云南师范大学学术技术文库

西南联大暨云南师范大学60周年校庆自然科学文集

云南师范大学
学术技术文库
编辑委员会编

民族出版社

Z·53
Y98

·云南师范大学学术技术文库·

西南联大暨云南师范大学60周年校庆自然科学文集

云南师范大学学术技术文库编辑委员会

民族出版社

图书在版编目(CIP)数据

西南联大暨云南师范大学60周年校庆自然科学文集/云南师范大学学术技术文库编辑委员会编. -北京：民族出版社，1998.9

(云南师范大学学术技术文库)

ISBN 7-105-03143-3

Ⅰ.西… Ⅱ.云… Ⅲ.自然科学-文集 Ⅳ.N53

中国版本图书馆CIP数据核字(98)第10285号

民族出版社出版发行

(北京市和平里北街14号 邮编100013)

清利微机照排 固安县印刷厂印刷

各地新华书店经销

1998年9月第1版 1998年9月北京第1次印刷

开本:850×1168毫米 1/32 印张:13.5 字数:330千字

印数:0001—1800册 定价:27.00元

换位群为巡回群且属于中核的 p 群*

刘声烈

(昆明师范学院)

在 p 群 $\mathfrak{G}$ 的上中心群列(central series) $e = \mathfrak{z}_0 \subset \mathfrak{z}_1 = \mathfrak{z} \subset \mathfrak{z}_2 = \subset \cdots \subset \mathfrak{z}_C = \mathfrak{G}$ 中,因子群(factor group) $\mathfrak{z}_i/\mathfrak{z}_{i-1}$ 属于因子群 $\mathfrak{z}_{i+1}/\mathfrak{z}_{i-1}$ 的中核(center). $\mathfrak{z}_{i+1}/\mathfrak{z}_i$ 为可换群,故相对换位群 (relative commutator group) $(\mathfrak{z}_{i+1}\cdot\mathfrak{z}_{i+1}) \subset \mathfrak{z}_i$。因此因子群 $\mathfrak{z}_{i+1}/\mathfrak{z}_{i-1}$ 的换位群 $(\mathfrak{z}_{i+1}, \mathfrak{z}_{i+1})/\mathfrak{z}_{i-1}$ 属于 $\mathfrak{z}_i/\mathfrak{z}_{i-1}$,因之亦属于其中核,特别,$\mathfrak{z}_2$ 的换位群於 $\mathfrak{z}_2$ 的中核。本文拟对此种换位群属于中核的 p 群 $\mathfrak{G}$ 作一研究,但仅限于 $\mathfrak{G}$ 的换位群为一巡回群的情拟。所得主要结果在定理 1 与定理 3 中。

所用符号采取 Hans Zassenhaus: Lebrbuch der Gruppentheorie 144 面所载的:

$\mathfrak{e}$ $\mathfrak{G}$ 的主单位元(unit elennent);

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

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

Z_f $\mathfrak{G}$ 中与 $\mathfrak{G}$ 的一部分集合 f 的每一元素交换可能的一切元素所成的群;

f^r 一切 xfx^{-1} 的集合,f 为 $\mathfrak{G}$ 之一的部分集合,x 为 $\mathfrak{G}$ 中任意元;

$D\mathfrak{G}$ $\mathfrak{G}$ 的换位群(commutator group);

$(a, b) = aba^{-1}b^{-1}$ $\mathfrak{G}$ 中元素 a 与 b 的换位元素(commutator).

---

* 本文原载于《数学学报》,卷 2,期 1 - 2(合),页 50 - 64。1952 年。

以下均假定 $\mathfrak{E}$ 为 p 群，$\mathfrak{E}: e = p^n$，$\mathfrak{E}$ 的换位群 $D\mathfrak{E}$ 属于 $\mathfrak{E}$ 的中核 $\mathfrak{z}$. $D\mathfrak{E}$ 为巡回群：$D\mathfrak{E} = (t)$，t 为 $D\mathfrak{E}$ 的一生成元，其巡回率 P^m，$D\mathfrak{E}$: $e = p^m$.

一、换位元素的运算

若 $D\mathfrak{E} \subset \mathfrak{z}$，则对 $\mathfrak{E}$ 中任意元素 a,b,c…换位元素(a,b)的计算符合下列简单规则。

(1.1) $aba^{-1} = b^a = (abc^{-1}b^{-1})b = (a,b)b = b(a,b)$

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

(1.3) $(ab,c) = (a,c)(b,c)$.

证： $(ab,c) = abc(ab)^{-1}c^{-1} = abcb^{-1}a^{-1}c^{-1}$

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

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

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

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

$a_i (i = 1,2,\cdots,m)$，$b_j (j = 1,2\cdots,n)$均为 $\mathfrak{E}$ 中任意元素.

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

(1.6) $a^x b^y = b^y a^x (a,b)^{xy}$

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

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

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

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

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

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

试读结束，需要全本PDF请购买 www.ertongbook.com

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

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

(1.10) $(b,a)=(c,a)$，则$(bc^{-1},a)=e$ 于是 $bc^{-1}\varepsilon Za$.

证：$(bc^{-1},a)=(b,a)(c^{-1},a)=(b,a)(c,a)^{-1}$按(1.3)(1.8)

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

二、群 $\mathfrak{E}$ 的构造

(2.1)若 $D\mathfrak{E}=(t)$，t 的巡回率为p^m.则 $\mathfrak{E}$ 中必有一对元素 $g,\bar{g}$ 使 $(g,\bar{g})=t$. $D\mathfrak{E}=(t)$中的任一元素皆为换位元素.

证：令 x,y 跑过 $\mathfrak{E}$ 中所有元素，而$(x,y)=t^{\sigma}$，$0<\sigma\leqq p^m$.若 σ 中有一σ_0 与 p 互质，$(x_0,y_0)a=t^{\sigma_0}$则合同方程式 $\sigma_0 u\equiv 1(\mathrm{mod}p^m)$有整数解 $u=\alpha$，于是$(x_0^{\alpha},y_0)=(x_0,y_0)^{\alpha}=t^{\sigma_0\alpha}=t$，而定理得证.否则若任一 σ 皆不与 P 互质，则 σ 均有 cp^s 形，$1\leqq s<m$，c 为与p 互质的正整数.所有换位元素 t^{σ} 均为 t^p 的质，于是换位元素所生成的换位群为巡回群(t)的真部分群，此与 $D\mathfrak{E}=(t)$的假设抵触，故 $\mathfrak{E}$ 中必有一对元素 $g,\bar{g}$ 使$(g,\bar{g})=t$，又按(1.5)，对任意正整数 c，$(g^c,\bar{g})=(g,\bar{g})^c=t^c$，故 $D\mathfrak{E}$ 中的任意一元素皆为换位元素.

