§ 14 Some Special p-Groups

(A) *Lemma 14·1* Let f be a representation of the group H by automorphisms of the group K and let $\overline{G} = \langle H, K ; f \rangle$. Let θ be an isomorphic mapping of a normal subgroup M of H into K such that for all $\mu \in M$, $\eta \in H$ and $\xi \in K$ we have

$$\mu^{\theta f(\eta)} = \mu^{\eta\theta} \quad \text{and} \quad \xi^{f(\mu)} = \xi^{\mu^\theta}. \tag{1}$$

Then the set of all pairs (μ^{-1}, μ^θ) with $\mu \in M$ forms a normal subgroup $\overline{M}$ of $\overline{G}$ such that $\overline{H} \cap \overline{M} = \overline{K} \cap \overline{M} = 1$ and $\overline{M} \cong M$.

Here ~~we identify~~ $\overline{H}$ is the subgroup of G with the set of all pairs $(\eta, 1)$, $\eta \in H$; and similarly for $\overline{K}$.

Proof: Let μ_1, μ_2 be in M. Then $\mu_1^{\theta f(\mu_2^{-1})} \mu_2^\theta = \mu_1^{\mu_2^{-1}\theta} \mu_2^\theta = (\mu_2 \mu_1)^\theta$ and so $(\mu_1^{-1}, \mu_1^\theta)(\mu_2^{-1}, \mu_2^\theta) = (\mu_1^{-1}\mu_2^{-1}, \mu_1^{\theta f(\mu_2^{-1})}\mu_2^\theta) = (\mu_1^{-1}\mu_2^{-1}, (\mu_2\mu_1)^\theta) \in \overline{M}$. Thus $\overline{M}$ is a subgroup of $\overline{G}$. The transform of (μ^{-1}, μ^θ) by $(\eta, 1)$ is $(\eta^{-1}\mu^{-1}\eta, \mu^{\theta f(\eta)}) = ((\mu^\eta)^{-1}, \mu^{\eta\theta})$ which is in $\overline{M}$. The transform of (μ^{-1}, μ^θ) by $(1, \xi)$ is $(\mu^{-1}, \xi^{-f(\mu^{-1})} \mu^\theta \xi)$ $= (\mu^{-1}, (\mu^\theta)\xi^{-1}(\mu^\theta)^{-1}\mu^\theta \xi) = (\mu^{-1}, \mu^\theta)$ which is also in $\overline{M}$. Thus $\overline{M} \triangleleft \overline{G} = HK$. It is clear that $H \cap \overline{M} = K \cap \overline{M} = 1$ since θ is an isomorphism. The mapping $(\mu^{-1}, \mu^\theta) \to \mu^{-1}$ is an isomorphism of $\overline{M}$ onto M. Thus 14·1 is proved.

Clearly, $G = \overline{G}/\overline{M} = H_1 K_1$ where $H_1 = \overline{M}\,\overline{H}/\overline{M} \cong H$ and $K_1 = \overline{M}\,\overline{K}/\overline{M} \cong K$. Moreover $K_1 \triangleleft G$ and $H_1 \cap K_1 = M_1 \cong M$.

Conversely, let $G = HK$ with $K \triangleleft G$ and let $M = H \cap K$. Let $f(\eta)$, $\eta \in H$, be the automorphism of K induced by transforming with η. Then f is a representation of K. Since $(\eta_1 \xi_1)(\eta_2 \xi_2) = \eta_3 \xi_3$ where $\eta_3 = \eta_1 \eta_2$ and $\xi_3 = \xi_1^{f(\eta_2)} \xi_2$ for all $\eta_i \in H$, $\xi_i \in K$, the mapping $(\eta, \xi) \to \eta\xi$ of $\overline{G} = \langle H, K ; f \rangle$ onto G is a homomorphism, with kernel $\overline{M}$ such that $\overline{H} \cap \overline{M} = \overline{K} \cap \overline{M} = 1$. Moreover $\overline{M}$ consists of all pairs (μ, μ^{-1}) with $\mu \in M$. If θ is the identity mapping of M considered as a subgroup of H onto itself considered as a subgroup of K, the relations $\mu^{\theta f(\eta)} = \mu^{\eta\theta}$ and $\xi^{f(\mu)} = \xi^{\mu^\theta}$ hold for all $\xi \in K$,

$\eta \in H$ and $\mu \in M$. Hence $\overline{M}$ is one of the normal subgroups of $\overline{G}$ described in 14·1. Hence we have

<u>Lemma 14·12</u>. If $G = HK$ with $K \triangleleft G$, then $G \cong \overline{G}/\overline{M}$ where $\overline{G} = \langle H, K ; f \rangle$, f is the representation of H by the automorphisms of K induced by transforming in G and $\overline{M}$ consists of all pairs (μ, μ^{-1}) with $\mu \in M = H \cap K$. ~~then~~

The conditions (1) of 14·1 are therefore necessary and sufficient for the existence of a <u>semi-normal product</u> $G = HK$ obtained with a given representation f of H by automorphisms of K and a given identification θ of a subgroup M of H with a subgroup ~~there~~ M^θ of K, and such that $M = H \cap K$.

