PACIFIC JOURNAL OF MATHEMATICS
Vol. 81, No. 1, 1979

AUTOMORPHISM GROUPS RETRACTING ONTO SYMMETRIC GROUPS

MATTHEW GOULD AND HELEN H. JAMES

The main result of this note is that if a group G retracts onto the symmetric group S_n (n finite) then G is isomorphic to the automorphism group of the nth direct power of a multi-unary algebra (equivalently: G is isomorphic to the automorphism group of an algebra that is free on a basis of n elements). It will be shown that the converse fails for all $n > 1$, but a restricted form of the converse will be proved.

It was noted by G. Birkhoff in [1] that for any group G the right translations of G are precisely the automorphisms of the algebra defined on G by taking the left translations as operations. Thus our main result stated above is true for $n = 1$, in which case the class of groups in question is simply the class of all groups. Moreover, as the algebra of left translations is easily seen to be freely generated by any one of its elements, the equivalent formulation of our result is also true for $n = 1$. We therefore stipulate that $n > 1$ throughout the sequel.

1. **Preliminaries.** Concepts and notations of universal algebra used here and not explicitly defined are taken from Grätzer [5], while group and semigroup teminology comes from Hall [6] and Clifford and Preston [2] respectively. Additionally, the notations $\mathrm{Aut}(\mathfrak{A})$ and $\mathrm{End}(\mathfrak{A})$ will denote respectively the automorphism group and endomorphism monoid of an algebra $\mathfrak{A}$, and the term *rigid* will be applied to an algebra $\mathfrak{A}$ satisfying $|\mathrm{End}(\mathfrak{A})| = 1$. An algebra is said to be *multi-unary* if all its operations are unary.

We shall utilize the following four theorems from the literature. The first (but for a slight modification) and second come from the first author's work [3]; the first characterizes the endomorphism monoids of direct powers, while the second (with its obvious converse) characterizes the nontrivial automorphism groups of direct squares (thereby implying our main result in the case $n = 2$).

THEOREM 1.1. *Given a monoid M, the following are equivalent.*

(a) $M \cong \mathrm{End}(\mathfrak{A}^n)$ *for some algebra* $\mathfrak{A}$.

(b) *There exist an n-ary operation* [ ] *on M and distinct elements $d_1, \cdots, d_n$ of M satisfying the identities*

(b.1) $d_i d_j = d_i$

(b.2) $[xd_1, \cdots, xd_n] = x$

(b.3) $[x_1, \cdots, x_n]d_i = x_i d_i$

for all $i, j \in \{1, \cdots, n\}$ *and* $x, x_1, \cdots, x_n \in M$.

Moreover, for every monoid M *satisfying* (b) *there is a multi-unary algebra* $\mathfrak{A}$ *of cardinality* $|Md_1|$ *such that* $M \cong \mathrm{End}(\mathfrak{A}^n)$, *and* $\mathfrak{A}$ *is rigid if* d_1 *is a left zero of* M.

THEOREM 1.2. *For every group* G *containing an element of order two there is an algebra* $\mathfrak{A}$ *such that* $G \cong \mathrm{Aut}(\mathfrak{A}^2)$. *Moreover,* $\mathfrak{A}$ *can be chosen to be rigid and multi-unary.*

The next result, due to the first author [4], establishes the equivalence mentioned in the first paragraph; the additional equivalence of (a) and (b) below is an immediate consequence of Theorem 1.1.

THEOREM 1.3. *Given a group* G, *the following are equivalent.*

(a) $G \cong \mathrm{Aut}(\mathfrak{A}^n)$ *for some nontrivial algebra* $\mathfrak{A}$.

(b) $G \cong \mathrm{Aut}(\mathfrak{A}^n)$ *for some nontrivial multi-unary algebra* $\mathfrak{A}$.

(c) $G \cong \mathrm{Aut}(\mathfrak{B})$ *for some algebra* $\mathfrak{B}$ *that is free on an* n*-element basis.*

(d) $G \cong \mathrm{Aut}(\mathfrak{B})$, *where* $\mathfrak{B}$ *is free on an* n*-element basis and the operations of* $\mathfrak{B}$ *are all* n*-ary.*

Moreover, if there is a finite algebra satisfying one of these conditions, then each condition is satisfied by a finite algebra.

