Chin. Ann. of Math.
4B (1) 1983

THE STRUCTURES OF GROUPS OF ORDER $2^3 P^2$

ZHANG YUANDA (张远达)
(Wuhan University)

Abstract

In this paper, the following theorem is proved:

Let p be a prime distinct from 3 and 7, then the groups of order $2^3 p^2$ have

1) 60 types when $p\equiv 1 \pmod 8$,
2) 52 types when $p\equiv 5 \pmod 8$,
3) 42 types when $p\equiv 3, 7 \pmod 8$.

To determine the structures of groups of order n is a classifical problem in finite group theory. It is well known that a group of prime order p is cyclic, and a group of order p^2 is always abelian. O. Hölder has determined the groups of order pqr, p^3, p^4, p^2q (p, q, r are distinct primes)[1]; A. E. Western has done those of order p^3q[2]; recently the groups of order p^2q^2 have been solved[3]. In this paper we try to determine the structures of groups of order 2^3p^2 (p–odd prime).

Notation: $A\lhd G$ means that A is normal in G, Z_n is cyclic of order n, Z_n^* means the reduced residue (multiplicative) group (mod n), $o(G)$ denotes the order of the group G. $Z(G)$–the center of G.

Now let $o(G)=2^3p^2$, and n_p denote the number of Sylow p–subgroups in G. Then Sylow's theorem shows $n_p\equiv 1 \pmod p$ and $n_p \mid o(G)=2^3p^2$, thence $n_p=1, 2, 4,$ or 8. Therefore $n_p=1$ when $p\neq 3, 7$, i. e. G has a unique Sylow p–subgroup A, hence $A\lhd G$. $o(A)=p^2$ implies that A is either cyclic or elementary abelian. In § 1 consider the case A being cyclic, and in § 2 treat the case A being elementary abelian.

§ 1. $A=\langle a\rangle$, cyclic of order p^2

Let B be a Sylow 2–subgroup of G. Then $G=AB$, $A\cap B=1$. $o(B)=2^3$ implies that B is either cyclic of order 8, or abelian of type [4, 2], or elementary abelian, or quaternion, or dihedral. We shall treat them separately as follows

$$B=Z_8=\langle b\rangle,\ b^8=1. \tag{1.1}$$

Now $G=\langle a, b\rangle$, $a^{p^2}=1=b^8$, $b^{-1}ab=a^r$. Thence $r^8\equiv 1 \pmod{p^2}$, consequently one and onlyone of the four cases $r\equiv 1$, $r\equiv -1$, $r^2\equiv -1$ and $r^4\equiv -1 \pmod{p^2}$ can hold. $r\equiv 1$ and $r\equiv -1 \pmod{p^2}$ give respectively two types, say:

Manuscript received March 24, 1981

(i) $G=Z_{2^3p^2}$;

(ii) $G=\langle a, b\rangle$, $a^{p^2}=1=b^8$, $b^{-1}ab=a^{-1}$; $Z(G)=\langle b^2\rangle\simeq Z_4$.

When $r^2\equiv-1 \pmod{p^2}$, $p\equiv1 \pmod 4$. Let $Z^*_{p^2}=\langle\alpha\rangle(\simeq Z_{p(p-1)})$, then $r^2\equiv-1 \pmod{p^2}$ has two solutions $r\equiv\pm\alpha^{\frac{p(p-1)}{4}}$. But $b^{-1}ab=a^r$ implies $bab^{-1}=a^{-r}$, and $G=\langle a, b\rangle=\langle a, b^{-1}\rangle$, this shows that we have only one type, say:

(iii) $G=\langle a, b\rangle$, $a^{p^2}=1=b^8$, $b^{-1}ab=a^r$, $r^2\equiv-1 \pmod{p^2}$, where $p\equiv1 \pmod 4$,

$$Z(G)=\langle b^4\rangle\simeq Z_2.$$

When $r^4\equiv-1 \pmod{p^2}$, $p\equiv1 \pmod 8$. Now $r^4\equiv-1 \pmod{p^2}$ has 4 solutions $r_{(i)}\equiv\alpha^{\frac{ip(p-1)}{8}} \pmod{p^2}$, $(i=1, 3, 5, 7)$; while $b^{-1}ab=a^{r_{(1)}}$ implies $b^{-j}ab^j=a^{r^j_{(1)}}=a^{r_{(j)}}$ $(j=3, 5, 7)$, and also $G=\langle a, b\rangle=\langle a, b^j\rangle$. This says that these 4 solutions determine the same group G, say:

(iv) $G=\langle a, b\rangle$, $a^{p^2}=1=b^8$, $b^{-1}ab=a^r$, $r^4\equiv-1 \pmod{p^2}$, where $p\equiv1 \pmod 8$]

$$Z(G)=1.$$

$$B=\langle x, y\rangle,\ x^4=y^2=1=[x, y]\ (=x^{-1}y^{-1}xy). \tag{1.2}$$

Now $G=\langle a, x, y\rangle$, $a^{p^2}=1=x^4=y^2=[x, y]$, $x^{-1}ax=a^r$, $y^{-1}ay=a^s$, so that $r^4\equiv1\equiv s^2 \pmod{p^2}$. But $s^2\equiv1 \pmod{p^2}$ implies $s\equiv\pm1 \pmod{p^2}$; and $r^4\equiv1 \pmod{p^2}$ implies either $r\equiv\pm1 \pmod{p^2}$, or $r\equiv\pm\alpha^{\frac{p(p-1)}{4}} \pmod{p^2}$ when $p\equiv1 \pmod 4$, where $Z^*_{p^2}=\langle\alpha\rangle$.

Since $B=\langle x\rangle\times\langle y\rangle=\langle x^3\rangle\times\langle y\rangle=\langle x\rangle\times\langle x^2y\rangle=\langle x^3\rangle\times\langle x^2y\rangle$, and $x^{-1}ax=a^{\alpha^{\frac{p(p-1)}{4}}}$, $y^{-1}ay=a\Rightarrow x^{-3}ax^3=a^{-\alpha^{\frac{p(p-p)}{4}}}$, $(x^2y)^{-1}a(x^2y)=a^{-1}$, hence $r\equiv\pm\alpha^{\frac{p(p-1)}{4}}$ and $s\equiv\pm1 \pmod{p^2}$ will determine only one group G. Again $B=\langle x\rangle\times\langle y\rangle=\langle xy\rangle\times\langle y\rangle$ and $x^{-1}ax=a$, $y^{-1}ay=a^{-1}\Rightarrow(xy)^{-1}a(xy)=a^{-1}$ also show that $x^{-1}ax=a^{\pm1}$, $y^{-1}ay=a^{-1}$ determine the same group G. Consequently the case (1.2) gives us 4 groups, say:

(i) $G\simeq Z_{p^2}\times Z_4\times Z_2$;

(ii) $G=\langle a, x, y\rangle$, $x^{-1}ax=a$, $y^{-1}ay=a^{-}$, $Z(G)=\langle x\rangle=Z_4$;

(iii) $G=\langle a, x, y\rangle$, $x^{-1}ax=a^{-1}$, $y^{-1}ay=a$, $Z(G)=\langle x^2\rangle\times\langle y\rangle=Z_2\times Z_2$;

(iv) $G=\langle a, x, y\rangle$, $x^{-1}ax=a^r$, $y^{-1}ay=a$, $r^2\equiv-1 \pmod{p^2}$ and $p\equiv1 \pmod 4$,

$$Z(G)=\langle y\rangle=Z_2.$$

$$B=\langle x\rangle\times\langle y\rangle\times\langle z\rangle=Z_2\times Z_2\times Z_2. \tag{1.3}$$

Now $G=\langle a, x, y, z\rangle$, $a^{p^2}=x^2=y^2=z^2=1=[x, y]=[x, z]=[y, z]$, $x^{-1}ax=a^r$, $y^{-1}ay=a^s$, $z^{-1}az=a^t$. Thence $r^2\equiv s^2\equiv t^2\equiv1 \pmod{p^2}$, implying $r\equiv\pm1$, $s\equiv\pm1$, $t\equiv\pm1 \pmod{p^2}$. In view of x, y, z being situated symmetrically in G, we only need to consider 4 cases: 1) $r\equiv s\equiv t\equiv1 \pmod{p^2}$, 2) $r\equiv s\equiv1\equiv-t \pmod{p^2}$, 3) $r\equiv1\equiv-s\equiv-t \pmod{p^2}$, 4) $r\equiv s\equiv t\equiv-1 \pmod{p^2}$.

Since $B=\langle x\rangle\times\langle y\rangle\times\langle z\rangle=\langle x\rangle\times\langle yz\rangle\times\langle z\rangle=\langle xz\rangle\times\langle yz\rangle\times\langle z\rangle$, and $x^{-1}ax=a$, $y^{-1}ay=a$, $z^{-1}az=a^{-1}\Rightarrow(yz)^{-1}a(yz)=a^{-1}$, $(xz)^{-1}a(xz)=a^{-1}$, hence 2)、3)、4) give the same group. This says that case (1.3) gives us two groups, i. e.

