ON THE COMMUTATIVITY OF A CORRESPONDENCE AND A PERMUTATION

MILO W. WEAVER

Foreword. A permutation is a one-to-one mapping of a finite set *onto* itself. The necessary and sufficient conditions for two permutations S_1 and S_2 to satisfy

$$s_1 s_2 \cong s_2 s_1 \tag{0.1}$$

are known[1]: S_1 and S_2 satisfy (0.1) if and only if S_2 is a product PQ of a permutation P which is a product of powers of cycles of S_1 and a permutation Q which permutes cycles of S_1 with equal numbers of symbols. For example if $S_1 \cong (1\,2\,3\,4)(5\,6\,7\,8)$, $P \cong (1\,3)(2\,4)$, and $Q \cong (1\,5)(2\,6)(3\,7)(4\,8)$, then PQ commutes with S_1. A correspondence is a mapping of a finite set *into* itself. Hence a permutation is a special case of a correspondence. It is our major object in this paper to find the necessary and sufficient conditions for a permutation to commute with a correspondence. These conditions are stated in Theorem 3.15 below.

As the literature[2] has very little on "correspondences," all the fundamental definitions needed in this paper and pertaining to correspondences are given.

It is assumed that the reader knows a little about groups of permutations.

1. Fundamental definitions.[3] A *correspondence* relates each symbol of a finite set $\mathfrak{N}$ to exactly one symbol of $\mathfrak{N}$. A permutation is a correspondence such that each image symbol is the image of exactly one symbol of $\mathfrak{N}$. The statement, *m is the image of n under the corre-*

Received April 27, 1959. The work on this paper was done under National Science Foundation Grant 8238. The writer wishes to express his appreciation to his 1958 University of Texas class, and particularly to Robert R. Bunten, for suggestions concerning terminology and explanations. He also wishes to thank the referee for a valuable suggestion relating to the definition at the beginning of Section 3.

[1] Burnside, *Theory of Groups of Finite Order*, Cambridge University Press, 1897, pp. 215, 216.

[2] Two papers on correspondences are: R. R. Stoll, "Representations of Finite Simple Semigroups," *Duke Math J.*, vol. 11, no. 2 (1944), 251–265; Milo Weaver, "On the Imbedding of a Finite Commutative Semigroup of Idempotents in a Uniquely Factorable Semigroup, "*Proc. Nat. Acad. Sci.*, vol. 42, no. 10 (1956), 772–775.

[3] Most of the definitions in this section and Theorem 1.5 were given: H. S. Vandiver and M. W. Weaver, " A Development of Associative Algebra and an Algebraic Theory of Numbers, III," *Math. Mag.*, vol. 29 (1956), 135–149.

spondence D is abbreviated $nD = m$.

The notation for a correspondence D:

$$\begin{pmatrix} a_1 a_2 & & a_r \\ & \cdots & \\ b_1 b_2 & & b_r \end{pmatrix} \tag{1.1}$$

is interpreted: "the a's are distinct symbols of $\mathfrak{N}$ and $a_i D = b_i$, $i = 1, 2, \cdots, r$." If $n \in \mathfrak{N}$ and $nD = n$ and $xD = n$ has no solution x, $x \neq n$, $x \in \mathfrak{N}$, n may be omitted from both lines of (1.1). The single-lined notation for a *cycle* C:

$$(d_1 d_2 \cdots d_s) \tag{1.2}$$

means that the d's are distinct symbols of $\mathfrak{N}$, $d_i C = d_{i+1}$, $i = 1, 2, \cdots, s-1$, but $d_s C = d_1$; and that $nC = n$ if $n \in \mathfrak{N}$ and n is not one of the d's. If $s = 1$, (1.2) becomes (d_1) and means that this cycle is the *identity* permutation, E, defined by $nE = n$, for each n of $\mathfrak{N}$. The example $\binom{1\,2\,3}{2\,3\,3}$ suggests that some correspondence cannot be described either by (1.2) or by a "product" of cycles. We describe the particular correspondence D' by the notation

$$(d_1 d_2 \cdots d_s\} \tag{1.3}$$

and interpret this exactly as we did (1.2), except here $s > 1$ and $d_s D' = d_s$. A correspondence of the type (1.3) is called a 1-1-*excycle*, or just a 1-excycle.

The correspondences D_1 and D_2 are said to be *equivalent* if $nD_1 = nD_2$, for each $n \in \mathfrak{N}$. We describe this by $D_1 \cong D_2$.

