On the general products of two finite cyclic groups one of which being of order p^2.

By K. R. YACOUB (Alexandria).

A group G is said to be the general product of its subgroups A and B if $G = AB$, $A \cap B = \{e\}$ where e denotes the unit element of G.[1]) From this definition it follows that every element of G can be expressed uniquely in the form ab and uniquely in the form $b'a'$ where a and a' are elements of A whilst b and b' are elements of B. Thus to every pair of elements a of A and b of B there exist unique elements a_b of A and b_a of B such that $ab = b_a a_b$.

If A and B are given groups, it is natural to ask for a survey of all the groups that can be represented as general products of subgroups isomorphic to A and B respectively. This problem was first studied by ZAPPA [3] and the general products were determined by means of permutations satisfying certain conditions. An important result due to ZAPPA is the following 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

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

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

These four relations, we have called the "Fundamental Relations" of the general product G (Cf. [4], § 1, Theorem 1. 1).

[1]) This definition was first introduced by NEUMANN [1]. Some writers (RÉDEI [2] and others) use the term "Zappa—Szép product" instead of "general product".

The case of two cyclic groups is of special interest. Rédei [2] has determined the structure of the general products of two cyclic groups in the cases in which one is finite and the other infinite or both are infinite but subject to certain conditions.

The case of two finite cyclic groups has been dealt with by Douglas [5] and [6]. His results are essentially concerned with certain permutations which we call Douglas special (Cf. § 1, Definition 4).

Later on, Huppert [7] studied succesfully the structure of all the general products of two cyclic groups which are both finite. The approach of Huppert requires however deep knowledge of group theory.

In this paper, the author considers a particular case of the problem studied by Huppert namely that when one of the groups is of order p^2, p being an odd prime. The approach of the author is completely different from that of Huppert's. In fact our approach is completely elementary and requires only a rudimentary knowledge of group theory.

§ 1. Definitions, notation and preliminary results.

Throughout this paper, we use $[n]$ to denote briefly the set of numbers $1, 2, \ldots, n$. Permutations will be written as left hand operators.

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

Definition 2. A permutation φ defined on $[n]$ by $\varphi x \equiv rx \pmod{n}$, where r is prime to n, is called a *linear permutation*.

Definition 3. A permutation φ defined on $[n]$ is called *semi-special* if $\varphi n = n$ and if, for every $y \in [n]$, the permutation

$$\varphi_y x \equiv \varphi(x+y) - \varphi y \pmod{n}$$

is again a permutation, namely a power (depending on y) of φ.

Definition 4. A permutation φ defined on $[n]$ is called *Douglas special* if it is induced by one the generators of a general product of two finite cyclic groups, that is if it is defined by $ab = b^{\varphi x} a_{b^x}$; here n denotes the order of $\{b\}$.

The following results were proved by the author in previous papers.

Lemma 1. *If φ is a linear permutation, then $\varphi_u = \varphi$ for every u; therefore a linear permutation is semi-special.*

Lemma 2. *The order of a semi-special permutation is equal to the length of its principal cycle* ([4], Lemma 4. 2).

Lemma 3. *If p is an odd prime, the non-linear semi-special permutations on $[p^2]$ can be written in the form*

$$\pi x \equiv tx + \mu p\, x(x-1) \pmod{p^2},$$

where $t\ (t \not\equiv 1 \pmod{p})$ and μ are chosen arbitrarily prime to p in such a way that $u - \mu h t^{h-1}$ is also prime to p, h being the order of t mod p and u is defined mod p by $t^h \equiv 1 + up \pmod{p^2}$ ([8], Theorem 4. 2).

If we put $t - \mu p \equiv r \pmod{p^2}$, then $r \not\equiv 1 \pmod{p}$, and

$$\pi x \equiv rx + \mu p x^2 \pmod{p^2};$$

also

$$r^h \equiv t^h - h\mu p\, t^{h-1} \equiv 1 + (u - \mu h\, t^{h-1})\, p \pmod{p^2}$$

because

$$t^h \equiv 1 + up \pmod{p^2}.$$

We have thus established the following

Lemma 4. *The semi-special permutations on $[p^2]$, where p is an odd prime are*

$$\pi x \equiv tx \pmod{p^2},$$

and

$$\pi x \equiv rx + \mu p\, x^2 \pmod{p^2},$$

where $t, r\ (r \not\equiv 1 \pmod{p})$ and μ are all prime to p and r is chosen in such a way that the u appearing in the relation $r^h \equiv 1 + up \pmod{p^2}$ (h being the order of r mod p) is prime to p.

