CONSTRUCTIVE ANALOGUES OF THE GROUP OF PERMUTATIONS OF THE NATURAL NUMBERS

BY

CLEMENT F. KENT(1)

A portion of the theory of recursive functions is concerned with properties which are recursive invariants of sets of natural numbers, i.e., properties of such sets which are invariant under recursive isomorphisms. Thus the group of recursive isomorphisms, or permutations, of the natural numbers, and certain related groups of permutations, defined by more "generous" constructivity conditions are of interest in the theory of recursive functions. In this paper it is shown that two families of such groups, satisfying two different kinds of constructivity conditions, have algebraic properties similar to those of S_∞, the group of all permutations of the natural numbers. The group S_∞ has been studied by Schreier and Ulam in 1933 and 1937 in references [SU(1); SU(2)], and earlier by Onofri, reference [O(1)].

The group S_∞ is uncountable while all the groups considered in this paper are countable. Since permutations of the set of natural numbers(2), N, like permutations of finite sets can be factored into products of disjoint cycles, two permutations can be said to have the same cycle structure if, in their disjoint factorizations, there appear the same cardinal number of cycles of each possible length (including infinity). In S_∞, two permutations, π_1 and π_2, are conjugate, $\pi_1=\sigma\pi_2\sigma^{-1}$ for some $\sigma\in S_\infty$, when and only when they have the same cycle structure. Using the equivalence of conjugacy and cycle structure, it is shown in [SU(1)] that any normal subgroup, G, of S_∞, which contains a permutation, π, moving an infinity of numbers, must be all of S_∞. Thus it is shown that $S_\infty \supset F \supset A \supset \{\epsilon\}$ is the unique composition series for S_∞. Here, F is the subgroup of S_∞ composed of permutations which are, almost everywhere, the identity, while A is the subgroup of F composed of the even permutations, and ϵ is the identity permutation.

In §1 we show that equivalent cycle structure does not necessarily produce conjugacy in R, the group of recursive permutations. Nevertheless, in §2, it is shown that $R \supset F \supset A \supset \{\epsilon\}$ is the unique composition series for R, and indeed, for any group R_M of permutations of N, recursive in an arbitrary subset M of N, that $R_M \supset F \supset A \supset \{\epsilon\}$ is the unique composition series.

Presented to the Society, June 18, 1960 and August 24, 1961 under the titles, *Algebraic structure of the group of recursive permutations* and *Automorphism group of recursive permutations*; received by the editors June 22, 1961.

(1) With the exception of §4, the results of this paper are contained in a thesis presented to the Department of Mathematics, Massachusetts Institute of Technology, in August, 1960, in partial fulfillment of the requirements for the Ph.D. degree. The author wishes to thank Professor Hartley Rogers, Jr. for very considerable encouragment and advice.

(2) We always assume that $0\in N$.

In §3, we consider a group A_r, defined to be the union

$$R_\phi \cup R_\phi' \cup R_\phi'' \cup \cdots \cup R_\phi^{(n)} \cup \cdots$$

where the prime denotes the jump operation of the Kleene-Mostowski arithmetical hierarchy. These permutations are called arithmetical(3), and for a résumé of basic information regarding this hierarchy see, for example, [R(1)]. It is shown in §3 that, in A_r equivalent cycle structure again produces conjugacy, and that $A_r \supset F \supset A \supset \{\epsilon\}$ is the unique composition series. The results of part 3 are applicable to other, analogously defined, groups of permutations.

In [SU(2)] it is shown that S_∞ is isomorphic to its group of automorphisms. Here, in §4, we show that all of the groups considered above, like S_∞, are isomorphic to their automorphism groups.

The presentation of proofs in this paper is informal, in that sets of recursion equations are not always written for functions asserted to be recursive. This is an application of Church's Thesis in an attempt to present the ideas of the proofs in sufficient detail that their translation into a formal system for recursive functions is a routine step. The proofs in §§2 and 4 owe much to those of [SU(1); SU(2); O(1)]. In some cases it has been necessary only to supply effectiveness arguments and in others to make easy replacements of noneffective arguments by effective ones.

In addition to the notation already introduced, we comment that small Greek letters are used for permutations of N, small Latin letters for numbers and number variables, and capital Latin letters for subsets of N (in addition to the various permutation groups). We use a standard enumeration of the partial recursive functions of a single variable, denoted

$$\psi_0, \psi_1, \psi_2, \cdots, \psi_n, \cdots$$

and $T_1(x, y, z)$ for the Kleene T-predicate. In addition, $p_1(x)$ and $p_2(x)$ are used to denote the primitive recursive coordinate functions which map N onto $N \times N$. The characteristic function of a set A, χ_A, is that function

$$\chi_A(x) = \begin{cases} 0 & \text{if } x \in A, \\ 1 & \text{if } x \in \overline{A}, \end{cases}$$

where $\overline{A}$ denotes $N - A$. Other notation is introduced as needed.

1. **Conjugacy classes in** R. As commented earlier, cycle-structure is a necessary and sufficient condition for conjugacy in S_∞, a fact which is central in the proofs of [SU(1); O(1)]. As we proceed to show in this section, the same is not true in R (although it is again in A_r). The cycle structure classes of R may be sorted into two categories, those whose cycle structure contains only finitely many infinite cycles and those whose cycle structure contains

(3) They are the permutations which can be defined by formulas of arithmetic.

infinitely many infinite cycles. It will be shown that those cycle structure classes of the first kind are also conjugacy classes, while those of the second kind are always properly partitioned into two or more conjugacy classes.

If σ is a member of R (more generally of S_∞) we define $\Sigma_\sigma \subseteq N$ to be a *choice-set*(4) for σ if Σ_σ is composed of numbers, precisely one drawn from each of the disjoint cycles of σ. The following two lemmas are easily proved and are stated without proof.

