CLOSED HULLS IN INFINITE SYMMETRIC GROUPS

BY

FRANKLIN HAIMO(1)

ABSTRACT. Let Sym M be the symmetric group of an infinite set M. What is the smallest subgroup of Sym M containing a given element if the subgroup is subject to the further condition that it is also the automorphism group of some finitary algebra on M? The structures of such closed hulls are related to the disjoint-cycle decompositions of the given elements. If the closed hull is not just the cyclic subgroup on the given element then it is nonminimal as a closed hull and is represented as a subdirect product of finite cyclic groups as well as by a quotient group of a group of infinite sequences. We determine the conditions under which it has a nontrivial primary component for a given prime p and show that such components must be bounded abelian groups.

1. Introduction. Let M be an infinite set, and let a be some member of Sym M, the symmetric group on M. It is not difficult to describe those n-ary operations on M which commute with a. By definition, a is an automorphism of a finitary universal algebra A on M precisely when a ∈ Sym M commutes with each operation f of A; that is, when (x₁, ..., xₙ)a = (x₁a, ..., xₙa) for all possible xᵢ ∈ M. If a ∈ Aut A then (a), the cyclic subgroup of Sym M with generator a, is a subgroup of Aut A. But so is (a)⁻, the closure of (a) in Sym M under the Karrass-Solitar topology [5]. Here, the closure W⁻ of a subset W of Sym M is the set of all y ∈ Sym M, each of which coincides with some y = 8(y, F) ∈ W on each finite subset F of M. We write F | y = F | δ. Jónsson ([3], [4]) has shown that the closed subgroups of Sym M are precisely the automorphism groups of the finitary algebras on M. For a simplification of this result see [2]. This closure is known [5] to turn Sym M into a totally disconnected, noncompact topological group in which the closure of a subgroup G is a subgroup, abelian if G is, and in which all the proper normal subgroups are dense. Further, each finite

---

Received by the editors September 8, 1972.


Key words and phrases. Closed hull, infinite symmetric group, finitary algebra, disjoint-cycle decomposition, subdirect product, primary component, Yih-hing (Stieltjes) theorem.

(1) Partial support has been received from the National Science Foundation under grants numbered GP-20291 and GP-32837.
subset of Sym $M$ is closed in this topology. Hence $\langle a \rangle^-$ emerges as the smallest closed subgroup of Sym $M$ in which a given permutation $a$ lies, the closed hull of $a$ in Sym $M$. If $\langle a \rangle$ is of finite order it is closed, but if $\langle a \rangle$ is of infinite order, an examination of the disjoint-cycle decomposition (d.c.d.) of $a$ [7] shows that in some, but not in all, cases $\langle a \rangle$ is closed. If $\langle a \rangle^- \neq \langle a \rangle$ then $\langle a \rangle^-$ as a group is isomorphic to a certain subdirect product of finite cyclic groups of strictly increasing orders. We find a faithful representation for such groups as factor groups of subgroups of the group of integral sequences. These closures may have nontrivial torsion subgroups; we determine precisely when this is so, identifying primary components and showing that these last are bounded. The set of all such $\langle a \rangle^- \neq \langle a \rangle$ will be shown to have no minimal members, and each appropriate subdirect product will be isomorphic to some $\langle a \rangle^- \neq \langle a \rangle$.

We adopt the dual notation $x_i = x(i)$ in order to avoid excessive use of double subscripts and superscripts. No further mention will be made of this notational convention.

2. Closures of cyclic subgroups.

Theorem 1. If $a \in$ Sym $M$ where $M$ is infinite then the distinct lengths of the nontrivial cycles in the disjoint-cycle decomposition of $a$ can be arranged into a strictly increasing sequence $\mathbb{N}$: $m_1 < m_2 < \cdots$ if and only if $\langle a \rangle^- \neq \langle a \rangle$. In this case, $\langle a \rangle^-$ is a subdirect product of the cyclic subgroups $\mathbb{Z}(m_i)$ of orders $m_i$.

Proof. If $a$ moves only a finite number of elements of $M$ then $a$ is of finite order so that $\langle a \rangle$ is closed. Likewise, suppose that $a$ moves an infinite number of elements of $M$ but that there is an upper bound on the distinct lengths of the cycles in the d.c.d. of $a$. Let these distinct lengths be $m_1 < \cdots < m_r$. Then $a$ is of finite order $[m_1, \cdots, m_r]$ (least common multiple) so that $\langle a \rangle$ is closed.

Suppose that the d.c.d. of $a$ has at least one infinite cycle, say $(\cdots, x_{-1}, x_0, x_1, \cdots)$. If $y \in \langle a \rangle^-$ then $x_0 y = x_0 a^n = x_n$ for some integer $n = n(y, x_0)$. Let $F = \{x_0, y\}$ where $y \in M \setminus \{x_0\}$. Then there exists an integer $m$ such that $F \setminus y = F \setminus a^m$, from which $x_0 y = x_0 a^m = x_m$. Thus, $m = n$, and $y y = y a^n$ for every $y \in M$. We have $y = a^n$, and $\langle a \rangle$ is closed.

