GENERAL PRODUCTS OF TWO FINITE CYCLIC GROUPS

by K. R. YACOUB

Groups that can be represented as the product of two proper subgroups have been studied extensively ; one of the latest contributions is a paper by Wielandt (8), in which references to previous work can be found. In the case where the two proper subgroups have only the unit element in common, we adopt the term " general product " introduced by Neumann (1).

A group G is, then, the general product of its subgroups A and B if

$$G = AB, \quad A \cap B = \{e\},$$

where e denotes the unit element of G.

If A and B are given groups, it is natural to ask for a survey over all the groups that can be represented as general products of subgroups isomorphic to A and B, respectively. This " extension problem " was first studied by Zappa (2).

The case of two cyclic groups has attracted attention. Rédei (3) has determined the structure of the general product of two cyclic groups in the cases in which one is finite and the other infinite or both are infinite, but subject to certain restrictions. General products of two finite cyclic groups have been investigated by Douglas (4–7). He is concerned with the properties of permutations that can be associated with such a general product. These permutations, which we shall call Douglas special permutations, are closely connected with, but conceptually distinct from, " semi-special " permutations which will be studied in the present paper and which are not, by their definition, associated with a general product. We shall give here a general method of constructing semi-special permutations. In subsequent papers we shall apply our results to the special cases of cyclic groups whose orders are primes, squares of primes, cubes of primes, products of two primes, and others.

§ 1. DEFINITIONS AND GENERAL THEOREMS

Definition. A group G is said to be the general product of its subgroups A and B if

$$G = AB, \quad A \cap B = \{e\}.$$

From this definition it follows that every element of G can be expressed, in one and only one way, in the form ab where $a \in A$ and $b \in B$. Similarly every element of G can be expressed, in one and only one way, as the product of an element of B by an element of A. Hence there exist, corresponding to given elements a of A and b of B, uniquely determined elements a' of A and b' of B such that $ab = b'a'$.

Since each of the elements a' and b' depends on both a and b, we write

$$a' = a_b, \quad b' = b_a, \quad ab = b_a a_b.$$

We state without proof the following theorems.

1.1. *Theorem.* Let A and B be two groups and G be a general product of A and B. Then to every element b of B there corresponds a permutation $\begin{pmatrix} a \\ a_b \end{pmatrix}$ of the elements of A, and to

every element a of A there corresponds a permutation $\begin{pmatrix} b \\ b_a \end{pmatrix}$ of the elements, of B, such that

$$(aa')_b = a_{b_{a'}} a'_b, \quad \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\text{(I)}$$
$$(bb')_a = b_a b'_{a_b}, \quad \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\text{(II)}$$
$$(a_b)_{b'} = a_{bb'}, \quad \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\text{(III)}$$
$$(b_a)_{a'} = b_{a'a}, \quad \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\text{(IV)}$$

where $a' \in A$ and $b' \in B$.

These four relations will be called the " Fundamental Relations " of the general product G. They were first obtained by Zappa (2), and are consequences of the associative property in G.

1.2. *Corollary*. The Fundamental Relations (I–IV) imply the following relations :

$$\left.\begin{array}{ll} e_b = e, & e_a = e \\ a_e = a, & b_e = b \end{array}\right\} , \quad \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\text{(V)}$$

These relations are obtained by taking $a' = e$ and $b' = e$, in turn, in the Fundamental Relations.

1.3. *Theorem*. Let A and B be two given groups, and suppose that to each element b of B there corresponds a permutation $\begin{pmatrix} a \\ a_b \end{pmatrix}$ of the elements of A, and to each element a of A a permutation $\begin{pmatrix} b \\ b_a \end{pmatrix}$ of the elements of B such that the Fundamental Relations of Theorem 1.1 are satisfied. Then there exists a group G which is the general product of two groups $\overline{A}$ and $\overline{B}$ isomorphic to A and B, respectively, in such a way that if $\overline{a}$, $\overline{a}_b$, and $\overline{b}$, $\overline{b}_a$ denote the elements corresponding to a, a_b and b, b_a in the isomorphism of A and $\overline{A}$ and of B and $\overline{B}$, then

$$\overline{a}\,\overline{b} = \overline{b}_a\,\overline{a}_b.$$

1.4. *Theorem*. With the notation of the previous theorem, if H is some general product of groups isomorphic to A and B which leads to the same permutations $\begin{pmatrix} a \\ a_b \end{pmatrix}$ and $\begin{pmatrix} b \\ b_a \end{pmatrix}$ as does G, then G is isomorphic to H.

