Chin. Ann. of Math
5B (4) 1984

ON FINITE GROUPS OF ORDER 2^3pq

WEN ZHIXIONG (文志雄)
(*Wuhan University*)

Abstract

Zhang Yuanda has determined the groups of order 2^3p^2 (p is an odd prime$\neq 3, 7$)[1]. Now this paper is to determine the structures of groups of order 2^3pq (p, q are odd primes and $p<q$).

Let G be a finite group of order $|G|=2^3pq$, and let O, P, and Q denote respectively the Sylow 2-, p-, and q-subgroups of G.

§ 1. G has Sylow-tower

Since the Sylow 2-subgroups O possess 5 possibilities:

I. $O=Z_8$(cyclic group of order 8);

II. $O=Z_4\times Z_2$ (abelian group of order 8 of type $[2^2, 2]$);

III. $O=E_8$(elementary abelian);

IV. $O=D_8$(dihedral group);

V. $O=Q_8$(quarternion group).

we shall discuss G according to these five cases.

G having sylow-tower implies that the Hall (p, q)-subgroup $PQ \lhd G$, thus $G=O[PQ]$-the semi-direct product of PQ by O. It is known that $PQ=Z_{pq}$ (cyclic of order pq) when $p\nmid(q-1)$; and either $PQ=Z_{pq}$ or $PQ=\langle a, b\rangle$, $a^q=b^p=1$, $b^{-1}ab=a^h$, where $h^p\equiv 1 \pmod q$ and $h\not\equiv 1 \pmod q$, when $p|(q-1)$.

I. $O=Z_8$

I. 1) $p\nmid(q-1)$.

Now $G=Z_8[Z_{pq}]=\langle x, y\rangle$, $x^{pq}=y^8=1$, $x^y=x^r$; thence $r^8\equiv 1 \pmod{pq}$. Since $(p, q)=1$, there exists k so that $kp\equiv 1 \pmod q$. We choose r_1, r_2, s_1, s_2 such that $r_1^2\equiv -1$, $r_2^2\equiv r_1 \pmod p$; $s_1^2\equiv -1$, $s_2^2\equiv s_1 \pmod q$. Now $r^8\equiv 1 \pmod{pq}$ has the following possible solutions: $r\equiv r_2^i+k_p(s_2^j-r_2^i) \pmod{pq}$, $i, j=0, 1, 2, 3, 4, 5, 6, 7$. It has 4 soltuions, $i, j=0, 4$, when $2^2\nmid(q-1), (p-1)$; 8 solutions, $i=0, 2, 4, 6$, $j=0.4$, when $2^2\nmid(q-1)$, $2^2\|(p-1)$: 16 solutions, $0\leqslant i\leqslant 7$, $j=0.4$, when $2^2\nmid(q-1)$,

Manuscript received Novenber 17, 1982, Revised April 12, 1983.

$2^3|(p-1)$; 8 solutions $i=0.4$, $j=0, 2, 4, 6$, when $2^2\|(q-1)$, $2^2\nmid(p-1)$; 16 solutions,
$i, j=0, 2, 4, 6$, when $2^2\|(q-1)$, $(p-1)$; 32 solutions, $0\leqslant i\leqslant 7$, $j=0, 2, 4, 6$, when
$2^2\|(q-1)$, $2^3|(p-1)$; 16 solutions, $i=0.4$, $0\leqslant j\leqslant 7$, when $2^3|(q-1)$, $2^2\nmid(p-1)$; 32
solutions, $i=0, 2, 4, 6$, $0\leqslant j\leqslant 7$, when $2^3|(q-1)$, $2^2\|(p-1)$; 64 solutions, $0\leqslant i, j\leqslant 7$
when $2^3|(q-1)$, $(p-1)$.

If $i=1, 3, 5, 7$, by means of $i^2\equiv 1 \pmod 8$ we find that
$[r_1^j+kp(s_2^i-r_1^j)]^i\equiv r_1^{ij}+kp(s_2-r_1^{ij})$,
$[r_2^i+kp(s_2^j-r_2^i)]^i\equiv r_2+kp(s_2^{ij}-r_2)$, $[\pm 1+kp(s_1^i\mp 1)]^i\equiv \pm 1+kp(s_1\mp 1) \pmod{pq}$.
$[r_1^i+kp(s_1^j-r_1^i)]^i\equiv r_1+kp(s_1^{ij}-r_1)$, the group structures of G have 22 types, say
Thus replacing y by y^i, we find that
$G=\langle x, y\rangle$, $x^{pq}=y^8=1$, but

(i) $x^y=x$; (ii) $x^y=x^{-1}$; (iii) $x^y=x^{1-2kp}$; (iv) $x^y=x^{2kp-1}$; (v) $x^y=x^{r_1+kp(1-r_1)}$;
(vi) $x^y=x^{r_1-kp(1+r_1)}$; (vii) $x^y=x^{r_2+kp(1-r_2)}$; (viii) $x^y=x^{r_2-kp(1+r_2)}$; (ix) $x^y=x^{kp(s_1-1)+1}$;
(x) $x^y=x^{kp(s_1+1)-1}$; (xi) $x^y=x^{r_1+kp(s_1-r_1)}$; (xii) $x^y=x^{r_1+kp(s_1^3-r_1)}$; (xiii) $x^y=x^{r_2+kp(s_1-r_2)}$;
(xiv) $x^y=x^{r_2+kp(s_1^3-r_2)}$; (xv) $x^y=x^{1+kp(s_2-1)}$; (xvi) $x^y=x^{kp(s_2+1)-1}$; (xvii) $x^y=x^{r_1+kp(s_2-r_1)}$;
(xviii) $x^y=x^{r_1^3+kp(s_2-r_1^3)}$; (xix) $x^y=x^{r_2+kp(s_2-r_2)}$; (xx) $x^y=x^{r_2+kp(s_2^3-r_2)}$;
(xxi) $x^y=x^{r_2+k_p(s_2^5-r_2)}$; (xxii) $x^y=x^{r_2+k_p(s_2^7-r_2)}$.

Now we shall show that the 22 types mentioned above are non-isomorphie with
one another in the following:

On the contrary, if we put $G_1=\langle x, y\rangle$, $x^{pq}=1=y^8$, $x^y=x^{r_2^i+kp(s_2^j-r_2^i)}$, and $G_2=\langle a,b\rangle$,
$a^{pq}=1=b^8$, $a^b=a^{r_2^{i'}+kp(s_2^{j'}-r_2^{i'})}$ and $(i, j)\neq(i', j')$, then $G_1\simeq G_2$ means that there exists
an isomophic mapping σ from G_1 onto G_2, hence letting $\sigma(x)=a_1$, $\sigma(y)=b_1$, we have
$a_1, b_1\in G_2$ and in fact $a_1=a^\lambda$, $b_1=a^\mu b^\nu$ such that $(\lambda, pq)=1$, $(2, \nu)=1$, consequently
$x^y=x^{r_2^i+kp(s_2^j-r_2^i)}$ implies $a_1^{r_2^i+kp(s_2^j-r_2^i)}=a_1^{b_1}=(a^\lambda)^{a^\mu b^\nu}=b^{-\nu}a^\lambda b^\nu=a^{\lambda[r_2^{i'}+kp(s_2^{j'}-r_2^{i'})]^\nu}=a_1^{[r_2^{i'}+kp(s_2^{j'}-r_2^{i'})]^\nu}$,
thus $r_2^i+kp(s_2^j-r_2^i)\equiv[r_2^{i'}+kp(s_2^{j'}-r_2^{i'}]^\nu \pmod{pq}$, which is equivalent to $r_2^i\equiv r_2^{i'\nu}$
$\pmod p$ and $s_2^j\equiv s_2^{j'\nu} \pmod q$. It follows that $i\equiv i'\nu \pmod 8$ and $j\equiv j'\nu \pmod 8$. But
(i, j) is one of the forms (0, 0), (4, 0), (0, 4), (4, 4), (2, 0), (2, 4), (1, 0), (1,
4), (0, 2), (4, 2), (2, 2), (2, 6), (1, 2), (1, 6), (0, 1), (4, 1), (2, 1), (6, 1),
(1, 1), (1, 3), (1, 5), (1, 7), so is (i', j'). Thus the congruences $i\equiv i'\nu$, $j\equiv j'\nu$
$\pmod 8$ hold if and only if $i=i'$, $j=j'$, contradiction to $(i, j)\neq(i', j')$.

I. 2) $p|(q-1)$.

Now $G=Z_8[Z_{pq}]$ or $Z_8(Z_p[Z_q])$. If $G=Z_8[Z_{pq}]$, then the group structures of G
are the same as we have discussed in I. 1). Therefore we now need only to consider
$G=Z_8[Z_p[Z_q]]$, i. e. $G=\langle a, b, c\rangle$, $a^q=b^p=c^8=1$, $a^b=a^h$, $h^p\equiv 1 \pmod q$, $h\not\equiv 1 \pmod q$,
$a^c\in\langle a, b\rangle$, $b^c\in\langle a, b\rangle$. Since G has Sylow-tower, hence $P\lhd OP$, consequently we
cannot help to have $a^c=a^r$, $b^c=b^s$. Thus $a^{rh^s}=(a^r)^{b^s}=(a^c)^{b^c}=a^{bc}=a^{hr}$ implies

$$\mathrm{r}h^s\equiv hr \pmod q \Rightarrow h^s\equiv h \pmod q$$

$$(\because (r, q)=1)\Rightarrow s\equiv 1 \pmod p \Rightarrow b^c=b.$$

Again $a=a^{c^8}=a^{r^8}$ impliei $r^8\equiv 1 \pmod q$.