The simplest particular case is that of <u>cyclic extensions</u>. Here we have

<u>Lemma 14·13</u> Let α be an automorphism of the group K which leaves invariant a certain element ξ of K and suppose that α^n is the inner automorphism $t(\xi)$ of K. Then there is a group $G = \{K, \eta\}$ such that $\eta^n = \xi$, $\eta^{-1}\beta\eta = \beta^\alpha$ for all $\beta \in K$ and $|G : K| = n$.

If ξ is of order m, we take $H = \{\eta\}$ to be of order mn, $M = \{\eta^n\}$ and $(\eta^n)^\theta = \xi$. The conditions (1) of 14·1 are then fulfilled.

Since the composition factors of a soluble group are all cyclic of prime order, 14·13 gives by repeated application a method of constructing all ~~finite~~ soluble groups, at least in principle. In simple enough cases, this method is usable and we shall illustrate it by discussing some special types of p-groups.

(B) The <u>exponent</u> of a group G is the least integer $n > 0$ such that $\theta^n = 1$ for all $\theta \in G$. Obviously n divides $|G|$ and is the l.c.m. of the orders of the elements of G. A nilpotent group of exponent n actually has elements of order n.

<u>Lemma 14·21</u> A group G of exponent 2 is Abelian.
For, $\xi = \xi^{-1}$ for all $\xi \in G$ and so $\eta\xi = (\eta\xi)^{-1} = \xi^{-1}\eta^{-1} = \xi\eta$ for all ξ and $\eta \in G$.

<u>Theorem 14·2</u> (i) In a group G of exponent 3, every element commutes with all its conjugates in G, and so $\{\xi^G\}$ is Abelian for all $\xi \in G$.
(ii) If $\{\xi^G\}$ is Abelian for all $\xi \in G$, then G is nilpotent of class at most 3 and $\gamma_3 G$ is of exponent 3.

Proof (i). We have $(\xi\eta)^3 = 1$ for all ξ, η in G and so $\xi^{-1}\eta^{-1}\xi^{-1} = \eta\xi\eta$. Hence
$[\eta, \xi, \xi] = \xi^{-1}\eta^{-1}\xi\eta \cdot \underline{\xi^{-1}\cdot\eta^{-1}\xi^{-1}}\eta\xi \cdot \xi = \xi^{-1}\eta^{-1}\xi\eta \cdot \underline{\eta\xi\eta} \cdot \eta\xi \cdot \xi = \xi^{-1}(\eta^{-1}\xi)^3\xi$ since $\eta^2 = \eta^{-1}$ and so $[\eta, \xi, \xi] = 1$. Hence ξ commutes with $\xi^\eta = \xi[\xi,\eta] = \xi[\eta,\xi]^{-1}$ for all $\eta \in G$.

(ii) We now merely assume $[\eta, \xi, \xi] = 1$ for all ξ, η in G, so that every element of G commutes with all its conjugates in G. Then we have ① $1 = [\xi\xi^{-1}, \eta] = [\xi, \eta]^{\xi^{-1}}[\xi^{-1}, \eta]$ and so $[\xi^{-1}, \eta] = [\xi, \eta]^{-1}$ since ξ^{-1} commutes with $[\xi, \eta]$. Here and repeatedly we shall use 7·1 (i) and (ii). If ζ is a third element of G, we have $1 = [\xi, \eta\zeta, \eta\zeta] = [[\xi,\zeta][\xi,\eta]^\zeta, \eta\zeta]$
$= [\xi, \zeta, \eta\zeta][[\xi,\eta]^\zeta, \eta\zeta]$ since $[\xi,\eta]^\zeta$ and $[\xi,\zeta]$ both lie in $X = \{\xi^G\}$ and therefore commute. $[\xi, \zeta, \eta\zeta] = [\xi, \zeta, \eta]$ since $[\xi,\zeta,\zeta] = 1$ and ζ commutes with the element $[\xi,\zeta,\eta] \in Z = \{\zeta^G\}$. Similarly η commutes with the element $[\xi,\eta]^\zeta \in Y = \{\eta^G\}$ and so $[[\xi,\eta]^\zeta, \eta\zeta] = [[\xi,\eta]^\zeta, \zeta] = [\xi, \eta, \zeta]$. Thus we obtain $[\xi, \zeta, \eta] = [\xi, \eta, \zeta]^{-1}$. ② Since $[\eta, \xi^{-1}] = [\xi^{-1}, \eta]^{-1} = [\xi, \eta]$ by ①, we have $[\xi, \eta^{-1}, \zeta]^\eta = [\xi, \eta^{-1}, \zeta] = [\eta, \xi, \zeta]$ and 7·7 (i) gives the relation
$[\eta, \xi, \zeta][\zeta, \eta, \xi][\xi, \zeta, \eta] = 1$ ——— ③
① and ② together show that $[\xi, \zeta, \eta]$ changes into its inverse when any two of ξ, η, ζ are interchange. Hence it is unaltered by a cyclic permutation of ξ, η, ζ and this gives $[\xi, \zeta, \eta]^3 = 1$ ——— ④ from ③

