換位羣爲巡廻羣且屬於中核的 p 羣*

劉 聲 烈

（昆明師範學院）

在 p 羣 $\mathfrak{G}$ 的上中心羣列 (central series) $e=\mathfrak{d}_0\subset\mathfrak{d}_1=\mathfrak{z}\subset\mathfrak{d}_2\subset\cdots\subset\mathfrak{d}_c=\mathfrak{G}$ 中，因子羣 (factor group) $\mathfrak{d}_i/\mathfrak{d}_{i-1}$ 屬於因子羣 $\mathfrak{d}_{i+1}/\mathfrak{d}_{i-1}$ 的中核 (center). $\mathfrak{d}_{i+1}/\mathfrak{d}_i$ 爲可換羣，故相對換位羣 (relative commutator group) $(\mathfrak{d}_{i+1},\mathfrak{d}_{i+1})\subset\mathfrak{d}_i$. 因此因子羣 $\mathfrak{d}_{i+1}/\mathfrak{d}_{i-1}$ 的換位羣 $(\mathfrak{d}_{i+1},\mathfrak{d}_{i+1})/\mathfrak{d}_{i-1}$ 屬於 $\mathfrak{d}_i/\mathfrak{d}_{i-1}$，因之亦屬於其中核. 特別，$\mathfrak{d}_2$ 的換位羣屬於 $\mathfrak{d}_2$ 的中核. 本文擬對此種換位羣屬於中核的 p 羣 $\mathfrak{G}$ 作一研究，但僅限於 $\mathfrak{G}$ 的換位羣爲一巡廻羣的情款. 所得主要結果在定理 1 與定理 3 中.

所用符號採取 Hans Zassenhaus: Lebrbuch der Gruppentheorie 144 面所載的:

e $\mathfrak{G}$ 的主單位元 (unit element);

$\mathfrak{G}:e$ $\mathfrak{G}$ 的階 (order);

$\mathfrak{z}$ $\mathfrak{G}$ 的中核 (center);

$Z_{\mathfrak{t}}$ $\mathfrak{G}$ 中與 $\mathfrak{G}$ 的一部分集合 $\mathfrak{t}$ 的每一元素交換可能的一切元素所成的羣;

$\mathfrak{t}^x$ 一切 $x\mathfrak{t}x^{-1}$ 的集合，$\mathfrak{t}$ 爲 $\mathfrak{G}$ 之一部分集合，x 爲 $\mathfrak{G}$ 中任意元;

$D\mathfrak{G}$ $\mathfrak{G}$ 的換位羣 (commutator group);

$(a,b)=aba^{-1}b^{-1}$ $\mathfrak{G}$ 中元素 a 與 b 的換位元素 (commutator).

以下均假定 $\mathfrak{G}$ 爲 p 羣，$\mathfrak{G}:e=p^r$，$\mathfrak{G}$ 的換位羣 $D\mathfrak{G}$ 屬於 $\mathfrak{G}$ 的中核 $\mathfrak{z}$，$D\mathfrak{G}$ 爲巡廻羣: $D\mathfrak{G}=(t)$，t 爲 $D\mathfrak{G}$ 的一生成元，其巡廻率爲 p^m，$D\mathfrak{G}:e=p^m$.

一、 換位元素的運算

若 $D\mathfrak{G}\subset\mathfrak{z}$，則對 $\mathfrak{G}$ 中任意元素 $a,b,c,\cdots$，換位元素 (a,b) 的計算符合下列簡單規則.

* 1952 年 2 月 27 日收到

(1.1)　$a\,b\,a^{-1}=b^a=(a\,b\,a^{-1}\,b^{-1})\,b=(a,b)\,b=b\,(a,b)$.

(1.2)　$(a,b)=(b,a)^{-1}$.

(1.3)　$(a\,b,c)=(a,c)\,(b,c)$.

證：　$(a\,b,c)=a\,b\,c\,(a\,b)^{-1}\,c^{-1}=a\,b\,c\,b^{-1}\,a^{-1}\,c^{-1}$

$=a\,c^b\,a^{-1}\,c^{-1}=a\,c\,(b,c)\,a^{-1}\,c^{-1}$　　按 (1.1).

$=a\,c\,a^{-1}\,(b,c)\,c^{-1}$

$=c\,(a,c)\,(b,c)\,c^{-1}=(a,c)\,(b,c)$.

(1.4)　$(a_1\,a_2\cdots a_m,\ b_1\,b_2\cdots b_n)=\prod_{i=1}^{m}\prod_{j=1}^{n}(a_i,b_j)$,

a_i　$(i=1,2,\cdots,m)$,　　b_j　$(j=1,2,\cdots,n)$ 均爲 G 中任意元素.

(1.5)　$(a^m,b^n)=(a^m,b)^n=(a,b^n)^m=(a,b)^{mn}$.

(1.6)　$a^x\,b^y=b^y\,a^x\,(a,b)^{xy}$

證：　按　(1.5), $(a^x,b^y)=(a,b)^{xy}$,　所以　$a^x\,b^y\,a^{-x}\,b^{-y}=(a,b)^{xy}$,

所以 $a^x\,b^y=b^y\,a^x\,(a,b)^{xy}=(a,b)^{xy}\,b^y\,a^x$.

(1.7)　$(a^x\,b^y)^n=(a,b)^{xy\frac{n(n-1)}{2}}\,a^{nx}\,b^{ny}$.

證：　$(a^x\,b^y)^n=(a,b)^{xy}\,a^{2x}\,b^{2y}\,(a^x\,b^y)^{n-2}=(a,b)^{xy+2xy}\,a^{3x}\,b^{3y}\,(a^x\,b^y)^{n-3}$

$=\cdots=(a,b)^{xy(1+2+\cdots+n-1)}\,a^{nx}\,b^{ny}$

$=(a,b)^{xy\frac{n(n-1)}{2}}\,a^{nx}\,b^{ny}$.

(1.8)　$(a^{-1},b)=(a,b^{-1})=(b,a)$

證：　$(a\,a^{-1},b)=(e,b)=e$,　又 $(a\,a^{-1},b)=(a,b)\,(a^{-1},b)$, 所以 $(a,b)\,(a^{-1},b)=e$,

所以 $(a^{-1},b)=(a,b)^{-1}=(b,a)$.

(1.9)　$(a,b)=e$ 則 $a\,\varepsilon\,Z_b$,　$b\,\varepsilon\,Z_a$.

(1.10)　$(b,a)=(c,a)$, 則 $(b\,c^{-1},a)=e$, 於是 $b\,c^{-1}\,\varepsilon\,Z_a$.

證：　$(b\,c^{-1},a)=(b,a)\,(c^{-1},a)=(b,a)\,(c,a)^{-1}$　按 (1.3), (1.8).

$=(c,a)\,(c,a)^{-1}=e$.

二、 羣 $\mathfrak{G}$ 的構造

(2.1) 若 $D\mathfrak{G}=(t)$, t 的巡廻率爲 p^m. 則 $\mathfrak{G}$ 中必有一對元素 $g,\bar{g}$ 使 $(g,\bar{g})=t$. $D\mathfrak{G}=(t)$ 中的任一元素皆爲換位元素.

證: 令 x,y 跑過 $\mathfrak{G}$ 中所有元素, 而 $(x,y)=t^\sigma$, $0<\sigma\leqq p^m$. 若 σ 中有一 σ_0 與 p 互質, 而 $(x_0,y_0)=t^{\sigma_0}$; 則合同方程式 $\sigma_0 u\equiv 1 \pmod{p^m}$ 有整數解 $u=\alpha$, 於是 $(x_0^\alpha,y_0)=(x_0,y_0)^\alpha=t^{\sigma_0\alpha}=t$, 而定理得證. 否則若任一 σ 皆不與 p 互質, 則 σ 均有 cp^s 形, $1\leqq s<m$, c 爲與 p 互質的正整數. 所有換位元素 t^σ 均爲 t^{p^s} 的冪, 於是換位元素所生成的換位羣爲巡廻羣 (t) 的眞部分羣, 此與 $D\mathfrak{G}=(t)$ 的假設抵觸, 故 $\mathfrak{G}$ 中必有一對元素 $g,\bar{g}$ 使 $(g,\bar{g})=t$. 又按 (1.5), 對任意正整數 c, $(g^c,\bar{g})=(g,\bar{g})^c=t^c$, 故 $D\mathfrak{G}$ 中的任意一元素皆爲換位元素.

