

PRODUCTS OF CONJUGATE PERMUTATIONS

MANFRED DROSTE AND RÜDIGER GÖBEL

Using combinatorial methods, we will prove the following theorem on the permutation group S_0 of a countable set: If a permutation $p \in S_0$ contains at least one infinite cycle then any permutation of S_0 is a product of three permutations each conjugate to p . Similar results for permutations of uncountable sets are shown and classical group theoretical results are derived from this.

1. Introduction. We will deal with the symmetric group S_ν of all permutations of a set of cardinality \aleph_ν . Let us denote by $|p|$ the cardinality of the support [the underlying set without fixed points], by $(p)_\infty$ the set of infinite cycles and by p^{S_ν} the set of all conjugates of some permutation $p \in S_\nu$. The following theorem is shown in E. A. Bertram [3] and G. Moran [6] (see also [4]).

If $s, p \in S_\nu$, $|s| \leq |p|$ and $|p|$ is infinite, then s is a product of 4 elements each conjugate to p . Furthermore, 4 is minimal with this property. The latter follows by examining $s = (123)$ and any permutation p containing only transpositions (without fixed points) in its disjoint cycle decomposition, cf. G. Moran [6, p. 76] and [4, p. 288, 289]. If p is odd and s is even (with finite supports), then obviously $s \notin (p^{S_\nu})^3$, and similar examples with finite $|p|$ show $S_\nu \neq (p^{S_\nu})^2$.

Therefore, we have to exclude such examples in order to improve the bound 4 of the theorem above. From the last two examples follows our assumption $|p| = \aleph_\nu$ and from the first, the more specific hypothesis $|(p)_\infty| \geq 1$. It is the aim of this paper to show that $|p| = \aleph_\nu$ and $|(p)_\infty| \geq 1$ will be sufficient to improve the bound:

THEOREM 1. *Let $s, p \in S_0$.*

(a) *If $|(s)_\infty| \geq 1$ and $|(p)_\infty| \geq 1$, then s is a product of two elements each conjugate to p .*

(b) *If $|(s)_\infty| = 0$ and $|(p)_\infty| \geq 2$, then s is a product of two elements each conjugate to p .*

(c) *If $|(s)_\infty| = 0$ and $|(p)_\infty| = 1$, then s is a product of three elements each conjugate to p .*

Furthermore, the number of factors is minimal and may be replaced by any greater integer.

THEOREM 2. *Let $s, p \in S_\nu$ and $|(p)_\infty| = \aleph_\nu$. Then s is a product of n elements each conjugate to p for any $n \geq 2$.*

If $\nu = 0$ and p is just one infinite cycle (without fixed points), Theorem 1 sharpens various results of E. A. Bertram [2; pp. 275, 276, 278, 279, 281, 283].

If $\nu = 0$ it shows the range of validity of a conjecture in another interesting paper of E. A. Bertram's [3; p. 322] which fails in general as already shown in G. Moran [6] and independently in [4]. If p consists of \aleph_ν infinite cycles only [and $\nu \geq 0$], Theorem 2 is due to A. B. Gray [5]. In addition, we obtain an interesting generalization of O. Ore's theorem [7; p. 313] that all elements of S_ν are commutators: If $w(x_1, \dots, x_n)$ is a word of group theory with free variables x_1, \dots, x_n , P. Hall calls a group G w -elliptic of degree d , if any element of G is a product of at most d w -elements $w(g_1, \dots, g_n)$ with $g_1, \dots, g_n \in G$. From Theorem 2 we derive:

S_ν is w -elliptic of degree 2 for any word w . The degree 2 cannot be improved in general.

In order to extend Ore's theorem, that S_ν is w -elliptic of degree 1 if $w = w(x_1, x_2) = x_1^{-1} \cdot x_2^{-1} \cdot x_1 \cdot x_2$, to its full generality, it would be interesting to classify all words w such that S_ν is w -elliptic of degree 1.

2. Notation. $K \leq M$: K is a subset of M .

$K \cup K'$, $\bigcup_{i \in I} K_i$ are disjoint unions; $f|_K$ is the restriction of a map f to K . a^f denotes the value of the mapping f at a , and so maps are action from the right.

\mathbf{Z} denotes the integers, $\mathbf{Z}^0 = \mathbf{Z} \setminus \{0\}$.

N denotes the positive integers, $N_0 = N \cup \{0\}$, $N_\infty = N \cup \{\infty\}$.

$-N$ denotes the negative integers.

$g^G = \{x^{-1} \cdot g \cdot x; x \in G\}$ denotes the conjugacy class of g in the group G .

S_ν denotes the group of all permutations of a set M of cardinality \aleph_ν .

Particular permutations are finite cycles of length n of M which we denote by $(x_1 x_2 \dots x_n) = (x_i)_{i \in [1, n]}$ where $[1, n]$ is the interval of integers from 1 to n and $x_i \in M$. Infinite cycles are denoted by $(\dots x_{-1} x_0 x_1 \dots) = (x_i)_{i \in \mathbf{Z}}$. Sometimes it will be convenient to replace the index sets $[1, n]$ or \mathbf{Z} of cyclic permutations by order isomorphic sets; e.g., $[n+1, 2n]$. Similarly \mathbf{Z}^0 will often serve as an index set for an infinite cycle. Then cycles act in the natural way (from left to right) on their underlying set and are extended trivially to M .

Cycles will be identified with subsets of M which carry a natural order given by a bijection onto $[1, n]$ or \mathbf{Z} , and its fixed points will not be mentioned explicitly. We will reserve z for the infinite "shift-cycle" $z = (\dots -2 -1 1 2 \dots)$ acting on \mathbf{Z}^0 .

It is well known that a permutation can be written uniquely as a product of possibly infinitely many cycles, which act nontrivially on pairwise disjoint subsets of M . For details we refer to H. Wielandt [9].

If $p \in S_\nu$, let $(p)_k$ be the uniquely determined set of all cycles of length $k \in N_\infty$ of this disjoint-cycle decomposition (DCD) of p , $|(p)_k|$ its cardinality, $\{p\}_k$ the set of all elements in the support of $(p)_k$. Let $\{p\}_1$ denote the set of fixed points of p . Let $\{p\} = \bigcup_{1 \neq k \in N_\infty} \{p\}_k$ be the support of p and $|p| = |\{p\}|$ its cardinality. We put $(p) = \bigcup_{1 \neq k \in N_\infty} (p)_k$.