(i) $G=\langle a, x, y, z\rangle=Z_{p^2}\times Z_2\times Z_2\times Z_2$,

(ii) $G=\langle a, x, y, z\rangle$, $a^{p^2}=x^2=y^2=z^2=[x, y]=[x, z]=[y, z]=1$,

$$x^{-1}ax=y^{-1}ay=z^{-1}az=a^{-1}.$$

$$B=\langle x, y\rangle,\ x^4=1,\ x^2=y^2,\ y^{-1}xy=x^{-1}(\text{Quaternion}). \tag{1.4}$$

Now $G=\langle a, x, y\rangle$, $a^{p^2}=1=x^4$, $x^2=y^2$, $y^{-1}xy=x^{-1}$, $x^{-1}ax=a^r$, $y^{-1}ay=a^s$, so that $r^4\equiv1\equiv s^4$ and $r^2\equiv s^2 (\bmod p^2)$. By means of $y^{-1}xy=x^{-1}$, we have

$$a^{r^3}=xax^{-1}=(y^{-1}xy)^{-1}a(y^{-1}xy)=y^{-1}x^{-1}a^{s^3}xy=a^{rs^4}=a^r,$$

hence $r^2\equiv1 (\bmod p^2)$. Consequently $r\equiv\pm1$, $s\equiv\pm1$ $(\bmod p^2)$. Since x and y situate symmetrically in G, we only need to consider 3 possibilities, i. e. 1) $r\equiv1\equiv s (\bmod p^2)$, 2) $r\equiv-1\equiv s (\bmod p^2)$, 3) $r\equiv1\equiv-s (\bmod p^2)$. In view of $B=\langle x, y\rangle=\langle x_1, y\rangle$, $x_1=xy$, and $\begin{cases} x^{-1}ax=a^{-1} \\ y^{-1}ay=a^{-1}\end{cases}\Rightarrow\begin{cases} x_1^{-1}ax_1=a \\ y^{-1}ay=a^{-1}\end{cases}$, it follows that the two subcases 2) and 3) give the same group. Thus case (1.4) gives us two groups, say:

(i) $G=\langle a, x, y\rangle$, $x^{-1}ax=a=y^{-1}ay$, $Z(G)=\langle ax^2\rangle\simeq Z_{2p^2}$;

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

in which $a^{p^2}=1=x^4$, $x^2=y^2$, $y^{-1}xy=x^{-1}$.

$$B=\langle x, y\rangle,\ x^4=1=y^2,\ y^{-1}xy=x^{-1}(\text{Dihedral}). \tag{1.5}$$

Now $G=\langle a, x, y\rangle$, $a^{p^2}=1=x^4=y^2$, $y^{-1}xy=x^{-1}$, $x^{-1}ax=a^r$, $y^{-1}ay=a^s$, thence we have $r^4\equiv1\equiv s^2$ $(\bmod p^2)$. Also by $y^{-1}xy=x^{-1}$ we find $a^{r^3}=a^{rs^2}=a^r\Rightarrow r^2\equiv1$ $(\bmod p^2)$, therefore $r\equiv\pm1$, $s\equiv\pm1$ $(\bmod p^2)$. Since $B=\langle x, y\rangle=\langle x, y_1\rangle$, $y_1=xy$ and $x^{-1}ax=a^{-1}=y^{-1}ay\Rightarrow y_1^{-1}ay_1=a$, hence $r\equiv s\equiv-1$ $(\bmod p^2)$ and $r\equiv-1$, $s\equiv1$ $(\bmod p^2)$ determine the same group, consequently (1.5) gives us three groups, say:

(i) $G=\langle a, x, y\rangle$, $x^{-1}ax=a=y^{-1}ay$, $Z(G)=\langle ax^2\rangle\simeq Z_{2p^2}$;

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

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

in all of which we have $a^{p^2}=x^4=y^2=1$, $y^{-1}xy=x^{-1}$.

Note that (ii) is non-isomorphic to (iii), since the group (ii) has $4p^2+1$ elements of order 2 ($a^\lambda x^\alpha y$, x^2; $0\leqslant\lambda<p^2$, $0\leqslant\alpha<4$), and (iii) has $2p^2+3$ elements of order 2 ($a^\lambda x^2y$ and $a^\lambda y$, x^2, xy, x^3y).

Summarizing § 1, we have

Lemma 1. *If p is an odd prime $\neq3$, 7, then the groups of order 2^3p^2, when the Sylow p-subgroups are cyclic, have:*

(1) 15 *types when* $p\equiv1(\bmod 8)$ [(i)、(ii)、(iii)、(iv) of (1.1) *and* (1.2); (i)、(ii) of (1.3) *and* (1.4); (i)、(ii)、(iii) *of* (1.5)];

(2) 14 *types when* $p\equiv5(\bmod 8)$ [*all occuring in* (1) *except* (iv) *of* (1.1)];

(3) 12 *types when* $p\equiv3(\bmod 4)$ [*all occuring in* (1) *except* (iii) *and* (iv) of (1.1), *and* (iv) *of* (1.2)].

§ 2. $A=\langle a\rangle\times\langle b\rangle=Z_p\times Z_p$

As we have done in § 1, $G=AB$, $A\cap B=1$, where B is a Sylow 2-subgroup of G, hence $o(B)=8$, and B is one of (1.1)—(1.5).

$$B=Z_8=\langle x\rangle. \tag{2.1}$$

Now $G=\langle a, b, x\rangle$, $a^p=b^p=[a, b]=1=x^8$, $\begin{cases} x^{-1}ax=a^\alpha b^\beta \\ x^{-1}bx=a^\gamma b^\delta \end{cases}$, $\Delta=\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\in GL(2,p)$; $x^8=1$ implies $\Delta^8=E$ in Z_p (prime field of characteristic p), thence the minimum polynomial $m(\lambda)$ of Δ is of the property $m(\lambda)\,|\,(\lambda^8-1)$. But $m(\lambda)\,|\det(\lambda E-\Delta)$, therefore $m(\lambda)$ is of degree $\partial^\circ m(\lambda)$ either $=1$ or $=2$.

(I) $\partial^\circ m(\lambda)=1$.

Now $m(\lambda)=\lambda-\xi$, $\Delta=\xi E$, $\xi^8\equiv1$ (mod p), hence either $\xi\equiv1$, or $\xi\equiv-1$, or $\xi^2\equiv-1$, or $\xi^4\equiv-1$ (mod p), one and only one holds. Consequently we have 4 types of groups G, say:

(i) $G=\langle a, b, x\rangle$, $\begin{cases} x^{-1}ax=a \\ x^{-1}bx=b \end{cases}$, i. e. $G\simeq Z_p\times Z_p\times Z_8$;

(ii) $G=\langle a, b, x\rangle$, $\begin{cases} x^{-1}ax=a^{-1} \\ x^{-1}bx=b^{-1} \end{cases}$, $Z(G)=\langle x^2\rangle\simeq Z_4$;

(iii) $G=\langle a, b, x\rangle$, $\begin{cases} x^{-1}ax=a^\xi \\ x^{-1}bx=b^\xi \end{cases}$, where $\xi^2\equiv-1$ (mod p) and hence $p\equiv1$ (mod 4), with $Z(G)=\langle x^4\rangle\simeq Z_2$,

(Note that two solutions of $\xi^2\equiv-1$ (mod p) determine the same structure (iii) as we have done in proving (iii) of (1.1) in § 1);

(iv) $G=\langle a, b, x\rangle$, $\begin{cases} x^{-1}ax=a^\zeta \\ x^{-1}bx=b^\zeta \end{cases}$, where $\zeta^4\equiv-1$ (mod p) and hence $p\equiv1$ (mod 8), with $Z(G)=1$,

(Note the 4 solutions of $\zeta^4\equiv-1$ (mod p) determine the same structure (iv) which can be shown similarly as done in proving (iv) of (1.1) in § 1).

(II) $\partial^\circ m(\lambda)=2$.

Now $m(\lambda)=\det(\lambda E-\Delta)=\lambda^2+\omega\lambda+\theta$ with $\omega=-(\alpha+\delta)$, $\theta=\alpha\delta-\beta\gamma$.

(II. 1) $\omega\equiv0$ (mod p). Now $m(\lambda)=\lambda^2+\theta\Rightarrow E=\Delta^8=\theta^4E$, thence $\theta^4\equiv1$ (mod p), consequently either $\theta\equiv1$, or $\theta\equiv-1$, or $\theta^2\equiv-1$ (mod p), one and only one holds.

$\theta\equiv1$ (mod p)$\Rightarrow m(\lambda)=\lambda^2+1$, thus the rational canonical form of Δ is $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, showing that a, b can be suitably chosen so that $\begin{cases} x^{-1}ax=b \\ x^{-1}bx=a^{-1} \end{cases}$, hence

(v) $G=\langle a, b, x\rangle$, $\begin{cases} x^{-1}ax=b \\ x^{-1}bx=a^{-1} \end{cases}$, $Z(G)=\langle x^4\rangle\simeq Z_2$.

$\theta\equiv -1 \pmod p \Rightarrow m(\lambda)=(\lambda-1)(\lambda+1)\Rightarrow \Delta\sim\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$, showing that we can suitably choose a, b with the type

(vi) $G=\langle a, b, x\rangle$, $\begin{cases} x^{-1}ax=a \\ x^{-1}bx=b^{-1}\end{cases}$, $Z(G)=\langle ax^2\rangle\simeq Z_{4p}$.

$\theta^2\equiv -1 \pmod p\Rightarrow p\equiv 1 \pmod 4$; and $\theta^2\equiv -1 \pmod p$ has two solutions θ and $-\theta$. For the solution θ, $m(\lambda)=\lambda^2+\theta$ means that the rational canonical form of Δ is $\begin{pmatrix}0 & 1\\ -\theta & 0\end{pmatrix}$, hence a, b can be chosen suitably with the group structure

(vii) $G=\langle a, b, x\rangle$, $\begin{cases} x^{-1}ax=b \\ x^{-1}bx=a^{-\theta}\end{cases}$, where $\theta^2\equiv -1 \pmod p$ and $p\equiv 1 \pmod 4$,

$$Z(G)=1.$$

Note: putting $a_1=b$, $b_1=a$, $x_1=x^7$, we have $G=\langle a, b, x\rangle=\langle a_1, b_1, x_1\rangle$ with $x_1^{-1}a_1x_1=b_1$ and $x_1^{-1}b_1x_1=a_1^{\theta}$. This shows that the two solutions of $\theta^2\equiv -1 \pmod p$ determine the same group structure (vii).

