TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 288, Number 1, March 1985

CUBES OF CONJUGACY CLASSES COVERING THE INFINITE SYMMETRIC GROUP

BY
MANFRED DROSTE

ABSTRACT. Using combinatorial methods, we prove the following theorem on the group S of all permutations of a countably-infinite set: Whenever $p \in S$ has infinite support without being a fixed-point-free involution, then any $s \in S$ is a product of three conjugates of p. Furthermore, we present uncountably many new conjugacy classes C of S satisfying that any $s \in S$ is a product of two elements of C. Similar results are shown for permutations of uncountable sets.

1. Introduction. We will deal with the infinite symmetric group S of all permutations of a countably-infinite set. Let us denote by $[p]$ the conjugacy class and by the support of p the underlying set without fixed points of $p \in S$. The following theorem was first shown by Bertram [**4**] and Moran [**15**] (cf. [**9**] for a generalization to the uncountable case):

Whenever $p \in S$ has infinite support, any permutation $s \in S$ is a product of 4 *conjugates of p, i.e. $S = [p]^4$. Moreover, the number* 4 *is minimal with this property.*

Hence, in order to improve the bound 4 of the theorem above, the question arises to classify all conjugacy classes C in S satisfying $S = C^3$. In the literature, various authors have dealt with this problem, cf. [**2, 5, 7, 10, 14, 17**]. In particular, if $p \in S$ has infinite support, in [**7**] we showed that $[p]^3$ always contains all elements $s \in S$ with infinite support; moreover, if in addition either p has at least one infinite orbit or p is an involution having at least one fixed point, we get $S = [p]^3$ (Droste and Göbel [**9**]; Moran [**14**]). On the other hand, it is known that $S \neq [p]^3$ whenever $p \in S$ is a fixed-point-free involution (see Moran [**15**] or Droste and Göbel [**9**]). It is the aim of this paper to show:

THEOREM 1. *Let $p \in S$ have infinite support without being a fixed-point-free involution. Then $S = [p]^3$.*

This affirms a conjecture in [**7**] and "almost confirms" another conjecture in Bertram [**4**]. In our proof, we will use some recent and powerful results of an interesting paper of G. Moran [**17**] as well as several other theorems of the literature, and we will generalize Theorem 1 to a result for permutations of uncountable sets.

It still remains an open problem to classify all conjugacy classes C in S satisfying $S = C^2$. In [**7**], we gave a description of the set $[p]^2$ whenever $p \in S$ has at least one

Received by the editors August 12, 1983 and, in revised form, April 18, 1984.
1980 *Mathematics Subject Classification*. Primary 20B30.
Key words and phrases. Infinite symmetric groups, finite symmetric groups, alternating groups, permutations, conjugacy classes, involutions, orbits, fixed points.

0002-9947/85 $1.00 + $.25 per page

infinite orbit. Now we show

THEOREM 2. *Let $p \in S$ have no infinite orbit, and let $(+)$ be the following property:*

$(+)$ *p has infinitely many finite orbits of length ≥ 3.*

Then the following is true:

(a) *If $[p]^2 = S$, then $(+)$ holds.*

(b) *Assume that p has infinitely many fixed points and infinitely many orbits of length 2. Then:*

(1) *If $(+)$ does not hold, then*

$$[p]^2 = \{s \in S; s \text{ has infinitely many orbits}\}.$$

(2) *If $(+)$ holds, then $[p]^2 = S$.*

In particular, there are $2^{\aleph_0}$ different conjugacy classes $[p]$ in S with $S = [p]^2$, where p has no infinite orbit.

Here (a) and (b)(1) generalize results of Gray [**12**, Theorem 2.10] and Moran [**15**, Corollary 2.4, 2.5] who considered the case where $p \in S$ is an involution, i.e. has *no* orbits of length ≥ 3. Under the additional assumption that p has only finitely many fixed points, (a) follows also from Moran [**16**, Theorem 3] or from [**7**, Theorem 4.5]. Part (b)(2) generalizes Bertram [**4**, Theorem 1] which states the result under the assumption that p has infinitely many orbits of lengths 1, 2, 3, respectively (and no others). Previously, this has been the only conjugacy class $[p]$ in S known satisfying $S = [p]^2$, where p has no infinite orbit.

2. Notation and remarks. Let $\dot{\bigcup} A_i$ denote a *disjoint* union; $\mathbf{N}_0 = \mathbf{N} \,\dot{\cup}\, \{0\}$, $\mathbf{N}_\infty = \mathbf{N} \,\dot{\cup}\, \{\aleph_0\}$; $A \cdot B = \{a \cdot b; a \in A, b \in B\}$ for subsets $A, B \subseteq G$, and $[a] = \{x^{-1} \cdot a \cdot x; x \in G\}$ = conjugacy class of $a \in G$ (any group). For a mapping f let $f|_A$ denote its restriction to A and a^f its value at a; so the composition of mappings is from left to right.

S_M denotes the symmetric group of all permutations of a set M, $A_M \subseteq S_M$ the alternating group if M is finite, id_M (or id, if there is no ambiguity) the identity permutation of M, and $S = S_X$ for some fixed countably-infinite set X, e.g. $X = \mathbf{Z}$. Now let $p \in S_M$. An orbit of p is a minimal p-invariant subset of M. The length of an orbit is its cardinality. We put:

$\overline{p}(n) = |\{X; X \text{ orbit of length } n \text{ of } p\}|$ $(n \in \mathbf{N}_\infty)$;

$\overline{p}$ = the function from $\mathbf{N}_\infty$ into $\{c; 0 \leq c \leq |M|\}$ with $\overline{p}(n)$ $(n \in \mathbf{N}_\infty)$ as defined above;

$F(p) = \{a \in M; a^p = a\}$ = fixed point set of p;

$|p| = |M \backslash F(p)| = \sum_{2 \leq n \in \mathbf{N}_\infty} n \cdot \overline{p}(n)$.

Then $\overline{p}(1) = |F(p)|$ and $M \backslash F(p)$ is the support of p. The following fact is well known (e.g. [**20**, 11.3.1]) and will be used throughout this paper without mentioning it again:

Whenever $p, q \in S_M$, then $[p] = [q]$ iff $\overline{p} = \overline{q}$.

Hence $\mathrm{id} = p \cdot p^{-1} \in [p]^2$ for any $p \in S_M$.

A permutation $p \in S$ is called *nicely even* (Moran [**15**]), if $\overline{p}(n)$ is an even cardinal for each $n \in \mathbf{N}_\infty$ (here $\aleph_0$ is considered even). The following subsets of S will be important.

NE = set of all nicely even permutations in S;

$R_i = \{s \in S; s^2 = \mathrm{id}, |s| = \aleph_0, \overline{s}(1) = i\}$ = conjugacy class of all involutions in S with infinite support and i fixed points $(0 \leq i \leq \aleph_0)$.

