On a Theorem of Baer, Schreier, and Ulam for Permutations

MANFRED DROSTE AND RÜDIGER GÖBEL

FB 6, Mathematik, University of Essen, Gesamthochschule, Universitätsstr. 12, D 4300 Essen, Germany

Communicated by B. Huppert

Received April 17, 1978

1. INTRODUCTION

If \( w = w(x_1, \ldots, x_n) \) is a word in free variables \( x_1, \ldots, x_n \) of a group, it leads to complicated (quite often combinatorial or unsolvable) problems to ask for those elements \( g \) of a given group \( G \) which are expressible in the form \( g = g_1 \cdot \ldots \cdot g_n \) for some \( g_1, \ldots, g_n \in G \). In the case of commutators \( w = x_1 \circ x_2 = x_1^{-1} \cdot x_2^{-1} \cdot x_1 \cdot x_2 \) we know of finite groups \( G \) and \( g \in G' (= \text{commutator subgroup}) \) such that \( g \neq w(g_1, g_2) \) for all \( g_1, g_2 \in G \); cf. Huppert [12, p. 258]. More general results of this type are to be found in Hall’s lecture notes [11] or for arbitrary words in Griffith [10], Rhemtulla [15], or Wilson [18]. This was exploited in Göbel [7, 8].

Again, for \( w = x_1 \circ x_2 \) it was shown dually that each element is expressible by commutators in the cases of permutation groups \( S_n, A_n \) (\( n > 5 \)); cf. Ore [14] and Ito [13]. Analogous results are known for matrix groups; cf. Clowes and Hirsch [6]. Hence every element of \( S_n \) is a product of four elements \( g_1 \circ g_2 \) from two conjugacy classes \( g_1^S \) and \( g_2^S \). The analogy is true for \( A_n \); cf. Hsü-Ch'eng-hao [5]. This result was generalized and carried over to the countable case \( S_{\aleph_0} \) of all permutations on \( \mathbb{N} \) by Bertram [3]:

\[ (*) \text{ Let } \rho \text{ be any permutation of } S_{\aleph_0} \text{ with infinite support. Then every permutation of } S_{\aleph_0} \text{ is a product of four permutations, each conjugate to } \rho. \]

This theorem reflects—in a very strong version—the fact that \( S_{\aleph_0} \) has only “very few” normal subgroups as known since 1933 from Schreier and Ulam [16]. From Baer’s result [1] we know the Jordan–Hölder series in the general case \( S_K \) of all permutations on a set of cardinality \( K \geq \aleph_0 \), which is even unique if this series is finite. Therefore a generalization of (*) for \( K \geq \aleph_0 \) is to be expected, where, of course, the cardinalities associated with permutations are to be taken in account. Surprisingly, the cardinality \( |s| \) of the support of a permutation \( s \in S_K \), will be sufficient; the support of \( s \) is the set of those elements of the underlying set which are not fixpoints of \( s \):

**THEOREM.** For a natural number \( n \) the following are equivalent:

\[ 282 \]

Copyright © 1979 by Academic Press, Inc.
All rights of reproduction in any form reserved.
(1) $n$ is minimal with the following property for any elements $s, p \in S_n$ with $|p| = \infty$: $s$ is product of $n$ elements of $S_n$ which are conjugate to $p$ if and only if $|s| \leq |p|$.

(2) $n = 4$.

This result contains (*), our starting point, as a corollary again. In addition, it answers a conjecture of Bertram [4, p. 322] negatively: There are permutations $p$ and $s$ of $S_n$ such that $s$ is not a product of three permutations, each conjugate to $p$ for all $n \geq 4$.

In particular, it contains Baer's well-known result and Ore's theorem on commutators of $S_n$ in its full generality, which are mentioned above; cf. Section 4.

In order to prove $n \geq 4$ in the Theorem, we show that the permutation $(123)$ is not a product of three permutations each consisting of 2-cycles only.

2. Notations

$K \subseteq M$: $K$ is subset of $M$, $\overline{K}$ its complement in $M$; $\{\infty\} = \mathbb{N} \cup \{\infty\}$

$K \cup K'$, $\bigcup_{i \in I} K_i$ are disjoint unions; $f|_K$ is the restriction of a map $f$ to $K$ and maps are acting from the right. $g^{a} = \{x^{-1}gx; x \in G\} = \text{conjugacy class of } g \in G$.