The following theorem, due to J. R. Senft [8], concretely characterizes the endomorphism monoids of free algebras.

THEOREM 1.4. *Given a submonoid* M *of the monoid of all transformations of a set* A, *and given a subset* B *of* A *with* $|B| = n$, *the following are equivalent.*

(a) $M = \mathrm{End}(\mathfrak{A})$ *for an algebra* $\mathfrak{A}$ *defined on* A *and freely generated by* B.

(b) $M = \mathrm{End}(\mathfrak{A})$ *for an algebra* $\mathfrak{A}$ *defined on* A, *freely generated by* B, *and having only* n*-ary operations.*

(c) *Every map of* B *into* A *extends to a unique member of* M.

As we shall be dealing with retractions of groups, it will be useful to adopt the equivalent concept of (external) semidirect product. Given groups A and S and a homomorphism $\theta: S \to \mathrm{Aut}(A)$, define a multiplication in $S \times A$ by: $\langle s, a\rangle \cdot \langle t, b\rangle = \langle st, (a\theta_t)b\rangle$ for all $\langle s, a\rangle$, $\langle t, b\rangle \in S \times A$, where θ_t denotes the image of t under θ. With this operation $S \times A$ is a group, denoted $S \times_\theta A$, which retracts onto a copy of S. Conversely, if we are given a retraction φ of a group

G onto a subgroup S, then $G \cong S \times_\theta A$, where $A = \operatorname{Ker} \varphi$ and $\theta: S \to \operatorname{Aut}(A)$ is given by $a\theta_s = s^{-1}as$ for all $s \in S$ and $a \in A$. (See pp. 88-90 of Hall [6].)

Finally, we adopt throughout the sequel the notation $x = \langle x_1, \cdots, x_n \rangle$ for elements x of A^n.

2. The retraction theorem.

We can now prove our main result, in a formulation that generalizes Theorem 3.1 of [3].

THEOREM 2.1. *Given a group G that retracts onto S_n, there is a rigid multi-unary algebra $\mathfrak{A}$ such that $G \cong \operatorname{Aut}(\mathfrak{A}^n)$, and $\mathfrak{A}$ is finite if G is.*

Proof. We have a subgroup A of G and a homomorphism $\theta: S_n \to \operatorname{Aut}(A)$ such that $G \cong S_n \times_\theta A$. Set $M = T_n \times A^n$, where T_n denotes the set of all transformations of $\{1, \cdots, n\}$.

For $\langle \alpha, a \rangle \in M$ define $a^\alpha \in A^n$ by: $(a^\alpha)_i = a_{i\alpha}$ for all i. Also, let Δ denote the diagonal of A^n, i.e., $\Delta = \{a \in A^n \mid a_1 = a_2 = \cdots = a_n\}$. Now, define a multiplication in M as follows. For all $\langle \alpha, a \rangle, \langle \beta, b \rangle \in M$,

$$\langle \alpha, a \rangle \cdot \langle \beta, b \rangle = \begin{cases} \langle \alpha\beta, (a\bar{\theta}_\beta)b \rangle & \text{if } \langle \beta, b \rangle \in S_n \times \Delta, \\ \langle \alpha\beta, b^\alpha \rangle & \text{otherwise,} \end{cases}$$

where $\bar{\theta}_\beta$ is the pointwise application of θ_β, and multiplication in A^n is pointwise as well.

We shall show that M, with the above multiplication, is a monoid whose group of units (invertibles) is isomorphic to G. Moreover, we shall exhibit distinct elements $d_1, \cdots, d_n$ of M and an n-ary operation $[\ ]$ such that the duals of the identities (b.1)-(b.3) hold. (The dual of an identity is the identity that results when every product xy is replaced by yx.) Thus, by Theorem 1.1 M will be anti-isomorphic to $\operatorname{End}(\mathfrak{A}^n)$ for a multi-unary algebra $\mathfrak{A}$, which will be rigid because we will show that d_1 is a right zero of M. Because anti-isomorphic groups are isomorphic, we will have $G \cong \operatorname{Aut}(\mathfrak{A}^n)$. Finally, the cardinality statement in Theorem 1.1 will ensure the finiteness of $\mathfrak{A}$ if G is finite. (Indeed, the algebra will have cardinality $|G|/(n-1)!$.)