In the one remaining case, the distinct finite lengths $m_i$ of the nontrivial cycles in the d.c.d. of $a$ can be arranged into a strictly increasing sequence $\mathbb{N}$: $m_1 < m_2 < \cdots$, where $1 < m_1$. It may be that there are at least two cycles of the same length $r > 1$ in the d.c.d. of $a$, say $(x_1, \cdots, x_r)$ and $(y_1, \cdots, y_r)$. Suppose that $y \in \langle a \rangle^-$, and consider $F = \{x_1, \cdots, x_r, y_1, \cdots, y_r\}$. There exists an integer $q$ such that $F \setminus y = F \setminus a^q$. Let $q(r)$ be the $r$-residue of $q$; that is,
\( q(r) = q \mod r \) with \( 0 \leq q(r) < r \). Then \( \{x_1, \ldots, x_r\} \mid \gamma = \{x_1, \ldots, x_r\} \mid \alpha \gamma(q(r)) \). Likewise, \( \{y_1, \ldots, y_r\} \mid \gamma = \{y_1, \ldots, y_r\} \mid \alpha \gamma(q(r)) \), so that \( F \mid \gamma = F \mid \alpha \gamma(q(r)) \). Conversely, if \( F \mid \gamma = F \mid \alpha^m \) where \( 0 \leq m < r \) then \( m = q(r) \). From this last, one readily shows \( \gamma \) coincides with \( \alpha \gamma(q(r)) \) on each cycle of length \( r \) in the d.c.d. of \( \alpha \).

Consider an initial segment \( m_1 < \cdots < m_k \) of \( \mathbb{N} \). Choose cycles \( \alpha_1, \ldots, \alpha_k \) in the d.c.d. of \( \alpha \) where \( \alpha_i \) has length \( m_i \) for each \( i \in k^n \) \( (= \{1, \ldots, k\}) \). Let \( C_i = \text{set} (\alpha_i) \), the subset of those elements of \( M \) that are moved by the cycle \( \alpha_i \); let \( F_k = \bigcup_{i=1}^{k} C_i \), a finite subset of \( M \). There exists an integer \( n \) such that \( F_k \mid \gamma = F_k \mid \alpha^n \). Let \( n_i \) denote the \( m_i \)-residue of \( n \). As above, it does not matter which particular \( \alpha_i \) of length \( m_i \) is chosen from the d.c.d. of \( \alpha \); \( \gamma \) coincides with \( \alpha^n(i) \) on each such \( C_i = \text{set} (\alpha_i) \). Specifically, the finite set of simultaneous congruences \( x \equiv n_i \mod m_i \) \( i \in k^n \), has a solution \( x = n \). By the Yih-hing (Stieltjes) theorem [1, p. 58, p. 64] [6, pp. 31–32], the greatest common divisor \( (m_i, m_j) \) of \( m_i \) and \( m_j \) divides \( n_i - n_j \). It is convenient to write \( m_{ij} = (m_i, m_j) \), so that \( m_{ij} \mid (n_i - n_j) \) for all \( i, j \) such that \( 1 \leq i < j \leq k \). This divisibility result holds even if each \( n_i \) is replaced by \( n_i + k \cdot m_i \) for integers \( k_i \). Thus \( \gamma \in \langle \alpha \rangle^- \) generates an infinite sequence of residue classes \( \{\gamma(y) = (n_i + (m_i)) \mid i \in k^n \} \). By the Yih-hing theorem, there exists an integer \( n \) such that \( \gamma \equiv n \mod m_i \) for all \( i \in k^n \) (in the former case). For such \( i \), \( F_i \mid \gamma = F_i \mid \alpha^n(i) = F_i \mid \alpha^n \). Further, \( (F \setminus \bigcup_{i=1}^{k} F_i) \mid \gamma(\Xi) = \gamma(\Xi) \mid \Xi(\alpha^m) \) is the identity map on \( F \setminus \bigcup_{i=1}^{k} F_i \), as are \( \alpha \) and \( \alpha^n \). We now have \( F \mid \gamma(\Xi) = F \mid \alpha^n \), from which \( \gamma(\Xi) \equiv \delta \) for each \( \delta \in \langle \alpha \rangle^m \) and that \( \gamma(\Xi) = \delta(\Xi) = \delta \) for every \( \delta \in G(M) \). At once, the map \( \gamma(\Xi) \) from \( \langle \alpha \rangle^m \) onto \( G(M) \) is an isomorphism with inverse \( \Xi \). Observe that \( \gamma(\alpha^{k}) = \{k + (m_i)\} \) so that if \( \{n_i + (m_i)\} \in G(M) \) then \( \{n_i - k + (m_i)\} \in G(M) \) for each integer \( k \). That is, in the \( i \)th component each residue class of \( m_i \) must appear for some member of \( G(M) \), and this last is, accordingly, a subdirect product of the direct product \( \bigotimes Z(m_i) \).

