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

By K. R. YACOUB (Trieste)

Finite groups with two independent generators have been widely studied by several authors in the last three decades. Later on the author studied finite groups with three independent generators when two of these generators have given orders [1], [2].

It is the object of the present paper to study the structure of finite groups with four generators three of which have the same odd prime order p. Throughout this paper, the symbol p is used for an odd prime and congruences without explicit modulus are considered to be taken mod p. The symbol e is used throughout to denote the identity element of the group unless otherwise stated.

§ 1. Preliminaries

Theorem 1. *Finite groups with three independent generators exist when two of the generators have the same odd prime order p. Such groups, denoted by H_1, H_2 and H_3 have the defining relations*

H_1: $\{a, b, c;\ a^m = b^p = c^p = e,\ ab = ba^r,\ ac = ca^s,\ bc = cb\}$; $r^p \equiv s^p \equiv 1 \pmod m$,

H_2: $\{a, b, c;\ a^m = b^p = c^p = e,\ ab = ba^r,\ ac = c^u a,\ bc = cb\}$; $u \in \{2, \ldots, p-1\}$,

$k|m, k|r-1$, $r^p \equiv 1 \pmod m$, k *being the order of* $u \bmod p$,

H_3: $\{a, b, c;\ a^m = b^p = c^p = e,\ ab = b^u a,\ ac = c^v a,\ bc = cb\}$; $u, v \in \{2, \ldots, p-1\}$,

$k|m, k'|m, k$ *and* k' *being the orders of* u *and* $v \bmod p$.

PROOF. The proof of this theorem was given in 1964 by the author [1].

Corollary 1. *The only finite group with three independent generators having the same order p is an Abelian group.*

For if we take $m=p$ in H_1, we have

$$r^p \equiv 1, \quad s^p \equiv 1 \pmod p$$

which, on using Fermat's Theorem, imply directly $r \equiv s \equiv 1 \pmod{p}$ and H_1 will be an Abelian group in this case.

But if we take $m=p$ in H_2 we have $k|p$ which if we remember that k divides also $p-1$ implies at once $k=1$. Thus $u=1$ which leads to a contradiction as $u \in \{2, \ldots, p-1\}$. Hence no group of the type H_2 exists when $m=p$. Similar argument applies for H_3 when $m=p$. This completes the proof.

§ 2. Description of the problem

Let G be a finite group with four independent generators a, b, c and d of orders m (arbitrary), p, p, p respectively. Then we have

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

By the above corollary, the subgroup $\{b, c, d\}$ is an Abelian group of order p^3. But the subgroups $\{a, b, c\}$, $\{a, b, d\}$ and $\{a, c, d\}$ may be of the types H_1 or H_2 or H_3 described in the above theorem. Thus ten cases may arise and may be listed in the following table, in case they exist.

Table of expected types of groups

Type of $\{a, b, c\}$	Type of $\{a, b, d\}$	Type of $\{a, c, d\}$	Type of $G=\{a, b, c, d\}$
H_1	H_1	H_1	$T(1, 1, 1)$
H_1	H_1	H_2	$T(1, 1, 2)$
H_1	H_1	H_3	$T(1, 1, 3)$
H_1	H_2	H_2	$T(1, 2, 2)$
H_2	H_2	H_2	$T(2, 2, 2)$
H_3	H_2	H_2	$T(3, 2, 2)$
H_1	H_3	H_3	$T(1, 3, 3)$
H_2	H_3	H_3	$T(2, 3, 3)$
H_3	H_3	H_3	$T(3, 3, 3)$
H_1	H_2	H_3	$T(1, 2, 3)$

REMARK. It should be remarked that other types may arise, but they are not actually distinct from the above types. For example the type $T(2, 2, 1)$ which arises when $\{a, b, c\}$ and $\{a, b, d\}$ are of the same type H_2 while $\{a, c, d\}$ is of the type H_1. This is the same type $T(1, 2, 2)$ if we just interchange the two generators b and d which already have the same order p.