$S_M$ = group of all permutations of a set $M$. If $|M| = \aleph_\alpha$ or $|M| = n$, we identify $S_M = S_{\aleph_\alpha} = S_n$, respectively $S_M = S_\aleph_\alpha$.

If $p \in S_M$, let be $(p)_k$ the uniquely determined set of all cycles of length $k \in \mathbb{N}_\infty$ of the disjoint-cycle decomposition (DCD) of $p$, $|(p)_k|$ its cardinality, and $(p)_k$ the set of all elements in $(p)_k$. Then $(p)_1$ are the fixpoints of $p$, and $(p) = \bigcup_{k \in \mathbb{N}_\infty} (p)_k$ is the support of $p$ and $|p| = |(p)| = \sum_{k \in \mathbb{N}_\infty} |(p)_k|$ its cardinality. We put $(p) = \bigcup_{k \in \mathbb{N}_\infty} (p)_k$ of all cycles $\neq 1$ of $p$. Let be $|p| = \bigcup_{r < k \leq t} (p)_i$, if $r \leq t$, and $(p) = \bigcup_{r < k \leq t} (p)_i$.

$C_{\aleph_\alpha} = C_{\aleph_\alpha} = \{p \in S_M = S_\aleph_\alpha; |(p)_1| = \aleph_\alpha, |(p)_{\infty}| = |(p)_{\infty}| = \aleph_\alpha, |(p)_k| = 0 \text{ if } k \in \mathbb{N}_\infty \text{ and } k \geq 4\}$; $C_{\aleph_\alpha}^\circ = p_{\circ}^\circ$ for all $p \in C_{\aleph_\alpha}\circ$.

The latter follows from a well-known result which will be used without mentioning it again:

Two permutations $a, b \in S_\aleph_\alpha$ are conjugate if and only if $|(a)_k| = |(b)_k|$ for all $k \in \mathbb{N}_\infty$, cf. Wielandt [17, Lemma 2.5, p. 6]. So, in particular, $a$ and $a^{-1}$ are conjugate for every permutation $a$.

3. Proof of the Theorem

Let $s_n = (1 \cdots n)$ be the $n$-cycle of $S_\infty$, $n \in \mathbb{N}$ and $s_\infty = (\cdots -1012 \cdots)$ be the shift $(i^* = i + 1$ for all $i \in \mathbb{Z})$ of $\mathbb{Z}$. Then $s_n$ can be decomposed into
(3.1) \( s_n = g_n \cdot h_n \) such that

\[(n = 4): g_4 = (1)(234), h_4 = (12)(34),\]

\[(n = 5): g_5 = (1)(4)(235), h_5 = (3)(12)(45),\]

\[(n = 2k, k > 2): g_{2k} = (1) \prod_{j=0}^{k-3} (j + 2k - j)(k + 1 k + 2),\]

\[h_{2k} = (12)(k + 1)(k + 2) \prod_{j=0}^{k-3} (k - j k + 3 + j),\]

\[(n = 2k + 1, k > 2): g_{2k+1} = (1)(2)(3 4 2k + 1) \prod_{j=0}^{k-3} (5 + j 2k - j),\]

\[h_{2k+1} = (123)(4)(k + 3) \prod_{j=0}^{k-3} (k + 4 + j k + 2 - j),\]

\[(n = \infty): g_\infty = (0)(1 -1)(2 -3 -2)(3 -5)(-4) \prod_{j=2}^{\infty} (3j -3j - 2 3j - 1)\]

\[h_\infty = (0 1)(2 -1)(3 -4 -3)(-2) \prod_{j=2}^{\infty} (3j)(3j - 2 -3j + 1)\]

The elements \( g_n, h_n \) are given in DCD.

