Y群引论

Y QUN YIN LUN

曹义著

科学出版社

Y 群引论

曹 义 著

科学出版社

北 京

内 容 简 介

本书主要介绍 Y 群理论、有限群的组合结构、群谱等在有限群理论中的新概念. 内容包括: Y 矩阵及其扩张、Y 群表示理论、Y 直积、Γ 矩阵、有限群的组合结构、Z^n 上的除法定理、群的编码等，其中许多内容是第一次面世. 在书中，作者提出了大量的问题供读者思考，这成为本书的一大特点.

本书适读人群：从事数学研究的学者、数学专业的研究生、大学数学教师以及从事与群有关的物理学和化学研究的人员. 阅读本书并不需要太多的预备知识，只要具备大学高等代数理论的知识即可.

图书在版编目(CIP)数据

Y 群引论/曹义著. —北京:科学出版社，2012.1
ISBN 978-7-03-033272-1

Ⅰ.①Y… Ⅱ.①曹… Ⅲ.①有限群 Ⅳ.①O152.1

中国版本图书馆 CIP 数据核字（2011）第 281014 号

责任编辑：杨 岭 莫永国/封面设计：陈思思

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

四川煤田地质制图印刷厂印刷
科学出版社发行 各地新华书店经销
*
2012 年 1 月第 一 版 开本：720×1000 B5
2012 年 1 月第一次印刷 印张：7
字数：120 千字
定价：40.00 元

献给我的母亲——
为我开启算术之门的人。

序　　言

抽象代数是数学的一个核心理论, 群论是该理论的支架. 代数理论发展至今已近乎完美, 各个中心概念及其间的关联均有很好的描述和整齐的形式计算, 给它的应用, 特别是在物理、化学、计算科学、通信工程、生物工程等学科中的应用, 提供了有力的技术支持. 然而, 伴随着理论的发展也产生了大量的新问题. 这正是数学的特点：没有最完美, 只有更完美. 另外, 理论建立初期就存在的基本问题, 例如有限群的分类, 再次被数学界设定为“千年计划”的硬骨头, 仍然在考验着人类的智力. 前不久, 数学界总算宣称“有限单群的分类”工作完成了, 除了几个“例外群”, 单群总算有了归宿. 然而, 作为一个更大的团体, 有限群还紧紧地关闭着它的大门, 它在等待一种崭新的思想方法来开启它.

群的分解是群理论的焦点, 设整数 $n = p \times m$, 如果 n 阶有限群 F_n 有正规子群 H_p, 则 F_n 可以被 H_p 除, 得到的商 Q_m 是 F_n 的子群, 写成 $F_n = H_p \otimes Q_m$, 或 $Q_m = F_n/H_p$, 这是经典群的分解定理. 交换群的任何一个子群都是正规的, 所以交换群可以被彻底分解, 因此交换群很容易被完整地分类. 在群的分解定理中, 整数与群在运算形式上是统一的, 但是群毕竟是更复杂的对象, 当 F_n 中不含 (非平凡的) 正规子群时, 统一便被打破, 数学概念的协调性似乎也遭到质疑. 而且这一情况直接影响到对有限群结构的深度剖析, 使分类也失去了依据. 不含 (非平凡) 正规子群的群叫单群, 在经典理论中单群是不能被分解的群, 就像整数中的素数一样. 但是除了素数阶群之外 (素数阶的群自然都是单群), 还有合数阶的单群, 例如 $n \neq 4$ 的所有交错群 A_n 都是单群, 与整数分解的算术基本定理相比较似乎有点不合乎常理：合数阶单群中应该有更素的因子才能体现数学结构之美.

在给学生开设抽象代数课过程中接触了一些有限群的知识, 给我印象比较深的是单群作为群的素因子, 作为整数, 又具有一个可以被分解的阶数. 这种不合情理的事因在哪里？当我认识“四顶点法则”后, 谜团慢慢地被打开了. 四顶点法则是一个动力体系, Y 群的概念在这个动力下自然地产生. Y 群的发现可以说彻底打破了上述僵局：Y 群的任何一个碎片都是 Y 群, 经典的群在我们这里是一类特殊的、被称为完全 Y 群的对象. 在我们的系统中, 任何合数阶的群都是可以分解的, 当然是以 Y 群为因子, 单群在这里也被分解成了两个 Y 群的“直积”(在附录中我们给出一个 60 阶的单群被分解成一个 5 阶循环群与一个 12 阶 Y 群的 Y 直积的例子). Y 群的定义中并没有运算、结合律、逆元和单位元等算术概念. 在证明完