§ 2. Description of the problem.

Let $A = \{a\}$ be a cyclic group of order m and $B = \{b\}$ be of order n and let G be a general product of A and B. Then associated with G (Cf. [4], § 2) there exist two permutations π and ϱ such that

$$ab^x = b^{\pi x} a_{b^x},\ a^y b = b_{a^y} a^{\varrho y}, \tag{1}$$

and

$$a^y b^x = b^{\pi^y x} a^{\varrho^x y}, \tag{2}$$

where π is semi-special on $[n]$ and ϱ on $[m]$. Furthermore, we have

$$\pi^m x \equiv x \pmod{n}, \qquad \varrho^n y \equiv y \pmod{m} \tag{3}$$

where $x \in [n]$ and $y \in [m]$.

Lemma 5. *With the same notation*

$$a^m b^x = b^x a^m,\ x \in [n], \tag{4}$$

$$a^y b^n = b^n a^y,\ y \in [m]. \tag{5}$$

The proof is obvious and is therefore omitted.

Retaining the above notation, we prove

Lemma 6. *Let k be the order of π. Then*

(i) *k divides m;*

(ii) *a number s, prime to $\frac{m}{k}$, exists such that*

$$a^k b = b a^{ks}, \quad ks^h \equiv k \pmod{m}, \tag{6}$$

where h is the highest common divisor of all the differences $v - u$; u and v being any numbers in the principal cycle of π;

(iii) $a^k b^h = b^h a^k$.

Proof. To prove (i), suppose on the contrary that k does not divide m and let precisely $m = kt + r$ where $0 < r < k$. Since k is the order of π, then $\pi^k 1 \equiv 1 \pmod{n}$ and thus

$$\pi^m 1 = \pi^{kt+r} 1 = \pi^r (\pi^{kt} 1) \equiv \pi^r 1 \pmod{n};$$

on the other hand $\pi^m 1 \equiv 1 \pmod{n}$, by the first of (3); thus $\pi^r 1 \equiv 1 \pmod{n}$ which by using Lemma 2 shows that r is the order of π; this contradicts the hypothesis. Hence k divides m.

Next, to prove (ii), we put $x = 1, y = k$ in (2) and remember that $\pi^k 1 \equiv 1 \pmod{n}$, so that $a^k b = b a^{\varrho k}$, thus $a^{\varrho k}$ has the same order $\frac{m}{k}$ of a^k, hence $\varrho k \equiv ks \pmod{m}$ for a suitable number s which is prime to $\frac{m}{k}$ and therefore $a^k b = b a^{ks}$, this proves the first of (6).

For the second of (6), we use the Fundamental Relation I. Let u and v be any two numbers which belong to the principal cycle of π, then by a repeated application of the Fundamental Relation I, we obtain:

$$a^k_{b^u} = \prod_{i=0}^{k-1} a_{b^{\pi^i u}}, \quad a^k_{b^v} = \prod_{i\ 0}^{k-1} a_{b^{\pi^i v}}. \tag{7}$$

Since k is the order of π, then by Lemma 2 the length of the principal cycle of π is k. Moreover, since u and v belong to the principal cycle of π, then $u, \pi u, \pi^2 u, \ldots, \pi^{k-1} u$ is a permutation of $v, \pi v, \pi^2 v, \ldots, \pi^{k-1} v$. Furthermore, since $a_{b^u}, a_{b^{\pi u}}, \ldots, a_{b^{\pi^{k-1} u}}$ are powers of a they commute; hence from (7) it would follow that

$$a^k_{b^u} = a^k_{b^v}. \tag{8}$$

Again, since $\pi^k u \equiv u \pmod{n}$ and $\pi^k v \equiv v \pmod{n}$, then by (2)

$$a^k b^u = b^u a^k_{b^u}, \quad a^k b^v = b^v a^k_{b^v}. \tag{9}$$

From (8) and (9) we deduce that

(10) $$a^k b^{v-u} = b^{v-u} a^k,$$

which by using the first of (6) gives $ks^{v-u} \equiv k \pmod{m}$; this is true for all the differences $v-u$ and therefore true for their highest common divisor h, thus $ks^h \equiv k \pmod{m}$. This completes the proof of (ii).

