现代数学基础丛书 169

有限p群构造

（下 册）

张勤海 安立坚 著

科学出版社

现代数学基础丛书 169

有限 p 群构造

（下　册）

张勤海　安立坚　著

科学出版社

北京

内 容 简 介

全书分上下册出版. 下册介绍我国学者在交换性较强和正规性较强的 p 群的结构、临界 p 群及 p 群其他方面的成果.

本书供高等院校数学专业群论研究生及有关研究人员阅读, 也可供数学史研究人员参考.

图书在版编目（CIP）数据

有限 p 群构造. 下册/张勤海, 安立坚著. —北京: 科学出版社, 2017.5
(现代数学基础丛书; 169)
ISBN 978-7-03-052831-5

Ⅰ. ①有… Ⅱ. ①张… ②安… Ⅲ. ①有限群 Ⅳ. ①O152.1

中国版本图书馆 CIP 数据核字 (2017) 第 107947 号

责任编辑: 李静科 / 责任校对: 张凤琴
责任印制: 张 伟 / 封面设计: 陈 敬

科学出版社 出版
北京东黄城根北街 16 号
邮政编码: 100717
http://www.sciencep.com

北京教图印刷有限公司 印刷
科学出版社发行 各地新华书店经销
*
2017 年 5 月第 一 版 开本: 720×1000 1/16
2017 年 5 月第一次印刷 印张: 23 3/4
字数: 460 000

定价: 139.00 元

(如有印装质量问题, 我社负责调换)

《现代数学基础丛书》序

对于数学研究与培养青年数学人才而言, 书籍与期刊起着特殊重要的作用. 许多成就卓越的数学家在青年时代都曾钻研或参考过一些优秀书籍, 从中汲取营养, 获得教益.

20 世纪 70 年代后期, 我国的数学研究与数学书刊的出版由于文化大革命的浩劫已经破坏与中断了 10 余年, 而在这期间国际上数学研究却在迅猛地发展着. 1978 年以后, 我国青年学子重新获得了学习、钻研与深造的机会. 当时他们的参考书籍大多还是 50 年代甚至更早期的著述. 据此, 科学出版社陆续推出了多套数学丛书, 其中《纯粹数学与应用数学专著》丛书与《现代数学基础丛书》更为突出, 前者出版约 40 卷, 后者则逾 80 卷. 它们质量甚高, 影响颇大, 对我国数学研究、交流与人才培养发挥了显著效用.

《现代数学基础丛书》的宗旨是面向大学数学专业的高年级学生、研究生以及青年学者, 针对一些重要的数学领域与研究方向, 作较系统的介绍. 既注意该领域的基础知识, 又反映其新发展, 力求深入浅出, 简明扼要, 注重创新.

近年来, 数学在各门科学、高新技术、经济、管理等方面取得了更加广泛与深入的应用, 还形成了一些交叉学科. 我们希望这套丛书的内容由基础数学拓展到应用数学、计算数学以及数学交叉学科的各个领域.

这套丛书得到了许多数学家长期的大力支持, 编辑人员也为其付出了艰辛的劳动. 它获得了广大读者的喜爱. 我们诚挚地希望大家更加关心与支持它的发展, 使它越办越好, 为我国数学研究与教育水平的进一步提高做出贡献.

杨 乐

2003 年 8 月

前　言

本书分上下两册. 上册介绍了有限 p 群的基本理论和方法、我国学者在 p 群领域的早期工作、p 群的计数以及交换性较强的几类重要 p 群的分类. 下册分 5 章.

第 10 章继续从不同的角度研究交换性 "较强" 的有限 p 群. 我们观察到, 内交换 p 群的导群的阶是 p, 反之不然. 另外, 内交换 p 群的真子群的导群是平凡的. 由这些观察出发, 导群 p 阶的 p 群、二元生成导群循环的 p 群、真子群的导群的阶不超过 p 的 p 群等被研究和分类. 另外, 对于非交换 p 群, 考虑非交换元生成 p^3, p^4 阶的内交换子群、非交换子群的中心均相等等条件, 这样的 p 群也被分类. 本章介绍这些结果.

第 11 章介绍正规性 "较强" 的有限 p 群. 研究正规性 "较强" 的 p 群, 人们主要从以下三个角度考虑: 一是对非正规子群加以某种限制. 这方面的一个重要结果是 Passman 给出的非正规子群均循环的 p 群的分类. 之后, 非正规子群均同阶、非正规子群的阶不超过 p^2, p^3 的 p 群分别被分类. 二是对非正规子群的正规闭包加以某种限制, 例如, 非正规子群的正规闭包均同阶、非正规子群的正规闭包均包含导群、非正规子群的正规闭包较小等, 这样的 p 群也被研究和分类. 三是研究非正规子群的正规化子较小的 p 群. 再就是弱化正规性条件, 例如, 每个子群为共轭置换子群、TI 子群的 p 群分别被研究和分类. 另外, 还有 Hamilton p 群的其他一些推广. 本章介绍这方面的结果.

