Kumamoto J. Sci. (Math.)
Vol. 10, 1-24 (1973)

ON A CLASS OF P-GROUPS

Minoru KANAZAWA

(Received November 29, 1972)

Introduction

We know that nonabelian p-groups of order p^n which contains a cyclic subgroup of order p^{n-1} are completely classified (See Theorem 2). In this paper we study nonabelian p-groups of order p^n ($n \geqq 4$) which contain a cyclic subgroup of order p^{n-2}.

In section 1 we shall determine the p-groups with a self-centralizing, normal cyclic subgroup and in section 2 the p-groups with a non-self-centralizing, normal cyclic subgroup are studied. Since $[P:P'] \geqq p^2$ for any nonabelian p-group P, we have $cl(P) \leqq n-1$ if P is of order p^n ($n>2$). p-group of class $(n-1)$ is said to be of maximal class. Blackburn studied in [1], [2] maximal class of p-groups. We define p-group P of order p^n ($n>2$), as of second maximal class if $cl(P)=n-2$.

In section 3 we deal with the 2-groups of second maximal class with the cyclic commutator subgroup.

Now, we use the following standard notations. When H is a subset of a group G, $|H|$ denotes its cardinal number, and we denote by $<H>$ the subgroup of G generated by the whole elements in H: in particular the cyclic subgroup of G generated by an element x in G is denoted by $<x>$. Also we shall use the exponential notation H^f for the image of H under the mapping f. In particular, for an element x in G we denote by H^x the subset $x^{-1} H x$. If H is a normal subgroup of G, we write $H \triangleleft G$. If H is a subgroup of G, then we write $H \leq G$, while if H is a proper subgroup of G, then we write $H<G$. If H is a subset of G, $C_G(H)$ and $N_G(H)$ denote the centralizer and the normalizer of H in G, respectively. Also $Z(G)$, G' and $\Phi(G)$ denote the center, the commutator subgroup and Frattini subgroup of G, respectively. If G is nilpotent, then the class of G is denoted by $cl(G)$. The automorphism group of G is denoted by $Aut(G)$. For a p-group P, $\Omega^i(P)$ denotes the subgroup of P generated by its elements of order dividing p^i and $\mho^i(P)$ denotes the subgroup of P generated by the whole elements x^{p^i} for x in P. For a subset H of G, we denote by $I(G)$ the number of elements of order 2 in G. Finally, if p-group P possesses cyclic subgroup of index p^2 in P, but if P

does not possess any normal cyclic subgroups of index p^2 in P, then we say that P has the property $(\mathfrak{P}_p.)$

Now we know the following theorem about the automorphism group of a cyclic p-group.

THEOREM 1. *Let A be the automorphism group of a cyclic group of order p^n generated by x, where p is a prime and $n \geqq 2$. Then the followings hold:*
(1) *If $p=n=2$, then $A=\langle\sigma;\ x^{\sigma}=x^{-1}\rangle$, i. e. $|A|=2$,*
(2) *If $p=2$ and $n>2$, then A is an abelian 2-group of type $(2^{n-2}, 2)$ generated by two elements σ, τ with the relations $x^{\sigma}=x^5$ and $x^{\tau}=x^{-1}$.*
(3) *If p is odd, then an S_p-subgroup of A is a cyclic group of order p^{n-1} generated by σ, where $x^{\sigma}=x^{1+p}$.*

By using this theorem, we can kow the existence of the following particular p-groups of order p^n, for $p=2$, $n>3$ and for p odd, $n>2$.

$$M_n(p)=\langle x, y;\ x^{p^{n-1}}=y^p=1,\ x^y=x^{1+p^{n-2}}\rangle,$$
$$S_n=\langle x, y;\ x^{2^{n-1}}=y^2=1,\ x^y=x^{-1+2^{n-2}}\rangle.$$

The latter group S_n is called a semidihedral group of order 2^n. The dihedral group and the generalized quaternion group of order 2^n are denoted by D_n and Q_n, respectively. Each of $M_n(p)$, D_n, Q_n and S_n possesses a cyclic subgroup of order p^{n-1}. However, this property characterizes these groups among nonabelian p-groups, that is, we have

THEOREM 2. *Let P be a nonabelian p-group of order p^n which contains a cyclic subgroup of order $p^{n-1} (n \geqq 3)$. Then*
(1) *If p is odd, then P is isomorphic to $M_n(p)$.*
(2) *If $p=2$ and $n=3$, then P is isomorphic to D_3 or Q_3.*
(3) *If $p=2$ and $n>3$, then P is isomorphic to $M_n(2)$, D_n, Q_n or S_n.*

§1. p-groups with a self-centralizing, normal cyclic subgroup of index p^2.

With the aid of Theorem 1 we can construct several p-groups. Let H be a cyclic group of order p^{n-2} generated by x and for σ, τ defined in Theorem 1 we denote by K_1 the group $\langle\sigma^{p^{n-5}}\rangle$ for p odd, $n \geqq 5$, the group $\langle\sigma^{2^{n-6}}\rangle$ for $p=2$, $n \geqq 6$, by K_2 the group $\langle\sigma^{2^{n-6}}\cdot\tau\rangle$ for $n \geqq 6$. and by K_3 the group $\langle\sigma^{2^{n-5}}\rangle \times\langle\tau\rangle$ for $n \geqq 5$. Then in consideration of the semidirect product of H by K_i $(i=1,2,3)$, we can define the following groups;

$$N_n(p)=\langle x, y;\ x^{p^{n-2}}=y^{p^2}=1,\ x^y=x^{1+p^{n-4}+\varepsilon_p\cdot\frac{p^{n-5}-1}{2}p^{n-3}}\rangle,$$
$$S_1(n)=\langle x, y;\ x^{2^{n-2}}=y^4=1,\ x^y=x^{-1-2^{n-4}+\varepsilon_2\cdot 2^{n-3}}\rangle,$$
$$S_2(n)=\langle x, y, z;\ x^{2^{n-2}}=y^2=z^2=1,\ x^y=x^{1+2^{n-3}},\ x^z=x^{-1},\ y^z=y\rangle,$$

where ε_p is defined in the following:

$$(1.1)\qquad \begin{array}{l} \varepsilon_p=0 \text{ for all primes } p \text{ if } n \text{ takes its smallest value,} \\ \varepsilon_2=1,\ \varepsilon_3=-1 \text{ and } \varepsilon_p=\dfrac{p-1}{2}\ (p\neq 2,3) \text{ otherwise.} \end{array}$$

Moreover, by using the property of partial semidirect product we shall define another 2-group of order 2^n than the above ones. A group G is called a partial semidirect product of H by K with respect to M if $G=KH$ with $H\lhd G$ and K is a proper subgroup of G and $K\cap H=M$. Then we have the following proposition for the proof of which we can refer to [3]:

From the groups H, K, M with $M\leq H$ we can construct a partial semidirect product of H by K with respect to M if and only if there exist a homomorphism φ of K into $Aut(H)$ and an isomorphism f of M into K which satisfy the following conditions for all x, y, z in H, K, M, respectively;

$$(1.2)\qquad x^{(z^f)^\varphi}=x^z,\quad (z^{(y)^\varphi})^f=(z^f)^y.$$

Assume $n\geq 5$. Let H be a cyclic group of order 2^{n-2} generated by an element x and M be a subgroup of H generated by $x^{2^{n-3}}$. Let K be an abelian 2-group of type (4,2), *i.e.* we put

$$K=\langle y,\ z;\ y^2=z^4=1,\ yz=zy\rangle.$$

We put $(x^{2^{n-3}\cdot k})^f=z^{2k}$. Let $(y^iz^j)^\varphi$ be the automorphism of H which maps x^k into $x^{k(1+2^{n-3})^i(-1)^j}$ for y^iz^j in K. Then φ determines a homomorphism of K into $Aut(H)$ and it is easily verified that (1.2) is satisfied. Hence the partial semidirect product $S_3(n)$, exists and is given by the following defining relations;

$$S_3(n)=\langle x, y, z;\ y^2=z^4=1,\ z^2=x^{2^{n-3}},\ x^y=x^{1+2^{n-3}},\ x^z=x^{-1},\ yz=zy\rangle.$$

Before we study the properties of p-groups defined above, we must have the following two lemmas.

LEMMA 1.1. *For x, y in a group G, assume $[x, y]=z$ commutes with x and y. Then the next two relations hold for all i, j.*

(1) $[x^i, y^j]=z^{ij}$.

(2) $(yx)^i=z^{\frac{1}{2}i(i-1)}y^i x^i$.

PROOF: $[x, y]=z$ implies $x^y=xz$. Since x and z commute, $(x^i)^y=(x^y)^i=(xz)^i=x^i z^i$, and so $(x^i)^{y^2}=(x^i z^i)^y=x(^i)^y z^i=x^i z^{2i}$. Replacing this argument j times, we obtain $(x^i)^{y^j}=x^i z^{ij}$. Hence $[x^i, y^j]=z^{ij}$. For $i=1$, (2) holds clearly. If $(yx)^{i-1}=z^{\frac{1}{2}(i-1)(i-2)}y^{i-1}x^{i-1}$, then $(yx)^i=(yx)^{i-1}\ yx=z^{\frac{1}{2}(i-1)(i-2)}\ y^{i-1}\ x^{i-1}yx$. By (1) $x^{i-1}\ y=z^{i-1}\ yx^{i-1}$, and so (2) holds.

LEMMA 1.2. *Let P be a p-group with $cl(P)\leqq 2$, where p is odd. If $P/Z(P)$ is of exponent at most p, then $(xy)^{p^i}=x^{p^i}y^{p^i}$ for all x, y in P and for all i.*

PROOF: Put $[y, x]=z$ for x, y in P. Since P is of class at most 2, z is contained in $Z(P)$, whence by Lemma 1.1

(1.3) $$[y, x^j]=z^j, \quad (xy)^j=z^{\frac{1}{2}j(j-1)}x_j\ y^j$$

hold for all j. Sicce $P/Z(P)$ is of exponent at most p^i and p is odd, by putting $j=p^i$ in (1.3) we have

$$1=[y,\ x^{p^i}]=z^{p^i}, \quad (xy)^{p^i}=z^{\frac{1}{2}p^i(p^i-1)}x^{p^i}\ y^{p^i}=x^{p^i}\ y^{p^i}.$$

REMARK. The conclusion of this lemma does not hold for $p=2$.

For any integer α, there exists an integer β satisfying the congruence

(1.4) $$\alpha+\beta\ (1+2^{n-i-1})\equiv 0 \quad (mod.\ 2^{n-i})$$

if $i+1<n$.