(2.2)设$(g,\bar{g})=t$，Z_g，$Z_{\bar{g}}$ 分别为 $\mathfrak{E}$ 中 $g,\bar{g}$ 的交换可能群，则 $\mathfrak{E}=(g).Z_{\bar{g}}=(\bar{g}).Z_g$.

证：设 s 为 $\mathfrak{E}$ 中任意元，$(s,\bar{g})=t^{\sigma}$，$sg^{s-1}=gt^{\sigma}$，所以 $\bar{g}$ 的共轭元(conjugate)皆为 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 $\bar{g}$ 所属的共轭类(conjugate set)为 $\bar{g}t,\bar{g}t^2,\cdots,\bar{g}t^{p^m}=\bar{g}$.因$(\mathfrak{E}:e/Z_{\bar{g}}:e)=\bar{g}$ 所属的共轭类中元素数 $=p^m$，所以 $\mathfrak{E}:e=(Z\bar{g}:e)p^m$.当 $\alpha=\backslash\ \beta,0<\beta<\alpha\leqq p^m$，则旁系(co-set)$g^{\alpha}Z\bar{g}$ 与旁系 $b^{\beta}Z\bar{g}$ 无共同元；否则 $g^{\alpha-\beta}\subset Z_{\bar{g}}$，于是$(g^{\alpha-\beta},\bar{g})=(g,\bar{g})^{\alpha-\beta}=t^{\alpha-\beta}=e$，但 $0<\beta<\alpha\leqq p^m$，此为不可能.故 p^m 个旁系 $g^iZ_{\bar{g}}(i=1,2\cdots,p^m)$的元系皆互异，而此 p^m 个旁系共有 $p^m(Z_{\bar{g}}:e)=\mathfrak{E}:e$ 个元素.因此 $\mathfrak{E}=Z_{\bar{g}}+gZ\bar{g}+\cdots+gp^{m-1}Z_{\bar{g}}$，即 $\mathfrak{E}=(g).Z_{\bar{g}}$.又$(\bar{g},g)=(g,\bar{g})^{-1}=t^{-1}$，按(1.5)$(\bar{g}g)^i=(\bar{g}^i,g)$，所以

$\bar{g}^i g \bar{g}^{-i} = gt^{-i}(i = 1,2,\cdots,p^m)$，所以 g 所属的共轭类为 $gt, gt^2, \cdots, gt^{p^m} = g$. 同样的理由可以证明 $\mathfrak{E} = (\bar{g}) \cdot Z_g$.

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

证：群 $(\bar{g})$ 的任意元与群 $Z_{\bar{g}}$ 的任意元皆交换可能，因之与群 $Z_g \cap Z_{\bar{g}}$ 的任意元皆交换可能，故 $(\bar{g}) \cdot (Z_g \cap z_{\bar{g}})$ 为一群 $\mathfrak{J}$. 若 $Z_{\bar{g}} \neq \mathfrak{J}$，则 $\mathfrak{E}$ 中有一元 $S \in Z_{\bar{g}}$ 而 $s \notin \mathfrak{J}$. 因 $S \in Z_{\bar{g}}$，故 $(s,\bar{g}) = c \cdot (s,g) \neq c$；否则 $(s,g) = c, (s,\bar{g}) = c$，于是 $S \in Zg \cap Z_{\bar{g}}$. 于是 $S \in (\bar{g}) \cdot (Z_g \cap Z_{\bar{g}}) = \mathfrak{J}$ 而与 $s \notin \mathfrak{J}$ 的假设抵触了. 令 $(s,g) = t^\lambda, 0 < \lambda < p^m$，因 $(\bar{g},g) = t^{-1}$，按(1.3)，(1.5)，$(\bar{g}^\lambda s, g) = (\bar{g}^\lambda, g)(s,g) = (\bar{g},g)^\lambda (s,g) = t^{-\lambda} \cdot t^\lambda = e$，于是 $\bar{g}^\lambda S \in Z_g$. 因 $S \in Z_{\bar{g}}$，故 $s\bar{g}^\lambda S \in Z_{\bar{g}}$，故 $\bar{g}^\lambda S \in Z_g \cap Z_{\bar{g}}$，故 $s \in (\bar{g}) \cdot (Z_g \cap Z_{\bar{g}}) = \mathfrak{J}$. 此与 $s \notin \mathfrak{J}$ 的假设矛盾，故 $Z_{\bar{g}} = (\bar{g}) \cdot (Z_g \cap Z_{\bar{g}})$. 同样的理由可以证明 $Z_g = (g) \cdot (Z_g \cap Z_{\bar{g}})$.

(2.4)设 $(g,\bar{g}) = t$，命 $g = g_1, \bar{g} = \bar{g}_1$. 由 $g_1, \bar{g}_1, \mathfrak{d}$ 生成一群 $\mathfrak{E}_1 = (g_1, \bar{g}_1, \mathfrak{d})$，$Z_{\mathfrak{E}_1}$ 为 $\mathfrak{E}$ 中与 $\mathfrak{E}_1$ 的每元交换可能的元素所成的群，则 $\mathfrak{E} = \mathfrak{E}_1 \cdot Z_{\mathfrak{E}_1} = Z_{\mathfrak{E}_1} \cdot \mathfrak{E}_1$. $\mathfrak{E}_1 \cap Z_{\mathfrak{E}_1} = \mathfrak{d}$.

证：按(2.2)(2.3) $\mathfrak{E} = (g_1) \cdot Z_{\bar{g}_1} = (g_1) \cdot (\bar{g}_1) \cdot (Z_{g_1} \cap Z_{\bar{g}_1})$. 显然 $Z_{g_1} \cap Z_{\bar{g}_1} = Z_{(g_1,\bar{g}_1)} = Z_{(g_1,\bar{g}_1,\mathfrak{d})} = Z_{\mathfrak{E}_1}$，所以 $\mathfrak{E} = \mathfrak{E}_1 \cdot Z_{\mathfrak{E}_1}$. 若 $s \in \mathfrak{E}_1 \cap Z_{\mathfrak{E}_1}$，因 $s \in Z_{\mathfrak{E}}$，故 s 与 $\mathfrak{E}_1$ 的每元交换，因 $s \in \mathfrak{E}_1$ 故 s 与 $Z_{\mathfrak{E}_1}$ 的每元交换；因此 s 与 $\mathfrak{E} = \mathfrak{E}1 \cdot Z_{\mathfrak{E}_1}$ 的每元交换，于是 $s \in \mathfrak{d}$，另一方面 $\mathfrak{d} \subset \mathfrak{E}_1, \mathfrak{d} \subset Z_{\mathfrak{E}_1}$，所以 $\mathfrak{d} \subset \mathfrak{E}_1 \cap Z_{\mathfrak{E}_1}$. 所以 $\mathfrak{E}_1 \cap Z_{\mathfrak{E}_1} = \mathfrak{d}$.