There are at most 8 solutions: $r\equiv s_2^i \pmod q$, $0\leqslant i\leqslant 7$. It has 2 solutions, $i=0, 4$, when $2^2\nmid(q-1)$; 4 solutions, $i=0, 2, 4, 6$, when $2^2\|(q-1)$; It has 8 solutions, $0\leqslant i\leqslant 7$, when $2^3|(q-1)$. Thus replacing c by c^i as I. 1), we find that the group structures of G have 4 types, say $G=\langle a, b, c\rangle$, $a^q=b^p=c^8=1=[b, c]$, $a^b=a^h$,

(xxiii) $a^c=a$; (xxiv) $a^c=a^{-1}$; (xxv) $a^c=a^{s_1}$; (xxvi) $a^c=a^{s_2}$.

Their centers are $\langle c\rangle$, cyclic of order 8; $\langle c^2\rangle$, cyclic of order 4; $\langle c^4\rangle$, cyclic of order 2; and 1, identity for (xxiii); (xxiv); (xxv); (xxvi) respectively. So no two of these groups are isomorphic.

If we set $x=a$, $y=bc$. Then $G=\langle x, y\rangle$, $x^q=y^{8p}=1$, and (xxiii) $x^y=x^h$; (xxiv) $x^y=x^{-h}$; (xxv) $x^y=x^{s_1h}$; (xxvi) $x^y=x^{s_2h}$.

II. $C=Z_4\times Z_2$

II. 1) $p\nmid(q-1)$.

Now $G=(Z_4\times Z_2)[Z_{pq}]=\langle a, b, c\rangle$, $a^{pq}=b^4=c^2=1=[b, c]$, $a^b=a^r$, $a^c=a^s$, so that

$$r^4\equiv 1 \pmod{pq} \quad \text{and} \quad s^2\equiv 1 \pmod{pq}. \tag{1}$$

There are at most 64 solutions for the system of congruences (1)

$$r\equiv r_1^i+kp(s_1^j-r_1^i),\ 0\leqslant i, j\leqslant 3,\ s\equiv \pm1, \pm(1-2kp) \pmod{pq}.$$

It has 16 sets of solutions, $\begin{cases} r\equiv \pm1, \pm(1-2kp) \\ s\equiv \pm1, \pm(1-2kp)\end{cases} \pmod{pq}$, when $2^2\nmid(q-1), 2^2\nmid(p-1)$;

It has 32 sets of solutions, $\begin{cases} r\equiv r_1^i+kp(s_1^j-r_1^i) \\ s\equiv \pm1, \pm(1-2kp)\end{cases} \pmod{pq}$, $0\leqslant i\leqslant 3$, $j=0, 2$, when $2^2\nmid(q-1)$, $2^2|(p-1)$; It has 32 sets of solutions,

$$\begin{cases} r\equiv r_1^i+kp(s_1^j-r_1^i) \\ s\equiv \pm1, \pm(1-2kp)\end{cases} \pmod{pq},\quad i=0, 2,\ j=0, 1, 2, 3,$$

when $2^2|(q-1)$, $2^2\nmid(p-1)$; It has 64 sets of solutions,

$$\begin{cases} r\equiv r_1^i+kp(s_1^j-r_1^i) \\ s\equiv \pm1, \pm(1-2kp)\end{cases} \pmod{pq},\quad 0\leqslant i, j\leqslant 3.$$

when $2^2|(q-1), (p-1)$.

If i is odd, then $i^2\equiv 1 \pmod 4$, and therefore $[r_1^i+kp(s_1^j-r_1^i)]^i\equiv r_1+kp(s_1^{ij}-r_1)$, $[\pm1+kp(s_1^i\mp1)]^i\equiv \pm1+kp(s_1\mp1) \pmod{pq}$. On the other hand, $(1-2kp)^2\equiv 1$, $(1-2kp)[r_1+k_p(s_1^j-r_1)]\equiv r_1+kp(s_1^{j+2}-r_1)\equiv r_1-kp(s_1^j+r_1) \pmod{pq}$, and

$$[r_1^i+kp(s_1^j-r_1^i)]^2\equiv(-1)^i+kp[(-1)^j-(-1)^i] \pmod{pq}.$$

Thus replacing b by b^i, bc, or b^ic, and c by b^2c, we find that the group structures of G have 19 types, say $G=\langle a, b, c\rangle$, $a^{pq}=b^4=c^2=1=[b, c]$, but

(i) $a^b=a^c=a$, $G\simeq Z_{4pq}\times Z_2$, $Z(G)=G$;

(ii) $a^b=a$, $a^c=a^{-1}$, with $Z(G)=\langle b\rangle\simeq Z_4$;

(iii) $a^b=a^{-1}$, $a^c=a$, with $Z(G)=\langle b^2, c\rangle\simeq E_4$;

(iv) $a^b=a^{1-2kp}$, $a^c=a$, with $Z(G)=\langle a^q, b^2, c\rangle=E_{4p}$;

(v) $a^b=a^{2kp-1}$, $a^c=a$, with $Z(G)=\langle a^p, b^2, c\rangle=E_{4q}$;

(vi) $a^b=a^{1-2kp}$, $a^c=a^{-1}$, with $Z(G)=\langle b^2\rangle\simeq Z_2$;
(vii) $a^b=a$, $a^c=a^{1-2kp}$, with $Z(G)=\langle a^q, b\rangle\simeq Z_{4p}$;
(viii) $a^b=a$, $a^c=a^{2kk-1}$, with $Z(G)=\langle a^pb\rangle\simeq Z_{4q}$;
(ix) $a^b=a^{-1}$, $a^c=a^{2kp-1}$, with $Z(G)=\langle b^2\rangle\simeq Z_2$;
(x) $a^b=a^{-1}$, $a^c=a^{1-2kp}$, with $Z(G)=\langle b^2\rangle\simeq Z_2$;
(xi) $a^b=a^{r_1+kp(1-r_1)}$, $a^c=a$, with $Z(G)=\langle a^pc\rangle\simeq Z_{2q}$;
(xii) $a^b=a^{r_1+kp(1-r_1)}$, $a^c=a^{-1}$, with $Z(G)=1$;
(xiii) $a^b=a^{r_1-kp(1+r_1)}$, $a^c=a$, with $Z(G)=\langle c\rangle\simeq Z_2$;
(xiv) $a^b=a^{1+kp(s_1-1)}$, $a^c=a$, with $Z(G)=\langle a^qc\rangle\simeq Z_{2p}$;
(xv) $a^b=a^{1+kp(s_1-1)}$, $a^c=a^{-1}$, with $Z(G)=1$;
(xvi) $a^b=a^{kp(s_1+1)-1}$, $a^c=a$, with $Z(G)=\langle c\rangle\simeq Z_2$;
(xvii) $a^b=a^{r_1+kp(s_1-r_1)}$, $a^c=a$, with $Z(G)=\langle c\rangle\simeq Z_2$;
(xviii) $a^b=a^{r_1-kq(s_1+r_1)}$, $a^c=a$; with $Z(G)=\langle c\rangle\simeq Z_2$;
(xix) $a^b=a^{r_1+kp(s_1-r_1)}$, $a^c=a^{1-2kp}$, with $Z(G)=1$.

Looking at the centers, we must shou that the 7 types (vi), (ix), (x), (xiii), (xvi), (xvii), (xviii) are non-isomorphic with one another, and also that the 3 types (xii), (xv), (xix) are also non-isomorphic with one another.

By counting the number of elements of order 2 and 4 in each group mentioned in the last paragraph, we obtain the following two tables:

Table 1

order	type						
	(vi)	(ix)	(x)	(xiii)	(xvi)	(xvii)	(xviii)
	Number of elements						
2	$2pq+1$	$2p+1$	$2q+1$	$2p+1$	$2q+1$	$2pq+1$	$2pq+1$
4	$2(p+q)$	$2q(p+1)$	$2p(q+1)$	$4pq$	$4pq$	$4pq$	$4pq$

Table 2

order	type		
	(xii)	(xv)	(xix)
	Nnmber of elements		
2	$pq+p+q$	$pq+p+q$	$pq+p+q$
4	$2(pq+p+1)$	$2(pq+q+1)$	$2(2pq+1)$

Thus it remains only to show that (xvii) is not isomorphic to (xviii) from the tables 1 and 2.

