On finite groups with three independent generators two of which have distinct odd prime orders

By K. R. YACOUB (Cairo)

In a recent paper [1], the structure of finite groups with three independent generators has been studied when two of the generators have the same odd prime order. In the present paper, we consider a similar problem namely that when two of the generators have also odd prime orders but distinct.

In § 1, we state without proof some results which will be required. Throughout this paper, the symbols p, q are used to denote distinct odd primes with $p<q$.

§ 1. Preliminary results

Lemma 1 (i). *The general products of* $\{a\}$ *and* $\{b\}$ *when* b *is of order* p *are* (*cf* [2]) *of the types*

L_1: $a^m=b^p=e,\quad ab=ba^r,\quad r^p\equiv 1 \pmod m$

L_2: $a^m=b^p=e,\quad ab=b^u a,\quad u^m\equiv 1 \pmod p,\ u\not\equiv 1 \pmod p.$

For the sake of reference, this lemma (on using different symbols) may be written

Lemma 1 (ii). *The general products of* $\{a\}$ *and* $\{c\}$ *when* c *is of order* q *are of the types*

N_1: $a^m=c^q=e,\quad ac=ca^s,\quad s^q\equiv 1 \pmod m$

N_2: $a^m=c^q=e,\quad ac=c^v a,\quad v^m\equiv 1 \pmod q,\ v\not\equiv 1 \pmod q.$

Lemma 2. *The congruences* $x^p\equiv 1 \pmod q$, $y^q\equiv 1 \pmod p$ *have in respective the solutions* $x\equiv 1 \pmod q$, $y\equiv 1 \pmod p$. *Moreover, if* p *divides* $q-1$, *the congruence* $x^p\equiv 1 \pmod q$ *has besides the solution* $x\equiv 1 \pmod q$ *other solutions for which* x *may be a number whose order modulo* q *is* p.

Now, if in Lemma 1 (ii), we take $m=p$, replace a by b, then use Lemma 2, we deduce

Lemma 3. *Let* b, c *be of orders* p, q *respectively.*

(i) *If* p *is not a divisor of* $q-1$, *the general product of* $\{b\}$ *and* $\{c\}$ *is Abelian*

$$b^p=c^q=e,\quad bc=cb.$$

(ii) *If p divides $q-1$, the general products of $\{b\}$ and $\{c\}$ are*

$$b^p = c^q = e, \quad bc = cb,$$

and $b^p = c^q = e, \quad bc = c^\omega b, \quad \omega^p \equiv 1 \pmod{q}, \quad \omega \not\equiv 1 \pmod{q}$.

For the convenience of reference, the two types of groups described in Lemma 3 (both Abelian and non-Abelian) will be referred together by

$$K(\omega): b^p = c^q = e, \quad bc = c^\omega b, \quad \omega^p \equiv 1 \pmod{q}.$$

It may be remarked that $\omega \equiv 1 \pmod{q}$ for the Abelian type and that both types arise only when p divides $q-1$.

§ 2. Description of the problem

Let G be a finite group with three independent generators a, b, c of orders m, p, q respectively. Then, by Lemma 1 (i), $\{a, b\}$ is either of the type L_1 or of the type L_2. Also, by Lemma 1 (ii), $\{a, c\}$ is either of the type N_1 or of the type N_2. Further, $\{b, c\}$ is by Lemma 3 of the type $K(\omega)$.

Thus in determining all groups G, we have four cases to consider.

(1) $\{a, b\} = L_1$, $\{a, c\} = N_1$, $\{b, c\} = K(\omega)$. We denote this group by $T(1, 1; \omega)$.

(2) $\{a, b\} = L_1$, $\{a, c\} = N_2$, $\{b, c\} = K(\omega)$. We denote this group by $T(1, 2; \omega)$.

(3) $\{a, b\} = L_2$, $\{a, c\} = N_1$, $\{b, c\} = K(\omega)$. We denote this group by $T(2, 1; \omega)$.

(4) $\{a, b\} = L_2$, $\{a, c\} = N_2$, $\{b, c\} = K(\omega)$. We denote this group by $T(2, 2; \omega)$.