1.5. *Conclusion*. From the above theorems we see that the problem of determining all general products of two groups A and B is reduced to that of determining all possible permutations $\begin{pmatrix} a \\ a_b \end{pmatrix}$ and $\begin{pmatrix} b \\ b_a \end{pmatrix}$ such that

$$(aa')_b = a_{b_{a'}} a'_b, \quad (bb')_a = b_a b'_{a_b},$$
$$(a_b)_{b'} = a_{bb'}, \qquad (b_a)_{a'} = b_{a'a}.$$

§ 2. The Case of Two Finite Cyclic Groups

In the particular case where the groups A and B are both cyclic and finite, let $A = \{a\}$ be of order m and $B = \{b\}$ be of order n.

If G is a general product of A and B, then in G we have

$$ab^x = b_a^x a_{b^x}.$$

Evidently b_a^x is an element of $\{b\}$ which depends on x and can therefore be written as $b^{\pi x}$. Thus

$$b_a^x = b^{\pi x}, \quad ab^x = b^{\pi x} a_{b^x}. \quad \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\text{(2.1)}$$

Dual relations to (2.1) are

$$a_b^y = a^{\rho \nu}, \quad a^\nu b = b_{a^\nu} a^{\rho \nu}. \quad \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots(2.2)$$

From (2.1) and (2.2) we deduce

$$a^\nu b^x = b^{\pi^\nu x} a^{\rho^x \nu}.$$

By Theorem 1.1 we see that $x \to \pi x$ is a permutation of the numbers $1, 2, \dots, n$ and that $y \to \rho y$ is a permutation of the numbers $1, 2, \dots, m$. Relations (V) of Corollary 1.2 imply the following relations

$$\rho m \equiv m \pmod{m}, \quad \pi n \equiv n \pmod{n},$$
$$\rho^n y \equiv y \pmod{m}, \quad \pi^m x \equiv x \pmod{n}.$$

Now by the Fundamental Relation (II) we have

$$b^{\pi(x+u)} = (b^{x+u})_a = (b^u b^x)_a = b_a^u b_{a_{bu}}^x.$$

Putting $a_{bu} = a'$ and $b_{a'}^x = b^{\pi'x}$, we have

$$b^{\pi(x+u)} = b^{\pi u} b^{\pi'x} \ ;$$

thus $\pi(x+u) \equiv \pi u + \pi'x \pmod{n}$,

or $\pi'x \equiv \pi(x+u) - \pi u \pmod{n}$.

It is clear that $x \to \pi'x$ is a permutation of the numbers $1, 2, \dots, n$. Moreover since a' is a power of a, π' is a power of π. We observe that π' depends on the choice of u; we thus have a condition for every u. For simplicity we denote $\pi(x+u) - \pi u$ by $\pi_u x$ and the induced permutation by π_u. Thus

$$\pi_u x \equiv \pi(x+u) - \pi u \pmod{n}.$$

We have thus shown the following

2.3. *Lemma.* π_u is a power of π for every u.

In what follows we adopt the Douglas notation $[n]$ for the range n, which is the set of integers $1, 2, \dots, n$.

Definition. A permutation π defined on $[n]$ is called a " Douglas special permutation " if it is induced by one of the generators of a general product of two cyclic groups, that is, if it is defined by

$$ab^x = b^{\pi x} a_{b^x}.$$

Definition. A permutation π defined on $[n]$ is called a " semi-special permutation " if $\pi n \equiv n$ and if the permutation π_u defined by

$$\pi_u x \equiv \pi(x+u) - \pi u \pmod{n},$$

is a power of π for every u.

An obvious example of a semi-special permutation is the identical permutation which is usually denoted by ι.

Necessary and sufficient conditions for a permutation to be a Douglas special permutation were given by Douglas (**4**).

Lemma 2.3 shows that Douglas special permutations are semi-special. Conversely, it can be shown * that every semi-special permutation is Douglas special, but we shall not make use of this result. Instead we shall derive results for semi-special permutations because it is easier to check up whether a given permutation is semi-special than whether it is Douglas special.

* B. H. Neumann (unpublished).

§ 3. Some Properties of Semi-Special Permutations

In this paragraph we use the symbol π to denote a semi-special permutation defined on $[n]$ and k to denote the order of π. Congruences with no modulus stated are to be understood modulo n.

3.1. *Lemma.* If $\pi 1 \equiv 1$, then $\pi = \iota$.