Let $G_1=\langle x, y, z\rangle$, $x^{pq}=y^4=z^2=1=[y, z]$, $x^y=x^{r_1+kp(s_1-r_1)}$, $x^z=x$ for the type (xvii) and $G_2=\langle a, b, c\rangle$, $a^{pq}=b^4=c^2=1=[b, c]$, $a^b=a^{r_1-kp(s_1+r_1)}$, $a^c=a$ for the type (xviii). If, otherwise, $G_1 \simeq G_2$, then let a_1, b_1, c_1 be respectively the images of x, y, z of G_1 into G_2, we must have $a_1 = a^\alpha$, $(\alpha, pq) = 1$, $b_1 = a^\beta b^\gamma c^\delta$, $(\gamma, 4) = 1$, consequently $a_1{}^{kp(s_1-r_1)+r_1} = a_1^{b_1} = c^{-\delta} b^{-\gamma} a^\alpha b^\gamma c^\delta = a^{\alpha[r_1 - kp(s_1+r_1)]^\gamma} = a_1{}^{[r_1-kp(s_1+r_1)]^\gamma}$ which implies that $r_1 \equiv r_1^\gamma$ (mod p) and $s_1 \equiv (-1)^\gamma s_1^\gamma$ (mod q), so that $\gamma \equiv 1$ (mod 4) and $s_1 \equiv -s_1$ (mod q), i. e. $s_1 \equiv 0$ (mod q). It is impossible. Therefore the 19 groups (i)—(xix) are distinct from, one another.

II. 2) $p \mid (q-1)$.

Now either $G = (Z_4 \times Z_2)[Z_{pq}]$ or $G = (Z_4 \times Z_2)[Z_p[Z_q]]$. If $G = (Z_4 \times Z_2)[Z_{pq}]$, then G has at most 19 types (i)—(xix) as we have discussed in II. 1). Thus we need only to consider $G = (Z_4 \times Z_2)[Z_p[Z_q]]$, i. e.

$G = \langle a, b, c, d \rangle$, $a^q = b^p = c^4 = d^2 = 1 = [c, d]$, $a^b = a^h$, $h^p \equiv 1$ (mod q), $h \not\equiv 1$ (mod q), and it is easy to know that $a^c = a^r$, $a^d = a^s$, $b^c = b^u$, $b^d = b^v$ just as we have done in I. 2) Consequently $r^4 \equiv 1$ (mod q), $u^4 \equiv 1$ (mod p), $s^2 \equiv 1$ (mod q), $v^2 \equiv 1$ (mod p). Hence $a^{h^u} = a^{b^u} = a^{b^c} = (a^{r^3})^{bc} = a^{hr^4} = a^h \Rightarrow h^u \equiv h$ (mod q) $\Rightarrow u \equiv 1$ (mod p), similarly $v \equiv 1$ (mod p), thus $[b, c] = 1 = [b, d]$. Therefore only r and s are to be determined, where

$$r^4 \equiv 1 \equiv s^2 \pmod q. \tag{2}$$

There are at most 8 sets of solutions for the system of congruences (2):

$$r \equiv \pm 1, \pm s_1 \pmod q, \quad s \equiv \pm 1 \pmod q.$$

It has 4 sets of solutions, $r \equiv \pm 1$, $s \equiv \pm 1$ (mod q) when $2^2 \nmid (q-1)$; it has 8 sets of solutions, $r \equiv \pm 1$, $\pm s_1$; $s \equiv \pm 1$ (mod q) when $2^2 \mid (q-1)$. Since

$$O = \langle c \rangle \times \langle d \rangle = \langle c^3 \rangle \times \langle d \rangle = \langle cd \rangle \times \langle d \rangle = \langle c^3 d \rangle \times \langle d \rangle = \langle c \rangle \times \langle c^2 d \rangle$$
$$= \langle c^3 \rangle \times \langle c^2 d \rangle = \langle cd \rangle \times \langle c^2 d \rangle = \langle c^3 d \rangle \times \langle c^2 d \rangle,$$

hence by suitably choosing c and d we find that the groups have 4 types, i. e.

$$G = \langle a, b, c, d \rangle, \ a^q = b^p = c^4 = d^2 = 1 = [b, c] = [b, d] = [c, d], \ a^b = a^h,$$

but

(xx) $a^c = a = a^d$, with $Z(G) = \langle c, d \rangle \simeq Z_4 \times Z_2$;

(xxi) $a^c = a$, $a^d = a^{-1}$, with $Z(G) = \langle c \rangle \simeq Z_4$;

(xxii) $a^c = a^{-1}$, $a^d = a$, with $Z(G) = \langle c^2, d \rangle \simeq E_4$;

(xxiii) $a^c = a^{s_1}$, $a^d = a$, with $Z(G) = \langle d \rangle \simeq Z_2$. (Now it is necessary that $q \equiv 1$ (mod 4).)

III. $O = E_8$.

III. 1) $p \nmid (q-1)$.

Now $G = E_8[Z_{pq}] = \langle a, b, c, d \rangle$, $a^{pq} = b^2 = c^2 = d^2 = 1 = [b, c] = [b, d] = [c, d]$, $a^b = a^r$, $a^c = a^s$, $a^d = a^t$ so that $r^2 \equiv s^2 \equiv t^2 \equiv 1$ (mod pq). Consequently r, s, $t \equiv \pm 1$, $\pm(1 - 2kp)$ (mod pq) which gives us 64 sets (r, s, t); but in view of b, c, d situated symmetrically in G and by suitably choosing b, c, d, we find that the associated group structures have only 5 types, i. e.

$$G=\langle a,\ b,\ c,\ d\rangle,\ a^{pq}=b^2=c^2=d^2=1=[b,\ c]=[b,\ d]=[c,\ d]$$

but

(i) $a^b=a^c=a^d=a$, $Z(G)=G\simeq Z_{pq}\times E_8$;

(ii) $a^b=a^c=a$, $a^d=a^{-1}$, $Z(G)=\langle b,\ c\rangle\simeq E_4$;

(iii) $a^b=a^c=a$, $a^d=a^{1-2kp}$, with $Z(G)=\langle a^q,\ b,\ c\rangle\simeq Z_p\times E_4$;

(iv) $a^b=a^c=a$, $a^d=a^{2kp-1}$, with$Z(G)=\langle a^p,\ b,\ c\rangle\simeq Z_q\times E_4$;

(v) $a^b=a$, $a^c=a^{-1}$, $a^d=a^{1-2kp}$, with $Z(G)=\langle b\rangle\simeq Z_2$.

III. 2) $p\mid(q-1)$

Now the group structures except those mentioned in III. 1) are of the forms such as

$$G=E_8[Z_p[Z_q]]=\langle a,\ b,\ x,\ y,\ z\rangle,\ a^q=b^p=x^2=y^2=z^2=1=[x,\ y]$$
$$=[x,\ z]=[y,\ z],\ a^b=a^h,$$

with more relations $a^x=a^r$, $a^y=a^s$, $a^z=a^t$, $b^x=b^u$, $b^y=b^v$, $b^z=b^w$; henceforth

$$a^{h^u}=a^{b^u}=a^{b^x}=a^{r^2h}=a^h$$

implies $u\equiv1\pmod p$, similarly $v\equiv1\equiv w\pmod p$, i. e. $[x,\ b]=[y,\ b]=[z,\ b]=1$. Consequently it only needs to determine r, s, t so that $r^2\equiv s^2\equiv t^2\equiv1\pmod q$, thus r, s, $t\equiv\pm1\pmod q$ which give us 8 sets $(r,\ s,\ t)$, therefore in view of x, y, z situating symmetrically in G and

$$E_8=\langle x\rangle\times\langle y\rangle\times\langle z\rangle=\langle x\rangle\times\langle yz\rangle\times\langle z\rangle=\langle xz\rangle\times\langle yz\rangle\times\langle z\rangle,$$

we have only 2 distimct types G of groups, say

(vi) $G=\langle a,\ b,\ x,\ y,\ z\rangle$, $a^p=b^q=x^2=y^2=z^2=1=[x,\ b]=[y,\ b]=[z,\ b]=[x,\ y]$ $=[x,\ z]=[y,\ z]=[a,\ x]=[a,\ y]=[a,\ z]$, $a^b=a^h$, with $Z(G)=\langle x,\ y,\ z\rangle\simeq E_8$;

(vii) $G=\langle a,\ b,\ x,\ y,\ z\rangle$, $a^q=b^p=x^2=y^2=z^2=1=[x,\ b]=[y,\ b]=[z,\ b]=[x,\ y]$ $=[x,\ z]=[y,\ z]=[a,\ x]=[a,\ y]$, $a^b=a^h$, $a^z=a^{-1}$, with $Z(G)=\langle x,\ y\rangle\simeq E_4$,

