TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 180, June 1973

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 α 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 α. By definition, α is an automorphism of a finitary universal algebra A on M precisely when $\alpha \in$ Sym M commutes with each operation f of A; that is, when $(x_1, \cdots, x_n)f\alpha = (x_1\alpha, \cdots, x_n\alpha)f$ for all possible $x_i \in M$. If $\alpha \in$ Aut A then $\langle\alpha\rangle$, the cyclic subgroup of Sym M with generator α, is a subgroup of Aut A. But so is $\langle\alpha\rangle^-$, the closure of $\langle\alpha\rangle$ 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 $\gamma \in$ Sym M, each of which coincides with some $\delta = \delta(\gamma, F) \in W$ on each finite subset F of M. We write $F \mid \gamma = F \mid \delta$. 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.

AMS (MOS) subject classifications (1970). Primary 20F55, 20E35; Secondary 08A25, 10A10.

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 $\langle\alpha\rangle^-$ emerges as the smallest closed subgroup of Sym M in which a given permutation α lies, *the closed hull of* α *in* Sym M. If $\langle\alpha\rangle$ is of finite order it is closed, but if $\langle\alpha\rangle$ is of infinite order, an examination of the disjoint-cycle decomposition (d.c.d.) of α [7] shows that in some, but not in all, cases $\langle\alpha\rangle$ is closed. If $\langle\alpha\rangle^- \neq \langle\alpha\rangle$ then $\langle\alpha\rangle^-$ 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 $\langle\alpha\rangle^- \neq \langle\alpha\rangle$ will be shown to have no minimal members, and each appropriate subdirect product will be isomorphic to some $\langle\alpha\rangle^- \neq \langle\alpha\rangle$.

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

Proof. If α moves only a finite number of elements of M then α is of finite order so that $\langle\alpha\rangle$ is closed. Likewise, suppose that α 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 α. Let these distinct lengths be $m_1 < \cdots < m_t$. Then α is of finite order $[m_1, \cdots, m_t]$ (least common multiple) so that $\langle\alpha\rangle$ is closed.

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

In the one remaining case, the distinct finite lengths m_i of the nontrivial cycles in the d.c.d. of α can be arranged into a strictly increasing sequence $\mathfrak{M}$: $m_1 < m_2 < \cdots$, 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 α, say $(x_1, \cdots, x_r)$ and $(y_1, \cdots, y_r)$. Suppose that $\gamma \in \langle\alpha\rangle^-$, and consider $F = \{x_1, \cdots, x_r, y_1, \cdots, y_r\}$. There exists an integer q such that $F|\gamma = F|\alpha^q$. Let $q(r)$ be the r-residue of q; that is,

$q(r) \equiv q \bmod r$ with $0 \le q(r) < r$. Then $\{x_1, \cdots, x_r\} \mid \gamma = \{x_1, \cdots, x_r\} \mid \alpha^{q(r)}$. Likewise, $\{y_1, \cdots, y_r\} \mid \gamma = \{y_1, \cdots, y_r\} \mid \alpha^{q(r)}$, so that $F \mid \gamma = F \mid \alpha^{q(r)}$. Conversely, if $F \mid \gamma = F \mid \alpha^m$ where $0 \le m < r$ then $m = q(r)$. From this last, one readily shows γ coincides with $\alpha^{q(r)}$ on each cycle of length r in the d.c.d. of α.

Consider an initial segment $m_1 < \cdots < m_k$ of $\mathfrak{M}$. Choose cycles $\alpha_1, \cdots, \alpha_k$ in the d.c.d. of α where α_i has length m_i for each $i \in k^\#$ $(= \{1, \cdots, k\})$. Let $C_i = \underline{\text{set}}\ (\alpha_i)$, the subset of those elements of M that are moved by the cycle α_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 α_i of length m_i is chosen from the d.c.d. of α: γ coincides with $\alpha^{n(i)}$ on each such $C_i = \underline{\text{set}}\ (\alpha_i)$. Specifically, the finite set of simultaneous congruences $x \equiv n_i \bmod m_i$, $i \in k^\#$, 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 $m_{ij} = (m_i, m_j) = m_{ij}$, so that $m_{ij} \mid (n_i - n_j)$ for all i, j such that $1 \le i < j \le k$. This divisibility result holds even if each n_i is replaced by $n_i + k_i m_i$ for integers k_i. Thus $\gamma \in \langle\alpha\rangle^-$ generates an infinite sequence of residue classes $\mathfrak{A}(\gamma) = (n_i + (m_i),$ $n_2 + (m_2), \cdots)$ where (m_1) is the integral subgroup generated by m_i and where (a) each $n_i + (m_i)$ lies in $Z(m_i)$, and (b) $n_i \equiv n_j \bmod m_{ij}$ for each pair of distinct positive integers i and j. Two distinct members of $\langle\alpha\rangle^-$ will produce two distinct values of $\mathfrak{A}$. Under component addition the set of all sequences $\mathfrak{S}$ satisfying (a) and (b) is a group $G(\mathfrak{M})$.