Lastly (iii) is an immediate consequence of (ii) and the lemma is now proved.

Now, since π is semi-special, then π_y is a power of π for every y. We prove (with the above notation) the following

Lemma 7. *If $\pi_y = \pi^{\omega(y)}$, then $a b^y = b^{\pi y} a^{k r(y) + \omega(y)}$ for a suitable number $r(y)$ which depends on y.*

PROOF. By the Fundamental Relation II, we have

$$b^{\pi(x+y)} = (b^{x+y})_a = b^x_{a_{b^y}} b^y_a = b^x_{a_{b^y}} b^{\pi y},$$

thus

(11) $$b^x_{a_{b^y}} = b^{\pi(x+y) - \pi y} = b^{\pi_y x} = b^{\pi^{\omega(y)} x}.$$

Further since a_{b^y} is a power of a (Cf. [4], § 2), let $a_{b^y} = a^Y$, say, then

(12) $$b^x_{a_{b^y}} = b^x_{a^Y} = b^{\pi^Y x}.$$

Comparing (11) and (12) we see that $Y \equiv \omega(y) \pmod{k}$, where k denotes as before the order of π and thus $Y = k r(y) + \omega(y)$ for a suitable $r(y)$ and the lemma is proved.

We turn now to our problem.

By Lemma 4, we have seen that the semi-special permutations on $[p^2]$ are $\pi x \equiv tx \pmod{p^2}$ and $\pi x \equiv rx + \mu p x^2 \pmod{p^2}$ where t, r and μ are subject to certain restrictions described in the lemma. We deal seperately with the permutation $\pi x \equiv x \pmod{p^2}$; $\pi x \equiv tx \pmod{p^2}$ where $t \not\equiv 1 \pmod{p^2}$ and finally with the permutations $\pi x \equiv rx + \mu p x^2 \pmod{p^2}$. Our aims are to (i) describe all groups in terms of some simple parameters; (ii) prove the existence of such groups for permissible parameter values and (iii) distinguish the non-isomorphic types of groups.

§ 3. The permutation $\pi x \equiv x \pmod{p^2}$.

Theorem 1. *If there is a general product G corresponding to the semi-special permutation π, then it has the defining relations*

(13) $$G = \{a, b;\ a^m = b^{p^2} = e,\ ab = ba^u\}$$

where

(14) $$u^{p^2} \equiv 1 \pmod{m}.$$

Conversely if u is any number satisfying (14), *then the group G generated by a and b with the defining relations* (13) *is the general product of $\{a\}$ and $\{b\}$ of the desired type.*

The proof is direct and is therefore omitted.

To distinguish the non-isomorphic types of groups defined in Theorem 1 we have the following

Theorem 2. *Let G and H be two groups whose defining relations are*

$$G=\{a, b;\ a^m=b^{p^2}=e,\ ab=ba^u;\ u^{p^2}\equiv 1 \pmod{m}\},$$

$$H=\{a, b;\ a^m=b^{p^2}=e,\ ab=ba^v;\ v^{p^2}\equiv 1 \pmod{m}\},$$

where $v\not\equiv u \pmod{m}$. Then a necessary and sufficient condition for G and H to be isomorphic is $v\equiv u^\lambda \pmod{m}$ for some number λ which is prime to p.

The proof of the theorem follows the same procedure used by the author in [9] (Cf. Chapter VII, Theorem 26. 4) and the proof is omitted.

§ 4. The permutation $\pi x\equiv tx \pmod{p^2}$, where $t\not\equiv 1 \pmod{p^2}$.

Since $t\not\equiv 1 \pmod{p^2}$, we may distinguish the two cases namely that (i) when $(t-1, p)=1$ and (ii) when $(t-1, p^2)=p$.

