On classification of finite groups with four generators three of which having orders p, p, q $(p<q)$ I

By K. R. YACOUB (Cairo)

Finite groups with two independent generators attracted the attention of authors for several years. The author (having started on such groups (1)) discussed later on the existence and the structure of finite groups with three generators one being of arbitrary order and the other two having given orders (2), (3) and others.

Recently, the author (4) started the problem of finite groups with four generators a, b, c and d when b, c and d have the same odd prime order p.

It is the object of the present paper to deal with a similar problem when the given orders are p, p and q with $p<q$. Throughout this paper, the order m of a is arbitrary but $m \notin \{p, q\}$. The case $p>q$ together with the particular case when $m \in \{p, q\}$ will be kept to a further discussion.

The present paper consists actually of two main parts, the first deals with the case p does not divide $q-1$ while the second deals with the case p divides $q-1$.

1. Notation and Preliminaries

Throughout this paper the symbol e denotes the identity of the group unless otherwise stated. Various parameters namely λ, μ and ν are used frequently where

$$\lambda, \mu \in \{2, \ldots, p-1\}, \quad \text{i.e.} \quad \lambda, \mu \not\equiv 1 \pmod{p},$$

$$\nu \in \{2, \ldots, q-1\} \quad \text{i.e.} \quad \nu \not\equiv 1 \pmod{q}.$$

We introduce k, k' and k^* as the respective orders of

$$\lambda \bmod p, \quad \mu \bmod p, \quad \nu \bmod q.$$

Thus $\lambda^k \equiv 1 \pmod{p}$, $\mu^{k'} \equiv 1 \pmod{p}$, $\nu^{k^*} \equiv 1 \pmod{q}$. It should be noted that $k, k', k^* > 1$.

Two other parameters, denoted by ω, ω', are used mainly in the second part of the paper where

$$\omega, \omega' \in \{1, 2, \ldots, q-1\}.$$

It may be noted that possibly $\omega, \omega' \equiv 1 \pmod{q}$, but $\nu \not\equiv 1 \pmod{q}$.

Finally, for positive integers x, y and z, we use the symbol $[x, y]$ for the L.C.M. of x and y while the symbol $[x, y, z]$ is used for the L.C.M. of x, y and z.

The two following theorems, due to the author (3), are stated here without proof mainly for subsequent use.

Theorem 1. *Let p and q be two distinct odd primes such that*

$$\text{(i)}\quad p < q, \qquad \text{(ii)}\quad p \text{ does not divide } q-1.$$

Then, for $m \notin \{p, q\}$, there exist four types of groups with three generators a, b, d of respective orders m, p and q. These groups which we denote by M_i: $i=1, 2, 3, 4$ are

$$M_1 = \{a, b, d;\ a^m = b^p = d^q = e,\ ab = ba^r,\ ad = da^t,\ bd = db\}$$

with

$$r^p \equiv 1 \equiv t^q \pmod{m},$$

$$M_2 = \{a, b, d;\ a^m = b^p = d^q = e,\ ab = ba^r,\ ad = d^v a,\ bd = db\}$$

with

$$r^p \equiv 1 \pmod{m},\ k^* | [m, r-1],$$

$$M_3 = \{a, b, d;\ a^m = b^p = d^q = e,\ ab = b^\lambda a,\ ad = da^t,\ bd = db\}$$

with

$$t^q \equiv 1 \pmod{m},\quad k | [m, t-1],$$

$$M_4 = \{a, b, d,\ a^m = b^p = d^q = e,\ ab = b^\lambda a,\ ad = d^v a,\ bd = db\}$$

with

$$[k, k^*] | m.$$

Cor. 1. *Groups of the types M_2, M_3 and M_4 do not exist for $m=p$.* For M_2, if $m=p$, then $k^* | p$ implies $k^*=p$ since $v \not\equiv 1 \pmod{q}$ and its order mod q, namely $k^* > 1$. Thus $v^p \equiv 1 \pmod{q}$ which implies $v \equiv 1 \pmod{q}$ since p does not divide $q-1$. This obvious contradiction shows that M_2 does not exist. Similar arguments apply for M_3 and M_4.

Cor. 2. *The group M_1 exists when $m=p$ and is Abelian.* For, in this case, we have $r^p \equiv 1 \pmod{p}$ which implies, on using Fermat's Theorem, $r \equiv 1 \pmod{p}$. Also $t^q \equiv 1 \pmod{p}$ implies $t \equiv 1 \pmod{p}$; this in fact follows directly if we observe that $q > p$ and that the odd prime q cannot be a multiple of the even number $p-1$ which contradicts the fact that $t^{p-1} \equiv 1 \pmod{p}$.