(II. 2) $\omega\not\equiv 0 \pmod p$. Since $m(\lambda)=\lambda^2+\omega\lambda+\theta$ is a factor of

$$\lambda^8-1=(\lambda-1)(\lambda+1)(\lambda^2+1)(\lambda^4+1),$$

hence our problem is reduced to find the quadratic factors of λ^8-1, with the coefficient of λ not zero. In later, we set $Z_p^*=\langle r\rangle$.

a) $p\equiv 5 \pmod 8$. Now $\lambda^2+1=(\lambda-r^{\frac{p-1}{4}})(\lambda+r^{\frac{p-1}{4}})$, and

$$\lambda^4+1=(\lambda^2-r^{\frac{p-1}{4}})(\lambda^2+r^{\frac{p-1}{4}}).$$

But it is easy to check that $\lambda^2\pm r^{\frac{p-1}{4}}$ are all irreducible in the prime field Z_p, in view of $p\not\equiv 1 \pmod 8$, therefore the quadratic factors of the form $m(\lambda)=\lambda^2+\omega\lambda+\theta$ with $\omega\not\equiv 0 \pmod p$ of λ^8-1 are only $(\lambda\pm 1)(\lambda\pm r^{\frac{p-1}{4}})$, consequently Δ is similar to $\begin{pmatrix}\pm 1 & 0\\ 0 & \pm r^{\frac{p-1}{4}}\end{pmatrix}$ in the field Z_p, this shows that a, b can be so chosen that $x^{-1}ax=a^{\pm 1}$, $x^{-1}bx=b^{\pm r^{\frac{p-1}{4}}}$. Again $G=\langle a, b, x\rangle=\langle a, b, x^3\rangle$ means that $\begin{pmatrix}1 & 0\\ 0 & \pm r^{\frac{p-1}{4}}\end{pmatrix}$ determine the same structure of G. Similarly $\begin{pmatrix}-1 & 0\\ 0 & \pm r^{\frac{p-1}{4}}\end{pmatrix}$ do so too. Hence we obtain two groups, say:

(viii) $G=\langle a, b, x\rangle$, $x^{-1}ax=a$, $x^{-1}bx=b^{r^{\frac{p-1}{4}}}$; $Z(G)=\langle ax^4\rangle\simeq Z_{2p}$.

(ix) $G=\langle a, b, x\rangle$, $x^{-1}ax=a^{-1}$, $x^{-1}bx=b^{r^{\frac{p-1}{4}}}$; $Z(G)=\langle x^4\rangle\simeq Z_2$.

} $p\equiv 5 \pmod 8$.

b) $p\equiv 1 \pmod 8$. Now

$$\lambda^4+1=(\lambda-\varepsilon)(\lambda+\varepsilon)(\lambda-\varepsilon^3)(\lambda+\varepsilon^3),\ \lambda^2+1=(\lambda-\varepsilon^2)(\lambda+\varepsilon^2),$$

where $\varepsilon=r^{\frac{p-1}{8}}$. Thence the quadratic factors of the form $m(\lambda)=\lambda^2+\omega\lambda+\theta$ with $\omega\not\equiv 0$

(mod p) of λ^8-1 are only of the forms such as $(\lambda\pm\varepsilon^i)(\lambda\pm\varepsilon^j)$, $1\leqslant i<j\leqslant 4$. From $\varepsilon^i\neq\pm\varepsilon^j$ we can find $P\in GL(2, p)$ so that $P^{-1}\Delta P=\begin{pmatrix}\pm\varepsilon^i & 0\\ 0 & \pm\varepsilon^j\end{pmatrix}$, i. e. a, b can be chosen with $x^{-1}ax=x^{\pm\varepsilon^i}$, $x^{-1}bx=b^{\pm\varepsilon^j}$, $1\leqslant i<j\leqslant 4$.

Because of a, b being symmetrically situated in G, and $G=\langle a, b, x^k\rangle$ with $k=1$, 3, 5, 7, it is easy to know that $\begin{pmatrix}\pm\varepsilon & 0\\ 0 & \varepsilon^2\end{pmatrix}$, $\begin{pmatrix}-\varepsilon^2 & 0\\ 0 & \pm\varepsilon^3\end{pmatrix}$ determine the same group. Similarly $\begin{pmatrix}\pm\varepsilon & 0\\ 0 & -\varepsilon^2\end{pmatrix}$, $\begin{pmatrix}\varepsilon^2 & 0\\ 0 & \pm\varepsilon^3\end{pmatrix}$; $\begin{pmatrix}\pm\varepsilon & 0\\ 0 & \varepsilon^4\end{pmatrix}$, $\begin{pmatrix}\pm\varepsilon^3 & 0\\ 0 & \varepsilon^4\end{pmatrix}$; and $\begin{pmatrix}\pm\varepsilon & 0\\ 0 & -\varepsilon^4\end{pmatrix}$, $\begin{pmatrix}\pm\varepsilon^3 & 0\\ 0 & -\varepsilon^4\end{pmatrix}$ respectively do so. Again $\begin{pmatrix}\varepsilon & 0\\ 0 & \varepsilon^3\end{pmatrix}$ and $\begin{pmatrix}-\varepsilon & 0\\ 0 & -\varepsilon^3\end{pmatrix}$, $\begin{pmatrix}\varepsilon & 0\\ 0 & -\varepsilon^3\end{pmatrix}$ and $\begin{pmatrix}-\varepsilon & 0\\ 0 & \varepsilon^3\end{pmatrix}$, $\begin{pmatrix}\varepsilon^2 & 0\\ 0 & \varepsilon^4\end{pmatrix}$ and $\begin{pmatrix}-\varepsilon^2 & 0\\ 0 & \varepsilon^4\end{pmatrix}$, or $\begin{pmatrix}\varepsilon^2 & 0\\ 0 & -\varepsilon^4\end{pmatrix}$ and $\begin{pmatrix}-\varepsilon^2 & 0\\ 0 & -\varepsilon^4\end{pmatrix}$ all respectively give the same types of groups. Therefore we have in this case eight distinct group structures, respectively represented by the following eight matrices, say

$$\begin{pmatrix}\varepsilon & 0\\ 0 & \varepsilon^2\end{pmatrix}, \begin{pmatrix}\varepsilon & 0\\ 0 & -\varepsilon^2\end{pmatrix}, \begin{pmatrix}\varepsilon & 0\\ 0 & -1\end{pmatrix}, \begin{pmatrix}\varepsilon & 0\\ 0 & 1\end{pmatrix}, \begin{pmatrix}\varepsilon & 0\\ 0 & \varepsilon^3\end{pmatrix}, \begin{pmatrix}\varepsilon & 0\\ 0 & -\varepsilon^3\end{pmatrix}, \begin{pmatrix}\varepsilon^2 & 0\\ 0 & -1\end{pmatrix}$$

and $\begin{pmatrix}\varepsilon^2 & 0\\ 0 & 1\end{pmatrix}$. However $\begin{pmatrix}\varepsilon^2 & 0\\ 0 & 1\end{pmatrix}$ and $\begin{pmatrix}\varepsilon^2 & 0\\ 0 & -1\end{pmatrix}$ determine groups respectively represented by the types (viii) and (ix) mentioned in the subcase $p\equiv5 \pmod 8$, i. e. the types (viii) and (ix) will also occur in the case $p\equiv1 \pmod 8$. Except them, we have the other six types, such as

$$\left.\begin{array}{l}
(\text{x})\ G=\langle a, b, x\rangle,\ x^{-1}ax=a^{\varepsilon},\ x^{-1}bx=b^{\varepsilon^2},\ Z(G)=1;\\
(\text{xi})\ G=\langle a, b, x\rangle,\ x^{-1}ax=a^{\varepsilon},\ x^{-1}bx=b^{-\varepsilon^2},\ Z(G)=1;\\
(\text{xii})\ G=\langle a, b, x\rangle,\ x^{-1}ax=a^{\varepsilon},\ x^{-1}bx=b^{\varepsilon^3},\ Z(G)=1;\\
(\text{xiii})\ G=\langle a, b, x\rangle,\ x^{-1}ax=a^{\varepsilon},\ x^{-1}bx=b^{-\varepsilon^3},\ Z(G)=1;\\
(\text{xiv})\ G=\langle a, b, x\rangle,\ x^{-1}ax=a^{\varepsilon},\ x^{-1}bx=b^{-1},\ Z(G)=1;\\
(\text{xv})\ G=\langle a, b, x\rangle,\ x^{-1}ax=a^{\varepsilon},\ x^{-1}bx=b,\ Z(G)=1.
\end{array}\right\} p\equiv1 \pmod 8$$

c) $p\equiv3 \pmod 8$ Now $\left(\frac{-2}{p}\right)=(-1)^{\frac{p-1}{2}}\cdot(-1)^{\frac{p^2-1}{8}}=1\Rightarrow\exists\ s$, so that $s^2\equiv-2 \pmod p$, hence $\lambda^4+1=(\lambda^2+s\lambda-1)(\lambda^2-s\lambda-1)$; but λ^2+1 is irreducible in the field Z_p ($\because p\not\equiv1 \pmod 4$), therefore the quadratic factors of the forms $m(\lambda)=\lambda^2+\omega\lambda+\theta$ with $\omega\not\equiv0 \pmod p$ are of only two: $\lambda^2+s\lambda-1$ and $\lambda^2-s\lambda-1$. If $m(\lambda)=\lambda^2+s\lambda-1$, then $\alpha+\delta=-s$, $\alpha\delta-\beta\gamma=-1$, $\Delta=\begin{pmatrix}\alpha & \gamma\\ \beta & \delta\end{pmatrix}\Rightarrow\Delta^{-1}=\Delta^7=\begin{pmatrix}\alpha' & \beta'\\ \gamma' & \delta'\end{pmatrix}$ with $\alpha'=\alpha+s$, $\delta'=\delta+s$, $\beta'=\beta$, $\gamma'=\gamma$, thus $\alpha'+\delta'=s$, $\det\Delta^7=\alpha'\delta'-\beta'\gamma'=-1$; consequently from $G=\langle a, b, x\rangle=\langle a, b, x^7\rangle$, it follows that $m(\lambda)=\lambda^2+s\lambda-1$ and $m(\lambda)=\lambda^2-s\lambda-1$ determine the same group-structure, therefore without loss of generality we can assume $m(\lambda)$

$=\lambda^2-s\lambda-1$, and thence the rational canonical form of Δ is $\begin{pmatrix}0 & 1\\ 1 & s\end{pmatrix}$, i. e. a, b can be chosen suitably so that

(xvi) $G=\langle a, b, x\rangle$, $x^{-1}ax=b$, $x^{-1}bx=ab^s$, with $s^2\equiv-2(\text{mod } p)$, $p\equiv3(\text{mod } 8)$, where $Z(G)=1$.

d) $p\equiv7(\text{mod } 8)$. Now $\left(\frac{2}{p}\right)=1\Rightarrow\exists\ t$, so that $t^2\equiv2(\text{mod } p)$, thus

$$\lambda^4+1=(\lambda^2+t\lambda+1)(\lambda^2-t\lambda+1),$$

λ^2+1 is also irreducible in the field Z_p, hence the factors $m(\lambda)=\lambda^2+\omega\lambda+\theta$ with $\omega\not\equiv0$ (mod p) of λ^8-1 are of only two: $\lambda^2+t\lambda+1$ and $\lambda^2-t\lambda+1$. From $G=\langle a, b, x\rangle=\langle a, b, x^3\rangle$, we readily find that $\lambda^2+t\lambda+1$ and $\lambda^2-t\lambda+1$ give the same group, as we have done in c). Hence we obtain a new type, as

(xvii) $G=\langle a, b, x\rangle$, $x^{-1}ax=b$, $x^{-1}bx=a^{-1}b^t$, with $t^2\equiv2$ (modp), $p\equiv7$ (mod 8), where $Z(G)=1$.

