On a certain class of finite groups with two independent generators

By K. R. YACOUB (Cairo)

A group G may have several independent generators; but it is completely defined, as an abstract group, by means of any set of abstract generators and all the independent relations by which they are connected.

For a finite group with two independent generators certain permutations (or substitutions [1]) are however sufficient for the determination of the structure of the group [2]. In order to be precise, let G be such a group and let a, b (of orders m and n respectively) be its independent generators. Then [2], associated with G, there corresponds two permutations π and ϱ such that

$$a^y b^x = b^{\pi^y x} a^{\varrho^x y} : x \in [n],\ y \in [m] \tag{1}$$

where π is semi-special on $[n]$ and ϱ on $[m]$.

By means of these two permutations, the product of any two elements in G can be easily formed according to the rule

$$b^x a^y \cdot b^{x'} a^{y'} = b^x b^{\pi^y x'} a^{\varrho^{x'} y} a^{y'}$$

i. e. according to the rule

$$b^x a^y \cdot b^{x'} a^{y'} = b^{x+\pi^y x'} a^{\varrho^{x'} y+y'}.$$

For this reason, the structure of the group G depends entirely on the determination of the two permutations π and ϱ.

In particular, if both π and ϱ are the identity permutations i. e. if $\pi x \equiv x \pmod n$ and $\varrho y \equiv y \pmod m$; then (1) implies at once

$$a^y b^x = b^x a^y.$$

In this case, every element of $\{a\}$ commutes with every element of $\{b\}$ and the group G is, in fact, the direct product of $\{a\}$ and $\{b\}$. The defining relations of G are simply

$$G = \{a, b;\ a^m = b^n = e,\ ab = ba\}.$$

This is the simplest type of a finite group with two independent generators. Other types do, in fact, exist; but their structure properties are not so simple.

However, the structure of the group G seems to be of particular interest when one of the permutations π and ϱ is linear i. e. when π, say is defined by $\pi x \equiv ux \pmod n$ for some number u which is prime to n. It is the object of the present note to describe in a simple way the structure of all such groups.

In § 1, we collect together some unrelated lemmas mainly for subsequent use. The proofs are omitted and the reader if interested may be referred to a previous paper by the author ([3], § 2).

§ 1. Some fundamental results

Lemma 1. *For all* $x \in [n]$ *and* $y \in [m]$

$$a^m b^x = b^x a^m, \quad a^y b^n = b^n a^y.$$

Lemma 2. *Let k be the order of π (which may be linear or not). Then*

(i) *k divides m,*

(ii) *a number s prime to m/k exists such that*

$$a^k b = b a^{ks}, \; ks^H \equiv k \pmod m$$

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) $a^k b^H = b^H a^k$.

Lemma 3. *Let π be a linear permutation, say $\pi x \equiv ux \pmod n$ and let $(u-1, n) = h$. Then*

$$ks^h \equiv k \pmod m, \quad a^k b^h = b^h a^k.$$

For in this case, the principal cycle of π is $(1, u, u^2, \ldots, u^{k-1})$; thus the H of the previous lemma is $u-1$ and the lemma follows at once if we remark that $a^k b^n = b^n a^k$ (see Lemma 1).

Now, since π is semi-special; then by definition the permutation π_y defined by $\pi_y x \equiv \pi(x+y) - \pi y \pmod n$ is a power of π. In particular, if π is linear then $\pi_y = \pi$ for every y ([1], Theorem 4. 10). Accordingly, we have the following lemma.

Lemma 4. *If π is a linear permutation, then*

$$a b^y = b^{\pi y} a^{kr(y)+1}$$

for a suitable $r(y)$ which depends on y (see [3], Lemma 7).

§ 2. Description of the problem

In this investigation, we deal with the case in which π is linear. Our aims are to (i) describe all the corresponding groups in terms of some simple parameters and (ii) prove the existence of such groups for permissible parameter values.

We deal seperately with the permutations $\pi x \equiv x \pmod{n}$, $\pi x \equiv ux \pmod{n}$ where $(u-1, n)=1$ and finally with the permutations $\pi x \equiv ux \pmod{n}$ where $(u-1, n) \neq 1$.

