DEMONSTRATIO MATHEMATICA
Vol. XXIV No 1-2 1991

Elżbieta Ambrosiewicz

POWERS OF SETS OF INVOLUTION IN LINEAR GROUPS

In paper [1] it was proved that $K_2 K_2 \neq GL(2,K)$ if char $K \neq 2$ and that $K_2 K_2 \neq PSL(2,K)$ if char $K \neq 2$ and the element -1 is not a square, where K_2 denotes a set of all involutions of a group. In this paper we will prove that $(K_2 K_2)^2 = SL^*(2,K)$ where $SL^*(2,K)$ denotes the subgroup of all matrices with determinant ± 1 and that $(K_2 K_2)^2 = PSL(2,q)$ where q is odd and $q \geq 5$. We will also prove that $PSL(2,2^m) = C_2^4 (m>1)$ where C_2 denotes the conjugacy class of involution $[0,1;1,0]$.

Theorem 1. If char $K \neq 2$ then $(K_2 K_2)^2 = SL^*(2,K)$ in the group $GL(2,K)$.

Proof. We will use the next two lemmas.

Lemma 1. (see [1]). Let G be a group. An element $g \in G$ belongs to $K_2^m (m \geq 2)$ if and only if there is an element $t \in K_2^{m-1}$, $t \neq g^{-1}$ such that $(gt)^2 = 1$.

Lemma 2. If M is a non-empty subset of the group G, $M = M^{-1}$ and $x M \cap M \neq \emptyset$ for each $x \in G$, then $MM = G$.

The proof of Lemma 2 is obvious. From Lemma 2 there results a remark.

Remark. If M is a subset of a finite group G such that $M = M^{-1}$ and $|M| > \frac{1}{2}|G|$ then $MM = G$.

If $A \in K_2 K_2$ then $\det A = \pm 1$ by Lemma 1. From [2] (Corollary 4.7, p.360) we know that each matrix in the group $GL(2,K)$ is silimar to $[a,0;0,a]$ $(a \neq 0)$ or to $[0,1;a_1,a_2]$. Hence we can restrict our investigations of the set $K_2 K_2$ to the matrices $[a,0;0,a]$ $(a=\pm 1)$ and $[0,1;a_1,a_2]$ with $a_1 = \pm 1$.

We have $T^{-1}N_i\, T=N_i^{-1}$ $(i=1,2)$ where $N_1=[a,0;0,a]$, $N_2=[0,1;-1,a_2]$ $T=[0,1;1,0]$, $T^2=E$, $T \neq N_i\,(i=1,2)$. Therefore $N_1, N_2 \in K_2K_2$. If $a_2 \neq 0$ and char $K \neq 2$, then $N=[0,1;1,a_2] \notin K_2K_2$, which one can easily verify. If $a_2=0$ then $N \in K_2K_2$, because the matrices $N_3=[0,1;1,0]$, $T=[0,-1;-1,0]$ fulfil all the conditions of Lemma 1. Therefore we have $K_2K_2=SL(2,K) \cup \{[0,1;1,0]^A, A \in GL(2,K)\} \subseteq SL^*(2,K)$. The set K_2K_2 fulfils all the conditions of Lemma 2. Naturally $(K_2K_2)^{-1}= K_2K_2$. If the second condition of Lemma 2 is not fulfilled, then exists an element $x_0 \in SL^*(2,K)$ such that for each $A \in K_2K_2$, $x_0A = A_1 \notin K_2K_2$ and $\det A_1= -1$. Thus $\det A = \det A_1 \det x_0^{-1}= -\det x_0^{-1}$, which contradicts with the construction of set K_2K_2. Therefore $(K_2K_2)^2 = SL^*(2,K)$. Since $GL(2,3)=SL^*(2,3)$ so $(K_2K_2)^2= GL(2,3)$.

Theorem 2. If $q \geq 5$ (q-odd) then $(K_2K_2)^2=PSL(2,q)$.