全Y群是群的过程中, 我们发现群定义中的那些算术概念被还原成了组合拓扑对象. 在把逻辑还原为算术时, 哥德尔发现了形式逻辑系统的不完备性. 在进一步的还原中我们还会看到什么? 这倒是非常有趣的. 黑格尔在他的逻辑学中提出的第一个问题就是逻辑的起点问题. 至少在这里, 可以说, 还有比算术更初始的东西.

Y群让我们很快看到群的那个非常美妙的组合结构, 从技术上来说, 如果已经有了全体m阶群的结构图, 那么就很容易绘出全体$p\times m$阶群的结构图, p在这里是素数. 在这种递归结构中也是用F_n的子群H_p去除F_n, 但是H_p不一定是正规的, 我们得到的商

$$F_n/H_p=\{M_{m,d_1},M_{m,d_2},\cdots,M_{m,d_k}\}$$

是一组Y群, 这种商分别有α和β两种类型. 不失一般性, 我们只要讨论p是素数的情况就可以了. 若H_p是F_n的子群, 则存在F_n的k个互不同构的Y子群 $\{M_{m,d_1},M_{m,d_2},$
$\cdots,M_{m,d_k}\}$ 满足

$$F_n=H_p\hat{\otimes}_\rho M_{m,d_i},\quad i=1,2,\cdots,k$$

我们把H_p除F_n所得的k个商叫做H_p在F_n中的谱, 谱描述的是子群在群中的拓扑位置.

这些听起来有点怪的概念并非凭空捏造, 而是严格的逻辑结论. 上面那个被称为Y直积的符号之所以加上一顶帽子和一个下标, 是为了与传统的直积区别开来. Y直积是带参数的直积运算, 当参数等于平凡值时它就是传统的直积. 很有趣的是, 一个n阶群 F_n的分解信息完全包含在它的一个$m+p-1$阶子式中$(n=mp)$, 这个子式记成$\Gamma_{p,n}$, 它是群分解的计算形式. 也就是说, 当给定一个群H_p和一个Y群$M_{m,d}$以后, 按确定的程序就可以构造一个Y矩阵$\Gamma_{p,n}$, 这样就完成了整个Y直积运算, 因为$\Gamma_{p,n}$可以扩张为唯一的一个群.

书中提出的许多问题, 并没有被一一解答, 其中部分是笔者正在思考的问题, 还有一部分打算留给读者思考. 有些命题没有给出证明, 留作练习.

本书主要目的是介绍Y群中那种结构蕴含的思想方法, 为此我们以有限群的组合结构为例, 编码问题也是作为一个例子顺便提出, 希望读者能从解决具体问题的过程中去领悟该方法的本质. 这一方法像一把钥匙, 打开了抽象代数这座宝库的一扇窗, 让我们看到了前所未见的景象.

本书在编写过程中得到许多朋友的支持和帮助. 退休后我面临为女儿自费去法国留学筹集经费, 不得不放下正开始的研究工作. 这时, 广东金亚集团总裁欧伟雄先生慷慨地给予资助, 还经常和我讨论数学问题, 给我很多启示. 广东工业大学的谭中华副教授在我研究Y群期间, 为我编写了近百个计算程序, 生成上千个群的加法表, 为理论研究提供了思路和依据. 这期间, 我女儿也利用假期闲暇的时间为我编写程序, Y群这个名字就是她推荐的. 没有朋友和家人的鼎力协助, 我的工

作将举步维艰, 我要向他们表示衷心的感谢！还值得一提的是本书的两位责任编辑, 科学出版社的莫永国先生和杨岭先生. 在编辑过程中，他们逐字逐句地审阅了我的书稿, 提出大量修改意见, 使本书避免了很多疏漏和谬误. 他们一再叮嘱: “质量是重中之重, 出不得半点差错!” 这正是目前学术界最需要推崇的一种精神. 我在这里向他们致敬!

曹　义

2011年8月于贵阳

目　录

第 1 章　导　　论

本书由三个部分组成: 第一部分从第 2 章到第 5 章是 Y 群的定义及基本性质; 第二部分从第 6 章至第 10 章讨论有限群的结构; 第三部分是书的最后三章, 讨论编码理论.

