On sets of elements of the same order in the alternating group A_n

By CZESŁAW BAGIŃSKI (Białystok)

In a series of works J. L. BRENNER and others investigated the existence of a conjugacy class C such that $CC=G$, where G is a finite non-abelian simple group. An analogous property of a set K_m of all elements of order m of G is studied here. In [1] it was shown that in the alternating group A_n, $n>6$, conjugacy classes with elements of order 2 or 3 do not satisfy this condition. Here we establish the following

Theorem A. *If $n>4$, then in the alternating group A_n $K_2K_2=A_n$ if and only if $n\in\{5, 6, 10, 14\}$.*

This is the essential strenghtening of the theorem 3.05 of [1]. We also prove

Theorem B. *If $n>2$, then in the alternating group A_n $K_3K_3=A_n$.*

The notation and terminology is standard with the following addition: if f is a permutation of a finite set X, then $\operatorname{supp}(f)$ denotes the set $\{x\in X\colon f(x)\neq x\}$.

Lemma 1. *Let f and g be two involutions of S_n. If $fg\neq gf$, then there exist involutions f_1, g_1 such that $\operatorname{supp}(f_1), \operatorname{supp}(g_1)\subset\operatorname{supp}(fg)$ and $f_1g_1=fg$.*

PROOF. Each involution of S_n is a product of disjoint transpositons. Let $g=(\mathrm{i\,j})(\mathrm{k\,l})\dots$ and $i\in\operatorname{supp}(g)-\operatorname{supp}(fg)$. Then $i=fg(i)=f(j)$ and $j=f(i)=$ $=fg(j)$. Hence $j\in\operatorname{supp}(g)-\operatorname{supp}(fg)$ and $f=(\mathrm{i\,j})(k'\,l')\dots$. Let us take $f'=(\mathrm{i\,j})f$ $=(k'\,l')\dots$, $g'=(i\,j)g=(k\,l)\dots$. By our assumptions f', g' are not identities and of course $fg=f'g'$. Thus by induction on $|\operatorname{supp}(f)|$ we obtain the lemma.

Lemma 2. *If h is a product of disjoint cycles with pairwise distinct lengths and for involutions f, g $h=fg$, then for an arbitrary orbit X of h $f(X)=g(X)=X$.*

PROOF. Let us observe first that $fg(X)=X$ implies $f(X)=g(X)$. Let now X be an orbit of h with the smallest number of elements for which $g(X)\neq X$ and let $Y=X\cup g(X)$. Then $g(Y)=Y=f(Y)$ and so $h(Y)=Y$ and $h(Y-X)=Y-X$. If A is an orbit of h contained in $Y-X$ then by our assumptions and by inequality $|Y-X|\leqq|X|$ we have $|A|<|X|$. But $g(A)\subset g(Y-X)\subset X$ implies $g(A)\neq A$. This is a contradiction.

Lemma 3. *A product of two disjoint cycles with equal or even lengths can be expressed as a product of two involutions which are simultaneously odd or simultaneously even.*

PROOF. The lemma is an immediate consequence of the following decompositions:

$$(1\,2\dots 2k) = [(1\,2k)(2\,2k-1)\dots(k\,k+1)][(1\,2k-1)(2\,2k-2)\dots(k-1\,k+1)]$$

$$(1\,2\dots 2k) = [(2\,2k)(3\,2k-1)\dots(k\,k+2)][(1\,2k)(2\,2k-1)\dots(k\,k+1)]$$

$$(1\,2\dots 2k+1) = [(1\,2k+1)(2\,2k)\dots(k\,k+2)][(1\,2k)(2\,2k-1)\dots(k\,k+1)]$$

$$(1\,2\dots 2k+1)(2k+2\,2k+3\dots 4k+2) =$$
$$= [(1\,2k+2)(2k+1\,2k+3)(2k\,2k+4)\dots(2\,4k+2)]\cdot$$
$$\cdot[(1\,4k+2)(2\,4k+1)\dots(2k+1\,2k+2)].$$

By the above lemma and 2.5.7 of [3] we have then

Lemma 4. *If f is a cycle of odd length or f is a product of two disjoint cycles of even lengths, then f can be expressed as a product of two involutions conjugated in S_n.*

Corollary 1. *If $n>4$ then in the symmetric group S_n $K_2K_2=S_n$. Moreover each odd permutation is a product of two involutions conjugated in S_n.*

In [2] it was shown that each element of the alternating group A_n is a commutator of two elements from this group. By corollary 1 we immediately obtain

Corollary 2. *Each element of A_n is a commutator of two elements from S_n one of which has order 2.*

Lemma 5. *Let h be a cycle of length $2k+1$ and f, g be involutions such that* $\operatorname{supp}(f), \operatorname{supp}(g)\subset\operatorname{supp}(h)$. *If $h=fg$, then f and g are products of k disjoint transpositions.*

PROOF. Clearly S_n may be regarded as a group of permutations of the additive group $Z_n=\{0, 1, \dots, n-1\}$, where $n=2k+1$. We also may assume that $h=(0, 1, \dots \dots 2k)$. Let $h=fg$ with involutions f, g and $x\in Z_n-\operatorname{supp}(g)$. Thus $x+1=fg(x)= =f(x)$ and so $x, x+1\in\operatorname{supp}(f)$. Since $f(x+1)=x=fg(x-1)$ we have $g(x-1)= =x+1$ and so $x-1, x+1\in\operatorname{supp}(g)$. Hence by easy induction we can show that $f(x-m)=x+m+1$ and $g(x-m)=x+m$. Therefore $x-m\notin\operatorname{supp}(f)$ if and only if $x-m=x+m+1$ (that is $m=k$) and similarly $x-m\notin\operatorname{supp}(g)$ if and only if $x-m= =x+m$ (i.e. $m=0$). This ends the proof.