Conversely, if $\mathfrak{S} = \{n_i + (m_i)\} \in G(\mathfrak{M})$, define $\Xi(\mathfrak{S}) \in M^M$ by $x\Xi(\mathfrak{S}) = x\alpha^{n(i)}$ if x lies in the set of any α_i in the d.c.d. of α where $|\underline{\text{set}}\ (\alpha_i)| = m_i$; otherwise, let $x\Xi(\mathfrak{S}) = x$. Clearly, $\Xi(\mathfrak{S}) \in \operatorname{Sym} M$. If F is any finite subset of M let F_i be the subset of all $x \in F$ that lie in cycles α_i of length m_i in the d.c.d. of α. Since F is finite, there exists a largest positive integer t such that F_t is nonvoid, or each F_i is void. By the Yih-hing theorem, there exists an integer n such that $n \equiv n_i \bmod m_i$ for all $i \in t^\#$ (in the former case). For such i, $F_i \mid \Xi(\mathfrak{S}) = F_i \mid \alpha^{n(i)} = F_i \mid \alpha^n$. Further, $(F \setminus \bigcup_{i=1}^t F_i) \mid \Xi(\mathfrak{S})$ is the identity map on $F \setminus \bigcup_{i=1}^t F_i$, as are α and α^n. We now have $F \mid \Xi(\mathfrak{S}) = F \mid \alpha^n$, from which $\Xi(\mathfrak{S}) \in \langle\alpha\rangle^-$. It is easy to see that $\Xi(\mathfrak{A}(\delta)) = \delta$ for each $\delta \in \langle\alpha\rangle^-$ and that $\mathfrak{A}(\Xi(\mathfrak{H})) = \mathfrak{H}$ for every $\mathfrak{H} \in G(\mathfrak{M})$. At once, the map $\mathfrak{A}$ from $\langle\alpha\rangle^-$ onto $G(\mathfrak{M})$ is an isomorphism with inverse Ξ. Observe that $\mathfrak{A}(\alpha^k) = \{k + (m_i)\}$ so that if $\{n_i + (m_i)\} \in G(\mathfrak{M})$ then $\{n_i - k + (m_i)\} \in G(\mathfrak{M})$ for each integer k. That is, in the ith component each residue class of m_i must appear for some member of $G(\mathfrak{M})$, and this last is, accordingly, a subdirect product of the direct product $\prod Z(m_i)$.

Since there are instances of subdirect products which are cyclic, we must proceed with caution. (For instance, the cyclic subgroup generated by $(1_2, 2_3, 3_5, 4_7, \cdots)$ in the direct product $\Pi Z(p)$ (over all primes p) is a subdirect product.) We produce a specific $\gamma \in \langle\alpha\rangle^- \setminus \langle\alpha\rangle$. Let $\mathfrak{R} = (r_1, r_2, \cdots)$ be any sequence of positive integers. Let $\mathfrak{S} = \mathfrak{S}(\mathfrak{M}, \mathfrak{R}) = (s_1, s_2, \cdots)$ 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 $\mathfrak{R}$ of positive integers exists for which $r_1 = 1$, $r_2 = 2$, and, for all positive integers i, if $s_i \in \mathfrak{S}(\mathfrak{M}, \mathfrak{R})$ 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 $\mathfrak{M}$ is strictly increasing there exists a least positive integer r_{k+1} such that $[s_1, \cdots, s_k] < [m_{r(k)+1}, \cdots, m_{r(k+1)}]$. That is, $[s_1, \cdots, s_k] < s_{k+1}$. □ Observe that $\mathfrak{R}$, as constructed here, is strictly increasing.

