有限亚Hamilton p群的分类

安立坚 著

北京工业大学出版社

有限亚Hamilton p群的分类

安立坚 著

北京工业大学出版社

图书在版编目（CIP）数据

有限亚 Hamilton p 群的分类 / 安立坚著. -- 北京 : 北京工业大学出版社, 2015.8

ISBN 978-7-5639-4414-9

Ⅰ. ①有… Ⅱ. ①安… Ⅲ. ①有限群－群论－研究 Ⅳ. ①O152.1

中国版本图书馆 CIP 数据核字(2015)第 207923 号

有限亚 Hamilton p 群的分类

著　　者：安立坚
责任编辑：邢春光
封面设计：张海龄
出版发行：北京工业大学出版社
（北京市朝阳区平乐园100 号 邮编：100124）
010-67391722（传真） bgdcbs@sina.com
出 版 人：郝　勇
经销单位：全国各地新华书店
承印单位：廊坊市金虹宇印务有限公司
开　　本：850毫米×1168毫米　1/32
印　　张：5.5
字　　数：210 千字
版　　次：2015年8月第1版
印　　次：2016年5月第1次印刷
定　　价：26.00元
标准书号：ISBN 978-7-5639-4414-9

前言

群论是近代数学的一个重要分支. 它是一门研究群的性质与结构的学科. 近年来, 随着科学技术的不断进步以及有限群论的逐步完善, 群论的思想、理论与方法已经渗透到科学领域的各个方面. 诸如在密码学、物理学、化学的分子结构等方面的应用就是明证, 而且群论的许多结果已被这些学科所吸收和利用.

在群论的众多分支中, 有限群论无论从理论本身还是从实际应用来说, 都占据着更为突出的地位. 同时, 它也是近年来比较活跃的一个数学分支, 有着十分丰富的内容. 在上个世纪, 经过很多数学家的努力, 在有限群中取得了一连串的突破, 并终于在 1981 年解决了著名的有限单群分类问题. 这项重大的科学成果的得来是很不容易的. 如果从 1832 年 Galois 证明交错群 A_5 是单群算起, 整整经历了 150 年. 参加这项工作的数学家前后共达几百人. 为了证明单群分类定理, 即有限单群共有 18 个无限族和 26 个零散单群, 人们使用了抽象群论的、表示论的 (包括常表示和模表示)、几何的以及组合论和图论的方法, 在杂志上发表了数千页以至上万页的证明. 直到 2005 年, D. Gorenstein, R. Lyons 和 R. M. Solomon 用六本专著才给出了单群分类定理的完整证明, 见文献 [26, 27, 28, 29, 30, 31] 等.

近年来, 随着有限单群分类的最终完成, 有限 p 群的研究才变得越来越活跃. 群论研究的许多领头科学家, 如 G. Glauberman, Z. Janko 等人开始转入对有限 p 群的研究, 发表了许多有限 p 群研究的论文, 见文献 [16, 23, 24, 25, 35, 36, 37, 38, 39, 40, 41, 42] 等.

在 p 群的研究领域中, 内交换 p 群和 Hamilton p 群的分类是两个经典的结果. 作为这两个经典结果的推广, 本书研究了子群或者交换或者正规的有限非交换 p 群, 我们称这类群为有限亚 Hamilton p 群. 本书给出了有限亚 Hamilton p 群的一些基本性质, 完成了有限亚

Hamilton p 群的完全分类, 并彻底解决了同构问题, 从而完整地解决了亚 Hamilton 群的分类问题. 为了方便读者, 我们对有限 p 群的一些基本结论和方法作了较详细的介绍. 本书还介绍了一些与亚 Hamilton p 群有关的工作.

安立坚

email: anlj@sxnu.edu.cn

2015 年 4 月于山西师范大学

目 录

第一章　基本概念和方法

本章介绍一些本书用到的基本结论和方法. 事实上, 这些结论和方法也是有限 p 群的研究中常常要用到的.

§1.1　基本概念和公式

本节首先给出有限 p 群的一些术语和符号, 其他未提及的术语和符号都是标准的, 见 [5, 7].

