DEMONSTRATIO MATHEMATICA
Vol. XXIII No 2 1990

Jan Ambrosiewicz

POWERS OF SETS IN LINEAR GROUPS

It has been proved in the paper [1] that the set K_2^2 is not a subgroup of groups: $GL(n,F)$, $SL(n,F)$, $PSL(n,F)$ for $n>2$, where $K_2 = \{g \in G: o(g) = 2\}$. In the present paper we will prove: 1^o $SL(n,F) = K_2^4$ for $2<n<|F|-1$, 2^o $GL_1(n,F) = K_2^4$ for $n<|F|-1$, where $GL_1(n,F)$ denotes the group of all n by n matrices of determinant ± 1, 3^o $SL(n,F) = C_V^4$ for $n<|F|-1$, where C_V denotes the conjugacy class of the matrix $V = diag(v_1,\dots,v_n)$, $v_i \neq v_j$ for $i \neq j$, 4^o $PSL(n,F) = C_V^2 = K_2^4$ for $n<|F|-1$ (the result $PSL(n,F) = C_V^2$ was proved in [3] on another way), 5^o $SL(3,F) = K_2^4$, 6^o $PSL(n,F) = K_2^4$, 7^o $GL_1(n,F) = K_2^4$. We will give also condition under which $SL(n,F) = C_V^2$ (see the question stated in [3], p.66).

Throughout this paper E' will denote the matrix $\begin{bmatrix} 0 & & 1 \\ & \cdot^{\cdot^{\cdot}} & \\ 1 & & 0 \end{bmatrix} \in M_{n\times n}$.

We will use the following lemmas.

Lemma 1 (see [1]). Let G be a group. An element $g \in K_2^2$ if end only if there is an element $x \in K_2$, $x \neq g^{-1}$ such that $(gx)^2 = 1$.

Lemma 2 (see [2]). If M is a non-empty subset of $G, M = M^{-1}$ and $xM \cap M \neq 0$ for each $x \in G$, then $M^2 = G$.

Lemma 3. Let $V = diag(v_1,\dots,v_n)$, $W = diag(w_1,\dots,w_n)$, $v_i \neq v_j$, $w_i \neq w_j$ for $i \neq j$. If $\det A = \det V \det W, A \notin Z(GL(n,F))$ and A has a rational canonical form then there are matrices $X,Y \in GL(n,F)$ with arbitrary chosen det X, det $Y \in F^*$ such that

(1) $$A = (X^{-1}V\,X)(Y^{-1}W\,Y).$$

The proof of Lemma 3, for $n = 3$ has been given in [2]. Using the same method one can prove Lemma 3 for any $n \geq 2$, (see [6]).

Lemma 4. Let $V = \mathrm{diag}(v_1,\dots,v_n)$, $v_i \neq v_j$ for $i \neq j$. Let $v_n = 1$, $v_{2i-1}v_{2i} = 1$ for $i = 1,\dots,\frac{n-1}{2}$ if n is odd. Let $v_{2i-1}v_{2i} = 1$ for $i = 1,\dots,\frac{n}{2}$ if n is even. Then there exists $T \in SL(n,F)$ such that

(2) $$V\,T^{-1}V\,T = E,\ T^2 = E \text{ for } n > 2 \text{ and } T^2 = -E \text{ for } n = 2,\ T \neq V^{-1},$$

(3) $$xE \in C_V C_{xV} \quad \text{for} \quad x \in F^{*},$$

(4) $$\text{If } n > 2, \text{ then } \quad C_{xV} \subseteq K_2^2 \quad \text{iff} \quad x_2 = 1.$$

Proof. If n is odd, we put $T = \mathrm{diag}\left(L_1,\dots,L_{\frac{n-1}{2}}, L_{\frac{n+1}{2}}\right)$, $L_i = E_2'$, $i = 1,\dots,\frac{n-1}{2}$, $L_{\frac{n+1}{2}} = [\pm 1]$ where we take $+1$ when $\frac{n-1}{2}$ is even and -1 when $\frac{n-1}{2}$ is odd; if n is even, we put $T = \mathrm{diag}(L_1,\dots,L_{\frac{n}{2}})$, $L_i = E_2'$, $i = 1,\dots,\frac{n}{2}$ when $n > 2$ and $T = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ when $n = 2$.

