

有限群论基础

(第2版)

王萼芳 编著

清华大学出版社

1541327

015.2.1

016



CS1702220-2

有限群论基础

(第2版)

王萼芳 编著

O152.1

016

重庆师大图书馆

清华大学出版社
北京

内 容 简 介

本书讲述有限群论的基本知识,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.具体内容包括: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.

本书内容深入浅出,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相关的书籍.本书可用做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.

版权所有,侵权必究.侵权举报电话:010-62782989 13701121933

图书在版编目(CIP)数据

有限群论基础/王萼芳编著.--2 版.--北京:清华大学出版社,2012.11
ISBN 978-7-302-30389-3

I. ①有… II. ①王… III. ①有限群—群论 IV. ①O152.1

中国版本图书馆 CIP 数据核字(2012)第 242840 号

责任编辑:刘 颖

封面设计:常雪影

责任校对:刘玉霞

责任印制:王静怡

出版发行:清华大学出版社

网 址: <http://www.tup.com.cn>, <http://www.wqbook.com>

地 址:北京清华大学学研大厦 A 座 邮 编:100084

社总机:010-62770175

邮 购:010-62786544

投稿与读者服务:010-62776969, c-service@tup.tsinghua.edu.cn

质 量 反 馈:010-62772015, zhiliang@tup.tsinghua.edu.cn

印 刷 者:北京鑫丰华彩印有限公司

装 订 者:三河市新茂装订有限公司

经 销:全国新华书店

开 本:140mm×203mm 印 张:7.25 字 数:180 千字

版 次:2002 年 9 月第 1 版 2012 年 11 月第 2 版 印 次:2012 年 11 月第 1 次印刷

印 数:1~4000

定 价:15.00 元

产品编号:044860-01

第 2 版前言

本书第 1 版出版后,受到广大读者的欢迎,经常有读者来信提出一些很好的意见.趁此再版之机,首先向读者表示感谢.

众所周知,群论特别是有限群论,是一个历史悠久、内容丰富、应用广泛的数学学科.由于内容丰富,因此一般有关有限群论的专著多为洋洋巨作,而且需要读者具有一定的近世代数基础.于是,初学者往往对之望而却步.一些不是专攻群论的读者,如果需要应用或查阅一些关于群论的基本结论,也往往不知从何入手.可能这也是读者欢迎本书的一个原因,因为本书的编写恰恰照顾了这些需求或学习基础.有鉴于此,本书再版时,基本保持原状,不多增加内容,只是作了一些必要的修改和补充.

做题练习是学习任何一门数学学科的重要环节.通过做题,可以熟悉巩固书中内容,加深加宽对内容的理解,并可开阔思路、熟练手法、培养运用这门知识的能力和解决问题的技巧.本书习题较多,希望读者加以好好利用.

本书可作为本科高年级学生的专业选修课教材,也可以供报考代数方向研究生的读者作为备考复习的参考书,还可作为从事相关学科的科技工作者自学的参考书.

作 者

2012 年 6 月于北京大学

第 1 版前言

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门类, 诸如结晶学、理论物理、量子力学以及密码学、系统科学、数理经济等领域中, 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, 但大多为篇幅较大的专著. 本书则以较少的篇幅介绍了有限群理论及其表示论的基本概念和结论. 书中给出了较多的例子, 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, 让基本技能得到训练, 并且补充了有限群论的一些重要结论.

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,这一章可以不讲授.

为了适应广大读者的需要,使更多的读者能受益,阅读本书的读者不要求学习过抽象代数或类似的课程、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所需的有限群及其表示的基本概念和理论.

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 作用	37
习题	49
第 2 章 正规子群与同态定理	52
2.1 同态	52
2.2 共轭子群与共轭元素	57
2.3 正规子群	65
2.4 商群 同态定理	71
2.5 $A_n (n \neq 4)$ 的单性	76
2.6 自同构群	80
习题	89
第 3 章 置换群的进一步讨论	92
3.1 置换群的一些特殊子群	92
3.2 传递群	97
3.3 非传递群	103
3.4 传递群作为群的置换表示	107

3.5 本原性	112
习题	121
第4章 交换群	124
4.1 直积	124
4.2 基	129
4.3 有限交换群的构造	133
习题	141
第5章 Sylow 定理	144
5.1 Sylow 定理	144
5.2 有限 p -群	152
5.3 一些特殊 p -群	154
习题	156
第6章 可解群	158
6.1 合成群列	158
6.2 可解群	165
6.3 亚循环群、幂零群和超可解群	171
习题	175
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、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 中任一元素 a , 都有

$$0+a = a+0 = a.$$

(3') 负元素的存在 对于 G 中任一元素 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 $\mathbb{Z}$ 对于数的加法成一交换群. 因为 $\mathbb{Z}$ 对数的加法满足条件(1')~(4'), 群 $\mathbb{Z}$ 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 $\mathbb{Q}$, 全体实数所成集合 $\mathbb{R}$, 全体复数所成集合 $\mathbb{C}$, 对于数的加法也都成为交换群.

例 2 全体非零有理数 $\mathbb{Q}^*$, 全体非零实数 $\mathbb{R}^*$, 全体非零复数 $\mathbb{C}^*$ 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 设 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 $M_{n,m}(\mathbb{R})$ 表示全部 $n \times m$ 实矩阵所成的集合. $M_{n,m}(\mathbb{R})$ 对矩阵的加法构成一个交换群.

例 5 设 F 是一个域^①, 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 $n \geq 2$ 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 $n \geq 2$ 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. $GL_n(V)$ 对该变换的乘法构成一个群. 当 $n \geq 2$ 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

① 设 F 是一个至少包含两个元素的集合. F 中定义了两种运算: 加法和乘法. 如果 F 对加法构成一个交换群, F 中非零元素全体对乘法也构成一个交换群, 并且 F 的乘法对加法满足分配律, 那么 F 就称为一个域. 元素个数有限的域称为有限域, 元素个数无限的域称为无限域.

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. ■

(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

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

$$a' \cdot (a \cdot a^{-1}) = a' \cdot e = a'.$$

由结合律, 即得

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

所以逆元素是唯一的. ■

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. ■

(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. ■

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

$$\underbrace{a \cdot a \cdot \cdots \cdot a}_{n \text{ 个}} = a^n.$$

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

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

规定

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

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 称为 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 F^* 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

$$(1) a^l = e \Leftrightarrow k \mid l;$$

$$(2) a^l = a^m \Leftrightarrow k \mid l - m.$$

如果 a 是一个无限阶元素,那么

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

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

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

故由(1)即得

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

关于无限阶元素的结论可以从定义直接得到. ■

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 Ω 是由 n 个文字组成的集合:

$$\Omega = \{\alpha_1, \alpha_2, \dots, \alpha_n\}.$$

Ω 到自身的一个一一映射称为(作用于) Ω 上的一个置换, 或 n 元置换, 简称置换. 有时候也称为 $\alpha_1, \alpha_2, \dots, \alpha_n$ 的一个置换.