Proof. For $q=5$ we have $K_2K_2=PSL(2,5)$ (see[1]). Let us observe that a matrix T has the order two iff $T=[x,y;-y^{-1}(1+x^2),-x]$ or $T=[-x,-y;y^{-1}(1+x^2),x]$. A matrix $A=[a_{11},a_{12};a_{21},a_{22}]$ belongs to $K_2K_2 \subseteq PSL(2,q)$ iff

$$TA = A^{-1}T \quad \text{and } A \neq T \in K_2 \tag{1}$$

by Lemma 1.

The condition $TA=A^{-1}.T$ is equivalent to the equation

(2) $$a_{21}y^2 + yx(a_{11} - a_{22}) - a_{12}(1+x^2) = 0.$$

The solvability of the equation (2) is equivalent to the solvability of the equation

(3) $$x^2[(a_{11}+a_{22})^2-4]-u^2 = 4(1-a_{11}\,a_{22})$$

with unknowns x,u.

If $a_{11}+a_{22}\neq \pm 2$, then the equation (3) over the field K with char $K\neq 2$ has a solutions (see[3] p.46). Hence in this case there exists a matrix T such that $T^{-1}AT=A^{-1}$. But if $a_{11}+a_{22}= 0$, then the case T=A is possible.

If $a_{11}+a_{22}= \pm 2$, then the equation (3) may not have a solution and thus the matrix T may not exist. Therefore, in the case $a_{11}+a_{22}\neq \pm 2,0$ there exists T such that $T^{-1}AT=A^{-1}$ and $A\neq T\in K_2$. All the matrices M with $a_{11}+a_{22}\neq \pm 2,0$ belong to K_2K_2. It is evident that $|M| > \frac{1}{2}\,|PSL(2,q)|$ for $q\geq 7$. Naturally, $M=M^{-1}$. Therefore MM=PSL(2,q) for $q\geq 7$ by the Remark. Since $M\leq K_2K_2$ so we have $PSL(2,q)=(K_2K_2)^2$ for q=7. In the paper [1] there has been proved that $K_2K_2=PSL(2,2^m)$ (m>1). Now we will give another result.

Theorem 3. If m>1 then $PSL(2,2^m)=C_2^4$, where C_2 denotes the conjugacy class of the matrix [0,1;1,0].

Proof. Since each noncentral matrix is similar to [0,1;1,s] in the group $PSL(2,2^m)$ and the equation $x^2= a$ has a solution in the field $GF(2^m)$, so we have

(4) $$\begin{bmatrix}0 & 1\\ 1 & s\end{bmatrix} = X^{-1}\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix} XY \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix} Y^{-1}$$

where

$$X = \begin{bmatrix} \sqrt{s^{-1}}, & 0 \\ \sqrt{s^{-1}}, & s\sqrt{s^{-1}} \end{bmatrix} \quad Y = \begin{bmatrix} 1 & s \\ 0 & 1 \end{bmatrix}, \quad s \neq 0.$$

We have also

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

From the last identity and from (4) there results $M = PSL(2,2^m) - C_2 \subseteq C_2C_2$. For $m>1$, $|M| > \frac{1}{2}|PSL(2,2^m)|$. We also have $M^{-1} = M$. Thus $MM = PSL(2,2^m)$ by the Remark. Since $M \subseteq C_2C_2$ so we have $PSL(2,2^m) = C_2^4$ for $m>1$. This ends the proof of Theorem 3.

REFERENCES

[1] **J. Ambrosiewicz:** On the square of sets of linear groups, Rend. Sem. Mat. Univ., Padova, 75(1985) 253-256.

[2] **T. W. Hungerford:** Algebra, Springer-Verlag, New York, Heidelberg, Berlin 1974.

[3] **L. E. Dickson:** Linear groups. Berlin, Teubner, reprinted Dover. 1958.

INSTITUTE OF MATHEMATICS, UNIVERSITY OF WARSAW,
BIALYSTOK BRANCH, 15-267 BIALYSTOK, POLAND

Received December 8, 1989; revised version July 20, 1990.