为了避开那些叫人望而生畏的数学形式, 我们先用举例的方式, 比较直观地把主要概念描述一下.

1. "(四) 顶点法则"可以用下面矩阵形式来描述

$$\begin{pmatrix} a & d \\ b & c \end{pmatrix}$$

从拓扑位置看, 矩阵的每一项作为一个顶点, 由另外三点的相对位置关系所确定, 如 a 由 b, c, d 三点的分布而定, 数学上我们可以用函数

$$F(d, c, b) = a$$

表述. 因为四个顶点处于完全平等的地位, 所以有以下等价关系

$$F(d, c, b) = a \Leftrightarrow F(c, d, a) = b \Leftrightarrow F(b, a, d) = c \Leftrightarrow F(a, b, c) = d$$

该关系确定一个固定的"块"结构, 一个元素表示一个顶点, 容易看出, 一共有三种块, 分别有二、三和四个不同的顶点:

$$\begin{pmatrix} a & b \\ b & a \end{pmatrix}, \begin{pmatrix} a & c \\ b & a \end{pmatrix}, \begin{pmatrix} a & d \\ b & c \end{pmatrix}$$

设 $\Omega = \{1, 2, 3, \cdots, n\}$ 是有 n 个元素的集合, 注意这里的数字, 除非有特别的申明, 总是表示抽象的元素. 我们定义一个称为**顶点法则**的函数

$$\begin{array}{rccc} F: & \Omega^3 & \to & \Omega \\ & (a, b, c) & \mapsto & d \end{array}$$

满足以下条件:

(1) 对任意 $a, b, c, d \in \Omega$ 有

$$F(a, b, c) = d \Leftrightarrow F(d, c, b) = a \Leftrightarrow F(c, d, a) = b \Leftrightarrow F(b, a, d) = c$$

(2) $F(F(x,y,a),a,z)=F(x,y,z)$; $F(x,a,F(a,y,z))=F(x,y,z)$.

第 (2) 条是下面两种形式 (块) 的拼接产生的, 表示一种结合关系:

$$\begin{array}{ccccc} & & & & x \cdots w \\ x & \cdots & u & \cdots & w \\ \vdots & & \vdots & & \vdots \\ y & \cdots & a & \cdots & z \end{array} \quad , \quad \begin{array}{c} \\ a \cdots u \\ \vdots \\ y \cdots z \end{array}$$

具有以上性质的函数称为 Ω 上的 Y 函数. 其实, Ω 可以是可数集合或连续统, 这并不影响 Y 函数的定义. 假如 Ω 是可微分流形, 在满足结构相容的条件下 Y 函数确定一个"广义" 李群. 本书中我们只涉及有限群不讨论其他问题. 上面定义指出 Y 函数是由一个函数方程组定义的, 用 Y 函数可以把 Ω 的元素安排到一个称为**Y 矩阵**的形式中去, 这个矩阵的每个 2×2 子式满足上述顶点法则. 容易证明, 任意交换一个 Y 矩阵的两行或两列得到的是与原矩阵同构的 Y 矩阵. 另外, 一个 Y 矩阵的任意一个子式仍然是一个 Y 矩阵. 假如 Ω 中有 m 个元素, 一个容积为 m 的 n 阶 Y 矩阵 ($n\leqslant m$) 就是由 Ω 的元素构成的 n 阶矩阵 (矩阵中所含不同元素的个数, 叫矩阵的容积), 矩阵的每行、每列上 Ω 的元素最多出现一次, 并且满足四顶点法则, 即有一个 Y 函数 F. 例如

$$M_{4,6}=\begin{pmatrix} a & b & c & d \\ b & a & e & f \\ c & d & a & b \\ e & f & b & a \end{pmatrix}, \quad M_{4,4}=\begin{pmatrix} a & b & c & d \\ b & a & d & c \\ d & c & a & b \\ c & d & b & a \end{pmatrix}$$