Now we shall study the properties of $N_n(p)$ and $S_i(n)$, $i=1, 2, 3$.

THEOREM 1.1. *The followings hold.*

(1) *If $P=N_n(p)$*, then
  (a) *$cl(P)=3$ for p odd, $n=5$ and $cl(P)=2$ for $n\geqq 6$. $Z(P)$ is cyclic of order p^{n-4} and P' is cyclic of order p^2*
  (b) *$\Phi(P)$ is abelian of type (p^{n-3}, p).*
  (c) *$\Omega_1(P)$ is abelian of type (p, p)*

(2) *If $P=S_1(n)$, then*
  (a) *$cl(P)=n-2$, P' is cyclic of order 2^{n-3} and $|Z(P)|=2$.*
  (b) *$\Phi(P)$ is abelian of type $(2^{n-3}, 2)$.*

(c) $\Omega_1(P)$ *is abelian of type* $(2,2)$.

(3) *If* $P=S_2(n)$ *or* $P=S_3(n)$, *then*

(a) $cl(P)=n-2$, $P'=\Phi(P)$ *is cyclic of order* 2^{n-3} *and* $|Z(P)|=2$.

(b) $\Omega_1(P)=P$.

(c) $I(S_2(n))=3+2^{n-3}+2^{n-2}$ *and* $I(S_3(n))=3+2^{n-3}$.

(4) *No two of the groups* $N_n(p)$, $S_1(n)$, $S_2(n)$ *and* $S_3(n)$ *are isomorphic.*

PROOF: Put $P=N_n(p)$ or $S_i(n)$, $i=1,2,3$, as the case may be and let P be generated by x and y, or by x, y and z satisfying the appropriate relations. In the first case $(x^{p^2})^y=(x^y)^{p^2}=x^{p^2}$, whence x^{p^2} is contained in $Z(P)$. On the other hand, if $x^i\, y^j$ is contained in $Z(P)$, after an elementary calculation we have $i\equiv 0$ and $j\equiv 0$ (mod. p). Therefore $Z(P)=\langle x^{p^2}\rangle$ is cyclic of order p^{n-4}. Since $P/\Phi(P)$ is elementary abelian, both x^p and y^p are contained in $\Phi(P)$, whence $\Phi(P)$ contains a subgroup of order p^{n-2} generated by x^p and y^p. However, since P is nonabelian and $[x^p, y^p]=1$, we have $[P: \Phi(P)]\geqq p^2$, whence $\Phi(P)=\langle x^p\rangle\times\langle y^p\rangle$ is abelian of type (p^{n-3}, p). Since $\Phi(P)=\langle x^p\rangle\times\langle y^p\rangle$ and $Z(P)=\langle x^{p^2}\rangle=\mho(\Phi(P))$, $P/Z(P)$ is of exponent p^2. $[x, y]=x^{p^{n-4}+\varepsilon p\cdot\frac{p^{n-5}-1}{2}\cdot p^{n-3}}$, and so P' is cyclic of order p^2 generated by $x^{p^{n-4}}$. Therefore, if p is odd and $n=5$, we have $cl(P)=3$, while if $n\geqq 6$, then we have $cl(P)=2$. Since $(y^i\, x^j)^p=y^{ip}\prod_{k=1}^{p}(x^j)^{y^{i(p-k)}}=y^{ip}\, x^l$ for some integer l, the order of $y^i\, x^j$ does not divide p if $i\not\equiv 0$ (mod. p). First assume that p is odd. If $n=5$, $x^y=x^{1+p}$ and $x^{y^p}=x^{1+p^2}$, whence

$$
\begin{aligned}
(y^p\, x^i)^p &= y^{p^2}\prod_{j=1}^{p}(x^i)^{y^{p(p-j)}}\\
&= x^{i\sum_{j=0}^{p-1}(1+p^2)^j}\\
&= x^{ip}
\end{aligned}
$$

since $x^{p^3}=1$. If $n\geqq 6$, $[x, y]=u$ is of order p^2 and is contained in $Z(P)$, whence by Lemma 1.1 $[x^i, y^p]=u^{ip}$ and $(y^p\, x^i)^p=u^{ip\cdot\frac{1}{2}p(p-1)}\, y^{p^2}x^{ip}=x^{ip}$. In either case $(y^p\, x^i)^p=x^{ip}$, and so we have the fact that $y^p\, x^i$ is of order p if and only if $i\equiv 0$ (p^{n-3}). Hence $\Omega_1(P)$ is generated by $x^{p^{n-3}}$ and y^p, and is abelian of type (p, p). On the other hand, if $p=2$, then $(y^2\, x^i)^2=y^4(x^i)^{y^2}x^i=x^{2i(1+2^{n-4})}$, whence we obtain the same result as p is odd. Therefore (1) holds.

Now consider (2). Since $x^y=x^{-1-2^{n-4}+2^{n-3}\cdot\varepsilon_2}$, P' contains x^2. On the other hand, for all i and j $[x^i, y^j]=x^{i\{(-1-2^{n-4}+2^{n-3}\cdot\varepsilon_2)^j-1\}}$ is contained in a group $\langle x^2\rangle$. Therefore P' is a cyclic group of order 2^{n-3} with a generator x^2. If x^i

commutes with y, then $i \equiv 0 \pmod{2^{n-3}}$. However $x^{2^{n-3}}$ is contained in $Z(P)$, whence $Z(P)$ is a cyclic group of order 2 generated by $x^{2^{n-3}}$. Since x^2 commutes with y^2 and since both x^2 and y^2 are contained in $\Phi(P)$, $\Phi(P)$ contains an abelian group $\langle x^2 \rangle \times \langle y^2 \rangle$ of order 2^{n-2}. But P is nonabelian, and so we have $[P: \Phi(P)] \geqq 4$. Therefore $\Phi(P) = \langle x^2 \rangle \times \langle y^2 \rangle$ is abelian of type $(2^{n-3}, 2)$. Since $[x^{2i}, y] = x^{-2i+2i(-1-2^{n-4}+2^{n-3} \cdot \varepsilon_2)} = x^{4i(-1-1^{n-5}+2^{n-4} \cdot \varepsilon_2)}$, by the induction on j we shall obtain $P^{(j+1)} = [P^{(j)}, P] = \langle x^{2^{j+1}} \rangle$. Thus $cl(P) = n-2$. Since $y^2 \neq 1$, we have $(y^{\pm 1} x^i)^2 = y^{\pm 2} (x^i)^{y^{\pm 1}} x^i \neq 1$ and $(y^2 x^i)^2 = y^4 (x^i)^{y^2} x^i = x^{2i(1+2^{n-4})}$. Hence $y^2 x^i$ is an involution in P if and only if $i \equiv 0 \pmod{2^{n-3}}$. Therefore we obtain that $\Omega_1(P)$ is an abelian group of type $(2, 2)$ generated by $x^{2^{n-3}}$ and y^2.

Next consider (3). Since, in this case, $[x^i, y] = x^{2^{n-3} \cdot i}$ and $[x^i, z] = x^{-2i}$, $Z(P)$ is a cyclic group of order 2 generated by $x^{2^{n-3}}$ and P' contains x^2. However, both $[x^i, y]$ and $[x^i, z]$ are contained in the subgroup $\langle x^2 \rangle$, and so the factor group $P/\langle x^2 \rangle$ is an elementary abelian group, whence we conclude that $P' = \Phi(P) = \langle x^2 \rangle$ is cyclic of order 2^{n-3}. Since x^{2i} commutes with y and $[x^{2i}, z] = x^{-4i}$, by the induction on j we shall have $P^{(j+1)} = [P^{(j)}, P] = \langle x^{2^{j+1}} \rangle$, whence, in particular, we obtain $cl(P) = n-2$. An elementary calculation will show that the full set of elements of order 2 in $S_2(n)$ and $S_3(n)$ are $\{x^{2^{n-3}}, y, yx^{2^{n-3}}, z, zx, zx^2, \ldots, zx^{2^{n-2}-1}, yz, yzx^2, \ldots, yzx^{2^{n-2}-2}\}$ and $\{x^{2^{n-3}}, y, yx^{2^{n-3}}, yzx, yzx^3, \ldots, yzx^{2^{n-2}-1}\}$, respectively. Thus we have $\Omega_1(P) = P$ in either case, and $I(S_2(n)) = 3 + 2^{n-3} + 2^{n-2}$ and $I(S_3(n)) = 3 + 2^{n-3}$.

By comparing with the order of P', $Z(P)$ and $\Phi(P)$, or with the number of involutions in P, immediately we obtain (4). Thus the proof is completed.

Each of $N_n(p)$, $S_1(n)$, $S_2(n)$ and $S_3(n)$ possesses a self-centraling, normal cyclic subgroup of order p^{n-2}. However, this property characterizes these groups among all nonabelian p-groups of order p^n.

THEOREM 1.2. *Let P be a nonabelian p-group of order p^n which contains a self-centralizing, normal cyclic subgroup H of order p^{n-2}. Then $n \geqq 5$ and*

(1) *If p is odd, then P is isomorphic to $N_n(p)$.*

(2) *If $p=2$, $n=5$, then P is isomorphic to $S_2(5)$ or $S_3(5)$.*

(3) *If $p=2$, $n>5$, then P is isomorphic to $N_n(2)$, $S_1(n)$, $S_2(n)$ or $S_3(n)$.*

PROOF: Let x be a generator of a cyclic group H of ordes p^{n-2}. Since H is a self-centralizing normal subgroup of P, the factor group P/H is isomorphic to a subgroup of order p^2 of the automorphism group of H whose

S_p-subgroup is of order p^{n-3}. Therefore we have $n \geqq 5$. First consider the case that p is odd. By Theorem 1, P/H is cyclic and there exists an element u in $P-H$ such that P is generated by x and u with the relations $x^u = x^{1+p^{n-4}+\varepsilon_p \cdot \frac{p^{n-5}-1}{2} \cdot p^{n-3}}$, where ε_p is defined as in (1.1). Since $(x^{p^2})^u = (x^u)^{p^2} = x^{p^2}$, $(x^p)^u \neq x^p$ and $x^{u^p} \neq x$, it follows that $Z(P)$ is generated by x^{p^2}. From the manner of the conjugation of x by u and from the fact that P is generated by x and u, we conclude that P' is generated by $x^{p^{n-4}}$. Therefore we have $cl(P)=3$ if n=5 and $cl(P)=2$ if $n>5$. Since u^{p^2} is contained in H, u^{p^2} is also contained in $Z(P)$. Hence for some integer α we have $u^{p^2} = x^{\alpha p^2}$. If $n=5$, then $x^u = x^{1+p}$. If we put $y = ux^{-\alpha}$, then $P = \langle x, y \rangle$ and $x^y = x^u = x^{1+p}$, and

$$\begin{aligned} y^{p^2} &= (ux^{-\alpha})^{p^2} \\ &= u^{p^2} \prod_{i=0}^{p^2-1} (x^{-\alpha})^{u^i}. \\ &= x^{\alpha p^2} \cdot x^{-\alpha \sum_{i=0}^{p^2-1} (1+p)^i} \end{aligned}$$