This decomposition (3.1) is due to Bertram [4, Lemma 1, p. 317, proof of Lemma 2, p. 318]. It can be easily verified by elementwise calculation and will be used to prove:

**Theorem 3.2.** The following conditions on \( p \in S_\nu \) are equivalent:

\[(1) \quad |p| \leq \kappa_\sigma.\]

\[(2) \quad There are \( q(\tau), r(\tau) \in C_\nu^r \) such that \( p = q(\tau) \cdot r(\tau) \) for all ordinals \( \tau \) with \( \sigma \leq \tau \leq \nu.\)

**Proof.** (2) \( \rightarrow \) (1) From the case \( \tau = \sigma \) follows \( p = q(\sigma) \cdot r(\sigma) \) and \( |p| \leq |q(\sigma)| + |r(\sigma)| = \kappa_\sigma.\)

(1) \( \rightarrow \) (2) We can distinguish between the following possibilities:

(i) \( |p| = \kappa_\sigma \leq \kappa_\tau \ll \kappa_\nu, \quad (ii) \quad |(p)_\nu| = \kappa_\nu, \quad (iii) \quad |(p)_\nu| = \kappa_\nu.\)

(iv) \( |(p)_k| = \kappa_\nu \) for some \( k \in \mathbb{N}, k > 3, \quad (v) \quad |(p)_\infty| = \kappa_\nu,\)
and the additional cases if \( \nu = 0 \):\\

\[\begin{align*}
& (vi) \quad |(p)_\infty| \geq 1, \\
& (vii) \quad \sum_{k \in \mathbb{N}} |(p)_k| = \kappa_0.
\end{align*}\]

(i) Since \( |(p)_1| \neq \kappa_\nu \), split \( M = T \cup V \) such that \( T \subseteq \{p\}_1 \), \( |T| = \kappa_\nu \). Now split \( T \) again into \( \kappa_\nu \) subsets of cardinality 6, i.e., \( T = \bigcup_{i \in \mathbb{N}} \{1, 2, \ldots, 6\} \) and \( |I| = \kappa_\nu \). We define \( q|_T = \prod_{i \in \mathbb{N}} (1, 2, 3i)(4i, 5i, 6i) \) and \( r|_T = (q|_T)^{-1} \). Put \( U = V \cap \{p\}_3^1 \). Now we conclude as follows \\

\((*)\) Let be \( q|_U = 1|_U \) and \( r|_U = p|_U \). If \( s_n \) is a \( n \)-cycle of \( p \) for \( n \in \mathbb{N}_\infty \) and \( n \geq 4 \), we define \( q|_{(s_n)} = g_n \) and \( r|_{(s_n)} = h_n \) according to (3.1).

(ii) According to suitable numeration let be \\

\( T = \{p\}_2 = \bigcup_{i \in \mathbb{N}} \{1, 2, \ldots, 8\} \), where \( |I| = \kappa_\nu \)

and \( \{1, 2, 3, 4, \ldots, 7, 8\} \in (p)_2 \).

We define \\

\[ q|_T = \prod_{i \in \mathbb{N}} (1, 2, 3i)(4i, 5i, 6i) \]

and \\

\[ r|_T = \prod_{i \in \mathbb{N}} (1, 4i, 3i)(2i, 5i, 6i) \]

If \( U = \{p\}_1 \cup \{p\}_3 \), we apply (*)

(iii) Since \( |(p)_2| = \kappa_\nu \), we split \( T = \{p\}_3 = \bigcup_{i \in \mathbb{N}} \{1, 2, \ldots, 6\} \) with \( |I| = \kappa_\nu \), and \( \{1, 2, 3i, 4i, 5i, 6i\} \in (p)_3 \). We define \( q|_T = \prod_{i \in \mathbb{N}} (1, 2, 3i)(4i, 5i, 6i) \) and \( r|_T = \prod_{i \in \mathbb{N}} (1, 2, 3i)(4i, 5i, 6i) \). Now we put \( U = \{p\}_3^1 \) and apply (*).

(iv) If \( |(p)_k| = \kappa_\nu \) for some integer \( k > 3 \), we split \\

\( T = \{p\}_k = \bigcup_{i \in \mathbb{N}} \{1, \ldots, k, 1^*, \ldots, k^*\} \), where \( |I| = \kappa_\nu \)

and \( s_k = (1, \ldots, k), s_k^* = (1^*, \ldots, k^*) \in (p)_k \).