LEMMA 1.0. *If π is a permutation of N, then π possesses a choice-set Σ_π, which can be expressed in both two-quantifier forms relative to π.*

LEMMA 1.1. *If π has a choice set, Σ_π, which is recursively enumerable in π, then each cycle of π is a set recursive in π.*

THEOREM 1.2. *Let σ_1 and σ_2 be two recursive permutations with the same cycle structure and such that each has only a finite number of infinite cycles. Then σ_1 and σ_2 are conjugate in R.*

Proof. Let $C_1^1, C_2^1, \cdots, C_n^1$ be the disjoint infinite cycles of σ_1 and $C_1^2, C_2^2, \cdots, C_n^2$ the disjoint infinite cycles of σ_2. Each of the C_i^j is a recursively enumerable set and thus

$$I_1 = \bigcup_{i=1}^{n} C_i^1 \quad \text{and} \quad I_2 = \bigcup_{i=1}^{n} C_i^2$$

are recursively enumerable sets. We note that the complements $F_1 = N - I_1$ and $F_2 = N - I_2$ are composed of the elements which lie in finite cycles of σ_1, respectively σ_2. F_1 and F_2 are thus recursively enumerable sets. Then I_1 and I_2 are recursive. It follows that the sets C_i^j are recursive sets.

It is now an easy step to complete the proof by constructing a recursive permutation, τ, which sends cycles of σ_1 into cycles of σ_2, preserving order. Such a τ will give $\sigma_2 = \tau\sigma_1\tau^{-1}$. The construction details are omitted.

We next note that, if σ_1 and σ_2 are conjugate members of R, then the cycles of σ_1 are carried onto the cycles of σ_2 by a recursive isomorphism. Thus, there is a pairing of cycles of σ_1 with cycles of σ_2 which preserves isomorphism type. It is not difficult to construct a recursive permutation, σ_0, which is composed of infinitely many infinite recursive cycles. In the next theorem we show that there is a recursive permutation, ρ, in the cycle structure class of σ_0, but having a creative cycle. By the remarks above, σ_0 and ρ cannot be conjugate(5).

(4) This term is introduced in [$M(1)$]. The author is indebted to the referee for calling attention to the close connections of some of these results to those in [M(1); U(1)], and for several interesting additional results and conjectures (below).

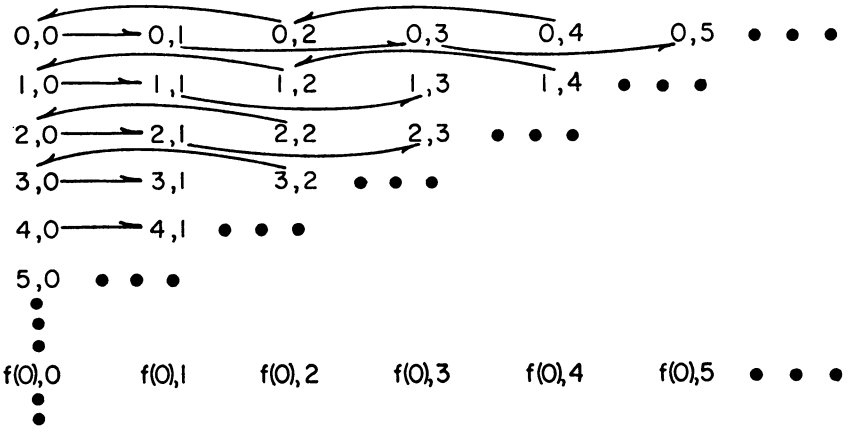
(5) The present statement and proof of Theorem 1.3 follow from suggestions of the referee which resulted in a great simplification of the original. In addition, Corollaries 1.5 and 1.6 were obtained from the restated theorem. The referee conjectured that any creative set is the splinter of some recursive permutation. This can be proved by a slight modification of the present proof.

THEOREM 1.3. *Let C be a creative set. There is a recursive permutation, ρ, composed of infinitely many infinite cycles, one of which is C.*

Proof. In [M(1)] the symbol j is used to denote a one-one recursive function mapping $N \times N$ onto N. If A is an arbitrary recursively enumerable set, the notation $\mathrm{Cy}(A)$ is introduced in [M(1)] to denote the set $j(A \times N)$. Such sets are called *cylinder sets*. The cylinder set $j(A \times N)$ is many-one equivalent to A. If A is creative, then so is $\mathrm{Cy}(A)$ and thus $\mathrm{Cy}(A)$ is carried onto A by a recursive permutation, τ. We shall construct a permutation, π, having $\mathrm{Cy}(A)$ as a cycle. Then the recursive permutation $\rho = \tau\pi\tau^{-1}$ will have A as a cycle. Thus it suffices to prove the following lemma.

LEMMA 1.4. *If A is a nonvoid recursively enumerable set, there is a recursive permutation, π, composed of infinitely many infinite cycles, one of which is* $\mathrm{Cy}(A)$.

Proof. Let A be a nonvoid recursively enumerable set. If A is finite the proof is trivial. Suppose that A is infinite and that f is a one-one recursive function which enumerates A. We lose no generality and we simplify the proof if we define π as a permutation on $N \times N$. Consider the following diagram of $N \times N$. The arrows in the diagram, present in every row except the $f(0)$th row, define the basic *pattern* of definition for π, to be followed until interrupted by the procedure below.



To simplify further the presentation of the computation procedure we make the following definitions.

$b(p, q, k)$ = the largest natural number b for which $\pi^{-b}(p, q)$ has been defined during the first k stages of the computation procedure.

$t(p, q, k)$ = the largest natural number t for which $\pi^{t}(p, q)$ has been defined during the first k stages of the computation procedure.

$L_k((p_1, q_1), (p_2, q_2))$ is an instruction to define $\pi^{t(p_1,q_1,k)+1}(p_1, q_1) = \pi^{-b(p_2,q_2,k)}(p_2, q_2)$.

The procedure follows.

Stage 0: Define $\pi(0, 0) = (0, 1)$.

Stage k, $k>0$: Let p and q be chosen so that $j(p, q) = k$, then proceed with the following steps, in order.

Step (i): If $(\exists i)(0 \leqq i \leqq k \,\&\, p = f(i) \,\&\, i$ is odd) then apply $L_k((p, q), (f(0), 0))$.