§ 3. The permutation $\pi x \equiv x \pmod{n}$

Theorem 1. *If there is a group G corresponding to the permutation π, then it has the defining relations*

$$G=\{a, b;\ a^m=b^n=e,\ ab=ba^r\} \tag{2}$$

where

$$r^n \equiv 1 \pmod{m}. \tag{3}$$

Conversely if r is any number satisfying (3), then the group G generated by a and b with the defining relations (2) is of the desired type.

The proof is direct and is omitted.

§ 4. The permutation $\pi x \equiv ux \pmod{n}$ where $(u-1, n)=1$

Theorem 2. *Let u be any number prime to n such that $(u-1, n)=1$. If there is a group G corresponding to the linear permutation π given by $\pi x \equiv ux \pmod{n}$, then it has the defining relations*

$$G=\{a, b;\quad a^m=b^n=e,\quad ab=b^u a\} \tag{4}$$

where

$$u^m \equiv 1 \pmod{n}. \tag{5}$$

Conversely, if u and $u-1$ are both prime to n and if m is any integer such that (5) *is satisfied; then the group G generated by a and b with the defining relations* (4) *is of the type desired.*

Proof. Assume the existence of the group G. Let k be the order of u mod n i. e. k is the least positive integer such that $u^k \equiv 1 \pmod{n}$. Then it is evident that k is the order of π and by Lemma 2 (i), m is a multiple of k; this confirms (5).

Moreover, since $(u-1, n)=1$; then by Lemma 3

$$a^k b = ba^k. \tag{6}$$

Next, by Lemma 4 (with $y=1$) we have

$$ab=b^u a^{kr+1} \quad \text{for a suitable number } r.$$

Then by induction and by using (6), we find that

$$ab^x=b^{ux}a^{xkr+1}.$$

Now, if we take $x=n$ and use the second of Lemma 1 we get

$$nkr\equiv 0 \pmod{m}. \tag{7}$$

We remark that (7) is satisfied by $kr\equiv 0 \pmod{m}$; in this case G has the defining relations

$$G=\{a,b;\quad a^m=b^n=e,\ ab=b^u a;\quad u^m\equiv 1 \pmod{n}\}.$$

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

$$G_r=\{a,b;\ a^m=b^n=e,\ ab=b^u a^{kr+1},\ a^k b=ba^k;\quad u^m\equiv 1 \pmod{n}\}.$$

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

$$G=\{c,d;\ c^m=d^n=e, cd=d^u c;\ u^m\equiv 1 \pmod{n}\}.$$

Then the isomorphism between G and G_r is established by the correspondence

$$a\leftrightarrow c;\quad b\leftrightarrow dc^{-xkr}$$

where x is defined by $x(u-1)\equiv 1 \pmod{n}$.

Thus, in all cases G has the defining relations (4) and (5).

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

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

where $x''\equiv x+u^y x' \pmod{n}$; $y''\equiv y+y' \pmod{m}$.

This multiplication is associative, for

$$\begin{aligned}[x,y]\,\{[x',y']\,[x'',y'']\} &= [x,y]\,[x'+u^{y'}x'',y'+y'']\\ &= [x+u^y x'+u^{y+y'}x'',y+y'+y'']\\ &= [x+u^y x',y+y']\,[x'',y'']\\ &= \{[x,y]\,[x',y']\}\,[x'',y''].\end{aligned}$$

Also $[0,0]$ is a unit element and $[-xu^{-y},m-y]$ is the inverse of $[x,y]$ where the value of u^{-y} can always be reffered to a positive exponent by

* This process merely replaces the generators a and b of G by c and d respectively.

means of the relation $u^k \equiv 1 \pmod{n}$ i. e. by adding a multiple of k to the exponent.

Moreover if $a' = [0, 1]$ and $b' = [1, 0]$ then it is easy to see that

$$b'^x = [x, 0], \;\; a'^y = [0, y], \;\; b'^x a'^y = [x, y].$$

Thus every element of H is uniquely of the form $b'^x a'^y$. The order of a' is m and that of b' is n; therefore the order of H is mn. Thus corresponding to the defining relations of G we have

$$a'^m = b'^n = e'$$

where e' denotes the unit element $[0, 0]$.

Also
$$a' b' = [0, 1]\,[1, 0] = [u, 1],$$

and
$$b'^u a' = [u, 0]\,[0, 1] = [u, 1].$$

Thus
$$a' b' = b'^u a'.$$

From this, we see first that a' induces the permutation π described in the theorem and further that H is a homomorphic image of G. But as the order of H is mn and that of G is at most mn; then G and H have the same order and are isomorphic. Hence G is the desired group.

