

有限群论基础

王萼芳 编著

清华大学出版社

(京)新登字 158 号

内 容 简 介

本书讲述有限群论的基本知识,内容包括了常用的有限群理论及其表示论的一般概念及结论,具体为:基本概念、正规子群、同态定理、置换群、置换表示、交换群、Sylow 定理、可解群及有限群表示论初步.作者以较少的篇幅完整地阐述了有限群论的基本概念及处理有限群的方法,并介绍了有限群表示的基本概念及常用的结论.

本书是作者根据在北京大学讲授有限群论课程的讲义,进一步修改、充实之后成书的.其内容深入浅出,富有启发性,并配备较多的例子和习题,便于讲授和自学.

学习本书不要求读者学习过抽象代数课程或阅读过这方面的有关书籍.它可用作高等院校有限群论课程的教材,也可供科技工作者作为自学资料或参考书.

图书在版编目(CIP)数据

有限群论基础/王萼芳编著.—北京:清华大学出版社,2002

ISBN 7-302-05535-1

.有... .王... .有限群—群论 .O152 .1

中国版本图书馆 CIP 数据核字(2002)第 037391 号

出 版 者:清华大学出版社(北京清华大学学研大厦,邮编 100084)

<http://www.tup.tsinghua.edu.cn>

责任编辑:刘 颖

版式设计:肖 米

印 刷 者:清华大学印刷厂

发 行 者:新华书店总店北京发行所

开 本:850×1168 1/32 印张:7.125 字数:179 千字

版 次:2002 年 9 月第 1 版 2002 年 9 月第 1 次印刷

书 号:ISBN 7-302-05535-1/O·283

印 数:0001~4000

定 价:12.00 元

前 言

群是抽象代数中最早的而且是最基本的一个代数系统.它也是现代数学中一个极其重要的概念.群论不仅在数学的各个分支有广泛的应用,而且在许多现代科学,诸如结晶学、理论物理、量子力学以及密码学、系统科学、数理经济等领域,群的理论和方法也有很多应用.

有限群论是群论的基础部分,也是群论中应用最为广泛的一个分支.近年来,随着有限群理论的迅速发展及其应用的日益增多,有限群论已经成为现代科技的数学基础之一,是一般科技工作者乐于掌握的一个数学工具.

目前,国内外关于群论的著作及教材很多,但大都为篇幅较大的专著.本书则以较少的篇幅介绍有限群理论及其表示论的基本概念及结论.书中给出较多的例子,通过这些例子能帮助读者理解概念,掌握群论的一些基本方法.

书中附有大量习题,这些习题不仅能帮助读者巩固所学的内容,基本技能得到训练,并且补充了有限群论的一些基本结论.

作者在北京大学讲授有限群论课程时,曾出版过《有限群论基础》(北京大学出版社出版,1986年)一书.本书是在此书基础上进一步修改而成,可以作为开设一学期有限群论课程的教材.

置换群是一类计算方便,应用极为广泛的有限群.本书对置换群的初步理论做了较详细的介绍.

鉴于群表示论对群论本身的重要性以及在其他学科的广泛应用.本书最后一章介绍了有限群表示论的基本理论.如果作为一个

学期课程的教材而学时不够的话,这一章可以不必讲授.

为了适应广大读者的需要,使更多的读者能接受,阅读本书的读者不需要学习过抽象代数或类似的课程或有关书籍.

对于有兴趣研究群论的读者,本书可作为入门教材.使读者对有限群及其表示理论有初步了解,得到初步训练,初步掌握群论方法,为进一步学习群论打好基础.对其他专业的读者及科技工作者,书中内容包含了足够应用的有限群及其表示论的基本概念及理论.

限于作者水平,书中难免有疏漏错误之处,衷心希望读者批评指正.

作 者

2002年3月于北京大学

目 录

| | |
|--------------------------------|-----|
| 第 1 章 基本概念..... | 1 |
| 1.1 群的概念 | 1 |
| 1.2 置换群 | 9 |
| 1.3 子群..... | 18 |
| 1.4 循环群..... | 23 |
| 1.5 群的陪集分解..... | 26 |
| 1.6 同构..... | 33 |
| 1.7 群的置换表示..... | 37 |
| 习题 | 48 |
| 第 2 章 正规子群与同态定理 | 51 |
| 2.1 同态..... | 51 |
| 2.2 共轭子群与共轭元素..... | 56 |
| 2.3 正规子群..... | 64 |
| 2.4 商群 同态定理..... | 70 |
| 2.5 $A_n (n \geq 4)$ 的单性 | 75 |
| 2.6 自同构群..... | 79 |
| 习题 | 88 |
| 第 3 章 置换群的进一步讨论 | 91 |
| 3.1 置换群的一些子群..... | 91 |
| 3.2 传递群..... | 96 |
| 3.3 非传递群 | 102 |
| 3.4 传递群作为群的置换表示 | 106 |

| | |
|---------------------------|-----|
| 3.5 本原性 | 111 |
| 习题..... | 120 |
| 第4章 交换群 | 123 |
| 4.1 直积 | 123 |
| 4.2 基 | 128 |
| 4.3 有限交换群的构造 | 132 |
| 习题..... | 140 |
| 第5章 Sylow 定理 | 143 |
| 5.1 Sylow 定理 | 143 |
| 5.2 有限 p -群 | 151 |
| 5.3 一些特殊 p -群 | 153 |
| 习题..... | 155 |
| 第6章 可解群 | 157 |
| 6.1 合成群列 | 157 |
| 6.2 可解群 | 164 |
| 6.3 亚循环群、幂零群和超可解群..... | 170 |
| 习题..... | 174 |
| 第7章 有限群表示论初步 | 177 |
| 7.1 线性群 | 177 |
| 7.2 群的表示和特征标 | 183 |
| 7.3 正交关系 | 191 |
| 7.4 有限群不可约表示的个数 | 199 |
| 7.5 几个应用 | 213 |
| 习题..... | 216 |
| 复习题..... | 218 |

第1章 基本概念

这一章介绍群的定义和一些基本概念及性质.并在1.2节中详细介绍置换和置换群的概念,作为进一步研究一般群和置换群的基础.

1.1 群的概念

1 群的定义

定义1 设 G 是一个非空集合,在 G 中定义了一种代数运算,称为乘法,记作“ \cdot ”.即对于 G 中任意两个元素 a, b ,都唯一确定 G 中一个元素 $a \cdot b$,称为 a, b 的乘积.如果 G 对这种运算满足下面几个条件:

1) 结合律 对 G 中任意3个元素 a, b, c ,都有

$$(a \cdot b) \cdot c = a \cdot (b \cdot c);$$

2) 单位元素的存在 G 中存在一个元素 e ,对于 G 中任意元素 a ,都有

$$e \cdot a = a \cdot e = a;$$

3) 逆元素的存在 对于 G 中任一个元素 a ,都可找到 G 中一个元素 a^{-1} ,使得

$$a^{-1} \cdot a = a \cdot a^{-1} = e,$$

那么 G 就称为一个群.元素 e 称为 G 的单位元素, a^{-1} 称为 a 的逆元素.

定义 2 如果群 G 还满足:

4) 交换律 对于 G 中任意两个元素 a, b , 都有

$$a \cdot b = b \cdot a,$$

那么 G 就称作一个交换群或阿贝尔群.

如果群 G 的运算不满足交换律, 则称 G 为非交换群.

为了简便起见, 在不致混淆的情况下, 我们常用 ab 表示 a 与 b 的乘积.

有时候, 有些交换群的运算用加法表示, 记作“+”, $a+b$ 称为 a 与 b 的和. 那么条件 1) ~ 4) 就成为:

1) 结合律 对 G 中任意 3 个元素 a, b, c , 都有

$$(a + b) + c = a + (b + c);$$

2) 零元素的存在 G 中存在一个元素 0 , 对于 G 中任一个元素 a , 都有

$$0 + a = a + 0 = a;$$

3) 负元素的存在 对于 G 中任一个元素 a , 都可找到 G 中一个元素 $-a$, 使得

$$(-a) + a = a + (-a) = 0;$$

4) 交换律 对于 G 中任意两个元素 a, b , 都有

$$a + b = b + a.$$

0 称为 G 的零元素, $-a$ 称为 a 的负元素.

2 群的例子

例 1 全体整数所成的集合 Z 对于数的加法成一交换群. 因为 Z 对数的加法满足条件 1) ~ 4), 群 Z 的零元素就是整数 0 , 整数 n 的负元素就是 $-n$.

同样地, 全体有理数所成集合 Q , 全体实数所成集合 R , 全体复数所成集合 C , 对于数的加法也都成为交换群.

例 2 全体非零有理数 Q^* , 全体非零实数 R^* , 全体非零复数 C^* 对数的乘法都构成交换群.

但是全体非零整数对数的乘法不构成群, 因为不满足条件 3). 全体正整数对数的加法也不构成群, 因为不满足条件 2) 及 3).

例 3 n 是一个正整数. 全部 n 次单位根所成集合 U_n 对于数的乘法组成一个交换群.

例 4 用 $M_{n,m}(R)$ 表示全部 $n \times m$ 实矩阵所成的集合. $M_{n,m}(R)$ 对矩阵的加法构成一个交换群.

例 5 F 是一个域, 用 $GL_n(F)$ 表示 F 上全部 n 阶可逆矩阵所成的集合. $GL_n(F)$ 对矩阵的乘法构成一个群, 称为 F 上 n 级一般线性群. 当 $n = 2$ 时, $GL_n(F)$ 是非交换的.

例 6 用 $SL_n(F)$ 表示域 F 上全部行列式等于 1 的矩阵组成的集合. $SL_n(F)$ 对矩阵的乘法构成一个群, 称为 F 上 n 级特殊线性群. 当 $n = 2$ 时, $SL_n(F)$ 是非交换的.

例 7 设 V 是域 F 上一个 n 维线性空间, 用 $GL_n(V)$ 表示 V 的全部可逆线性变换所成的集合. $GL_n(V)$ 对变换的乘法构成一个群. 当 $n = 2$ 时, 这个群是非交换的.

例 8 设 F 是一个域, F 对 F 的加法构成一个交换群. F 中非零元素的集合 F^* 对 F 的乘法也成为一个交换群.

例 9 设 V 是域 F 上一个线性空间. V 对向量的加法构成一

个交换群 .

例 10 设 $G = \{a, b, c, d\}$.用下列乘法表定义 G 的运算:

| | | | | |
|-----|-----|-----|-----|-----|
| | a | b | c | d |
| a | a | b | c | d |
| b | b | a | d | c |
| c | c | d | a | b |
| d | d | c | b | a |

表中第 i 行第 j 列处的元素表示左边的第 i 个元素与表上边第 j 个元素之积 .例如, 上表说明

$$a \cdot a = a, \quad b \cdot c = d,$$

等等 .

请读者自己验证 G 对这个运算构成一个交换群 .

用乘法表来给出一个群是常常采用的方法, 我们在以后还会遇到 .

3 简单性质

从群的定义, 可以推出下面的一些性质:

1) 群中单位元素是唯一的 .

证明 设 G 是一个群, e 是 G 的单位元素 .如果 e 也是 G 的单位元素, 那么, 因为 e 是单位元素, 所以

$$e \cdot e = e .$$

又因 e 也是单位元素, 所以

$$e \cdot e = e .$$

因此, 必须有

$$e = e,$$

所以 G 的单位元素是唯一的 x

2) 在群中, 每个元素只有一个逆元素.

证明 设 a 是群 G 中的一个元素, e 是 G 的单位元素, a^{-1} 是 a 的逆元素. 如果 a 也是 a 的逆元素, 那么, 根据逆元素的定义, 有

$$\begin{aligned}(a \cdot a)a^{-1} &= e \cdot a^{-1} = a^{-1}, \\ a \cdot (a \cdot a^{-1}) &= a \cdot e = a.\end{aligned}$$

由结合律, 即得

$$a = a^{-1}.$$

所以逆元素是唯一的 x

由逆元素的唯一性, 可得

$$3) (a^{-1})^{-1} = a.$$

4) 群中消去律成立, 即: 如果 $ab = ac$, 则有 $b = c$; 如果 $ba = ca$, 则有 $b = c$.

证明 设 $ab = ac$. 用 a^{-1} 左乘等式两端, 得

$$a^{-1}(ab) = a^{-1}(ac).$$

于是

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

从而

$$eb = ec, \quad b = c.$$

同样可证第二个等式 x

5) 在群中,对于任意两个元素 a, b , 方程

$$ax = b \quad \text{及} \quad ya = b$$

都有解,而且解是唯一的.

证明 显然,元素 $a^{-1}b$ 及 ba^{-1} 分别是这两个方程的解,解的唯一性可由消去律得出 x

需要注意的是,因为群中交换律不一定成立,所以上面两个方程的解一般是不相等的,只有在 a 与 b 可交换,即 $ab = ba$ 时,这两个解才相等.

对于群中一个元素 a ,我们把 $n(n > 0)$ 个 a 相乘所得的元素记作 a^n , 即

$$a \cdot a \cdot \dots \cdot a = a^n .$$

n 个

对于负整数 $-n(n > 0)$, 规定

$$a^{-n} = (a^{-1})^n ,$$

并约定 a^0 表示群的单位元素. a^n (n 为任意整数) 称为 a 的方幂. 根据结合律, 可知

6) 群中指数律成立, 即

$$a^n \cdot a^m = a^{n+m}, \quad n, m \text{ 为任意整数};$$

$$(a^n)^m = a^{nm}, \quad n, m \text{ 为任意整数} .$$

如果 $ab = ba$, 则有

$$(ab)^n = a^n b^n, \quad n \text{ 为任意整数} .$$

如果所讨论的群是交换群, 而且群的运算用加法表示, 那么, 上面的一些性质可以叙述为:

- 1) 群中只有一个零元素 .
- 2) 在群中, 每个元素只有一个负元素 .
- 3) $-(-a) = a$.

以后, 常用 $a - b$ 表示 $a + (-b)$.

- 4) 如果 $a + b = a + c$, 则有 $b = c$.
- 5) 对于任意两个元素 a, b , 方程

$$a + x = b$$

有唯一解 $x = b - a$.

对于加法交换群来说, 一个元素的方幂就是这个元素的倍数 . 当 $n > 0$ 时, 我们用 na 表示 n 个 a 相加所得之和, 即

$$\underbrace{a + a + \dots + a}_{n \text{ 个}} = na .$$

规定

$$(-n)a = -(na),$$

并约定 $0a$ 表示群的零元素 . 于是下列倍数律成立:

- 6) $na + ma = (n + m)a$, n, m 为任意整数;
- $m(na) = mna$, n, m 为任意整数;
- $n(a + b) = na + nb$, n 为任意整数 .

4 阶

定义 3 如果群 G 包含的元素个数有限, 则称 G 为有限群 . 否则称 G 为无限群 . 有限群 G 所包含的元素个数称为 G 的阶 .

定义 4 设 a 是群 G 中一个元素, 如果存在正整数 k 使得 $a^k = e$, 则 a 称为有限阶元素 . 满足 $a^k = e$ 的最小正整数 k 叫做 a 的阶 . 如果不存在正整数 k 使得 $a^k = e$, 则 a 称为无限阶元素 .

定义中的条件 $a^k = e$ 在加法群时应改为 $ka = e$. 以后我们只讨

论乘法群,而对加法群的情形就不另外说明了.

例如,在前面所举的群例中,例3中的群的阶等于 n ;例10中的群的阶等于4;其余的群,除例8外,都是无限群.至于例8中的群则要根据域 F 来决定:当 F 是无限域时,加法群 F 及乘法群都是无限群.当 F 是有限域时,加法群 F 的阶等于 F 中元素数 $|F|$;而乘法群 F^* 的阶 $|F^*|$ 等于 $|F| - 1$.

在例1中,除去零元素的阶等于1外,其他元素都是无限阶元素.在例10中,单位元素 a 是1阶元素,其他元素的阶都等于2.

从定义可以看出,在一个群中,单位元素(零元素,如果是加法群)是唯一的一个1阶元素.

我们以后主要讨论有限群.有限群中的元素一定都是有限阶元素.这个事实可以这样来证明,设 a 是有限群 G 中一个元素.考虑下列元素

$$a, a^2, a^3, \dots$$

由于 G 是一个有限群,所以这些元素中一定有相同的.即有正整数 $k_1 < k_2$,使得

$$a^{k_1} = a^{k_2}.$$

于是

$$a^{k_2 - k_1} = e, \quad k_2 - k_1 > 0.$$

根据定义, a 是一个有限阶元素.

如果一个群中的所有元素都是有限阶元素,那么这个群称为周期群.有限群一定是周期群.

关于元素的阶有下述重要性质.

定理 1 如果 a 是群 G 的一个 k 阶元素, e 是 G 的单位元素.那么

- 1) $a^l = e \quad k | l$;
- 2) $a^l = a^m \quad k | l - m$.

如果 a 是一个无限阶元素, 那么

$$a^l = a^m \quad l = m.$$

证明 1) 如果 $k|l$, 那么可设 $l = kd$, d 是一个整数.
于是

$$a^l = a^{kd} = (a^k)^d = e^d = e.$$

反之, 如果 $k \nmid l$, 可设

$$l = kd + r, \quad 0 < r < k.$$

于是

$$a^l = a^{kd+r} = a^{kd} \cdot a^r = e \cdot a^r = a^r \neq e.$$

2) 因为

$$a^l = a^m \quad a^{l-m} = e,$$

故由 1) 即得

$$a^l = a^m \quad k|l - m.$$

关于无限阶元素的结论可以从定义直接得到 x

关于群及元素的阶还有一些重要的性质. 请读者参考本章习题.

1 2 置 换 群

置换群是一类最重要的有限群. 作为群的例子, 这一节介绍置换及置换群的概念. 关于置换的进一步性质, 将在第 3 章中讨论.

1 置换及对称群

设 S_n 是由 n 个文字组成的集合:

$$S_n = \{ 1, 2, \dots, n \}.$$

到自身的一个一一映射称为 (作用于) 上的一个置换, 或 n 元置换, 简称置换. 有时候也称为 $1, 2, \dots, n$ 的一个置换.

设 σ 是 $S = \{1, 2, \dots, n\}$ 上的一个置换. 用 $\sigma_i (i = 1, 2, \dots, n)$ 表示 i 在 σ 下的象, 而把 σ 表成

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma_1 & \sigma_2 & \dots & \sigma_n \end{pmatrix},$$

或者可以简单地表成

$$\sigma = \begin{pmatrix} i \\ i \end{pmatrix}.$$

为了简单起见, 有时常用 $1, 2, \dots, n$ 表示 S 的 n 个元素, 此时, σ 就可表成

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma_1 & \sigma_2 & \dots & \sigma_n \end{pmatrix} = \begin{pmatrix} i \\ i \end{pmatrix}.$$

因为 σ 是一个一一映射, 所以 $\sigma_1, \sigma_2, \dots, \sigma_n$ 是 $1, 2, \dots, n$ 的一个排列. 两个不同的置换 σ, τ 所对应的排列 $\sigma_1, \sigma_2, \dots, \sigma_n$ 与 $\tau_1, \tau_2, \dots, \tau_n$ 是不同的. 而且, 任给 $1, 2, \dots, n$ 的一个排列 $\tau_1, \tau_2, \dots, \tau_n$, 都有唯一的一个置换 τ 使得

$$\tau_i = \tau_i, \quad i = 1, 2, \dots, n,$$

即

$$\tau = \begin{pmatrix} 1 & 2 & \dots & n \\ \tau_1 & \tau_2 & \dots & \tau_n \end{pmatrix}.$$

因此 n 元置换与 n 元排列之间有一个一一对应. 我们知道 n 元排列一共有 $n!$ 个, 所以一共有 $n!$ 个 n 元置换. 我们用 S_n 表示这 $n!$ 个 n 元置换所成的集合. 例如, 一共有 6 个 3 元置换:

$$\begin{aligned} \sigma_1 &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, & \sigma_2 &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \\ \sigma_3 &= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, & \sigma_4 &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \end{aligned}$$

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

即 $S_3 = \{ 1, 2, 3, 4, 5, 6 \}$ 包含 6 个元素.

在 S_n 中可以按照映射的乘法定义运算. 设 σ, τ 是 $1, 2, \dots, n$ 的两个置换, 那么我们规定 $\sigma\tau$ 的乘积 为将 τ 连续作用, 即

$$(\sigma\tau)(i) = \sigma(\tau(i)), \quad i = 1, 2, \dots, n.$$

例如, 4 元置换

$${}^1 = \begin{matrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{matrix} \quad \text{与} \quad {}^2 = \begin{matrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{matrix}$$

的乘积为

$${}^1 {}^2 = \begin{matrix} 1 & 2 & 3 & 4 & 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 & 2 & 1 & 4 & 3 \end{matrix} = \begin{matrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{matrix}.$$

置换的乘法有下述一些性质:

1) 满足结合律

$$(\sigma\tau)\rho = \sigma(\tau\rho), \quad \sigma, \tau, \rho \in S_n;$$

2) n 元恒等置换

$$e = \begin{matrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{matrix}$$

是 S_n 的单位元素

$$e\sigma = \sigma e = \sigma, \quad \sigma \in S_n;$$

3) 每个 n 元置换在 S_n 中都有逆元素

$$\begin{matrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{matrix}^{-1} = \begin{matrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{matrix}.$$

因此, 我们有下面的定理.

定理 2 n 元置换全体组成的集合 S_n 对置换的乘法构成一个群, 称为 n 元对称群, 其阶为 $n!$.

需要注意的是, 当 $n \geq 3$ 时, S_n 是非交换的. 例如对上面例子

中的 σ, τ , 就有

$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix}.$$

例 1 $S_2 = \{e, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}\}$ 是一个 2 阶交换群.

例 2 $S_3 = \{1 = e, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6\}$ (σ_i 的定义如前) 是一个 6 阶非交换群. S_3 的运算可以用下列乘法表给出:

| | e | 2 | 3 | 4 | 5 | 6 |
|-----|-----|-----|-----|-----|-----|-----|
| e | e | 2 | 3 | 4 | 5 | 6 |
| 2 | 2 | e | 6 | 5 | 4 | 3 |
| 3 | 3 | 5 | e | 6 | 2 | 4 |
| 4 | 4 | 6 | 5 | e | 3 | 2 |
| 5 | 5 | 3 | 4 | 2 | 6 | e |
| 6 | 6 | 4 | 2 | 3 | e | 5 |

2 置换的轮换表法

这一小节介绍置换的轮换表法.

首先看几个例子. 在 S_3 中, σ_2 将 1 映到 2, 2 映到 3, 3 映到 1, 我们将它表成 $(1, 2, 3)$; σ_3 将 1 保持不变, 将 2 映到 3, 3 映到 2, 我们将它表成 $(1)(2, 3)$, 或简单地表成 $(2, 3)$.

一般地, 如果 n 元置换 σ 把 n 个文字中的一部分 $1, 2, \dots, m$ ($m \leq n$) 作如下变换:

$$1 \rightarrow 2, \quad 2 \rightarrow 3, \quad \dots, \quad m-1 \rightarrow m, \quad m \rightarrow 1,$$

而把其余 $n - m$ 个文字保持不变, 则称 σ 为一个 m -轮换, 简称轮换, 记作

$$= (1, 2, \dots, m).$$

m 称为轮换的长度.当 $m=1$ 时,就是恒等置换.当 $m=2$ 时,只把两个文字互换,而保持其余的文字不变,称为一个对换.显然有

$$(1, 2, \dots, m) = (i, i+1, \dots, m, 1, \dots, i-1), \quad 1 < i < m.$$

两个轮换 $\sigma = (1, 2, \dots, m)$ 与 $\tau = (1, 2, \dots, l)$ 称为不相交的,如果 $1, 2, \dots, m$ 与 $1, 2, \dots, l$ 是各不相同的.

很容易看出,不相交的轮换是可交换的.

定理 3 任何一个置换都可表成一些不相交的轮换的乘积,而且表法(除轮换的次序外)是唯一的.

证明 设 σ 是 $1, 2, \dots, n$ 的一个置换.任取 $1, 2, \dots, n$ 中的一个,设为 a_0 .作序列

$$a_0, a_1, a_2, \dots.$$

因为

$$\sigma^k \{1, 2, \dots, n\} \quad (k = 0, 1, 2, \dots),$$

因此这个序列一定包含重复的文字.设 a_m 是其中第一个在前面出现过的文字,并设它与 a_i ($0 < i < m$) 相同,于是 a_0, a_1, \dots, a_{m-1} 各不相同.如果 $i=0$,那么由

$$a_i = a_m$$

可推出

$$\sigma^{i-1}(a_0) = \sigma^{m-1}(a_0),$$

即将两个不同的文字 a_{i-1} 与 a_{m-1} 映到相同的文字,这是不可能的.所以 $i=0$,即 $a_m = a_0$.作轮换

$$\sigma_1 = (a_0, a_1, \dots, a_{m-1}),$$

则 σ 与 σ_1 在 a_0, a_1, \dots, a_{m-1} 上的作用相同.

如果 $m=n$,那么 $\sigma = \sigma_1$ 是一个轮换.如果 $m < n$,在 $1, 2, \dots, n$ 中去掉 a_0, a_1, \dots, a_{m-1} 后,在剩下的文字中任取一个 a ,仿照上面的方法可以得到一个轮换

$$\sigma_2 = (\sigma_1, \dots, \sigma_{r-1}),$$

与 σ_2 在 $\sigma_1, \dots, \sigma_{r-1}$ 上的作用相同. 因为 σ_1 是一一映射, 所以 σ_1 与 σ_2 不相交.

这样继续下去, 直到 $1, 2, \dots, n$ 用完为止, 我们就得到一些不相交的轮换 $\sigma_1, \sigma_2, \dots, \sigma_s$, 使

$$\sigma = \sigma_1 \sigma_2 \dots \sigma_s.$$

表法的唯一性是很明显的. σ

例 3

$$\begin{aligned} & \begin{array}{cccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ = & 3 & 1 & 5 & 4 & 2 & 8 & 7 & 6 \end{array} \\ & = (1, 3, 5, 2)(4)(6, 8)(7). \end{aligned}$$

置换的这种表法称为置换的轮换表法. 如果在置换 σ 的轮换表法中, x 是一个文字组成一个轮换, 那么 $\sigma(x) = x$, 即 x 保持不变. 为了简单起见, 在轮换表法中可以把这样的轮换省略不写. 这种简单的表法, 称为 σ 的轮换表法的省略形式. 例如, 例 3 中 σ 的轮换表法的省略形式为

$$(1, 3, 5, 2)(6, 8).$$

恒等置换保持每个文字都不变, 我们可以任取一个文字把它表成一个 1-轮换, 例如 (1) . 不过, 我们常用 e 表示恒等置换.

应用置换的轮换表法, 可以很容易计算置换的阶. 一个长度为 l 的轮换的阶为 l . 一般地, 如果 σ 的轮换表法是

$$\sigma = \sigma_1 \sigma_2 \dots \sigma_s,$$

其中 σ_i 的长度为 l_i ($i = 1, 2, \dots, s$), 那么 σ 的阶等于 l_1, l_2, \dots, l_s 的最小公倍数 $[l_1, l_2, \dots, l_s]$. 下面我们来证明这个结论.

设 σ 的阶为 d . 记 $[l_1, l_2, \dots, l_s] = m$. 则因

$$\sigma^m = \sigma_1^m \sigma_2^m \dots \sigma_s^m = e,$$

所以

$$d \mid m .$$

另一方面, 因为

$$d = \overset{d}{1} \overset{d}{2} \dots \overset{d}{s} = e,$$

而 $\overset{d}{1}, \overset{d}{2}, \dots, \overset{d}{s}$ 没有公共文字, 故

$$\overset{d}{1} = \overset{d}{2} = \dots = \overset{d}{s} = e,$$

因此

$$li \mid d, \quad i = 1, 2, \dots, s,$$

由最小公倍数的性质, 知 $m \mid d$.

综上得

$$d = m .$$

例 4 试求置换

$$= \begin{array}{cccccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 2 & 8 & 6 & 9 & 1 & 12 & 10 & 4 & 5 & 7 & 3 & 11 \end{array}$$

的阶 .

解 因为 的轮换表法为

$$(1, 2, 8, 4, 9, 5)(3, 6, 12, 11)(7, 10),$$

所以 的阶等于 6, 4, 2 的最小公倍数, 为 12 .

置换的轮换表法有许多方便的地方, 读者将在以后看到轮换表法的一些应用 .

3 置换的奇偶性 交错群

因为每个轮换都可表成一些对换的乘积:

$$(\overset{1}{1}, \overset{2}{2}, \dots, \overset{m}{m}) = (\overset{1}{1}, \overset{2}{2})(\overset{1}{1}, \overset{3}{3}) \dots (\overset{1}{1}, \overset{m}{m}),$$

因此, 每个置换也都可以表成对换的乘积 . 但是, 一个置换表成对换的乘积的方法不是唯一的 . 例如

$$\begin{aligned}
 &= \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{array} = (1, 2, 3)(4, 5) \\
 &= (1, 2)(1, 3)(4, 5) = (2, 3)(1, 2)(4, 5) \\
 &= (2, 3)(1, 2)(1, 3)(4, 5)(1, 3).
 \end{aligned}$$

然而, 我们可以证明下述定理.

定理 4 n 元置换 表成对换的乘积后, 乘积中对换个数的奇偶由 唯一确定, 而且与 n 元排列 $1, 2, \dots, n$ 的奇偶一致.

证明 设 表成 m 个对换的乘积:

$$= \tau_1 \tau_2 \dots \tau_m.$$

我们来证明 m 的奇偶与 n 元排列 $1, 2, \dots, n$ 的奇偶一致. 将排列 $1, 2, \dots, n$ 变成排列 $1, 2, \dots, n$, 因此将 m 个对换 $\tau_1, \tau_2, \dots, \tau_m$ 依次连续作用于排列 $1, 2, \dots, n$ 也得到排列 $1, 2, \dots, n$. 我们知道对换改变排列的奇偶, 所以作 m 次对换就将排列的奇偶改变 m 次. 由于 $1, 2, \dots, n$ 是一个偶排列, 所以排列 $1, 2, \dots, n$ 的奇偶与 m 一致. 因此 m 的奇偶由 唯一确定.

根据这个定理, 我们可以定义置换的奇偶性.

定义 5 如果 n 元置换 可以表成奇数个对换的乘积, 则称为奇置换; 如果 可以表成偶数个对换的乘积, 则称为偶置换.

由定义可知: 如果 $1, 2, \dots, n$ 是一个奇排列, 则 是一个奇置换; 如果 $1, 2, \dots, n$ 是一个偶排列, 则 是一个偶置换.

从定义还知, 在 $n!$ 个 n 元置换中, 奇、偶置换的个数相同, 各有 $\frac{n!}{2}$ 个. 恒等置换是偶置换. 两个偶置换之积是偶置换. 偶置换的

逆置换也是偶置换 .

因此有下面的定理 .

定理 5 n 元偶置换全体对置换的乘法构成一个群, 其阶为 $n!/2$.

以后我们用 A_n 表示全部 n 元偶置换所成的群, 称为 n 元交错群 .

4 置换群

最后来讨论置换群 .

由 n 元置换组成的群称为 n 元置换群, 简称置换群 . 例如, n 元对称群及 n 元交错群都是 n 元置换群 . 我们还可举出一些例子, 这些例子在以后的讨论中还会用到 .

例 5 $G = \{e, (1, 2, 3), (1, 3, 2)\}$ 是一个 3 元置换群, 它的阶等于 3 .

例 6 $G = \{e, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}$ 是一个 4 阶 4 元置换群 .

例 7 $G = \{e, (1, 2), (3, 4), (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3), (1, 3, 2, 4), (1, 4, 2, 3)\}$ 是一个 8 阶 4 元置换群 .

例 8 仅由恒等置换组成的群也是一个置换群 .

为了确切起见, 我们称一个置换实际变动的文字个数为这个置换的次数, 而称一个置换群实际变动的文字个数为这个群的次

数.例如, $(1, 2, 3)$ 可以说是一个3元置换,也可以说是一个4元置换,等等,但是它是一个3次置换.又如,例5中的置换群可以看成3元置换群,也可看成是4元置换群等,但是它是一个3次置换群.

置换群的计算在代数学中占有很重要的地位.给定了一个正整数 n 以后,决定全部 n 次置换群是置换群理论中一个重要的问题.当 $n = 11$ 时, n 次置换群已经全部找出,而当 n 较大时,只能找出一些具有特殊性质的 n 次置换群,有关置换群的进一步结论将在以后再介绍.

1.3 子群

1 定义及例

定义 6 G 是一个群,如果 G 的一个子集 H 对 G 的运算构成一个群,则称 H 是 G 的一个子群.如果 G 的子群 H 不等于 G ,则称 H 是 G 的一个真子群.

我们用 $H \leq G$ (或 $G \supseteq H$)表示 H 是 G 的子群,用 $H < G$ (或 $G > H$)表示 H 是 G 的真子群.

任何一个群 G 都有两个明显的子群,一个是由一个单位元素组成的子群 $\{e\}$,称为 G 的单位子群;还有一个就是 G 本身.这两个子群称为 G 的平凡子群,其余的子群(如果存在的话)称为非平凡子群.

下面再来看一些例子.

例 1 由全部偶数组成的集合对数的加法组成一个群,是加法群 \mathbb{Z} 的一个子群.

例 2 复数加法群 C 以实数加法群 R , 有理数加法群 Q 及整数加法群 Z 为真子群:

$$C > R > Q > Z .$$

例 3 关于非零复数所成的乘法群也有类似的结果:

$$C^* > R^* > Q^* .$$

例 4 行列式等于 1 的 n 级实矩阵全体对矩阵的乘法组成一个群, 是 n 级可逆实矩阵群 $M_n(R)$ 的一个真子群 .

例 5 n 元交错群 A_n 是 n 元对称群的一个真子群 .

例 6 任一个 n 元置换群都是 n 元对称群的子群 .

需要注意的是, G 的子群 H 不只是一个包含在 G 中的群, 而且 H 的运算必须与 G 的运算一样 . 例如, 乘法群 R^* 不能看成加法群 R 的子群 .

因为群 G 的子群 H 的运算与 G 的运算一样, 所以 H 的单位元素就是 G 的单位元素, H 中任一元素 a 在 H 中的逆元素也就是 a 在 G 中的逆元素 .

2 判别条件

群 G 的一个子集 H 满足什么条件才能成为 G 的一个子群呢? 我们来分析群 G 的子集 H 对 G 的运算是一个群的条件 . 首先 H 必须是非空的 . 其次, 如果 a, b 在 H 中, 那么它们的乘积必须也在 H 中, 即 H 对 G 的运算是封闭的 . 下面再来考察群的三个条件 . 因为 H 包含在 G 中, 所以结合律当然成立, 这一条可以不必检验 . 由于子群的单位元素即群的单位元素, 子群中元素的逆元素

就是它在群中的逆元素.所以只要检查 G 的单位元素及 H 中元素的逆元素是否在 H 中,而且从 H 中元素的逆元素在 H 中以及 H 对运算的封闭性可以推出单位元素在 H 中,因此可以总结为下列判别条件.

判别条件一 H 是群 G 的一个非空子集. H 是 G 的子群的充分必要条件是:

- 1) 如果 $a, b \in H$, 则 $ab \in H$;
- 2) 如果 $a \in H$, 则 $a^{-1} \in H$.

证明 条件的必要性是显然的.为了证明充分性,只要证明单位元素 e 属于 H 就行了.因为 H 是非空集合,可取 $a \in H$.由 2), $a^{-1} \in H$.再由 1), $aa^{-1} = e \in H$.

这两个条件还可以综合成一条,这就是

判别条件二 群 G 的非空子集 H 是一个子群的充分必要条件是:如果 $a, b \in H$, 则 $ab^{-1} \in H$.

证明 条件的必要性是显然的.现在来证条件的充分性.设 G 的非空子集 H 满足判别条件二.任取 $a \in H$, 则 $aa^{-1} = e \in H$, 由此又有 $ea^{-1} = a^{-1} \in H$.对于 H 中任两个元素 a, b , 上面已证 $b^{-1} \in H$, 于是 $a(b^{-1})^{-1} = ab \in H$.所以判别条件一成立, H 是 G 的一个子群.

对于有限子群来说,有以下更简单的判别条件.

判别条件三 设 H 是群 G 的一个有限非空子集, 则 H 是 G

的子群的充分必要条件是 H 对 G 的运算是封闭的, 即, 如果 $a, b \in H$, 则 $ab \in H$.

证明 条件的必要性是显然的. 为了证明充分性, 根据判别条件一, 只要证明对于任意 $a \in H$, 都有 $a^{-1} \in H$. 下面来证明这一点.

设 a 是 H 中任一元素. 因为 H 对运算是封闭的, 所以 a 的正方幂也都属于 H . 又因 H 是一个有限集合, 所以一定有自然数 l, m 使得 $a^l = a^m$ 并且 $l > m + 1$. 于是 $l - m - 1$ 是正整数, $a^{l-m-1} = a^{-1} \in H$. 由判别条件一, H 是 G 的一个子群. \square

如果 G 是一个有限群, 那么 G 的子集都是有限集, 因此总可以应用判别条件三来判断 G 的非空子集是否是一个子群.

例 7 在整数加法群 \mathbf{Z} 中任意取定一个整数 n , 由 n 的一切倍数组成的集合记作 $n\mathbf{Z}$:

$$n\mathbf{Z} = \{kn \mid k = 0, \pm 1, \pm 2, \dots\}.$$

因为对于 $n\mathbf{Z}$ 中任意两个元素 mn 及 ln , 都有

$$mn - ln = (m - l)n \in n\mathbf{Z}.$$

所以根据判断条件二, $n\mathbf{Z}$ 是 \mathbf{Z} 的一个子群.

当 $n = 0$ 时, $n\mathbf{Z} = \{0\}$ 是由一个零元素组成的单位子群 (也可称为零子群). 当 $n = \pm 1$ 时, $n\mathbf{Z} = \mathbf{Z}$. 对任意的 n , 都有 $(-n)\mathbf{Z} = n\mathbf{Z}$. 而当 $n = \pm m$ 时, $n\mathbf{Z} = m\mathbf{Z}$.

例 8 n 级正交矩阵全体 O_n 对矩阵的乘法组成一个群.

证明 O_n 是 $M_n(\mathbf{R})$ 的一个非空子集. 因为两个正交矩阵的乘积还是正交矩阵, 正交矩阵的逆矩阵也是正交矩阵, 所以满足判

别条件一, O_n 是 $M_n(\mathbb{R})$ 的一个子群. 因此 O_n 对矩阵的乘法成为一个群. \times

例 9 设 a 是群 G 中一个元素. 用 $\langle a \rangle$ 表示由 a 的一切方幂组成的集合, 则 $\langle a \rangle$ 是 G 的一个子群.

证明 任取 $\langle a \rangle$ 中两个元素 a^l, a^m , 都有

$$a^l (a^m)^{-1} = a^{l-m} \in \langle a \rangle.$$

故由判别条件二, $\langle a \rangle$ 是 G 的一个子群. \times

$\langle a \rangle$ 称为 G 的由 a 生成的循环子群, a 叫做它的生成元. a 的阶等于 a 的阶.

一般地, 由一个元素生成的群称做循环群. 关于这一类群, 我们将在下一节中仔细讨论.

例 10 G 是一个 n 元置换群, 用 G^+ 表示 G 中全部偶置换所成的集合, 则 G^+ 是 G 的一个子群.

证明 因为恒等置换是偶置换, 所以 G^+ 是 G 的有限非空子集. G^+ 中的元素都是 G 中偶置换, 因此它们的乘积仍是 G 中偶置换, 也属于 G^+ . 故由判别条件三, G^+ 是 G 的子群. \times

例 11 G 是一个群, 用 $Z(G)$ 表示 G 中与所有元素都可交换的元素全体:

$$Z(G) = \{a \mid ax = xa, \forall x \in G\}.$$

请读者自己证明 $Z(G)$ 是 G 的一个子群.

$Z(G)$ 称为 G 的中心. $Z(G)$ 中的元素称为 G 的中心元素. 如果

G 的中心是单位子群, 那么 G 称为无中心的. G 是交换群的充分必要条件是 $Z(G) = G$.

例 12 设 H_1, H_2 是群 G 的两个子群. 由 H_1 与 H_2 的公共元素组成的集合 $H_1 \cap H_2$ 称为 H_1 与 H_2 的交:

$$H_1 \cap H_2 = \{a \mid a \in H_1, a \in H_2\}.$$

$H_1 \cap H_2$ 也是 G 的子群.

证明 因为 $e \in H_1 \cap H_2$, 所以 $H_1 \cap H_2$ 是 G 的一个非空子集. 任取 $a, b \in H_1 \cap H_2$. 则 $a, b \in H_1$; $a, b \in H_2$. 因为 H_1, H_2 都是 G 的子群, 所以 $ab^{-1} \in H_1$; $ab^{-1} \in H_2$. 因此 $ab^{-1} \in H_1 \cap H_2$. 由判断条件二, $H_1 \cap H_2$ 是 G 的一个子群. \square

1.4 循环群

1 循环群的定义及生成元

定义 7 如果群 G 的每个元素都能表成一个固定元素 a 的方幂, 那么 G 称为由 a 生成的循环群, 记作 $\langle a \rangle$. a 称为 a 的一个生成元.

根据元素的阶的性质, 可知循环群共有两种类型:

1) 当生成元 a 是无限阶元素时, $\langle a \rangle$ 是一个无限阶循环群:

$$\langle a \rangle = \{\dots, a^{-3}, a^{-2}, a^{-1}, e, a, a^2, a^3, \dots\}.$$

2) 当生成元 a 是有限阶元素时, 如果 a 的阶为 n , 那么这时,

$$\langle a \rangle = \{e, a, a^2, \dots, a^{n-1}\}$$

是一个 n 阶有限群.

例 1 \mathbf{Z} 是由 1 生成的无限循环群. $n\mathbf{Z}$ 是由 n 生成的无限循环群.

例 2 n 个 n 次单位根对数的乘法组成一个 n 阶群 U_n . 设 ζ 是一个 n 次本原单位根, 那么任一个 n 次单位根都可表成 ζ^k 的一个方幂, 因此 U_n 是一个循环群, ζ 是它的一个生成元.

循环群的生成元不是唯一的. 例如, \mathbf{Z} 也可看成是由 -1 生成的循环群. 在例 2 中 ζ 的取法也不是唯一的. 那么, 在一个循环群中, 怎样的元素才能作为生成元呢? 为了解决这个问题, 首先必须弄清楚生成元的条件.

设 a 是由 a 生成的循环群, 如果 a^l 是 a 的一个生成元, 那么 a 中每个元素都可表成 a^l 的方幂. 特别地, a 也可以表成 a^l 的方幂. 设

$$a = (a^l)^m = a^{lm}.$$

如果 a 是无限循环群, 那么 a 是无限阶元素, 所以必须有

$$lm = 1,$$

因此得出

$$l = \pm 1.$$

当然, 容易看出, a 及 a^{-1} 都是 a 的生成元.

如果 a 是一个 n 阶有限群, 那么

$$n \mid lm - 1,$$

因此

$$lm - 1 = nq, \quad lm - nq = 1.$$

这说明 l 必须与 n 互素. 另一方面, 如果 l 与 n 互素, 那么可找到整数 u, v 使

$$un + vl = 1.$$

于是

$$(a^l)^v = a^{l \cdot uv} = a,$$

所以 a 可表成 a^l 的方幂. 因而 a 中任一元素也都可表成 a^l 的方幂, a^l 是 a 的一个生成元.

于是我们得到下面这个定理.

定理 6 1) 无限循环群 a 一共有两个生成元: a 及 a^{-1} .

2) n 阶循环群 a 中, 元素 a^l 是 a 的生成元的充要条件是 $(n, l) = 1$. 所以 a 一共有 (n) 个生成元 ((n) 是欧拉函数).

例 3 设 ϵ 是一个 12 次本原单位根, 则全部 12 次单位根所成的群 U_{12} 是由 ϵ 生成的循环群:

$$U_{12} = \langle \epsilon \rangle = \{ \epsilon^k \mid k = 0, 1, 2, \dots, 11 \}.$$

U_{12} 一共有 $(12) = 4$ 个生成元:

$$\epsilon^5, \epsilon^7, \epsilon^{11}.$$

2 循环群的子群

在循环群 a 中任取一个元素 a^k , 可以生成一个循环群 $\langle a^k \rangle$. 我们来证明 a 的每个子群都可以这样生成, 即循环群的子群都是循环群.

定理 7 1) 无限循环群的非单位子群都是无限循环群.

2) n 阶有限循环群 a 的子群都是循环群, 其阶为 n 的因子, 而且对于 n 的每个因子 d 都有唯一的一个子群以 d 为阶, 因此 a 的子群的个数等于 n 的正因子的个数.

证明 首先证明循环群的子群都是循环群.

设 H 是循环群 a 的一个子群. 如果 H 是单位子群, 那么 H 当然是循环群; 如果 H 不是单位子群, 那么 H 中一定有 a 的正方

幂. 设 a^m 是 H 中指数最小的正方幂, 证明 $H = \langle a^m \rangle$. 任取 H 中一个元素 a^l , 存在整数 q 及 r , 满足

$$l = qm + r, \quad 0 \leq r < m,$$

于是

$$a^l (a^m)^{-q} = a^r \in H.$$

由 m 的取法知必有 $r=0$, 于是 $a^l = (a^m)^q \in H$, 所以

$$H = \langle a^m \rangle.$$

因为无限循环群中的非单位元素都是无限阶元素, 所以无限阶循环群的子群也都是无限循环群.

如果 a 是 n 阶有限群, 则由上面的证明可知 m 能整除 n . 因此 a^m 的阶是 n 的因子 n/m , a^m 的阶也等于 n/m .

对于 n 的任一个因子 d , $\langle a^{n/d} \rangle$ 就是 a 的一个 d 阶子群, 并且从上面的证明知道, a 的 d 阶子群可以由 a 中的 d 阶元素 $a^{n/d}$ 生成, 所以是唯一的.

例 4 因为 12 一共有 6 个正因子: 1, 2, 3, 4, 6, 12, 所以 U_{12} 共有 6 个子群:

$$1 \text{ 阶子群 } H_1 = \langle a^{12} \rangle = \{e\};$$

$$2 \text{ 阶子群 } H_2 = \langle a^6 \rangle = \{e, a^6\};$$

$$3 \text{ 阶子群 } H_3 = \langle a^4 \rangle = \{e, a^4, a^8\};$$

$$4 \text{ 阶子群 } H_4 = \langle a^3 \rangle = \{e, a^3, a^6, a^9\};$$

$$6 \text{ 阶子群 } H_5 = \langle a^2 \rangle = \{e, a^2, a^4, a^6, a^8, a^{10}\};$$

$$12 \text{ 阶子群 } H_6 = \langle a \rangle = U_{12}.$$

1.5 群的陪集分解

设 H 是群 G 的一个子群. 在有些问题中, 为了讨论 G 与 H 的关系, 并且应用 H 来讨论 G , 常常需要将 G 按照子群 H 分解成一

些没有公共元素的子集的并.

例如,在整数加群 \mathbf{Z} 中,所有7的倍数组成一个子群 $7\mathbf{Z}$.其余的数可以按照用7来除所得的余数分类,余数相同的数组成一类.把余数为 i 的类记作 $i+7\mathbf{Z}$:

$$i+7\mathbf{Z} = \{i, i \pm 7, i \pm 14, i \pm 21, \dots\}, \quad i = 1, 2, \dots, 6.$$

而 \mathbf{Z} 可以表成 $7\mathbf{Z}$ 与这些类的并:

$$\mathbf{Z} = 7\mathbf{Z} \cup (1+7\mathbf{Z}) \cup (2+7\mathbf{Z}) \cup \dots \cup (6+7\mathbf{Z}).$$

一般地,我们有下述子群的陪集的概念.

定义 8 设 H 是群 G 的一个子群, a 是 G 中一个元素,用 a 右乘 H 中一切元素所得的集合记作 Ha :

$$Ha = \{xa \mid x \in H\},$$

称为 H 在 G 中的一个右陪集.同样可以定义 H 在 G 中的左陪集 aH :

$$aH = \{ax \mid x \in H\}.$$

以下讨论右陪集.关于右陪集的结果对于左陪集也成立.