In this paper, we aim to describe groups of these types in terms of some simple parameters and prove the existence of such groups for permissible parameter values. We deal seperately with the cases $p \nmid q-1$ and $p \mid q-1$. (by the symbol $p \nmid q-1$, we mean that p is not a divisor of $q-1$.)

The case $p \nmid q-1$.

In this case $\{b, c\}$ is Abelian, so that $\{b, c\} = K(\omega)$ with $\omega \equiv 1 \pmod{q}$, and the types we have to deal with are therefore $T(1, 1; 1)$, $T(1, 2; 1)$, $T(2, 1; 1)$, $T(2, 2; 1)$.

§ 3. Groups of the type $T(1, 1; 1)$

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

(1) $$a^m = b^p = c^q = e, \quad ab = ba^r, \quad ac = ca^s, \quad bc = cb,$$

where

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

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

PROOF. Assume the existence of a group G of the type $T(1, 1; 1)$. For this type $\{a, b\}=L_1$, $\{a, c\}=N_1$, $\{b, c\}$ is Abelian. Then by Lemma 1

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

$$a^m=c^q=e, \quad ac=ca^s, \quad s^q\equiv 1 \pmod m$$

Also $bc=cb$, and the first part of the theorem then follows.

For the converse, let H be the system of all formal triads $[x, y, z]$ where x is taken mod m, y mod p, z mod q. The triads $[x, y, z]$ and $[x', y', z']$ are regareded identical if $x'\equiv x \pmod m$, $y'\equiv y \pmod p$, $z'\equiv z \pmod q$. In this system, we define multiplication by means of the formula

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

Under this multiplication, it is easy to verify that H forms a group (the identity is $[0, 0, 0]$ and the inverse of $[x, y, z]$ is $[-r^{-y}s^{-z}x, -y, -z]$).

Further, if $a'=[1, 0, 0]$, $b'=[0, 1, 0]$ and $c'=[0, 0, 1]$, then by direct calculation one can show that

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

where e' denotes the identity element $[0, 0, 0]$ of the group H. This shows that H is a homomorphic image of G. But as the order of H is pqm, and the order of G is at most pqm, they have the same order and are isomorphic. This completes the proof of the theorem.

§ 4. Groups of the type $T(1, 2; 1)$

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

$$a^m=b^p=c^q=e, \quad ab=ba^r, \quad ac=c^va, \quad bc=cb \tag{3}$$

where

$$r^p\equiv 1 \pmod m, \quad v^m\equiv v^{r-1}\equiv 1 \pmod q, \quad v\not\equiv 1 \pmod q. \tag{4}$$

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

PROOF. Assume the existence of a group G of the type $T(1, 2; 1)$. For this type $\{a, b\}=L_1$, $\{a, c\}=N_2$, $\{b, c\}$ is Abelian. Then by Lemma 1

$$a^m=b^p=e, \quad ab=ba^r, \tag{5}$$

$$a^m=c^q=e, \quad ac=c^va, \tag{6}$$

$$r^p\equiv 1 \pmod m, \quad v^m\equiv 1 \pmod q, \quad v\not\equiv 1 \pmod q.$$

Also, since $\{b, c\}$ is Abelian, then $bc=cb$. Thus it remains to show that

$$v^{r-1}\equiv 1 \pmod q.$$

For by using (5), (6) together with the associative law in G and the fact that $\{b, c\}$ is Abelian, we have

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

$$a(bc) = a(cb) = c^v ab = c^v ba^r.$$

But since $(ab)c = a(bc)$, it follows that $v^r \equiv v \pmod q$ which, on noting that v is prime to q, implies $v^{r-1} \equiv 1 (\text{mod } q)$. Thus we have shown that (3) and (4) are necessary.

For the converse, we use again the system H of Theorem 3 where multiplication of triads is defined here by the formula

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

That H forms, under this multiplication, a group can be easily verified (the identity is $[0, 0, 0]$ and the inverse of $[x, y, z]$ is $[-r^{-y}x, -y, -v^{-x}z]$). Moreover $a' = [1, 0, 0], b' = [0, 1, 0], c' = [0, 0, 1]$ are generators which satisfy relations $T(1, 2; 1)$.

