On finite groups with three independent generators two of which being of odd prime order

By K. R. YACOUB (Cairo)

A finite 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. If the group has just a single generator, then it is cyclic and the group is completely determined if its order is given. But if the group G has two independent generators, the determination of G is no further simple. However, certain permutations (called by the author [1] semi-special permutations and by DOUGLAS [2] conjugate substitutions) are sufficient for the determination of G.

Precisely speaking, let G be such a group and let a, b (of orders m, n respectively) be its independent generators. Then [1], associated with G, there corresponds two permutations π and ϱ such that

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

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

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

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

This shows the importance of the role played by the permutations π and ϱ in association with the structure of the group G. A detailed study of these permutations, done recently by the author, helped a lot in the determination of all the groups G specially when $n=p$, $2p$ (Cf. [3]) and also when $n=p^2$ (Cf. [4]) where p is an odd prime number*).

Moreover, if the group G has three independent generators, the structure of the group is much more complicated. In such cases, the determination of the group G will be treated in a different manner. However, it is the object of the present paper to make a complete determination of the group G when two of its generators have equal order p. The way of tackling such a problem depends mainly on the results already obtained by the author for groups with two independent generators.

*) The symbol p is used throughout this paper to denote an odd prime number.

§ 1. Description of the problem

We start by collecting some unrelated results for frequent use.

Theorem 1. *The general products of two cyclic groups, one of which being of order p, are*

$$G_1=\{a, b; a^m=b^p=e, ab=ba^r, r^p\equiv 1 \pmod m\}$$

$$G_2=\{a, b; a^m=b^p=e, ab=b^u a, u\not\equiv 1 \pmod p), u^m\equiv 1 \pmod p)\}.$$

Theorem 2. *No group of the type G_1 is isomorphic to a group of the type G_2.* For the proofs of Theorems 1 and 2, the reader may be referred to [3] or to [5].

Theorem 3. *Every group of order p^2 is Abelian.*

Returning now to our problem, let G be a finite group with three independent generators namely a, b, c and suppose that m is the order of a while b and c are of order p. Then $a^m=b^p=c^p=e$.

Moreover, the subgroup $\{a, b\}$, being a general product, of $\{a\}$ and $\{b\}$ must be either of the type G_1 or of the type G_2. Similarly for the subgroup $\{a, c\}$, thus four cases have to be considered seperately namely:

(1) the subgroups $\{a, b\}$ and $\{a, c\}$ are both of the type G_1, in this case the associated group G, if it does exist, is said to be of the type $T(1, 1)$.

(2) the subgroup $\{a, b\}$ is of the type G_1 but $\{a, c\}$ is of the type G_2 and the associated group G, if it exists, is said to be of the type $T(1, 2)$.

(3) the subgroup $\{a, b\}$ is of the type G_2 but $\{a, c\}$ is of the type G_1, and the associated group, if it exists, is said to be of the type $T(2, 1)$,

(4) the subgroups $\{a, b\}$ and $\{a, c\}$ are both of the type G_2, and the associated group G is said to be of the type $T(2, 2)$.

It may be remarked that the existence of groups of the type $T(1, 2)$ implies directly the existence of groups of the type $T(2, 1)$. Moreover, the interchange of the generators b and c in groups of the type $T(2, 1)$ leads at once to groups of the type $T(1, 2)$. Accordingly, we shall deal only with groups of the types $T(1, 1)$, $T(1, 2)$ and $T(2, 2)$. Our aims are to describe all groups in terms of some simple parameters and then prove the existence of such groups for permissible parameter values.

§ 2. Groups of the type $T(1, 1)$

Theorem 4. *If there is a group G of the type $T(1, 1)$, then it has the defining relations*

$$G=\{a, b, c; a^m=b^p=c^p=e, ab=ba^r, ac=ca^s, bc=cb\} \tag{1}$$

where

$$r^p\equiv 1 \pmod m), \quad s^p\equiv 1 \pmod m). \tag{2}$$

Conversely if r and s are any numbers satisfying (2), *then the group G generated by a, b and c with the defining relations* (1) *is of the desired type.*

PROOF. Assume the existence of the group G. Then since $\{a, b\}$ and $\{a, c\}$ are both of the type G_1, their defining relations may be written as

$$\{a, b\} = a^m = b^p = e,\ ab = ba^r,\ r^p \equiv 1 \pmod{m},$$

$$\{a, c\} = a^m = c^p = e,\ ac = ca^s,\ s^p \equiv 1 \pmod{m}.$$

Moreover $\{b, c\}$ being of order p^2 is Abelian and therefore $bc = cb$. Thus we have shown that (1) and (2) are necessary.