Proof. Since π is semi-special, π_y is a power of π for every y; and $\pi 1 \equiv 1$. Therefore $\pi_y 1 \equiv 1$. But $\pi(y+1) - \pi y \equiv \pi_y 1 \equiv 1$; thus $\pi(y+1) \equiv 1 + \pi y$ for all y. Moreover $\pi 1 \equiv 1$. The lemma follows by induction.

3.2. *Lemma.* If $\pi_u = \iota$ for some u, then $\pi = \iota$.

Proof. By hypothesis we have

$$x \equiv \pi(x + u) - \pi u.$$

Taking $x + u = n$ and observing that $\pi n \equiv n$, we get $\pi u \equiv u$; thus

$$x \equiv \pi(x + u) - u, \quad \text{or} \quad \pi(x + u) \equiv x + u.$$

The result follows at once if we here replace $x + u$ by x.

3.3 *Lemma.* $(\pi^r)_u$ is a power of π for all r and u.

Proof. The lemma is true for $r = 1$ and for all u; this is obvious, because π is semi-special. We complete the proof by induction over r. Assume that the lemma is true for $r = s$, i.e., assume that $(\pi^s)_u x = \pi^{\tau(s, u)} x$, say. Then

$$(\pi^{s+1})_u x \equiv \pi^{s+1}(x+u) - \pi^{s+1} u \equiv \pi(\pi^s(x+u)) - \pi(\pi^s u) \equiv \pi_{\pi^s u}(\pi^s(x+u) - \pi^s u) \equiv \pi_{\pi^s u}((\pi^s)_u x),$$

i.e., $$(\pi^{s+1})_u x \equiv \pi_{\pi^s u}(\pi^{\tau(s, u)} x),$$

and the right-hand side is a power of π, since π is semi-special. The lemma now follows by induction.

We shall denote $(\pi^r)_u$ by $\pi^{\tau(r, u)}$, where $\tau(r, u)$ is determined modulo k, the order of π.

3.4. *Lemma.* With the above notation

$$\tau(r, u+v) \equiv \tau(\tau(r, u), v) \pmod{k}, \quad \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots(3.5)$$
$$\tau(r+s, u) \equiv \tau(r, \pi^s u) + \tau(s, u) \pmod{k}. \quad \dots\dots\dots\dots\dots\dots\dots(3.6)$$

Proof. For the first formulae, we have

$$\pi^{\tau(r, u+v)} x \equiv (\pi^r)_{u+v} x \equiv \pi^r(x + u + v) - \pi^r(u + v)$$
$$\equiv \pi^r(x + u + v) - \pi^r u + \pi^r u - \pi^r(u + v)$$
$$\equiv (\pi^r)_u(x + v) - (\pi^r)_u v = ((\pi^r)_u)_v x$$
$$\equiv (\pi^{\tau(r, u)})_v x.$$

Thus $$\tau(r, u+v) \equiv \tau(\tau(r, u), v) \pmod{k}.$$

For the second formulae, we have

$$\pi^{\tau(r+s, u)} x \equiv (\pi^{r+s})_u x \equiv \pi^{r+s}(x + u) - \pi^{r+s} u$$
$$\equiv \pi^r(\pi^s(x + u)) - \pi^r(\pi^s u)$$
$$\equiv \pi^r_{\pi^s u}((\pi^s)_u x) \equiv \pi^{\tau(r, \pi^s u)}(\pi^{\tau(s, u)} x).$$

Thus $$\tau(r+s, u) \equiv \tau(r, \pi^s u) + \tau(s, u) \pmod{k}.$$

3.7. *Lemma.* With the same notation

(i) if $\tau(r, u) \equiv \tau(r, v) \pmod{k}$, then

$$\tau(r, v - u) \equiv r \pmod{k}; \quad \dots\dots\dots\dots\dots\dots\dots\dots\dots(3.8)$$

(ii) if $\tau(r, u) \equiv r \pmod{k}$, then for all y and z

$$\tau(r, uy + z) \equiv \tau(r, z) \pmod{k}. \quad \dots\dots\dots\dots\dots\dots\dots\dots(3.9)$$

Proof. If $\tau(r, u) \equiv \tau(r, v) \pmod{k}$, then

$$\pi^r(x + u) - \pi^r u \equiv \pi^r(x + v) - \pi^r v \quad \text{for all } x.$$

Thus

$$\pi^r(x + u) \equiv \pi^r(x + u + v - u) - \pi^r(v - u) + \pi^r(v - u) + \pi^r u - \pi^r v,$$

i.e.,

$$\pi^r(x + u) \equiv (\pi^r)_{v-u}(x + u) + \pi^r(v - u) + \pi^r u - \pi^r v.$$

For $x + u = n$, we have

$$0 \equiv 0 + \pi^r(v - u) + \pi^r u - \pi^r v ;$$

thus

$$\pi^r(x + u) \equiv (\pi^r)_{v-u}(x + u) \equiv \pi^{\tau(r, v-u)}(x + u).$$

Hence $\tau(r, v - u) \equiv r \pmod{k}$.