§ 5. Groups of the type $T(2, 1; 1)$

Theorem 3. *If there is a group G of the type $T(2,1; 1)$, then it has the defining relations*

(7) $$a^m = b^p = c^q = e, \quad ab = b^u a, \quad ac = ca^s, \quad bc = cb$$

where

(8) $$s^q \equiv 1 \pmod m, \quad u^m \equiv u^{s-1} \equiv 1 \pmod p, \quad u \not\equiv 1 \pmod p.$$

Conversely, if s, u, m satisfy (8), *then the group G generated by a, b, c with the defining relations* (7) *is of the desired type.*

The proof is similar to that of Theorem 2 and is omitted.

§ 6. Groups of the type $T(2, 2; 1)$

Theorem 4. *If there is a group G of the type $T(2,2 ;1)$, then it has the defining relations*

(9) $$a^m = b^p = c^q = e, \quad ab = b^u a, \quad ac = c^v a, \quad bc = cb$$

where

(10) $$u^m \equiv 1, \ u \not\equiv 1 \pmod p, \quad v^m \equiv 1, v \not\equiv 1 \pmod q.$$

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

PROOF. The proof follows the same pattern of as Theorem 1, where for the converse, of the theorem multiplication of triads is defined by the formula

$$[x, y, z][x', y', z'] = [x + x', y + u^x y', z + v^x z'].$$

We omit this proof.

The case $p|q-1$.

In this case $\{b, c\}=K(\omega)$ where $\omega\equiv 1$ or $\omega\not\equiv 1 \pmod q$. In §§ 9,10 we shall prove that groups of the types $T(2, 1;\ \omega)$, $T(2, 2;\ \omega)$ with $\omega\not\equiv 1 \pmod q$ do not exist.

§ 7. Groups of the type $T(1,\ 1;\ \omega)$

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

$$a^m=b^p=c^q=e,\quad ab=ba^r,\quad ac=ca^s,\quad bc=cb \tag{11}$$

where

$$r^p\equiv 1 \pmod m,\quad s^q\equiv 1 \pmod m. \tag{12}$$

Conversely, if r, s satisfy (12), *then the group G generated by a, b, c with the defining relations* (11) *is of the desired type.*

The proof is exactly the same as that of Theorem 1 and is therefore omitted.

Theorem 5(ii). *If there is a group G of the type $T(1,1;\omega)$, $\omega\not\equiv 1 \pmod q$, then it has the defining relations*

$$a^m=b^p=c^q=e,\quad ab=ba^r,\quad ac=ca,\quad bc=c^\omega b \tag{13}$$

where

$$r^p\equiv 1 \pmod m,\quad \omega^p\equiv 1 \pmod q. \tag{14}$$

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

Proof. Assume the existence of a group G of the type $T(1, 1;\ \omega)$, $\omega\not\equiv 1 \pmod q$. For this type $\{a, b\}=L_1$, $\{a, c\}=N_1$, $\{b, c\}=K(\omega)$, so that by Lemmas 1, 3

$$a^m=b^p=c^q=e,\quad ab=ba^r,\quad ac=ca^s,\quad bc=c^\omega b \tag{15}$$

where

$$r^p\equiv 1 \pmod m,\quad s^q\equiv 1 \pmod m,\quad \omega^p\equiv 1,\quad \omega\not\equiv 1 \pmod q. \tag{16}$$

Now, it remains to show that $s\equiv 1 \pmod m$. By using relations (15) and the associative law in G, we have

$$a(bc)=a(c^\omega b)=c^\omega a^{s^\omega}b=c^\omega ba^{rs^\omega},$$

$$(ab)c=ba^rc=bca^{rs}=c^\omega ba^{rs}.$$

But $a(bc)=(ab)c$, and hence $rs^\omega\equiv rs \pmod m$ which if we note that r and s are both prime to m implies at once

$$s^{\omega-1}\equiv 1 \pmod m. \tag{17}$$

Calling the second and the fourth of (16), namely

$$s^q\equiv 1 \pmod m,\quad \omega\not\equiv 1 \pmod q \tag{18}$$

we see that (17) and (18) cannot be satisfied simultaneously unless $s \equiv 1 \pmod{m}$. This completes the proof of the first part of the theorem.

For the converse, we call again the system H of formal triads $[x, y, z]$ used in Theorem 1 and follow the same lines of proof.