§ 5. The permutation $\pi x \equiv ux$ *(mod n)* where $(u-1, n) \neq 1$

Theorem 3. *Let u be any number prime to n such that $(u-1, n) \neq 1$ and let k be the order of u mod n and $(u-1, n) = h$. If there is a group G corresponding to the linear permutation given by $\pi x \equiv ux \pmod{n}$; then it has the defining relations*

$$G = \{a, b;\;\; a^m = b^n = e,\;\; ab = b^u a^{kr+1},\; a^k b = b a^{ks}\} \tag{8}$$

where

$$m \equiv 0 \pmod{k}, \;\; ks^h \equiv k \pmod{m}; \tag{9}$$

$$Nkrf(h) \equiv 0 \pmod{m}, \;\; n = Nh \tag{10}$$

$$ks \equiv k + kr \sum_{i=0}^{k-1} f(u^i) \pmod{m} \tag{11}$$

and where $f(x)$ is defined mod $\dfrac{m}{k}$ *by*

$$krf(x) \equiv kr(1 + s + \cdots + s^{x-1}) \pmod{m}.$$

PROOF. Assume the existence of the group G. Then by Lemma 2, k divides m; this proves the first of (9). Again by the same lemma

$$a^k b = b a^{ks} \tag{12}$$

for some number s which is prime to $\frac{m}{k}$.

Moreover, by Lemma 3

$$k s^h \equiv k \pmod{m} \tag{13}$$

which proves the second of (9); also

$$a^k b^h = b^h a^k.$$

Now if we use (12), (13) and remark that h divides $u-1$ we obtain

$$a^k b^u = b^u a^{ks}. \tag{14}$$

Next, by Lemma 4 (with $y=1$) we have

$$a b = b^u a^{kr+1} \tag{15}$$

for a suitable number r.

Then by an induction process and by using (14), we get

$$a b^x = b^{ux} a^{kr(1+s+\cdots+s^{x-1})} + 1$$

which, in the notation of the theorem, becomes

$$a b^x = b^{ux} a^{krf(x)+1}. \tag{16}$$

For $x=h$, we have

$$a b^h = b^{uh} a^{krf(h)+1}. \tag{17}$$

But since a^k and b^h commute, then by induction we can show that

$$a b^{yh} = b^{yuh} a^{ykrf(h)+1}. \tag{18}$$

Now if, in (18), we put $y=N$ and remark that $ab^n = b^n a$; we get

$$Nkrf(h) \equiv 0 \pmod{m}$$

which proves (10).

Again by repeated application of (15) and by using (16), we have

$$a^2 b = a a b = a b^u a^{kr+1} = b^{u^2} a^{kr\{1+f(u)\}+2}$$

and generally

$$a^z b = b^{u^z} a^{kr} \sum_{i=0}^{z-1} f(u^i) + z.$$

If we take $z=k$ and compare with (12), we get

$$ks \equiv kr \sum_{i=0}^{k-1} f(u^i) + k \pmod{m};$$

this proves (11). Thus we have shown that (8), (9), (10) and (11) are necessary.

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

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

$$\beta[x, ky+z] = [x+u^z, kys+kr\theta(z)+z]$$

where $z = 0, 1, \dots, k-1$ and

$$kr\theta(0) \equiv 0,\ kr\theta(z) \equiv kr \sum_{i=0}^{z-1} f(u^i) \pmod{m} \text{ for } z \neq 0.$$

We show first that β is, in fact, a permutation. For if

(19) $$x' + u^{z'} \equiv x + u^z \pmod{n}$$

and

(20) $$ky's + kr\theta(z') + z' \equiv kys + kr\theta(z) + z \pmod{m};$$

then from (20) (since k divides m and $z, z' < k$) it would follow that $z' = z$ and then from (19) $x' \equiv x \pmod{n}$. Consequently from (20) we deduce $ky's \equiv kys \pmod{m}$ or equivalently $ky' \equiv ky \pmod{m}$ since s is prime to $\frac{m}{k}$. This shows that β is actually a permutation.

The proof of the converse is rather long and is affected by means of the following lemma.

