot \mathbb{Z}_{(2,q_0+1)}$ if m is even and $q = q_0^2$ (in fact, for $q > 2$ this is done in [7], Section 2.4). However, then

$$|\overline{M}| = q_0^{15}(q_0^2 - 1)(q_0^3 + 1)(q_0^4 - 1)(q_0^5 + 1)(q_0^6 - 1)/(3, q_0 + 1)$$

and it is not difficult to see that $|\overline{M}|$ is not divisible by $Q/(d,Q)$. As for the groups in case (iii), r does not divide $|PSL_3(q)| = q^3(q^2-1)(q^3-1)/(3,q-1)$ and the remaining groups have elements of order at most 24 whereas $Q/(d,Q) \geq 2^5-1 = 31$.

The lemma is proved. $\square$

2.1. We first assume that $q \neq 2,4$. Let $\omega \in GF(q^5)^*$ be of order Q and

$$f(t) = (t-\omega)(t-\omega^q)(t-\omega^{q^2})(t-\omega^{q^3})(t-\omega^{q^4}) = t^5 - \alpha t^4 + \beta t^3 - \gamma t^2 + \delta t - \varepsilon.$$

Then $f(t) \in F[t]$ and the polynomial $f(t)$ is irreducible over F. Note that $\varepsilon = \omega^{\frac{q^5-1}{q-1}}$ has order $q-1$ if $q \neq 3,7$, $\varepsilon = 1$ if $q = 3$, and $\varepsilon^3 = 1 \neq \varepsilon$ if $q = 7$.

Now let

$$x = \begin{pmatrix} -1 & 0 & 0 & \gamma\varepsilon^{-1} & 0 & \gamma \\ 0 & -1 & 0 & \beta\varepsilon^{-1} & 0 & \beta \\ 0 & 0 & 0 & \alpha\varepsilon^{-1} & -1 & \delta \\ 0 & 0 & 0 & 0 & 0 & \varepsilon \\ 0 & 0 & -1 & \delta\varepsilon^{-1} & 0 & \alpha \\ 0 & 0 & 0 & \varepsilon^{-1} & 0 & 0 \end{pmatrix}, \qquad y = \begin{pmatrix} 0&0&1&0&0&0 \\ 1&0&0&0&0&0 \\ 0&1&0&0&0&0 \\ 0&0&0&0&0&1 \\ 0&0&0&1&0&0 \\ 0&0&0&0&1&0 \end{pmatrix}.$$

Then x and y are elements of G of orders 2 and 3, respectively. Denote

$$z = xy = \begin{pmatrix} 0 & 0 & -1 & 0 & \gamma & \gamma\varepsilon^{-1} \\ -1 & 0 & 0 & 0 & \beta & \beta\varepsilon^{-1} \\ 0 & 0 & 0 & -1 & \delta & \alpha\varepsilon^{-1} \\ 0 & 0 & 0 & 0 & \varepsilon & 0 \\ 0 & -1 & 0 & 0 & \alpha & \delta\varepsilon^{-1} \\ 0 & 0 & 0 & 0 & 0 & \varepsilon^{-1} \end{pmatrix}.$$

Then the characteristic polynomial of z is $f_z(t) = (t-\varepsilon^{-1})f(t)$ and the characteristic roots ε^{-1}, ω, ω^q, ω^{q^2}, ω^{q^3}, ω^{q^4} of z are pairwise distinct. Then, in $GL_6(q^5)$, z is conjugate to $\mathrm{diag}(\varepsilon^{-1}, \omega, \omega^q, \omega^{q^2}, \omega^{q^3}, \omega^{q^4})$ and hence z is an element of G of order Q.

Let $H = \langle x, y\rangle$, $H \leq G$.

Lemma 2. *The group H acts irreducibly on the space V.*

P r o o f. Assume that W is an H-invariant subspace of V and $k = \dim W$, $1 \leq k \leq 5$.