子群 H 在 G 中的右陪集有下述一些性质:

1) Ha 中元素个数与 H 一样.

这是因为由 $xa = ya$ 可推出 $x = y$.

2) H 本身也是 H 的一个右陪集: $H = He$. $Ha = H$ 的充分必要条件是 $a \in H$.

3) a 在陪集 Ha 中.

根据这一点,我们把 a 叫做右陪集 Ha 的一个陪集代表.

4) 对于右陪集 Ha 中任一个元素 b , 都有 $Ha = Hb$.

证明 因为 $b \in Ha$, 所以有 $h \in H$ 使 $b = ha$. 于是

$$Hb = Hha = Ha$$

5) $Ha = Hb \iff ab^{-1} \in H$.

6) 任意两个右陪集 Ha 及 Hb 或者相等或者不相交, 即

$$Ha = Hb \text{ 或 } Ha \cap Hb = \emptyset.$$

证明 如果 $Ha \cap Hb \neq \emptyset$, 则它们包含公共元素 c :

$$c \in Ha, \quad c \in Hb,$$

因此, 由 4) 得

$$Ha = Hc, \quad Hb = Hc.$$

因而有 $Ha = Hb$.

由于每个元素 a 都属于一个右陪集 Ha , 故可将有限群 G 对于子群分解成一些互不相交的右陪集的并:

$$G = Ha_1 \cup Ha_2 \cup \dots \cup Ha_r,$$

其中

$$Ha_i \cap Ha_j = \emptyset, \quad i, j = 1, 2, \dots, r, \quad i \neq j.$$

这个式子称为 G 对 H 的(右)陪集分解式. 其中 r 是右陪集的个数, 称为 H 在 G 中的指数, 记作 $|G/H|$. a_1, a_2, \dots, a_r 称为 H 在 G 中的一个右陪集代表系.

类似地, 群 G 也可以表成子群 H 的互不相交的左陪集的并:

$$G = b_1 H \cup b_2 H \cup \dots \cup b_r H,$$

其中

$$b_i H \cap b_j H = \emptyset, \quad i, j = 1, 2, \dots, r, \quad i \neq j,$$

称为 G 对 H 的左陪集分解式. b_1, b_2, \dots, b_r 称为 H 在 G 中的左陪集代表系. 显然, H 在 G 中的右陪集个数与左陪集个数是相等的, 都等于 H 在 G 中的指数.

从一个群对子群的陪集分解式可以得到下列关于群的子群及元素的阶的重要结论.

定理 8 (Lagrange 定理) 群 G 的阶等于子群 H 的阶及 H 在 G 中的指数的乘积, 即

$$|G| = |H| \cdot |G/H|.$$

证明 设 G 对 H 的陪集分解式为

$$G = Ha_1 \cup Ha_2 \cup \dots \cup Ha_r.$$

因为 $|Ha_i| = |H|$, $i = 1, 2, \dots, r$, 所以

$$|G| = |H| \cdot r = |H| \cdot |G/H|.$$

推论 有限群 G 中每个元素的阶都是 G 的阶 $|G|$ 的因子. 如果 G 的阶等于 n , 那么 G 中每个元素都满足方程

$$x^n = e.$$

证明 设 a 是 G 中一个 m 阶元素, 则 $H = \langle a \rangle$ 是 G 的一个 m 阶子群. 根据上述定理, 即得 $m \mid |G|$. 根据元素的阶的性质, 即得另一个结论.

例 1 n 元交错群 A_n 在 n 元对称群 S_n 中的指数为 2:

$$S_n = A_n \cup A_n(1, 2).$$

例 2 考虑上节例 4 中的群 U_{12} 及其 4 阶子群 H_4 ,

$$U_{12} = H_4 \cup H_4 \cup H_4^2,$$

所以 $|U_{12}/H_4| = 3$.

例3 用 G_1 表示 $G = S_n$ 中保持 1 不动的全部置换. 如果 $\sigma \in G_1$, 则 $\sigma(1) = 1$. 因此 $\sigma^{-1}(1) = 1$, $\sigma \in G_1$. 所以 G_1 是 G 的一个子群.

下面来证明 $e, (1, 2), (1, 3), \dots, (1, n)$ 组成 G_1 在 G 中的一个右陪集代表系.

首先, 这 n 个元素属于 G_1 的不同右陪集, 这是因为

$$e(1, i)^{-1} = (1, i) \in G_1, \quad i = 2, 3, \dots, n;$$

$$(1, j)(1, i)^{-1} = (1, j, i) \notin G_1, \quad i, j = 2, 3, \dots, n, \quad i \neq j.$$

所以陪集

$$G_1 = G_1 e, G_1(1, 2), \dots, G_1(1, n)$$

两两不同.

其次, 可证明 G 中任一元素都属于上列陪集中的一个. 对任一 $\sigma \in G$, 如果 $\sigma(1) = 1$, 则 $\sigma \in G_1$; 如果 $\sigma(1) = i \neq 1$, 则

$$\sigma^{-1}(1, i)^{-1} = \sigma^{-1}(1, i) = 1.$$

所以

$$\sigma \in G_1(1, i).$$

因此, $G = S_n$ 对 G_1 的右陪集分解为

$$S_n = G_1 \cup G_1(1, 2) \cup G_1(1, 3) \cup \dots \cup G_1(1, n).$$

$e, (1, 2), (1, 3), \dots, (1, n)$ 是 G_1 在 S_n 中的一个右陪集代表系. G_1 在 S_n 中的指数为 n .

例4 设 G 是一个置换群, 仍用 G^+ 表示 G 中全部偶置换组成的子群. 如果 G 中没有奇置换, 那么 $G = G^+$; 如果 G 中有奇置换, 那么对于 G 中任意两个奇置换 σ, τ , $\sigma\tau^{-1}$ 是 G 中一个偶置换, 因此 $\sigma\tau^{-1} \in G^+$. 这说明 G 中的奇置换都属于 G^+ 的同一个陪集. 任取 G 中一个奇置换 σ , 就可得到 G 对 G^+ 的陪集分解

$$G = G^+ \cup \sigma G^+.$$

可以看出,例 1 是例 4 的一个特例.由例 4 得

$$|G/G^+| = \begin{cases} 1, & \text{如果 } G \text{ 中无奇置换;} \\ 2, & \text{如果 } G \text{ 中有奇置换.} \end{cases}$$

这是关于置换群的一个重要性质,今后常常要用到.

最后,我们来证明关于子群的指数及陪集分解的一个重要性质.

定理 9 设

$$G = H K,$$

则

$$1) |G/K| = |G/H| \cdot |H/K|.$$

2) 如果 G 对 H 的陪集分解为

$$G = Hg^1 \quad Hg^2 \quad \dots \quad Hg^l, \quad Hg^1 = H;$$

H 对 K 的陪集分解为

$$H = Kh_1 \quad Kh_2 \quad \dots \quad Kh_m, \quad Kh_1 = K,$$

则 G 对 K 的陪集分解为

$$G = \bigcup_{\substack{i=1, \dots, m \\ j=1, \dots, l}} Kh_i g_j, \quad Kh_i g_1 = K.$$

3) 如果 G 对 K 的陪集分解为

$$G = Ka_1 \quad Ka_2 \quad \dots \quad Ka_t, \quad Ka_1 = K.$$

那么可以适当地排列 $a_i (i=1, 2, \dots, t)$ 的次序,使得

$$H = Ha_1 = Ka_1 \quad Ka_2 \quad \dots \quad Ka_m,$$

.....

$$Ha_{m+1} = Ka_{m+1} \quad Ka_{m+2} \quad \dots \quad Ka_{2m},$$

.....

$$Ha_{(l-1)m+1} = Ka_{(l-1)m+1} \quad Ka_{(l-1)m+2} \quad \dots \quad Ka_{lm}, \quad (lm = t).$$

而且 G 对 H 的陪集分解为

$$G = Ka_1 \quad Ka_{m+1} \quad \dots \quad Ka_{(l-1)m+1}.$$

证明 1) 因为

$$|G| = |G \setminus H| \cdot |H|, \quad |H| = |H \setminus K| \cdot |K|,$$

所以

$$|G| = |G \setminus H| \cdot |H \setminus K| \cdot |K|,$$

即

$$|G \setminus K| = |G \setminus H| \cdot |H \setminus K|.$$

2) 陪集 $Kh_i g_j$ ($i=1, 2, \dots, m; j=1, 2, \dots, l$) 共有 lm 个, 与 G 对 K 的指数相等, 因此只要证明这些陪集两两不相交就可以了. 如果

$$Kh_i g_j = Kh_i g_j, \quad 1 \leq i, i \leq m, 1 \leq j, j \leq l,$$

则

$$h_i g_j (h_i g_j)^{-1} = h_i g_j g_j^{-1} h_i^{-1} \in K \setminus H.$$

因为 $h_i, h_i^{-1} \in H$, 所以

$$g_j g_j^{-1} \in H.$$

这说明

$$H g_j = H g_j.$$

于是 $g_j = g_j, j = j$. 从而

$$h_i h_i^{-1} \in K.$$

同样的理由可得 $h_i = h_i, i = i$. 因此这 lm 个陪集是两两不相交的.

3) 因为 K 在 H 中的陪集也一定是 K 在 G 中的陪集, 因此一定是 Ka_i ($i=1, 2, \dots, t$) 中的一部分. 可以调动次序使

$$H = Ka_1 \cup Ka_2 \cup \dots \cup Ka_m \quad (m = |K \setminus H|),$$

于是 $a_{m+1} \in H$. 考虑 H 的陪集

$$Ha_{m+1} = Ka_1 a_{m+1} \cup Ka_2 a_{m+1} \cup \dots \cup Ka_m a_{m+1},$$

陪集 $Ka_1 a_{m+1}, Ka_2 a_{m+1}, \dots, Ka_m a_{m+1}$ 各不相同, 而且与 Ka_1, Ka_2, \dots, Ka_m 也都不同, 因此可以调动 a_i 的次序使

$$Ha_{m+1} = Ka_{m+1} \quad Ka_{m+2} \quad \dots \quad Ka_{2m} .$$

这样逐次调动即可得到最后的分解式 x

推论 设 $G = H \rtimes K$, 则

1) 如果 g_1, g_2, \dots, g_l 是 H 在 G 中的一个右陪集代表系, h_1, h_2, \dots, h_m 是 K 在 H 中的一个右陪集代表系, 那么

$g_1 h_1, g_1 h_2, \dots, g_1 h_m, g_2 h_1, g_2 h_2, \dots, g_2 h_m, \dots, g_l h_1, g_l h_2, \dots, g_l h_m$ 是 K 在 H 中的一个右陪集代表系. 特别地, 如果取 $g_1 = e$, 那么这个右陪集代表系中包含 H 对 K 的陪集代表系 h_1, h_2, \dots, h_m .

2) 在 G 对 K 的任一个右陪集代表系中, 总能找出一部分组成 H 对 K 的右陪集代表系.

1.6 同 构

设 G 和 G_1 是两个群, 在很多情况下往往会提出这样的问题: G 和 G_1 是否有相同的构造? 什么叫做构造相同呢? 要回答这个问题, 必须建立同构的概念.

定义 9 设 G 和 G_1 是两个群. 如果存在一个由 G 到 G_1 上的一一映射 φ , 对于 G 中任意两个元素 a, b , 都有

$$\varphi(ab) = \varphi(a)\varphi(b),$$

那么就称 G 同构于 G_1 , 记作 $G \cong G_1$. 称为 G 到 G_1 的一个同构映射 (简称同构). 当 $G = G_1$ 时, 称为 G 的一个自同构映射 (简称自同构).

例 1 域 F 上 n 维线性空间 V 的可逆线性变换群 $GL_n(V)$ 与 F 上 n 阶可逆矩阵群 $GL_n(F)$ 是同构的.

证明 在 V 中取定一组基 $\alpha_1, \alpha_2, \dots, \alpha_n$. V 的每个线性变换 \mathbf{A} 在这组基下对应于 F 上的一个 n 级矩阵 \mathbf{A} ; 反之, F 上每个 n 级矩阵 \mathbf{A} 可看作 V 的某个线性变换 \mathbf{A} 在基 $\alpha_1, \alpha_2, \dots, \alpha_n$ 下的矩阵. 而且当且仅当 \mathbf{A} 为可逆线性变换时, \mathbf{A} 为可逆矩阵. 由于不同的线性变换在同一组基下的矩阵是不同的, 映射

$$\varphi: \mathbf{A} \mapsto \mathbf{A}$$

是 $GL_n(V)$ 到 $GL_n(F)$ 上的一个一一映射. 我们知道, 映射 φ 保持乘法, 所以 φ 是 $GL_n(V)$ 到 $GL_n(F)$ 的一个同构映射, 即 $GL_n(V) \cong GL_n(F)$.

例 2 1.1 节中例 10 的 G 与置换群

$$K = \{e, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}$$

是同构的.

证明 G 到 K 的映射 φ :

$$\begin{aligned} a \mapsto e, \quad b \mapsto (1, 2)(3, 4), \\ c \mapsto (1, 3)(2, 4), \quad d \mapsto (1, 4)(2, 3) \end{aligned}$$

是一个一一映射而且保持运算, 所以是一个同构映射, 因而 $G \cong K$.

读者可以再找一个 G 到 K 的同构映射.

例 3 $S_3 = \{e, (1, 2), (1, 3), (2, 3), (1, 2, 3), (1, 3, 2)\}$. 定义 S_3 到自身的一个映射:

$$\begin{aligned} e \mapsto e, \quad (1, 2) \mapsto (2, 3), \quad (1, 3) \mapsto (1, 2), \\ (2, 3) \mapsto (1, 3), \quad (1, 2, 3) \mapsto (1, 2, 3), \quad (1, 3, 2) \mapsto (1, 3, 2) \end{aligned}$$

请读者验证这个映射是 S_3 的一个自同构映射.

群的同构关系是一个等价关系.也就是说,群的同构映射具有下列 3 个性质:

- 1) 反身性: $G \cong G$;
- 2) 对称性: 如果 $G \cong G_1$, 则有 $G_1 \cong G$;
- 3) 传递性: 如果 $G \cong G_1$, $G_1 \cong G_2$, 则有 $G \cong G_2$.

这是因为恒等映射、同构映射的逆映射以及两个同构映射的乘积都是同构映射的缘故.

因为群的同构映射是一个一一映射, 所以同构的群有相同的阶. 下面来证明群的同构映射的一些重要性质.

设 φ 是群 G 到 G_1 的一个同构映射, 则有

- 1) 将 G 的单位元素 e 映到 G_1 的单位元素 e_1 .

证明 因为 $e^2 = e$, 所以

$$(\varphi(e))^2 = \varphi(e),$$

于是

$$e e_1 = e = e_1 e_1.$$

根据消去律, 即得

$$e = e_1 x$$

- 2) 将 G 中元素 a 的逆元素 a^{-1} 映到 a 的象 a_1 的逆元素 $(a_1)^{-1}$, 即

$$(\varphi(a^{-1})) = (\varphi(a))^{-1}.$$

证明 因为 $aa^{-1} = e$, 所以

$$(aa^{-1}) = e, \quad a \cdot (\varphi(a^{-1})) = e,$$

因此

$$(\varphi(a^{-1})) = (\varphi(a))^{-1} x$$

3) G 中元素 a 与它在 G_1 中的象 a 有相同的阶 .

证明 这是因为

$$a^k = e \quad (a)^k = e$$

的缘故 .

4) 对 G 中元素 a, b 有

$$ab = ba \quad a b = b a .$$

证明 由定义即得 .

设 a, b 是群中两个元素, 如果 $ab = ba$, 就称这两个元素是可交换的 . 上述性质说明群的同构映射保持元素在运算下的交换性 . 由此可知, 把 G 的中心元素映到 G_1 的中心元素, 所以交换群的同构象也一定是交换群 .

5) 设 H 是 G 的一个子集 . 用 H 表示 H 中元素在 σ 下的象组成的集合:

$$H = \{h \mid h \in H\},$$

则 H 是 G 的子群当且仅当 H 是 G_1 的子群 .

证明 如果 $H \leq G$, 对 G 中任意两个元素 a, b , 因为 σ 是一一映射, 故有 $a, b \in H$ 使

$$a = a, \quad b = b .$$

于是 $ab^{-1} \in H$, 且

$$(ab^{-1}) = a(b^{-1}) = a(b)^{-1} = a b^{-1} \in H .$$

所以 $H \leq G_1$.

如果 $H \leq G_1$, 则对 G 中任意两个元素 a, b , 都有

$$(ab^{-1})^{-1} = a(b^{-1})^{-1} = a(b)^{-1} \in H.$$

因为 ϕ 是一一映射, 所以

$$ab^{-1} \in H.$$

因此 $H = G$.

同构的定义及性质说明, 在同构映射下, 对应的元素在各自的运算之下有相同的关系. 因此, 如果我们抽象地研究一个群, 也就是说如果不考虑群的元素是什么, 也不考虑群中的运算是怎样定义的, 而只考虑群在所定义的运算下的代数性质, 那么同构的群是可以不加区别的. 例如, 可以证明同阶的循环群一定是同构的, 因此从同构的角度来看, 对于任一个自然数 n , 都恰有一个 n 阶循环群.

1.7 群的置换表示

置换群是比较具体的一种群, 它的元素和运算都可以具体地写出来而且便于计算. 置换群之所以重要还在于: 每个有限群都和一个置换群同构. 我们知道同构的群具有相同的构造, 说得具体一些, 就是, 有关群的那些不依赖于元素的特性而根据运算的性质就可以证明的结论, 都能够自动地转移到与这个群同构的群上去. 例如, 两个同构的群有相同的阶, 与一个交换群或循环群同构的群一定也是交换群或循环群, 等等. 因此, 可以应用置换群来研究一般群.

这一节介绍将一个群表示成置换群的几种方法.

1 右正则表示

设 G 是一个群, 阶等于 n . 它的元素是

$$a_1 = e, a_2, \dots, a_n.$$

取定一个元素 a_i , 用它依次右乘 G 中每个元素, 得到 n 个元素

$$a_i a_1, a_i a_2, \dots, a_i a_n .$$

这 n 个元素仍在 G 中, 而且由消去律可知这 n 个元素各不相同, 因此它们是 a_1, a_2, \dots, a_n 的一个排列. 作 a_1, a_2, \dots, a_n 的置换

$$\begin{array}{cccc} a_1 & a_2 & \dots & a_n \\ a_i a_1 & a_i a_2 & \dots & a_i a_n \end{array} ,$$

简记成 $\begin{array}{c} a \\ a_i a_1 \end{array}$. 以后我们把这个置换记作 a_i , 简记作 i .

用这个方法, 我们得到 n 个 n 元置换 i ($i = 1, 2, \dots, n$), 其中单位元素 a_1 对应的置换是恒等置换. 因为 i 把单位元素 a_1 映到 $a_i a_1 = a_i$, 所以这 n 个置换各不相同. 用 R_G 表示这 n 个置换所成的集合:

$$R_G = \{ 1, 2, \dots, n \} .$$

这是作用于 $\{ a_1, a_2, \dots, a_n \}$ 上的 n 元对称群 S_n 的一个非空子集. 下面来证明 R_G 是 S_n 的一个子群, 并且 G 与 R_G 同构.

首先证明

引理 1 R_G 是 S_n 的一个子群.

证明 在 R_G 中任取两个置换 a_i 与 a_j . 它们的乘积

$$\begin{aligned} a_i a_j &= \begin{array}{ccc} a & a & a \\ a a_i & a a_j & a a_i a_j \end{array} \\ &= a_i a_j R_G, \end{aligned}$$

所以根据子群的判别条件三, R_G 是 S_n 的一个子群. \times

其次证明

引理 2 G 与 R_G 是同构的.

证明 考虑 G 到 R_G 上的映射:

$$a^i \mapsto a_i,$$

来证这是一个同构映射. 因为当 $a_i = a_j$ 时, $a_i = a_j$, 所以这是一个一一映射. 因此为了证明它是一个同构映射, 只要证明它保持运算就可以了. 而这一点在引理 1 的证明中已经指出了. \times

R_G 中的置换有一个特点: 除了恒等置换把 G 中每个元素都保持不变外, 其他置换没有不变元素, 这样的置换称做正则置换, 而 R_G 称做 G 的右正则表示.

以上的讨论给出了构造与已知群同构的置换群的一个方法. 从而证明了下面的定理.

定理 10 (Cayley) 每个 n 阶群都与一个 n 元 (n 次) 置换群同构.

下面给出几个例子.

例 1 G 是一个 6 阶循环群, a 是 G 的一个生成元:

$$G = \{e = a^0 = a^6, a, a^2, a^3, a^4, a^5\}.$$

求 G 的右正则表示.

解 $e^i \mapsto e$ (恒等置换),

$$a^i \mapsto a = \begin{matrix} e & a & a^2 & a^3 & a^4 & a^5 \\ a & a^2 & a^3 & a^4 & a^5 & e \end{matrix}.$$

因为置换的性质与它所作用的文字的符号没有关系, 所以为了方便起见, 可以写成

$$a = \begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 6 & 1 \end{matrix} = (1, 2, 3, 4, 5, 6).$$

a 是一个 6 阶轮换. R_G 就是 a 生成的 6 阶循环群:

$$R_G = \{ e = a^6, a, a^2, a^3, a^4, a^5 \}.$$

例 2 设 G 是由 a, b 两个元素生成的有限群, G 中元素的运算满足下述关系:

$$a^4 = e, \quad a^2 = b^2 = e, \quad ab = ba^3.$$

从这些关系式可以推出 G 中共有 8 个元素, 即

$$G = \{ e, a, a^2, a^3, b, ab, a^2b, a^3b \}.$$

而 G 的乘法表是

| | e | a | a^2 | a^3 | b | ab | a^2b | a^3b |
|--------|--------|--------|--------|--------|--------|--------|--------|--------|
| e | e | a | a^2 | a^3 | b | ab | a^2b | a^3b |
| a | a | a^2 | a^3 | e | ab | a^2b | a^3b | b |
| a^2 | a^2 | a^3 | e | a | a^2b | a^3b | b | ab |
| a^3 | a^3 | e | a | a^2 | a^3b | b | ab | a^2 |
| b | b | a^3b | a^2b | ab | a^2 | a | e | a^3 |
| ab | ab | b | a^3b | a^2b | a^3 | a^2 | a | e |
| a^2b | a^2b | ab | b | a^3b | e | a^3 | a^2 | a |
| a^3b | a^3b | a^2b | ab | b | a | e | a^3 | a^2 |

这个群叫做四元数群, 记作 Q_8 . 下面来求它的右正则表示.

$$\begin{aligned}
 e^1 &= e \text{ (恒等置换)}, \\
 a^1 &= \begin{pmatrix} e & a & a^2 & a^3 & b & ab & a^2b & a^3b \\ a & a^2 & a^3 & e & a^3b & b & ab & a^2b \end{pmatrix}.
 \end{aligned}$$

因为置换的作用与文字的符号无关, 所以为了简便起见, 我们把 G 中元素编号:

$$\begin{aligned}
 e^1 &= 1, & a^1 &= 2, & a^2 &= 3, & a^3 &= 4, \\
 b^1 &= 5, & ab^1 &= 6, & a^2b^1 &= 7, & a^3b^1 &= 8.
 \end{aligned}$$

于是 可写成

$$a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 1 & 8 & 5 & 6 & 7 \end{pmatrix}$$

$$= (1, 2, 3, 4)(5, 8, 7, 6).$$

同样可以算出

$$\begin{aligned} a^2 &= \begin{array}{cccccccc} e & a & a^2 & a^3 & b & ab & a^2 b & a^3 b \\ a^2 & a^3 & e & a & a^2 b & a^3 b & b & ab \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ = & 3 & 4 & 1 & 2 & 7 & 8 & 5 & 6 \\ = & (1, 3)(2, 4)(5, 7)(6, 8); \end{array} \end{aligned}$$

$$\begin{aligned} a^3 &= \begin{array}{cccccccc} e & a & a^2 & a^3 & b & ab & a^2 b & a^3 b \\ a^3 & e & a & a^2 & ab & a^2 b & a^3 b & b \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ = & 4 & 1 & 2 & 3 & 6 & 7 & 8 & 5 \\ = & (1, 4, 3, 2)(5, 6, 7, 8); \end{array} \end{aligned}$$

$$\begin{aligned} b &= \begin{array}{cccccccc} e & a & a^2 & a^3 & b & ab & a^2 b & a^3 b \\ b & ab & a^2 b & a^3 b & a^2 & a^3 & e & a \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ = & 5 & 6 & 7 & 8 & 3 & 4 & 1 & 2 \\ = & (1, 5, 3, 7)(2, 6, 4, 8); \end{array} \end{aligned}$$

$$\begin{aligned} ab &= \begin{array}{cccccccc} e & a & a^2 & a^3 & b & ab & a^2 b & a^3 b \\ ab & a^2 b & a^3 b & b & a & a^2 & a^3 & e \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ = & 6 & 7 & 8 & 5 & 2 & 3 & 4 & 1 \\ = & (1, 6, 3, 8)(2, 7, 4, 5); \end{array} \end{aligned}$$

$$\begin{aligned} a^2 b &= \begin{array}{cccccccc} e & a & a^2 & a^3 & b & ab & a^2 b & a^3 b \\ a^2 b & a^3 b & b & ab & e & a & a^2 & a^3 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ = & 7 & 8 & 5 & 6 & 1 & 2 & 3 & 4 \\ = & (1, 7, 3, 5)(2, 8, 4, 6); \end{array} \end{aligned}$$

$$\begin{aligned}
 a^3 b &= \begin{array}{cccccccc} e & a & a^2 & a^3 & b & ab & a^2 b & a^3 b \\ a^3 b & b & ab & a^2 b & a^3 & e & a & a^2 \end{array} \\
 &= \begin{array}{cccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 5 & 6 & 7 & 4 & 1 & 2 & 3 \end{array} \\
 &= (1, 8, 3, 6)(2, 5, 4, 7).
 \end{aligned}$$

于是得

$$R_G = \{ e, a, a^2, a^3, b, ab, a^2 b, a^3 b \} \quad G.$$

这个方法也可以用来讨论无限群.一般地,一个集合 A (有限或无限)到自身的一个映射称为 A 的一个变换. A 到自身的一一映射称为 A 的一个可逆变换(或一一变换).用 $S(A)$ 表示 A 的全部可逆变换所成的集合.易证 $S(A)$ 对映射的乘法构成一个群,称为 A 的全变换群.由 A 的一部分可逆变换组成的群称为 A 的一个变换群.显然, A 的变换群就是 A 的全变换群的子群.可以和证明定理 10 同样地证明:任何一个群都与一个变换群同构,而且从证明的方法可以看出,这个变换群可以取作某一个作用于这个群的变换群.

2 左正则表示

仍用 $a = e, a_1, \dots, a_n$ 表示 n 阶 G 群中全部元素.取定 G 中一个元素 a_i ,用 a_i^{-1} 依次左乘 a_1, a_2, \dots, a_n ,也得到 G 中 n 个不同的元素:

$$a_i^{-1} a_1, a_i^{-1} a_2, \dots, a_i^{-1} a_n.$$

这 n 个元素也各不相同,组成 a_1, a_2, \dots, a_n 的一个排列,和上一节相仿,我们可以作一个 n 元置换

$$a_i = \begin{array}{cccc} a_1 & a_2 & \dots & a_n \\ a_i^{-1} a_1 & a_i^{-1} a_2 & \dots & a_i^{-1} a_n \end{array} = a_i^{-1} a.$$

这样,我们又得到作用于 $\{a_1, a_2, \dots, a_n\}$ 的 n 个 n 元置换,组成 S_n

的另一个子集 L_G :

$$L_G = \{ a_1, a_2, \dots, a_n \}.$$

因为

$$\begin{aligned} a_i a_j &= \begin{matrix} a & a \\ a_i^{-1} a & a_j^{-1} a \end{matrix} \\ &= \begin{matrix} a & a \\ a_j^{-1} a_i^{-1} a & (a_i a_j)^{-1} a \end{matrix} \\ &= a_i a_j, \end{aligned}$$

所以可以和前面一样地证明 L_G 是 S_n 的一个子群, 映射

$$a_i \mapsto a_i$$

是 G 到 L_G 的一个同构映射. G 与置换群 L_G 是同构的. L_G 中的置换也都是正则置换, L_G 称为 G 的左正则表示. 证明留给读者.

下面给出一个例子.

例 3 求四元数群的左正则表示.

解 e 的恒等置换.

$$\begin{aligned} a &= \begin{matrix} x & x \\ a^{-1} x & a^3 x \end{matrix} \\ &= \begin{matrix} e & a & a^2 & a^3 & b & ab & a^2 b & a^3 b \\ a^3 & e & a & a^2 & a^3 b & b & ab & a^2 b \end{matrix} \\ &= \begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 1 & 2 & 3 & 8 & 5 & 6 & 7 \end{matrix} \\ &= (1, 4, 3, 2)(5, 8, 7, 6); \\ a^2 &= (a)^2 = (1, 3)(2, 4)(5, 7)(6, 8); \\ a^3 &= (a)^3 = (1, 2, 3, 4)(5, 6, 7, 8); \end{aligned}$$

$$\begin{aligned}
 {}^b = & \begin{array}{cccccccc} & x & & & x & & & \\ & b^{-1} x & = & & a^2 b x & & & \\ & e & a & a^2 & a^3 & b & ab & a^2 b & a^3 b \\ = & a^2 b & ab & b & a^3 b & e & a^3 & a^2 & a \\ = & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ = & 7 & 6 & 5 & 8 & 1 & 4 & 3 & 2 \\ = & (1, 7, 3, 5)(2, 6, 4, 8); \\ ab = & a b = (1, 8, 3, 6)(2, 7, 4, 5); \\ a^2 b = & a^2 b = (1, 5, 3, 7)(2, 8, 4, 6); \\ a^3 b = & a^3 b = (1, 6, 3, 8)(2, 5, 4, 7). \end{array}
 \end{aligned}$$

于是得

$$L_G = \{ e, a, a^2, a^3, b, ab, a^2 b, a^3 b \} \quad G.$$

读者学习到这里,也许会提出一个问题:在作 a_i 时为什么不用 a_i 来左乘 G 中各个元素,而要用 a_i^{-1} 来左乘呢?这个问题是值得考虑的.如果用 a_i 来左乘,将 a_i 对应于置换

$${}^{a_i} = \begin{array}{cccc} a_1 & a_2 & \dots & a_n \\ a_i a_1 & a_i a_2 & \dots & a_i a_n \end{array}.$$

这样也得到 n 个 n 元置换.问题是,这 n 个置换是否也具有上面所说的那些性质呢?其实,由于 $a_i = a_i^{-1}$,所以这样得到的 n 个置换所成的集合仍是 L_G .但是,由于

$$\begin{aligned}
 {}^{a_i} {}^{a_j} &= \begin{array}{ccc} a & a & a \\ a_i a & a_j a & a_j a_i a \end{array} \\ &= \begin{array}{ccc} a & & \\ (a_j a_i) a & & \end{array} = {}^{a_j a_i} a,
 \end{aligned}$$

因此,如果 G 是一个非交换群,那么映射

$$a_i \mapsto a_i^{-1}$$

就不是一个同构映射了。

3 陪集置换表示

前面介绍了群的正则表示,给出了与 n 阶群 G 同构的两个 n 元置换群.但是当 G 的阶比较大的时候,这两个置换群作用的文字比较多,运算也就比较复杂.因此为了减少置换所作用的文字个数,有时需要用其他方法将一个群表示为置换群.这一小节介绍用子群的陪集将群表成置换群的方法.

设 G 是一个群, H 是 G 的一个子群, G 的阶等于 n , H 在 G 中的指数等于 r .我们知道, G 可以分解成 H 的不相交的右陪集之并:

$$G = Hx_1 \quad Hx_2 \quad \dots \quad Hx_r,$$

其中 $Hx_1 = H$.

如果 a 是 G 中一个元素,那么用 a 右乘右陪集 Hx_i (即:用 a 右乘 Hx_i 中各个元素)得到一个右陪集 Hx_ia .用 a 依次右乘 H 的 r 个右陪集 Hx_i ($i=1, 2, \dots, r$), 得到 r 个右陪集

$$Hx_1a, Hx_2a, \dots, Hx_ra.$$

这 r 个陪集各不相同,因此是原来 r 个陪集的一个排列.这样得到一个作用于这 r 个陪集的一个置换

$$\begin{array}{ccccccc} Hx_1 & Hx_2 & \dots & Hx_r & & Hx_i & \\ Hx_1a & Hx_2a & \dots & Hx_ra & = & Hx_ia & \end{array},$$

记作 α_a .很明显地,单位元素 e 所对应的置换 α_e 是恒等置换,而且

$$\alpha_a \alpha_b = \alpha_{ab}, \quad \alpha_a^{-1} = (\alpha_a)^{-1}.$$

用 $S_{G/H}$ 表示由 α_a ($a \in G$) 所成的集合:

$$S_{G/H} = \{ \alpha_a \mid a \in G \}.$$

可以和以前一样证明 $S_{G/H}$ 是作用于 $\{Hx_1, Hx_2, \dots, Hx_r\}$ 上的 r 元对称群 S_r 的一个子群.而且映射:

$$\alpha_a \mapsto a, \quad a \in G$$

是 G 到 $S_{G/H}$ 上的一个满映射, 这个映射保持运算. $S_{G/H}$ 称为 G 对子群 H 的陪集置换表示.

例 4 G 是由 x, y 两个元素生成的有限群, G 中运算满足下述关系:

$$x^3 = y^2 = e, \quad xy = yx^2.$$

从这些关系式, 可以推知 G 中共有 6 个元素:

$$G = \{e, x, x^2, y, xy, x^2y\}.$$

用 H 表示 G 的由 y 生成的子群:

$$H = \langle y \rangle = \{e, y\}.$$

G 对 H 的陪集分解是:

$$G = H \cup Hx \cup Hx^2,$$

其中

$$Hx = \{x, x^2y\}, \quad Hx^2 = \{x^2, x^2y\}.$$

下面来计算 G 对 H 的陪集置换表示:

$$e^1 \quad e \text{ (恒等置换)},$$

$$x^1 \quad x = \begin{pmatrix} H & Hx & Hx^2 \\ Hx & Hx^2 & H \end{pmatrix} = (1, 2, 3),$$

$$x^2^1 \quad x^2 = (x^{-1})^2 = (1, 3, 2),$$

$$y^1 \quad y = \begin{pmatrix} H & Hx & Hx^2 \\ H & Hx^2 & Hx \end{pmatrix} = (2, 3),$$

$$xy^1 \quad xy = x^{-1}y = (1, 3),$$

$$x^2y^1 \quad x^2y = (x^{-1})^2(y) = (1, 2).$$

所以

$$S_{G/H} \cong S_3.$$

例 5 设 G 是四元数群, H 为 a^2 生成的 2 阶循环子群:

$$H = \{e, a^2\}.$$

求 $S_{G/H}$.

解 G 对 H 的陪集分解为

$$G = H \quad Ha \quad Hb \quad Hab,$$

其中

$$Ha = \{a, a^3\}, Hb = \{b, a^2b\}, Hab = \{ab, a^3b\}.$$

把这些陪集编号:

$$H \mapsto 1, Ha \mapsto 2, Hb \mapsto 3, Hab \mapsto 4.$$

于是

$$\begin{aligned} e \mapsto e &= (1) \text{ (恒等置换)}, \\ a \mapsto a &= \begin{array}{cccc} H & Ha & Hb & Hab \\ Ha & H & Hab & Hb \end{array} \\ &= \begin{array}{cccc} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{array} = (1, 2)(3, 4), \\ a^2 \mapsto a^2 &= (a)^2 = (1), \\ a^3 \mapsto a^3 &= (a)^3 = a, \\ b \mapsto b &= \begin{array}{cccc} H & Ha & Hb & Hab \\ Hb & Hab & H & Ha \end{array} \\ &= \begin{array}{cccc} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{array} = (1, 3)(2, 4), \\ ab \mapsto ab &= a \ b = (1, 4)(2, 3), \\ a^2b \mapsto a^2b &= (a)^2 \ b = b, \\ a^3b \mapsto a^3b &= (a)^3 \ b = a \ b = ab. \end{aligned}$$

所以

$$S_{G/H} = \{(1), (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}$$

是 S_3 的一个 4 阶子群.

群 G 到置换群 $S_{G/H}$ 上的映射:

$$a \mapsto a^H$$

是保持运算的. 如果这个映射还是一一的, 那么就是一个同构映射, 此时 G 与 r 元置换群 $S_{G/H}$ 是同构的. 例如, 例 4 中的陪集置换表示就给出了群 G 与 $S_{G/H}$ (即 S_3) 的一个同构映射, 从而知道 $G \cong S_3$. 但是, 一般地这个映射不一定是一个一一对应. 例如, 例 5 中那个映射就不是一一的, 这时, 这个映射就不是一个同构映射, G 与 $S_{G/H}$ 就不是同构的. 但是, 既然这个映射保持运算, 那么它一定能反映这两个群之间的一些关系. 关于这一类映射以及由子群 H 的陪集得出的置换群与原来的群同构的条件等问题, 将在下一章中进行讨论.

习 题

1. 设 a, a_2, \dots, a_r 是群 G 中任意 r ($r \geq 2$) 个元素, 求证:

$$(a a_2 \dots a_r)^{-1} = a_r^{-1} a_{r-1}^{-1} \dots a_2^{-1} a^{-1}.$$

2. 证明: 如果群 G 中每个元素的平方都等于单位元素, 那么 G 一定是一个交换群.

3. 设 a, b 是群 G 中两个元素, 求证:

(1) $a, a^{-1}, a^{-1}ba$ 有相同的阶;

(2) ab 与 ba 有相同的阶.

4. 设 a 是群 G 中一个元素, a 的阶等于 n . 求证: a^m 的阶等于 n/n' (n, m), 其中 (n, m) 是 n 与 m 的最大公因数.

5. 设 a, b 是群 G 中两个可交换的元素, 它们的阶分别为 l, m . 试证: 如果 $a^l = b^m = \{e\}$. 则 ab 的阶等于 l 与 m 的最小公倍数 $[l, m]$.

6. 试证: 如果群 G 中只有一个 2 阶元素, 那么这个元素一定是 G 的中心元素.

7. 证明 4 阶群都是交换的.

8. 设

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

是 S_6 中两个置换.

(1) 写出 σ , τ 的轮换表法, 并求 σ^{-1} , τ^{-1} 的阶.

(2) 计算 $\sigma\tau$, $\tau\sigma$, $\sigma^{-1}\tau$, $\tau\sigma^{-1}$.

9. 解置换方程 $x\sigma = \tau$ 及 $y\tau = \sigma$, 其中

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}.$$

10. 设 σ, τ 是两个 n 元置换, 其中 σ 是一个 r -轮换:

$$\sigma = (i_1, i_2, \dots, i_r).$$

试证:

$$\sigma^{-1} = (i_r, i_{r-1}, \dots, i_1),$$

并将这个结论推广到 σ 是一个任意置换的情形.

11. 证明 S_n ($n > 2$) 是无中心群.

12. 设 σ 的轮换表法为

$$\sigma = (i_1 i_2 \dots i_s),$$

其中 i_i ($i = 1, 2, \dots, s$) 的长度为 l_i . 试证: σ 的奇偶与 $l_1 + l_2 + \dots + l_s - s$ 一致.

13. 设 a 是群 G 中一个 n 阶元素, H 是 G 的一个子群. 试证: 如果 $a^m \in H$, $(n, m) = 1$, 则 $a \in H$.

14. 试证阶为素数的群一定是循环群.

15. 证明: 群 G 没有非平凡子群的充分必要条件是 G 为素数阶循环群.

16. 设 G 是一个 pq 阶群, p, q 都是素数且 $p < q$. 证明: G 不可

能有两个不同的 q 阶子群 .

17 . A 是有限群 G 的一个非空子集 . 试证 : 当且仅当 $AA = A$ 时, A 是 G 的一个子群 (群 G 的两个子集 A 与 B 的乘积 AB 定义为 $AB = \{ab \mid a \in A, b \in B\}$) .

18 . 设 A, B 都是群 G 的子群 . 则当且仅当 $AB = BA$ 时, AB 是 G 的子群 .

19 . 设 A, B, C 都是 G 的子群 . 求证 : 如果 $A \subseteq C$, 则 $AB \subseteq C = A(B \cap C)$.

20 . 设 H 是群 G 的子群, $|G/H| = 2$. 证明 : 对于 G 中任一元素 a 都有 $Ha = aH$.

21 . 求 S_4 对子群

$$K = \{e, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}$$

的陪集分解 .

22 . 找出四元数群 Q_8 的全部子群及其陪集分解 .

23 . 试求 S_3 的左、右正则表示 .

24 . 求 S_4 对 S_3 的陪集置换表示并证明 S_4 与这个置换表示是同构的 .

第 2 章 正规子群与同态定理

同构映射是一个一一映射并且保持运算,所以就保证了同构的群具有相同的构造.在有些问题中,我们还会遇到一些保持运算的映射,但是不一定是——的.例如在上一章中我们利用子群的陪集分解所作的置换表示就是这样的.这种映射叫做同态映射.同态映射既然保持运算,它必然能反映这两个群之间的关系以及它们的一些共同的性质.由于一个群的同态象的阶比这个群的阶小,研究起来比较方便,找出一个群的同态象对于研究这个群是非常有用的.

这一章主要讨论同态映射的性质,以及一个群与其同态象的关系.

这一章还介绍一些重要的概念:共轭元素、共轭子群、正规子群、商群、特征子群、自同构群等.

正规子群等概念不仅在讨论同态映射时起着重要的作用,它们在整个群论中都占有很重要的地位.

2.1 同 态

定义 1 G 与 H 是两个群, φ 是 G 到 H 的一个映射.如果对于 G 中任意两个元素 a, b , 都有

$$(\varphi a)\varphi b = \varphi(ab),$$

就叫做 G 到 H 的一个同态映射.当 φ 是一个映上的同态时,称为一个满同态, H 称为 G 的一个同态象,记作 $G \sim H$.群 G 到自身的同态称为自同态.

要注意, $G \sim H$ 与 $H \sim G$ 是不同的.

例 1 设 H 是 G 的一个子群, G 到陪集置换表示 $S_{G/H}$ 上的映射

$$a \mapsto a, \quad a \in G$$

是一个满同态映射, $S_{G/H}$ 是 G 的一个同态象.

例 2 设 F 是一个域, 用 $ML_n(F)$ 表示系数在 F 中的全体 n 级可逆矩阵所成的乘法群. 仍用 F^* 表示 F 中全体非零元素所成的乘法群. 定义 $ML_n(F)$ 到 F^* 的映射 为

$$\mathbf{A} \mapsto \mathbf{A} = |\mathbf{A}|, \quad \mathbf{A} \in ML_n(F)$$

$|\mathbf{A}|$ 表示矩阵 \mathbf{A} 的行列式. 因为

$$(\mathbf{AB}) = |\mathbf{AB}| = |\mathbf{A}| |\mathbf{B}| = \mathbf{A} \mathbf{B}, \quad \mathbf{A}, \mathbf{B} \in ML_n(F)$$

所以 是 $ML_n(F)$ 到 F^* 的一个同态映射, 而且, 对于 F^* 中任一元素 a , 令

$$\mathbf{A}(a) = \begin{pmatrix} a & & \\ & 1 & \\ & & \ddots \\ & & & 1 \end{pmatrix},$$

则 $\mathbf{A}(a) \in ML_n(F)$, 且

$$(\mathbf{A}(a)) = |\mathbf{A}(a)| = a,$$

所以 是一个满同态, $ML_n(F) \sim F^*$.

例 3 U_n 是 n 次单位根所成的 n 阶循环群. 取定一个 n 次本原单位根. 定义整数加法群 \mathbb{Z} 到 U_n 上的映射 :

$$k \mapsto k = \zeta^k, \quad k \in \mathbb{Z}$$

是一个满同态, $\mathbb{Z} \sim U_n$.

同态映射有下述一些重要的性质 .

设 φ 是群 G 到 H 的一个同态映射, 则有:

- 1) 将 G 的单位元素 e 映到 H 的单位元素 e .
- 2) 将 G 中元素 a 的逆元素 a^{-1} 映到 a 的逆元素, 即

$$(\varphi(a^{-1})) = (\varphi(a))^{-1} .$$

这两条性质可以与以前关于同构映射的相同性质一样地证明, 留给读者去完成 .

- 3) $\varphi(a)$ 的阶是 a 的阶的一个因数 .

证明 设 a 的阶为 k , 则 $a^k = e$. 于是

$$(\varphi(a))^k = (\varphi(a^k)) = \varphi(e) = e ,$$

所以 $\varphi(a)$ 的阶是 k 的一个因数 x

- 4) 把 G 中可交换的元素映到 H 中可交换的元素, 即

$$ab = ba (a, b \in G) \quad \varphi(ab) = \varphi(ba) .$$

如果 φ 是满同态, 那么 φ 把 G 的中心元素映到 H 的中心元素 .

需要注意的是, 由 $\varphi(ab) = \varphi(ba)$ 不能推出 $ab = ba$, 因此, 即使 φ 是一个满同态, 也只有 $(Z(G)) \subseteq Z(H)$.

- 5) 如果 A 是 G 的一个子群, 则 $\varphi(A)$ 是 H 的一个子群 .

- 6) 设 B 是 H 的一个子群. 用 B^{-1} 表示 B 的逆象, 即

$$B^{-1} = \{a \in G \mid \varphi(a) \in B\} ,$$

则 B^{-1} 是 G 的一个子群.

证明 因为 B 是一个子群, 所以 B^{-1} 当然是 G 的一个非空子集. 如果 a, b 都在 B^{-1} 中, 那么

$$a, b \in B.$$

于是

$$(ab^{-1})^{-1} = a(b)^{-1} \in B,$$

因此

$$ab^{-1} \in B^{-1}.$$

所以 B^{-1} 是 G 的一个子群. \square

当 $B = \{e\}$ 是 H 的单位子群时, 它的逆象也是 G 的一个子群, 称为 φ 的核.

定义 2 设 φ 是群 G 到 H 的一个同态映射, e 是 H 的单位元素. e 的逆象

$$K = \{a \in G \mid a\varphi = e\}$$

是 G 的一个子群, 称为 φ 的核, 记作 $\ker \varphi$.

同构映射是一一映射的同态映射, 可以应用同态映射的核来判断一个同态映射是不是同构映射.

定理 1 设 φ 是群 G 到 H 上的一个满同态映射, 则 φ 是同构映射的充分必要条件是 φ 的核 $K = \{e\}$.

证明 条件显然是必要的. 现在来证明条件也是充分的. 假设 $K = \{e\}$, 证明 φ 是一个一一映射. 如果 G 中两个元素 a, b 在 φ 下的象相同, 即

$$a = b,$$

那么

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

因此

$$ab^{-1} \in K.$$

由 $K = \{e\}$, 得

$$ab^{-1} = e,$$

即

$$a = b,$$

所以 φ 是一个一一映射, 因而它是一个同构映射 φ .

从定理的证明还可以看出: 如果 φ 是 G 到 H 的一个同态映射, K 是 φ 的核, 那么从 $a = b$ 可以推出

$$ab^{-1} \in K,$$

因此 a, b 属于 K 的同一个右陪集. 另一方面, 当 a, b 属于 K 的同一个右陪集时, 一定有

$$a = bx,$$

其中 $x \in K$. 于是有

$$a = (bx) = b x = b.$$

这就是说, G 中两个元素在 φ 下的象相同的充分必要条件是 a, b 属于核 K 的同一个陪集.

由此可见, 如果 φ 是 G 到 H 上的一个同态映射, K 是 φ 的核, 那么 G 在 φ 下的象集合 $\varphi(G)$ 可以由 K 在 G 中的一个陪集代表系的象得到. 这就给出了构造群的同态象的一个方法. 问题是: 是不是 G 的每个子群都可以作为某个同态的核? 更进一步, 如果 K 是 G 到 H 上的一个同态映射的核, 那么, K 与 H 有什么关系? 这些问题将在下面两节中得到解决.