In order to explain that (i)—(xvii) are distinct from one another, we must show that the 3 types (iii)、(v)、(ix) are non-isomorphic with one another, and also that the 10 types (iv)、(vii)、(x)、(xi)、(xii)、(xiii)、(xiv)、(xv)、(xvi) and (xvii) are non-isomorphic with one another. For example, (iii)$\cong$(v) means that there exist two elements $a_1=a^\mu b^\nu$, $b_1=a^\sigma b^\tau$ in (iii) with $\bar{\Delta}=\begin{pmatrix}\mu & \nu\\ \sigma & \tau\end{pmatrix}\in GL\ (2, p)$, and an element $y=x^j$ ($j=1$, 3, 5, or 7) of order 8 in (iii), such that

$$y^{-1}a_1y=b_1,\ y^{-1}b_1y=a_1^{-1},$$

equivalent to

$$a^\sigma b^\tau=a^{\mu\xi^j}b^{\nu\xi^j},\ a^{-\mu}b^{-\nu}=a^{\sigma\xi^j}b^{\tau\xi^j},$$

thence we have $\xi^j\ \bar{\Delta}=\begin{pmatrix}\sigma & \tau\\ -\mu & -\nu\end{pmatrix}=\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}\bar{\Delta}\Rightarrow\xi^jE=\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}$, evidently impossible. By the similar method, we can prove the others. Hence we have

Lemma 2. *If p is an odd prime$\neq3$, 7, then the groups of order 2^3p^2, when the Sylow p-subgroups are elementary abelian and the Sylow 2-subgroups are cyclic, have*

(1) 15 *types when* $p\equiv1$(*mod* 8) [(i)—(xv) of (2.1)];

(2) 8 *types when* $p\equiv5$(*mod* 8) [(i)—(ix) of (2.1), except(iv)];

(3) 5 *types when* $p\equiv3$(*mod* 8) [(i)、(ii)、(v)、(vi)、(xvi) of (2.1)];

(4) 5 *types when* $p\equiv7$(*mod* 8) [(i)、(ii)、(v)、(vi)、(xvii) of (2.1)].

$$B=\langle x\rangle\times\langle y\rangle\simeq Z_4\times Z_2(x^4=1=y^2). \tag{2.2}$$

Now $G=\langle a, b, x, y\rangle$, $a^p=b^p=[a, b]=1=x^4=y^2=[x, y]$,

$$\begin{cases}x^{-1}ax=a^\alpha b^\beta\\ x^{-1}bx=a^\gamma b^\delta\end{cases},\ \begin{cases}y^{-1}ay=a^\mu b^\nu\\ y^{-}by=a^\sigma b^\tau\end{cases},\ \Delta=\begin{pmatrix}\alpha & \gamma\\ \beta & \delta\end{pmatrix}\text{ and }\Lambda=\begin{pmatrix}\mu & \sigma\\ \nu & \tau\end{pmatrix}$$

all $\in GL(2, p)$. Thence $\Delta^4=E=\Lambda^2$ and $\Delta\Lambda=\Lambda\Delta$ (in the field Z_p). Let $m_\Delta(\lambda)$ and $m_\Lambda(\lambda)$ denote the minimum polynomials of Δ and Λ respectively.

If $\partial^\circ m_\Delta(\lambda)=1$, $m_\Delta(\lambda)\mid(\lambda^4-1)=\lambda-1)(\lambda+1)(\lambda^2+1)$ will imply that either $m_\Delta(\lambda)=\lambda-1$; or $m_\Delta(\lambda)=\lambda+1$; or $m_\Delta(\lambda)=\lambda\pm\xi$ when $p\equiv1 \pmod 4$, where $\xi=r^{\frac{p-1}{4}}$ and $Z_p^*=\langle r\rangle$. But $m_\Delta(\lambda)=\lambda-\xi$ means $x^{-1}ax=a^\xi$ and $x^{-1}bx=b^\xi$; while $G=\langle a, b, x, y\rangle=\langle a, b, x^3, y\rangle$ will imply therefore $x^{-3}ax^3=a^{-\xi}$ and $x^{-3}bx^3=b^{-\xi}$; this says that $m_\Delta(\lambda)=\lambda-\xi$ and $m_\Delta(\lambda)=\lambda+\xi$ are of no difference. Hence under the case $\partial^\circ m_\Delta(\lambda)=1$, we only need to consider three possibilities, i. e. $\begin{cases}x^{-1}ax=a\\x^{-1}bx=b\end{cases}$, or $\begin{cases}x^{-1}ax=a^{-1}\\x^{-1}bx=b^{-1}\end{cases}$, or $\begin{cases}x^{-1}ax=a^\xi\\x^{-1}bx=b^\xi\end{cases}$ when $p\equiv1 \pmod 4$ where $\xi=r^{\frac{p-1}{4}}$ and $Z_p^*=\langle r\rangle$.

If $\partial^\circ m_\Delta(\lambda)=2$, either $m(\lambda_\Delta)=\lambda^2-1$, or $=\lambda^2+1$, or $=(\lambda\pm1)(\lambda\pm\xi)$ when $p\equiv1 \pmod 4$, thus there exists $P\in GL(2, p)$ such that $P^{-1}\Delta P=\begin{pmatrix}1&0\\0&-1\end{pmatrix}$, or $=\begin{pmatrix}0&1\\-1&0\end{pmatrix}$ (rational canonical form), or $=\begin{pmatrix}\pm1&0\\0&\pm\xi\end{pmatrix}$ when $p\equiv1 \pmod 4$. Combining the two cases $\partial^\circ m_\Delta(\lambda)=1$ and $=2$, it follows that a, b can be suitably chosen so that we need only to consider the following nine possibilities:

$$(1)\ \Delta=E,\quad (2)\ \Delta=-E,\quad (3)\ \Delta=\begin{pmatrix}1&0\\0&-1\end{pmatrix},\quad (4)\ \Delta=\begin{pmatrix}0&1\\-1&0\end{pmatrix},\quad (5)\ \Delta=\xi E,$$

$$(6)\ \Delta=\begin{pmatrix}1&0\\0&\xi\end{pmatrix},\quad (7)\ \Delta=\begin{pmatrix}-1&0\\0&\xi\end{pmatrix},\quad (8)\ \Delta=\begin{pmatrix}1&0\\0&-\xi\end{pmatrix},\quad (9)\ \Delta=\begin{pmatrix}-1&0\\0&-\xi\end{pmatrix}.$$

Note that ξ will occur iff $p\equiv1 \pmod 4$.

Since $G=\langle a, b, x, y\rangle=\langle a, b, x^3, y\rangle$, hence (8)、(9) respectively coincide with (6)、(7). Thence only 7 cases (1)—(7) are needed to be considered.

When a, b, x have been chosen, we consider Λ. Of course, $\Lambda^2=E$ implies $m_\Lambda(\lambda)=\lambda-1$, or $=\lambda+1$, or $=\lambda^2-1$. But $m_\Lambda(\lambda)=\lambda\mp1$ implies $\Lambda=\pm E$, evidently satisfying $\Delta\Lambda=\Lambda\Delta$. It therefore remains to consider the case $m_\Lambda(\lambda)=\lambda^2-1$, which implies $\mu+\tau=0$ and $\mu^2+\nu\sigma=1$, i. e. $\Lambda=\begin{pmatrix}\mu&\nu\\\sigma&-\mu\end{pmatrix}$ with $\det\Lambda\equiv-1 \pmod p$.

Evidently $\Lambda=\begin{pmatrix}\mu&\nu\\\sigma&-\mu\end{pmatrix}$ commutes with $\Delta=E$, $-E$, ξE in (1), (2), (5) respectively; but such Λ commutes with $\Delta=\begin{pmatrix}1&0\\0&-1\end{pmatrix}$ of (3), or with $\Delta=\begin{pmatrix}\pm1&0\\0&\xi\end{pmatrix}$ of (6). and (7) when and only when $\nu=0=\sigma$ (which therefore in turn implies $\mu\equiv\pm1$ (mod p)), thus $\Lambda=\begin{pmatrix}1&0\\0&-1\end{pmatrix}$ or $=\begin{pmatrix}-1&0\\0&1\end{pmatrix}$; while $\Lambda=\begin{pmatrix}\mu&\nu\\\sigma&-\mu\end{pmatrix}$ commutes with $\Delta=\begin{pmatrix}0&1\\-1&0\end{pmatrix}$ of (4) iff $\mu\equiv0$ and $\nu+\sigma\equiv0 \pmod p\Rightarrow\nu^2\equiv-1 \pmod p$ which can hold only when $p\equiv1 \pmod 4$, and thence $\nu\equiv\pm\xi \pmod p$, consequently $\Lambda=\pm\xi\Delta$.

