SOME REMARKS ON COMMUTATORS

OYSTEIN ORE

In a group the product of two commutators need not be a commutator, consequently the commutator group of a given group cannot be defined as the set of all commutators, but only as the group generated by these. There seems to exist very little in the way of criteria or investigations on the question when all elements of the commutator group are commutators. In the following it is shown that in the finite symmetric group Σ_n all elements of the alternating group are commutators; one can extend this and show that when $n \geqq 5$ all elements in the alternating group are commutators of elements in A_n. For the infinite symmetric group the situation is different since we obtain: *Any one-to-one correspondence of an infinite set to itself is a commutator.*

1. We shall begin by making a few general remarks which apply both to the finite and the infinite cases. Any one-to-one correspondence T of an arbitrary set S to itself can be written uniquely as a product of cycles which operate on disjoint sets of elements

$$(1) \qquad\qquad T = \prod C_n.$$

These cycles may be finite of the type $C_n = (1, 2, \cdots, n)$ or infinite of the type

$$(2) \qquad\qquad C_\infty = (\cdots, -2, -1, 0, 1, 2, \cdots).$$

One *transforms* T by another correspondence U

$$T' = UTU^{-1}$$

by performing the substitutions of U in each of the cycles of T. Thus two such correspondences T and T' are *transforms* or *similar* if and only if they have *conformal cyclic decompositions* (1), that is, there exists a one-to-one correspondence between their cycles for each order $n = 1, 2, \cdots, \infty$.

Since one obtains the inverse of a correspondence by reversing the order in a cycle, T and T^{-1} are conformal. Furthermore, a commutator has the form

$$K = A \cdot BA^{-1}B^{-1}$$

so that we arrive at the following criterion which we shall use in the following

---

307

LEMMA. *A correspondence T is a commutator if and only if it can be written as a product*

$$(3) \qquad\qquad T = V \cdot V'$$

of two conformal correspondences V and V'.

We shall also need the observation that if K_1 and K_2 are two commutators

$$K_1 = A_1 B_1 A_1^{-1} B_1^{-1}, \qquad K_2 = A_2 B_2 A_2^{-1} B_2^{-1}$$

where A_1 and B_1 commute with A_2 and B_2, then the product

$$K_1 K_2 = K_2 K_1 = (A_1 A_2)(B_1 B_2)(A_1 A_2)^{-1}(B_1 B_2)^{-1}$$

is a commutator, and similarly for an arbitrary number of factors. This remark makes it possible to find commutators equal to certain parts of a product (1) in the elements which these cycles involve and combine them to a commutator representation for T.

Let us also remark that any one-to-one correspondence T of the set S to itself may be regarded as such a correspondence for sets $S' > S$, obtained by adding to the cyclic expansion (1) the single element cycles $C_1 = (a')$ for the elements a' in $S' - S$.

2. For the symmetric group Σ_n of a finite set of n elements the alternating group A_n is the commutator group and in this instance we can show:

THEOREM 1. *Every element in the alternating group A_n is a commutator of Σ_n.*

PROOF. Let T be a permutation in A_n. Its cyclic decomposition (1) may contain cycles of odd order and an even number of cycles of even order. Our theorem follows, therefore, if one can show that every cycle of odd order and every pair of cycles of even order are commutators in the elements they involve.

For a cycle of odd order

$$(4) \qquad\qquad C_{2i+1} = (1, 2, \cdots, 2i + 1)$$

one has the representation

$$(5) \qquad C_{2i+1} = (1, 2, \cdots, i + 1)(i + 1, i + 2, \cdots, 2i + 1)$$

in the form (3) of the lemma, namely, as the product of cycles of order $i+1$. [All products of permutations are executed from right to left in the following.]

Next let

(6) $\mathcal{C}_{2i} = (1, 2, \cdots, 2i), \qquad D_{2j} = (2i + 1, \cdots, 2i + 2j)$

be a pair of even order cycles where we suppose that $j \geqq i$. Then one can write

(7)
$$\mathcal{C}_{2i}D_{2j} = (1, 2, \cdots, 2i, 2i + 1, \cdots, i + j + 1)$$
$$\cdot (2i, i + j + 1, i + j + 2, \cdots, 2i + 2j)$$

and we have again a representation (3) as the product of two cycles of order $i+j+1$.