However

$$1+(1+p)+\dots+(1+p)^{p^2-1} \equiv p^2 \pmod{p^3}$$

since p is odd. Therefore we have $y^{p^2}=1$. Consequently P is isomorphic to $N_5(p)$. If $n>5$, then $cl(P)=2$. Let v be any element in $P-H$. If v^p is not contained in H, then v^{p^2} is contained in $Z(P)$, because two elements x and v generate P. If v^p is contained in H, then the group P_1 generated by x and v is isomorphic to $M_{n-1}(p)$, and so v^p is contained in its center $Z(P_1)$. However, $Z(P_1)$ is generated by x^p, whence v^{p^2} is also contained in $Z(P) = \langle x^{p^2} \rangle$. In either case, v^{p^2} is contained in $Z(P)$. Therefore, it follows that the factor group $P/Z(P)$ is of exponent p^2. If we put $y = ux^{-\alpha}$, then P is generated by x and y with the retalion $x^y = x^u = x^{1+p^{n-4}+\varepsilon_p \cdot \frac{p^{n-5}-1}{2} \cdot p^{n-3}}$. By Lemma 1.2 we have $y^{p^2} = (ux^{-\alpha})^{p^2} = u^{p^2} x^{-\alpha p^2} = 1$. Thus P is isomorphic to $N_n(p)$.

Next suppose $p=2$. Since $[P : H]=4$, P/H is cyclic of order 4 or abelian of type (2, 2).

Case 1. P/H is cyclic of order 4. In this case, by Theorem 1 we must have $n \geqq 6$, and there exists an element u in $P-H$ such that P is generated by x and u with the relation $x^u = x^{1+2^{n-4}+2^{n-3} \cdot \varepsilon_2}$ or $x^u = x^{-1-2^{n-4}+2^{n-3} \cdot \varepsilon_2}$. If $x^u = x^{1+2^{n-4}+2^{n-3} \cdot \varepsilon_2}$, then $(x^4)^u = x^4$, whence x^4 is contained in $Z(P)$. Since $[x, u] = x^{2^{n-4}+2^{n-3} \cdot \varepsilon_2}$, we have $P' = \langle x^{2^{n-4}} \rangle$. It follows that P' is contained in $Z(P)$, in particular we have $cl(P)=2$. In our case it is easily verified that $Z(P)=$

$<x^4>$. Since u^4 is contained in H, u^4 is also contained in $Z(P)$. Therefore we can put $u^4=x^{4\alpha}$ for some integer α. Since $n\geqq 6$, for β in (1.4) with $i=4$ we put $y=ux^\beta$. Then P is generated by x and y with the relations $x^y=x^u$ and

$$\begin{aligned} y^4=(ux^\beta)^4 &= u^4\ (x^\beta)^{u3}\ (x^\beta)^{u2}\ (x^\beta)^u x^\beta \\ &= x^{4\alpha}\cdot x^{\beta\{(1-2^{n-4}+2^{n-3}\cdot\varepsilon_2)+(1+2^{n-3})+(1+2^{n-4}+2^{n-3}\cdot\varepsilon_2)+1\}} \\ &= x^{4\alpha+4\beta(1+2^{n-5})} \\ &= 1. \end{aligned}$$

Hence P is isomorphic to $N_n(2)$. If $x^u=x^{-1-2^{n-4}+2^{n-3}\cdot\varepsilon_2}$, then $[x^i, u]=x^{2i(-1-2^{n-5}+2^{n-4}\cdot\varepsilon_2)}$. Therefor x^i commutes with u if and only if $i\equiv 0$ (mod. 2^{n-3}). Hence we have $Z(P)=<x^{2^{n-3}}>$. On the other hand, since u^4 is contained in H, u^4 is also contained in $Z(P)$, whence $u^4=1$ or $u^4=x^{2^{n-3}}$. If $u^4=x^{2^{n-3}}$, then P is generated by two elements x and ux with the relations $x^{ux}=x^u$ and $(ux)^4=1$. Hence we may assume $u^4=1$. Then P is isomorphic to $S_1(n)$.

Case 2. P/H is abelian of type (2,2). By Theorem 1 we have $n\geqq 5$ and there exist two elements u, v in $P-H$ with the relations $x^u=x^{1+2^{n-3}}$ and $x^v=x^{-1}$ such that P is generated by x, u and v, and such that all of $[u, v]$, u^2 and v^2 are contained in H. Let K and L be the subgroups of P generated by x and u, and by x and v, respectively. Then by using Theorem 2 we obtain that L is isomorphic to D_{n-1} or Q_{n-1} (in particular v is of order 2 or of order 4 not contained in $Z(L)$). Since K is nonabelian and $[x^2, u]=1$, $Z(K)$ is generated by x^2. Therefore we may put $u^2=x^{2\alpha}$ for some integer α, since u^2 is in $Z(K)$ Since $n\geqq 5$, we put $y=ux^\beta$ for β in (1.4) with $i=3$. Then we have $K=<x,y\ ;\ x^{2^{n-2}}=y^2=1,\ x^y=x^{1+2^{n-3}}>$. Also we have $v^y=v$ or $v^y=vx^{2^{n-3}}$. Because, since L is normal in P generated by y and elements in L, if we put $v^y=vx^i$ (if L is isomorphicto D_{n-1}, $\{vx^i;\ i=1, \ldots, 2^{n-2}\}$ is the full set of involutions in $L-H$, while if L is isomorphic to Q_{n-1}, $\{vx^i;\ i=1, \ldots, 2^{n-2}\}$ is the full set of elements of order 4 in $L-H$), then $v=v^{y^2}=(vx^i)^y=vx^{2i(1+2^{n-4})}$, which implies $i\equiv 0$ (mod. 2^{n-3}). First assume $v^y=v$. If L is isomorphic to D_{n-1}, *i. e.* $v^2=1$, then P is isomorphic to $S_2(n)$. On the other hand, if L is isomorphic to Q_{n-1}, then P is isomorphic to $S_3(n)$, since $v^2=x^{2^{n-3}}$. Next assume $v^y=vx^{2^{n-3}}$. If we put $z=vx$, then P is generated by x, y and z with the following relations:

$$\begin{aligned} &z^2=(vx)^2=v^2x^vx=1 \text{ or } x^{2^{n-3}}, \\ &z^y=(vx)^y=vx^{2^{n-3}}\cdot\ x^{1+2^{n-3}}=vx=z, \\ &x^z=x^{vx}=x. \end{aligned}$$

Therefore P is isomorphic to $S_2(n)$ or $S_3(\mathrm{n})$. Thus the proof is completed.

§ 2. p-groups with a non-self-centralizing, normal cyclic subgroup of index p^2.

In this section we treat the p-groups with a non-self-centralizing, normal cyclic subgroup of index p^2. First, by using Theorem 1 we construct some particular p-groups. Let H be an abelian p-group of order p^{n-1} ($\mathrm{n}\geqq 4$) generated by two elements x and y with the following defining relations

$$x^{p^{n-2}}=y^p=[x, y]=1$$

Let K_l be a cyclic group of order p^l ($l=1,2,3$) generated by z_l. For elements $z_1{}^i$ ($i=1, \ldots, p$) in K_1, the mappings $(z_1{}^i)^{\varphi_1}$ and $(z_1{}^i)^{\varphi_2}$ defined the relations

$$(x^jy^k)^{(z_1{}^i)\varphi_1}=x^{j(1+p^{n-3})^i}\ y^k,\ (x^j\ y^k)^{(z^i{}_1)\varphi_2}=x^{j(1+p^{n-3})^i}(yx^{i\cdot p^{n-3}})^k$$

are cleary automorphisms of H and both φ_1 and φ_2 are homomorphisms of K_1 into $Aut(H)$ Hence the following two semidirect products of H by K_1 with respect to φ_1 and φ_2 exist for p odd, $n\geqq 4$ and for $p=2$, $n\geqq 5$;

$$I_n(p)=\langle x, y, z;\ x^{p^{n-2}}=y^p=z^p=1,\ x^y=x,\ x^z=x^{1+p^{n-3}},\ y^z=y\rangle,$$
$$J_n(p)=\langle x, y, z;\ x^{p^{n-2}}=y^p=z^p=1,\ x^y=x,\ x^z=x^{1+p^{n-3}},\ y^z=yx^{p^{n-3}}\rangle.$$

Also for $z_2^i(i=1, \ldots, p^2)$ in K_2, it is easily verified that the mappings $(z_2^i)^\varphi$ defined the relation

$$(x^j)^{(z_2{}^i)\varphi}=x^{j(1+p^{n-3})^i}$$

are automorphisms of the group generated by x and that φ is a homomorphism of K_2 into $Aut(\langle x\rangle)$. Therefore the semidirect product of the group $\langle x\rangle$ by K_2 with respect to φ exists for p odd, $n\geqq 4$ and for $p=2$, $n\geqq 5$;

$$K_n(p)=\langle x,\ y;\ x^{p^{n-2}}=y^{p^2}=1,\ x^y=x^{1+p^{n-3}}\rangle.$$

Next assume $p=2$. For $z_1{}^i$ ($i=1,2$) in K_1, if we define

$$(x^j\ y^k)^{(z_1{}^i)\varphi}=x^{(-1)^i\cdot j}\ y^k,\ (x^j\ y^k)^{(z_1{}^i)\varphi_2}=x^{(-1+2^{n-3})^i\cdot j}\ y^k,$$
$$(x^j\ y^k)^{(z_1{}^i)\varphi_3}=x^{(-1)^i\cdot j}(yx^{2^{n-3}\cdot i})^k,$$

then the mapping$(z_1^i)^{\varphi_m}$ ($i=1,2;\ m=1,2,3$) is an automorphism of H and each of φ_m is a homomorphism of K_1 into $\mathrm{Aut}\,(H)$. Hence also we obtain the following three groups;