The following well-known result will be used without mentioning it again:

Two permutations $a, b \in S_\nu$ are conjugate if and only if $|(a)_k| = |(b)_k|$ for all $k \in N_\infty$, cf. H. Wielandt [9, Lemma 2.5, p. 6].

3. Essential constructions for Theorem 1(a). The essential techniques of this paper are the following natural and elementary *cutting-* and *inserting-arguments*:

If I and J are linearly ordered sets, write $I \sim J$ if there is an order-isomorphism from I onto J . If j is an immediate successor of i in I , we will write $j = i + 1$ or $i = j - 1$ in the following.

Let $c = (c_i)_{i \in I}$ be a cyclic permutation of a given set M with $I \sim Z$ or $I \sim [1, n]$ for some $n \in N$. If $K \neq \emptyset$ is a subset of I with the induced order and $K \sim Z$ or $K \sim [1, m]$ for some $m \in N$, we are led to a new cycle $(c_i)_{i \in K}$. This cycle acts in the natural way on its support $\{c_i, i \in K\}$ and all c_i , for $i \in I \setminus K$, are fixed points. This process will be called "*cutting off $I \setminus K$ (or $\{c_i, i \in I \setminus K\}$) from c* ".

Now let $I \sim Z$ and let $K = [1, n]$ for some $n \in N$ be disjoint from I . For $i \in I$ we will consider a new set $X = I \cup K$ which carries a natural order induced from i, I and K :

Let $x \leq y$ for $x, y \in X$ if one the following conditions is satisfied:

- (a) $x, y \in I$ and $x \leq y$ with respect to the order in I .
- (b) $x, y \in K$ and $x \leq y$ with respect to the order in K .
- (c) $x \in I, y \in K$ and $x \leq i$ with respect to the order in I .
- (d) $y \in I, x \in K$ and $i < y$ with respect to the order in I .

Then $X \sim Z$ and this process will be called "*inserting K into I at i* ". If $i + 1$ is the successor of i in I , we will say "*inserting K between i and $i + 1$ (or after i)*" as well.

Furthermore, let $c_k \in M$ be given for each $k \in K$. Assume $\{c_i; i \in I\} \cap \{c_k; k \in K\} = \emptyset$ and that the mapping $k \mapsto c_k$ for $k \in K$ is one-to-one (as well as $i \mapsto c_i$ for $i \in I$). Inserting K into I at i leads naturally to a new cycle $(c_i)_{i \in X}$ which acts according to the order of X on its support $\{c_i, i \in X\}$. This will be called "*inserting $(c_i)_{i \in K}$* ".

into $(c_i)_{i \in I}$ at i " (or at c_i or between i and $i + 1$ or between c_i and c_{i+1} if there is no ambiguity).

More generally, for any permutation d on M consisting of at least one infinite cycle in its DCD and any element $x \in \{d\}_\infty$, we define "inserting $(c_i)_{i \in K}$ after $x \in M$ into d " by "inserting $(c_i)_{i \in K}$ into that infinite cycle c of d which contains x in its support". We will define a two-parameter family $g(n, k)$ of infinite cycles acting on \mathbf{Z}^0 for all $k \in N_\infty$ and $1 \leq n \leq k$. These cycles will be modified, in particular, by cutting- and inserting-arguments.

3.1. Construction of $g(n, k) \in S_{\mathbf{Z}^0}$ for $k \in N_\infty$ and $1 \leq n \leq k$:

(a) If $m \in \mathbf{Z}$ and $1 \leq n \leq k \in N$, we define

$$\begin{aligned} g(n, k)_0 &= n - 1 \quad \text{if } n \neq 1, \\ g(n, k)_{2m} &= (2m - 1)k + n - 1 \quad \text{if } m \geq 1 \quad \text{and} \\ g(n, k)_{2m} &= -2mk + n - 1 \quad \text{if } m \leq -1, \\ g(n, k)_{2m+1} &= -[(2m + 1)k + n] \quad \text{if } m \geq 0 \quad \text{and} \\ g(n, k)_{2m-1} &= 2mk - n \quad \text{if } m \leq 0. \end{aligned}$$

(a*) Then put

$$\begin{aligned} g(1, k) &= (g(1, k))_{i \in \mathbf{Z}^0} = (\cdots g(1, k)_{-2} g(1, k)_{-1} g(1, k)_1 g(1, k)_2 \cdots) \quad \text{and} \\ g(n, k) &= (g(n, k))_{i \in \mathbf{Z}} = (\cdots g(n, k)_{-2} g(n, k)_{-1} g(n, k)_0 g(n, k)_1 g(n, k)_2 \cdots) \\ &\quad \text{for all } 1 \neq n \leq k \in N. \end{aligned}$$

(b) If $k = \infty$ and $1 \neq n \in N$, $j \in \mathbf{Z}$ define

$$\begin{aligned} g(n, \infty)_0 &= 2(n - 2)^2 + 1 \quad \text{and} \quad g(n, \infty)_2 = 2n^2 - 2n + 3, \\ g(n, \infty)_{2j} &= 2[(n + j)^2 - 2j - 3n] + 5 \quad \text{for } j \geq 2, \\ g(n, \infty)_{2j} &= 2[(n - j - 1)^2 - 2n + j] + 7 \quad \text{for } j \leq -1, \\ g(n, \infty)_{2j+1} &= -g(n, \infty)_{2(j+1)} - 1. \end{aligned}$$

(b*) Then put

$$\begin{aligned} g(1, \infty) &= g(1, 2) \quad \text{and} \\ g(n, \infty) &= (g(n, \infty))_{i \in \mathbf{Z}} \\ &= (\cdots g(n, \infty)_{-2} g(n, \infty)_{-1} g(n, \infty)_0 g(n, \infty)_1 g(n, \infty)_2 \cdots) \\ &\quad \text{for all } 1 \neq n \in N. \end{aligned}$$

(c) Let

$$g_k = \prod_{n=1}^k g(n, k).$$

Next we modify $g(n, k)$ and derive a second two-parameter family of cycles:

3.2. Construction of $h(n, k) \in S_{\mathbf{Z}^0}$ for all $k \in N_\infty$ and $1 \leq n \leq k$:

Define $h(n, k)_{2j} = 2jk + n$ for all $j \geq 0$, $h(n, k)_{2j} = -(2j + 1)k + n$ if $j \leq -1$ and $h(n, k)_{2j+1} = -h(n, k)_{2j}$ for all $j \in \mathbf{Z}$ and $k \in N$. If $k = \infty$, put $h(n, \infty)_{2j} = g(n, \infty)_{-2j} + 1$ and $h(n, \infty)_{2j+1} = g(n, \infty)_{-(2j+1)}$ for all $n \neq 1$ using (3.1).