Since there are instances of subdirect products which are cyclic, we must
FRANKLIN HAIMO

proceed with caution. (For instance, the cyclic subgroup generated by \( (1_2, 2_3, 3_4, 4_5, \cdots) \) in the direct product \( \prod \mathbb{Z}(p) \) (over all primes \( p \)) is a subdirect product.) We produce a specific \( \gamma \in \langle \alpha \rangle^{-\langle \alpha \rangle} \). Let \( \mathcal{R} = (r_1, r_2, \cdots) \) be any sequence of positive integers. Let \( \mathcal{S} = \mathcal{S}(\mathcal{R}, \mathcal{R}) = (s_1, s_2, \cdots) \) be the sequence of integers \( s_i \) where \( s_1 = m_1 \) and where, for \( i > 1 \), \( s_i = [m_{r(i-1)+1}, m_{r(i-1)+2}, \cdots, m_{r(i)}] \).

We need an intermediate step for dealing with these least common multiples.

**Lemma 1.** A sequence \( \mathcal{R} \) of positive integers exists for which \( r_1 = 1, r_2 = 2, \) and, for all positive integers \( i \), if \( s_i \in \mathcal{S}(\mathcal{R}, \mathcal{R}) \) then \( [s_1, \cdots, s_i] < s_{i+1} \).

**Proof.** If \( r_1 = 1 \) and \( r_2 = 2 \) then \( s_2 = m_2 \). Suppose that \( r_1, \cdots, r_k \) have been defined with the requisite properties. Since \( \mathcal{R} \) is strictly increasing there exists a least positive integer \( r_{k+1} \) such that \( [s_1, \cdots, s_k] < [s_{r(k)+1}, \cdots, m_{r(k+1)}] \). That is, \( [s_1, \cdots, s_k] < s_{k+1} \). \( \square \) Observe that \( \mathcal{R} \), as constructed here, is strictly increasing.

Returning to the main proof, consider a sequence \( \mathcal{B} = (b_1, b_2, \cdots) \) of integers, to be specified later. Let \( n_1 = 1 \) and suppose that integers \( n_1, \cdots, n_k \) have been constructed with the properties \( (1_k) \) for \( 1 \leq i < j \leq k \), \( s_{ij} \mid (n_i - n_j) \) (where \( s_{ij} = (s_i, s_j) = s_{i,j} \)), the \( s_i \)'s taken as in Lemma 1; and \( (2_k) n_i \neq b_i \text{ mod } s_i \) for all \( i \in k^\# \). Let \( t_{ij} = (s_{i,k+1}, s_{j,k+1}) \) for \( 1 \leq i < j \leq k \). Then \( t_{ij} \mid s_{i,k+1} \mid s_j \); likewise, \( t_{ij} \mid s_j \), so that \( t_{ij} \mid s_{ij} \mid (n_i - n_j) \). By the Yih-hing theorem, there is a solution \( x = x_{k+1} \) of the set of simultaneous congruences

\[
(A_k) \quad x = n_i \text{ mod } s_{i,k+1}, \quad i \in k^#,
\]

and \( s_{j,k+1} \mid (n_j - x_{j+1}) \) for all \( j \in k^\# \). Define

\[
 n_{k+1} = \begin{cases} 
 x_{k+1} & \text{if } x_{k+1} \neq b_{k+1} \text{ mod } s_{k+1}, \\
 b_{k+1} + [s_1, \cdots, s_k] & \text{otherwise}.
\end{cases}
\]

In the first instance, we have a new finite sequence \( n_1, \cdots, n_k, n_{k+1} \) subject to \( (1_{k+1}) \) and \( (2_{k+1}) \). In the second instance, \( n_{k+1} = x_{k+1} + cs_{k+1} + [s_1, \cdots, s_k] \) for some integer \( c \). From the fact that \( s_{i,k+1} \mid (cs_{k+1} + [s_1, \cdots, s_k]) \) for all \( i \in k^\# \) we see that \( n_{k+1} \) is also a solution of \( (A_k) \).

In case \( n_{k+1} \equiv b_{k+1} \text{ mod } s_{k+1} \) then \( s_{k+1} \mid [s_1, \cdots, s_k] \). By previous construction, however, \( [s_1, \cdots, s_k] < s_{k+1} \). Thus, \( n_{k+1} \neq b_{k+1} \text{ mod } s_{k+1} \) and \( \mathcal{R} \) has been constructed inductively in such a way that \( s_{ij} \mid (n_i - n_j) \) and \( n_i \neq b_i \text{ mod } s_i \) for all pertinent \( i \) and \( j \).

Note that \( 1 < m_1 \leq m_{r(1)} \) since \( r_1 = 1 \). If \( i > 1 \) there exists a unique positive integer \( d_i \) such that

\[
(B_i) \quad m_{r(d(i)-1)} < m_i \leq m_{r(d(i))}.
\]
For completeness, we take $d_1 = 1$, $r_0 = 0$, and $m_0 = 1$. Note that $\mathbb{E} = (d_1, d_2, \cdots)$ is a nondecreasing sequence depending only on $\mathbb{R}$ and $\mathbb{R}$ and not on $\mathbb{R}$ and $\mathbb{B}$. Specify the sequence $\mathbb{B}$ in any way such that $b_{d(i)} = (-1)^{i-1}[(1 - i)/2]$. For each positive integer $k$, $b_{d(2k)} = k$ and $b_{d(2k-1)} = 1 - k$. The range of the composite sequence $\mathbb{B} \mathbb{B}$ (with values $b_{d(i)}$) is thus the entire set $Z$ of integers.