Therefore all possible combinations of (Δ, Λ) are: (1°) $\Delta=E=\Lambda$; (2°) $\Delta=E=-\Lambda$; (3°) $\Delta=-E=-\Lambda$; (4°) $\Delta=-E=\Lambda$; (5°) $\Delta=\begin{pmatrix}1&0\\0&-1\end{pmatrix}=\Lambda$; (6°) $\Delta=\begin{pmatrix}1&0\\0&-1\end{pmatrix}$

$=-A$; (7°) $\Delta=\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$, $A=E$; (8°) $\Delta=\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$, $A=-E$; (9°) $\Delta=\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}$, $A=E$; (10°) $\Delta=\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}$, $A=-E$; (11°) $\Delta=\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}$, $A=-\xi\Delta$; (12°) $\Delta=\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}$, $A=\xi\Delta$; (13°) $\Delta=\xi E$, $A=E$; (14°) $\Delta=\xi E$, $A=-E$; (15°) $\Delta=\begin{pmatrix}1 & 0\\ 0 & \xi\end{pmatrix}$, $A=E$; (16°) $\Delta=\begin{pmatrix}1 & 0\\ 0 & \xi\end{pmatrix}$, $A=-E$; (17°) $\Delta=\begin{pmatrix}1 & 0\\ 0 & \xi\end{pmatrix}$, $A=\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$; (18°) $\Delta=\begin{pmatrix}1 & 0\\ 0 & \xi\end{pmatrix}$, $A=\begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix}$; (19°) $\Delta=\begin{pmatrix}-1 & 0\\ 0 & \xi\end{pmatrix}$, $A=E$; (20°) $\Delta=\begin{pmatrix}-1 & 0\\ 0 & \xi\end{pmatrix}$, $A=-E$; (21°) $\Delta=\begin{pmatrix}-1 & 0\\ 0 & \xi\end{pmatrix}$, $A=\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$; (22°) $\Delta=\begin{pmatrix}-1 & 0\\ 0 & \xi\end{pmatrix}$, $A=\begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix}$; (23°) $\Delta=E$, $A=\begin{pmatrix}\mu & \nu\\ \sigma & -\mu\end{pmatrix}$; (24°) $\Delta=-E$, $A=\begin{pmatrix}\mu & \nu\\ \sigma & -\mu\end{pmatrix}$; (25°) $\Delta=\xi E$, $A=\begin{pmatrix}\mu & \nu\\ \sigma & -\mu\end{pmatrix}$.

Since (23°)、(24°)、(25°) all mean that $m_A(\lambda)=\lambda^2-1=(\lambda-1)(\lambda+1)$, hence $P\in GL(2, p)$ exists so that $P^{-1}AP=\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$, and also $P^{-1}(kE)P=kE\ (k=1, -1, \xi)$ of course holds, this says that a, b can be suitably chosen so that (23°)、(24°)、(25°) can be reduced respectively to (23°_1) $\Delta=E$, $A=\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$; ($24^\circ_1$) $\Delta=-E$, $A=\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$; ($25^\circ_1$) $\Delta=\xi E$, $A=\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$.

Again

$$B=\langle x\rangle\times\langle y\rangle=\langle x^3\rangle\times\langle y\rangle=\langle xy\rangle\times\langle y\rangle=\langle x^3y\rangle\times\langle y\rangle$$
$$=\langle x\rangle\times\langle x^2y\rangle=\langle x^3\rangle\times\langle x^2y\rangle=\langle xy\rangle\times\langle x^2y\rangle=\langle x^3y\rangle\times\langle x^2y\rangle,$$

also
$$\begin{cases}x\to\Delta\\ y\to A\end{cases}\Rightarrow x^3\to\Delta^3,\ xy\to\Delta A,\ x^3y\to\Delta^3A,\ x^2y\to\Delta^2A,$$

this says that (2°) and (4°) give the same G, simply denoted by (2°) = (4°). Similarly (5°) = (23°_1), (6°) = (24°_1) by the symmetry of a、b in G, hence (9°) = (10°), (11°) = (12°), (13°) = (14°), (15°) = (17°), (19°) = (21°), (16°) = (18°) = (20°) = (22°). Therefore we need only to treat the types (1°)、(2°)、(3°)、(23°_1)、(24°_1)、(7°)、(8°)、(9°)、(13°)、(15°)、(16°)、(19°)、(25°_1) and (12°). But in (12°), $G=\langle a, b, x, y\rangle=\langle a_1, b_1, x_1, y_1\rangle$ where $a_1=a^{-\xi}b$, $b_1=a^{\xi}b$, $x_1=x^3y$, $y_1=y$ so that

$$\begin{cases}x_1^{-1}a_1x_1=a_1^{\xi}\\ x_1^{-1}b_1x_1=b_1^{\xi},\end{cases}\quad\begin{cases}y_1^{-1}a_1y_1=a_1\\ y_1^{-1}b_1y_1=b_1^{-1},\end{cases}$$

this says that (12°) = (25°_1). Consequently we have only 13 group structures, determined by (1°)、(2°)、(3°)、(23°_1)、(24°_1)、(7°)、(8°)、(9°)、(13°)、(15°)、(16°)、(19°)、(25°_1) respectively, which are written as follows:

(i) $G=Z_p\times Z_p\times Z_4\times Z_2$;

(ii) $G=\langle a, b, x, y\rangle$, $\begin{cases} x^{-1}ax=a \\ x^{-1}bx=b \end{cases}$, $\begin{cases} y^{-1}ay=a^{-1} \\ y^{-1}by=b^{-1} \end{cases}$, $Z(G)=\langle x\rangle\simeq Z_4$;

(iii) $G=\langle a, b, x, y\rangle$, $\begin{cases} x^{-1}ax=a^{-1} \\ x^{-1}bx=b^{-1} \end{cases}$, $\begin{cases} y^{-1}ay=a \\ y^{-1}by=b \end{cases}$, $Z(G)=\langle x^2\rangle\times\langle y\rangle\simeq Z_2\times Z_2$;

(iv) $G=\langle a, b, x, y\rangle$, $\begin{cases} x^{-1}ax=a \\ x^{-1}bx=b \end{cases}$, $\begin{cases} y^{-1}ay=a \\ y^{-1}by=b^{-1} \end{cases}$, $Z(G)=\langle ax\rangle\simeq Z_{4p}$;

(v) $G=\langle a, b, x, y\rangle$, $\begin{cases} x^{-1}ax=a^{-1} \\ x^{-1}bx=b^{-1} \end{cases}$, $\begin{cases} y^{-1}ay=a \\ y^{-1}by=b^{-1} \end{cases}$, $Z(G)=\langle x^2\rangle\simeq Z_2$;

(vi) $G=\langle a, b, x, y\rangle$, $\begin{cases} x^{-1}ax=a \\ x^{-1}bx=b^{-1} \end{cases}$, $\begin{cases} y^{-1}ay=a \\ y^{-1}by=b \end{cases}$

$$Z(G)=\langle a\rangle\times\langle x^2\rangle\times\langle y\rangle\simeq Z_p\times Z_2\times Z_2;$$

(vii) $G=\langle a, b, x, y\rangle$, $\begin{cases} x^{-1}ax=a \\ x^{-1}bx=b^{-1} \end{cases}$, $\begin{cases} y^{-1}ay=a^{-1} \\ y^{-1}by=b^{-1} \end{cases}$, $Z(G)=\langle x^2\rangle\simeq Z_2$;

(viii) $G=\langle a, b, x, y\rangle$, $\begin{cases} x^{-1}ax=b \\ x^{-1}bx=a^{-1} \end{cases}$, $\begin{cases} y^{-1}ay=a \\ y^{-1}by=b \end{cases}$, $Z(G)=\langle y\rangle\simeq Z_2$;

(ix) $G=\langle a, b, x, y\rangle$, $\begin{cases} x^{-1}ax=a^{\xi} \\ x^{-1}bx=b^{\xi} \end{cases}$, $\begin{cases} y^{-1}ay=a \\ y^{-1}by=b \end{cases}$, $Z(G)=\langle y\rangle\simeq Z_2$;

(x) $G=\langle a, b, x, y\rangle$, $\begin{cases} x^{-1}ax=a \\ x^{-1}bx=b^{\xi} \end{cases}$, $\begin{cases} y^{-1}ay=a \\ y^{-1}by=b \end{cases}$, $Z(G)=\langle ay\rangle\simeq Z_{2p}$;

(xi) $G=\langle a, b, x, y\rangle$, $\begin{cases} x^{-1}ax=a \\ x^{-1}bx=b^{\xi} \end{cases}$, $\begin{cases} y^{-1}ay=a^{-1} \\ y^{-1}by=b^{-1} \end{cases}$, $Z(G)=1$;

(xii) $G=\langle a, b, x, y\rangle$, $\begin{cases} x^{-1}ax=a^{-1} \\ x^{-1}bx=b^{\xi} \end{cases}$, $\begin{cases} y^{-1}ay=a \\ y^{-1}by=b \end{cases}$, $Z(G)=\langle y\rangle\simeq Z_2$;

(xiii) $G=\langle a, b, x, y\rangle$, $\begin{cases} x^{-1}ax=a^{\xi} \\ x^{-1}bx=b^{\xi} \end{cases}$, $\begin{cases} y^{-1}ay=a \\ y^{-1}by=b^{-1} \end{cases}$, $Z(G)=1$.