IV. $O=D_8$

IV. 1) $p\nmid(q-1)$.

Now $G=D_8[Z_{pq}]=\langle a,\ x,\ y\rangle$, $a^{pq}=x^4=y^2=1$, $x^y=x^{-1}$, $a^x=a^r$, $a^y=a^s$; of course, $r^4\equiv1\equiv s^2\pmod{pq}$. However, $a^{r^3}=a^{x^3}=a^{x^y}=(a^s)^{xy}=a^{rs^2}$ implies

$$r^3\equiv rs^2\pmod{pq}\Rightarrow r^2\equiv s^2\pmod{pq},$$

consequently $r\equiv\pm1,\ \pm(1-2kp)$; $s\equiv\pm1,\ \pm(1-2kp)\pmod{pq}$ which gives us 16 sets of $(r,\ s)$ by formimg all combinations of r and s. But

$$O=D_8=\langle x,\ y\rangle=\langle x^3,\ y\rangle=\langle x,\ x^2y\rangle=\langle x^3,\ x^2y\rangle=\langle x,\ xy\rangle$$
$$=\langle x^3,\ xy\rangle=\langle x,\ x^3y\rangle=\langle x^3,\ x^3y\rangle$$

shows us that the 16 sets of $(r,\ s)$ only determine 10 types of G, i. e.

$$G=\langle a,\ x,\ y\rangle,\ a^{pq}=x^4=y^2=1,\ x^y=x^{-1},$$

but

(i) $a^x=a^y=a$, with $Z(G)=\langle ax^2\rangle\simeq Z_{2pq}$;

(ii) $a^x=a$, $a^y=a^{-1}$, with $Z(G)=\langle x^2\rangle\simeq Z_2$;

(iii) $a^x=a^{-1}=a^y$, with $Z(G)=\langle x^2\rangle\simeq Z_2$;
(iv) $a^x=a$, $a^y=a^{1-2kp}$, with $Z(G)=\langle a^q x^2\rangle\simeq Z_{2p}$;
(v) $a^x=a$, $a^y=a^{2kp-1}$, with $Z(G)=\langle a^p x^2\rangle\simeq Z_{2q}$;
(vi) $a^x=a^{-1}$, $a^y=a^{1-2kp}$, with $Z(G)=\langle x^2\rangle\simeq Z_2$;
(vii) $a^x=a^{1-2kp}$, $a^y=a$, with $Z(G)=\langle a^q x^2\rangle\simeq Z_{2p}$;
(viii) $a^x=a^{1-2kp}$, $a^y=a^{-1}$, with $Z(G)=\langle x^2\rangle\simeq Z_2$;
(ix) $a^x=a^{2kp-1}$, $a^y=a$, with $Z(G)=\langle a^p x^2\rangle\simeq Z_{2q}$;
(x) $a^k=a^{2kp-1}$, $a^y=a^{-1}$, with $Z(G)=\langle x^2\rangle\simeq Z_2$.

Thence the 5 types (ii), (iii), (vi), (viii), (x) have the center$\simeq Z_2$; (iv) and (vii) have the ceriter$\simeq Z_{2p}$; also (v) and (ix) have the same center Z_{2q}. But by counting the number of elements of order 2 in each group, we obtain the following table:

Table 3

order	type (ii)	(iii)	(vi)	(viii)	(x)	(iv)	(vii)	(v)	(ix)
	Number of elements								
2	$4pq+1$	$2pq+3$	$2(p+q)+1$	$2p(q+1)+1$	$2q(p+1)+1$	$4q+1$	$2q+3$	$4p+1$	$2p+3$

Thus the 10 types (i)—(x) are distinct from one another.

IV. 2) $p\mid(q-1)$.

Now, except for those mentioned in IV. 1) the remaining group structures are of the forms such as

$$G=D_8[Z_p[Z_q]]=\langle a,\ b,\ x,\ y\rangle,\ a^q=b^p=x^4=y^2=1,\ a^b=a^h,$$
$$x^y=x^{-1},\ a^x=a^r,\ a^y=a^s,\ b^x=b^u,\ b^y=b^v.$$

Thus we have $a^{rh^u}=(a^x)^{b^x}=a^{bx}=a^{rh}$, which implies $h^u\equiv h \pmod q\Rightarrow u\equiv1 \pmod p$. Similarly $v\equiv1 \pmod p$. Thence $[x,\ b]=1=[y,\ b]$. Again $a^{r^2s}=a^{x^2y}=a^{yx}=a^{rs}$ implies $r^2\equiv1 \pmod q$, therefore the undetermined r, s must satisfy

$$r^2\equiv1\equiv s^2 \pmod q,$$

which gives us 4 sets of $(r,\ s)$, determined by $r\equiv\pm1$, $s\equiv\pm1 \pmod q$, thus the associated group structures are $G=\langle a,\ b,\ x,\ y\rangle$, $a^q=b^p=x^4=y^2=1=[x,\ b]=[y,\ b]$, but

(xi) $a^x=a=a^y$, with $C_G(Q)=\langle a,\ x,\ y\rangle\simeq Z_q\times D_8$, where $Q=\langle a\rangle$;
(xii) $a^x=a$, $a^y=a^{-1}$, with $C_G(Q)=\langle a,\ x\rangle\simeq Z_{4q}$;
(xiii) $a^x=a^{-1}=a^y$, with $C_G(Q)=\langle a,\ x^2,\ xy)\simeq Z_q\times E_4$.

V. $O=Q_8$.

V. 1) $p\nmid(q-1)$.

Now $G=Q_8[Z_{pq}]=\langle a,\ x,\ y\rangle$, $a^{pq}=x^4=1$, $x^2=y^2$, $x^y=x^{-1}$, $a^x=a^r$, $a^y=a^s$. Hence $r^4\equiv1\equiv s^4$, $r^2\equiv s^2 \pmod{pq}$. But $x^2=[y,\ x]$ implies $a^{r^2}=a^{x^2}=a^{[y,x]}=a^{y^3x^3yx}=a^{s^3r^3sr}=a$, then $r^2\equiv 1 \pmod{pq}$, and therefore $r^2\equiv 1\equiv s^2 \pmod{pq}$. This implies

$$r\equiv \pm 1,\ \pm(1-2kp),\ s\equiv \pm 1,\ \pm(1-2kp) \pmod{pq}.$$

Thus we obtain 16 sets of (r, s). However, in view of the fact that x and y are situated symmetrically in Q_8, and $Q_8=\langle x, y\rangle=\langle xy, y\rangle=\langle x, xy\rangle=\langle y, xy\rangle$, we obtain, by suitably choosing x, y, 5 types of groups, say

$$G=\langle a, x, y\rangle,\ a^{pq}=x^4=1,\ x^2=y^2,\ x^y=x^{-1},$$

but

(i) $a^x=a=a^y$, with $Z(G)=\langle ax^2\rangle\simeq Z_{2pq}$;

(ii) $a^x=a^{-1}=a^y$, with $Z(G)=\langle x^2\rangle\simeq Z_2\simeq Z(G/Z(G))=\langle xyZ(G)\rangle$;

(iii) $a^x=a$, $a^y=a^{1-2kp}$, with $Z(G)=\langle a^qx^2\rangle\simeq Z_{2p}$;

(iv) $a^x=a$, $a^y=a^{2kp-1}$, with $Z(G)=\langle a^px^2\rangle\simeq Z_{2q}$;

(v) $a^x=a^{-1}$, $a^y=a^{1-2kp}$, with $Z(G)=\langle x^2\rangle\simeq Z_2$, $Z(G/Z(G))=1$.

V. 2). $p\mid(q-1)$.

Now $G=Q_8[Z_{pq}]$ or $G=Q_8[Z_p[Z_q]]$. Thence we have 5 types (i)—(v) when $G=Q_8[Z_{pq}]$, and besides these when $G=Q_8\ [Z_p[Z_q]]$, we have also $G=\langle a, b, x, y\rangle$, $a^q=b^p=x^4=1$, $y^2=x^2$, $a^b=a^h$, $x^y=x^{-1}$, $a^x=a^r$, $a^y=a^s$, $b^x=b^u$, $b^y=b^v$. But

$$a^{rh^u}=(a^r)^{b^u}=a^{xb^x}=a^{bx}=a^{hr}$$

implies $u\equiv 1 \pmod p$, similarly $v\equiv 1 \pmod p$, thus $[x, b]=1=[y, b]$. Again

$$a^{r^3s}=a^{x^3y}=a^{yx}=a^{sr}$$

implies $r^2\equiv 1 \pmod q$, similarly $s^2\equiv 1 \pmod q$. Consequently, we have 4 sets of solutions of (r, s), which come from $r\equiv\pm 1$, $s\equiv\pm 1 \pmod q$, and therefore they give only two types of groups, i. e.

$$G=\langle a, b, x, y\rangle,\ a^q=b^p=x^4=1=[x, b]=[y, b],\ x^2=y^2,\ a^b=a^h,\ x^y=x^{-1},$$

but

(vi) $a^x=a=a^y$, $G=Q_8\times Z_p[Z_q]$;

(vii) $a^x=a^{-1}=a^y$, which is evidently not the direct product of Q_8 and $Z_p[Z_q]$.