Lemma 5. *The functions $f(x)$ and $\theta(z)$ satisfy, in virtue of* (9) *and* (11) *the following relations:*

(21) $$krf(u^i) \equiv krf(u^{i-1}) \cdot f(u) \pmod{m}$$

(22) $$kr\theta(z+1) \equiv kr + krf(u) \cdot \theta(z) \pmod{m} \qquad 0 \leqq z < k-1$$

(23) $$ks - k \equiv kr + krf(u) \cdot \theta(k-1) \pmod{m}$$

Proof. For (21), we have by the definition of $f(x)$

$$krf(u^i) \equiv kr(1+s+s^2+\cdots+s^{u^i}-1) \equiv$$

$$\equiv kr(1+s+s^2+\cdots+s^{u^{i-1}-1})(1+s^{u^{i-1}}+s^{2u^{i-1}}+\cdots+s^{u^{i-1}(u-1)}) \text{ mod } m).$$

But since h divides $u-1$ and $ks_h \equiv k \pmod{m}$ (see (9)); then it would follow that $ks^u \equiv ks \pmod{m}$ and consequently that $ks^{yu^z} \equiv ks^y \pmod{m}$ for all y and z. Therefore

$$krf(u^i) \equiv kr(1+s+s^2+\cdots+s^{u^{i-1}-1})(1+s+s^2+\cdots+s^{u-1}) \equiv$$
$$\equiv krf(u^{i-1})\cdot f(u) \pmod{m}$$

which proves (21).

Next: For (22), we have by the definition of $\theta(z)$ for $0 \leqq z < k-1$,

$$\begin{aligned} kr\theta(z+1) &\equiv kr\sum_{i=0}^{z} f(u^i) \equiv \\ &\equiv kr + kr\sum_{i=1}^{z} f(u^i) \equiv \\ &\equiv kr + krf(u)\cdot\sum_{i=1}^{z} f(u^{i-1}) \equiv \qquad \text{(by (21))}, \\ &\equiv kr + krf(u)\cdot\theta(z) \pmod{m}; \end{aligned}$$

this proves (22).

Finally, for (23) we have

$$\begin{aligned} krf(u)\cdot\theta(k-1)+kr &\equiv krf(u)\sum_{i=0}^{k-2} f(u^i) + kr \equiv \\ &\equiv kr\sum_{i=0}^{k-2} f(u^{i+1}) + kr \equiv \\ &\equiv kr\sum_{i=0}^{k-1} f(u^i) \equiv \qquad \text{(by using (21))} \\ &\equiv ks-k \pmod{m} \qquad \text{in virtue of (11)}; \end{aligned}$$

this completes the proof of the lemma.

We return now to the proof of the converse of the theorem. By direct calculation, we can show that $\alpha^m = \varepsilon$ wehre ε denotes the identity permutation.

Moreover

$$\beta^2[x, ky+z] = [x+2u^z, kys^2+kr(1+s)\theta(z)+z]$$

and generally

$$\beta^i[x, ky+z] = [x+iu^z, kys^i+kr(1+s+\cdots+s^{i-1})\theta(z)+z]$$

which, by using the notation of $f(x)$, gives

$$(24) \qquad \beta^i[x, ky+z] = [x+iu^z, kys^i+krf(i)\cdot\theta(z)+z].$$

Now if we take $i=h$ and remark that $ks^h \equiv k \pmod{m}$, we deduce

$$\beta^h[x, ky+z] = [x+hu^z, ky+krf(h)\theta(z)+z]$$

which, by induction on the multiples of h, gives at once

$$\beta^{jh}[x, ky+z] = [x+jhu^z, ky+jkrf(h)\cdot\theta(z)+z].$$

Taking $j=N$ and remembering that $Nkrf(h)\equiv 0 \pmod{m}$ (see (10)), we find that

$$\beta^{Nh}[x, ky+z] = [x, ky+z]$$

showing that $\beta^n = \varepsilon$. Furthermore

$$(25)\qquad \begin{cases} \alpha\beta[x, ky+z] = [x+u^{z+1}, kys+kr\theta(z+1)+z+1] \text{ for } z<k-1 \\ \text{and} \\ \alpha\beta[x, ky+k-1] = [x+1, (ky+k)s]. \end{cases}$$

Again if we take $i=u$ in (24) and remember that $ks^u\equiv ks \pmod{m}$ we get

$$\beta^u[x, ky+z] = [x+u^{z+1}, kys+krf(u)\cdot\theta(z)+z]$$

and consequently

$$\beta^u\alpha^{kr+1}[x, ky+z] = [x+u^{z+1}, kys+krf(u)\cdot\theta(z)+kr+z+1].$$

Which on comparing with (25) and using (22) and (23) gives

$$\alpha\beta = \beta^u\alpha^{kr+1}.$$

Sim

Similarly

$$\alpha^k\beta[x, ky+z] = [x+u^z, k(y+1)s+kr\theta(z)+z]$$

and

and

$$\beta\alpha^{ks}[x, ky+z] = [x+u^z, kys+kr\theta(z)+z+ks].$$

Hen

Hence $\alpha^k\beta = \beta\alpha^{ks}$.