第 12 章专门介绍亚 Hamilton p 群的分类. 所谓亚 Hamilton p 群, 就是子群或交换或正规的非交换有限 p 群. 容易看出, Hamilton p 群、内交换 p 群及前几章介绍的 $\mathcal{A}_2$ 群、非正规子群均循环的 p 群、非正规子群的阶不超过 p^2 的 p 群等均是亚 Hamilton p 群. 因而它既可看作交换性较强, 也可看作正规性较强的非交换 p 群. 分类亚 Hamilton p 群也是 p 群中的一个老问题. 安立坚在其北京大学博士学位论文中彻底完成了其同构分类. 本章给予专门介绍.

第 13 章介绍几类临界 p 群的分类. 所谓临界群就是群 G 本身不具有性质 $\mathcal{P}$, 但它的每个真子群 (真商群、截段) 具有性质 $\mathcal{P}$ 的群. 当 G 为 p 群时, 也称之为临界 p 群. 例如, 内交换 p 群、内亚循环 p 群、极小非正则 p 群等都是临界 p 群. 本章介绍另外三类临界 p 群的分类, 即极小非 3 交换 3 群、极小非 $\mathcal{P}_2$-p 群以及内 $\mathcal{P}_2$-p 群. p 交换 p 群是有限 p 群中 "接近" 交换群的一个重要群类. 例如, 当 $p=2$ 时, 2 交换 2 群即为交换群. 另外, 幂零类为 1 的群恰是交换群. 因而幂零类为 2 的 p 群也可看作是 "接近" 交换群的 p 群. 显然, 内类 2 的 p 群的分类可看作是内交

换 p 群分类的一个自然的、较大的推广.

第 14 章介绍我国学者在 p 群其他方面取得的结果. 我们知道, p 群有太多问题是未知的, 从不同角度探索 p 群结构是有益的. 本章的内容主要有 p 群的幂结构、余次数、特征标的核、子群交、Wielandt 子群等问题的研究结果, 以及拟 NC 群、平衡 p 群、自对偶 p 群、特殊类型的 p 群、子群具有某种特定性质的 p 群的分类等结果的介绍.

本书是为具有 p 群初等知识的读者编写的, 在 p 群知识上力图做到自包含. 另外, 对于不以英文发表的文献或不易找到的文献, 都列出了它在 MathSciNet 数据库中的编号, 以方便读者查阅该文的摘要. 再者, 在引用前述结果时, 都按章节统一编号. 例如, 命题 1.1.3 指的是第 1 章第 1 节的第 3 个命题.

由于作者水平有限, 缺陷与不足之处在所难免, 热忱欢迎读者批评指正.

张勤海　安立坚

2016 年 9 月于山西师范大学

目　　录

第 10 章　交换性较强的有限 p 群

前面看到, 最接近交换群的非交换群自然是内交换群, 也称为 $\mathcal{A}_1$ 群. 研究比 $\mathcal{A}_1$ 群类更大的群类被许多群论学家关注, 并取得了基础性的结果. 例如, $\mathcal{A}_2$ 群、$\mathcal{A}_3$ 群的同构分类, 以及具有一个内交换极大子群的 p 群的分类等. 除此之外, 从其他的角度研究内交换群类的推广也有许多成果, 例如, 文献 [1], [35], [36], [182] 研究导群 p 阶的 p 群. 文献 [202], [218] 研究了导群是 (p,p) 型的 p 群. 导群循环的有限 p 群的研究在文献上也可以找到很多论文, 参见 [48], [49], [63], [81], [120], [158], [219] 等. 值得一提的是, Miech[158] 在 1975 年给出了二元生成、导群循环的有限 p 群 $(p>2)$ 的完全分类. 但他使用了过多的参数, 不太好应用. 2013 年, 宋蔷薇在 [209] 中使用文献 [242] 描述的方法, 对这类群重新给出了分类. 该分类比 Miech 在 [158] 给出的分类简单. 对于 $p=2$ 的情形, 这个问题仍未解决. 注意到内交换群的真子群的导群是平凡的. 黎先华等[256, 257] 研究每个真子群的导群均较小的 p 群. Janko 在文献 [102], [104], [106] 中进一步减弱文献 [256] 的条件, 得到了这些 p 群结构的描述. 张勤海等[265] 进一步研究真子群亚循环或真子群的导群的阶不超过 p 的 p 群. 安立坚等[7]、张勤海等[274] 则从两个非交换元生成较小阶的内交换群的角度研究交换性较强的 p 群. 总之, 研究交换性较强或较好的 p 群是 p 群领域的活跃课题. 本节介绍该领域的有关结果.

10.1　导群 p 阶的 p 群

导群 p 阶的有限 p 群的结构可由中心积描述.

引理 10.1.1　设 G 是有限 p 群且 $|G'|=p$, H 是 G 的内交换子群. 则 $G=H*C_G(H)$.