设 G 是有限 p 群, 我们分别用 $c = c(G)$、$d(G)$ 表示群 G 的幂零类、极小生成元的个数. G 的下中心群列和上中心群列分别是:

$$G = G_1 > G_2 > \cdots > G_{c+1} = 1,$$

和

$$1 = Z_0(G) < Z_1(G) < \cdots < Z_c(G) = G.$$

设 $\exp(G) = p^e$, 我们称 e 为群 G 的幂指数, 对于任意的 s, $0 \leqslant s \leqslant e$, 我们规定

$$\Lambda_s(G) = \{a \in G \mid a^{p^s} = 1\}, \quad V_s(G) = \{a^{p^s} \mid a \in G\},$$

并且规定

$$\Omega_s(G) = \langle \Lambda_s(G) \rangle, \quad \mho_s(G) = \langle V_s(G) \rangle,$$

则 G 的 Frattini 子群 $\Phi(G) = G'\mho_1(G)$.

下面我们重点来介绍证明和计算过程中反复使用的一些换位子公式.

命题 1.1.1. *设 G 是群, $a, b, c \in G$, 则*

(1) $a^b = a[a, b]$;

(2) $[a,b]^c=[a^c,b^c]$;

(3) $[a,b]^{-1}=[b,a]=[a,b^{-1}]^b=[a^{-1},b]^a$;

(4) $[ab,c]=[a,c]^b[b,c]=[a,c][a,c,b][b,c]$;

(5) $[a,bc]=[a,c][a,b]^c=[a,c][a,b][a,b,c]$;

(6) (*Witt*公式) $[a,b^{-1},c]^b[b,c^{-1},a]^c[c,a^{-1},b]^a=1$;

(7) $[a,b,c^a][c,a,b^c][b,c,a^b]=1$.

证明 (1)–(3) 由定义直接验证.

(4) $[ab,c]=(ab)^{-1}c^{-1}abc=(c^{-1})^{ab}c=(a^{-1}c^{-1}a)^bc^b(c^{-1})^bc=(a^{-1}c^{-1}ac)^b[b,c]=[a,c]^b[b,c]=[a,c][a,c,b][b,c]$.

(5) $[a,bc]=[bc,a]^{-1}=([b,a]^c[c,a])^{-1}=[a,c][a,b]^c=[a,c][a,b][a,b,c]$.

(6) 令 $u=aca^{-1}ba$. 轮换 a,b,c 三字母, 又令 $v=bab^{-1}cb$, $w=cbc^{-1}ac$. 则有

$$\begin{aligned}[a,b^{-1},c]^b &= b^{-1}[a,b^{-1}]^{-1}c^{-1}[a,b^{-1}]cb\\ &= b^{-1}ba^{-1}b^{-1}ac^{-1}a^{-1}bab^{-1}cb\\ &= (aca^{-1}ba)^{-1}(bab^{-1}cb)=u^{-1}v.\end{aligned}$$

同理有

$$[b,c^{-1},a]^c=v^{-1}w,\qquad [c,a^{-1},b]^a=w^{-1}u.$$

于是

$$[a,b^{-1},c]^b[b,c^{-1},a]^c[c,a^{-1},b]^a=u^{-1}vv^{-1}ww^{-1}u=1.$$

(7) 首先有

$$[a,b^{-1},c]^b=[[a,b^{-1}]^b,c^b]=[b,a,c^b].$$

同理又有

$$[b,c^{-1},a]^c=[c,b,a^c],\qquad [c,a^{-1},b]^a=[a,c,b^a],$$

于是由 Witt 公式有

$$[b,a,c^b][c,b,a^c][a,c,b^a]=1.$$

再互换 a,b 两个字母即得 (7) 式. □

若 G' 是交换群, 我们称 G 为亚交换群.

命题 1.1.2. 设 G 为亚交换群且 $x,y,z\in G$,

(1) 若 $z\in G'$, 则 $[z,x]^{-1}=[z^{-1},x]$;

(2) 若 $y\in G'$, 则 $[xy,z]=[x,z][y,z]$ 且 $[z,xy]=[z,x][z,y]$;

(3) $[x,y^{-1},z]^y=[y,x,z]$, $[x,y,z^x]=[x,y,z]$;

(4) $[x,y,z][y,z,x][z,x,y]=1$;

(5) 若 $z\in G'$, 则 $[z,y,x]=[z,x,y]$.

证明 (1) 由命题 1.1.1(3) 及 G' 的交换性得

$$[z,x]^{-1}=[z^{-1},x]^z=[z^{-1},x].$$

(2) 由命题 1.1.1(4–5) 及 G' 的交换性立得.