Observe that the map $\Xi$ from $G(\mathbb{R})$ to $\langle a \rangle^{-1}$ has an obvious extension to a map (also indicated by $\Xi$) from $\Pi Z(m_i)$ to $M^\mathbb{M}$. Let $\mathbb{S} = \Pi Z(m_i)$ be given by $\mathbb{S} = \{n_{d(i)+1}(m_i)\}$, the $n$'s defined inductively as above. Denote $\Xi(\mathbb{S})$ by $\gamma$. First, $\gamma \in \operatorname{Sym} M$; for, if $x \in M$ is fixed by $\alpha$, $x \in \operatorname{Im} \gamma$. If $x \alpha \neq x$ then $x \in C_i = \text{set} (\alpha_i)$ for some cycle $\alpha_i$ of length $m_i \geq 2$ in the d.c.d. of $\alpha$. Denote this particular cycle by $(x_1 x_2 \cdots x_{m(i)})$ where $x_1 = x$. Now choose the unique solution $y = u \gamma$ of the congruence $\gamma = (1 - n_{d(i)}) \mod m_i$ that obeys $1 \leq u \leq m_i$. Then $x_u y = x_u \alpha^n = x_v$ where $n = n_{d(i)}$ and where $1 \leq v \leq m_i$ such that $u + n_{d(i)} \equiv v \mod m_i$. But $u = 1 - n_{d(i)} + cm_i$ for some integer $c$, from which $v \equiv 1 \mod m_i$. The only possibility is that $v = 1$ whence $x_u y = x_1 = x$. Again, $x \in \operatorname{Im} \gamma$, and $\gamma$ is epic.

It is also monic; for, suppose $xy = yx$, where $x, y \in M$. If $x$ and $y$ were in different cycles of the d.c.d. of $\alpha$, then, by the definition of $\gamma$, $xy$ and $yx$ could not be in the same cycle, contrary to their being equal. That is, $xy = x \alpha^n = y \alpha^n = yx$ for $n = n_{d(i)}$. Since, however, $\alpha^n$ as a permutation is monic, $x = y$; $\gamma$ is monic as well as epic, and $\gamma \in \operatorname{Sym} M$.

To show that $\gamma \in \langle a \rangle^{-1}$, recall that $s_{d(i),d(i)} = (n_{d(i)} - n_{d(i)})$. But $s_{d(i)}$ is the least common multiple of all $m_k$ such that $r_{d(i)-1} + 1 \leq k \leq r_{d(i)}$, and $i$ is in this last interval, as (B) attests. Then $m_j | s_{d(i),d(j)}$, $m_j | s_{d(j)},$ from which $m_{ij} | (n_{d(i)} - n_{d(j)})$. We now have $\mathbb{S} \in G(\mathbb{R})$ so that $\gamma = \Xi(\mathbb{S}) \in \langle a \rangle^{-1}$.

To show that $\gamma \notin \langle a \rangle$, consider sample cycles $\alpha_j$ of lengths $m_j$ where $j$ is restricted by $r_{d(i)-1} < j \leq r_{d(i)}$ possible since $\mathbb{R}$ is strictly increasing. Let $C_j = \text{set} (\alpha_j)$, and let $F^i = \bigcup_j C_i, j = r_{d(i)-1} + 1, \ldots, r_{d(i)}$. Then $F^i \mid \gamma^i = F^i \mid \alpha^n$ where $n = n_{d(i)}$ for all these last described $j$ have the property that $d_j = d_i$. We need an auxiliary result.

Lemma 2. For an integer $\nu$, $F^i \mid \alpha^\nu = F^i \mid \alpha^n$ where $n = n_{d(i)}$ if and only if $\nu \equiv n_{d(i)} \mod s_{d(i)}$.

Proof. If $\nu \equiv n_{d(i)} \mod s_{d(i)}$ and if $x \in F^i$ then $x \alpha^\nu$ reduces to $x \alpha^n$, $n = n_{d(i)}$. Conversely, if $F^i \mid \alpha^\nu = F^i \mid \alpha^n$ then $\nu \equiv n_{d(i)} \mod m_i$ for all $j = r_{d(i)-1} + 1, \ldots, r_{d(i)}$. Hence $\nu \equiv n_{d(i)} \mod [m_{r_{d(i)-1}+1}, \ldots, m_{r_{d(i)}}]$. But this last is just $s_{d(i)}$. □

Return to the main proof, and recall that, for all pertinent $i$, $n_i \neq b_i \mod s_i$. 
In particular, \( n_{d(i)} \neq b_{d(i)} \mod s_{d(i)} \). By Lemma 2, \( F^i \mid y \neq F^i \mid \alpha^n \), \( n = n_{d(i)} \), \( i = 1, 2, \ldots \). If \( y \) were in \( \langle \alpha \rangle \) then \( y = \alpha^k \) for some integer \( k \). But \( \text{Im}(\beta \gamma) = \mathbb{Z} \), so that there exists a positive integer \( i \) for which \( b_{d(i)} = k \). In particular, since \( y = \alpha^k \), \( F^i \mid y = F^i \mid \alpha^k \), contradicting what has just been proved. □