$$P_1(n)=\langle x, y, z;\ x^{2^{n-2}}=y^2=z^2=1,\ x^y=x,\ x^z=x^{-1},\ y^z=y\rangle,$$
$$P_2(n)=\langle x, y, z;\ x^{2^{n-2}}=y^2=z^2=1,\ x^y=x,\ x^z=x^{-1+2^{n-3}},\ y^z=y\rangle,$$
$$P_3(n)=\langle x, y, z;\ x^{2^{n-2}}=y^2=z^2=1,\ x^y=x,\ x^z=x^{-1},\ y^z=yx^{2^{n-3}}\rangle,$$

where $P_1(n)$ and $P_3(n)$ are defined for $n \geqq 4$ and $P_2(n)$ is defined for $n \geqq 5$. Also for $z_2^i (i=1, \ldots, 4)$ in K_2, we can verify that the mappings $(z_2^i)^{\varphi_1}$ and $(z_2^i)^{\varphi_2}$ defined

$$(x^j)^{(z_2^i)\varphi_1} = x^{j\cdot(-1)^i}, \quad (x^j)^{(z_2^i)\varphi_2} = x^{j(-1+2^{n-3})^i}$$

are automorphisms of the group generated by x and that both φ_1 and φ_2 are homomorphisms of K_2 into $Aut\,(<x>)$. Hence we have the following two semidirect products of the group $<x>$ by K_2 with respect to φ_1 and φ_2;

$$P_4(n) = <x,\ y;\ x^{2^{n-4}} = y^4 = 1,\ x^y = x^{-1}>,$$
$$P_5(n) = <x,\ y;\ x^{2^{n-4}} = y^4 = 1,\ x^y = x^{-1+2^{n-3}}>,$$

where $P_4(n)$ and $P_5(n)$ are defined for $n \geqq 4$ and $n \geqq 5$, respectively.

Now we denote by M a group generated by $x^{2^{n-3}}$. Let $f_l (l=2,3)$ be the isomorphism of M into K_l determined by

$$(x^{2^{n-3}})^{f_2} = z_2^2, \quad (x^{2^{n-3}})^{f_3} = z_3^4.$$

Also let $z_l^{\varphi_l} (l=2,3)$ be an automorphism of H which inverts all its elements. Then each φ_l determines a homomorphism of K_l into $Aut\,(H)$ and we can easily verified that (1.2) is satisfied. Therefore there are the following two partial semidirect products of H and the group $<x>$ by K_2 and K_3 with respect to φ_2 and the restriction of φ_3 to the group $<x>$ $\varphi_3|_{<x>}$, respectively;

$$P_6(n) = <x, y, z;\ x^{2^{n-3}} = z^2,\ y^2 = z^4 = 1,\ x^y = x,\ x^z = x^{-1},\ y^z = y>,$$
$$P_7(n) = <x, y;\ x^{2^{n-3}} = y^4,\ y^8 = 1,\ x^y = x^{-1}>,$$

where both $P_6(n)$ and $P_7(n)$ are defined for $n \geqq 4$.

First of all, we study the properties of p-groups defined above.

THEOREM 2.1. *The followings hold;*

(1) (a) *If P is one of the groups $I_n(p)$, $J_n(p)$ and $K_n(p)$, then $cl(P)=2$ and P' is cyclic of order p.*

(b) *If $P=I_n(p)$, then $Z(P)$ is abelian of type (p^{n-3}, p)* and *$\Phi(P)$ is cyclic of order p^{n-3}.*

(c) *If $P=J_n(p)$, then $Z(P)$ is cyclic of order p^{n-2} and $\Phi(P)$ is cyclic of order p^{n-3}.*

(d) *If $P=K_n(p)$, then $Z(P)=\Phi(P)$ is abelian of type (p^{n-3}, p).*

(2) (a) *$cl(P_i(n))=n-2$ and the commutator subgroup $P_i(n)'$ of $P_i(n)$ is cyclic*

of order 2^{n-3} *for* $i=1, \ldots, 7$.

(b) $Z(P_i(n))$ *is abelian of type* $(2,2)$ *for* $i=1,2,4,5,6$, *while* $Z(P_i(n))$ *is cyclic of order* 4 *for* $i=3,7$.

(c) $\Phi(P_i(n))=P_i(n)'$ *for* $i=1,2,3,6$ *and* $\Phi(P_i(n))$ *is abelian* of *type* $(2^{n-3},2)$ *for* $i=4,5,7$.

(d) $I(P_1(n))=3+2^{n-3}$, $I(P_2(n))=3+2^{n-3}$, $I(P_6(n))=3$, $I((P_4(n))^2)=2$ *and* $I((P_5(n))^2)=3$.

(3) *No two of the groups* $I_n(p)$, $J_n(p)$, $K_n(p)$ *and* $P_i(n)$ *for* $i=1, \ldots, 7$ *are isomorphic.*

PROOF: Put $P=I_n(p)$, $J_n(p)$, $K_n(p)$ and $P_t(n)$ for $i=1, \ldots, 7$ as the case may be and let P be generated by or by x, y and z satisfying the appropriate relations. In the first case, we can easily verify that $Z(I_n(p))$, $Z(J_n(p))$ and $Z(K_n(p))$ cantains the subgroup $<x^p>\times<y>$, $<yx^{p-1}>$ and $<x_p>\times<y^p>$ of order p^{n-2}, respectively. On the other hand, P is nonabelian, and the order of $Z(P)$ is less than p^{n-1}, whence $Z(I_n(p))=<x^p>\times<y>$, $Z(J_n(p))=<yx^{p-1}>$ and $Z(K_n(p))=<x^p>\times<y^p>$. By the defining relations of the generators of P, we can easily verify that P' is generated by $x^{p^{n-3}}$ in all cases. Therefore, in particular, it follows $cl(P)=2$ in each case. Since $K_n(p)$ is nonabelian and $\Phi(K_n(p))$ contains x^p and y^p, we conclude $\Phi(K_n(p))=Z(K_n(p))$. Let P be either of $I_n(p)$ or $J_n(p)$, then the factor group $P/<x>$ is elementary abelian. Therefore we have the series of the subgroups of P: $<x^p>\leq\Phi(P)\leq<x>$. Since the subgroup of P generated by y and z is abelian of type (p, p) for $P=I_n(p)$, P is not to be generated by y and z. Therefore $\Phi(I_n(p))=<x^p>$ is cyclic of order p^{n-3}. Since two factor groups $J_n(p)/<x>$ and $J_n(p)/Z(J_n(p))$ are both elementary abelian and $Z(J_n(p))=<yx^{p-1}>$, the group $<x^p>=<x>\cap Z(J_n(p))$ contains $\Phi(J_n(p))$. Hence we obtain $\Phi(J_n(p))=<x^p>$.

Now consider (2). We can directly verify the following equations by an elementary calculation:

$$Z(P_in))=\begin{cases} <x^{2^{n-3}}>\times<y> & \text{if } i=1,2,6, \\ <yx^{2^{n-4}}> & \text{if } i=3, \\ <x^{2^{n-3}}>\times<y^2> & \text{if } i=4,5, \\ <y^2> & \text{if } i=7, \end{cases}$$

$$(P_i(n))^{(j)}= \quad <x^{2^j}> \quad \text{for } i=1, \ldots, 7 \text{ and for all } j.$$

$$\Phi(P_i(n))=\begin{cases} <x^2> & \text{if } i=1,2,3,6 \\ <x^2>\times<y^2> & \text{if } i=4,5 \\ <x^2>\times<y^2\, x^{2^{n-4}}> & \text{if } i=7. \end{cases}$$

Let H_i be the subgroup of $P_i(n)$ generated by the element x for $i=1, \ldots, 7$. Then $zH_1 \cup yzH_1$ consists of only involutions and $z\mho^1(H_2) \cup yz\mho^1(H_2)$ is the full set of involutions in $zH_2 \cup yzH_2$, while $zH_6 \cup zyH_6$ consists of elements of order 4. Therefore we have

$$I(P_1(n))=3+2^{n-3},\ I(P_2(n))=3+2^{n-4},\ I(P_6(n))=3.$$

After an easy calculation we have $(yH_4 \cup y^3H_4)^2=\{y^2\}$, $(y\mho^1(H_5) \cup y^3\mho^1(H_5))^2=\{y^2\}$ and $(yx\mho^1(H_5) \cup y^3 x\mho^1(H_5))^2=\{y^2 x^{2^{n-3}}\}$, whence it follows that $(yH_5 \cup y^3H_5)^2=\{y^2, y^2 x^{2^{n-3}}\}$. Hence $I((P_4(n))^2)=2$ and $I((P_5(n))^2)=3$, that is, we obtain (2).

(3) follows from (1) and (2) immediately.

Now we shall determine the p-groups of order $p^n (n \geqq 4)$ with a non-self-centralizing, normal cyclic subgroup of index p^2.

THEOREM 2.2. *Let P be a nonabelian p-group of order $p^n (n \geqq 4)$ which contains a non-self-centralizing, normal cyclic subgroup of order p^{n-2}. Then the followings hold:*

(1) *If p is odd, then P is isomorphic to $I_n(p)$, $J_n(p)$, $K_n(p)$ or $M_n(p)$.*

(2) *If $p=2$, then P is isomorphic to D_n, Q_n, S_n, $M_n(2)$, $I_n(2)$, $J_n(2)$, $K_n(2)$ or $P_i(n)$ $(i=1, \ldots, 7)$.*

PROOF: Let H be a non-self-centralizing, normal cyclic subgroup of order p^{n-2} of P with its generator x and let K be the centralizer of H in P. If $K=P$, then H is contained in $Z(P)$. Since P is nonabelian, H is the center of P, whence, in particular. we obtain $cl(P)=2$. If P contains a cyclic subgroup of order p^{n-1}, by Theorem 2 and Theorem 3 in section 3, P is isomorphic to M_n(p). Assume that P does not contain any cyclic subgroups of order p^{n-1}. Then, by the nonabelian property of P, the factor group $P/H=P/Z(P)$ is not cyclic of order p^2, and so this factor group is abelian of type (p, p). Moreover, any proper subgroup L of P containing H properly is abelian of type (p^{n-2}, p), since H is a maximal cyclic subgroup in L. Therefore we can find two elements y and z of order p in P-H such that

$$P=\langle x, y, z;\ x^{p^{n-2}}=y^p=z^p=1,\ x^y=x^z=x,\ y^z=y^i x^{p^{n-3}\cdot j}\rangle.$$