Theorem 3. *If there is a general product G corresponding to the semi-special permutation π given by $\pi x\equiv tx \pmod{p^2}$ where $(t-1, p)=1$, then G has the defining relations*

$$G=\{a, b;\ a^m=b^{p^2}=e,\ ab=b^t a\}, \tag{15}$$

where

$$t^m\equiv 1 \pmod{p^2}. \tag{16}$$

Conversely if t is any number such that t and $t-1$ are both prime to p and if m is any integer such that (16) *is satisfied, then the group G generated by a and b with the defining relations* (15) *is the general product of $\{a\}$ and $\{b\}$ of the desired type.*

PROOF. Assume the existence of the general product G. If k be the order of t mod p^2, then π is of order k and, by Lemma 6, m is a multiple of k; this confirms (16).

Furthermore the h of Lemma 6 (ii) is 1 and thus

$$a^k b=ba^k. \tag{17}$$

Next, by direct calculation $\pi_1=\pi$, hence by Lemma 7

$$ab=b^t a^{kr+1} \tag{18}$$

for a suitable r. Then by induction and by using (17), we find that

$$a b^x = b^{tx} a^{xkr+1}$$

Thus $a b^{p^2} = b^{tp^2} a^{p^2kr+1}$, which by using Lemma 5, (5) (with $y=1$ and $n=p^2$) gives at once

$$(19) \qquad p^2 kr \equiv 0 \pmod{m}.$$

We remark that (19) is satisfied by $kr \equiv 0 \pmod{m}$; in this case G has the defining relations

$$G = \{a, b;\ \ a^m = b^{p^2} = e,\ \ ab = b^t a;\ \ t^m \equiv 1 \pmod{p^2}\}.$$

If $kr \not\equiv 0 \pmod{m}$, the group which we denote now by G_r has the defining relations

$$G_r = \{a, b;\ a^m = b^{p^2} = e,\ a b = b^t a^{kr+1},\ a^k b = b a^k;\ t^m \equiv 1 \pmod{p^2}\}.$$

The groups G and G_r are however isomorphic. This is easily seen if the defining relations of G are written in the form[2])

$$G = \{c, d;\ \ c^m = d^{p^2} = e.\ \ cd = d^t c;\ \ t^m \equiv 1 \pmod{p^2}\},$$

and the isomorphism between G and G_r is in fact established by the correspondence

$$a \longleftrightarrow c,\ b \longleftrightarrow d c^{-xkr},$$

where x is defined by $x(t-1) \equiv 1 \pmod{p^2}$. (Note that x is prime to p since $t-1$ is prime to p). Thus in all cases G has the defining relations (15) and (16).

For the converse, let H be the system of all formal pairs $[x, y]$ where $x = 0, 1, \ldots, p^2-1$; $y = 0, 1, \ldots, m-1$. In this system define multiplication by means of the formulae

$$[x, y]\,[x', y'] = [x'', y''],$$

where

$$x'' \equiv x + t^y x' \pmod{p^2} \qquad \text{and} \qquad y'' \equiv y + y' \pmod{m}.$$

Then by direct calculation one can show that the system H forms a group whose unit element is $[0, 0]$. Moreover, if $b' = [1, 0]$ and $a' = [0, 1]$, then $b'^x a'^y = [x, y]$) i.e. every element of H is uniquely of the form $b'^x a'^y$, hence H is the general product of $\{b'\}$ and $\{a'\}$ and thus also of $\{a'\}$ and $\{b'\}$. The order of $\{a'\}$ is m and that of $\{b'\}$ is p^2, therefore the order of H is p^2m. Thus corresponding to the defining relations of G we have

$$a'^m = b'^{p^2} = e'$$

[2]) This process merely replaces the generators a and b of G by the generators c and d respectively.

where e' denotes the unit element $[0, 0]$ of H. Furthermore $a'b' = b'^{t}a'$. From this we see first that a' induces the permutation π, described in the theorem, and furthermore that H is a homomorphic image of G. But as the order of H is $p^2 m$ and that of G is at most $p^2 m$, then G and H have the same order and are isomorphic. Hence G is the desired general product.