2.2 共轭子群与共轭元素

在解决有关同态的一些问题之前,我们先介绍共轭子群与共轭元素的概念,这些概念也是群论中的重要概念.

1 共轭子群

设 G 对子群 H 的陪集分解为

$$G = Ha_1 \cup Ha_2 \cup \dots \cup Ha_r.$$

在我们作群 G 对子群 H 的陪集置换表示的时候,一般地,映射

$$\begin{aligned} & Hx_i \\ : a \mapsto & Hx_i a \end{aligned}$$

只是一个同态映射而不一定是同构映射.那么,在什么情形下这个映射是同构映射呢?根据定理 1,我们只要讨论什么时候这个映射的核,即恒等映射的原象只有单位元素就可以了.

我们首先来看 G 中什么样的元素在 σ_a 下的象是恒等置换.如果 a 是恒等置换 e , 即

$$\sigma_a = \sigma_e = \begin{pmatrix} Hx_i \\ Hx_i a \end{pmatrix} = e,$$

那么就有

$$Hx_i = Hx_i a, \quad i = 1, 2, \dots, r,$$

于是

$$x_i a x_i^{-1} \in H, \quad i = 1, 2, \dots, r.$$

设

$$x_i a x_i^{-1} = h_i, \quad i = 1, 2, \dots, r,$$

则

$$a = x_i^{-1} h_i x_i \in x_i^{-1} H x_i, \quad i = 1, 2, \dots, r,$$

其中

$$x_i^{-1} H x_i = \{x_i^{-1} h x_i \mid h \in H\}, \quad i = 1, 2, \dots, r.$$

很容易验证 $x_i^{-1} H x_i (1 \leq i \leq r)$ 是 G 的一个子群. 令

$$K = \bigcap_i x_i^{-1} H x_i,$$

那么上面的讨论说明 α 为恒等置换的必要条件是 $\alpha \in K$. 这个条件也是 $\alpha = e$ 的充分条件, 因此 K 就是 α 的核. 当且仅当 $K = \{e\}$ 时, α 是同构映射.

子群 $x_i^{-1} H x_i$ 称为 H 的共轭子群. 这一小节首先讨论共轭子群的一些性质. 然后再进一步讨论陪集置换表示.

定义 3 设 H_1 及 H_2 是群 G 的两个子群. 如果存在 G 中一个元素 a 使得

$$a^{-1} H_1 a = H_2,$$

则称 H_1 与 H_2 是共轭的.

子群的共轭关系具有下面一些性质:

1) 每个子群都与自己共轭.

这是因为 $e^{-1} H e = H$.

2) 如果 H_1 与 H_2 共轭, 那么 H_2 与 H_1 共轭.

这是因为从 $a^{-1} H_1 a = H_2$ 可推出 $(a^{-1})^{-1} H_2 a^{-1} = H_1$.

3) 如果 H_1 与 H_2 共轭, H_2 与 H_3 共轭, 那么 H_1 与 H_3 共轭.

理由是: 从 $a^{-1} H_1 a = H_2, b^{-1} H_2 b = H_3$ 可推出

$$(ab)^{-1} H_1 (ab) = H_3.$$

因此, 子群的共轭关系是一个等价关系. G 的子群可以分成一些互不相交的共轭子群的集合, 称为共轭子群类. 在同一个类中的子群

都是共轭的,而不同类中的子群互不共轭.同一个共轭子群类中的子群都有相同的阶及指数.

例 1 $A_4 = \{e, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3), (1, 2, 3), (1, 3, 2), (1, 2, 4), (1, 4, 2), (1, 3, 4), (1, 4, 3), (2, 3, 4), (2, 4, 3)\}$.

A_4 的子群可以分成下列 5 个共轭子群类:

- 1) $\{e\}$;
- 2) $\{e, (1, 2)(3, 4)\}, \{e, (1, 3)(2, 4)\}, \{e, (1, 4)(2, 3)\}$;
- 3) $\{e, (1, 2, 3), (1, 3, 2)\}, \{e, (1, 2, 4), (1, 4, 2)\}, \{e, (1, 3, 4), (1, 4, 3)\}, \{e, (2, 3, 4), (2, 4, 3)\}$;
- 4) $\{e, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}$;
- 5) A_4 .

设 H_1, H_2, \dots, H_l 是某个共轭子群类中全部子群.对于 G 中任一元素 a , $a^{-1}H_i a$ ($i=1, 2, \dots, l$) 仍然是这 l 个子群中的一个,而且当 $i \neq j$ 时, $a^{-1}H_i a \cap a^{-1}H_j a = \{e\}$, 所以

$$a^{-1}H_1 a, a^{-1}H_2 a, \dots, a^{-1}H_l a$$

是这 l 个子群的一个排列,由此可作一个置换:

$$\begin{array}{cccc} H_1 & H_2 & \dots & H_l \\ a^{-1}H_1 a & a^{-1}H_2 a & \dots & a^{-1}H_l a \end{array} .$$

可以用这种方法得到 G 的一个置换表示.这里就不仔细讨论了.

2 正规化子

设 H 是 G 的一个子群.这一小节讨论 H 的共轭子群的个数以及如何找出 G 的全部共轭子群.

作 G 的子集

$$N_G(H) = \{x \mid x^{-1}Hx = H\} .$$

因为单位元素在 $N_G(H)$ 中, 所以 $N_G(H)$ 是 G 的一个非空子集. 如果 $x, y \in N_G(H)$, 那么

$$x^{-1} H x = H, \quad y^{-1} H y = H.$$

于是

$$\begin{aligned} (x^{-1})^{-1} H x^{-1} &= H, \\ (x y)^{-1} H (x y) &= y^{-1} (x^{-1} H x) y = y^{-1} H y = H. \end{aligned}$$

因此

$$x^{-1} \in N_G(H), \quad x y \in N_G(H).$$

所以 $N_G(H)$ 是 G 的一个子群.

定义 4 H 是 G 的一个子群, $N_G(H)$ 称做 H 在 G 内的正规化子.

显然有 $H \leq N_G(H)$.

可以应用 $N_G(H)$ 来计算 H 的共轭子群的个数.

定理 2 H 在 G 中的共轭子群的个数等于其正规化子 $N_G(H)$ 在 G 中的指数.

证明 $N_G(H)$ 在 G 中的指数等于 $N_G(H)$ 的右陪集的个数. 因此只要证明: 对于 G 中两个元素 a 及 b , 共轭子群 $a^{-1} H a$ 与 $b^{-1} H b$ 相等的充分必要条件是 a, b 属于 H 的同一个右陪集.

容易看出, $a^{-1} H a = b^{-1} H b$ 的充分必要条件为

$$b a^{-1} H a b^{-1} = H,$$

即

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

亦即

$$a b^{-1} \in N_G(H).$$

而这一条件又等价于 a, b 属于 $N_G(H)$ 的同一个右陪集 x

定理 2 的证明还告诉我们: H 的全部共轭子群可以由 $N_G(H)$ 在 G 中的一个右陪集代表系给出.

例 2 设 $G = S_4$, $H = \{e, (1, 2), (3, 4), (1, 2)(3, 4)\}$. 计算 H 在 G 中的共轭子群.

根据计算, 可得

$$N_G(H) = \{e, (1, 2), (3, 4), (1, 2)(3, 4), (1, 3)(2, 4), \\ (1, 4)(2, 3), (1, 3, 2, 4), (1, 4, 2, 3)\},$$

所以 $|G/N_G(H)| = 3$. H 有 3 个共轭子群, 这 3 个共轭子群可以由 $N = N_G(H)$ 的右陪集代表给出. 因为

$$G = N \cup N(1, 3) \cup N(1, 4),$$

所以 H 的 3 个共轭子群为

- 1) H ;
- 2) $(1, 3)^{-1} H(1, 3) = \{e, (1, 4), (2, 3), (1, 4)(2, 3)\}$;
- 3) $(1, 4)^{-1} H(1, 4) = \{e, (1, 3), (2, 4), (1, 3)(2, 4)\}$.

现在我们反过来讨论 G 对子群 H 的陪集置换表示. 我们在以前已经分析过, 映射

$$a \mapsto a^{-1} a = \begin{matrix} Hx_i \\ Hx_i a \end{matrix}$$

是一个同构映射的充要条件是

$$\bigcap_{i=1}^r x_i^{-1} Hx_i = \{e\},$$

其中 x_1, x_2, \dots, x_r 是 H 在 G 中的一个右陪集代表系. 因为 H 的全部共轭子群可以由 $N_G(H)$ 在 G 中的陪集代表得出, 又因 $N_G(H) \cap H = H$, 所以 $N_G(H)$ 在 G 中的陪集代表可以在 x_1, x_2, \dots, x_r

中选取. 这说明 $x_1^{-1} H x_1, x_2^{-1} H x_2, \dots, x_r^{-1} H x_r$ 给出了 H 的全部共轭子群(可能有重复的). 因此, 我们有下述定理.

定理 3 设 H 是 G 的一个子群. G 对 H 的陪集置换表示 $S_{G/H}$ 与 G 同构的充要条件是

$${}_x G x^{-1} H x = \{e\}.$$

我们来回顾一下以前的例子.

应用上面的方法, 对第 1 章 1.7 节例 4, 可以算出 H 一共有 3 个共轭子群:

- 1) H ;
- 2) $x^{-1} H x = \{e, xy\}$;
- 3) $(x^2)^{-1} H x^2 = \{e, x^2 y\}$.

这 3 个子群的交等于 $\{e\}$, 所以 G 与 $S_{G/H}$ 是同构的.

在第 1 章 1.7 节的例 5 中, H 是一个 2 阶子群, 与 H 共轭的子群一定也是 2 阶子群. 但是 G 中只有一个 2 阶元素, 所以 G 只有一个 2 阶子群, H 的共轭子群只有 H 自己. 由此知

$${}_x G x^{-1} H x = H,$$

从而映射

$$a \mapsto a = \begin{matrix} Hx_i \\ Hx_i a \end{matrix}$$

的核就是 H . G 与 $S_{G/H}$ 不是同构的.

3 共轭元素 中心化子

以上我们讨论了共轭子群. H 的共轭子群 $x^{-1} H x$ 由形如 $x^{-1} h x$ ($h \in H$) 的元素组成, $x^{-1} h x$ 称为 h 的共轭元素.

定义 5 a, b 是群 G 中两个元素, 如果 G 中有一个元素 x 使 $x^{-1}ax = b$, 则称 a 与 b 是共轭的.

显然, 共轭元素有相同的阶.

和子群的共轭关系一样, 元素的共轭关系也有下述 3 个性质:

1) 任一元素 a 都与自己共轭.

2) 如果 a 与 b 共轭, 那么 b 与 a 也共轭.

3) 如果 a 与 b 共轭, b 与 c 共轭, 那么 a 与 c 共轭. 因此, 元素的共轭关系是一个等价关系

这 3 个性质的证明方法与前面关于共轭子群的证明相仿, 这里就不再重复了.

根据这 3 个性质, G 中元素可以分成一些互不相交的共轭元素的集合, 称为共轭元素类. 在同一类中的元素互相共轭, 而不同类中的元素彼此不共轭.

例 3 A_4 的 12 个元素分成下列 4 个共轭元素类:

1) $G = \{e\}$;

2) $G = \{(1, 2, 3), (1, 3, 4), (1, 4, 2), (2, 4, 3)\}$;

3) $G = \{(1, 3, 2), (1, 4, 3), (1, 2, 4), (2, 3, 4)\}$;

4) $G = \{(1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}$.

$$A_4 = G \cup G \cup G \cup G; \quad C_i \cap C_j = \emptyset \quad (i \neq j).$$

设 G 共有 s 个共轭类, 记作 C_1, C_2, \dots, C_s . 再设 G 中包含 n_i 个元素 ($i = 1, 2, \dots, s$). 那么因为

$$G = C_1 \cup C_2 \cup \dots \cup C_s,$$

$$C_i \cap C_j = \{e\} \quad (i \neq j),$$

所以

$$|G| = n_1 + n_2 + \dots + n_s.$$

这个式子称为 G 的类方程.

下面来讨论 G 的共轭元素类中元素的个数.

和处理共轭子群的情形相仿, 设 a 是群 G 的一个元素. 作 G 的子集

$$Z_G(a) = \{x \mid x^{-1}ax = a\}.$$

很容易验证 $Z_G(a)$ 是 G 的一个子群.

定义 6 子群 $Z_G(a)$ 称为 a 在 G 内的中心化子.

和共轭子群的个数一样, 我们有下述结果.

定理 4 a 是群 G 中一个元素. a 在 G 中的共轭元素的个数等于 a 在 G 内的中心化子 $Z_G(a)$ 在 G 中的指数.

证明 只要证明, 对于 G 中两个元素 x, y , 共轭元素 $x^{-1}ax$ 与 $y^{-1}ay$ 相等的充要条件是 x 与 y 属于 $Z_G(a)$ 的同一个右陪集. 证明了这一点以后, 就知道 a 的共轭元素的个数等于 $Z_G(a)$ 的右陪集的个数, 即等于 $Z_G(a)$ 的指数. 这就是定理所要证明的.

容易看出 $x^{-1}ax = y^{-1}ay$ 的充要条件为

$$a = yx^{-1}axy^{-1} = (xy^{-1})^{-1}a(xy^{-1}),$$

即

$$xy^{-1} \in Z_G(a).$$

而这个条件又是 x, y 属于 $Z_G(a)$ 的同一个右陪集的充分必要条件. x

从这个定理可以得到下列推论 .

推论 1) 共轭元素类 G_i 中元素的个数 n_i 是 G 阶的一个因子 .

2) 共轭元素的中心化子具有相同的指数, 因而有相同的阶 .

不仅如此, 还可证明共轭元素的中心化子是共轭的(习题 3) .

和讨论共轭子群的情形相仿, 可以应用共轭元素类中的元素来作出群的置换表示 .

2.3 正规子群

这一节讨论什么样的子群可以作为同态的核 ?

设 G 是一个群, φ 是 G 到群 G_1 的一个同态映射 . 我们曾经证明过, $\varphi^{-1}(e)$ 的核

$$K = \{x \in G \mid x\varphi = e\} \quad (e \text{ 是 } G_1 \text{ 的单位元素})$$

是 G 的一个子群, 而且 K 的一个右陪集 Ka 中的每个元素在 φ 下的象都是 a , 而不同右陪集中的元素的象一定不同 . 如果我们仔细回想一下这些结论的证明, 可以看出: 把右陪集换成左陪集, 这些结论仍然成立 . 因此得到下述结论:

设 φ 是群 G 到 G_1 的一个同态映射, K 是 $\varphi^{-1}(e)$ 的核, 则对 G 的任意元素 a , 左陪集 aK 及右陪集 Ka 中元素在同态映射 φ 下的象都是 a .

又因为其他陪集中元素的象都与 a 不同, 所以必须有

$$aK = Ka, \quad \forall a \in G.$$

我们把这样的群称做正规子群 .

定义 7 设 H 是 G 的一个子群 . 如果 G 对 H 的右陪集分解

与右陪集分解一致, H 就称为 G 的一个正规子群.

以后, 如果 H 是 G 的一个正规子群, 就记作 $H \triangleleft G$ (或 $G \triangleright H$). 如果 H 是 G 的一个正规的真子群, 就记作 $H \triangleleft G$ (或 $G \triangleright H$).

从定义可以直接看到: G 的平凡子群 $\{e\}$ 及 G 都是 G 的正规子群. 还可看到: 交换群的子群都是正规的. 下面再来举几个例子.

例 1 在四元数群 G 中, 仍设子群 $H = \{e, a^2\}$. 已知 G 对 H 的陪集分解是

$$G = H \cup Ha \cup Hb \cup Hab.$$

可以验证

$$Ha = aH, \quad Hb = bH, \quad Hab = abH,$$

所以

$$H \triangleleft G.$$

例 2 群 G 的中心 Z 是 G 的一个正规子群.

因为 Z 与 G 中每个元素都可交换, 所以对 G 中任意元素 x , 都有

$$Zx = xZ.$$

因此 Z 是 G 的一个正规子群.

例 3 在 A_4 中取子群 $H = \{e, (1, 2)(3, 4)\}$, 那么

$$H(1, 2, 3) = \{(1, 2, 3), (1, 3, 4)\},$$

$$(1, 2, 3)H = \{(1, 2, 3), (2, 4, 3)\} \neq H(1, 2, 3),$$

所以 H 不是 G 的正规子群.

从上面的例子可以看到, 的确有不是正规子群的子群存在. 而

直接从正规子群的定义来判断某个子群是否是正规子群有时比较麻烦,因此,讨论正规子群的一些判别条件是很有必要的.

判别条件一 指数等于 2 的子群一定是正规的.

证明 设 H 是 G 的一个指数为 2 的子群,那么 H 共有两个右陪集,也共有两个左陪集.取 $x \in G$,但 $x \notin H$,就有

$$G = H \cup Hx = H \cup xH, \quad Hx = xH.$$

因此, G 对 H 的左、右陪集分解相同,故 $H \triangleleft G$.

由此可知 n 元交错群是 n 元对称群的一个正规子群.这是下述例子的一个特殊情形.

例 4 设 G 是一个置换群.以前已经证明过 G 中全部偶置换组成的子集 G^+ 是 G 的一个子群,并且

$$|G/G^+| = \begin{cases} 1, & \text{如果 } G \text{ 中无奇置换,} \\ 2, & \text{如果 } G \text{ 中有奇置换,} \end{cases}$$

即 $G^+ = G$ 或 G^+ 在 G 中的指数为 2,所以 $G^+ \triangleleft G$.

判别条件二 设 H 是 G 的一个子群. $H \triangleleft G$ 的一个充分必要条件是:对 G 中任一元素 a ,都有 $a^{-1}Ha = H$,即 H 只有一个共轭子群,就是 H 自己.

证明 因为 $a^{-1}Ha = H \iff aH = Ha$,故由定义即可知

$$H \triangleleft G \iff a^{-1}Ha = H, \quad \forall a \in G.$$

因此,正规子群也称自共轭子群.

例 5 求 A_4 的全部正规子群.

解 在 2.2 节例 1 中, 我们已经求出了 A_4 的全部共轭子群类. 由判别条件二, 知子群 H 是正规子群的充分必要条件是包含 H 的共轭类中只有 H 一个子群, 所以可知 A_4 共有 3 个正规子群:

- 1) $\{e\}$;
- 2) $\{e, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}$;
- 3) A_4 .

其中只有一个非平凡正规子群.

从判别条件二可以看出, 如果 H 是 G 的一个正规子群, 那么 H 也是任一中间群 G_i ($G \supset G_i \supset H$) 的正规子群. 而且, 即使 H 不是 G 的正规子群, H 也可能是某个中间群的正规子群. 子群 H 在 G 内的正规化子 $N_G(H)$ 就以 H 为正规子群, 这一点可以从判别条件二看出. 因此当 $N_G(H) = G$ 时, $H \triangleleft G$, 可以证明这个条件也是充分的, 即有

判别条件三 $H \triangleleft G \iff N_G(H) = G$.

证明 $H \triangleleft G \iff x^{-1} H x = H, \forall x \in G$
 $N_G(H) = G$.

这个条件也可以叙述为:

判别条件四 G 的子群 H 是正规子群的一个充分必要条件是: 对 G 中任一元素 g 及 H 中任一元素 h , 都有

$$g^{-1} h g \in H.$$

例 6 设 H 是 G 的一个子群. 用 $Z_G(H)$ 表示 G 中与 H 的每个元素都可交换的元素全体:

$$Z_G(H) = \{x \in G \mid xh = hx, \forall h \in H\}.$$

容易看出

$$Z_G(H) = \bigcap_{h \in H} Z_G(h),$$

所以 $Z_G(H)$ 是 G 的一个子群.

定义 8 设 H 是群 G 的一个子群, $Z_G(H)$ 称为 H 在 G 内的中心化子.

根据定义有 $Z_G(H) \leq N_G(H)$. 可以证明

定理 5 设 H 是群 G 的一个子群, 则 $Z_G(H)$ 是 $N_G(H)$ 的一个正规子群.

证明 任取 $z \in Z_G(H)$, $g \in N_G(H)$. 对 H 中任一个元素 h , 都有

$$\begin{aligned} (g^{-1}zg)^{-1}h(g^{-1}zg) &= g^{-1}z^{-1}ghg^{-1}zg \\ &= g^{-1}z^{-1}(ghg^{-1})zg. \end{aligned}$$

因为 $g \in N_G(H)$, 所以 $ghg^{-1} \in H$. 因此 z 与 ghg^{-1} 可交换. 于是

$$(g^{-1}zg)^{-1}h(g^{-1}zg) = g^{-1}(ghg^{-1})g = h.$$

由 $Z_G(H)$ 的定义, 知 $g^{-1}zg \in Z_G(H)$. 因此 $Z_G(H) \triangleleft N_G(H)$. \square

判别条件五 G 的子群 H 是正规子群的一个充分必要条件是: 如果 h 在 H 中, 那么 H 一定包含 h 在 G 中的一切共轭元素, 即 H 由一些共轭元素类组成.

证明 设 $H \triangleleft G$. 任取 $h \in H$, $x \in G$, 则由 $x^{-1}Hx = H$ 可得 $x^{-1}hx \in H$, 因此 H 包含 h 的一切共轭元素. 这就证明了条件的必

要性.

如果对任一个 $h \in H$, H 都包含 h 在 G 中的一切共轭元素, 那么对任一 $x \in G$, 都有 $x^{-1}hx \in H$, 于是 $x^{-1}Hx \subseteq H$. 另一方面, 对于 x^{-1} 来说, 有 $(x^{-1})^{-1}H(x^{-1}) \subseteq H$, 即 $xHx^{-1} \subseteq H$. 由此得 $H \subseteq x^{-1}Hx$, 因此必须有 $x^{-1}Hx = H$, 所以 $H \triangleleft G$. 条件的充分性得证.

例 7 由 $(1, 2, 3, 4, 5)$ 生成的 5 阶循环群 H 是 S_5 的一个循环子群, 但不是 S_5 的正规子群. 因为 $(1, 2, 3, 4, 5)$ 在 S_5 中一共有 24 个共轭元素, 不能都在 H 中, 所以 H 在 S_5 中不是正规的.

例 8 四元数群 Q_8 的阶等于 8, 所以它的非平凡子群的阶只可能等于 2 或 4. 前面已经看到 Q_8 只有一个 2 阶子群, 所以这个子群是 Q_8 的正规子群. 而 Q_8 的 4 阶子群在 Q_8 中的指数等于 2, 所以这一类子群也都是正规的.

四元数群 Q_8 给出了一个非交换群, 它的子群都是正规子群的例子. 这样的群通常称为哈密尔顿群. 四元数群是哈密尔顿群的一个例子, 而且是阶最小的一个哈密尔顿群.

我们举例说明一点需要注意的地方. 正规子群没有传递性, 即可能有下述情况:

$$G > G_1 > G_2,$$

其中

$$G_1 \triangleleft G, \quad G_2 \triangleleft G_1,$$

但是 G_2 不是 G 的正规子群.

例 9 令

$$G = A_4,$$

$$G = \{e, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\},$$

$$G_2 = \{e, (1, 2)(3, 4)\},$$

则

$$G \neq G_2, G_2 \neq G.$$

但是, 由于

$$(1, 2, 3)^{-1} G_2 (1, 2, 3) = \{e, (1, 4)(2, 3)\} \neq G_2,$$

所以 G_2 不是 G 的正规子群.

最后, 我们以正规子群的两个重要性质来结束这一节.

如果 A 是 G 的一个子群, H 是 G 的一个正规子群, 那么:

1) $A \cap H$ 是 A 的正规子群, 特别地, G 的正规子群之交是 G 的正规子群;

2) $AH = \{ah \mid a \in A, h \in H\}$ 是 G 的一个子群, 而且 $AH = HA$.

证明留给读者作为练习.

2.4 商群 同态定理

上一节我们证明了同态映射的核一定是正规子群, 我们把所得的结果写成一个定理.

定理 6(第一同态定理) 群 G 到 G_1 的同态映射 φ 的核 K 是 G 的一个正规子群. G 中两个元素在 φ 下的象相同的充分必要条件是它们属于 G 的同一个陪集.

现在进一步来证明每个正规子群都可以作为某个同态映射

的核.

设 H 是 G 的一个正规子群. G 对 H 的陪集分解为

$$G = Hx_1 \quad Hx_2 \quad \dots \quad Hx_r,$$

其中 $Hx_1 = H$.

根据定理 5, 如果 H 是 G 到某个群 G_1 上的同态映射 φ 的核, 那么 G 的阶等于 r , 而且 G_1 的 r 个元素就是

$$x_1, x_2, \dots, x_r,$$

其中 $x_1 = e$ 是 G_1 的单位元素. 又因为 φ 是保持运算的, 所以 G_1 中的运算应该是

$$x_i x_j = (x_i x_j).$$

为了证明 H 是某个同态映射的核, 我们需要证明满足上述条件的群是存在的. 下面我们就来构造一个这样的群.

取正规子群 H 的 r 个陪集为元素, 作一个集合 F :

$$F = \{ Hx_1, Hx_2, \dots, Hx_r \}.$$

在 F 中定义一个乘法如下:

$$Hx_i Hx_j = Hx_i x_j,$$

其中 $Hx_i x_j$ 是 H 的一个陪集, 一定是 Hx_1, Hx_2, \dots, Hx_r 中的某一个. 因为 H 是一个正规子群, 所以这样规定的 $Hx_i x_j$ 是与陪集代表的取法无关的, 因此这样定义的运算是合理的.

下面来验证 F 对这样定义的乘法成一个群.

1) 结合律成立

$$\begin{aligned} (Hx_i Hx_j) Hx_k &= (Hx_i x_j) Hx_k = H(x_i x_j) x_k \\ &= Hx_i (x_j x_k) = Hx_i Hx_j x_k \\ &= Hx_i (Hx_j Hx_k). \end{aligned}$$

2) Hx_1 就是 F 的单位元素.

3) 如果 $x_i^{-1} \in Hx_l$, 那么

$$Hx_i Hx_l = Hx_i Hx_i^{-1} = H = Hx_1,$$

故

$$(Hx_i)^{-1} = Hx_i^{-1}.$$

这说明 F 中元素都有逆元素. 因此, F 成为一个群, 称为 G 对 H 的商群.

定义 9 设 H 是 G 的一个子群. H 在 G 中的全部陪集对群子集的乘法成一个群, 称为 G 对 H 的商群, 记作 G/H .

定理 7 (第二同态定理) 设 H 是 G 的一个正规子群, G/H 是 G 对 H 的商群. 那么 G 到 G/H 上的映射 :

$$g \mapsto Hg$$

是一个满同态映射, 其核为 H .

证明 显然是映上的. 为了证明 是一个同态映射, 只要证明 保持运算就可以了.

对于 G 中任意两个元素 g_1, g_2 , 我们有

$$(g_1 g_2) = Hg_1 g_2 = Hg_1 Hg_2 = g_1 g_2,$$

因此 保持运算, 是一个同态映射.

最后来计算 的核. 核是 G/H 的单位元素的原象. 因为 G/H 的单位元素是 $Hx_1 = H$, 又因

$$g = H \quad Hg = H \quad g \quad H,$$

所以 的核就是 H .

定理 7 中规定的同态映射 称为 G 到商群 G/H 的自然同态.

以上我们证明了 G 的每个正规子群都可作为某个同态映射的核, 而且每个商群都是 G 的同态象. 下面来证明 G 的每个同态象都可这样得到, 即, G 的每个同态象都与 G 的某一个商群同构. 这样, G 的全部同态象就都可以由 G 的商群给出.

定理 8(第三同态定理) 设 G, G_1 是两个群. 如果

$$\varphi: G \rightarrow G_1$$

是一个满同态映射, φ 的核是 K , 那么 $G/K \cong G_1/K_1$.

证明 设 G 对 K 的陪集分解为

$$G = Kx_1 \cup Kx_2 \cup \dots \cup Kx_r,$$

则

$$G/K = \{Kx_1, Kx_2, \dots, Kx_r\}.$$

根据第一同态定理, Kx_i 中的元素在 φ 下的象都等于 $\varphi(x_i)$, 因此可以定义商群 G/K 到 G_1 上的映射:

$$\varphi(Kx_i) = \varphi(x_i).$$

很容易看出, 这个映射是一个一一对应, 而且是保持运算的:

$$\begin{aligned} (\varphi(Kx_i) \varphi(Kx_j)) &= (\varphi(Kx_i x_j)) = (\varphi(x_i x_j)) = \varphi(x_i x_j) \\ &= (\varphi(Kx_i)) (\varphi(Kx_j)), \end{aligned}$$

因此 φ 是一个同构映射. 这就证明了

$$G/K \cong G_1/K_1.$$

这样, 我们就完全解决了群 G 的同态象的问题. 我们把所得到的结论综述如下:

群 G 的任一同态映射的核都是 G 的正规子群; 群 G 的任一个正规子群都是 G 的同态映射的核, 而且以 G 的同一个正规子群为核的同态象都与 G 关于这个正规子群的商群同构, 因此在同构的意义下是唯一的.

我们给出关于正规子群的一个重要定理.

定理 9(同构定理) 设 A 是 G 的一个子群, H 是 G 的一个正规子群. 那么有

$$AH/H \cong A/A \cong H/H.$$

证明 AH/H 中的元素都可表成 $aH(a \in A)$. 如果 $aH = a'H(a', a' \in A)$, 那么 $a^{-1}a' \in A \cap H$. 所以 AH/H 中每个元素都唯一决定 $A/A \cap H$ 中一个元素. 我们可以定义 AH/H 到 $A/A \cap H$ 上的一个映射:

$$aH \mapsto a(A \cap H).$$

很明显, 映射 φ 是一个同态映射. 下面来求 φ 的核.

如果 aH 属于 φ 的核, 那么它在 φ 下的象 $a(A \cap H)$ 就是 $A/A \cap H$ 的单位元素 $A \cap H$. 因此 $a \in A \cap H$, 从而 $aH = H$, 即 φ 的核只包含一个单位元素 H . 因此 φ 是一个同构映射. 这就证明了

$$AH/H \cong A/A \cap H \times$$

最后, 我们来举几个例子.

例 1 设 G 是四元数群 Q_8 , $H = \{e, a^2\}$. 已知 H 是 G 的正规子群, 现在来求 G 关于 H 的商群. 因为 G 对 H 的陪集表示为

$$G = H \cup Ha \cup Hb \cup Hab,$$

所以

$$G/H = \{H, Ha, Hb, Hab\}.$$

G/H 中的运算见下表:

| | H | Ha | Hb | Hab |
|-------|-------|-------|-------|-------|
| H | H | Ha | Hb | Hab |
| Ha | Ha | H | Hab | Hb |
| Hb | Hb | Hab | H | Ha |
| Hab | Hab | Hb | Ha | H |

所以 G/H 是一个 4 阶交换群, 其中非单位元素都是 2 阶元素.

例 2 $G = S_4$,

$$H = \{e, (1, 2)(2, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}.$$

已知 $H \leq G$, 计算 G/H . 由 G 对 H 的陪集分解, 知

$$G/H = \{H, H(1, 2), H(1, 3), H(2, 3), H(1, 2, 3), H(1, 3, 2)\}.$$

因为当 H 是正规子群时, 有 $Ha \cdot Hb = Hab$, 因此知

$$G/H \cong S_3.$$

还可看出, 如果 S_3 表示作用于 $\{1, 2, 3\}$ 上的对称群, 那么

$$G = HS_3 = S_3H.$$

例 3 G 及 H 同例 2, 再令

$$A = \{e, (1, 2, 3, 4), (1, 3)(2, 4), (1, 4, 3, 2)\}.$$

则

$$AH = \{e, (1, 3), (2, 4), (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3), (1, 2, 3, 4), (1, 4, 3, 2)\} < G;$$

$$A/H = \{e, (1, 3)(2, 4)\} < G/H;$$

$$AH/H = \{H, H(1, 3)\} < G/H;$$

$$A/A \cap H = \{A \cap H, (A \cap H)(1, 2, 3, 4)\}.$$

其中 AH/H 与 $A/A \cap H$ 都是 2 阶循环群, 所以

$$AH/H \cong A/A \cap H.$$

下列映射是 AH/H 到 $A/A \cap H$ 上的一个同构映射:

$$H \mapsto A \cap H, H(1, 3) \mapsto (A \cap H)(1, 2, 3, 4).$$

2.5 $A_n(n \geq 4)$ 的单性

对于任意一个群 G , 它的平凡子群 $\{e\}$ 及 G 都是正规子群. 除了这两个平凡子群之外, 如果 G 不再包含其他正规子群, G 就称为一个单群.

定义 10 没有非平凡正规子群的群称为单群.

当 G 是交换群的时候, 任一个子群都是正规子群, 所以 G 是否是单群就根据 G 是不是有非平凡子群而决定. 因此可以用 G 的阶来判断.

定理 10 有限交换群 G 是单群的充分必要条件是 G 的阶是一个素数.

证明 条件的充分性是明显的, 因为根据拉格朗日定理, G 的子群的阶必须是 $|G|$ 的因数. 现在来证条件的必要性. 设 G 的阶不是一个素数, 在 G 中取定一非单位元素 a . 如果 a 的阶小于 G 的阶, 那么 a 生成的循环群就是 G 的一个非平凡子群. 如果 a 的阶等于 G 的阶, 取 $|G|$ 的一个真因数 k :

$$1 < k < |G|.$$

令

$$b = a^k,$$

那么 b 是 G 中一个阶小于 $|G|$ 的非单位元素, $\langle b \rangle$ 就是 G 的一个非平凡子群. \times

非交换的单群也是存在的. 这一节的主要内容就是证明交错群 A_n ($n \geq 4$) 都是单群.

为此, 我们首先需要讨论 A_n 的构造.

引理 A_n ($n \geq 3$) 由一切长度为 3 的轮换生成.

证明 A_n 中每个元素都有偶置换, 因此都可以表成偶数个对换的乘积. 两个不相同的对换如果有一个公共文字, 那么它们的乘积就等于一个 3-轮换:

$$(\dots, i, j, \dots)(\dots, j, k, \dots) = (\dots, i, j, k, \dots).$$

如果它们没有公共文字, 那么它们的乘积可以表成两个 3-轮换的乘积:

$$(\alpha, \beta)(\beta, \gamma) = (\alpha, \beta, \gamma)(\alpha, \beta, \gamma)$$

所以 A_n 中每个元素都可表成 3-轮换的乘积.

另一方面, 长度为 3 的轮换都是偶置换, 故都在 A_n 中.

总结这两方面, 就得到所要证明的结论. \square

定理 11 A_n ($n \geq 4$) 是单群.

证明 当 $n=2$ 时, $A_2 = \{e\}$. 当 $n=3$ 时, A_3 是 3 阶循环群, 因此都是单群. 下面对 $n \geq 5$ 的情形来证明.

设 H 是 A_n ($n \geq 5$) 的一个正规子群, 并设 $H \neq \{e\}$, 来证明 $H = A_n$.

如果 H 包含一个 3-轮换 (α, β, γ) , 我们来证明 H 一定包含任一个 3-轮换 (α, β, γ) . 作 n 元置换

$$= (\alpha, \beta, \gamma) \dots$$

可以适当地调动 (α, β, γ) 的次序使 (α, β, γ) 是一个偶置换, 因此 $(\alpha, \beta, \gamma) \in A_n$. 具有下述性质:

$$(\alpha, \beta, \gamma)^{-1} = (\alpha, \beta, \gamma)$$

因为 H 是 A_n 的正规子群, 所以 $(\alpha, \beta, \gamma) \in H$. 由引理即得

$$H = A_n.$$

现在来证明 H 中一定有 3-轮换.

我们称一个置换所实际变动的文字个数为这个置换的次数. 在 H 中取定一个次数最小的非单位元素, 设为 σ . 因为 σ 是偶置换, 所以 σ 的次数至少是 3. 我们来证 σ 的次数恰等于 3, 因此是一个长度为 3 的轮换.

我们用反证法来证明这个结论. 如果 σ 的次数大于 3, 那么在

它的轮换表法的省略形式中至少出现 4 个文字. 因此 σ 或者是一些不相交的对换的乘积:

$$\sigma = (\dots)(\dots)\dots,$$

或者包含一个长度不小于 3 的轮换

$$= (\dots).$$

这时 σ 至少变动 5 个文字, 否则 $\sigma = (\dots)$ 将是一个奇置换, 不可能在 A_n 中.

在第一种情形, 令 $\sigma = (\dots)$. 再令

$$\sigma^{-1} = (\dots)$$

在第二种情形, 设 $\sigma = (\dots)$ 是 σ 变动的另两个文字. 令 $\tau = (\dots)$, 则得

$$\sigma^{-1} = (\dots)$$

在这两种情形, 都有 $\sigma^{-1} \in H$. 因此 $\sigma^{-1} \in H$. 而因 H 是正规子群, 故有 $\sigma \in H$. 但是 σ^{-1} 的次数比 σ 的次数少, 这与 σ 的取法相矛盾, 所以 σ 一定是一个 3-轮换. 从而

$$H = A_n.$$

当 $n=4$ 时, 我们已知 A_4 有一个 4 阶正规子群, 所以 A_4 不是单群.

定理 12 $A_n (n \geq 4)$ 是 S_n 的唯一的非平凡正规子群.

证明 设 H 是 S_n 的一个非平凡正规子群. H 中全部偶置换组成 H 的一个指数为 2 的正规子群 H^+ , $H^+ = H \cap A_n$ 是 A_n 的一个正规子群. 由 A_n 的单性, 知 $H^+ = A_n$ 或 $H^+ = \{e\}$. 如果 H^+ 是单位子群, 那么 H 是一个 2 阶子群, 由恒等置换和一个奇置换组成, 不可能是 S_n 的正规子群. 所以 $H^+ = A_n$, $H = A_n$, 又因 H 是 S_n 的真子群, 所以 $H = A_n$. \square

交错群是一类很重要的单群, 其中 A_5 是阶数最小的非交换单群. Galois 理论利用 $A_n (n \geq 5)$ 的单性成功地证明了五次和五次以上的一元代数方程不能用根式来求解.

2.6 自同构群

1 自同构群

群 G 到它自身的同构映射称为 G 的自同构. 自同构的一个最简单的例子就是恒等映射, 称为恒等自同构. 在恒等自同构下, 群中每个元素都保持不变. 下面再来举几个自同构的例子.

例 1 用 \mathbb{Z} 表示整数加法群, 将整数 n 映到 $-n$ 的映射是 \mathbb{Z} 的一个自同构.

例 2 设 G 是一个交换群, 将 G 的每个元素映到其逆元素的映射:

$$a \mapsto a^{-1}, \quad a \in G$$

是 G 的一个自同构.

这个例子包含例 1 作为特例. 如果 G 中包含阶不等于 1 或 2 的元素, 那么这个自同构不是恒等自同构.

例 3 设 G 是一个群, a 是 G 中一个取定的元素. 定义映射 α_a :

$$x \mapsto x^a = a^{-1} x a, \quad x \in G.$$

这个映射是一个一一映射, 而且是保持运算的:

$$(xy)^a = a^{-1} (xy) a = (a^{-1} x a)(a^{-1} y a) = x^a y^a,$$

所以 α 是 G 的一个自同构. 这样的自同构称为内自同构. 一个自同构如果不是内自同构, 就称为外自同构.

自同构是群到自身的同构映射, 因此与同构映射一样, 有下述一些性质.

- 1) 自同构将单位元素映到单位元素.
- 2) 自同构将一个元素的逆元素映到这个元素的象的逆元素.
- 3) 自同构将中心元素映到中心元素.

因此, 如果用 Z 表群 G 的中心, 那么对 G 的任一自同构 α , 都有

$$Z^\alpha = Z.$$

4) 如果 H 是 G 的一个子群, α 是 G 的一个自同构, 那么 H 的象集合

$$H^\alpha = \{h^\alpha \mid h \in H\}$$

也是 G 的一个子群. 当然 H 与 H^α 是同构的.

5) 如果 $H \triangleleft G$, 那么 $H^\alpha \triangleleft G$.

证明 任取 $g \in G, h \in H$. 设 g_1 是 g 的原象, h_1 是 h 的原象, 即 $g_1^\alpha = g, h_1^\alpha = h$, 那么

$$\begin{aligned} g^{-1} h g &= (g_1^{-1})^\alpha h_1 g_1 = (g_1^{-1}) h_1 g_1 \\ &= (g_1^{-1} h_1 g_1)^\alpha. \end{aligned}$$

因此 $h \in H$ 而 $H \triangleleft G$, 所以 $g_1^{-1} h_1 g_1 \in H$. 因此 $g^{-1} h g \in H$, H

是 G 的一个正规子群 X .

如果 σ_1, σ_2 是 G 的两个自同构, 那么它们的乘积 $\sigma_1 \sigma_2$ 也是 G 的自同构. 又 G 的自同构的逆映射也是 G 的自同构. 用 $\text{Aut}(G)$ 表示 G 的全部自同构组成的集合, 则 $\text{Aut}(G)$ 对映射的乘法构成一个群, 称为 G 的自同构群. 恒等自同构是 $\text{Aut}(G)$ 的单位元素.

例 4 设 $G = \{e, a\}$ 是一个 2 阶循环群, 那么 G 只有一个自同构, 即恒等自同构. 所以 $\text{Aut}(G)$ 是由一个单位元素组成的群. 2 阶群是唯一的除恒等自同构外不再有其他自同构的群.

例 5 $G = \{e, a, b, c\}$ 是 4 阶非循环交换群. G 中运算为

$$\begin{aligned} a^2 = b^2 = c^2 = e, \quad ab = ba = c, \\ ac = ca = b, \quad bc = cb = a. \end{aligned}$$

我们来计算它的自同构群.

如果 σ 是 G 的一个自同构, 那么 σ 必须把 e 映到 e , 而把 a, b, c 分别映到 a, b, c 中的某一个, 而且各不相同. 因此, σ 的作用有下述 6 种可能:

$$1: e, a, b, c \mapsto e, a, b, c;$$

$$2: e, a, b, c \mapsto e, a, c, b;$$

$$3: e, a, b, c \mapsto e, b, a, c;$$

$$4: e, a, b, c \mapsto e, b, c, a;$$

$$5: e, a, b, c \mapsto e, c, a, b;$$

$$6: e, a, b, c \mapsto e, c, b, a.$$

很容易验证这 6 个映射都是 G 的自同构, 所以 G 的自同构群一共包含 6 个元素:

$$\text{Aut}(G) = \{1, 2, 3, 4, 5, 6\},$$

其中 σ_i 是恒等自同构.

从 $\sigma_i (i=1, 2, \dots, 6)$ 的作用还可看出: $\text{Aut}(S_3) \cong S_3$.

例 6 试证: S_3 共有 6 个自同构, 都是内自同构, 而且 S_3 的自同构群与 S_3 同构.

证明 如果 σ 是 S_3 的一个自同构, 那么 σ 将 S_3 中的 2 阶元素映到 2 阶元素. 因此, σ 将 $(1, 2), (1, 3), (2, 3)$ 这 3 个元素作置换. 因为这 3 个元素生成 S_3 , 所以 S_3 的自同构被它在这 3 个 2 阶元素上的作用唯一确定. 这说明 S_3 最多有 6 个自同构. 考虑 S_3 的内自同构. 如果 S_3 中两个元素 σ, τ 所对应的内自同构相同: $\sigma(x) = \tau(x)$, 则对 S_3 中任一个元素 x , 都有

$$\sigma^{-1}x = \tau^{-1}x,$$

于是

$$x(\sigma^{-1}) = (\tau^{-1})x,$$

τ^{-1} 是 S_3 的中心元素. 但是 S_3 是无中心群, 所以 $\tau^{-1} = e$, 即 $\sigma = \tau$. 这样, S_3 恰有 6 个内自同构, 因而 S_3 的 6 个自同构都是内自同构, 其自同构群为

$$\text{Aut}(S_3) = \{ e, (1, 2), (1, 3), (2, 3), (1, 2, 3), (1, 3, 2) \}.$$

容易证明, S_3 到 $\text{Aut}(S_3)$ 上的映射

$$\sigma \mapsto \sigma$$

是一个同构映射. 因此 $S_3 \cong \text{Aut}(S_3)$.

如果群 G 是无中心群, 并且 G 的自同构都是内自同构, 就称 G 是一个完全群. 例 6 说明 S_3 是一个完全群. 事实上, 只要 $n \geq 3$ 且 $n \neq 6$, S_n 都是完全群. 这一结论我们在这里不予证明.

要找出一个已知群的自同构群一般是很困难的. 在大多数情形下, 群本身的性质不能转移到它的自同构上去. 例如, 例 5 说明

一个交换群的自同构群可以是非交换的. 例 5 和例 6 说明不同构的群可能有同构的自同构群.

可以断定, 一个有限群的自同构群一定也是一个有限群. 因为群 G 的自同构将 G 的元素作置换, 所以 G 的自同构群可以看成作用于 G 上的置换群, 而且因为每个自同构都把单位元素保持不变, 因此, 如果 G 的阶为 n , 那么 $\text{Aut}(G)$ 可以看成是 S_{n-1} 的一个子群. 例 5 给出一个例子说明存在 n 阶群 G 使 $\text{Aut}(G)$ 等于 S_{n-1} .

2 内自同构群

群 G 的两个内自同构的乘积还是一个内自同构:

$$a \circ b = ab,$$

而且内自同构的逆映射也是内自同构:

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

所以 G 的内自同构全体组成 G 的自同构群 $\text{Aut}(G)$ 的一个子群, 记作 $\text{Inn}(G)$, 称为 G 的内自同构群.

内自同构群有下述一些性质.

1) G 到内自同构群 $\text{Inn}(G)$ 上的映射

$$a \mapsto a, \quad a \in G$$

是一个同态映射, 其核为 G 的中心 $Z(G)$, 所以

$$\text{Inn}(G) \cong G/Z(G).$$

2) 设 a, b 是 G 的两个元素, 那么

$$a = b \iff Z(G)a = Z(G)b,$$

即 a 与 b 属于 G 的中心 $Z(G)$ 的同一个陪集.

3) $\text{Inn}(G)$ 是 $\text{Aut}(G)$ 的一个正规子群.

证明 设 α 是 G 的一个自同构, α 是 G 的一个内自同构, 则对 G 中任一元素 x , x 在 $\alpha^{-1} \alpha$ 下的象为

$$\begin{aligned} x^{\alpha^{-1} \alpha} &= (x^{\alpha^{-1}})^{\alpha} = (\alpha^{-1} x \alpha) \\ &= (\alpha)^{-1} x \alpha = x^{\alpha} . \end{aligned}$$

所以 $\alpha^{-1} \alpha = \alpha$ 也是一个内自同构. 因此 $\text{Inn}(G)$ 是 $\text{Aut}(G)$ 的正规子群. α

群 G 的自同构群对内自同构群的商群 $\text{Aut}(G)/\text{Inn}(G)$ 称为 G 的外自同构群.

3 特征子群

如果 H 是 G 的一个子群, α 是 G 的一个自同构, 那么 H^{α} 也是 G 的一个子群. 当然, 一般地 H^{α} 不一定与 H 相同.

定义 11 如果群 G 的子群 H 在群 G 的任一个自同构下的象都等于 H , H 就称为 G 的一个特征子群.

根据特征子群的定义, G 的特征子群在 G 的内自同构下的象也等于自己, 所以特征子群一定是正规子群. 而正规子群是仅对内自同构保持不变的子群, 所以正规子群也称不变子群. 但是正规子群不一定是特征子群. 这一点可以从下面的例子看到.

例 7 我们已知四元数群 Q_8 的子群都是正规子群. 因为群的同自同构保持元素的阶不变, 而 Q_8 中只有一个 2 阶元素 a^2 , 所以子群 $\{e, a^2\}$ 是 Q_8 的一个特征子群. 但是子群

$$b = \{e, b, a^2, a^2 b\}$$

就不是特征子群. 因为 b 在下述自同构下的象不等于 b .

令 α 为 Q_8 到自身的映射:

$$e^1 = e, a^1 = a, a^2 = a^2, a^3 = a^3,$$

$$b^1 = ab, ab^1 = a^2 b, a^2 b^1 = a^3 b, a^3 b^1 = b,$$

那么, σ 是 Q_8 的一个自同构(请读者自己验证). 而

$$b = \{e, ab, a^2, a^3 b\},$$

所以 b 是 Q 的正规子群但不是特征子群.