According to (3.1) it is possible to define \( (q|_{(s_k)}), (q|_{(s_k^*)}) \) and \( (r|_{(s_k)}), (r|_{(s_k^*)}) \) such that each pair contains 1-, 2-, and 3-cycles and no others. Therefore \\

\[ q|_T \cdot r|_T = p|_T \]

If \( U = \{p\}_3 \) the case is settled by application of (*) for \( n \neq k \).

(v) If \( |(p)_\infty| = \kappa_\nu \), we split \( \{p\}_\infty = \bigcup_{i \in \mathbb{N}} Z_i \), where \( Z_i (i \in I) \) are \( \kappa_\nu \) infinite cycles of \( p \). Then we put \( q|_{(z_i)} = g_\infty \) and \( r|_{(z_i)} = h_\infty \) according to (3.1).

If \( U = \{p\}_3^1 \), this case follows from (*) again for \( n \neq \infty \). In each of the cases we have \( q, r \in C_{\nu}^* \) since \( |I| = \kappa_\nu \), and \( p = q \cdot r \). If \( \nu = 0 \), we have to deal with two additional cases:

(vi) \( |(p)_\nu| \geq 1 \): Observe that a decomposition of one infinite cycle as in (v) already produces \( \kappa_\nu \) cycles of length 1, 2, and 3 of \( q \) and \( r \), cf. (3.1).
(vii) $\sum_{k \in \mathbb{N}/k \geq 4} |(p)_k| = \aleph_0$. Decompose $\aleph_0$ cycles of finite length $\geq 4$ according to (3.1) and observe that the decomposition of any cycle produces $1$-, $2$-, and $3$-cycles of $q$ and $r$; for the details of this case we refer to Bertram [4, p. 319, 320]. Q.E.D.

We add a few elementary formulas of $2$-, $3$-cycle splittings for further reference

(3.3) (a) $(123) = (132)(321)$ and for $k \geq 4$:

$$(123)(4) \cdots (k) = (1324 \cdots k)(k \cdots 4321).$$

(b) $(123)(456) = (14)(35)(26) \cdot (15)(24)(36)$.

(c) $(12)(34) = (14)(23) \cdot (13)(24)$.

(d) $(12)(34)(5)(6) = (135)(246) \cdot (154)(326)$.

(e) $(12)(34)(5) \cdots (k) = (k \cdots 1 \cdots 54132) \cdot (13245 \cdots k)$ for $k \geq 4$.

(f) $(1)(2) \cdots (k) = (1 \cdots k)(k \cdots 1)$ for $k \geq 1$.

(g) $\prod_{i \in \mathbb{Z}} (1_i, 2_i, \ldots , 8_i) = \sum_{i \in \mathbb{Z}} (1_i, 2_i, \ldots , 8_i)$.

if

$$q = (\cdots 5_{i+1} 1_i 6_i 8_i 7_i 4_i 3_i 2_i 5_i 1_{i-1} 6_{i-1} \cdots)$$

and

$$r = (\cdots 5_{i-1} 1_{i-1} 4_i 8_i 7_i 2_i 3_i 5_i 1_i 4_{i+1} 8_{i+1} \cdots)$$

for all $i \in \mathbb{Z}$.

THEOREM 3.4. For a permutation $p \in S_\sigma$ with $|p| = \infty$ the following are equivalent:

1. $|p| \geq \aleph_0$.

2. For all $t \in C_\tau$ and $0 \leq \tau < \sigma$ there are elements $q = q(t), r = r(t) \in p^S_\sigma$ such that $t = q \cdot r$.

3. For all ordinals $\tau$ with $0 \leq \tau < \sigma$ there are permutations $q, r \in S_\sigma$ such that

   (a) $|(q \cdot r)_1| = \aleph_0$, $|(q \cdot r)_2| = |(q \cdot r)_3| = \aleph_\tau$, and $|(q \cdot r)_k| = 0$ with $k \in \mathbb{N}_0$, $k \geq 4$.

1 (g) can be used to prove Theorem 4.2 in Bertram [3, p. 280] where the proof is wrong, since the constructed elements $R$ and $S$ have two infinite cycles. Theorem 4.2 was also used in Bertram [4, proof of Theorem 2, p. 320]. (a) and (b) are special cases of Bertram [1, p. 373, 374].
(b) \(|(q)_k| = |(r)_k| = |(p)_k|\) for all \(k \in \mathbb{N}_0\).