(3) 应用命题 1.1.1 中的诸换位子公式, 得

$$\begin{aligned}[x,y^{-1},z]^y &= [[x,y^{-1}]^y,z^y]=[[y,x],z[z,y]]\\ &= [y,x,z][[y,x],[z,y]]=[y,x,z].\end{aligned}$$

(4) 由 (3) 及 Witt 公式 (命题 1.1.1(6)) 立得.

(5) 由 $z\in G'$ 及 (4) 得

$$[y,z,x][z,x,y]=1,$$

即 $[z,x,y]=[y,z,x]^{-1}$. 由 (1), $[y,z,x]^{-1}=[[y,z]^{-1},x]=[z,y,x]$, 于是得 $[z,x,y]=[z,y,x]$. □

为了更好的叙述下面两个命题, 我们约定: 对于任意的正整数 i,j,

$$[ia,jb]=[a,b,\underbrace{a,\ldots,a}_{i-1},\underbrace{b,\ldots,b}_{j-1}].$$

命题 1.1.3. 设 G 为亚交换群, $a,b\in G$, m,n 为正整数, 则

$$[a^m,b^n]=\prod_{i=1}^{m}\prod_{j=1}^{n}[ia,jb]^{\binom{m}{i}\binom{n}{j}}.$$

证明 对 $m+n$ 用归纳法. 若 $m+n=2$, 公式显然成立. 下面设 $m+n>2$, 这时 m, n 中至少有一个大于 1.

若 $n>1$, 则

$$[a^m,b^n]=[a^m,b][a^m,b^{n-1}]^b.$$

据归纳假设得

$$\begin{aligned}[a^m,b^n] &= \prod_{i=1}^{m}[ia,b]^{\binom{m}{i}}\left(\prod_{i=1}^{m}\prod_{j=1}^{n-1}[ia,jb]^{\binom{m}{i}\binom{n-1}{j}}\right)^b\\ &= \prod_{i=1}^{m}[ia,b]^{\binom{m}{i}}\cdot\prod_{i=1}^{m}\prod_{j=1}^{n-1}([ia,jb][ia,(j+1)b])^{\binom{m}{i}\binom{n-1}{j}}\end{aligned}$$

$$\begin{aligned}&= \prod_{i=1}^{m}\left([ia,b]^{\binom{m}{i}}[ia,b]^{\binom{m}{i}\binom{n-1}{1}}[ia,nb]^{\binom{m}{i}}\right.\\ &\quad\left.\cdot\prod_{j=2}^{n-1}[ia,jb]^{\binom{m}{i}\binom{n-1}{j}+\binom{m}{i}\binom{n-1}{j-1}}\right)\\ &= \prod_{i=1}^{m}\left([ia,b]^{\binom{m}{i}\binom{n}{1}}[ia,nb]^{\binom{m}{i}\binom{n}{n}}\prod_{j=2}^{n-1}[ia,jb]^{\binom{m}{i}\binom{n}{j}}\right)\\ &= \prod_{i=1}^{m}\prod_{j=1}^{n}[ia,jb]^{\binom{m}{i}\binom{n}{j}}.\end{aligned}$$

而若 $n=1$, 则 $m>1$. 这时有

$$[a^m,b]=[a^{m-1},b]^a[a,b].$$

应用归纳假设得

$$\begin{aligned}
[a^m,b] &= \left(\prod_{i=1}^{m-1}[ia,b]^{\binom{m-1}{i}}\right)^a [a,b] \\
&= \prod_{i=1}^{m-1}[ia,b]^{\binom{m-1}{i}} \prod_{i=1}^{m-1}[(i+1)a,b]^{\binom{m-1}{i}}\cdot[a,b] \\
&= [a,b][a,b]^{\binom{m-1}{1}} \prod_{i=2}^{m-1}[ia,b]^{\binom{m-1}{i}} \prod_{i=2}^{m}[ia,b]^{\binom{m-1}{i-1}} \\
&= [a,b]^{\binom{m}{1}} \left(\prod_{i=2}^{m-1}[ia,b]^{\binom{m}{i}}\right)[ma,b]^{\binom{m}{m}} \\
&= \prod_{i=1}^{m}[ia,b]^{\binom{m}{i}}. \qquad \square
\end{aligned}$$