To distinguish the non-isomorphic types of groups defined in Theorem 3, we prove the following

Theorem 4. *Let G and H be two groups whose defining relations are*

$$G = \{a, b;\quad a^m = b^{p^2} = e,\quad ab = b^t a\},$$
$$H = \{c, d;\quad c^m = d^{p^2} = e,\quad cd = d^{t'} c\},$$

where t and t' are any numbers prime to p such that $t-1$ and $t'-1$ are both prime to p and $t^m \equiv 1 \pmod{p^2}$, $t'^m \equiv 1 \pmod{p^2}$. Let k and k' be the least possible numbers such that $t^k \equiv 1 \pmod{p^2}$ and $t'^{k'} \equiv 1 \pmod{p^2}$. Then G and H are isomorphic if and only if $k = k'$.

Proof. From the defining relations of G, it is easy to deduce that the the centre of G is $\{a^k\}$, its order is $\dfrac{m}{k}$. Similarly the centre of H is $\{c^{k'}\}$, its order is $\dfrac{m}{k'}$. If G is isomorphic to H, then their centres will have the same order, hence $k = k'$. This shows the necessity of the condition stated.

Next, to show that the condition is sufficient, we point out that if $k = k'$, then there exists a number λ which can be suitably chosen such that $(\lambda, m) = 1$ and $t \equiv t'^{\lambda} \pmod{p^2}$ and the isomorphism of G and H is established by the correspondence

$$a \leftrightarrow c^{\lambda},\quad b \leftrightarrow d.$$

This completes the proof of the theorem.

We consider now the permutations $\pi x \equiv tx \pmod{p^2}$ when $(t-1, p^2) = p$. We prove the following

Theorem 5. *If there is a general product G corresponding to the semi-special permutation π given by $\pi x \equiv tx \pmod{p^2}$ where $(t-1, p^2) = p$, then it has the defining relations*

$$G = \{a, b;\quad a^m = b^{p^2} = e,\quad ab = b^t a^{pr+1},\quad a^p b = b a^{p(pr+1)}\}, \tag{20}$$

where m is divisible by p and where

$$p(pr+1)^p \equiv p \pmod{m}. \tag{21}$$

Conversely, if m is divisible by p and if r satisfies (21), then the group G generated by a and b with the defining relations (20) is the general product of $\{a\}$ and $\{b\}$ of the type required.

PROOF. By hypothesis, $t \equiv 1+\lambda p \pmod{p^2}$ for some number λ which is prime to p, and evidently the order of π is p.

Assume now the existence of the general product G. Since π is of order p, then by Lemma 6 m is a multiple of p and

$$a^p b = b a^{ps} \tag{22}$$

for a suitable number s which is prime to $\frac{m}{p}$. Moreover, the h of Lemma 6 is p; in this case

$$ps^p \equiv p \pmod m \qquad \text{and} \qquad a^p b^p = b^p a^p. \tag{23}$$

Further, by direct calculation $\pi_1 = \pi$; hence by Lemma 7

$$ab = b^t a^{pr+1}, \tag{24}$$

for a suitable number r. Then by an induction argument and by using (22) and (23), we get

$$a b^x = b^{tx} a^{pr(1+s+s^2+\cdots+s^{x-1})+1} \tag{25}$$

$$a b^{yp} = b^{yp} a^{ypr(1+s+s^2+\cdots+s^{p-1})+1} \tag{26}$$

(note that $t \equiv 1+\lambda p \pmod{p^2}$). Relations (25) and (26) combine together to give

$$a b^{x+yp} = b^{tx+yp} a^{ypr(1+s+\cdots+s^{p-1})+pr(1+s+\cdots+s^{x-1})+1}. \tag{27}$$

Now, if we put $y=p$ in (26), we obtain

$$a b^{p^2} = b^{p^2} a^{p^2 r(1+s+s^2+\cdots+s^{p-1})+1},$$

on the other hand, by Lemma 5, (5) we have $ab^{p^2} = b^{p^2} a$, and therefore

$$p^2 r(1+s+s^2+\cdots+s^{p-1}) \equiv 0 \pmod m. \tag{28}$$

Furthermore, if we apply an induction argument to (24), use (27) and remember that $t \equiv 1+\lambda p \pmod{p^2}$, we can show that

$$a^z b = b^{1+\lambda p z} a^{\frac{1}{2} z(z-1)\lambda pr(1+s+s^2+\cdots+s^{p-1})+z(pr+1)} \tag{29}$$

Now, if we put $z=p$ in (29), then compare with (22) and use (28), we obtain $ps \equiv p(pr+1) \pmod m$; hence by the first of (23), we see that $p(pr+1)^p \equiv p \pmod m$. Thus we have shown that (20) and (21) are necessary.