We know that \( \beta \in \langle \alpha \rangle^\perp \) if and only if \( \beta \) coincides on each finite subset \( F \) of \( M \) with some \( \alpha^m \), \( m = m(\beta, F) \). It is possible if \( \langle \alpha \rangle^\perp \neq \langle \alpha \rangle \) to reduce the number of \( F \)'s that must be considered. Each \( x \in M \) lies in a unique cycle \( \alpha[x] \) of the d.c.d. of \( \alpha \). Let \( m[x] \) be the length of \( \alpha[x] \), finite by Theorem 1. Consider those finite subsets \( F = \{a_1, \ldots, a_{n+1}\} \) (no repetitions allowed) of \( M \) with the property that there is at least one possible ordering \( a_1, \ldots, a_{n+1} \) of the \( a_i \)'s such that if \( n > 0 \) then \( m[a_i] \mid m[a_{i+1}] \mid \ldots \mid m[a_{n+1}] \). Call such \( F \)'s \( \alpha \)-good subsets of \( M \).

Theorem 2. If \( \alpha \in \text{Sym} M \), \( M \) infinite, if \( \langle \alpha \rangle^\perp \neq \langle \alpha \rangle \), and if \( \beta \in \text{Sym} M \) has the property of coinciding on each \( \alpha \)-good (finite) subset \( F \) of \( M \) with some \( \alpha^m \), \( m = m(\beta, F) \), then \( \beta \in \langle \alpha \rangle^\perp \).

Proof. If \( \beta \in (\text{Sym} M) \setminus \langle \alpha \rangle^\perp \) the Jónsson result ([3], [4]) gives us a finitary algebra \( A \) on \( M \) with \( \text{Aut} A = \langle \alpha \rangle^\perp \), an operation \( f \) of rank \( n \) of \( A \), and a set \( U \) of \( n + 1 \) elements \( a_i \in M \), possibly with repetitions, such that \( (a_1, \ldots, a_n) f = a_{n+1} \) but that \( (a_1 \beta, \ldots, a_n \beta) f \neq a_{n+1} \beta \). If the set \( U \) has repetitions, discard duplicates to obtain a finite subset \( F = \{b_1, \ldots, b_{k+1}\} \) of \( M \) with no repetitions. We lose no generality in taking \( b_{k+1} = a_{n+1} \). Since \( (a_1 \alpha, \ldots, a_n \alpha) f = a_{n+1} \alpha \), \( m[a_{n+1}] \) must divide the least common multiple \( r \) of all the \( m[a_i] \) where \( a_i \neq a_{n+1} \) (if there are any such \( i \)'s). But \( m[b_{k+1}] = m[a_{n+1}] \), and \( \{m[b_1], \ldots, m[b_k]\} = r \). Hence \( F \) is an \( \alpha \)-good subset of \( M \).

If \( \beta \) were to coincide with some \( \alpha^m \) on \( F \) then \( \beta \) would coincide with that \( \alpha^m \) on \( U \). Hence \( (a_1 \beta, \ldots, a_n \beta) f = (a_1 \alpha^m, \ldots, a_n \alpha^m) f = (a_1, \ldots, a_n) f /\alpha^m = a_{n+1} \alpha^m = a_{n+1} \beta \), ruled out in the preceding paragraph. We have established the contrapositive of the required result. □

3. Representations. In this section we shall represent \( G(\mathbb{Z}) \) faithfully as a closed hull and as a factor group of a group of integral sequences. Again take \( m_1 > 1 \), and let \( \mathbb{S} \) be \( m_1 < m_2 < \ldots \). Let \( V(\mathbb{S}) \) be the set of all sequences \( \mathbb{S} = (t_0, t_1, \ldots) \) of integers for which \( m_{i,j+1} \mid (t_i + \ldots + t_j) \) for all \( i, j \) subject to \( 1 \leq i \leq j \). Then \( V(\mathbb{S}) \) is a subgroup of the group \( \mathbb{Z} \) of all integral-valued sequences \( \mathbb{S} = (s_0, s_1, \ldots) \). Let \( W(\mathbb{S}) \) be the set of all \( \mathbb{S} \) for which \( m_{i+1} \mid (s_0 + \ldots + s_i) \), a subgroup of \( V(\mathbb{S}) \). Let \( X(\mathbb{S}) = V(\mathbb{S})/W(\mathbb{S}) \), an abelian group.