容易检验这两个矩阵都是 Y 矩阵, $M_{4,6}$ 的容积为 6, $M_{4,4}$ 的容积为 4. 因为 $M_{4,4}$ 的容积等于阶数所以又称为**CY 矩阵**. Y 矩阵在集合 Ω 上确定了一种结构, 有这种结构的集合就称为**Y 群**, 记成 (Ω,F). 我们将要证明完全的 Y 函数 (也叫 CY 函数, 对应的矩阵就是 CY 矩阵) 定义一个群. Y 函数确定 Ω 中元素的一种序, 使我们可以从"序" 这个角度去剖析群的组合结构. 我们证明, 除了素数阶的 (循环) 群以外任意的群都可以分解为以下形式的乘积

$$G=A\hat{\otimes}_{\rho}B$$

这里的 A 是 CY 矩阵, 所以是群, B 是 Y 矩阵 (Y 群), 不一定是群. 符号 $\otimes$ 上面的帽子和下面的映射 ρ 表示块参数. 在 A,B 都是群和块参数取平凡值的情况下, 这个乘积就是经典的直积. 这里我们以 6 阶群为例, 来解释以上概念. 一共有两个 (互不同构的)6 阶群: F_6^1 和 F_6^2, 其中 F_6^1 是交换群, F_6^2 是非交换群. 它们为以下矩

阵形式: 每行、每列均由$\{1,2,3,4,5,6\}$的排列构成, 而且满足顶点法则,

$$F_6^1=\begin{pmatrix}1&2&3&4&5&6\\6&1&2&3&4&5\\5&6&1&2&3&4\\4&5&6&1&2&3\\3&4&5&6&1&2\\2&3&4&5&6&1\end{pmatrix},\quad F_6^2=\begin{pmatrix}1&2&3&4&5&6\\2&1&5&6&3&4\\3&4&1&2&6&5\\5&6&2&1&4&3\\4&3&6&5&1&2\\6&5&4&3&2&1\end{pmatrix}$$

其实CY矩阵就是(广义的)Cayley表(也叫加法表或乘法表). 如果我们选1为单位元(任意元素都可以作为单位元), 则矩阵中的2×2子式

$$\begin{pmatrix}1&b\\a&c\end{pmatrix}$$

定义一个乘法运算: $a\cdot b=c$, 有时为了强调单位元也记成$(a\cdot b)_{(1)}=c$. 如果选另外一个元素r作为单位元, 则子式

$$\begin{pmatrix}r&b\\a&c\end{pmatrix}$$

给出由r确定的乘法运算: $(a\cdot b)_{(r)}=c$. 如果记 $a\cdot a=a^2$,$\underbrace{a\cdot a\cdots a}_{k}=a^k$, 则有子式

$$\begin{pmatrix}1&a&\cdots&a^{k-1}\\a&a^2&\cdots&a^k\end{pmatrix}$$

如果k是使$a^k=1$的最小正整数, 则称a是关于1的k阶元. 在有k阶元的CY矩阵中, 有如下的子式

$$C_k=\begin{pmatrix}1&a&a^2&\cdots&a^{k-1}\\a^{k-1}&1&a&\cdots&a^{k-2}\\a^{k-2}&a^{k-1}&1&\cdots&a^{k-3}\\\vdots&\vdots&\vdots&&\vdots\\a&a^2&a^3&\cdots&1\end{pmatrix}$$

C_k叫k阶循环子式, 也可以写成$(1)_{k-1}$, (1)代表集合$\{1,a,\cdots,a^{k-1}\}$. 记号$(a)_r^*$表示元素组$a=\{a_1,a_2,a_3,\cdots,a_p\}$的$p$阶循环子式

$$(a)_r^*=\begin{pmatrix}a_1&a_2&a_3&\cdots&a_p\\a_{1+r}&a_{2+r}&a_{3+r}&\cdots&a_{p+r}\\a_{1+2r}&a_{2+2r}&r&\cdots&a_{p+2r}\\\vdots&\vdots&\vdots&&\vdots\\a_{1+(p-1)r}&r_{2+(p-1)r}&r_{3+(p-1)r}&\cdots&a_{p+(p-1)r}\end{pmatrix}$$

这里, 下标按 $(\mathrm{mod}\ p)$ 计数 (约定 $kp \equiv p\ (\mathrm{mod}\ p)$). r 叫循环的欧拉数, 对一个正整数 n, 每个小于 n 而与 n 互素的正数 (包括 1) 叫关于 n 的**欧拉数**. 关于 n 的全体欧拉数构成一个 $(\mathrm{mod}\ n)$ 的乘法群.