If $j \equiv 0 \pmod{p}$, *i.e.* $y^z \equiv y^i$, then $i \equiv 1 \pmod{p}$, since the subgroup generated by y and z is of order p^2. Consequently P is abelian, which is contrary to the assumption to P. Therefore $j \not\equiv 0 \pmod{p}$. Then, by replacing x^j by x, we have $y^z=y^i x^{p^{n-3}}$. Since the subgroup L generated by x and z is also normal in P and since $\Omega_1(L)$ is generated by z and $x^{p^{n-3}}$, for some integers k and l we can put $z^y=z^k\ x^{p^{n-3}\cdot l}$. Then, from two relations $y^z=y^i\ x^{p^{n-3}}$ and $z^y=z^k\ x^{p^{n-3}\cdot l}$, we have

$$y^{i-1}\ z^{-1}\ x^{p^{n-3}}=z^{-k}\ x^{-p^{n-3}\cdot l}.$$

In particular, it follows $i\equiv 1\pmod{p}$. In this case, we may choose the appropriate generators of P as follows;

$$P=\langle y^{-1}x^{p-1},y,\ z;\ (y^{-1}\ z^{p-1})^{p^{n-2}}=y^p=z^p=1,\ (y^{-1}\ x^{p-1})^y=y^{-1}\ x^{p-1},$$
$$(y^{-1}\ x^{p-1})^z=(y^{-1}\ x^{p-1})^{1+p^{n-3}}\rangle.$$

Therefore P is isomorphic to $J_n(p)$. Hence we may assume $K<P$. Then by the assumption $[P:K]=[K:H]=p$ and P/K is isomorphic to a subgroup of order p of $Aut(H)$. Since $H\leq Z(K)$, and since $[K:H]=p$, K is abelian. If K is cyclic, then by Theorem 2 P is isomorphic to D_n, Q_n or S_n. Hence also we may assume that P does not contain any cyclic subgroups of order p^{n-1}. Then since H is a maximal cyclic subgroup of K, there exists an element y in $K-H$ such that $K=H\times\langle y\rangle$. In this case, by Theorem 1 we must have $n\geqq 4$ and there exists an element u in $P-K$ such that P is generated by the elements x, y and u with the following relations:

(2.1) $x^u=x^{1+p^{n-3}}$, $y^u=y^i\ x^{jp^{n-3}}(1\leqq i\leqq p-1,\ 0\leqq j\leqq p-1)$ for p odd, and for $p=2$ $y^u=y$ or $y^u=yx^{2^{n-3}}$ and

(2.2) $x^u=x^{-1}$ if $n=4$,
$x^u=x^{-1}$, $x^u=x^{1+2^{n-3}}$ or $x^u=x^{-1+2^{n-3}}$ if $n\geqq 5$.

First assume p odd and denote by $P_{i,j}$ the group generated by x, y and u with the relation (2.1). Since $[P:K]=p$ and K is abelian, any element v in P-K generates the factor group P/K and v^p is contained in K, whence v^p is contained in $Z(P)$. On the other hand, $(x^p)^u=(x^u)^p=x^p$. Therefore, for every element w in K, w^p is contained in $Z(P)$. We conclude at once that the factor group $P/Z(P)$ is of exponent p. If $j\neq 0$, then in $P_{i,j}$ by replacing x^j by x $P_{i,j}$ is isomorphic to $P_{i,1}$. Next assume $i\neq 1$. Then we may choose an integer i' satisfying the congruence

$$i'(i-1)\equiv 1\pmod{p}.$$

For such integer i' we have $(yx^{i'p^{n-3}})^u=y^u\ x^{i'p^{n-3}}=y^i\ x^{p^{n-3}}\cdot x^{i'p^{n-3}}=(yx^{i'p^{n-3}})^i$ in $P_{i,1}$, whence $P_{i,1}$ is isomorphic to $P_{i,0}$ if we replace $yx^{i'p^{n-3}}$ by y. On the other hand, in $P_{i,0}$ two elemens u and y generate the subgroup of order p^2, and so we have $i=1$. Therefore we may assume that $P=P_{1,0}$ or $P=P_{1,1}$. If

$P=P_{1,0}$, then $Z(P)$ contains an abelian subgroup $<x^p>\times<y>$ of order p^{n-2}. On the other hand, since P is nonabelian, $[P: Z(P)]\geqq p^2$. Hence $Z(P)=<x^p>\times<y>$. In particular $cl(P)=2$. Since u^p is contained in $Z(P)$, for some integers α and β we can put $u^p=x^{\alpha p}y^{\beta}$. In this case we put $z=ux^{-\alpha}$. Then P is generated by three elements x, y and z, and we have two relations $x^z=x^{ux^{-\alpha}}=x^{1+p^{n-3}}$, $y^z=y$. Moreover by Lemma 1.2 $z^p=(ux^{-\alpha})^p=u^p x^{-\alpha p}=y^{\beta}$ since $P/Z(P)$ is of exponent p and $cl(P)=2$. Therefore, if $\beta\equiv 0$ (mod. p), P is isomorphic to $I_n(p)$, while if $\beta\not\equiv 0$ (mod. p), P is isomorphic to $K_n(p)$. If $P=P_{1,1}$, then $(x^i y^j)^u=x^{i(1+p^{n-3})} y^j x^{p^{n-3}\cdot j}=x^i y^j\cdot x^{(i+j)p^{n-3}}$. Hence $x^i y^j$ is contained in $Z(P)$ if and only if $i+j\equiv 0$ (mod. p). Consequently $Z(P)$ is a cyclic group of order p^{n-2} generated by an element yx^{p-1}. Since u^p is contained in K, u^p is also contained in $Z(P)$. u does not generate $Z(P)$, since otherwise P would possess a cyclic subgroup of order p^{n-1}, which is contrary to our assumption. Therefore we can write $u^p=x^{\alpha p(p-1)}$ for some integer α. In this case, if we put $z=ux^{-\alpha(p-1)}$, then we may easily verify that P is generated by x, y and z and that P is isomorphic to $J_n(p)$.

Next assume p=2. We denote by Q the 2-group generated by x, y and u with $y^u=y$ and one of the relations (2.2), wihle we denote by $Q^\star$ the 2-group generated by x, y and u with $y^u=yx^{2^{n-3}}$ and one of the relations (2.2). First suppose $x^u=x^{1+2^{n-3}}$. By the similar method used in the case that p is odd we have $Z(Q)=<x^2>\times<y>$ and $Z(Q^\star)=<xy>$. On the other hand, since u^2 is contained in K, u^2 is also contained in $Z(P)$ (where P denotes one of the groups Q and $Q^\star$), whence for some integer α we can put

$$u^2=x^{2\alpha} \text{ or } u^2=x^{2\alpha}y \qquad \text{if } P=Q,$$
$$u^2=x^{2\alpha} \qquad \text{if } P=Q^\star$$

since by our assumption P does not contain any cyclic subgroups of order 2^{n-1}. Assume $u^2=x^{2\alpha}$. Since $n\geqq 5$, for β in (1.3) with $i=3$ we put $z=ux^{\beta}$. Then we obtain $z^2=1$. Also assume $u^2=x^{2\alpha}y$. If we put $z=ux^{2^{n-4}-\alpha}$ in case α odd, while if we put $z=ux^{2^{n-3}-\alpha}$ in case α even, then we have $z^2=y$ in either case. Thus Q is isomorphic to $I_n(2)$ or $K_n(2)$, while $Q^\star$ is isomorphic to $J_n(2)$. Next consider $x^u=x^{-1}$ or $x^u=x^{-1+2^{n-3}}$. In either case, it is easily verified that $Z(Q)=<x^{2^{n-3}}>\times<y>$ is an abelian group of type (2,2) and that $Z(Q^\star)=<yx^{2^{n-4}}>$ is a cyclic group of order 4. First assume $P=Q$. Since u^2 is contained in $Z(P)$, one of the following four relations holds; $u^2=1$, $u^2=x^{2^{n-3}}$, $u^2=y$ or $u^2=x^{2^{n-3}}y$. If $u^2=1$, then P is isomorphic to $P_1(n)$ or $P_2(n)$. If $u^2=x^{2^{n-3}}$, and $x^u=x^{-1}$, then P is isomorphic to $P_6(n)$, while if $u^2=x^{2^{n-3}}$ and

$x^u=x^{-1+2^{n-3}}$, then P is isomorphic to $P_2(\mathrm{n})$ since by putting $z=ux$ P is generated by the elements x, y and z with the relations $x^z=x^u=x^{-1+2^{n-3}}$ and $z^2=1$. Suppose $u^2=x^{2^{n-3}}y$. If $x^u=x^{-1}$, then we replace $x^{2^{n-3}}y$ and ux by y and u, respectively, while if $x^u=x^{-1+2^{n-3}}$, then we replace ux by u. Then we shall have the relation $u^2=y$. In this case P is generated by the elements x and u with the relations $u^4=1$ and $x^u=x^{-1}$ or $x^u=x^{-1+2^{n-3}}$, and so P is isomorphic to $P_4(n)$ or $P_5(n)$. Next assume $P=Q^\star$. If $x^u=x^{-1+2^{n-3}}$, then $(xy)^u=x^{-1+2^{n-3}}\cdot yx^{2^{n-3}}=(xy)^{-1}$, whence by replacing x by xy we may assume $x^u=x^{-1}$. In this case we may put $u^2=(yx^{2^{n-4}})^\alpha$ for $\alpha=0,1,2$ or 3 since u^2 is contained in $Z(Q^\star)=\langle yx^{2^{n-4}}\rangle$. If $\alpha=2$ *i.e.* $u^2=x^{2^{n-3}}$, then for the element $z=uy$, we have $y^z=y^u=yx^{2^{n-3}}$ and $z^2=1$. Hence if $\alpha=0$ or $\alpha=2$, then P is isomorphic to $P_3(n)$. If $\alpha=1$ or $\alpha=3$, then it is easily verified that P is isomorphic to $P_7(n)$. Thus the proof is completed.

§ 3. 2-groups of second maximal class

In this section we deal with the 2-groups with the property ($\mathfrak{P}_2$). Moreover, we determine the 2-groups of second maximal class with the cyclic commutator subgroup.

Now we know the following theorem about the 2-groups of maximal class.