因为群的自同构把中心映到中心, 所以群 G 的中心 Z 是 G 的特征子群.

我们在以前曾经举例说明过, 正规子群这个性质不是可传的. 而一个子群是特征子群这一性质却是可传的: 如果 G_1 是 G 的特征子群, G_2 是 G_1 的特征子群, 那么 G_2 一定是 G 的特征子群. 这是因为: G 的任一个自同构 σ 把 G_1 映到它自身, 因此可以看成是 G_1 的一个自同构. 又由于 G_2 是 G_1 的特征子群, 所以 $G_2 = \sigma G_2$.

但是要注意: 如果

$$G > G_1 > G_2,$$

而且 G_2 是 G 的一个特征子群, 这时 G_1 有可能不是 G 的特征子群. 我们举例说明这一事实.

例 8 设 G 是由 a, b, c 三个元素生成的有限群, G 中元素的运算满足

$$a^3 = b^3 = c^3 = e, ab = bac,$$

$$ac = ca, bc = cb,$$

因此, G 中元素可表成

$$a^k b^l c^m, 0 \leq k, l, m < 3.$$

G 是一个 27 阶非交换群. G 的中心 Z 是由 c 生成的 3 阶子群. Z 是 G 的一个特征子群.

用 G_1 表示 G 的由 a, c 生成的子群. G_1 是一个 9 阶非循环交换群:

$$G > G_1 > Z.$$

G_1 中元素可表成

$$a^k c^l, \quad 0 \leq k, l < 3.$$

映射 σ :

$$a^k c^l \mapsto a^l c^k$$

是 G 的一个自同构. 因为

$$Z = \langle a \rangle \neq Z,$$

所以 Z 不是 G_1 的特征子群.

4 换位子群

下面介绍一类重要的特征子群.

定义 12 设 G 是一个群, a, b 是 G 中两个元素, 元素 $a^{-1} b^{-1} a b$ 称为 a, b 的换位元素. 由 G 的全部换位元素生成的子群称为 G 的换位子群, 或称导群.

我们常用 $[a, b]$ 表示 a, b 的换位元素, 而用 $[G, G]$ 或 G' 表示 G 的换位子群.

需要注意的是, G 的导群 G' 是由 G 中换位元素生成的子群. 一般来说, G 的全体换位元素不一定组成一个子群, 因此, G 中的元素是一些换位元素的乘积, 但不一定都是换位元素.

因为对于 G 的任一自同构 σ , 都有

$$\begin{aligned} \sigma([a, b]) &= \sigma(a^{-1} b^{-1} a b) = (\sigma(a))^{-1} (\sigma(b))^{-1} \sigma(a) \sigma(b) \\ &= [\sigma(a), \sigma(b)], \end{aligned}$$

所以 G' 是 G 的一个特征子群.

容易看出, G 中两个元素 a, b 可交换的充分必要条件是它们的换位元素 $[a, b] = e$. 当 G 是交换群的时候, $G' = \{e\}$. 这也是 G 为交换群的一个充分条件. 我们有下述更为一般的结果.

定理 13 1) G 关于换位子群 G' 的商群 G/G' 是交换的 .

2) 如果 H 是 G 的一个正规子群, 那么当且仅当 H/G' 是交换群时, 商群 G/H 是交换的 .

证明 1) 对于 G 中任意两个元素 a, b , 来证 Ga 与 Gb 可交换 . 因为它们的换位元素是

$$\begin{aligned} (Ga)^{-1}(Gb)^{-1}(Ga)(Gb) &= Ga^{-1} \cdot Gb^{-1} \cdot Ga \cdot Gb \\ &= Ga^{-1}b^{-1}ab = G, \end{aligned}$$

所以 $GaGb = Gb \cdot Ga$, 即 G/G' 是交换的 .

2) G/H 是交换群的涵意是对 G 中任意两个元素 a, b , 都有

$$(Ha)(Hb) = (Hb)(Ha) .$$

这个条件等价于

$$(Ha)^{-1}(Hb)^{-1}(Ha)(Hb) = H,$$

即

$$Ha^{-1}b^{-1}ab = H,$$

亦即

$$a^{-1}b^{-1}ab = [a, b] \in H .$$

因此当且仅当 H/G' 是交换群时, G/H 是交换的 . \square

例 9 交错群 A_4 的不同的换位元素共有 4 个:

$$e, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3) .$$

这 4 个元素组成一个子群, 即 A_4 .

例 10 在对称群 S_n 中, 任一偶置换都是换位元素 . 另一方面, 凡是换位元素一定是偶置换 . 所以 S_n 的换位子群就是 A_n .

这个结论对一切 n 都成立 . S_n 的换位子群是 A_n , 而且 A_n 中的元素都是换位元素 .

因为 G 的换位子群 G' 是 G 的正规子群, 因此当 G/G' 是非交换

单群时, $G = G$. 由此可知, A_n 的换位子群就等于 A_n .

习 题

1. 求四元数群 Q_8 的全部互不同构的同态象.
2. 设 φ 是群 G 到群 H 上的一个满同态映射, A 是 G 的一个子群. 试证: 如果 A 的阶与 H 的阶互素, 那么 A 包含在 $\ker \varphi$ 的核中.
3. 试证: 共轭元素的中心化子是共轭的.
4. 试证: 共轭元素的正规化子是共轭的.
5. 证明: 如果有限群 G 只有两个共轭元素类, 那么 G 的阶等于 2.
6. 如果 H 是有限群 G 的一个真子群, 那么 G 中必有元素不属于 H 的任一个共轭子群.
7. 设 σ, τ 是对称群 S_n 中两个元素. 证明: σ, τ 在 S_n 中共轭的充分必要条件是它们的轮换表法中轮换的个数相同, 而且可以排列轮换的次序, 使得对应的轮换长度相同 (这样的置换称作是同型的).
8. 证明: 如果 n 元置换 σ 的轮换表法中有 m_1 个 1-轮换, m_2 个 2-轮换, \dots , m_n 个 n -轮换, 则 σ 在 S_n 内的中心化子的阶等于

$$k^{m_k} \cdot m_k ! (\text{规定 } 0! = 1).$$

9. 设 $G = \{e, (1, 2, 3), (1, 3, 2), (4, 6)(5, 7), (1, 2, 3)(4, 6)(5, 7), (1, 3, 2)(4, 6)(5, 7), (1, 2)(4, 5, 6, 7), (1, 2)(4, 7, 6, 5), (1, 3)(4, 7, 6, 5), (2, 3)(4, 7, 6, 5)\}$

是 S_7 的一个子群 .

(1) 求 G 在 S_7 内的中心化子 Z 及正规化子 N .

(2) 验证 $Z = N$.

10 . 证明: 正规子群的交是正规子群 .

11 . 证明: 如果 A, B 都是 G 的正规子群, 那么 AB 也是 G 的正规子群 .

12 . 设 A, B 都是群 G 的正规子群, 并设它们的阶互素, 试证: A 中任一元素与 B 中任一元素都可交换 .

13 . 设 H 是群 G 的一个正规子群, a 是 G 中一个元素 . 试证: 如果 a 的阶与 H 在 G 中的指数互素, 则 $a \in H$.

14 . 设 H 是 G 的一个正规子群, A 是 G 的一个子群 . 试证:

(1) 如果 A 的阶与 H 在 G 中的指数互素, 则 $HA = H$.

(2) 如果 A 在 G 中的指数与 H 的阶互素, 则 $HA = A$.

15 . 如果群 G 有一个交换的正规子群 H 包含于 G 的中心, 并且 G/H 是循环群, 那么 G 是交换群 .

16 . 试证: 群 G 的循环正规子群的子群仍是 G 的正规子群 .

17 . 如果 H 是 G 的正规子群, 则 $G/H \cong S_{G/H}$.

18 . 设 ϕ 是 G 到 G_1 的一个满同态, H 是 G 的一个正规子群 . 求证:

(1) H 是 G_1 的正规子群 .

(2) $G/H \cong G_1/H_1$.

19 . 如果 H 和 K 都是群 G 的正规子群, 并且 $K \subseteq H$, 则

$$G/H \cong (G/K)/(G/H).$$

因此还有

$$G/K \cong (G/H)/(G/H).$$

20 . G 是一个群 . 证明: G 是交换群的充分必要条件是 G 到自身的映射

$$a \mapsto a^{-1}, \quad a \in G$$

是 G 的一个自同构 .

21 . 设 G 是一个 n 阶循环群 .

(1) 求 G 的自同构群 $\text{Aut}(G)$.

(2) 证明: 如果 n 是一个素数, 则 $\text{Aut}(G)$ 是一个循环群 .

22 . 设 a, b 是群 G 的两个元素 . 试证:

(1) 如果 a 与 $[a, b]$ 可交换, 则对任意正整数 n , 都有

$$[a^n, b] = [a, b]^n .$$

(2) 如果 a, b 都与 $[a, b]$ 可交换, 则对任意正整数 n , 都有

$$[a, b]^n = a^n b^n [b, a]^n .$$

23 . 已知 $H = \langle a \rangle$ 是四元数群 Q_8 的一个正规子群, 证明 H 不是 Q_8 的特征子群 .

24 . 证明循环群的子群都是特征子群 .

25 . 如果 H 是 G 的正规子群, A 是 H 的特征子群, 试证: A 是 G 的正规子群 .

第 3 章 置换群的进一步讨论

因为每个抽象群都与一个置换群同构, 所以从代数结构来看, 这两类群是没有什么差别的. 然而, 置换群有其独特的研究方法, 有些关于置换群的概念, 例如不动点和传递性等概念以及由此而得出的置换群的一些特殊子群等, 是置换群所独有的. 而且我们还可以很方便地利用置换群来构造一般群. 此外, 置换群在其他学科中也有很好的应用. 因此我们有必要对置换群进行独立的研究.

这一章对置换群作初步的讨论, 并介绍置换群对抽象群的一些应用.

3.1 置换群的一些子群

在这一章中, 我们用 G 表示 n 元集合 $\Omega = \{ \omega_1, \omega_2, \dots, \omega_n \}$ 上的一个置换群. Ω 中的文字称为点. 如果 g 是 G 中的一个元素, 用 ω_i^g 表示 ω_i 在 g 下的象, 即

$$g = \begin{pmatrix} 1 & 2 & \dots & n \\ \omega_1^g & \omega_2^g & \dots & \omega_n^g \end{pmatrix} = \begin{pmatrix} \omega_1 & \omega_2 & \dots & \omega_n \\ \omega_1^g & \omega_2^g & \dots & \omega_n^g \end{pmatrix}.$$

这一节介绍置换群的一些子群.

1 稳定子群 G_ω

取定 Ω 中一个点 ω , 用 G_ω 表示 G 中保持 ω 不变的全部置换所成的集合, 用 ω^G 表示 ω 在 G 中置换作用下的象集合:

$$G_\omega = \{ g \in G \mid \omega^g = \omega \};$$
$$\omega^G = \{ \omega^g \mid g \in G \}.$$

定理 1 G 是 G 的一个子群, G 的阶满足等式

$$|G| = |G| |G^g|.$$

证明 首先来证 G 是一个子群. G 当然不是一个空集, 因为恒等置换一定属于 G . 如果 g_1 与 g_2 都在 G 中, 那么

$$g_1^{-1} g_2 = g_1^{-1} g_2.$$

因此

$$g_1^{-1} g_2 \in G,$$

所以 $g_1^{-1} g_2 \in G$. G 是 G 的一个子群.

为了计算 G 的阶, 我们讨论 G 对 G 的陪集分解.

设

$$G = \{g_1, g_2, \dots, g_r\},$$

并设

$$g_i = g_i^{-1} g_i, \quad g_i \in G, \quad i = 1, 2, \dots, r,$$

则 G 的陪集分解式为

$$G = G g_1 \cup G g_2 \cup \dots \cup G g_r.$$

这一点可如下证明.

陪集 $G g_i$ ($i = 1, 2, \dots, r$) 中每个置换都把 i 映到 i , 所以陪集 $G g_1, G g_2, \dots, G g_r$ 各不相同. 下面证明 G 中每个元素都必属于这些陪集中的一个. 任取 $g \in G$, 那么 $g \in G$. 设 $g = g_k, 1 \leq k \leq r$, 则

$$g = g_k, \quad g g_k^{-1} \in G, \quad g \in G g_k,$$

这就证明了上述陪集分解式. 从这个陪集分解式就可得出等式

$$|G| = |G| |G^g|.$$

定理证毕. \square

G 称为 G 对 i 的稳定子群.

如果 $g = g$, 则称 i 是 g 的一个不动点. 关于不动点和稳定子

群, 有下述一些简单性质.

命题 1 设 h 及 g 都是 X 上的置换, $x \in X$. 如果 x 是 h 的不动点, 那么 $g^{-1}x$ 是 $g^{-1}hg$ 的不动点.

证明 根据假设, 有

$$(g^{-1}x)^{g^{-1}hg} = hg(g^{-1}x) = x,$$

所以 $g^{-1}x$ 是 $g^{-1}hg$ 的不动点. \square

命题 2 设 G 是 X 上一个置换群, $g \in G$, $H \leq G$, 则

$$g^{-1}Hg = H^g.$$

证明 由命题 1, 知 $g^{-1}Hg \leq H^g$. 另一方面, 由命题 1 可得到

$$(g^{-1})^{-1}H^g g^{-1} = H,$$

因而 $H^g \leq g^{-1}Hg$. 所以 $g^{-1}Hg = H^g$. \square

定理 2 1) 如果 $G = \{g_1, g_2, \dots, g_r\}$, 则与 G 共轭的子群一定是下述子群之一:

$$G_1, G_2, \dots, G_r \text{ (其中可能有相同的).}$$

2) 如果 G 在 x_1, x_2, \dots, x_r 中共有 t 个不动点, 那么 G 一共有 r/t 个不同的共轭子群.

证明 根据 G 对 X 的陪集分解

$$G = Gg_1 \cup Gg_2 \cup \dots \cup Gg_r \\ (g_i = x_i, \quad i = 1, 2, \dots, r)$$

以及 $G \leq N_G(G)$, 可知 G 的共轭子群一定是

$$g_i^{-1}Gg_i = G^{g_i} = G_i \quad (i = 1, 2, \dots, r)$$

中的一个.

如果 G 还保持 $(i \ i^{-1})^G$ 不变, 那么

$$G = G_i.$$

但是上面已经证明了 G 与 G_i 是共轭的, 所以 $G = G_i$. 如果 G 在 G 中一共有 t 个不动点, 不妨设为 i_1, i_2, \dots, i_t , 那么就有

$$G_{i_1} = G_{i_2} = \dots = G_{i_t}.$$

对于 $G_{g_i} (i=1, 2, \dots, r)$ 中任一元素 h_i , 都有

$$h_i^{-1} G h_i = G h_i = G_{i_i},$$

所以

$$G_{g_i} = N_G(G), \quad i=1, 2, \dots, t.$$

而当 $i=t+1, \dots, r$ 时, G_{g_i} 中任一元素都不属于 $N_G(G)$. 因此

$$N_G(G) = G = G_{g_2} = \dots = G_{g_t}.$$

于是

$$|N_G(G) \setminus G| = t, \quad |G \setminus N_G(G)| = r - t.$$

所以 G 共有 $r - t$ 个共轭子群. \square

例 1 $G = \{e, (1, 2), (1, 3), (2, 3),$
 $(1, 2, 3), (1, 3, 2), (4, 5),$
 $(1, 2)(4, 5), (1, 3)(4, 5),$
 $(2, 3)(4, 5), (1, 2, 3)(4, 5),$
 $(1, 3, 2)(4, 5)\}.$

G 是 S_5 的一个 12 阶子群. 下面列出 $G_i (i=1, 2, \dots, 5)$ 及其共轭子群.

$$G_1 = \{e, (2, 3), (4, 5), (2, 3)(4, 5)\};$$

$$G_2 = \{e, (1, 3), (4, 5), (1, 3)(4, 5)\};$$

$$G_3 = \{e, (1, 2), (4, 5), (1, 2)(4, 5)\};$$

$$G_4 = G_5 = \{e, (1, 2), (1, 3), (2, 3),$$

 $(1, 2, 3), (1, 3, 2)\}.$

因为

$$G_1^G = G_2^G = G_3^G = \{1, 2, 3\},$$

所以 G_1, G_2, G_3 组成一个共轭子群类.

又因

$$G_4^G = G_5^G = \{4, 5\},$$

而且

$$G_4 = G_5,$$

因而 G_4 的共轭子群只有它自己. 所以

$$G_4 \triangleleft G.$$

2. G 及 G_i

可以将稳定子群的概念加以推广. 设 S 是 Ω 的一个非空子集, 用 G_S 表示 G 中那些保持 S 中每个点都不变的置换所成的集合:

$$G_S = \{g \in G \mid g^s = s, \forall s \in S\}.$$

可以和前面一样证明 G_S 是 G 的一个子群. 当 S 由一个点 s 组成时, G_S 就是 G_s . 我们有

$$G_S = G \cap G_S \quad (S \subseteq \Omega),$$

$$G_S = G \cap G_S = (G_S)^G.$$

由定理 1 可得下述的有用公式.

命题 3 $|G_S| = |G| \cdot |G_S^G| = |G_S| \cdot |G_S^G|.$

用 S^g 表示 S 在 g 下的象集, 则 G_S 的共轭子群也有和 G_S 类似的性质:

$$g^{-1} G_S g = G_{S^g},$$

其中 g 是 G 中任意置换. 特别地, 如果对 G 中每个置换 g 都有 $S^g = S$, 那么 $G_S \triangleleft G$.

如果我们考虑 G 中那些保持集合 S 不变的置换, 令

$$G_S = \{g \in G \mid g^s = g\},$$

那么 G_S 也是 G 的一个子群. 由 G 及 G_S 的定义知

$$G = G_S \ltimes G_S^c.$$

不仅如此, 我们还有下述结论.

定理 3 G_S 是 G 的正规子群.

证明 任取 $g \in G_S, h \in G$, 要证 $h^{-1}gh \in G_S$. 如果 S 是 X 中的一个点, 那么因为 $h^{-1} \in G_S^c$, 故有

$$h^{-1}gh \in G_S^c,$$

因此

$$h^{-1}gh = [(h^{-1})^g]^h = (h^{-1})^g \in G_S.$$

所以

$$h^{-1}gh \in G_S, G \triangleleft G_S \ltimes G_S^c.$$

例 2 对于例 1 中的 G , 令 $S = \{1, 2\}$, 则

$$G_S = \{e, (4, 5)\},$$

$$G_S^c = \{e, (1, 2), (4, 5), (1, 2)(4, 5)\}.$$

很容易看出

$$G \triangleleft G_S \ltimes G_S^c.$$

3.2 传递群

1 传递群

上一节我们讨论了 X 上置换群 G 的稳定子群, 知道 G 的阶等于 $|G| \cdot |G^g|$, 其中 $G^g = \{s \in X \mid g^s = g\}$. 这一节进一步讨论 $G^g = X$ 的

情形,这时, G 称为一个传递群.

定义 1 G 是 $\Omega = \{1, 2, \dots, n\}$ 上的一个置换群. 如果对任一 $i (i=1, 2, \dots, n)$ 都有 G 中一个元素 g_i 使 ${}^g i = i$, 那么 G 就称为 Ω 上的传递群, 简称传递群. 如果 G 不是传递群, 就称 G 为非传递群.

如果 ${}^g i = i, {}^g j = j$, 那么置换 $g_i^{-1} g_j$ 将 i 映到 j :

$${}^g i^{-1} g_j = {}^g j = j.$$

因此, 如果 G 在 Ω 上是传递的, 那么对 Ω 中任意两个点 i, j 都可找到 G 中一个置换 g , 使得

$${}^g i = j.$$

例如, S_n 及 $A_n (n > 2)$ 都是传递群; 3.1 节例 1 中的置换群不是传递群; 任一群的正则表示以及群对子群的陪集置换表示都是传递群.

对于传递群来说, 任一 $i \in \Omega$ 都有

$$G_i = G.$$

因此, 我们可以将 3.1 节中的结果用于传递群而得出以下定理.

定理 4 设 G 是 $\Omega = \{1, 2, \dots, n\}$ 上的一个传递群, G_i 是 G 对 i 的稳定子群. 则有

1) 任取 G 中将 i 映到 j 的一个置换 $g_j (j=1, 2, \dots, n)$, 那么陪集 $G g_j$ 由 G 中将 i 映到 j 的全体置换组成. 而

$$G = G_i \cup G_i g_2 \cup \dots \cup G_i g_n.$$

2) $|G_i| = n$.

这说明 n 元传递群的阶一定是 n 的一个倍数.

定理 5 G 是 n 元集合 Ω 上的传递置换群, Ω 有 t 个不动点, 那么 G 共有 n/t 个共轭子群.

2 多重传递群

定义 2 设 G 是 $\Omega = \{ \omega_1, \omega_2, \dots, \omega_n \}$ 上的一个置换群. 如果对于 Ω 中任意 k 个点 $\omega_1, \omega_2, \dots, \omega_k$, 都有 G 中一个置换 g 使得

$$g \omega_1 = \omega_1, g \omega_2 = \omega_2, \dots, g \omega_k = \omega_k,$$

那么就称 G 为 **k 重传递群 (或 k -传递群)**.

和传递群一样, 由 k 重传递群的定义可推出: 对于 Ω 的任意两个 k 元子集 $\omega_1, \omega_2, \dots, \omega_k$ 及 j_1, j_2, \dots, j_k , 都有 G 中一个置换 g 使得

$$g \omega_1 = j_1, g \omega_2 = j_2, \dots, g \omega_k = j_k.$$

当然, 传递群是 k 重传递群的一个特殊情形. 从定义还可以看出, k 重传递群一定也是 $k-1$ (如果 $k-1 > 0$) 重传递群. 一个置换群如果包含一个 k 重传递的子群, 那么这个群也一定是 k 重传递的. 如果 G 是一个传递群, 但不是 2 重传递的, 则称 G 是一个单传递群.

例 1 由轮换 $(1, 2, 3, 4, 5, 6)$ 生成的 6 元置换群

$$\{ e, (1, 2, 3, 4, 5, 6), (1, 3, 5)(2, 4, 6), (1, 4)(2, 5)(3, 6), \\ (1, 5, 3)(2, 6, 4), (1, 6, 5, 4, 3, 2) \}$$

是一个传递群, 但不是 2 重传递的, 所以是一个单传递群.

例 2 5 元置换群

$$\{ e, (1, 2, 3, 4, 5), (1, 3, 5, 2, 4), (1, 4, 2, 5, 3), (1, 5, 4, 3, 2), \\ (2, 3, 5, 4), (1, 3, 2, 5), (1, 5, 3, 4), (1, 2, 4, 3), (1, 4, 5, 2), \\ (2, 4, 5, 3), (1, 4, 3, 5), (1, 2, 5, 4), (1, 5, 2, 3), (1, 3, 4, 2), \}$$

$$(2,5)(3,4), (1,5)(2,4), (1,4)(2,3), (1,3)(4,5), \\ (1,2)(3,5)\}$$

是一个双传递群.证明留给读者.

因为 S_n 包含全部 n 元置换,所以 S_n 是 n 重传递群.下述例子给出 A_n 的传递重数.

例 3 $A_n(n \geq 3)$ 是 $n-2$ 重传递的.

证明 对于任意 $n-2$ 个点 i_1, i_2, \dots, i_{n-2} , 总可适当选取 i_{n-1}, i_n 的次序使

$$g = \begin{matrix} 1 & 2 & \dots & n-2 & n-1 & n \\ i_1 & i_2 & \dots & i_{n-2} & i_{n-1} & i_n \end{matrix}$$

是一个偶置换.因此 $g \in A_{n-2}$, A_{n-2} 是 $n-2$ 重传递群. x

从定义直接判断一个置换群是否为 k 重传递的是很麻烦的.下面来给出一个较为简单的方法.

定理 6 设 G 是 $\Omega = \{1, 2, \dots, n\}$ 上的一个传递群. G 是 $k(k \geq 2)$ 重传递群的一个必要充分条件是 G_1 作为 $n-1$ 个点 $\{2, \dots, n\}$ 上的置换群是 $k-1$ 重传递的.

证明 设 G 是 k 重传递的.在 $\{2, \dots, n\}$ 中任取 $k-1$ 个点 i_2, i_3, \dots, i_k , 由 G 的 k 重传递性, 在 G 中有一个置换 g 使得

$$g \cdot 1 = 1, \quad g \cdot 2 = i_2, \quad \dots, \quad g \cdot k = i_k,$$

$g \in G_1$ 并把 $2, \dots, k$ 依次映到 i_2, \dots, i_k , 所以 G_1 是 $k-1$ 重传递的.

设 G_1 是 $k-1$ 重传递的.任取 Ω 中 k 个点 i_1, i_2, \dots, i_k , 因为

G 是传递的, 故有 $g \in G$ 使 $g_{i_1} = 1$. 设

$$g = \begin{pmatrix} i_1 & i_2 & \cdots & i_k & \cdots \\ 1 & j_2 & \cdots & j_k & \cdots \end{pmatrix}.$$

由 G_1 的 $k-1$ 重传递性, 存在 $h \in G_1$ 使

$$h_{i_2} = j_2, h_{i_3} = j_3, \dots, h_{i_k} = j_k.$$

于是

$$gh = \begin{pmatrix} i_1 & i_2 & \cdots & i_k & \cdots \\ 1 & 2 & \cdots & k & \cdots \end{pmatrix},$$

$$(gh)^{-1} = \begin{pmatrix} 1 & 2 & \cdots & k & \cdots \\ i_1 & i_2 & \cdots & i_k & \cdots \end{pmatrix}.$$

所以 G 是 k 重传递的. \square

从定理 6 的证明可看出, 如果把 i_1 换成另一个点 i , 结论仍然成立. 因此有下述推论.

推论 1 设 G 是 n 元传递群. 如果 G_1 是 $n-1$ 元 $k-1$ 重传递群, 那么 $G_i (i=2, 3, \dots, n)$ 也都是 $n-1$ 元 $k-1$ 重传递群.

证明 如果 G_1 是 $n-1$ 元 $k-1$ 重传递群, 那么 G 是 n 元 k 重传递群. 因此 $G_i (i=2, \dots, n)$ 是 $n-1$ 元 $k-1$ 重传递群. \square

反复应用定理 6, 还可得出下述结论.

推论 2 如果 G 是 n 元 k 重传递群, 那么 G 的保持 $r (r < k)$ 个点的稳定子群是 $n-r$ 元 $k-r$ 重传递群. 而 G 的保持 k 个点的稳定子群是一个 $n-k$ 元非传递群.

定理 6 不仅可以用来推断传递群的传递重数, 还可以用来讨论多重传递群的阶.

定理 7 如果 G 是 n 元 k 重传递群, 那么 G 的阶是

$$P_n^k = n(n-1)\dots(n-k+1)$$

的一个倍数.

证明 反复应用定理 4 及定理 6, 即得

$$\begin{aligned} |G| &= n |G_1| = n(n-1) |G_{1,2}| = \dots \\ &= n(n-1)\dots(n-k+1) |G_{1,\dots,k}| \times \end{aligned}$$

设 G 是一个 n 元置换群. 如果 G 是 n 重或 $n-1$ 重传递的, 那么 G 的阶一定是

$$n(n-1)\dots 2 = n!$$

的倍数. 所以 G 一定是 n 元对称群 S_n .

如果 G 是一个 n 元 $n-2$ 重传递群, 那么 G 的阶一定是

$$n(n-1)\dots 3 = n!/2$$

的倍数. 所以 G 是 n 元对称群 S_n 或 n 元交错群 A_n .

我们也知道 S_n 确实是 n 重传递群, A_n 确实是 $n-2$ 重传递群, 所以, S_n 是唯一的 n 元 n 重传递置换群; A_n 是唯一的 n 元 $n-2$ 重(非 $n-1$ 重)传递置换群.

有很多非平凡的(即不等于 S_n 或 A_n 的)双传递群和 3 重传递群. 但是已知的非平凡 4 重传递群只有 4 个, 就是 Mathieu 群 M_{11} , M_{12} , M_{23} , M_{24} . 它们的次数分别是 11, 12, 23, 24, 是法国数学家 Emile Mathieu 在 1861 年发现的. 其中 M_{12} 和 M_{24} 是 5 重传递的, 这是仅有的两个非平凡 5 重传递群, 而且 M_{11} 是 M_{12} 的稳定子群; M_{23} 是 M_{24} 的稳定子群. 这 4 个群都是单群. 已经证明没有传递重数大于或等于 6 的非平凡传递置换群, 而交错群 A_n ($n \geq 6$) 与这

4 个 Mathieu 群是仅有的 4 重传递的单置换群 .

M_{23} 的稳定子群是 Mathieu 群 M_{22} , Mathieu 群 M_{11} , M_{12} , M_{23} , M_{24} 及 M_{22} 的换位子群是最早发现的不属于有限单群的无穷系列的 5 个零散单群 .顺便提一下, 已经证明共有 26 个零散单群 .

5 个 Mathieu 群的阶是:

$$|M_1| = 8 \cdot 9 \cdot 10 \cdot 11,$$

$$|M_2| = 8 \cdot 9 \cdot 10 \cdot 11 \cdot 12,$$

$$|M_2| = 48 \cdot 20 \cdot 21 \cdot 22,$$

$$|M_3| = 48 \cdot 20 \cdot 21 \cdot 22 \cdot 23,$$

$$|M_4| = 48 \cdot 20 \cdot 21 \cdot 22 \cdot 23 \cdot 24 .$$

3.3 非传递群

设 G 是作用在 $\Omega = \{\omega_1, \omega_2, \dots, \omega_n\}$ 上的非传递群, 那么 $\Omega^G = \Omega_1$ 是 Ω 的一个真子集, 在 Ω_1 中取 $\omega_k \in \Omega_1$, 令 $\Omega_2 = \omega_k^G$, 则必有

$$\Omega_1 \cap \Omega_2 = \emptyset .$$

如果 $\Omega_1 \cap \Omega_2 \neq \emptyset$, 那么还可在 Ω_1 中找一个既不属于 Ω_1 也不属于 Ω_2 的点 ω_l . 令 $\Omega_3 = \omega_l^G$, 则 $\Omega_1, \Omega_2, \Omega_3$ 是 Ω 的两两不相交的非空子集 .这样继续下去, 就可把 Ω 分成一些不相交的子集 $\Omega_1, \Omega_2, \dots, \Omega_s$, 使得 Ω 中每个点恰属于一个 $\Omega_i (1 \leq i \leq s)$, 而且每个 Ω_i 中的点都可以用 G 中的置换互变, 而不同的 Ω_i 中的点不能用 G 中的置换互变 .这些 Ω_i 称做 G 的传递集 .更一般地, 我们有下述定义 .

定义 3 设 G 是 Ω 上的一个置换群, Ω_1 是 Ω 的一个子集 .如果 $\Omega_1^G = \Omega_1$, 则称 Ω_1 是 G 的一个不变区 .如果 Ω_1 是 G 的一个不变区, 而且 Ω_1 中任意两个点都可以用 G 中的置换互变, 就称 Ω_1 是 G 的一个传递集或轨道 .

如果 G 是 S_n 上的置换群, 那么对任一 G 的传递集 G_1 , $g^{-1}G_1g$ 就是 G 的一个传递集, 而且, G 的每个传递集都可这样得到.

从定义立即可知: G 是传递群的充分必要条件是 G 只有一个传递集, 即 G .

根据定理 1, 有以下推论.

推论 G 的传递集的长度是 G 的阶的因子.

如果 G_1 是 G 的一个传递集, 那么对任一 $g \in G$ 都有 $g^{-1}G_1g = G_1$. 因此

$$g^{-1}G_1g = G_1g = G_1, \quad \forall g \in G,$$

所以 G_1 是 G 的一个正规子群.

例 1 3.1 节例 1 中的置换群 G 共有两个传递集:

$$G_1 = \{1, 2, 3\} \text{ 及 } G_2 = \{4, 5\}.$$

$$G_1 = \{e, (4, 5)\} \leq G,$$

$$G_2 = G_4 \leq G.$$

设 G 是 S_n 上一个非传递群, 取定 G 的一个不变区 G_1 . 设

$$G_1 = \{1, 2, \dots, k\} \quad (k < n),$$

把 G 中其他文字记成 l_1, l_2, \dots, l_l ($l + k = n$). 那么 G 中每个置换都可以表成

$$g = \begin{array}{cccccccc} 1 & 2 & \dots & k & l_1 & l_2 & \dots & l_l \\ i_1 & i_2 & \dots & i_k & j_1 & j_2 & \dots & j_l \end{array}$$

$$= \begin{array}{cccccccc} 1 & 2 & \dots & k & l_1 & l_2 & \dots & l_l \\ i_1 & i_2 & \dots & i_k & j_1 & j_2 & \dots & j_l \end{array}$$

$$= \begin{pmatrix} 1 & 2 & \cdots & l \\ j_1 & j_2 & \cdots & j_l \end{pmatrix} \begin{pmatrix} 1 & 2 & \cdots & k \\ i_1 & i_2 & \cdots & i_k \end{pmatrix}.$$

令

$$g_1 = \begin{pmatrix} 1 & 2 & \cdots & k \\ i_1 & i_2 & \cdots & i_k \end{pmatrix}, \quad g_2 = \begin{pmatrix} 1 & 2 & \cdots & l \\ j_1 & j_2 & \cdots & j_l \end{pmatrix},$$

那么 g_1 是 Ω 上的一个置换, 其作用与 g 在 Ω 上的作用一样; g_2 是 $\Omega \setminus \Omega_1$ 上的置换, 其作用与 g 在 $\Omega \setminus \Omega_1$ 上的作用一样. g_1, g_2 由 g 唯一确定而且 g_1 与 g_2 是可交换的:

$$g = g_1 g_2 = g_2 g_1.$$

g_1 称为由 g 诱导出的 Ω_1 上的置换. 用 G^1 表示 G 中全部置换诱导出的 Ω_1 上的置换所成的集合. 我们来证明下面的定理.

定理 8 设 Ω_1 是 G 的一个不变区, 则

- 1) G^1 是 Ω_1 上的置换群. 如果 Ω_1 是一个传递集, 则 G^1 在 Ω_1 上是传递的.
- 2) G^1 是 G 的一个同态象, $G^1 \cong G_{\Omega_1}$.

证明 1) 如果 $g_1, h_1 \in G^1$, 那么有 $g, h \in G$, 使

$$g = g_1 g_2, \quad h = h_1 h_2,$$

其中 g_2, h_2 都是作用于 $\Omega \setminus \Omega_1$ 上的置换. 于是

$$gh = (g_1 g_2)(h_1 h_2) = (g_1 h_1)(g_2 h_2),$$

式中 $g_1 h_1$ 是 Ω_1 上的置换, $g_2 h_2$ 是 $\Omega \setminus \Omega_1$ 上的置换. 因此, $g_1 h_1$ 是 gh 诱导出的 Ω_1 上的置换, $g_1 h_1 \in G^1$, 所以 G^1 是一个群.

如果再设 Ω_1 是 G 的传递集, 那么对 Ω_1 中任意两个文字 i, j , 有 $g \in G$, 使

$$g_i = j,$$

所以 G^1 在 \mathcal{I}_1 上是传递的.

2) 作 G 到 G^1 上的映射

$$: g^1 \rightarrow g^1 .$$

这个映射是映上的而且是保持运算的, 所以是一个满同态, 因此 G^1 是 G 的一个同态象.

如果 $g = g^1$ 是恒等置换, 那么 g 一定把 \mathcal{I}_1 中每个点都保持不变, 故 $g \in G_1$. 当然, 当 $g \in G_1$ 时, g 所诱导出的 \mathcal{I}_1 上的置换一定是恒等置换, $g \in G_1$. 所以 \mathcal{I}_1 的核是 G_1 , $G/G_1 \cong G^1$. \square

定义 4 G^1 称为 G 在 \mathcal{I}_1 上的成分. 如果 \mathcal{I}_1 是 G 的一个传递集, 则称 G^1 为 G 的一个传递成分.

从 G 的每个传递集都可以得到 G 的一个传递成分. 因此, 如果 G 有 s 个传递集, 那么 G 就有 s 个传递成分, 因而得到 G 的 s 个传递的同态象.

例 2 例 1 中的 G 有两个传递集:

$$\mathcal{I}_1 = \{1, 2, 3\}, \quad \mathcal{I}_2 = \{4, 5\},$$

所以 G 有两个传递成分:

$$\begin{aligned} G^1 &= \{e, (1, 2), (1, 3), (2, 3), (1, 2, 3), \\ &\quad (1, 3, 2)\} \cong G/G_1, \\ G^2 &= \{e, (4, 5)\} \cong G/G_2. \end{aligned}$$

例 3 $G = \{e, (1, 2)(3, 4), (5, 6),$

$$(1, 2)(3, 4)(5, 6), (1, 3)(2, 4)(7, 8),$$

$$(1, 3)(2, 4)(5, 6)(7, 8),$$

$$(1, 4)(2, 3)(7, 8),$$

$$(1, 4)(2, 3)(5, 6)(7, 8)\}$$

是一个 8 元非传递群, 有 3 个传递集:

$$G_1 = \{1, 2, 3, 4\}, \quad G_2 = \{5, 6\}, \quad G_3 = \{7, 8\}.$$

相应的传递成分为

$$G^1 = \{e, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\},$$

$$G^2 = \{e, (5, 6)\},$$

$$G^3 = \{e, (7, 8)\}.$$

保持 G_i 不动的正规子群是

$$G_1 = \{e, (5, 6)\},$$

$$G_2 = \{e, (1, 2)(3, 4), (1, 3)(2, 4)(7, 8), \\ (1, 4)(2, 3)(7, 8)\},$$

$$G_3 = \{e, (1, 2)(3, 4), (5, 6), (1, 2)(3, 4)(5, 6)\}.$$

容易验证

$$G = G_i \rtimes G^i, \quad i=1, 2, 3.$$

因为非传递置换群 G 的传递成分是 G 的传递的同态象, 因此可以通过传递群来研究和构造非传递置换群.

3.4 传递群作为群的置换表示

1 置换同构

以前我们讨论了群的正则表示及陪集置换表示, 这样就可以利用置换群来讨论一般群. 这一节来证明可以把传递群看成某个群的正则表示或陪集表示, 因而我们可以应用群的传递置换表示的性质来讨论传递群.

为了确切地理解这个问题, 需要引入置换同构的概念.

定义 5 设 G 是 X 上的一个置换群, G' 是 X' 上的一个置换群. 如果存在 X 到 X' 上的一个一一对应 σ , 以及 G 到 G' 的一个一

一一对应, 使得对任一 $i \in X$ 都有

$$(\sigma^{-1})^g(i) = (\sigma^{-1})^g(\sigma(i)),$$

则称 G 与 G 是置换同构的, 记作 $G \cong G$.

如果 G 与 G 是满足定义中条件的一对置换同构的群, 设

$$X = \{1, 2, \dots, n\},$$

则

$$X = \{1, 2, \dots, n\}.$$

如果 g 是 G 中任一元素:

$$g = \begin{pmatrix} i \\ j_i \end{pmatrix},$$

g 在映射 σ 下所对应的置换为 g :

$$g = \begin{pmatrix} i \\ i \end{pmatrix}^g = \begin{pmatrix} i \\ \sigma(i) \end{pmatrix}.$$

这就是说, 在 g 中把每个 i 换成 i 在 σ 下的象 $\sigma(i)$ 就得到 g . 因此 g 与 g 只是所作用的点的表法不一样, 而它们的作用是相同的. 因而 G 与 G 作为置换群可以看成是相同的.

可以证明, 定义 5 中的一一对应 σ 一定是 G 到 G 的一个同构映射. 因为对于 G 中任意两个元素 g_1, g_2 , 任取 X 中一个点 i , 从定义可知

$$\begin{aligned} (\sigma^{-1})^{g_1 g_2}(i) &= ((\sigma^{-1})^{g_1})^{g_2}(i) = ((\sigma^{-1})^{g_1})(\sigma(i))^{g_2} \\ &= ((\sigma^{-1})^{g_1})^{g_2}(\sigma(i)) = (\sigma^{-1})^{g_1 g_2}(i) \\ &= (\sigma^{-1})^{(g_1 g_2)}(i), \end{aligned}$$

其中 i 可以是 X 中任一个点. 因此有

$$(\sigma^{-1})^{g_1 g_2} = \sigma^{-1} g_1 g_2.$$

又因 σ 是一一的, 所以 σ^{-1} 是一个同构映射.

因此, 置换同构的群一定是同构的. 但是同构的群不一定是置

换同构的.

例 1 设

$$G = \{e, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\},$$

$$G = \{e, (1, 2), (3, 4), (1, 2)(3, 4)\},$$

那么, G 与 G 作为抽象群是同构的, 但是它们不是置换同构的. 不仅如此, G 在 $\{1, 2, 3, 4\}$ 上是传递的, 而 G 是非传递的, 因此它们作为置换群是有很大差别的. 这说明同构(而非置换同构)的群不一定有相同的传递性. 这一点在讨论置换群时是需要注意的.

2 一般传递群作为陪集置换表示

定理 9 任一传递置换群置换同构于某个群的陪集置换表示.

证明 设 G 是 n 元集合

$$= \{1, 2, \dots, n\}$$

上的一个传递置换群. 再设 $H = G_1$ 是 G 对 1 的稳定子群. 于是

$$G = Hg_1 \quad Hg_2 \quad \dots \quad Hg_n, \quad Hg_1 = H,$$

式中的置换 g_i 满足

$${}^g_i = i \quad (i = 1, 2, \dots, n).$$

下面来证 G 对 H 的陪集置换表示 $S_{G/H}$ 与 G 是置换同构的.

任取 G 中一个置换 g , 设

$$g = \begin{matrix} 1 & 2 & \dots & n \\ j_1 & j_2 & \dots & j_n \end{matrix}$$

g 所对应的陪集置换为

$${}^g = \begin{matrix} Hg_1 & Hg_2 & \dots & Hg_n \\ Hg_1 g & Hg_2 g & \dots & Hg_n g \end{matrix}.$$

$Hg_i g$ 等于哪个陪集取决于 1 在 $g_i g$ 下的象. 由于

$${}^g_i g = {}^g_i = j_i,$$

所以

$$Hg_i g = Hg_{j_i} \quad (i=1, 2, \dots, n),$$

$$s = \begin{pmatrix} Hg_1 & Hg_2 & \dots & Hg_n \\ Hg_{j_1} & Hg_{j_2} & \dots & Hg_{j_n} \end{pmatrix}.$$

用 s 表示 G 到 $S_{G/H}$ 上的映射.

$$g \mapsto s_g,$$

那么, 由于

$$s_g^{-1} G_1 g = G_i = \{e\},$$

所以 s 是 G 到 $S_{G/H}$ 的一个同构映射. 再定义 s 到

$$s = \{Hg_1, Hg_2, \dots, Hg_n\}$$

的映射 σ 为

$$\sigma_i^{-1} = Hg_i, \quad i=1, 2, \dots, n,$$

那么 σ 是一一对应, 并且

$$\begin{aligned} \left(\begin{smallmatrix} s \\ i \end{smallmatrix} \right) &= \left(\begin{smallmatrix} i_j \\ i \end{smallmatrix} \right) = Hg_{i_j} = (Hg_i)^s \\ &= \left(\begin{smallmatrix} i \\ i \end{smallmatrix} \right)^s = \left(\begin{smallmatrix} i \\ i \end{smallmatrix} \right)^s, \end{aligned}$$

所以 G 与 $S_{G/H}$ 是置换同构的. \square

因此, 任一传递置换群都可看作是某个群的陪集置换表示.

3 正则置换群作为正则表示

定义 6 G 是 X 上的一个置换群, 如果 G 对于 X 中任一个点的稳定子群都是单位子群, 则称 G 是半正则群. 传递的半正则群称为正则群.

从定义可知, 正则群一定是半正则的. 半正则群的子群及成分也都是半正则的. 正则群和半正则群中的非单位元素都是正则置换.

我们知道, 一个群的正则表示一定是正则群; 反之, 有以下定理.

定理 10 任一正则群都与某个群的正则表示置换同构.

证明 设 G 是一个正则群, 那么 G 的稳定子群为单位子群 E , 而 G 对 E 的陪集置换表示就是 G 的右正则表示. 因此从定理 9 的证明可知 G 与其右正则表示是置换同构的. \times

正则群是一类重要的置换群. 下面介绍正则群的一些重要性质.

设 G 是 X 上的一个正则群, $|G|$ 为 G 的阶. 从关于稳定子群的阶的重要公式

$$|G| = |G| \cdot |G^x|$$

可推知正则群的传递集都有相同的长度, 即 $|G|$. 因此, 我们有下述定理.

定理 11 n 元半正则群的阶一定是 n 的一个因数. 一个 n 元传递群是正则群的充分必要条件是它的阶等于 n .

我们来给出另一类正则群.

定理 12 设 G 是 X 上一个交换的传递群, S 是 X 上的对称群, 则

- 1) G 是一个正则群.
- 2) G 在 S 内的中心化子就等于 G .

证明 1) 因为 G 是传递的, 所以对于 X 中任意两个文字 x, y ,

, 存在 G 中一个置换 g 使得 $g^s = e$. 又因 G 是交换的, 所以

$$G = g^{-1} G^s = G^s = G.$$

因为 e 可以是 S 中任意的文字, 所以 $G = \{e\}$, G 是半正则的. 再因 G 是交换群, 所以 G 是正则的.

2) 用 Z 表示 G 在 S 内的中心化子. 因为 G 是交换的, 所以 $G \subseteq Z$, 因此 Z 是传递的. 设 $g \in G$, 如上, 则

$$Z = g^{-1} Z g = Z g = Z,$$

所以 $Z = \{e\}$, Z 是正则的. 比较 Z 与 G 的阶, 即得 $G = Z$.

3.5 本原性

1 定义

定义 7 G 是 S 上的一个传递群. 如果 S 可以分成一些不相交的子集的并:

$$S = \bigcup_{i=1}^s \Omega_i \quad (1 < s < n),$$

$$\Omega_i \cap \Omega_j = \emptyset \quad (i \neq j),$$

使得 G 中每个置换将每个 $\Omega_i (i = 1, 2, \dots, s)$ 仍变为某个 Ω_j , 那么 G 就称为一个非本原群, $\Omega_i (i = 1, 2, \dots, s)$ 称为 G 的非本原集, $\Omega_1, \Omega_2, \dots, \Omega_s$ 称为 G 的一个非本原系. 如果 G 不是非本原群, 则称 G 为本原群.

例 1 由 $(1, 2, 3, 4, 5)$ 生成的 5 元 5 阶传递置换群 G 是一个本原群.

例 2 G 是 S_6 的一个子群, 它由下列两个置换生成

$$g = (1, 2, 3, 4, 5, 6), \quad h = (2, 6)(3, 5).$$

因为

$$hg = g^5 h,$$

所以 G 中共有 12 个元素:

$$g^l h^m, \quad l=0, 1, 2, \dots, 5, \quad m=0, 1.$$

很容易看出 G 是传递的. 将 $\Omega = \{1, 2, 3, 4, 5, 6\}$ 分成 3 个不相交的子集

$$\Omega = \{1, 4\} \cup \{2, 5\} \cup \{3, 6\}.$$

那么, 因为

$$\begin{aligned} & \{1, 4\} \stackrel{g}{\mapsto} \{2, 5\}, \{1, 4\} \stackrel{h}{\mapsto} \{1, 4\}, \\ & \{2, 5\} \stackrel{g}{\mapsto} \{3, 6\}, \{2, 5\} \stackrel{h}{\mapsto} \{3, 6\}, \\ & \{3, 6\} \stackrel{g}{\mapsto} \{1, 4\}, \{3, 6\} \stackrel{h}{\mapsto} \{2, 5\}, \end{aligned}$$

所以 G 是一个本原群. $\{\{1, 4\}, \{2, 5\}, \{3, 6\}\}$ 是 G 的 3 个非本原集, 构成 G 的一个非本原系.