Theorem 3. \( G(\mathbb{S}) \) and \( X(\mathbb{S}) \) are isomorphic and can be represented faithfully as a closed hull \( \langle \alpha \rangle^\perp \neq \langle \alpha \rangle \) in \( \text{Sym} M \).
Proof. For \( \{n_i + (m_j)\} \in G(\mathbb{N}) \) construct an integral sequence \( S = (t_0, t_1, \ldots) \) by setting \( t_0 = n_1 \) and, for \( i \geq 1 \), \( t_i = n_{i+1} - n_i \). Then \( \sum_{u=1}^{i} t_u = n_{i+1} - n_i \) for all integers \( i \) and \( j \) subject to \( 1 \leq i \leq j \). By construction, \( S \in V(\mathbb{N}) \). If we replace each \( n_i \) by an alternate representative \( n_i + m_i \) for integers \( c_i \), we then have \( S' = (t'_0, t'_1, \ldots) \) where \( t'_0 = t_0 + c_1 m_1 \) and where, for \( i \geq 1 \), \( t'_i = t_i + c_i + m_i + 1 - c_i m_i \). Since the sequence \( (c_1 m_1, c_2 m_2 - c_1 m_1, \ldots) \in W(\mathbb{N}) \), each \( S \in G(\mathbb{N}) \) determines some \( \Psi(S) = S + W(\mathbb{N}) \) in \( X(\mathbb{N}) \). It is clear that \( \Psi \in \text{Hom}(G(\mathbb{N}), X(\mathbb{N})) \). If \( \mathbb{S} = \{n_i + (m_j)\} \in \ker \Psi \) then \( t_0 = c_1 m_1 \) and, for \( i \geq 1 \), \( t_i = c_i + m_i + 1 - c_i m_i \) for appropriate integers \( c_i \). But \( n_{i+1} = \sum_{u=0}^{i} t_u \) for all nonnegative integers \( i \), so that \( n_{i+1} = c_i + m_i + 1 \). Since \( \mathbb{S} = \{n_i + (m_j)\} \in G(\mathbb{N}) \), \( \Psi(\mathbb{S}) = \mathbb{S} + W(\mathbb{N}) \); \( \Psi \) is epic and is thus an isomorphism from \( G(\mathbb{N}) \) onto \( X(\mathbb{N}) \).

Given \( \mathbb{N} \), construct \( \alpha \in M^\mathbb{N} \) as follows: First choose a countable (but not necessarily proper) subset \( L \) of distinct elements \( x_{ij} \) of \( M \) for positive integral \( i \) and \( j \). Let

\[
\begin{cases}
  x_{i,j+1} & \text{if } x = x_{ij} \text{ and } 1 \leq j < m_i, \\
  x_{i,1} & \text{if } x = x_{i,m(i)}, \\
  x & \text{otherwise}.
\end{cases}
\]

Then \( \alpha \in \text{Sym M, } \) and the nontrivial cycles in its d.c.d. are the \( \alpha_j = (x_{11}, \cdots, x_{i,m(i)}) \). Thus \( X(\mathbb{N}) \) is faithfully represented by \( \langle \alpha \rangle^* \not= \langle \alpha \rangle \), and each \( L \) gives a distinct representation. \( \square \)

Corollary. If the set \( m_i \) of \( \mathbb{N} \) is a relatively prime set of integers then \( G(\mathbb{N}) \) is isomorphic to the direct product \( \Pi Z(m_i) \).

The corollary shows that, even though \( \alpha \) is of infinite order in \( \text{Sym M, } \langle \alpha \rangle^* \) may have nonzero torsion elements. One could conjecture that the infinite order of \( \alpha \) would predispose each nontrivial primary component to have elements of arbitrarily high order, but the facts are otherwise.

4. Torsion elements.

Theorem 4. If \( \mathbb{S} = \{n_i + (m_j)\} \in G(\mathbb{N}) \) then \( \mathbb{S} \) is a torsion element if and only if the set of all \( m_i (m_j, n_j)^{-1} \) is bounded. In that case, the order of \( \mathbb{S} \) is the least common multiple of the distinct \( m_i (m_j, n_j)^{-1} \).

Proof. If the order \( |\mathbb{S}| \) of \( \mathbb{S} \) is finite then \( n_i \mid |\mathbb{S}| = 0 \mod m_i \) so that
$n_i(m_i, n_i)^{-1} \equiv 0 \mod m_i(m_i, n_i)^{-1}, i = 1, 2, \ldots$. Since $u_i = n_i(m_i, n_i)^{-1}$ and $v_i = m_i(m_i, n_i)^{-1}$ are coprime, each $v_i$ divides $|\mathfrak{a}|$. Hence the $v_i$ are bounded and finite in number. Conversely, if the $v_i$ are bounded let their distinct values be $c_1, \ldots, c_r$, and let $c = [c_1, \ldots, c_r]$. Each $v_i$ equals some $c_{i(j)},$ and $n_i = [m_i, n_i]e_i$ for some integer $e_i$, from which $n_i = [m_i, n_i]e_i$. Since, however, $m_i | [m_i, n_i], n_i \equiv 0 \mod m_i$ for $i = 1, 2, \ldots$, and $\mathfrak{a}$ is periodic with order dividing $c$.

Should $|\mathfrak{a}| < c$, there would have to exist some prime $p$ dividing $c$ such that $\exp_p |\mathfrak{a}| < \exp_p c = k$. Since $\exp_p c = \max_i \exp_p c_i$, there will be some $c_i$ with $\exp_p c_i = k$. There must be some integer $a$ for which $j(a) = i$, and $n_a |\mathfrak{a}| = q_a m_a$ for a suitable integer $q_a$. It follows that $u_a |\mathfrak{a}| = v_a q_a = q_a c_i$. Since $u_a$ and $v_a$ are coprime, $p^k | c_i$ implies that $p^k | |\mathfrak{a}|$, a contradiction. Hence $|\mathfrak{a}| = c$. □

Theorem 5. A necessary and sufficient condition that $G(\mathfrak{a})$ have a nontrivial $p$-component is that $1 \leq \text{l.u.b.} \exp_p m_i$ where this last is finite.