(2.2) 設 $(g,\bar{g})=t$, $Z_g,Z_{\bar{g}}$ 分別爲 $\mathfrak{G}$ 中 $g,\bar{g}$ 的交換可能羣, 則 $\mathfrak{G}=(g)\cdot Z_{\bar{g}}=(\bar{g})\cdot Z_g$.

證: 設 s 爲 $\mathfrak{G}$ 中任意元, $(s,\bar{g})=t^\sigma$, $sgs^{-1}=gt^\sigma$, 所以 $\bar{g}$ 的共軛元 (conjugate) 皆爲 gt^σ 形. 因 $(g,\bar{g})=t$, $g^i\bar{g}g^{-i}=\bar{g}t^i$, $(i=1,2,\cdots,p^m)$ 故 $\bar{g}$ 所屬的共軛類 (conjugate set) 爲 $\bar{g}t,\bar{g}t^2,\cdots,\bar{g}t^{p^m}=\bar{g}$. 因 $(\mathfrak{G}:e/Z_g:e)=\bar{g}$ 所屬的共軛類中元素數 $=p^m$, 所以 $\mathfrak{G}:e=(Z_{\bar{g}}:e)p^m$. 當 $\alpha\neq\beta$, $0<\beta<\alpha\leqq p^m$, 則傍系 (co-set) $g^\alpha Z_{\bar{g}}$ 與傍系 $g^\beta Z_{\bar{g}}$ 無共同元; 否則 $g^{\alpha-\beta}\subset Z_{\bar{g}}$, 於是 $(g^{\alpha-\beta},\bar{g})=(g,\bar{g})^{\alpha-\beta}=t^{\alpha-\beta}=e$, 但 $0<\beta<\alpha\leqq p^m$, 此爲不可能. 故 p^m 個傍系 $g^iZ_{\bar{g}}$ $(i=1,2,\cdots,p^m)$ 的元素皆互異, 而此 p^m 個傍系共有 $p^m(Z_g:e)=\mathfrak{G}:e$ 個元素. 因此 $\mathfrak{G}=Z_{\bar{g}}+gZ_{\bar{g}}+\cdots+g^{p^m-1}Z_{\bar{g}}$, 即 $\mathfrak{G}=(g)\cdot Z_{\bar{g}}$. 又 $(\bar{g},g)=(g,\bar{g})^{-1}=t^{-1}$, 按 (1.5) $(\bar{g},g)^i=(\bar{g}^i,g)$, 所以 $\bar{g}^igg^{-i}=gt^{-i}$ $(i=1,2,\cdots,p^m)$, 所以 g 所屬的共軛類爲 $gt,gt^2,\cdots,gt^{p^m}=g$. 同樣的理由我們可以證明 $\mathfrak{G}=(\bar{g})\cdot Z_g$.

(2.3) 若 $(g,\bar{g})=t$, 則 $Z_{\bar{g}}=(\bar{g})\cdot(Z_g\cap Z_{\bar{g}})$, $Z_g=(g)\cdot(Z_g\cap Z_{\bar{g}})$.

證: 羣 $(\bar{g})$ 的任意元與羣 $Z_{\bar{g}}$ 的任意元皆交換可能, 因之與羣 $Z_g\cap Z_{\bar{g}}$ 的任意元皆交換可能, 故 $(\bar{g})\cdot(Z_g\cap Z_{\bar{g}})$ 爲一羣 $\mathfrak{J}$. 若 $Z_{\bar{g}}\neq\mathfrak{J}$, 則 $\mathfrak{G}$ 中有一元 $s\in Z_{\bar{g}}$, 而 $s\notin\mathfrak{J}$. 因 $s\in Z_{\bar{g}}$, 故 $(s,\bar{g})=e$. 又 $(s,g)\neq e$; 否則 $(s,g)=e$, $(s,\bar{g})=e$, 於是 $s\in Z_g\cap Z_{\bar{g}}$. 於是 $s\in(\bar{g})\cdot(Z_g\cap Z_g)=\mathfrak{J}$ 而與 $s\notin\mathfrak{J}$ 的假設抵觸了. 令

$(s,g)=t^{\lambda}$, $0<\lambda<p^m$, 因 $(\bar{g},g)=t^{-1}$, 按 (1.3),(1.5), $(\bar{g}^{\lambda}s,g)=(\bar{g}^{\lambda},g)(s,g)$ $=(\bar{g},g)^{\lambda}(s,g)=t^{-\lambda}\cdot t^{\lambda}=e$, 於是 $\bar{g}^{\lambda}s\varepsilon Z_{\bar{g}}$. 因 $s\varepsilon Z_{\bar{g}}$, 故 $\bar{g}^{\lambda}s\varepsilon Z_{\bar{g}}$, 故 $\bar{g}^{\lambda}s\varepsilon Z_g\cap Z_{\bar{g}}$, 故 $s\varepsilon(\bar{g})\cdot(Z_g\cap Z_{\bar{g}})=\mathfrak{H}$. 此與 $s\notin\mathfrak{H}$ 的假設矛盾, 故 $Z_{\bar{g}}=(\bar{g})\cdot(Z_g\cap Z_{\bar{g}})$. 同樣的理由可以證明 $Z_g=(g)\cdot(Z_g\cap Z_{\bar{g}})$.

(2.4) 設 $(g,\bar{g})=t$, 命 $g=g_1$, $\bar{g}=\bar{g}_1$. 由 $g_1,\bar{g}_1,\mathfrak{H}$ 生成一羣 $\mathfrak{G}_1=(g_1,\bar{g}_1,\mathfrak{H})$, $Z_{\mathfrak{G}_1}$ 爲 $\mathfrak{G}$ 中與 $\mathfrak{G}_1$ 的每元交換可能的元素所成的羣, 則 $\mathfrak{G}=\mathfrak{G}_1\cdot Z_{\mathfrak{G}_1}=Z_{\mathfrak{G}_1}\cdot\mathfrak{G}_1$, $\mathfrak{G}_1\cap Z_{\mathfrak{G}_1}=\mathfrak{H}$.

證: 按 (2.2) (2.3) $\mathfrak{G}=(g_1)\cdot Z_{\bar{g}_1}=(g_1)\cdot(\bar{g}_1)\cdot(Z_{g_1}\cap Z_{\bar{g}_1})$. 顯然 $Z_{g_1}\cap Z_{\bar{g}_1}$ $=Z_{(g_1,\bar{g}_1)}=Z_{(g_1,\bar{g}_1,\mathfrak{H})}=Z_{\mathfrak{G}_1}$. 所以 $\mathfrak{G}=\mathfrak{G}_1\cdot Z_{\mathfrak{G}_1}$. 若 $s\varepsilon\mathfrak{G}_1\cap Z_{\mathfrak{G}_1}$, 因 $s\varepsilon Z_{\mathfrak{G}_1}$ 故 s 與 $\mathfrak{G}_1$ 的每元交換, 因 $s\varepsilon\mathfrak{G}_1$ 故 s 與 $Z_{\mathfrak{G}_1}$ 的每元交換; 因此 s 與 $\mathfrak{G}=\mathfrak{G}_1\cdot Z_{\mathfrak{G}_1}$ 的每元交換, 於是 $s\varepsilon\mathfrak{H}$. 另一方面 $\mathfrak{H}\subset\mathfrak{G}_1$, $\mathfrak{H}\subset Z_{\mathfrak{G}_1}$, 所以 $\mathfrak{H}\subset\mathfrak{G}_1\cap Z_{\mathfrak{G}_1}$. 所以 $\mathfrak{G}_1\cap Z_{\mathfrak{G}_1}=\mathfrak{H}$.