The relations (2) can be easy verified by direct computations. The relations (3) follows immediately from (2). By Lemma 1, $xV \in K_2^2$ iff there exists $T \in K_2$ such that $T^{-1} \neq xV$ and $T^{-1}(xV)T = x^{-1}V^{-1}$. But by (2) and by $x^2 = 1$ these relations hold for $n > 2$. The inclusion $C_{xV} \subseteq K_2^2$ results from the fact that K_2^2 is a normal subset.

Lemma 5. Let $V = \mathrm{diag}(v_1,\dots,v_n)$, $v_i \neq v_j$ for $i \neq j$. If n is odd, we put $v_n = \pm 1$, $v_{2i-1}v_{2i} = 1$ for $i = 1,\dots,\frac{n-1}{2}$; if n is even, we put (i) $v_{2i-1}v_{2i} = 1$ for $i = 1,\dots,\frac{n}{2}$ or (ii) $v_1 = 1$, $v_2 = -1$, $v_{2i-1}v_{2i} = 1$ for $i = 2,\dots,\frac{n}{2}$. Then there exists a matrix T such that

(5) $$VT^{-1}VT = E,\ T^2 = E,\ T \neq V^{-1},\ \det T = \pm 1,$$

(6) $$xE \in C_V C_V \quad \text{for} \quad x \in F^*,$$

(7) $$C_{xV} \subseteq K_2^2 \quad GL_1(n,F) \quad \text{iff } x^2 = 1.$$

Proof. If n is odd, we put $T = \operatorname{diag}(L_1,\dots,L_{\frac{n-1}{2}},L_{\frac{n+1}{2}})$, $L_i = E_2'$, $i = 1,\dots,\frac{n-1}{2}$, $L_{\frac{n+1}{2}} = 1$; if n is even, we put $T = \operatorname{diag}(L_1,\dots,L_{\frac{n}{2}})$, $L_i = E_2'$, $i = 1,\dots,\frac{n}{2}$ in the case (i) and $T = \operatorname{diag}(L_1,\dots,L_{\frac{n}{2}})$, $L_1 = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$, $L_i = E_2'$, $i = 2,\dots,\frac{n}{2}$ in the case (ii). By direct computation it is easy to verify the relations (5). The relation (6) follows from (5). The condition (7) holds by relations $T^{-1} \neq xV$, $T^{-1}(xV)T = x^{-1}V^{-1}$, $T \in K_2$ and by Lemma 1.

Lemma 6. $Z(SL(n,F)) \subseteq K_2^4$ except for $n = 2$ and char $F \neq 2$.

Proof. Let $a^n = 1$. In the proof we will distinguish two cases: (i) n is even, (ii) n is odd. If $n = 2k > 2$, then we put

$$A = \operatorname{diag}(a^2,a^4,\dots,a^{2k},a^2,a^4,\dots,a^{2k}),$$

$$B = \operatorname{diag}(a^{2k-1},a^{2k-3},\dots,a,a^{2k-1},a^{2k-3},\dots,a),$$

$S = \operatorname{diag}(E_{k-1}',-1,E_{k-1}',-1)$, $R = \operatorname{diag}(E_k',E_k')$. One can verify that the following relations $A,B,S,R \in SL(n,F)$; $aE = AB$; $S^{-1}A\,S = A^{-1}$; $R^{-1}B\,R = B^{-1}$; $S^2 = R^2 = E$; $S^{-1} \neq A$; $R^{-1} \neq B$ hold. Hence $A,B \in K_2^2$ by Lemma 1. Therefore $aE = AB \in K_2^4$. If $n = 2$, char $F = 2$ then obviously $Z(SL(n,F)) = \{E\} \subseteq K_2^2$. If $n = 2$, char $F \neq 2$ then $Z(SL(n,F)) = \{E,-E\} \not\subseteq K_2^4 = \{E\}$, (see [1]).