Summarizing all the results discussed in § 1 above, we obtain the following lemmas (all groups, G Considered with order 2^3pq, $p<q$-odd primes, are assumed to have Sylow towers):

Lemma 1. *If the Sylow 2-subgroups are cyclic (i. e. Z_8), then the groups have*

$\left.\begin{matrix}4\\6\end{matrix}\right\}$ *types when* $\begin{cases} q \text{ and } p\equiv 7 \text{ or } 3 \pmod 8 \text{ and } p\nmid(q-1)\ [\text{(i)—(iv) in case I}], \\ q \text{ and } p\equiv 7 \text{ or } 3 \pmod 8 \text{ and } p\mid(q-1)\ [\text{(i)—(iv), (vxiii), (xxiv) } \textit{in case} \text{ I}]; \end{cases}$

or have $\left.\begin{matrix}6\\8\end{matrix}\right\}$ *types when* $\begin{cases} q\equiv 3 \text{ or } 7,\ p\equiv 5 \pmod 8 \text{ and } p\nmid(q-1)\ [\text{(i)—(vi) } \textit{in case} \text{ I}], \\ q\equiv 3 \text{ or } 7,\ p\equiv 5 \pmod 8\ \textit{and}\ p\mid(q-1)\ [\text{(i)—(vi), (xxiii), (xxiv) } \textit{in case} \text{ I}]; \end{cases}$

or have $\left.\begin{matrix}8\\10\end{matrix}\right\}$ *types when* $\begin{cases} q\equiv 3 \text{ or } 7,\ p\equiv 1 \pmod{8} \text{ and } p\nmid(q-1)\ [\text{(i)—(viii) } \textit{in case } \text{I}], \\ q\equiv 3 \text{ or } 7,\ p\equiv 1 \pmod{8} \text{ and } p\mid(q-1)\ [\text{(i)—(viii), (xxiii),} \\ \quad \text{(xxiv) } \textit{in case } \text{I}]; \end{cases}$

or have $\left.\begin{matrix}6\\9\end{matrix}\right\}$ *types when* $\begin{cases} q\equiv 5,\ p\equiv 7 \text{ or } 3 \pmod{8} \text{ and } p\nmid(q-1)\ [\text{(i)—(iv), (ix), (x)} \\ \quad \textit{in case } \text{I}], \\ q\equiv 5,\ p\equiv 7 \text{ or } 3 \pmod{8} \text{ and } p\mid(q-1)\ [\text{(i)—(iv), (ix), (x),} \\ \quad \text{(xxiii)—(xxv) } \textit{in case } \text{I}]; \end{cases}$

or have $\left.\begin{matrix}10\\13\end{matrix}\right\}$ *types when* $\begin{cases} q\equiv p\equiv 5 \pmod{8} \text{ and } p\nmid(q-1)\ [\text{(i)—(vi), (ix)—(xii) } \textit{in} \\ \quad \textit{case } \text{I}], \\ q\equiv p\equiv 5 \pmod{8} \text{ and } p\mid(q-1)\ [\text{(i)—(vi), (ix)—(xii),} \\ \quad \text{(xxiii)—(xxv) } \textit{in case } \text{I}]; \end{cases}$

or have $\left.\begin{matrix}14\\17\end{matrix}\right\}$ *types when* $\begin{cases} q\equiv 5,\ p\equiv 1 \pmod{8} \text{ and } p\nmid(q-1)\ [\text{(i)—(xiv) } \textit{in case } \text{I}], \\ q\equiv 5,\ p\equiv 1 \pmod{8} \text{ and } p\mid(q-1)\ [\text{(i)—(xiv), (xxiii)—} \\ \quad \text{(xxv) } \textit{in case } \text{I}]; \end{cases}$

or have $\left.\begin{matrix}8\\12\end{matrix}\right\}$ *types when* $\begin{cases} q\equiv 1,\ p\equiv 7 \text{ or } 3 \pmod{8} \text{ and } p\nmid(q-1)\ [\text{(i)—(iv), (ix), (x),} \\ \quad \text{(xv), (xvi) } \textit{in case } \text{I}], \\ q\equiv 1,\ p\equiv 7 \text{ or } 3 \pmod{8} \text{ and } p\mid(q-1)\ [\text{(i)—(iv), (ix), (x),} \\ \quad \text{(xv), (xvi), (xxiii)—(xxvi) } \textit{in case } \text{I}]; \end{cases}$

or have $\left.\begin{matrix}14\\18\end{matrix}\right\}$ *types when* $\begin{cases} q\equiv 1,\ p\equiv 5 \pmod{8} \text{ and } p\nmid(q-1)\ [\text{(i)—(vi), (ix)—(xii),} \\ \quad \text{(xv)—(xviii) } \textit{in case } \text{I}], \\ q\equiv 1,\ p\equiv 5 \pmod{8} \text{ and } p\mid(q-1)\ [\text{(i)—(vi), (ix)—(xii),} \\ \quad \text{(xv)—(xviii), (xxiii)—(xxvi) } \textit{in case } \text{I}]; \end{cases}$

or have $\left.\begin{matrix}22\\26\end{matrix}\right\}$ *types when* $\begin{cases} q\equiv p\equiv 1 \pmod{8} \text{ and } p\nmid(q-1)\ [\text{(i)—(xxii) } \textit{in case } \text{I}], \\ q\equiv p\equiv 1 \pmod{8} \text{ and } p\mid(q-1)\ [\text{(i)—(xxvi) } \textit{in case } \text{I}]. \end{cases}$

Lemma 2. *If the sylow 2-subgroups are abelian of type*$(4, 2)$ *(i. e.* $Z_4\times Z_2$*), then the groups have:*

$\left.\begin{matrix}10\\13\end{matrix}\right\}$ *types when* $\begin{cases} q,\ p\equiv 3, \text{ or } 7 \pmod{8} \text{ and } p\nmid(q-1)\ [\text{i. e. (i)—(x) } \textit{in case } \text{II}], \\ q,\ p\equiv 3 \text{ or } 7 \pmod{8} \text{ and } p\mid(q-1)\ [\text{i. e. (i)—(x), (xx)—(xxii) } \textit{in} \\ \quad \textit{case } \text{II}]; \end{cases}$

or $\left.\begin{matrix}13\\16\end{matrix}\right\}$ *types when* $\begin{cases} q\equiv 3 \text{ or } 7,\ p\equiv 1 \text{ or } 5 \pmod{8} \text{ and } p\nmid(q-1)\ [\text{(i)—(xiii) } \textit{in case } \text{I}], \\ q\equiv 3 \text{ or } 7,\ p\equiv 1 \text{ or } 5 \pmod{8} \text{ and } p\mid(q-1)\ [\text{(i)—(xiii), (xx)—} \\ \quad \text{(xxii) } \textit{in case } \text{II}]; \end{cases}$

or $\left.\begin{matrix}13\\17\end{matrix}\right\}$ *types when* $\begin{cases} q\equiv 1 \text{ or } 5,\ p\equiv 3 \text{ or } 7 \pmod{8} \text{ and } p\nmid(q-1)\ [\text{(i)—(x), (xiv)—} \\ \quad \text{(xvi) } \textit{in case } \text{II}]; \\ q\equiv 1 \text{ or } 5,\ p\equiv 3 \text{ or } 7 \pmod{8} \text{ and } p\mid(q-1)\ [\text{(i)—(x), (xiv)—} \\ \quad \text{(xvi), (xx)—(xxiii) } \textit{in case } \text{II}]; \end{cases}$

or $\left.\begin{matrix}19\\23\end{matrix}\right\}$ *types when* $\begin{cases} q\equiv 1 \text{ or } 5,\ p\equiv 1 \text{ or } 5 \pmod{8} \text{ and } p\nmid(q-1)\ [\text{(i)—(xix) } \textit{in case } \text{II}], \\ q\equiv 1 \text{ or } 5,\ p\equiv 1 \text{ or } 5 \pmod{8} \text{ and } p\mid(q-1)\ [\text{(i)—(xxiii) } \textit{in case} \\ \quad \text{II}]. \end{cases}$

Lemma 3. *If the sylow 2-subgroups are elementary abelian (i. e. $Z_2\times Z_2\times Z_2$), then the groups have*

5 *types when* $p\nmid(q-1)$ *for any* p, q [i. e. (i)—(v) *in case* III]

or 7 *types when* $p\mid(q-1)$ *for any* p, q [(i)—(vii) *in case* III].

Lemma 4. *If the sylow 2-subgroups are dihedral (i. e. D_8), then the groups have*

10 *types when* $p\nmid(q-1)$ *for any* p, q [i. e. (i)—(x) *in case* IV];

or 13 *types when* $p\mid(q-1)$ *for any* p, q [i. e. (i)—(xiii) *in case* IV].

Lemma 5. *If the sylow 2-subgroups are quaternion (i. e. Q_8), then the groups have*

5 *types when* $p\nmid(q-1)$ *for any* p, q [i. e. (i)—(v) *in case* V]

or 7 *types when* $p\mid(q-1)$ *for any* p, q [i. e. (i)—(vii) *in case* V].