THE PROOF OF THEOREM A. Let $n\notin\{5, 6, 10, 14\}$, $n>4$. If f is an involution of A_n, then $|\operatorname{supp}(f)|$ is divisible by 4. Hence by lemmas 1, 2 and 5 the following permutations cannot be expressed as products of involutions from A_n:

for $n=4k-1$ or $n=4k$ a cycle of length $4k-1$,

for $n=4k$ or $n=4k+1$ a product of two disjoint cycles of lengths 3 and $4k-3$,

for $n=4k+2$ a product of three disjoint cycles of lengths 3,5 and $4(k-2)+1$.

Let us assume now that $n\in\{5, 6, 10, 14\}$, h is a permutation from A_n and f, g are involutions from S_n such that $h=fg$ and $\operatorname{supp}(f), \operatorname{supp}(g)\subset\operatorname{supp}(h)$. If $|\operatorname{supp}(h)|<n-1$ then for $i, j\notin\operatorname{supp}(h)$ either f and g or $f(i\,j)$ and $(i\,j)g$ belong to A_n and $h=fg=f(i\,j)(i\,j)g$. Let then $|\operatorname{supp}(h)|\geqq n-1$. If in the decomposition of h into the product of disjoint cycles the cycles of equal or even lengths occure then by lemma 3 involutions f and g can be chosen from A_n. Permutations which are not regarded yet are cycles or products of odd cycles with pairwise distinct lengths. There

are only a few types of such permutations. Using Lemmas 2, 5 and the decomposition of a cycle of length $2k+1$ in the proof of Lemma 3 we can easely find the desired decompositions.

THE PROOF OF THEOREM B. Let k be an odd natural number. Then

$$(1\,2\ldots 2k+1) = \big((1\,2\,3)(4\,5\,2k)(6\,7\,2(k-1))\ldots(k+1\;k+2\;k+3)\big)\cdot$$
$$\cdot\big((k+3\;k+4\;k)(k+5\;k+6\;k-2)\ldots(2k\;2k+1\;3)\big).$$

If k is even, then

$$(1\,2\ldots 2k+1) = \big((1\,2\,3)(4\,5\,2k)(6\,7\,2(k-1))\ldots(k\;k+1\;k+4)\big)\cdot$$
$$\cdot\big((k+2\;k+3\;k+1)(k+4\;k+5\;k-1)\ldots(2k\;2k+1\;3)\big).$$

Let us consider now a product of two cycles of even lengths. We have

$$(1\,2\ldots 2k)(2k+1\;2k+2\ldots 2k+2m) =$$
$$=\big((2k+2\;2k+1\;2k)(2k-1\;1\;2\ldots 2k-2)\big)\cdot$$
$$\cdot\big((2k+3\;2k+4\ldots 2k+2m\;2k+2)(2k+1\;2k\;2k-1)\big).$$

By the above decompositions of cycles of odd lengths we can find permutations f_1, f_2, g_1, g_2 such that each of them has order 3, $\operatorname{supp}(f_1)\subset\{1, 2, \ldots, 2k-1\}$, $\operatorname{supp}(f_2)\subset\{1, 2, \ldots, 2k-2\}$, $\operatorname{supp}(g_1)\subset\{2k+3, 2k+4, \ldots, 2k+2m\}$, $\operatorname{supp}(g_2)\subset\{2k+2, 2k+3, \ldots, 2k+2m\}$ and $(2k-1\;1\;2\ldots 2k-2)=f_1f_2$, $(2k+3\;2k+4\ldots\ldots 2k+2m\;2k+2)=g_1g_2$. Thus $(2k+2\;2k+1\;2k)f_1g_1$ and $f_2g_2(2k+1\;2k\;2k-1)$ are of order 3 and their product is equal to $(1\,2\,\ldots\,2k)(2k+1\;2k+2\,\ldots\,2k+2m)$.

References

[1] J. L. BRENNER, M. RANDAL, J. RIDDEL, Covering theorems for finite nonabelian simple groups, *Colloq. Math.* **32** (1974), 39—45.

[2] N. ITO, A theorem on the alternating group A_n, $n\geqq 5$, *Mathematica Japonica* **2** (1950—1952), 59—60.

[3] М. И. Каргаполов, Ю. И. Мерзляков, Основы теории групп, *Москва* 1982.

UNIVERSITY OF WARSAW
DIVISION BIAŁYSTOK
INSTITUTE OF MATHEMATICS
AKADEMICKA 2, BIAŁYSTOK

(Received October 9, 1985.)