By the similar method applied in the end of (2.1) it is easy to see that the types (v)、(vii)、(viii)、(ix)、(xii) are non-isomorphic with one another, although they have centers$\simeq Z_2$. Similarly (xi) is not isomorphic to (xiii). Thus the group structures (i)—(xiii) are actually distinct from one another. Hence we have the following

Lemma 3. *If p is an odd prime$\neq 3$, 7, then the groups of order 2^3p^2 when the Sylow p-subgroups are elementary abelian and the Sylow 2-subgroups are abelian of type* [4, 2] *have:*

(1) 13 *types in case* $p\equiv 1$ (*mod* 4) [i. e. (i)—(xiii) of (2.2)],

(2) 8 *types in case* $p\equiv 3$ (*mod* 4) [i. e. (i)—(viii) of (2.2)].

$$B=\langle x\rangle\times\langle y\rangle\times\langle z\rangle\simeq Z_2\times Z_2\times Z_2 (x^2=y^2=z^2=1). \qquad (2.3)$$

Now $G=\langle a, b, x, y, z\rangle$, $a^p=b^p=[a, b]=1=x^2=y^2=z^2=[x, y]=[x, z]=[y, z]$,

$$\begin{cases} x^{-1}ax=a^{\alpha}b^{\beta} \\ x^{-1}bx=a^{\gamma}b^{\delta}, \end{cases} \begin{cases} y^{-1}ay=a^{\mu}b^{\nu} \\ y^{-1}by=a^{\sigma}b^{\tau}, \end{cases} \begin{cases} z^{-1}az=a^{\xi}b^{\zeta} \\ z^{-1}bz=a^{\eta}b^{\theta}, \end{cases}$$

with $$\Delta=\begin{pmatrix}\alpha & \gamma\\ \beta & \delta\end{pmatrix},\quad \Lambda=\begin{pmatrix}\mu & \sigma\\ \nu & \tau\end{pmatrix},\quad K=\begin{pmatrix}\xi & \zeta\\ \eta & \theta\end{pmatrix}$$
all lying in $GL(2, p)$. From $x^2=y^2=z^2=1=[x, y]=\cdots$, it follows that $\Delta^2=\Lambda^2=K^2=E$ and Δ, Λ, K are commutative two-by-two, therefore there exist $P\in GL(2, p)$ so that $P^{-1}\Delta P$, $P^{-1}\Lambda P$, $P^{-1}KP$ are simultaneously all diagonal matrices E, $-E$, J, or $-J$, where $J=\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$, this says that we can choose a, b so that $\Delta=E$, $-E$, J, or $-J$; but in view of a, b being situated symmetrically in G, we find that $\Delta=J$ and $\Delta=-J$ are of no difference, hence concerning Δ it needs us to consider 3 possibilities: $\Delta=E$, $-E$, J. After Δ has been given, Λ and K have respectively 4 possibilities i. e. E, $-E$, J and $-J$; but y, z situating symmetrically in G implies that we need only to treat the combinations of Λ, K, and not the permutations of them, consequently the number of combinations of Λ, K is equal to $C^2_{4+2-1}=10$, therefore the number of combinations of (Δ, Λ, K) is equal to $3\times 10=30$, as

Δ	E	E	E	E	E	E	E	E	E	E	−E	−E	−E	−E	−E	−E	−E	−E	−E	−E	J	J	J…
Λ	E	E	E	E	−E	−E	−E	J	J	−J	E	E	E	E	−E	−E	−E	J	J	−J	E	E	E…
K	E	−E	J	−J	−E	J	−J	J	−J	−J	E	−E	J	−J	−E	J	−J	J	−J	−J	E	−E	J…

Since x, y, z situate symmetrically in G, hence it is sufficient to consider the combinations of Δ, Λ, K, disregarding their permutations, thus only 19 cases on the above table are worthy to be discussed, denoted by

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)	(13)	(14)	(15)	(16)	(17)	(18)	(19)
$x\to\Delta$	E	E	E	E	E	E	E	E	E	E	−E	−E	−E	−E	−E	−E	J	J	J
$y\to\Lambda$	E	E	E	E	−E	−E	−E	J	J	−J	−E	−E	−E	J	J	−J	J	J	−J
$z\to K$	E	−E	J	−J	−E	J	−J	J	−J	−J	−E	J	−J	J	−J	−J	J	−J	−J

Again since $B=\langle x\rangle\times\langle y\rangle\times\langle z\rangle=\langle xz\rangle\times\langle yz\rangle\times\langle z\rangle=\langle xy\rangle\times\langle y\rangle\times\langle z\rangle=\cdots$, hence (2) = (5) = (11) (i. e. (2)、(5)、(11) give the same group), (3) = (8) = (17), (4) = (10), and (6) = (7) = (9) = (12) = (13) = (14) = (15) = (16) = (18) = (19). Thus it is sufficient to consider the following 5 possibilities: (1), (11), (17), (4), (6). Again a and b situating symmetrically in G also implies that (3) = (4) and hence (17) = (4). Consequently we actually have only 4 group-structures, i. e.

(i) $G\simeq Z_p\times Z_p\times Z_2\times Z_2\times Z_2$;

(ii) $G=\langle a, b, x, y, z\rangle$, $x^{-1}ax=y^{-1}ay=z^{-1}az=a^{-1}$, $x^{-1}bx=y^{-1}by=z^{-1}bz=b^{-1}$,
$$Z(G)=\langle xy\rangle\times\langle xz\rangle\simeq Z_2\times Z_2;$$

(iii) $G=\langle a, b, x, y, z\rangle$, $x^{-1}ax=y^{-1}ay=z^{-1}az=a$, $x^{-1}bx=y^{-1}by=z^{-1}bz=b^{-1}$,
$$Z(G)=\langle a\rangle\times\langle xy\rangle\times\langle xz\rangle\simeq Z_p\times Z_2\times Z_2;$$

(iv) $G=\langle a, b, x, y, z\rangle$, $\begin{cases} x^{-1}ax=a \\ x^{-1}bx=b \end{cases}$, $\begin{cases} y^{-1}ay=a^{-1} \\ y^{-1}by=b^{-1} \end{cases}$, $\begin{cases} z^{-1}az=a \\ z^{-1}bz=b^{-1} \end{cases}$,

$$Z(G)=\langle x\rangle\simeq Z_2.$$

Hence we obtain the following

Lemma 4. *If p is an odd prime $\neq 3, 7$, then the groups of order 2^3p^2 when all Sylow subgroups are elementary abelian have 4 types [(i)—(iv) of (2.3)].*

$$B=Q_8=\langle x, y\rangle,\ x^4=1,\ y^2=x^2,\ y^{-1}xy=x^{-1}\text{(Quaternion group)}. \tag{2.4}$$

Now $G\langle a, b, x, y\rangle$, $a^p=b^p=[a, b]=1=x^4(=y^4)$, $y^2=x^2$, $y^{-1}xy=x^{-1}(x^{-1}yx=y^{-1})$, $\begin{cases} x^{-1}ax=a^\alpha b^\beta \\ x^{-1}bx=a^\gamma b^\delta \end{cases}$, $\begin{cases} y^{-1}ay=a^\mu b^\nu \\ y^{-1}by=a^\sigma b^\tau \end{cases}$, where $\Delta=\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ and $\Lambda=\begin{pmatrix} \mu & \nu \\ \sigma & \tau \end{pmatrix}$ all lie in $GL(2, p)$, consequently $\Delta^4=E=\Lambda^4$, $\Lambda^2=\Delta^2$, $\Lambda^{-1}\Delta\Lambda=\Lambda^{-1}$ (in the field Z_p). Concerning Δ, we proceed in the same way as we have done in (2.2), so that a, b, x can be chosen suitably with $\Delta=E$, $-E$, $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ 0 & \xi \end{pmatrix}$, $\begin{pmatrix} -1 & 0 \\ 0 & \xi \end{pmatrix}$, or ξE, i. e. only these 7 possibilities are needed to be discussed. Note that $\xi=r^{\frac{p-1}{4}}$, $Z_p^*=\langle r\rangle$ where $p\equiv 1 \pmod 4$.

If $\Delta=\begin{pmatrix} \pm 1 & 0 \\ 0 & \xi \end{pmatrix}$ or ξE, by means of $\Delta\Lambda=\Lambda\Delta^{-1}$ it readily follows that we always have $\nu\equiv\sigma\equiv\tau\equiv 0 \pmod p$, contradiction with $\Lambda\in GL(2, p)$. Thence it can only be that $\Delta=E$, $-E$, $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ or $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.

(I) $\Delta=E$.

Now $\Lambda^2=\Delta^2=E$ implies $m_\Lambda(\lambda)=\lambda-1$, $\lambda+1$, or $(\lambda-1)(\lambda+1)$. But $m_\Lambda(\lambda)=\lambda-1$ or $\lambda+1$ gives respectively

(i) $G=\langle a, b, x, y\rangle$, $\begin{cases} x^{-1}ax=a \\ x^{-1}bx=b \end{cases}$, $\begin{cases} y^{-1}ay=a \\ y^{-1}by=b \end{cases}$, $Z(G)=\langle a\rangle\times\langle b\rangle\times\langle x^2\rangle\simeq Z_p\times Z_p\times Z_2$;

(ii) $G=\langle a, b, x, y\rangle$, $\begin{cases} x^{-1}ax=a \\ x^{-1}bx=b \end{cases}$, $\begin{cases} y^{-1}ay=a^{-1} \\ y^{-1}by=b^{-1} \end{cases}$, $Z(G)=\langle x^2\rangle\simeq Z_2$.

When $m_\Lambda(\lambda)=(\lambda-1)(\lambda+1)$, $P\in GL(2, p)$ exists so that $P^{-1}\Lambda P=\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ which inturn implies $a_1, b_1\in A=\langle a\rangle\times\langle b\rangle$ so that $A=\langle a_1\rangle\times\langle b_1\rangle$ with $\begin{cases} y^{-1}a_1y=a_1 \\ y^{-1}b_1y=b_1^{-1} \end{cases}$; but $\Delta=E$ also implies $P^{-1}\Delta P=E$, i. e. $\begin{cases} x^{-1}a_1x=a_1 \\ x^{-1}b_1x=b_1 \end{cases}$. This shows G can be written as

(iii) $G=\langle a, b, x, y\rangle$, $\begin{cases} x^{-1}ax=a \\ x^{-1}bx=b \end{cases}$, $\begin{cases} y^{-1}ay=a \\ y^{-1}by=b^{-1} \end{cases}$, $Z(G)=\langle ax^2\rangle\simeq Z_{2p}$.

(II) $\Delta=-E$.