For a finite set T with $|T| = n \geq 3$ we define the following conjugacy classes in S_T:

$C_{T,k} = \{p \in S_T; \overline{p}(k) = 1, \overline{p}(1) = n - k\}$ = class of all $p \in S_T$ with precisely one nontrivial orbit which is of length k and $n - k$ fixed points $(2 \leq k \leq n)$;

$C_T = C_{T,n}$;

$D_T = \{p \in S_T; \overline{p}(2) = \overline{p}(n-2) = 1\}$ = class of all $p \in S_T$ with precisely two orbits, one of length 2 and the other of length $n - 2$ (here $n \geq 5$).

Finally, if $M = \dot{\bigcup}_{i\in I} M_i$, $p_i \in S_{M_i}$ and $p \in S_M$ satisfy $p|_{M_i} = p_i$ $(i \in I)$, then we also write $p = \bigoplus_{i\in I} p_i$. Clearly, in this case $\overline{p}(n) = \sum_{i\in I} \overline{p}_i(n)$ for each $n \in \mathbf{N}_\infty$, and if also $q_i \in S_{M_i}$ $(i \in I)$ and $q = \bigoplus_{i\in I} q_i$, then $p \cdot q = \bigoplus_{i\in I}(p_i \cdot q_i)$.

3. Proof of Theorem 1. One of the main tools for the proofs of this paper is the *splitting-argument-technique* which may be best described by an example. Let $s, p \in S$ and suppose we wish to show that s is a product of two conjugates of p. Assume that it is possible to decompose $s = s_1 \oplus s_2$ such that the domains of s_1, s_2 are infinite, and that, for instance and simplicity, p consists of precisely $\aleph_0$ orbits of length m for some $2 \leq m \in \mathbf{N}_\infty$. Now if we can find permutations q_i, r_i of the domain of s_i, each consisting only of $\aleph_0$ orbits of length m, such that $s_i = q_i \cdot r_i$ $(i = 1, 2)$, then $q = q_1 \oplus q_2$ and $r = r_1 \oplus r_2 \in S$ each have precisely $\aleph_0$ orbits of length m, hence are conjugate to p, and satisfy

$$s = s_1 \oplus s_2 = (q_1 \cdot r_1) \oplus (q_2 \cdot r_2) = q \cdot r \in [p]^2,$$

establishing our goal. Let us now give the formal statement of the technique which is a bit more general than the above example:

(3.0) THE SPLITTING-ARGUMENT-TECHNIQUE. *Let $2 \leq n \in \mathbf{N}$, M, M_i be sets and $a_i, b_{ij} \in S_{M_i}$ for each $i \in I$, $j = 1, \ldots, n$, such that $a_i \in \prod_{j=1}^n [b_{ij}]$ $(i \in I)$. Then $a \in \prod_{j=1}^n [b_j]$ whenever $a, b_j \in S_M$ satisfy $\overline{a}(m) = \sum_{i\in I} \overline{a_i}(m)$, $\overline{b_j}(m) = \sum_{i\in I} \overline{b_{ij}}(m)$ for each $m \in \mathbf{N}_\infty$ and $j = 1, \ldots, n$.*

PROOF. Assume $a, b_j \in S_M$ $(j = 1, \ldots, n)$ as stated. We split $M = \dot{\bigcup}_{i\in I} C_i$, $a = \bigoplus_{i\in I} c_i$ such that $c_i = a|_{C_i} \in S_{C_i}$ and $\overline{c_i} = \overline{a_i}$ for each $i \in I$. Let $i \in I$. By $|C_i| = \sum_{m\in\mathbf{N}_\infty} m \cdot \overline{c_i}(m) = \sum_{m\in\mathbf{N}_\infty} m \cdot \overline{a_i}(m) = |M_i|$ and assumption there are $d_{ij} \in S_{C_i}$ with $\overline{d_{ij}} = \overline{b_{ij}}$ $(j = 1, \ldots, n)$ and $c_i = \prod_{j=1}^n d_{ij}$. Let $d_j = \bigoplus_{i\in I} d_{ij} \in S_M$, hence

$$\overline{d_j}(m) = \sum_{i\in I} \overline{d_{ij}}(m) = \sum_{i\in I} \overline{b_{ij}}(m) = \overline{b_j}(m)$$

for each $n \in \mathbf{N}_\infty$ and $j = 1, \ldots, n$. Thus

$$a = \bigoplus_{i\in I} \left(\prod_{j=1}^n d_{ij} \right) = \prod_{j=1}^n d_j \in \prod_{j=1}^n [b_j].$$

For the convenience of the reader, we list several results of the literature which we are going to use. First note that if a permutation $p \in S$ has at least one infinite orbit, any element $s \in S$ is a product of three conjugates of p:

LEMMA 3.1 (DROSTE AND GÖBEL [**10**], also [**7**, COROLLARY 3.3]). *Let $p \in S$ satisfy $\overline{p}(\aleph_0) \geq 1$. Then $S = [p]^3$.*

The following two results show that whenever $p \in S$ has infinite support, both any $s \in S$ with infinite support and also the identity-permutation are products of three conjugates of p:

LEMMA 3.2 ([**7**, THEOREM 2]). *Let $s, p \in S$ both have infinite support. Then $s \in [p]^3$.*

LEMMA 3.3 (MORAN [**17**, PROPOSITION 6.6]). *Let $p \in S$ have infinite support. Then* $\mathrm{id} \in [p]^3$.

The following recent result due to G. Moran states that if $s, p \in S$ have infinite support and no orbits of length 2 or $\aleph_0$, but s or p has at least one fixed point, then s is a product of two conjugates of p.

LEMMA 3.4 (MORAN [**17**, PROPOSITION 5.1, THEOREM 3]). *Let $s, p \in S$ both have infinite support and satisfy $\overline{s}(2) = \overline{s}(\aleph_0) = \overline{p}(2) = \overline{p}(\aleph_0) = 0$. If $\overline{s}(1) \geq 1$ or $\overline{p}(1) \geq 1$, then $s \in [p]^2$.*

The next lemma states that the products of two involutions of S without fixed points are precisely the nicely even permutations.

LEMMA 3.5 (MORAN [**15**, p. 64]). $R_0^2 = NE$.

The following two results are due to Moran [**14**], but in [**14**] no proof was given. Therefore we include a proof here, leaving details to the reader. First we show that all permutations $s \in S$ with finite support and an even total number of orbits of lengths 3 or 5 can be written as a product of three involutions each without fixed points.