命题 1.1.4. 设 G 为亚交换群, $a,b\in G$, $m\geqslant 2$, 则

$$(ab^{-1})^m = a^m \prod_{i+j\leqslant m}[ia,jb]^{\binom{m}{i+j}}b^{-m}.$$

证明 用对 m 的归纳法. 当 $m=2$ 时,

$$(ab^{-1})^2 = ab^{-1}ab^{-1} = a^2b^{-1}[b^{-1},a]bb^{-2} = a^2[a,b]b^{-2},$$

结论成立. 现在设 $m>2$, 由归纳假设有

$$\begin{aligned}
(ab^{-1})^m &= (ab^{-1})^{m-1}ab^{-1} \\
&= a^{m-1}\prod_{i+j\leqslant m-1}[ia,jb]^{\binom{m-1}{i+j}}b^{-m+1}ab^{-1} \\
&= a^{m-1}\prod_{i+j\leqslant m-1}[ia,jb]^{\binom{m-1}{i+j}}a[a,b^{m-1}]b^{-m} \\
&= a^m \prod_{i+j\leqslant m-1}[ia,jb]^{\binom{m-1}{i+j}} \\
&\quad \cdot\left(\prod_{i+j\leqslant m-1}[(i+1)a,jb]^{\binom{m-1}{i+j}}\right)[a,b^{m-1}]b^{-m}.
\end{aligned}$$

应用命题 1.1.3,

$$[a,b^{m-1}]=\prod_{j=1}^{m-1}[a,jb]^{\binom{m-1}{j}},$$

代入上式得

$$\begin{aligned}(ab^{-1})^m &= a^m\prod_{j=1}^{m-2}[a,jb]^{\binom{m-1}{j+1}}\prod_{\substack{i+j\leqslant m-1\\ i>1}}[ia,jb]^{\binom{m-1}{i+j}}\\ &\quad\cdot\prod_{\substack{i+j\leqslant m\\ i>1}}[ia,jb]^{\binom{m-1}{i+j-1}}\prod_{j=1}^{m-1}[a,jb]^{\binom{m-1}{j}}b^{-m}\\ &= a^m\prod_{j=1}^{m-2}[a,jb]^{\binom{m}{j+1}}[a,(m-1)b]\prod_{\substack{i+j\leqslant m-1\\ i>1}}[ia,jb]^{\binom{m}{i+j}}\\ &\quad\cdot\prod_{\substack{i+j=m\\ i>1}}[ia,jb]\cdot b^{-m}\\ &= a^m\prod_{j=1}^{m-1}[a,jb]^{\binom{m}{j+1}}\prod_{\substack{i+j\leqslant m\\ i>1}}[ia,jb]^{\binom{m}{i+j}}b^{-m}\\ &= a^m\prod_{i+j\leqslant m}[ia,jb]^{\binom{m}{i+j}}b^{-m}.\end{aligned}$$

□

§1.2 Engel 条件

定义 1.2.1. *称群 G 满足n 次 Engel* **条件**, *如果对任意的 $g,h\in G$,*

有

$$[g,\underbrace{h,\ldots,h}_{n}]=1.$$

著名的 Zorn 定理断言, 满足 n 次 Engel 条件的有限群必为幂零群. 熟悉内幂零群的读者可以很容易地应用极小反例法证明这点. 这里就不证明了.

定理 1.2.2. *设群 G 满足 2 次 Engel 条件, 则 G 是幂零类至多为 3 的幂零群. 如果 G 中没有 3 阶元素, 则 $c(G)\leqslant 2$.*

为证明这个定理, 先证明一个引理.

引理 1.2.3. *群 G 满足 2 次 Engel 条件当且仅当 G 中任意两个共轭元素可换.*

证明 因为

$$[g,h,h]=[[g,h],h]=[h^{-g}h,h]=[h^{-g},h]^h,$$

$[g,h,h]=1$ 等价于 $[h^{-g},h]=1$, 即 h^g 与 h 可换. □

定理 1.2.2 的证明:

由引理 1.2.3, 任意元素 g 在 G 中的正规闭包 $A(g):=g^G=\langle g^x \mid x\in G\rangle$ 是 G 的交换正规子群.

我们分下列步骤来证明定理.