还可以将 Ω 分成两个非本原集

$$\Omega = \{1, 3, 5\} \cup \{2, 4, 6\}.$$

$\{\{1, 3, 5\}, \{2, 4, 6\}\}$ 也是 G 的一个非本原系.

上面的例子说明一个非本原群的非本原系不是唯一的. 但是我们有下述定理.

定理 13 G 是一个非本原群, $\Omega_1, \Omega_2, \dots, \Omega_s$ 是一个非本原系, 那么 $|\Omega_i|$ ($i=1, 2, \dots, s$) 的长度都相等.

证明 任取 $i, j \in \{1, 2, \dots, s\}$. 因为 G 是传递的, 所以有一个置换 $g \in G$ 将 Ω_i 映到 Ω_j . 于是

$$\Omega_j = g(\Omega_i) = \{g(\alpha) \mid \alpha \in \Omega_i\}.$$

由非本集的定义, 得

$$i = j.$$

因此 $|i| = |j| \cdot x$

推论 1 n 元非本原群的非本原集的长度是 n 的因子, 其非本原系中非本原集的个数也是 n 的因子.

推论 2 对于任意素数 p , p 元传递群一定是本原的.

从本原群的定义还可以证明多重传递群一定是本原的. 证明留给读者作为习题(本章习题 18).

2 判别定理

首先来讨论陪集置换表示的本原性.

设 G 是一个 n 阶群, H 是 G 的一个真子群. 如果 G 没有一个异于 H 的真子群能包含 H , 则称 H 为 G 的一个极大子群. 因此, 如果 H 是 G 的一个极大子群, 那么从

$$G > K > H$$

可推出 $K = G$ 或 H ; 如果 H 不是 G 的极大子群, 那么可找到 G 的一个子群 K 使

$$G > K > H.$$

当 $G > K > H$ 时, G 对 K , G 对 H , K 对 H 的指数及陪集代表的关系, 我们已在第 1 章 1.5 节定理 9 中讨论过.

定理 14 G 对子群 H 的陪集置换表示 $S_{G/H}$, 是本原群的充分必要条件是 H 是 G 的一个极大子群.

证明 设 $S_{G/H}$ 是非本原的, 并设

$$\{H = Hg_1, Hg_2, \dots, Hg_l\}$$

是包含 H 的一个非本原集. 令

$$K = H g_1 \quad H g_2 \quad \dots \quad H g_l,$$

来证 K 是 G 的一个子群.

任取 K 中两个元素 $h g_i, h g_j$ ($h, h \in H, 1 \leq i, j \leq l$). 考虑 $h g_i$ 对应的陪集置换:

$$\begin{aligned} & \begin{matrix} H & H g_2 & \dots & H g_l \\ h g_i = & H h g_i & H g_2 h g_i & \dots & H g_l h g_i \\ & H & H g_2 & \dots & H g_l \\ = & H g_i & H g_2 h g_i & \dots & H g_l h g_i \end{matrix} \end{aligned}$$

因为 $\{H g_1, H g_2, \dots, H g_l\}$ 是一个非本原集, 而且 H 在 $h g_i$ 下的像仍在这个集合中, 所以由非本原集的定义, 有

$$\{H g_i, H g_2 g_i, \dots, H g_l g_i\} = \{H g_1, H g_2, \dots, H g_l\}.$$

设

$$H g_j h g_i = H g_t, \quad 1 \leq t \leq l,$$

则

$$h g_j h g_i = h g_t \in K.$$

所以 K 是 G 的一个子群. 因为 $S_{G/H}$ 的非本原集是 $S_{G/H}$ 作用的集合

$$\{H, H g_2, \dots, H g_r\} \quad (r = G/H)$$

的非平凡真子集, 故有 $1 < l < r$, 所以 $G > K > H$. H 不是 G 的极大子群.

另一方面, 如果 H 不是极大子群, 则有 G 的子群 K 满足

$$G > K > H.$$

设 G 对 K , K 对 H 的陪集分解为

$$\begin{aligned} G &= K g_1 \quad K g_2 \quad \dots \quad K g_l, \\ K &= H h_1 \quad H h_2 \quad \dots \quad H h_m, \end{aligned}$$

则 G 对 H 的陪集分解为

$$G = \bigcup_{i,j} Hh_i g_j .$$

我们来证

$$\begin{aligned} \sigma_1 &= \{ Hh_1 g_1, Hh_2 g_1, \dots, Hh_m g_1 \}, \\ \sigma_2 &= \{ Hh_1 g_2, Hh_2 g_2, \dots, Hh_m g_2 \}, \\ &\dots\dots\dots \\ \sigma_l &= \{ Hh_1 g_l, Hh_2 g_l, \dots, Hh_m g_l \} \end{aligned}$$

是 $S_{G/H}$ 的一个非本原系 .

任取 $g \in G$, 设 g 所对应的陪集置换为 σ_g . 考虑

$$\sigma_i = \{ Hh_1 g_i, Hh_2 g_i, \dots, Hh_m g_i \}$$

在置换 σ_g 下的象

$$\sigma_i^g = \{ Hh_1 g_i g, Hh_2 g_i g, \dots, Hh_m g_i g \} .$$

因为

$$\bigcup_{t=1}^m Hh_t g_i = Kg_i$$

是 K 的一个陪集, 所以

$$\bigcup_{t=1}^m Hh_t g_i g = (\bigcup_{t=1}^m Hh_t g_i) g = Kg_i g$$

也是 K 的一个陪集 .

再设

$$Kg_i g = Kg_j ,$$

那么

$$Hh_1 g_i g, Hh_2 g_i g, \dots, Hh_m g_i g$$

就是

$$Hh_1 g_j, Hh_2 g_j, \dots, Hh_m g_j$$

的一个排列, 因此

$$\sigma_i^g = \sigma_j .$$

这就证明了 $\sigma_1, \sigma_2, \dots, \sigma_s$ 是 G 的一个非本原系, G 是非本原的. \square

例 3 第1章1.7节例4中的 H 是 G 的极大子群, 所以这个陪集置换表示是本原的. 而例5中的 H 不是极大子群, 所以相的陪集置换表示是非本原的. $\{H, Ha\}$ 与 $\{H, Hab\}$ 是 $S_{G/H}$ 的一个非本原系.

因为传递群 G 可看成 G 对 G_1 的陪集置换表示, 所以我们可以应用上述定理得到关于置换群的本原性的一个判别法则.

定理 15 设 G 是 Ω 上一个传递群. G 是本原群的充分必要条件是 G 的稳定子群 $G(\alpha)$ 是 G 的一个极大子群.

从定理 15 可以得到下面一些推论.

推论 1 设 G 是 Ω 上一个传递群. 如果 $G(\alpha)$ 还保持 Ω 中另一个点 β 不变, 那么 G 或者是非本原的, 或者是素数次正则群.

证明 如果 G 是正则群, 则因 $|G|$ 是复合数时, G 一定有非平凡子群. 故如果 $|G|$ 不是素数, 那么 G 一定是非本原的.

设 G 是非正则的, 即 $G \neq \{1\}$, 并设 G 一共有 t 个不动点, 那么 $1 < t < n$. 由定理 5, G 有 t 个共轭子群, 因此

$$|G : N_G(G)| = n/t > 1.$$

又因 $|G : G| = n > \frac{n}{t}$, 所以

$$G > N_G(G) > G.$$

G 不是 G 的极大子群, G 是非本原的. \square

推论 2 设 G 是 X 上一个传递群. 如果 X 有一个真子集 A , 不止包含一个文字, 而且

$$g(A) \cap A = \emptyset, \quad g^2(A) \cap A = \emptyset, \quad \dots$$

那么 G 是非本原的.

证明 取定 $x \in A$, 只要证明 G_x 不是 G 的极大子群. 为此考虑 G 的子群 $G_{(x)}$. 我们来证 $G_{(x)}$ 是 G_x 与 G 的中间群.

由假设, 知 $G_{(x)} \neq G_x$. 但是由 G 的传递性, 对于 $x \in A$, $g(x) \in A$ 一定有一个 $g \in G$ 使 $g(x) = x$. 这个置换 $g \in G_{(x)}$ 但不属于 G_x , 所以 $G_{(x)} > G_x$.

再取 $y \in X \setminus A$, 由 G 的传递性, 存在 $g \in G$ 使 $g(x) = y$, 于是

$$g(G_{(x)}) = G_{(y)}, \quad G_{(y)} < G_x.$$

因此 G_x 不是 G 的极大子群, G 是非本原的. \square

这个推论给出了一个求非本原系的方法, 推论中的 A 就是一个非本原集. 因为由假设可知对任一 $g \in G$, 有

$$g(A) \cap A = \emptyset \quad \text{或} \quad g(A) \supseteq A.$$

故由 G 的传递性可将 X 表成不相交的子集之并

$$X = A \cup g_2(A) \cup \dots \cup g_s(A),$$

于是 $A, g_2(A), \dots, g_s(A)$ 就是 G 的一个非本原系.

定理 16 如果 X 上传递群 G 有一个非传递正规子群 $N \neq \{e\}$, 那么 G 是非本原的, 而且 N 的传递集是 G 的一个非本原集.

证明 任取 N 的一个传递集

$$A = \{x_1, x_2, \dots, x_m\}, \quad 1 < m < |X|,$$

本原系, P 是 G 的对应于 $\alpha_1, \alpha_2, \dots, \alpha_s$ 的非本原系置换群. 令

$$K = \{ g \in G \mid g^s \alpha_i = \alpha_i, i = 1, 2, \dots, s \},$$

那么 K 是 G 的一个正规子群, 而且 $P \leq G/K$.

非本原群 G 的一个非本原集置换群 P 是一个传递群, 它的次数比 G 的次数小得多. 因为 P 是 G 的一个同态像, 所以可以利用非本原系置换群来讨论非本原群.

非本原群 G 的非本原系置换群可能还是非本原的. 下面来证明总可选择 G 的一个非本原系, 使 G 对此非本原系的置换表示是本原的, 从而可以通过本原群来讨论非本原群.

设 G 是一个非本原群, $\alpha_1, \alpha_2, \dots, \alpha_s$ 是 G 的一个非本原系, P 是 G 对 $\alpha_1, \alpha_2, \dots, \alpha_s$ 的非本原系置换群. 如果 P 是一个非本原群, 则 $\{\alpha_1, \alpha_2, \dots, \alpha_s\}$ 可以分成一些不相交的非本原集, 设为

$$\{ \alpha_{i1}, \alpha_{i2}, \dots, \alpha_{it} \}, \quad i = 1, 2, \dots, s', 1 < t < s.$$

令

$$\beta_i = \alpha_{ij}, \quad i = 1, 2, \dots, s', t,$$

下面来证 $\beta_1, \beta_2, \dots, \beta_r$ ($r = s't$) 也是 G 的一个非本原系.

首先有

$$\beta_i = \alpha_{i1} \alpha_{i2} \dots \alpha_{it}, \quad \beta_j = \alpha_{j1} \alpha_{j2} \dots \alpha_{jt}, 1 < r < n.$$

任取 $g \in G$, 则

$$g^s \beta_i = \alpha_{i1} \alpha_{i2} \dots \alpha_{it} \quad g^s \beta_j = \alpha_{j1} \alpha_{j2} \dots \alpha_{jt}.$$

因为 $\{\alpha_{i1}, \alpha_{i2}, \dots, \alpha_{it}\}$ ($i = 1, 2, \dots, r$) 是一个非本原系, 所以可找到一个 j ($1 \leq j \leq r$) 使得

$$\{ g^s \beta_{i1}, g^s \beta_{i2}, \dots, g^s \beta_{it} \} = \{ \beta_{j1}, \beta_{j2}, \dots, \beta_{jt} \}.$$

于是

$$g^s \beta_i = \beta_j.$$

这就证明了 $\beta_1, \beta_2, \dots, \beta_r$ 也是 G 的一个非本原系.

考虑 G 对 $\beta_1, \beta_2, \dots, \beta_r$ 的非本原系置换群 P_1 . 如果 P_1 是

非本原的,那么又可将 Ω_i 合并成一些较大的非本原集.由于 Ω 是一个有限集合,这个过程一定会在若干次之后终止.这样就得到 G 的一个非本原系,使 G 的对应的非本原系置换群是本原的.

置换群理论的重要问题之一是找出给定次数的全部互不置换同构的置换群.置换群论的早期工作有很多是有关构造低次置换群方面的问题.在第1章中我们曾经提到过,次数不超过11的置换群已经全部决定;当 $12 \leq n \leq 15$ 时,已决定了全部 n 次传递群;而当 n 再大时,仅对 $16 \leq n \leq 50$ 找出了全部 n 次本原群.

习 题

1. 对第2章习题9中的置换群 G , 求 $G_i (i=1, 2, \dots, 7)$ 及其共轭子群.
2. 令 $\Omega = \{\omega_1, \omega_2\}$. 求上题中 G 的 G 及 G_i , 并验证 $G = G_i$.
3. (1) 设 G 是 Ω 上一个传递群, T 是 G 的一个传递子群, 则对任一 $\omega \in \Omega$, 都有 $G = TG$.
- (2) 对 $G = A_4$ 验证这一结论.
4. G 是 n 次对称群 S_n 的一个子群, $\Omega \subseteq S_n$. 如果 ω 是 G 的一个轨道, 则 ω^{-1} 是 G 的一个轨道.
5. 设 N 是传递置换群 G 的一个正规子群, 则 N 的轨道长度都相等.
6. G 是 S_n 的一个传递子群, 则 $Z_{S_n}(G)$ 是半正则的.
7. (1) 如果 G 是 $\Omega = \{\omega_1, \omega_2, \dots, \omega_n\}$ 上一个2重传递群, 则 $G_{i,j}$ 与 $G_{k,l}$ 共轭 ($i \neq j, k \neq l, 1 \leq i, j, k, l \leq n$).
- (2) 假设 $G_{i,j}$ 一共保持 k 个文字不变, 问 S_n 有多少个与 $G_{i,j}$ 共轭的子群?
8. $G = \langle (1, 3, 6), (2, 5, 9), (4, 7) \rangle < S_9$. 求 G 的全部传递集,

并对每个传递集 求 G 及 G .

9. 求第 1 题中置换群 G 的传递集及传递成分 .

10. 设 $G = \langle \sigma \rangle$, 则 σ 的轮换表示中同一轮换中的点组成 G 的传递集 .

11. 设 H 是置换群 G 的一个传递集, 证明: H 在 G 中的共轭子群的个数等于 (G/H) 在 G 中的共轭子群的个数 .

12. 如果 G 是一个传递群, 那么 G 中每个置换平均有一个不动点, 即 G 中各置换的不动点的总数等于 $|G|$.

13. 如果 G 是一个非传递群, 共有 k 个传递集, 则 G 中每个置换平均有 k 个不动点 .

14. 证明 n 次传递群中一定有 n 次置换 .

15. 设 G_1 是 $\Omega_1 = \{ \alpha_1, \alpha_2, \dots, \alpha_s \}$ 上一个置换群, G_2 是 $\Omega_2 = \{ \beta_1, \beta_2, \dots, \beta_t \}$ 上一个置换群, $\alpha_1, \dots, \alpha_s, \beta_1, \dots, \beta_t$ 各不相同. 对 $g_1 \in G_1, g_2 \in G_2, g_1 g_2$ 可看成作用于

$$\Omega = \Omega_1 \cup \Omega_2 = \{ \alpha_1, \dots, \alpha_s, \beta_1, \dots, \beta_t \}$$

上的一个置换. 令

$$G = \{ g_1 g_2 \mid g_1 \in G_1, g_2 \in G_2 \} .$$

证明:

(1) G 是 Ω 上的一个置换群 .

(2) 如果 G_1 在 Ω_1 上传递, G_2 在 Ω_2 上传递, 则 G 以 Ω_1 及 Ω_2 作为传递集 .

(3) G_1, G_2 都是 G 的正规子群 .

G 称为 G_1 与 G_2 的直积, 记作 $G_1 \times G_2$.

16. 设 G 是一个非传递群, 有两个传递集 Ω_1, Ω_2 . 证明 .

(1) $G = G^{\Omega_1} G^{\Omega_2}$.

(2) $G = G^{\Omega_1} G^{\Omega_2} G^{\Omega_i}, i=1, 2$.

17. 设 G 是由 $(1, 2, \dots, n)$ 生成的循环群, 看成 S_n 的子群 .

(1) 证明 G 是本原群的充分必要条件是 n 是一个素数 .

(2) 当 n 是复合数时, 求 G 的非本原集 .

18. 证明双传递群一定是本原的.

19. 对 3.5 节例 2 验证定理 17.

20. 设 G 是 pq 次非本原群, p 与 q 都是素数, 证明 G 的非本原系置换群一定是本原的.

第4章 交换群

交换群是很重要也是很常见的一类群.因为任何一个群都可能交换的子群及交换的商群,所以交换群的理论在整个群论中占有很重要的地位.

交换群的理论研究已经相当完善.这一章介绍交换群的构造理论.

4.1 直积

为了将一个群用它的子群来表示,需要用到子群的直积的概念.这一节介绍子群的直积的一些性质.

定义 1 设 G 是一个群, A 与 B 是 G 的子群.如果

(1) G 中每个元素 g 都可表成

$$g = ab, \quad a \in A, b \in B,$$

而且表法是唯一的.

(2) A 中元素与 B 中元素可交换.

那么称 G 为子群 A 与 B 的直积,记作 $G = A \times B$, A 与 B 称为 G 的直积因子.

当 G 是交换群的情形,直积称为直和,记作 $G = A \oplus B$, A 与 B 称为 G 的直和因子.

从直积的定义可以看出,如果 $G = A \times B$,那么有:

- (1) $G = BA$;
- (2) $|G| = |A| \cdot |B|$;
- (3) G 是交换群的充分必要条件是 A 与 B 都是交换群.

下面来对直积的定义作一点补充: 定义中表法的唯一性只要对单位元素要求就够了, 即从单位元素表法的唯一性可以推出任一元素表法的唯一性. 可以这样来证明: 如果

$$g = ab = a'b', \quad a, a' \in A; b, b' \in B$$

是 G 中元素 g 的两种表法, 那么

$$(a^{-1}a')(bb'^{-1}) = e.$$

根据单位元素表法的唯一性, 有

$$a^{-1}a' = bb'^{-1} = e,$$

即

$$a = a', \quad b = b'.$$

这就是我们所要证明的.

子群的直积有下述重要性质, 这个性质也可以用来作为直积的定义.

定理 1 如果 $G = AB$, 那么有:

- (1) A, B 都是 G 的正规子群;
- (2) $G = AB$;
- (3) $A \cap B = \{e\}$.

反之, 如果 G 的子群 A, B 满足上述 3 个条件, 那么 $G = AB$.

证明 设 $G = AB$, 那么从定义立刻推出 $G = AB$. $A \cap B = \{e\}$ 可以从表法的唯一性推出: 如果 $c \in A \cap B$, 那么 c 可表成

$$c = c \cdot e, \quad c \in A, e \in B.$$

又可表成

$$c = e \cdot c, \quad e \in A, c \in B.$$

所以从表法的唯一性立刻得到

$$c = e,$$

即

$$A \cap B = \{e\}.$$

再来证 A, B 是 G 的正规子群. 任取 $a \in A, g \in G$, 要证 $g^{-1}ag \in A$. 根据直积的定义, 有 $a_1 \in A, b_1 \in B$, 使 $g = a_1 b_1$, 于是

$$\begin{aligned} g^{-1}ag &= (a_1 b_1)^{-1} a (a_1 b_1) = b_1^{-1} a_1^{-1} a a_1 b_1 \\ &= a_1^{-1} a a_1 b_1^{-1} b_1 = a_1^{-1} a a_1 \in A. \end{aligned}$$

所以 $A \triangleleft G$. 同样可证 $B \triangleleft G$.

现在假设 G 的子群 A, B 满足定理 1 中的 3 个条件, 来证 $G = AB$.

从 $G = AB$ 可以推出对 G 中任一元素 g , 都有 $a \in A, b \in B$ 使 $g = ab$. 下面来证表法是唯一的. 如果

$$g = ab = a'b', \quad a, a' \in A; b, b' \in B,$$

那么

$$a^{-1}a' = b'b^{-1} \in A \cap B.$$

由假设 $A \cap B = \{e\}$, 所以

$$a^{-1}a' = b'b^{-1} = e,$$

即

$$a = a', \quad b = b'.$$

这就证明了表法的唯一性.

最后来证 A 中元素与 B 中元素可交换. 任取 $a \in A, b \in B$, 因为 A, B 都是正规子群, 所以有

$$aba^{-1}b^{-1} = a(ba^{-1}b) \in A$$

及

$$aba^{-1}b^{-1} = (aba^{-1})b^{-1} \in B.$$

从 $A \quad B = \{e\}$, 即得

$$aba^{-1}b^{-1} = e,$$

亦即

$$ab = ba.$$

定理证毕 \times

子群的直积可以推广到几个直积因子的情形.

定义 2 设 $A_1, A_2, \dots, A_s (s \geq 2)$ 都是 G 的子群. 如果

(1) G 中任一元素 g 都可以唯一地表示成

$$g = a_1 a_2 \dots a_s, \quad a_i \in A_i (i = 1, 2, \dots, s);$$

(2) A_i 中任意元素与 A_j 中任意元素可交换 ($i, j = 1, 2, \dots, s; i \neq j$). 那么 G 称为 A_1, A_2, \dots, A_s 的直积, 记作 $G = A_1 \times A_2 \times \dots \times A_s$, $A_i (i = 1, 2, \dots, s)$ 称做 G 的直积因子.

多个子群的直积也和两个子群的直积一样具有下述性质: 直积因子的次序可以更换; G 的阶等于各直积因子的阶的乘积; 从各直积因子的交换性可以推出 G 的交换性. 同样地, 任意元素表法的唯一性也可以从单位元素表法的唯一性推出.

从定义可以看出, 如果

$$G = A_1 \times A_2 \times B, \quad A = A_1 \times A_2, \quad B = B_1 \times B_2,$$

那么

$$G = A_1 \times A_2 \times B_1 \times B_2.$$

反之, 如果

$$G = A_1 \times A_2 \times B_1 \times B_2,$$

那么, 令

$$A = A_1 \times A_2, \quad B = B_1 \times B_2,$$

就有

$$G = A \quad B,$$

即

$$G = (A_1 \quad A_2) \quad (B_1 \quad B_2).$$

所以在多个子群的直积中,可以任意添加或去掉括号.

最后,和两个子群的直积相仿,多个子群的直积也有与定理 1 类似的结论.

定理 2 设 A_1, A_2, \dots, A_s ($s \geq 2$) 是 G 的子群.

$$G = A_1 \quad A_2 \quad \dots \quad A_s$$

的充分必要条件是

- (1) A_1, A_2, \dots, A_s 都是 G 的正规子群;
- (2) $G = A_1 A_2 \dots A_s$;
- (3) $A_1 \dots A_{i-1} A_{i+1} \dots A_s \cap A_i = \{e\}, \quad i = 1, 2, \dots, s.$

这个定理的证明与定理 1 的证明差不多,这里就不重复了.

利用子群的直积这个概念可以将群的一些问题化为子群的问题来研究.例如,群的运算可以归结为子群的运算,设

$$\begin{aligned} G &= A_1 \quad A_2 \quad \dots \quad A_s, \\ g &= g_1 g_2 \dots g_s, \quad g_i \in A_i \quad (i = 1, 2, \dots, s), \\ h &= h_1 h_2 \dots h_s, \quad h_i \in A_i \quad (i = 1, 2, \dots, s), \end{aligned}$$

那么

$$\begin{aligned} gh &= (g_1 h_1)(g_2 h_2) \dots (g_s h_s), \\ g_i h_i &\in A_i \quad (i = 1, 2, \dots, s). \end{aligned}$$

又如上面已经提到过, G 的交换性可以从 A_i 的交换性得出.更进一步,我们有:如果 Z, Z_1, Z_2, \dots, Z_s 分别是 G, G_1, G_2, \dots, G_s 的中心,那么有

$$Z = Z_1 \quad Z_2 \quad \dots \quad Z_s.$$

证明留作习题.

$$\begin{aligned} & (1, 3)(2, 4)(1, 3, 2), \\ & (1, 4)(2, 3)(1, 3, 2) \}. \end{aligned}$$

很容易看出

$$(1, 2)(3, 4), (1, 3)(2, 4), (1, 2, 3)$$

是 G 的一组生成元, 而且从

$$[(1, 2)(3, 4)]^l [(1, 3)(2, 4)]^m (1, 2, 3)^k = e$$

可推出

$$l \equiv 0 \pmod{2}, m \equiv 0 \pmod{2}, k \equiv 0 \pmod{3},$$

即

$$(1, 2)(3, 4)^l = [(1, 3)(2, 4)]^m = (1, 2, 3)^k = e.$$

所以这 3 个元素组成 G 的一组基.

G 的基不是唯一的, 读者可以自己再找出 G 的另一组基.

交换群的基有下述一些性质:

1. 如果 $G = A \times B$, a_1, a_2, \dots, a_s 是 A 的一组基, b_1, b_2, \dots, b_r 是 B 的一组基, 那么 $a_1, \dots, a_s, b_1, \dots, b_r$ 是 G 的一组基.

2. 如果 a_1, a_2, \dots, a_s 是 G 的一组基, 设 a_1, a_2, \dots, a_l ($0 < l < s$) 生成的子群是 A ; $a_{l+1}, a_{l+2}, \dots, a_s$ 生成的子群是 B , 那么

$$G = A \times B.$$

特别地, 有

$$G = \langle a_1 \rangle \times \langle a_2 \rangle \times \dots \times \langle a_s \rangle,$$

其中 $\langle a_i \rangle$ 是 a_i 生成的循环群.

这两条性质可以从基的定义和直积的性质直接推出, 从这两条性质可以看到交换群的直积分解与基的选择有密切的关系. 下面对交换群证明基的存在.

定理 3 有限交换群一定有基 .

证明 设 G 是一个有限交换群 . a_1, a_2, \dots, a_r 是 G 的一组生成元 . 我们对 r 作归纳法 .

当 $r=1$ 时, G 是由 a_1 生成的循环群, a_1 就是 G 的一组基 .

当 $r \geq 2$ 时, 设定理对于具有一组元素个数少于 r 的生成元的有限交换群成立 . 来证定理对于由 r 个元素生成的群也成立 .

在所有使

$$a_1^{k_1} a_2^{k_2} \dots a_r^{k_r} = e$$

成立的 k_i 中有一个最小的正整数, 设为 m , 我们再对 m 作归纳法 .

可以调动 a_i 的次序使 m 是 a_1 的指数, 于是有整数 m_2, \dots, m_r 使

$$a_1^m a_2^{m_2} \dots a_r^{m_r} = e. \quad (1)$$

如果 $m=1$, 那么

$$a_1 = a_2^{-m_2} \dots a_r^{-m_r}.$$

G 可以由 $r-1$ 个元素 a_2, a_3, \dots, a_r 生成, 由归纳法假设 G 有基 .

下面设 $m > 1$. 将 m_i 表成

$$m_i = t_i m + s_i, \quad 0 \leq s_i < m (i = 2, \dots, r).$$

令

$$a^* = a_1 a_2^{t_2} \dots a_r^{t_r}. \quad (2)$$

由(1), (2)两式得

$$(a^*)^m a_2^{s_2} \dots a_r^{s_r} = e.$$

如果 $s_i (i = 2, \dots, r)$ 中有一个不等于 0, 那么它一定小于 m , 对这个 s_i 应用归纳法假设, 知 G 有基 . 因此可设

$$s_2 = s_3 = \dots = s_r = 0.$$

此时有

$$(a^*)^m = e.$$

因为 a_1 可以用 a^*, a_2, \dots, a_r 表示:

$$a_1 = a_1^* a_2^{-l_2} \dots a_r^{-l_r},$$

所以 a_1^*, a_2, \dots, a_r 也是 G 的一组生成元, 我们来证明

$$G = \langle a_1^*, a_2, \dots, a_r \rangle.$$

根据定理 1, 为了证明这个分解式, 只要证明

$$\langle a_1^*, a_2, \dots, a_r \rangle = \{e\}.$$

任取 $a = a_1^* a_2^{l_2} \dots a_r^{l_r}$, 那么 a 可以表成

$$a = (a_1^*)^l = (a_1 a_2^{l_2} \dots a_r^{l_r})^l = a_2^{l_2} \dots a_r^{l_r},$$

于是

$$a_1^l a_2^{l_2} \dots a_r^{l_r} = e. \quad (3)$$

对于整数 l, m , 可以找到整数 x 使

$$0 < l - xm < m.$$

由(1), (3)两式得

$$a_1^{l-xm} a_2^{l_2} \dots a_r^{l_r} = e.$$

根据 m 的选择, 必须有

$$l - xm = 0.$$

因此

$$a = (a_1^*)^l = (a_1^*)^{xm} = e.$$

这样就证明了 $G = \langle a_1^*, a_2, \dots, a_r \rangle$.

因为 a_2, \dots, a_r 可以由 $r-1$ 个元素生成, 根据归纳法假设, a_2, \dots, a_r 有一组基, 设为 b_2, \dots, b_u . 于是 a_1^*, b_2, \dots, b_u 就是 G 的一组基, 定理证毕. \square

根据有限交换群的基的存在性, 可以得到下列推论.

推论 任一有限交换群都可以表成循环群的直积.

设 G 是一个有限群, 在 G 中取定一组基 a_1, a_2, \dots, a_s , 那么

$$G = \langle a_1, a_2, \dots, a_s \rangle.$$

设 a_i 的阶为 n_i ($i = 1, 2, \dots, s$), 那么 G 中任一元素 g 都可唯一地表示成

$$g = a_1^{k_1} a_2^{k_2} \dots a_s^{k_s}, \quad 0 \leq k_i < n_i \quad (i = 1, 2, \dots, s).$$

如果 h 也是 G 中一个元素, 设

$$h = a_1^{l_1} a_2^{l_2} \dots a_s^{l_s}, \quad 0 \leq l_i < n_i \quad (i = 1, 2, \dots, s),$$

那么

$$gh = a_1^{m_1} a_2^{m_2} \dots a_s^{m_s},$$

式中的 m_i 满足

$$m_i \equiv h_i + l_i \pmod{n_i}, \quad 0 \leq m_i < n_i, \quad i = 1, 2, \dots, s.$$

在下一节中我们将进一步讨论有限交换群的直积分解.

4.3 有限交换群的构造

我们以前讨论过循环群, 循环群可以由一个元素生成, 它的构造是很简单的. 上一节我们通过基的存在性, 证明了有限交换群可以表示成循环子群的直积, 这一节我们进一步来证明有限交换群可以分解成阶为素数的方幂的循环子群的直积, 而且表示法是唯一的. 这样就完全解决了有限交换群的构造问题.

我们先来证明一个更为一般的结论. 设 G 是一个有限交换群, 用 $G(p)$ 表示 G 中阶为素数 p 的方幂的元素全体, 那么 $G(p)$ 显然是非空集合, 而且对 G 的运算是封闭的, 所以 $G(p)$ 是 G 的一个子群.

定理 4 设 G 是一个 n 阶交换群, $n = p_1^{i_1} p_2^{i_2} \dots p_s^{i_s}$, 其中 p_1, \dots, p_s 是两两不同的素数, $i_i > 0$ ($i = 1, 2, \dots, s$), 那么

$$G = G(p_1) \times G(p_2) \times \dots \times G(p_s).$$

为了证明定理 4, 需要用到一个结果, 这个结果在任何群中都

是成立的, 我们把它写成一个引理.

引理 设 a 是群 G 中一个元素, a 的阶等于 $m = m_1 m_2$, 其中 m_1 与 m_2 是两个互素的正整数, 那么 a 可以唯一地表成 $a = a_1 a_2$, 式中 a_i 的阶是 m_i ($i = 1, 2$); $a_1 a_2 = a_2 a_1$; 而且 a_i ($i = 1, 2$) 都是 a 的方幂.

证明 因为 m_1 与 m_2 互素, 故有整数 u_1, u_2 使得

$$u_1 m_1 + u_2 m_2 = 1,$$

于是

$$a = a^{u_1 m_1 + u_2 m_2} = a^{u_1 m_1} \cdot a^{u_2 m_2} = a^{u_2 m_2} \cdot a^{u_1 m_1}$$

令

$$a_1 = a^{u_2 m_2}, \quad a_2 = a^{u_1 m_1},$$

则 a_1, a_2 都是 a 的方幂, 而且

$$a = a_1 a_2 = a_2 a_1.$$

下面来看 a_1, a_2 的阶. 因为

$$a_1^{m_1} = a^{u_2 m_2 m_1} = e, \quad a_2^{m_2} = a^{u_1 m_1 m_2} = e,$$

所以 a_1 的阶是 m_1 的一个因子 d_1 , a_2 的阶是 m_2 的一个因子 d_2 .

由于 a_1 与 a_2 可交换, 并且 d_1 与 d_2 互素, 故 $a_1 a_2$ 的阶等于 $d_1 d_2$.

但是已知 a 的阶是 $m_1 m_2$, 所以必须有

$$d_1 = m_1, \quad d_2 = m_2.$$

最后来证表法的唯一性. 设

$$a = a' a'' = a_1' a_2',$$

其中 a', a'', a_1', a_2' 都满足条件, 那么

$$a'^{-1} a_1' = a_2' a_2'^{-1}.$$

因为 a', a_1' 都是 a 的方幂, 所以它们可以交换, 于是 $a'^{-1} a_1'$ 的阶是 m_1 的因子, 同样可知 $a_2' a_2'^{-1}$ 的阶是 m_2 的因子. 由假设知 m_1 与 m_2 互素, 故必有

$$a^{-1} a_1 = a_2 a^{-1} = e,$$

从而

$$a_1 = a_1, a_2 = a_2.$$

唯一性得证 \times

反复应用引理, 可以得到 m 分解成几个互素的因子的一般情形:

设 a 是群 G 中一个元素, a 的阶为 $m = m_1 m_2 \dots m_r$ ($r \geq 2$), 其中 m_1, m_2, \dots, m_r 是两两互素的正整数, 那么 a 可以唯一地表成

$$a = a_1 a_2 \dots a_r,$$

其中 a_i 的阶为 m_i , $a_i a_j = a_j a_i$, 而且 a_i 都是 a 的方幂 ($i, j = 1, 2, \dots, r$).

定理 4 可以从这个结论直接得出.

因为 $G(p_i)$ 中元素的阶都是 p_i 的方幂, 故由定理 3 及其推论可知 $G(p_i)$ 的阶也是 p_i 的方幂. 又因

$$|G| = \prod_{i=1}^s |G(p_i)|,$$

所以可得

$$|G(p_i)| = p_i^i, \quad i = 1, 2, \dots, s.$$

定义 4 如果群 G 中一个元素 g 的阶为素数 p 的一个方幂, 则称 g 为一个 p -元素. 如果群 G 的阶是素数 p 的一个方幂, 则称 G 为一个 p -群.

因为群中元素的阶为这个群的阶的因子, 故 p -群中的元素都是 p -元素. 以后我们将看到, 如果有限群 G 中每个元素都是 p -元素, 那么 G 一定是一个 p -群. 因此 p -群也可以定义为其元素皆为 p -元素的群.

定义 5 设群 G 的阶为 $n = p n_1$, 其中 p 是一个素数, $1, n_1$ 与 p 互素, 那么 G 的 p 阶子群称为 G 的一个 Sylow p -子群.

定理 4 说明: 当 G 是 n 阶有限交换群的时候, 对于 n 的每个素因子 p , G 的 Sylow p -子群都是存在且唯一的, 而且 G 可以表成它的 Sylow p -子群的直积.

从定理 4 以及上节的结果, 还可以知道任一有限交换群都可以表成循环 p -子群的直积. 下面来证明表法是唯一.

首先对表法的唯一性作一点说明, 先来看两个例子.

例 1 G 是上节例 1 中的群, 已知 G 有一组基是

$$(1, 2)(3, 4), (1, 3)(2, 4), (1, 2, 3),$$

所以 G 可以分解成循环 2-子群

$$(1, 2)(3, 4), (1, 3)(2, 4)$$

及循环 3-子群 $(1, 2, 3)$ 的直积:

$$G = (1, 2)(3, 4) (1, 3)(2, 4) (1, 2, 3).$$

很容易看出 G 还有另一种分解:

$$G = (1, 2)(3, 4) (1, 4)(2, 3) (1, 2, 3).$$

例 2 设 G 是由 6 阶元素 a 及 4 阶元素 b 生成的 24 阶交换群, 那么

$$G = \langle a, b \rangle.$$

但是 a 的阶不是素数的方幂, 我们再把 G 进一步分解:

$$G = \langle a^3, a^2, b \rangle.$$

G 就表成了循环 p -子群的直积. G 还可以分解成:

$$G = \langle a^3 b^2, a^2, a^3 b \rangle.$$

这也是循环 p -子群的直积.

这两个例子说明同一个交换群可以用几种方法分解成循环 p -子群的直积. 但是我们可以看出在同一个群的不同分解式中, 直积因子的个数和阶都是一样的. 所谓表法的唯一性就是指的这个事实.

因为在直积分解中可以交换直积因子的次序并且可以随意添加或去掉括号, 所以我们只要对交换 p -群来证明分解的唯一性.

定理 5 设有限交换 p -群 G 用两种方法表成循环 p -群的直积:

$$G = A_1 \times A_2 \times \dots \times A_r = B_1 \times B_2 \times \dots \times B_s,$$

那么必有 $r = s$, 而且可以适当地排列 B_i 的次序使得 B_i 与 A_i ($i = 1, 2, \dots, r$) 有相同的阶.

证明 我们对 G 的阶作归纳法, 当 $|G| = p$ 时定理显然成立.

用 G_p 表示 G 中满足 $a^p = e$ 的元素全体组成的子群; 用 G^p 表示 G 中形如 b^p ($b \in G$) 的全体元素组成的子群.

用 a_i 表示 A_i ($i = 1, 2, \dots, r$) 的一个生成元, 那么 a_1, a_2, \dots, a_r 是 G 的一组基. 设 a_i 的阶是 p^{e_i} ($i = 1, 2, \dots, r$), 并设 (必要时可调动 A_i 的次序)

$$e_1 \leq e_2 \leq \dots \leq e_r = 1,$$

于是 $a_1^{p^{e_1-1}}, a_2^{p^{e_2-1}}, \dots, a_r^{p^{e_r-1}}$ 是 G_p 的一组基, G_p 的阶为 p^r . 如果 $a_1 = \dots = a_r = 1$, 那么 $G^p = \{e\}$, 否则如果

$$e_1 \leq e_2 \leq \dots \leq e_m > e_{m+1} = \dots = e_r = 1 \quad (1 \leq m < r),$$

那么 $a_1^p, a_2^p, \dots, a_m^p$ 就是 G^p 的一组基.

B_i 的生成元 b_i ($i = 1, 2, \dots, s$) 给出 G 的另一组基 b_1, b_2, \dots, b_s . 设 b_i 的阶是 p^{f_i} 并调动 B_i 的次序使 $f_1 \leq f_2 \leq \dots \leq f_r = 1$. 如上可知 G_p 的阶等于 p^s , 所以必有 $r = s$. 如果 $G^p = \{e\}$, 那么必有

$f_1 = f_2 = \dots = f_s = 1$ 定理得证. 如果 $G^p = \{e\}$, 那么设

$f_1 > f_2 > \dots > f_m > f_{m+1} = \dots = f_r = 1$ ($1 \leq m < r$), 则 a^p, b^p, \dots, b_m^p 是 G^p 的另一组基, G^p 有两种方法表成循环子群的直积:

$$\begin{aligned} G^p &= \langle a^p \rangle \times \langle b^p \rangle \times \dots \times \langle b_m^p \rangle \\ &= \langle a^p \rangle \times \langle b^p \rangle \times \dots \times \langle b_m^p \rangle. \end{aligned}$$

因为 G^p 的阶小于 G 的阶, 对 G^p 应用归纳法假设可得 $m = m$, 而且 a^p 与 b^p ($i = 1, 2, \dots, m$) 有相同的阶, 因此 a 与 b_i ($i = 1, 2, \dots, s$) 也有相同的阶, 即 A_i 与 B_i ($i = 1, 2, \dots, s$) 有相同的阶. \square

由此可得出关于有限交换群的基本定理.

定理 6 有限交换群可以唯一地表成循环 p -群的直积.

定理 6 也说明了有限交换群的由阶为素数幂的元素组成的基中元素的个数及其阶的唯一性, 由此引入下述概念.

定义 6 如果有限交换群 G 可以表成循环 p -群 G_1, G_2, \dots, G_s 的直积, G_i 的阶为 n_i ($i = 1, 2, \dots, s$), 则 n_1, n_2, \dots, n_s 称为 G 的型不变量, 也称 G 为 (n_1, n_2, \dots, n_s) 型群. 如果 G 的型不变量都是素数, 那么 G 称为初等交换群.

推论 两个有限交换群同构的充分必要条件是它们的型不变量相同.

例 3 例 1 中 G 的型不变量是 $2, 2, 3$, 所以 G 是一个初等交换群.

例4 由置换 $(1, 2, 3, 4), (1, 2, 3)$ 生成的群是12阶交换群, 它的型不变量是 $2^2, 3$. 这个群与上题中的 G 不同构.

例5 p^4 阶交换群的型不变量有下述5种可能:

$$p, p, p, p; \quad p^2, p, p; \quad p^2, p^2; \quad p^3, p; \quad p^4.$$

所以 p^4 阶交换群在同构的意义下共有5个.

下面来说明交换群的型不变量与其子群的不变量之间的关系.

定理7 设 G 是一个交换 p -群, 它的型不变量是 $p^{e_1}, p^{e_2}, \dots, p^{e_s} (e_1 \geq e_2 \geq \dots \geq e_s > 0)$, 则 G 有以 $p^{f_1}, p^{f_2}, \dots, p^{f_t} (f_1 \geq f_2 \geq \dots \geq f_t > 0)$ 为型不变量的子群的必要充分条件是 $t \leq s$, 并且 $f_i \leq e_i (i = 1, 2, \dots, t)$.

证明 首先来证明 G 的子群 H 的型不变量 $p^{f_1}, p^{f_2}, \dots, p^{f_t} (f_1 \geq f_2 \geq \dots \geq f_t > 0)$ 满足定理中的条件.

对 G 的阶作归纳法. 当 $|G| = p$ 时, 结论显然是成立的.

设 G 的阶大于 p , 如果 G 是初等交换群, 那么 H 也是初等交换群, 此时

$$e_1 = e_2 = \dots = e_s = 1; \quad f_1 = f_2 = \dots = f_t = 1.$$

比较 G 与 H 的阶即得 $t \leq s$. 所以结论是成立的. 如果 G 不是初等交换群, 则 G_p 是 p^s 阶初等交换群, H_p 是 p^t 阶初等交换群. 所以有 $t \leq s$. 再设

$$\begin{aligned} e_1 &\geq e_2 \geq \dots \geq e_m > e_{m+1} = \dots = e_s = 1, \\ f_1 &\geq f_2 \geq \dots \geq f_l > f_{l+1} = \dots = f_t = 1. \end{aligned}$$

于是 G 的型不变量是

$$\begin{aligned} &p^{e_1-1}, p^{e_2-1}, \dots, p^{e_m-1} \\ &(e_1 - 1, e_2 - 1, \dots, e_m - 1, 1), \end{aligned}$$

H^p 的型不变量是

$$p^{f_1-1}, p^{f_2-1}, \dots, p^{f_l-1} \\ (f_1 - 1 \quad f_2 - 1 \quad \dots \quad f_l - 1 \quad 1).$$

因为 H^p 是 G^p 的子群而且 G^p 的阶小于 G 的阶, 故由归纳法假设, 有

$$l = m; f_i - 1 = e_i - 1, \quad i = 1, 2, \dots, l.$$

又因

$$f_{l+1} = \dots = f_t = 1,$$

所以

$$f_i = e_i, \quad i = l+1, \dots, t.$$

因此有

$$f_i = e_i, \quad i = 1, 2, \dots, t.$$

再证如果 f_1, f_2, \dots, f_t 满足定理中的不等式, 一定存在以 $p^{f_1}, p^{f_2}, \dots, p^{f_t}$ 为型不变量的子群. 设 a_1, a_2, \dots, a_s 是 G 的一组基, 它们的阶依次为 $p^{e_1}, p^{e_2}, \dots, p^{e_s}$. 令

$$b_i = a_i^{p^{e_i - f_i}}, \quad i = 1, 2, \dots, t,$$

则 b_i 的阶为 p^{f_i} ($i = 1, 2, \dots, t$).

$$H = \langle b_1, b_2, \dots, b_t \rangle$$

就是 G 的一个以 $p^{f_1}, p^{f_2}, \dots, p^{f_t}$ 为型不变量的子群. \square

定理 7 可以推广到更一般的情形: 设交换群 G 的型不变量是

$$p_1^{e_1 s_1}, \dots, p_1^{e_1 s_{s_1}}, p_2^{e_2 s_2}, \dots, p_2^{e_2 s_{s_2}}, \dots, p_u^{e_u s_u}, \dots, p_u^{e_u s_{s_u}},$$

其中

$$s_i > 0; e_1 = e_2 = \dots = e_{s_i} \quad (i = 1, 2, \dots, u),$$

则 G 有以

$$p_1^{f_1 t_1}, \dots, p_1^{f_1 t_{s_1}}, p_2^{f_2 t_2}, \dots, p_2^{f_2 t_{s_2}}, \dots, p_u^{f_u t_u}, \dots, p_u^{f_u t_{s_u}}, \\ (\text{其中 } t_i > 0; f_{i1} = f_{i2} = \dots = f_{i s_i}, i = 1, 2, \dots, u)$$

为不变量的子群的充分必要条件是

$t_i = s_i$, 并且 $f_{ij} = e_{ij} \quad (i = 1, 2, \dots, u; j = 1, 2, \dots, t_i)$.

由此可以看出, 如果 G 是一个 n 阶交换群, 那么对于 n 的任一个正因子 m , G 都有 m 阶子群, 这个结论当 G 非交换时是不成立的.

最后, 我们来证明循环群的一个重要性质, 我们知道, 如果 G 是一个 n 阶循环群, 那么对于 n 的任一个正因数 m , G 都恰有一个 m 阶子群. 特别的, 对 n 的素因数 p , G 恰有一个 p 阶子群. 这个性质也是一个交换群为循环群的充分条件. 即有下面的定理.

定理 8 设 G 是一个交换 p -群, 如果 G 只有一个 p 阶子群, 那么 G 是一个循环群.

证明 设 G 的型不变量为 $p^{e_1}, p^{e_2}, \dots, p^{e_s}$, 则 G 有一组基 a_1, a_2, \dots, a_s , 其中 a_i 的阶为 $p^{e_i} \quad (i = 1, 2, \dots, s)$.

如果 $s > 1$, 令

$$H_1 = \langle a_1^{p^{e_1-1}} \rangle, H_2 = \langle a_2^{p^{e_2-1}} \rangle,$$

则 H_1 与 H_2 是 G 的两个不同的 p 阶子群, 与假设矛盾. 因此 $s = 1$, G 是循环群. \square

这个结论可以推广到一般交换群的情形(参考习题 13).

这个结论对非交换群是不成立的. 例如, 四元数群只有一个 2 阶子群, 但是它不是交换群, 当然更不可能为循环群.

习 题

1. 设 $G = G_1 \times G_2$, $A_1 \triangleleft G_1$, $A_2 \triangleleft G_2$. 求证:

$$A_1 \times A_2 \triangleleft G.$$

2. 设 $G = G_1 \times G_2$, $H = H_1 \times H_2$ 并且

$$G = G_1 \times G_2, H_1 = H_2.$$

求证: $G = H$.

3. $G = A \times B$. 已知 $|A|$ 与 $|B|$ 互素, 求证 A 与 B 都是 G 的特征子群.

4. 证明: $(G \times H)_p = G_p \times H_p$;

$$(G \times H)^p = G^p \times H^p.$$

5. 证明: $(A \times B)^p = A^p \times B^p$.

6. G 是一个交换 p 群, i 是一个正整数. 令

$$p_i(G) = \{a \in G \mid a^{p^i} = 1\},$$

$$p^i(G) = \{a^{p^i} \mid a \in G\}.$$

证明:

(1) $p_i(G)$ 及 $p^i(G)$ 都是 G 的子群;

(2) $G/p^i(G) \cong p^i(G)$;

(3) $G/p^i(G) \cong p_i(G)$.