LEMMA 3.6. *Let $s \in S$ have finite support and satisfy $\overline{s}(3) + \overline{s}(5) = 2 \cdot m$ for some $m \in \mathbf{N}_0$. Then $s \in R_0^3$.*

PROOF. Note that $\mathrm{id} \in R_0^3$. Hence, using a splitting-argument, it is easy to see that we only have to consider the following special cases:

Case I. s has precisely one nontrivial orbit which is of length $n \in \mathbf{N}$, and either (a) $n = 4$, (b) $n = 2k$ with $3 \leq k \in \mathbf{N}$, (c) $n = 7$, or (d) $n = 2k + 1$ with $4 \leq k \in \mathbf{N}$.

Case II. s has precisely two nontrivial orbits which are either (a) both of length 3 or both of length 5, or (b) of length 3 *and* of length 5, respectively.

We now show for each of these cases except II(a) that there exists a $q \in R_0$ such that $s \cdot q \in NE$; then $s \in R_0^3$ by Lemma 3.5. The following formulae establish this claim. Recall that the composition of mappings is from left to right.

We have $a \cdot b = c$ in each of the following cases:

(Ia) $$a = (1\ 2\ 3\ 4), \quad b = (1\ 2)(3\ 4), \quad c = (1)(3)(2\ 4);$$

(Ib) $$\begin{aligned} a &= (1\ 2\ 3\ \cdots\ 2k-1\ 2k), \\ b &= (1\ 2)(3\ 2k)(4\ 2k-1)\cdots(k+1\ k+2), \\ c &= (1)(k+1)(2\ 2k)(3\ 2k-1)\cdots(k\ k+2); \end{aligned}$$

$$\text{(Ic)}\qquad \begin{aligned} &a = (1\ 2\ 3\ 4\ 5\ 6\ 7)(8), \quad b = (1\ 3)(2\ 8)(4\ 5)(6\ 7),\\ &c = (1\ 8\ 2)(3\ 5\ 7)(4)(6); \end{aligned}$$

$$\text{(Id)}\qquad \begin{aligned} &a = (1\ 2\ 3\ 4\ 5\ \cdots\ 2k\ 2k+1)(2k+2),\\ &b = (1\ 3)(2\ 2k+2)(4\ 5)(6\ 2k+1)(7\ 2k)\cdots(k+3\ k+4),\\ &c = (1\ 2k+2\ 2)(3\ 5\ 2k+1)(4)(k+3)(6\ 2k)(7\ 2k-1)\cdots(k+2\ k+4); \end{aligned}$$

$$\text{(IIb)}\qquad \begin{aligned} &a = (1\ 2\ 3)(4)(5\ 6\ 7\ 8\ 9)(10),\\ &b = (1\ 2)(3\ 4)(5\ 6)(7\ 9)(8\ 10),\\ &c = (1)(5)(4\ 3\ 2)(10\ 8\ 7)(6\ 9). \end{aligned}$$

For (IIa) observe $s \in NE = R_0^2 \subseteq R_0^3$ by Lemma 3.5. This finishes the proof.

As a consequence of the previous results we obtain that any $s \in S$ can be written as a product of three involutions each with infinite support and i fixed points, whenver $i \geq 1$.

COROLLARY 3.7 (MORAN [**14**]). *Let $0 < i \leq \aleph_0$. Then $S = R_i^3$.*

PROOF. By Lemmas 3.2 and 3.6, and a splitting-argument, it suffices to show $s \in R_i^3$ for $s \in S$ with $\overline{s}(n) = 1$, $\overline{s}(m) = 0$ for $m \neq n$, and $n \in \{3, 5\}$. If $n = 3$, observe $(1\ 2\ 3) = ((1)(2\ 3)) \cdot ((1\ 2)(3))$ and $R_i \subseteq R_i^2$ to obtain $s \in R_i^2 \subseteq R_i^3$. Now let $n = 5$. Then $s \in R_i^3$ follows directly from

$$(1\ 2\ 3\ 4\ 5) = ((1\ 3)(2)(4\ 5)) \cdot ((1\ 3)(2\ 4)(5)) \cdot ((1\ 2)(3\ 4)(5))$$

and $\mathrm{id} \in R_0^3$.

The following lemma states that whenever $p \in S$ has only finite orbits of length ≥ 3 and $s \in S$ has precisely one nontrivial orbit which is finite, then s is a product of three conjugates of p.

LEMMA 3.8. *Let $s, p \in S$ and $2 \leq m \in \mathbf{N}$ satisfy $\overline{s}(m) = 1$, $\overline{s}(n) = 0$ if $n \notin \{1, m\}$, and $\overline{p}(1) = \overline{p}(2) = \overline{p}(\aleph_0) = 0$. Then $s \in [p]^3$.*

PROOF. We distinguish between two cases.

Case I. Assume $m = 2$ and $\overline{p}(n) = 0$ for all $4 \leq n \in \mathbf{N}$.

Then we have $\overline{p}(3) = \aleph_0$. W.l.o.g. let $\mathbf{N}_0$ be the underlying set. The equation $(0\ 2) = a \cdot b \cdot c$, where

$$\begin{aligned} &a = (0\ 1\ 2)(5\ 4\ 3)(8\ 7\ 6)(11\ 10\ 9)(14\ 13\ 12)\ldots,\\ &b = (0\ 1\ 3)(2\ 4\ 6)(5\ 7\ 9)(8\ 10\ 12)(11\ 13\ 15)\ldots,\\ &c = (1\ 0\ 4)(3\ 2\ 7)(6\ 5\ 10)(9\ 8\ 13)(12\ 11\ 16)\ldots, \end{aligned}$$

immediately yields the required result.

Case II. Assume either $(+)$ $m = 2$ and $\overline{p}(n) \neq 0$ for some $n \geq 4$, or $(++)$ $m \geq 3$.

Step 1. We claim there exists a $q \in S$ with $\overline{q}(1) = 1$, $\overline{q}(2) = \overline{q}(\aleph_0) = 0$ and $q \in [p] \cdot [s]$.

If $(+)$ holds, our claim follows from the equation $(1\ 2\ 3\ 4\ \cdots\ n) \cdot (2\ 1) = (1)(2\ 3\ 4\ \cdots\ n)$. Now let us assume $(++)$. Then choose $k = m - 1$ orbits

$\{1_j, \ldots, n_j\}$ $(j = 1, \ldots, k)$ of length ≥ 3 of p. The result follows from the observation that

$$((1_1\ 2_1\ \cdots\ n_1)(1_2\ 2_2\ \cdots\ n_2)\cdots(1_k\ 2_k\ \cdots\ n_k))\cdot(2_1\ 1_1\ 1_2\ \cdots\ 1_k)$$
$$= (1_1)(2_1\ \cdots\ n_1\ 1_2\ 2_2\ \cdots\ n_2\ 1_3\ \cdots\ 1_k\ 2_k\ \cdots\ n_k).$$

Step 2. If we choose $q \in S$ as in Step 1, we obtain $q \in [p]^2$ by Lemma 3.4 and thus $s \in [p]^3$, finishing Case II.