如果 CY 阶矩阵中有如下子式

$$\begin{pmatrix} r & b \\ a & c \end{pmatrix}, \begin{pmatrix} r & a \\ b & d \end{pmatrix}, c \neq d$$

则群非交换. 总之, 群的运算是以子式的形式来表达的. 因为在 F_6^2 中有

$$\begin{pmatrix} 1 & 4 \\ 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 3 \\ 4 & 6 \end{pmatrix}$$

所以 F_6^2 是非交换群.

2. 如果 m 阶 CY 矩阵 G 含有 p 阶循环子式, p 是素数, 则经过适当的交换行或列的变换后可以化成如下分块形式

$$G = \begin{pmatrix} B_{1,1} & B_{1,2} & \cdots & B_{1,r} \\ B_{2,1} & B_{2,2} & \cdots & B_{2,r} \\ \vdots & \vdots & & \vdots \\ B_{r,1} & B_{r,2} & \cdots & B_{r,r} \end{pmatrix} \tag{1.1}$$

其中, 对角线上的块 $B_{i,i}$ 全是相同的 p 阶循环矩阵 C_p. 这就有了以下两种情况.

(1) 对角线之外的块 $B_{i,j}, i \neq j$, 都是 p 阶循环矩阵, 这种分块形式中 (包括 $B_{i,i}$) 共有 r 个不同的循环矩阵块. 这种分块形式叫 p-α 型或简称 α 型. 例如

$$F_6^1 = \left(\begin{array}{ccc|ccc} 1 & 3 & 5 & 2 & 4 & 6 \\ 5 & 1 & 3 & 6 & 2 & 4 \\ 3 & 5 & 1 & 4 & 6 & 2 \\ \hline 2 & 4 & 6 & 1 & 3 & 5 \\ 6 & 2 & 4 & 5 & 1 & 3 \\ 4 & 6 & 2 & 3 & 5 & 1 \end{array}\right) = \begin{pmatrix} (1)_2 & (2)_2 \\ (2)_2 & (1)_2 \end{pmatrix} = C_3 \otimes C_2$$

$$F_6^2 = \left(\begin{array}{ccc|ccc} 1 & 3 & 5 & 2 & 4 & 6 \\ 5 & 1 & 3 & 4 & 6 & 2 \\ 3 & 5 & 1 & 6 & 2 & 4 \\ \hline 2 & 4 & 6 & 1 & 3 & 5 \\ 4 & 6 & 2 & 5 & 1 & 3 \\ 6 & 2 & 4 & 3 & 5 & 1 \end{array}\right) = \begin{pmatrix} (1)_2 & (2)_1 \\ (2)_1 & (1)_2 \end{pmatrix} = C_3 \hat{\otimes} C_2$$

这里块的阶数是默认的, 下标是块的欧拉数. 这是有限群块结构的一个重要参数, 将在后面详细描述. 上面两个6阶群的3×3块结构中, 由于块的欧拉数不同产生了不同的群. $F_6^1=C_3\otimes C_2$表示3阶循环群与2阶循环群的直积, 这与经典群论里的直积是一致的. $F_6^2=C_3\hat{\otimes}C_2$表示3阶循环群与2阶循环群的带有(非平凡)欧拉群参数的直积. 这是本书给出的群的一种新的分解. 当且仅当C_p是F_n的正规子群时C_p确定的分块矩阵是α型的.

(2) 对角线之外存在这样的块$B_{i,j},i\neq j$, 是由不同元素构成的容积为p^2的p阶矩阵. 这种分块矩阵叫p-β型或简称β型. 例如12阶群之一的F_{12}^*的3×3块结构

$$F_{12}^*=\left(\begin{array}{cccc|cccc|cccc}
1&2&3&4&5&6&7&8&9&10&11&12\\
3&1&2&7&8&9&10&11&12&4&5&6\\
2&3&1&10&11&12&4&5&6&7&8&9\\
\hline
4&5&6&1&2&3&11&12&10&9&7&8\\
7&8&9&3&1&2&5&6&4&12&10&11\\
10&11&12&2&3&1&8&9&7&6&4&5\\
\hline
5&6&4&9&7&8&1&2&3&11&12&10\\
8&9&7&12&10&11&3&1&2&5&6&4\\
11&12&10&6&4&5&2&3&1&8&9&7\\
\hline
6&4&5&11&12&10&9&7&8&1&2&3\\
9&7&8&5&6&4&12&10&11&3&1&2\\
12&10&11&8&9&7&6&4&5&2&3&1
\end{array}\right)$$

$$=\left(\begin{array}{cccc}
(1)&d_1^1&d_3^1&d_2^1\\
d_1^1&(1)&d_2^3&d_3^2\\
d_1^3&d_3^2&(1)&d_2^3\\
d_1^2&d_2^3&d_3^2&(1)
\end{array}\right)=C_3\hat{\otimes}_\rho M_{4,8}\tag{1.2}$$