Then define

$$h(n, k) = (h(n, k)_i)_{i \in \mathbf{Z}} = (\cdots h(n, k)_{-2} h(n, k)_{-1} h(n, k)_0 h(n, k)_1 \cdots)$$

for all $n \in N$ and $k \in N_\infty$ and put $h(1, \infty) = h(1, 2)$. Let $h_k = \prod_{n=1}^k h(n, k)$.

LEMMA 3.3. *Each infinite cycle [which moves every element] of a countable set is a product of two permutations each consisting of k infinite cycles and no other cycles (including fixed points) for all $k \in N_\infty$.*

Proof. We may assume w.l.o.g. $s \in S_{z^0}$ and $s = z$ is the given infinite cycle and $k \in N_\infty$. Elementary calculations show that the cycles $g(n, k)$ with $1 \leq n \leq k$ constructed in (3.1) define a decomposition of \mathbf{Z}^0 into k subsets of cardinality \aleph_0 . Hence $g_k = \prod_{n=1}^k g(n, k)$ consists of k infinite cycles. Similarly $h_k = \prod_{n=1}^k h(n, k)$ consists of k infinite cycles, and $z = g_k h_k$ can be checked elementwise (recall that by our convention g_k acts first).

LEMMA 3.4. *Let $p = a \cdot b \cdot c$ be a product of three permutations of S_0 each consisting of fixed points and infinite cycles only. If $|(a)_\infty| = |(b)_\infty| = 1$, $|\{a\} \cap \{b\}| = \infty$ and $\{a\} \cup \{b\} = \{c\}_1$, then p is a product of two permutations g and h each consisting of just one infinite cycle and with fixed points precisely $\{b\} \setminus \{a\}$ and $\{a\} \setminus \{b\}$ respectively.*

Proof. Let \mathbf{Z} be the index set of the following cycles. We may assume w.l.o.g. $a = (\cdots -3 -2 -1 0 1 2 3 \cdots)$ and $b = (\cdots -3^* -2^* -1^* 0^* 1^* \cdots)$ which have a set X of infinitely many numbers in common. Assume $e|_{\{c\}} = \prod_{j \in J} e_j$ is its DCD with infinite cycles $e_j = (\cdots j_{-2} j_{-1} j_0 j_1 j_2 \cdots)$.

First we decompose X into $|J|$ countable subsets. Hence, the numbers in X may be denoted as pairs j/n for $n \in N_0$ and $j \in J$. The following modification of the cycle a leads to the infinite cycle g which moves all the elements of $\{a\} \cup \{c\}$ and no others: Insert j_0 into a between $j/0 - 1$ and $j/0$, and j_{-k}, j_k between $j/k - 1$ and j/k for all $k \in N$ and $j \in J$. Define g to be the identity on the set $\{b\} \setminus \{a\}$.

Next we modify b to obtain an infinite cycle h : Insert j_{k+1}, j_{-k} into b between (j/k) and $(j/k)^b$ for all $k \in N_0, j \in J$ and define h to be the identity on $\{a\} \setminus \{b\}$.

We will show that $p = g \cdot h$ and distinguish between five cases:

- (i) $x \in \{a\}$ and $x + 1 \in X$.
- (ii) $x \in \{a\}$ and $x + 1 \notin X$.
- (iii) $x = j_{-k}$ for some $k \in N$ and $j \in J$.
- (iv) $x = j_k$ for some $k \in N_0$ and $j \in J$.
- (v) $x \notin \{g\}$.

In case (i) we have $x = j/k - 1$ for some $k \in N_0$ and $j \in J$. Hence $x^{g^k} = (j/k - 1)^{g^k} = j_{-k}^h = (j/k)^b = (j/k - 1)^{ab} = x^p$.

In case (ii) we have $x^{g^h} = (x + 1)^h = x + 1 = (x + 1)^b = x^{ab} = x^p$.

In case (iii) we get $x^{g^h} = j_{-k}^{g^h} = j_k^h = j_{-k+1}^h = j_{-k}^{g^h} = x^p = x^p$.

In case (iv) we have $x^{g^h} = j_k^{g^h} = (j/k)^h = j_{k+1}^h = j_k^h = x^p$.

In case (v) we have $x \in \{b\} \setminus \{a\}$ and $x^{g^h} = x^h = x^b = x^{ab} = x^p$. \square

LEMMA 3.5. *If s and p are permutations of a countable set each containing at least one infinite cycle, then s is a product of two elements conjugate to p .*

Proof. For brevity, write $m = |(p)_\infty|$. Then by our assumption $m \in N_\infty$. Set $k = 2$ if $m = \infty$, and $k = m$ otherwise. We will consider first the case $|(s)_\infty| = 1$ which splits into four parts.

Case 1. s contains one finite cycle and p has no finite cycles in its DCD.

First we label the underlying countable set in an appropriate manner: Let $f = (1^* 2^* \dots n^*)$ be the only finite cycle of s . If $c = (\bar{1} \bar{2} \dots \overline{n-1})$ derive z^* from the shift-cycle z acting on Z^0 inserting c into z after $(2r + 1)k$ for some positive integer r . Then w.l.o.g. choose the underlying set $M = Z^0 \cup \{c\} \cup \{f\}$ and $s = z^* \cdot f$. (This includes $s = z(1^*)$ if $n = 1$.)

Observe again, that permutations are extended trivially to the bigger set M .)