Step (ii): If $(\exists i)(0 \leqq i \leqq k \,\&\, p = f(i) \,\&\, i$ is even) then apply $L_k((f(0), 0), (p, q))$.

Step (iii): If $\pi(p, q)$ is already defined, go to stage $k+1$.

Step (iv): If $\pi(p, q)$ is undefined and (i) $(0 \leqq i \leqq k \Rightarrow p \neq f(i))$ then define $\pi(p, q)$ by the *pattern*.

Step (v): If $\pi(p, q)$ is undefined but $(\exists i)(0 \leqq i \leqq k \,\&\, p = f(i))$ then define $\pi(p, q) = (p, \mu r(\pi^{-1}(p, r)$ is undefined at stage $k))$.

This completes the description of the defining procedure for π. Note

(a) π is a partial recursive function by Church's Thesis,

(b) π is a total function, since $\pi(p, q)$ is always defined at or before stage k, where $j(p, q) = k$,

(c) π is a permutation,

(d) for any p which is not in A, the pth row of the $N \times N$ diagram becomes an infinite cycle of π,

(e) for any p which is in A, the pth row becomes a part of the cycle which is built about $f(0)$, 0.

This completes the proof of the lemma.

COROLLARY 1.5. *For any recursively enumerable set A, there is a recursive permutation with a cycle of the same many-one degree as A. Also, there is a recursive permutation for which the set, F, of elements of finite algebraic order, is many-one equivalent to A.*

Proof. The first part is proved in the lemma. The second follows from a modification of the construction of the proof of the lemma which causes all of the members of $\mathrm{Cy}(A)$ to appear in finite cycles.

Corollary 5.3 of [U(1)] states the following.

"The set T of theorems of any consistent system which contains elementary number theory can be generated from any $\phi \in T$ by a one-premise rule of inference R, which, under Gödel numbering, is a one-one recursive function."

This result, applicable to any theory with a creative set of theorems, follows as an immediate corollary to the result, proved in [M(1); U(1)], that every creative set, C, is the x-splinter of a one-one recursive function f_x for any $x \in C$, where the choice of f_x depends upon the choice of $x \in C$. A modification of the proof of Theorem 1.3 shows that the rule R, above, can

in fact be made a recursive permutation, but Theorem 1.3 can be used directly to prove the following interesting variant of Ullian's Corollary 5.3.

COROLLARY 1.6. *The set T of theorems of any consistent system which contains number theory can be generated from any $\phi \in T$ by the repeated application of one of two one-premise rules of inference, R or L, which are mutually inverse, and whose choice does not depend upon ϕ.*

Proof. The set, T_G, of Gödel numbers of members of T is a creative set. Consequently, it is a cycle of a recursive permutation, π. We may define R and L as follows.

To apply R to a formula ϕ, obtain the Gödel number x of ϕ. Evaluate $\pi(x)$ and let $R(\phi)$ be that formula whose Gödel number is $\pi(x)$. To obtain the rule L, replace R by L and π by π^{-1} in the instruction. Clearly, for any formula ϕ we have $R(L(\phi)) = L(R(\phi)) = \phi$. This proves the corollary.

THEOREM 1.7. *In the group R, a cycle structure class, C, is also a conjugacy class if and only if it is the cycle structure class of a permutation with finitely many infinite cycles*([6]).

Proof. The sufficiency of the condition follows immediately from Theorem 1.2. To prove the necessity, take a recursive permutation, σ, with infinitely many infinite cycles. If σ has no finite cycles, the necessity is proven by Lemma 1.4. In case σ has only finitely many finite cycles, then F_σ is finite, thus recursive. There is a one-one recursive function, g, which enumerates I_σ, and, since I_σ is recursive, g can be used to transfer the structure of either σ_0, or of the π of Lemma 1.4 onto I_σ. In this manner the case of finitely many finite cycles is proved.

Finally, suppose that σ has infinitely many finite cycles. Let f be the recursive function $f(x) = 2x+1$. Define

$$\sigma_0'(x) = f\sigma_0 f^{-1}(x) \text{ if } x \text{ is odd},$$
$$\pi'(x) = f\pi f^{-1}(x) \text{ if } x \text{ is odd}.$$

The definitions of σ_0' and of π' are completed for even x so as to transfer the finite cycle structure of σ to the even integers. To do this we define a partial recursive function $\Delta(x)$ which gives the σ-order of x if x has finite σ-order, and consider a simultaneous calculation of $\Delta(x)$ for all x. We know that $\Delta(x)$ will converge for infinitely many x. Define a set $X = \{x_1, x_2, x_3, \cdots, x_j, \cdots\}$, where the elements are listed in order in which $\Delta(x)$ converges and, for all i, x_i does not belong to the finite cycle determined by any x_j for $j<i$. Then X is an infinite recursively enumerable set which is a choice-set for the finite

([6]) The referee has shown that at least one cycle structure class of infinitely many infinite cycles splits into infinitely many conjugacy classes. His proof also gave him the present Corollary 1.5, strengthening the original version.

part of σ. Let $\Delta(x_i) = o_i$. Then the common definition of σ_0' and π' on the even natural numbers is the following.

$$(0, 2, 4, \cdots, 2(o_1 - 1))(2o_1, 2o_1 + 2, \cdots, 2(o_1 + o_2 - 1)) \cdots$$
$$\left(2\sum_1^n o_i,\ 2\sum_1^n o_i + 2, \cdots, 2\left(\sum_1^{n+1} o_i - 1\right)\right), \cdots.$$

Then, π' and σ_0' have the same cycle structure, which is the cycle structure of σ. They cannot be conjugate, for under conjugation the infinite cycles of one permutation are pairwise recursively isomorphic to the infinite cycles of the other. However, like σ_0, the infinite cycles of σ_0' are all recursive sets while, like π, one of the infinite cycles of π' is creative. This completes the proof of Theorem 1.7.