If n is odd, then we put $A = \operatorname{diag}(a^n,a^{n-1},\dots,a)$, $B = \operatorname{diag}(a,a^2,\dots,a^{n-1},a^n)$, $M = \operatorname{diag}(r,E_{n-1}')$, $N = \operatorname{diag}(E_{n-1}',r)$

where $r \in \{1,-1\}$. It is easy to see that we can choose r such that $M,N \in SL(n,F)$. One can verify that the following relations: $A,B \in$ $\in SL(n,F)$; $AB = aE$; $M^{-1}A\,M = A^{-1}$; $N^{-1}B\,N = B^{-1}$; $M^2 = N^2 = E$; $M^{-1} \neq A$; $N^{-1} \neq B$; $M,N \in SL(n,F)$ hold for suitable $r \in \{1,-1\}$. Hence by Lemma 1 $A,B \in K_2^2$, so $aE = AB \in K_2^4$. Therefore $Z(SL(n,F)) \subseteq K_2^4$.

Lemma 7. $Z(GL_1(n,F)) \subseteq K_2^4$.

Proof. If $aE \in Z(GL_1(n,F))$ and $a^n = 1$, $n > 2$ then Lemma 7 is true by Lemma 6. If $n = 2$, $a^2 = 1$ then Lemma 7 is true by the identity $E_2'(-E_2)E_2' = -E_2$ and by Lemma 1 and by the fact that $E_2 \in K_2^4$.

Let $a^n = -1$. We will consider four cases: (i) $n = 2k$; k - even; (ii) $n = 2k$, $k>1$, k - odd; (iii) $n = 2$; (iv) n - odd.

If $n = 2k$, k - even, then we put $A = \mathrm{diag}(a^2,-a^4,\dots,-a^{2k},-a^2,$ $a^4,-a^6,\dots,a^{2k})$, $B = \mathrm{diag}(-a^{2k-1},a^{2k-3},\dots,a,a^{2k-1},-a^{2k-3},\dots,-a)$, $S = \mathrm{diag}(E_{2k-1}',1)$, $R = \mathrm{diag}(E_k',E_k')$. The following relations are easily checked: $AB = aE$, $S^{-1}A\,S = A^{-1}$, $R^{-1}B\,R = B^{-1}$, $S^2 = R^2 = E$, $S^{-1} \neq A$, $R^{-1} \neq B$ hold. Hence by Lemma 1 we have $A,B \in K_2^2$. Therefore $aE = AB \in K_2^4$. If $n = 2k$, k - odd, $k>1$, we put $A =$ $= \mathrm{diag}(a^2,-a^4,\dots,a^{2k},-a^2,a^4,\dots,-a^{2k})$, $B = \mathrm{diag}(-a^{2k-1},a^{2k-3},\dots$ $\dots,-a,a^{2k-1},-a^{2k-3},\dots,a)$, $S = \mathrm{diag}(E_{k-1}',1,E_{k-1}',1)$, $R = E_{2k}'$. One can easy verify the following relations: $AB = aE$, $S^{-1}A\,S = A^{-1}$, $R^{-1}B\,R = B^{-1}$, $S^2 = R^2 = E$, $S^{-1} \neq A$, $R^{-1} \neq B$. Hence $A,B \in K_2^2$ by Lemma 1, so $aE = AB \in K_2^4$. If $n = 2$, then Lemma 7 follows from the following identities

$$\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}\begin{bmatrix}a & 0\\ 0 & -a\end{bmatrix} = aE, \quad \begin{bmatrix}-1 & 0\\ 0 & 1\end{bmatrix}\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}\begin{bmatrix}-1 & 0\\ 0 & 1\end{bmatrix} = \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}^{-1}$$

$$\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\begin{bmatrix}a & 0\\ 0 & -a\end{bmatrix}\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix} = \begin{bmatrix}a & 0\\ 0 & -a\end{bmatrix}^{-1}$$

and by Lemma 1. If n is odd and $a^n = -1$, then Lemma 7 is true by the equation $(-a)^n = 1$ and by Lemma 6.