Combining lemmas 1—5, we have

Theorem 1. *If G is of order $|G|=2^3pq$ (p, q—odd primes) and G has Sylow-tower, then when $p\nmid(q-1)$, G has:*

(1) 34 *types under* $p,\ q\equiv3$ or 7 (mod 8),

(2) 39 *types under* $q\equiv3$ or 7, $p\equiv5$ (mod 8),

(3) 41 *types under* $q\equiv3$ or 7, $p\equiv1$ (mod 8),

(4) 39 *types under* $q\equiv5$, $p\equiv3$ or 7 (mod 8),

(5) 49 *types under* $q\equiv p\equiv5$ (mod 8),

(6) 53 *types under* $q\equiv5$, $p\equiv1$ (mod 8),

(7) 41 *types under* $q\equiv1$, $p\equiv3$ or 7 (mod 8),

(8) 53 *types rnder* $q\equiv1$, $p\equiv5$ (mod 8),

(9) 61 *types under* $q\equiv1\equiv p$ (mod 8);

while when $p\mid(q-1)$, *G has respectively* 46, 51, 53, 53, 63, 67, 56, 68, 76 *types under* (1), (2), (3), (4), (5), (6), (7), (8), (9).

§ 2. G has no Sylow-tower but is soluble

Since $|G|=2^3pq$ ($p<q$), and G has no Sylow-tower, hence

$$(2^3-1)(2^2-1)(2-1)=21$$

must be divisible by p or q. Thus we need to consider the following three possibilities: (I) $p=7$; (II) $p=3$; (III) $p=5$ but $q=7$.

(I) $p=7$.

Let O, P, Q be a Sylow basis of G. Since $Q\lhd PQ$, $Q\lhd OQ$ ($\because OQ$ is 2-nilpotent), hence $Q\lhd G$, thus in view of the fact that G has no Sylow-tower, OP must contain P as a non-normal subgroup, then the structure of OP is unique,[2] i. e.

$$OP=P[E_8]=\langle x,\ a,\ b,\ c\rangle,$$

$$x^7=a^2=b^2=c^2=1=[a,\ b]=[a,\ c]=[b,\ c],\ a^x=c,\ b^x=a,\ c^x=bc.$$

Consequently, $G=OP[Q]=\langle y, x, a, b, c\rangle$ with more relations $y^q=1$, $y^x=y^u$, $y^a=y^r$, $y^b=y^s$, $y^c=y^t$. But $y^{tu}=y^{xc}=y^{ax}=y^{ru}\Rightarrow t\equiv r \pmod q$;

$$y^{ur}=y^{xa}=y^{bx}=y^{su}\Rightarrow r\equiv s \pmod q;$$

and

$$y^{ust}=y^{xbc}=y^{cx}=y^{tu}\Rightarrow s\equiv 1 \pmod q,$$

thence

$$r\equiv s\equiv t\equiv 1 \pmod q,$$

this shows $[a, y]=[b, y]=[c, y]=1$. Again x induces an automophism of Q, with order dividing $7\neq q$, then $y^x=y^{u_0^i}$, where $u_0^7\equiv 1$, $u_0\not\equiv 1 \pmod q$, $0\leqslant i\leqslant 6$.

If $7\nmid(q-1)$. then x induces the identity automorphism in Q, and we have only one type, say

(i) $G=Z_7[E_8]\times Z_q=\langle x, y, a, b, c\rangle$,

$$x^7=y^q=a^2=b^2=c^2=1=[a, b]=[a, c]=[b, c]=[x, y]=[y, a]$$
$$=[y, b]=[y, c],\ a^x=c,\ b^x=a,\ c^x=bc.\ Z(G)\simeq Z_q.$$

If $7\mid(q-1)$, $y^x=y^{u_0^i}$, $0\leqslant i\leqslant 6$. Thus we need only to consider the cases $1\leqslant i\leqslant 6$.

Let $G=\langle y, x, a, b, c\rangle$,

$$y^q=x^7=a^2=b^2=c^2=1=[a, b]=[a, c]=[b, c]=[a, y]$$
$$=[b, y]=[c, y],\ a^x=c,\ b^x=a,\ c^x=bc,\ y^x=y^{u_0^i};$$

and

$$G_1=\langle y_1, x_1, a_1, b_1, c_1\rangle,\ y_1^q=x_1^7=a_1^2=b_1^2=c_1^2=1=[a_1, b_1]=[a_1, c_1]$$
$$=[b_1, c_1]=[a_1, y_1]=[b_1, y_1]=[c_1, y_1],\ a_1^{x_1}=c_1,\ b_1^{x_1}=a_1,\ c_1^{x_1}=b_1c_1,\ y_1^{x_1}=y^{u_0^j}.$$

Now we go to seek the necessary and sufficient condition that $G\simeq G_1$.

$G\simeq G_1$ iff $G=\langle y', x', a', b', c'\rangle$ with

$$a'^2=b'^2=c'^2=y'^q=x'^7=1=[a', b']=[a', c']=[b', c']=[a', y']$$
$$=[b', y']=[c', y'],\ a'^{x'}=c',\ b'^{x'}=a',\ c'^{x'}=b'c',\ y'^{x'}=y'^{u_0^j}.$$

Hence from $O\lhd G$, $Q\lhd G$, we have $y'=y^r$, $(r, q)=1$, $x'=a^\lambda b^\mu c^\nu y^s x^t$ for some $t(1\leqslant t\leqslant 6)$, $a'=a^{\lambda_1}b^{\mu_1}c^{\nu_1}$, $b'=a^{\lambda_2}b^{\mu_2}c^{\nu_2}$, $c'=a^{\lambda_3}b^{\mu_3}c^{\nu_3}$. But $O=E_8$ can be regarded as a linear space over Z_2, thence let

$$\alpha=\begin{pmatrix}a\\b\\c\end{pmatrix},\quad \alpha'=\begin{pmatrix}a'\\b'\\c'\end{pmatrix},\quad \alpha_1=\begin{pmatrix}a_1\\b_1\\c_1\end{pmatrix},\quad \Lambda=\begin{pmatrix}\lambda_1&\mu_1&\nu_1\\\lambda_2&\mu_2&\nu_2\\\lambda_3&\mu_3&\nu_3\end{pmatrix}\in GL(3, 2),$$

$$\Delta=\begin{pmatrix}0&0&1\\1&0&1\\0&1&1\end{pmatrix}\in GL(3, 2),$$

we can write $\alpha'=\Lambda\alpha$, $\alpha^x=\Delta\alpha$, $\alpha_1^{x_1}=\Delta\alpha_1$. From $G\simeq G_1$ we have $\alpha'^{x'}=\Delta\alpha'=\Delta\Lambda\alpha$, but, in fact, we have also $\alpha'^{x'}=\Lambda\alpha^{x'}=\Lambda\alpha^{x^t}=\Lambda\Delta^t\alpha$, thus $\Delta\Lambda\alpha=\Lambda\Delta^t\alpha$. And

$$y^{ru_0^j}=y'^{u_0^j}=y'^{x'}=(y^r)^{x'}=(y^r)^{x^t}=y^{ru_0^{it}},$$

therefore $it\equiv j \pmod 7$. But the fact that a, b, c are linearly independent implies

$\Lambda^{-1}\Delta\Lambda=\Delta^t$, and it shows that Δ^t and Δ have the same characteristic polynomial $\lambda^3+\lambda^2+1$ in the field Z_2. This holds iff $t=2, 4$, for $|\lambda E-\Delta^t|=\lambda^3+\lambda+1$ when $t=3, 5$, or 6. Thence $it\equiv j \pmod 7$ reduces to $2i\equiv j$ or $4i\equiv j \pmod 7$; consequently, in view of $\left(\frac{2}{7}\right)=\left(\frac{4}{7}\right)=1$, we obtain $\left(\frac{i}{7}\right)=\left(\frac{j}{7}\right)$. This proves that $G\simeq G_1$, iff i and j are at the same time the quadratic residues or non-residues $\pmod 7$. Thus we have three groups, i. e. (i) and

$$G=\langle x, y, a, b, c\rangle, y^q=x^7=a^2=b^2=c^2=1=[a, b]=[a, c]=[b, c]=[a, y]$$
$$=[b, y]=[c, y], a^x=c, b^x=a, c^x=bc,$$

but

(ii) $y^x=y^{u_0}$, (iii) $y^x=y^{u_0^3}$ (Note $Z(G)=1$).

(II) $p=3$.

Now $|G|=2^3\cdot 3\cdot q$, and we consider two cases: $Q\lhd G$ and $Q\ntriangleleft G$.

(II. 1) $Q\lhd G$.