It is immediately verified that $\langle 1, e \rangle$ serves as an identity element for M, where 1 is the identity of G and $e_i = 1$ for all i. To prove associativity of multiplication, we first assert four claims; as the first three are very easily demonstrated we prove only the fourth.

For all $\alpha, \beta \in T_n$ and $a, b \in A^n$:

(1) $(a^\alpha)^\beta = a^{\beta\alpha}$;

(2) $a^\alpha \bar{\theta}_\beta = (a\bar{\theta}_\beta)^\alpha$;

(3) $(ab)^\alpha = a^\alpha b^\alpha$;

(4) $\langle \alpha, a\rangle \cdot \langle \beta, b\rangle \in S_n \times \Delta$ if and only if $\langle \alpha, a\rangle$ and $\langle \beta, b\rangle$ both belong to $S_n \times \Delta$.

To prove (4), let $\langle \alpha, a\rangle$ and $\langle \beta, b\rangle$ belong to $S_n \times \Delta$ and note that $a\bar{\theta}_\beta \in \Delta$, whereupon $\langle \alpha, a\rangle \cdot \langle \beta, b\rangle = \langle \alpha\beta, (a\bar{\theta}_\beta)b\rangle \in S_n \times \Delta$. For the reverse implication, let $\langle \alpha, a\rangle \cdot \langle \beta, b\rangle \in S_n \times \Delta$. Then $\alpha\beta \in S_n$, whence $\alpha \in S_n$ and $\beta \in S_n$. Also, $b \in \Delta$ since otherwise we would have (from the definition of multiplication) $b^\alpha \in \Delta$, implying $b = b^{\alpha^{-1}\alpha} = (b^\alpha)^{\alpha^{-1}} \in \Delta$. Thus $\langle \beta, b\rangle \in S_n \times \Delta$, and so the definition of multiplication yields $(a\bar{\theta}_\beta)b \in \Delta$, whereupon $a\bar{\theta}_\beta \in \Delta$. As θ_β is one-to-one it follows that $a \in \Delta$. Hence $\langle \alpha, a\rangle$ and $\langle \beta, b\rangle$ belong to $S_n \times \Delta$.

We now establish associativity, dividing the proof into four cases. Let $x = \langle \alpha, a\rangle$, $y = \langle \beta, b\rangle$, and $z = \langle \gamma, c\rangle$ be elements of M.

Case 1. Suppose neither y nor z belongs to $S_n \times \Delta$. Then by (4) the same is true of yz, and so (using (1)) we have

$$\begin{aligned}(xy)z &= \langle \alpha\beta, b^\alpha\rangle z = \langle \alpha\beta\gamma, c^{\alpha\beta}\rangle = \langle \alpha\beta\gamma, (c^\beta)^\alpha\rangle = \langle \alpha, a\rangle \cdot \langle \beta\gamma, c^\beta\rangle \\ &= x(yz) .\end{aligned}$$

Case 2. Suppose both y and z belong to $S_n \times \Delta$. Then by (4) the same is true of yz, and

$$\begin{aligned}(xy)z &= \langle \alpha\beta, (a\bar{\theta}_\beta)b\rangle z = \langle \alpha\beta\gamma, [(a\bar{\theta}_\beta)b]\bar{\theta}_\gamma \cdot c\rangle \\ &= \langle \alpha\beta\gamma, (a\bar{\theta}_\beta\bar{\theta}_\gamma)(b\bar{\theta}_\gamma)c\rangle = \langle \alpha\beta\gamma, (a\bar{\theta}_{\beta\gamma})(b\bar{\theta}_\gamma)c\rangle \\ &= \langle \alpha, a\rangle\langle \beta\gamma, (b\bar{\theta}_\gamma)c\rangle = x(yz) .\end{aligned}$$

Case 3. Suppose $y \in S_n \times \Delta$ and $z \notin S_n \times \Delta$. Then (4) implies $yz \notin S_n \times \Delta$ and so (using (1)) we have

$$\begin{aligned}(xy)z &= \langle \alpha\beta, (a\bar{\theta}_\beta)b > z = \langle \alpha\beta\gamma, c^{\alpha\beta}\rangle = \langle \alpha\beta\gamma, (c^\beta)^\alpha\rangle \\ &= \langle \alpha, a\rangle \cdot \langle \beta\gamma, c^\beta\rangle = x(yz) .\end{aligned}$$