Thus according to the defining relations of G, we have

$$\alpha^m = \beta^n = \varepsilon,\ \alpha\beta = \beta^u\alpha^{kr+1},\ \alpha^k\beta = \beta\alpha^{ks}.$$

$$\alpha^m = \beta^n = \varepsilon,\ \alpha\beta = \beta^u\alpha^{kr+1},\ \alpha^k\beta = \beta\alpha^{ks}.$$

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. But as the order of H is mn and that of G is at most mn, they have the same order and are isomorphic. Hence G is the desired group. This completes the proof of the theorem.

In previous notes, the author had come across some special cases of this theorem. We mention here the cases: $n=4$ (Cf. [4], Theorem 3); $n=8$ (Cf. [5], Theorems 3,5) and $n=p^2$ where p is an odd prime (Cf. [3], Theorem 5). The case $n=4$ will be worked out as an illustrative example.

Special case: Let $n=4$; in this case $u=3, h=k=N=2$. Moreover the function $f(x)$ which appears in conditions (9), (10) and (11) is now defined by

$$(26)\qquad 2rf(x)\equiv 2r(1+s+\cdots+s^{x-1}),\ \pmod{m}.$$

Condition (9), in this case, requires that m is even and also that

$$2s^2 \equiv 2 \pmod{m}. \tag{27}$$

Next, condition (10) reduces to $4rf(2) \equiv 0 \pmod{m}$ which by using (26) gives at once

$$4r(1+s) \equiv 0 \pmod{m}. \tag{28}$$

Finally, condition (11) implies

$$\begin{aligned} 2s &\equiv 2 + 2r\{1+f(3)\} \pmod{m} \\ &\equiv 2+2r(2+s+s^2) \pmod{m}, \text{ by using (26)}, \\ &\equiv 2+2r(3+s) \pmod{m}, \text{ in virtue of (27)}, \\ &\equiv 2+4r+2r(1+s) \pmod{m} \\ &\equiv 2+4r-2r(1+s) \pmod{m}, \text{ in virtue of (28)}. \end{aligned}$$

Hence

$$2(1+r)(s-1) \equiv 0 \pmod{m}. \tag{29}$$

Thus besides the condition imposed on m conditions (27), (28) and (29) must also hold. In this case, G has the defining relations

$$G = \{a, b; a^m = b^4 = e, ab = b^3a^{2r+1}, a^2b = ba^{2s}\}$$

where m is even and

$$2s^2 \equiv 2,\ 4r(1+s) \equiv 0,\ 2(1+r)(s-1) \equiv 0 \pmod{m}$$

(Cf. [4], Theorem 3).

In a similar manner we can check up the special cases mentioned above together with others.

§ 6. Conclusion

Theorems 1, 2 and 3 describe all the finite groups, with two independent generators, when the permutations induced by one of the generators on the powers of the other are linear.

However, in some particular cases no other group can be furnished. This is the case when the semi-special permutations on $[n]$ are all linear. Such cases arise for example when $n=p$ is an odd prime (Cf. [1] Corollary 4. 13), or when $n=pq$ for distinct odd primes p and q with $p<q$, say, and p not dividing $q-1$ (Cf. [6] Theorem 4; 6). The above theorems, thus, show themselves fruitful as they give a complete description of the groups in such cases.

Bibliography

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

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

[3] K. R. Yacoub, On the general products of two finite cyclic groups one of which being or orderer p^2, *Publ. Math. Debrecen* **6** (1955), 26—39.

[4] K. R. Yacoub, On general products of two finite cyclic groups one being of order 4 *Proc. Math. Phys. Soc. Egypt.* **21** (1957), 119—126.

[5] K. R. Yacoub, On general products of two finite cyclic groups one being of order 8 *Proc. Math. Phys. Soc. Egypt.* **22** (1958), 93—99.

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

(Received December 2, 1959.)