For the converse, let P be the set of classes of formal pairs $[x, y]$ where x is taken $\operatorname{mod} p^2$ and y $\operatorname{mod} m$. The pairs $[x, y]$ and $[x', y']$ are to be considered identical when $x \equiv x' \pmod{p^2}$ and $y \equiv y' \pmod m$. Let H be the group of permutations of P generated by the permutations α and β where

$$\alpha[x, y] = [x, y+1]$$

and

$$\beta[x, yp+z] = \left[x+\lambda pz+1,\ (yp+z)(pr+1)+\frac{1}{2}z(z-1)pK\right]$$

where

$$pK \equiv \lambda\{(pr+1)^p-1\} \pmod{m}.$$

That β is in fact a permutation, can be shown as follows: If

$$x'+\lambda pz'+1 \equiv x+\lambda pz+1 \pmod{p^2} \tag{30}$$

and

$$\begin{aligned}(y'p+z')(pr+1)+\frac{1}{2}z'(z'-1)pK &\equiv \\ \equiv (yp+z)(pr+1)+\frac{1}{2}z(z-1)pK &\pmod{m}\end{aligned} \tag{31}$$

then from (31) it would follow (since p divides m), that $z' \equiv z \pmod{p}$ and then $x' \equiv x \pmod{p^2}$ by (30). Further since $z' \equiv z \pmod{p}$ and $p^2K \equiv 0 \pmod{m}$ (this follows from (21)) and since $pr+1$ is prime to $\frac{m}{p}$ $\left(\text{because } s \equiv pr+1 \left(\text{mod}\,\frac{m}{p}\right) \text{ is prime to } \frac{m}{p}\right)$, then from (31) it follows at once that $y'p+z' \equiv yp+z \pmod{m}$. This shows that β is actually a permutation.

Now, if ε denotes the identity permutation, then by direct calculation and by using (21) together with the fact that m is divisible by p, we can show that

$$\alpha^m = \beta^{p^2} = \varepsilon,\ \alpha\beta = \beta^t\alpha^{pr+1},\ \alpha^p\beta = \beta\alpha^{p(pr+1)}.$$

From this we see first that H is a homomorphic image of G. Furthermore no power of $\{\alpha\}$ (except the unit element) is in $\{\beta\}$ and vice versa and thus H is the general product of $\{\alpha\}$ and $\{\beta\}$. But as the order of H is p^2m and that of G is at most p^2m, they have the same orders and are isomorphic. Hence G is the desired general product. This completes the proof of the theorem.

To distinguish the non-isomorphic types of groups defined in Theorem 5 we prove the following

Lemma 8. *Let the notation be as in Theorem 5 and let t' be any number prime to p such that $(t'-1, p^2) = p$. Then the permutation π' defined by $\pi'x \equiv t'x \pmod{p^2}$ leads to the same groups as does the permutation π described in the theorem.*

Proof. Since π and π' are both of order p, then there exists a number v prime to p such that $t'^v \equiv t \pmod{p^2}$. Further m being divisible by p, let precisely $m=p^g M$ where $g \geqq 1$ and $(M,p)=1$. Choose now a number i such that

$$i \equiv v \pmod{p^g} \qquad \text{and} \qquad i \equiv 1 \pmod{M}.$$

This is legitimate as $(M,p)=1$ and the above congruences can be solved simultaneously. Then i is prime to m.

Suppose now that G is a general product generated by a and b where a induces the permutation π'. We generate G by $a' \equiv a^i$ (note that i is prime to m) and b and let π^* be the permutation by $a'=a^i$ on the powers of b, we find that

$$b^{\pi^* x} = b^x_{a'} = b^x_{a^i} = b^{\pi'^i x} = b^{\pi'^v x} = b^{t'^v x} = b^{tx}, \quad i \equiv v \pmod{p}$$

and p is the order of π', this shows that $\pi^* = \pi$. Thus π^* and hence π' leads to the same groups as in Theorem 5. This proves the lemma.