这里d_*^*表示块, 例如

$$d_1^1=\left(\begin{array}{ccc}4&5&6\\7&8&9\\10&11&12\end{array}\right),\ d_3^2=\left(\begin{array}{ccc}9&10&11\\12&7&8\\6&4&5\end{array}\right)$$

上标和下标分别是元素所在的行和列的序号, 又叫旋转数. $M_{4,8}$表示容积为8的4阶Y矩阵. ρ是块d_*^*到自身的映射, 它控制整个结构. 这在后面将会详细论述. 这里C_3不是F_{12}^*的正规子群, 但是作为一个因子它仍然能把群分解. **在经典群论中单群是不能分解的. 在我们的系统中, 除素数阶单群外, 其他单群都是可以分解**

的, 只是分解式中有一个 (非经典群的)Y 群因子. 所以单群的组合分类必然会涉及到Y 群的分类.

令 $B_{i,i}=C_p,(i=1,\cdots,r)$, 在块分解 (1.1) 中选取这样一个子式:

$$M_{r,d}=\begin{pmatrix} 1 & b_{1,2} & b_{1,3} & \cdots & b_{1,r} \\ b_{2,1} & 1 & b_{2,3} & \cdots & b_{2,r} \\ b_{3,1} & b_{3,2} & 1 & \cdots & b_{3,r} \\ \vdots & \vdots & \vdots & & \vdots \\ b_{r,1} & b_{r,2} & b_{r,3} & \cdots & 1 \end{pmatrix}, \quad b_{i,j}\in B_{i,j}$$

它叫做 C_p 除 G 所得的一个**商代表**. 可以证明, 容积相等的商代表是同构的 Y 矩阵. 以 (1.2) 为例, C_3 除 F_{12}^* 所得的商代表共有 4 个, 它们的容量分别是 $4,7,8,10$:

$$M_{4,4}=\begin{pmatrix} 1 & 4 & 8 & 12 \\ 4 & 1 & 12 & 8 \\ 8 & 12 & 1 & 4 \\ 12 & 8 & 4 & 1 \end{pmatrix}, \quad M_{4,7}=\begin{pmatrix} 1 & 10 & 5 & 8 \\ 6 & 1 & 12 & 7 \\ 7 & 12 & 1 & 6 \\ 8 & 5 & 10 & 1 \end{pmatrix}$$

$$M_{4,8}=\begin{pmatrix} 1 & 5 & 8 & 11 \\ 7 & 1 & 6 & 10 \\ 8 & 10 & 1 & 6 \\ 9 & 6 & 10 & 1 \end{pmatrix}, \quad M_{4,10}=\begin{pmatrix} 1 & 5 & 10 & 9 \\ 7 & 1 & 12 & 4 \\ 6 & 12 & 1 & 8 \\ 11 & 4 & 8 & 1 \end{pmatrix}$$

我们有

$$C_3\hat{\otimes}_\rho M_{4,i}=F_{12}^*, \quad i=4,7,8,10$$

商代表表示子群在群中的代数地位, 称为子群在群中的**谱**, 写成

$$SP(3/F_{12}^*)=4\times\{4,7,8,10\}_3^\beta$$

这里, 括号前的整数表示群 F_{12}^* 中有 4 个 3 阶循环, 它们有同样的谱. 群的任意子群都有谱. 一个群的所有 p^k 阶 (p 是素数) 子群的谱是群的不变量. 在附录中我们给出了全体 36 阶群和 12 阶群的谱.

3. 在群的组合结构中有一个重要的概念: Γ 矩阵. 任意一个群 F_n 都有一个子矩阵, 记成 $\Gamma_{p,n}$, p 是 n 的素因子, 它的阶为 $p+\dfrac{n}{p}-1$. $\Gamma_{p,n}$ 可以唯一地扩张成 F_n.