证明　由定理 1.7.7 可知 $d(H)=2$. 不妨设 $H=\langle a,b\rangle$. 则 $C_G(H)=C_G(a)\bigcap C_G(b)$. 考虑 a 在 G 中的共轭类, 则

$$a^G=\{a^g \mid g\in G\}=\{a[a,g] \mid g\in G\}\subseteq aG'.$$

因为 $|G'|=p$, 故 $|a^G|\leqslant p$. 从而 $|a^G|=p$, 即 $|G:C_G(a)|=p$. 同理 $|G:C_G(b)|=p$. 于是 $|G:C_G(H)|=p^2$. 现在有

$$|HC_G(H)|=\frac{|H||C_G(H)|}{|H\bigcap C_G(H)|}=\frac{|H||C_G(H)|}{|Z(H)|}.$$

因为 H 内交换, 再由定理 1.7.7 可知 $|H:Z(H)|=p^2$. 于是 $|HC_G(H)|=|G|$. □

定理 10.1.2　设 G 是有限 p 群且 $|G'|=p$. 则

(1) 存在 G 的内交换子群 $A_1,A_2,\cdots,A_s$ 使得 $G=(A_1*A_2*\cdots*A_s)Z(G)$;

(2) $G/Z(G)$ 是 p^{2s} 阶的初等交换群, 记为 $\mathrm{E}_{p^{2s}}$;

(3) 若 G/G' 初等交换, 则对 $1\leqslant i\leqslant s$ 均有 $|A_i|=p^3$, $A_1*A_2*\cdots*A_s$ 为超特殊 p 群.

证明　(1) 对 G 作归纳. 设 A_1 是 G 的内交换子群. 由引理 10.1.1, 即得 $G=A_1*C_G(A_1)$. 令 $C=C_G(A_1)$. 若 C 交换, 则 $G=A_1Z(G)$. 若 C 不交换, 则 $|C'|=p$. 由归纳假设, 对于群 C 定理成立. 不妨设

$$C=(A_2*A_3*\cdots*A_s)Z(C),$$

其中 $A_2,A_3,\cdots,A_s$ 是内交换子群. 明显地, $Z(C)=Z(G)$.

(2) 对 s 进行归纳. 当 $s=1$ 时, $G=A_1Z(G)$. 于是

$$G/Z(G)=A_1Z(G)/Z(G)\cong A_1/(A_1\bigcap Z(G))=A_1/Z(A_1)=A_1/\Phi(A_1)\cong \mathrm{E}_{p^2}.$$

结论成立. 当 $s\geqslant 2$ 时, 设 $G=A_1*N_1$, 其中 $N_1=(A_2*\cdots*A_s)Z(G)$. 下证

$$G/Z(G)=A_1Z(G)/Z(G)\times N_1/Z(G).$$

因为 $Z(G)=Z(N_1)$, 由归纳假设可知

$$N_1/Z(N_1)=N_1/Z(G)\cong \mathrm{E}_{p^{2(s-1)}}.$$

又因为 $Z(G)=Z(N_1)\leqslant N_1$, 由模律可得 $A_1Z(G)\bigcap N_1=(A_1\bigcap N_1)Z(G)$. 又 $A_1\bigcap N_1\leqslant Z(G)$, 于是 $A_1Z(G)\bigcap N_1\leqslant Z(G)$. 从而

$$G/Z(G)=A_1Z(G)/Z(G)\times N_1/Z(G)\cong \mathrm{E}_{p^2}\times \mathrm{E}_{p^{2(s-1)}}\cong \mathrm{E}_{p^{2s}}.$$

(3) 由于 $1\neq A_i'\leqslant G'$, 故 $G'=A_i'$ 对所有的 $1\leqslant i\leqslant s$. 又 G/G' 初等交换, 故

$$A_iG'/G'\cong A_i/G'\bigcap A_i=A_i/A_i'$$

初等交换. 从而 $\Phi(A_i)=A_i'$. 因为 $d(A_i)=2$, 于是 $|A_i/\Phi(A_i)|=p^2$. 由此可得 $|A_i|=p^3$ 对所有的 $1\leqslant i\leqslant s$.

令 $K=A_1*A_2*\cdots*A_s$, 其中 $A_i=\langle a_i,b_i\rangle$. 由归纳法可证

$$K/G'=\langle\bar{a}_1\rangle\times\langle\bar{b}_1\rangle\times\langle\bar{a}_2\rangle\times\langle\bar{b}_2\rangle\times\cdots\times\langle\bar{a}_s\rangle\times\langle\bar{b}_s\rangle,$$

任取 $k \in K$, 则

$$\bar{k} = \bar{a}_1^{x_1}\bar{b}_1^{y_1}\bar{a}_2^{x_2}\bar{b}_2^{y_2}\cdots\bar{a}_s^{x_s}\bar{b}_s^{y_s}.$$

因为 K/G' 初等交换, 故 $0 \leqslant x_i, y_i \leqslant p-1$. 从而存在 $z \in G'$ 使得

$$k = a_1^{x_1}b_1^{y_1}a_2^{x_2}b_2^{y_2}\cdots a_s^{x_s}b_s^{y_s}z.$$

由于 $K = A_1 * A_2 * \cdots * A_s$ 是中心积, 故 $[k, a_i] = [b_i^{y_i}, a_i]$ 且 $[k, b_i] = [a_i^{x_i}, b_i]$. 显然, 对于 $1 \leqslant x_i, y_i \leqslant p-1$, 有

$$A_i = \langle a_i, b_i\rangle = \langle a_i^{x_i}, b_i\rangle = \langle a_i, b_i^{y_i}\rangle$$