7. $p_i(G)$ 的定义如上题. 再设

$$|p^i(G) : p^{i-1}(G)| = p^{n_i}.$$

求证 $n_i = n_{i+1}$ ($i = 1, 2, \dots$).

8. 设 G 是由 $(1, 2, 3, 4, 5, 6), (7, 8)$ 生成的 8 次置换群.

(1) 求 G 的两组基.

(2) 将 G 表成循环 p -群的直积.

9. 已知交换 p 群 G 的型不变量为 p^3, p^2 . 问 G 有多少个 p 阶子群, 多少个 p^2 阶子群, 多少个 p^2 阶循环子群?

10. 证明: 交换 p 群可以由它的全部最高阶元素生成.

11. G 是一个 p 群, 它的型不变量是 p, p^{n-1} ; m 是一个小于 n 的正整数. 证明:

(1) G 共有 $p+1$ 个 p^m 阶子群.

(2) 当 $m=1$ 时, G 共有 $p+1$ 个 p^m 阶循环子群; 当 $m>1$ 时,

G 共有 p 个 p^m 阶循环群 .

12 . G 是一个有限交换群 . 证明 G 有一组基 a_1, a_2, \dots, a_s , 它们的阶 n_1, n_2, \dots, n_s 满足

$$n_i \mid n_{i+1}, \quad i = 1, 2, \dots, s .$$

13 . G 是一个交换群 . 如果对 $|G|$ 的每个素因数 p , G 都恰有一个 p 阶子群, 那么 G 是一个循环群 .

14 . G 是一个 p 群, 如果 G 的指数为 p 的子群只有一个, 那么 G 是一个循环群 .

15 . 把上题中的结论推广到一般有限交换群的情形并加以证明 .

16 . 证明: p^n 阶交换群的自同构群的阶可被 p^{n-1} 整除 .

17 . G 是一个 p^n 阶循环群, 求 $\text{Aut}(G)$ 的阶 .

18 . 定出 180 阶交换群的所有可能的型 .

19 . 证明: 如果交换群 G 有 m, n 阶元素, 则 G 有 $[m, n]$ 阶元素 ($[m, n]$ 表示 m 与 n 的最小公倍数) .

20 . 证明: 有限交换群 G 是循环群的充分必要条件是 G 的阶等于 G 中一切元素的阶的最小公倍数 .

第 5 章 Sylow 定理

我们知道, n 阶群的子群的阶一定是 n 的一个因数, 而且, 对于 n 阶交换群来说, 如果 m 是 n 的一个正因数, 那么 G 一定有 m 阶子群. 但是这个结论对于非交换群是不成立的. 例如 4 元交错群 A_n 的阶等于 12, 我们已知 A_n 有阶为 1, 2, 3, 4 及 12 的子群, 但是 A_n 没有 6 阶子群.

然而, 如果 n 的因数 m 是一个素数的方幂, 那么 n 阶群 G 一定有 m 阶子群. 特别地, G 一定有 Sylow p -子群.

这一章的内容主要是证明 G 的 p -子群的存在, 讨论 Sylow p -子群的个数及其共轭性, 并且讨论 G 可以表成 Sylow p -子群的直积的条件, 最后讨论了有限 p -群的构造并介绍了一些特殊 p -群.

5.1 Sylow 定理

定理 1 (第一 Sylow 定理) 设群 G 的阶为 $n = p^r m$, 其中 p 是一个素数, $r \geq 1, (p, m) = 1$. 则 G 有 p^i ($i = 1, 2, \dots, r$) 阶子群. 特别地, G 有 Sylow p -子群.

证明 对 G 的阶作归纳法. 如果 $n = p$, 结论显然成立. 设结论对于阶小于 n 的群成立.

用 Z 表示 G 的中心, 并设 Z 的阶为 z . 如果 $p \mid z$, 那么 Z 中一定有一个 p 阶元素 a . 于是 $\langle a \rangle$ 是 G 的一个 p 阶正规子群. G 关于 $\langle a \rangle$ 的商群 $G/\langle a \rangle$ 的阶为 $p^{-1}n$, 小于 n . 由归纳法假设, $G/\langle a \rangle$ 有

$p^i (i=1, 2, \dots, r-1)$ 阶子群 $P_i \not\subseteq a$. 因此, P_i 是 G 的 $p^{i+1} (i=1, 2, \dots, r-1)$ 阶子群.

如果 $p \nmid z$. 考虑 G 的共轭元素类. 设 G 的非中心元素分成 s 个类, 它们的元素数分别是 h_1, h_2, \dots, h_s , 那么

$$n = z + \sum_{i=1}^s h_i.$$

因为 $p \mid n, p \nmid z$, 所以一定有一个 $h_k (1 \leq k \leq s)$ 不能为 p 整除. 设 b 是这个共轭类中的一个元素, 用 N 表示 b 在 G 内的中心化子, 那么 N 的指数为

$$|G/N| = h_k > 1,$$

并且 $p \mid |N|$. 因为 $|N| < n$, 故由归纳法假设 N 有 $p^i (i=1, 2, \dots, r-1)$ 阶子群 P_i . P_i 也是 G 的 $p^i (i=1, 2, \dots, r-1)$ 阶子群. x

由定理 1 可以得到下述重要结论.

推论 如果素数 p 能整除有限群 G 的阶, 那么 G 中一定有 p 阶元素.

定理 2 (第二 Sylow 定理) G 的 Sylow p -子群都是共轭的. G 的 Sylow p -子群的个数可以表成 $1 + kp$, 而且是 G 的阶 n 的一个因数.

证明 设 P, P_1, P_2, \dots, P_r 是 G 的全部 Sylow p -子群. 因为 Sylow p -子群的共轭子群一定也是 Sylow p -子群, 所以对于 G 的任一个元素 a , 可以定义一个 $r+1$ 元置换 σ_a :

$$\sigma_a = \begin{pmatrix} P & P_1 & \dots & P_r \\ a^{-1}Pa & a^{-1}P_1a & \dots & a^{-1}P_r a \end{pmatrix}.$$

令

$$S_p = \{ a \mid a \in P \},$$

S_p 是 P 的一个同态象, 因此也是一个 p -群.

如果 $P_i(1 \leq i \leq r)$ 在 S_p 下不变, 那么对任一 $a \in P$, 都有 $aP_i = P_i a$, 因此 PP_i 是 G 的一个 p -子群. 由于 P, P_i 都是 Sylow p -子群, 必有 $PP_i = P = P_i$, 这是不可能的, 因此 P 是 S_p 的唯一的不动点, 其他 r 个 $P_i (i=1, 2, \dots, r)$ 分别属于 S_p 的一些传递集. 每个传递集中子群的个数都是 $|S_p|$ 的因数, 而且不等于 1, 因为 $|S_p|$ 是一个 p 幂, 所以 r 是 p 的一个倍数. G 的 Sylow p -子群的总数可以表成 $1 + kp$.

设与 P 共轭的子群共有 s 个, 可以同前面一样地证明 $s \equiv 1 \pmod{p}$. 如果 G 还有另一个共轭 Sylow p -子群类, 其中包含 s_1 个子群, 那么这 s_1 个子群可以分成 S_p 的一些传递集, 因此 $p \mid s_1$. 但是和 s 一样, $s_1 \equiv 1 \pmod{p}$. 这是一个矛盾. 所以 G 只能有一个共轭 Sylow p -子群类, 即 G 的所有的 Sylow p -子群都是共轭的.

因为所有 Sylow p -子群组成一个共轭类, 所以它们的总数 $1 + kp$ 一定是 n 的一个因数. x

推论 设 P 是 G 的一个 Sylow p -子群. 则:

- (1) P 是 G 的正规子群的充分必要条件是 P 是 G 的唯一的 Sylow p -子群;
- (2) P 是 $N_G(P)$ 的唯一的 Sylow p -子群.

定理 3 (第三 Sylow 定理) G 的任一个 p -子群 A 都包含在一个 Sylow p -子群中.

证明 仍用 σ 表示定理 2 的证明中所定义的 $r+1$ 元置换.

令

$$S_A = \{ a \mid a \in A \},$$

那么 G 的 Sylow p -子群 $P = P_0, P_1, \dots, P_r$ 分成 S_A 的一些传递集. 这些传递集中包含的 Sylow p -子群的个数或者是 1, 或者是 p 的一个不等于 1 的方幂. 但是因为 $r \equiv 1 \pmod{p}$, 所以至少有一个传递集只包含一个 Sylow p -子群, 设为 $P_l (0 \leq l < r)$. 于是对 A 中任一个元素 a , 都有

$$a^{-1} P_l a = P_l.$$

于是 AP_l 是一个 p -群, 比较 P_l 及 AP_l 的阶, 即得

$$AP_l = P_l.$$

因此

$$A = P_l \times$$

在进一步讨论 Sylow 子群的其他性质以前, 我们先来举例说明 Sylow 定理的一些应用.

例 1 如果 G 的阶为 $2n$, n 是一个奇数, 那么 G 一定有指数为 2 的正规子群.

证明 用 R_G 表示 G 的右正则表示, R_G 是 G 的一个同构象. 根据定理 1 的推论, G 中包含一个 2 阶元素 a . a 在右正则表示下的象 a 是一个 2 阶正则置换, 因此是 n 个不相交的对换的乘积, 所以 a 是一个奇置换. 于是 R_G 中全部偶置换组成 R_G 的一个指数为 2 的正规子群 R_G^+ . 因为 G 与 R_G 是同构的, 所以 G 也有指数为 2 的正规子群 χ .

这个例子说明阶为 $2n$ (n 为奇数) 的群不可能是单群.

例 2 证明 455 阶群一定是循环群.

证明 设 G 是一个 455 阶群. 因为 $455 = 5 \times 7 \times 13$, 所以由定理 1, G 有阶为 13, 7 及 5 的元素. 又由定理 2, 知 G 的 Sylow 13-子群及 Sylow 7-子群都只有一个, 设为 P_{13} 及 P_7 , 那么 $P_{13} P_7$ 是 G 的一个 91 阶正规子群. 考虑 G 的 Sylow 5-子群, 由定理 2, Sylow 5-子群的个数为 1 或 91. 如果 G 有 91 个 Sylow 5-子群, 那么 G 共有 $91 \times 4 = 364$ 个 5 阶元素. 而 $P_{13} P_7$ 中包含 91 个阶与 5 互素的元素. 这两种元素共有 455 个, 就是 G 的全部元素. 任取一个 Sylow 5-子群 P_5 , 则 $P = P_7 P_5$ 是 G 的一个 35 阶子群. 因为

$$P_5 \cap P = P, \quad P_7 \cap P = P, \quad P_5 \cap P_7 = \{e\},$$

所以

$$P = P_5 P_7.$$

因此 P 是一个 35 阶循环群. G 包含一个 35 阶元素, 这个元素不在前面所列的 455 个元素中, 这是不可能的. 所以 G 只有一个 Sylow 5-子群 P_5 . 于是

$$G = P_{13} P_7 P_5,$$

G 是一个 455 阶循环群. \square

例 3 60 阶单群都与 A_5 同构. 因此在同构的意义下, 60 阶单群只有一个.

证明 设 G 是一个 60 阶单群. 由于 G 是单群, 故 G 的非单位同态象都一定是同构象. 因此 G 对任一真子群的陪集置换表示也一定与 G 同构. 所以我们只要证明 G 有指数为 5 的子群.

因为 $60 > 4!$, 所以 G 不可能与 S_4 的子群同构, 所以 G 没有指数小于 5 的子群.

考虑 G 的 Sylow 子群. 因为对同一个素数 p , G 的 Sylow p -子群组成一个共轭子群类, 类中子群的总数等于此共轭类中任一子群的正规化子的指数. 所以对于 $|G|$ 的任一素因数 p , G 的

Sylow p -子群的个数都不能少于 5 个.

因为 $60 = 2^2 \times 3 \times 5$, 故由上述分析知 G 的 Sylow 5-子群共有 6 个. G 共有 24 个 5 阶元素.

G 的 Sylow 2-子群只能是 5 个或 15 个(已知不可能是 3 个). 如果 G 有 5 个 Sylow 2-子群, 那么 G 的 Sylow 2-子群的正规化子就是 G 的指数为 5 的子群. 如果 G 有 15 个 Sylow 2-子群. 假如 G 的任两个 Sylow 2-子群之交都是单位子群, 那么 G 将有 45 个 2-元素. 但是 G 已有 24 个 5-元素, 所以这是不可能的. 因此 G 一定有两个 Sylow 2-子群 P_1, P_2 , 它们的交是一个 2 阶子群 A . 因为 4 阶群都是交换群, 所以

$$P_1, P_2 \quad Z_G(A) < G.$$

因此 $Z_G(A)$ 的阶是 4 的倍数且大于 4. 但是 $Z_G(A)$ 的指数不能为 3, 故 $Z_G(A)$ 的指数为 5.

以上证明了 G 有指数为 5 的子群, 设为 H . G 对 H 的陪集置换表示 $S_{G/H} \cong S_5$. 因为 S_5 只有一个 60 阶子群, 即 A_5 , 所以 $G \cong S_{G/H} \cong S_5 \times H$.

定理 4 如果 $G/H \cong N_G(P)/P$, 其中 P 是 G 的一个 Sylow 子群, 那么 H 在 G 中的正规化子就等于 H , 即

$$H = N_G(H).$$

证明 设 G 中元素 a 使 $a^{-1}Ha = H$, 来证 $a \in H$.

从 $a^{-1}Ha = H$ 可推出 $a^{-1}Pa \in H$. 因为 $a^{-1}Pa$ 也是 H 的一个 Sylow 子群, 与 P 共轭, 因此存在 $b \in H$ 使 $b^{-1}(a^{-1}Pa)b = P$. 从而 $ab \in N_G(P) \cap H$. 所以 $a \in H$. \square

当 $H = N_G(P)$ 时, 可知 P 的正规化子等于它自己的正规化子.

定理 5 如果有限群 G 的 p -子群 A 不是 G 的 Sylow p -子群, 那么 A 的正规化子不等于 A 自己.

证明 如果 $p \nmid |G/N_G(A)|$, 那么由 $p \mid |G/A|$, 即得

$$N_G(A) = A.$$

如果 $p \mid |G/N_G(A)|$, 设 $|G/N_G(A)| = pl$, 并设 $A = A_1, A_2, \dots, A_{pl}$ 是与 A 共轭的全部子群. 对 $a \in A$, 作置换

$$\sigma_a = \begin{pmatrix} A_1 & A_2 & \dots & A_{pl} \\ a^{-1}A_1a & a^{-1}A_2a & \dots & a^{-1}A_{pl}a \end{pmatrix}.$$

令 $S_A = \{ \sigma_a \mid a \in A \}$, S_A 是 $\{ A_1, A_2, \dots, A_{pl} \}$ 上的一个置换群, A 是 S_A 的一个不动点. A 的 pl 个共轭子群 A_1, A_2, \dots, A_{pl} 分成 S_A 的一些传递集, 每个传递集中子群的个数等于 1 或 p 的方幂 (> 1). 因此至少有 p 个 A_i 在 S_A 下保持不变, 设 A_2 是其中的一个, 那么对任一 $a \in A$, 都有 $a^{-1}A_2a = A_2$, 于是 $A_1 \leq N_G(A_2)$. 由此得 $N_G(A_2) > A_2$. 由于 A_1 与 A_2 共轭, 故有 $N_G(A_1) > A_1$. \times

从定理 5 的证明可看出, $p \mid |N_G(A_1) - A_1|$. 因此有下述一些推论.

推论 1 如果群 G 的阶等于 p^m , 其中 $1 < m$, $(p, m) = 1$, 则 G 的每个 p^i ($1 < i < m$) 阶子群都是某个 p^{i+1} 阶子群的正规子群.

推论 2 设 P 是一个 p 阶 p -群, 则 P 的极大子群一定都是 p^{m-1} 阶群, 并且都是正规子群.

推论 3 p 群的真子群的正规化子不能等于它自己.

下面来讨论群 G 表成其 Sylow 子群的直积的条件. 如果

$$G = P_1 P_2 \dots P_s$$

是其 Sylow 子群的直积, 那么有 $P_i \triangleleft G$ ($i = 1, 2, \dots, s$). 如果 G 的每个 Sylow 子群都是正规子群. 设 P_i 是 G 的 Sylow p_i -子群 ($i = 1, 2, \dots, s$). 则因当 $i \neq j$ 时, P_i 的阶与 P_j 的阶互素, 故 P_i 中元素与 P_j 元素可交换. 又由定理 3 知 P_i 包含了 G 的全部 p_i -元素 ($i = 1, 2, \dots, s$), 因此 $G = P_1 P_2 \dots P_s$. 这样就得到下面的定理.

定理 6 有限群 G 是其 Sylow 子群的直积的充分必要条件是 G 的 Sylow 子群都是正规子群.

我们还可证明如下的定理.

定理 7 有限群 G 是其 Sylow 子群的直积的充分必要条件是 G 没有真子群等于它自己的正规化子.

证明 设 G 没有真子群等于它自己的正规化子. 然而根据定理 4, G 的 Sylow 子群 P 的正规化子 $N_G(P)$ 等于它自己的正规化子. 因此必须有 $N_G(P) = G$, 故 $P \triangleleft G$. 所以由定理 6, G 是 Sylow 子群的直积.

现在设 $G = P_1 P_2 \dots P_s$, 其中 P_i ($i = 1, 2, \dots, s$) 是 G 的 Sylow p_i -子群, 则 P_i 是 G 的唯一的 p_i -子群. G 的 p_i -元素都在 P_i 中, $i = 1, 2, \dots, s$. 设 H 是 G 的一个真子群, 任取 $g \in G$. 由 4.3 节的引理知 g 可表成

$$g = g_1 g_2 \dots g_s, \quad g_i \in P_i \quad (i = 1, 2, \dots, s),$$

而且 g_i 都是 g 的方幂, 所以 $g_i \in H$. 令

$$H_i = H \cap P_i, \quad i = 1, 2, \dots, s,$$

则有

$$H = H_1 H_2 \dots H_s.$$

因为 H 是 G 的真子群, 所以一定有一个 $H_r (1 \leq r \leq s)$ 是 P_r 的真子群. 用 N 表示 H_r 在 P_r 中的正规化子, 那么 $N > H_i$, 并且

$$H = H_1 \cdots H_{r-1} N H_{r+1} \cdots H_s.$$

这说明 H 的正规化子不能等于 H , 定理证毕. \times

最后来证明关于 Sylow 子群的一个定理, 这个定理说明 Sylow 子群在有限群研究中的重要性.

定理 8 设 N 是 G 的一个正规子群, P 是 N 的一个 Sylow p -子群, 则 $G = N_G(P)N$.

证明 任取 G 中一个元素 a . 因为 N 是 G 的正规子群, 所以 $a^{-1}Pa \in N$, $a^{-1}Pa$ 也是 N 的一个 Sylow p -子群. 故由第二 Sylow 定理, 存在 N 中一个元素 b 使得 $b^{-1}(a^{-1}Pa)b = P$. 于是 $ab \in N_G(P)$, $a \in N_G(P)N$. 因此 $G = N_G(P)N$. \times

5.2 有限 p -群

上一节我们证明了有限群的 Sylow 子群的存在性, 并且证明了对同一个素数 p , G 的 Sylow p -子群都是共轭的, 因此都是同构的. 如果 G 的阶 $n = p_1^{l_1} p_2^{l_2} \cdots p_s^{l_s}$, 其中 p_1, p_2, \dots, p_s 是不同素数: l_1, l_2, \dots, l_s 是正整数. 对每个 $i (1 \leq i \leq s)$ 取定一个 Sylow p_i -子群 P_i , 这些 $P_i (i=1, 2, \dots, s)$ 就生成群 G . 因此讨论有限 p -群的构造对研究有限群的构造很有用处. 在上一节中我们已经涉及有限 p -群的一些结论. 这一节再介绍关于有限 p -群的一些基本结论.

定理 9 有限 p -群 $G(\neq \{e\})$ 的中心大于 $\{e\}$.

证明 设 $|G| = p^m$.将 G 分解成共轭元素类之并:

$$G = C_1 \cup C_2 \cup \dots \cup C_t, \quad C_i \cap C_j = \{e\} \quad (i \neq j),$$

其中 $C_1 = \{e\}$.设 C_i 中包含 h_i 个元素 ($i = 1, 2, \dots, t$), 那么 h_i 是 p^m 的一个因数, 因此是 1 或是 p 的倍数 .但是

$$h_1 + h_2 + \dots + h_t = p^m,$$

式中 $h_1 = 1$, 所以至少还有另一个 $h_r = 1$ ($1 < r < t$) .于是共轭类 C_r 由一个元素 a 组成, a 属于 G 的中心, 所以 G 的中心大于 $\{e\}$.

定理 10 p^2 (p 是素数) 阶群一定是交换群 .

证明 设 G 是一个 p^2 阶群, 如果 G 中有一个 p^2 阶元素, 那么 G 是一个循环群 .如果 G 不是循环群, 那么 G 中非单位元素都是 p 阶元素 .由定理 8, $Z(G) \neq \{e\}$, 取 $a \in Z(G)$, $a \neq e$, 再取 $b \notin \langle a \rangle$, 那么 $G = \langle a, b \rangle$, 所以 G 是交换的 .

定理 11 如果 p -群 P 只有一个指数为 p 的子群, 那么 G 是一个循环群 .

证明 设 $|P| = p^n$, 对 n 作归纳法 .当 $n = 1$ 时, 结论显然成立 .

设定理对阶为 p^s ($s < n$) 的群都成立 .用 Z 表示 G 的中心, 如果 $|G/Z| = 1$, 则 G 是交换群, 因此, G 是循环群, 而且 $|G/Z| = p$.来证明 $|G/Z| = p^2$ 也不可能 .如果 $|G/Z| = p^2$, 则 G/Z 是 p^{n-2} 阶 p -群 .如果 H/Z 是 G/Z 的指数为 p 的子群, 那么 H 是 G 的指数为 p 的子群, 因此由假设 G/Z 只有一个指数为 p 的子群, 由归纳法假设, G/Z 为循环群, 所以 G 是一交换群 .与 $|G/Z| = p^2$ 相矛盾, 所以只能有 $|G/Z| = 1$, 定理证毕 .

5.3 一些特殊 p -群

本节介绍一些特殊 p -群的构造而不予证明.

1 阶为 p, p^2, p^3 的群

(1) p 阶群

循环群 $a, a^p = e$.

(2) p^2 阶群

(i) 循环群 $a, a^{p^2} = e$.

(ii) 初等交换群 $a, b, a^p = e, b^p = e, ba = ab$.

(3) p^3 阶群

交换群

(i) $a, a^{p^3} = e$.

(ii) $a, b, a^{p^2} = e, b^p = e, ba = ab$.

(iii) $a, b, c,$

$$a^p = b^p = c^p = e, ba = ab, ca = ac, cb = bc.$$

非交换群, $p = 2$

(iv) 二面体群 $a, b, a^4 = b^2 = e, ba = a^{-1}b$.

(v) 四元数群 $a, b, a^4 = e, b^2 = a^2, ba = a^{-1}b$.

非交换群, $p \neq 2$

(iv) $a, b, a^{p^2} = e, b^p = e, b^{-1}ab = a^{1+p}$.

(v) $a, b, c,$

$$a^p = b^p = c^p = e, ab = bac, ca = ac, cb = bc.$$

2 包含指数为 p 的循环子群的 p^n 阶群

交换群

(1) $n = 1$

循环群 a , $a^{p^n} = e$.

(2) $n = 2$

a, b , $a^{p^{n-1}} = e, b^p = e, ba = ab$.

非交换群

(3) p 为奇数, $n = 3$

a, b , $a^{p^{n-1}} = e, b^p = e, ba = a^{1+p^{n-2}} b$.

(4) $p = 2, n = 3$

广义四元数群 a, b ,

$a^{2^{n-1}} = e, b^2 = a^{2^{n-2}}, ba = a^{-1} b$.

(5) $p = 2, n = 3$

二面体群 a, b , $a^{2^{n-1}} = e, b^2 = e, ba = a^{-1} b$.

(6) $p = 2, n = 4$

a, b , $a^{2^{n-1}} = e, b^2 = e, ba = a^{1+2^{n-2}} b$.

(7) $p = 2, n = 4$

a, b , $a^{2^{n-1}} = e, b^2 = e, ba = a^{-1+2^{n-2}} b$.

3 关于 p -群的其他结果

我们知道, 只包含一个 p 阶子群的交换 p -群一定是循环群, 然而只包含一个 p 阶子群的非交换 p -群也是存在的, 例如四元数群就是一例. 我们把四元数群加以推广, 得到所谓广义四元数群 Q_{4n} , 定义如下: Q_{4n} 由元素 a, b 生成: $Q_{4n} = \langle a, b \rangle$, 而元素 a, b 满足下列关系:

$$a^{2^n} = 1, \quad b^2 = a^n, \quad b^{-1} a b = a^{-1}, \quad n \geq 2.$$

Q_{4n} 称为 $4n$ 阶广义四元数群, 当 $n = 2$ 时, 就是四元数群 Q_8 . 我

们有

定理 12 只包含一个 p 阶子群的 p -群或者是循环群,或者是广义四元数群.

我们曾证明过,只包含一个指数为 p 的子群的 p -群一定是循环群,更一般地,有下面的结论.

定理 13 设 $1 < m < n$, 则只包含一个 p^m 阶子群的 p^n 阶群一定是循环群.

习 题

1. 设 H 是 G 的一个正规子群, $|G/H|$ 与 p 互素, 证明 G 的任一 Sylow p -子群都包含在 H 中.

2. 设 K 是 G 的一个正规 p 子群, 证明 K 包含于 G 的任一 Sylow p -子群之中.

3. 证明: 阶为 $p^2 q$ (p, q 为相异素数) 的群一定不是单群.

4. H 是 G 的子群, P 是 H 的 Sylow p -子群, 证明: 存在 G 的一个 Sylow p -子群 Q 使得

$$P = Q \cap H.$$

5. 设 G 包含一个指数为 p 的循环正规子群, 证明 G 的任一子群也都有指数为 p 的循环正规子群.

6. 问: 在 168 阶群中可能有多少个 7 阶元素?

7. 证明恰有 5 个不同构的 12 阶群.

8. 证明 155 阶群一定是循环群.

9. 证明 546 阶群一定是循环群.

10. 证明: 阶为 200 的群一定不是单群.

11. 设 $|G| = p^s \cdot n$, $(p, n) = 1$. 证明: 如果 G 中恰有 p^s 个 p 元素, 则 G 不是单群.

12. N 是有限群 G 的一个正规子群, P 是 G 的 Sylow p -子群. 求证: $P \cap N$ 是 N 的 Sylow p -子群.

13. G, N, P 同上题, 试证: PN/N 是 G/N 的 Sylow p -子群.

14. 设 P 是非交换 p -群, Z 是 P 的中心, 则 $|P/Z| \geq 2$.

15. 设 A 是 p -群 P 的一个正规子群, $Z(P)$ 是 P 的中心. 证明: $A \cap Z(P) \neq \{e\}$.

16. 如果置换群 G 的阶可被素数 p 整除, 则 G 中一定有一个元素是不相交 p -轮换的乘积.

17. 设 p 是一个素数, P 是 G 上置换群 G 的一个 Sylow p -子群, $|G| = p^m \cdot n$, 证明: 如果 $p^m \mid |G|$, 则 $p^m \mid |P|$.

18. P, G 的假设同上题, 如果 p^m 是能整除 $|G|$ 的最高 p 幂, 再设 Ω 是 P 在 G 中的最短传递集, 则 $|\Omega| = p^m$.

第6章 可解群

可解群是一类较常见的群.特别在证明了奇数阶群的可解性之后,可解群的构造在群论中更占有重要的地位.可解群在其他学科,特别在方程式论中也有重要的应用.

这一章主要介绍可解群的定义和有限可解群的一些判别条件.

在介绍可解群之前,先介绍次正规群列,正规群列,合成群列等概念.这些概念都是应用一些子群来讨论大群的重要工具.

最后一节介绍亚循环群、幂零群及超可解群的定义及有关结论.

6.1 合成群列

1 次正规群列及正规群列

设 G 是一个群, H 是 G 的一个非平凡正规子群:

$$G/H \cong \{e\}.$$

我们知道商群 G/H 是 G 的一个同态象, H 是 G 到 G/H 的自然同态的核.因此, H 与 G/H 的构造可以部分地反映 G 的构造.

如果 H 还有一个非平凡正规子群 F :

$$H/F \cong \{e\},$$

那么我们又可以利用 F 与商群 H/F 来研究 H .这样继续下去,我们可以利用 G 的一系列子群及其商群来研究 G .这就是所谓次正规群列的概念.

定义 1 设 G 是一个群, $G_0, G_1, G_2, \dots, G_s$ 是 G 的一些子群, 满足

$$G = G_0 \triangleright G_1 \triangleright G_2 \triangleright \dots \triangleright G_s = \{e\}. \quad (1)$$

那么(1)称为 G 的一个次正规群列, $G_i (i=0, 1, \dots, s)$ 称为 G 的次正规子群.

如果每个 $G_i (i=1, 2, \dots, s)$ 都是 G 的正规子群, 那么(1)称为 G 的一个正规群列.

商群 $G/G_1, G_1/G_2, \dots, G_{s-1}/G_s$ 称为(1)的因子. 因子的个数 s 称为(1)的长度.

例 1 对于 G 的任一个正规子群 H ,

$$G \triangleright H \triangleright \{e\}$$

总是一个正规群列.

例 2 设 $G = Q_8$ 是四元数群:

$$Q_8 = \langle a, b \mid a^4 = e, a^2 = b^2, ab = ba^3 \rangle.$$

令

$$G_1 = \langle a \rangle, \quad G_2 = \langle a^2 \rangle,$$

则

$$G \triangleright G_1 \triangleright G_2 \triangleright \{e\}$$

是 Q_8 的一个正规群列.

例 3 $G = S_4$. 令

$$G = \{e, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\},$$

$$G_2 = \{e, (1, 2)(3, 4)\},$$

则

$$G \triangleright G_2 \triangleright \{e\}$$

是 G 的一个次正规群列但不是正规群列.

例 4 用 $G^{(1)} = G$ 表示群 G 的换位子群, $G^{(2)}$ 表示 $G^{(1)}$ 的换位子群, ..., 用 $G^{(k+1)}$ 表示 $G^{(k)}$ 的换位子群, 那么对于任意正整数 s , 可得

$$G = G^{(0)} \triangleright G^{(1)} \triangleright G^{(2)} \triangleright \dots \triangleright G^{(s)} \triangleright \{e\}$$

是 G 的一个正规群列.

请读者自己证一下 $G^{(k)} \triangleright G$ ($k = 1, 2, \dots, s$).

在应用次正规群列来讨论群的构造时, 这个群列的因子群起着重要的作用. 因此我们需要下述定义.

定义 2 设

$$G = G_0 \triangleright G_1 \triangleright G_2 \triangleright \dots \triangleright G_s = \{e\} \quad (2)$$

及

$$G = H_0 \triangleright H_1 \triangleright H_2 \triangleright \dots \triangleright H_t = \{e\} \quad (3)$$

是群 G 的两个次正规群列. 如果 $s = t$ 而且可以在 (2) 与 (3) 的因子之间建立一个一一对应, 使得对应的因子是同构的, 那么我们就说 (2) 与 (3) 是同构的.

例 5 G 是 S_6 的一个 18 阶子群:

$$\begin{aligned} G = \{ & e, (1, 2, 3, 4, 5, 6), (1, 3, 5)(2, 4, 6), (1, 4)(2, 5)(3, 6), \\ & (1, 5, 3)(2, 6, 4), (1, 6, 5, 4, 3, 2), (1, 3, 5), \\ & (1, 2, 5, 6, 3, 4), (1, 5, 3)(2, 4, 6), (1, 4, 3, 6, 5, 2), \\ & (2, 6, 4), (1, 6)(2, 3)(4, 5), (1, 5, 3), \\ & (1, 2)(3, 4)(5, 6), (2, 4, 6), (1, 4, 5, 2, 3, 6), \\ & (1, 3, 5)(2, 6, 4), (1, 6, 3, 2, 5, 4) \}. \end{aligned}$$

G 的两个次正规群列

$$\begin{aligned} G & \{e, (1, 3, 5)(2, 4, 6), (1, 5, 3)(2, 6, 4), (1, 3, 5), \\ & (1, 5, 3), (1, 5, 3)(2, 4, 6), (2, 6, 4), (2, 4, 6), \end{aligned}$$

$$(1, 3, 5)(2, 6, 4)\}$$

$$\{e, (1, 3, 5), (1, 5, 3)\} \quad \{e\}$$

及

$$G \quad \{e, (1, 5, 3)(2, 4, 6), (1, 3, 5)(2, 6, 4), (1, 4)(2, 5)(3, 6),$$

$$(1, 6)(2, 3)(4, 5), (1, 2)(3, 4)(5, 6)\}$$

$$\{e, (1, 5, 3)(2, 4, 6), (1, 3, 5)(2, 6, 4)\} \quad \{e\}$$

的长度都是 3, 它们的因子的阶分别是 2, 3, 3 及 3, 2, 3. 因为阶为素数的群都是循环群, 而且同阶的循环群一定是同构的, 所以可以排列这两个次正规群列的因子, 使得对应的因子同构. 这说明这两个次正规群列是同构的.

还可以看出这两个次正规群列中, 第一个不是正规群列, 而第二个却是正规群列.

显然, 次正规群列的同构关系是一个等价关系.

2 合成群列

为了能有效地应用次正规群列来研究一个群, 我们希望这个次正规群列的因子越简单越好. 从正规子群的角度来看, 我们希望这些因子都是单群. 那么, 如何从 G 的一个正规子群 H 来判断 G/H 是否是单群呢? 下述定理给出了一个条件.

定理 1 商群 G/H 是单群的充分必要条件是 H 是 G 的一个极大正规子群.

证明 如果 H 不是 G 的极大正规子群, 那么 G 有一个正规子群 F 使得

$$G \supset F \supset H.$$

于是 F/H 是 G/H 的一个非平凡正规子群, 所以 G/H 不是单群.

反之,如果 G/H 不是单群. 设 F/H 是 G/H 的一个非平凡正规子群, 那么必有

$$G = F \cdot H,$$

所以 H 不是 G 的极大正规子群. \times

于是我们可以引入下面的定义.

定义 3 如果在 G 的无重复次正规群列

$$G = G_0 \supset G_1 \supset \dots \supset G_s = \{e\} \quad (4)$$

中, 每个 $G_i (i=1, 2, \dots, s)$ 都是 G_{i-1} 的极大正规子群, 那么 (4) 就称为 G 的一个合成群列. 合成群列的因子称为 G 的合成因子.

在前面的一些例子中, 例 2 中的正规群列是合成群列; 例 3 中的正规群列则不是合成群列; 例 5 中的两个次正规群列都是合成群列; 而例 1 和例 4 则不一定.

当然, 从定理 1 可以看出, 一个无重复的次正规群列是合成群列的充要条件是每个因子都是单群.

有限群总是有合成群列的. 而且, 每个正规子群都可以作为某个合成群列中的一项; 每个无重复的次正规群列都可以作为某个合成群列的一部分. 这个事实可以这样来说明: 设

$$G = G_0 \supset G_1 \supset G_2 \supset \dots \supset G_s = \{e\} \quad (5)$$

是有限群 G 的一个无重复的次正规群列. 如果每个 $G_i (i=1, 2, \dots, s)$ 都是 G_{i-1} 的极大正规子群, 那么 (5) 就是 G 的一个合成群列; 如果 $G_i (1 \leq i \leq s)$ 不是 G_{i-1} 的极大正规子群, 那么可以找到 G_{i-1} 的一个正规子群 H 使得

$$G_{i-1} = H \cdot G_i,$$

于是可以将 H 添入 (5) 中 G_{i-1} 与 G_i 之间而得到一个新的无重复的次正规群列

$$G = G_0 \triangleright G_1 \triangleright \dots \triangleright G_{t-1} \triangleright H \triangleright G_t \triangleright \dots \triangleright G_s = \{e\}. \quad (6)$$

如果这还不是一个合成群列,那么还可以用同样的方法在这个次正规群列中添加一项,这样继续下去,由于 G 的有限性,最后总可得到一个合成群列.

次正规群列(6)称为(5)的一个加密.一般地,有下面的定义.

定义 4 设

$$G = G_0 \triangleright G_1 \triangleright G_2 \triangleright \dots \triangleright G_s = \{e\} \quad (7)$$

及

$$G = H_0 \triangleright H_1 \triangleright H_2 \triangleright \dots \triangleright H_t = \{e\} \quad (8)$$

是群 G 的两个次正规群列.如果(7)的各项都包含在(8)中,就称(8)是(7)的一个加密.

显然,此时必有 $t \leq s$,上面所说的事实用这个定义来说就是下面的结论.

定理 2 有限群的任一个无重复的次正规群列都可以加密成一个合成群列.

例如,例 3 中的次正规群列可以加密成一个合成群列

$$S_4 \triangleright A_4 \triangleright G \triangleright G \triangleright \{e\}.$$

值得注意的是,一个有限群可以有不止一个合成群列.例如,例 5 就给出同一个群的两个不同的合成群列,而且我们已经证明过这两个合成群列是同构的.读者可能在其他例子中遇到过同一个群的不同合成群列,它们也都是同构的.于是不禁要问:这不是一个一般的规律呢?下述定理给出了肯定的答案.这个定理是可以利用某个群的任一个合成群列来研究这个群的重要根据.

定理 3(Jordan-Hölder) 有限群 G 的任两个合成群列都是同构的.

证明 我们对 G 的阶作归纳法来证明定理.

设

$$G = G_0 \supset G_1 \supset G_2 \supset \dots \supset G_s = \{e\} \quad (9)$$

及

$$G = H_0 \supset H_1 \supset H_2 \supset \dots \supset H_t = \{e\} \quad (10)$$

是 G 的两个合成群列.

如果 $G_i = H_i$, 则

$$G \supset G_2 \supset \dots \supset G_s = \{e\} \quad (9')$$

与

$$H_1 \supset H_2 \supset \dots \supset H_t = \{e\} \quad (10')$$

是 G_i 的两个合成群列. 因为 G_i 的阶小于 G 的阶, 故由归纳法假设知(9')与(10')是同构的, 从而(9)与(10)也是同构的.

如果 $G_i \neq H_i$, 则因 G_i 是 G 的一个极大子群, 故 $G = G_i H_i$. 任取 $G_i \supset H_i = F_1$ 的一个合成群列:

$$G_i \supset H_i = F_1 \supset F_2 \supset \dots \supset F_r = \{e\}.$$

作 G 的次正规群列

$$G \supset G_i \supset G \supset H_i \supset F_2 \supset \dots \supset F_r = \{e\} \quad (11)$$

及

$$G \supset H_i \supset G \supset H_i \supset F_2 \supset \dots \supset F_r = \{e\}. \quad (12)$$

则因

$$G/G_i \cong H_i/H_i, \quad G/H_i \cong G/G \cong H_i$$

都是单群, 所以(11)与(12)都是 G 的合成群列, 而且是同构的.

又因 G_i, H_i 的阶都比 G 的阶小, 所以由归纳法假设知(9')(10')分别与

$$G \supset G \supset H_i \supset F_2 \supset \dots \supset F_r = \{e\}$$

及

$$H_1 \quad G \quad H_1 \quad F_2 \quad \dots \quad F_r = \{e\}$$

同构. 因此(9)与(11), (10)与(12)分别同构. 由同构关系的传递性知(9)与(10)同构. 定理证毕. \times

这个定理说明: 一个有限群的合成因子除次序外是唯一确定的(在同构的意义下), 因此我们可以任取一个合成群列来进行讨论.

最后, 我们给出定理 3 的一个推论.

定理 4 有限群的任两个次正规群列都有同构的加密.

证明 如果这两个次正规群列都是无重复的, 那么只要将它们加密到合成群列就可以应用定理 3 而得到结论. 在有重复的情形, 可以先将重复的项去掉而得到同构的加密, 然后再在两个加密群列中同时添上重复的项. \times

当然, 在具体应用时, 有时不必加密到合成群列, 可以针对具体的次正规群列来考虑.

6.2 可 解 群

我们在前面曾介绍过, G 的换位子群 G' 是 G 的一个正规子群, 其商群 G/G' 是一个交换群, 用 G'' 表 G' 的换位子群, \dots , 用 $G^{(k+1)}$ 表 $G^{(k)}$ 的换位子群, 这样可以得到一系列子群

$$G \triangleright G' \triangleright G'' \triangleright \dots \triangleright G^{(k)} \triangleright G^{(k+1)} \triangleright \dots$$

对于有限群来说, 总有某个正整数 s 使得

$$G^{(s)} = G^{(s+1)} = \dots$$

关于 $G^{(s)}$ 有两种可能: 或者 $G^{(s)} = \{e\}$, 或者 $G^{(s)} = S_n$. 满足 $G^{(s)} = \{e\}$ 的群称为可解群.

定义 5 如果有正整数 s 使得 $G^{(s)} = \{e\}$, 那么 G 称为可解群.

例 1 交换群都是可解群.

例 2 四元数群 Q_8 是可解群.

例 3 S_n 及 $A_n (n > 4)$ 都不是可解群.

证明 已知当 $n > 4$ 时, S_n 只有一个非平凡正规子群, 即 A_n , 而 A_n 是一个单群.

因为 S_n 的换位元素都是偶置换, 所以 $A_n \trianglelefteq S_n$, 但是 S_n 不是交换群, 因此 $A_n \neq \{e\}$. 这两点说明 A_n 是 S_n 的非平凡正规子群, 所以 $S_n = A_n$.

$A_n (n > 4)$ 不是交换群, 所以 $A_n \neq \{e\}$. 由 A_n 的单性, 知 $A_n = A_n \times \{e\}$.

请读者自己验证一下 S_3 及 S_4 都是可解群.

因为, 对群 G 的子群 H , 总有 $G^{(i)} = H^{(i)}$, 所以可解群的子群也是可解的, 不但如此, 可解群的商群也是可解的.

定理 5 可解群的子群和商群都是可解的.

证明 只要对商群来证明. 如果 H 是 G 的一个正规子群, 那么商群 $Q = G/H$ 是 G 的一个同态象. 因此, $Q^{(i)}$ 是 $G^{(i)}$ 的同态象, 于是从 $G^{(s)} = \{e\}$ 可推出 $Q^{(s)} = \{e\}$.

定理 6 可解单群一定是素数阶循环群 .

证明 由 G 的可解性知 $G \cong G$, 再由 G 的单性得 $G = \{e\}$, 所以 G 是一个交换群 . 我们已知交换的单群一定是素数阶循环群 .

下面给出可解群的几个充分必要条件 .

定理 7 对于有限群 G , 下面几个条件都是等价的 .

- (1) G 是一个可解群 .
- (2) G 有一个正规群列, 其因子都是交换的 .
- (3) G 有一个次正规群列, 其因子都是交换的 .
- (4) G 的合成因子都是素数阶循环群 .

证明 (1) \rightarrow (2) . 当 G 可解时, G 的换位子群列就是一个正规群列, 其因子都是交换的 .

(2) \rightarrow (3) . 因为凡是正规群列一定是次正规群列, 所以从 (2) 可推出 (3) .

(3) \rightarrow (4) . 设

$$G = G_0 \triangleright G_1 \triangleright G_2 \triangleright \dots \triangleright G_s = \{e\}$$

是 G 的一个次正规群列, 因子 $G_{i-1}/G_i (i=1, 2, \dots, s)$ 都是交换的, 来证明 G 的合成因子都是素数阶循环群 . 为了方便起见, 可设这个群列是无重复的 .

对 G 的阶作归纳法 .

取 G 的包含 G_1 的一个极大正规子群 H_1 , 则 G/H_1 是一个单群, 而且是交换的, 所以 G/H_1 一定是一个素数阶循环群 .

$$H_1 \triangleright G_1 \triangleright G_2 \triangleright \dots \triangleright G_s = \{e\}$$

是 H_1 的一个次正规群列, 其因子都是交换的, 因为 H_1 的阶比 G 的阶小, 故由归纳法假设, H_1 的合成因子都是素数阶循环群 . 设

$$H_1 \quad H_2 \quad \dots \quad H_t = \{e\}$$

是 H_1 的一个合成群列, 那么

$$G \quad H_1 \quad H_2 \quad \dots \quad H_t = \{e\}$$

是 G 的一个合成群列, 所以 G 的合成因子也都是素数阶循环群.

(4) (1) 设

$$G = G_0 \quad G_1 \quad G_2 \quad \dots \quad G_s = \{e\}$$

是 G 的一个合成群列, 其因子都是素数阶循环群, 因为 G_{i+1}/G_i 是交换的, 故必有

$$G \quad G, G_2 \quad G_1 \quad G, \dots, G_i \quad G^{(i)}, \dots, G_s \quad G^{(s)}.$$

现在 $G_s = \{e\}$, 所以 $G^{(s)} = \{e\}$, G 是可解的. \times

推论 如果群 G 有一个可解正规子群 H , 使得商群 G/H 是可解的, 那么 G 也是可解的.

证明 如果

$$H \quad H_1 \quad \dots \quad H_{s-1} \quad \{e\}$$

及

$$G/H \quad G_1/H \quad \dots \quad G_{t-1}/H \quad H/H$$

分别是 H 及 G/H 的次正规群列, 它们的因子群都是交换的, 那么

$$G \quad G_1 \quad \dots \quad G_{t-1} \quad H \quad H_1 \quad \dots \quad H_{s-1} \quad \{e\}$$

就是 G 的一个次正规群列, 其因子也都是交换的. \times

根据第 5 章定理 5 推论 2, 我们有下述结论.

定理 8 有限 p 群是可解群.

证明 设 G 是一个 p^m 阶群, 则 G 有一个次正规群列

$$G_0 = G \quad G_1 \quad G_2 \quad \dots \quad G_m = \{e\},$$

其中 $G_i (i=1, 2, \dots, m)$ 是 p^{m-i} 阶群. 于是 $G_{i-1}/G_i (i=1, 2, \dots, m)$ 是 p 阶循环群, 所以 G 是可解的. \times

下面的两个定理说明可解群是一类很广的有限群.

定理 9 (Burnside) 阶为 $p^a q^b$ (p, q 为素数, a, b 为自然数) 的群一定是可解的.

定理 10 (Feit-Thompson) 奇数阶群是可解群.

定理 9 通常称为 $p^a q^b$ 定理, 是 Burnside 首先应用群指标的理论证明的. 近年来, 虽然有一些纯群论的证明, 但是都非常复杂. 我们将在第 7 章介绍群指标以后予以证明. 至于定理 10, Feit-Thompson 两人原来的证明长达二百多页, 虽经多次改进, 其证明仍可成为一本专著, 远远超出了本书的范围, 我们只是利用它来证明下述定理.

定理 11 设群 G 的阶 $|G| = 2n$, n 是一个奇数, 则 G 是可解群.

证明 已知 G 有一个指数为 2 的正规子群 H , 于是 H 的阶为 n , 由定理 10, H 是一个可解群. G 对 H 的商群 G/H 是一个 2 阶群, 也是可解的. 根据定理 7 的推论, G 是可解的. \times

应用定理 9 可以证明可解群的一个充分条件.

定理 12 如果有限群 G 的所有极大子群的指数都是素数或素数的平方, 那么 G 是可解的.

证明 对 G 的阶进行归纳法, 设结论对阶比 $|G|$ 小的群都成立.

设 p 是整除 $|G|$ 的最大素数, P 是 G 的一个 Sylow p -子群. 用 N 表示 P 在 G 内的正规化子. 如果 $N=G$, 那么 P 是 G 的正规子群, 商群 G/P 的极大子群的指数也是素数或素数的平方. 因为 G/P 的阶比 G 的阶小, 故由归纳法假设, G/P 是可解的, P 是一个 p -群, 故由定理 8, P 是可解的, 再应用定理 7 的推论, 即可得 G 的可解性.