This generalizes Bertram [4, Theorem 2, p. 320] and Göbel [7, Lemma 4.5, p. I.44].

**Proof.** (2) \(\iff\) (3) follows from the definition of \(C_{\tau}\).

(2) \(\implies\) (1) If \(\tau = \sigma\), we have \(|t| = \mathbb{K}_\sigma\), \(t = q \cdot r\), and \(|q| = |r| = |p|\). Therefore \(\mathbb{K}_\sigma = |t| = |q \cdot r| \leq |q| + |r| = |p|\) since \(|p| = \infty\).

(1) \(\implies\) (3) Without loss of generality we may assume \(\sigma = \tau\); take the restriction of \(p\) to \(X = \{p\}_2^\infty\) and \(S_X\) otherwise.

Elementary cardinal arithmetic shows, that we have to consider the following cases for \(1 \neq k \in \mathbb{N}_0\) with \(|(p)_k| = \mathbb{K}_\sigma\) only:

(i) \(k = 2\),
(ii) \(k = 3\),
(iii) \(k > 4\), \(k \in \mathbb{N}\),
(iv) \(k = \infty\) and the case \(|(p)_\infty| \geq 1\) if \(\nu = 0\),
(v) \(\sum_{k \geq 4} |(p)_k| = \mathbb{K}_0\) if \(\nu = 0\).

In the cases (i)-(iv), define for each \(n \neq k\) the elements \(q\) and \(r\) on an \(n\)-cycle \(s \in \{p\}_n\) as \(q s_{1:} = s\) and \(r s_{1:} = s^{-1}\). Therefore we get already

(a*) \(q \cdot r|_{\{p\}_k} = 1, \quad |(q)_n| = |(r)_n| = |(p)_n|\) for all \(n \neq k\).

(i) Since \(|(p)_2| = \mathbb{K}_\sigma\), split

\[
\{p\}_2 = \bigcup_{i \in I_1} \{1_i, 2_i, 3_i, 4_i\} \cup \bigcup_{i \in I_2} \{1_i, \ldots, 6_i\} \cup \bigcup_{i \in I_3} \{1_i, 2_i\},
\]

where \((1_i, 2_i), (3_i, 4_i), (5_i, 6_i) \in \{p\}_2\) are all different and \(|I_1| = |I_2| = \mathbb{K}_r\), \(|I_3| = \mathbb{K}_\sigma\). Define \(q\) and \(r\) on \(|p\)_2\) as follows:

If \(i \in I_1\), define \(q\) and \(r\) as two 2-cycles according to (3.3c) on \(\{1_i, 2_i, 3_i, 4_i\}\).

If \(i \in I_2\), use (3.3b) to define three 2-cycles of \(q\) and \(r\) with 3-cycle product on \(\{1_i, \ldots, 6_i\}\). If \(i \in I_3\), take \(q = r = (1_i, 2_i)\) on \(\{1_i, 2_i\}\) and (3) follows from (a*).

(ii) Since \(|(p)_3| = \mathbb{K}_\sigma\), we split

\[
\{p\}_3 = \bigcup_{i \in I_1} \{1_i, \ldots, 6_i\} \cup \bigcup_{i \in I_2} \{1_i, 2_i, 3_i\} \cup \bigcup_{i \in I_3} \{1_i, 2_i, 3_i\},
\]

where \((1_i, 2_i, 3_i), (4_i, 5_i, 6_i) \in \{p\}_3\) are all different and \(|I_1| = |I_2| = \mathbb{K}_r\), \(|I_3| = \mathbb{K}_\sigma\). If \(i \in I_1\), define \(q\) and \(r\) on \(\{1_i, \ldots, 6_i\}\) with (3.3d), if \(i \in I_2\), on \(\{1_i, 2_i, 3_i\}\) with (3.3a) and if \(i \in I_3\) with (3.3f) for \(k = 3\) on \(\{1_i, 2_i, 3_i\}\).