(1) 简单换位子 w 中有两项相等其值必为 1: 可设

$$w=[a_1,\ldots,a_s,x,b_1,\ldots,b_t,x,c_1,\ldots,c_u],$$

其中 s,t,u 均可以为 0, 即可以没有 $\{a_i\}$, $\{b_j\}$ 或 $\{a_k\}$. 于是

$$w_1=[a_1,\ldots,a_s,x]\in A(x).$$

由 $A(x) \trianglelefteq G$, $w_2 = [w_1, b_1, \ldots, b_t] \in A(x)$. 再由 $A(x)$ 交换, $[w_2, x] = 1$, 从而 $w = 1$.

(2) 对任意的 $x, y \in G$, 有 $[x^{-1}, y] = [x, y^{-1}] = [x, y]^{-1}$: 由 $1 = [xx^{-1}, y] = [x, y]^{x^{-1}}[x^{-1}, y]$, 用 (1) 即得 $1 = [x, y][x^{-1}, y]$, $[x^{-1}, y] = [x, y]^{-1}$. 由此又得 $[x, y^{-1}] = [y^{-1}, x]^{-1} = [y, x] = [x, y]^{-1}$.

(3) Jakobi 恒等式成立: 对任意的 $x, y, z \in G$, 有 $[x, y, z][z, x, y][y, z, x] = 1$: 因为 $[x, y^{-1}, z] \in A(y)$, $[x, y^{-1}, z]^y = [x, y^{-1}, z]$. 再由 (2), $[x, y^{-1}, z] = [[x, y]^{-1}, z] = [x, y, z]^{-1}$. 由 Witt 恒等式得

$$[x, y, z]^{-1}[y, z, x]^{-1}[z, x, y]^{-1} = 1,$$

即 $[z, x, y][y, z, x][x, y, z] = 1$. 轮换 x, y, z 的位置, 即得所需结果.

(4) $[x, z, y] = [x, y, z]^{-1}$: 由 $[x, yz] = [x, z][x, y][x, y, z]$, 再用 (1) 得

$$[x, yz]^y = [x, z]^y[x, y]^y[x, y, z]^y = [x, z][x, z, y][x, y][x, y, z].$$

于是

$$\begin{aligned} [x, yz]^{yz} &= ([x, yz]^y)^z = [x, z]^z[x, z, y]^z[x, y]^z[x, y, z]^z \\ &= [x, z][x, z, y][x, y][x, y, z]^2. \end{aligned}$$

由 (1),

$$[x, yz]^{yz} = [x, yz] = [x, z][x, y][x, y, z].$$

因为上面两式右端的诸换位子都包含 x, 因此均属于 $A(x)$, 彼此交换. 由此二式相等, 得到 $[x, y, z][x, z, y] = 1$, 即 $[x, z, y] = [x, y, z]^{-1}$.

(5) $[x, y, z] = [y, x, z]^{-1}$: 由 (2), $[x, y, z] = [[y, x]^{-1}, z] = [y, x, z]^{-1}$, 得证.

由 (4) 和 (5) 说明, 任意交换 $[x, y, z]$ 中的两项, 其值变为原换位子的逆. 因此, 更一般地, 作 x, y, z 的奇置换, 其值变逆, 而作偶置换, 其值不变. 于是再应用 (3) 立得

(6) $[x,y,z]^3=1$.

至此, 如果 G 中没有 3 阶元素, 则 $[x,y,z]=1$, 即 G 是幂零类至多为 2 的幂零群.

(7) $[x,y,z,u]=[x,y,u,z]^{-1}$: 把 $[x,y]$ 作为一个整体, 应用 (4) 立得结论.

应用 (7), (6) 前面的那段话以及 (2), 对换位子 $[x,y,z,u]$, 作 x, y, z, u 的奇置换, 其值变逆, 而作偶置换, 其值不变. 细节从略.

(8) $[x,y,z,u]^2=1$: 由 $[x,y,z,u]=[[x,y],z,u]=[z,u,[x,y]]=[[z,u],[x,y]]=[[x,y],[z,u]]^{-1}=[x,y,[z,u]]^{-1}=[z,u,x,y]^{-1}=[x,y,z,u]^{-1}$, 得到结果.