Γ 矩阵在有限群的计数问题中是一个重要角色. 例如 (1.2) 的一个 Γ 矩阵是

$$\Gamma_{3,12}=\left(\begin{array}{ccc|ccc}
1 & 2 & 3 & 4 & 8 & 12 \\
3 & 1 & 2 & 7 & 11 & 6 \\
2 & 3 & 1 & 10 & 5 & 9 \\
\hline
4 & 5 & 6 & 1 & 12 & 8 \\
8 & 9 & 7 & 12 & 1 & 4 \\
12 & 10 & 11 & 8 & 4 & 1
\end{array}\right)$$

其中左上角是3阶循环子矩阵 H_3; 右上角和左下角是由相同的元素构成的子块 A 和 B; 右下角的块 D 中除对角线上元素为1外, 其余元素都是 A 中的元素. 该矩阵包含了群 F_{12}^* 的所有信息, 所以可以唯一地扩张成 F_{12}^*.

从 Γ 矩阵计算群的方法, 以上面 $\Gamma_{3,12}$ 为例, 第一步是写出下面形式的矩阵

$$\left(\begin{array}{ccc|ccc|ccc|ccc}
1 & 2 & 3 & 4 & & & 8 & & & 12 & & \\
3 & 1 & 2 & 7 & & & 11 & & & 6 & & \\
2 & 3 & 1 & 10 & & & 5 & & & 9 & & \\
\hline
4 & 5 & 6 & 1 & 2 & 3 & 12 & & & 8 & & \\
 & & & 3 & 1 & 2 & & & & & & \\
 & & & 2 & 3 & 1 & & & & & & \\
\hline
8 & 9 & 7 & 12 & & & 1 & 2 & 3 & 4 & & \\
 & & & & & & 3 & 1 & 2 & & & \\
 & & & & & & 2 & 3 & 1 & & & \\
\hline
12 & 10 & 11 & 8 & & & 4 & & & 1 & 2 & 3 \\
 & & & & & & & & & 3 & 1 & 2 \\
 & & & & & & & & & 2 & 3 & 1
\end{array}\right)$$

第二步是根据 $\Gamma_{3,12}$ 中的信息, 逐一地把空白处的值 (唯一地) 计算出来. 例如, 在第一块行第二块列

$$B_{1,2}=\left(\begin{array}{ccc}
4 & x_1 & x_2 \\
7 & x_3 & x_4 \\
10 & x_5 & x_6
\end{array}\right)$$

中

$$x_1=F(4,1,2)=5,\quad x_2=F(4,1,3)=6,\quad x_3=F(7,1,2)=8$$
$$x_4=F(7,1,3)=9,\quad x_5=F(10,1,2)=11,\quad x_6=F(10,1,3)=12$$

又如, 在

$$B_{2,3}=\left(\begin{array}{ccc}
12 & t_1 & t_2 \\
x_3 & x_4 & t_5 \\
t_6 & t_7 & t_8
\end{array}\right)$$

中

$$t_1 = F(12,1,2) = 10, \quad t_2 = F(12,1,3) = 11, \quad t_3 = F(3,1,12) = 6$$
$$t_4 = F(6,1,2) = 4, \quad t_5 = F(6,1,3) = 5, \quad t_6 = F(2,1,12) = 9$$
$$t_7 = F(9,1,2) = 7, \quad t_8 = F(9,1,3) = 8$$

构造一个 Γ 矩阵就构造了一个群, 反之亦然. 当给定整数 $m = pn$(p 是素数), 矩阵 $\Gamma_{p,n}$ 的块 H_p 和 A 可以预先固定下来. 满足一定条件的映射 $\rho : A \to A$ 将把块 B 和 D 完全确定下来. 对 ρ 分类, 每一类决定一个群, Γ 矩阵对群的计数起重要作用.

