ГОДИШНИК НА СОФИЙСКИЯ УНИВЕРСИТЕТ „СВ. КЛИМЕНТ ОХРИДСКИ"

ФАКУЛТЕТ ПО МАТЕМАТИКА И ИНФОРМАТИКА
Том 96

ANNUAIRE DE L'UNIVERSITE DE SOFIA „ST. KLIMENT OHRIDSKI"

FACULTE DE MATHEMATIQUES ET INFORMATIQUE
Tome 96

(2,3)-GENERATION OF THE GROUPS $\mathrm{PSL}_4(2^m)$

PETAR MANOLOV, KEROPE TCHAKERIAN

We prove that the group $\mathrm{PSL}_4(2^m)$, $m > 1$, is (2,3)-generated.

Keywords: (2,3)-generated group
2000 MSC: main 20F05, secondary 20D06

1. INTRODUCTION

A group G is said to be (2,3)-generated if $G = \langle x, y \rangle$ for some elements x and y of orders 2 and 3, respectively. So far, (2,3)-generation has been proved for a number of series of finite simple groups, for example A_n, $n \neq 6, 7, 8$ (see [2]), $\mathrm{PSL}_2(q)$, $q \neq 9$ [3], $\mathrm{PSL}_3(q)$, $q \neq 4$ (see [1]), and $\mathrm{PSL}_4(q)$, q odd [5]. In a note added in proof to [5], the authors mention that they have recently proved (2,3)-generation for $\mathrm{PSL}_4(q)$ also in the case of even $q > 2$. As we have not been able to find a proof in the literature and as our approach seems to be quite different from that of the authors of [5], here we give a short proof of this fact. Thus we prove the following

Theorem. *The group* $\mathrm{PSL}_4(2^m)$ *is (2,3)-generated for any* $m > 1$.

2. PROOF OF THE THEOREM

Let $G = \mathrm{SL}_4(q) = \mathrm{PSL}_4(q)$, where $q = 2^m$. It is well-known that the group $\mathrm{PSL}_4(2) \cong \mathrm{A}_8$ is not (2,3)-generated, so we assume $m > 1$ in what follows.

The group G acts naturally on a four-dimensional vector space V over the field $\mathrm{GF}(q)$ with a fixed basis e_1, e_2, e_3, e_4. Let ω be a generator of the group $\mathrm{GF}(q^3)^*$ and $\alpha = \omega + \omega^q + \omega^{q^2}$, $\beta = \omega^{1+q} + \omega^{q+q^2} + \omega^{q^2+1}$, $\gamma = \omega^{1+q+q^2}$. Then α, β, $\gamma \in \mathrm{GF}(q)$ and γ has order $q-1$ in the group $\mathrm{GF}(q)^*$, in particular $\gamma \neq 1$ as $q > 2$. The polynomial

$$f(t) = (t+\omega)(t+\omega^q)(t+\omega^{q^2}) = t^3 + \alpha t^2 + \beta t + \gamma$$

is irreducible over $\mathrm{GF}(q)$.

Now, the matrices

$$x = \begin{pmatrix} 0 & \alpha\gamma^{-1} & 1 & \beta \\ 0 & 0 & 0 & \gamma \\ 1 & \beta\gamma^{-1} & 0 & \alpha \\ 0 & \gamma^{-1} & 0 & 0 \end{pmatrix} \quad \text{and} \quad y = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

are elements of G of orders 2 and 3, respectively. Let

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

The characteristic polynomial of z is $(t+\gamma^{-1})f(t)$ and the characteristic roots γ^{-1}, ω, ω^q, ω^{q^2} of z are pairwise distinct. Then, in $\mathrm{GL}_4(q^3)$, z is conjugate to $\mathrm{diag}\,(\gamma^{-1}, \omega, \omega^q, \omega^{q^2})$ and hence z is an element of G of order q^3-1.

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

Lemma 2.1. *The group H acts irreducibly on the space V.*

Proof. Assume that W is a non-trivial H-invariant subspace of V. Let first $\dim W = 1$ and $W = \langle w\rangle$, $w \neq 0$. Then $x(w) = w$, which yields $w = \mu e_1 + \nu e_2 + (\mu + \gamma^{-1}(\alpha+\beta)\nu)e_3 + \gamma^{-1}\nu e_4$, μ, $\nu \in \mathrm{GF}(q)$, $\mu \neq 0$ or $\nu \neq 0$. Now $y(w) = \lambda w$, $\lambda \in \mathrm{GF}(q)$, $\lambda^3 = 1$, which produces consecutively $\nu \neq 0$, $\lambda = \gamma^{-1} \neq 1$, whence $\gamma^2+\gamma+1 = 0$, $\mu = 0$, and $\alpha+\beta = \gamma^2$. This yields $f(1) = 1+\alpha+\beta+\gamma = \gamma^2+\gamma+1 = 0$, an impossibility as $f(t)$ is irreducible over $\mathrm{GF}(q)$.