Finally, we will need the fact that the squares of certain conjugacy classes (defined in §2) in the finite symmetric group cover the alternating group.

LEMMA 3.9 (GLEASON [**13**, PROPOSITION 4, p. 172]; cf. BERTRAM [**3**]). *Let T be a finite set with $|T| \geq 5$. Then $A_T = C_T^2$.*

LEMMA 3.10 (HSÜ CH′ENG-HAO [**6**]). *Let T be a finite set with $|T| = 2k$ for some $k \in \mathbf{N}$ with $k \geq 3$. Then $D_T \subseteq A_T$ and $A_T = D_T^2$.*

We are now ready for the

PROOF OF THEOREM 1. Let $p \in S \backslash R_0$ have infinite support and let $s \in S$. We want to show $s \in [p]^3$. Therefore we can assume $\overline{p}(\aleph_0) = 0$ by Lemma 3.1, $|s| < \infty$ by Lemma 3.2, and $s \neq \mathrm{id}$ by Lemma 3.3. We distinguish between two cases.

Case I. Assume $\sum_{n \geq 3} \overline{p}(n) = \aleph_0$.

Applying Lemma 3.3 and a splitting-argument, we see that we only have to show $s \in [p]^3$ in the special case $\overline{p}(1) = \overline{p}(2) = 0$. A further splitting-argument yields that we only have to examine permutations $s \in S$ which have precisely one nontrivial (finite) orbit. Now the result follows from Lemma 3.8.

Case II. Assume $\sum_{n \geq 3} \overline{p}(n) < \aleph_0$.

Here we have $\overline{p}(2) = \aleph_0$, since p has infinite support. If $\overline{s}(3) + \overline{s}(5) = 2m$ for some $m \in \mathbf{N}_0$, we obtain $s \in [p]^3$ by Lemmas 3.6 and 3.3, and a splitting-argument. Hence let $\overline{s}(3) + \overline{s}(5)$ be an odd number. Again using Lemma 3.6 and a splitting-argument, we see that it suffices to consider the special case that $s \in S$ has precisely one nontrivial orbit which is of length 3 or 5. If $p(n) = 0$ for all $n \geq 3$, we get $\overline{p}(1) \geq 1$ by $p \notin R_0$, thus $s \in [p]^3$ by Corollary 3.7. Therefore assume now $\overline{p}(n) \neq 0$ for some $n \geq 3$. We distinguish between three cases according to whether $n \geq 5$ and n is odd, $n \geq 4$ and n is even, or $n = 3$, respectively.

Subcase 1. Let $n \geq 5$ be odd.

Let T be a subset of the domain of s, p such that $|T| = n$ and T contains the nontrivial orbit of s. Then $s|_T \in A_T$ and $A_T = C_T^2$ according to Lemma 3.9. Since $n \geq 5$ is odd, we have $C_T \subseteq A_T$. Hence $s|_T \in C_T^3$ and thus, by Lemma 3.3 and a splitting-argument, $s \in [p]^3$.

Subcase 2. Let $n \geq 4$ be even.

Put $m = n + 2$ and let T be a subset of the underlying set such that $|T| = m$ and T contains the nontrivial orbit of s. Then $s|_T \in A_T$ and $D_T \subseteq A_T \subseteq D_T^2$ by Lemma 3.10, thus $s|_T \in D_T^2 \subseteq D_T^3$. Using a splitting-argument and Lemma 3.3, we get $s \in [p]^3$.

Subcase 3. Let $n = 3$.

The nontrivial orbit of s has length either 3 or 5. Observe the identities $(1\ 2\ 3) = (1\ 2\ 3)\cdot(3\ 2\ 1)\cdot(1\ 2\ 3)$ and $(1\ 2\ 3\ 4\ 5)(6)(7) = ((1\ 2\ 4)(3\ 6)(5\ 7))\cdot((4\ 2\ 1)(5\ 6)(3\ 7))\cdot$

$((1\ 2\ 3)(4\ 5)(6\ 7))$. Together with Lemma 3.3, these equations yield $s \in [p]^3$. This finishes Case II and hence the theorem is proved.

Finally, we generalize Theorem 1 to the case of arbitrarily infinite underlying sets.

COROLLARY 3.11. *Let M be any infinite set and $s, p \in S_M$ such that p has infinite support without being a fixed-point-free involution. Then $|s| \leq |p|$ and $s \in [p]^3$ are equivalent. Moreover, the number 3 is minimal with this property.*

PROOF. Let $s, p \in S_M$ as stated in the first sentence of the corollary. If $s = u \cdot v \cdot w$ with $u, v, w \in [p]$, we get $|s| \leq |u| + |v| + |w| = 3 \cdot |p| = |p|$ by cardinal arithmetic. Conversely, assume $|s| \leq |p|$. Then $s \in [p]^3$ follows via a splitting-argument from (3.2) and (3.3) if $|s| \geq \aleph_0$, and from Theorem 1 and (3.3) if $|s| \leq \aleph_0$. The minimality part of the corollary is contained in Moran [**15**, Corollary 2.5] or in [**7**, (4.5)].

For a description of the set $[p]^3$, when $p \in S$ is a fixed-point-free involution, see Moran [**14**].

4. Squares of conjugacy classes. This section is devoted to the proof of Theorem 2. Again we will make extensive use of splitting-arguments as in §3. First we establish necessary conditions (Theorem 4.1) and sufficient conditions (Lemma 4.2) for certain permutations $s, p_1, p_2 \in S$, where, in particular, s has only finitely many orbits and hence at least one infinite orbit and p_1, p_2 each have no infinite orbits, such that s is a product of two conjugates of p_1 and p_2, respectively. The following result generalizes Moran [**15**, Corollary 2.3(1)].

THEOREM 4.1. *Let $s, p_1, p_2 \in S$ with $s \in [p_1] \cdot [p_2]$ such that s has only finitely many orbits and p_1, p_2 each have no infinite orbit and only finitely many orbits of length ≥ 3. Then p_1, p_2 each have only finitely many fixed points. Moreover, if s has, say, i infinite orbits and $k_j = \sum_{2 \neq n \in \mathbf{N}} n \cdot \overline{p_j}(n)$ $(j = 1, 2)$, then $k_1, k_2 \in \mathbf{N}_0$ and $k_1 - k_2 \equiv i \bmod 2$. In particular, $[p_1] \neq [p_2]$ if i is odd.*

PROOF. Let $M = \dot{\bigcup}_{j=1}^{i} (\mathbf{Z} \times \{j\}) \,\dot{\cup}\, A$, where A is a finite (possibly empty) set. W.l.o.g. assume $s, p_1, p_2 \in S_M$ such that $s = p_1 \cdot p_2$, p_1, p_2 each have no infinite orbit and only finitely many orbits of length ≥ 3, the union of all finite orbits of s equals A, and s acts on each $\mathbf{Z} \times \{j\}$ like a shift, i.e. $(m, j)^s = (m + 1, j)$ for each $m \in \mathbf{Z}$, $j = 1, \ldots, i$. Thus the infinite orbits of s are precisely the sets $\mathbf{Z} \times \{j\}$.