(iii) Since \(|(p)_k| = \mathbb{K}_\sigma\) (4 \(\leq k \in \mathbb{N}\)), we split

\[
\{p\}_k = \bigcup_{i \in I_1} \{1_i, \ldots, k_i\} \cup \bigcup_{i \in I_2} \{1_i, \ldots, k_i\} \cup \bigcup_{i \in I_3} \{1_i, \ldots, k_i\},
\]

where \((1_i, 2_i, 3_i), (4_i, 5_i, 6_i) \in \{p\}_3\) are all different and \(|I_1| = |I_2| = \mathbb{K}_r\), \(|I_3| = \mathbb{K}_\sigma\). If \(i \in I_1\), define \(q\) and \(r\) on \(\{1_i, \ldots, k_i\}\) with (3.3d), if \(i \in I_2\), on \(\{1_i, 2_i, 3_i\}\) with (3.3a) and if \(i \in I_3\) with (3.3f) for \(k = 3\) on \(\{1_i, 2_i, 3_i\}\).
where \((1_i \cdots k_i) \in (p)_k\) are all different and \(|I_1| = |I_2| = \kappa_1, |I_3| = \kappa_3\). If \(i \in I_1\), we define \(q\) and \(r\) on \(\{1_i, \ldots, k_i\}\) with (3.3e), if \(i \in I_2\), use (3.3a) on \(\{1_i, \ldots, k_i\}\), and if \(i \in I_3\), apply (3.3f) to define \(q\) and \(r\) on \(\{1_i, \ldots, k_i\}\).

(iv) If \(|(p)_\infty| = \kappa_0\), we split \(\{p\}_\infty = \bigcup_{j \in \mathbb{Z}_i} \mathbb{Z}_i\), where \(\mathbb{Z}_i \in (p)_\infty\) and \(|I| = \kappa_0\) if \(\nu > 0\) and \(|I| \geq 1\) if \(\nu = 0\).

Decompose each \(\mathbb{Z}_i = \bigcup_{i \in \mathbb{Z}} \{1_i, \ldots, k_i\}\) and define \(q\) and \(r\) via (3.3g) with products in \(C_0\).

(v) If \(|\sum k \in \mathbb{N} \cup \{4\}|(p)_k| = \kappa_0\) and w.l.o.g. \(|(p)_k| < \infty\) for all \(k \in \mathbb{N}\) and \(|(p)_\infty| = 0\), split

\[\{p\}_4^N = \bigcup_{k \in I_1} \{p\}_k \cup \bigcup_{k \in I_2} \{p\}_k \cup \bigcup_{k \in I_3} \{p\}_k\]

where \(|I_1| = |I_2| = |I_3| = \kappa_0\). If \(k \in I_1\), we define \(q|_{\{4\}_k}\) and \(r|_{\{4\}_k}\) according to (3.3e), if \(k \in I_2\) according to (3.3a), and if \(k \in I_3\) according to (3.3f). Since \(\{p\}_4^N = \{p\}_4^{3}\), we add \(q|_{(c)} = c\) and \(r|_{(c)} = c^{-1}\) for all \(c \in (p)_4^{3}\).

Proof that \(n < 4\) in the Theorem. Let \(s, p \in S_n\) and \(|p| = \infty\). If \(s = x_1 \cdots x_n\) and \(x_i \in p^{S\nu}\) for \(i = 1, \ldots, n\), then \(|s| = |x_1 \cdots x_n| \leq |x_1| + \cdots + |x_n| = n \cdot |p| = |p|\). Hence it will be sufficient to show that \(s = t \cdot u \cdot v \cdot w\) and \(t, u, v, w \in p^{S\nu}\) for \(|s| \leq |p|\). If \(|p| = \kappa_0\), we apply (3.2) (for \(\tau = 0\)) to obtain \(q = q(\sigma), r = r(\tau) \in C_\nu\) such that \(p = q \cdot r\). There are elements \(t, u, v, w\) associated with \(q\) and \(r\) as follows from (3.4) (for \(\tau = 0\)), i.e., \(q = t \cdot u, r = v \cdot w\) and \(t, u, v, w \in p^{S\nu}\) and \(p = t \cdot u \cdot v \cdot w\) is shown.