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

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

where

$$x'' \equiv r^{y'}s^{z'}x + x' \pmod{m},$$

$$y'' \equiv y + y' \pmod{p},$$

and

$$z'' \equiv z + z' \pmod{p}.$$

The multiplication defined above is associative, for

$$[x, y, z]\{[x', y', z'][x'', y'', z'']\} = [x, y, z][r^{y''}s^{z''}x' + x'', y' + y'', z' + z''] =$$
$$= [r^{y'+y''}s^{z'+z''}x + r^{y''}s^{z''}x' + x'', y + y' + y'', z + z' + z'']$$

and

$$\{[x, y, z][x', y', z']\}[x'', y'', z''] = [r^{y'}s^{z'}x + x', y + y', z + z'][x'', y'', z''] =$$
$$= [r^{y''}s^{z''}(r^{y'}s^{z'}x + x') + x'', y + y' + y'', z + z' + z''].$$

Also $[0, 0, 0]$ is the unit element for this multiplication and $[-r^{p-y}s^{p-z}x, p-y, p-z]$ is the inverse of $[x, y, z]$. Therefore H is a group. Moreover, if

$$a' = [1, 0, 0], \quad b' = [0, 1, 0], \quad c' = [0, 0, 1],$$

then it is easy to show that

$$a'^x = [x, 0, 0], \quad b'^y = [0, y, 0], \quad c'^z = [0, 0, z].$$

Thus

$$a'^m = b'^p = c'^p = e.$$

Also

$$a'b' = [1, 0, 0][0, 1, 0] = [r, 1, 0],$$

$$b'a'^r = [0, 1, 0][r, 0, 0] = [r, 1, 0],$$

therefore

$$a'b' = b'a'^r.$$

Similarly

$$a'c' = [1, 0, 0][0, 0, 1] = [s, 0, 1],$$

and

$$c'a'^s = [0, 0, 1][s, 0, 0] = [s, 0, 1],$$

hence

$$a'c' = c'a'^{s'}.$$

Finally

$$b'c' = [0, 1, 0]\,[0, 0, 1] = [0, 1, 1],$$

and

$$c'b' = [0, 0, 1]\,[0, 1, 0] = [0, 1, 1].$$

Thus corresponding to the defining relations of G

$$a'^m = b'^p = c'^p = e, \quad a'b' = b'a'^r, \quad a'c' = c'a'^s, \quad b'c' = c'b'.$$

From this we see that H is a homomorphic image of G. But as the order of H is p^2m and the order of G is at most p^2m, they have the same order and are isomorphic.

§ 3. Groups of the type $T(1, 2)$

Theorem 5. *If there is a group G of the type $T(1, 2)$, then it has the defining relations*

$$(3) \qquad G = \{a, b, c;\ \ a^m = b^p = c^p = e, \quad ab = ba^r, \quad ac = c^u a, \quad bc = cb\}$$

with $u = 2, 3, \ldots, p-1$ *where*

$$(4) \qquad k|m, \quad k|(r-1), \quad r^p \equiv 1 \pmod m$$

k being the order of u modulo p.

Conversely, if m and r satisfy (4), *then the group G generated by a, b and c with the defining relations* (3) *is of the desired type.*

Proof. Assume the existence of the group G. Then since $\{a, b\}$ is of the type G_1 and $\{a, c\}$ is of the type G_2, their defining relations may be written as

$$\{a, b\} = a^m = b^p = e, \quad ab = ba^r, \quad r^p \equiv 1 \pmod m.$$

$$\{a, c\} = a^m = c^p = e, \quad ac = c^u a, \quad u^m \equiv 1 \pmod p,$$

but as k is the order of u modulo p, it follows that m is a multiple of k. Moreover $\{b, c\}$ being of order p^2 is Abelian and therefore $bc = cb$. Furthermore, by the associative law in G, $a(bc) = (ab)c$. But

$$a(bc) = a(cb) = (ac)b = c^u ab = c^u ba^r = bc^u a^r,$$

and

$$(ab)c = ba^r c = bc^{u^r} a^r,$$

therefore $u^r \equiv u \pmod p$, and hence k divides $(r-1)$. Thus we have shown that (3) and (4) are necessary.

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

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

where

$$x'' \equiv r^{y'} x + x' \pmod m, \quad y'' \equiv y + y' \pmod p, \quad \text{and} \quad z'' \equiv z + u^x z' \pmod p.$$

The multiplication defined above is associative, for

$$[x, y, z]\{[x', y', z'][x'', y'', z'']\} = [x, y, z][r^{y''}x' + x'', y' + y'', z' + u^{x'}z''] =$$
$$= [r^{y'+y''}x + r^{y''}x' + x'', y + y' + y'', z + u^{x}(z' + u^{x'}z'')]$$

and

$$\{[x, y, z][x', y', z']\}[x'', y'', z''] = [r^{y'}x + x', y + y', z + u^{x}z'][x'', y'', z''] =$$
$$= [r^{y''}(r^{y'}x + x') + x'', y + y' + y'', z + u^{x}z' + u^{r^{y'}x + x'}z''] =$$
$$= [r^{y'+y''}x + r^{y''}x' + x'', y + y' + y'', z + u^{x}z' + u^{x+x'}z'']$$

since $u^{r^{y'}} \equiv u \pmod p$ in virtue of $k|(r-1)$.