We introduce some abbreviations. For $k = 1, 2$, let A_k denote the smallest p_k-invariant subset of M containing A, B_k the union of all orbits of length 3 of p_k, and S_k (U_k) the set (union) of all orbits of length 2 of p_k, respectively; thus $M = F(p_k) \,\dot{\cup}\, U_k \,\dot{\cup}\, B_k$. Let $C = A_1 \cup A_2 \cup B_1 \cup B_2$. Then C is finite.

First let $j \in \{1, \ldots, i\}$. Since $s = p_1 \cdot p_2$, p_2 has no infinite orbit, and s acts on $\mathbf{Z} \times \{j\}$ like a shift, it is impossible that for some $x \in \mathbf{Z}$, each $y \in \mathbf{Z}$ with $y \geq x$ satisfies $(y, j) \in F(p_1)$. Hence, since C is finite, there is $b_j \in \mathbf{Z}$ with $(b_j, j) \in U_1$ and $(x, j) \notin C$ for any $x \in \mathbf{Z}$ with $b_j \leq x$, in particular $(x, j)^{p_k} \in M \backslash A$ for $k = 1, 2$. Let $m = m(j) \in \{1, \ldots, i\}$, $a_j \in \mathbf{Z}$ such that $(b_j, j)^{p_1} = (a_j, m)$, thus $\{(a_j, m), (b_j, j)\} \in S_1$. If $m = j$, we may w.l.o.g. assume that $a_j < b_j$ (otherwise rename these elements). This ensures $(a_j, m) \neq (b_j + 1, j)$. Hence by $(a_j, m)^{p_2} = (b_j, j)^{p_1 \cdot p_2} = (b_j, j)^s = (b_j + 1, j) \notin C$ we obtain $\{(a_j, m), (b_j + 1, j)\} \in S_2$. It follows that $(b_j+1,j)^{p_2} = (a_j,m) = (a_j-1,m)^s = (a_j-1,m)^{p_1\cdot p_2}$, thus $(a_j-1,m)^{p_1} = (b_j+1,j)$ and, as before, $\{(a_j-1,m),(b_j+1,j)\} \in S_1$. By induction this shows

$$(+)\quad \{(a_j-k,m(j)),(b_j+k,j)\} \in S_1 \quad \text{and} \quad \{(a_j-k,m(j)),(b_j+k+1,j)\} \in S_2$$

for all $k \in \mathbf{N}_0$.

Now assume that for each $j \in \{1,\ldots,i\}$, the elements $a_j, b_j \in \mathbf{Z}$, $m(j) \in \{1,\ldots,i\}$ are chosen as in the above paragraph. Then, by (+), the mapping $j \mapsto m(j)$ is an injection from $\{1,\ldots,i\}$ into, hence onto, itself. It may happen that $a_j \geq b_{m(j)}$ for some $j \in \{1,\ldots,i\}$ with $j \neq m(j)$. Then we replace b_j by $b'_j = b_j + n_j$ and a_j by $a'_j = a_j - n_j$, where $n_j = a_j - b_{m(j)} + 1 \in \mathbf{N}$. Then $a'_j < b_{m(j)}$, and (+), with a_j, b_j replaced by a'_j, b'_j, is obviously still satisfied. Hence we may assume w.l.o.g. that $a_j < b_{m(j)}$ for all $j \in \{1,\ldots,i\}$.

For each $j \in \{1,\ldots,i\}$, let $D_j = \{(x,m(j)); x \in \mathbf{Z}, a_j < x < b_{m(j)}\}$ and $E_j = \{(x,m(j)); x \in \mathbf{Z}, a_j < x \leq b_{m(j)}\}$. We put $D = A \,\dot\cup\, \dot{\bigcup}_{j=1}^{i} D_j$ and $E = A \,\dot\cup\, \dot{\bigcup}_{j=1}^{i} E_j$. Thus D and E are finite sets, and by (+) the set $M\backslash D = \dot{\bigcup}_{j=1}^{i}((\mathbf{Z}\times\{m(j)\})\backslash D_j)$ is a union of orbits of length 2 of p_1. This shows $F(p_1) \subseteq M\backslash U_1 \subseteq D$ and $k_1 = |M\backslash U_1| \equiv |D| \bmod 2$. Similarly, $M\backslash E = \dot{\bigcup}_{j=1}^{i}((\mathbf{Z}\times\{m(j)\})\backslash E_j)$ is a union of orbits of length 2 of p_2, $F(p_2) \subseteq M\backslash U_2 \subseteq E$, and $k_2 = |M\backslash U_2| \equiv |E| \bmod 2$. In particular, p_1 and p_2 each have only finitely many fixed points, since D and E are finite, and $k_1, k_2 \in \mathbf{N}_0$. Since $E\backslash D = \{(b_j,j); j = 1,\ldots,i\}$, we have $k_1 - k_2 \equiv i \bmod 2$. So, if i is odd, $k_1 \neq k_2$ and thus $\overline{p_1} \neq \overline{p_2}$ and $[p_1] \neq [p_2]$.

Next we prove a partial converse to Theorem 4.1.

LEMMA 4.2. *For $i = 1,2$, let $p_i \in S$ have infinitely many nontrivial finite, but no infinite orbits such that $\overline{p_1}(1) = \sum_{n\geq 3}(n-2)\cdot\overline{p_2}(n)$ and $\overline{p_2}(1) = 1 + \sum_{n\geq 3}(n-2)\cdot\overline{p_1}(n)$. Then $s \in [p_1]\cdot[p_2]$ for each permutation $s \in S$ which has precisely one (infinite) orbit.*

PROOF. Let $\{P_i; i \in \mathbf{N}\}$ ($\{P^i; i \in \mathbf{N}\}$) be an enumeration of the set of all nontrivial orbits of p_1 (p_2), respectively. Inductively, we now construct a family of nonempty sets $A_1, B_1, A_2, B_2, A_3, \ldots \subseteq \mathbf{N}_0$ such that $0 \in A_1$ and for each $i \in \mathbf{N}$ the following conditions hold:

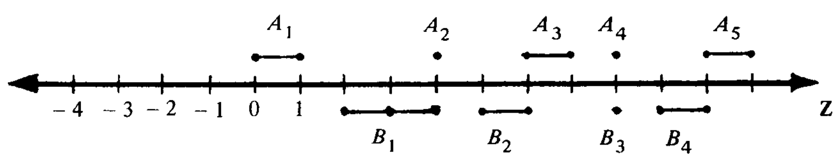
(I) A_i, B_i are convex (here a subset $S \subseteq \mathbf{N}_0$ is called convex, if $a, b \in S$, $c \in \mathbf{N}_0$, $a < c < b$ imply $c \in S$),

(II) $(\max A_i) + 1 = \min B_i$, $\max B_i = \min A_{i+1}$,

(III) $|A_i| = |P_i| - 1$, $|B_i| = |P^i| - 1$.