§ 3. Non-existence of certain types

Theorem 2. *No group of the type $T(1, 1, 2)$ or $T(1, 1, 3)$ exists.*

PROOF. For if a group of the type $T(1, 1, 2)$ exists, then the two subgroups $\{a, b, c\}$ and $\{a, b, d\}$ will be of the same type H_1 while the subgroup $\{a, c, d\}$ will be of the type H_2. By Theorem 1, we thus have

$$\text{for } \{a, b, c\}: ab = ba^r, \quad ac = ca^s, \quad bc = cb,$$

$$\text{for } \{a, b, d\}: ab = ba^r, \quad ad = da^t, \quad bd = db,$$

$$\text{for } \{a, c, d\}: ac = ca^s, \quad ad = d^u a, \quad cd = dc; \quad u \in \{2, \ldots, p-1\}$$

for suitable parameter values of r, s and t. Thus

$$ad = da^t, \quad ad = d^u a$$

which leads to a contradiction as $u \in \{2, \ldots, p-1\}$. Hence no group of the type $T(1, 1, 2)$ exists. A similar argument applies for the type $T(1, 1, 3)$.

Theorem 3. *No group of the type $T(2, 2, 2)$ exists.*
For if a group of the type $T(2, 2, 2)$ exists, then the three subgroups $\{a, b, c\}$, $\{a, b, d\}$ and $\{a, c, d\}$ will all be of the same type H_2. By Theorem 1, we have

$$\text{for } \{a, b, c\}: ab = ba^r, \quad ac = c^u a, \quad bc = cb,$$

$$\text{for } \{a, b, d\}: ab = ba^r, \quad ad = d^v a, \quad bd = db,$$

$$\text{for } \{a, c, d\}: ac = ca^s, \quad ad = d^v a, \quad cd = dc,$$

for suitable r, s and where $u, v \in \{2, \ldots, p-1\}$. Thus we have

$$ac = c^u a = ca^s$$

which again leads to a contradiction as $u \in \{2, \ldots, p-1\}$. Hence no group of the type $T(2, 2, 2)$ exists.

Theorem 4. *No group of the types $T(1, 3, 3)$ or $T(2, 3, 3)$ exists.*
For the type $T(1, 3, 3)$, we have by Theorem 1

$$\text{for } \{a, b, c\} \text{ (being of the type } H_1) \quad ab = ba^r, \quad ac = ca^s$$

$$\text{for } \{a, b, d\} \text{ (being of the type } H_3) \quad ab = b^u a, \quad ad = d^v a$$

where $u, v \in \{2, \ldots, p-1\}$ and the contradiction is obvious. A similar contradiction arises if the type $T(2, 3, 3)$ exists.

Theorem 5. *No group of the type $T(1, 2, 3)$ exists.*
For such a type, we have

$$\text{for } \{a, b, c\} \text{ (being of the type } H_1) \quad ab = ba^r, \quad ac = ca^s,$$

$$\text{for } \{a, b, d\} \text{ (being of the type } H_2) \quad ab = ba^r, \quad ad = d^v a,$$

$$\text{for } \{a, c, d\} \text{ (being of the type } H_3) \quad ac = c^u a, \quad ad = d^v a$$

where $u, v \in \{2, \ldots, p-1\}$. A direct contradiction shows that no group of the type $T(1, 2, 3)$ can exist.

Theorems 2—5 show that it remains to discuss the existence of just four types namely $T(1, 1, 1)$, $T(1, 2, 2,)$ $T(3, 3, 3)$ and $T(3, 2, 2)$.

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

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

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 defining relations* (1) *is of the desired type.*

Proof. Assume the existence of a group G of the type $T(1, 1, 1)$. Then the subgroups $\{a, b, c\}$, $\{a, b, d\}$ and $\{a, c, d\}$, being all of the type H_1 have by Theorem 1 the defining relations

$$\{a, b, c\}\colon a^m = b^p = c^p = e,\quad ab = ba^r,\quad ac = ca^s,\quad bc = cb;\quad r^p \equiv s^p \equiv 1 \pmod m,$$

$$\{a, b, d\}\colon a^m = b^p = d^p = e,\quad ab = ba^r,\quad ad = da^t,\quad bd = db;\quad r^p \equiv t^p \equiv 1 \pmod m,$$

$$\{a, c, d\}\colon a^m = c^p = d^p = e,\quad ac = ca^s,\quad ad = da^t,\quad cd = dc;\quad s^p \equiv t^p \equiv 1 \pmod m.$$

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 $x \in \{0, 1, \ldots, m-1\}$ and $y, z, w \in \{0, 1, \ldots, p-1\}$.