(2.5) 設 $D\mathfrak{G}=(t)\subset\mathfrak{H}$, t 的巡廻率爲 p^m, $(g_1,\bar{g}_1)=t$, 由 $g_1,\bar{g}_1,\mathfrak{H}$ 生成一羣 $\mathfrak{G}_1=(g_1,\bar{g}_1,\mathfrak{H})$, 則 g_1 及 $\bar{g}_1$ 關於 $\mathfrak{H}$ 的相對巡廻率均爲 p^m, $\mathfrak{G}_1/\mathfrak{H}$ 爲 (p^m,p^m) 型可換羣.

證: 設 g_1 關於 $\mathfrak{H}$ 的相對巡廻率爲 d, 因 $g_1^d\varepsilon\mathfrak{H}$, $(g_1^d,\bar{g}_1)=(g_1,\bar{g}_1)^d=t^d=e$, 所以 $d\equiv 0\,(\mathrm{mod}\,p^m)$. 另一方面 $(g_1^{p^m},\bar{g}_1)=t^{p^m}=e$, 按 (1.9) $g_1^{p^m}\varepsilon Z_{\bar{g}_1}$, 所以 $g_1^{p^m}\varepsilon Z_{g_1}\cap Z_{\bar{g}_1}=Z_{\mathfrak{G}_1}$, 按 (2.4) $g_1^{p^m}\varepsilon\mathfrak{G}_1\cap Z_{\mathfrak{G}_1}=\mathfrak{H}$, 所以 $p^m\equiv 0\,(\mathrm{mod}\,d)$. 所以 $d=p^m$. 同樣可證 $\bar{g}$ 關於 $\mathfrak{H}$ 的相對巡廻率亦爲 p^m. 所以 $\mathfrak{G}_1/\mathfrak{H}$ 爲 (p^m,p^m) 型可換羣.

設 $DZ_{\mathfrak{G}_1}$ 爲 $Z_{\mathfrak{G}_1}$ 的換位羣. 若 $DZ_{\mathfrak{G}_1}=e$, 則 $\mathfrak{G}=\mathfrak{G}_1$; 因若 $s\varepsilon Z_{\mathfrak{G}_1}$, 則 s 與 $Z_{\mathfrak{G}_1}$ 的每元交換, s 又與 $\mathfrak{G}_1$ 的每元交換, 於是 $s\varepsilon\mathfrak{H}$, 於是 $Z_{\mathfrak{G}_1}\subset\mathfrak{H}$, 又 $\mathfrak{H}\subset Z_{\mathfrak{G}_1}$, 所以 $Z_{\mathfrak{G}_1}=\mathfrak{H}$; 於是 $\mathfrak{G}=\mathfrak{G}_1\cdot Z_{\mathfrak{G}_1}=\mathfrak{G}_1\cdot\mathfrak{H}=\mathfrak{G}_1$. 若 $DZ_{\mathfrak{G}_1}\neq e$, 設 $DZ_{\mathfrak{G}_1}$ $=(t_2)\subset(t)\subset\mathfrak{H}$, $DZ_{\mathfrak{G}_1}:e=p^{m_2}$, $(0<m_2\leqq m)$, 則 $t_2^{p^{m_2}}=e$; 因 $t_2\varepsilon(t)$, 我們可選 t_2 令 $t_2=t^{p^{m-m_2}}$ 而使 $DZ_{\mathfrak{G}_1}=(t_2)$. 又 $Z_{\mathfrak{G}_1}$ 的中核等於 $\mathfrak{G}$ 的中核 $\mathfrak{H}$; 因若 s 屬於 $Z_{\mathfrak{G}_1}$ 的中核, 則 s 屬於 $\mathfrak{G}_1\cdot Z_{\mathfrak{G}_1}=\mathfrak{G}$ 的中核 $\mathfrak{H}$, 而 $\mathfrak{H}\subset Z_{\mathfrak{G}_1}$, 故 $Z_{\mathfrak{G}_1}$ 的中核等於 $\mathfrak{G}$ 的中核 $\mathfrak{H}$. 命 $t=t_1$, $m=m_1$. 當 $DZ_{\mathfrak{G}_1}\neq e$, 因 $DZ_{\mathfrak{G}_1}=(t_2)\subset\mathfrak{H}$,

$t_2 = t_1^{p^{m-m_2}}$, t_2 的巡廻率爲 p^{m_2}, 又 $D/Z_{\mathfrak{G}_1}$ 的中核等於 $\mathfrak{z}$, 故按 (2.4) 如同 $\mathfrak{G} = \mathfrak{G}_1 \cdot Z_{\mathfrak{G}_1}$ 的分解同樣可得 $Z_{\mathfrak{G}_1}$ 的一分解: $Z_{\mathfrak{G}_1} = \mathfrak{G}_2 \cdot Z_{(\mathfrak{G}_1,\mathfrak{G}_2)}$; $\mathfrak{G}_2 = (g_2, \bar{g}_2, \mathfrak{z})$, $(g_2, g_2) = t_2$, $\mathfrak{G}_2 \cap Z_{(\mathfrak{G}_1,\mathfrak{G}_2)} = \mathfrak{z}$. 如此繼續下去, 終之得將 $\mathfrak{G}$ 分解爲若干部分羣的乘積: $\mathfrak{G} = \mathfrak{G}_1 \cdot \mathfrak{G}_2 \cdots \mathfrak{G}_r$; $\mathfrak{G}_i = (g_i, \bar{g}_i, \mathfrak{z})$, $(g_i, \bar{g}_i) = t_i = t_1^{p^{m-m_i}}$, $m = m_1 \geqq m_2 \geqq \cdots \geqq m_r$, $i = 1, 2, \cdots, r$. 當 $i \neq j$, $\mathfrak{G}_i$ 的任意元與 $\mathfrak{G}_j$ 的任意元交換可能, 且 $\mathfrak{G}_i \cap \mathfrak{G}_j = \mathfrak{z}$. 綜上所述, 遂得

定理 1: 若 p 羣 $\mathfrak{G}$ 的換位羣 $D\mathfrak{G}$ 爲一巡廻羣且屬於 $\mathfrak{G}$ 的中核 $\mathfrak{z} : D\mathfrak{G} = (t) \subset \mathfrak{z}$, $D\mathfrak{G} : e = p^m$, 則 $\mathfrak{G}$ 可分解爲部分羣的乘積: $\mathfrak{G} = \mathfrak{G}_1 \cdot \mathfrak{G}_2 \cdots \mathfrak{G}_r$; 當 $i \neq j$, $\mathfrak{G}_i$ 的每元與 $\mathfrak{G}_j$ 的每元交換可能, 且 $\mathfrak{G}_i \cap \mathfrak{G}_j = \mathfrak{z}$. 命 $t = t_1$, $m = m_1$. $\mathfrak{G}_i$ 乃如是定義的羣:

$\mathfrak{G}_i = (g_i, \bar{g}_i, \mathfrak{z})$, $(g_i, \bar{g}_i) = t_i = t^{p^{m-m_i}}$, $m = m_1 \geqq m_2 \geqq \cdots \geqq m_r$, $(i = 1, 2, \cdots, r)$. $\mathfrak{G}_i$ 的換位羣 $D\mathfrak{G}_i = (t_i)$, $D\mathfrak{G}_i : e = p^{m_i}$ $(i = 1, 2, \cdots, r)$. g_i 及 $\bar{g}_i$ 關於 $\mathfrak{z}$ 的相對巡廻率均爲 p^{m_i}. $\mathfrak{G}_i$ 的中核等於 $\mathfrak{G}$ 的中核. 因子羣 $\mathfrak{G}/\mathfrak{z} = \mathfrak{H}$ 乃 $(p^{m_1}, p^{m_1}, \cdots, p^{m_r}, p^{m_r})$ 型可換羣. $\mathfrak{H} : e = p^{2r}$, $r = m_1 + m_2 + \cdots + m_r$, $\mathfrak{H}$ 之階爲 p 的偶數冪.