(2.5)设 $D\mathfrak{E} = (t) \subset \mathfrak{d}$，$t$ 的巡回率为 p^m，$(g_1, \bar{g}_1) = t$，由 $g_1, \bar{g}_1, \mathfrak{d}$ 生成一群 $\mathfrak{E}_1 = (g_1, \bar{g}_1, \mathfrak{d})$，则 g_1 及 $\bar{g}_1$ 关于 $\mathfrak{d}$ 的相对巡回率均为 p^m，$\mathfrak{E}_1/\mathfrak{d}$ 为 (p^m, p^m) 型可换群.

证：设 g_1 关于 $\mathfrak{d}$ 的相对巡回率为 d，因 $g_1^d \in \mathfrak{d}$，$(g_1^d, \bar{g}_1) = (g_1, \bar{g}_1)^d = t^d = e$，所以 $d \equiv 0 \pmod{p^m}$. 另一方面 $(g_1^{p^m}, \bar{g}_1) = t^{p^m} = e$，按(1.9) $g_1^{p^m} \in Z_{\bar{g}_1}$，所以 $g_1^{p^m} \in Z_{g_1} \cap Z_{\bar{g}_1} = Z_{\mathfrak{E}_1}$，按(2.4) $g_1^{p^m} \in \mathfrak{E}_1 \cap Z_{\mathfrak{E}_1} = \mathfrak{d}$，所以 $p^m \equiv 0 \pmod{d}$. 所以 $d = p^m$. 同样可证 $\bar{g}$ 关于 $\mathfrak{d}$ 的相对巡回率亦为 p^m. 所以 $\mathfrak{E}_1/\mathfrak{d}$ 为 (p^m, p^m) 型可换群.

设 $DZ\mathfrak{E}_1$ 为 $Z\mathfrak{E}_1$ 的换位群，若 $D\,Z_{\mathfrak{E}1}=e$，则 $\mathfrak{E}=\mathfrak{E}_1$；因若 $s\varepsilon Z_{\mathfrak{E}1}$，则 s 与 $Z_{\mathfrak{E}1}$，的每元交换，s 又与 $\mathfrak{E}_1$ 的每元交换，于是 $s\varepsilon\mathfrak{z}$，于是 $Z_{\mathfrak{E}1}\subset\mathfrak{z}$，又 $\mathfrak{z}\subset Z_{\mathfrak{E}1}$，所以 $Z_{\mathfrak{E}1}=\mathfrak{z}$；于是 $\mathfrak{E}=\mathfrak{E}_1\cdot\mathfrak{z}=\mathfrak{E}_1$. 若 $DZ_{\mathfrak{E}1}\neq e$，设 $DZ_{\mathfrak{E}1}=(t_2)\subset(t)\subset\mathfrak{z}$，$DZ_{\mathfrak{E}1}:e=p^{m_2}$，$(0<m_2\leqq m)$，则 $t_2^{p^{m_2}}=e$；因 $t_2\varepsilon(t)$，我们可选 t_2 令 $t_2=t^{p^{m-m_2}}$ 而使 $DZ_{\mathfrak{E}1}=(t_2)$. 又 $Z_{\mathfrak{E}1}$ 的中核等于 $\mathfrak{E}$ 的中核 $\mathfrak{z}$；因若 s 属于 $Z_{\mathfrak{E}1}$ 的中核，则 s 属于 $\mathfrak{E}_1\cdot Z_{\mathfrak{E}1}=\mathfrak{E}$ 的中核 $\mathfrak{z}$，而 $\mathfrak{z}\subset Z_{\mathfrak{E}1}$，故 $Z_{\mathfrak{E}1}$ 的中核等于 $\mathfrak{E}$ 的中核 $\mathfrak{z}$. 命 $t=t_1$，$m=m_1$. 当 $DZ_{\mathfrak{E}1}\neq e$，因 $DZ_{\mathfrak{E}1}=(t_2)\subset\mathfrak{z}$，$t_2=t_1^{p^{m-m_2}}$，$t_2$ 的巡回率为 P^{m_2}，又 $DZ_{\mathfrak{E}1}$ 的中核等于 $\mathfrak{z}$ 故按(2.4)如同 $\mathfrak{E}=\mathfrak{E}_1\cdot Z_{\mathfrak{E}1}$ 的分解同样可得 $Z_{\mathfrak{E}1}$ 的一分解：$Z_{\mathfrak{E}1}=\mathfrak{E}_2\cdot Z(\mathfrak{E}_1,\mathfrak{E}_2)$；$\mathfrak{E}_2=(g_2,\bar{g}_2,\mathfrak{z})$，$(g_2,\bar{g}_2)=t_2$，$\mathfrak{E}_2\cap Z_{(\mathfrak{E}1,\mathfrak{E}2)}=\mathfrak{z}$. 如此继续下去，终之得将 $\mathfrak{E}$ 分解为若干部分群的乘积：$\mathfrak{E}=\mathfrak{E}_1\cdot\mathfrak{E}_2,\cdots,\mathfrak{E}_r$；$\mathfrak{E}_i=(g_i,\bar{g}_i,\mathfrak{z})$，$(g_i,\bar{g}_i)=t_i=t_1^{p^{m-m_i}}$，$m=m_1\geqq m_2\geqq\cdots\geqq m_r$，$i=1,2,\cdots,r$. 当 $i\neq j$，$\mathfrak{E}_i$ 的任意元与 $\mathfrak{E}_j$ 的任意元交换可能，且 $\mathfrak{E}_i\cap\mathfrak{E}_j=\mathfrak{z}$. 综上所述，遂得.