The *product* $D_3 \cong D_1 D_2$ is defined by $nD_3 = (nD_1)D_2 = nD_1 D_2$ for each $n \in \mathfrak{N}$. We illustrate: if $P \cong \binom{1\,2\,3\,4\,5\,6\,7\,8\,9}{2\,3\,3\,2\,6\,3\,6\,9\,8}$ and $S \cong \binom{1\,4\,5\,7\,2\,6\,8\,9}{5\,7\,4\,1\,6\,2\,9\,8}$ then

$$\begin{aligned} PS \cong SP &\cong (3)\,(1\;2\;3\}\,(4\;2\}\,(5\;6\;3\}\,(7\;6\}\,(8\;9) \cdot (1\;5\;4\;7)\,(8\;9)\,(2\;6) \\ &\cong (3)\,(1\;6\;3\}\,(4\;6\}\,(5\;2\;3\}\,(7\;2\}\ . \end{aligned} \tag{1.4}$$

Positive integral exponents will be interpreted exactly as in permutation theory. If it is convenient, $m \in \mathfrak{N}$, and A is a correspondence, mA^0 may be used to denote m. Only non-negative exponents will be used for correspondences which are not permutations.

In (1.3) above, the set of d's are elements of a set called $\mathfrak{J}(D')$; d_1 is the only element of a set called $\mathscr{E}(D')$; and d_s is the only element of a set called $\mathfrak{K}(D')$. These sets get their notations, respectively, from the words: *involved*, *end*, and *core*, spelled *k-o-r-e*. We now define these sets, formally.

If D is a correspondence, the set $\mathfrak{J}(D)$ is defined by $i \in \mathfrak{J}(D)$ if and only if $i \in N$ and either $iD \neq i$ or $xD = i$ has a solution x, $x \in \mathfrak{N}$,

$x \neq i$. If $i \in \mathfrak{J}(D)$, we notice that $iD^r \in \mathfrak{J}(D)$ also, for each positive integer r.

The set $\mathscr{E}(D)$ is defined by $j \in \mathscr{E}(D)$ if and only if $xD = j$, $j \in \mathfrak{N}$, has no solution x, $x \in \mathfrak{N}$. Clearly, $jD \neq j$ and $\mathscr{E}(D) \subseteq \mathfrak{J}(D)$.

The set $\mathfrak{K}(D)$ is defined by $k \in \mathfrak{K}(D)$ if and only if $k \in \mathfrak{J}(D)$ and $kD^s = k$ for some non-negative integer s. We note that D acts either as a cycle or as a product of cycles on $\mathfrak{K}(D)$. If $k \in \mathfrak{K}(D)$, $kD^r \in \mathfrak{K}(D)$ also, for each positive integer r. The d's of (1.3) exemplify the fact that it is not necessarily true that $\mathfrak{K}(D) \cup \mathscr{E}(D) = \mathfrak{J}(D)$.

Let D be a correspondence and $k \in \mathfrak{K}(D)$. If each symbol of $\mathfrak{K}(D)$ is one of the symbols $k, kD, kD^2, \cdots$, then D is called an *excycle*. Apparently, if $i \in \mathfrak{J}(D)$, there exists a non-negative integer r such that $iD^r \in \mathfrak{K}(D)$. If D is an excycle and $\mathscr{E}(D)$ and $\mathfrak{K}(D)$ contain exactly r and s symbols, respectively, then D is called an *r-s-excycle*. This explains the term, 1-1-*excycle*. A 0-s-excycle is a cycle with s symbols. The product PS of (1.4) is a 4-1-excycle.

THEOREM 1.5 (known). *Each correspondence is either an excycle or a product of excycles with disjoint $\mathfrak{J}$-sets.*

The proof is not given here as it is very similar to that for the well-known theorem: *Each permutation, not a cycle, is a product of cycles with disjoint $\mathfrak{J}$-sets.* The excycles (*cycles*) of Theorem 1.5 are called *excycles* (*cycles*) *of the given correspondence.* The excycles of P of (1.4) are $(3)(1\,2\,3\}\,(4\,2\}\,(5\,6\,3\}\,(7\,6\}$ and $(8\,9)$.

If $j \in \mathscr{E}(D)$, clearly, for some u and v, the operation of D on a subset of $\mathfrak{J}(D)$ is described by $D_j \cong (jD^v\, jD^{v+1} \cdots jD^u)\,(j\; jD \cdots jD^v\}$. We call D_j a 1-$(u-v+1)$-*subexcycle of D* determined by j and the first factor of D_j a *subcycle* of D. D_j may also be called simply a 1-subexcycle.

2. Some properties of a correspondence and a permutation which commute.

We next make three simple remarks about commutativity of correspondences. The usual proofs of the corresponding remarks about permutations are valid here.