Theorem 1. If $V = \mathrm{diag}(v_1,\dots,v_n)$, $W = \mathrm{diag}(w_1,\dots,w_n)$, $v_i \neq v_j$, $w_i \neq w_j$ for $i \neq j$ and $V,W \in SL(n,F)$, then $SL(n,F) = C_V C_W \cup Z(SL(n,F))$.

Proof. Let $B \in SL(n,F) - Z(SL(n,F))$. By Corollary 4.7 p.360 of [5] there exists $S \in GL(n,F)$ such that $S^{-1}B\,S = A \in SL(n,F)$ has a rational canonical form. It is clear that $\det B = \det V \det W$, so by Lemma 3, $S^{-1}B\,S = A = (X^{-1}V\,X)(Y^{-1}W\,Y)$ or

$$(8)\qquad B = \left[(XS^{-1})^{-1}V(XS^{-1})\right]\cdot\left[(YS^{-1})^{-1}W(YS^{-1})\right].$$

By Lemma 3 we can assume that $\det X = \det Y = \det S$. Hence $B \in C_V C_W$ by (8).

If we will put $V = W$ in Theorem 1, then we will receive

Corollary 1.1. If $V = \mathrm{diag}(v_1,\dots,v_n)$, $v_i \neq v_j$ for $i \neq j$ and $V \in SL(n,F)$, then

$$(9)\qquad SL(n,F) = C_V^2 \cup Z(SL(n,F)).$$

Theorem 2. If V is a matrix described in Lemma 4, then

$$(10)\qquad SL(n,F) = \bigcup_{x \in Z(SL(n,F))} C_V C_{xV} \quad \text{for } n>2.$$

Proof. By Lemma 4, $xE \in C_V C_{xV}$, so $Z(SL(n,F)) \subseteq \bigcup_{x \in Z(SL(n,F))} C_V C_{xV}$.

By Corollary 1.1, $SL(n,F) - Z(SL(n,F)) = C_V C_V$. Hence the equality (10) holds.

Corollary 2.1. If $2 < n < |F|-1$ and $Z(SL(n,F)) = E$ then there exists a matrix V such that $SL(n,F) = C_V^2$.

P r o o f . Let V be a matrix described in Lemma 4. An existence of V ensures the inequality $n<|F|-1$. By (2), $E \in C_V^2$. Hence by Theorem 2, $SL(n,F) = C_V^2$.

C o r o l l a r y 2.2. If n,q are even numbers and $n<q$, then there exists $V \in SL(n,q)$ such that $SL(n,q) = C_V^2$.

P r o o f . Let V be a matrix described in Lemma 4. The existence of V ensures the inequality $n<q$. It is clear that Lemma 4 is true also for $n = 2$, because q is even. Now our Corollary results from Corollary 2.1, because $|Z(SL(n,Q))| = (n,q-1) = 1$, by assumption.

C o r o l l a r y 2.3. Let $s = o(V)$ denotes an order of V described in Lemma 4, $r = |Z(SL(n,q))|$. If $r|s$, then $SL(n,q) = K_s^2$.

The proof results from Theorem 2 and from the fact that $o(Va) = o(V)$ provided $a \in F_q^*$.

T h e o r e m 3. If $2<n<|F|-1$, then $SL(n,F) = K_2^4$.

P r o o f . Let V be a matrix described in Lemma 4. An existence of V follows by the inequality $n<|F|-1$. By Lemma 4, we have $C_V \subseteq K_2^2$, so $C_V^2 \subseteq K_2^4$. By Lemma 6, we obtain $Z(SL(n,F)) \subseteq K_2^4$. Hence $SL(n,F) \subseteq K_2^4$, by Corollary 1.1. An inverse inclusion is obvious.