2. **Normal subgroups of R_M.** In [SU(1); O(1)], Schreier-Ulam, and previously Onofri, have shown that

$$S_\infty \supset F \supset A \supset \{\epsilon\}$$

is the unique composition series for S_∞. In this section we establish, through a sequence of lemmas, that the analogous result holds for a group R_M, of permutations recursive in an arbitrary set, M. It will be shown that

$$R_M \supset F \supset A \supset \{\epsilon\}$$

is the unique composition series for any such R_M. The group F is the subgroup of S_∞ composed of permutations moving only finitely many natural numbers. Each such permutation is recursive and hence, $F \subseteq R_M$, for any $M \subseteq N$. Moreover, it is clear that F is normal in R_M. The subgroup A, of F, consists of those finite permutations which are even and hence is a subgroup of F of index 2, and thus is maximal normal in F. The simplicity of A follows in the same way that the simplicity of the alternating group on n-letters, $n \geqq 4$, is proven.

We shall show that any normal subgroup G, of R_M, which contains a non-finite permutation, is all of R_M (Theorem 2.1). Hence F is maximal normal in R_M. Presuming the result of 2.1, it is easily seen, by using the Jordan-Hölder theorem and the elementary isomorphism theorems for groups, that the only normal subgroups of R_M are those in the composition series

$$R_M \supset F \supset A \supset \{\epsilon\}.$$

THEOREM 2.1. *If G is a normal subgroup of R_M, and if G contains a permutation, π, which moves an infinite number of numbers, then $G = R_M$.*

Proof. The proof is contained in four lemmas. The first lemma was obtained in [SU(1)], although here the proof is shortened, while the next two and their proofs are close to results obtained in [O(1)]. The level of presentation in the proofs of these four lemmas, is expository, which means that

liberal use is made of Church's Thesis, to avoid writing systems of recursion equations. Henceforth, a permutation which moves an infinite number of numbers is called an infinite permutation.

LEMMA 2.2. *If G is a normal subgroup of R_M, containing an infinite permutation, π, then G contains a permutation, τ, with infinitely many disjoint 2-cycles.*

Proof. Since π is infinite, we may define an infinite set $X=\{x_0<x_1<x_2<\cdots\}$, recursive in M, as follows:

$$x_0 = \mu z(\pi(z) \neq z),$$

$$x_k = \mu z\left(z > \max_{i=0}^{k-1}\{\pi^{-1}(x_i), x_i, \pi(x_i)\} \;\&\; \pi(z) \neq z\right).$$

The set $Y=X\cup\pi X$ is infinite, recursive in M, and the elements of Y; $x_0, \pi(x_0), x_1, \pi(x_1), \cdots$ are all distinct since π is a permutation. We may now define a permutation, σ, recursive in M, as follows:

$$\sigma(x) = \begin{cases} \pi(x) & \text{if } x \in X, \\ x_{i+1} & \text{if } x \in \pi X \text{ and } \pi^{-1}(x) = x_i \text{ for } i \text{ even}, \\ x_{i-1} & \text{if } x \in \pi X \text{ and } \pi^{-1}(x) = x_i \text{ for } i \text{ odd}, \\ x & \text{if } x \notin Y. \end{cases}$$

If we use σ to conjugate π, we get the following picture:

$$\begin{array}{rl} \pi = & \cdots, x_0, \pi(x_0), \cdots, x_1, \pi(x_1), \cdots, x_2, \pi(x_2), \cdots, x_3, (\pi x_3), \cdots \\ & \quad | \quad | \quad | \quad | \quad | \quad | \quad | \quad | \\ & \quad \sigma \quad \sigma \quad \sigma \quad \sigma \quad \sigma \quad \sigma \quad \sigma \quad \sigma \\ & \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \\ \sigma\pi\sigma^{-1} = & \cdots, \pi(x_0), x_1, \cdots, \pi(x_1), x_0, \cdots, \pi(x_2), x_3, \cdots, \pi(x_3), x_2, \cdots \end{array}$$

Since σ is recursive in M, $\sigma\in R_M$, and since G is normal $\sigma\pi\sigma^{-1}\in G$. Then $\sigma\pi\sigma^{-1}\pi\in G$. Let $\tau=\sigma\pi\sigma^{-1}\pi$. It is easily seen that τ has the infinitely many 2-cycles

$$(x_0, x_1), (x_2, x_3), (x_4, x_5), \cdots, (x_{2k}, x_{2k+1}), \cdots,$$

and this concludes the proof of Lemma 2.2.

In preparation for the next lemma we note that if X and Y are infinite sets with infinite complements (such sets we shall call C-infinite), which are recursive in M, and if $f_X, f_Y, f_{\bar{X}}$ and $f_{\bar{Y}}$ are one-one functions, recursive in M, which enumerate the indicated sets, then, there is a permutation, $\sigma\in R_M$, so that, for all x:

$$\sigma(f_X(x)) = f_Y(x), \qquad \sigma(f_{\bar{X}}(x)) = f_{\bar{Y}}(x).$$

This result, restated, is that R_M is infinitely transitive with respect to C-infinite M-recursive sets, and is immediate. It follows from the next lemma

that a normal subgroup of R_M is infinitely transitive with respect to C-infinite M-recursive sets, if and only if it contains an infinite permutation.

LEMMA 2.3([7]). *Let G be a normal subgroup of R_M containing a permutation, π, with infinitely many disjoint 2-cycles. If X is a C-infinite set, recursive in M, and f_1 and f_2 are two M-recursive, one-one functions enumerating X, then there is $\rho \in G$ so that, for all x, $\rho(f_1(x)) = f_2(x)$.*

Proof. The lemma follows immediately from the following result. (α): If X and Y are M-recursive, infinite sets, with Y a subset of $\overline{X}$, and if $\overline{X} - Y$ is infinite, then, if f_X and f_Y are one-one M-recursive functions enumerating X and Y, there is a $\rho_1 \in G$ so that, for all x, $\rho_1(f_X(x)) = f_Y(x)$.