For the sake of later quotation, we replace a by c, we thus have

Cor. 3. *Let p and q be two distinct odd primes with $p < q$ and p is not a divisor of $q-1$. Then only one group $\{b, c, d\}$ exists with three generators having orders p, p and q, and this group is Abelian.*

Theorem 1*; *Let p and q be two distinct odd primes such that*

$$\text{(i)}\quad p < q, \qquad \text{(ii)}\quad p \text{ divides } q-1.$$

Then there exist four types of groups with three generators a, b, d of orders m, p, q with m arbitrary such that $m \notin \{p, q\}$. These groups are

$$M_1^* = \{a, b, d;\ a^m = b^p = d^q = e,\ ab = ba^r,\ ad = da^t,\ bd = d^\omega b,$$

with

$$r^p \equiv 1 \equiv t^{f(\omega)} \pmod m, \quad \omega^p \equiv 1 \pmod q, \quad f(\omega) = \begin{cases} q & \text{if } \omega = 1 \\ 1 & \text{if } \omega \neq 1 \end{cases}$$

$$M_2^* = \{a, b, d;\ a^m = b^p = d^q = e,\ ab = ba^r,\ ad = d^v a,\ bd = d^\omega b$$

with

$$v \not\equiv 1 \pmod q, \quad r^p \equiv 1 \pmod m, \quad \omega^p \equiv 1 \pmod q, \quad k^* | [m, r-1],$$

$$M_3^* = \{a, b, d;\ a^m = b^p = d^q = e,\ ab = b^\lambda a,\ ad = da^t,\ bd = db\}$$

with

$$\lambda \not\equiv 1 \pmod p, \quad t^q \equiv 1 \pmod m, \quad k | [m, t-1],$$

$$M_4^* = \{a, b, d;\ a^m = b^p = d^q = e,\ ab = b^\lambda a,\ ad = d^v a,\ bd = db\}$$

with

$$\lambda \not\equiv 1 \pmod p, \quad v \not\equiv 1 \pmod q, \quad [k, k^*] | m.$$

Remark 1. The defining relations of M_1^*, originally given by the author, seperate the two cases $\omega=1$ and $\omega\not\equiv 1$, but for further and easier application they are combined together by the introduction of the function f.

Remark 2. From Theorem 1* (when p divides $q-1$) and Theorem 1 (when p does not divide $q-1$), we observe that

(i) $M_3 = M_3^*$, (ii) $M_4 = M_4^*$, (iii) $M_1 = M_1^*$ with $\omega = 1$,

iv) $M_2 = M_2^*$ with $\omega = 1$.

Cor. 1*. *Groups of the types M_3^* and M_4^* do not exist for $m=p$.* This result follows immediately as in Cor. 1 if we use Remark 1 (i), (ii).

Cor. 2*. *Groups of the types M_1^* and M_2^* exist when $m=p$.* For by taking $m=p$ in M_1^*, we have $r^p\equiv 1 \pmod p$ which implies directly $r\equiv 1 \pmod p$. Moreover $t^{f(\omega)}\equiv 1 \pmod p$ implies always $t\equiv 1 \pmod p$ whether $\omega\equiv 1$ or $\omega\not\equiv 1 \pmod q$. This result is immediate for $\omega\not\equiv 1 \pmod q$ from the definition of f. Also by definition of f, we have $f(1)=q$ and hence $t^q\equiv 1 \pmod p$. But if we remark again that the odd prime q cannot be a multiple of the even $p-1$, it follows directly that $t\equiv 1 \pmod q$. In this case $M_1^*=\{a, b, d;\ a^m=b^p=d^q=e,\ ab=ba,\ ad=da,\ bd=db\}$.

Moreover, by taking $m=p$ in M_2^*, we have again $r\equiv 1 \pmod p$ and $k^*|p$ implies $k^*=p$ since $k^*>1$. Thus $v^p\equiv 1 \pmod q$ and M_2^* will be

$$M_2^* = \{a, b, d;\ a^p = b^p = d^q = e,\ ab = ba,\ ad = d^v a,\ bd = d^\omega b\},$$

with $v\not\equiv 1 \pmod q$, $\omega^p\equiv 1\equiv v^p \pmod q$.

Moreover, if we observe that the two elements a, b (being of the same order) play the same role in the structure of the group, then $\omega\not\equiv 1 \pmod q$. Replacing a by c and v by ω' we have thus shown

Cor. 3*. *Let p and q be two distinct odd primes such that $p<q$ and p divides $q-1$. Then there exist two groups with three generators b, c, d of orders p, p, q re-*

spectively. One of these groups is Abelian and the other is non-Abelian namely

$$\{b, c, d;\ b^p = c^p = d^q = e,\ bc = cb,\ bd = d^\omega b,\ cd = d^{\omega'} c\}$$

with

$$\omega, \omega' \not\equiv 1 \pmod{q}, \quad \omega^p = 1 \equiv \omega'^p \pmod{q}.$$

Part I. The case p does not divide $q-1$

Let G be a finite group with four generators a, b, c and d whose orders are respectively m (arbitrary), p, p and q where p and q are two distinct odd primes such that $p<q$ and p does not divide $q-1$. Then

$$a^m = b^p = c^p = d^q = e.$$

Now since p does not divide $q-1$, then by Cor. 3 the subgroup $\{b, c, d\}$ is always Abelian. But the two subgroups $\{a, b, d\}$ and $\{a, c, d\}$ may be any one of the four types M_1, M_2, M_3 and M_4 which are described in Theorem 1. Thus ten cases may arise and the corresponding groups, if they exist, may be listed in the following table.