Case 4. Suppose $y \notin S_n \times \Delta$ and $z \in S_n \times \Delta$. Then (4) implies $yz \notin S_n \times \Delta$, whence by (2), (3) and the fact that $c^\alpha = c$ (because $c \in \Delta$) we have

$$\begin{aligned}(xy)z &= \langle \alpha\beta, b^\alpha\rangle z = \langle \alpha\beta\gamma, (b^\alpha\bar{\theta}_\gamma)c\rangle \\ &= \langle \alpha\beta\gamma, (b\bar{\theta}_\gamma)^\alpha c^\alpha\rangle = \langle \alpha\beta\gamma, (b\bar{\theta}_\gamma \cdot c)^\alpha\rangle \\ &= \langle \alpha, a\rangle \cdot \langle \beta\gamma, (b\bar{\theta}_\gamma)c\rangle = x(yz) .\end{aligned}$$

Thus M is a monoid. As the map $\langle \alpha, a\rangle \to \langle \alpha, a_1\rangle$ is obviously an isomorphism of $S_n \times \Delta$ onto $S_n \times_\theta A$, we have $S_n \times \Delta \cong G$. To see that G is isomorphic to the group of units of M it therefore remains only to note that, by (4), $S_n \times \Delta$ contains every invertible member of M.

As noted earlier our final task is to define in M distinct elements

$d_1, \cdots, d_n$ and an n-ary operation $[\ ]$ so that the duals of (b.1)-(b.3) are satisfied and d_1 is a right zero. We begin by endowing T_n with such structure.

For each $i \in \{1, \cdots, n\}$ let δ_i be the constant member of T_n whose image is $\{i\}$. For $\alpha_1, \cdots, \alpha_n \in T_n$ let $[\alpha_1, \cdots, \alpha_n]$ be the member of T_n that maps each i to $i\alpha_i$. It is clear that each δ_i is a right zero, and it is readily verified (as was done in [4] in a more general context) that T_n satisfies the duals of (b.1)-(b.3).

In A^n define an n-ary operation $[\ ]$ in the same manner as in T_n: for elements $U_1, \cdots, U_n$ of A^n, let $[U_1, \cdots, U_n]$ be that member V of A^n satisfying $V_i = (U_i)_i$ for all i.

Finally, set $d_i = \langle \delta_i, e\rangle \in M$ for all $i \in \{1, \cdots, n\}$, and define $[\ ]$ on M by stipulating that $[\langle \alpha_1, U_1\rangle, \cdots, \langle \alpha_n, U_n\rangle] = \langle [\alpha_1, \cdots, \alpha_n], [U_1, \cdots, U_n]\rangle$.

Since $n > 1$, the d_i are distinct and are not members of $S_n \times A$. Thus $\langle \alpha, a\rangle d_i = \langle \alpha\delta_i, e^\alpha\rangle = \langle \delta_i, e\rangle = d_i$ for all $\langle \alpha, a\rangle \in M$, whence each d_i is a right zero; in particular the dual of (b.1) holds.

Before verifying the other identities we note that $d_i\langle \alpha, a\rangle = \langle \delta_i\alpha, a^{\delta_i}\rangle$ whether or not $\langle \alpha, a\rangle \in S_n \times A$, and that $a^{\delta_i} = \langle a_i, \cdots, a_i\rangle$. From the latter observation it follows that $[a^{\delta_i}, \cdots, a^{\delta_n}] = a$, and that $[U_1, \cdots, U_n]^{\delta_i} = (U_i)^{\delta_i}$ whenever $U_1, \cdots, U_n$ are members of A^n.