Now also $\Lambda^2=\Delta^2=E$, hence as mentioned in (I) we have $\Lambda=E$, $-E$ or $m_\Lambda(\lambda)=(\lambda-1)(\lambda+1)$. Since x, y situate symmetrically in G, we find that $\Lambda=E$, $\Delta=-E$

will determine the same gronp as $\Delta=E$, $A=-E$ does i. e. the type (ii). Again $\Delta=-E$, $A=-E$ means $x\to -E$, $y\to -E$, hence $x_1=xy\to E$, but alse $B=\langle x_1, y\rangle$, $x_1^4=1$, $y^2=x_1^2$, $y^{-1}x_1y=x_1^{-1}$, this says that the group structure is also the type (ii). Thence we need only to consider $m_A(\lambda)=(\lambda-1)(\lambda+1)$, therefore $P\in GL(2, p)$ exists so that $P^{-1}AP=\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$, and at the same time $P^{-1}\Delta P=-E(=\Delta)$, this shows a, b can be chosen suitably with the group type

(iv) $G=\langle a, b, x, y\rangle$, $\begin{cases} x^{-1}ax=a^{-1} \\ x^{-1}bx=b^{-1}\end{cases}$, $\begin{cases} y^{-1}ay=a \\ y^{-1}by=b^{-1}\end{cases}$, $Z(G)=\langle x^2\rangle\simeq Z_2$.

Note that the type (ii) has $4p^2+2$ elements of order 4 ($a^\lambda b^\mu x^\alpha y$, $0\leqslant\lambda$, $\mu\leqslant p-1$, $0\leqslant\alpha\leqslant 3$; x, x^3), while (iv) has $2p^2+4p$ elements of order 4($a^\lambda b^\mu x^i$, $a^\lambda x^j y$, $b^\mu x^j y$, $0\leqslant\lambda$, $\mu\leqslant p-1$, $i=1$ or 3, $j=0$ or 2), hence (ii) is non-isomorphic to (iv).

(III) $\Delta=\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$.

Now $A^2=\Delta^2=E\Rightarrow\begin{cases}\mu^2+\nu\sigma\equiv 1\\ \tau^2+\nu\sigma\equiv 1\end{cases}$ and $\begin{cases}\sigma(\mu+\tau)\equiv 0\\ \nu(\mu+\tau)\equiv 0\end{cases}$ (mod p), again $\Delta A=A\Delta^{-1}\Rightarrow\nu\equiv 0\equiv\sigma$ (mod p), thence $\mu\equiv\pm 1$, $\tau\equiv\pm 1$ (mod p), and hence $A=E$, $-E$, Δ, or $-\Delta$. But $A=E$ or $-E$ means that tne group-structure is (iii) or (iv), in view of x and y being symmetrically situated in G. While $A=\Delta$ implies $x_1=xy\to\Delta A=E$, hence from $B=\langle x, y\rangle=\langle x_1, y\rangle$ we find that it reduces to (iii). Similarly $A=-\Delta$ reduces to (iv).

(IV) $\Delta=\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}$.

Now $A^2=\Delta^2=-E$. Again $\Delta A=A\Delta^{-1}$ implies $\nu\equiv\sigma$ and $\mu+\tau\equiv 0$ (mod p), thus $A=\begin{pmatrix}\mu & \nu\\ \nu & -\mu\end{pmatrix}$, therefore $A^2=-E$ implies $\mu^2+\nu^2\equiv -1$ (mod p), which is always soluble: infact, if $p\equiv 1$ (mod 4), take $\mu=0$, and ν satisfying $\nu^2\equiv -1$ (mod p). If $p\equiv 3$ (mod 4), since $1^c, 2^c, \cdots, (p-1)^c$ and $r^0\equiv 1, r^c, r^{2c}, \cdots, r^{(p-2)c}$ are identical (mod p), where $Z_p^*=\langle r\rangle$, hence

$$\sum_{t=1}^{p} t^c\equiv\sum_{i=0}^{p-2} r^{ic}=\frac{1-r^{(p-1)c}}{1-r^c}\equiv 0 \text{ (mod } p) \text{ when } 0<c<p-1,$$

Consequently by substituting it into the binomial expansions, we find

$$\sum_{t=1}^{p}\left(\frac{t^2+1}{p}\right)\equiv\sum_{t=1}^{p}(t^2+1)^{\frac{1}{2}(p-1)}\equiv\sum_{t=1}^{p} t^{p-1}\equiv p-1\equiv -1 \text{ (mod } p),$$

thus from $p\equiv 3$ (mod 4) we have $(t^2+1, p)=1$ for all t, i. e. $\left(\frac{t^2+1}{p}\right)=\pm 1$ for any t, therefore by $\sum_{t=1}^{n}\left(\frac{t^2+1}{p}\right)\equiv -1$ (mod p) there exists at least one t so that $\left(\frac{t^2+1}{p}\right)=-1$, and thus putting such $t=\mu$ we have $\left(\frac{\mu^2+1}{p}\right)=-1$, thence $\left(\frac{-(\mu^2+1)}{p}\right)=1$, this means an ν exists so that $\nu^2\equiv -(\mu^2+1)$ or $\mu^2+\nu^2\equiv -1$ (mod p).

Although $\mu^2+\nu^2\equiv-1 \pmod p$ has always solutions, yet the solution (μ, ν) is not unique in general, i. e. $A=\begin{pmatrix}\mu & \nu\\ \nu & -\mu\end{pmatrix}$ is not unique, however the determined group structures are isomorphic:

In fact, let $G=\langle a, b, x, y\rangle$, $a^p=b^p=[a, b]=1=x^4$, $y^2=x^2$, $y^{-1}xy=x^{-1}$,

$$\begin{cases}x^{-1}ax=b\\ x^{-1}bx=a^{-1}\end{cases}, \begin{cases}y^{-1}ay=a^{\mu}b^{\nu}\\ y^{-1}by=a^{\nu}b^{-\mu}\end{cases},$$

$\mu^2+\nu^2\equiv-1 \pmod p$; and assume $\mu_1^2+\nu_1^2\equiv-1 \pmod p$. In the group G we try to choose $\begin{cases}a'=a^sb^t\\ b'=a^kb^l\end{cases}$ with $P=\begin{pmatrix}s & t\\ k & l\end{pmatrix}\in GL(2, p)$ [hence $G=\langle a', b', x, y\rangle$], and hope to have

$$\begin{cases}x^{-1}a'x=b'\\ x^{-1}b'x=a'^{-1}\end{cases} \text{and} \begin{cases}y^{-1}a'y=a'^{\mu_1}b'^{\nu_1}\\ y^{-1}b'y=a'^{\nu_1}b'^{-\mu_1}\end{cases}. \qquad (*)$$

By computation, the first one of $(*)$ is equivalent to $k\equiv-t$, $l\equiv s \pmod p$, thus

$$P=\begin{pmatrix}s & t\\ -t & s\end{pmatrix}\in GL(2, p)\Leftrightarrow s^2+t^2\not\equiv 0 \pmod p,$$

and hence the latter one of $(*)$ is equivalent to

$$\begin{cases}(\mu-\mu_1)s+(\nu+\nu_1)t\equiv 0\\ (\nu-\nu_1)s-(\mu+\mu_1)t\equiv 0.\end{cases} \pmod p \qquad (**)$$

Since $\begin{vmatrix}\mu-\mu_1 & \nu+\nu_1\\ \nu-\nu_1 & -(\mu+\mu_1)\end{vmatrix}=-(\mu^2-\mu_1^2)-(\nu^2-\nu_1^2)\equiv 0 \pmod p$, hence $(**)$ has actually solutions(s, t), in which at least one of s, t is $\not\equiv 0 \pmod p$. Now we can assert moreover that $s^2+t^2\not\equiv 0 \pmod p$, for $(**)$ implies

$$\begin{cases}(\mu-\mu_1)^2s^2\equiv(\nu+\nu_1)^2t^2\\ (\nu-\nu_1)^2s^2\equiv(\mu+\mu_1)^2t^2\end{cases} \pmod p,$$

by adding them we find $s^2(-2-2\mu\mu_1-2\nu\nu_1)\equiv t^2(-2+2\mu\mu_1+2\nu\nu_1) \pmod p\Rightarrow(s^2-t^2)+(s^2+t^2)(\mu\mu_1+\nu\nu_1)\equiv 0 \pmod p\Rightarrow s^2\equiv t^2 \pmod p$ in case $s^2+t^2\equiv 0 \pmod p\Rightarrow 2s^2\equiv 0 \pmod p\Rightarrow s\equiv 0\equiv t \pmod p$, impossible. Thence $s^2+t^2\not\equiv 0 \pmod p$.

This says nothing other than that $\Delta=\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}$ and $A=\begin{pmatrix}\mu & \nu\\ \nu & -\mu\end{pmatrix}$ with $\mu^2+\nu^2\equiv -1 \pmod p$ will determine the unique group-structure, as

(v) $G=\langle a, b, x, y\rangle$, $\begin{cases}x^{-1}ax=b\\ x^{-1}bx=a^{-1}\end{cases}$, $\begin{cases}y^{-1}ay=a^{\mu}b^{\nu}\\ y^{-1}by=a^{\nu}b^{-\mu}\end{cases}$, $\mu^2+\nu^2\equiv-1 \pmod p$, $Z(G)=1$.

Hence we have

Lemma 5. *If p is an odd prime $\neq 3, 7$, then the groups of order 2^3p^2 when the Sylow p-subgroups are elementary abelian and the Sylow 2-subgroups are quaternion have 5 types* [(i)—(v) of (2.4)].

$B=\langle x, y\rangle$, $x^4=y^2=1$, $y^{-1}xy=x^{-1}$ (Dihedral group D_8 of order 8). (2.5)

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

$$\begin{cases} x^{-1}ax=a^\alpha b^\beta \\ x^{-1}bx=a^\gamma b^\delta \end{cases}, \quad \begin{cases} y^{-1}ay=a^\mu b^\nu \\ y^{-1}by=a^\sigma b^\tau \end{cases} \text{with } \Delta=\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}, \ \Lambda=\begin{pmatrix} \mu & \nu \\ \sigma & \tau \end{pmatrix}$$

all$\in GL(2, p)$. Hence the defining relations of B imply $\Delta^4=\Lambda^2=E$ and $\Lambda^{-1}\Delta\Lambda=\Delta^{-1}$. Concerning Δ we can proceed in the same way as done in (2.2), and also by means of $\Delta\Lambda=\Lambda\Delta^{-1}$ we know that we can choose a, b, x as done in (2.4), so that $\Delta=E$, $-E$, $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, or $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, i. e. we can restrict ourselves in these four cases.