To obtain the proof of (α), we define an infinite M-recursive set, B, whose elements are selected from disjoint 2-cycles of the M-recursive permutation, π, in such a way that infinitely many 2-cycles of π are not represented in B. We may represent π (effectively in M) as follows:

$$\pi = (x_0, x_1)(x_2, x_3) \cdots (x_{2k}, x_{2k+1}) \cdots \gamma$$

where, for all k; $x_{2k} < x_{2k+1}$, $x_{2k} < x_{2k+2}$, and γ contains no 2-cycles. Define B to be the C-infinite M-recursive set $\{x_{4k} \mid k = 0, 1, 2, \cdots\}$ and let f_B be the M-recursive function which enumerates B in increasing order. Then, by remarks preceding the lemma, there is an M-recursive permutation, ξ, which, for all x, gives $\xi(f_B(x)) = f_X(x)$. Let $\sigma = \xi\pi\xi^{-1}$. Then $\sigma \in G$. Note that σ has the cycle structure of π and that distinct elements of X appear in distinct 2-cycles of σ. By hypothesis of result (α) and the construction of σ, the two sets

$$X \cup \sigma X = \{f_X(0), \sigma f_X(0), f_X(1), \sigma f_X(1), \cdots\},$$
$$X \cup Y = \{f_X(0), f_Y(0), f_X(1), f_Y(1), \cdots\}$$

are C-infinite, M-recursive, and, there is $\mu \in R_M$ which sends the elements of $X \cup \sigma X$ onto the elements of $X \cup Y$, in the order indicated, i.e., for all x:

$$\mu(f_X(x)) = f_X(x), \qquad \mu(\sigma f_X(x)) = f_Y(x).$$

Finally, let $\rho_1 = \mu\sigma\mu^{-1}$, and result ($\alpha$) follows. This completes the proof of Lemma 2.3.

LEMMA 2.4. *Let G be a normal subgroup of R_M having the property: If X is a C-infinite, M-recursive set, and f_1 and f_2 two M-recursive, one-one, functions enumerating X, then there is $\pi \in G$ so that, for all x, $\pi(f_1(x)) = f_2(x)$. Further, let $\rho \in R_M$ be an arbitrary permutation with infinitely many disjoint 2-cycles and infinitely many numbers not in 2-cycles, then: (conclusion of the lemma) $\rho \in G$.*

Proof. (It will be noted that the proof depends only on the existence of an M-recursive, C-infinite subset closed under ρ, A_1, which in this case we take to be the set of elements in 2-cycles.) It is possible, effectively in M, to de-

([7]) The ideas of this proof and the next are from [O(1)].

compose $\overline{A}_1$ into an infinite union of infinite M-recursive sets, which we call X, Y, A_2, A_3, $\cdots$. (When the recursion equations are written, these sets need not make an overt appearance, the equations for the M-recursive permutation ξ being produced directly. Here however, the aim is exposition and the idea, rather than the detail of the formal proof is presented.) We denote the elements of these sets, and A_1, as follows.

$$\begin{aligned} X &= \{x_1, x_2, x_3, \cdots\}, \\ Y &= \{y_1, y_2, y_3, \cdots\}, \\ A_1 &= \{a_{11}, a_{12}, a_{13}, \cdots\}, \\ A_2 &= \{a_{21}, a_{22}, a_{23}, \cdots\}, \\ &\vdots \\ A_k &= \{a_{k1}, a_{k2}, a_{k3}, \cdots\}, \\ &\vdots \end{aligned}$$

The sets $A_1, A_2, A_3, \cdots$ are all M-isomorphic and it is possible (effectively in M) to produce a sequence of M-isomorphisms, $\sigma_2, \sigma_3, \sigma_4, \cdots$; where, for all i and j,

$$\sigma_i(a_{1j}) = a_{ij}, \qquad i > 1, j \geqq 1.$$

Now, since A_1 is an M-recursive closed set for ρ, we may define an M-recursive permutation ρ_1 by:

$$\rho_1(x) = \begin{cases} \rho(x) & \text{if } x \in A_1, \\ x & \text{if } x \notin A_1. \end{cases}$$

Next, we use the permutations σ_i to "induce" permutations $\rho_2, \rho_3, \rho_4, \cdots$, on the sets $A_2, A_3, A_4, \cdots$, by conjugation; $\rho_i = \sigma_i \rho_1 \sigma_i^{-1}$. The permutation ρ_i possesses, on A_i, the same cycle structure that ρ_1 has on A_1 and is the identity on $\overline{A}_i$.

The product[8] $\xi = \rho_1\rho_2\rho_3 \cdots \rho_k \cdots$, of the infinitely many disjoint, ρ_i, is an M-recursive permutation mapping each A_i upon itself and which is the identity on $X \cup Y$. Let

$$A = Y \cup A_1 \cup A_2 \cup A_3 \cup \cdots;$$

then A is C-infinite and M-recursive. Let its elements, $w_i = f_A(i)$, be enumerated by the one-one M-recursive function f_A. Let

$$B = \{\xi(w_0), \xi(w_1), \xi(w_2), \cdots\}.$$

Then $A = B$ and both f_A and ξf_A are M-recursive, one-one functions enumerating A. By hypothesis, there is $\mu \in G$ so that, for all i, $\mu f_A(i) = \xi f_A(i)$, or, for all

(8) Of course, there is no infinite product in a permutation group. However, when the permutations involved act, as here, on disjoint sets of elements the meaning is clear.

i, $\mu(w_i)=\xi(w_i)$; and so that $\mu(X)=X$. Thus, μ is the identity on Y and may be represented

$$\mu = \beta\rho_1\rho_2\rho_3\cdots$$

where β is a permutation on X. We now define an M-recursive permutation ν, as follows:

$$\begin{aligned}
\nu(x_i) &= x_i,\\
\nu(a_{1i}) &= a_{2i},\\
\nu(a_{2i}) &= a_{3i},\\
&\vdots\\
\nu(y_{2i-1}) &= y_i,\\
\nu(y_{2i}) &= a_{1i},
\end{aligned}$$

and consider the conjugate θ of μ under ν, $\theta=\nu\mu\nu^{-1}$. Now, θ may be represented

$$\theta = \beta\rho_2\rho_3\rho_4\cdots$$

and, since G is normal, $\theta\in G$. Then $\theta^{-1}\in G$. But, $\rho_1=\mu\theta^{-1}$ and thus, $\rho_1\in G$.