The identity E commutes with each correspondence.

If L is a correspondence, then $L^aL^b \cong L^bL^a$.

If L and M are correspondences and $\mathfrak{J}(L) \cap \mathfrak{J}(M) = 0$, then $LM \cong ML$.

The relation (1.4) illustrates Theorem 2.1 and Theorem 2.4 below.

THEOREM 2.1. *If S is a permutation on $\mathfrak{N}$ and P is a correspondence, not a substitution on $\mathfrak{N}$ such that $SP \cong PS$, then S maps $\mathfrak{J}(P)$ onto itself* and *$\mathscr{E}(P)$ onto itself.*

Suppose that the hypothesis of the theorem is satisfied and that $n \in \mathfrak{J}(P)$, but that $nS \notin \mathfrak{J}(P)$. Then if $nP = m$, we have

$$nS = nSP = nPS = mS \ . \tag{2.2}$$

Whence $m = n$. Since $n \in \mathfrak{J}(P)$ and $nP = n$, there exists an a, $a \in \mathfrak{J}(P)$ such that $aP = n \neq a$. And since $nS \notin \mathfrak{J}(P)$, it follows from the equation

$$aSP = aPS = nS \tag{2.3}$$

that $aS = nS$ and $a = n$, a contradiction to $a \neq n$. Hence $nS \in \mathfrak{J}(P)$, and since S is a permutation S maps $\mathfrak{J}(P)$ onto itself. Also if we assume $n \in \mathscr{E}(P)$ and $nP = m$ in (2.2), the conclusion $nP = n$ contradicts the hypothesis, $n \in \mathscr{E}(P)$. Whence S maps $\mathscr{E}(P)$ onto itself.

The following is also a theorem, but we shall not prove it as it is not needed in this paper.

THEOREM 2.4. *If P is a correspondence with $j \in \mathscr{E}(P)$ and P_j is a 1-$(u - v + 1)$-subexcycle of P, determined by j, and if S is a permutation such that $SP \cong PS$ and $jS^bP^m = jP^n$, for $b > 0$, $m \leq u$, $n \leq u$, and either $m < v$ or $n < v$, then $m = n$.*

3. **Products of cycles which permute 1-(u − v + 1)-excycles.** We shall first generalize the idea of a permution permuting cyclically a set of cycles of equal numbers of symbols. Let u, v, and t be any integers such that $u \geq v > 0$ and $t \geq 1$, and $F_0, F_1, \cdots, F_t$ be 1-$(u - v + 1)$-excycles whose $\mathscr{E}$-symobols are, respectively, the distinct symbols, $j_0, j_1, \cdots, j_t$ such that if c is an integer, $0 < c < u$, and d is the least nonnegative residue of the positive integer e, $e \leq t$, modulo $t_c + 1$, with $t_c + 1$, defined below, then

$$j_eF_e^c = j_dF_d^c \ . \tag{3.1}$$

Let $C_0, C_1, \cdots, C_u$ be cycles of a permutation S such that

$$C_i \cong (j_0F_0^i \ j_1F_1^i \cdots j_{t_i}F_{t_i}^i), \tag{3.2}$$

with $t_0 = t$ and the order $t_w + 1$ of C_w dividing that $t_z + 1$ of C_z whenever $0 \leq z \leq w \leq u$. Then S is said to *permute cyclically* the 1-excycles $F_0, F_1, \cdots F_t$.

We give examples here. The permutation (1 4) (2 5) (3 6) permutes cyclically each of the pairs: (2 3) (1 2}, (5 6) (4 5}; (1 2 3}, (4 5 6}; (1 2 3 7}, (4 5 6 7}. Also (1 4 6 7) (2 5) permutes cyclically the set (1 2 3}, (4 5 3}, (6 2 3}, (7 5 3}; and (5 6) (1 3) (2 4) permutes cyclically the set (1 2 3 4) (5 1}, (3 4 1 2) (6 3}. The reader should study each of these examples and refer to them, frequently, while studying the rest of this paper.

We shall use the above terminology for the F's and C's, hereafter.

LEMMA 3.3. *If $C_x \cong E$ and $0 \leq x \leq y \leq u$, then $C_y \cong E$, also.*

This is true, since $t_y + 1$ divides $t_x + 1$.

Let r be the largest integer x such that $x \leq u$ and $C_x \not\cong E$. We impose the added restriction on r, that it be the smallest integer x such that C_i, $i = 0, 1, \cdots, x$ gives all the distinct C_i's.