By the above lemma, it is sufficient to distinguish for isomorphism the groups (described in Theorem 5) with the same t but with different r. For this purpose, we give the following

Theorem 6. *Let G and H be two groups whose defining relations are*

$$G = \{a, b;\ a^m = b^{p^2} = e,\ ab = b^t a^{pr+1},\ a^p b = b a^{p(pr+1)}\},$$
$$H = \{a, b;\ a^m = b^{p^2} = e,\ ab = b^t a^{pr'+1},\ a^p b = b a^{p(pr'+1)}\},$$

where t is some number prime to p such that $(t-1, p^2)=p$; m is divisible by p and where

$$p(pr+1)^p \equiv p \pmod{m}, \qquad p(pr'+1)^p \equiv p \pmod{m}.$$

Then a necessary and sufficient condition for G and H to be isomorphic is $pr'+1 \equiv (pr+1)^\theta \left(\bmod \dfrac{m}{p}\right)$ for some number θ which is prime to p.

The proof of this theorem is rather long and needs laborious considerations; for this reason it is omitted. The reader, if intersted in the proof, is referred to the method used by the author (Cf. [9], Chapter VII, Theorem 28. 18).

§ 5. The permutation $\pi x \equiv rx + \mu p x^2 \pmod{p^2}$.

We show that this permutation leads to the same groups as does the permutation described in Theorem 3. We prove the following

Lemma 9. *Let the notation be as in Theorem 3 and let m be divisible by p and put $\dfrac{m}{(m,p^2)} = \lambda$. Then*

(i) *the element* ba^{λ} *is of order* p^2;

(ii) *the group* G *may be generated by* a *and* b' *instead of by* a *and* b, *where* $b' = ba^{\lambda}$.

PROOF. From the relation $ab = b^t a$ (see (15)), we see at once

$$a^x b^y = b^{t^x y} a^x. \tag{32}$$

Thus

$$b^{2} = (ba^{\lambda})^2 = ba^{\lambda} ba^{\lambda} = b^{1+t^{\lambda}} a^{2\lambda},$$

and then by induction

$$b'^x = b^{1+t^{\lambda}+t^{2\lambda}+\cdots+t^{(x-1)\lambda}} a^{x\lambda}. \tag{33}$$

If k' be the order of $t \bmod p$, then from the defining relations of G (see (16)) m and therefore λ is a multiple of k'. Let precisely $\lambda = \nu k'$ and $t^{k'} \equiv 1 + up \pmod{p^2}$. Then

$$1 + t^{\lambda} + t^{2\lambda} + \cdots + t^{(x-1)\lambda} = \sum_{i=0}^{x-1} t^{i\lambda} = \sum_{i=0}^{x-1} t^{i\nu k'} \equiv x + \frac{1}{2} up\nu\, x(x-1) \pmod{p^2}$$

(by substitung for $t^{k'} \equiv 1 + up \pmod{p^2}$ and reducing each term $\bmod p^2$). Hence (33) implies (note that the exponent of b is to be taken $\bmod p^2$)

$$b'^x = b^{x+\frac{1}{2}up\nu x(x-1)} a^{x\lambda}, \tag{34}$$

this shows that no power of b' (except the unit element) lies in $\{a\}$ and vice versa. Also

$$b'^p = b^p a^{p\lambda},$$

by (34).

Now, if $(m, p^2) = p$, then $p\lambda = m$; in this case $b'^p = b^p$ which shows that b' is of order p^2.

Further, if $(m, p^2) = p^2$, then $p^2\lambda = m$ and by (34) we have

$$b'^p = b^p a^{p\lambda} = b^p a^{p\nu k'}. \tag{35}$$

Now, if we take $x = k'$ and $y = p$ in (32) and remember that $t^{k'} \equiv 1 + up \pmod{p^2}$, we obtain $a^{k'} b^p = b^p a^{k'}$, thus $a^{k'}$ and b^p commute; hence from (35), we see at once that b' is of order p^2. Thus in both cases b' is of order p^2 and (i) is proved.

(ii) is an immediate consequence of (i).

Retaining the same notation, we prove

Lemma 10. *The permutation* π^* *induced by* a *on the powers of* b' *is of the form* $\pi^* x \equiv tx + \mu p x^2 \pmod{p^2}$, *for suitable* t *and* μ.