4. 像经典的群表示理论一样, Y 群也有一套(矩阵的)表示理论. 设 Λ_n 是全体 n 阶 $(0,1)$ 矩阵的集合, $(0,1)$ 矩阵是指每行、每列最多有一个 1, 其余元素为零的矩阵. 直接用 Λ_n 的元素表示 Y 群是不行的, 因为奇异 $(0,1)$ 矩阵的乘法具有非零的零因子. 在第 5 章中, 我们按一定条件 σ 对 Λ_n 进行了分类:

$$\tilde{\Lambda}_n = \Lambda_n/\sigma$$

类之间有自然的乘法, 设

$$[\Lambda_n/\sigma] = \{A_1, A_2, \cdots, A_m\}$$

构造一个 n 阶矩阵 $M = \{s_{i,j}\}$

$$s_{i,j} = k \quad \text{如果} \quad (A_k)_{i,j} = 1$$

这里 $(A_k)_{i,j}$ 表示 $(0,1)$ 矩阵 A_k 的 (i,j) 项. 不难证明 M 是 Y 群. Y 群表示理论与经典的群表示理论一样, 是揭示 Y 群结构的基本原理, 而且是有良好计算形式的工具, 特别在计算 Y 群的 p 子群谱方面起着重要作用. 这里涉及到奇异矩阵的特征理论, 在本书中没有展开这方面的工作.

5. 在本书的编码理论中提出了 Y 群码的新问题: 用一个 Y 群给一个形式对象——w 群或 w 环编码的问题. 这里的两个基本概念 w 群和 w 环, 它们与现有编码理论中的编码对象的形式相同, 结构则大不相同. Y 群码的最基本的结构是加法表(和乘法表). 由于有无穷多互不同构的加法表, 所以外形相同的码结构也是无限的. 这就为不同目的的编码提供了更广阔的空间, 例如寻找最好码的问题. 有限群的编码可以说是群的表示之一, 在例 13.2 中显示一个 18 阶群可以用它的 6 阶子群作为加法表来编码. 加法表的扩散和加法表的特征多项式的进一步讨论都是很有趣的问题, 都是值得做专题研究题目的. 在本书中, 我们只是提出了 Y 群的一些可能的发展方向.

第 2 章　Y 矩阵

定义 2.1 设 $[F,\eta,N_p,\Omega]$ 是一个四元组, 其中, F 和 η 是两个映射; Ω 是一个集合; $N_p=\{1,2,\cdots,p\}$ 是前 p 个自然数之集. 映射

$$\eta : N_p \times N_p \to \Omega$$

确定的矩阵:

$$[\eta]=\begin{pmatrix} \eta(1,1) & \eta(1,2) & \cdots & \eta(1,p) \\ \eta(2,1) & \eta(2,2) & \cdots & \eta(2,p) \\ \vdots & \vdots & & \vdots \\ \eta(p,1) & \eta(p,2) & \cdots & \eta(p,p) \end{pmatrix}$$

称为 (由 $[F,\eta,N_p,\Omega]$ 确定的) Y **矩阵**. 它的全体 (2×2) 子式为

$$\begin{pmatrix} \eta(i,r) & \cdots & \eta(i,j) \\ \vdots & & \vdots \\ \eta(s,r) & \cdots & \eta(s,j) \end{pmatrix}, \quad 1\leqslant i,j,r,s\leqslant p$$

定义一个函数:

$$F:\Omega^3\to\Omega$$
$$(\eta(i,r),\eta(s,r),\eta(s,j))\mapsto\eta(i,j)$$

称之为 (由 $[F,\eta,N_p,\Omega]$ 确定的) $\boldsymbol{Y}$ **函数**. 称 $[F,\eta,N_p,\Omega]$ 为 $\boldsymbol{Y}$ **四元组**.

注释 2.1 (1) 为简单起见, 我们说 M 是 Y 矩阵 $[F,\eta,N_p,\Omega]$, 就是说 $M=[\eta]$. 我们也用 $[\eta,N_p,\Omega]$ 表示一般的 $p\times p$ 矩阵.

(2) 定义 2.1中 Y 函数 F 的定义域为 $\mathrm{Im}(\eta)\times\mathrm{Im}(\eta)\times\mathrm{Im}(\eta)$, 这里 $\mathrm{Im}(\eta)$ 是映射 η 的象集合. F 的值域为 $\mathrm{Im}(\eta)$, 当 η 不是满射时, F 在某些点处会没有定义, 这正是 Y 函数的特点. 对 CY 函数 (见下面定义 2.4) 就不会出现上述情况.

(3) 根据上面定义不难看出, 交换 Y 矩阵的行或列, 仍然是一个 Y 矩阵而且不会改变 Y 函数. 容易看出, Y 矩阵的任意子式也是一个 Y 矩阵.

(4) 在不会引起误解时, 我们常常把 Y 矩阵称 Y **群**.