THEOREM 3. *Let P be a nonabelian 2-group of order 2^n, of maximal class or with $[P\colon P']=4$. Then P is isomorphic to D_n, Q_n or S_n.*

We begin with the construction of some particular 2-groups with the property ($\mathfrak{P}_2$). Let N_1 and N_2 be $M_{n-1}(2)$ and an abelian group of type $(2^{n-2},2)$, respectively, that is

$$N_1=\langle x_1,\ y_1;\ x_1^{2^{n-2}}=y_1^{\,2}=1,\ x_1^{y_1}=x_1^{1+2^{n-3}}\rangle,$$
$$N_2=\langle x_2,\ y_2;\ x_2^{2^{n-2}}=y_2^{\,2}=1,\ x_2^{y_2}=x_2\rangle.$$

For $l=1,2$ let K_l be a cyclic group of order 2^l generated by z_l. Then we may define the homomorphisms φ_1 and φ_2 of K_1 into the automorphism group of N_1 and the homomorphisms φ_3 and φ_4 of K_1 into the automorphism group of N_2 as follows:
For element z_1 in K_1 and for $y_i^{\,j}\ x_i^{\,k}$ in N_i $(i=1,2)$,

$$(y_1^{\,j}\ x_1^{\,k})^{z_1^{\varphi_1}}=(y_1\ x_1^{\,2^{n-3}})^j\ (y_1x_1^{\,-1})^k$$
$$(y_1^{\,j}\ x_1^{\,k})^{z_1^{\varphi_2}}=y_1^{\,j}\ (y_1x_1^{\,-1+2^{n-4}})^k$$

$$(y_2^j\ x_2^k)^{z_1\varphi_3}=y_2^j\ (y_2x_2^{-1})^k$$
$$(y_2^j\ x_2^k)^{z_1\varphi_4}=(y_2\ x_2^{2^{n-3}})^j\ (y_2x_2^{-1+2^{n-4}})^k.$$

Therefore we have the following four semidirect products of N_1 or N_2 by K_1.

$$Q_1(n)=\langle x,y,z;\ x^{2^{n-2}}=y^2=z^2=1,\ x^y=x^{1+2^{n-3}},\ x^z=yx^{-1},\ y^z=yx^{2^{n-3}}\rangle,$$
$$Q_2(n)=\langle x,y,z;\ x^{2^{n-2}}=y^2=z^2=1,\ x^y=x^{1+2^{n-3}},\ x^z=yx^{-1+2^{n-4}},\ y^z=y\rangle,$$
$$Q_3(n)=\langle x,y,z;\ x^{2^{n-2}}=y^2=z^2=1,\ x^y=x,\ x^z=yx^{-1},\ y^z=y\rangle,$$
$$Q_4(n)=\langle x,y,z;\ x^{2^{n-2}}=y^2=z^2=1,\ x^y=x,\ x^z=yx^{-1+2^{n-4}},\ y^z=yx^{2^{n-4}}\rangle.$$

Next, let M_1 be a subgroup of N_1 generated by $x_1^{2^{n-3}}$ and let M_2 be a subgroup of N_2 generated by y_2. For z_2 in K_2 and for $y_i^j\ x_i^k$ in $N_i(i=1,2)$, we may define the homomorphism φ_i of K_2 into the automorphism group of N_i and the isomorphism f_i of M_i into K_2 such that

$$(y_1^j\ x_1^k)^{z_2\varphi_1}=y_1^j(y_1x_1^{-1+2^{n-4}})^k,\ (x_1^{2^{n-3}})^{f_1}=z_2^2,$$
$$(y_2^j\ x_2^k)^{z_2\varphi_2}=y_2^j(y_2\ x_2^{-1})^k,\ y_2^{f_2}=z_2^2.$$

Then it is easily verified that (1.2) is satisfied. It follows that the partial semidirect products $Q_5(n)$, $Q_6(n)$ exist.

$$Q_5(n)=\langle x,y,z;\ x^{2^{n-3}}=z^2,\ y^2=z^4=1,\ x^y=x^{1+2^{n-3}},\ x^z=yx^{-1+2^{n-4}},\ y^z=y\rangle,$$
$$Q_6(n)=\langle x,y,z;\ x^{2^{n-3}}=z^2,\ y^2=z^4=1,\ x^y=x,\ x^z=yx^{-1},\ y^z=y\rangle.$$

If we replace zx^{-1} by y in $Q_1(n)$, while if we replace zx by y in $Q_i(n)$ for $i=2,\ \dots,\ 6$, then we can rewrite the groups $Q_i(n)$ in the followings;

$$Q_1(n)=\langle x,\ y;\ x^{2^{n-2}}=y^4=1,\ x^y=y^2x^{-1},\ x^{y^2}=x^{1+2^{n-3}}\rangle,$$
$$Q_2(n)=\langle x,\ y;\ x^{2^{n-3}}=y^4,\ y^8=1,\ x^y=y^2\ x^{-1+2^{n-3}},\ x^{y^2}=x^{1+2^{n-3}}\rangle,$$
$$Q_3(n)=\langle x,\ y;\ x^{2^{n-2}}=y^4=1,\ x^y=y^2\ x^{-1},\ x^{y^2}=x\rangle,$$
$$Q_4(n)=\langle x,\ y;\ x^{2^{n-3}}=y^4,\ y^8=1,\ x^y=y^2\ x^{-1},\ x^{y^2}=x\rangle,$$
$$Q_5(n)=\langle x,\ y;\ x^{2^{n-3}}=y^4,\ y^8=1,\ x^y=y^2\ x^{-1},\ x^{y^2}=x^{1+2^{n-3}}\rangle,$$
$$Q_6(n)=\langle x,\ y;\ x^{2^{n-2}}=y^4=1,\ x^y=y^2\ x^{-1+2^{n-3}},\ x^{y^2}=x\rangle.$$

Now we study the properties of six 2-groups defined above.

THEOREM 3.1. *The followings hold:*

(1) *If P is one of the groups $Q_i(n)$ $(i=1,\ \dots,\ 6)$, then P' is cyclic of order 2^{n-3}, $|Z(P)|=2$, $\Phi(P)$ is abelian* of *type $(2^{n-3},\ 2)$ and $cl\,(P)=n-2$.*

(2) *If P is one of the groups $Q_1(n)$, $Q_2(n)$ or $Q_5(n)$, then a maximal abelian*

subgroup of P is of order 2^{n-2}, *while if P is one of the groups* $Q_3(n)$, $Q_4(n)$ *or* $Q_6(n)$, *then a maximal subgroup of P is of order* 2^{n-1}.

(3) *No two of the groups* $Q_1(n)$, $Q_2(n)$, $Q_3(n)$, $Q_4(n)$, $Q_5(n)$ *or* $Q_6(n)$ *are isomorphic.*

PROOF: Put $P=Q_i(n)$ $(i=1, \dots, 6)$ and let P is generated by x and y satisfying the appropriate relations . Then we can directly obtain

$$Z(P)=\langle x^{2n-3}\rangle,\ \Phi(P)=\langle x^2, y^2\rangle,$$
$$P'=\langle y^2\ x^2\rangle,\ P^{(j)}=[P^{(j-1)}, P]=\langle x^{2j}\rangle \text{ for } j=2,3, \dots ,$$

whence (1) holds. By the definition of $Q_i(n)$ $(i=1, \dots, 6)$ we can easily verified that (2) holds. The full set of involutions in $Q_1(n)$, $Q_2(n)$, $Q_3(n)$, $Q_4(n)$, $Q_5(n)$ and $Q_6(n)$ are $\{y^2, x^{2n-3}, y^2 x^{2n-3}, yx, yx^5, \dots, y^{-1}x^3, y^{-1}x^7, \dots\}$, $\{x^{2n-3}, y^2 x^{\pm 2n-4}, yx, yx^3, \dots, y^{-1} x, y^{-1}x^3, \dots\}$, $\{y^2, x^{2n-3}, y^2 x^{2n-3}, yx, yx^3, \dots, y^{-1} x, y^{-1} x^3, \dots\}$, $\{x^{2n-3}, y^2x^{\pm 2n-4}, yx^3, yx^7, \dots, y^{-1} x^3, y^{-1} x^7, \dots\}$, $\{x^{2n-3}, y^2 x^{\pm 2n-4}\}$ and $\{y^2, x^{2n-3}, y^2 x^{2n-3}\}$, respectively. Therefore $I(Q_1(n))=3+2^{n-3}$. $I(Q_2(n))=3+2^{n-2}$ and $I(Q_5(n))=3$, whence no two of $Q_1(n)$, $Q_2(n)$ or $Q_5(n)$ are isomorphic. Since elements of order 8 of $Q_3(n)$ or $Q_6(n)$ are contained in the subgroup generated by two elements x and y^2, and since $I(Q_3(n))=3+2^{n-2}$ and $I(Q_6(n))=3$, no two of $Q_3(n)$, $Q_4(n)$ or $Q_6(n)$ are isomorphic. Thus (3) holds.

Each $Q_i(n)$ $(i=1, \dots, 6)$ possesses the property $(\mathfrak{P}_2)$. However, we show in the following lemma that this property $(\mathfrak{P}_2)$ characterizes these groups among 2-groups of order $2^n (n\geqq 6)$ if the class number is more than 3.

LEMMA 3.1. *Let P be a nonabelian 2-group of order* $2^n (n\geqq 6)$ *with the property* $(\mathfrak{P}_2)$. *Then we have that* $cl(P)\leqq 3$ *or that P is isomorphic to one of the groups* $Q_i(n)$ *for* $i=I, \dots, 6$.

PROOF: Let H be a cyclic subgroup of order 2^{n-2} generated by x and let K be the normalizer of H in P. By the assumption we have $[P: K]=2$.

Case 1. H is a self-centralizing subgroup of P. Then by Theorem 2 K is isomorphic to $M_{n-1}(2)$, D_{n-1} Q_{n-1} or S_{n-1}. If K is isomorphic to one of D_{n-1}, Q_{n-1}, or S_{n-1}, then a cyclic subgroup H of order 2^{n-2} of K is a characteristic one since $n\geqq 6$. Therefore H is normal in P, which is contrary to the assumption. Hence K must be isomorphic to $M_{n-1}(2)$. Let K be generated by two elements x and y.

$$K=\langle x,\ y;\ x^{2^{n-2}}=y^2=1,\ x^y=x^{1+2^{n-3}}\rangle.$$

In this case the center of K which is generated by x^2 is normal in P and $\Omega_1(K)$ is an abelian group of type $(2,2)$. Moreover, H is not normal in P and $[P:K]=2$, and the order of yx^i is 2^{n-2} if and only if i is odd. These facts imply that there is an element u in $P-K$ such that P is generated by three elements x, y and u with the relations

$$y^u=y \text{ or } y^u=yx^{2^{n-3}},\quad x^u=yx^i \text{ for } i \text{ odd}.$$

Since $(yx^i)^2=x^{i(2+2^{n-3})}$, for i odd

$$(yx^i)^i=yx^i\cdot x^{i(2+2^{n-3})\cdot\frac{i-1}{2}}=yx^{i\{i(1+2^{n-4})-2^{n-4}\}},$$

whence we have the following equations

$$x^{u^2}=(yx^i)^u=y^u\cdot(x^u)^i=y^u\ (yx^i)^i=y^uy\cdot x^{i\{i(1+2^{n-4})-2^{n-4}\}} \tag{3.1}$$

hold. However, since u^2 is contained in K, we have $x^{u^2}=x$ or $x^{u^2}=x^{1+2^{n-3}}$. Hence by (3.1) one of the congruences

$$i\ \{i(1+2^{n-4})-2^{n-4}\}\equiv 1 \text{ or } 1+2^{n-3} \pmod{2^{n-2}}$$

holds. Since i is odd, the following congruences are obtained from (3.1)

$$i^2\equiv 1 \text{ or } i^2\equiv 1+2^{n-3} \pmod{2^{n-2}}. \tag{3.2}$$

If $i\equiv 1 \pmod 4$, then (3.2) implies one of the three equations $i=1$, $i=1+2^{n-3}$ or $i=1\pm 2^{n-4}$. If $i=1$ or $i=1+2^{n-3}$, then P' is contained in a group $\langle y\rangle\times\langle x^{2^{n-3}}\rangle$ of order 4, whence $cl(P)\leqq 3$. If $i=1\pm 2^{n-4}$, then P' is contained in a group $\langle yx^{2^{n-4}}\rangle$ of order 4.