定理 1 若 p 群 $\mathfrak{E}$ 的换位群 $D\mathfrak{E}$ 为一巡回群且属于 $\mathfrak{E}$ 的中核 $\mathfrak{z}$：$D\mathfrak{E}=(t)\subset\mathfrak{z}$，$D\mathfrak{E}:e=p^m$，则 $\mathfrak{E}$ 可分解为部分群的乘积：$\mathfrak{E}=\mathfrak{E}_1\cdot\mathfrak{E}_2\cdots\mathfrak{E}_r$；当 $i\neq j$，$\mathfrak{E}_j$ 的每元与 $\mathfrak{E}_j$ 的每元交换可能，且 $\mathfrak{E}_i\cap\mathfrak{E}_j=\mathfrak{z}$. 命 $t=t_1$，$m=m_1$. $\mathfrak{E}_i$ 乃如是定义的群：

$\mathfrak{E}_i=(gi,\bar{g}_i,\mathfrak{z})$，$(gi,\bar{g}_i)=t_i=t^{p^{m-m_i}}$，$m=m_1\geqq m_2\geqq\cdots\geqq m_r$，$(i=1,2,\cdots,r)$. $\mathfrak{E}_i$ 的换位群 $D\mathfrak{E}_i=(t_i)$，$D\mathfrak{E}_i:e=p^{m_i}(i=1,2,\cdots,r)$. g_i 及 g_i 关于 $\mathfrak{z}$ 的相对巡回率均为 P^{m_i}. $\mathfrak{E}_i$ 的中核等于 $\mathfrak{E}$ 的中核. 因子群 $\mathfrak{E}/\mathfrak{z}=\mathfrak{J}$ 乃 $(p^{m_1},p^{m_1},\cdots,p^{m_r},p^{m_r})$ 型可换群. $\mathfrak{J}:e=p^{2r}$，$r=m_1+m_2+\cdots+m_r$，$\mathfrak{J}$ 之皆为 P 的偶数幂.

因 $\mathfrak{z}/\mathfrak{E}=\mathfrak{J}$ 为 $(p^{m_1},p^{m_1},p^{m_2},p^{m_2},\cdots,p^{m_r},p^{m_r})$ 型可换群，所以 $m=m_1\geqq m_2\geqq\cdots\geqq m_r$ 乃属于 $\mathfrak{E}$ 的一组不变系. 又 $\mathfrak{E}_1\cdots\mathfrak{E}_{i-1}\cdot\mathfrak{E}_{i+1}\cdots\mathfrak{E}_r\subset Z_{\mathfrak{E}_i}$，所以 $\mathfrak{E}=\mathfrak{E}_i\cdot Z_{\mathfrak{E}i}$，$(i=1,2,\cdots,r)$. 且 $\mathfrak{E}_i\cap Z_{\mathfrak{E}i}=\mathfrak{z}$；因若 $s\varepsilon\mathfrak{E}_i\cap Z_{\mathfrak{E}_i}$，则 s 与 $\mathfrak{E}_i$ 的每元又与 $Z_{\mathfrak{E}i}$ 的每元交换可能，故 $s\varepsilon\mathfrak{z}$，故 $\mathfrak{E}_i\cap Z_{\mathfrak{E}i}\subset\mathfrak{z}$，而 $\mathfrak{z}\subset\mathfrak{E}_i$，$\mathfrak{z}\subset Z_{\mathfrak{E}i}$，故 $\mathfrak{E}_i\cap Z_{\mathfrak{E}i}=\mathfrak{z}$.

如定理 1 中所述之 $\mathfrak{E}$ 的一组生成元 $g_1,\bar{g}_1,g_2,\bar{g}_2,\cdots,g_r,\bar{g}_r$ 称为

群 $\mathfrak{G}$ 的一组底.其特征为$(g_i,\bar{g}_i)=t_i=t^{p^{m}-m_i}$, $m=m_1\geqq m_2\geqq\cdots\geqq m_r$, $(i=1,2,\cdots,r)$;当 $i\neq j$,$(g_i,g_j)=(g_i,\bar{g}_j)=(\bar{g}_i,g_j)=(\bar{g}_i,\bar{g}_j)=e$, g_i 及 $\bar{g}_i$ 关於 $\mathfrak{d}$ 的相对巡回率均为 p^{mi}

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

证:因 g_i 及 $\bar{g}$ 关于 $\mathfrak{d}$ 的相对巡回率均为 p^{mi},故 $\mathfrak{G}_i=(g_i,\bar{g}_i,\mathfrak{d})$,中的元素恒可表为 $g^x\bar{g}_i^y\mathfrak{d}$ 形$(0\leqq x<p^{m_i},0\leqq y<p^{m_i},x\in\mathfrak{d})$.今证此表示为一意的.设 $g_i^x=\bar{g}_i^y\mathfrak{d}$,$(0\leqq x<p^{m_i},0\leqq y<p^{m_i},x\in\mathfrak{d})$,则$(g_i^x,\bar{g}_i)=(\bar{g}_i^y\mathfrak{d},\mathfrak{d}\bar{g}_i)=e$,又$(g_i^x,\bar{g}_i)=t_i^x$,所以 $t_i^x=e$,所以 $x\equiv0(\mathrm{mod}\ p^{mi})$,但 $0\leqq x<P^{mi}$,所以 $x=0$;于是 $\bar{g}_i^y z=g_i^x=e$,$\bar{g}_i^y=z^{-1}\varepsilon\mathfrak{d}$,按定理 1,$\bar{g}_i$ 关于 $\mathfrak{d}$ 的相对巡回率为 P^{m_i}所以 $y\equiv0(\mathrm{mod}\ p^{m_i})$;但 $0\leqq y<p^{m_i}$,所以 $y=0,z=e$.若 $g_i^a\bar{g}_i^b z=g_i^{a'}\bar{g}_i^{b'}z'(0\leqq a<p^{m_i},0\leqq b<p^{m_i},0\leqq a'<p^{m_i},0\leqq b'<p^{m_i},x\in\mathfrak{d},z'\varepsilon\mathfrak{d})$,则 $g_i^{a-a'}=\bar{g}_i^{b'-b}z'z^{-1}$,于是 $a-a'=0,b'-b=0$.于是 $a=a',b=b',z=z'$.