In order to define the elements g^* and h^* conjugate to p such that $s = g^* \cdot h^*$, we choose $g = g_m$ and $h = h_m$ defined in (3.1) and (3.2) respectively, acting on Z^0 . Let $e = (1^* \bar{1} 2^* \bar{2} \dots \overline{n-1} n^*)$ (and, in particular, $e = (1^*)$ if $n = 1$). We obtain \bar{g} by inserting e into $g(1, m)$ after the element $(2r + 1)k = g(1, m)_{2r+2}$. Similarly, insert e into $h(1, m)$ after the element $-(2r + 3)k - 1 = [(2r + 1) \cdot k]^{g(1, m)} = g(1, m)_{2r+3} = h(1, m)_{-2r-3}$ to obtain \bar{h} . Let $g^* = \bar{g} \cdot \prod_{n=2}^m g(n, m)$ and $h^* = \bar{h} \cdot \prod_{n=2}^m h(n, m)$. The new elements consist of m infinite cycles, since all cycles of g and h remain unchanged, except for the two first ones $g(1, m)$ and $h(1, m)$, which are "enlarged". Thus g^* , h^* are conjugate to p , and their product $g^* \cdot h^*$ equals s .

Case 2. s contains no finite cycles and p has, beside infinite cycles, only one finite cycle of odd length $2n + 1$.

In this case we need two cycles $f = (1^* 2^* \cdots (2n + 1)^*)$ and $e = (\bar{1} \bar{2} \cdots \overline{2n + 1})$ of length $2n + 1$. They are disjoint and contain no integers. Chose two different natural numbers x and y . Then we obtain an infinite cycle z^* acting on $\mathbf{Z}^0 \cup \{e\} \cup \{f\}$ by inserting e into z after the element $(2x + 1)k$ and f into z after the element $(2y + 1)k$. We choose $s = z^*$ w.l.o.g. Next we take $g = g_m$ from (3.1) and insert $(\bar{2} \bar{4} \cdots \overline{2n} \bar{1} \bar{3} \cdots \overline{2n + 1})$ into the cycle $g(1, m)$ of g after the element $(2x + 1)k = g(1, m)_{2x+2}$ which leads to a product g' of m disjoint infinite cycles acting on $(\mathbf{Z}^0) \cup \{e\}$. Similarly, take $h = h_m$ from (3.2) and insert $(1^* 3^* \cdots (2n + 1)^* 2^* 4^* \cdots 2n^*)$ into the cycle $h(1, m)$ of h after the element $-(2y + 3)k - 1 = h(1, m)_{-2y-3}$ to get a product h' of m disjoint cycles acting on $(\mathbf{Z}^0) \cup \{f\}$. Finally, put $g^* = g' \cdot f^{-1}$ and $h^* = h' \cdot e^{-1}$, which are the required elements, obviously conjugate to p and with product s by construction. For later use we remark that if p has only one fixed point (i.e., $n = 0$) then the fixed point $1^*(\bar{1})$ of $g^*(h^*)$ is an element of the infinite cycle $h(1, m)$ ($g(1, m)$) of $h(g)$.

Case 3. s contains no finite cycles and p has, beside infinite cycles, only one finite cycle of even length $2n$ in its DCD.

Let $s = z$ w.l.o.g. and choose any natural number r . Next we define g^* acting on \mathbf{Z}^0 by a modification of $g = g_m$ taken from (3.1). First, cut the interval $[-2r - 2n + 1, -2r]$ from the first cycle $g(1, m)$ of g to obtain a permutation g' . The missing numbers are $g(1, m)_{-2(r+j)} = 2kr + 2kj$ and $g(1, m)_{-2r-2t-1} = -2kr - 2kt - 1$ for $0 \leq j \leq n - 1$ and $0 \leq t \leq n - 1$. Multiplication of g' with the disjoint cycle of length $2n$ $(-2kr - 2(n - 1)k - 1, 2kr + 2(n - 1)k, -2kr - 2(n - 2)k - 1, \dots, 2kr + 2k, -2kr - 1, 2kr)$ will define g^* . Then g^* is obviously conjugate to p . Similarly, take $h = h_m$ from (3.2) and cut the interval $[2r, 2r + 2n - 1]$ from $h(1, m)$. This leads to a product h' of m cycles acting nontrivially one the set $\mathbf{Z} \setminus \{0, 2kr + 2kj + 1, -2kr - 2kt - 1; 0 \leq j \leq n - 1, 0 \leq t \leq n - 1\}$.

Multiplication of h' with the disjoint cycle of length $2n$ $(2kr + 1, -2kr - 1, 2kr + 1 + 2k, \dots, 2kr + 1 + (n - 1)2k, -2kr - 1 - (n - 1)2k)$ leads to a permutation h^* conjugate to p .

Elementary calculation shows $s = g^* \cdot h^*$.

Case 4. $|(s)_\infty| = 1$ (and no other restriction).

The inserting-argument described in Cases 1 and 2 can be applied simultaneously for all finite cycles of s and all odd cycles of p using (possibly infinitely many) different natural numbers r, x, y .

For even cycles of p , apply Case 3 (possibly infinitely many times simultaneously) at different numbers r at a distance such that the cutting described above can be carried out at disjoint intervals

separated by nonempty open intervals of the index set \mathbf{Z}^0 . Thus we get permutations g^* , h^* conjugate to p with $s = g^* \cdot h^*$; furthermore we can carry out the cutting and inserting so that g^* and h^* have infinite cycles g' resp. h' in their DCD with $|\{g'\} \cap \{h'\}| = \infty$ and $\{g^*\}_1 \subseteq \{h'\}$ resp. $\{h^*\}_1 \subseteq \{g'\}$. (Compare the remark at the end of Case 2.)