R e m a r k 2. If $n = 2$ and char $F \neq 2$, then Theorem 3 is not true, because in this case $K_2^2 = E$ (see [1], Theorem 3). If $n = 2$, char $F = 2$ and $|F|>2$, then $SL(n,F) = K_2^2$, (see [1], Theorem 2).

C o r o l l a r y 3.1. If $n>2$, then $SL(n,F) = K_2^4$ where $F = Q,R,C$.

T h e o r e m 4. If $n<|F|-1$, then $GL_1(n,F) = K_2^4$.

P r o o f . We will consider two cases: a) n is even, b) n is odd.

Ad a). Let V and W are matrices from Lemma 5 described in (i) and in (ii) respectively. The existence of matrices V and W ensures the inequality $n<|F|-1$. Hence we have $C_V, C_W \subseteq K_2^2$ by Lemma 5 and $Z(GL_1(n,F)) \subseteq K_2^4$, by Lemma 7. From (1) $GL_1(n,F) = C_V^2 \cup C_V C_W \cup \cup Z(GL_1(n,F))$. Therefore $GL_1(n,F) \subseteq K_2^4$.

Ad b). In this case a proof is similar to Ad a).

Corollary 4.1. If $F = Q,R,C$, then $GL_1(n,F) = K_2^4$.

Theorem 5. If n is odd and $|Z(SL(n,F))| = n$, then there exists $V \in SL(n,F)$ such that $SL(n,F) = C_V^2 = K_2^4$.

Proof. Let $a \in F^*$ be a n^{th} root of 1. Then the matrices $V = \mathrm{diag}(a^n, a^{n-1}, \ldots, a)$, $a^i V = \mathrm{diag}(\underbrace{a^{n+i}, a^{n-1+i}, \ldots, a^2, a}_{i}, \underbrace{a^n, a^{n-1}, \ldots, a^{2+i}, a^{1+i}}_{n-i})$ have distinct entries for $i = 1,\ldots,n-1$ and we have $V, a^iV \in SL(n,F)$. Let $S = \mathrm{diag}(r, E'_{n-1})$, $r = \pm 1$;

$$R = \begin{bmatrix} 0 & E_{n-i} \\ E_i & 0 \end{bmatrix}, \quad i=1,\ldots,n-1.$$

It is clear that $\det R = 1$ and that we can choose r such that $\det S = 1$. The following identities are easily checked: (i) $VS^{-1}VS = E$, (ii) $R\, a^iV\, R^{-1} = V$. By Corollary 1.1 we get $SL(n,F) = C_V^2 \cup Z(SL(n,F))$. From (i) results $(a^iV)S^{-1}V\, S = a^iE$. Hence, by (ii), $(R^{-1}VR)(S^{-1}VS) = a^iE$ for $i = 1,\ldots,n-1$. Since $E \in C_V^2$, by (i), then $Z(SL(n,F)) \subseteq C_V^2$. Therefore $SL(n,F) = C_V^2$, by Corollary 1.1. By (i) and by Lemma 1, $V \in K_2^2$, so $C_V^2 \subseteq K_2^4$, because the set K_2^2 is a normal set.

Theorem 5 is a partial answer on a question stated in paper 3 , p.66.

Corollary 5.1. If n is odd, then there exists $V \in SL(n,C)$ such that $SL(n,C) = C_V^2$.

The proof results from Theorem 5 and from the fact that $|Z(SL(n,C))| = n$.

Theorem 6. If $n < |F|-1$, $|F| > 2$, then there exists $V \in SL(n,F)$ such that $SL(n,F) = C_V^4$.