Remark. The condition \(|p| = \infty\) in the theorem is necessary for otherwise we get a contradiction if \(|p| < \infty\) and \(s\) is an odd permutation with finite support: Observe that any product of four elements conjugate to \(p\) is an even permutation if \(|p| < \infty\).

This provides a negative answer to a conjecture of Bertram [4, p. 322]:

Proof of \(n \geq 4\) in the Theorem. Choose \(M = \{1, 2, 3\} \cup R, s = (123)\) and \(p \in S_M\) a product of disjoint 2-cycles and no others. The assumption \(s = u \cdot v \cdot w\), where \(u, v, w \in p^{S\nu}\) will lead to contradictions: If \(X = \{s\} \cup \{s^u\}\) then \(X\) is finite and \(|X|\) either 4 or 6.

In the first case put \(3^u = 4, 1^u = 2\) and therefore \(X = \{1, 2, 3, 4\}\). Hence \(u \cdot s\) restricted to \(X\) equals \((12)(34)(123)(4) = (134)(2)\). Since 2 is the only fixed point of \(us = vw\), it is left invariant under \(v\) and \(w\) which contradicts our choice of \(p\).

If \(X = \{1, 2, \ldots, 6\}\) we have \((us)^2 = s^u \cdot s\) and w.l.o.g. \((us)^2 = (173)(456)\). Because of \(us = vw = (vw)^e = (vw)^w\), the support \(X\) of \((us)^2\) is left invariant.

2 This case was already considered (differently) in Bertram [4, p. 321, 322]. His proof, however, contains a gap, e.g., the cases \(|(p)_k| = 0\) for all \(k \neq 3\) or for all \(k \neq 4\).
under \( v \) and \( w \) and consequently invariant under \( u \) as well. Therefore \( u, v, w \) will be restricted to \( X \). Since \( u, v, w \) are odd and \( s \) is even, we have a contradiction to \( s = uvw \). If we assume \( s = uw \) we obtain contradictions with the same argument. Therefore the theorem is shown.

4. Discussions

In order to illustrate the efficiency of the theorem, we derive two classical corollaries:

Let be \( S^o_v = \{ p \in S_v; \ |p| < \aleph \} \) and \( S^{-1}_v \) the alternating group of \( S_v \).

(4.1) \((\text{Baer [1] and Ulam and Schreier [16, if } v = 0]): \text{ Then } S^o_v (-1 \leq \sigma \leq v + 1) \text{ is a Jordan-H"{o}lder composition series of } S_v . \text{ It is unique if it is finite. } \)

It is "Jordan-H"{o}lder":

If \( S^o_v \leq N < S^{o+1}_v \) then \( N < S_v \) as follows from Wielandt [17, Lemma 2.6, p.6].

If \( S^o_v \neq N \) then there is \( q \in N \) with \( |q| = \aleph \) and \( N = S^{o+1}_v \) follows from the theorem.

Uniqueness. Let be \( l \neq N \leq S_v \) and \( I = \{ \sigma; \text{there is } q \in N \text{ with } |q| = \aleph \} \).

We assume \( I \neq \emptyset \) and finite. Let be \( m = \max(I) \). Hence there is \( q \in N \) with \( |q| = \aleph \) and \( |x| \leq |q| \) for all elements \( x \) in \( N \) and \( N \leq S^{m+1}_v \). Application of the theorem shows \( N = S^{m+1}_v \).

(4.2) \((\text{Ore [14]}). \text{ Every permutation } s \in S_v \text{ is a commutator } s = x \circ y = x^{-1}y^{-1}xy \text{ of elements } x, y \in S_v \text{ if and only if } |s| < \aleph \).

Proof. Let be \( s = x \circ y \) and \( x, y \in S^*_v \). Then

\[
|s| = |x \circ y| = |x^{-1}y| \leq |x^{-1}| + |y| = |x| + |y| < \aleph .
\]

If \( |s| < \aleph \), there are permutations \( x^*, y \in C^{s_1}_v \leq S^*_v \) with \( s = x^* \cdot y \) according to (3.2). By application of Wielandt [17, Lemma 2.6, p.6] we obtain an element \( x \in S^*_v \) with \( x^* = (y^{-1})^* \). Hence \( s = x^* \cdot y = (y^{-1})^* \cdot y = x \circ y \).

References