定理 2 如定理 1 中所假设,若 $g_1,\bar{g}_1,\cdots,g_r,\bar{g}_r$ 为群 $\mathfrak{G}$ 的一组底,则 $\mathfrak{G}$ 的元素可一意表为

$$g_1^{x_1}\bar{g}_1^{y_1}\cdots g_r^{x_r}\bar{g}_r^{y_r}z\qquad(0\leqq x_i<p^{m_i},0\leqq y_i<p^{m_i},i=1,2,\cdots,r,z\varepsilon\mathfrak{d})$$

证[1]:设 $s_1s_2\cdots s_r x\in\mathfrak{d}$,而 $si\varepsilon\mathfrak{G}_i$,$(i=1,2,\cdots,r)$,$x\in\mathfrak{d}$,则 $s_i\varepsilon\mathfrak{d}(i=1,2\cdots,r)$.因 $s_i^{-1}=s_1s_2\cdots s_{i-1}s_{i+1}\cdots s_r x Z\ \mathfrak{G}_i$,又 $s_i^{-1}\varepsilon\mathfrak{G}_i$ 于是 $s_i^{-1}\varepsilon\mathfrak{G}_i\cap Z\,\mathfrak{d}_i=\mathfrak{d}$,于是 $s_i\varepsilon\mathfrak{d}$ 设

$$g_1^{a_1}\bar{g}_1^{b_1}=\bar{g}_r^{a_r}\bar{g}_r^{b_r}z\cdots g_1^{c_1}\bar{g}_1^{d_1}\cdots g_r^{c_r}\bar{g}_r^{d_r}z'\ (0\leqq a_i<p^{m_i},0\leqq b_i<p^{m_i},0\leqq c_i<p^{m_i},0\leqq d_i<p^{m_i},i=1,2,\cdots,r,x\in\mathfrak{d},z'\varepsilon\mathfrak{d}),\text{则}$$

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

于是$(g_i^{ai}\bar{g}_i^{bi})(g_i^{ci}\bar{g}_i^{di})^{-1}\varepsilon\mathfrak{d}(i=1,2,\cdots,r)$,按(2.6),于是得 $a_i=c_i$, $b_i=d_i(i=1,2,\cdots,r)$, $z=z'$.

三、底的变换

(3.1) 设 $\mathfrak{M}_2$ 为一切 2 行 2 列方阵的集合,方阵的元素取自整数

环，σ 为 $\mathfrak{M}_2$ 中方阵间的一单值对应如下定意的：

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

则对 $\mathfrak{M}_2$ 中任意方阵 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)$A \cdot A^{\sigma} = \begin{pmatrix} |A| & 0 \\ 0 & |A| \end{pmatrix}$，$|A|$ 为 A 的行列式.

证：由简单的计算易验其为真.

(3.2) 设 $\mathfrak{M}_{2r}$ 为所有 2r 行 2r 列方阵的集合，方阵中的元素取自整数环 $\mathfrak{M}_{2r}$ 中方阵

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

命 $\mathfrak{M}_2$ 中方阵

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

采用符号 $X = (X_{ij}), (X)_{ij} = X_{ij} (i, j = 1, 2, \cdots, r)$

ϱ 与 τ 为 $\mathfrak{M}_{2r}$ 中方程间如下所定义的单值对应：

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

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

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

i)$(X^{Q})^{\tau} = (X^{\tau})^{Q} = X^{\theta}$，ii)$(X^{\theta})^{\theta} = X$，iii)$(X^{\theta})_{ij} = X_{ji}^{Q}$，$\sigma$ 如(3.1)所定义。iv)$(X + Y)^{\theta} = X^{\theta} + Y^{\theta}$，v)$(XY)^{\theta} = Y^{\theta} X^{\theta}$.

证：i)ii)iii)iv) 由简单的计算易验其为真，今证 v)

$((XY)^{\sigma})_{ij} = (\sum_{k=1}^{r} X_{ik} Y_{kj})^{\sigma} = \sum_{k=1}^{r} Y_{kj}^{\sigma} X_{ik}^{\sigma}$ 按(3.1)的 ii)及 iii)

$$= \sum_{h=1}^{r} (Y^{Q})_{kj} (X^{Q})_{ik} = \sum_{k=1}^{r} (Y^{\delta\tau})_{jk} (X^{\delta\tau})_{kj}$$ 按 τ 的定义。

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

所以 $(XY)^{\delta\tau} = y^{\delta\tau} X^{\delta\tau}$，所以 $(XY)^{\theta} = Y^{\theta} X^{\theta}$

$\mathfrak{E}/\mathfrak{d} = \mathfrak{I}$ 为 $(P^{m_1}, P^{m_1}, \cdots P^{m_r} P^{m_r})$ 型可换群，设 $g_1, \bar{g}_1, \cdots g_r, \bar{g}_r$ 与 $h_1, \bar{h}_1, \cdots h_r, \bar{h}_r$ 为 $\mathfrak{E}$ 的两组底，按定理 2，设

$$h_s = g_1^{a_{s1}} \bar{g}_1^{b_{s1}} \cdots g_r^{a_{sr}} \bar{g}_r^{b_{sr}} z_s, z_s \varepsilon \mathfrak{d}, \quad 0 \leqq a_{si} < p^{m_i}, 0 \leqq b_{si} < p^{m_i},$$

$$(i, s = 1, 2 \cdots, r)$$

$$\bar{h}_s = g_1^{c_{s1}} \bar{g}_1^{d_{s1}} \cdots g_r^{c_{sr}} \bar{g}_r^{d_{sr}} \bar{z}_s, \bar{z}_s \varepsilon \mathfrak{d}, \quad 0 \leqq c_{si} < p^{mi}, 0 \leqq d_{si} < p^{m_i}, \tag{1}$$

$$(i, s = 1, 2 \cdots, r)$$

$$g_s = h_1^{a_{s1}} \bar{h}_1^{\beta_{s1}} \cdots h_r^{a_{sr}} \bar{h}_r^{\beta_{sr}} z_s', \bar{z}_s' \varepsilon \mathfrak{d}, \quad 0 \leqq \alpha_{si} < p^{m_i}, 0 \leqq \beta_{si} < p^{m_i},$$

$$(i, s = 1, 2 \cdots, r)$$

$$\bar{g}_s = h_1^{\gamma_{s1}} \bar{h}_1^{\delta_{s1}} \cdots h_r^{r_{sr}} \bar{h}_r^{\delta_{sr}} \bar{z}_s', \bar{z}_s' \varepsilon \mathfrak{d}, \quad 0 \leqq \gamma_{si} < p^{m_i}, 0 \leqq \beta_{si} < p^{m_i},$$

$$(i, s = 1, 2 \cdots, r)$$

因 $\mathfrak{E}/\mathfrak{d} = \mathfrak{I}$ 是可换群，将 $\mathfrak{I}$ 中元素的结合法写为加法，单位元素写为零，则关于 mod $\mathfrak{d}$，(1)式可写为

$$h_s = a_{s1} g_1 + b_{s1} \bar{g}_1 + \cdots + a_{si} g_r + b_{sr} \bar{g}_r . (\mathrm{mod}\mathfrak{d})$$

$$0 \leqq a_{si} < p^{m_i}, 0 \leqq b_{si} < p^{m_i}, (s, i = 1, 2, \cdots, r)$$

$$\bar{h}_s = c_{s1} g_1 + d_{s1} \bar{g}_1 + \cdots + c_{sr} g_r + d_{sr} \bar{g}_r . (\mathrm{mod}\mathfrak{d}) \tag{2}$$