THEOREM 3.4. *Let P be a correspondence and R be a permutation such that:*

(i) $\mathfrak{J}(P) \supseteq \mathfrak{J}(R)$.

(ii) *R is a product of the distinct cycles of a set of permutations, each of which permutes cyclically 1-subexcycles of P.*

(iii) *If F is a 1-subexcycle of P, then $\mathfrak{J}(F) \cap \mathfrak{J}(R) = 0$, unless F is one of a set permuted cyclically by R.*
Then

$$RP \cong PR \ . \tag{3.5}$$

If $n \notin \mathfrak{J}(R)$, then neither is nP, by (iii); and

$$nPR = nP = nRP \ . \tag{3.6}$$

If $n \in \mathfrak{J}(P)$. Let $n \in \mathfrak{J}(\prod_{i=1}^{r} C_i)$, where $\prod_{i=1}^{r} C_i$ permutes cyclically the 1-subexcycles $F_l, l = 0, 1, \cdots, t$; further let $n \in \mathfrak{J}(C_q)$ and $n = j_p F_p^q$, for $0 \leq q \leq r$, and $j_p \in \mathscr{E}(P)$. Then from (3.2), for $0 \leq p \leq t_q$,

$$\begin{aligned} nPR &= nP\Big(\prod_{i=1}^{r} C_i\Big) = j_p F_p^{q+1} C_{q+1} = j_{p+1} F_{p+1}^{q+1} \\ &= j_{p+1} F_{q+1}^{q} F_{p+1} = j_p F_p^q \Big(\prod_{i=1}^{r} C_i\Big) P = n\Big(\prod_{i=1}^{r} C_i\Big) P = nRP \ ; \end{aligned} \tag{3.7}$$

while if $p = t_q$, both the leftmost and rightmost members of (3.7) yield $j_0 E_0^{q+1}$. Hence, by (3.6) and (3.7), we have (3.5).

THEOREM 3.8. *Let P be a correspondence and S be a permutation such that $SP \cong PS$, with $j \in \mathscr{E}(P)$ and $jP^s \in \mathfrak{J}(S)$ for some non-negative s; further let $t+1$ be the least positive integer such that $jS^{t+1} = j$ and F_l, $l = 0, 1, \cdots, t$ be the 1-subexcycle of P whose $\mathscr{E}$-symbol is jS^l. Then S permutes the set $F_0, F_1, \cdots, F_t$ cyclically.*

Let g be the largest value, if there is one, of x such that $jP^x \in \mathfrak{J}(S)$, with $0 \leq x \leq u$, $u + 1$ the order of the subexcycle P_j, and $u - v + 1$ the order of its subcycle. Let $C_i, i = 0, 1, \cdots, g$ be the cycle of S, possibly the identity, such that

$$C_i \cong (jP^i \, jP^iS \ jP^iS^2 \cdots jP^iS^{t_i}) \tag{3.9}$$

for some non-negative integer t_i. Certainly $t = t_0$. The order of C_i is

$t_i + 1$. By Theorem 2.1, $jP^tS^l \in \mathfrak{J}(P)$ and $jS^l \in \mathscr{E}(P)$, for $i \leq g$, $0 \leq l \leq t_i$. Since S is a permutation, we have cancellation by S^l and both equations in each of the pairs of equations hold simultaneously:

$$(3.10) \qquad \begin{array}{ll} jP^{u_0+1} = j^{v_0}\,, & jS^lP^{u_0+1} = jS^lP^{v_0} \\ jP^{u_l+1} = jP^{v_l}\,, & jS^lP^{u_l+1} = jS^lP^{v_l}\,. \end{array}$$

Hence, $u_l = u_0$ and $v_l = v_0$. We notice that for $0 \leq z \leq w \leq g$, and $h + z = w$, we have

$$(3.11) \qquad jP^w = jP^zS^{t_z+1}P^h = jP^{z+h}S^{t_z+1} = jP^wS^{t_z+1}\,.$$

Therefore, since $t_w + 1$ is the order of C_w, it follows from group theory that $t_w + 1$ divides $t_z + 1$. Also if $e \equiv d (\text{mod } t_c + 1)$, we have $e = m(t_c + 1) + d$, m a non-negative integer and

$$(3.12) \qquad jS^eF_e^c = jS^{m(t_c+1)+d}P^c = jP^cS^d = jS^dP^c = jS^dF_d^c\,,$$

which gives (3.1), since here $j_e = jS^e$ and $j_d = jS^d$. Hence S permutes the F's cyclically.