内交换. 故 $1 \neq [a_i, b_i] = [b_i^{y_i}, a_i] = [a_i, b_i^{y_i}]$. 由此可得 $\forall i$, $[k, a_i] = 1 \Leftrightarrow y_i = 0$ 和 $[k, b_i] = 1 \Leftrightarrow x_i = 0$. 由此进一步可得, $k \in Z(K)$ 当且仅当 $x_i = y_i = 0, \forall i$. 故 $k = z \in G'$. 所以 $Z(K) \leqslant G'$. 因为 $1 < |Z(K)|$, 所以 $Z(K) = G'$. 由 (1) 可知, $Z(G) = Z(K)$. 显然 $G' = K'$. 另一方面, $\Phi(K) \leqslant \Phi(G)$. 由 G/G' 初等交换得 $\Phi(G) = G'$. 故 $\Phi(K) = K'$. 由此可知 $Z(K) = \Phi(K) = K'$ 且阶为 p. 故 $K = A_1 * A_2 * \cdots * A_s$ 是超特殊 p 群. □

注 张勤海等在文献 [272] 给出了超特殊 p 群的三个等价性质.

10.2 二元生成导群循环的 p 群

本节介绍文献 [209] 获得的导群循环二元生成的有限 p 群 ($p > 2$) 的分类结果.

命题 10.2.1 *设 G 是有限正则 p 群, $H \trianglelefteq G$. 则 $\omega(G/H) + \omega(H) \geqslant \omega(G)$.*

证明 因为

$$|G/\mho_1(G)| = p^{\omega(G)}, \quad p^{\omega(G/H)} = |(G/H)/\mho_1(G/H)| = |G/\mho_1(G)H|,$$

有 $|\mho_1(G)H/\mho_1(G)| = p^{\omega(G)-\omega(G/H)}$. 注意到

$$\mho_1(G)H/\mho_1(G) \cong H/\mho_1(G)\bigcap H, \quad \mho_1(H) \leqslant \mho_1(G)\bigcap H.$$

由此可得

$$p^{\omega(G)-\omega(G/H)} = |\mho_1(G)H/\mho_1(G)| = |H/\mho_1(G)\bigcap H| \leqslant |H/\mho_1(H)| = p^{\omega(H)}.$$

因而 $\omega(G) - \omega(G/H) \leqslant \omega(H)$. 故 $\omega(G/H) + \omega(H) \geqslant \omega(G)$. □

定理 10.2.2 *设 G 为二元生成的有限 p 群, G' 循环, p 为奇素数. 则 G 正则且 $\omega(G) \leqslant 3$.*

证明　由于 $p>2$ 且 G' 循环, 因此由定理 1.11.4(3) 可知, G 正则. 进一步, 由于 G' 循环, 因此 $G''=1$. 故 $\Phi(G')=\mho_1(G')$. 因而

$$p^{\omega(G')}=|G'/\mho_1(G')|=|G'/\Phi(G')|=p.$$

故 $\omega(G')=1$. 接下来, 因为

$$p^{\omega(G/G')}=|G/G'/\mho_1(G/G')|=|G/\mho_1(G)G'|=|G/\Phi(G)|=p^2,$$

所以 $\omega(G/G')=2$. 因而由命题 10.2.1 知, $\omega(G)\leqslant\omega(G')+\omega(G/G')=3$. □

由于 $d(G)=2$ 且 $d(G)\leqslant\omega(G)$, 因此 $\omega(G)=2$ 或 3. 若 $\omega(G)=2$, 由定理 7.2.1 可知 G 亚循环. 而亚循环 p 群已被分类. 故下面仅考虑 $\omega(G)=3$ 的情形. 因为 G 正则且 $p^3=p^{\omega(G)}=|G/\mho_1(G)|$, 因此可设 G 的型不变量为 (n,m,r). 显然, $\exp(G)=p^n$ 且 $n\geqslant m\geqslant r$. 任取 G 的一个 L 群列

$$G=L_0(G)>L_1(G)>L_2(G)>L_3(G)=\mho_1(G).$$

由于 $|G/L_2(G)|=p^2$, 因此 $G'\leqslant L_2(G)$. 显然 $\mho_1(G)\leqslant L_2(G)$. 故 $\Phi(G)\leqslant L_2(G)$. 又因 $d(G)=2$, 所以 $|G/\Phi(G)|=p^2$. 故总可假设 $L_2(G)=\Phi(G)$.

取 $a\in L_0(G)\backslash L_1(G)$, $b\in L_1(G)\backslash L_2(G)$, $d\in L_2(G)\backslash L_3(G)$ 且为最小阶元素. 由定理 4.2.17 可知, (a,b,d) 为一组唯一性基底, 其中 $o(a)=p^n$, $o(b)=p^m$, $o(d)=p^r$ 且 $G=\langle a,b\rangle$. 由于 G' 循环, 因此总可假设 $G'=\langle c\rangle$ 且 $o(c)=p^u$. 容易证明 $c\in L_2(G)\backslash L_3(G)$. 由于 $G'=\langle c\rangle=\langle[a,b]\rangle$ 且 G 正则, 由定理 1.11.5(5) 可知 $u\leqslant m$. 故 $n\geqslant m\geqslant u\geqslant r$.