Table 1. The case p does not divide $q-1$

Type of $\{a, b, d\}$	Type of $\{a, c, d\}$	Type of $G=\{a, b, c, d\}$
M_1	M_1	$T(1, 1)$
M_1	M_2	$T(1, 2)$
M_1	M_3	$T(1, 3)$
M_1	M_4	$T(1, 4)$
M_2	M_2	$T(2, 2)$
M_2	M_3	$T(2, 3)$
M_2	M_4	$T(2, 4)$
M_3	M_3	$T(3, 3)$
M_3	M_4	$T(3, 4)$
M_4	M_4	$T(4, 4)$

Remark 1. It should be remarked that other types may arise but they are not actually distinct from the above types. For example, the type $T(2, 1)$ arises when the subgroup $\{a, b, d\}$ is of the type M_2 while the subgroup $\{a, c, d\}$ is of the type M_1. Such a type is exactly the same as the type $T(1, 2)$ if we just interchange the two generators b and c which have the same order p.

Remark 2. Groups of the types $T(1, 2)$ and $T(1, 4)$ do not exist. For such two types, the subgroup $\{a, b, d\}$ is of the type M_1 for which $ad=da^t$, while the subgroup $\{a, c, d\}$ is either of the type M_2 or M_4 for both of which $ad=d^v a$ with $v\not\equiv 1 \pmod{q}$. This obvious contradiction shows that no such types of groups exist.

Remark 3. Groups of the types $T(2, 3)$ and $T(3, 4)$ do not exist. Similar arguments apply as in the previous remark. Thus it remains to discuss the existence of the six types

$$T(i, i): i = 1, 2, 3, 4 \quad \text{and} \quad T(1, 3), T(2, 4).$$

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

$$(1)\quad G = \{a, b, c, d;\ a^m = b^p = c^p = d^q = e,\ ab = ba^r,\ ac = ca^s,\ ad = da^t,$$
$$bc = cb,\ bd = db,\ cd = dc\}$$

where

$$(2)\qquad r^p \equiv s^p \equiv t^p \equiv 1 \pmod m.$$

Conversely, if r, s and t satisfy (2), *then the group G generated by a, b, c and d with the derining relations* (1) *is of the required type.*

Proof. Assume the existence of a group G of the type $T(1, 1)$. Then, for such a group, the two subgroups $\{a, b, d\}$ and $\{a, c, d\}$ are both of the same type M_1 for which we have by Theorem 1

$$\{a, b, d;\ a^m = b^p = d^q = e,\ ab = ba^r,\ ad = da^t,\ bd = db\},$$
$$\{a, c, d;\ a^m = c^p = d^q = e,\ ac = ca^s,\ ad = da^t,\ cd = dc\},$$

with

$$r^p \equiv 1 \equiv t^q \pmod m,\quad s^p = 1 = t^q \pmod m.$$

Moreover, the subgroup $\{b, c, d\}$ is by Cor. 1, Abelian and $bc=cb$. Thus we have shown that (1) and (2) are necessary.

For the converse, let K be the system of all formal quadruples $[x, y, z, w]$ where x is taken mod m, y and z taken mod p and w mod q. In this system define multiplication by means of the formulae

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

where

$$x'' \equiv r^{y'} s^{z'} t^{w'} x + x' \pmod m,$$
$$y'' \equiv y + y',\quad z'' \equiv z + z' \pmod p,$$
$$w'' \equiv w + w' \pmod q.$$

This multiplication is associative, for

$$([x, y, z, w][x', y', z', w'])[x'', y'', z'', w''] =$$
$$= [r^{y'} s^{z'} t^{w'} x + x', y + y', z + z', w + w'][x'', y'', z'', w''] =$$
$$= [r^{y''} s^{z''} t^{w''} (r^{y'} s^{z'} t^{w'} x + x') + x'', y + y' + y'', z + z' + z'', w + w' + w''] =$$
$$= [r^{y' + y''} s^{z' + z''} t^{w' + w''} x + r^{y''} s^{z''} t^{w''} x' + x'', y + (y' + y''), z + (z' + z''), w + (w' + w'')] =$$
$$= [x, y, z, w][r^{y''} s^{z''} t^{w''} x' + x'', y' + y'', z' + z'', w' + w''] =$$
$$= [x, y, z, w][(x', y', z', w'][x'', y'', z'', w'']).$$

Also $e' = [0, 0, 0, 0]$ is the unit element for this multiplication and the element $[-r^{p-y} s^{p-z} t^{q-w} x, p-y, p-z, q-w]$ is the inverse of $[x, y, z, w]$. Thus the system K is a group of order $p^2 qm$. Moreover, if

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

then, corresponding to the defining relations of G, it is easily shown

$$a'^m = b'^p = c'^p = d'^q = e',\ a'b' = b'a'^r,\ a'c' = c'a'^s,\ a'd' = d'a'^t,$$
$$b'c' = c'b',\quad b'd' = d'b',\quad c'd' = d'c'.$$