In this system we define multiplication by means of the formulae

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

where

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

and

$$y'' \equiv y + y',\quad z'' \equiv z + z',\quad w'' \equiv w + w' \pmod p.$$

It shoud be remembered that throughout the paper, all congruences without explicit modulus are taken mod p. 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 $[-r^{p-y}s^{p-z}t^{p-w}x, p-y, p-z, p-w]$ is the inverse of $[x, y, z, w]$, in virtue of (2). Therefore K is a group. Moreover if

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

one can easily show that

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

Also

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

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

$$a'd' = [1, 0, 0, 0][0, 0, 0, 1] = [t, 0, 0, 1] = [0, 0, 0, 1][t, 0, 0, 0] = d'a'^t.$$

Thus corresponding to the defining relations of G

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

From this we see that the group K is a homomorphic image of G. But as the order of K is $p^3 m$ and the order of G is at most $p^3 m$, they have the same order and are isomorphic. This proves the existence of a group G of the desired type.

Theorem 7. *If there is a group G of the type $T(1, 2, 2)$, then it has the defining relations*

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

with $u \in \{2, 3, \ldots, p-1\}$ *and*

$$(4) \qquad r^p \equiv s^p \equiv 1 \pmod m,$$

$$(5) \qquad k|m, \quad k|r-1, \quad k|s-1.$$

Conversely, if $r, s,$ and u satisfy (4) *and* (5), *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 $T(1, 2, 2)$. Then the subgroup $\{a, b, c\}$ is of the type H_1 while the two subgroups $\{a, b, d\}$ and $\{a, c, d\}$ are both of the type H_2. Then by Theorem 1, we have

$$a^m = b^p = c^p = e, \quad ab = ba^r, \quad ac = ca^s, \quad bc = cb; \quad r^p \equiv s^p \equiv 1 \pmod m$$

$$a^m = b^p = d^p = e, \quad ab = ba^r, \quad ad = d^u a, \quad bd = db; \quad u \in \{2, 3, \ldots, p-1\}$$

$$a^m = c^p = d^p = e, \quad ac = ca^s, \quad ad = d^u a, \quad cd = dc$$

where for the last two subgroups, we have respectively

$$r^p \equiv 1 \pmod m,\ k|m,\ k|r-1 \quad \text{and} \quad s^p \equiv 1 \pmod m,\ k|m,\ k|s-1$$

k being the order of $u \bmod p$. Thus we have shown that (3), (4), (5) are necessary.

For the converse, let K be the same system of all formal quadruples $[x, y, z, w]$ used in the previous theorem with a new multiplication formula

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

where

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

$$y'' \equiv y+y',\ z'' \equiv z+z',\ w'' \equiv w+u^{x}w' \pmod{p}.$$

Now if we observe that k is the order of u mod p and that $k|r-1, k|s-1$ it follows that

(6) $$u^{r} \equiv u,\ u^{s} \equiv u \pmod{p} \quad \text{and} \quad u^{r^{\lambda}s^{\mu}} \equiv u \pmod{p}$$

for all natural numbers λ, μ. This multiplication is associative, for

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

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

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

$$X = r^{y}s^{z'}x+x',\ u^{X} \equiv u^{x+x'} \pmod{p} \quad \text{using} \quad (6)$$

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

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

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

Also $e'=[0, 0, 0, 0]$ is the unit element for this multiplication and $[-r^{p-y}s^{p-z}x, p-y, p-z, -u^{m-x}w]$ is the inverse of $[x, y, z, w]$ in virtue of

$$r^{p} \equiv 1,\ s^{p} \equiv 1 \pmod{m} \quad \text{and} \quad u^{m} \equiv 1,\ u^{r} \equiv u,\ u^{s} \equiv u \pmod{p}$$

as $k|m, k|r-1, k|s-1$ (k being the order of u mod p). Therefore the system K is a group of order p^3m.