3. Let us now turn to the infinite symmetric group Σ_S of some set S. It is clear that there exist one-to-one correspondences T of S to itself, which are commutators and actually involve all elements in S, for instance, the elements in S may be paired into transpositions with T as their product. Since the commutator group is normal it follows from a theorem of R. Baer (Studia Mathematica vol. 5 (1934) pp. 15–17) on the infinite symmetric group that Σ_S *is its own commutator group when S is infinite.*

An essential new element in the infinite case is the occurrence of the infinite cycles (2). We shall now show:

THEOREM 2. *Every infinite cycle is a commutator in the elements it involves.*

PROOF. It is clear that it suffices to show the existence of a single infinite cycle which is a commutator in its elements. The subsequent construction may appear relatively complicated, but I have been unable to find any simpler procedure.

An infinite cycle involves a denumerable set of elements and for our purposes it is advantageous to represent them by two-way indices

(8) a_{ij}, $i = 0, \pm 1, \pm 2, \cdots ; j = 0, 1, 2, \cdots ,$

which is also a denumerable set. In this notation we construct the infinite set of infinite cycles

$$A_j = (\cdots, a_{-1,j}, a_{0,j}, a_{1,j}, \cdots), \qquad j = 0, 1, 2, \cdots ,$$

without common elements; their product shall be denoted by

(9) $$A = \prod_{j=0}^{\infty} A_j.$$

When the elements (8) are interpreted as lattice points in the upper half of the coordinate plane the correspondence (9) has the effect of moving each element one step to the right on the lines parallel to the x-axis.

Our second correspondence is also an infinite product of infinite cycles

$$(10) \qquad\qquad B = \prod_{i=1}^{\infty} B_i$$

where the cycles B_i are defined as follows:

$$B_1 = (\ \cdots\ , a_{-1,2},\ a_{-1,1},\ a_{-1,0},\ a_{1,0},\ a_{1,1},\ a_{1,2},\ \cdots\ ),$$

$$B_2 = (\ \cdots\ , a_{-2,2},\ a_{-2,1},\ a_{-2,0},\ a_{0,0},\ a_{2,0},\ a_{2,1},\ a_{2,2},\ \cdots\ ),$$

and in general

$$B_i = (\ \cdots\ , a_{-i,2},\ a_{-i,1},\ a_{-i,0},\ a_{0,i-2},\ a_{i,0},\ a_{i,1},\ a_{i,2},\ \cdots\ ).$$

One can describe B_i geometrically: Under it, each lattice point in the $-i$th column moves one step downward and when one reaches the x-axis it jumps to the point $a_{0,i-2}$ on the y-axis and from there to the zero-point in the ith column on which it moves upward again. The cycle B_1 is slightly irregular since it contains no lattice point on the y-axis.

From these constructions it is clear that both A and B are one-to-one correspondences of S to itself leaving no element fixed. Furthermore, the cyclic product decompositions (9) and (10) show that they are conformal. According to the lemma the product

$$(11) \qquad\qquad C = BA^{-1}$$

is therefore a commutator and the proof of Theorem 2 follows from the fact that C is actually an infinite cycle involving all elements (8). We leave it to the reader to verify that C is the cycle

$$C = (\ \cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad ,$$

$$a_{0,4},\ a_{-1,3},\ a_{-2,2},\ a_{-3,1},\ a_{-4,0},$$

$$a_{0,3},\ a_{-1,2},\ a_{-2,1},\ a_{-3,0},$$

$$a_{0,2},\ a_{-1,1},\ a_{-2,0},$$

$$a_{0,1},\ a_{-1,0},$$

$$a_{0,0},$$

$$a_{1,0},$$

$$a_{2,0},\ a_{1,1},$$

$$a_{3,0},\ a_{2,1},\ a_{1,2},$$

$$\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad).$$

(12)

As one sees, $\mathcal{C}$ represents a diagonal progress through the lattice points of the two quadrants.

4. Before we can give a proof of the main theorem on infinite correspondences we shall need a few other auxiliary results. The first of these is the following theorem.