In fact, apart from the first four and last three obvious relations, we have

$$a'b' = [1, 0, 0, 0][0, 1, 0, 0] = [r, 1, 0, 0] = [0, 1, 0, 0][r, 0, 0, 0] = b'a'^r,$$
$$a'c' = [1, 0, 0, 0][0, 0, 1, 0] = [s, 0, 1, 0] = [0, 0, 1, 0][s, 0, 0, 0] = c'a'^s,$$
$$a'd' = [1, 0, 0, 0][0, 0, 0, 1] = [t, 0, 0, 1] = [0, 0, 0, 1][t, 0, 0, 0] = d'a'^t.$$

Therefore the group K is a homomorphic image of G. But as the order of K is p^2qm and the order of G is at most p^2qm, they have the same order and are isomorphic. This shows that a group of the required type exists.

Theorem 3. *If there is group G of the type $T(2, 2)$, then it has the defining relations*

$$(3)\quad G = \{a, b, c, d;\ a^m = b^p = c^p = d^q = e,\ ab = ba^r,\ ac = ca^s,\ ad = d^v a,$$
$$bc = cb,\quad bd = db,\quad cd = dc\}$$

with $v \not\equiv 1 \pmod q$ *and*

$$(4)\qquad r^p \equiv 1 \equiv s^p \pmod m,\quad k^* | [m, r-1],\ k^* | [m, s-1].$$

Conversely, if r, s and k^* (the order of v mod q) satisfy (4), *then the group G generated by a, b, c and d with the defining relations* (3) *is of the desired type.*

Proof. Assume the existence of a group G of the type $T(2, 2)$. Then for such a group, the two subgroups $\{a, b, d\}$ and $\{a, c, d\}$ are both of the same type M_2 for which we have by Theorem 1

$$\{a, b, d;\ a^m = b^p = d^q = e,\ ab = ba^r,\ ad = d^v a,\ bd = db\},$$
$$r^p \equiv 1 \pmod m,\quad k^* | [m, r-1],$$
$$\{a, c, d;\ a^m = c^p = d^q = e,\ ac = ca^s,\ ad = d^v a,\ cd = dc\},$$
$$s^p \equiv 1 \pmod m,\quad k^* | [m, s-1].$$

Moreover $bc = cb$ since the subgroup $\{b, c, d\}$ is Abelian by Cor. 1. Thus we have shown that (3) and (4) are necessary.

For the converse, we use the same system K of all formal quadruples les $[x, y, z, w]$ of the previous theorem but with the multiplication formulae

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

where

$$x'' \equiv r^{y'} s^{z'} x + x' \pmod m,$$
$$y'' \equiv y + y',\quad z'' \equiv z + z' \pmod p,$$
$$w'' \equiv w + v^x w' \pmod q.$$

This multiplication is associative, for

$$([x, y, z, w][x', y', z', w'])[x'', y'', z'', w''] =$$

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

$$= [r^{y''} s^{z''}(r^{y'} s^{z'} x+x')+x'', y+y'+y'', z+z'+z'', w+v^x w'+v^X w''],$$

$$(X = r^{y'} s^{z'} x+x',\ v^X \equiv v^{x+x'} \pmod q \quad \text{in virtue of}$$

$$v^r \equiv v,\ v^s \equiv v \pmod q \text{ since } k^*|\, r-1,\ k^*|\, s-1) =$$

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

$$= [x, y, z, w]([x', y', z', w'][x'', y'', z'', w'']).$$

Again $e'=[0, 0, 0, 0]$ is the unit element for this multiplication and the element $[-r^{p-y} s^{p-z} x, p-y, p-z, -v^{-x} w]$ is the inverse of the the element $[x, y, z, w]$ in virtue of (4).

Therefore the system K is again a group of order p^2qm. Moreover if

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

then, corresponding to the defining relations of G, it is easily shown

$$a'^m = b'^p = c'^p = d'^q = e',\ a'b' = b'a'^r,\ a'c' = c'a'^s,\ a'd' = d'^v a',$$

$$b'c' = c'b', \quad b'd' = d'b', \quad c'd' = d'c'.$$

Apart from the first four and last three direct relations, we have

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

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

$$a'd' = [1, 0, 0, 0][0, 0, 0, 1] = [1, 0, 0, v] = [0, 0, 0, v][1, 0, 0, 0] = d'^v a'.$$

Thus the group K is a homomorphic image of G. But as the order of K is p^2qm and the order of G is at most p^2qm, they have the same order and are isomorphic. This proves the existence of a group of the required type.