把 $[x,y]$ 作为整体, 由 (6) 又得 $[x,y,z,u]^3=1$, 结合 (8) 即得到 $[x,y,z,u]=1$, 即 G 的幂零类至多为 3. □

§1.3 循环扩张理论

本节主要介绍循环扩张的基本理论. 所得结论不仅仅限于有限 p 群, 对有限群也是成立的.

定义 1.3.1. *称群 G 为* **群 N 被群 F 的扩张**, *如果 N 是 G 的正规子群, 并且 $G/N\cong F$. 若 F 是一个 m 阶循环群, 则这时的扩张叫做* **N 的 m 次循环扩张**. *若 $N\leqslant Z(G)$, 则这时的扩张叫做* **中心扩张**.

设 G 是 N 的 m 次循环扩张. 因为 G/N 是 m 阶群, 所以有 $b^m\in N$, 其中 $G/N=\langle bN\rangle$. 又因为 $N\trianglelefteq G$, 所以 b 诱导出 N 的一个自同构 τ. 由于 $b^m\in N$, 存在 $a\in N$ 使得 $b^m=a$. 显然, $b^{-1}ab=a$. 所以我们有

$$a^\tau=a,\qquad \tau^m=\varphi(a). \tag{1.1}$$

其中 $\varphi(a)$ 表示由 a 诱导的 N 的内自同构. 反过来, 假定存在 $a\in N$ 和 $\tau\in\mathrm{Aut}(G)$ 满足 (1.1) 式, 则令 $G=\{(g^i,n)\mid 0\leqslant i\leqslant m-1,n\in N\}$

(只看成符号的集合). 如下规定 G 的乘法:

$$(g^i,n)\cdot(g^j,n')=\begin{cases}(g^{i+j},n^{\tau^j}n'), & i+j<m,\\ (g^{i+j-m},an^{\tau^j}n'), & i+j\geqslant m.\end{cases}\tag{1.2}$$

则 G 对上述乘法组成一个群, 有正规子群 $\overline{N}=\{(g^0,n)\mid n\in N\}\cong N$, 并且 $G/\overline{N}\cong \mathrm{C}_m$ (验证均从略). 我们把上面叙述的事实写成一个定理.

定理 1.3.2. *设 N 是群, $F=\langle g\rangle$ 是 m 阶循环群. 又设 $a\in N$, $\tau\in \mathrm{Aut}(N)$, a 与 τ 满足 (1.1) 式. 则集合 $G=\{(g^i,n)\mid 0\leqslant i\leqslant m-1, n\in N\}$ 对于由 (1.2) 式定义的乘法组成一个群. G 是 N 被循环群 $F\cong \mathrm{C}_m$ 的扩张.*

对于 N 是有限群的情形, 为了使用方便, 我们经常将定理 1.3.2 中的群 G 用生成元和定义关系组写出来. 即, 我们有下面的定理.

定理 1.3.3. *设 N 是有限群, $N=\langle n_1,n_2,\ldots,n_r\rangle$ 且*

$$V=\{f_i(n_1,n_2,\ldots,n_r)=1\mid i\in I\}$$

为 N 的一个定义关系组. 若 $a\in N$, $\tau\in \mathrm{Aut}(N)$, a 与 τ 满足 (1.1) 式, 则 $G=\langle n_1,n_2,\ldots,n_r,b\rangle$ 是 N 的 m 次循环扩张, 其中 G 的定义关系组为:

$$V\cup\{b^{-1}n_ib=n_i^{\tau},b^m=a\mid i\in I\}.$$

定理 1.3.2 给出了决定群 N 的所有循环扩张的方法. 但对于不同的 a,τ 确定的扩张何时同构的问题并没有回答. 下面的命题说明由与 τ 共轭的 N 的自同构 $\sigma^{-1}\tau\sigma$ 和元素 a^{σ} 得到的循环扩张与由 a,τ 确定的扩张是同构的.

命题 1.3.4. *如定理 1.3.2, 设 G 是 N 的 m 次循环扩张, 由满足 (1.1) 式的 $a\in N$ 和 $\tau\in \mathrm{Aut}(N)$ 得到. 再设 $\tau_1=\sigma^{-1}\tau\sigma$ 是 $\mathrm{Aut}(N)$ 中与 τ 共轭的自同构, 则 $a_1=a^{\sigma}$ 与 τ_1 满足 (1.1) 式, 并且由 a_1 和 τ_1 得到的 N 的 m 次循环扩张 G_1 与 G 同构.*