Returning to the main proof, consider a sequence $\mathfrak{B} = (b_1, b_2, \cdots)$ 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) $n_i \not\equiv b_i \bmod s_i$ for all $i \in k^\#$. Let $t_{ij} = (s_{i,k+1}, s_{j,k+1})$ for $1 \leq i < j \leq k$. Then $t_{ij} \mid s_{i,k+1} \mid s_i$; 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

$$(\mathrm{A}_k) \qquad x \equiv n_i \mod s_{i,k+1}, \qquad i \in k^\#,$$

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

$$n_{k+1} = \begin{cases} x_{k+1} & \text{if } x_{k+1} \not\equiv b_{k+1} \bmod s_{k+1}, \\ b_{k+1} + [s_1, \cdots, s_k], & \text{otherwise.} \end{cases}$$

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 $n_{k+1} \equiv b_{k+1} \bmod s_{k+1}$ then $s_{k+1} \mid [s_1, \cdots, s_k]$. By previous construction, however, $[s_1, \cdots, s_k] < s_{k+1}$. Thus, $n_{k+1} \not\equiv b_{k+1} \bmod s_{k+1}$ and $\mathfrak{R}$ has been constructed inductively in such a way that $s_{ij} \mid (n_i - n_j)$ and $n_i \not\equiv b_i \bmod s_i$ 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

$$(\mathrm{B}_i) \qquad m_{r(d(i)-1)} < m_i \leq m_{r(d(i))}.$$

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

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

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

To show that $\gamma \in \langle\alpha\rangle^-$, recall that $s_{d(i),d(j)} \mid (n_{d(i)} - n_{d(j)})$. 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_i) attests. Then $m_i \mid s_{d(i)}$, $m_j \mid s_{d(j)}$, from which $m_{ij} \mid s_{d(i),d(j)} \mid (n_{d(i)} - n_{n(j)})$. We now have $\mathfrak{H} \in G(\mathfrak{M})$ so that $\gamma = \Xi(\mathfrak{H}) \in \langle\alpha\rangle^-$.

To show that $\gamma \notin \langle\alpha\rangle$, consider sample cycles α_j of lengths m_j where j is restricted by $r_{d(i)-1} < j \leq r_{d(i)}$, possible since $\mathfrak{R}$ is strictly increasing. Let $C_j = \underline{\mathrm{set}}\,(\alpha_j)$, and let $F^i = \bigcup_j C_j$, $j = r_{d(i)-1} + 1, \cdots, r_{d(i)}$. Then $F^i \mid \gamma^j = F^i \mid \alpha^n$ 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* v, $F^i \mid \alpha^v = F^i \mid \alpha^n$ *where* $n = n_{d(i)}$ *if and only if* $v \equiv n_{d(i)} \mod s_{d(i)}$.

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

Return to the main proof, and recall that, for all pertinent i, $n_i \not\equiv b_i \mod s_i$.

In particular, $n_{d(i)} \not\equiv b_{d(i)} \bmod s_{d(i)}$. By Lemma 2, $F^i \mid \gamma \neq F^i \mid \alpha^n$, $n = n_{d(i)}$, $i = 1, 2, \cdots$. If γ were in $\langle\alpha\rangle$ then $\gamma = \alpha^k$ for some integer k. But $\mathrm{Im}(\mathfrak{B}\mathfrak{D}) = Z$, so that there exists a positive integer i for which $b_{d(i)} = k$. In particular, since $\gamma = \alpha^k$, $F^i \mid \gamma = F^i \mid \alpha^k$, contradicting what has just been proved. □

We know that $\beta \in \langle\alpha\rangle^-$ if and only if β coincides on each finite subset F of M with some α^m, $m = m(\beta, F)$. It is possible if $\langle\alpha\rangle^- \neq \langle\alpha\rangle$ 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 α. Let $m[x]$ be the length of $\alpha[x]$, finite by Theorem 1. Consider those finite subsets $F = \{a_1, \cdots, a_{n+1}\}$ (no repetitions allowed) of M with the property that there is at least one possible ordering $a_{i(1)}, \cdots, a_{i(n+1)}$ of the a_i's such that if $n > 0$ then $m[a_{i(n+1)}] \mid [m[a_{i(1)}], \cdots, m[a_{i(n)}]]$. Call such F's *α-good subsets of M.*