Finally, if τ is yet another element of G, we obtain
$\theta = [\xi, \eta, \zeta, \tau] = [\zeta, \tau, [\xi, \eta]]$ by cyclic permutation, $= [\xi, \eta, [\zeta, \tau]]^{-1}$
~~assumarots~~ But by ① and ②, θ changes to its inverse for any odd permutation of its four arguments. Hence $\theta = [\zeta, \tau, \xi, \eta] = [\xi, \eta, [\zeta, \tau]] = \theta^{-1}$.
So we have $\theta^2 = 1$. By ④, $\theta^3 = 1$. Hence $\theta = 1$. This is true for all ξ, η, ζ, τ of G and so $\gamma_4 G = 1$ by 7.5(i). Thus G is nilpotent of class at most 3. By 7.5(i) again, the Abelian group $\gamma_3 G$ is generated by elements $[\xi, \eta, \zeta]$ of order 1 or 3, so $\gamma_3 G$ is of exponent 3.

<u>Corollary 14.23</u> If $p \neq 3$, any p-group G in which $\{\xi^G\}$ is Abelian for all $\xi \in G$ is of class at most 2.

Note that in 14.2, the assumption that G is finite is irrelevant. It is clear that in any nilpotent group G of class 2, every element ξ commutes with all its conjugates. For $G' \leq \mathfrak{z}G$ and $\{\xi, G'\} \lhd G$.

<u>Lemma 14.24</u> Let G be a p-group of class 2 and let p be odd. Then the elements $\theta \in G$ such that $\theta^{p^n} = 1$ from a subgroup $\Omega_n G$, just as in an Abelian p-group.

Proof: let $\xi, \eta \in G$ and let $\zeta = [\xi, \eta]$. Then $\zeta \in G' \leq \mathfrak{z}G$ and so $\eta^{-r} \xi \eta^r = \xi \zeta^r$ for all $r = 1, 2, \ldots$ by induction on r. Now in any group we have the identity

$$(\eta\xi)^r = \eta^r \xi^{\eta^{r-1}} \xi^{\eta^{r-2}} \cdots \xi^{\eta} \xi .$$

In our case, this gives $(\eta\xi)^r = \eta^r \xi^r \zeta^{\binom{r}{2}}$ since ξ commutes with ζ.
Suppose that $\xi^{p^n} = \eta^{p^n} = 1$ and take $r = p^n$. Then $\zeta^{p^n} = [\xi, \eta^{p^n}] = 1$; and if $p \neq 2$, $\frac{1}{2}p^n(p^n - 1)$ is a multiple of p^n. Hence $(\eta\xi)^{p^n} = \eta^{p^n} \xi^{p^n} \zeta^{\frac{1}{2}p^n(p^n-1)} = 1$.

~~As a corollary of this we have~~

~~Lemma 14.25 If p is odd, a p-group G with only one subgroup of order p must be cyclic.~~

(C) We shall now consider the structure of a non-Abelian p-group G which has a cyclic subgroup of index p. By 7·2 (iv), $|G| = p^n$ with $n > 2$.

<u>Lemma 14·31</u> Let $C = \{\xi\}$ be a cyclic group of order p^n, $n \geq 2$.
(i) If $p = 2$, $n = 2$, then $A = \text{Aut}\, C$ is of order 2 and is generated by the automorphism $\beta : \xi \to \xi^{-1}$.
(ii) If $p = 2$, $n > 2$, then A is an Abelian 2-group of type $(n-2, 1)$ with a basis α, β defined by

$$\alpha : \xi \to \xi^5 \quad \text{and} \quad \beta : \xi \to \xi^{-1}.$$

(iii) If p is odd, the Sylow p-subgroup of the Abelian group A is generated by the automorphism $\alpha : \xi \to \xi^{1+p}$ and has order p^{n-1}.