下面分 $u=r$ 和 $u>r$ 两种情形对导群循环二元生成的有限 p 群进行分类.

先看 $u=r$ 的情形.

定理 10.2.3　*设 G 为二元生成导群循环的奇阶有限 p 群, 且设 G 的型不变量为 (n,m,r), $|G'|=p^r$. 则*

$$G=\langle a,b,c\mid a^{p^n}=b^{p^m}=c^{p^r}=1,[a,b]=c,[c,a]=c^{p^s},[c,b]=c^{p^t}\rangle,$$

其中 n,m,r,s,t 为正整数, $r\leqslant m\leqslant n$, $s\leqslant t=r$ 或者 $r\leqslant m<n$, $s\leqslant t<\min\{r,n-m+s\}$, 且对于参数 n,m,r,s,t 的不同取值, 对应的群互不同构.

证明　注意到 $|G'|=p^r$, 因此 (a,b,c) 为 G 的一组唯一性基底. 显然

$$\langle a\rangle\bigcap\langle b\rangle=\langle a\rangle\bigcap\langle c\rangle=\langle b\rangle\bigcap\langle c\rangle=1.$$

考虑群 $\langle a,c\rangle$ 和 $\langle b,c\rangle$. 因为 $\langle c\rangle\trianglelefteq G$, 所以 $\langle a,c\rangle$, $\langle b,c\rangle$ 均为亚循环 p 群. 由定理 2.1.6, 分别用 a, b 的适当方幂替换 a,b 可得

$$a^{p^n}=b^{p^m}=c^{p^r}=1,\quad a^{-1}ca=c^{1+p^s},\quad b^{-1}cb=c^{1+p^t},$$

其中 n,m,r,s,t 为正整数且 $s,t\leqslant r$. 由于 $G'=\langle[a,b]\rangle=\langle c\rangle$, 因此不妨设 $[a,b]=c$.

若 $s>t$, 由 [247] 中的引理 6.2.3 知, 可取适当的 i 并用 ab^i 替换 a 可得 $(ab^i)^{-1}c(ab^i)=c^{1+p^t}$. 进而总可设 $s\leqslant t$.

若 $\langle b,c\rangle$ 交换, 则可得定理中的群, 此为 $r\leqslant m\leqslant n$, $s\leqslant t=r$ 的情形. 若 $\langle b,c\rangle$ 非交换. 断言 $t<n-m+s$. 若否, 则 $t\geqslant n-m+s$. 由 [247] 中的引理 6.2.3 知, 可取适当的 i, 并用 $a^{ip^{n-m}}b$ 替换 b 可得

$$(a^{ip^{n-m}}b)^{-1}c(a^{ip^{n-m}}b)=c,\quad o(a^{ip^{n-m}}b)=p^m.$$

并且 $(a,a^{ip^{n-m}}b,c)$ 仍为 G 的一组唯一性基底. 由于 $s\leqslant t<n-m+s$, 因此 $n>m$. 从而可得定理中的群, 此为 $r\leqslant m<n$, $s\leqslant t<\min\{r,n-m+s\}$ 的情形.

下面将证明定理中所有参数均是 G 的不变量. 由于 G 的型不变量为 (n,m,r) 且 $|G_3|=p^{r-s}$, 因此 n,m,r,s 为不变量. 最后我们来证明 t 也是不变量. 显然只需考虑 $r\leqslant m<n$, $s\leqslant t<\min\{r,n-m+s\}$ 的情形. 不失一般性, 令

$$a_1=a^{i_1}b^{j_1}c^{k_1},\quad b_1=a^{i_2p^{n-m}}b^{j_2}c^{k_2},\quad c_1=[a_1,b_1],$$

其中 $p\nmid i_1j_2$. 经计算知 $b_1^{-1}c_1b_1=c_1^{(1+p^s)^{i_2p^{n-m}}(1+p^t)^{j_2}}$. 由于 $t<n-m+s$ 且 $p\nmid j_2$, 因此可记 $b_1^{-1}c_1b_1=c_1^{(1+wp^t)}$, 其中 $p\nmid w$. 故 t 是不变量.

综上可知, 参数 n,m,r,s,t 均为不变量. 因此, 对于参数 n,m,r,s,t 的不同取值, 对应的群互不同构.

最后, 利用循环扩张理论可以证明, 对于定理中得到的群而言, $|G|=p^{n+m+r}$, 并且通过计算可知 G' 循环且 G 的型不变量为 (n,m,r). □

下面处理 $u>r$ 的情形.

定理 10.2.4 设 G 为二元生成导群循环的奇阶有限 p 群, 其型不变量为 (n,m,r). 再设 $|G'|=p^u$. 则 G 同构于以下群之一, 这里 $n,m,u,r,s,t,\theta,i,\sigma$ 均为正整数.