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

Proof. If $\beta \in (\mathrm{Sym}\, M)\setminus\langle\alpha\rangle^-$ the Jónsson result ([3], [4]) gives us a finitary algebra A on M with $\mathrm{Aut}\, A = \langle\alpha\rangle^-$, 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 $(a_1, \cdots, a_n)f = a_{n+1}$ but that $(a_1\beta, \cdots, a_n\beta)f \neq a_{n+1}\beta$. If the set U has repetitions, discard duplicates to obtain a finite subset $F = \{b_1, \cdots, b_{k+1}\}$ of M with no repetitions. We lose no generality in taking $b_{k+1} = a_{n+1}$. Since $(a_1\alpha, \cdots, a_n\alpha)f = a_{n+1}\alpha$, $m[a_{n+1}]$ 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 $[m[b_1], \cdots, m[b_k]] = r$. Hence F is an α-good subset of M.

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

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

Theorem 3. *$G(\mathfrak{M})$ and $X(\mathfrak{M})$ are isomorphic and can be represented faithfully as a closed hull $\langle\alpha\rangle^- \neq \langle\alpha\rangle$ in* Sym M.

Proof. For $\{n_i + (m_i)\} \in G(\mathfrak{M})$ construct an integral sequence $\mathfrak{T} = (t_0, t_1, \cdots)$ by setting $t_0 = n_1$ and, for $i \geq 1$, $t_i = n_{i+1} - n_i$. Then $\Sigma_{u=i}^{j} t_u = n_{j+1} - n_i$ for all integers i and j subject to $1 \leq i \leq j$. By construction, $\mathfrak{T} \in V(\mathfrak{M})$. If we replace each n_i by an alternate representative $n_i + c_i m_i$ for integers c_i, we then have $\mathfrak{T}' = (t_0', t_1', \cdots)$ where $t_0' = t_0 + c_1 m_1$ and where, for $i \geq 1$, $t_i' = t_i + c_{i+1} m_{i+1} - c_i m_i$. Since the sequence $(c_1 m_1, c_2 m_2 - c_1 m_1, \cdots) \in W(\mathfrak{M})$, each $\mathfrak{G} \in G(\mathfrak{M})$ determines some $\Psi(\mathfrak{G}) = \mathfrak{T} + W(\mathfrak{M})$ in $X(\mathfrak{M})$. It is clear that $\Psi \in \operatorname{Hom}(G(\mathfrak{M}), X(\mathfrak{M}))$. If $\mathfrak{G} = \{n_i + (m_i)\} \in \ker \Psi$ then $t_0 = c_1 m_1$ and, for $i \geq 1$, $t_i = c_{i+1} m_{i+1} - c_i m_i$ for appropriate integers c_i. But $n_{i+1} = \Sigma_{u=0}^{i} t_u$ for all nonnegative integers i, so that $n_{i+1} = c_{i+1} m_{i+1}$, $\mathfrak{G} = 0$, and Ψ is monic.

For preassigned $\mathfrak{T} + W(\mathfrak{M}) \in X(\mathfrak{M})$, define $n_{i+1} = \Sigma_{u=0}^{i} t_u$ for all nonnegative integers i. From the definition of $V(\mathfrak{M})$, $m_{i,j+1} \mid \Sigma_{u=i}^{j} t_u$ for all integers i and j subject to $1 \leq i \leq j$. Since $\Sigma_{u=i}^{j} t_u = n_{j+1} - n_i$, we have $m_{i,j+1} \mid (n_i - n_{j+1})$. Hence $\mathfrak{G} = \{n_i + (m_i)\} \in G(\mathfrak{M})$, $\Psi(\mathfrak{G}) = \mathfrak{T} + W(\mathfrak{M})$; Ψ is epic and is thus an isomorphism from $G(\mathfrak{M})$ onto $X(\mathfrak{M})$.

Given $\mathfrak{M}$, construct $\alpha \in M^M$ 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

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

Then $\alpha \in \operatorname{Sym} M$, and the nontrivial cycles in its d.c.d. are the $\alpha_i = (x_{i1}, \cdots, x_{i,m(i)})$. Thus $X(\mathfrak{M})$ is faithfully represented by $\langle\alpha\rangle^- \neq \langle\alpha\rangle$, and each L gives a distinct representation. □

Corollary. *If the set m_i of $\mathfrak{M}$ is a relatively prime set of integers then $G(\mathfrak{M})$ is isomorphic to the direct product $\Pi\, Z(m_i)$.*