如果 $N \neq G$, 设 H 是 G 的包含 N 的一个极大子群, P 在 H 内的正规化子也就是 N , 故由第二 Sylow 定理, 得

$$|G/N| = 1 + k_1 p, \quad |H/N| = 1 + k_2 p,$$

因此

$$|G/H| = 1 + kp.$$

由假设, H 在 G 内的指数等于某个素数 q 或 q^2 . 由 p 是 $|G|$ 的最大素因数, 推出 $|G/H| = q^2$, 于是

$$kp = q^2 - 1 = (q - 1)(q + 1).$$

由于 $p > q$, 故必有 $p = q + 1$. 因此必须有 $p = 3, q = 2$. 于是 $|G| = 2^a 3^b$, 由定理 9, 知 G 是可解群. \square

最后我们介绍关于可解群的推广的 Sylow 定理. 我们以前证明了 Sylow 定理: 如果 G 的阶等于 p^n , p 是素数, $(p, n) = 1$, 那么 G 一定有 p 阶子群, 称为 Sylow p -子群; G 的 Sylow p -子群都是共轭的; G 的 Sylow p -子群的个数 h 是 $|G|$ 的一个因数而且模 p 同余于 1. 对于可解群, 这个结论可以推广, 我们将关于可解群的推广的 Sylow 定理叙述如下而不作证明.

定理 13 设 G 是一个可解群, G 的阶为 mn , $(m, n) = 1$, 则:

(1) G 有 m 阶子群;

(2) G 的 m 阶子群都是共轭的;

(3) G 的任一个阶为 m 的因数的群一定包含在 G 的某个 m 阶子群之中;

(4) G 的 m 阶子群的个数 h_m 可以表成一些因数之积, 而使每个因子满足:

- (a) 模 m 的某个素因子同余于 1,
- (b) 是一个素数的方幂.

定理 13 中的第(1)点事实上也是可解群的一个特征性质, 为了叙述这一结论, 要用到一个定义: 如果 G 的阶为 p^n , $(n, p) = 1$, 那么 G 的 n 阶子群称为 G 的一个 p -补群.

定理 14 如果对 $|G|$ 的每个素因子 p , G 都有 p -补群, 那么 G 是一个可解群.

6.3 亚循环群、幂零群和超可解群

这一节介绍亚循环群、幂零群及超可解群的定义及它们的一些重要性质.

定义 6 如果群 G 的导群 G' 和商群 G/G' 都是循环群, 则称 G 为亚循环群.

如果 G 是亚循环群, 那么 $G' = \{e\}$, 所以 G 是可解的.

定理 15 如果有限群 G 的 Sylow 子群都是循环群, 那么 G 一定是亚循环群, 并且 G 可以由两个元素 a, b 生成, a, b 满足下述关系:

$$a^m = e, \quad b^n = e, \quad b^{-1}ab = a^r,$$

$$mn = |G|, \quad ((r-1)n, m) = 1, \quad r^n \equiv 1 \pmod{m}.$$

反之, 如果群 G 由满足上述关系的元素 a, b 生成, 那么 G 的 Sylow 子群一定都是循环群, 因之 G 是亚循环群.

因为亚循环群一定是可解的, 所以定理 15 给出可解群的一个充分条件.

推论 如果群 G 的 Sylow 子群都是循环群, 那么 G 是可解的. 特别地, 如果群 G 的阶是一些相异素数的乘积, 那么 G 是可解的, 并且还是循环的.

定义 7 设 G 是一个群.

$$G = G_0 \triangleright G_1 \triangleright G_2 \triangleright \dots \triangleright G_s = \{e\}$$

是 G 的一个正规群列. 如果 G_{i-1}/G_i 包含在 G/G_i 的中心内 ($i=1, 2, \dots, s$), 则称这个群列为 G 的一个中心群列. 具有中心群列的 (有限) 群称为幂零群.

因为上述定义中 G_{i-1}/G_i ($i=1, 2, \dots, s$) 都是交换的, 所以幂零群一定是可解群.

定义 8 设 G 是一个群, 规定子群 $G_k(G)$ 如下: $G_1(G) = G$; 当 $k > 1$ 时, $G_k(G) = [G, G, \dots, G]$, 即 $G_k(G)$ 是由 $[g_1, g_2, \dots, g_k] =$

$$\underbrace{[[[g_1, g_2], g_3], \dots, g_k]}_{k \uparrow} (g_1, g_2, \dots, g_k \text{ 是 } G \text{ 中任意元素}) \text{ 生成的子群, 则 } G_k(G) \text{ 是 } G \text{ 的全不变子群, 且有}$$

$$G_{k+1}(G) \triangleleft G_k(G).$$

群列

$$G = G_1(G) \supseteq G_2(G) \supseteq \dots \supseteq G_k(G) \supseteq \dots$$

称为 G 的下中心群列 .

定义 9 设 G 是一个群,

$$Z_0 = \{e\} \subset Z_1(G) \subset Z_2(G) \subset \dots \subset Z_k(G) \subset \dots$$

是 G 的一个子群列 . 如果 $Z_{k+1}(G)/Z_k(G)$ 是 G/Z_k 的中心, 则称此群列为 G 的上中心群列 .

如果

$$G = G_0 \triangleright G_1 \triangleright G_2 \triangleright \dots \triangleright G_s = \{e\}$$

是 G 的一个中心群列, 那么

$$\begin{aligned} G_i &= G_i(G), & i &= 1, 2, \dots, s, \\ G_{s-j} &= Z_j(G), & j &= 0, 1, \dots, s-1. \end{aligned}$$

因此有下面的结论 .

定理 16 如果 G 是一个幂零群, 那么 G 的下中心群列终止于 $\{e\}$, 上中心群列终止于 G . 它们都是中心群列, 而且有相同的长度 $c = c(G)$. G 没有长度小于 c 的中心群列 .

定理 16 中的 c 称为幂零群 G 的幂零类 .

下面我们介绍幂零群的性质而不予证明 .

定理 17 幂零群的子群及商群都是幂零群 .

定理 18 (1) 幂零群的每个真子群的正规化子都不能等于这个子群 .

(2) 幂零群 G 的每个极大子群都是正规的, 其指数为奇数, 而且包含 G 的导群 .

(3) 若 H 是幂零群 G 的子群且 $G = G H$, 那么 $H = G$.

定理 19 有限 p -群是幂零群. 有限群 G 是幂零群当且仅当 G 可表成它的 Sylow 子群的直积.

推论 有限群是幂零的当且仅当它的极大子群都是正规的.

我们介绍群的一类幂零子群.

定义 10 群 G 的所有极大子群之交称为 G 的 **Frattini** 子群, 记作 $\Phi(G)$.

从定义 10 可以看出 $\Phi(G)$ 是 G 的一个正规子群.

定理 20 (1) 有限群的 Frattini 子群是幂零的.

(2) 有限群 G 是幂零群的充分必要条件是 $\Phi(G) = G$.

最后我们介绍超可解群的概念及有关结论.

定义 11 如果群 G 有一个次正规群列

$$G = G_0 \triangleright G_1 \triangleright G_2 \triangleright \dots \triangleright G_s = \{e\},$$

其中每个商群 G_{i-1}/G_i ($i = 1, 2, \dots, s$) 都是循环群, 则 G 叫做超可解的.

由定义可看出超可解群一定是可解的. 超可解群有下述一些性质.

定理 21 超可解群的子群和商群都是超可解群. 超可解群的

导群是幂零 .

定理 22 有限群 G 是超可解群的充分必要条件是 G 的极大子群的指数都是素数 .

习 题

1. 找出 20 阶循环群的所有可能的合成群列 .
2. 证明 S_3, S_4 都是可解群 .
3. 设 H 是 G 的一个同态象, N 是 G 到 H 的某个同态映射的核, 证明:

(1) 如果 G 是可解群, 则 H 也是可解的 .

(2) 如果 H 是可解群, 则当且仅当 N 可解时 G 是可解的 .

4. 证明可解群的直积也是可解群 .

5. 证明 pq (p, q 是素数) 阶群是可解群 .

6. 证明 p^2q (p, q 是不同素数) 阶群是可解群 .

7. 证明: 如果 G 的 Sylow 2-子群是循环群, 那么 G 是可解群 .

8. 证明: $A \triangleleft G, B \triangleleft G \Rightarrow A, B \triangleleft G$ ($A \triangleleft G$ 表示 A 是 G 的次正规子群) .

9. 证明: 有限群 G 是幂零群的充分必要条件是 G 的子群都是次正规的 .

10. 设 a, b 是有限幂零群 G 中的两个元素 . 证明: 如果 a, b 的阶互素, 那么 $ab = ba$.

11. 设 M, N 都是群 G 的正规子群 . 证明: 如果 $G/M, G/N$ 都是幂零的, 那么 G 也是幂零的 .

12. 设 G 是有限交换群, $|G| = p_1^{n_1} p_2^{n_2} \dots p_r^{n_r}$, 其中 p_1, \dots, p_r 是

不素数,那么 G 的合成群列的长等于 $\sum_{i=1}^r n_i$.

13 . 设 $Z(G)$ 是 G 的中心, $A \leq Z(G)$. 试证: 如果 G/A 是幂零群, 则 G 也是幂零群 .

14 . 证明: 非交换可解群 G 的换位子群 G' 不可能是 G 的直积因子 .

15 . 证明: 非交换幂零群 G 的中心不能作为 G 的直积因子 .

16 . 证明: 非交换群 G 为 2 类幂零群的充要条件是

$$G = Z(G) (Z(G) \text{ 是 } G \text{ 的中心}) .$$

17 . 设 $G = G_0 \triangleright G_1 \triangleright G_2 \triangleright \dots \triangleright G_l = 1$ 是 G 的一个中心群列, H 是 G 的一个子群 . 试证: 如果 $H \leq G_i (1 \leq i < l)$, 则 H 的正规化子 $N_G(H) \leq G_{i-1}$.

18 . 设 $N \triangleleft G, H \leq G$, 且 $N \leq (H)$, 则 $N \leq (G)$.

19 . 证明从 $N \triangleleft G$ 可推出 $(H) \leq (G)$.

20 . 设 G/N 是超可解群, N 是循环群, 证明 G 是超可解群 .

第 7 章 有限群表示论初步

群表示论是群论的一个重要分支,也是研究群论的一个有力工具,并有极其广泛的应用,它在理论和应用方面都有非常丰富的内容.我们在这一章只是简单地介绍有限群的线性表示的一些基本概念、性质及结论,并且作为应用证明了 Burnside 定理及 $p^a q^b$ 定理.

7.1 线性群

这一节介绍线性群,这是研究群的线性表示的基础.

设 F 是一个域, V 是 F 上一个有限维线性空间.用 $GL(V)$ 表示 V 的全部可逆线性变换构成的群,称为 V 上一般线性群.所谓 V 上(或 F)上一个线性群就是 $GL(V)$ 的一个子群. V 上线性群的级数就是 V 的维数.

设 V 是 F 上一个 n 维线性空间.如果在 V 中取定了一组基,那么 V 的每个可逆线性变换都可以表成一个 F 上的 n 阶可逆矩阵.而任一个 F 上的 n 阶可逆矩阵可以看成 V 的某个可逆线性变换在这组基下的矩阵,并且不同的线性变换所对应的矩阵是不同的.因此 V 上一般线性群与全部 n 阶可逆矩阵构成的全线性群 $GL_n(F)$ 是同构的,而任一个 n 级线性群都可表成一个 n 阶可逆矩阵群.线性群和矩阵群除了形式不同外,本质上是一致的,因此,我们以后谈到线性群时,就不再特别区分是线性变换群,还是矩阵群,而根据所讨论的问题的需要,采取便于讨论的形式.

定义 1 线性空间 V 上的一个线性群 G 称为可约的, 如果 G 有一个非平凡的不变子空间; 否则为不可约的. G 称为可分解的, 如果 V 可表成两个 G 的非零不变子空间的直和; 否则称 G 为不可分解的. 如果 V 可以分解成一些 G 的不可约不变子空间的直和, 则 G 称为完全可约的.

定义 2 V 上两个线性群 G 与 H 称为等价的, 如果它们在 $GL(V)$ 中共轭.

如果线性空间 V 上两个线性变换 \mathbf{G} 与 \mathbf{H} 是等价的, 那么就有 V 的线性变换 \mathbf{X} 使得 $\mathbf{X}^{-1}\mathbf{G}\mathbf{X} = \mathbf{H}$. 于是 V 的子空间 W 是 \mathbf{G} 的不变子空间的充分必要条件是: $W\mathbf{X}$ 是 \mathbf{H} 的不变子空间. 因此, 等价的线性群同时是可约的、不可约的、可分解的、不可分解的或完全可约的.

对矩阵群来说, 一个线性群 G 是可约的, 就是可以找到一个可逆矩阵 \mathbf{C} , 使得对 G 中每个矩阵 \mathbf{A} , 都有

$$\mathbf{C}^{-1}\mathbf{A}\mathbf{C} = \begin{pmatrix} \mathbf{A}_1 & \mathbf{0} \\ \mathbf{0} & \mathbf{A}_2 \end{pmatrix},$$

其中 $\mathbf{A}_1, \mathbf{A}_2$ 分别是 n_1, n_2 阶可逆矩阵; \mathbf{A}_2 是一个 $n_2 \times n_2$ 矩阵; $\mathbf{0}$ 是 $n_1 \times n_2$ 零矩阵. 如果对每个 $\mathbf{A} \in G, \mathbf{A}_2$ 都是零矩阵, 则 G 是可分解的.

例 1 V 是二维复空间

$$G = \left\{ \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix}, n = 0, \pm 1, \pm 2, \dots \right\}.$$

G 是一个可约线性群, 但不是可分解的.

例 2 实线性群

$$G = \left\{ \begin{array}{cc|cc|cc|cc} 1 & 0 & & 0 & 1 & & -1 & 0 & 0 & -1 \\ 0 & 1 & & -1 & 0 & & 0 & -1 & 1 & 0 \end{array} \right\}$$

是不可约的.

例 3 实线性群

$$G = \begin{array}{ccc|c} 1 & 0 & 0 & \\ n & 1 & 0 & n = 0, \pm 1, \pm 2, \dots \\ 0 & 0 & 1 & \end{array}$$

是完全可约的.

需要注意的是, 一个线性群 G 是否可约与基域 F 有关. 例如, 例 2 中的 G 作为实线性群是不可约的, 然而作为复线性群, 则与

$$H = \left\{ \begin{array}{cc|cc|cc|cc} 1 & 0 & i & 0 & -1 & 0 & -i & 0 \\ 0 & 1 & 0 & -i & 0 & -1 & 0 & i \end{array} \right\}$$

等价, 因而是可约的, 而且是可分解的、完全可约的.

如果 G 是 V 上一个可约线性群, W 是它的一个不变真子空间. 对于 G 中任一线性变换 \mathbf{G} , 用 $\mathbf{G}|_W$ 表示 \mathbf{G} 在 W 上诱导出来的线性变换, 那么 $\mathbf{G}|_W$ 一定也是可逆的: $(\mathbf{G}|_W)^{-1} = \mathbf{G}^{-1}|_W$. 令

$$G|_W = \{\mathbf{G}|_W : \mathbf{G} \in G\},$$

则 $G|_W$ 是 W 上一个线性群, 称为 G 在 W 上诱导出来的线性群或称 G 的一个成分. 有时候, 在不致引起误解时, 为了方便起见, 仍用 G 来表示 $G|_W$.

定理 1 (Maschke 定理) 设 G 是 F 上一个有限线性群, 而且 F 的特征除不尽 G 的阶, 那么, 如果 G 是可约的, 则一定是可分解的.

证明 设 G 是一个 n 级线性群. 因为 G 是可约的, 因此可以假设 G 中矩阵都可表成

$$\mathbf{G} = \begin{pmatrix} \mathbf{G}_1 & \mathbf{0} \\ \mathbf{G}_1 & \mathbf{G}_2 \end{pmatrix},$$

其中 \mathbf{G}_1 是 r ($0 < r < n$) 阶可逆矩阵; \mathbf{G}_2 是 $n - r$ 阶可逆矩阵; \mathbf{G}_1 是一个 $(n - r) \times r$ 矩阵.

为了证明定理, 需要找出一个 n 阶可逆矩阵 \mathbf{S} 使得对 G 中任一元素 \mathbf{G} 都有

$$\mathbf{S}^{-1} \mathbf{G} \mathbf{S} = \begin{pmatrix} \mathbf{G}_1 & \mathbf{0} \\ \mathbf{0} & \mathbf{G}_2 \end{pmatrix},$$

即

$$\begin{pmatrix} \mathbf{G}_1 & \mathbf{0} \\ \mathbf{G}_1 & \mathbf{G}_2 \end{pmatrix} \mathbf{S} = \mathbf{S} \begin{pmatrix} \mathbf{G}_1 & \mathbf{0} \\ \mathbf{0} & \mathbf{G}_2 \end{pmatrix}. \quad (1)$$

令

$$\mathbf{S} = \begin{pmatrix} \mathbf{I} \\ \mathbf{U} \quad \mathbf{I}_{n-r} \end{pmatrix},$$

其中 \mathbf{I} , \mathbf{I}_{n-r} 分别是 r , $n - r$ 阶单位矩阵. 则 (1) 式要求对 \mathbf{G} 有

$$\mathbf{U} \mathbf{G}_1 = \mathbf{G}_1 + \mathbf{G}_2 \mathbf{U}.$$

任取 $\mathbf{H} \in G$, 记

$$\begin{aligned} \mathbf{H} \mathbf{G} &= \begin{pmatrix} (\mathbf{H} \mathbf{G})_{11} & \mathbf{0} \\ (\mathbf{H} \mathbf{G})_{21} & (\mathbf{H} \mathbf{G})_{22} \end{pmatrix} \\ &= \begin{pmatrix} \mathbf{H}_1 & \mathbf{0} & \mathbf{G}_1 & \mathbf{0} \\ \mathbf{H}_1 & \mathbf{H}_2 & \mathbf{G}_1 & \mathbf{G}_2 \end{pmatrix}, \end{aligned}$$

则有

$$\begin{aligned} (\mathbf{H} \mathbf{G})_{11} &= \mathbf{H}_1 \mathbf{G}_1, \\ (\mathbf{H} \mathbf{G})_{22} &= \mathbf{H}_2 \mathbf{G}_2, \\ (\mathbf{H} \mathbf{G})_{21} &= \mathbf{H}_1 \mathbf{G}_1 + \mathbf{H}_2 \mathbf{G}_1. \end{aligned}$$

于是有

$$\begin{aligned} \mathbf{G}_1 &= \mathbf{H}_2^{-1} [(\mathbf{HG})_{21} - \mathbf{H}_1 \mathbf{G}_1] \\ &= \mathbf{G}_2 (\mathbf{G}^{-1} \mathbf{H}^{-1})_{22} (\mathbf{HG})_{21} - \mathbf{H}_2^{-1} \mathbf{H}_1 \mathbf{G}_1. \end{aligned}$$

因为上式对 G 中任意元素 \mathbf{H} 都成立, 故得

$$\mathbf{G}_1 = \frac{1}{|G|_{\mathbf{H} \in G}} \{ \mathbf{G}_2 (\mathbf{G}^{-1} \mathbf{H}^{-1})_{22} (\mathbf{HG})_{21} - \mathbf{H}_2^{-1} \mathbf{H}_1 \mathbf{G}_1 \}.$$

令

$$\begin{aligned} \mathbf{U} &= - \frac{1}{|G|_{\mathbf{H} \in G}} \mathbf{H}_2^{-1} \mathbf{H}_1 \\ &= - \frac{1}{|G|_{\mathbf{H} \in G}} (\mathbf{G}^{-1} \mathbf{H}^{-1})_{22} (\mathbf{HG})_{21}, \end{aligned}$$

则有

$$\mathbf{G}_1 = - \mathbf{G}_2 \mathbf{U} + \mathbf{U} \mathbf{G}_1,$$

即

$$\mathbf{U} \mathbf{G}_1 = \mathbf{G}_1 + \mathbf{G}_2 \mathbf{U}.$$

(1)式成立. 定理得证. \times

定理中的 G 的有限性是不能省略的, 这一点可以从例 1 看出. 下面的例子说明定理中关于域 F 的特征的条件也是不可省略的.

例 4 设 $F = F_2$ 是 2 元素域, F 上 2 级线性群

$$G = \left\{ \begin{array}{cc|cc} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{array} \right\}$$

是可约而不可分解的.

反复应用定理 1, 可以得到下述完全分解定理.

定理 2 如果 G 是 F 上一个有限线性群, F 的特征不能整除 G 的阶, 则 G 是完全可约的.

下面来证明一个非常有用的结论.

定理 3 (Schur 引理) 如果 G 与 H 是 F 上两个不可约线性群, 它们的级数分别是 m 与 n , \mathbf{A} 是 F 上一个 $m \times n$ 矩阵, 使得 $G\mathbf{A} = \mathbf{A}H$, 那么, 下列两种情况之一成立:

- (1) $\mathbf{A} = \mathbf{0}$;
- (2) $m = n$, \mathbf{A} 可逆, 此时 \mathbf{A} 与 H 等价.

证明 设 G 与 H 的作用空间分别是 V 与 W , 则 $V\mathbf{A} \subseteq W$. 对 H 中元素 h , 有 G 中元素 g 使得 $V\mathbf{A}h = Vg\mathbf{A} \subseteq V\mathbf{A}$, 所以 $V\mathbf{A}$ 是 H 的不变子空间. 由 H 的不可约性知 $V\mathbf{A} = \mathbf{0}$ 或 $V\mathbf{A} = W$. 如果 $V\mathbf{A} = \mathbf{0}$, 则 $\mathbf{A} = \mathbf{0}$. 如果 $V\mathbf{A} = W$, 则 $m = n$. 现在 $\ker \mathbf{A} \subseteq V$, 故有 $(\ker \mathbf{A})g\mathbf{A} = (\ker \mathbf{A})\mathbf{A}h$, 所以 $(\ker \mathbf{A})g \subseteq \ker \mathbf{A}$, $\ker \mathbf{A}$ 是 G 的不变子空间. 由 G 的不可约性知 $\ker \mathbf{A} = \mathbf{0}$ 或 $\ker \mathbf{A} = V$. 因为 $\mathbf{A} \neq \mathbf{0}$, 所以 $\ker \mathbf{A} = \mathbf{0}$, 故有 $\ker \mathbf{A} = \mathbf{0}$. 此时 $m = n$, \mathbf{A} 可逆, G 与 H 等价. \square

应用定理 3 可以证明下面的定理.

定理 4 G 是复数域上一个不可约 n 级线性群, 则 G 在 n 级一般线性群内的中心化子 C 由全部 n 阶数量矩阵构成.

证明 显然, 数量矩阵均在 C 中. 反之, 任取 C 中一个矩阵 \mathbf{A} , 则对 G 中任一元素 g , 都有

$$g\mathbf{A} = \mathbf{A}g,$$

对任一复数 x , 都有

$$g(\mathbf{A} - x\mathbf{I}) = (\mathbf{A} - x\mathbf{I})g.$$

取 x_0 使得

$$\det[\mathbf{A} - x_0\mathbf{I}] = 0,$$

则由 Schur 引理, $\mathbf{A} - x_0\mathbf{I} = \mathbf{0}$, $\mathbf{A} = x_0\mathbf{I}$, 即 \mathbf{A} 为数量矩阵 x

复数域的条件是必要的, 可以从前面的例 2 看出.

例 5 G 是由 $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ 生成的线性群:

$$G = \left\{ \begin{pmatrix} 0 & 1 & -1 & 0 & 0 & -1 & 1 & 0 \\ -1 & 0 & 0 & -1 & 1 & 0 & 0 & 1 \end{pmatrix} \right\}.$$

G 看成实数域上的线性群是不可约的, 但是它是一个交换群, 因此 G 包含在它的一般线性群内的中心化子 C 之中, 而 G 中的元素不全是数量矩阵.

7.2 群的表示和特征标

本节中用 F 表示一个域, V 是 F 上一个 n 维线性空间. $GL(V)$ 表示 V 的全体可逆线性变换构成的乘法群, $GL_n(F)$ 表示 F 上全体 n 阶可逆矩阵构成的乘法群.

首先介绍群的表示及有关的一些概念.

定义 3 设 G 是一个群, G 到 $GL(V)$ 内的一个同态映射称为 G 的一个(线性)表示, F 称为表示的基域, V 称为表示空间, V 的维数称为表示的级.

称群到 $GL_n(F)$ 内的一个同态映射为 G 的一个(矩阵)表示, F 也称做表示的基域, 而矩阵的阶 n 称做表示的级.

根据 $GL(V)$ 与 $GL_n(F)$ 的同构关系, 可知线性表示与矩阵表示在本质上也是一致的. 因此以后我们谈到群的表示时, 就不再区分是线性表示还是矩阵表示.

定义 4 设 ρ 是 G 到 $GL(V)$ 的一个表示, 称同态 ρ 的核 $\ker \rho$ 为表示 ρ 的核, 则 $\ker \rho$ 是 G 的正规子群. 如果 $\ker \rho = G$, 则称 ρ 是 G 的平凡表示. 如果 $\ker \rho = \{e\}$, 则称 ρ 是 G 的一个忠实表示.

设 ρ 是 G 的一个 n 级表示, 对 G 中元素 g 用 $\rho(g)$ 表示 g 在 ρ 下的象, 并用

$$\rho(G) = \{ \rho(g) \mid g \in G \}$$

表示 g 在 ρ 下的象集合, 则 $\rho(G)$ 是 $GL(V)$ 的一个子群.

定义 5 设 ρ_1, ρ_2 是群 G 的两个表示, 如果 $\rho_1(G)$ 与 $\rho_2(G)$ 是等价的, 则称表示 ρ_1, ρ_2 是等价的.

等价的线性表示在适当选取表示空间的基以后, 有相同的矩阵形式. 因此, 在讨论表示时, 常把等价表示看作是同样的.

定义 6 群 G 的表示 ρ 称为可约的、不可约的、可分解的、不可分解的、完全可约的. 如果线性群 $H = \rho(G)$ 是可约的、不可约的、可分解的、不可分解的、完全可约的.

下面介绍一些群的表示的例子.

例 1 $G = S_3$ 是 3 次对称群, G 到 $GL_3(\mathbb{R})$ 的映射 ρ 定义为:

$$\begin{array}{l}
 e \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \mathbf{I}, \\
 (1, 2) \quad \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \\
 (1, 3) \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \\
 (2, 3) \quad \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \\
 (1, 2, 3) \quad \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \\
 (1, 3, 2) \quad \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.
 \end{array}$$

可以验证 是 G 的一个 3 级表示 .

令

$$\mathbf{A} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & -2 & 1 \\ 1 & 1 & -2 \end{pmatrix},$$

则

$$\mathbf{A}^{-1} (e) \mathbf{A} = \mathbf{I}$$

$$\mathbf{A}^{-1} ((1, 2)) \mathbf{A} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & -1 & 1 \end{pmatrix},$$

$$\begin{aligned}
 \mathbf{A}^{-1}((1,3))\mathbf{A} &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \\
 \mathbf{A}^{-1}((2,3))\mathbf{A} &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & -1 \end{pmatrix}, \\
 \mathbf{A}^{-1}((1,2,3))\mathbf{A} &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & -1 \end{pmatrix}, \\
 \mathbf{A}^{-1}((1,3,2))\mathbf{A} &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 1 \\ 0 & -1 & 0 \end{pmatrix}.
 \end{aligned}$$

所以 ρ 是可约的, 而且是可分解的. 可以表成 $\rho = \rho_1 + \rho_2$, 其中 ρ_1 是平凡表示, 而 ρ_2 是一个 2 级表示:

$$\begin{aligned}
 e & \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \\
 (1,2) & \begin{pmatrix} -1 & 0 \\ -1 & 1 \end{pmatrix}, \\
 (1,3) & \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \\
 (2,3) & \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix}, \\
 (1,2,3) & \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, \\
 (1,3,2) & \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}.
 \end{aligned}$$

下面来证明 ρ_2 是不可约的. 如果 ρ_2 可约, 则有 2 阶可逆矩阵 \mathbf{S} 使得

$$\mathbf{S}^{-1} \begin{pmatrix} -1 & 0 \\ -1 & 1 \end{pmatrix} \mathbf{S} = \begin{pmatrix} x & 0 \\ * & y \end{pmatrix},$$

$$\mathbf{S}^{-1} \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix} \mathbf{S} = \begin{pmatrix} u & 0 \\ * & v \end{pmatrix}.$$

根据相似矩阵的特征值间的关系, 知

$$\begin{aligned} x &= 1, & \text{或} & & x &= -1, \\ y &= -1, & & & y &= 1; \\ u &= \omega, & \text{或} & & u &= \omega^2, \\ v &= \omega^2, & & & v &= \omega. \end{aligned}$$

其中 ω 是一个 3 次单位根. 于是

$$\begin{aligned} & \mathbf{S}^{-1} \left\{ \begin{pmatrix} -1 & 0 \\ -1 & 1 \end{pmatrix} + \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix} \right\} \mathbf{S} \\ &= \mathbf{S}^{-1} \begin{pmatrix} -2 & 1 \\ -2 & 1 \end{pmatrix} \mathbf{S} \\ &= \begin{pmatrix} x+u & 0 \\ * & y+v \end{pmatrix}. \end{aligned}$$

但是

$$\det \begin{pmatrix} -2 & 1 \\ -2 & 1 \end{pmatrix} = 0,$$

而

$$\det \begin{pmatrix} x+u & 0 \\ * & y+v \end{pmatrix} \neq 0,$$

得到一个矛盾. 所以 ρ 是不可约的, χ 是完全可约的.

我们有置换群的置换表示的概念. 设 G 是作用于 $\Omega = \{1, 2, \dots, n\}$ 上的一个置换群, 对 G 中元素 g , 规定 n 级矩阵

$$\mathbf{P}(g) = (g_{ij}),$$

其中

$$g_{ij} = \begin{cases} 1, & \text{若 } i^g = j, \\ 0, & \text{若 } i^g \neq j. \end{cases}$$

则映射 $\rho: g \rightarrow \mathbf{P}(g)$ 是 G 的一个矩阵表示, 称为 G 的置换表示, 每个 $\mathbf{P}(g)$ 中, 每行每列都恰有一个元素为 1, 其余元素都为 0, 这样的矩阵称为置换矩阵.

上面例 1 中的表示, 就是 3 级对称群的置换表示.

可以证明: 同级的置换矩阵相乘后还是置换矩阵; 置换矩阵都是可逆的, 而且置换矩阵的逆矩阵仍是置换群. 因此, n 级置换矩阵对矩阵乘法构成一个群, 这个群与 n 级对称群是同构的.

上一节中讨论的关于线性群的结论都可以用于群表示. 特别地, 有下面的定理.

定理 5 (完全分解定理) 如果有限群 G 的阶不能被基域 F 的特征整除, 那么 G 在 F 上的表示, 都是完全可约的.

以后我们讨论的群都是有限的, 讨论的表示都是复数域上的表示, 所以所讨论的表示都是完全可约的.

下面的定理经常要用到.

定理 6 设 ρ_1, ρ_2 是 G 的两个表示, 次数分别为 m, n , \mathbf{A} 是一个 $m \times n$ 矩阵, 令

$$\mathbf{B} = \sum_{g \in G} \rho_1(g) \mathbf{A} \rho_2(g^{-1}),$$

则

(1) 对任意 $\mathbf{C} \in G$, 都有 $\rho_1(\mathbf{C}) \mathbf{B} = \mathbf{B} \rho_2(\mathbf{C})$.

(2) 如果 ρ_1, ρ_2 是不等价的不可约表示, 则 $\mathbf{B} = \mathbf{0}$, 即

$$\sum_{g \in G} \rho_1(g) \mathbf{A} \rho_2(g^{-1}) = \mathbf{0}.$$

$$\begin{aligned}
 \text{证明} \quad (1) \quad {}_1(\mathbf{C})\mathbf{B} &= {}_1(\mathbf{C}) {}_1(\mathbf{H})\mathbf{A} {}_2(\mathbf{H}^{-1}) \\
 &= {}_1(\mathbf{CH})\mathbf{A} {}_2((\mathbf{CH})^{-1}) {}_2(\mathbf{C}) \\
 &= \mathbf{B} {}_2(\mathbf{C}).
 \end{aligned}$$

(2) 如果 ρ_1, ρ_2 是不等价的不可约表示, 则由 Schur 引理, 即得 $\mathbf{B} = \mathbf{0}$.

下面我们来介绍群的特征标的定义及简单性质.

如果 ρ 是 G 的一个 n 级表示, 那么 G 中每个元素 \mathbf{A} , 都对应一个 n 阶矩阵

$$\rho(\mathbf{A}) = \begin{pmatrix} \rho_{11}(\mathbf{A}) & \rho_{12}(\mathbf{A}) & \dots & \rho_{1n}(\mathbf{A}) \\ \rho_{21}(\mathbf{A}) & \rho_{22}(\mathbf{A}) & \dots & \rho_{2n}(\mathbf{A}) \\ \dots & \dots & \dots & \dots \\ \rho_{n1}(\mathbf{A}) & \rho_{n2}(\mathbf{A}) & \dots & \rho_{nn}(\mathbf{A}) \end{pmatrix},$$

其中每个 $\rho_{ij}(\mathbf{A})$ ($i, j = 1, 2, \dots, n$) 都可以看成群 G 上的函数. 我们给出下面的定义.

定义 7 设 ρ 是群 G 的一个 n 级表示, χ 的特征标 定义为

$$\chi(\mathbf{A}) = \text{tr}(\rho(\mathbf{A})) = \sum_{i=1}^n \rho_{ii}(\mathbf{A}).$$

例 2 对例 1 中的 3 个表示 ρ_1, ρ_2, ρ_3 , 它们的特征标 χ_1, χ_2, χ_3 分别为

$$\begin{aligned}
 \chi_1(e) &= 3, \quad \chi_1(1, 2) = \chi_1(1, 3) \\
 &= \chi_1(2, 3) = \chi_1(1, 2, 3) = \chi_1(1, 3, 2) = 1; \\
 \chi_2(e) &= 2, \quad \chi_2(1, 2) = \chi_2(1, 3) = \chi_2(2, 3) = 0, \\
 \chi_3(1, 2, 3) &= \chi_3(1, 3, 2) = -1;
 \end{aligned}$$

而

$$= \quad + \quad .$$

关于群的特征标, 有以下一些性质, 以后这些性质经常要用到 .

定理 7 等价表示有相同的特征标 .

证明 这是因为相似矩阵有相同的迹 x

根据定理 7 证明的同一理由, 我们有下面的定理 .

定理 8 设 χ 是 G 的一个表示, 则其特征标 χ 在共轭元素上的值相等 .

因此, 特征标 χ 在一个共轭类中各元素上的值都相等, 即特征标是一个类函数 .

定理 9 如果 χ 是 G 的一个可约表示, 可以分解成

$$\chi(\mathbf{A}) = \begin{matrix} \chi_1(\mathbf{A}) \\ * \\ \chi_2(\mathbf{A}) \\ \dots \\ * \\ \dots \\ * \\ \dots \\ \chi_s(\mathbf{A}) \end{matrix} \quad W .$$

设 $\chi_1, \chi_2, \dots, \chi_s$ 分别是表示 $\chi_1, \chi_2, \dots, \chi_s$ 的特征标, 则

$$\chi = \chi_1 + \chi_2 + \dots + \chi_s .$$

定理 10 设 χ 是 G 的一个 n 级表示, \mathbf{A} 是 G 中一个 m 阶元素, 则 $\chi(\mathbf{A})$ 是 n 个 m 次单位根之和, 而且有 $\chi(\mathbf{A}^{-1}) = \overline{\chi(\mathbf{A})}$.

证明 (\mathbf{A}) 是一个 n 阶矩阵, 满足 $(\mathbf{A})^m = \mathbf{I}$. 因此 (\mathbf{A}) 的特征值都是 m 次单位根, (\mathbf{A}) 是 n 个 m 次单位根之和. 而 (\mathbf{A}^{-1}) 的特征值是 (\mathbf{A}) 的特征值的倒数, 即其共轭数, 因此有 $(\mathbf{A}^{-1}) = \overline{(\mathbf{A})}^x$

如果 G 是一个有限群, 其阶用 $|G|$ 表示, G 包含 r 个共轭元素类, 那么 G 的一个 n 级表示包含 $|G|$ 个 n 阶矩阵, 而 G 的一个特征标只包含 r 个数. 我们还可以证明定理 7 之逆命题, 即如果两个表示的特征标相同, 那么这两个表示必等价. 因此为了找出不可约表示, 只要找出它的特征标就可以了. 所以特征标是讨论群表示的非常重要的概念. 下面几节将进一步讨论特征标的一些重要性质. 为此, 首先要介绍群函数及正交等概念.

7.3 正交关系

为了研究有限群的特征标, 必须先讨论群函数的性质.

设 G 是一个有限群, ρ 是 G 的一个 n 级表示, 那么对 G 中元素 \mathbf{A} , (\mathbf{A}) 是一个 n 阶矩阵:

$$(\mathbf{A}) = \begin{pmatrix} \rho_{11}(\mathbf{A}) & \rho_{12}(\mathbf{A}) & \dots & \rho_{1n}(\mathbf{A}) \\ \rho_{21}(\mathbf{A}) & \rho_{22}(\mathbf{A}) & \dots & \rho_{2n}(\mathbf{A}) \\ \dots & \dots & \dots & \dots \\ \rho_{n1}(\mathbf{A}) & \rho_{n2}(\mathbf{A}) & \dots & \rho_{nn}(\mathbf{A}) \end{pmatrix},$$

每个 $\rho_{ii}(\mathbf{A}) (i = 1, 2, \dots, n)$ 都是 G 上一个函数, 取值在基域 F 中.

我们考虑 F 是复数域 \mathbb{C} 的情形. 特征标 $\chi = \sum_{i=1}^n \rho_{ii}$ 也是 G 上一个函数. 为了以后的讨论作准备, 我们先讨论关于群函数的一些性质.

定义 8 设 f_1, f_2 是群 G 上的两个函数, 定义 f_1 与 f_2 的内积为

$$(f_1, f_2) = \frac{1}{|G|} \sum_{\mathbf{A} \in G} f_1(\mathbf{A}) f_2(\mathbf{A}^{-1}).$$

内积有下述一些性质:

$$(1) (f_1, f_2) = (f_2, f_1);$$

$$(2) (f_1 + f_2, f_3) = (f_1, f_3) + (f_2, f_3);$$

(3) $(kf_1, f_2) = k(f_1, f_2), k \in \mathbb{C}$. 这说明内积是一个对称双线性函数.

例 1 7.2 节例 1 中的 给出 S_3 上 4 个函数:

| | $g = e$ | $(1, 2)$ | $(1, 3)$ | $(2, 3)$ | $(1, 2, 3)$ | $(1, 3, 2)$ |
|-------------|---------|----------|----------|----------|-------------|-------------|
| χ_{11} | 1 | -1 | 0 | 1 | 0 | -1 |
| χ_{12} | 0 | 0 | 1 | -1 | -1 | 1 |
| χ_{21} | 0 | -1 | 1 | 0 | 1 | -1 |
| χ_{22} | 1 | 1 | 0 | -1 | -1 | 0 |

它们中一些内积为

$$(\chi_{11}, \chi_{12}) = 0,$$

$$(\chi_{21}, \chi_{22}) = 0,$$

$$(\chi_{11}, \chi_{11}) = \frac{1}{2},$$

$$(\chi_{12}, \chi_{21}) = \frac{1}{2}.$$

可以证明下述一般结论.

定理 11 G 是一个有限群, χ 及 ψ 是 G 的两个不可约表示, 其级数分别为 m 与 n , 且

$$(\mathbf{A}) = (ij(\mathbf{A})), (\mathbf{A}) = (ij(\mathbf{A})), \mathbf{A} \in G.$$

则有

(1) 如果 \mathbf{A} 与 \mathbf{B} 不等价, 则 $(ij, rs) = 0$ ($i, j = 1, \dots, m; r, s = 1, \dots, n$).

$$(2) (ij, rs) = \delta_{is} \delta_{jr} \frac{1}{m} \quad (i, j, r, s = 1, \dots, m).$$

证明 用 \mathbf{E}_r 表示在第 j 行第 r 列元素为 1, 其他元素为 0 的 $m \times n$ 矩阵, m, n 分别为 \mathbf{A} 的级数.

(1) 根据定理 6, 有

$$\frac{1}{|G|} \sum_{\mathbf{A} \in G} (\mathbf{A}) \mathbf{E}_r (\mathbf{A}^{-1}) = 0.$$

上述矩阵的第 i 行第 s 列处的元素为

$$\begin{aligned} & \frac{1}{|G|} \sum_{\mathbf{A} \in G} ij(\mathbf{A}) \delta_{rs} (\mathbf{A}^{-1}) \\ & = (ij, rs) = 0. \end{aligned}$$

(2) 令

$$b_{jr} = \frac{1}{|G|} \sum_{\mathbf{A} \in G} (\mathbf{A}) \mathbf{E}_r (\mathbf{A}^{-1}),$$

则由定理 6, 对 G 中元素 \mathbf{C} 有

$$(\mathbf{C}) b_{jr} = b_{jr} (\mathbf{C}).$$

因为 \mathbf{C} 是 G 中任意元素, 故由定理 4 得 b_{jr} 是一个数量矩阵, 设

$$b_{jr} = c_{jr} \mathbf{I},$$

其中 c_{jr} 是一个复数. 取第 i 行第 s 列处元素, 得

$$\frac{1}{|G|} \sum_{\mathbf{A} \in G} ij(\mathbf{A}) \delta_{rs} (\mathbf{A}^{-1}) = c_{jr} \delta_{is},$$

即

$$(ij, rs) = c_{jr} \delta_{is}.$$

由内积的对称性得

$$(ij, rs) = (rs, ij) = c_{si jr}.$$

因此(2)中等式当 $i = s$ 或 $j = r$ 时成立.

当 $i = s, j = r$ 时

$$(ij, ji) = c_{ii} = c_{jj},$$

所以

$$\begin{aligned} c_1 &= c_2 = \dots = c_m = c, \\ mc &= \sum_{i=1}^m c_{ii} = \sum_{i=1}^m (1i, i1) \\ &= \frac{1}{|G|} \sum_{i=1}^m \sum_{\mathbf{A} \in G} 1i(\mathbf{A}) i1(\mathbf{A}^{-1}) \\ &= \frac{1}{|G|} \sum_{\mathbf{A} \in G} \sum_{i=1}^m 1i(\mathbf{A}) i1(\mathbf{A}^{-1}) \\ &= \frac{1}{|G|} \sum_{\mathbf{A} \in G} 11(e) \\ &= \frac{1}{|G|} \cdot |G| = 1. \end{aligned}$$

从而

$$c = \frac{1}{m},$$

即

$$(ij, ji) = \frac{1}{m} \cdot x$$

下面来证明不可约特征标的正交性.

定理 12(第一正交关系) 设 χ, ψ 是有限群 G 的两个不可约表示, χ, ψ 分别是它们的特征标, 则

$$(\chi, \psi) = \begin{cases} 1, & \text{当 } \chi \text{ 与 } \psi \text{ 等价,} \\ 0, & \text{当 } \chi \text{ 与 } \psi \text{ 不等价.} \end{cases}$$

特别地,有

$$(\chi, \chi) = 1.$$

证明 设 χ, χ' 的级数分别为 m, n , 则

$$\begin{aligned} (\chi, \chi') &= \frac{1}{|G|} \sum_{g \in G} \chi(g) \overline{\chi'(g)} \\ &= \frac{1}{|G|} \sum_{i=1}^m \chi(i) \overline{\chi'(i)} \\ &= \frac{1}{|G|} \sum_{i,j} \chi(i) \overline{\chi'(j)} \\ &= \sum_{i,j} (\chi, \chi')_{i,j}. \end{aligned}$$

当 χ, χ' 不等价时, 和号中各项为 0, 故上式为 0.

当 χ, χ' 等价时, 它们的特征标相同, 故有

$$\begin{aligned} (\chi, \chi) &= \sum_{i,j} (\chi, \chi)_{i,j} \\ &= \sum_{i,j} \chi(i) \overline{\chi(j)} \\ &= \sum_i \chi(i) \overline{\chi(i)} \\ &= m \cdot \frac{1}{m} = 1. \end{aligned}$$

从定理 12 可以推出下述关于特征标的重要结论.

定理 13 有限群的两个不可约表示等价的充分必要条件是它们的特征标相等.

证明 条件的必要性为已知.

设 G 的两个不可约表示 χ, χ' 的特征标相同, 即 $\chi = \chi'$, 则

$$(\chi, \chi) = 1.$$

由定理 12 知 χ 与 χ 等价.

根据这一结论, 我们以后就可以用等价或不等价的特征标来说明等价或不等价的表示的特征标.

由定理 10 知, $(\chi^{-1}) = \overline{(\chi)}$. 因此定理 12 还可写成下面的形式.

定理 12 (第一正交关系) 设 χ_1, χ_2 是群 G 的两个不可约特征标, 则有

$$\begin{aligned} & \frac{1}{|G|} \sum_{g \in G} \chi_1(g) \overline{\chi_2(g)} \\ &= \frac{1}{|G|} \sum_{g \in G} \chi_1(g) \overline{\chi_2(g)} \\ &= \begin{cases} 1, & \text{当 } \chi_1 \text{ 与 } \chi_2 \text{ 等价,} \\ 0, & \text{当 } \chi_1 \text{ 与 } \chi_2 \text{ 不等价.} \end{cases} \end{aligned}$$

定理 13 将有限群的不可约表示的问题归结为不可约特征标的问题. 这些结果可以推广到有限群的任意表示的情形.

如果 G 的表示 χ 的作用空间为 V , 分解成一些不变子空间的直和

$$V = W_1 \oplus W_2 \oplus \dots \oplus W_s,$$

χ 在 $W_i (i=1, 2, \dots, s)$ 上不可约, 诱导出不可约表示 $\chi_i = \chi|_{W_i}$. 将 χ 表成 $\chi_i (i=1, 2, \dots, s)$ 之和, 即

$$\chi = \chi_1 + \chi_2 + \dots + \chi_s.$$

用 $\chi_i (i=1, 2, \dots, s)$ 分别表示 $\chi_i (i=1, 2, \dots, s)$ 的特征标, 则有

$$\chi = \chi_1 + \chi_2 + \dots + \chi_s.$$

还可利用特征标的正交关系来推出表法的唯一性.

定理 14 有限群 G 的表示 χ 可表成不可约表示之和:

$$= \sum_{i=1}^s \chi_i.$$

的特征标也可表成 χ_i 的特征标之和:

$$= \sum_{i=1}^s \chi_i,$$

而且 $\chi_i (i=1, 2, \dots, s)$ 除等价及次序外是唯一确定的.

证明 只要证明唯一性.

已知 $V = W_i$, $\dim W_i = \chi_i$, χ_i 作用于 W_i 上不可约. 分别在 W_i ($i=1, 2, \dots, s$) 上取基, 合成 W 的基. 于是, 对 G 中元素 \mathbf{A} 有

$$\begin{aligned} \chi_1(\mathbf{A}) &= \text{tr}_{W_1}(\mathbf{A}), \\ \chi_2(\mathbf{A}) &= \text{tr}_{W_2}(\mathbf{A}), \\ &\vdots \\ \chi_s(\mathbf{A}) &= \text{tr}_{W_s}(\mathbf{A}). \end{aligned}$$

$$\chi(\mathbf{A}) = \text{tr}_W(\mathbf{A}) = \sum_{i=1}^s \text{tr}_{W_i}(\mathbf{A}) = \sum_{i=1}^s \chi_i(\mathbf{A})$$

所以

$$= \sum_{i=1}^s \chi_i.$$

如果 χ 还可分解为不可约表示之和:

$$= \chi_1 + \chi_2 + \dots + \chi_t.$$

设 χ_i 是 $\chi_1, \dots, \chi_s, \chi_1, \dots, \chi_t$ 中任一不可约特征标, k, l 分别是 χ_i 在 χ_1, \dots, χ_s 中及 χ_1, \dots, χ_t 中出现的次数, 则

$$\begin{aligned} k &= \sum_{i=1}^s (\chi_i, \chi_i) = \sum_{i=1}^s (\chi_i, \chi_i) \\ &= \sum_{j=1}^t (\chi_j, \chi_j) = \sum_{j=1}^t (\chi_j, \chi_j) \\ &= l. \end{aligned}$$

证毕 χ

于是定理 13 可推广为下面的形式 .