Let $\dim W = 2$. Then the characteristic polynomial of $z_{|W}$ has degree two and must divide the polynomial $(t+\gamma^{-1})f(t)$, again contradicting the irreducibility of $f(t)$.

Lastly, let $\dim W = 3$. The subspace $U = \langle e_1, e_2, e_3\rangle$ of V is $\langle z\rangle$-invariant. Suppose that $W \neq U$. Then $U \cap W$ is a 2-dimensional $\langle z\rangle$-invariant subspace of V, which (as shown above) is impossible. Thus $W = U$, but obviously U is not $\langle x\rangle$-invariant, a contradiction. The lemma is proved. □

Lemma 2.2. *Let M be a maximal subgroup of G having an element of order*

$q^3 - 1$. *Then M is the stabilizer of a subspace W of V with* $\dim W = 1$ *or* 3.

Proof. Suppose false. Then the list of maximal subgroups of G [4] implies that one of the following holds:

1) $|M| = q^6(q-1)^3(q+1)^2$.
2) $|M| = 24(q-1)^3$ if $q > 4$.
3) $|M| = 2q^2(q-1)^3(q+1)^2$.
4) $|M| = 2q^2(q-1)(q+1)^2(q^2+1)$.
5) $M \cong \mathrm{SL}_4(q_0)$ if $q = q_0^r$ and r is a prime, $|M| = q_0^6(q_0-1)^3(q_0+1)^2(q_0^2+1)(q_0^2+q_0+1)$.
6) $M \cong \mathrm{Sp}_4(q)$, $|M| = q^4(q-1)^2(q+1)^2(q^2+1)$.
7) $M \cong \mathrm{SU}_4(q_0)$ if $q = q_0^2$, $|M| = q_0^6(q_0-1)^2(q_0+1)^3(q_0^2+1)(q_0^2-q_0+1)$.

As q^3-1 divides $|M|$ and as $\big(q^2+q+1, 2(q+1)(q^2+1)\big) = 1$, in cases 1), 2), 3), 4), 6) it follows that q^2+q+1 divides $(q-1)^2$, $3(q-1)^2$, $(q-1)^2$, 1, $q-1$, respectively. This is easily seen to be impossible. Similarly, in case 7) it follows that $q_0^2+q_0+1$ divides q_0-1. In case 5), if $r > 2$, then $\big(q^3-1, 2(q_0+1)(q_0^2+1)\big) = 1$ and hence q^3-1 divides $(q_0-1)^3(q_0^2+q_0+1)$. This is impossible as $(q_0-1)^3(q_0^2+q_0+1) < q_0^6 - 1 < q_0^{3r} - 1 = q^3 - 1$. Lastly, in case 5) and $r = 2$, as $\big(q_0^2 - q_0 + 1, 2(q_0-1)(q_0^2+1)\big) = 1$, it follows that $q_0^2 - q_0 + 1$ divides $q_0 + 1$, which yields $q_0 = 2$ and $q = 4$. However, then $M \cong \mathrm{SL}_4(2) \cong \mathrm{A}_8$ has no element of order $4^3 - 1 = 63$, a contradiction. The lemma is proved. □

We can now complete the proof of the theorem. Assume that $H \neq G$. Let M be a maximal subgroup of G containing H. As M has an element z of order q^3-1, Lemma 2.2 implies that M is the stabilizer of a subspace W of V with $\dim W = 1$ or 3. But then W is H-invariant, which contradicts Lemma 2.1. Thus $H = G$ and $G = \langle x, y\rangle$ is a (2,3)-generated group.

REFERENCES

1. Cohen, J. On non-Hurwitz groups and noncongruence of the modular group. *Glasgow Math. J.*, **22**, 1981, 1–7.
2. Dey, I. M. S., J. Wiegold. Generators for alternating and symmetric groups. *J. Austr. Math. Soc.*, **12**, 1971, 63–68.
3. Macbeath, A. M. Generators of the linear fractional groups. *Proc. Symp. Pure Math.*, **12**, 1969, 14–32.
4. Mwene, B. On the subgroups of the group $\mathrm{PSL}_4(2^m)$. *J. Algebra*, **41**, 1976, 79–107.

5. Tamburini, M. C., S. Vassallo. (2,3)-generazione di $SL_4(q)$ in caratteristica dispari e problemi collegati. *Boll. U. M. I.*, **(7) 8-B**, 1994, 121–134.

Received on January 15, 2003

Faculty of Mathematics and Informatics
"St. Kl. Ohridski" University of Sofia
5, J. Bourchier blvd., 1164 Sofia
BULGARIA
E-mail: kerope@fmi.uni-sofia.bg