Now we will drop the restriction $|(s)_\infty| = 1$ and consider (3.5) in general. Because of Case 4 we may assume $|(s)_\infty| \geq 2$. Hence we may decompose s into a product $u \cdot v$ of permutations with disjoint supports $\{u\}$ and $\{v\}$ such that u contains just one infinite cycle and all the finite cycles (including fixed points) of s and v consists of all the other infinite cycles in the DCD of s . Let C be the complement of $\{v\}$ in the underlying set. Let us consider for a moment u as a permutation on C . By Case 4 there are permutations g^* and h^* on C such that $u = g^* \cdot h^*$ and $|(g^*)_n| = |(h^*)_n| = |(p)_n|$ for all $n \in \mathbf{N}_\infty$ and there are two infinite cycles g' , h' in the DCD of g^* , h^* respectively with $\{g'\} \cap \{h'\}$ infinite, and so that $\{h'\}$ includes all points fixed by g^* , $\{g'\}$ contains all points fixed by h^* . Let g^+ (h^+) be the product of all the other cycles in the DCD of g^* (h^*). Thus we have $g^* = g^+ \cdot g'$ ($h^* = h^+ \cdot h'$), and

$$(*) \quad \{g^*\}_1 \subseteq \{g^+\}_1 \cap \{h'\} \quad (\{h^*\}_1 \subseteq \{h^+\}_1 \cap \{g'\}) .$$

Now consider g' , h' , v as permutations of the set $D = (\{g'\} \cup \{h'\}) \cup \{v\}$. Apply Lemma 3.4 to get $g' \cdot h' \cdot v = \bar{g} \cdot \bar{h}$ on D , where \bar{g} (\bar{h}) consists precisely of one infinite cycle and fixes the points of the set $\{h'\} \setminus \{g'\}$ ($\{g'\} \setminus \{h'\}$). Now consider again all permutations as acting on all of M . We have $s = u \cdot v = g^* \cdot h^* \cdot v = g^+ \cdot g' \cdot h' \cdot v \cdot h^+ = (g^+ \cdot \bar{g}) \cdot (\bar{h} \cdot h^+)$. Since $\{g^+\} \cap \{\bar{g}\} = \emptyset$ we have

$$\{g^+ \cdot \bar{g}\}_1 = \{g^+\}_1 \cap \{\bar{g}\}_1 = \{g^+\}_1 \cap (\{h'\} \setminus \{g'\}) = \{g^*\}_1 \quad \text{by } (*).$$

Therefore $|(g^+ \cdot \bar{g})_n| = |(g^*)_n| = |(p)_n|$ for all $n \in \mathbf{N}_\infty$. A similar argument holds for $\bar{h} \cdot h^+$. Hence $g^+ \cdot \bar{g}$ and $\bar{h} \cdot h^+$ are the required elements. \square

4. Essential constructions for Theorem 1(b). As in § 3, we first define a permutation on a countable set which will be modified by a cutting- and inserting-argument. In this section we will very frequently make use of the permutations $a(k)$ for $k \in \mathbf{Z}$ acting on \mathbf{Z} defined by $x^{a(k)} = x + k$ for all $x \in \mathbf{Z}$. Then $a(k)$ consists of $|k|$ infinite cycles if $k \neq 0$, the permutations $a(k)$ and $a(-k)$ are inverse elements and $a(0)$ is the identity. In the following, an interval $[m, n]$ will be identified with the cyclic permutation $(m, m + 1, \dots, n)$ which acts trivially on the remaining points of \mathbf{Z} . The following notion will be useful:

DEFINITION 4.1. Let $\{s_i; i \in \mathbf{Z}\}$ be a decomposition of \mathbf{Z} into finite (naturally ordered) intervals s_i such that

- (i) if $x \in s_i, y \in s_j$ and $x \leq y$, then $i \leq j$;
- (ii) if $x \in s_i$, then $x < 0$ iff $i < 0$.

For $i \in \mathbf{Z}$ let $\sigma(i) = 1$ if $i \geq 0$ and $\sigma(i) = -1$ if $i < 0$. Then the permutation $s = \prod_{i \in \mathbf{Z}} s_i^{\sigma(i)}$ acting on \mathbf{Z} will be called a uniform permutation.

Observe that s maps negative integers onto negative integers and that s leaves N_0 invariant. Under the action of s any negative integer moves at most one step down and any nonnegative integer moves at most one step up, i.e.,

$$i^s \geq i - 1 \text{ for all } i \in -N \quad \text{and} \quad i^s \leq i + 1 \text{ for all } i \in N_0.$$

Here is a typical example

$$s = \dots (-6) (-4 -5) (-1 -2 -3) (0 1 2 3) (4 5 6 7) (8) \dots$$

In this case $s_{-2} = [-5, -4]$, $s_{-1} = [-3, -1]$, $s_0 = [0, 3]$, $s_1 = [4, 7] \dots$. It is clear that every permutation on \mathbf{Z} without infinite cycles is conjugate to a uniform permutation.

Immediately from (4.1) follows:

LEMMA 4.2. Any permutation of a countable set without infinite cycles is a product of two (conjugate) permutations each consisting of precisely k infinite cycles for any natural number $k \geq 2$.

Proof. We may assume that s is uniform, say $s = \prod_{i \in \mathbf{Z}} s_i^{\sigma(i)}$. Let $a = a(k)$ and $b = a(-k)$ defined as above, then the product $c = \prod_{i \leq -1} s_i^{\sigma(i)} \cdot a$ operators after "Lenin's tactics": Hence every number moves at least one step up under the action of c . Consequently, c consists of infinite cycles only. Since c coincides with a on the positive integers, c decomposes into exactly k infinite cycles. The dual argument shows that $d = b \cdot \prod_{i \geq 0} s_i$ consists of precisely k infinite cycles as well. Since $a \cdot b = 1$, we get $s = c \cdot d$.

The following lemma generalizes (4.2) and will be used to show (4.4), which is exactly the part (b) of Theorem 1.

LEMMA 4.3. Let s be a permutation of a countable set M without infinite cycles and let G and H be subsets of $\{s\}$ with the following properties:

- (i) If $\{s_i\} \cap G \neq \emptyset$, then $\{s_i\} \not\subseteq G$ and $\{s_i\} \cap H = \emptyset$ and if $\{s_i\} \cap H \neq \emptyset$, then $\{s_i\} \not\subseteq H$ and $\{s_i\} \cap G = \emptyset$ for all cycles s_i of s .
- (ii) $\{s_i\} \cap (G \cup H) = \emptyset$ for infinitely many cycles $s_i \neq 1$ of s .