To verify the dual of (b.2), let $x = \langle \alpha, a\rangle \in M$ and compute:

$$\begin{aligned}[d_1x, \cdots, d_nx] &= [\langle \delta_1\alpha, a^{\delta_1}\rangle, \cdots, \langle \delta_n\alpha, a^{\delta_n}\rangle] \\ &= \langle [\delta_1\alpha, \cdots, \delta_n\alpha], [a^{\delta_1}, \cdots, a^{\delta_n}]\rangle = x\ .\end{aligned}$$

Finally, to establish the dual of (b.3), let $x_i = \langle \alpha_i, U_i\rangle \in M$ and compute:

$$\begin{aligned}d_i[x_1, \cdots, x_n] &= \langle \delta_i[\alpha_1, \cdots, \alpha_n], [U_1, \cdots, U_n]^{\delta_i}\rangle \\ &= \langle \delta_i\alpha_i, U_i^{\delta_i}\rangle = d_ix_i\ ,\end{aligned}$$

whereupon the theorem is proved.

COROLLARY 2.2. *Given a group G that retracts onto S_n, there is an algebra $\mathfrak{A}$ such that $\mathfrak{A}$ is free on an n-element basis and $G \cong \mathrm{Aut}(\mathfrak{A})$. Moreover, $\mathfrak{A}$ can be taken to have operations of rank n only.*

Proof. Apply Theorem 1.3 to the above theorem.

COROLLARY 2.3. *If $n \neq 6$, every group containing S_n as a normal subgroup is isomorphic to $\mathrm{Aut}(\mathfrak{A}^n)$ for some rigid multi-unary algebra $\mathfrak{A}$.*

Proof. In Rotman [7], pp. 132-135, it is proved that for $n \notin \{2, 6\}$, S_n is a direct factor of every group in which S_n is normal. Thus Theorem 2.1 applies, proving the corollary for $n \neq 2$. However, for $n = 2$ the corollary is an immediate consequence of Theorem 1.2.

3. **Counterexamples and a restricted converse.** It is easily seen that the converse of Theorem 2.1 is false, i.e., that there exist rigid multi-unary algebras $\mathfrak{A}$, even finite as well, for which $\mathrm{Aut}(\mathfrak{A}^n)$ does not retract onto a copy of S_n.

For $n > 2$, choose any k such that $k^n - k > \max\{4, n\}$. On a set of cardinality k define an algebra by taking all constant functions as unary operations: the resulting rigid multi-unary algebra $\mathfrak{A}$ satisfies $\mathrm{Aut}(\mathfrak{A}^n) \cong S_{k^n - k}$. Since the only proper normal subgroup of the latter group is its alternating group, it has no proper retract other than S_2. (If one were to omit the requirement that the algebra be rigid and multi-unary, a more interesting example would be $S_{nk} \cong \mathrm{Aut}(\mathfrak{A}^n)$, where $\mathfrak{A}$ is the kth direct power of the two-element Boolean algebra, and k is chosen so that $nk > \max\{4, n\}$.)

For $n = 2$, counterexamples are immediately provided by Theorem 1.2, but the proof of this theorem (in [3]) does not produce a finite algebra with the required properties. To exhibit such a finite algebra, consider the alternating group A_4 (which does not retract onto S_2, as A_4 contains no subgroup of order 6), and note (by inspection) that every one-to-one map of $\{1, 2\}$ into $\{1, 2, 3, 4\}$ extends to a unique member of A_4. Thus, if we let M denote the union of A_4 with the constant transformations of $\{1, 2, 3, 4\}$, M will be a monoid satisfying condition (c) of Theorem 1.4 with respect to the set $B = \{1, 2\}$. Theorems 1.4 and 1.3 now provide the desired finite multi-unary algebra, which can (by inspecting the proofs of these theorems) be shown to be rigid.

Although the converse of Theorem 2.1 fails, we have the following restricted converse of Corollary 2.2. This result also shows that while unary operations are sufficient to represent a group as the automorphism group of a direct power, the corresponding situation does not obtain in the case of free algebras.

THEOREM 3.1. *If $\mathfrak{A}$ is a finite multi-unary algebra freely generated by an n-element set, then* $\mathrm{Aut}(\mathfrak{A})$ *retracts onto a copy of* S_n.