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

4. Torsion elements.

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

Proof. If the order $|\mathfrak{G}|$ of $\mathfrak{G}$ is finite then $n_i |\mathfrak{G}| \equiv 0 \bmod m_i$ so that

$n_i(m_i, n_i)^{-1} \,|\, \mathfrak{G} \,| \equiv 0 \bmod m_i(m_i, n_i)^{-1}$, $i = 1, 2, \cdots$. 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 $|\mathfrak{G}|$. Hence the v_i are bounded and finite in number. Conversely, if the v_i are bounded let their distinct values be $c_1, \cdots, c_r$, and let $c = [c_1, \cdots, c_r]$. Each v_i equals some $c_{j(i)}$, and $n_i c = n_i c_{j(i)} e_i$ for some integer e_i, from which $n_i c = [m_i, n_i] e_i$. Since, however, $m_i \,|\, [m_i, n_i]$, $n_i c \equiv 0 \bmod m_i$ for $i = 1, 2, \cdots$, and $\mathfrak{G}$ is periodic with order dividing c.

Should $|\mathfrak{G}| < c$, there would have to exist some prime p dividing c such that $\exp_p |\mathfrak{G}| < \exp_p c = k$. 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 $n_a |\mathfrak{G}| = q_a m_a$ for a suitable integer q_a. It follows that $u_a |\mathfrak{G}| = v_a q_a = q_a c_i$. Since u_a and v_a are coprime, $p^k \,|\, c_i$ implies that $p^k \,|\, |\mathfrak{G}|$, a contradiction. Hence $|\mathfrak{G}| = c$. □

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

Proof. Let $k = \text{l.u.b.}_i \exp_p m_i$ be finite and at least 1, and let $\exp_p m_i$ be denoted by k_i. Let $u(1), u(2), \cdots$ be the distinct indices i for which $k_i = k$. This set U of $u(t)$'s may be finite or infinite, but U is nonempty since $1 \leq k$. We write $m_i = p^{k(i)} b_i$ 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

$$\text{(C)} \qquad x_{u(i)} b_{u(i)} \equiv x_{u(i+1)} b_{u(i+1)} \mod p.$$

Since each $(b_j, p) = 1$, 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 $i = 1, 2, \cdots$. Now $n_{u(1)} \equiv 0 \bmod m_{u(1)}$ would imply that $p \,|\, x_{u(1)}$, contrary to choice. Thus, at least one $n_i \not\equiv 0 \bmod m_i$. For all i, $pn_i = p^k x_i b_i$. If $k_i < k$, $x_i = 0$ and $pn_i = 0$. Since $m_{u(t)} = p^k b_{u(t)}$, one has $pn_{u(t)} \equiv 0 \bmod m_{u(t)}$. As a member of $\Pi Z(m_i)$, $\mathfrak{G} = \{n_i + (m_i)\}$ has order p.

We now show that $\mathfrak{G} \in G(\mathfrak{M})$, so that this last has a nontrivial p-component. (1) If $k_i, k_j < k$ 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 $m_{ij} = p^{k(i)}(b_i, b_j)$, 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 $\mathfrak{G} \in G(\mathfrak{M})$, as required.

Conversely, if $\mathfrak{G} \in G(\mathfrak{M})$ with $|\mathfrak{G}| = p$ where $\mathfrak{G} = \{n_i + (m_i)\}$ choose the n_i

subject to $0 \leq n_i < m_i$. By hypothesis, $m_i \mid pn_i$, $i = 1, 2, \cdots$. Let the prime decomposition of m_i be $p^{k(i)} q_j^{r(1)} \cdots q_j^{r(j)}$. If $n_i \neq 0$, $n_i = p^{l(i)} q_1^{s(1)} \cdots q_j^{s(j)} c$ where $c = 1$ or where c is a product of one or more prime powers for a prime or primes not in the set $\{p, q_1, \ldots, q_j\}$. Since $m_i \mid pn_i$ we have $k_i \leq l_i + 1$, and $1 \leq r_t \leq s_t$ for each $t \in j''$. Since $m_i > n_i$, $0 < m_i - n_i = q_1^{r(1)} \cdots q_j^{r(j)} p^{k(i)-1}(p - p^{w(i)} q_1^{s(1)-r(1)} \cdots q_j^{s(j)-r(j)} c)$ where $w(i) = l_i - k_i + 1 \geq 0$. If $w(i) > 0$, $p^{k(i)} \mid (m_i - n_i)$ and $p^{k(i)} \mid n_i$, incompatible with $0 \leq n_i < m_i$ and $m_i \mid pn_i$. We have $l_i + 1 = k_i$.