因 $\mathfrak{G}/\mathfrak{z} = \mathfrak{H}$ 爲 $(p^{m_1}, p^{m_1}, p^{m_2}, p^{m_2}, \cdots, p^{m_r}, p^{m_r})$ 型可換羣, 所以 $m = m_1 \geqq m_2 \geqq \cdots \geqq m_r$ 乃屬於 $\mathfrak{G}$ 的一組不變系. 又 $\mathfrak{G}_1 \cdots \mathfrak{G}_{i-1} \cdot \mathfrak{G}_{i+1} \cdots \mathfrak{G}_r \subset Z_{\mathfrak{G}_i}$, 所以 $\mathfrak{G} = \mathfrak{G}_i \cdot Z_{\mathfrak{G}_i}$, $(i = 1, 2, \cdots, r)$. 且 $\mathfrak{G}_i \cap Z_{\mathfrak{G}_i} = \mathfrak{z}$; 因若 $s \in \mathfrak{G}_i \cap Z_{\mathfrak{G}_i}$, 則 s 與 $\mathfrak{G}_i$ 的每元又與 $Z_{\mathfrak{G}_i}$ 的每元交換可能, 故 $s \in \mathfrak{z}$, 故 $\mathfrak{G}_i \cap Z_{\mathfrak{G}_i} \subset \mathfrak{z}$, 而 $\mathfrak{z} \subset \mathfrak{G}_i$, $\mathfrak{z} \subset Z_{\mathfrak{G}_i}$, 故 $\mathfrak{G}_i \cap Z_{\mathfrak{G}_i} = \mathfrak{z}$.

如定理 1 中所述之 $\mathfrak{G}$ 的一組生成元 $g_1, \bar{g}_1, g_2, \bar{g}_2, \cdots, g_r \cdot \bar{g}_r$ 稱爲羣 $\mathfrak{G}$ 的一組底. 其特徵爲 $(g_i, \bar{g}_i) = t_i = t_1^{p^{m-m_i}}$, $m = m_1 \geqq m_2 \geqq \cdots \geqq m_r$, $(i = 1, 2, \cdots, r)$; 當 $i \neq j$, $(g_i, g_j) = (g_i, \bar{g}_j) = (\bar{g}_i, g_j) = (\bar{g}_i, \bar{g}_j) = e$, g_i 及 $\bar{g}_i$ 關於 $\mathfrak{z}$ 的相對巡廻率均爲 p^{m_i}.

(2.6) 在定理 1 中所述的 $\mathfrak{G}_i = (g_i, \bar{g}_i, \mathfrak{z})$, 其元素可一意表爲 $g_i^x \bar{g}_i^y \mathfrak{z}$ $(0 \leqq x < p^{m_i}, 0 \leqq y < p^{m_i}, z \in \mathfrak{z})$.

證: 因 g_i 及 $\bar{g}_i$ 關於 $\mathfrak{z}$ 的相對巡廻率均爲 p^{m_i}, 故 $\mathfrak{G}_i = (g_i, \bar{g}_i, \mathfrak{z})$ 中的元素恆可表爲 $g^x \bar{g}_i^y \mathfrak{z}$ 形 $(0 \leqq x < p^{m_i}, 0 \leqq y < p^{m_i}, z \in \mathfrak{z})$. 今證此表示爲一意

的. 設 $g_i^x = \bar{g}_i^y \mathfrak{z}, (0 \leqq x < p^{mi}, 0 \leqq y < p^{mi}, z \varepsilon \mathfrak{z})$, 則 $(g_i^x, \bar{g}_i) = (\bar{g}_i^y \mathfrak{z}, \bar{g}_i) = e$, 又 $(g_i^x, \bar{g}_i) = i_i^x$, 所以 $i_i^x = e$, 所以 $x \equiv 0 \pmod{p^{mi}}$, 但 $0 \leqq x < p^{mi}$, 所以 $x = 0$; 於是 $\bar{g}_i^y z = g_i^x = e$, $\bar{g}_i^y = z^{-1} \varepsilon \mathfrak{z}$. 按定理 1, $\bar{g}_i$ 關於 $\mathfrak{z}$ 的相對巡廻率爲 p^{mi}, 所以 $y \equiv 0 \pmod{p^{mi}}$; 但 $0 \leqq y < p^{mi}$, 所以 $y = 0, z = e$. 若 $g_i^a \bar{g}_i^b z = g_i^{a'} \bar{g}_i^{b'} z'$ $(0 \leqq a < p^{mi}, 0 \leqq b < p^{mi}, 0 \leqq a' < p^{mi}, 0 \leqq b' < p^{mi}, z \varepsilon \mathfrak{z}, z' \varepsilon \mathfrak{z})$, 則 $g_i^{a-a'} = g_i^{b'-b} z' z^{-1}$, 於是 $a - a' = 0, b' - b = 0$. 於是 $a = a', b = b', z = z'$.

定理 2　如定理 1 中所假設, 若 $g_1, \bar{g}_1, \cdots, g_r, \bar{g}_r$ 爲羣 $\mathfrak{G}$ 的一組底, 則 $\mathfrak{G}$ 的元素可一意表爲

$$g_1^x \bar{g}_1^y \cdots g_r^x \bar{g}_r^y z \qquad (0 \leqq x_i < p^{mi}, 0 \leqq y_i < p^{mi}, i = 1, 2, \cdots, r, z \varepsilon \mathfrak{z})$$

證[1]: 設 $s_1 s_2 \cdots s_r z \varepsilon \mathfrak{z}$, 而 $s_i \varepsilon \mathfrak{G}_i, (i = 1, 2, \cdots, r), z \varepsilon \mathfrak{z}$, 則 $s_i \varepsilon \mathfrak{z} (i = 1, 2, \cdots, r)$. 因 $s_i^{-1} = s_1 s_2 \cdots s_{i-1} s_{i+1} \cdots s_r z \varepsilon Z_{\mathfrak{G}_i}$, 又 $s_i^{-1} \varepsilon \mathfrak{G}_i$, 於是 $s_i^{-1} \varepsilon \mathfrak{G}_i \cap Z_{\mathfrak{G}_i} = \mathfrak{z}$, 於是 $s_i \varepsilon \mathfrak{z}$. 設

$$g_1^{a_1} \bar{g}_1^{b_1} \cdots \bar{g}_r^{a_r} \bar{g}_r^{b_r} z = g_1^{c_1} \bar{g}_1^{d_1} \cdots g_r^{c_r} \bar{g}_r^{d_r} z' \qquad (0 \leqq a_i < p^{mi}, 0 \leqq b_i < p^{mi},$$

$0 \leqq c_i < p^{mi}, 0 \leqq d_i < p^{mi}, i = 1, 2, \cdots, r, z \varepsilon \mathfrak{z}, z' \varepsilon \mathfrak{z})$, 則

$$(g_1^{a_1} \bar{g}_1^{b_1}) (g_1^{c_1} \bar{g}_1^{d_1})^{-1} \cdots (g_r^{a_r} \bar{g}_r^{b_r}) (g_r^{c_r} \bar{g}_r^{d_r})^{-1} = z^{-1} z' \varepsilon \mathfrak{z}$$

於是 $(g_i^{a_i} \bar{g}_i^{b_i}) (g_i^{c_i} \bar{g}_i^{d_i})^{-1} \varepsilon \mathfrak{z}$ $(i = 1, 2, \cdots, r)$, 按 $(2 \cdot 6)$, 於是得 $a_i = c_i$, $b_i = d_i$ $(i = 1, 2, \cdots, r)$, $z = z'$.

三、底 的 變 換

(3.1) 設 $\mathfrak{M}_2$ 爲一切 2 行 2 列方陣的集合, 方陣的元素取自整數環, σ 爲 $\mathfrak{M}_2$ 中方陣間的一單值對應如下所定義的:

$$\sigma: \qquad A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \longrightarrow A^\sigma = \begin{pmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{pmatrix}$$

1) 本文審查者指出若應用阿倍爾羣基礎定理於因子羣 $\mathfrak{G}/\mathfrak{z}$, 則可推得定理 1,2 之一簡捷的證法.

則對 $\mathfrak{M}_2$ 中任意方陣 A, B, 有 i) $(A^\sigma)^\sigma = A$, ii) $(A \cdot B)^\sigma = B^\sigma \cdot A^\sigma$, iii) $(A+B)^\sigma = A^\sigma + B^\sigma$, iv) $A \cdot A^\sigma = \begin{pmatrix} |A| & 0 \\ 0 & |A| \end{pmatrix}$, $|A|$ 爲 A 的行列式.