Theorem 4. *If there is a group G of the type $T(3, 3)$, then it has the defining relations*

$$(5) \quad G = \{a, b, c, d;\ a^m = b^p = c^p = d^q = e,\ ab = b^\lambda a,\ ac = c^\mu a,\ ad = da^t,$$

$$bc = c\ b,\ bd = db, \quad cd = dc\},$$

with $\lambda, \mu \not\equiv 1 \pmod p$ *and*

$$(6) \qquad t^q \equiv 1 \pmod p, \quad k|\,[m, t-1],\ k'|\,[m, t-1].$$

Conversely if t and k, k' (the respective orders of λ, $\mu \bmod p$) satisfy (6), *then the group G generated by a, b, c and d with the defining relations* (5) *is of the desired type.*

PROOF. Assume the existence of a group G of the type $T(3, 3)$. Then, for such a group, the two subgroups $\{a, b, d\}$ and $\{a, c, d\}$ are both of the type M_3 for

which we have by Theorem 1

$$\{a, b, d;\ a^m = b^p = d^q = e,\ ab = b^\lambda a,\ ad = da^t,\ bd = db\},$$

with

$$t^q \equiv 1 \pmod m, \quad k|[m, t-1];$$

$$\{a, c, d;\ a^m = c^p = d^q = e,\ ac = c^\mu a,\ ad = da^t,\ cd = dc\},$$

with

$$t^q \equiv 1 \pmod m, \quad k'|[m, t-1].$$

Again since the subgroup $\{b, c, d\}$ is Abelian, then $bc=cb$. Thus we have shown that (5) and (6) are necessary.

For the converse, we use again the same system K of the previous theorems but with the multiplication formulae

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

where

$$x'' \equiv t^{w'} x + x' \pmod m,$$

$$y'' \equiv y + \lambda^x y', \quad z'' \equiv z + \mu^x z' \pmod p,$$

$$w'' \equiv w + w' \pmod q.$$

Following a similar procedure, it is easily shown that the system K is again a group under this multiplication, which is isomorphic to the group of the required type.

Theorem 5. *If there is a group G of the type $T(4, 4)$, then it has the defining relations*

(7) $$G = \{a, b, c, d;\ a^m = b^p = c^p = d^q = e,\ ab = b^\lambda a,\ ac = c^\mu a,\ ad = d^\nu a,$$
$$bc = cb,\ bd = db,\ cd = dc\},$$

where $\lambda, \mu \not\equiv 1 \pmod p$, $\nu \not\equiv 1 \pmod q$ *and*

(8) $$[k, k', k^*]|m.$$

Conversely, if k, k' and k^* (the respective orders of $\lambda \bmod p$, $\mu \bmod p$ and $\nu \bmod q$), then the group G generated by a, b, c and d with the defining relations (7) *is of the desired type.*

PROOF. Assume the existence of a group of the type $T(4, 4)$. Then for such a group the two subgroups $\{a, b, d\}$ and $\{a, c, d\}$ are both of the same type M_4 described in Theorem 1 and the necessity of conditions (7) and (8) is direct.

For the converse, we use again the same system K of all formal quadruples $[x, y, z, w]$ but with the multiplication formulae

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

where

$$x'' \equiv x + x' \pmod m,$$

$$y'' \equiv y + \lambda^x y', \quad z'' \equiv z + \mu^x z' \pmod p,$$

$$w'' = w + \nu^x w' \pmod q.$$

By using a similar procedure, it is easily shown that the system K is a group of order p^2qm which is isomorphic to the group G of the type required.

Theorem 6. *If there is a group G of the type $T(1, 3)$, then it has the defining relations*

$$(9)\quad G=\{a, b, c, d;\ a^m=b^p=c^p=d^q=e,\ ab=ba^r,\ ac=c^\mu a,\ ad=da^t,\ bc=cb,\ bd=db,\ cd=dc\}.$$

with $\mu\not\equiv 1 \pmod p$, *and*

$$(10)\quad r^p\equiv 1\equiv t^q \pmod m,\quad k'|[m, t-1].$$

Conversely, if r, t and k' (the order of $\mu \bmod p$), then the group G generated by a, b, c, d with the defining relations (9) *is of the desired type.*

Proof. Assume the existence of a group G of the type $T(1, 3)$. Then, for such a group the subgroup $\{a, b, d\}$ is of the type M_1 while the subgroup $\{a, c, d\}$ is of the type M_3. Thus by Theorem 1, we have

$$\{a, b, d;\ a^m=b^p=d^q=e,\ ab=ba^r,\ ad=da^t,\ bd=db\}$$

with

$$r^p\equiv 1\equiv t^q \pmod m$$

$$\{a, c, d;\ a^m=c^p=d^q=e,\ ac=c^\mu a,\ ad=da^t,\ cd=dc\}$$

with

$$t^q\equiv 1 \pmod m,\quad k'|[m, t-1].$$

Again $bc=cb$ as the subgroup $\{b, c, d\}$ is Abelian.

For the converse, we use the multiplication formulae

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

with

$$x''\equiv r^{y'}t^{w'}x+x' \pmod m,$$

$$y''\equiv y+y',\quad z''\equiv z+\mu^x z' \pmod p,$$

$$w''\equiv w+w' \pmod q.$$

Again by using a similar procedure, it can be easily shown that, under this multiplication, the system K is a group of order p^2qm which is isomorphic to the group G of the required type.