定理 13 有限群 G 的两个表示等价的充分必要条件是它们的特征标相同 .

这个定理充分说明了特征标的重要性 . 为了确定群的表示, 只要确定它的特征标就可以了 . 但是如何来找出群的全部不可约特征标, 还需要进一步讨论特征标的性质 .

定理 15 有限群 G 的不同的不可约特征标是线性无关的 .

证明 设 $\chi_1, \chi_2, \dots, \chi_s$ 是有限群 G 的 (全部) 不同的不可约特征标, 如果有复数 a_1, a_2, \dots, a_s 使得

$$a_1 \chi_1 + a_2 \chi_2 + \dots + a_s \chi_s = 0,$$

则由正交性可得

$$\begin{aligned} \sum_{i=1}^s a_i \chi_i(j) &= \sum_{i=1}^s a_i \chi_i(j) \\ &= a_j = 0 \quad (j = 1, 2, \dots, s), \end{aligned}$$

所以 $\chi_1, \chi_2, \dots, \chi_s$ 线性无关 χ

因此, 如果有限群 G 有 r 个共轭类, 那么因为每个特征标都是类函数, 可以看成 r 维向量 . 根据定理 15, G 最多有 r 个不同的不可约特征标 . 以后我们将证明恰有 r 个不同的不可约特征标 .

用 $\chi_1, \chi_2, \dots, \chi_r$ 表示 G 的全部不可约特征标, 其中 χ_1 为单位特征标: $\chi_1(\mathbf{A}) = 1$. 用 C_1, C_2, \dots, C_r 表示 G 的 r 个共轭元素类, 其中 $C_1 = \{e\}$, $|C_i| = h_i$, 用 χ_i^j 表示 χ_i 在 C_j 上的值 .

应用这些符号, 以及以前的结论, 我们还可得出群特征标的一些性质.

$$(1) \quad (\chi_i, \chi_j) = \delta_{ij}.$$

(2) 如果群 G 的两个特征标 χ, ψ 表成不可约特征标的等式为

$$\chi = \sum_i m_i \chi_i, \quad \psi = \sum_i n_i \chi_i,$$

则

$$(\chi, \psi) = \sum_i m_i n_i.$$

$$(3) \quad \chi_1(\mathbf{A}) = |G|,$$

当 $i > 1$ 时, $\chi_i(\mathbf{A}) = 0$.

$$(4) \quad h_j^j = \chi_1 |G|.$$

我们只要对(3)加以证明:

对 $i > 1$, 则

$$\begin{aligned} 0 &= (\chi_i, \chi_1) = \frac{1}{|G|} \sum_{\mathbf{A} \in G} \chi_i(\mathbf{A}) \chi_1(\mathbf{A}^{-1}) \\ &= \frac{1}{|G|} \sum_{\mathbf{A} \in G} \chi_i(\mathbf{A}), \end{aligned}$$

所以, 当 $i > 1$ 时

$$\sum_{\mathbf{A} \in G} \chi_i(\mathbf{A}) = 0.$$

7.4 有限群不可约表示的个数

为了讨论有限群不可约表示的个数, 还需要用到群代数的概念.

一个复数称为代数整数, 如果它是某个首项系数为 1 的整系数多项式的根. 可以证明, 代数整数的和、差与积还是代数整数. 因此全部代数整数组成一个环. 作为准备我们首先来证明.

引理 1 设 F 是一个域, 包含 n 次单位根. 如果 \mathbf{A} 是 F 上的一个矩阵, 对某个正整数 n , $\mathbf{A}^n = \mathbf{I}$, 则 \mathbf{A} 与一个对角矩阵相似.

证明 因为 $\mathbf{A}^n = \mathbf{I}$, 所以 \mathbf{A} 满足多项式 $x^n - 1$, \mathbf{A} 的最小多项式是 $x^n - 1$ 的一个因式, 没有重根. 因此 \mathbf{A} 与一个对角矩阵相似. \square

由引理 1, 可得引理 2.

引理 2 是群 G 的一个表示, \mathbf{A} 是 G 中的一个元素, 则有的等价表示, 使 (\mathbf{A}) 为对角矩阵.

定理 16 设 是群 G 的一个表示 的特征标, \mathbf{A} 是 G 中一个元素, 则 (\mathbf{A}) 是一个代数整数.

证明 根据引理 2, 可设 (\mathbf{A}) 是一个对角矩阵. 对某个正整数 n , $(\mathbf{A})^n = \mathbf{I}$. 因此 (\mathbf{A}) 的对角线元素都是代数整数. 因为代数整数组成环, 所以 (\mathbf{A}) 也是代数整数. \square

下面介绍群代数的概念.

设 G 是一个群, F 是一个域. 令

$$S = \left\{ \sum_{\mathbf{A} \in G} c_{\mathbf{A}} \mathbf{A} \mid c_{\mathbf{A}} \in F \right\},$$

定义 S 的运算:

$$\sum_{\mathbf{A} \in G} c_{\mathbf{A}} \mathbf{A} + \sum_{\mathbf{A} \in G} d_{\mathbf{A}} \mathbf{A} = \sum_{\mathbf{A} \in G} (c_{\mathbf{A}} + d_{\mathbf{A}}) \mathbf{A},$$

$$a \sum_{\mathbf{A} \in G} c_{\mathbf{A}} \mathbf{A} = \sum_{\mathbf{A} \in G} (ac_{\mathbf{A}}) \mathbf{A},$$

$$\sum_{A \in G} c_A \mathbf{A} \cdot \sum_{A \in G} d_A \mathbf{A} = \sum_{A \in G} \sum_{H \in G} c_H d_H^{-1} \mathbf{A} \mathbf{A},$$

则 S 构成域 F 上一个代数, 称为 G 在 F 上的群代数. 将 $1 \cdot \mathbf{A}$ 记作 \mathbf{A} , 则 $S = G$. 设 C_1, C_2, \dots, C_r 是 G 的 r 个共轭元素类, 令

$$\bar{C}_i = \sum_{A \in C_i} \mathbf{A}, \quad i = 1, 2, \dots, r,$$

是对应于 C_i 的 S 中的元素.

定理 17 如果 S 是有限群 G 在复数域 C 上的群代数, 则 $\bar{C}_1, \bar{C}_2, \dots, \bar{C}_r$ 组成 S 的中心 $Z(S)$ 的一组基.

证明 如果 $\mathbf{A} \in G$, 则 $\mathbf{A}^{-1} C_i \mathbf{A} = C_i$, $\bar{C}_i \mathbf{A} = \mathbf{A} \bar{C}_i$, $i = 1, 2, \dots, r$, 所以 $\bar{C}_i \in Z(S)$. 因为共轭元素类不相交, 所以 C_1, C_2, \dots, C_r 线性无关.

设 $\mathbf{U} = \sum_{A \in G} c_A \mathbf{A} \in Z(S)$, 则对 G 中 \mathbf{X} 有 $\mathbf{U}\mathbf{X} = \mathbf{X}\mathbf{U}$, 于是

$$\sum_{A \in G} c_A \mathbf{A}\mathbf{X} = \sum_{A \in G} c_A \mathbf{X}\mathbf{A} = \sum_{A \in G} c_{\mathbf{X}\mathbf{A}\mathbf{X}^{-1}} (\mathbf{X}\mathbf{A}\mathbf{X}^{-1}) \mathbf{X},$$

所以

$$c_A = c_{\mathbf{X}^{-1}\mathbf{A}\mathbf{X}}.$$

这说明同一共轭类中元素的系数相同, 故 \mathbf{U} 可表成 $\sum_{i=1}^r c_i \bar{C}_i$.

根据定理 17, \bar{C}_j, \bar{C}_k 的乘积 $\bar{C}_j \bar{C}_k$ 仍在 $Z(S)$ 中, 记

$$\bar{C}_j \bar{C}_k = \sum_{m=1}^r c_{jkm} \bar{C}_m, \quad c_{jkm} \in F.$$

如果将等式左边的乘积用 G 中元素展开, 那么其系数是非负整数. 因此, 上式中右边的系数 c_{jkm} 也是非负整数. 这个公式在以后要用到.

下面利用群代数来进一步讨论群特征标.

群 G 的一个 n 级表示 ρ 可以用唯一的方法扩张为代数 S 到 n 阶矩阵代数中的一个同态映射, 仍用 ρ 来表示:

$$\rho_{\mathbf{A}}(\mathbf{C}_A \mathbf{A}) = \rho_{\mathbf{A}}(\mathbf{C}_A) (\mathbf{A}),$$

因此 ρ 也可认为是群代数 S 的一个表示.

定理 18 如果 S 是群 G 在复数域 \mathbb{C} 上的群代数, ρ 是 G 的一个不可约表示, χ 是 ρ 的特征标. 则:

$$(1) \quad \overline{(\chi_j)} = d_j \mathbf{I}, \quad d_j \in \mathbb{C};$$

$$(2) \quad d_j d_k = \sum_{m=1}^r c_{jkm} d_m;$$

$$(3) \quad d_j = h_j \sqrt{\frac{1}{|G|}}, \quad h_j = |C_j|, \quad \frac{1}{d_j} = \chi_j(e), \quad \frac{1}{d_i} = \chi_i(e).$$

证明 (1) 由定理 2, $\overline{(\chi_j)} \in Z(S)$, 因此 $\overline{(\chi_j)}$ 属于 (G) 的中心化子. 由于 ρ 是不可约的, 故由定理 4 知 $\overline{(\chi_j)}$ 是数量矩阵:

$$\overline{(\chi_j)} = d_j \mathbf{I}, \quad d_j \in \mathbb{C}.$$

(2) 由(1)

$$\begin{aligned} d_j d_k \mathbf{I} &= \overline{(\chi_j)} \overline{(\chi_k)} = \overline{(\chi_j \chi_k)} \\ &= \sum_m c_{jkm} \overline{(\chi_m)} = \sum_m c_{jkm} d_m \mathbf{I}, \end{aligned}$$

故(2)中等式成立.

(3) 由(1)

$$h_j \sqrt{\frac{1}{|G|}} = \text{tr}(\overline{(\chi_j)}) = \text{tr}(d_j \mathbf{I}) = d_j \sqrt{\frac{1}{|G|}},$$

因此

$$d_j = h_j \sqrt{\frac{1}{|G|}} \times$$

定理 19 定理 18 中的 d_j 是代数整数.

证明 根据定理 18, $d_j d_k = \sum_m c_{jkm} d_m$ 是非负整数. 取定 k , 作 r 级方阵 \mathbf{B} :

$$\mathbf{B} = (c_{jkm})$$

及列矩阵 \mathbf{D} :

$$\mathbf{D} = \begin{pmatrix} d_1 \\ \dots \\ d_m \end{pmatrix},$$

则有

$$(d_k \mathbf{I} - \mathbf{B}) \mathbf{D} = \mathbf{0}.$$

因为

$$d_1 = h_i^{1/i} / i = h_i \quad 0,$$

所以 $\mathbf{D} \neq \mathbf{0}$. 于是

$$\det[d_k \mathbf{I} - \mathbf{B}] = 0.$$

因为 c_{jkm} 都是整数, 上式说明 d_k 是一个首项系数为 1 的整系数多项式的根, 因此 d_k 是一个代数整数.

如果 C_i 是群 G 的一个共轭类, 用 \bar{C}_i 表示由 C_i 中元素的逆元素构成的共轭类, 即 $\bar{C}_i = \{x \in G \mid x^{-1} \in C_i\}$.

定理 20 对每个 j, k , 有

$$\sum_i \bar{c}_{ij} \bar{c}_{ik} = \sum_j c_{jki} / |G| h_j.$$

证明 由定理 19, $\bar{C}_j \bar{C}_k = \sum_m c_{jkm} \bar{C}_m$. 当且仅当 $j = k$ 时单位元素 e 出现在 $\bar{C}_j \bar{C}_k$ 中, 因此, 如果 $j \neq k$, 则 $c_{jki} = 0$ 而 $c_{jki} = h_j$. 对每个 i , 有

$$(h_j^{j/i} / i) (h_k^{k/i} / i)$$

$$= \sum_m C_{jkm} h_m \begin{matrix} m \\ i \end{matrix} \begin{matrix} 1 \\ i \end{matrix},$$

$$h_j h_k \begin{matrix} j \\ i \end{matrix} \begin{matrix} k \\ i \end{matrix} = \sum_m C_{jkm} \begin{matrix} m \\ i \end{matrix} \begin{matrix} 1 \\ i \end{matrix},$$

因此

$$h_j h_k \begin{matrix} j \\ i \end{matrix} \begin{matrix} k \\ i \end{matrix}$$

$$= \sum_m C_{jkm} \begin{matrix} 1 \\ i \end{matrix} \begin{matrix} m \\ i \end{matrix}$$

$$= C_{jk1} h_1 / |G| = C_{jk} h_1 / |G|.$$

于是

$$\begin{matrix} j \\ i \end{matrix} \begin{matrix} k \\ i \end{matrix} = C_{jk} / |G| \cdot h_k = C_{jk} / |G| \cdot h_j \cdot x$$

现在可以来证明关于不可约特征标个数的结论.

定理 21 群 G 的不可约特征标的个数等于 G 的共轭类个数.

证明 根据定理 20, 如果 $j \neq k$, 则 $\begin{matrix} j \\ i \end{matrix} \begin{matrix} k \\ i \end{matrix} = 0$, 而当 $j = k$

时 $\begin{matrix} j \\ i \end{matrix} \begin{matrix} k \\ i \end{matrix} = |G| / h_i$. 考虑 s 维向量

$$\left(\begin{matrix} j \\ 1 \end{matrix}, \begin{matrix} j \\ 2 \end{matrix}, \dots, \begin{matrix} j \\ s \end{matrix} \right), \quad j = 1, 2, \dots, r.$$

来证这 r 个向量线性无关. 设有复数 $\alpha_1, \alpha_2, \dots, \alpha_r$ 使

$$\sum_{j=1}^r \alpha_j \left(\begin{matrix} j \\ 1 \end{matrix}, \begin{matrix} j \\ 2 \end{matrix}, \dots, \begin{matrix} j \\ s \end{matrix} \right) = \mathbf{0},$$

则

$$\sum_{j=1}^r \alpha_j \begin{matrix} j \\ i \end{matrix} = 0, \quad i = 1, 2, \dots, s.$$

于是对每个 k 有

$$C_{i,j} \begin{matrix} j \\ i \end{matrix} \begin{matrix} k \\ i \end{matrix}$$

$$= c_k |G| / h_k = 0,$$

因此 $c_k = 0$, 于是 $c_1 = c_2 = \dots = c_k = 0$. 从而证明了这 r 个 s 维向量是线性无关的, $r \leq s$. 已知 $r \geq s$, 所以 $r = s$.

关于群 G 的特征标的级数, 有下列重要性质.

定理 22 群 G 的全部不可约特征标的级数的平方和等于 G 的阶.

证明 由定理 20 得

$$\sum_i (\chi_i^1)^2 = \sum_i \chi_i^1 \chi_i^1 = |G| / h_1 = |G|,$$

式中 χ_i^1 即为不可约特征标 χ_i 的级数. 定理得证.

为了证明关于群的不可约特征标的级数的另一个重要性质, 还需要引入表示 χ 的相关表示 χ^T .

如果 χ 是 G 的一个表示, 用下式定义 G 到 $GL_n(\mathbb{C})$ 的映射:

$$(\chi^T) = ((\chi^{-1}))^T,$$

其中 χ^T 表示 χ 的转置矩阵. 可以证明 χ^T 也是 G 的一个表示, 而且当 χ 不可约时, χ^T 也不可约, χ 与 χ^T 等价时, χ 与 χ^T 等价. 这些性质留作习题请读者完成. 由此可以定义 χ_i^j ($i = 1, 2, \dots, r$): 如果表示 χ_i 的特征标为 χ_i , 则 χ_i^j 的特征标为 χ_i^j . χ_i^j 也是不可约的. $1, 2, \dots, r$ 是 $1, 2, \dots, r$ 的一个排列.

定理 23 (1) $\chi_i^j = \chi_j^i$.

(2) $\sum_j h_j \chi_i^j \chi_k^j = \delta_{ik} |G|$.

证明 (1) 用 χ_i 表示以 χ_i 为特征标的一个表示, g 是 C_i 中一

个元素.于是

$$\begin{aligned} h_i^j &= \text{tr}(\mathbf{A}) = \text{tr}(\mathbf{A}^{-1})^T \\ &= \text{tr}(\mathbf{A}^{-1}) = h_i^j. \end{aligned}$$

(2) 由 $(h_i, h_j) = h_{ij}$ 及 (1), 得

$$\begin{aligned} h_j^j h_i^j &= h_j^j h_i^k \\ &= h_i(\mathbf{A}) h_k(\mathbf{A}^{-1}) \\ &= |G| (h_i, h_k) \\ &= h_{ik} |G|. \quad \times \end{aligned}$$

下面证明群的不可约特征标的级数的一个重要性质.

定理 24 G 的不可约指标的级数能整除 G 的阶.

证明 由定理 19, 对一切 $i, j, h_j^j / |G|$ 是一个代数整数. 由定理 16, 每个 h_k^j 是代数整数. 于是 $h_j^j h_k^j / |G|$ 是一个代数整数. 根据定理 23 得

$$\begin{aligned} h_j^j h_k^j / |G| &= h_{jk} |G| \\ &= |G| h_{jk} \end{aligned}$$

是一个有理数. 但是一个代数整数如果是有理数则一定是一个整数, 因此 $|G|$ 能整除 $|G| h_{jk}$, 即 h_{jk} 的级数能整除 G 的阶. \times

根据定理 22 及定理 24, 当群 G 的阶较小或具有某种特殊性质时, 一般可以把 G 的不可约特征标的级数全部或部分计算出来.

我们以前介绍过群 G 的右正则表示 $R \cdot R$ 看成矩阵表示是一个 $|G|$ 级表示. 有下述结论.

定理 25 ρ 是群 G 的右正则表示, 则其特征表 $\rho = \sum_i n_i \chi_i$, 其中 n_i 是 χ_i 的级数.

证明 设 $\rho = \sum_i n_i \chi_i$, n_i 是非负整数, 来证 n_j 是 χ_j 的级数.

因为 ρ 是右正则表示, 所以对 G 中非单位元素 \mathbf{A} , $\rho(\mathbf{A})$ 改变 G 中 $|G|$ 个元素. 而 $\chi_j(e)$ 保持 G 中每个元素都不变, 故有

$$\rho(\mathbf{A}) = \begin{cases} 0, & \mathbf{A} \neq e, \\ |G|, & \mathbf{A} = e. \end{cases}$$

于是

$$\sum_i n_i \chi_i(\mathbf{A}) = \begin{cases} 0, & \mathbf{A} \neq e, \\ |G|, & \mathbf{A} = e. \end{cases}$$

由不可约特征标的正交性, 有

$$\begin{aligned} n_j |G| &= \sum_i n_i (\chi_i, \chi_j) |G| \\ &= \sum_{\mathbf{A} \in G} n_i \chi_i(\mathbf{A}) \chi_j(\mathbf{A}^{-1}) \\ &= \sum_{\mathbf{A} \in G} \chi_j(\mathbf{A}^{-1}) \sum_i n_i \chi_i(\mathbf{A}) \\ &= \chi_j(e) |G|, \end{aligned}$$

所以 $n_j = \chi_j(e)$, 即为 χ_j 的级数. \square

用 χ_j^{-1} 表示 $\chi_j(e)$, 从上面的证明还可得到 $\sum_i \chi_i^{-1} \chi_i = \chi_j^{-1} |G|$.

这个定理说明右正则表示的重要性: G 的右正则表示的分解式中包含了 G 的全部不可约表示, 即 G 的所有不可约表示都可由右正则表示分解得到.

把一个群的全部特征标用矩阵来表示, 计算及应用起来都更为方便. 设 $\chi_1, \chi_2, \dots, \chi_r$ 是 G 的全部不可约指标, C_1, C_2, \dots, C_r 是 G 的全部共轭元素类. 类代表为 A_1, A_2, \dots, A_r . 记 $\chi_i(A_j) = \chi_{ij}$, $i, j = 1, 2, \dots, r$, 则 G 的特征标表为

| | $A_1 = e$ | ... | A_j | ... | A_r |
|-----|-----------|-----|-------------|-----|-------------|
| 1 | 1 | ... | χ_{1j} | ... | χ_{1r} |
| ... | ... | | ... | | ... |
| i | 1 | ... | χ_{ij} | ... | χ_{ir} |
| ... | ... | | ... | | ... |
| r | 1 | ... | χ_{rj} | ... | χ_{rr} |

有时候为了应用方便, 还可以把共轭类 C_j 中的元素 $|C_j| = h_j$ 列入表中.

作为特征标表的应用, 我们来证明下面关于特征标的一个重要性质.

定理 26 (第二正交关系) χ_i, χ_j, h_j ($i, j = 1, 2, \dots, r$) 等的意义如前, 则有

$$\sum_i \chi_i^j \chi_i^k = \delta_{jk} h_j.$$

证明 把特征标表的各列除以 h_j , 得到一个 r 级方阵

$$\mathbf{X} = \frac{\chi_{ij}}{h_j},$$

则

$$\overline{\mathbf{X}} \mathbf{X}^T = \mathbf{I},$$

其中 $\overline{\mathbf{X}}$ 表示 \mathbf{X} 的共轭矩阵, \mathbf{X}^T 表示 \mathbf{X} 的转置. 于是有

$$\mathbf{X}^T \overline{\mathbf{X}} = \mathbf{I}.$$

由此得

$$\frac{h_j}{h_i} \cdot \frac{h_k}{h_i} = \frac{h_{jk}}{h_i},$$

从而得

$$\frac{h_j}{h_i} \cdot \frac{h_k}{h_i} = \frac{h_{jk}}{h_i} \cdot \chi$$

定理 26 的一般形式如下 .

定理 26 设 χ_1, \dots, χ_r 是 G 的全部不可约特征标, \mathbf{A}, \mathbf{B} 是 G 中两个元素, 则有

$$\frac{\chi_i(\mathbf{A}) \overline{\chi_i(\mathbf{B})}}{|C(\mathbf{A})|} = \begin{cases} 0, & \text{当 } \mathbf{A} \text{ 与 } \mathbf{B} \text{ 不共轭,} \\ 1, & \text{当 } \mathbf{A} \text{ 与 } \mathbf{B} \text{ 共轭.} \end{cases}$$

在有些问题中, 需要作出给定群的特征标表. 构造群特征标表没有一般的方法, 下面给出几个例子 .

例 1 作出对称群 S_3 的特征标表 .

解 S_3 有 3 个共轭类, 其代表元为 $e, (1, 2), (1, 2, 3)$. 因此 S_3 共有 3 个不可约特征标. 根据不可约特征标的级数的性质, 知道这 3 个特征标的级数分别为 1, 1, 2 .

其中一个 1 级特征标 χ_1 为单位特征标, 另一个 1 级特征标可以把奇置换映到 -1, 偶置换映到 1 而得到. 因此 S_3 的特征标表为

| | e | $(1, 2)$ | $(1, 2, 3)$ |
|---|-----|---------------|---------------|
| 1 | 1 | 1 | 1 |
| 2 | 1 | -1 | 1 |
| 3 | 2 | $\frac{2}{3}$ | $\frac{3}{3}$ |

根据第二正交关系, 得

$$\sum_{j=1}^3 \overline{\chi_j^1} \chi_j^2 = 0.$$

由此得

$$\chi_3^2 = 0, \text{ 即 } \chi_3^2 = 0.$$

再由第二正交关系, 用同法可得

$$\chi_3^3 = -1.$$

因此完成了 S_3 的特征标表的计算, 得出 S_3 的特征标表为

| | e | $(1, 2)$ | $(1, 2, 3)$ |
|---|-----|----------|-------------|
| 1 | 1 | 1 | 1 |
| 2 | 1 | -1 | 1 |
| 3 | 2 | 0 | -1 |

例 2 计算 S_3 的右正则表示的置换表示及其特征标.

解 记 $S_3 = \{ \mathbf{A}_1 = e, \mathbf{A}_2 = (1, 2), \mathbf{A}_3 = (1, 3), \mathbf{A}_4 = (2, 3), \mathbf{A}_5 = (1, 2, 3), \mathbf{A}_6 = (1, 3, 2) \}$.

$$\begin{aligned} {}_R(\mathbf{A}_1) &= \mathbf{I}, \\ {}_R(\mathbf{A}_2) &= \begin{array}{cccccc} \mathbf{A}_1 & \mathbf{A}_2 & \mathbf{A}_3 & \mathbf{A}_4 & \mathbf{A}_5 & \mathbf{A}_6 \\ \mathbf{A}_2 & \mathbf{A}_1 & \mathbf{A}_6 & \mathbf{A}_5 & \mathbf{A}_4 & \mathbf{A}_3 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{array}, \\ {}_R(\mathbf{A}_3) &= \begin{array}{cccccc} \mathbf{A}_1 & \mathbf{A}_2 & \mathbf{A}_3 & \mathbf{A}_4 & \mathbf{A}_5 & \mathbf{A}_6 \\ \mathbf{A}_3 & \mathbf{A}_5 & \mathbf{A}_1 & \mathbf{A}_6 & \mathbf{A}_4 & \mathbf{A}_2 \end{array} \end{aligned}$$

$$\begin{aligned}
 & \begin{matrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{matrix} \\
 & = \\
 & \begin{matrix} \mathbf{A}_1 & \mathbf{A}_2 & \mathbf{A}_3 & \mathbf{A}_4 & \mathbf{A}_5 & \mathbf{A}_6 \\ \mathbf{A}_4 & \mathbf{A}_5 & \mathbf{A}_6 & \mathbf{A}_1 & \mathbf{A}_2 & \mathbf{A}_3 \end{matrix} \\
 {}_R(\mathbf{A}_4) & = \\
 & \begin{matrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \end{matrix} \\
 & = \\
 & \begin{matrix} \mathbf{A}_1 & \mathbf{A}_2 & \mathbf{A}_3 & \mathbf{A}_4 & \mathbf{A}_5 & \mathbf{A}_6 \\ \mathbf{A}_5 & \mathbf{A}_6 & \mathbf{A}_1 & \mathbf{A}_2 & \mathbf{A}_3 & \mathbf{A}_4 \end{matrix} \\
 {}_R(\mathbf{A}_5) & = \\
 & \begin{matrix} 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{matrix} \\
 & = \\
 & \begin{matrix} \mathbf{A}_1 & \mathbf{A}_2 & \mathbf{A}_3 & \mathbf{A}_4 & \mathbf{A}_5 & \mathbf{A}_6 \\ \mathbf{A}_5 & \mathbf{A}_1 & \mathbf{A}_2 & \mathbf{A}_3 & \mathbf{A}_4 & \mathbf{A}_6 \end{matrix} \\
 {}_R(\mathbf{A}_6) & =
 \end{aligned}$$

$$\begin{array}{cccccc}
 0 & 0 & 0 & 0 & 0 & 1 \\
 0 & 0 & 0 & 1 & 0 & 0 \\
 0 & 1 & 0 & 0 & 0 & 0 \\
 = & 0 & 0 & 1 & 0 & 0 \\
 1 & 0 & 0 & 0 & 0 & 0 \\
 0 & 0 & 0 & 0 & 1 & 0
 \end{array} \cdot$$

R 的特征标 χ_R 为

$$\chi_R(\mathbf{A}) = 6, \quad \chi_R(\mathbf{A}_i) = 0, \quad i = 2, \dots, 6.$$

R 可以分解为

$$R = \chi_1 + \chi_2 + 2\chi_3.$$

例 3 计算交错群 A_4 的特征标表.

解 A_4 中有 12 个元素, 分成 4 个共轭类, 其代表元为

$$e, (1, 2)(3, 4), (1, 2, 3), (1, 3, 2),$$

共轭类中元素数分别为

$$h_1 = 1, h_2 = 3, h_3 = h_4 = 4.$$

A_4 共有 4 个不可约特征标. 根据定理 22, 定理 24, 可以算出这 4 个特征标的级数分别为 1, 1, 1 及 3. 因为 $(1, 2, 3), (1, 3, 2)$ 都是 3 阶元素, 所以它们在 1 级特征标的值一定是一些 3 次单位根的值. 用 ω 表示一个 3 次单位根, 则另一个 3 次单位根为 ω^2 且有

$$1 + \omega + \omega^2 = 0.$$

而 $(1, 2)(3, 4)$ 在 1 级特征标的值只能是 ± 1 . 由正交关系, 可知 A_4 的特征标表为

| | e $h_1 = 1$ | $(1,2)(3,4)$ $h_2 = 3$ | $(1,2,3)$ $h_3 = 4$ | $(1,3,2)$ $h_4 = 4$ |
|---|------------------|---------------------------|------------------------|------------------------|
| 1 | 1 | 1 | 1 | 1 |
| 2 | 1 | 1 | | 2 |
| 3 | 1 | 1 | 2 | |
| 4 | 3 | -1 | 0 | 0 |

下面列出 A_5 的特征标表供读者参考 .

例 4 A_5 的特征标表为

| | e $h_1 = 1$ | $(1,2,3)$ $h_2 = 20$ | $(1,2)(3,4)$ $h_3 = 15$ | $(1,2,3,4,5)$ $h_4 = 12$ | $(1,2,3,5,4)$ $h_5 = 12$ |
|---|------------------|-------------------------|----------------------------|-----------------------------|-----------------------------|
| 1 | 1 | 1 | 1 | 1 | 1 |
| 2 | 4 | 1 | 0 | -1 | -1 |
| 3 | 5 | -1 | 1 | 0 | 0 |
| 4 | 3 | 0 | -1 | $\frac{1+\sqrt{5}}{2}$ | $\frac{1-\sqrt{5}}{2}$ |
| 5 | 3 | 0 | -1 | $\frac{1-\sqrt{5}}{2}$ | $\frac{1+\sqrt{5}}{2}$ |

7.5 几个应用

作为群表示的应用,在这一节列举几个必须要用群表示论才能证明的定理.这些定理都是群论中很重要的结论.

首先来证 Burnside 的一个定理.为此先来证明下列引理.

引理 设 ρ 是有限群 G 的一个表示, χ 是其特征标. C 是 G 的一个共轭元素类, C 中元素的个数 h 与 $\chi(C)$ 的级数互素, 则对 C 中元素 A 有: 或者 $\chi(A) = 0$, 或者 $\chi(C)$ 包含在 $\chi(G)$ 的中心内, 并有

$(\mathbf{A}) = n_0$, 其中 $n_0 = (e)$ 是 G 的级数, ϵ 是一个单位根.

证明 由假设 h 与 n_0 互素, 故有整数 u, v 使

$$uh + vn_0 = 1.$$

已知, $(\mathbf{A}), h(\mathbf{A})/n_0$ 都是代数整数, 于是

$$uh(\mathbf{A})/n_0 + v(\mathbf{A}) = (\mathbf{A})/n_0$$

也是一个代数整数.

取 $M \in (C)$, 则有可逆矩阵 P 使 $P^{-1}MP$ 为对角矩阵.

如果 $P^{-1}MP$ 是一个数量矩阵, 则 M 也是数量矩阵. M 在 (G) 的中心内, $(C) = M$ 是一个元素. $(\mathbf{A}) = n_0$, ϵ 是一个单位根.

如果 $P^{-1}MP$ 是一个对角矩阵但不是数量矩阵, 那么 $P^{-1}MP$ 的对角线元素都是单位根, 但不全相等, 于是 $|(A)| < n_0, |(A)/n_0| < 1$.

现在设 $f(x) = x^m + a_{m-1}x^{m-1} + \dots + a_1x + a_0$ 是 $(A)/n_0$ 在有理数域 \mathbb{R} 上的最小多项式. $(A)/n_0$ 的共轭数的绝对值也小于 1. 但是 $(A)/n_0$ 的全部共轭数的乘积等于 $\pm a_0$, 于是 $|a_0| < 1$. 但是 $(A)/n_0$ 是代数整数, 所以 a_0 是整数. 因此得 $a_0 = 0$. 由 $f(x)$ 的不可约性, 知 $f(x) = x$, 于是 $(A)/n_0 = 0$, 即 $(A) = 0 \cdot x$.

定理 27 (Burnside 定理) 设 G 是一个有限群, 如果 G 有一个共轭元素类 C , 其元素数 $|C|$ 是素数 p 的方幂 p^d , $d > 0$, 则 G 不可能是单群.

证明 设 G 的阶等于 n , 并设 G 的全部不可约特征标的级数为 $n_1 = 1, n_2, \dots, n_r$:

$$n = 1 + n_2^2 + \dots + n_r^2.$$

因为 p 能整除 n , 故必有某个 n_i ($1 < i \leq r$) 不能为 p 所整除, 设为

n_i . 于是 n_i 与 p 互素. 取 C 中元素 \mathbf{A} , 由引理知 $\chi_i(\mathbf{A}) = 0$ 或 $\chi_i(C)$ 包含在 (G) 的中心内. 在后一种情况, 用 N_0 表示 $\chi_i(G)$ 的中心. 令

$$N = \{ \mathbf{X} \in G \mid \chi_i(\mathbf{X}) \in N_0 \},$$

则 $N \subseteq C$, 且 N 是 G 的一个非平凡正规子群, 因此 G 不是单群.

如果 G 是单群, 则对每个与 p 互素的 $n_i (1 < i \leq r)$ 都有 $\chi_i(\mathbf{A}) = 0$. 由正交关系得

$$\sum_{i=1}^r \chi_i(e) \chi_i(\mathbf{A}) = 0,$$

在此式左边, 有一项 $\chi_1(e) \chi_1(\mathbf{A}) = 1$, 还有一些满足 $(n_i, p) = 1$ 的项等于 0. 而其余的项 $\chi_i(e) \chi_i(\mathbf{A}) = n_i \chi_i(\mathbf{A})$ 都能被 p 整除. 于是

$$\chi_i(e) \chi_i(\mathbf{A}) = 1 + pa = 0,$$

其中 a 是一个代数整数. 这是不可能的, 所以 G 不能是单群. \square

根据定理 27, 可推出下列重要结论.

定理 28 有限单群的共轭类元素数不可能是素数的正方幂.

下面来证明 $p^a q^b$ 定理, 即第 6 章定理 9: $p^a q^b$ (p, q 为不同素数, a, b 为正整数) 阶群一定是可解的.

$p^a q^b$ 定理的证明 如果结论不成立, 设 G 是不满足结论的阶最小的群.

首先证明 G 是单群. 否则 G 有一个非平凡正规子群 N , 则 N 与 G/N 一定是可解的. 由此得 G 也是可解的.

设 P 是 G 的一个 p -Sylow 子群, 则 P 的中心 $Z(P) = \{e\}$. 取 $Z(P)$ 中一个非单位元 z , 则 z 的共轭元素类中元素个数是素数 q

的一个正方幂.由定理 28 知这是不可能的 x

习 题

1. 设 ρ 是群 G 的一个表示, 则映射

$$g \mapsto \det(\rho(g)), \quad \rho \in G,$$

其中 $\det(\rho(g))$ 表示 $\rho(g)$ 的行列式, 也是 G 的一个表示.

2. G 是一个 $(2, 2)$ 型交换群. 求出 G 的右正则表示的置换表示.

3. 证明: 当 $n = 2$ 时, 置换表示都是可约的.

4. 设 ρ 是 G 的一个不可约表示, C 是 G 的一个共轭元素类. 证明: $\chi_C(\rho)$ 是一个数量矩阵.

5. 设 χ 是群 G 的正则表示的特征标, 则有: $\chi(e) = |G|$, 当 $\rho \neq e$ 时, $\chi(\rho) = 0$.

6. 设 χ 是 G 的一个 n 级特征标, 则有 $\chi(e) = n$, 而当 $\rho \neq e$ 时, $\chi(\rho) = 0$.

7. 设 χ 是 G 的一个特征标, σ 是复数域 C 的一个自同构. 定义

$$\chi^\sigma(\rho) = \sigma(\chi(\rho)), \quad \rho \in G.$$

证明: χ^σ 也是 G 的特征标, 而且: χ^σ 不可约当且仅当 χ 不可约; χ^σ 忠实当且仅当 χ 是忠实的.

8. 设 χ, ψ 是 G 的两个特征标. 定义

$$(\chi/\psi)(\rho) = \chi(\rho)/\psi(\rho), \quad \rho \in G,$$

则 χ/ψ 也是 G 的特征标, 并且:

(1) 若 $\chi/\psi(e) = 1$, 则 χ/ψ 不可约当且仅当 χ 不可约;

(2) 若 $\chi/\psi = \bar{\psi}$, 且 $\chi(1) > 1$, 则 χ/ψ 一定可约.

9. 证明: 群 G 的不可约表示都是 1 级表示的充要条件是 G 是一个交换群.

10. 用表示论的结论证明 p^k (p 是一个素数) 阶群一定是交换群.

11. 试构造 21 阶非交换群的特征标表.

12. 设 ρ 是 G 的一个表示. 试证关于 ρ :

$$(\rho^{-1}) = (\rho(\mathbf{A}^{-1}))^T, \quad \mathbf{A} \in G$$

的一些有关结论:

(1) ρ^{-1} 是 G 的一个表示;

(2) 如 ρ 不可约, 则 ρ^{-1} 也不可约;

(3) 如果表示 ρ 与 ρ' 等价, 则 ρ^{-1} 与 $(\rho')^{-1}$ 也等价.

复 习 题

1. a_1, a_2, \dots, a_n 是群 G 中 n 个元素, 证明: $a_1 a_2 \dots a_n$ 与 $a_r \dots a_n a_1 \dots a_{r-1}$ ($2 \leq r \leq n$) 共轭, 因而它们的阶相等.

2. 证明: 在阶大于 2 的群中, 存在非单位元素 a, b , 且 $a \neq b$, 使 $ab = ba$.

3. A, B 是群 G 的子群, a, b 是群 G 的元素, 证明: 如果 $Aa = Bb$, 则 $A = B$.

4. 如果 K 是群 G 的一个子集, 用 K^{-1} 表示由 K 中每个元素的逆元素组成的子集:

$$K^{-1} = \{a^{-1} \mid a \in K\}.$$

证明: 如果 K 是 G 的子群 H 的一个右陪集, 则 K^{-1} 是 H 的一个左陪集.

5. 证明: 如果 a_1, a_2, \dots, a_r 是 G 的子群 H 在 G 中的一个右陪集代表系, 那么 $a_1^{-1}, a_2^{-1}, \dots, a_r^{-1}$ 是 H 在 G 中的一个左陪集代表系.

6. 设 H, K 都是群 G 的子群, a 是 G 中的一个元素. 子集 HaK 称为子群 H, K 的一个双倍集. 证明:

$$|HaK| = |H| \cdot |K| \quad a^{-1}Ha \in K.$$

7. 设 H 是 G 的一个非平凡子群. 证明

$$G = \bigcup_{g \in G} g^{-1}Hg.$$

8. 设 A 与 B 是群 G 的两个子群. 证明: 如果 A 与 B 的并集 $A \cup B$ 是 G 的一个子群, 那么必有 $A \subseteq B$ 或 $B \subseteq A$.

9. 设 G 是一个 pq 阶群, p, q 都是素数且 $p < q$, 则 G 的 q 阶子群是 G 的特征子群.

10. 证明每个循环群都是无限循环群的同态象.

11. H 是 G 的一个指数为 r 的子群, a 是 G 的一个中心元素, 则 $a^r \in H$.

12. 设 A 是群 G 的一个极大交换子群, 则 $Z_G(A) = A$.

13. 设 A 是群 G 的一个交换子群, 且对 A 中任一元素 $a \neq 1$ 都有 $Z_G(a) = A$, 则对 G 中任一元素 x 都有

$$x^{-1}Ax = A \text{ 或 } x^{-1}Ax = A = \{e\}.$$

14. 证明: 不同构的 4 阶群共有两个, 作出它们的乘法表.

15. 证明: 如果 G 有一个指数为 4 的正规子群, 那么 G 一定有指数为 2 的正规子群.

16. 设素数 p 是群 G 的阶 $|G|$ 的最小素因子, 则 G 的指数为 p 的子群(如果存在)一定是 G 的正规子群.

17. 设 G 是一个群, a 是 G 中的一个元素. 证明: 如果 G 中恰有两个元素与 a 共轭, 则 G 一定不是单群.

18. 设 H 是群 G 的一个正规子群, p 是一个素数, $|G/H|$ 与 p 互素. 求证: G 的任一个 Sylow p -子群都包含在 H 中.

19. 设 G 是一个单群, G 的阶不等于 2, φ 是 G 到群 H 上的一个同态映射. 证明: 如果 H 有一个指数为 2 的正规子群 A , 那么 $G \cong A$.

20. 设 A 是 G 的一个正规子群, G/A 是奇数阶有限群. 证明: G 中满足 $a^2 = e$ 的元素 a 都在 A 中.

21. 证明: 如果 $H \triangleleft G$ 且 $(|H|, |G/H|) = 1$, 则 H 是 G 的特征子群.

22. 设 M 是单群 G 的一个极大子群, 则 $N_G(M) = M$.

23. 设 A 是 G 的特征子群, B 是 G 的子群, B/A 是 G/A 的特征子群, 那么 B 是 G 的特征子群.

24. 设 φ 是群 G 的一个自同构, 并设对 G 中任意元素 a 都有 $a^{-1}a \in Z(G)$. 试证: 对 G 中任一元素 b 都有 $b = \varphi(b)$.

25. 设 a_1, a_2, \dots, a_n 是群 G 中 n 个元素, i_1, i_2, \dots, i_n 是 $1, 2, \dots, n$ 的一个排列. 求证: $a_{i_1} a_{i_2}^{-1} \dots a_{i_n} a_{i_n}^{-1} \in G$.

26. 证明: 在 n 次对称群中, 阶为奇数的置换必为偶置换.

27. 证明:

$$\begin{aligned} S_n &= (1, 2), (1, 3), \dots, (1, n) \\ &= (1, 2), (1, 2, \dots, n), \\ A_n &= (1, 2, 3), (1, 2, 4), \dots, (1, 2, n). \end{aligned}$$

28. 证明: S_n 中一个置换 是一个换位元素的充分必要条件是 可以表成两个同型置换之积.

29. 验证下列等式:

$$\begin{aligned} (1, 2, \dots, 2k+1) &= (k+1, k+2, \dots, 2k+1)(1, 2, \dots, k+1); \\ &= (1, 2, \dots, 2k)(2k+1, 2k+2, \dots, 2k+2l) \\ &= (2k, k+l+1, k+l+2, \dots, 2k+2l) \times \\ &= (1, 2, \dots, 2k, 2k+1, \dots, k+l+1)(k+l). \end{aligned}$$

30. 证明 $S_n = A_n$, 而且 A_n 中元素都是 S_n 的换位元素.

31. 证明 $\{1, 2, 3, 4, 5\}$ 上的置换群

$$(1, 2, 3, 4, 5), (2, 3, 5, 4), (1, 6)(3, 4)$$

是一个 3 重传递群, 其阶为 120.

32. 证明: $(1, 2, 3, 4, 5, 6, 7), (2, 6)(3, 4)$ 是一个 168 阶单群.

33. 设 G 是一个正则群. 证明: 当且仅当 $|G|$ 是一个素数时, G 是本原的.

34. 证明: 如果本原群 G 的次数是一个大于 2 的偶数, 那么 G 的阶可被 4 整除.

35. G 是 S_n 的一个半正则子群, 证明 G 在 S_n 内的中心化子是传递的.

36. G 是一个有限交换群, 对 G 中任意元素 a 都有 $a^d = e$ 的最小正整数 d 称做 G 的指数. 证明 G 中有 d 阶元素.

37. G 是 n 阶交换群, 证明: G 是循环群 G 的指数为 n .

38. 证明: (1) 有限域的乘法群是循环群.

(2) 任一域的乘法群的有限子群是循环群.

39. 证明: (1) 交换 p 群 G 的初等交换子群都包含在 G_p 中.

(2) 如果 G 的型不变量为 $p^{n_1}, p^{n_2}, \dots, p^{n_r}$, 则 G 共有 $p^r - 1$ 个 p 阶元素.

40. 证明: p^r 阶初等交换群的自同构群的阶为

$$p^{\binom{r}{2}} (p^r - 1)(p^{r-1} - 1) \dots (p - 1).$$

41. 证明: p^r 阶初等交换群的 p^m 阶子群的个数为

$$\frac{(p^r - 1)(p^{r-1} - 1) \dots (p^{r-m+1} - 1)}{(p^m - 1)(p^{m-1} - 1) \dots (p - 1)}.$$

42. 证明: 如果交换 p 群 G 的型不变量为 $p^{n_1}, p^{n_2}, \dots, p^{n_r}$, 则 G 的 p^m 阶初等交换子群的个数同上题.

43. 设 G 的阶为 $p_1^{k_1} p_2^{k_2} \dots p_s^{k_s}$ (p_1, p_2, \dots, p_s 为不同素数). 证明: G 为交换群的充分必要条件为 G 有指数为 $p_i^{k_i}$ ($i = 1, 2, \dots, s$) 的交换正规子群.

44. 已知有限群 G 中恰有一半元素的阶都是 2, 而另一半元素组成的 G 的一个子群 H , 试证 H 是一个奇阶交换群.

45. 证明: p^2 阶非循环群是两个 p 阶循环群的直积.

46. p 是一个素数, 证明: S_p 有 $(p - 1)!$ 个 p 阶元素, $(p - 2)!$ 个 p 阶子群.

47. p 是一个素数, $p < n < 2p$, 问 S_n 有多少个 p 阶元素, 多少个 p 阶子群? 如果 $n = 2p$ 呢?

48. 证明: $p^2 q^2$ (p, q 为相异素数) 阶群必可解.

49. 证明: $p^2 qr$ (p, q, r 为相异素数) 阶群或为可解群或与 60 阶单群 A_5 同构.

50. 证明 30 阶群一定是可解群.

51. 找出全部互不同构的 30 阶群.

52. 如果 p -群 P 有一个指数为 p^2 的交换子群, 则 P 必有指数为 p^2 的正规交换子群.

53. 如果有限群 G 的每个极大子群都是单群, 且在 G 中正规, 那么 G 是交换群.

54. 用 $I^{(1)}(G)$ 表示群 G 的内自同构群, $I^{(2)}(G)$ 表示 $I^{(1)}(G)$ 的内自同构群, 一般地用 $I^{(k+1)}$ 表示 $I^{(k)}$ 的内自同构群. 证明: G 是幂零群的充分必要条件是存在一个正整数 n 使 $G^{(n)}$ 为单位群.

55. 设 G 是可解群, $|G| = mn$; $(m, n) = 1$, m 是 m 的一个因数. 证明: 如果 H 是 G 的一个 m_1 阶正规子群, 那么 H 一定是 G 的任一个 m 阶子群的正规子群.

56. 设 G 为有限幂零群, G 为循环群, 证明 G 是循环群.

57. p 是一个素数, 试决定 p 元有限域 $F_p = \mathbb{Z}(p)$ 上一般线性群 $GL_n(F_p)$ 的阶.

58. 给定复矩阵

$$\mathbf{I} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \mathbf{J} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \mathbf{K} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix},$$

(i 为虚单位). 令 $S = \{\mathbf{I}, \mathbf{J}, \mathbf{K}\}$, 求复数域上一般线性群 $GL_2(\mathbb{C})$ 中包含集合 S 的最小子群.

59. (1) 设 χ 是交换群 G 的一个特征标, 则

$$\sum_{\mathbf{A} \in G} |\chi(\mathbf{A})|^2 = |G|. \quad (1)$$

(2) 设 H 是 G 的一个交换子群, χ 是 G 的一个不可约特征标, 则

$$(1) \quad \sum_{\mathbf{A} \in H} \chi(\mathbf{A}) = 0.$$

60. 设 χ 是群的一个不可约特征标, $H = \{e\}$ 是 G 的一个交换子群, 并设 $(1) = |G - H|$, 则有:

(1) 对 $G - H$ 中的元素 \mathbf{A} , 均有 $\chi(\mathbf{A}) = 0$;

(2) H 中包含 G 的非平凡交换正规子群.