證: 由簡單的計算易驗其爲眞.

(3.2) 設 $\mathfrak{M}_{2r}$ 爲所有 $2r$ 行 $2r$ 列方陣的集合, 方陣中的元素取自整數環. $\mathfrak{M}_{2r}$ 中方陣

$$X = \begin{pmatrix} a_{11} & b_{11} & \cdots & a_{1r} & b_{1r} \\ c_{11} & d_{11} & \cdots & c_{1r} & d_{1r} \\ \cdot & \cdot & \cdots & \cdot & \cdot \\ \cdot & \cdot & \cdots & \cdot & \cdot \\ a_{r1} & b_{r1} & \cdots & a_{rr} & b_{rr} \\ c_{r1} & d_{r1} & \cdots & c_{rr} & d_{rr} \end{pmatrix}$$

命 $\mathfrak{M}_2$ 中方陣

$$X_{ij} = \begin{pmatrix} a_{ij} & b_{ij} \\ c_{ij} & d_{ij} \end{pmatrix} \qquad i,j = 1,2,\cdots,r.$$

採用符號 $X = (X_{ij})$, $(X)_{ij} = X_{ij}$ $(i,j = 1,2,\cdots,r)$.

ϱ 與 τ 爲 $\mathfrak{M}_{2r}$ 中方陣間如下所定義的單值對應:

$$\varrho: \quad X = (X_{ij}) \longrightarrow X\varrho,\ (X\varrho)_{ij} = X^\sigma_{ij},\ \sigma \text{ 如 (3.1) 所定義.}$$

$$\tau: \quad X = (X_{ij}) \longrightarrow X^\tau,\ (X^\tau)_{ij} = X_{ji} \quad (i,j = 1,2,\cdots,r).$$

命 $\varrho\tau = \theta$, 則對 $\mathfrak{M}_{2r}$ 中任意方陣 X, Y 有

i) $(X\varrho)^\tau = (X^\tau)\varrho = X^\theta$, ii) $(X^\theta)^\theta = X$, iii) $(X^\theta)_{ij} = X^\sigma_{ji}$, σ 如 (3.1) 所定義. iv) $(X+Y)^\theta = X^\theta + Y^\theta$, v) $(XY)^\theta = Y^\theta X^\theta$.

證: i) ii) iii) iv) 由簡單的計算易驗其爲眞, 今證 v)

$$((XY)^\varrho)_{ij} = \Big(\sum_{k=1}^{r} X_{ik}Y_{kj}\Big)^\sigma = \sum_{k=1}^{r} Y^\sigma_{kj} X^\sigma_{ik} \qquad \text{按 (3.1) 的 ii) 及 iii).}$$

$$= \sum_{k=1}^{r} (Y^\varrho)_{kj}(X^\varrho)_{ik} = \sum_{k=1}^{r} (Y^{\varrho\tau})_{jk}(X^{\varrho\tau})_{ki} \qquad \text{按 } \tau \text{ 的定義.}$$

$$= (Y^{\varrho\tau}X^{\varrho\tau})_{ji}.$$

所以 $(X\ Y)^{\varrho^\tau} = Y^{\varrho^\tau} X^{\varrho^\tau}$，所以 $(X\ Y)^\theta = Y^\theta X^\theta$.

$\mathfrak{G}/\mathfrak{z} = \mathfrak{H}$ 爲 $(p^{m_1}, p^{m_1}, \cdots, p^{m_r}, p^{m_r})$ 型可換羣. 設 $g_1, \bar{g}_1, \cdots, g_r, \bar{g}_r$ 與 $h_1, \bar{h}_1, \cdots, h_r, \bar{h}_r$ 爲 $\mathfrak{G}$ 的兩組底，按定理 2，設

$$h_s = g_1^{a_{s1}} \bar{g}_1^{b_{s1}} \cdots g_r^{a_{sr}} \bar{g}_r^{b_{sr}} z_s,\ z_s \in \mathfrak{z}, \qquad 0 \leqq a_{si} < p^{m_i},\ 0 \leqq b_{si} < p^{m_i}, \quad (i, s = 1, 2, \cdots, r).$$

$$\bar{h}_s = g_1^{c_{s1}} \bar{g}_1^{d_{s1}} \cdots g_r^{c_{sr}} \bar{g}_r^{d_{sr}} \bar{z}_s,\ \bar{z}_s \in \mathfrak{z}, \qquad 0 \leqq c_{si} < p^{m_i},\ 0 \leqq d_{si} < p^{m_i}, \quad (i, s = 1, 2, \cdots, r).$$

(1)

$$g_s = h_1^{\alpha_{s1}} \bar{h}_1^{\beta_{s1}} \cdots h_r^{\alpha_{sr}} \bar{h}_r^{\beta_{sr}} z_s',\ z_s' \in \mathfrak{z}, \qquad 0 \leqq \alpha_{si} < p^{m_i},\ 0 \leqq \beta_{si} > p^{m_i}, \quad (i, s = 1, 2, \cdots, r).$$

$$\bar{g}_s = h_1^{\gamma_{s1}} \bar{h}_1^{\delta_{s1}} \cdots h_r^{\gamma_{sr}} \bar{h}_r^{\delta_{sr}} \bar{z}_s',\ \bar{z}_s' \in \mathfrak{z}, \qquad 0 \leqq \gamma_{si} < p^{m_i},\ 0 \leqq \delta_{si} < p^{m_i}, \quad (i, s = 1, 2, \cdots, r).$$

因 $\mathfrak{G}/\mathfrak{z} = \mathfrak{H}$ 是可換羣，將 $\mathfrak{H}$ 中元素的結合法寫爲加法，單位元素寫爲零，則關於 $\bmod \mathfrak{z}$，(1) 式可寫爲

$$h_s = a_{s1} g_1 + b_{s1} \bar{g}_1 + \cdots + a_{sr} g_r + b_{sr} \bar{g}_r. \pmod{\mathfrak{z}}.$$
$$0 \leqq a_{si} < p^{m_i},\ 0 \leqq b_{si} < p^{m_i},\ (s, i = 1, 2, \cdots, r)$$

$$\bar{h}_s = c_{s1} g_1 + d_{s1} \bar{g}_1 + \cdots + c_{sr} g_r + d_{sr} \bar{g}_r. \pmod{\mathfrak{z}}.$$
$$0 \leqq c_{si} < p^{m_i},\ 0 \leqq d_{si} < p^{m_i}\ (s, i = 1, 2, \cdots, r)$$

(2)

$$g_s = \alpha_{s1} h_1 + \beta_{s1} \bar{h}_1 + \cdots + \alpha_{sr} h_r + \beta_{sr} \bar{h}_r. \pmod{\mathfrak{z}}.$$
$$0 \leqq \alpha_{si} < p^{m_i},\ 0 \leqq \beta_{si} < p^{m_i}\ (s, i = 1, 2, \cdots, r)$$

$$\bar{g}_s = \gamma_{s1} h_1 + \delta_{s1} \bar{h}_1 + \cdots + \gamma_{sr} h_r + \delta_{sr} \bar{h}_r. \pmod{\mathfrak{z}}.$$
$$0 \leqq \gamma_{si} < p^{m_i},\ 0 \leqq \delta_{si} < p^{m_i}\ (s, i = 1, 2, \cdots, r)$$