Theorem 7. *If there is a group G of the type $T(2, 4)$, then it has the defining relations*

$$(11)\quad G=\{a, b, c, d;\ a^m=b^p=c^p=d^q=e,\ ab=ba^r,\ ac=c^\mu a,\ ad=d^\nu a,\ bc=cb,\ bd=db,\ cd=dc\},$$

where $\mu\not\equiv 1 \pmod p$, $\nu\not\equiv 1 \pmod q$ and

$$(12)\quad r^p\equiv 1 \pmod m,\quad [k', k^*]|m,\ k'|r-1,\ k^*|[m, r-1].$$

Conversely, if r and k', k^* (the respective orders of $\mu \bmod p$ and $\nu \bmod q$) satisfy (12), *then the group G generated by a, b, c, d with the defining relations* (11) *is of the desired type.*

PROOF. The necessity of the conditions*) is direct if we observe that for the type $T(2, 4)$, the subgroups $\{a, b, d\}$ and $\{a, c, d\}$ are respectively of the types M_2 and M_4 described in Theorem 1.

For the converse, we use the multiplication formulae

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

with

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

$$y'' \equiv y + y' \pmod{p}, \quad z'' = z + \mu^x z' \pmod{p}, \quad w'' = w + v^x w' \pmod{q}$$

in the system K of all formal quadruples $[x, y, z, w]$.

Part II. The case p divides $q-1$

Let G be a finite group with four generators a, b, c, d whose orders are respectively m (arbitrary), p, p, q where p and q are distinct odd primes such that p divides $q-1$. Then

$$a^m = b^p = c^p = d^q = e.$$

By Cor. 3*, the subgroup $\{b, c, d\}$ is either Abelian or non-Abelian. Thus, corresponding to the Abelian or non-Abelian type, ten types of the group G may arise according as the subgroups $\{a, b, d\}$ and $\{a, c, d\}$ may be any of the types M_i^*: $i=1, 2, 3, 4$ described in Theorem 1*. These types, if they exist, may be arranged in the following table.

*Table 1**. The case p divides $q-1$

Type of $\{a, b, d\}$	Type of $\{a, c, d\}$	Type of $\{b, c, d\}$	Type of $G=\{a, b, c, d\}$
M_1^*	M_1^*	Abelian[non-Abelian]	$T^*(1, 1)[P^*(1, 1)]$
M_1^*	M_2^*	Abelian[non-Abelian]	$T^*(1, 2)[P^*(1, 2)]$
M_1^*	M_3^*	Abelian[non-Abelian]	$T^*(1, 3)[P^*(1, 3)]$
M_1^*	M_4^*	Abelian[non-Abelian]	$T^*(1, 4)[P^*(1, 4)]$
M_2^*	M_2^*	Abelian[non-Abelian]	$T^*(2, 2)[P^*(2, 2)]$
M_2^*	M_3^*	Abelian[non-Abelian]	$T^*(2, 3)[P^*(2, 3)]$
M_2^*	M_4^*	Abelian[non-Abelian]	$T^*(2, 4)[P^*(2, 4)]$
M_3^*	M_3^*	Abelian[non-Abelian]	$T^*(3, 3)[P^*(3, 3)]$
M_3^*	M_4^*	Abelian[non-Abelian]	$T^*(3, 4)[P^*(3, 4)]$
M_4^*	M_4^*	Abelian[non-Abelian]	$T^*(4, 4)[P^*(4, 4)]$

Remark 1. Other types may arise but they are, in fact, not distinct from the above types.

Remark 2. Groups of the types $T^*(1, 2)$ and $T^*(1, 4)$ do not exist.
Groups of the types $P^*(1, 2)$ and $P^*(1, 4)$ do not exist.

Remark 3. Groups of the types $T^*(2, 3)$ and $P^*(2, 3)$ do not exist.

*) The third of these relations follows in fact from the associative property in G. In fact, we have $a(bc)=a(cb)=c^\mu ab=c^\mu ba^r$, $(ab)c=ba^r c=bc^{\mu^r}a^r=c^{\mu^r}ba^r$. Thus $\mu^r \equiv \mu \pmod{m}$ or equivalently $\mu^{r-1}\equiv 1 \pmod{m}$ since $(\mu, m)=1$. Hence $k' | r-1$.

Remark 4. Groups of the types $T^*(3, 4)$ and $P^*(3, 4)$ do not exist.
For groups of the types $P^*(1, 2)$, $T^*(\ldots, \ldots)$ mentioned in the above remarks, arguments similar to those used when p does not divide $q-1$ apply. But for the types $P^*(\ldots, \ldots)$, if they exist, a direct contradiction arises if we observe that $cd=dc=d^{\omega'}c$ with $\omega' \not\equiv 1 \pmod q$.