Then for every natural number $k \geq 2$, there are permutations g and h on M such that $s = g \cdot h$, $\{g\}_1 = G$, $\{h\}_1 = H$ and g, h consist of exactly k infinite cycles and fixed points.

REMARK. G and H are disjoint subsets of the support of s by construction. We obtain (4.2) for $G = H = \emptyset$.

Proof. Case 1. Let s be without fixed points. W.l.o.g. choose s to be a uniform permutation so that $G \subseteq -N$, $H \subseteq N$ and $\min(s_i) \notin G \cup H$ for all $i \in \mathbf{Z}$. This is possible by (i). Because of (ii) we may further assume that $\bigcup_{j=1}^k \{s_{i+j}\} \cap (G \cup H) = \emptyset$ for infinitely many positive and infinitely many negative $i \in \mathbf{Z}$. Let c, d be defined as in (4.2). We observe that for every infinite cycle d_∞ of d and $i \in \mathbf{Z}$: $|\{d_\infty\} \cap \bigcup_{j=1}^k \{s_{i+j}\}| \geq 1$, hence we get

(iii) For every infinite cycle $d_\infty \in (d)$ and $c_\infty \in (c)$ the sets $(\{d_\infty\} \cap N) \setminus (G \cup H)$ and $(\{c_\infty\} \cap -N) \setminus (G \cup H)$ are infinite.

Next we use the argument of (4.2), but a more complex version. Define a map $d^*: \mathbf{Z} \rightarrow \mathbf{Z}$ by $x^{d^*} = x$ for all $x \in H$ and $x^{d^*} = \max(\{x^{d^n}; n \in N\} \setminus H)$ for all $x \in \mathbf{Z} \setminus H$. Thus, d^* fixes every element of H , and for $x \notin H$, $x^{d^*} = x^d$, unless $x^d \in H$, in which case $x^{d^*} = x^{d^n}$, where $n \in N$ is first with $x^{d^n} \in H$. The map d^* is obviously injective and well defined, since $H \subseteq N$. If $y \in H$, then $y^{d^*} = y$ and if $y \in \mathbf{Z} \setminus H$, define $x = \min(\{y^{d^{-m}}; m \in N\} \setminus H)$, which exists by (iii). Hence $x^{d^*} = y$ by definition of d^* and d^* is surjective as well. Therefore d^* is a permutation of \mathbf{Z} whose set of fixed points is H , and whose only nontrivial cycles are k infinite cycles.

We note that $x^{d^*} < x$ whenever $x \notin H$. As in (4.2) we put $c^* = s \cdot d^{*-1}$, which operates again after ‘‘Lenin tactics’’: If $x^s \in \mathbf{Z} \setminus H$, then $x^{c^*} = (x^s)^{d^{*-1}} \geq (x^s)^{d^{-1}} > x$ because $k \geq 2$. If $x^s \in H$, then $x^s \neq \min\{s_i\}$ for all $i \geq 0$ by assumption on H , hence $x \neq \max\{s_i\}$ for all $i \geq 0$ and $x^{c^*} = x^s = x + 1 > x$. Therefore c^* has infinite cycles only. Since c^{*-1} restricted to negative integers coincides with c^{-1} , both permutations have the same number k of infinite cycles. Finally, we modify c^* and d^* to get the required permutations g and h . Put $x^g = x$ for all $x \in G$ and $x^g = \min(\{x^{c^{*n}}; n \in N\} \setminus G)$ if $x \in \mathbf{Z} \setminus G$. Again by (iii), the map g is surjective and therefore a permutation of precisely k infinite cycles, whose set of fixed points is G and with no finite cycles of length > 1 . We put $h = g^{-1} \cdot s$. Therefore it remains to show that h decomposes into the fixed point set H and k infinite cycles. If $x \in H$, then $x \in \{s_i\}$ for some $i \geq 0$, hence $x^{s^{-1}} \geq 0$ and so $x^{s^{-1}} \notin G$, and also by $0 \leq x^{s^{-1}} < x^{s^{-1}c^*}$ we have $x^{s^{-1}c^*} \notin G$ whence $x^{s^{-1}c^*} = x^{s^{-1}g}$. Hence $x^{s^{-1}g} = x^{s^{-1}c^*} = x^{d^{*-1}} = x$. Therefore $x^h = x^{g^{-1} \cdot s} = x^{s^{-1} \cdot s} = x$, i.e., H is a set of fixed points under h . If $x \in \mathbf{Z} \setminus (G \cup H)$, there is an $n \in N$ such that $x^h = x^{g^{-1} \cdot s} = x^{(c^{*n})s} = x^{(d^* \cdot s^{-1})^{n-1} d^*} \leq x^{(d^* \cdot s^{-1})^{n-1}} =$

$x^{e^{n-1}-n} \leq x$. Therefore $x^h < x$, if $n \geq 2$. But if $n = 1$ then also $x^h = x^{d^*} < x$ by $x \notin H$. If $x \in G$, we have $x^h = x^s = x - 1 < x$. Therefore h has only infinite cycles outside H . Restriction of h^{-1} to N shows the number of infinite cycles to be k . Therefore h decomposes into the fixed point set H and k infinite cycles. Hence (4.3) is shown in this case.

Case 2. s may have fixed points.

First, we remark that s moves infinitely many points, $G \cup H \subseteq \{s\}$ and $|\{s\} \setminus (G \cup H)| = \infty$ by assumption of (4.3). Because of Case 1 there are permutations g' and h' acting on $\{s\}$ such that $s = g' \cdot h'$ if restricted to $\{s\}$. Also $\{g'\}_1 = G$, $\{h'\}_1 = H$ and g', h' decompose into fixed points and k infinite cycles only. Next, we enlarge the domain of g' and h' to obtain the required permutations g, h acting on the whole of Z . Since $\{s\} \setminus (G \cup H)$ is infinite, it is possible to select a set X of $|\{s\}_1|$ elements from $\{s\} \setminus (G \cup H)$ labelled by $\{s\}_1$. Insert t after $x_i \in X$ into g' and after x'_i into h' for all $t \in \{s\}_1$. The resulting elements satisfy (4.3).

LEMMA 4.4. *If s and p are permutations of a countable set, the first containing no infinite cycles, the second containing at least two infinite cycles, then s is a product of two permutations conjugate to p .*

Proof. We consider three cases.