(Ⅰ) $\langle a,b,c\mid a^{p^{n-u+r}}=c^{p^r},b^{p^m}=c^{p^u}=1,[a,b]=c,[c,a]=c^{p^s},[c,b]=1\rangle$, 其中 $r+1\leqslant u\leqslant m\leqslant n$, $u-r\leqslant s\leqslant u\leqslant n-u+r$.

(Ⅱ) $\langle a,b,c\mid a^{p^{n-u+r}}=c^{p^r},b^{p^m}=c^{p^u}=1,[a,b]=c^{\sigma},[c,a]=1,[c,b]=c^{p^t}\rangle$, 其中 $r+1\leqslant u\leqslant m\leqslant n$, $u-(r+m-\min\{m,n-u+r\})\leqslant t<u$, $p\nmid\sigma$ 且 $\sigma\leqslant\min\{p^{u-r},p^{u-t}\}$. 当 $n-u+r\geqslant u$ 时, $u-r\leqslant t$. 当 $n-u+r<u$ 时, $\sigma\equiv1(\mathrm{mod}\ p^{u-r-t})$ 且 $n-u=t$.

(Ⅲ) $\langle a,b,c\mid a^{p^{n-u+r}}=c^{p^r},b^{p^m}=c^{p^u}=1,[a,b]=c^{\sigma},[c,a]=c^{p^s},[c,b]=c^{p^t}\rangle$, 其中 $r+1\leqslant u\leqslant m\leqslant n$, $t<\min\{n-m+s,u\}$, $u-r\leqslant s<\min\{m-\min\{m,n-u+r\}+t,u\}$, $p\nmid\sigma$ 且 $\sigma\leqslant\min\{p^{u-r},p^{\min\{n-m+s,u\}-t}\}$. 当 $n-u+r\geqslant u$ 时, $u-r\leqslant t$. 当 $n-u+r<u$ 时, $\sigma\equiv1(\mathrm{mod}\ p^{u-r-t})$ 且 $n-u=t$.

(Ⅳ) $\langle a,b,c \mid a^{p^{n-u+r+\theta}}=c^{p^{r+\theta}}, b^{p^{m-\theta}}=c^{p^r}, c^{p^u}=1, [a,b]=c^{\sigma}, [c,a]=c^{p^s}, [c,b]=1\rangle$, 其中 $r+1\leqslant u\leqslant m<n-u+r+\theta$, $\theta\leqslant u-r$, $\theta<m-r$, $u-r-\theta\leqslant s\leqslant u$, $p\nmid\sigma$, $\sigma p^{m-\theta}+p^{r+s}\equiv 0(\mathrm{mod}\ p^u)$. 并且若 $n-u+r+\theta-m+\theta\geqslant u-s$, 则 $\sigma\leqslant\min\{p^{\theta},p^{u-s}\}$. 若 $n-u+r+\theta-m+\theta<u-s$, 则 $\sigma\leqslant\min\{p^{\theta+u-s-(n-u+r+\theta)+(m-\theta)},p^{u-r}\}$.

(Ⅴ) $\langle a,b,c \mid a^{p^{n-u+r+\theta}}=c^{p^{r+\theta}}, b^{p^{m-\theta}}=c^{p^r}, c^{p^u}=1, [a,b]=c^{\sigma}, [c,a]=1, [c,b]=c^{p^t}\rangle$, 其中 $r+1\leqslant u\leqslant m<n-u+r+\theta$, $\theta\leqslant\min\{u-r,m-u\}$, $u-r\leqslant t<u$, $p\nmid\sigma$ 且 $\sigma\leqslant\min\{p^{u-r-\theta},p^{u-t}\}$.

(Ⅵ) $\langle a,b,c \mid a^{p^{n-u+r+\theta}}=c^{ip^{r+\theta}}, b^{p^{m-\theta}}=c^{p^r}, c^{p^u}=1, [a,b]=c^{\sigma}, [c,a]=c^{p^s}, [c,b]=c^{p^t}\rangle$, 其中 $r+1\leqslant u\leqslant m<n-u+r+\theta$, $\theta\leqslant u-r$, $\theta<m-r$, $u-r-\theta\leqslant s<t$, $u-r\leqslant t<\min\{u,n-u+r+\theta-m+\theta+s\}$, $p\nmid i\sigma$, $\sigma p^{m-\theta}+p^{r+s}\equiv 0(\mathrm{mod}\ p^u)$, $\sigma\leqslant\min\{p^{\theta},p^{t-s}\}$ 并且 $i\leqslant\min\{p^{u-t},p^{u-r-\theta}\}$.

并且不同类型的群或者相同类型但不同参数的群互不同构.