THEOREM 3. *A product of two cycles without common elements is a commutator, provided one of the cycles is infinite.*

PROOF. When both cycles are infinite the statement is a direct consequence of the lemma. To produce a product of an infinite cycle and a finite cycle of arbitrary length a we notice that we need only multiply the cycle (2) by the transposition $(0, a)$ since

$$(13) \qquad \mathcal{C}_\infty(0, a) = (\ \cdots, \ -1, 0, a+1, a+2, \cdots\ ) \cdot (1, 2, \cdots, a).$$

We shall therefore multiply the cycle $\mathcal{C}$ in (12) on the right by some transposition

$$(14) \qquad\qquad X = (a_{i,j}, a_{k,l}).$$

To obtain a product $\mathcal{C} \cdot X$ conformal with (13) we can even choose $a_{i,j}$ and $a_{k,l}$ in the same line in (12), provided this line is taken so high up that its length exceeds a.

When (11) is multiplied by X the result is

$$(15) \qquad\qquad \mathcal{C} \cdot X = B \cdot (XA)^{-1}.$$

According to our selection of the two elements $a_{i,j}$ and $a_{k,l}$ in (14) the multiplication XA will affect only two of the infinite cycles in A, namely, A_j and A_l. But one verifies that

$$XA_j A_l = (\ \cdots, \ a_{i-2,j}, a_{i-1,j}, a_{k,l}, a_{k+1,l}, \cdots\ )$$
$$\cdot (\ \cdots, \ a_{k-2,l}, a_{k-1,l}, a_{i,j}, a_{i+1,j}, \cdots\ )$$

so that this product is again a product of two infinite cycles. Therefore, XA is conformal to A and to B, and from (15) we conclude, by means of the lemma, that $\mathcal{C} \cdot X$ and therefore (13) is a commutator.

Next we show:

THEOREM 4. *A correspondence is a commutator when its cyclic decomposition is an infinite sequence of cycles of finite orders greater than or equal to 2.*

PROOF. Let

$$(16) \qquad P = \cdots (a_1, \cdots, a_{i_1})(b_1, \cdots, b_{i_2})(c_1, \cdots, c_{i_3}) \cdots$$

be the given correspondence. If there should be an infinite number of
cycles of even order these may be arranged in pairs which are com-
mutators in the elements they involve. The cycles of odd orders are
already commutators in their elements so that P becomes a com-
mutator. Hence we can assume that there are only a finite number of
cycles of even order, in particular, there shall be only a finite number
of transpositions in (16).

We now multiply (16) on the right by

$$(17) \quad A = (\,\cdots\,,\, a_1,\, a_{i_1},\, b_1,\, b_{i_2},\, c_1,\, c_{i_3},\, \cdots\,)\,\cdots\,(a_2)\,\cdots\,(b_2)\,\cdots\,.$$

According to the remark just made, A in (17) consists of one infinite
cycle and a denumerable set of fixed elements. For the product

$$B = PA$$

one finds the expression

$$B = (\,\cdots\,,\, a_2,\, a_3,\, \cdots\,,\, a_{i_1},\, b_2,\, \cdots\,,\, b_{i_2},\, c_2,\, \cdots\,,\, c_{i_3},\, \cdots\,)$$
$$\cdots\,(a_1)(b_1)(c_1)\,\cdots$$

which is also an infinite cycle and a denumerable set of fixed points.
We conclude that A and B are conformal and according to the lemma
P is a commutator.

Somewhat surprising at first sight is the following fact.

THEOREM 5. *Every finite permutation in an infinite set is a com-
mutator.*

PROOF. It is evident that this is not true within the finite set of
elements involved in the permutation; however, the construction can
always be performed within a denumerable set. Let us first take the
given permutation to be a single finite cycle

$$P = (a_1,\, a_2,\, \cdots\,,\, a_i).$$

In the basic set S we select two disjoint infinite sequences

$$S_a = \{\,\cdots\,,\, a_{-2},\, a_{-1},\, a_0,\, a_1,\, \cdots\,,\, a_i,\, a_{i+1},\, \cdots\,\}, \qquad S_b = \{b_1,\, b_2,\, \cdots\,\}.$$

Within the set $S_a + S_b$ we form two correspondences, namely first

$$\mathcal{C}_a = (\,\cdots\,,\, a_{-2},\, a_{-1},\, a_0,\, a_1,\, \cdots\,,\, a_i,\, a_{i+1},\, \cdots\,)(b_1)(b_2)\,\cdots$$

consisting of a single cycle in the elements in S_a and having the ele-
ments in S_b as fixed points and secondly

$$\mathcal{C}_a' = (\,\cdots\,,\, a_{i+2},\, a_{i+1},\, a_1,\, a_0,\, a_{-1},\, \cdots\,)(a_2)\,\cdots\,(a_i)(b_1)(b_2)\,\cdots\,.$$

These two correspondences are clearly conformal and since

$$P = \mathcal{C}'_a \mathcal{C}_a$$

it is a commutator.