To complete the proof, the roles of $\overline{A}_1$ and A_1 are reversed, to prove that the M-recursive permutation

$$\omega_1(x) = \begin{cases}\rho(x) & \text{if } x\in\overline{A}_1,\\ x & \text{if } x\in A_1\end{cases}$$

belongs to G. Then $\rho=\rho_1\omega_1\in G$ and the proof of Lemma 2.4 is complete.

LEMMA 2.5. *Let π be an arbitrary permutation of N. It is possible to express π as a product, $\pi=\pi_2\pi_1$ of two permutations recursive in π such that both π_1 and π_2 possess infinitely many disjoint two-cycles and infinitely many numbers not in two-cycles.*

Proof. While it is possible to give a direct construction which explicitly determines π_1 and π_2 simultaneously recursively in π, the following proof is much simpler and serves the present purpose. We distinguish several cases:

(i) π has infinitely many fixed points.

(ii) π has finitely many fixed points, but infinitely many 2-cycles.

(iii) π has finitely many elements of order $\leqq 2$, but infinitely many 3-cycles.

(iv) π has finitely many elements of order $\leqq 3$, and therefore infinitely many elements of order >3.

In case (i), there is an infinite π-recursive set, $P_1=\{p_1<p_2<p_3<\cdots\}$, where the p_i are the fixed points of π. Define:

$$\begin{aligned}
\pi_1 &= (p_1, p_3)(p_2)(p_4)(p_5, p_7)(p_6)(p_8)\cdots,\\
\pi_2 &= \pi_1 \text{ on } P_1.
\end{aligned}$$

For $x\notin P_1$, see comment below.

In case (ii) there is an infinite π-recursive set $P_2=\{p_1, \pi(p_1), p_2, (\pi p_2), \cdots\}$ composed of the numbers in 2-cycles, selected so, that, for all i, $p_i<\pi(p_i)$ and $p_i<p_{i+1}$. Define:

$$\pi_1 = (p_1, \pi(p_1))(p_2)(\pi(p_2))(p_3, \pi(p_3))(p_4)(\pi(p_4)) \cdots,$$
$$\pi_2 = (p_1)(\pi(p_1))(p_2, \pi(p_2))(p_3)(\pi(p_3))(p_4, \pi(p_4)) \cdots.$$

In case (iii), there is an infinite π-recursive set,

$$P_3 = \{p_1, \pi(p_1), \pi^2(p_1), p_2, \pi(p_2), \pi^2(p_2), \cdots\},$$

composed of the number in 3-cycles of π, selected so that, for all i, $p_i<\pi(p_i)$, $p_i<\pi^2(p_i)$ and $p_i<p_{i+1}$. Define:

$$\pi_1 = (p_1)(\pi(p_1), \pi^2(p_1))(p_2)(\pi(p_2), \pi^2(p_2)) \cdots,$$
$$\pi_2 = (p_1, \pi(p_1))(\pi^2(p_1))(p_2, \pi(p_2))(\pi^2(p_2)) \cdots.$$

In each of the cases above, define $\pi_1=\pi$ on the complement of P_i, and π_2 =identity, on complement P_i.

In case (iv), we proceed as follows. First, we define a π-recursive set $X=\{x_0<x_1<x_2< \cdots\}$, by:

$x_0=\mu z$ (z, $\pi(z)$, $\pi^2(z)$, $\pi^3(z)$ are all distinct),

$x_k=\mu z$ ($z>x_{k-1}$, and z, $\pi(z)$, $\pi^2(z)$, $\pi^3(z)$ are all distinct, and, for no $j<k$, $-3\leqq i\leqq 3$, is $z=\pi^i(x_j)$).

Clearly, X is infinite and the infinite π-recursive sets X, $\pi(X)$, $\pi^2(X)$ and $\pi^3(X)$ are all disjoint. Let $A=X\cup\pi X\cup\pi^2X\cup\pi^3X$. For $x\in\overline{A}$, we define $\pi_1(x)=x$. For $x\in A$, we proceed as follows: For each index $2k$, define π_1 to have the following 4-cycle:

$$(x_{2k}, \pi(x_{2k}), \pi^2(x_{2k}), \pi^3(x_{2k})).$$

For each index $2k+1$, define π_1 to have the two 2-cycles:

$$(x_{2k+1}, \pi^3(x_{2k+1})), \qquad (\pi(x_{2k+1}), \pi^2(x_{2k+1})).$$

This completely defines π_1 to be recursive in π.

We now let $\pi_2=\pi\pi_1^{-1}$. It is immediate that π_1 has the properties of the lemma, and to see that π_2 also has, we note that, for x_{2k}, π_2 has the 1-cycles:

$$(\pi(x_{2k})), \quad (\pi^2(x_{2k})), \quad (\pi^3(x_{2k}))$$

and, for x_{2k+1}, the cycles:

$$(\pi^2(x_{2k+1})), \qquad (\pi(x_{2k+1}), \pi^3(x_{2k+1})).$$

This completes the proof of Lemma 2.5.

Returning now to the proof of Theorem 2.1, let G be a normal subgroup of R_M, containing an infinite permutation. By Lemmas 2.2, 2.3 and 2.4, G also contains every member of R_M which possesses a C-infinite closed set of natural numbers. By Lemma 2.5 any member $\pi\in R_M$ can be expressed as

the product $\pi_2\pi_1$, of two other members of R_M, each of which possesses a C-infinite closed set (the set of numbers in 2-cycles). Thus $G=R_M$, and Theorem 2.1 is proved. The following corollaries are immediate consequences of the fact that F is maximal normal in R_M. Similar results hold for the group S_∞, but are not specifically noted in [SU(1) or O(1)].

COROLLARY 2.6. *Any recursive permutation (more generally, recursive in M) can be represented as a finite product of recursive cycles (recursive in M).*

Proof. The subgroup of R generated by the cycles is a normal subgroup containing an infinite permutation. Hence, it is all of R. A similar remark yields:

COROLLARY 2.7. *For any $n\geqq 2$, any recursive permutation (generally, recursive in M) can be represented as a finite product of recursive permutations (recursive in M) of order n.*

3. **The group A_r.** The group A_r has been defined in the introduction. The discussion of this section could be phrased more generally; it is applicable in particular to the group of hyperarithmetical permutations (defined analogously to A_r), and to any group A_{r_M}, of permutations arithmetical in an arbitrary set, M.