Next if $\tau(r, u) \equiv r \pmod{k}$, then from (3.5) we deduce

$$\tau(r, uy + z) \equiv \tau(\tau(r, u), u(y - 1) + z) \pmod{k}$$
$$\equiv \tau(r, u(y - 1) + z) \pmod{k}$$

and (3.9) will follow by repeated application of (3.5).

3.10. *Lemma.* Let u be any number in the range $[n]$ and let h be the length of the cycle of π which contains u. Then with the previous notation

$$h \mid \tau(h, u), \quad \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots(3.11)$$
$$\pi^h yu \equiv yu \quad \text{for all } y. \quad \dots\dots\dots\dots\dots\dots\dots\dots(3.12)$$

Proof. $\pi^h u \equiv u$ by hypothesis ; hence, from (3.6),

$$\tau(r + h, u) \equiv \tau(r, \pi^h u) + \tau(h, u) \pmod{k}$$
$$\equiv \tau(r, u) + \tau(h, u) \pmod{k}.$$

By induction over multiples of h, we get

$$\tau(xh, u) \equiv x\tau(h, u) \pmod{k}.$$

Moreover k is a multiple of h, say $k = dh$; also $\tau(k, u) \equiv 0 \pmod{k}$.

Hence

$$0 \equiv \tau(dh, u) = d\tau(h, u) \pmod{k}.$$

Hence h divides $\tau(h, u)$.

If $\tau(h, u) = th$, say, then

$$\pi^h(x + u) - \pi^h u \equiv \pi^{th} x ;$$

but $\pi^h u \equiv u$ by hypothesis and hence

$$\pi^h(x + u) \equiv \pi^{th} x + u.$$

(3.12) now follows by induction over multiples of u, if we remark that $\pi^{th} u \equiv u$.

3.13. *Lemma.* Let u and v be any numbers in the range $[n]$ which belong to the same cycle of π. If h is the length of this cycle, then for all x and y

$$\pi^h(x + yw) \equiv \pi^h x + yw,$$

where $w \equiv v - u$.

Proof. From (3.6) we have

$$\tau(r + 1, u) \equiv \tau(r, \pi u) + \tau(1, u) \pmod{k}$$
$$\equiv \tau(r - 1, \pi^2 u) + \tau(1, \pi u) + \tau(1, u) \pmod{k}.$$

Repeated application of (3.6) gives

$$\tau(r+1, u) \equiv \sum_{i=0}^{r} \tau(1, \pi^i u) \quad (\text{mod } k).$$

If $h(x)$ denotes the length of the cycle containing the number x, then $h(u) = h(v) = h$ by hypothesis. Moreover, u and v belong to the same cycle of π; thus $v \equiv \pi^j u$ for some j, and $u, \pi u, \pi^2 u, \ldots, \pi^{h(u)-1} u$ is a permutation of the numbers $v, \pi v, \pi^2 v, \ldots, \pi^{h(v)-1} v$. Thus

$$\tau(h(v), v) \equiv \sum_{i=0}^{h(v)-1} \tau(1, \pi^i v) \quad (\text{mod } k)$$
$$\equiv \sum_{i=0}^{h(u)-1} \tau(1, \pi^i u) \equiv \tau(h(u), u) \quad (\text{mod } k),$$

i.e.,
$$\tau(h, v) \equiv \tau(h, u) \quad (\text{mod } k).$$

Hence
$$\pi^h(x+v) - \pi^h v \equiv \pi^h(x+u) - \pi^h u;$$

but $\pi^h u \equiv u$, $\pi^h v \equiv v$ and thus

$$\pi^h(x+v) - \pi^h(x+u) \equiv v - u.$$

Putting $v - u \equiv w$ and replacing x by $x - u$, we have

$$\pi^h(x+w) \equiv \pi^h x + w.$$

By induction over multiples of w, we get

$$\pi^h(x+yw) \equiv \pi^h x + yw.$$

§4. FURTHER PROPERTIES AND LINEAR PERMUTATIONS

Definition. If a permutation is written as the product of disjoint cycles, the cycle which contains the number 1 is called the principal cycle.