Proof. Let V be a matrix from Lemma 4. An existence of V follows from the inequality $n < |F|-1$. By Corollary 1.1, $SL(n,F) =$

$= C_V^2 \cup Z(SL(n,F))$. To prove Theorem 6 it enough to show that $[SL(n,F)-Z(SL(n,F))]^2 = SL(n,F)$. Let $M = SL(n,F)-Z(SL(n,F))$. It is clear that $M = M^{-1}$. We will show that for any $g \in SL(n,F)$ we have $gM \cap M \neq 0$. Indeed, if this is false, there exists $g_o \in SL(n,F)$ such that $g_oM = Z(SL(n,F))$ i.e. $M = g_o^{-1}Z(SL(n,F))$ which means that $SL(n,F) = Z(SL(n,F)) \cup g_o^{-1}Z(SL(n,F))$. But this contradicts $|F|>2$.

The center $Z(SL(n,F))$ is an unity $\overline{E}$ of the group $PSL(n,F)$. Lemma 4 can be used to the group $PSL(n,F)$ without the assumption concerning n because for $n = 2$ we have $T^2 = -E \in Z = \overline{E}$. The equality (9) has now a form $\overline{V}\, T^{-1}\overline{V}\, T = \overline{E}$, so $\overline{E} \in C_{\overline{V}}C_{\overline{V}}$. Therefore by Lemma 4 and by Corollary 1.1, we obtain the theorem.

Theorem 7. If $V \in PSL(n,F)$ satisfies the assumption of Lemma 4, then $PSL(n,F) = C_V^2$.

Theorem 8. If $n<|F|-1$, then there exists $V \in PSL(n,F)$ such that $PSL(n,F) = C_V^2 = K_2^4$.

Proof. The assumption ensures the existence of the matrix V described in Lemma 4. Since $Z(PSL(n,F)) = \{\overline{E}\}$, we have $C_V \subseteq K_2^2$ by (4). Therefore by Theorem 7, $PSL(n,F) = C_V^2 = K_2^4$.

Theorem 9. $SL(3,F) = K_2^4$.

Proof. If $|F|>4$, then the proof follows from Theorem 3. If $|F| = 4$, then the proof follows from Theorem 5. If $|F| = 2$, then the proof follows from Theorem 8 because in this case $SL(3,2) \cong PSL(2.7)$. To prove Theorem 9 in the case $|F| = 3$, we will use character table of group $SL(3,3)$ (see [4], p.68). Using Burnside's formula on multiplication of conjugacy classes, it has been showed in [4] that for each class $C \neq \{E\}$ of the group $SL(3,3)$, we have $C^4 = SL(3,3)$. Hence in the special case $C \subseteq K_2$, we have $SL(3,3) = K_2^4$.

Corollary 9.1. $GL_1(3,F) = K_2^4$.

Proof. We have $GL_1(3,F) = (-E)SL(3,F) \cup SL(3,F)$. If $A \in SL(3,F)$ then $A = A_1A_2A_3A_4$ with $A_i \in K_2 \subset SL(3,F)$, by Theorem 9. It is clear that $-A = (-EA_1)A_2A_3A_4$ and $(-EA_1), A_2, A_3, A_4 \in K_2 \subset GL_1(3,F)$. Hence $GL_1(3,F) = K_2^4$.

REFERENCES

[1] J. Ambrosiewicz: On the squares of linear groups, Rend. Sem. Mat. Univ. Padova, Vol.75 (1986).

[2] J. Ambrosiewicz: On the square of sets of the group SL(3,F), PSL(3,F), Demonstratio Math. 18 (1985) 963-968.

[3] J.L. Brenner: Covering Theorems for FINASIGS X. The group G=PSL(n,q) had a class C such that CC=G, ARS COMBINATORIA, Vol.16 (1983) pp.57-68.

[4] A. Dold, B. Eckmann, Z. Arad, M. Herzog: Products of conjugacy classes in groups. Springer-Verlag, Berlin Heidelberg (1985).

[5] T.W. Hungeerford: Algebra. Springer-Verlag, New York, Heidelberg, Berlin 1974.

[6] J. Ambrosiewicz: Products of sets in linear groups. Demonstratio Math. 22 (1989), (to appear).

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF WARSAW, BIAŁYSTOK BRANCH, 15-267 BIAŁYSTOK, POLAND

Received October 21, 1988.