THEOREM 3.1. *Two members, π_1 and π_2 of A_r are conjugate if and only if they have the same cycle structure.*

Proof. The proof of this theorem is straightforward but somewhat tedious. We describe the idea, and the details can easily be supplied. From known facts about the arithmetical hierarchy, there is an arithmetical set, M, such that both π_1 and π_2 are recursive in M. The plan of the proof is to define a permutation, σ, arithmetical in M, which carries cycles of π_1 onto cycles of π_2, preserving algebraic order. This will establish sufficiency; necessity is immediate.

From Lemma 1.0, there are choice-sets, Σ_1 and Σ_2 for π_1 and π_2 respectively, arithmetical in M. It is straightforward to construct a 1-1 partial function, ϕ, arithmetical in M, mapping Σ_1 onto Σ_2, and preserving algebraic order. It is also straightforward to construct functions, arithmetical in M, "identifying," for any x, the elements $y_1(x)$ and $y_2(x)$, of the respective choice-sets Σ_1 and Σ_2, belonging to the same π_1 (respectively π_2) cycle to which x belongs. In the same way, the "predecessor (respectively successor) number" of x relative to $y_1(x)$ and $y_2(x)$ can be given by functions arithmetical in M. (The π_1-successor number for x is the least k so that $\pi_1^{-k}(x)=y_1(x)$, etc.) In terms of these arithmetical functions (in M), the permutation σ can be explicitly defined, to carry each x into an appropriate predecessor (respectively successor) of $\phi(y_1(x))$. The resulting permutation, σ, will be arithmetical in M and hence a member of A_r.

Using the result of Theorem 3.1, it would be possible to prove the com-

position series result for A_r (Theorem 3.2) in a manner quite analogous to that used in [SU(1)]. However, here the result follows almost immediately from Theorem 2.1.

THEOREM 3.2. *Let G be a normal subgroup of A_r, containing an infinite permutation, π. Then $G=A_r$.*

Proof. A_r is the union of groups R_{M_i}, $A_r=\bigcup_{i=0}^{\infty} R_{M_i}$, where $M_0=\varnothing$ and $M_i=M_{i-1}'$ (where the prime denotes the "jump" operation of the arithmetical hierarchy). We note that, for all i, $R_{M_i}\supset R_{M_{i-1}}$. Now, $\pi\in R_{M_i}$ for some least i, say $i=m$.

$G\cap R_{M_m}$ is normal in R_{M_m}. Thus, by Theorem 2.1, $G\cap R_{M_m}=R_{M_m}$. Moreover, $G\cap R_{M_i}=R_{M_i}$ for all $i\geqq m$, since $\pi\in R_{M_i}$ for all $i\geqq m$. Thus, for all $i\geqq m$, $G\supseteq R_{M_i}$. Then $G\supseteq\bigcup_{i=0}^{\infty} R_{M_i}\supseteq A_r$. Since $A_r\supseteq G$, we have $A_r=G$, and Theorem 3.2 is proved.

COROLLARY 3.3. *$A_r\supset F\supset A\supset\{\epsilon\}$ is the unique composition series for A_r.*

Proof. By Theorem 3.2.

We note, in concluding this section, that corollaries similar to 2.6 and 2.7 can be added here, stating that any arithmetical permutation (hyperarithmetical permutation) can be expressed as a product of a finite number of arithmetical (hyperarithmetical) cycles, or as a finite product of arithmetical (hyperarithmetical) permutations of order n, for any $n\geqq 2$.

4. **Automorphism groups.** In [SU(2)], Schreier and Ulam prove that S_∞ and its group of automorphisms are isomorphic. Since the center of S_∞ (and of the groups of this paper) can easily be shown trivial, this follows from the result that any automorphism of S_∞ is an inner automorphism. In this section, we extend this latter result to a wide family of subgroups of S_∞, including all discussed in this paper. Interestingly, the proof in this case seems to require the normal subgroup result, Theorem 2.1, specifically Corollary 2.7, while the proof of the aforementioned result for S_∞ is independent of the corresponding normal subgroup result for S_∞. The proof we give here is, in detail, identical to the proof in [SU(2)], except for the last two parts. We repeat their proof for completeness.

Let a subgroup, G, of S_∞ be called *effectively closed*, if the set of permutations recursive in elements of G is contained in G. All of the groups R, R_M, A_r, of this paper are effectively closed.

THEOREM 4.1. *Let G be a subgroup of S_∞ having the following two properties:*

(a) *G is effectively closed;*

(b) *$G\supset F$, $G\neq F$ and for any normal subgroup $G'\leqq G$, containing an infinite permutation, it is true that $G'=G$.*

Let ψ be an automorphism of G. Then there is $\sigma\in G$ so that, for all $\tau\in G$,

$$\psi(\tau)=\sigma\tau\sigma^{-1}.$$

The statement of the theorem can be shortened to: any effectively closed subgroup of S_∞, having the normal subgroup property (b) is isomorphic to its automorphism group.

Proof. We first note that, if ψ is an automorphism of G, τ an arbitrary member of G and M_1 and M_2 arbitrary subsets of G, then

(i) $\psi(\tau)$ has the same algebraic order as τ.

(ii) If $\psi(M_1)\subseteq M_2$ and $\psi^{-1}(M_2)\subseteq M_1$, then $\psi(M_1)=M_2$.

(iii) If C is a conjugacy class of G, then $\psi(C)$ is a conjugacy class of G.

Following [SU(2)], we define C^* to be the conjugacy class of the transposition (1, 2) in G. We shall show that C^* is the unique conjugacy class, C, of elements of order 2, in G with property (α).

(α) If $\sigma_1, \sigma_2, \tau_1, \tau_2\in C$ and the products $\sigma_1\tau_1$ and $\sigma_2\tau_2$ are both elements of order 2, then $\sigma_1\tau_1$ and $\sigma_2\tau_2$ are conjugate.