Now we can assert $P\ntriangleleft OP$. This says that the subgroup OP of order $2^3\cdot 3$ of G has no normal subgroup of order 3, consequently the structures of OP have only 3 possibilities;[2]

(1) $OP=Z_3[E_8]=\langle x, a, b, c\rangle, x^3=a^2=b^2=c^2=1=[a, b]=[a, c]=[b, c],$
$$a^x=b, b^x=ab, c^x=c;$$

(2) $OP=Z_2[Z_3[E_4]]=\langle x, a, b, c\rangle, x^3=a^2=b^2=c^2=1=[a, b], a^x=b, b^x=ab,$
$$a^c=b, b^c=a, x^c=x^{-1};$$

(3) $OP=Z_3[Q_8]=\langle x, a, b\rangle, x^3=a^4=1, b^2=a^2, a^b=a^{-1}, a^x=b, b^x=ab.$

In the case (1), we have $G=OP[Q]=\langle y, x, a, b, c\rangle$ with more relations $y^q=1$, $y^x=y^u, y^a=y^r, y^b=y^s, y^c=y^t$. Hence $y^{us}=y^{xa^x}=y^{ax}=y^{ur}\Rightarrow r\equiv s \pmod q$, and

$$y^{rsu}=(y^x)^{ab}=y^{xb^x}=y^{bx}=y^{su}\Rightarrow r\equiv s\equiv 1 \pmod q,$$

i. e. $[a, y]=[b, y]=1$. Again $t^2\equiv 1\equiv u^3 \pmod q$ has at most 6 solutions: say $\begin{cases}u\equiv 1\\ t\equiv 1\end{cases} \pmod q$, $\begin{cases}u\equiv 1\\ t\equiv -1\end{cases} \pmod q$ when $3\nmid(q-1)$; and $u\equiv 1, u_1, u_1^2, t\equiv\pm 1 \pmod q$ when $3|(q-1)$, where $u_1^3\equiv 1 \pmod q$ and $u_1\not\equiv 1 \pmod q$. However, in view of the fact that a and b are situated symmetrically, and, replacing x by x^2, we obtain 4 types of G, say

$$G=\langle x, y, a, b, c\rangle, x^3=y^q=a^2=b^2=c^2=1=[a, b]=[a, c]=[b, c]$$
$$=[a, y]=[b, y], a^x=b, b^x=ab, c^x=c,$$

but

(i) $y^c=y, y^x=y$, with $G=OP\times Q$, $Z(G)=\langle cy\rangle\simeq Z_{2q}$;

(ii) $y^c=y^{-1}, y^x=y$, with $PQ=P\times Q$, $Z(G)=1$;

(iii) $y^c=y, y^x=y^{u_1}$, with $Z(G)=\langle c\rangle\simeq Z_2$;

(iv) $y^c=y^{-1}, y^x=y^{u_1}$, with $Z(G)=1$, but PQ is not the direct product P and Q.

In the case (2), we have $G=\langle y, x, a, b, c\rangle$ with more relations $y^q=1$, $y^x=y^u$, $y^a=y^r$, $y^b=y^s$, $y^c=y^t$. Similarly, we have $r\equiv s\equiv 1 \pmod q$, thus $[a, y]=[b, y]=1$. Again $y^{tu^2}=y^{cx^2}=y^{cx^{-1}}=y^{xc}=y^{ut}\Rightarrow u\equiv 1 \pmod q$, hence $y^x=y$. But $t^2\equiv 1 \pmod q$ implies $t\equiv \pm 1 \pmod q$, which correspond to 2 groups, say

$$G=\langle x, y, a, b, c\rangle,\ x^3=y^q=a^2=b^2=c^2=1=[a, b]=[a, y]=[b, y]$$
$$=[x, y],\ a^x=b,\ b^x=ab,\ a^c=b,\ b^c=a,\ x^c=x^{-1},$$

but

(v) $y^c=y$, with $Z(G)=\langle y\rangle\simeq Z_q$;

(vi) $y^c=y^{-1}$, with $Z(G)=1$.

In the case (3), $G=\langle y, x, a, b\rangle$, $y^q=1$, $y^x=y^u$, $y^a=y^r$, $y^b=y^s$ and the relatinos of x, a, b are mentioned in (3). But $y^{ru}=y^{ax}=y^{xb}=y^{us}=y^{su}=y^{bx}=y^{xab}=y^{urs}$ and, similarly, $y^{su}=y^{ru}$, hence $r\equiv s\equiv 1 \pmod q$, i. e. $[a, y]=[b, y]=1$. And $u^3\equiv 1 \pmod q$ has at most three solustions: $u\equiv 1$; u_1, $u_1^2 \pmod q$, where $u_1^3\equiv 1 \pmod q$ and $u_1\not\equiv 1 \pmod q$, $u\equiv 1 \pmod q$ when $3\nmid (q-1)$; $u\equiv 1$, u_1, $u_1^2 \pmod q$ when $3\mid (q-1)$. Hence we have two types (replacing x, a, b by x^2, a^3, a^3b respectively we find that $u=u_1^2$ will reduce to $u=u_1$), say

$$G=\langle x, y, a, b\rangle,\ x^3=y^q=a^4=1=[a, y]=[b, y],\ b^2=a^2,\ a^x=b,\ b^x=ab,\ a^b=a^{-1},$$

but

(vii) $y^x=y$, with $Z(G)=\langle a^2y\rangle=Z_{2q}$;

(viii) $y^x=y^{u_1}$, with $Z(G)=\langle a^2\rangle\simeq Z_2$.

(II. 2) $Q\ntriangleleft G$.

At first, we shall show that there is a normal subgroup A of G such that $|G:A|=3$. Since $Q\lhd PQ$ implies $P\leqslant N_G(Q)$, then $Q\leqslant O_{p'}(G)$ [3], (Lemma 2.6). But $Q\ntriangleleft G\Rightarrow Q<O_{p'}(G)\leqslant OQ$. Suppose, on the contrary, that $O_{p'}(G)<OQ$, then $|O_{p'}(G)|<2^3q$ $(q>3)$ implies Q char in $O_{p'}(G)\lhd G$. It contradicts to the condition $Q\ntriangleleft G$. Hence it must be $O_{p'}(G)=OQ=A$(say). Thence $A\lhd G$ and $|G:A|=3$.

Now $Q\ntriangleleft G\Rightarrow Q\ntriangleleft A$, and for $q>3$, it must be that $q=7$, therefore the structure of A of order $2^3\cdot 7$ is unique[2] as in (I), i. e.

$$A=\langle y, a, b, c\rangle,\ y^7=a^2=b^2=c^2=[a, b]=[a, c]$$
$$=[b, c]=1,\ a^y=c,\ b^y=a,\ c^y=bc.$$

Again, by sylow's theorem, $Q\lhd PQ$, we have $G=P[A]=\langle y, x, a, b, c\rangle$ with all relations among y, a, b, c as mentioned above and the other relations: $x^3=1$, $y^x=y^r$, $\alpha^x=\Lambda\alpha$, where $\alpha=\begin{pmatrix} a \\ b \\ c \end{pmatrix}$, $\Lambda\in GL(3, 2)$ as in (I), hence $\Lambda^3=E$ (the identity matrix of $GL(3, 2)$). Let $\Delta=\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}\in GL(3, 2)$, then $\alpha^y=\Delta\alpha$ and $\Delta^7=E$. But

$$\Delta\Lambda\alpha=\Delta\alpha^x=\alpha^{yx}=\alpha^{xy^r}=\Lambda\Delta^r\alpha\Rightarrow\Delta^r=\Lambda^{-1}\Delta\Lambda;$$

and $x^3=1$, $y^x=y^r$ implies $r^3\equiv 1 \pmod 7$, hence $r\equiv 1, 2, 4 \pmod 7$. Since

$$GL(3, 2)=SL(3, 2)=PSL(3, 2)^{[4]}$$

is simple and is of order $2^3\cdot 3\cdot 7$, hence it has 8 Sylow 7-subgroups. Consequently, we have $|GL(3,2):N|=8$, where $N=N_{GF(3,2)}(\langle\Delta\rangle)$ is the normalizer of $\langle\Delta\rangle$ in $GL(3,2)$, i. e. $|N|=3\cdot 7$.

Take $\Delta_1=\begin{pmatrix}0&1&0\\1&1&0\\0&0&1\end{pmatrix}\in GL(3, 2)$, then $\Delta_1^3=E$, and $\Delta_1^{-1}\Delta\Delta_1=\Delta^2$, hence $\Delta_1\in N$, and $N=\langle\Delta, \Delta_1\rangle$; also $\Lambda\in N\Rightarrow\Lambda=\Delta^i\Delta_1^j(j=1, 2)$, thus $\Lambda^{-1}\Delta\Lambda=\Delta^r$ implies $\Delta_1^{-j}\Delta\Delta_1^j=\Delta^r$, i. e. $\Delta^2=\Delta^r$. Consequently $j=0$ and $i=0$ when $r\equiv 1 \pmod 7$; $j=1$ when $r\equiv 2 \pmod 7$; $j=2$ when $r\equiv 4 \pmod 7$. Thus the group type when $r\equiv 1 \pmod 7$ is

(ix) $G=\langle x, y, a, b, c\rangle$, $x^3=y^7=a^2=b^2=c^2=1=[a, b]=[a, c]=[b, c]=[x, y]=[x, a]=[x, b]=[x, c]$, $a^y=c$, $b^y=a$, $c^y=bc$, with $Z(G)=\langle x\rangle\simeq Z_3$.