It follows that, in particular, $A_i < A_j$, $B_i < B_j$ if $i < j$, $\mathbf{N}_0 = \dot{\bigcup}_{i\in\mathbf{N}} A_i \cup \dot{\bigcup}_{i\in\mathbf{N}} B_i$, and $(\dot{\bigcup}_{i\in\mathbf{N}} A_i) \cap (\dot{\bigcup}_{i\in\mathbf{N}} B_i) = \{\min A_i; i \geq 2\} = \{\max B_i; i \in \mathbf{N}\}$.

EXAMPLE.



It now remains to show that there are $q, r \in S_{\mathbf{Z}}$ such that $q\cdot r = z$ (where $z \in S_{\mathbf{Z}}$ satisfies $a^z = a+1$ for all $a \in \mathbf{Z}$) and, if we put $Q_i = A_i \,\dot\cup\, \{-i\}$ ($R_i = B_i \,\dot\cup\, \{-i\}$)

for all $i \in \mathbf{N}$, such that $\{Q_i;\ i \in \mathbf{N}\}$ ($\{R_i;\ i \in \mathbf{N}\}$) is the set of all nontrivial orbits of q (r), respectively.

Indeed, if $q, r \in S_{\mathbf{Z}}$ are constructed in this way, by condition (III) it follows that $\overline{q}(n) = \overline{p_1}(n)$, $\overline{r}(n) = \overline{p_2}(n)$ if $2 \leq n \in \mathbf{N}$ and $\overline{q}(\aleph_0) = \overline{r}(\aleph_0) = 0$. Also, we get

$$F(q) = \mathbf{Z} \backslash \left(\dot{\bigcup_{i \in \mathbf{N}}} Q_i \right) = \mathbf{N}_0 \backslash \left(\dot{\bigcup_{i \in \mathbf{N}}} A_i \right) = \dot{\bigcup_{i \in \mathbf{N}}} (B_i \backslash (\max B_i))$$

and, similarly, $F(r) = \{0\} \mathbin{\dot\cup} \dot{\bigcup}_{i \in \mathbf{N}} (A_i \backslash (\min A_i))$. Using (III), this shows

$$\overline{q}(1) = \sum_{i \in \mathbf{N}} (|B_i| - 1) = \sum_{i \in \mathbf{N}} (|P^i| - 2) = \sum_{n \geq 3} (n-2) \cdot \overline{p_2}(n) = \overline{p_1}(1),$$

and similarly $\overline{r}(1) = 1 + \sum_{n \geq 3} (n-2) \cdot \overline{p}_1(n) = \overline{p_2}(1)$. Hence $\overline{q} = \overline{p_1}$, $\overline{r} = \overline{p_2}$, and $[s] = [z] \subseteq [q] \cdot [r] = [p_1] \cdot [p_2]$ is established.

We now show how to define the required elements $q, r \in S_{\mathbf{Z}}$ (here we will not need condition (III)). For each $i \in \mathbf{N}$, put $(-i)^q = \min A_i$, $x^q = x+1$ if $x \in A_i \backslash (\max A_i)$, and $(\max A_i)^q = -i$, also, $(-i)^r = \min B_i$, $x^r = x + 1$ if $x \in B_i \backslash (\max B_i)$, and $(\max B_i)^r = -i$. Finally, let $q|_Q = \mathrm{id}|_Q$ and $r|_R = \mathrm{id}|_R$, where

$$Q = \mathbf{Z} \backslash \left(\dot{\bigcup_{i \in \mathbf{N}}} (A_i \cup \{-i\}) \right) = \dot{\bigcup_{i \in \mathbf{N}}} (B_i \backslash (\max B_i))$$

and

$$R = \mathbf{Z} \backslash \left(\dot{\bigcup_{i \in \mathbf{N}}} (B_i \cup \{-i\}) \right) = \dot{\bigcup_{i \in \mathbf{N}}} (A_i \backslash (\min A_i)) \mathbin{\dot\cup} \{0\}.$$

Then it is obvious that $q, r \in S_{\mathbf{Z}}$ have the prescribed orbits, and it only remains to show that $q \cdot r = z$. If $2 \leq i \in \mathbf{N}$, we have $(-i)^{q \cdot r} = (\min A_i)^r = (\max B_{i-1})^r = -(i-1) = (-i)^z$. Also $(-1)^{q \cdot r} = (\min A_1)^r = 0^r = 0 = (-1)^z$. Now let $a \in \mathbf{N}_0$. There is an $i \in \mathbf{N}$ such that $a \in (B_i \backslash (\max B_i)) \mathbin{\dot\cup} A_i$. If $a \in B_i \backslash (\max B_i)$, we get $a^{q \cdot r} = a^r = a + 1 = a^z$. If $a \in A_i \backslash (\max A_i)$, we have $a + 1 \in A_i \backslash (\min A_i) \subseteq R$ and thus $a^{q \cdot r} = (a+1)^r = a + 1 = a^z$. Finally, if $a = \max A_i$, we obtain

$$a^{q \cdot r} = (-i)^r = \min B_i = (\max A_i) + 1 = a + 1 = a^z.$$

This proves $q \cdot r = z$.

The following three results deal with finite symmetric groups. The first lemma, due to Bertram, gives a sufficient condition for $3 \leq k \in \mathbf{N}$ and an even permutation s of a finite set such that s can be written as a product of two permutations, each having only one nontrivial orbit which is of length k.

LEMMA 4.3 (BERTRAM [**3**, THEOREM 2]). *Let T be a finite set and $k \in \mathbf{N}$ with $3 \leq k \leq |T|$, and $s \in A_T$. Let $j = \sum_{2 \leq n} \overline{s}(n)$ be the number of nontrivial orbits of s. If $\frac{1}{2} \cdot (|s| + j) \leq k$, then $s \in (C_{T,k})^2$.*

This lemma will be used for the proof of the subsequent result.