Let S be a permutation and P be a correspondence, which is not a permutation. Clearly, P is expressible in the form

$$(3.13) \qquad P \cong T_1T_2\,,$$

where either $T_1 \cong E$ or T_1 is a product of cycles of P, and T_2 is product of those excycles of P which are not cycles. And S is expressible in the form

$$(3.14) \qquad S \cong S_1S_2\,,$$

where S_1 is either a product of those cycles C of S such that $I(C) \cap I(T_2) = 0$ or $S_1 \cong E$, depending on whether or not such C's exist, and S_2 is either a product of those cycles D of S such that $\mathfrak{J}(D) \cap I(T_2) \neq 0$ or $S_2 \cong E$, depending on whether or not such D's exist.

THEOREM 3.15. *If S is a permutation and P is a correspondence, not a permutation, and S_1, S_2, T_1, and T_2 satisfy* (3.13) *and* (3.14), *then $SP \cong PS$ if and only if*:

(*i*) $S_1T_1 \cong T_1S_1$;

(*ii*) *Whenever $j \in \mathscr{E}(T_2)$ such that for some non-negative integer s, $jP^s \in \mathfrak{J}(S)$, then S_2 permutes cyclically the set of* 1-*excycles of T_2 whose $\mathscr{E}$-symbols are the distinct symbols obtained by applying all powers of S to j.*

Suppose that $PS \cong SP$. By Theorem 3.8, if $j \in \mathscr{E}(P)$ and $jP^s \in \mathfrak{J}(S)$, a product π defined as in (3.2) of cycles of S permutes cyclically a set of 1-subexcycles of P, and therefore of T_2, having powers of S applied to j as their $\mathscr{E}$-symbols. By (3.2) $I(\pi)$ is contained in the union of the $\mathfrak{J}$-sets of the subexcycles which it permutes. Clearly, S_2 is a product of the distinct cycles of all such π's, or $S_2 \cong E$, depending on whether or not such π's exist, and S_2 satisfies (ii) of Theorem 3.15. From (3.13) and (3.14)

$$\mathfrak{J}(T_1) \cap \mathfrak{J}(T_2) = \mathfrak{J}(S_1) \cap \mathfrak{J}(T_2) = 0 . \tag{3.16}$$

Since $\mathfrak{J}(S_2) \subseteq \mathfrak{J}(T_2)$, we have

$$\mathfrak{J}(T_1) \cap \mathfrak{J}(S_2) = 0 . \tag{3.17}$$

Hence $\mathfrak{J}(T_1) \cup \mathfrak{J}(S_1) \cap \mathfrak{J}(T_2) \cup \mathfrak{J}(S_2) = 0$, and S_1T_1 and T_1S_1 operate on $\mathfrak{J}(S_1) \cup \mathfrak{J}(T_1)$ exactly as ST and TS do; and for $n \notin \mathfrak{J}(T_1) \cup \mathfrak{J}(S_1)$, $nS_1T_1 = nT_1S_1 = n$. Whence $S_1T_1 \cong T_1S_1$, and (i) is satisfied. Now assume that (i) and (ii) of Theorem 3.15 are satisfied by S and P. From Theorem 3.4, we have $S_2T_2 \cong T_2S_2$. By (i), $S_1T_1 \cong T_1S_1$. From (3.16) and (3.17), $S_1T_2 \cong T_2S_1$, $T_1T_2 \cong T_2T_1$, and $S_2T_1 \cong T_1S_2$. Hence

$$SP \cong S_1S_2T_1T_2 \cong S_1T_1S_2T_2 \cong T_1S_1T_2S_2 \cong T_1T_2S_1S_2 \cong PS . \tag{3.18}$$

This completes the proof of Theorem 3.15 which was the major objective of this paper.

The necessary and sufficient conditions for (i) to hold were stated in the foreword. In each of the examples below (3.2), if S is taken to be the permutation and P to be the correspondence whose 1-subexcycles are permuted by S, then S and P obey (i) and (ii) of Theorem 3.15. A more complicated example of such a P and S is: $P \cong (4)\,(1\;2\;3\}\,(2\;3\}\,(8)\,(5\;7\;8\}\,(6\;7\}$, $S \cong (1\;5)\,(2\;6)\,(3\;7)\,(4\;8)$. On the other hand if $S \cong (1\;4\;6)\,(2\;5)$ and $P \cong (1\;2\;3\}\,(4\;5\;3\}\,(6\;5\}$, then $SP \not\cong PS$, since the order of $(2\;5)$ fails to divide that of $(1\;4\;6)$ and S_2 fails to permute cyclically the 1-1-subexcycles $(1\;2\;3\}$, $(4\;5\;3\}$, and $(6\;5\;3\}$ of P.