When $r\equiv 2$ or $4 \pmod 7$, $\Lambda=\Delta^i\Delta_1$ or $=\Delta^i\Delta_1^2$, replacing x by $y^{-i}x$ or $(y^{-i}x)^2$ respectively, we odtain another type of G:

(x) $G=\langle x, y, a, b, c\rangle$, $x^3=y^7=a^2=b^2=c^2=1=[a, b]=[a, c]=[b, c]=[x, c]$, $a^y=c$, $b^y=a$, $c^y=bc$, $y^x=y^2$, $a^x=b$, $b^x=ab$, with $Z(G)=1$

(III) $p=5$, but $q=7$.

Now $|G|=2^3\cdot 5\cdot 7$, by Sylow's theorem we have $PQ=P\times Q$ and $P\lhd OP$, hence $P\lhd G=OPQ$. Thus, in view of the fact that G has no Sylow-tower, it follows $Q\ntriangleleft OQ$ (order $2^3\cdot 7$), consequently

$$OQ=\langle y, a, b, c\rangle, y^7=1=a^2=b^2=c^2=[a, b]=[a, c]=[b, c],$$
$$a^y=c,\ b^y=a,\ c^y=bc^{[2]}$$

Thus $O=\langle a, b, c\rangle$ is elementary abelian and $O\lhd OQ$. Therefore from $P\lhd G$ we have $OP\lhd G$. Now we can assert that $O\lhd G$.

On the contrary, if $O\ntriangleleft G$ were true, then $O\ntriangleleft OP$, and since $|OP|=2^3\cdot 5$, hence OP is of the unique structure[2], i. e. $OP=\langle x, a, b, c\rangle$, $x^5=1=[a, x]=[b, x]$, $x^c=x^{-1}$. Thence $Z(OP)=\langle a, b\rangle$, $|G/Z(OP)|=2\cdot 5\cdot 7$, and

$$|G:PQ\cdot Z(OP)|=2\Rightarrow PQ\cdot Z(OP)\lhd G,$$

therefore sylow's theorem shows that $Q\lhd PQ\cdot Z(OP)$, thus Q cher in $PQ\cdot Z(OP)$, which implies $Q\lhd G$. Ir shows that G has Sylow-tower G, PQ, Q, and 1, and it is not allowable.

Hence $O\lhd G\Rightarrow O\lhd OP\Rightarrow OP=O\times P \Rightarrow G=OQ\times P$, Consequently, from the fact that $Q\ntriangleleft OQ$, $O\lhd OQ$, and O is elementary abelian, it follows that, $OQ=Z_7[E_8]$, and hence $G=Z_7[E_8]\times Z_5$, i. e.

(i) $G=Z_7[E_8]\times Z_5=\langle y, x, a, b, c\rangle$, $y^7=x^5=a^2=b^2=c^2=1=[a, b]=[a, c]=[b, c]=[a, x]=[b, x]=[c, x]=[y, x]$, $a^y=c$, $b^y=a$, $c^y=bc$.

Summarizing all mentioned in § 2, we obtain the following lemmas (all groups

G considered are of orders $2^3pq(p<q)$, and have no Sylow towers, but are soluble; thence we heve $p=3$, 7, or $p=5$ and $q=7$):

Lemma 1. *G has only one type for $p=7$ and $7\nmid(q-1)$, i. e.* (i) *in* (I); *has 3 types, i. e.* (i), (ii), (iii) *in* (I) *when $p=7$ and $7\mid(q-1)$.*

Lemma 2. *When $p=3$, the group G has 5 types* (i), (ii), (v), (vi), (vii) *in* (II) *for $3\nmid(q-1)$; for $3\mid(q-1)$, G has 8 or 10 types*(i)—(viii) *or* (i)—(x) *in* (II)) *according as $q\neq 7$ or $q=7$ respectively.*

Lemma 3. *When $p=5$, $q=7$, the group G has only one type, i. e.* (*i*) *in* (*III*).

Combining Lemmas 1—3, we have

Theorem 2. *If G is of order $|G|=2^3pq(p<q$, odd primes) and G has no Sylow-tower but is soluble, then when $p\nmid(q-1)$, G has only one type for $p=7$ or for $p=5$ and $q=7$, and five types for $p=3$; but when $p\mid(q-1)$, G has 3 types for $p=7$, 8 types for $p=3$ and $q\neq 7$, or 10 types for $p=3$ and $q=7$.*

§ 3. G is non-soluble

At first, we state Brauer's theorem ([5], Theorem 2): If a group G of order 2^mpq is simple, then G is only $\mathfrak{U}_5\simeq PSL(2, 5)$ or $PSL(2, 7)$. Thus the group G of order 2^3pq is PSL (2, 7) if G is simple. In view of $|G|=2^3pq$, if G is non-simple, we know easily that there is a non-trivial normal subgroup N of G, such that N or G/N is simple and isomorphic to $\mathfrak{U}_5$ as G is non-soluble. Thus when $N\simeq\mathfrak{U}_5$, then $|G|=120$, so that $G\simeq\mathfrak{S}_5$ or $Z_2\times\mathfrak{U}_5$[6]; when $G/N\simeq\mathfrak{U}_5$, then $|N|=2$, so that $N=Z(G)$, and it follows that $G\simeq SL$ (2, 5) if $G=G'=[G, G]$ or $G\simeq Z_2\times\mathfrak{U}_5$ if $G\neq G'=[G, G]$.

Summarizing all mentioned above, we obtain the following

Theorem 3. *If G is of order $|G|=2^3pq(p<q$, odd primes), and G is non-soluble, then $p=3$, $q=5$ or 7. And for $q=5$, G hat three types, i. e* $Z_2\times\mathfrak{U}_5$, $\mathfrak{S}_5$, $SL(2, 5)$; for *$q=7$, G has only one type, i. e. PSL (2.7).*

Combining Theorem- 1—3, we have

Theorem. *If G is of order $|G|=2^3pq(p<q-$odd primes), then when $p\nmid(q-1)$, G has*

(1) 34 *types under $p\ q\equiv 3$ or 7* (mod 8) *but $p\neq 3$, 7;*

(2) 39 *types under $q\equiv 3$* (mod 4), *$p\equiv 5$* (mod 8) *but $q\neq 7$;*

(3) 39 *types* under *$q\equiv 5$, $p\equiv 3$ or 7* (mod 8) *but $p\neq 3$;*

(4) 41 *types under $q\equiv 3$ or 7, $p\equiv 1$* (mod 8);

(5) 49 *types under $q\equiv 5\equiv p$* (mod 8);

(6) 53 *types under $q\equiv 5$, $p\equiv 1$* (mod 8);

(7) 41 *types under $q\equiv 1$, $p\equiv 3$ or 7* (mod 8) *but $p\neq 3$ or 7;*

(8) 53 *types under $q\equiv 1$, $p\equiv 5$* (mod 8);

(9) 61 *types under* $q \equiv 1 \equiv p \pmod 8$.

While when $p \mid (q-1)$, *G has respectively* 46, 51, 53, 53, 63, 67, 56, 68, 76 *types under* (1), (2), (3), (4), (5), (6), (7), (8), (9).

When $3 \nmid (q-1)$, *the group G of order* $2^3 \cdot 3q$ *has*

(1)′ 37 *types under* $q \equiv 3 \pmod 4$;

(3)′ 42 *types under* $q \equiv 5 \pmod 8$ *bmt* $q \neq 5$ *and* 45 *types under* $q = 5$(*i. e.* $|G| = 2^3 \cdot 3 \cdot 5$);

(7)′ 44 *types under* $q \equiv 1 \pmod 8$.

While when $3 \mid (q-1)$, *G has* 54 *types under* (1)′ *but* $q \neq 7$; *and* 57 *types under* $q = 7$; 61 *types under* $q \equiv 5 \pmod 8$, 64 *types under* (7)′.

When $7 \nmid (q-1)$, *the group G of order* $2^3 \cdot 7 \cdot q$ *has*

(1)″ 35 *types under* $q \equiv 3 \pmod 4$;

(3)″ 40 *types under* $q \equiv 5 \pmod 8$;

(7)″ 42 *types under* $q \equiv 1 \pmod 8$.

While when $7 \mid (q-1)$, *G has respectively* 49, 56, 59 *types under* (1)″, (3)″, (7)″. *And finally, the group G of order* $2^3 \cdot 5 \cdot 7$ *has* 40 *types.*

Similarly, we can derive all the structures of groups G of order r^3pq(r, p, q-prime).

References

[1] Zhang Yuanda, On finite groups of order 2^3p^2, *Chinese Ann. Math.*, **4 B**: 1. (1983).

[2] 张远达,有限群构造(下),科学出版社(1982), 687—713.

[3] Rowley, P. J., The π-separabilty of certain factorizable groups, *Math. Z.*, **153** (1977), 219—228.

[4] 华罗庚、万哲先,典型群,上海科技出版社(1963).

[5] Brauer, R. & Tuan, H. F., On simple groups of finite order, *I. Bull. Ann. Math. Soc.*, **51** (1945), 756—766.

[6] Kurzweil, H. Endliche Gruppen, Springer-Verlag (1977), 162.