证明　注意到, (a,b,d) 为 G 的一组唯一性基底且 $G'=\langle c\rangle$, $o(c)=p^u$ 其中 $u>r$. 因为 $\langle a\rangle\bigcap\langle b\rangle=1$, 断言 $\langle a\rangle\bigcap\langle c\rangle$, $\langle b\rangle\bigcap\langle c\rangle$ 中至少有一个为 1. 若否, 则可设

$$\langle a\rangle\bigcap\langle c\rangle=\langle c^{p^{\alpha}}\rangle,\quad \langle b\rangle\bigcap\langle c\rangle=\langle c^{p^{\beta}}\rangle.$$

故 $1\neq\langle c^{p^{\max\{\alpha,\beta\}}}\rangle\leqslant\langle a\rangle\bigcap\langle b\rangle$, 矛盾. 不妨设 $\langle b\rangle\bigcap\langle c\rangle=1$ 且 $\langle a\rangle\bigcap\langle c\rangle=\langle c^{p^{\alpha}}\rangle$. 则 $o(\bar{a})=p^{n-u+\alpha}$. 由于 $\langle b\rangle\bigcap\langle c\rangle=1$, 因此 $o(\bar{b})=p^m$. 设 $|\langle\bar{a}\rangle\bigcap\langle\bar{b}\rangle|=p^{\theta}$. 由于

$$p^{n+m+r}=|G|=|\overline{G}||G'|=\frac{p^{n-u+\alpha}p^m}{p^{\theta}}p^u=p^{n+m+\alpha-\theta},$$

因此 $\alpha=r+\theta$ 且 $o(\bar{a})=p^{n-u+r+\theta}$. 进而, 我们分以下两种情形讨论.

情形 1　总存在 G 的一组唯一性基底 (a,b,d) 使得 $\overline{G}=\langle\bar{a}\rangle\times\langle\bar{b}\rangle$, 即 $\theta=0$.

显然 $o(\bar{a})=p^{n-u+r}$, $o(\bar{b})=p^m$ 且 $\langle a^{p^{n-u+r}}\rangle=\langle c^{p^r}\rangle$. 由于 $\langle c\rangle\trianglelefteq G$, 因此 $\langle a,c\rangle$, $\langle b,c\rangle$ 均为亚循环 p 群. 由定理 2.1.6 知, 总可用 a, b 的适当方幂替换 a,b 可得

$$a^{p^{n-u+r}}=c^{p^r},\quad b^{p^m}=c^{p^u}=1,\quad a^{-1}ca=c^{1+p^s},\quad b^{-1}cb=c^{1+p^t},$$

其中 n,m,u,r,s,t 为正整数且 $s,t\leqslant u$. 由于 G' 循环, 因此总可假设 $[a,b]=c^{\sigma}$, 其中 $p\nmid\sigma$. 进一步, 因为 G 正则, 由定理 1.11.5 可知 $r+s\geqslant u$.

由于 G' 循环, 因此 G 亚交换. 由命题 1.1.9 和命题 1.1.10 知

$$[a^{p^{n-u+r}},b]=c^{\sigma\left(p^{n-u+r}+\sum_{k=2}^{p^{n-u+r}}\binom{p^{n-u+r}}{k}p^{s(k-1)}\right)}.$$

注意到 $r+s\geqslant u$, 因此 $[a^{p^{n-u+r}},b]=c^{\sigma p^{n-u+r}}$. 另一方面, $[a^{p^{n-u+r}},b]=[c^{p^r},b]=c^{p^{r+t}}$. 因此 $\sigma p^{n-u+r}\equiv p^{r+t}(\mathrm{mod}\ p^u)$. 进一步, 若 $n-u+r\geqslant u$, 则 $r+t\geqslant u$. 若 $n-u+r<u$, 则 $n-u=t$ 且 $\sigma\equiv 1(\mathrm{mod}\ p^{u-r-t})$.

子情形 1.1 $\langle b,c\rangle$ 交换.

因为 $t=u$ 且 $\sigma p^{n-u+r}\equiv p^{r+t}(\mathrm{mod}\ p^u)$, 故 $n-u+r\geqslant u$. 令 $b_1=b^\tau$, 其中 $\sigma\tau\equiv 1(\mathrm{mod}\ p^u)$. 则 $[a,b_1]=c$ 且 $[c,b_1]=1$. 故 G 同构于定理中的群 (Ⅰ). 此时, n,m,u,r 为不变量. 进一步, 因为 $|G_3|=p^{u-s}$, 所以 s 为不变量. 因此对于满足定理中条件的参数 n,m,u,r,s 的不同取值, 得到的群互不同构.

子情形 1.2 $\langle b,c\rangle$ 非交换.

类似定理 10.2.3 的讨论, 可得 $t<n-m+s$ 且

$$\begin{cases} s\leqslant t, & n-u+r\geqslant m,\\ s\leqslant m-(n-u+r)+t, & n-u+r<m. \end{cases}$$

从而 $t<\min\{n-m+s,u\}$ 且 $s\leqslant\min\{m-\min\{m,n-u+r\}+t,u\}$.

子情形 1.2.1 $s=\min\{m-\min\{m,n-u+r\}+t,u\}$.