Definition. The permutation π defined on $[n]$ by

$$\pi x \equiv rx \quad (\text{mod } n), \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots(4.1)$$

where r is some integer prime to n, is called a linear permutation.

It should be noted that (4.1) defines a permutation if and only if r is prime to n. The order of π is equal to the order of r modulo n, that is to say, it is the least positive number k such that $r^k \equiv 1 \pmod{n}$.

4.2. *Lemma.* If π is semi-special, then its order is equal to the length of its principal cycle. If k is the order of π and $[n]$ is the range on which π is defined, then $k \leqslant n - 1$.

Proof. If h is the length of the principal cycle, then it follows from (3.12) that $\pi^h y \equiv y$ for all y. The first part of the lemma follows. The second part becomes obvious if we remark that $\pi n \equiv n$.

4.3. *Theorem.* If π is a semi-special permutation on $[n]$, where $n > 2$, the permutations $\pi_1, \pi_2, \ldots, \pi_{n-1}$ are not all different.

Proof. $\pi_1, \pi_2, \ldots, \pi_{n-1}$ are all powers of π. If $\pi = \iota$ then they are all equal; if $\pi \neq \iota$, then by Lemma 3.2 none of them equals ι. But by Lemma 4.2 π has at most $n - 2$ different powers other than ι. The theorem follows.

4.4. *Theorem.* Let π be a permutation (which we need here not assume semi-special). If $\pi_u = \pi$ for some number u, then for all y and z

$$\pi y u \equiv y \pi u, \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots(4.5)$$
$$\pi_{yu+z} = \pi_z, \quad \pi_{yu} = \pi. \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots(4.6)$$

1

Proof.   By hypothesis we have

$$\pi(x+u) - \pi u \equiv \pi x,$$

i.e., $$\pi(x+u) \equiv \pi x + \pi u. \quad\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots(4.7)$$

Then (4.5) follows directly from (4.7), by induction over multiples of u.

Next, to show (4.6), we have on using (4.7),

$$\pi_{u+z}x \equiv \pi(x+u+z) - \pi(u+z) \equiv \pi(x+z) + \pi u - (\pi u + \pi z) \equiv \pi(x+z) - \pi z = \pi_z x.$$

We complete the proof of (4.6) by induction over y.   For this assume that

$$\pi_{ru+z}x \equiv \pi_z x.$$

Then $$\pi_{(r+1)u+z}x \equiv \pi(x+(r+1)u+z) - \pi((r+1)u+z)$$
$$\equiv \pi(x+ru+z) + \pi u - (\pi(ru+z)+\pi u), \quad \text{using (4.7)},$$
$$\equiv \pi(x+ru+z) - \pi(ru+z)$$
$$\equiv \pi_{ru+z}x \equiv \pi_z x, \quad \text{by assumption,}$$

and the first formula of (4.6) follows by induction.

The second formula of (4.6) is a particular case of the first one.

4.8. Corollary.   If π is semi-special on $[n]$ and if u is some divisor of n such that $\pi_u = \pi$, then $\pi u \equiv ud$, where $(ud, n) = u$.   Moreover, π permutes multiples of u among themselves.

Proof.   If $n = qu$, say, then from (4.5) we deduce that

$$\pi n \equiv \pi qu \equiv q\pi u,$$

and the first part of the corollary follows if we note that $\pi n \equiv n$.

For the second part we have

$$\pi yu \equiv y\pi u \equiv yud \quad \text{for all } y.$$

4.9. Lemma.   Let π be a semi-special permutation defined on $[n]$.   If u is some divisor of n such that $\pi_u = \pi$, then π defines modulo u a semi-special permutation ρ by $\rho x \equiv \pi x \pmod{u}$.

Proof.   By Corollary 4.8 we can write

$$\pi u \equiv ud, \quad \pi yu \equiv yud,$$

where d is some number prime to n/u.

Moreover, from (4.6) we have $\pi_{yu}x \equiv \pi x$; thus $\pi(x+yu) \equiv \pi x + yud$.   If in our previous notation $\pi_z = \pi^{\tau(1,z)}$, then $\rho_z = \rho^{\tau(1,z)}$ and therefore ρ is semi-special on $[u]$.

4.10. Theorem.   Let π be a permutation (which we need here not assume semi-special) defined on the range $[n]$.   If $\pi_u = \pi$ for some number u which is prime to n, then π is a linear permutation.