PROOF. By using (34) and (32) respectively, we get

$$ab'^x = ab^{x+\frac{1}{2}up\nu x(x-1)} a^{x\lambda},$$

i. e.

$$ab'^{x} = b^{tx+\frac{1}{2}upvt\,x(x-1)}a^{x\lambda+1} \tag{36}$$

On the other hand, if we use (34) once more, we find that

$$b'^{\pi^* x} = b^{\pi^* x+\frac{1}{2}up\nu(\pi^* x)(\pi^* x-1)}a^{\lambda\pi^* x} \tag{37}$$

Further, by hypothesis $ab'^{x} = b'^{\pi^* x}a_{b'x}$ where $a_{b'x}$ is a power of a, then by using (37), we obtain

$$ab'^{x} = b^{\pi^* x+\frac{1}{2}up\nu(\pi^* x)(\pi^* x-1)}a^{\lambda\pi^* x}a_{b'x}. \tag{38}$$

Comparing (36) and (38) and remembering that $a_{b'x}$ is a power of a, we get

$$\pi^* x+\frac{1}{2}up\nu(\pi^* x)(\pi^* x-1) \equiv tx+\frac{1}{2}up\nu t\,x(x-1) \pmod{p^2}. \tag{39}$$

Relation (39) implies at once $\pi^* x \equiv tx \pmod{p^2}$; furthermore π^* being determined $\bmod p^2$, let precisely $\pi^* x \equiv tx + pf(x) \pmod{p^2}$ where $f(x)$ is to be determined $\bmod p$. If we substitute for $\pi^* x$ in (39), we find that

$$tx+pf(x)+\frac{1}{2}up\nu\,tx(tx-1) \equiv tx+\frac{1}{2}up\nu\,tx(x-1) \pmod{p^2}.$$

Therefore $f(x) = \frac{1}{2}u\nu\,t(1-t)x^2 \equiv \mu x^2 \pmod{p}$, where $\mu \equiv \frac{1}{2}\nu t(1-t) \pmod{p}$ is prime to p because t and $t-1$ are both prime to p. Thus $\pi^* x \equiv tx+\mu p x^2 \pmod{p^2}$ where t is any number prime to p such that $t-1$ is prime to p i. e. such that $t \not\equiv 1 \pmod{p}$. This proves the lemma.

Lemmas 9 and 10 combine together to show that the permutations $\pi x \equiv rx+\mu p x^2 \pmod{p^2}$ will lead to the same groups which are described in Theorem 3.

CONCLUSION. The general products of $\{a\}$ and $\{b\}$ when $\{b\}$ is of order p^2, p being an odd prime, are described in Theorems 1, 3 and 5. The groups defined in these theorems will be distinguished for isomorphism in a separate note.

Bibliography.

[1] B. H. NEUMANN, Decompositions of groups, *J. London Math. Soc.* **10** (1935), 3—6.

[2] L. RÉDEI, Zur Theorie der faktorisierbaren Gruppen I, *Acta Math. Acad. Sci. Hungar.* **1** (1950), 74—98.

[3] G. ZAPPA, Sulla costruzione dei gruppi prodotto di due dati sottogruppi permutabili tra loro, *Atti Secondo Congresso Un. Mat. Ital. Bologna* (1940), 119—125.

[4] K. R. YACOUB, General products of two finite cyclic groups, *Proc. Glasgow Math. Assoc.* **2** (1955), 116—123.

[5] J. Douglas, On finite groups with two independent generators, *Proc. Nat. Acad. Sci. U. S. A.* **37** (1951), 604—610.

[6] J. Douglas, On finite groups with two independent generators, *Proc. Nat. Acad. Sci. U. S. A.* **37** (1951), 677—691.

[7] B. Huppert, Über das Produkt von paarweise vertauschbaren zyklischen Gruppen, *Math. Z.* **58** (1953), 243—264.

[8] K. R. Yacoub, On semi-special permutations I, *Proc. Glasgow Math. Assoc.* **3** (1956), 18—35.

[9] K. R. Yacoub, A thesis on general products of two cyclical groups, *London University,* (1953).

(Received December 21, 1957.)