If $n_i \neq 0 = n_j$ then $m_{ij} \mid n_i$ where $n_i = p_i^{l(i)} h_i$, $(p, h_i) = 1$ and $m_{ij} = p^{\min(k(i), k(j))} h'$, $(p, h') = 1$. Then $\min(k_i, k_j) \leq l_i = k_i - 1$, so that $k_j < k_i$ in this case. If m_i and m_j are both nonzero then $n_i - n_j = p^{\min(l(i), l(j))} d$, and $m_{ij} = p^{\min(l(i)+1, l(j)+1)} h'$, 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, $p^{k(i)} \mid (p^{k(i)-1} h_i - p^{k(j)-1} h_j)$, from which $p \mid (h_i - p^{k(j)-k(i)} h_j)$. If $k_i < k_j$ we would have to conclude that $p \mid h_i$, 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 $\text{l.u.b.}_i\, k_i = k$, a finite value. Since $\mathfrak{G} \neq 0$ 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* $G(\mathfrak{M})$ *is bounded.*

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

5. **Nonminimality.** For an infinite set M, let $\mathbf{C}$ be the set of all subgroups of Sym M of the form $\langle\alpha\rangle^- \neq \langle\alpha\rangle$.

Lemma 3. *If* $\langle\alpha\rangle^- \in \mathbf{C}$ *then those members* β *of* $\langle\alpha\rangle^-$ *with the property that* $\langle\beta\rangle^- = \langle\beta\rangle$ *are precisely the torsion elements of* $\langle\alpha\rangle^-$.

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

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

Proof. Let p be some prime divisor of m_1 of $\mathfrak{M}$ where $G(\mathfrak{M})$ 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 α is no torsion element of Sym M, neither is α^p. By Lemma 3, $\langle\alpha^p\rangle^- \neq \langle\alpha^p\rangle$ so that $\langle\alpha^p\rangle^- \in \mathbf{C}$. Since $G(\mathfrak{M})$ is a subdirect product of the $Z(m_i)$'s where the m_i's are the members of $\mathfrak{M}$, there exists some $\gamma \in \langle\alpha\rangle^-$ for which the first component $n_1 + (m_1)$ of $\mathfrak{A}(\gamma)$ (see proof of Theorem 1 for notation) is $1 + (m_1)$. Let α_1 be a cycle of length m_1 in the d.c.d. of α, and let $C_1 = \underline{\text{set}}\ (\alpha_1)$. If γ were to lie in $\langle\alpha^p\rangle^-$ then $C_1 \mid \gamma = C_1 \mid \alpha^{pk}$. Let $\alpha_1 = (x_1 \cdots x_{m(1)})$. Then $x_2 = x_1\gamma$ since $\mathfrak{A}(\gamma) = (1 + (m_1), *, *, \cdots)$. Hence $x_2 = x_1\alpha^{pk}$, possible only if $pk \equiv 1 \bmod m_1$. Since $p \mid m_1$ we have a contradiction, so that $\langle\alpha^p\rangle^-$ is a proper sub-group of $\langle\alpha\rangle^-$ which also belongs to $\mathbf{C}$. □

REFERENCES

1. L. E. Dickson, *History of the theory of numbers*. Vol. II, Carnegie Inst., Washington, D. C., 1920.

2. M. Gould, *Automorphism groups of algebras of finite type*, Canad. J. Math. 24 (1972), 1065–1069.

3. B. Jónsson, *Algebraic structures with prescribed automorphism groups*, Colloq. Math. 19 (1968), 1–4. MR 36 #6336.

4. ———, *Topics in universal algebra*, Lecture Notes in Math., vol. 250, Springer-Verlag, Berlin and New York, 1972.

5. A. Karrass and D. Solitar, *Some remarks on the infinite symmetric group*, Math. Z. 66 (1956), 64–69. MR **18**, 376.

6. T.-J. Stieltjes, *Essai sur la théorie des nombres; premiers élements*, Paris, 1895.

7. H. Wielandt, *Unendliche Permutationsgruppen*, Zweite Vervielfältigung, York University, 1967.

DEPARTMENT OF MATHEMATICS, WASHINGTON UNIVERSITY, ST. LOUIS, MISSOURI 63130

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