Conversely, if π is a linear permutation, then $\pi_u = \pi$ for every u ; therefore a linear permutation is semi-special.

Proof.   Since u is prime to n, there exist two integers i and j such that $iu + jn = 1$; thus $\pi_1 = \pi_{iu}$.   Moreover, since $\pi_u = \pi$, $\pi_{iu} = \pi$ by using (4.6), and hence $\pi_1 = \pi$.

If $\pi 1 \equiv r$, then by induction one can show that $\pi x \equiv rx$; also r must be prime to n and π is linear.

The converse of the theorem is obvious.

4.11. Corollary.   If π is semi-special and $\pi^2 = \iota$, then π is linear.

For π_1, being a power of π, is either ι or π.   If $\pi_1 = \iota$, then $\pi = \iota$ by Lemma 3.2 and there-fore π is linear ; if $\pi_1 = \pi$, then π is linear by the above theorem.

4.12. Theorem. Let $n > 2$; then to every semi-special permutation defined on $[n]$ there exists an integer r which divides n such that

$$1 \leqslant r < n \quad \text{and} \quad \pi_r = \pi.$$

Proof. By Theorem 4.3 we can find two integers u and v such that

$$1 \leqslant u < v < n, \quad \text{and} \quad \pi_v = \pi_u.$$

Then
$$\pi(x + v) - \pi v \equiv \pi(x + u) - \pi u,$$
i.e.,
$$\pi(x + v) - \pi(x + u) \equiv \pi v - \pi u.$$

Put $v - u \equiv w$ and replace x by $x - u$; then $1 \leqslant w < n$ and

$$\pi(x + w) - \pi x \equiv \pi v - \pi u \equiv \text{constant}.$$

The value of this constant is obtained by putting $x = n$; this gives

$$\pi(x + w) - \pi x \equiv \pi w, \quad \text{i.e.,} \quad \pi_w = \pi.$$

If $(w, n) = r$, then one can find two integers i and j such that $iw + jn = r$ and then $\pi_r = \pi_{iw}$. Moreover, as $\pi_w = \pi$, $\pi_{iw} = \pi$ by (4.6), and thus $\pi_r = \pi$. This proves the theorem.

4.13. Corollary. If p is an odd prime number, the semi-special permutations on $[p]$ are all linear.

For the r of the theorem is 1 and π is linear by Theorem 4.10.*

4.14. Theorem. Let π be a semi-special permutation defined on $[n]$. If u and v are any two numbers in this range such that (u, n) divides (v, n), then the length of the cycle containing v divides the length of the cycle containing u.

Proof. Since (u, n) divides (v, n), there exists some number y such that $v \equiv yu \pmod{n}$. If h is the length of the cycle which contains u, then, by Lemma 3.10,

$$\pi^h v \equiv \pi^h y u \equiv yu \equiv v,$$

that is to say, h is a multiple of the length of the cycle which contains v. This proves the theorem.

REFERENCES

(1) B. H. Neumann, "Decomposition of Groups", *J. London Math. Soc.*, **10** (1935), 3–6.

(2) G. Zappa, "Sulla costruzione dei gruppi prodotto di due dati sottogruppi permutabili tra loro", *Atti Secondo Congresso Un. Mat. Ital. Bologna* (1940), 119–125.

(3) L. Rédei, "Zur Theorie der faktorisierbaren Gruppen I", *Acta Math. Acad. Sci. Hungar.* **1** (1950), 74–98.

(4) J. Douglas, "On Finite Groups with Two Independent Generators", *Proc. Nat. Acad. Sci. U.S.A.*, **37** (1951), 604–610.

(5) J. Douglas, "On Finite Groups with Two Independent Generators", *Proc. Nat. Acad. Sci. U.S.A.*, **37** (1951), 677–691.

(6) J. Douglas, "On Finite Groups with Two Independent Generators. Exponential Substitutions", *Proc. Nat. Acad. Sci. U.S.A.*, **37** (1951), 749–760.

(7) J. Douglas, "On Finite Groups with Two Independent Generators. Conjugate Substitutions", *Proc. Nat. Acad. Sci. U.S.A.*, **37** (1951), 808–813.

(8) H. Wielandt, "Über das Product paarweise vertauschbarer nilpotenter Gruppen", *Math. Zeit.* **55** (1951), 1–7.

FACULTY OF SCIENCE,

UNIVERSITY OF ALEXANDRIA,

EGYPT.