Let first $k = 1$ and $0 \neq w \in W$. Then $y(w) = \lambda w$ where $\lambda \in F$ and $\lambda^3 = 1$. This yields

$$w = \mu_1(e_1 + \lambda^2 e_2 + \lambda e_3) + \mu_2(e_4 + \lambda^2 e_5 + \lambda e_6) \qquad (\mu_1,\ \mu_2 \in F).$$

Now $x(w) = \nu w$ where $\nu = \pm 1$. This yields consecutively $\mu_2 \neq 0$, $\lambda = \nu\varepsilon^{-1}$, $\mu_1 = \mu_2(\alpha + \nu\delta - \varepsilon^{-1})$, and

$$(1) \qquad (\nu + 1)(\alpha + \nu\delta - \beta\varepsilon - \varepsilon^{-1}) = 0,$$

$$(2) \qquad (\nu + 1)(\alpha + \nu\delta - \gamma\varepsilon^{-1} - \varepsilon^{-1}) = 0.$$

In particular, we have $\varepsilon^3 = \nu$ and $\varepsilon^6 = 1$. This is impossible if $q = 5$ or $q > 7$ since then ε has order $q - 1$. Thus $q = 3$ (and $\varepsilon = 1$) or $q = 7$ (and $\varepsilon^3 = 1 \neq \varepsilon$). So $\nu = 1$ and (1), (2) produce $\gamma = \beta\varepsilon^2$ and $\delta = -\alpha + \beta\varepsilon + \varepsilon^2$. Then $f(-1) = -(\beta + 1)(\varepsilon^2 + \varepsilon + 1) = 0$ both for $q = 3$ and $q = 7$, hence $\omega = -1$, an impossibility.

Now let $2 \leq k \leq 5$. Then the characteristic polynomial of $z|_W$ has degree k and must divide $f_z(t) = (t - \varepsilon^{-1})f(t)$. The irreducibility of $f(t)$ over F implies that this polynomial is $f(t)$ and $k = 5$. Now the subspace $U = \langle e_1,\ e_2,\ e_3,\ e_4,\ e_5\rangle$ of V is $\langle z\rangle$-invariant. If $W \neq U$ then $U \cap W$ is $\langle z\rangle$-invariant and $\dim(U \cap W) = 4$ which is impossible. Thus $W = U$ but obviously U is not $\langle y\rangle$-invariant, a contradiction.

The lemma is proved. (Note that the assertion is false for $q = 2$ or 4.) □

Now, in $\overline{G}$, the elements $\overline{x}$ and $\overline{y}$ have orders 2 and 3, respectively, and (as easily seen by the above-mentioned diagonal matrix) $\overline{z} = \overline{x} \cdot \overline{y}$ has order $Q/(d, Q)$. So the group $\overline{H} = \langle \overline{x}, \overline{y}\rangle$ has an element of order $Q/(d, Q)$ and $\overline{H}$ is irreducible on $P(V)$ as H is irreducible on V by Lemma 2. Then Lemma 1 implies that $\overline{H}$ cannot be contained in any maximal subgroup of $\overline{G}$. Thus $\overline{H} = \overline{G}$ and $\overline{G} = \langle \overline{x}, \overline{y}\rangle$ is a $(2, 3)$-generated group.

2.2. Let now $q = 2$ or 4. We keep the above element $y \in G$ of order three but this time choose the involution $x \in G$ to be

$$x = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & \eta & 0 & \eta^2 \\ 0 & 0 & 0 & \eta & 1 & \eta^2 \\ 0 & 0 & 0 & 0 & 0 & \eta \\ 0 & 0 & 1 & \eta & 0 & \eta^2 \\ 0 & 0 & 0 & \eta^2 & 0 & 0 \end{pmatrix},$$

where η is a generator of F^*. Now

$$z = xy = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & \eta^2 & \eta \\ 0 & 0 & 0 & 1 & \eta^2 & \eta \\ 0 & 0 & 0 & 0 & \eta & 0 \\ 0 & 1 & 0 & 0 & \eta^2 & \eta \\ 0 & 0 & 0 & 0 & 0 & \eta^2 \end{pmatrix}.$$

As in the proof of Lemma 2, one verifies that the group $H = \langle x, y\rangle$ acts irreducibly on the space V. Indeed, assume first that $W = \langle w\rangle$ is a one-dimensional H-invariant subspace of V. Then $y(w) = \lambda w$ ($\lambda \in F$, $\lambda^3 = 1$) yields again $w = \mu_1(e_1 + \lambda^2 e_2 + \lambda e_3) + \mu_2(e_4 + \lambda^2 e_5 + \lambda e_6)$ ($\mu_1, \mu_2 \in F$). Now $x(w) = w$ implies consecutively $\mu_2 \neq 0$, $\lambda = \eta^{-1}$, $\mu_1 = 0$, and $\eta = 0$, an impossibility. And if W is an H-invariant subspace with $2 \leq \dim W \leq 5$ then one reaches a contradiction just as in the proof of Lemma 2.