Theorem 8. *Let p and q be two distinct odd primes such that p divides $q-1$. Then groups of the types*

$$T^*(i, i): i = 1, 2, 3, 4 \quad \textit{and} \quad T^*(1, 3),\ T^*(2, 4)$$

exist and have the same structure as the corresponding groups when p does not divide $q-1$. In other words

$$T^*(i, i) = T(i, i): i = 1, 2, 3, 4 \quad \textit{and} \quad T^*(1, 3) = T(1, 3),\quad T^*(2, 4) = T(2,4).$$

This becomes obvious if we observe that for the types $T^*(\ldots, \ldots)$ the subgroup $\{b, c, d\}$ is Abelian which is just the case with the corresponding groups $T(\ldots, \ldots)$ when p does not divide $q-1$. This implies directly that $bd=db$ and accordingly, in the defining relations of M_1^* and M_2^*, we must have $\omega \equiv 1 \pmod q$. In this case

$$M_1^* = M_1, \quad M_2^* = M_2.$$

This combines together with the fact that, we have always (Remark 2(i), (ii)) $M_3^* = M_3$, $M_4^* = M_4$ to make the theorem direct and immediate. Now, it remains to discuss the existence of the groups $P^*(\ldots, \ldots)$ which arise when the subgroup $\{b, c, d\}$ is non-Abelian namely (Cor. 3*)

$$\{b, c, d;\ b^p = c^p = d^q = e,\ bc = cb,\ bd = d^{\omega} b,\ cd = d^{\omega'} c\}$$

with $\omega, \omega' \not\equiv 1 \pmod q$ and

$$\omega^p \equiv 1 \equiv \omega'^p \pmod q.$$

Remarks 2*, 3*, 4* show that groups of the types $P^*(1, 2)$, $P^*(1,4)$, $P^*(2, 3)$ and $P^*(3, 4)$ do not exist. In addition, we prove

Theorem 9. *Groups of the types $P^*(1, 3)$ and $P^*(2, 4)$ do not exist. For both types, if they exist, the subgroup $\{a, c, d\}$ is either of the type M_3^* or M_4^* for both of which we have $cd=dc$ which contradicts the fact that $cd=d^{\omega'}c$ with $\omega' \not\equiv 1 \pmod q$ from the defining relations of the subgroup $\{b, c, d\}$.*

Thus it remains to discuss the existence of the four types $P^*(i, i)$ for $i=1, 2, 3, 4$.

Theorem 10. *Groups of the types $P^*(3, 3)$ and $P^*(4, 4)$ do not exist. For both types of groups, if they exist, the subgroup $\{b, c, d\}$ is non-Abelian for which $bc=c^{\omega}b$ with $\omega \not\equiv 1 \pmod q$. But for both types the subgroup $\{a, b, c\}$, being either of the type M_3^* or M_4^*, has among its defining relations $bc=cb$. This obvious contradiction shows that groups of the types $P^*(3, 3)$ and $P^*(4, 4)$ do not exist.*

Theorem 11. *If there is a group G of the type $P^*(1, 1)$, then it has the defining relations*

$$(13)\quad G = \{a, b, c, d;\ a^m = b^p = c^p = d^q = e,\ ab = ba^r,\ ac = ca^s,\ ad = da,$$
$$bc = cb,\ bd = d^\omega b,\ cd = d^{\omega'} c,$$

where $\omega, \omega' \not\equiv 1 \pmod q$ *and*

$$(14)\quad r^p \equiv 1 \equiv s^p \pmod m,\quad \omega^p \equiv 1 \equiv \omega'^p \pmod q.$$

Conversely, if r, s, ω and ω' satisfy (14), *then the group G generated by a, b, c, d, with the defining relations* (13) *is of the desired type.*

PROOF. Assume the existence of a group G of the type $P^*(1, 1)$. Then, for such a group, the two subgroups $\{a, b, d\}$ and $\{a, c, d\}$ are both of the same type M_1^* which is described in Theorem 1*. Thus we have

$$\{a, b, d;\ a^m = b^p = d^q = e,\ ab = ba^r,\ ad = da^t,\ bd = d^\omega b\}$$

with

$$r^p \equiv 1 \equiv t^{f(\omega)} \pmod m,\quad \omega^p \equiv 1 \pmod q,\quad f(\omega) = \begin{cases} q & \text{if } \omega = 1 \\ 1 & \text{if } \omega \neq 1 \end{cases}$$

$$\{a, c, d;\ a^m = c^p = d^q = e,\ ac = ca^s,\ ad = da^t,\ cd = d^{\omega'} c\}$$

with

$$s^p \equiv 1 \equiv t^{f(\omega')} \pmod m,\quad \omega'^p \equiv 1 \pmod q,\quad f(\omega') = \begin{cases} q & \text{if } \omega' = 1 \\ 1 & \text{if } \omega' \neq 1 \end{cases}$$

Also for this type, the subgroup $\{b, c, d\}$ is non-Abelian whose defining relations are by Cor. 3*

$$\{b, c, d;\ b^p = c^p = d^q = e,\ bc = cb,\ bd = d^\omega b,\ cd = d^{\omega'} c$$

with $\omega, \omega' \not\equiv 1 \pmod q$, $\omega^p \equiv 1 \equiv \omega'^p \pmod q$. Now, since $\omega, \omega' \not\equiv 1 \pmod q$, then by the definition of f, we have

$$f(\omega) = 1,\quad f(\omega') = 1,$$

and consequently $t \equiv 1 \pmod m$.