When the permutation is a product of a finite number of cycles

$$P = \mathcal{C}_{i_1} \mathcal{C}_{i_2}, \cdots, \mathcal{C}_{i_r}$$

we select $2r$ disjoint sequences $S_a^{(t)}$ and $S_b^{(t)}$ from S and proceed in the same manner for each cycle.

We are now in a position to prove the main theorem.

THEOREM 6. *Any one-to-one correspondence of an infinite set to itself is a commutator.*

PROOF. As before let (1) be the cyclic decomposition of the correspondence T which we want to examine. If there exists an infinite number or an even number of cycles of even order these may be paired and a corresponding commutator may be constructed in these elements according to the preceding. The infinite cycles and the cycles of odd orders are already commutators in their elements so that T itself becomes a commutator.

We may therefore assume that the number of cycles of even order is finite and odd. If there is some cycle of infinite order one of the cycles of even order may be combined with it to give a commutator according to Theorem 3; again we conclude that T itself is a commutator. When one has no infinite cycles but an infinite number of finite cycles, these may be arranged in infinite sequences as in Theorem 4 and T is a commutator. This leaves us finally with the finite permutations and these are taken care of by Theorem 5.

5. A more thorough investigation whose details we shall omit here makes it possible to establish the stronger form of Theorem 1.

THEOREM 7. *When $n \geq 5$ every element in the alternating group A_n is a commutator of elements in A_n.*

It is possible that a similar theorem holds for any simple group of finite order, but it seems that at present we do not have the necessary methods to investigate the question.

[In the previously mentioned paper by Baer all normal subgroups of the group Σ of all one-to-one correspondences of an infinite set S to itself are determined. They form a composition chain

$$1 < A_0 < \Sigma_0 < \cdots < \Sigma_{\aleph} < \cdots < \Sigma$$

where A_0 is the group of all finite, even permutations, Σ_0 the group of all finite permutations and for each cardinal number $\aleph$ the group $\Sigma_\aleph$ consists of all correspondences involving at most $\aleph$ elements. The preceding considerations are sufficient (as pointed out by the referee) to show that each of them consists only of its own commutators with the obvious exception of Σ_0 whose commutators form A_0.]

YALE UNIVERSITY

NOTE ON A LEMMA OF A. W. GOODMAN

E.G.-RODEJA F.

In a recent and interesting paper on p-valent functions by A. W. Goodman we find the following lemma.[1]

LEMMA 1. *For all integers $n \geq k \geq 1$*

$$(1) \qquad \sum_{m=k}^{n} \frac{(-1)^{m+k} 2nk}{(m+k)!(m-k)!} \prod_{\alpha=1}^{m-1} (n^2 - \alpha^2) = \delta_n^k,$$

and for all integers $n > k \geq 1, \beta \geq 1$,

$$(2) \qquad \sum_{m=k}^{n} (-1)^m \prod_{\alpha=1}^{m-1} (n^\beta - \alpha^\beta) \prod_{\alpha=m+1}^{n} (\alpha^\beta - k^\beta) = 0.$$

Here the empty product is unity by definition.

The identity (1), which is the first half of the lemma, has been used in the said paper, while (2) is stated only as a generalization of (1).

In this note we intend to establish the identities (13) and (14) (where F_n and G_n are arbitrary functions of the natural number n), including the afore mentioned as particular cases; and for their demonstration we shall follow a method in part similar to the one used in the paper quoted.

Let $A_n^{(m)}$ be a function of the natural numbers n and m satisfying the conditions (a) $A_n^{(m)} = 0$ if $n < m$, (b) $A_n^{(m)} = 1$ if $n = m$.

$H(p, k, n)$ is defined by