用方陣寫法 (2) 式可寫爲

$$(3) \qquad \begin{pmatrix} h_1 \\ \bar{h}_1 \\ \cdot \\ \cdot \\ h_r \\ \bar{h}_r \end{pmatrix} = \begin{pmatrix} a_{11}\ b_{11} \cdots a_{1r}\ b_{1r} \\ c_{11}\ d_{11} \cdots c_{1r}\ d_{1r} \\ \cdot\ \cdot \cdots \cdot\ \cdot \\ \cdot\ \cdot \cdots \cdot\ \cdot \\ a_{r1}\ b_{r1} \cdots a_{rr}\ b_{rr} \\ c_{r1}\ d_{r1} \cdots c_{rr}\ d_{rr} \end{pmatrix} \begin{pmatrix} g_1 \\ \bar{g}_1 \\ \cdot \\ \cdot \\ g_r \\ \bar{g}_r \end{pmatrix} \pmod{\mathfrak{z}},$$

$$\begin{pmatrix} g_1 \\ \bar{g}_1 \\ \cdot \\ \cdot \\ g_r \\ \bar{g}_r \end{pmatrix} = \begin{pmatrix} \alpha_{11}\ \beta_{11} \cdots \alpha_{1r}\ \beta_{1r} \\ \gamma_{11}\ \delta_{11} \cdots \gamma_{1r}\ \delta_{1r} \\ \cdot\ \cdot \cdots \cdot\ \cdot \\ \cdot\ \cdot \cdots \cdot\ \cdot \\ \alpha_{r1}\ \beta_{r1} \cdots \alpha_{rr}\ \beta_{rr} \\ \gamma_{r1}\ \delta_{r1} \cdots \gamma_{rr}\ \delta_{rr} \end{pmatrix} \begin{pmatrix} h_1 \\ \bar{h}_1 \\ \cdot \\ \cdot \\ h_r \\ \bar{h}_r \end{pmatrix} \pmod{z}.$$

設 $\mathfrak{M}_{2r}$ 中方陣

$$T = (T_{ij}),\ T_{ij} = \begin{pmatrix} a_{ij} & b_{ij} \\ c_{ij} & d_{ij} \end{pmatrix}. \qquad H = (H_{ij}),\ H_{ij} = \begin{pmatrix} \alpha_{ij} & \beta_{ij} \\ \gamma_{ij} & \delta_{ij} \end{pmatrix}. \tag{4}$$

$$M = (M_{ij}),\ M_{ij} = \begin{pmatrix} p^{m_j} & p^{m_j} \\ p^{m_j} & p^{m_j} \end{pmatrix}. \tag{5}$$

$$P = (P_{ij}),\ \text{當 } i \neq j,\ P_{ij} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},\ P_{ii} = \begin{pmatrix} p^{m-m_i} & 0 \\ 0 & p^{m-m_i} \end{pmatrix}. \tag{6}$$

$$\bar{P} = (\bar{P}_{ij}),\ \text{當 } i \neq j,\ \bar{P}_{ij} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},\ \bar{P}_{ii} = \begin{pmatrix} p^{m_i} & 0 \\ 0 & p^{m_i} \end{pmatrix}. \tag{7}$$

由 (3) 式

$$\begin{pmatrix} h_1 \\ \bar{h}_1 \\ \cdot \\ \cdot \\ h_r \\ \bar{h}_r \end{pmatrix} \equiv T \begin{pmatrix} g_1 \\ \bar{g}_1 \\ \cdot \\ \cdot \\ g_r \\ \bar{g}_r \end{pmatrix} = TH \begin{pmatrix} h_1 \\ \bar{h}_1 \\ \cdot \\ \cdot \\ h_r \\ \bar{h}_r \end{pmatrix} \pmod{\mathfrak{z}}$$

因 h_i 及 $\bar{h}_i$ 關於 $\mathfrak{z}$ 的相對巡廻率爲 $p^{m_i}, (i = 1, 2, \cdots, r)$, 故有

$$TH \equiv HT \equiv E \pmod{M} \tag{8}$$

而 E 爲 $\mathfrak{M}_{2r}$ 中主方陣 (unit matrix). 於是 $THP \equiv HTP \equiv P \pmod{MP}$, 但 $MP \equiv O \pmod{p^m}$, O 爲 $\mathfrak{M}_{2r}$ 中的零方陣, 故有

$$THP \equiv HTP \equiv P \pmod{p^m}. \tag{9}$$

羣 $\mathfrak{G}$ 中兩組底間的變換可由 (3) 式中方陣 T 表示之, 今求得 T 的充分與必要條件如次:

定理 3　若 (5) 式中方陣 T 表示羣 $\mathfrak{G}$ 之兩組底間的變換，則其充分與必要條件爲

$$T P T^{\eta} \equiv P \pmod{p^m}$$

T, P 如 (4), (6) 所定義，$T \to T^{\eta}$ 如 (3.2) 所定義.

證： 應用底之性質，由 (1) 得

$$\begin{aligned}
&(h_i, g_j) = (h_i, \bar{h}_i^{\beta_{ji}}) = t^{p^{m-m_i}\beta_{ji}}, \qquad (h_i, \bar{g}_j) = (h_i, \bar{h}_i^{\delta_{ji}}) = t^{p^{m-m_i}\delta_{ji}} \\
&(\bar{h}_i, g_j) = (\bar{h}_i, h_i^{\alpha_{ji}}) = t^{-p^{m-m_i}\alpha_{ji}}, \qquad (\bar{h}_i, \bar{g}_j) = (\bar{h}_i, h_i^{\gamma_{ji}}) = t^{-p^{m-m_i}\gamma_{ji}} \\
&(g_i, h_j) = (g_i, \bar{g}_i^{b_{ji}}) = t^{p^{m-m_i}b_{ji}}, \qquad (g_i, \bar{h}_j) = (g_i, \bar{g}_i^{d_{ji}}) = t^{p^{m-m_i}d_{ji}} \\
&(\bar{g}_i, h_j) = (\bar{g}_i, g_i^{a_{ji}}) = t^{-p^{m-m_i}a_{ji}}, \qquad (\bar{g}_i, \bar{h}_j) = (\bar{g}_i, g_i^{c_{ji}}) = t^{-p^{m-m_i}c_{ji}}
\end{aligned} \tag{10}$$

(10) 對於任意 $i, j = 1, 2, \cdots, r$ 均爲眞，故有

$$\begin{aligned}
&(h_j, g_i) = t^{p^{m-m_j}\beta_{ij}} = (g_i, h_j)^{-1} = t^{-p^{m-m_i}b_{ji}} \\
&(\bar{h}_j, g_i) = t^{-p^{m-m_j}\alpha_{ij}} = (g_i, \bar{h}_j)^{-1} = t^{p^{m-m_i}d_{ji}} \\
&(h_j, \bar{g}_i) = t^{p^{m-m_j}\delta_{ij}} = (\bar{g}_i, h_j)^{-1} = t^{p^{m-m_i}a_{ji}} \\
&(\bar{h}_j, \bar{g}_i) = t^{-p^{m-m_j}\gamma_{ij}} = (\bar{g}_i, \bar{h}_j)^{-1} = t^{p^{m-m_i}c_{ji}}
\end{aligned} \qquad (i, j = 1, 2, \cdots, r)$$

於是有

$$\begin{aligned}
&p^{m-m_j}\beta_{ij} \equiv -p^{m-m_i}b_{ji} \pmod{p^m} \\
&p^{m-m_j}\alpha_{ij} \equiv p^{m-m_i}d_{ji} \pmod{p^m} \\
&p^{m-m_j}\delta_{ij} \equiv p^{m-m_i}a_{ji} \pmod{p^m} \\
&p^{m-m_j}\gamma_{ij} \equiv -p^{m-m_i}c_{ji} \pmod{p^m}
\end{aligned} \qquad (i, j = 1, 2, \cdots, r) \tag{11}$$

又因

$$(H P)_{ij} = \sum_{k=1}^{r} H_{ik} P_{kj} = H_{ij} P_{jj} = \begin{pmatrix} \alpha_{ij} & \beta_{ij} \\ \gamma_{ij} & \delta_{ij} \end{pmatrix} \begin{pmatrix} p^{m-m_j} & 0 \\ 0 & p^{m-m_j} \end{pmatrix}$$

$$= \begin{pmatrix} p^{m-m_j}\alpha_{ij} & p^{m-m_j}\beta_{ij} \\ p^{m-m_j}\gamma_{ij} & p^{m-m_j}\delta_{ij} \end{pmatrix}$$

$$(P\,T^{\eta})_{ij}=\sum_{h=1}^{r}P_{ik}(T^{\eta})_{kj}=P_{ii}(T^{\eta})_{ij}=P_{ii}\,T^{\eta}_{ij}=\begin{pmatrix}p^{m-m_i}&0\\0&p^{m-m_i}\end{pmatrix}\begin{pmatrix}d_{ji}&-b_{ji}\\-c_{ji}&a_{ji}\end{pmatrix}$$

$$=\begin{pmatrix}p^{m-m_i}d_{ji}&-p^{m-m_i}b_{ji}\\-p^{m-m_i}c_{ji}&p^{m-m_i}a_{ji}\end{pmatrix}$$

故 (11) 可寫爲 $(H'P)_{ij}\equiv(P\,T^{\eta})_{ij}\pmod{p^m}$, $(i,j=1,2,\cdots,r)$, 於是 $H'P\equiv P\,T^{\eta}\pmod{p^m}$, $T'H'P\equiv T'P\,T^{\eta}\pmod{p^m}$, 按 (9), $T'H'P\equiv P\pmod{p^m}$, 故得

$$T'P\,T^{\eta}\equiv P\pmod{p^m}. \tag{12}$$

以下證 (12) 亦爲充分條件.