Proof. Let $k = \text{l.u.b.} \exp_p m_i$ be finite and at least 1, and let $\exp_p m_i$ be denoted by $k_i$. Let $u(1), u(2), \ldots$ be the distinct indices $i$ for which $k_i = k$. This set $U$ of $u(i)$'s may be finite or infinite, but $U$ is nonempty since $1 \leq k$. We write $m_i = p^k b_i$ where $(p, b_i) = 1$. Select integers $x_i$ such that $x_i = 0$ if $i \notin U$ but where $x_{u(1)}$ is chosen subject to $0 < x_{u(1)} < pb_{u(1)}$ and $(p, x_{u(1)}) = 1$. If $u(1)$ is the sole member of $U$ the selection of the $x_i$'s is deemed to have been completed. If not, consider the set (finite or infinite) of simultaneous congruences

$$(C) \quad x_{u(i)} x_{u(i)} b_{u(i)} = x_{u(i+1)} b_{u(i+1)} \mod p.$$ 

Since each $(b_i, p) = 1$, and since $x_{u(1)}$ has already been chosen, the system (C) can be solved recursively (but not uniquely) for the $x_{u(i)}$'s.

Let $n_i = p^{k-1} x_i b_i$ for $i = 1, 2, \ldots$. Now $n_{u(1)} \equiv 0 \mod m_{u(1)}$ would imply that $p | x_{u(1)}$, contrary to choice. Thus, at least one $n_i \neq 0 \mod m_i$. For all $i$, $p n_i = p^{k} x_i b_i$. If $k_i < k$, $x_i = 0$ and $p n_i = 0$. Since $m_{u(t)} = p^k b_{u(t)}$, one has $p n_{u(t)} \equiv 0 \mod m_{u(t)}$. As a member of $\Pi Z(m_i)$, $\mathfrak{a} = \{n_i + (m_i)\}$ has order $p$.

We now show that $\mathfrak{a} \in G(\mathfrak{a})$, so that this last has a nontrivial $p$-component.

(1) If $k_i, k < k$ then $x_i = 0 = x_j$ and $n_i = 0 = n_j$, so that $m_{ij} | (n_i - n_j)$. (2) If $k_i < k = k_j$ then $m_{ij} = p^k b_i b_j$, and $n_i - n_j = p^{k-1} (x_i b_i - x_j b_j) = - p^{k-1} x_j b_j$.

Since $k_i < k$, $m_{ij} | (n_i - n_j)$. (3) If $k_i = k = k_j$ then $m_{ij} = p^k (b_i, b_j)$ while $n_i - n_j = p^{k-1} (x_i b_i - x_j b_j)$. From (C), $p^k | (n_i - n_j)$. But $(b_i, b_j) | (x_i b_i - x_j b_j)$, and $(p, b_i, b_j) = 1$. Again, $m_{ij} | (n_i - n_j)$, and we have treated all the conceptually different cases. Thus $\mathfrak{a} \in G(\mathfrak{a})$, as required.

Conversely, if $\mathfrak{a} \in G(\mathfrak{a})$ with $|\mathfrak{a}| = p$ where $\mathfrak{a} = \{n_i + (m_i)\}$ choose the $n_i$.
subject to $0 \leq n_i < m_i$. By hypothesis, $m_i | p n_i$, $i = 1, 2, \ldots$. Let the prime decomposition of $m_i$ be $p_k(i)^{q_k(i)} \cdots q_t(i)^{q_t(i)}$ where $c = 1$ or where $c$ is a product of one or more prime powers for a prime or primes not in the set $\{p, q_1, \ldots, q_t\}$. Since $m_i | p n_i$ we have $k_i \leq l_i + 1$, and $1 \leq r_i \leq s_i$ for each $t \in j^*$. Since $m_i > n_i$, $0 < m_i - n_i = q_1^{r_1(1)} \cdots q_j^{r_j(j)} p_k(i)^{-1}(p - p w(i) q_1^{1(1)} \cdots q_j^{1(j)} - r(j))$ where $w(i) = l_i - k_i + 1 \geq 0$. If $w(i) > 0$, $p^k(i) | (m_i - n_i)$ and $p^k(i) | n_i$ incompatible with $0 \leq n_i < m_i$ and $m_i | p n_i$.

We have $l_i + 1 = k_i$

If $n_i \neq 0 = n_j$ then $m_{ij} \mid n_i$ where $n_i = p^k(i) b_i$, $(p, b_i) = 1$ and $m_{ij} = p \min (k(i), k(j)) b_i$, $(p, b_i) = 1$. Then $\min (k_i, k_j) \leq l_i = k_i - 1$, so that $k_i < k_j$ in this case. If $m_i$ and $m_j$ are both nonzero then $n_i - n_j = p \min (l(i), l(j)) d_i$, and $m_{ij} = p \min (l(i) + 1, l(j) + 1) b_j$, giving $p \mid d$. No generality is lost in assuming $k_i \leq k_j$, so that $d = p^{1-k(i)}(n_i - n_j)$. Since $p \mid d$, $p^k(i) \mid (n_i - n_j)$. That is, $p^k(i) \mid (p k(i) b_i - p^k(i) b_i - b_i)$, from which $p \mid (b_i - p^k(i) b_i)$. If $k_i < k_j$ we would have to conclude that $p \mid b_i$, contrary to supposition. Thus $k_i = k_j$ whenever $n_i$ and $n_j$ are both nonzero. Let the common value of these $k_i$'s be denoted by $k$, so that $1.ub. k_i = k$, a finite value. Since $\emptyset \neq 0$ some $n_i(0) \neq 0$ whence $l_i(0) + 1 = k_i(0) = k$. At once, $k \geq 1$.