In this system multiplication is defined by

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

The proof is straightforward and may be omitted.

§ 8. Groups of the type $T(1, 2; \omega)$

Theorem 6. *If there is a group G of the type $T(1,2; \omega)$, then it has the defining relations*

$$a^m = b^p = c^q = e, \quad ab = ba^r, \quad ac = c^v a, \quad bc = c^\omega b \tag{19}$$

where

$$r^p \equiv 1 \pmod{m}, \; v^m \equiv v^{r-1} \equiv 1, \; v \not\equiv 1 \pmod{q}, \; \omega^p \equiv 1 \pmod{q}. \tag{20}$$

Conversely, if r, v, ω, m satisfy (20), *then the group G generated by a, b, c with the defining relations* (19) *is of the desired type.*

Proof. Assume the existence of a group G of the type $T(1, 2; \omega)$. For this type $\{a, b\} = L_1$, $\{a, c\} = N_2$, $\{b, c\} = K(\omega)$, so that by Lemmas 1, 3

$$a^m = b^p = c^q = e, \quad ab = ba^r, \quad ac = c^v a, \quad bc = c^\omega b \tag{21}$$

where

$$r^p \equiv 1 \pmod{m}, \; v^m \equiv 1 \pmod{q}, \; \omega^p \equiv 1 \pmod{q}, \; v \not\equiv 1 \pmod{q}.$$

Now, it remains to show that $v^{r-1} \equiv 1 \pmod{q}$. For by using relations (21) and the associative law in G, we have

$$a(bc) = a(c^\omega b) = c^{\omega v} ab = c^{\omega v} ba^r,$$

$$(ab)c = (ba^r)c = bc^{v^r} a^r = c^{\omega v^r} ba^r.$$

But $a(bc) = (ab)c$, and therefore $\omega v^r \equiv \omega v \pmod{q}$ which, on observing that ω and v are both prime to q, implies $v^{r-1} \equiv 1 \pmod{q}$.

Thus we have shown that (19) and (20) are necessary.

For the converse, we call again the system H of formal triads $[x, y, z]$ used in Theorem 1, where mutiplication is now defined by

$$[x, y, z][x', y', z'] = [r^{y'}x + x', \; y + y', \; z + v^x \omega^y z'].$$

Under this multiplication, it is easy to show that H forms a group (the identity is $[0, 0, 0]$ and the inverse of $[x, y, z]$ is $[-r^{-y}x, \; -y, \; -v^{-x}\omega^{-y}z]$).

Moreover, if $a' = [1, 0, 0]$, $b' = [0, 1, 0]$ and $c' = [0, 0, 1]$, then one can easily show that

$$a'^m = b'^p = c'^q = e', \; a'b' = b'a'^r, \; a'c' = c'^v a', \; b'c' = c'^\omega b'$$

where e' denotes the identity element $[0, 0, 0]$ of the group H.

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

§ 9. Groups of the type $T(2,1;\omega)$

Theorem 7(i). *There is no group of the type* $T(2,1;\omega)$ *when* $\omega \not\equiv 1 \pmod q$.
(ii) *Moreover, if there is a group* G *of the type* $T(2,1;1)$, *then it has the defining relations*

$$a^m = b^p = c^q = e, \quad ab = b^u a, \quad ac = ca^s, \quad bc = cb \tag{22}$$

where

$$u^m \equiv u^{s-1} \equiv 1 \pmod p, \quad u \not\equiv 1 \pmod p \quad s^q = 1 \pmod m. \tag{23}$$

Conversely, if u, s, m *satisfy* (23), *then the group* G *generated by* a, b, c *with the defining relations* (22) *is of the desired type.*

Proof. Assume the existence of a group G of the type $T(2, 1; \omega)$. For this type $\{a, b\} = L_2$, $\{a, c\} = N_1$, $\{b, c\} = K(\omega)$, so that by Lemmas 1, 3

$$a^m = b^p = c^q = e, \quad ab = b^u a, \quad ac = ca^s, \quad bc = c^\omega b \tag{24}$$

where

$$u^m \equiv 1 \pmod p, \quad u \not\equiv 1 \pmod p, \quad s^q \equiv 1 \pmod m, \quad \omega^p \equiv 1 \pmod q. \tag{25}$$