Hence also $cl(P)\leqq 3$. If $i\equiv -1 \pmod 4$, then from (3.2) we have $i=-1$, $i=-1+2^{n-3}$ or $i=-1\pm 2^{n-4}$. If $i=-1+2^{n-3}$, then by replacing $yx^{2^{n-3}}$ by y we may assume $i=-1$. If $i=-1-2^{n-4}$, then by replacing x^{-1} by x we may assume $i=-1+2^{n-4}$. Therefore we can assume $i=-1$ or $i=-1+2^{n-4}$. First assume $i=-1$, that is, $x^u=yx^{-1}$. Since $Z(K)$ is generated by x^2, obtain that x^{2j} is contained in $Z(P)$ if and only if $(x^{2j})^u=x^{-(2+2^{n-3})j}=x^{2j}$, *i.e.* $4j(1+2^{n-5})\equiv 0 \pmod{2^{n-2}}$. We conclude from this that $Z(P)$ is generated by $x^{2^{n-3}}$ since $n\geqq 6$. Since $[x,u]=yx^{-2+2^{n-3}}$, P' contains a group $\langle yx^2\rangle$ of order 2^{n-3}. Since P is nonabelian, we have $[P:P']\geqq 4$, whence P' is of order 2^{n-3} or 2^{n-2}. If P' is of order 2^{n-2}, then by Theorem 3 P is isomorphic to D_n, Q_n or S_n, which is contrary to the property $(\mathfrak{P}_2)$ of P. Therefore P' is of order 2^{n-3}, and so P' is generated by yx^2. Moreover, we obtain $P^{(j)}=[P^{(j-1)},P]$ is generated by x^{2^j} for $j=2,3,\ldots$. We have the same results for $i=-1+2^{n-4}$ as for $i=-1$;

that is, $Z(P)=\langle x^{2^{n-3}}\rangle$, $P'=\langle yx^2\rangle$ and $P^{(j)}=[P^{(j-1)}, P]=\langle x^{2^j}\rangle$ for $j=2,3,\dots$.

Since u^2 is contained in K, u^4 is contained in $\mho^1(K)=Z(K)$, whence u^4 is also contained in $Z(P)$. Since the element of K whose square is contained in $Z(P)=\langle x^{2^{n-3}}\rangle$ is only an element in the group $\langle x^{2^{n-4}}\rangle\times\langle y\rangle$, we have

$$u^2=1,\ u^2=x^{2^{n-3}},\ u^2=yx^{2^{n-2}},\ u^2=yx^{\pm 2^{n-4}},\ u^2=x^{\pm 2^{n-4}} \text{ or } u^2=y$$

u^2 does not coinside with $x^{\pm 2^{n-4}}$. Because, if $u^2=x^{\pm 2^{n-4}}$, then by $n\geqq 6$ u^2 is contained in $Z(K)$, and so u^2 is also contained in $Z(P)$, whence the order of u is at most 4. However, since $u^2=x^{\pm 2^{n-4}}$ is of order 4, u is of order 8, which is impossible. If $u^2=yx^{2^{n-4}}$, then we have $u^6=yx^{-2^{n-4}}$, whence we may assume $u^2=yx^{-2^{n-4}}$.

If u^2 is contained in H, then by (3.1) we have

$$(3.3)\qquad \begin{aligned} &i=-1+2^{n-4} && \text{if } y^u=y\\ &i=-1 && \text{if } y^u=yx^{2^{n-4}} \end{aligned}$$

Suppose that u^2 is contained in $K-H$. Then, since $x^{u^2}=x^{1+2^{n-3}}$, by (3.1) we have

$$(3.4)\qquad \begin{aligned} &i=-1 && \text{if } y^u=y\\ &i=-1+2^{n-4} && \text{if } y^u=yx^{2^{n-3}}. \end{aligned}$$

If $u^2=1$ or $u^2=x^{2^{n-3}}$, then by (3.3) $y^u=yx^{2^{n-3}}$ for $i=-1$ and $y^u=y$ for $i=-1+2^{n-4}$. First assume $i=-1$. If $u^2=1$, then P is isomorphic to $Q_1(n)$. In case $u^2=x^{2^{n-3}}$ we put $z=yu$ and replace $yx^{2^{n-3}}$ by y. Then P is generated by x, y and z with the relations $x^y=x^{1+2^{n-3}}$, $x^z=yx^{-1}$, $y^z=yx^{2^{n-3}}$ and $y^2=z^2=1$. Hence P is isomorphic to $Q_1(n)$. Next assume $i=-1+2^{n-4}$. If $u^2=1$, then P is isomorphic to $Q_2(n)$. If $u^2=x^{2^{n-3}}$, then P is isomorphic to $Q_5(n)$.

If $u^2=y$ or $u^2=yx^{2^{n-3}}$, then $y^u=y$, whence by (3.4) $i=-1$. If $u^2=y$, then P is isomorphic to $Q_1(n)$ since P is generated by x and u. If $u^2=yx^{2^{n-3}}$, then by replacing ux^2 by z we can easily verify that P is isomorphic to $Q_1(n)$. If $u^2=yx^{-2^{n-4}}$, then $yx^{-2^{n-4}}=(yx^{-2^{n-4}})=y^u x^{2^{n-4}}$. Therefore we obtain $y^u=yx^{2^{n-3}}$. Hence by (3.4) $i=-1+2^{n-4}$. In this case, if we replace ux^2 *by* z, then we have $z^4=x^{2^{n-3}}$, $x^z=z^2x^{-1+2^{n-3}}$ and $x^{z^2}=x^{1+2^{n-3}}$. Hence we have that P is isomorphic to $Q_2(n)$.

Case 2. H is a non-self-centralizing subgroup of P. In this case, $K=C_P(H)$, and so H is contained in $Z(K)$, whence K is abelian. If K is cyclic, then H is normal in P, which is contrary to our assumption. Therefore H is a maximal cyclic subgroup of K, and we may find an involution y in $K-H$ such that K is generated by two elements x and y. Since both $\mho^1(K)=\langle x^2\rangle$ and

$\Omega_1(K)=\langle x^{2^{n-3}}\rangle\times\langle y\rangle$ are normal in P, there is an element u in $P-K$ such that P is generated by x, y and u with the relations

$$y^u=y \text{ or } y^u=yx^{2^{n-3}},\ y^u=yx^i \text{ for } i \text{ odd}.$$

Since u^2 is contained in K, we have $x^{u^2}=x$, whence again (3.2) is obtained.

By the same argument as in case 1, we can easily verify that $cl(P)\leqq 3$ if $i\equiv 1$ (mod. 4), While for $i\equiv -1$ (mod. 4), we may assume $i=-1$ or $i=-1+2^{n-4}$, and if $y^u=y$, then $Z(P)$ is generated by $x^{2^{n-3}}$ and y, while if $y^u=yx^{2^{n-3}}$, then $Z(P)$ is generated by $x^{2^{n-3}}$. Therefore, if $y^u=y$, then we have $i=-1$ and one of the four relations $u^2=1$, $u^2=x^{2^{n-3}}$, $u^2=y$ or $u^2=yx^{2^{n-3}}$ holds since u^2 is contained in $Z(P)$ and $x=x^{u^2}=(yx^i)^u=y^u(x^u)^i=y(yx^i)^i=y^{i+1}x^{i2}=x^{i2}$ (because i is odd). If $u^2=1$ or $u^2=x^{2^{n-3}}$, then P is isomorphic to $Q_3(n)$ or $Q_6(n)$, respectively. If $u^2=y$, then P is isomorphic to $Q_3(n)$, while if $u^2=yx^{2^{n-3}}$, then by replacing ux by z, P is generated by x, y and z with the relations $x^z=x^u=yx^{-1}$, $y^z=y$ and $z^2=x^{2^{n-3}}$. Hence P is isomorphic to $Q_6(n)$. If $y^u=yx^{2^{n-3}}$, then we have $i=-1+2^{n-4}$ and one of the two relations $u^2=1$ or $u^2=x^{2^{n-3}}$ holds. If $u^2=1$, then P is isomorphic to $Q_4(n)$. If $u^2=x^{2^{n-3}}$, then, by replacing uy by z, P is generated by x, y and z with the relations $x^z=x^u=yx^{-1+2^{n-4}}$ and $z^2=1$. Therefore P is isomorphic to $Q_4(n)$. Thus the proof is completed.

By Theorem 1.1, Theorem 2.1 and Theorem 3.1, each of $P_i(n)$ $(i=1,\ldots,7)$, $Q_i(n)$ $(i=1,\ldots,6)$, $S_i(n)$ $(i=1,2,3)$ is a 2-group of class $(n-2)$ with the cyclic commutator subgroup. By using Lemma 3.1 we show that they are characterized among all 2-groups of order 2^n by these properties.

THEOREM 3.2. *Let P be a nonabelian 2-group of order 2^n, where $n\geqq 6$. If its commutator subgroup is cyclic and $cl(P)=n-2$, then P is isomorphic to $P_1(n),\ldots, P_7(n), Q_1(n),\ldots, Q_6(n), S_1(n), S_2(n)$ or $S_3(n)$.*

For proving this theorem we need the next lemma.