**Corollary.** Each $p$-component of $G(S_0^1)$ is bounded.

**Proof.** If $\emptyset = \{n_i + (m_i) \in G(S_0^1)\}$ has order $p^b$, then, by Theorem 4, $p^b = [c_1, \ldots, c_r]$ where the $c_i$'s are the distinct values of the various $v_t = m_t / (m_t, n_t)$. Then $p^b = c_j(t)$ for some $t$ where $c_j(t) = v_t$. Let us write $n_t = p^{l(t)} m_t$ and $m_t = p^{k(t)} m_t$, where $p$ divides neither $m_t$ nor $n_t$. We have $(m_t, n_t) = p^{\min (l(t), k(t))} (m_t, n_t) = m_t p^{b} - 1 = m_t p^{b}$, so that $b = k_t - \min (k_t, l_t)$. At once, $k_i \geq b$. Since, however, Theorem 5 gives $k \geq k_t$ where $k = 1.ub. \exp_p m_i$, we have $k \geq b$.

5. Nonminimality. For an infinite set $M$, let $C$ be the set of all subgroups of Sym $M$ of the form $(\alpha)^- \neq (\alpha)$.

**Lemma 3.** If $(\alpha)^- \in C$ then those members $\beta$ of $(\alpha)^-$ with the property that $(\beta)^- = (\beta)$ are precisely the torsion elements of $(\alpha)^-.$

**Proof.** Surely all the torsion elements $\beta$ of $(\alpha)^-$ have the property that $(\beta)$ is closed since each of these generates a finite, hence closed, cyclic subgroup. Conversely, suppose that $\beta \in (\alpha)^-$ with $(\beta)$ closed. Reference to the proof of Theorem 1 shows that there are only two possible cases: (A) the cycles in the d.c.d. of $\beta$ have bounded lengths, or (B) $\beta$ has at least one cycle of infinite length. But elements with (A) are known to be torsion (see proof of Theorem 1); and elements $\beta$ with (B) cannot lie in any $(\alpha)^- \neq (\alpha)$, since all
the cycles in the d.c.d. of such a $\beta$ are powers of the necessarily finite cycles of the d.c.d. of $\alpha$. \qed

**Theorem 6.** Let $M$ be an infinite set, and let $C = C(M)$ be the set of all subgroups of $\text{Sym} M$ of the form $\langle \alpha \rangle^- \neq \langle \alpha \rangle$. Then $C$ has no minimal members.

**Proof.** Let $p$ be some prime divisor of $m_1$ of $\mathbb{R}$ where $G(\mathbb{R})$ represents $\langle \alpha \rangle^- \neq \langle \alpha \rangle$, as in Theorem 1, proof. Then $\alpha^p \in \langle \alpha \rangle$ and $\langle \alpha^p \rangle^+ \leq \langle \alpha \rangle^-$. Since $\alpha$ is no torsion element of $\text{Sym} M$, neither is $\alpha^p$. By Lemma 3, $\langle \alpha^p \rangle^- \neq \langle \alpha^p \rangle$ so that $\langle \alpha^p \rangle^- \in C$. Since $G(\mathbb{R})$ is a subdirect product of the $Z(m_i)$'s where the $m_i$'s are the members of $\mathbb{R}$, there exists some $\gamma \in \langle \alpha \rangle^-$ for which the first component $\mathbb{R} + (m_i)$ of $\mathbb{R}(\gamma)$ (see proof of Theorem 1 for notation) is $1 + (m_i)$. Let $\alpha_1$ be a cycle of length $m_1$ in the d.c.d. of $\alpha$, and let $C_1 = \text{set} (\alpha_1)$. If $\gamma$ were to lie in $\langle \alpha^p \rangle^-$ then $C_1 | \gamma = C_1 | \alpha^{pk}$. Let $\alpha_1 = (x_1 \cdots x_{m(1)})$. Then $x_2 = x_1^y$ since $\mathbb{R}(\gamma) = (1 + (m_1), *, *, \cdots)$. Hence $x_2 = x_1^{\alpha^{pk}}$, possible only if $pk \equiv 1 \mod m_1$. Since $p | m_1$ we have a contradiction, so that $\langle \alpha^p \rangle^-$ is a proper subgroup of $\langle \alpha \rangle^-$ which also belongs to $C$. \qed

**REFERENCES**


DEPARTMENT OF MATHEMATICS, WASHINGTON UNIVERSITY, ST. LOUIS, MISSOURI

Current address: Institute for Advanced Study, Princeton, New Jersey 08540