LEMMA 4.4. *Let $k, n \in \mathbf{N}$ with $n < k$ and $k \geq 3$, and T a set with m elements, where $m \in \mathbf{N}$ is the least multiple of n ($2n$) with $m \geq k$ if n is odd (even), respectively. Assume $s \in S_T$ has only orbits of length n. If n is odd or if $k \neq 2n + 1$, then $s \in (C_{T,k})^2$. If n is even and $k = 2n + 1$, there are $q, r \in S_T$ with $s = q \cdot r$ such* *that q and r each have one orbit of length k, one orbit of length 2, and $m-k-2$ fixed points.*

PROOF. First assume that either n is odd or $k \neq 2n+1$. W.l.o.g. assume $n \neq 1$. Let $j = m/n$. Then $|s| = m$, s has j orbits of length n, and $s \in A_T$. By Lemma 4.3, it suffices to show that $m + j \leq 2k$. If n is odd, we have $m \leq k + n - 1$ and $n + j \leq k + 1$, hence $m + j \leq k + n - 1 + j \leq 2k$. Now let n be even. If $k \leq 2n$, we get $j = 2$ and $m + j = 2(n+1) \leq 2k$. If $2n + 2 \leq k \leq 4n$, clearly $j = 4$ and $m + j = 4n + 4 \leq 2k$. Finally let $2(i-1)n + 1 \leq k \leq 2in$ for some $3 \leq i \in \mathbf{N}$. Then $j = 2i$, and it suffices to show that $m + j = 2in + 2i \leq 4(i-1)n + 2$. But this inequality is equivalent to $i - 1 \leq (i-2)n$ which is true. Hence $m + j \leq 2k$ in any case.

Now assume that n is even and $k = 2n+1$. Then $m = 4n$. We put

$$T = \{1, 2, \ldots, 4n\}$$

and

$$s = (1\ 2\ \cdots\ n)(n+1\ n+2\ \cdots\ 2n)(2n+1\ 2n+2\ \cdots\ 3n)(3n+1\ 3n+2\ \cdots\ 4n).$$

If $n = 2$, let

$$q = (1\ 2\ 3\ 5\ 7)(6\ 8)(4)$$

and

$$r = (8\ 5\ 4\ 3\ 1)(6\ 7)(2).$$

If $n \geq 4$, let

$$q = (1\ 2\ \cdots\ n\ n+1\ n+2\ \cdots\ 2n-1\ 2n+1\ 3n+1)(2n+2\ 4n) \\ \cdot (2n)(2n+3)(2n+4)\cdots(3n)(3n+2)(3n+3)\cdots(4n-1),$$

and

$$r = (3n+2\ 3n+3\ \cdots\ 4n\ 2n+3\ 2n+4\ \cdots\ 3n\ 2n+1\ 2n\ n+1\ 1) \\ \cdot (2n+2\ 3n+1)(2)(3)\cdots(n)(n+2)(n+3)\cdots(2n-1).$$

Then, in any case, $q, r \in S_T$ satisfy the required conditions.

We will also need the following lemma on finite symmetric groups.

LEMMA 4.5. *Let $k, n \in \mathbf{N}$ with $3 \leq k \leq n$ and T a set with n elements. Let $s \in S_T$ have precisely one orbit (of length n). Then there are $q, r \in S_T$ such that $s = q \cdot r$, q has only orbits of lengths 1 or 2, and r has precisely one orbit of length k and possibly orbits of lengths 1 or 2, but no others.*

PROOF. W.l.o.g. let $T = \{1, 2, \ldots, n\}$ and $s = (1\ 2\ \cdots\ n)$. If $k = n$, let $q = \mathrm{id}_T$, $r = s$. If $n - k = 2j$ with $j \in \mathbf{N}$, put

$$q = (1)(2)\cdots(k-1)(k\ n)(k+1\ n-1)\cdots(k+j-1\ n-j+1)(k+j)$$

and

$$r = (1\ 2\ \cdots\ k)(k+1\ n)(k+2\ n-1)\cdots(k+j\ n-j+1).$$

If $n - k = 2j + 1$ with $j \in \mathbf{N}_0$, let

$$q = (1)(2)\cdots(k-1)(k\ n)(k+1\ n-1)\cdots(k+j\ n-j)$$

and

$$r = (1\ 2\ \cdots\ k)(k+1\ n)(k+2\ n-1)\cdots(k+j\ n-j+1)(n-j).$$

Then $q, r \in S_T$ satisfy the required conditions.

The next result describes products of two conjugate involutions with infinitely many fixed points:

LEMMA 4.6 (MORAN [**15**, COROLLARY 2.4]). *Let M be any infinite set and $p \in S_M$ an involution with infinitely many fixed points and support of cardinality $|M|$. Then, for any $s \in S_M$, $s \in [p]^2$ if and only if s has infinitely many orbits. In particular, $S_M = [p]^2$ iff M is uncountable.*

As a conclusion of the previous results, we have

LEMMA 4.7. *Let $p \in S$ have no infinite orbit, but infinitely many fixed points and infinitely many orbits of length 2. Then $s \in [p]^2$ for any permutation $s \in S$ with infinitely many orbits.*

PROOF. If s has at least one infinite orbit, $s \in [p]^2$ follows from a splitting-argument using Lemmas 4.2 and 4.6. Hence asume $\overline{s}(\aleph_0) = 0$ from now on. If p is an involution, then $p \in R_{\aleph_0}$ and $s \in [p]^2$ by Lemma 4.6. So let $\sum_{n \geq 3} \overline{p}(n) \neq 0$ now. By a splitting-argument, we may assume that p has precisely one orbit of length ≥ 3, say, of length $k \geq 3$. Clearly now we may distinguish between the following two (nonexclusive) cases.

Case I. Assume that s has infinitely many orbits of length $< k$.

There is $n \in \mathbf{N}$ with $n < k$ and $\overline{s}(n) = \aleph_0$. Let T be a union of finitely many orbits of s of length n such that $|T|$ is the least multiple of n $(2n)$ with $|T| \geq k$ if n is odd (even), respectively. By Lemma 4.4, there are $q, r \in S_T$ each consisting of precisely one orbit of length k and possibly of orbits of lengths 1 or 2, but no others, such that $s|_T = q \cdot r$. Together with a splitting-argument and Lemma 4.6, this implies $s \in [p]^2$.

Case II. Assume that s has at least two orbits, say, A and B, each of length $\geq k$.

By Lemma 4.5, there are $q_1, r_1 \in S_A$, $q_2, r_2 \in S_B$ such that $s|_A = q_1 \cdot r_1$, $s|_B = q_2 \cdot r_2$, q_1, r_2 each have only orbits of lengths 1 or 2, and r_1, q_2 each have precisely one orbit of length k and possibly orbits of lengths 1 or 2, but no others. Then $q = q_1 \oplus q_2$, $r = r_1 \oplus r_2 \in S_{A \dot\cup B}$ satisfy $s|_{A \dot\cup B} = q \cdot r$, $\overline{q}(k) = \overline{r}(k) = 1$, and $\overline{q}(m) = \overline{r}(m) = 0$ whenever $m \notin \{1, 2, k\}$. Together with a splitting-argument and Lemma 4.6, this shows $s \in [p]^2$.