(I) $\Delta=E$.

Now by $\Lambda^2=E$ we can proceed in the same way as done in (I) of (2.4), and we find that G has 3 types, say:

(i) $G=\langle a, b, x, y\rangle$, $\begin{cases} x^{-1}ax=a=y^{-1}ay \\ x^{-1}bx=b=y^{-1}by \end{cases}$, $Z(G)=\langle a\rangle\times\langle b\rangle\times\langle x^2\rangle\simeq Z_p\times Z_p\times Z_2$;

(ii) $G=\langle a, b, x, y\rangle$, $\begin{cases} x^{-1}ax=a=(y^{-1}ay)^{-1} \\ x^{-1}bx=b=(y^{-1}by)^{-1} \end{cases}$, $Z(G)=\langle x^2\rangle\simeq Z_2$;

(iii) $G=\langle a, b, x, y\rangle$, $\begin{cases} x^{-1}ax=a \\ x^{-1}bx=b \end{cases}$, $\begin{cases} y^{-1}ay=a \\ y^{-1}by=b^{-1} \end{cases}$, $Z(G)=\langle ax^2\rangle\simeq Z_{2p}$.

(II) $\Delta=-E$.

Now as in (I) we have $\Lambda=E$, $-E$, or $m_\Lambda(\lambda)=\lambda^2-1$. But $\Lambda=-E$ means now that $x\to -E$, $y\to -E$, thence $xy\to E$; and also in view of $B=\langle x, y\rangle=\langle x, xy\rangle$, we find that $\Delta=-E$, $\Lambda=-E$ and $\Delta=-E$, $\Lambda=E$ give the same group, as

(iv) $G=\langle a, b, x, y\rangle$, $\begin{cases} x^{-1}ax=a^{-1} \\ x^{-1}bx=b^{-1} \end{cases}$, $\begin{cases} y^{-1}ay=a \\ y^{-1}by=b \end{cases}$, $Z(G)=\langle x^2\rangle\simeq Z_2$.

When $m_\Lambda(\lambda)=\lambda^2-1$, $P\in GL(2, p)$ exists so that $P^{-1}\Lambda P=\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, i. e. a, b can be chosen with $\begin{cases} y^{-1}ay=a \\ y^{-1}by=b^{-1} \end{cases}$, and now $P^{-1}\Delta P=-E$ too such as $\Delta=-E$, hence we have another type, as

(v) $G=\langle a, b, x, y\rangle$, $\begin{cases} x^{-1}ax=a^{-1} \\ x^{-1}bx=b^{-1} \end{cases}$, $\begin{cases} y^{-1}ay=a \\ y^{-1}by=b^{-1} \end{cases}$, $Z(G)=\langle x^2\rangle\simeq Z_2$.

(III) $\Delta=\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

Now $\Delta\Lambda=\Lambda\Delta^{-1}=\Lambda\Delta$ implies $\Lambda=\begin{pmatrix} \mu & 0 \\ 0 & \tau \end{pmatrix}$, henca $\Lambda^2=E$ means $\mu^2\equiv 1\equiv\tau^2$ (mod p), consequently $\Lambda=E$, $-E$, $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ or $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$. But $y\to\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ implies now $xy\to E$, and $y\to\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ implies $xy\to -E$, therefore from $B=\langle x, y\rangle=\langle x, xy\rangle$ it follows that it is sufficient to consider $\Lambda=E$ and $\Lambda=-E$. Thus we have:

(vi) $G=\langle a, b, x, y\rangle$, $\begin{cases} x^{-1}ax=a \\ x^{-1}bx=b^{-1} \end{cases}$, $\begin{cases} y^{-1}ay=a \\ y^{-1}by=b \end{cases}$, $Z(G)=\langle ax^2\rangle\simeq Z_{2p}$;

(vii) $G=\langle a, b, x, y\rangle$, $\begin{cases} x^{-1}ax=a \\ x^{-1}bx=b^{-1}\end{cases}$ $\begin{cases} y^{-1}ay=a^{-1} \\ y^{-1}by=b^{-1}\end{cases}$, $Z(G)=\langle x^2\rangle\simeq Z_2$.

Since the group-types (ii), (iv), (v), (vii) respectively contain $4p^2+1$, $2p^2+3$, $4p+1$, $2p^2+2p+1$ elements of order 2 ($a^\lambda b^\mu x^\alpha y$ and x^2 in (ii); $a^\lambda b^\mu x^i y$, x^2, x^2y and y in (iv); $a^\lambda x^i y$, $b^\mu y$, $b^\mu x^2 y$ and x^2 in (v); $a^\lambda b^\mu x^2 y$, $a^\lambda b^\mu y$, $a^\lambda x^i y$ and x^2 in (vii); where $0\leqslant\lambda$, $\mu\leqslant p-1$, $0\leqslant\alpha\leqslant 3$, $i=1$ or 3), again the types (iii) and (vi) contain respectively $4p+1$ and $2p+3$ elements of order 2 ($b^\mu x^\alpha y$ and x^2 in (iii); $b^\mu x^i y$, y, $x^2 y$ and x^2 in (vi); where $0\leqslant\mu\leqslant p-1$, $0\leqslant\alpha\leqslant 3$, $i=1$ or 3), hence the types (i)—(vii) are actually distinct with one another.

(IV) $\Delta=\begin{pmatrix} 0 & 1 \\ -1 & 0\end{pmatrix}$.

Now $\Delta A=A\Delta^{-1}$ will imply $\nu\equiv\sigma$, $\mu+\tau\equiv 0 \pmod p$, thus $A=\begin{pmatrix} \mu & \nu \\ \nu & -\mu\end{pmatrix}$, and therefore $A^2=E$ implies $\mu^2+\nu^2\equiv 1 \pmod p$ which is evidently solvable. Taking $\mu=1$, $\nu=0$, we get

(viii) $G=\langle a, b, x, y\rangle$, $\begin{cases} x^{-1}ax=b \\ x^{-1}bx=a^{-1}\end{cases}$ $\begin{cases} y^{-1}ay=a \\ y^{-1}by=b^{-1}\end{cases}$, $Z(G)=1$.

Now assume $\mu^2+\nu^2\equiv 1 \pmod p$. In the type (viii) we try to find

$$\begin{cases} a'=a^s b^t \\ b'=a^k b^l\end{cases} \text{with } P=\begin{pmatrix} s & t \\ k & l\end{pmatrix}\in GL(2, p)$$

and hence $G=\langle a', b', x, y\rangle$, and hope

$$\begin{cases} x^{-1}a'x=b' \\ x^{-1}b'x=a'^{-1}\end{cases} \text{and } \begin{cases} y^{-1}a'y=a'^{\mu}b'^{\nu} \\ y^{-1}b'y=a'^{\nu}b'^{-\mu}.\end{cases}$$

By computation, the former is equivalent to $l\equiv s$, $k+t\equiv 0 \pmod p$, and the latter thus implies

$$\begin{cases} (\mu-1)s-\nu t\equiv 0 \\ \nu s+(\mu+1)t\equiv 0\end{cases} \pmod{p} \qquad (***)$$

Since $\begin{vmatrix} \mu-1 & -\nu \\ \nu & \mu+1\end{vmatrix}=\mu^2-1+\nu^2\equiv 0 \pmod p$, hence (***) has solutions $(s, t)\neq(0, 0)$, i. e. at least one of s, t is not zero $\pmod p$. Moreover from $(\mu-1)^2s^2\equiv\nu^2t^2$, $\nu^2s^2\equiv(\mu+1)^2t^2 \pmod p$ we have (by adding them):

$$[(\mu-1)^2+\nu^2]s^2\equiv[\nu^2+(\mu+1)^2]t^2 \pmod{p},$$

hence simplifying it, we have

$$(1-\mu)s^2\equiv(1+\mu)t^2 \pmod{p}\Rightarrow(s^2-t^2)\equiv\mu(s^2+t^2) \pmod{p}.$$

Consequently $s^2+t^2\not\equiv 0 \pmod p$–for otherwise we would have $s^2\equiv t^2 \pmod p$ and hence $2s^2\equiv 0 \pmod p$ by using of $s^2+t^2\equiv 0 \pmod p$, thence $s\equiv 0$ and therefore $t\equiv 0 \pmod p$, contradiction with $(s, t)\neq(0, 0)$. This says that $P=\begin{pmatrix} s & t \\ k & l\end{pmatrix}=\begin{pmatrix} s & t \\ -t & s\end{pmatrix}$ is of det P

relatively prime to p, or $P \in GL(2, p)$. This says nothing other than that the group-structure determined by $A=\begin{pmatrix} \mu & \nu \\ \nu & -\mu \end{pmatrix}$ with $\mu^2+\nu^2\equiv 1 \pmod p$ is unique, hence it can be represented by (viii).

Therefore we obtain

Lemma 6. *If p is an odd prime $\neq 3$, 7, then the groups of order 2^3p^2 when the Sylow p-subgroups are elementary abelian and the Sylow 2-subgroups are dihedral have 8 types* [(i)—(viii) of (2.5)].

Combining the Lemmas 1, 2, 3, 4, 5, 6 we have the following

Theorem. *The groups of order 2^3p^2 (p-odd prime $\neq 3$, 7) have:*

(1) 60 *types when* $p\equiv 1 \pmod 8$,

(2) 52 *types when* $p\equiv 5 \pmod 8$,

(3) 42 *types when* $p\equiv 3 \pmod 8$,

(4) 42 *types when* $p\equiv 7 \pmod 8$.

References

[1] Hölder, O., Die Gruppen der Ordnung p^3, pq^2, pqr, p^4, *Math. Ann.*, **43**(1893), 301—412.

[2] Western, A. E., Groups of order p^3q:, *Proc. London Math. Soc.*, **30**(1898), 209—263.

[3] Lin Huei-Lung, On groups of orders p^2q, p^2q^2, *Tamkang J. Math.*, **5**(1974), 167—190.