$$0 \leqq c_{si} < p^{m_i}, 0 \leqq d_{si} < p^{m_i}, (s, i = 1, 2, \cdots, r)$$

$$g_s = \alpha_{s1} h_1 + \beta_{s1} \bar{h}_1 + \cdots + \alpha_{sr} h_r + \beta_{sr} \bar{h}_r . (\mathrm{mod}\mathfrak{d})$$

$$0 \leqq \alpha_{si} < p^{m_i}, 0 \leqq \beta_{si} < p^{m_i}, (s, i = 1, 2, \cdots, r)$$

$$\bar{g}_s = \gamma_{s1} h_1 + \delta_{s1} \bar{h}_1 + \cdots + r_{sr} h_r + \delta_{sr} \bar{h}_r . (\mathrm{mod}\mathfrak{d})$$

$$0 \leqq \gamma_{si} < p^{m_i}, 0 \leqq \delta_{si} < p^{m_i}, (s, i = 1, 2, \cdots, r)$$

用方阵写法(2)式可写为

试读结束，需要全本PDF请购买 www.ertongbook.com

$$\begin{pmatrix} h_1 \\ \bar{h}_1 \\ \cdot \\ \cdot \\ h_r \\ \bar{h}_r \end{pmatrix} = \begin{pmatrix} a_{11} & b_{11} & \cdots & a_{1r} & b_{1r} \\ c_{11} & d_{11} & \cdots & c_{1r} & d_{1r} \\ \cdot & \cdot & \cdots & \cdot & \cdot \\ \cdot & \cdot & \cdots & \cdot & \cdot \\ a_{r1} & b_{r1} & \cdots & a_{rr} & b_{rr} \\ c_{r1} & d_{r1} & \cdots & c_{rr} & d_{rr} \end{pmatrix} \begin{pmatrix} g_1 \\ \bar{g}_1 \\ \cdot \\ \cdot \\ g_r \\ \bar{g}_r \end{pmatrix} (\mathrm{mod}\ \mathfrak{d}) \tag{3}$$

$$\begin{pmatrix} g_1 \\ \bar{g}_1 \\ \cdot \\ \cdot \\ g_r \\ \bar{g}_r \end{pmatrix} = \begin{pmatrix} a_{11} & \beta_{11} & \cdots & a_{1r} & \beta_{1r} \\ r_{11} & \delta_{11} & \cdots & r_{1r} & \delta_{1r} \\ \cdot & \cdot & \cdots & \cdot & \cdot \\ \cdot & \cdot & \cdots & \cdot & \cdot \\ a_{r1} & \beta_{r1} & \cdots & a_{rr} & \beta_{rr} \\ r_{r1} & \delta_{r1} & \cdots & r_{rr} & \delta_{rr} \end{pmatrix} \begin{pmatrix} h_1 \\ \bar{h}_1 \\ \cdot \\ \cdot \\ h_r \\ \bar{h}_r \end{pmatrix} (\mathrm{mod}\ z)$$

设 $\mathfrak{M}_{2r}$ 中方阵

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

$$M = (M_{ij}).\ M^{ij} = \begin{pmatrix} P^{mj} & P^{mj} \\ P^{mj} & P^{mj} \end{pmatrix}. \tag{5}$$

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

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

由(3)式

$$\begin{pmatrix} h_1 \\ \bar{h}_1 \\ \cdot \\ \cdot \\ h_r \\ \bar{h}_r \end{pmatrix} = T \begin{pmatrix} g_1 \\ \bar{g}_1 \\ \cdot \\ \cdot \\ g_r \\ \bar{g}_r \end{pmatrix} = TW \begin{pmatrix} h_1 \\ \bar{h}_1 \\ \cdot \\ \cdot \\ h_r \\ \bar{h}_r \end{pmatrix} (\mathrm{mod}\mathfrak{d})$$

因 h_i 为 $\bar{h}_i$ 关于 $\mathfrak{z}$ 的相对巡回率为 P^{m_i},$(i=1,2,\cdots,r)$,故有

$$TW \equiv WT \equiv E \pmod{M} \tag{8}$$

而 E 为 $\mathfrak{M}_{2r}$ 中主方阵(unit matrix).于是 $TWP \equiv WTP \equiv P \pmod{MP}$,但 $MP \equiv O \pmod{p^m}$,O 为 $\mathfrak{M}_{2r}$ 中的零方阵,故有

$$TWP \equiv WTP \equiv P \pmod{p^m}. \tag{9}$$

群 $\mathfrak{G}$ 中两组底间的变换可由(3)式中方阵 T 表示之,今求得 T 的充分与必要条件如次:

定理3 若(3)式中方阵 T 表示群 $\mathfrak{G}$ 之两组间的变换,则其充分与必要条件为

$$TPT^{\sigma} \equiv P \pmod{p^m}$$

T,P 如(4),(6)所定义 $T \to T^0$ 如(3.2)所定义

证:应用底之性质,由(1)得

$$(h_i, g_j) = (h_i, \bar{h}_i^{\beta ij}) = t^{p^{m-m_i}\beta ji}, \qquad (h_i, \bar{g}_j) = (h_i, \bar{h}_i^{\delta_{ji}}) = t^{p^{m-m_i}\delta ji}$$

$$(\bar{h}_i, g_j) = (\bar{h}_i, h_i^{a_{ij}}) = t^{-p^{m-m_i}aji}, \qquad (\bar{h}_i, \bar{g}_j) = (\bar{h}_i, h_i^{\gamma_{ji}}) = t^{p^{m-m_i}\gamma ji} \tag{10}$$

$$(g_i, h_j) = (g_i, \bar{g}_i^{b_{ji}}) = t^{p^{m-m_i}bji}, \qquad (g_i, \bar{h}_j) = (g_i, \bar{g}_i^{d_{ji}}) = t^{p^{m-m_i}cji}$$

$$(\bar{g}_i, h_j) = (\bar{g}_i, g_i^{a_{ij}}) = t^{-p^{m-m_i}aji}, \qquad (\bar{g}_i, \bar{h}_j) = (\bar{g}_i, \bar{g}_i^{c_{ij}}) = t^{p^{m-m_i}cji}$$