Proof. We may suppose that $\mathfrak{A}$ is freely generated by the set $\{1, \cdots, n\}$. For each $\pi \in S_n$, let π^* denote the extension of π to an endomorphism of $\mathfrak{A}$; then in fact $\pi^* \in \mathrm{Aut}(\mathfrak{A})$ and $S_n^* = \{\pi^* \mid \pi \in S_n\}$ is a subgroup of $\mathrm{Aut}(\mathfrak{A})$ and is isomorphic to S_n under the map $\pi \to \pi^*$. We shall exhibit a retraction of $\mathrm{Aut}(\mathfrak{A})$ onto S_n^*. For convenience,

the symbols i, j, k will invariably denote members of $\{1, \cdots, n\}$, and A will denote the carrier-set of $\mathfrak{A}$. Also, the symbol [ ] will denote the subalgebra of $\mathfrak{A}$ generated by the enclosed element.

Because the operations of $\mathfrak{A}$ are unary, A is the union of the sets $[i]$. By freeness, no member of the basis can belong to the subalgebra generated by any other member; thus, $[j] = [k]$ only if $j = k$.

Since each $[i]$ is freely generated by a one-element set (relative to the variety generated by $\mathfrak{A}$), it follows that all $[i]$ are isomorphic. Moreover, for $\alpha \in \mathrm{Aut}(\mathfrak{A})$, $[i\alpha] = [i]\alpha \cong [i]$. Hence all sets of the form $[j]$ and $[i\alpha]$ have the same finite cardinality, whence no such set can be properly contained in another.

Fixing $\alpha \in \mathrm{Aut}(\mathfrak{A})$, for each i we can find some j such that $i\alpha \in [j]$; it follows that $[i\alpha] \subseteq [j]$, and so $[i\alpha] = [j]$. Moreover, the above remarks imply that $[i\alpha] = [k]$ only when $j = k$. Thus we define a transformation π_α of $\{1, \cdots, n\}$ by setting $i\pi_\alpha$ equal to the unique j for which $[i\alpha] = [j]$. To see that $\pi_\alpha \in S_n$, note that $i\pi_\alpha = k\pi_\alpha$ implies $[i\alpha] = [k\alpha]$, i.e., $[i]\alpha = [k]\alpha$, whence $[i] = [k]$, and so $i = k$.

Clearly the map $\alpha \to \pi_\alpha^*$ maps $\mathrm{Aut}(\mathfrak{A})$ onto S_n^* and is identity on S_n^*. Moreover, for $\alpha, \beta \in \mathrm{Aut}(\mathfrak{A})$ we have $[i\pi_{\alpha\beta}] = [i\alpha\beta] = [i\alpha]\beta = [i\pi_\alpha]\beta = [i\pi_\alpha\beta] = [i\pi_\alpha\pi_\beta]$ for all i, whence $\pi_{\alpha\beta}^* = (\pi_\alpha\pi_\beta)^* = \pi_\alpha^*\pi_\beta^*$, whereupon the map $\alpha \to \pi_\alpha^*$ is the desired retraction.

Added in Proof. Professor J. B. Nation has pointed out to the authors that the proof of Theorem 3.1 can readily be recast so as to remove the assumption of finiteness. Moreover, Professor B. Jónsson has noted that for an algebra free in a regular variety the assumption of unary operations can similarly be removed.

References

1. G. Birkhoff, *Sobre los grupos de automorfismos*, Revista Unión Mat. Argentina, **11** (1946), 155-157.
2. A. H. Clifford and G. B. Preston, *The Algebraic Theory of Semigroups*, Amer. Math. Soc., Mathematical Surveys No. 7, **I** (1961), Vol. **II** (1967).
3. M. Gould, *Endomorphism and automorphism structure of direct squares of universal algebras*, Pacific J. Math., **59** (1975), 69-81.
4. ———, *Automorphism groups of free algebras and direct powers*, Colloquium on Universal Algebra of the J. Bolyai Math. Soc., to appear.
5. G. Grätzer, *Universal Algebra*, Van Nostrand Reinhold, 1968.
6. M. Hall, *The Theory of Groups*, Macmillan, 1959.
7. J. J. Rotman, *The Theory of Groups: An Introduction*, Allyn and Bacon, 1973.
8. J. R. Senft, *Endomorphism semigroups of free algebras*, Notices Amer. Math. Soc., **17** (1970), 562.

Received November 21, 1977.

VANDERBILT UNIVERSITY
NASHVILLE, TN 37235
AND
UNIVERSITY OF ALABAMA
HUNTSVILLE, AL 35806