Case 1. p has a finite number, $k \neq 1$, of infinite cycles and s has infinitely many fixed points.

Denote by M the underlying countable set.

Decompose the fixed point set $\{s\}_1$ into subsets A and B of cardinality $|A| = |M \setminus \{p\}_\infty|$ and $|B| = \aleph_0$. Next we define two permutations g and h . Let $g|_A = (h|_A)^{-1}$ such that $|(g|_A)_i| = |(h|_A)_i| = |(p)_i|$ for all $i \in N$ which is always possible. It follows from (4.2) that there are permutations g', h' restricted to $X = B \cup \{s\}$ such that $s|_X = g' \cdot h'$ and g', h' consist of k infinite cycles only. Therefore put $g|_X = g'$ and $h|_X = h'$ and (4.4) is shown in this case.

Case 2. p has a finite number, $k \neq 1$, of infinite cycles and s has only finitely many fixed points.

Let $(1_j \cdots m_j)$ with $1 \leq j \leq n \in N_\infty$ be an enumeration of all of the finite cycles of p and let $F = \{1_j, \cdots, m_j; 1 \leq j \leq n\}$. Since (s) [= set of all (finite) nontrivial cycles of s] is infinite, there are injections $*$: $F \rightarrow (s)$, $(i_j \rightarrow i_j^*)$ and $^\circ$: $F \rightarrow (s)$, $(i_j \rightarrow i_j^\circ)$ such that $F^* \cap F^\circ = \emptyset$ and $E = (s) \setminus (F^* \cup F^\circ)$ is infinite. Notice that $\{v\} \neq \emptyset$ for

every $v \in (s)$. Let f be a choice function defined on the set $\{\{v\}; v \in (s)\}$, i.e., $f(v) \in \{v\}$ for $v \in (s)$. Define for each j cycles j^* and j° (of disjoint supports) by $j^* = (f(1_j^*), \dots, f(m_j^*))$, $j^\circ = (f(1_j^\circ), \dots, f(m_j^\circ))$. Then the permutation *j (${}^\circ j$) defined by ${}^*j = j^* \cdot \prod_{i=1}^{m_j} i_j^*$ (${}^\circ j = \prod_{i=1}^{m_j} i_j^\circ \cdot j^\circ$) is easily seen to be a nontrivial cycle of length $\geq 2m_j > m_j \geq 1$ since $|\{^*j\}| = \sum_{i=1}^{m_j} |\{i_j^*\}|$, $|\{^\circ j\}| = \sum_{i=1}^{m_j} |\{i_j^\circ\}|$. Let $G = \{f(u^*); u \in F\}$, $H = \{f(u^\circ); u \in F\}$. Notice that $G \subseteq \bigcup_j \{j^*\}$, $H \subseteq \bigcup_j \{j^\circ\}$. Now apply 4.3 to $s^* = (\prod_j j^*) \cdot s \cdot (\prod_j j^\circ) = (\prod_j {}^*j) \cdot \prod_{v \in E} v \cdot (\prod_j {}^\circ j)$. Notice that the right hand side is a disjointed product of nontrivial cycles. Also $G \cap \{^*j\} = \{j^*\}$ and since $|\{j^*\}| \leq m_j < |\{^*j\}|$ we see that $\{^*j\} \setminus G \neq \emptyset$. Similarly, $\{^\circ j\} \setminus H \neq \emptyset$. This with $|E| = \aleph_0$ implies (i) and (ii) of Lemma 4.3. Hence there are permutations g^* and h^* such that $s^* = g^* \cdot h^*$, $\{g^*\}_1 = G$ and $\{h^*\}_1 = H$ and g^* , h^* decompose into fixed points and $|(p)_\infty|$ infinite cycles only. Finally, put $g = (\prod_{j=1}^n j^*)^{-1} \cdot g^*$ and $h = h^* \cdot (\prod_{j=1}^n j^\circ)^{-1}$ which are conjugate to p such that $s = g \cdot h$.

Case 3. p has infinitely many infinite cycles.

Since s has no infinite cycles, we decompose the underlying set into infinitely many s -invariant infinite subsets $M(i)$ for $i \in \mathbb{N}$. Then apply Case 1 and Case 2 to $s_i = s|_{M(i)}$ such that $s_i = g_i \cdot h_i$, $|(g_i)_\infty| = |(h_i)_\infty| = 2$ for all $i \in \mathbb{N}$, g_i , h_i have no finite cycles for all $i \geq 2$ and $|(g_1)_n| = |(h_1)_n| = |(p)_n|$ for all $n \in \mathbb{N}$. Then $g = \prod_{i=1}^\infty g_i$ and $h = \prod_{i=1}^\infty h_i$ are conjugate to p and $s = g \cdot h$.

5. Essential constructions for Theorem 1(c).

LEMMA 5.1. *If s and p are permutations on a countable set such that s contains no infinite cycles and p precisely one infinite cycle, then s is a product of three permutations conjugate to p .*

Proof. *Case 1.* s has finite support.

Decompose the fixed points $\{s\}_1$ into an infinite set A and a set B of cardinality $|(\{p\} \cup \{p\}_1) \setminus \{p\}_\infty|$. Obviously, there is an element $t \in S_0$ with $|(t)_n| = |(p)_n|$ for all $n \in \mathbb{N}_\infty$ and $\{t\}_\infty = A \cup \{s\}$. From $|s| < \infty$ follows $|(t^{-1}s)_\infty| \geq 1$ and an application of (3.5) for $t^{-1}s$ leads to elements u, v conjugate to P [as is t] such that $t^{-1}s = uv$ or $s = tuv$.