(10)对于任意 $i,j=1,2,\cdots,r$ 均为真,故有

$$(h_j, g_i) = t^{p^{m-m_j}\beta ij} = (h_i, g_j)^{-1} = t^{-p^{m-m_i}bji}$$

$$(\bar{h}_j, g_i) = t^{-p^{m-m_j}aij} = (g_i, \bar{h}_j)^{-1} = t^{p^{m-m_i}dji}$$

$$(i,j=1,2,\cdots,r)$$

$$(h_j, \bar{g}_i) = t^{p^{m-m_j}\delta ij} = (\bar{g}_i, h_j)^{-1} = t^{p^{m-m_i}aji}$$

$$(\bar{h}_j, \bar{g}_i) = t^{-p^{m-m_j}\delta ij} = (\bar{g}_i, \bar{h}_j)^{-1} = t^{p^{m-m_i}cji}$$

于是有 $p^{m-m_j}\beta_{ij} \equiv -p^{m-m_i}b_{ji} \pmod{p^m}$

$$p^{m-m_j}\alpha_{ij} \equiv p^{m-m_i}d_{ji} \pmod{p^m} \tag{11}$$

$$(i,j=1,2,\cdots,r)$$

$$p^{m-m_j}\delta_{ij} \equiv p^{m-m_i}a_{ji} \pmod{p^m}$$

$$p^{m-mj}\gamma_{ij} \equiv -p^{m-m_i}c_{ji} \quad (\mathrm{mod}\, p^m)$$

又因

$$(WP)_{ij} = \sum_{k=1}^{r} W_{ik}P_{kj} = W_{ij}P_{jj} = \begin{pmatrix} a_{ij} & \beta^{ij} \\ \gamma_{ij} & \delta_{ij} \end{pmatrix}\begin{pmatrix} P^{m-mj} & 0 \\ 0 & P^{m-m_j} \end{pmatrix}$$

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

$$(PT^{\theta})_{ij} = \sum_{k=1}^{r} P_{ik}(T^{\theta})_{ij} = P_{ii}(T^{\theta})_{ij} = P_{ii}T^{\sigma}_{ij}$$

$$= \begin{pmatrix} P^{m-mi} & 0 \\ 0 & P^{m-mi} \end{pmatrix}\begin{pmatrix} d_{ji} & -b_{ji} \\ -C_{ji} & a_{ji} \end{pmatrix}$$

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

故(11)可写为 $(WP)_{ij} \equiv (PT^{\theta})_{ij}(\mathrm{mod}\, p^m)$，$(i, j = 1, 2, \cdots, r)$，于是 $WP \equiv PT^{\theta}(\mathrm{mod}\, p^m)$，$TWP \equiv TPT^{\theta}(\mathrm{mod}\, p^m)$，按(9)，$TWP \equiv P(\mathrm{mod}\, p^m)$，故得

$$TWP^{\theta} \equiv P \quad (\mathrm{mod}\, p^m) \tag{12}$$

以下证(12)亦为充分条件。

由(12)，$TPT^{\theta}W^{\theta} \equiv PW^{\theta} \quad (\mathrm{mod}\, p^m)$；但 $P^{\theta} = P$，$PT^{\theta}W^{\theta} = P^{\theta}(WT)^{\theta} = (WTP)^{\theta}$，按(9) $WTP \equiv P \quad (\mathrm{mod}\, p^m)$；故得 $TP \equiv PW^{\theta} \quad (\mathrm{mod}\, p^m)$；由(6)(7)的定义知 $\bar{P}P \equiv O(\mathrm{mod}\, p^m)$；故得 $\bar{P}TP \equiv \bar{P}PW^{\theta} \equiv O(\mathrm{mod}\, p^m)$. 又

$$(PTP)_{ij} = \sum_{\lambda=1}^{r}\sum_{\mu=1}^{r}(\bar{P})_{i\lambda}(T)_{\lambda u}(P^0)_{uj} = \overline{P}_{ii}(T)_{ij}(p)_{jj}$$

$$= \begin{pmatrix} P^{mi} & 0 \\ 0 & P^{mi} \end{pmatrix}\begin{pmatrix} a_{ij} & b_{ij} \\ c_{ij} & P_{mij} \end{pmatrix}\begin{pmatrix} p^{m-mj} & 0 \\ 0 & p^{m-mj} \end{pmatrix}$$

$$= \begin{pmatrix} P^{m+m_i-m_j}aij & P^{m+m_i-m_j}b_{ij} \\ P^{m+m_i-m_j}cij & P^{m+m_i-m_j}d_{ij} \end{pmatrix}$$

所以

$$\begin{pmatrix} P^{m+mi-mj}a_{ij} & P^{m+mi-mj}b_{ij} \\ P^{m+mi-mj}c_{ij} & P^{m+mi-mj}d_{ij} \end{pmatrix} \equiv \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \quad (\mathrm{mod}\, p^m)$$

$$\begin{pmatrix} p^{mi}a_{ij} & p^{mi}b_{ij} \\ p^{mi}c_{ij} & p^{mi}d_{ij} \end{pmatrix} \equiv \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \quad (\mathrm{mod}\, p^{mj}) \qquad (i, j = 1, 2, \cdots, r). \tag{13}$$

又 $$(TPT^{\theta})_{ij}=\sum_{\lambda=1}^{r}\sum_{u=1}^{r}(T)_{i\lambda}(P)_{\lambda\mu}(T^{\theta})_{\mu j}=\sum_{s=1}^{r}(T)_{is}(P)_{ss}(T^{\theta})_{sj}$$

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

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

由(1)与定理 1 知

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

$$=\prod_{s=1}^{r}t^{pm-m_s}\begin{vmatrix}a_{is}&b_{is}\\c_{js}&d_{js}\end{vmatrix}=t_{s=1}^{\sum r}p^{m-mi}\begin{vmatrix}a_{is}&b_{is}\\c_{js}&d_{js}\end{vmatrix}\qquad(1,2,\cdots,r)$$

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

$$=\prod_{s=1}^{r}t^{pm-m_s}\begin{vmatrix}a_{is}&b_{is}\\a_{js}&b_{js}\end{vmatrix}=t_{s=1}^{\sum r}p^{m-m_s}\begin{vmatrix}a_{is}&b_{is}\\a_{js}&b_{js}\end{vmatrix}\qquad(i,j=1,2,\cdots,r)$$

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

$$=\prod_{s=1}^{r}t^{pm-m_s}\begin{vmatrix}c_{is}&d_{is}\\c_{js}&d_{js}\end{vmatrix}=t_{s=1}^{\sum r}p^{m-m}s\begin{vmatrix}c_{is}&d_{is}\\c_{js}&d_{js}\end{vmatrix}\qquad(i,j=1,$$

$2,\cdots,r)$

当 $TPT^{\theta}\equiv P(\mathrm{mod}p^m)$，比较(14)，(15)则得$(h_i,h_j)=(h_i,\bar{h}_j)=(\bar{h}_i,h_j)=(\bar{h}_i,\bar{h}_j)=e$，当 $i\neq j$ 时。$(h_i,\bar{h}_j)=t^{pm-m_i}$，$(i,j=1,2,\cdots,r)$.