Now we are ready for the

PROOF OF THEOREM 2. (a) Assume (+) does not hold. If $s \in S$ has precisely one (infinite) orbit, $s \notin [p]^2$ by Theorem 4.1, showing $S \neq [p]^2$.

(b)(1) By Lemma 4.7, it remains to show that $s \notin [p]^2$ if $s \in S$ has only finitely many orbits. Indeed, if we had $s \in [p]^2$ for such a permutation s, p would have only finitely many fixed points by Theorem 4.1, contradicting our assumption on p.

(b)(2) By Lemma 4.7, it remains to show that $s \in [p]^2$ if $s \in S$ has only finitely many orbits. But this follows by a splitting-argument from Lemma 4.2 and the well-known fact (see, e.g. [**20**, 10.1.17]) that every permutation is a product of two involutions.

As a consequence of Theorem 2(a) and a result in [**7**], we obtain the following condition for permutations $p \in S$ without infinite orbits which is necessary for $S = [p]^2$ to hold:

COROLLARY 4.8. *Let $p \in S$ satisfy $\overline{p}(\aleph_0) = 0$ and $S = [p]^2$. Then either $\overline{p}(1) = \overline{p}(2) = \sum_{n\geq 3} \overline{p}(n) = \aleph_0$, or there are $k, l, m \in \mathbf{N}$ with $k \leq l < m$, $m = k+l$, $l \geq 2$, and $\overline{p}(i) = \aleph_0$ for each $i \in \{k, l, m\}$.*

PROOF. Since $[p]^2$ contains, in particular, a transposition, by [**7**, Theorem 4.5] there are $k, l, m \in \mathbf{N}$ with $k \leq l < m$, $m = k+l$, and $\overline{p}(i) = \aleph_0$ for each $i \in \{k, l, m\}$. So either $l \geq 2$, or $k = l = 1$, $m = 2$, and $\sum_{n\geq 3} \overline{p}(n) = \aleph_0$ by Theorem 2(a).

As an immediate consequence of this result and Theorem 2(b), we obtain

COROLLARY 4.9. *Let $p \in S$ satisfy $\overline{p}(\aleph_0) = 0$ and $\overline{p}(m) = \aleph_0$ for at most one $m \in \mathbf{N}$ with $m \geq 2$. Then $S = [p]^2$ if and only if $\overline{p}(1) = \overline{p}(2) = \sum_{n\geq 3} \overline{p}(n) = \aleph_0$.*

Finally, we note a consequence for permutations of uncountably-infinite sets. This result uses and generalizes Moran [**15**, Corollary 2.4] (cf. Lemma 4.6).

COROLLARY 4.10. *Let M be any uncountable set and $\aleph$ a cardinal with $\aleph_0 \leq \aleph \leq |M|$. Let $p \in S_M$ have $\aleph$ fixed points, $|M|$ orbits of length 2, and at most $\aleph$ orbits of length ≥ 3. Then $S_M = [p]^2$.*

PROOF. Note that any permutation of M has infinitely many orbits, since M is uncountable. So the result follows from a splitting-argument using Lemmas 4.6 and 4.7 provided that $\overline{p}(\aleph_0) = 0$. Then this result obtained so far for permutations of M without infinite orbits and [**7**, Theorem 1(b)] imply the assertion of the corollary in case that p has at least one infinite orbit.

Finally we just remark that the Baer-Schreier-Ulam-Theorem [**1, 19**] on the Jordan-Hölder decomposition series of S and Ore's theorem [**18**] that every $p \in S$ is a commutator immediately follow from our results, cf. Droste and Göbel [**9**, §4]. For further group-theoretical applications of results of this type see [**7–11, 17**].

REFERENCES

1. R. Baer, *Die Kompositionsreihe der Gruppe aller eineindeutigen Abbildungen einer unendlichen Menge auf sich*, Studia Math. **5** (1934), 15–17.
2. E. A. Bertram, *Permutations as products of conjugate infinite cycles*, Pacific J. Math. **39** (1971), 275–284.
3. ——, *Even permutations as a product of two conjugate cycles*, J. Combin. Theory Ser. A **12** (1972), 368–380.
4. ——, *On a theorem of Schreier and Ulam for countable permutations*, J. Algebra **24** (1973), 316–322.
5. G. Boccara, *Sur les permutations d'un ensemble infini dénombrable, dont toute orbite essentielle est infinie*, C. R. Acad. Sci. Paris Sér. A **287** (1978), 281–283.
6. Hsü Ch'eng-hao, *The commutators of the alternating group*, Sci. Sinica **14** (1965), 339–342.
7. M. Droste, *Products of conjugacy classes of the infinite symmetric groups*, Discrete Math. **47** (1983), 35–48.
8. ——, *Classes of words universal for the infinite symmetric groups*, Algebra Universalis (to appear).
9. M. Droste and R. Göbel, *On a theorem of Baer, Schreier and Ulam for permutations*, J. Algebra **58** (1979), 282–290.
10. ——, *Products of conjugate permutations*, Pacific J. Math. **92** (1981), 47–60.
11. M. Droste and S. Shelah, *On the universality of systems of words in permutation groups* (to appear).
12. A. B. Gray, *Infinite symmetric and monomial groups*, Ph.D. Thesis, New Mexico State Univ., Las Cruces, N.M., 1960.
13. D. H. Husemoller, *Ramified coverings of Riemann surfaces*, Duke Math. J. **29** (1962), 167–174.
14. G. Moran, *The algebra of reflections of an infinite set*, Notices Amer. Math. Soc. **73T** (1973), A193.

15. ——, *The product of two reflection classes of the symmetric group*, Discrete Math. **15** (1976), 63–77.
16. ——, *Parity features for classes of the infinite symmetric group*, J. Combin. Theory Ser. A **33** (1982), 82–98.
17. ——, *Of planar Eulerian graphs and permutations* (to appear).
18. O. Ore, *Some remarks on commutators*, Proc. Amer. Math. Soc. **2** (1951), 307–314.
19. J. Schreier and S. Ulam, *Über die Permutationsgruppe der natürlichen Zahlenfolge*, Studia Math. **4** (1933), 134–141.
20. W. R. Scott, *Group theory*, Prentice-Hall, Englewood Cliffs, N.J., 1964.

FACHBEREICH 6, MATHEMATIK, UNIVERSITÄT ESSEN, 4300 ESSEN 1, WEST GERMANY