Proof: (i) is clear.

(ii) $5^{2^m} \equiv 1 \bmod 2^{m+2}$ but $\not\equiv 1 \bmod 2^{m+3}$. Hence α has order 2^{n-2}. Obviously $\beta \notin \{\alpha\}$. Hence $A = \{\alpha, \beta\}$ with basis α, β, since $|A| = \varphi(2^n) = 2^{n-1}$.

(iii) Here $|A| = \varphi(p^n) = p^{n-1}(p-1)$ and $(1+p)^{p^m} \equiv 1 \bmod p^{m+1}$ but $\not\equiv 1 \bmod p^{m+2}$. Hence α generates the Sylow p-subgroup of A.

<u>Corollary 14·32</u> If $C = \{\xi\}$ has order 2^n, $n > 2$, then C has exactly three involutory automorphisms viz.

$$\alpha^{2^{n-3}} : \xi \to \xi^{1+2^{n-1}} \; ; \quad \beta : \xi \to \xi^{-1} \; ; \text{ and } \alpha\beta : \xi \to \xi^{-1+2^{n-1}}.$$

We can now prove

<u>Theorem 14·3</u> Let G be a group of order p^n with a cyclic subgroup $H = \{\xi\}$ of index p. Suppose that $n > 2$ and that G is not Abelian.
(i) If p is odd, G is determined to within isomorphism and $G = \{H, \eta\}$ where $\eta^p = 1$ and $\eta^{-1}\xi\eta = \xi^{1+p^{n-2}}$. G is of class 2 and $\Omega_1 G = \{\xi^{p^{n-2}}, \eta\}$ is of order p^2.
(ii) If $p = 2$ and $n = 3$, there are to within isomorphism two distinct types of group $G = \{H, \eta\}$: the <u>octic group</u> O is determined by the equations $\eta^2 = 1$, $\eta^{-1}\xi\eta = \xi^{-1}$; the <u>quaternion group</u> Q by $\eta^2 = \xi^2$, $\eta^{-1}\xi\eta = \xi^{-1}$. H is a characteristic subgroup of O and the remaining two subgroups of order 4 in O are elementary. In Q, every element ~~of~~ not in $Q' = \mathfrak{z}Q$ has

order 4.

(iii) $\mathrm{Aut}\, O \cong O$; $\mathrm{Aut}\, Q \cong \Sigma_4$. The automorphisms

$$\alpha : \xi \to \eta \to \xi\eta \quad \text{and} \quad \beta : \xi \leftrightarrow \eta^{-1}$$

of Q generate a group isomorphic with Σ_3. The split extension $\{Q, \alpha, \beta\}$ of order 48 is called the <u>binary-octahedral group</u> ; $\{Q, \alpha\}$ of order 24 is the <u>binary-tetrahedral group</u>.

(iv) If $p = 2$ and $n > 3$, then G is of class either 2 or $n-1$. In the former case, $G = \{\xi, \eta\}$ is determined to within isomorphism by the relations $\eta^2 = 1$, $\eta^{-1}\xi\eta = \xi^{1+2^{n-2}}$. G has exactly three involutions, forming with 1 the characteristic subgroup $\{\xi^{2^{n-2}}, \eta\}$.

(v) If $p = 2$, $n > 3$ and G has class $n-1$, then there are three distinct types of group G to within isomorphism, ~~[illegible]~~ which will be denoted by O_{2^n}, P_{2^n} and Q_{2^n}. We have $G = \{\xi, \eta\}$ where

$\eta^2 = 1$, $\eta^{-1}\xi\eta = \xi^{-1}$ in the <u>dihedral group</u> O_{2^n}

$\eta^2 = 1$, $\eta^{-1}\xi\eta = \xi^{-1+2^{n-2}}$ in the <u>intermediate group</u> P_{2^n}

$\eta^2 = \xi^{2^{n-2}}$, $\eta^{-1}\xi\eta = \xi^{-1}$ in the <u>generalized quaternion group</u> Q_{2^n}

Note that $O = O_8$, $Q = Q_8$. Besides the cyclic subgroup $H = \{\xi\}$, G has two other subgroups of index 2. In O_{2^n}, these are both of type $O_{2^{n-1}}$. In P_{2^n}, one is of type $O_{2^{n-1}}$ and the other of type $Q_{2^{n-1}}$. In Q_{2^n}, both are of type $Q_{2^{n-1}}$. G has centre $\{\xi^{2^{n-2}}\} = Z$ of order 2 and in all three groups, G/Z is of type $O_{2^{n-1}}$.