Further, by using relations (24) and the associative law in G, we have

$$a(bc) = a(c^\omega b) = c^\omega a^{s^\omega} b = c^\omega b^{u^{s^\omega}} a^{s^\omega},$$

$$(ab)c = (b^u a)c = b^u c a^s = c^{\omega^u} b^u a^s,$$

but since $a(bc) = (ab)c$, we must have

$$\omega^u \equiv \omega \pmod q, \quad u^{s^\omega} \equiv u \pmod p, \quad s^\omega \equiv s \pmod m.$$

Moreover, if we remark that ω is prime to q, u prime to p, s prime to m, the above relations take the forms

$$\omega^{u-1} \equiv 1 \pmod q, \quad u^{s^\omega - 1} \equiv 1 \pmod p, \quad s^{\omega - 1} = 1 \pmod m. \tag{26}$$

It is obvious that the relation $s^q \equiv 1 \pmod m$ of (25) and the relation $s^{\omega-1} \equiv 1 \pmod m$ of (26) cannot be satisfied simulaneously unless $\omega \equiv 1 \pmod q$. This proves that no group of the type $T(2, 1; \omega)$ can exist when $\omega \not\equiv 1 \pmod q$, and the first part of the theorem follows.

For the second part of the theorem, we follow the same pattern of proof of Theorem 3 and we omit this proof.

§ 10. Groups of the type $T(2, 2; \omega)$

Theorem 8(i). *No group of the type* $T(2, 2; \omega)$ *exists when* $\omega \not\equiv 1 \pmod q$.
(ii) *Moreover, if there is a group* G *of the type* $T(2,2; 1)$, *then it has the defining relations*

$$a^m = b^p = c^q = e, \quad ab = b^u a, \quad ac = c^v a, \quad bc = cb \tag{27}$$

where

$$u^m \equiv 1, \; u \not\equiv 1 \pmod p, \quad v^m \equiv 1, \; v \not\equiv 1 \pmod q. \tag{28}$$

Conversely if u, v satisfy (28), *then the group G generated by a, b, c with the defining relations* (27) *is of the desired type.*

PROOF. Assume the existence of a group G of the type $T(2, 2; \omega)$. For this type $\{a, b\} = L_2$, $\{a, c\} = N_2$, $\{b, c\} = K(\omega)$, so that by Lemmas 1,3

$$a^m = b^p = c^q = e, \quad ab = b^u a, \quad ac = c^v a, \quad bc = c^\omega b \tag{29}$$

where

$$u^m \equiv 1,\ u \not\equiv 1 \pmod{p},\ v^m \equiv 1,\ v \not\equiv 1 \pmod{q},\quad \omega^p \equiv 1 \pmod{q}; \tag{30}$$

Further, by using (29) and the associative law in G, we have

$$a(bc) = a(c^\omega b) = c^{\omega v} ab = c^{\omega v} b^u a,$$

$$(ab)c = b^u ac = b^u c^v a = c^{\omega u v} b^u a,$$

but since $a(bc) = (ab)c$, we must have

$$\omega^u v \equiv \omega v \pmod{q}$$

which if we note that ω, v are both prime to q implies

$$\omega^{u-1} \equiv 1 \pmod{q}. \tag{31}$$

Calling the relations $\omega^p = 1 \pmod{q}$, $u \not\equiv 1 \pmod{p}$ of (30), we see (31) cannot be satisfied unless $\omega \equiv 1 \pmod{q}$. This shows that no group of the type $T(2,2; \omega)$ exist when $\omega \not\equiv 1 \pmod{q}$ which proves the first part of the theorem.

For the second part of the theorem, the proof follows the same pattern of proof as Theorem 4, and the proof is omitted.

Conclusion. Theorems 1—8, show that groups with three independent generators exist when two of the generators have odd prime orders p, q. If $p < q$, these groups are described in Theorems 5, 6, 7, 8 when p divides $q - 1$ and in Theorems 1, 2, 3, 4 when p is not a divisor of $q - 1$.

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 general products of two finite cyclical groups, *Athesis, London University*, 1953.

(Received June 8, 1964.)