Certainly C^* is a conjugacy class with property (α). If C is another conjugacy class of elements of order 2 in G, then the following possibilities must be considered for the disjoint cycle factorization of an element η of C.

(1) η has finitely many ($\geqq 2$) transpositions,

(2) η has finitely many fixed points (possibly none),

(3) η has infinitely many fixed points and infinitely many transpositions.

Corresponding to these various cases we must show how to pick $\sigma_1, \sigma_2, \tau_1, \tau_2\in C$ to violate (α).

(1) $\sigma_1=(1, 2)(3, 4)\cdots(2n-1, 2n)$; $\tau_1=(2n+1, 2n+2)\cdots(4n-1, 4n)$; $\sigma_2=\sigma_1$; $\tau_2=(1, 2)(2n+1, 2n+2)\cdots(4n-3, 4n-2)$

(2) The case given is for no fixed points. An obvious modification works when any finite number of fixed points is assumed.

$\sigma_1 = (2, 3)(1, 4)(6, 7)(5, 8)\cdots$; $\tau_1 = (1, 3)(2, 4)(5, 7)(6, 8)\cdots$;
$\sigma_2 = (2, 3)(1, 4)(5, 6)(7, 8)\cdots$; $\tau_2=(1, 3)(2, 4)(5, 6)(7, 8)\cdots$.

(3) $\sigma_1=(1, 2)(5, 6)(9, 10)\cdots$; $\tau_1=(3, 4)(7, 8)(11, 12)\cdots$; $\sigma_2=\sigma_1$; $\tau_2=(5, 6)(9, 10)(13, 14)\cdots$.

Now, property (α), as a property of conjugacy classes, is preserved under automorphism and, since by (iii) $\psi(C^*)$ is some conjugacy class of elements of order 2 (by (i)), $\psi(C^*)=C^*$. Following [SU(2)], consider the set $T_n = \{(n, x)\,|\,x\in N\}$ of all transpositions (n, x) as x runs through the set of all natural numbers, N. By noting that the product of any two elements of T_n is of order 3 and that, when the product of two transpositions is of order 3 they contain precisely one common element, we easily show, using (ii), that $\psi(T_n)=T_m$ for some $m\in N$.

The mapping $\psi(T_n)=T_m$ induces a map $\sigma: N\to N$; $\sigma(n)=m$, which is easily shown to be a permutation. Thus $\sigma\in S_\infty$ and we shall ultimately show $\sigma\in G$, using the effective closure of G.

We define, as in [SU(2)], the isomorphism of G,

$$\Phi(\tau) = \sigma^{-1}\psi(\tau)\sigma.$$

It is immediate from the definition of σ that $\Phi(\tau)$ is the identity for any transposition τ. Exactly as in [SU(2)] we show that Φ is the identity for any element τ, of G, of order 2. For completeness we repeat the argument.

Suppose $\Phi(\tau)=\eta\neq\tau$, for an element $\tau\in G$ of order 2. Then there is a natural number $x_1\in N$ so that $\eta(x_1)=x_2\neq\tau(x_1)$. Let ω be the transposition (x_1, x_2). Then $\omega\eta$ is of order $\leqq 2$, while $\omega\tau$ is of higher order. This is a contradiction, by (i), for

$$\Phi(\omega\tau) = \Phi(\omega)\Phi(\tau) = \omega\eta.$$

Thus, Φ is the identity for every element of order 2 in G. At this point, in the proof of [SU(2)], it is immediate that Φ is the identity on all of S_∞, for it is easy to see how to decompose any member of S_∞ into a product of two others, each having order 2. In the present case, a corresponding result follows from hypothesis (b) for G. If (b) holds, then there are infinite permutations in G, and any normal subgroup of G, containing one such must be all of G. Thus, as in Corollary 2.7, the subgroup generated by elements of order 2 is all of G. Then, any element of G is a finite product of elements of order 2 in G, and thus Φ is the identity on G.

It follows that $\psi(\tau)=\sigma\tau\sigma^{-1}$ for all $\tau\in G$. We now use the effective closure of G to argue that $\sigma\in G$. Let τ be the recursive permutation (hence recursive in every element of G).

$$\tau = (\cdots, 7, 5, 3, 1, 2, 4, 6, \cdots),$$
$$\sigma\tau\sigma^{-1} = (\cdots, \sigma(7), \sigma(5), \sigma(3), \sigma(1), \sigma(2), \sigma(4), \sigma(6), \cdots)$$

is a member of G, since ψ is an automorphism of G. But, it is clear that a set of recursion equations for σ can be written in terms of $\sigma\tau\sigma^{-1}$, and hence, σ is recursive in an element of G. Thus, by effective closure, $\sigma\in G$. The proof of 4.1 is now complete.

COROLLARY 4.2. *Every automorphism of any of the groups R_M, or A_r, is an inner automorphism.*

REFERENCES

K(1). S. Kleene, *Introduction to metamathematics*, Van Nostrand 1952.

M(1) J. Myhill, *Recursive digraphs, splinters and cylinders*, Math. Ann. **138** (1959), 211–218.

U(1). J. S. Ullian *Splinters and recursive functions*. J. Symb. Logic **25** (1960), 33–38.

O(1) L. Onofri, *Teoria delle sostituzioni che operano su una infinità numerabile di elementi*, Ann. Mat. Ser. (4) **4** (1927), 73–106; **5** (1928), 147–168; **7** (1930), 103–130.

R(1) H. Rogers, *Computing degrees of unsolvability*, Math. Ann. **138** (1959), 125–140.

SU(1). J. Schreier and S. Ulam, *Über die Permutationsgruppe der natürlichen Zahlenfolge*, Studia Math. **4** (1933), 134–141.

SU(2). ———, *Über die Automorphismen der Permutationsgruppe der natürlichen Zahlenfolge*, Fund. Math. **28**(1937), 258–260.

OPERATIONS EVALUATION GROUP, NAVY DEPARTMENT,
WASHINGTON, D. C.