又 h_λ 与 $\bar{h}_\lambda$ 关于 $\mathfrak{z}$ 的相对巡回率均为 P^{m_λ}，$(\lambda=1,2,\cdots,r)$.因按(1.7)知

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

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

当 $x=p^{m\lambda}$，按(13)$\begin{pmatrix}P^{m\lambda}a\lambda j&P^{m\lambda}b\lambda j\\P^{m\lambda}c\lambda j&P^{m\lambda}d\lambda j\end{pmatrix}\equiv\begin{pmatrix}0&0\\0&0\end{pmatrix}$ $(\mathrm{mod}p^{mj},(j=1,2,$ $\cdots,r)$，所以 $h_\lambda^{pm\lambda}\in\mathfrak{z}$，$\bar{h}_\lambda^{pm\lambda}\in\mathfrak{z}$，$(\lambda=1,2,\cdots,r)$。另一方面，因$(h_\lambda,\bar{h}_\lambda)=$

$t^{p^m-m^\lambda}$，设 $h_\lambda^x\varepsilon\mathfrak{z}$，则$(h_\lambda^x,\bar{h}_\lambda)=e=t^{p^m-m\lambda x}$，于是 $t^{p^m-m^\lambda}x\equiv 0(\mathrm{mod}p^m)$，于是 $x\equiv 0(\mathrm{mod}p^{m^\lambda})$，所以 h_λ 关于 $\mathfrak{z}$ 的相对巡回率为 p^{m^λ}，同样可证 $\bar{h}_\lambda$ 关于 $\mathfrak{z}$ 的相对巡回率亦为 p^{m^λ}。

在(3)中 $g_1,\bar{g}_1,\cdots,g_r,\bar{g}_r$ 为一组底，当 $TPT^\theta\equiv P(\mathrm{mod}p^m)$，已证当 $i\neq j(h_i,h_j)=(h_i,\bar{h}_j)=(\bar{h}_i,h_j)=(h_i,h_j)=e,(h_i,\bar{h}_j)=t^{p^m-m_i},h_i$，及 $\bar{h}_i$ 关于 $\mathfrak{z}$ 的相对巡回率为 $P^{mi}(i=1,2,..,r)$. 故 $h_1,\bar{h}_1,\cdots,h_r,\bar{h}_r$ 亦为群 $\mathfrak{E}$ 的一组底。

定理4 设 $\mathfrak{M}_{2r}$ 中方阵 T 表示群 $\mathfrak{E}$ 中两组底间的一变换，$TPT^\theta\equiv P(\mathrm{mod}p^m)$，则此等方阵的集合 $\mathfrak{N}$，依方阵的乘法结合关于 mod M 构成一群，方阵 M 如(5)所定义，方阵 P 如(6)所定义。

证：S,T 为 $\mathfrak{M}_{2r}$ 中方阵，若 $TPT^\theta\equiv P(\mathrm{mod}\ p^m)$，$SPS^\theta P\equiv(\mathrm{mod}\ p^m)$，则 $STP(ST)^\theta=STPT^\theta S^\theta\equiv SPS^\theta\equiv P(\mathrm{mod}\ p^m)$，故 $\mathfrak{N}$ 满足群的闭合律，又由(8)已知 $TW\equiv WT\equiv E(\mathrm{mod}\ M)$，按(11)，$WP\equiv PT^\theta P(\mathrm{mod}\ p^m)$，所以 $WPW^\theta\equiv PT^\theta W^\theta(\mathrm{mod}p^m)$，而 $PT^\theta W^\theta=P^\theta(WT)^\theta=(WTP)^\theta$，$WTP\equiv P(\mathrm{mod}\ MP)$，$MP\equiv O(\mathrm{mod}p^m)$，所以 $WPW^\theta\equiv P(\mathrm{mod}p^m)$。又 $EPE^\theta\equiv P(\mathrm{mod}p^m)$，所以对 $\mathfrak{N}$ 中任元系 T 有一逆元素及单位元素，组合律对于方阵乘法当然满足，所以 $\mathfrak{N}$ 为一群。*

On p-groups with cyclic commutator subgroup belonging to the center

LIU Shenglie

Let $\mathfrak{E}$ be a p - group of order p^n, its commutator group $D(\mathfrak{E})$ being cyclic and belonging to the center $\mathfrak{z}$, of $\mathfrak{E}$, Suppose that the order of $D(\mathfrak{E})$ is P^m, and $D(\mathfrak{E})=(t)$ where t is a enerating element of $D(\mathfrak{E})$. It is proved that the factor group $\mathfrak{E}/\mathfrak{z}=\mathfrak{F}$ is an Abelian group of type $\{p^{m_1},p^{m_1},p^{m_2},p^{m_2},\cdots,p^{m_r},$

* 注释：1)本文审查者指出若应用阿倍尔群基础定理于因子群 $\mathfrak{E}/\mathfrak{z}$，则可推得定理 1,2 之一简捷的证法。

$P^{m_r}\}$, where $m = m_1 \geqq m_2 \geqq \cdots \geqq m_r$. The order of $\mathfrak{F}$ is p^{2r}, $r = m_1 + m_2 + m_r$. $\mathfrak{E}$ is the product of its subgroups $\mathfrak{E}_1, \mathfrak{E}_2, \cdots \mathfrak{E}_r$.

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

When $i \neq j$, elements of $\mathfrak{E}_i$ commute with elements of $\mathfrak{E}_i$ and $\mathfrak{E}_i \cap \mathfrak{E}_j = \mathfrak{d}$. The group $\mathfrak{E}_i (i = 1, 2, \cdots, r)$ is defined as

$\mathfrak{E}_i = (g_i, \bar{g}_i, \mathfrak{d})$. $g_i^{p^{m_i}} = u\varepsilon\mathfrak{d}$, $\bar{g}_i^{p^{m_i}} = u\varepsilon\mathfrak{d}$, the commutator of $\bar{g}_i$ and $g_i = t^{p^{m-m_i}}$. Any element X of $\mathfrak{E}$ can be uniquely represented as

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

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

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 $TPT^{\theta} \equiv P \pmod{p^m}$, whtere $P = \mathrm{diag}\{p^{m-m_1}, p^{m-m_1}, \cdots p^{m-m_2}, p^{m-m_2}, p^{m-m_r}, p^{m-m_r}\}$, and θ be a transformation

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

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 forms a group.

试读结束，需要全本PDF请购买 www.ertongbook.com