由 (12), $T'P\,T^{\eta}H'^{\eta}\equiv P\,H'^{\eta}\pmod{p^m}$; 但 $P^{\eta}=P$, $P\,T^{\eta}H'^{\eta}=P^{\eta}(H'T)^{\eta}=(H'T'P)^{\eta}$, 按 (9), $H'T'P\equiv P\pmod{p^m}$, 故得 $T'P\equiv P\,H'^{\eta}\pmod{p^m}$. 由 (6) (7) 的定義知 $\bar{P}P\equiv O\pmod{p^m}$, 故得 $\bar{P}T'P\equiv\bar{P}P\,H'^{\eta}\equiv O\pmod{p^m}$. 又

$$(P\,T'P)_{ij}=\sum_{\lambda=1}^{r}\sum_{\mu=1}^{r}(\bar{P})_{i\lambda}(T')_{\lambda\mu}(P)_{\mu j}=\bar{P}_{ii}\,T'_{ij}\,P_{jj}$$

$$=\begin{pmatrix}p^{m_i}&0\\0&p^{m_i}\end{pmatrix}\begin{pmatrix}a_{ij}&b_{ij}\\c_{ij}&d_{ij}\end{pmatrix}\begin{pmatrix}p^{m-m_j}&0\\0&p^{m-m_j}\end{pmatrix}=\begin{pmatrix}p^{m+m_i-m_j}a_{ij}&p^{m+m_j-m_i}b_{ij}\\p^{m+m_i-m_j}c_{ij}&p^{m+m_j-m_j}d_{ij}\end{pmatrix}$$

所以

$$\begin{pmatrix}p^{m+m_i-m_j}a_{ij}&p^{m+m_i-m_j}b_{ij}\\p^{m+m_i-m_j}c_{ij}&p^{m+m_i-m_j}d_{ij}\end{pmatrix}\equiv\begin{pmatrix}0&0\\0&0\end{pmatrix}\pmod{p^m}.$$

$$\begin{pmatrix}p^{m_i}a_{ij}&p^{m_i}b_{ij}\\p^{m_i}c_{ij}&p^{m_i}d_{ij}\end{pmatrix}\equiv\begin{pmatrix}0&0\\0&0\end{pmatrix}\pmod{p^{m_j}}\qquad(i,j=1,2,\cdots,r). \tag{13}$$

又

$$(T\,P\,T^{\eta})_{ij}=\sum_{\lambda=1}^{r}\sum_{\mu=1}^{r}(T)_{i\lambda}(P)_{\lambda\mu}(T^{\eta})_{\mu j}=\sum_{s=1}^{r}(T)_{is}(P)_{ss}(T^{\eta})_{sj}$$

$$=\sum_{s=1}^{r}\begin{pmatrix}p^{m-m_s}&0\\0&p^{m-m_s}\end{pmatrix}\begin{pmatrix}a_{is}&b_{is}\\c_{is}&d_{is}\end{pmatrix}\begin{pmatrix}d_{js}&-b_{js}\\-c_{js}&a_{js}\end{pmatrix} \tag{14}$$

$$=\begin{pmatrix}\sum_{s=1}^{r}p^{m-m_s}\begin{vmatrix}a_{is}&b_{is}\\c_{js}&d_{js}\end{vmatrix}&\sum_{s=1}^{r}p^{m-m_s}\begin{vmatrix}a_{is}&b_{is}\\a_{js}&b_{js}\end{vmatrix}\\\sum_{s=1}^{r}p^{m-m_s}\begin{vmatrix}c_{is}&d_{is}\\c_{js}&d_{js}\end{vmatrix}&\sum_{s=1}^{r}p^{m-m_s}\begin{vmatrix}a_{is}&b_{is}\\c_{js}&d_{js}\end{vmatrix}\end{pmatrix}.$$

由 (1) 與定理 1 知

$$(h_i,\bar{h}_j)=\prod_{s=1}^{r}(g_s^{a_{is}}g^{b_{is}},g_s^{c_{js}}\bar{g}_s^{d_{js}})=\prod_{s=1}^{r}(g_s^{a_{is}},\bar{g}_s^{d_{js}})(\bar{g}_s^{b_{is}},g_s^{c_{js}})$$

$$=\prod_{s=1}^{r}t^{p^{m-m_s}\left|\begin{smallmatrix}a_{is}&b_{is}\\c_{js}&d_{js}\end{smallmatrix}\right|}=t^{\sum_{s=1}^{r}p^{m-m_i}\left|\begin{smallmatrix}a_{is}&b_{is}\\c_{js}&d_{js}\end{smallmatrix}\right|}\qquad(i,j=1,2,\cdots,r)$$

(15)
$$(h_i,h_j)=\prod_{s=1}^{r}(g_s^{a_{is}}\bar{g}_s^{b_{is}},g_s^{a_{js}}\bar{g}_s^{b_{js}})=\prod_{s=1}^{r}(g_s^{a_{is}},\bar{g}_s^{b_{js}})(\bar{g}_s^{b_{is}},g_s^{a_{js}})$$

$$=\prod_{s=1}^{r}t^{p^{m-m_s}\left|\begin{smallmatrix}a_{is}&b_{is}\\a_{js}&b_{js}\end{smallmatrix}\right|}=t^{\sum_{s=1}^{r}p^{m-m_s}\left|\begin{smallmatrix}a_{is}&b_{is}\\a_{js}&b_{js}\end{smallmatrix}\right|}\qquad(i,j=1,2,\cdots,r)$$

$$(\bar{h}_i,\bar{h}_j)=\prod_{s=1}^{r}(g_s^{c_{is}}\bar{g}_s^{d_{is}},g_s^{c_{js}}\bar{g}_s^{d_{js}})=\prod_{s=1}^{r}(g_s^{c_{is}},\bar{g}_s^{d_{js}})(\bar{g}_s^{d_{is}},g_s^{c_{js}})$$

$$=\prod_{s=1}^{r}t^{p^{m-m_s}\left|\begin{smallmatrix}c_{is}&d_{is}\\c_{js}&d_{js}\end{smallmatrix}\right|}=t^{\sum_{s=1}^{r}p^{m-m_s}\left|\begin{smallmatrix}c_{is}&d_{is}\\c_{js}&d_{js}\end{smallmatrix}\right|}\qquad(i,j=1,2,\cdots,r)$$

當 $TPT^{\eta}\equiv P\pmod{p^m}$, 比較 (14), (15) 則得 $(h_i,h_j)=(h_i,\bar{h}_j)=(\bar{h}_i,h_j)=(\bar{h}_i,\bar{h}_j)=c$, 當 $i\neq j$ 時. $(h_i,\bar{h}_i)=t^{p^{m-m_i}}$, $(i=1,2,\cdots,r)$.