Therefore

$$[x, y, z]\,\{[x', y', z'][x'', y'', z'']\} = \{[x, y, z][x', y', z']\}\,[x'', y'', z''].$$

Also $[0, 0, 0]$ is the unit element for this multiplication and $[-r^{p-y}x, p-y, -u^{m-x}z]$ is the inverse element of $[x, y, z]$. Therefore the system H is a group.

Moreover, if

$$a' = [1, 0, 0,] \quad b' = [0, 1, 0], \quad c' = [0, 0, 1]$$

then it is easy to show that

$$a'^{x} = [x, 0, 0], \quad b'^{y} = [0, y, 0], \quad c'^{z} = [0, 0, z].$$

Thus

$$a'^{m} = b'^{p} = c'^{p} = e.$$

Also

$$a'b' = [1, 0, 0][0, 1, 0] = [r, 1, 0], \quad \text{and} \quad b'a'^{r} = [0, 1, 0][r, 0, 0] = [r, 1, 0]$$

therefore

$$a'b' = b'a'^{r}.$$

Moreover

$$a'c' = [1, 0, 0][0, 0, 1] = [1, 0, u], \quad \text{and} \quad c'^{u}a' = [0, 0, u][1, 0, 0] = [1, 0, u],$$

hence

$$a'c' = c'^{u}a'.$$

Furthermore

$$b'c' = [0, 1, 0][0, 0, 1] = [0, 1, 1], \quad \text{and} \quad c'b' = [0, 0, 1][0, 1, 0] = [0, 1, 1]$$

therefore

$$b'c' = c'b'.$$

Thus corresponding to the defining relations of G

$$a'^{m} = b'^{p} = c'^{p} = e, \quad a'b' = b'a'^{r}, \quad a'c' = c'^{u}a', \quad b'c' = c'b'.$$

From this, we see that H is a homomorphic image of G. But as the order of H is p^2m and the order of G is at most p^2m, they have the same order and are isomorphic. This completes the proof of the theorem.

§ 4. Groups of the type $T(2, 2)$

Theorem 6. *If there is a group G of the type $T(2, 2)$, then it has the defining relations*

$$(5) \qquad G=\{a, b, c;\, a^m=b^p=c^p=e,\, ab=b^u a,\, ac=c^v a,\, bc=cb\}$$

with $u, v = 2, 3, \ldots, p-1$ *where*

$$(6) \qquad k|m, \quad k'|m,$$

k and k' being the respective orders of u and v modulo p.

Conversely, if m satisfy (6), then the group G generated by a, b and c with the defining relations (5) is of the desired type.

Proof. Assume the existence of the group G. Then, since $\{a, b\}$ and $\{a, c\}$ are both of the type G_2, their defining relations may be written as

$$\{a, b\}=a^m=b^p=e, \quad ab=b^u a, \quad u^m\equiv 1 \pmod p,$$

$$\{a, c\}=a^m=c^p=e, \quad ac=c^v a, \quad v^m\equiv 1 \pmod p.$$

But as k and k' are the respective orders of u and v modulo p, it follows that m is a multiple of both k and k'.

Moreover, $\{b, c\}$, being of order p^2, is Abelian and therefore $bc=cb$. Thus we have shown that (5) and (6) are necessary.

For the converse, we call again the system H of all formal triples $[x, y, z]$ where multiplication is here defined by means of the formulae

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

where

$$x''\equiv x+x' \pmod m, \quad y''\equiv y+u^x y' \pmod p, \quad \text{and} \quad z''\equiv z+v^x z' \pmod p.$$

Following the same pattern of proof as in Theorem 4 and 5, we can easily show that this multiplication is associative. Also $[0, 0, 0]$ is the unit element and $[m-x, -u^{m-x}y, -v^{m-x}z]$ is the inverse of $[x, y, z]$. Therefore the system H is a group. Moreover, if $a'=[1, 0, 0]$, $b'=[0, 1, 0]$ and $c'=[0, 0, 1]$, then it is easy to show that

$$a'^m=b'^p=c'^p=e, \quad a'b'=b'^u a', \quad a'c'=c'^v a', \quad b'c'=c'b'.$$

Thus H is a homomorphic image of G. But as the order of H is p^2m and the order of G is at most p^2m, they have the same order and are isomorphic.

§ 5. Conclusion

The preceding arguments show that finite groups with three independent generators two of which being of order p exist, the structure of such groups is described in Theorems 4,5 and 6. Among these groups, that one described in Theorem 4 with $r\equiv 1 \pmod m$, $s\equiv 1 \pmod m$ namely $\{a, b, c;\, a^m=b^p=c^p=e,\, ab=ba,\, ac=ca,\, bc=cb\}$ this group provides the direct product of $\{a\}$, $\{b\}$ and $\{c\}$ which is Abelian.

References

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

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

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

[4] K. R. Yacoub, On the general products of two finite cyclic groups one of which being of order p^2, *Publ. Math. Debrecen* **6** (1959), 26—39.

[5] K. R. Yacoub, On the general products of two finite cyclic groups one being of odd prime order, *Bull. Fac. Sci. Alexandria* **2** (1958), 15—22.

(Received May 30, 1963.)