Moreover, if $a'=[1, 0, 0, 0]$, $b'=[0, 1, 0, 0]$, $c'=[0, 0, 1, 0]$, $d'=[0, 0, 0, 1]$ then, according to the defining relations of G, one can easily show that

$$a'^{m} = b'^{p} = c'^{p} = d'^{p} = e',\quad b'c' = c'b',\quad b'd' = d'b',\quad c'd' = d'c'$$

$$a'b' = b'a'^{r},\quad a'c' = c'a'^{s},\quad a'd' = d'^{u}a'.$$

For the last three relations, we have in fact

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

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

$$a'd' = [1, 0, 0, 0][0, 0, 0, 1] = [1, 0, 0, u] = [0, 0, 0, u][1, 0, 0, 0] = d'^{u}a'.$$

Therefore the group K is a homomorphic image of G of order p^3m. But as the order of G is at most p^3m, they have the same order and are isomorphic. This shows that a group G of the required type exists.

Theorem 8. *If a group G of the type $T(3, 3, 3)$ exists, then it has the defining relations*

$$a^m = b^p = c^p = d^p = e, \quad ab = b^u a, \quad ac = c^v a, \quad ad = d^t a, \tag{7}$$
$$bc = cb, \quad bd = db, \quad cd = dc,$$

with $u, v, t \in \{2, 3, \ldots, p-1\}$ *and*

$$k|m, \quad k'|m, \quad k''|m, \tag{8}$$

where k, k' *and* k'' *are the orders of* u, v *and* $t \bmod p$ *respectively. Conversely, if* u, v *and* $t \in \{2, 3, \ldots, p-1\}$ *and if* k, k' *and* k'' *satisfy* (8), *then the group* G *generated by* a, b, c *and* d *with the defining relations* (7) *is of the required type.*

PROOF. The necessity of (7) and (8) is direct and can be established similarly as before. For the converse, we use the following multiplication formulae

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

with

$$x'' \equiv x + x' \pmod m,$$
$$y'' \equiv y + u^x y', \quad z'' \equiv z + v^x z', \quad w'' \equiv w + t^x w' \pmod p$$

in the system K of formal quadruples $[x, y, z, w]$ of the previous theorems. The proof follows similar lines and may be omitted.

Theorem 9. *If there is a group G of the type $T(3, 2, 2)$, then it has the defining relations*

$$a^m = b^p = c^p = d^p = e, \quad ab = b^u a, \quad ac = c^v a, \quad ad = da^r, \tag{9}$$
$$bc = cb, \quad bd = db, \quad cd = dc,$$

with $u, v \in \{2, 3, \ldots, p-1\}$ *and*

$$k|m, \quad k'|m, \quad k|r-1, \quad k'|r-1, \tag{10}$$

k *and* k' *being the orders of* u *and* $v \bmod p$ *respectively.*

Conversely if u, v *and* r *satisfy* (10), *then the group* G *generated by* a, b, c *and* d *with the defining relations* (9) *is of the desired type.*

The necessity of the conditions is obvious. For the converse, we use the same system K of formal quadruples $[x, y, z, w]$ but with the formula

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

where

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

The associativity of multiplication follows directly if we remark that

$$k|r-1, \quad k'|r-1 \quad \text{and} \quad u^r \equiv u, \quad v^r \equiv v \pmod p.$$

Also $e' = [0, 0, 0, 0]$ is the unit element for this multiplication and $[-r^{p-w}x, -u^{p-x}y, -v^{p-x}z, p-w]$ is the inverse of $[x, y, z, w]$. Hence the system K is a group of order $p^3 m$, which proves the existence of a group G of the required type by following similar lines as in the previous theorems.

CONCLUSION. Theorems 6—9 show that finite groups with four independent generators a, b, c and d exist when three of the generators have the same odd prime order p. The group of Theorem 6 with $r \equiv s \equiv t \equiv 1 \pmod{m}$ is in fact the direct product of $\{a\}$, $\{b\}$, $\{c\}$ and $\{d\}$.

References

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

[2] K. R. YACOUB, On finite groups with three independent generators two of which being of orders p and 4, *Nieuw Archief voo Wiskunde, Amsterdam* (3), **13** (1965), 180—191.

(Received November 28, 1983.)