又 h_λ 與 $\bar{h}_\lambda$ 關於 $\mathfrak{z}$ 的相對巡廻率均爲 p^{m_λ}, $(\lambda=1,2,\cdots,r)$. 因按 (1.7) 知

$$h_\lambda^x=g_1^{xa_{\lambda1}}\bar{g}_1^{xb_{\lambda1}}\cdots g_r^{xa_{\lambda r}}\bar{g}_r^{xb_{\lambda r}}z_\lambda.\qquad z_\lambda\in\mathfrak{z},\quad\lambda=1,2,\cdots,r.$$

$$h_\lambda^x=g_1^{xc_{\lambda1}}\bar{g}_1^{xd_{\lambda1}}\cdots g_r^{xc_{\lambda r}}\bar{g}_r^{xd_{\lambda r}}\bar{z}_\lambda.\qquad\bar{z}_\lambda\in\mathfrak{z},\quad\lambda=1,2,\cdots,r.$$

當 $x=p^{m_\lambda}$, 按 (13) $\begin{pmatrix}p^{m_\lambda}a_{\lambda j}&p^{m_\lambda}b_{\lambda j}\\p^{m_\lambda}c_{\lambda j}&p^{m_\lambda}d_{\lambda j}\end{pmatrix}\equiv\begin{pmatrix}0&0\\0&0\end{pmatrix}\pmod{p^{m_j}}$, $(j=1,2,\cdots,r)$, 所以 $h_\lambda^{p^{m_\lambda}}\in\mathfrak{z}$, $\bar{h}_\lambda^{p^{m_\lambda}}\in\mathfrak{z}$, $(\lambda=1,2,\cdots,r)$. 另一方面, 因 $(h_\lambda,\bar{h}_\lambda)=t^{p^{m-m_\lambda}}$, 設 $h_\lambda^x\in\mathfrak{z}$, 則 $(h_\lambda^x,\bar{h}_\lambda)=c=t^{p^{m-m_\lambda}x}$, 於是 $p^{m-m_\lambda}x\equiv0\pmod{p^m}$, 於是 $x\equiv0\pmod{p^{m_\lambda}}$, 所以 h_λ 關於 $\mathfrak{z}$ 的相對巡廻率爲 p^{m_λ}, 同樣可證 $\bar{h}_\lambda$ 關于 $\mathfrak{z}$ 的相對巡廻率亦爲 p^{m_λ}.

在 (3) 中 $g_1,\bar{g}_1,\cdots,g_r,\bar{g}_r$ 爲一組底, 當 $TPT^{\eta}\equiv P\pmod{p^m}$, 已證當 $i\neq j$

$(h_i, h_j) = (h_i, \bar{h}_j) = (\bar{h}_i, h_j) = (h_i, h_j) = e$, $(h_i, \bar{h}_i) = t^{p^n - m_i}$, h_i, 及 $\bar{h}_i$ 關於 $\mathfrak{d}$ 的相對巡廻率爲 p^{m_i} $(i = 1, 2, \cdots, r)$, 故 $h_1, \bar{h}_1, \cdots, h_r, \bar{h}_r$ 亦爲羣 $\mathfrak{G}$ 的一組底.

定理 4 設 $\mathfrak{M}_{2r}$ 中方陣 T 表示羣 $\mathfrak{G}$ 中兩組底間的一變換. $TPT^{\theta} \equiv P \pmod{p^m}$, 則此等方陣的集合 $\mathfrak{R}$, 依方陣的乘法結合關於 $\bmod M$ 構成一羣. 方陣 M 如 (5) 所定義, 方陣 P 如 (6) 所定義.

證: S, T 爲 $\mathfrak{M}_{2r}$ 中方陣, 若 $TPT^{\theta} \equiv P \pmod{p^m}$, $SPS^{\theta} \equiv P \pmod{p^n}$, 則 $STP(ST)^{\theta} = STPT^{\theta}S^{\theta} \equiv SPS^{\theta} \equiv P \pmod{p^n}$, 故 $\mathfrak{R}$ 滿足羣的閉合律, 又由 (8) 已知 $TW \equiv WT \equiv E \pmod{M}$, 按 (11), $WP \equiv PT^{\theta} \pmod{p^m}$, 所以 $WPW^{\theta} \equiv PT^{\theta}W^{\theta} \pmod{p^m}$, 而 $PT^{\theta}W^{\theta} = P^{\theta}(WT)^{\theta} = (WTP)^{\theta}$, $WTP \equiv P \pmod{MP}$, $MP \equiv O \pmod{p^m}$, 所以 $WPW^{\theta} \equiv P \pmod{p^m}$. 又 $EPE^{\theta} \equiv P \pmod{p^m}$, 所以對 $\mathfrak{R}$ 中任一元素 T 有一逆元素及單位元素. 組合律對於方陣乘法當然滿足, 所以 $\mathfrak{R}$ 爲一羣.

ON p-GROUPS WITH CYCLIC COMMUTATOR SUBGROUP BELONGING TO THE CENTER

SHENG-LIEH LIOU

Let $\mathfrak{G}$ be a p-group of order p^n, its commutator group $D(\mathfrak{G})$ being cyclic and belonging to the center $\mathfrak{z}$, of $\mathfrak{G}$. Suppose that the order of $D(\mathfrak{G})$ is p^m, and $D(\mathfrak{G}) = (t)$ where t is a generating element of $D(\mathfrak{G})$. It is proved that the factor group $\mathfrak{G}/\mathfrak{z} = \bar{\mathfrak{G}}$ is an Abelian group of type $\{p^{m_1}, p^{m_1}, p^{m_2}, p^{m_2}, \cdots, p^{m_r}, p^{m_r}\}$ where $m = m_1 \geqq m_2 \geqq \cdots \geqq m_r$. The order of $\bar{\mathfrak{G}}$ is p^{2r}, $r = m_1 + m_2 + m_r$. $\mathfrak{G}$ is the product of its subgroups $\mathfrak{G}_1, \mathfrak{G}_2, \cdots, \mathfrak{G}_r$.

$$\mathfrak{G} = \mathfrak{G}_1 \cdot \mathfrak{G}_2 \cdots \mathfrak{G}_r.$$

When $i \neq j$, elements of $\mathfrak{G}_i$ commute with elements of $\mathfrak{G}_j$ and $\mathfrak{G}_i \cap \mathfrak{G}_j = \mathfrak{z}$. The group $\mathfrak{G}_i (i = 1, 2, \cdots, r)$ is defined as
$\mathfrak{G}_i = (g_i, \bar{g}_i, \mathfrak{z})$. $g_i^{p^{m_i}} = u \varepsilon \mathfrak{z}$, $\bar{g}_i^{p^{m_i}} = \bar{u} \varepsilon \mathfrak{z}$, the commutator of $\bar{g}_i$ and $g_i = t^{p^{m-m_i}}$. Any element X of $\mathfrak{G}$ can be uniquely represented as

$$X = g_1^{x_1} \cdot \bar{g}_1^{y_1} \cdots g_r^{x_r} \bar{g}_r^{y_r} z \qquad 0 \leqq x_i < p^{m_i}, \qquad 0 \leqq y_i < p^{m_i}, \qquad z \varepsilon \mathfrak{z}$$

Such elements $g_1 \bar{g}_1, \cdots, g_r \bar{g}_r$ are called *basis* of $\mathfrak{G}$.

The transformation of two bases can be represented by a matrix of $\mathfrak{M}_{2n}$ where $\mathfrak{M}_{2n}$ is the set of all $2n$-rowed square matrices with integral elements. It is proved that the necessary and sufficient condition for the

matrix T to represent such a transformation is that $TPT^{\theta} \equiv P \pmod{p^m}$, where $P = \mathrm{diag}\{p^{m-m_1}, p^{m-m_1}, p^{m-m_2}, p^{m-m_2}, \cdots p^{m-m_r}, p^{m-m_r}\}$, and θ be a transformation

$$\theta: \quad T \longleftrightarrow T^{\theta}, \qquad (T \text{ and } T^{\theta} \text{ in } \mathfrak{M}_{2n})$$

of $\mathfrak{M}_{2n}$ specially defined such that $(A+B)^{\theta} = A^{\theta} + B^{\theta}$, $(AB)^{\theta} = B^{\theta}A^{\theta}$, $(A^{\theta})^{\theta} = A$ for every A and B of $\mathfrak{M}_{2n}$. The totality of such matrices T form a group.