Case 2. If s has infinite support, decompose $\{s\}$ into an infinite s -invariant set A and a set B with $|(\{p\} \cup \{p\}_1) \setminus \{p\}_\infty| \leq |B|$. Let B^* be a subset of B with cardinality $|B^*| = |(\{p\} \cup \{p\}_1) \setminus \{p\}_\infty|$. Next we define a permutation t conjugate to p . Put $t|_{B^*}$ such that $|(t|_{B^*})_n| = |(p)_n|$ for all $n \in \mathbb{N}$. Let $s|_A = \prod_{i \in \mathbb{Z}} s_i$ with $s_i = (1_i 2_i \dots m_i)$ given in its DCD. We “glue the cycles together” and let $t|_{\{s_i\} \setminus \{m_i\}} = s_i|_{\{s_i\} \setminus \{m_i\}}$

and $m_i^t = 1_{i+1}$. Next insert the elements in $\{s\}_1 \cup (B \setminus B^*)$ elementwise into t after 1_i for arbitrary different co-ordinates $i \in \mathbf{Z}$. The result is one infinite cycle which completes our permutation t . Since $(1_{i+1})^{t^{-1}s} = 1_i$ for every $i \in \mathbf{Z}$, we have $|(t^{-1}s)_\infty| \geq 1$. As in Case 1 we conclude $s \in (p^{s_0})^s$.

6. Proof of the theorems and consequences.

Theorem 1 follows directly from (3.5), (4.4) and (5.1). The minimality of the factors is either obvious or follows from an example due to M. Perles, which can be found in E. A. Bertram [2; p. 277, Theorem 2.2]. The number of factors can be enlarged, as follows immediately from part (a) of Theorem 1.

Proof of Theorem 2. Let $|(p)_\infty| = \aleph_\nu$ and decompose $s = \prod_{i \in I} s_i$ such that $(s_i) \leq (s)$ and each s_i has a countable infinite domain S_i . Next we split $(p)_k = \bigcup_{i \in I} p(i, k)$ with finite—possibly empty—subsets $p(i, k)$ for all $k \in N_\infty$ and take $p(i, \infty)$ to be any set of two elements. There are permutations c_i and c'_i acting on S_i with $s_i = c_i \cdot c'_i$ on S_i and $|(c_i)_k| = |(c'_i)_k| = |p(i, k)|$ for all $k \in N_\infty$ as follows from (3.5) and (4.4). Hence $c = \prod_{i \in I} c_i$ and $c' = \prod_{i \in I} c'_i$ are conjugate to p and satisfy $s = c \cdot c'$.

As in Theorem 1, the number of factors can be enlarged. There are two interesting consequences of this kind of theorem.

COROLLARY 6.1. (*R. Baer [1], J. Schreier and S. Ulam [8], cf. [4, § 4].*) *The alternating group and $S(\sigma) = \{p \in S_\nu; |p| < \aleph_\sigma\}$ for all $\sigma \leq \nu + 1$ constitute a Jordan-Hölder-chain of S_ν .*

This follows already from E. A. Bertram [3] for $\nu = 0$ and is shown in [4] for $\nu \geq 0$.

The other consequence is a generalization of a theorem by O. Ore. With the notation given in § 1, we have

COROLLARY 6.2. *S_ν is w -elliptic of degree 2 for any word w . The degree is minimal in general.*

REMARK. (a) Corollary 6.2 follows already from a result of A. B. Gray [5] by the subsequent argument. It is, however, false for finite symmetric groups (take the commutator word $w = x_1 \circ x_2 = x_1^{-1} \cdot x_2^{-1} \cdot x_1 \cdot x_2$ and any odd permutation).

(b) If $w = x_1 \circ x_2$, then S_ν is w -elliptic of degree 1; cf. O. Ore [7] or R. Göbel and M. Droste [4, p. 289, Corollary 4.2].

Proof of the corollary. Let $w(x_1, \dots, x_n) \neq 1$ be any nontrivial

word of Group Theory and let $F = \langle e_i; i < \omega_\nu \rangle$ be a free group of rank \aleph_ν with free generators e_i ; let ω_ν be the first ordinal with cardinality \aleph_ν . Then we have

- (+) for every $x \in F: x \cdot w(e_1, \dots, e_n)^m = x$ iff $m = 0$, and
 (++) for every k and r with $n < k < \omega_\nu$ and $r < \omega_\nu$:
 $e_k \cdot w(e_1, \dots, e_n)^m = e_r$ iff $m = 0$ and $k = r$.

Embed $\alpha: F \hookrightarrow S_\nu$ via right regular representation and identify S_ν with all permutations of F . Put $p = w(e_1, \dots, e_n)^\alpha = w(e_1^\alpha, \dots, e_n^\alpha)$ and $e_i^\alpha = s_i$. Then p consists of no finite cycles, but of precisely \aleph_ν infinite cycles as follows from (+) and (++) . Hence $S_\nu = (p^{S_\nu})^2$ from Theorem 2: If $s \in S_\nu$, there are $g, h \in S_\nu$ such that $s = p^g \cdot p^h = w(s_1^g, \dots, s_n^g) \cdot w(s_1^h, \dots, s_n^h)$.

In order to show the minimality of the degree, consider $w(x) = x^2$. However, infinite cycles are not squares, since every square has at least two cycles in its DCD.

REMARK. The above argument yields that all elements of F^α , especially s_1, \dots, s_n , consist of precisely \aleph_ν infinite cycles and no finite cycles (including fixed points).

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. ———, *On a theorem of Schreier and Ulam for countable permutations*, *J. Algebra*, **24** (1973), 316-322.
4. M. Droste and R. Göbel, *On a Theorem of Baer, Schreier and Ulam for Permutations*, *J. Algebra*, **58** (1979), 282-290.
5. A. B. Gray, *Infinite symmetric and monomial groups*, Ph. D.-Thesis, New Mexico State University, Las Cruces, N.M. 1960.
6. G. Moran, *The product of two reflection classes of the symmetric group*, *Discrete Math.*, **15** (1976), 63-77.
7. O. Ore, *Some remarks on commutators*, *Proc. Amer. Math. Soc.*, **2** (1951), 307-314.
8. J. Schreier and S. Ulam, *Über die Permutationsgruppe der natürlichen Zahlenfolge*, *Studia Math.*, **4** (1933), 134-141.
9. H. Wielandt, "Unendliche Permutationsgruppen", Tübingen 1959/60; reprinted, York University, Toronto, Canada, 1967.

Received February 2, 1979, and in revised form May 14, 1980.

FACHBEREICH 6-MATHEMATIK
 UNIVERSITÄT ESSEN, GHS
 D-4300 ESSEN, GERMANY