Thus, in case the group G exists, its defining relations will be

$$G = \{a, b, c, d;\ a^m = b^p = c^p = d^q = e,\ ab = ba^r,\ ac = ca^s,\ ad = da,$$
$$bc = cb,\ bd = d^\omega b,\ cd = d^{\omega'} c,$$

where $\omega, \omega' \not\equiv 1 \pmod q$ and

$$r^p \equiv 1 \equiv s^p \pmod m,\quad \omega^p \equiv 1 \equiv \omega'^p \pmod q.$$

Thus we have shown that (13) and (14) are necessary.

For the converse, we use the same system K of all formal quadruples [x, y, z, w[with the multiplication formulae

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

where

$$x'' \equiv r^{y'} s^{z'} x + x' \pmod{m},$$
$$y'' \equiv y + y', \quad z'' \equiv z + z' \pmod{p},$$
$$w'' \equiv w + \omega^{y} \omega'^{z} w' \pmod{q}.$$

Throug the same procedure which we have used frequently, it is easlily shown that, under this multiplication, the system K is a group of order p^2 q m which is isomorphic to the group G of the required type.

Theorem 12. *If there is a group G of the type* $P^*(2, 2)$, *then it has the defining relations*

$$(15) \quad G = \{a, b, c, d;\ a^m = b^p = c^p = d^q = e,\ ab = ba^r,\ ac = ca^s,\ ad = d^v a,$$
$$bc = cb,\ bd = d^{\omega} b,\ cd = d^{\omega'} c\},$$

where $v, \omega, \omega' \not\equiv 1 \pmod{q}$ *and*

$$(16) \quad r^p \equiv 1 \equiv s^p \pmod{m}, \quad \omega^p \equiv 1 \equiv \omega'^p \pmod{q}, \quad k^* | [m, r-1],\ k^* | [m, s-1].$$

Conversely, if r, s, v, ω, ω' *and* k^* *(the order of* $v \bmod q$*) satisfy* (16), *then the group G generated by a, b, c, d with the defining relations* (15) *is of the desired type.*

Proof. Assume the existence of a group G of the type $P^*(2, 2)$. Then, for such a group, the two subgroups $\{a, b, d\}$ and $\{a, c, d\}$ are both of the same type M_2^* which is described in Theorem 1*. Thus we have

$$\{a, b, d;\ a^m = b^p = d^q = e,\ ab = ba^r,\ ad = da^v,\ bd = d^{\omega} b\},\ v \not\equiv 1 \pmod{q},$$
$$r^p \equiv 1 \pmod{m}, \quad \omega^p \equiv 1 \pmod{q}, \quad k^* | [m, r-1],$$
$$\{a, c, d;\ a^m = c^p = d^q = e,\ ac = ca^s,\ ad = d^v a,\ cd = d^{\omega'} c\},\ v \not\equiv 1 \pmod{q},$$
$$s^p \equiv 1 \pmod{m}, \quad \omega'^p \equiv 1 \pmod{q}, \quad k^* | [m, s-1].$$

Again, by Cor. 3*,

$$\{b, c, d;\ b^p = c^p = d^q = e,\ bc = cb,\ bd = d^{\omega} b,\ cd = d^{\omega'} c\}$$

where $\omega, \omega' \not\equiv 1 \pmod{q}$, $\omega^p \equiv 1 \equiv \omega'^p \pmod{q}$. Thus we have shown that (15) and (16) are necessary.

For the converse, we use the system K of all formal quadruples $[x, y, z, w]$ with the multiplication formulae

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

where

$$x'' \equiv r^{y'} s^{z'} x + x' \pmod{m},$$
$$y'' \equiv y + y', \quad z'' \equiv z + z' \pmod{p},$$
$$w'' \equiv w + v^{x} \omega^{y} \omega'^{z} w' \pmod{q}.$$

It is easily shown that, under this multiplication, the system K is a group of order $p^2 qm$ which is isomorphic to the group G of the required type.

Conclusion. *Finite groups with four generators exist when three of them have the odd prime orders p, p and q. When p is not a divisor of* $q-1$, *there exist six types of groups which are described in Theorems* 2—7. *But when p divides* $q-1$, *there exist eight types of groups which are described in Theorems* 8, 11, 12.

References

[1] K. R. YACOUB, On general products of two finite cyclical groups, *Ph. D. Thesis, London University*, 1953.

[2] K. R. YACOUB, On finite groups with three independent generators, two of which being of odd prime orders, *Publ. Math. (Debrecen)* **11** (1964), 32—38.

[3] K. R. YACOUB, On finite groups with three independent generators, two of which having distinct odd prime orders, *Publ. Math. (Debrecen)* **13** (1966), 9—16.

[4] K. R. YACOUB, On finite groups with four generators three of which being of odd prime order (under publication).

Faculty of Science
Ain Shams University
Abbassia—Cairo