The characteristic polynomial of z is $f_z(t) = (t+\eta^2)g(t)$ where $g(t) = t^5 + \eta^2 t^4 + \eta^2 t^3 + \eta^2 t^2 + (\eta^2+\eta)t + \eta$. If $q = 2$ then the polynomial $g(t) = t^5+t^4+t^3+t^2+1$ is irreducible over F and hence its roots have order $2^5 - 1$ in $GF(2^5)^*$. Let $q = 4$, then $g(t) = t^5+\eta^2t^4+\eta^2t^3+\eta^2t^2+t+\eta$, and set $\overline{g}(t) = t^5+\eta t^4+\eta t^3+\eta t^2+t+\eta^2$. Now the polynomial $h(t) = g(t)\overline{g}(t) = t^{10} + t^9 + t^7 + t^6 + t^4 + t + 1$ is irreducible over $GF(2)$ and its roots have order $2^{10} - 1$ in $GF(2^{10})^*$ (see [6], Table C). It follows that both for $q = 2$ and $q = 4$ the element z has order $q^5 - 1 = Q$.

Now, in $\overline{G}$, the elements $\overline{x}$, $\overline{y}$, and $\overline{z}$ have orders 2, 3, and Q/d, respectively. So the group $\overline{H} = \langle \overline{x}, \overline{y}\rangle$ has an element of order Q/d and $\overline{H}$ is irreducible on $P(V)$. Again Lemma 1 implies that $\overline{H} = \overline{G}$ and $\overline{G} = \langle \overline{x}, \overline{y}\rangle$ is a (2, 3)-generated group.

This completes the proof of the theorem. □

REFERENCES

[1] J. Cohen. On non-Hurwitz groups and noncongruence of the modular group. *Glasgow Math. J.* **22** (1981), 1–7.

[2] L. Di Martino, N. A. Vavilov. (2,3)-generation of $SL(n, q)$. I. Cases $n = 5, 6, 7$. *Comm. Alg.* **22**, *4* (1994), 1321–1347.

[3] L. Di Martino, N. A. Vavilov. (2,3)-generation of $SL(n, q)$. II. Cases $n \geq 8$. *Comm. Alg.* **24**, *2* (1996), 487–515.

[4] D. Garbe. Über eine Klasse von arithmetisch definierbaren Normalteilern der Modulgruppe. *Math. Ann.* **235**, *3* (1978), 195–215.

[5] P. Kleidman. The Low-Dimensional Finite Simple Classical Groups and Their Subgroups. Ph. D. Thesis. Cambridge, 1987.

[6] R. Lidl, H. Niederreiter. Finite Fields. Encyclopedia of Mathematics and its Applications vol. **20**. Reading, Massachusetts etc., Addison-Wesley Company. Advanced Book Program, 1983.

[7] M. W. Liebeck, C. E. Praeger, J. Saxl. The Maximal Factorizations of the Finite Simple Groups and Their Automorphism Groups. *Mem. Amer. Math. Soc.* **86**, *432* (1990).

[8] A. M. Macbeath. Generators of the linear fractional group. *Proc. Symp. Pure Math.* **12** (1969), 14–32.

[9] P. Manolov, K. Tchakerian. (2,3)-generation of the groups $PSL_4(2^m)$. *Ann. Univ. Sofia, Fac. Math. Inf.* **96** (2004), 101–104.

[10] P. Sanchini, M. C. Tamburini. Constructive (2,3)-generation: a permutational approach. *Rend. Sem. Mat. Fis. Milano* **64** (1994), 141–158.

[11] A. Shalev. Asymptotic group theory. *Notices Amer. Math. Soc.* **48**, *4* (2001), 383–389.

[12] M. C. Tamburini, S. Vassallo. (2,3)-generazione di $SL_4(q)$ in caratteristica dispari e problemi collegati. *Boll. Un. Mat. Ital. B(7)* **8** (1994), 121–134.

[13] M. C. Tamburini, S. Vassallo. (2,3)-generazione di gruppi lineari. Scritti in onore di Giovanni Melzi. *Sci. Mat.* **11** (1994), 391–399.

[14] K. Tchakerian. (2,3)-generation of the groups $PSL_5(q)$. *Ann. Univ. Sofia, Fac. Math. Inf.* **97** (2005), 105–108.

Faculty of Mathematics and Informatics
"St. Kliment Ohridski" University of Sofia
5, J. Bourchier Blvd
1164 Sofia, Bulgaria
e-mail: ktabakov@fmi.uni-sofia.bg
kerope@fmi.uni-sofia.bg

Received April 25, 2012