LEMMA 3.2. *Let P be a nonabelian 2-group of order 2^n of second maximal class and led H be a normal abelian subgroup of P such that P/H is abelian of type (2,2). If P' is cyclic, then P contains a cyclic subgroup of order 2^{n-2}.*

PROOF: Suppose $cl(P)=n-2$. Since P is nonabelian, we have $[P: \Phi(P)]\geqq 4$. It follows that $[P: P']\geqq 4$. If $[P: P']=4$, then by Theorem 3 P is isomorphic to D_n, Q_n or S_n, which is contrary to $cl(P)=n-2$. Therefore $[P: P']\geqq 8$. If this equality were strict, then the lower central series of P

would necessarily terminate in less than $(n-2)$ steps, whence $cl(P)<n-2$. Hence we must have $[P: P']=8$. Since by the assumption the factor group P/H is abelian of type (2, 2), we have the series of subgroups of P; $H\geq\Phi(P)\geq P'$. Let x be a generator of a cyclic commutator subgroup P' of P. If H is cyclic, the result follows immediately. If H is not cyclic, then P' is a maximal cyclic subgroup of an abelian group H, whence there exists an involution y in $H-P'$ such that H is generated by x and y. Since P/H is abelian of type (2, 2) and $\Phi(P)$ contains P', we can find two elements u and v in $P-H$ such that both u^2 and v^2 are contained in H and such that P is generated by u, v and y. If u^2 or v^2 is of order 2^{n-3}, then the result follows. Therefore we may assume that neither u^2 nor v^2 is of order 2^{n-3}. In this case we shall show that at least one of uv or vu is of order 2^{n-2}. First assume that P is generated by only u and v, *i.e.* $H=\Phi(P)$. In this case both u^2 and v^2 are contained in a group $\langle x^2\rangle\times\langle y\rangle$. Hence we can put for some integers i, j, k and l

(3.5) $$u^2=x^{2i}y^j,\quad v^2=x^{2k}y^l.$$

Also for all integers i' and j' we can find integers i'' and i''' such that

(3.6) $$x^{2i'}y^{j'}u=ux^{2i''}y^{j'},\quad x^{2i'}y^{j'}v=vx^{2i'''}y^{j'}$$

since P' generated by x is normal in P. Since P is generated by u and v, and since P' is contained in H, we can put

(3.7) $$a_1\ \ldots\ a_r=x,$$

where each a_i denotes either of u or v. The number of u and v which appear in the left side of (3.7) are both even, since otherwise, by using (3.5) and (3.6), (3.7) would be equivalent to one of the following congruences for some integers α and β

$$ux^\alpha y^\beta\equiv x,\quad vx^\alpha y^\beta\equiv x \text{ or } uvx^\alpha y^\beta\equiv x \pmod{P'},$$

that is, u, v, or uv would be contained in H, which is contrary to the choice of u and v. If u's (resp. v's) arrange successively in the left side of (3.7), then we replace u^2 (resp. v^2) by $x^{2i}y^j$ (resp. $x^{2k}y^l$). After these process, we may rewrite (3.7) for some integers α, β and γ in the followings

(3.8) $$(uv)^{2\alpha}x^{2\beta}y^\gamma=x \text{ or } (vu)^{2\alpha}x^{2\beta}y^\gamma=x.$$

Then α is a positive integer, since it is clear that α is not equal to 0 in

(3.8). Therefore (3.8) implies that even power of uv or vu generates P' or a cyclic group $<yx>$, whence uv or vu is of order 2^{n-2}.

Next assume that P is not generated by u and v, but that P is generated by u, v and y. In this case we have $\Phi(P)=P'$. Therefore both u^2 and v^2 are contained in P', but neither u nor v is of order 2^{n-2} by our assumption, whence both u^2 and v^2 are contained in $\mho^1(P')=<x^2>$ Hence we can put for some integers i and i'

(3.9) $$u^2=x^{2i},\ v^2=x^{2i'}.$$

Since at least one of the elements u, v and uv cnmmutes with y, we can put for $j=0$ or 1

(3.10) $$yu=uy,\ yv=vyx^{2^{n-4}\cdot j},\ yuv=uvyx^{2^{n-4}\cdot j}$$

or

(3.11) $$yu=uyx^{2^{n-4}\cdot j},\ yv=vyx^{2^{n-4}\cdot j},\ yuv=uvy.$$

Since P is generated by u, v and y, and since P' is contained in H, we can also put

(3.12) $$a_1 \dots a_r=x,$$

where each a_k denotes one of u, v or y. Again, the number of u, v and y which appear in the left side of (3.12) ere all even since the number of u and v which appear in the left side of (3.12) are both even by the same argument as above, and since for the number β of y appearing in the left side of (3.12), (3.12) implies

$$x^{2\alpha}\ y^{\beta}\equiv x \pmod{P'}.$$

However, when each $b_l (l=1, \dots, s)$ denotes u or v, we denote by a and b the cardinality of the sets $\{l: b^l=v\}$ and $\{l: b_l=u\}$, respectively. Then by using (3.10) or (3.11) we have

(3.13) $$yb_1 \dots b_s y=b_1 \dots b_s\ x^{2^{n-4}\cdot aj}$$

or

(3.14) $$yb_1 \dots b_s\ y=b_1 \dots b_s\ x^{2^{n-4}\cdot (a+b)j}.$$

since $x^{2^{n-4}}$ is contained in $Z(P)$. Hence by (3.9) and (3.13) or by (3.9) and (3.14) we can rewrite (3.12) as follows for some integers α and β

$$(uv)^{2\alpha}\ x^{2^{n-4}\cdot\beta}=x \text{ or } (vu)^{2\alpha}\ x^{2^{n-4}\cdot\beta}=x.$$

In this case, α is a positive integer for the same reason as above. Hence one of $(uv)^2$ or $(vu)^2$ generates P', whence uv or vu is of order 2^{n-2}.

PROOF of THEOREM 3.2: We argue by induction on the order of P. Since $cl(P)=n-2$, from the way of the proof of Lemma 3.2 we have $[P: P']=8$. First assume $n=6$. Then P' is cyclic of order 8. If we put $P_1=C_P(P')$, then the factor group P/P_1 is abelian of order 2 or abelian of type (2,2) since $cl(P)=4$ and $Aut(P')$ is abelian of type (2,2). Since both $[P_1, P, P_1]$ and $[P, P_1, P_1]$ are contained in $[P', P_1]=1$, by Three-Subgroup-Lemma $[P_1, P_1, P]=1$. Hence P_1' is contained in the group $Z(P)\cap P'$.
However, $Z(P)\cap P'$ is of order 2 since $cl(P)=4$. In order to prove the theorem for $n=6$, by Theorem 1.2, Theorem 2.2 and Lemma 3.1 we have only to show the existence of a cyclic subgroup of order 16 of P. Let x be a generator of P'.

Case 1. $[P: P_1]=2$. For an element u in $P-P_1$, P is generated by u and the elements in P_1. Since P' is a cyclic group generated by x, we can find two elements v and w in P whose commutator is an odd power of x. Assume both v and w are contained in $P-P_1$, that is, for two elements y_1 and z_1 in P_1 $v=uy_1$ and $w=uz_1$. Then for some odd integer i we have

$$\begin{aligned} x^i=[uy_1, uz_1]&=[u, uz_1]^{y_1}[y_1, uz_1] \\ &=([u, z_1][u, u]^{z_1})^{y_1}[y_1, z_1][y_1, u]^{z_1} \\ &=[u, z_1]^{y_1}[y_1, z_1][y_1, u]^{z_1} \end{aligned}$$

However, since each of $[u, z_1]$, $[y_1, z_1]$ and $[y_1, u]$ is contained in $P'=\langle x\rangle$, at least one of the three commutators is an odd power of x. Hence we may assume that for some element y in P_1 and z in P we have $[y, z]=x$, *i.e.* $y^z=yx$. Since x is of order 8 and since y commutes with x, y must be of not less order than 8. However, if y is of order 8, then the subgroup generated by y possesses a nontrivial intersection to P' since P_1 is of order 32. Then we have $y^4=x^4$, whence $(yx)^4=y^4x^4=1$ contrary to the fact that yx is of order 8. Therefore order of y is at least 16. Thus P contains a cyclic subgroup of order 16.

Case 2. $[P: P_1]=4$. In this case, since P' is contained in $Z(P_1)$ and since $[P_1: P']=2$, P_1 is abelian. Hence by Lemma 3.2 P contains a cyclic subgroup of order 16. Therefore for $n=6$ Theorem 3.2 holds.

Assume $n>6$. Since P' is a nontrivial normal subgroup of P, we may choose the group Z of order 2 in $P'\cap Z(P)$. Let $\bar{P}$ be the factor group P/Z.

Then $\bar{P}^{(i)}=[\bar{P}^{(i-1)}, \bar{P}]=\overline{P^{(i)}}$ for $i=1, \ldots, n$ is cyclic and we have $cl(\bar{P})=n-3$ since $cl(P)=n-2$. Hence by the inductive hypothesis $\bar{P}$ is isomorphic to $P_i(n-1)$ $(i=1, .., 7)$, $Q_i(n-1)$ $(i=1, \ldots, 6)$ or $S_i(n-1)$ $(i=1,2,3)$. Therefore $\bar{P}$ contains a cyclic subgroup $\overline{H}$ of order 2^{n-3}. Let H be the inverse image of $\overline{H}$ in P. Then since H is the central extension of a cyclic group, H is abelian. If H is not cyclic, then for a cyclic group H_1 we must have $H=H_1\times Z$. However, P' is cyclic and Z is contained in P', whence we have $P'\cap H_1=1$. Hence the order of H is at most 2^4 since P' is of order 2^{n-3}. Therefore we have the inequality $2^{n-2}\leqq 2^4$, that is, $n\leqq 6$, which is contrary to $n>6$. Hence H is cyclic of order 2^{n-2}. Therefore by Theorem 1.2, Theorem 2.2 and Lemma 3.1 P is isomorphic to one of the groups $P_i(n)$ $(i=1, \ldots, 7)$, $Q_i(n)$ $(i=1, \ldots, 6)$ or $S_i(n)$ $(i=1,2,3)$.

References

1 N. Blackburn: On a special class of p-groups, Acta Math. 100 (1958), 45~92.
2 _______: Generalizations of certain elementary theorems on p-groups, Proc. London Math. Soc. 11 (1961), 1~22.
3 _______: Automorphisms of finite p-groups, J. Algebra 3 (1966), 28~29.
4 D. Gorenstein: Finite Groups, New York, Harp & Row, 1968.
5 B. Huppert: Endliche Gruppen I, Berlin, Springer, 1968.

Department of Mathematics
University of Electro-communications