注意到 $r+s\geqslant u$. 因此 $r+m-\min\{m,n-u+r\}+t\geqslant u$. 若 $s=u$, 则 $[c,a]=1$. 若 $s=m-\min\{m,n-u+r\}+t$, 则存在适当的 j 并用 $ab^{jp^{m-\min\{m,n-u+r\}}}$ 替换 a 可得

$$(ab^{jp^{m-\min\{m,n-u+r\}}})^{-1}c(ab^{jp^{m-\min\{m,n-u+r\}}})=c.$$

从而可设 $\langle a,c\rangle$ 交换. 进而 G 有如下定义关系:

$$a^{p^{n-u+r}}=c^{p^r},\quad b^{p^m}=c^{p^u}=1,\quad [a,b]=c^\sigma,\quad [c,a]=1,\quad [c,b]=c^{p^t},$$

其中

$$r+1\leqslant u\leqslant m\leqslant n,\quad u-(r+m-\min\{m,n-u+r\})\leqslant t<u,\quad p\nmid\sigma,$$

且 σ 为正整数.

因为 G 的型不变量为 (n,m,r), $|G'|=p^u$ 且 $|G_3|=p^{u-t}$, 故 n,m,u,r,t 均为不变量. 从而只需考虑当 σ 取何值时, 对应的群两两互不同构即可. 为方便证明, 用 $G(\sigma)$ 记群 G. 假设 $G(\sigma)\cong G(\sigma')$. 在群 $G(\sigma)$ 中, 令

$$a_1=a^{i_1}b^{j_1}c^{k_1},\quad b_1=a^{i_2}b^{j_2}c^{k_2},\quad c_1=c^v,$$

其中 $i_1,i_2,j_1,j_2,k_1,k_2,v$ 取适当的整数且 $p\nmid i_1j_2v$ 使得 a_1, b_1 生成 $G(\sigma)$, 且 a_1, $b_1,c_1^{\sigma'}=[a_1,b_1]$ 满足群 $G(\sigma')$ 的定义关系. 显然 $p^{m-\min\{m,n-u+r\}}\mid j_1$ 且 $p^{n-m}\mid i_2$.

经计算知,

$$\begin{cases} (i_1+k_1p^{n-u})p^r \equiv vp^r (\mathrm{mod}\ p^u), & (10.1)\\ \sigma i_1\dfrac{(1+p^t)^{j_2}-1}{p^t}(1+p^t)^{j_1}-\sigma i_2\dfrac{(1+p^t)^{j_1}-1}{p^t}(1+p^t)^{j_2} & \\ \quad +k_1[(1+p^t)^{j_2}-1]+k_2[1-(1+p^t)^{j_1}]=v\sigma', & (10.2)\\ (1+p^t)^{j_1}\equiv 1(\mathrm{mod}\ p^u), & (10.3)\\ (1+p^t)^{j_2-1}\equiv 1(\mathrm{mod}\ p^u). & (10.4) \end{cases}$$

由式 (10.3), (10.4) 可知 $p^{u-t}\mid j_1$ 且 $p^{u-t}\mid j_2-1$. 用 $\sigma'\times$(10.1) 得

$$\sigma'(i_1+k_1p^{n-u})p^r \equiv v\sigma' p^r (\mathrm{mod}\ p^u).$$

进而根据式 (10.2) 可知, $\sigma' i_1 \equiv \sigma i_1 j_2 - \sigma i_2 j_1 (\mathrm{mod}\ p^{u-r})$. 因此

$$\sigma \equiv \sigma' (\mathrm{mod}\ \min\{p^{u-r}, p^{u-t}\}).$$

下证总可取适当的元素满足前面的定义关系且使得 $\sigma \leqslant \min\{p^{u-r}, p^{u-t}\}$. 令 $a'=a, b'=b^j, c'=c^v$, 其中 $v\equiv 1(\mathrm{mod}\ p^{u-r})$, $j\equiv 1(\mathrm{mod}\ p^{u-t})$. 经计算知

$$[a',b'] = c^{\sigma(j+\binom{j}{2}p^t+\cdots+p^{t(j-1)})}.$$

容易证明: 总存在适当的 $j=j_0$ 使得

$$\sigma\left(j+\binom{j}{2}p^t+\cdots+p^{t(j-1)}\right)\leqslant p^{u-t}.$$

若 $p^{u-t}\leqslant p^{u-r}$, 令 $v=1$, 结论得证. 若 $p^{u-t}>p^{u-r}$, 则可取适当的 $v=v_0$, 其中 $v_0\equiv 1(\mathrm{mod}\ p^{u-r})$ 使得

$$v^{-1}\sigma(j+\binom{j}{2}p^t+\cdots+p^{t(j-1)})\leqslant p^{u-r}.$$

结论亦成立. 从而得定理中的群 (II).

子情形 1.2.2　$s<\min\{m-\min\{m,n-u+r\}+t,u\}$.

此时 G 有如下的定义关系:

$$a^{p^{n-u+r}}=c^{p^r},\quad b^{p^m}=c^{p^u}=1,\quad [a,b]=c^{\sigma},\quad [c,a]=c^{p^s},\quad [c,b]=c^{p^t},$$

其中

$$r+1\leqslant u\leqslant m\leqslant n,$$

$$t<\min\{n-m+s,u\},$$

$$u-r\leqslant s<\min\{m-\min\{m,n-u+r\}+t,u\},\quad p\nmid\sigma.$$