PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 127, Number 7, Pages 1973–1974
S 0002-9939(99)04818-2
Article electronically published on March 16, 1999

ON PERMUTATION REPRESENTATIONS OF POLYHEDRAL GROUPS

B. SURY

(Communicated by Ronald M. Solomon)

ABSTRACT. We answer affirmatively the following question of Derek Holt: Given integers $l, m, n \geq 2$, can one, in a simple manner, find a finite set Ω and permutations a, b such that a has order l, b has order m and ab has order n? The method of proof enables us to prove more general results (Theorems 2 and 3).

INTRODUCTION

Our purpose is to prove some results on representations of certain polyhedral groups. In particular, we answer affirmatively the question mentioned above. Our proof is short and elementary and has enough freedom to prove more general results.

We start with a simple observation.

Let K be any field. If $A, B \in SL_2(K)$ have the same trace $\neq \pm 2$, then they have the same order. This follows from the fact that A and B have the same characteristic polynomial and, hence, the same eigenvalues λ, λ^{-1}. Since these eigenvalues are necessarily distinct, A and B are conjugate in GL_2 over an algebraic closure of K. Let us start with $l, m, n \geq 2$. Let K be any field containing a primitive $2lmn$-th root of unity. We could take $K = \mathbb{C}$ or we could let $K = \mathbb{F}_p$ with p a prime $\equiv 1$ modulo $2lmn$. Consider $G = PSL_2(K)$. Let $\lambda \in K^*$ be a primitive $2l$-th root of unity. Note that since $2l \geq 4$, one has $\lambda \neq \lambda^{-1}$ so that the matrix $\begin{pmatrix} \lambda & 0 \\ \alpha & \lambda^{-1} \end{pmatrix} \in SL_2(K)$ has order $2l$, for any arbitrary $\alpha \in K$. In particular, $A = \begin{pmatrix} \lambda & 0 \\ 1 & \lambda^{-1} \end{pmatrix}$ has order $2l$ in $SL_2(K)$. Similarly, there exists $\mu \in K^*$ of order $2m \geq 4$; so $B = \begin{pmatrix} \mu & t \\ 0 & \mu^{-1} \end{pmatrix} \in SL_2(K)$ has order $2m$ for any t in K. Now, $AB = \begin{pmatrix} \lambda\mu & t\lambda \\ \mu & t + \lambda^{-1}\mu^{-1} \end{pmatrix}$. Look at its trace $\lambda\mu + \lambda^{-1}\mu^{-1} + t$. One can obtain any given element θ of K as trace(AB) by solving for $t \in K$. Choosing θ to be the trace of an element of order $2n \geq 4$ in $SL_2(K)$, we have got hold of A and B in $SL_2(K)$ such that AB has order $2n$ in $SL_2(K)$. Evidently, the images of A, B and AB in $G = PSL_2(K)$ have orders l, m, n respectively. Letting $K = \mathbb{F}_p$ with $p \equiv 1 \bmod 2lmn$, and embedding $PSL_2(\mathbb{F}_p)$ in a finite symmetric group, we have proved:

Received by the editors October 15, 1997.
1991 *Mathematics Subject Classification.* Primary 20B05.
Key words and phrases. Permutation representations, triangle groups.

©1999 American Mathematical Society

Theorem 1. *Given integers $l, m, n \geq 2$, there are a finite set Ω and permutations a, b such that a, b, ab have orders l, m, n respectively.*

As a matter of fact, the method has freedom enough to prove the following result:

Theorem 2. *Let $l, m, n \geq 2$. Then, there are a finite field $\mathbb{F}_q$ and elements $A, B \in PSL_2(\mathbb{F}_q)$ of orders l, m such that a given cyclically reduced word $W(A, B)$ involving both A and B has order n.*

Proof. Note that W can be taken to be of the form $A^{r_1}B^{s_1}\cdots A^{r_k}B^{s_k}$ with $0 < r_i < l$ and $0 < s_i < m$. We proceed as before by starting with a prime $p \equiv 1 \bmod 2lmn$. Once again, we choose $A = \begin{pmatrix} \lambda & 0 \\ 1 & \lambda^{-1} \end{pmatrix}$ of order $2l$ in $SL_2(K)$, and $B = \begin{pmatrix} \mu & t \\ 0 & \mu^{-1} \end{pmatrix}$ which is of order $2m \in SL_2(K)$ for any t in K. Let us write $L(d) = \frac{\lambda^d - \lambda^{-d}}{\lambda - \lambda^{-1}}$ and $M(d) = \frac{\mu^d - \mu^{-d}}{\mu - \mu^{-1}}$ for any $d > 0$. Then, an easy calculation shows that

$$Trace(A^{r_1}B^{s_1}\cdots A^{r_k}B^{s_k}) = L(r_1)\cdots L(r_k)M(s_1)\cdots M(s_k)t^k + \; O(t^{k-1})$$

where we have denoted by $O(t^d)$ a polynomial of degree at most d over $\mathbb{F}_p$. Thus, trace $W(A, B)$ is a nonconstant polynomial in t over $\mathbb{F}_p$ since $M(s_i) \neq 0 \neq L(r_j)$ as $\mu^{2s_i} \neq 1 \neq \lambda^{2r_j}$. We choose any root of this polynomial in $\overline{\mathbb{F}_p}$. Then, λ, μ, t lie in a finite field $\mathbb{F}_q$ and $A, B, W(A, B)$ have orders l, m, n respectively in $PSL_2(\mathbb{F}_q)$.

Remarks. (i) To prove our results, we work with $K = \mathbb{F}_p$ or $\overline{\mathbb{F}_p}$ to guarantee that the group generated by A and B is finite. If we work with $\mathbb{C}$ for instance, the finite subgroups of $PSL_2(\mathbb{C})$ with the presentation

$$\langle A, B \mid A^l = B^m = (AB)^n = 1\rangle$$

are exactly for $(l, m, n) = (2, 3, 3)$, $(2, 3, 4)$, $(2, 3, 5)$, $(2, 2, n)$ and the cyclic groups.

(ii) The reason one works with PSL_2 instead of with SL_2 is that one could work with matrices of orders at least 4 in $SL_2(K)$ and these are semisimple.

It is easily seen that the method proves the following result:

Theorem 3. *Let $G = \langle a, b \mid a^l = b^m = w(a, b)^n = 1\rangle$ where $l, m, n \geq 2$ and $w(a, b)$ is any word $a^{r_1}b^{s_1}\cdots a^{r_k}b^{s_k}$ with $0 < r_i < l, 0 < s_i < m$. Then, there is a homomorphism ϕ from G to $PSL_2(\mathbb{C})$ such that $\phi(a), \phi(b), \phi(w)$ have orders l, m, n.*

Acknowledgements

I would like to thank Prof. Ron Solomon as well as the referee for their comments. In particular, they drew attention to the old paper ([M]) of G.A.Miller on the subject.

References

[D] Derek Holt, Problem 22 of the Problems Book, Group Pub Forum Home Page, group-pub-forum at maths.bath.ac.uk

[M] G.A.Miller, *'Groups defined by the orders of two generators and the order of their product'*, Amer.J.Math. 24 (1902), 96-100.

School Of Mathematics, Tata Institute of Fundamental Research, Homi Bhabha Road, Bombay 400 005, India

E-mail address: `sury@math.tifr.res.in`