群论引论

[英] W·莱德曼

彭先愚 译

高等教育出版社

群 论 引 论

[英] W. 莱德曼
彭先愚 译

高等教育出版社

本书根据英国 Longman 公司 1973 年出版的《Introduction to Group Theory》(作者 W. Ledermann) 一书译出.

本书包括群论中最基本的概念和结果，是群论的入门书.

本书可供我国数学专业或其他专业学生学习群论时参考，也可用作群论课的教材.本书还可供有关专业人员参考.

群论引论

[英] W. 莱德曼

彭先愚 译

高等教育出版社出版

新华书店北京发行所发行

河北省香河县 印刷厂印装

开本 850×1168 1/32 印张 6 字数 150000

1987年10月第1版 1987年10月第1次印刷

印数 00 001— 4,620

书号 13010·01246 定价 1.40 元

序　言

自从我的《有限群引论》第一次出版后的二十五年来，群论教学日益普及，教学内容也变得更加丰富．现在，群论是每一个数学系学生的必修课，这门课程的基本概念成为教育学院教师进修的内容之一，而且，在近代学校教学计划中，群论是通常设立的一门课程．由于人们对群论热烈和普遍的兴趣，那个教本显得过时是不足为奇的．它的这一缺点不易于用修订本来改正．

这本《群论引论》有了崭新的开端：引进了最新的术语和记号；不着重讨论有限群（象书名所指出的那样）；增添了一些新论题的简单内容，比如中心群列和幂零群．尽管有这些改变，我仍尽力保留了旧书的初等的特点．前几章应该能为有钻研精神的中学六年级学生所接受．全书打算包括对优等生开设的群论课程的大部份内容．象先前一样，当我相信另一条路径更富于启发性和更有教益时，我不总是挑选最短的途径去达到某一特殊的目标．在书末列举了一些内容更高深和更充实的教材，我希望，读者为了更深入地学习群论会去参考这些书．

这些年来，我收到过许多对于前一本书的建议和批评．所有这些意见都是有益的，而且只要可能，本书都采纳了．不过，我特别感谢J. A. 格林教授，他很细心地看了我的手稿，提出了非常宝贵的意见，这些意见反映了他在这领域中突出的专长和丰富的经验．

最后，我十分感谢出版者，感谢他们的好意和协作．

W. 莱德曼

目　录

第一章 群的概念

§ 1. 引言. 算术的基本运算在于按照某些确定的规则结合两个数 a 与 b，以便得出一个唯一的数 c. 例如，假如合成规则是乘法，就有 $c=ab$. 当 a 与 b 给定时，数 c 总是能够得出的.

我们知道，两个或更多的数相乘服从某些形式法则，这些法则对所有的乘积都适用，而不论它们的数值怎样，比如

$$ab=ba \quad \text{(交换律)} \tag{1.1}$$

$$(ab)c=a(bc) \text{(结合律)} \tag{1.2}$$

$$1a=a1=a. \tag{1.3}$$

最后一个等式引入了一个特殊的数，称为单位元素. 第二个法则更明确地说是这样的：假如我们令 $ab=s$ 及 $bc=t$，那么 $sc=at$ 就总是正确的.

在算术的公理方法中，习惯于一开始就规定公设或公理，例如(1.1)，(1.2)和(1.3)，以及另外某些关于加法和乘法的公设或公理，然后推演出这些公设的逻辑推论. 在开始时，不管这些记号 $a,b,\cdots$ 代表我们通常所理解的数，或者代表另外一些数学实体，或者实际上它们是否容许作任何具体的解释，都是没有关系的. 许多公理系统逻辑上都是可能的，但是它们不是同样的有趣或同样的有意义. 正是由于公理系统在纯粹数学或应用数学中应用的广度和深度的不同，使得我们选择某一个公理系统而不选择另一个.

§ 2. 群论公理. 群的抽象理论论述有限或无限的元素集

$$G: a,b,c,\cdots.$$

关于它规定了一个单一的合成规则，通常(虽然不总是)约定采用乘法的记号和术语来表示元素的合成. 因而我们假定对于 G 的任

意两个相等或不相等的元素 a,b，具有一个唯一的乘积 c，写作

$$ab=c.$$

按照更形式的说法，即元素的每一有序对 (a,b) 与一个唯一的元素 c 相联系. 有序对这个术语的意义是，当 $a\neq b$ 时，对 (a,b) 与对 (b,a) 是不同的. 两个元素的乘积仍然是群的一个元素，这是群的一个本质特征. 或者用更专门的术语来说，群关于乘法是封闭的. 群中所用的乘法类型必须服从在下面的定义中陈述的某些公理.

定义 1 对于一个集 G 规定了一个合成规则(乘法)，假如下面的条件满足，那么这个集 G 形成一个**群**：

I. **封闭性** 对 G 中每一有序对 a,b，都结合着 G 中唯一的一个元素 c，记作

$$ab=c,$$

c 称为 a 与 b 的积.

II. **结合律** 假如 a,b,c 是 G 的任意三个元素，那么

$$(ab)c=a(bc).$$

因此两边都可以用 abc 表示.

III. **单位元素** 集合 G 包含一个元素 1，称为**单位元素**(或**恒等元素**或**中性元素**)，使得对于 G 的每一元素 a，有

$$a1=1a=a.$$

IV. **逆元素** 对应 G 的每一元素 a，G 中存在一个元素 a^{-1}，使得

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

可以看出，除了一般不要求交换律对群适用之外，这些公设与熟知的数系，例如有理数系中乘法服从的那些规则很相似.

定义 2 假如一个群具有附加的性质，即对于它的任意两个元素 a,b，有

$$ab=ba,$$

那么这群称为**阿贝尔***(或**交换**)**群**.

在群中不要求交换律就必须区别 ab 与 ba. 我们分别称它们为用 b 后乘(或右乘)与前乘(或左乘)a. 当交换律在群中不是处处成立时,它们仍可以适用于某些特殊的元素对.

定义 3 *元素 a,b 称为交换(或可交换的),假如*

$$ab=ba.$$

例如,1 与每一元素交换;象 IV 中所要求的那样,a 总是与 a^{-1} 交换.

我们现在要从公理中引出某些结论,它们将进一步阐明群的结构.

(i) 结合律只对三个元素而假设,但是将会看到,n 个因子(按一定次序给出)的乘积具有唯一的意义,因而只要这些因子保留所给的次序,括号可以任意写进或省略. 因为,利用公理 II作为归纳法的基础,我们可以假设少于 n 个因子的乘积已经有了定义,以及

$$a_1a_2\cdots a_r=(a_1a_2\cdots a_s)(a_{s+1}\cdots a_r),\text{此处 } 1<s<r<n.$$

需要证明

$$(a_1\cdots a_r)(a_{r+1}\cdots a_n)=(a_1\cdots a_s)(a_{s+1}\cdots a_n),\quad (1.4)$$

这意味任意两个不同的括号方式导致相同的结果. (1.4) 式的左边可以写成

$$[(a_1\cdots a_s)(a_{s+1}\cdots a_r)](a_{r+1}\cdots a_n)=[b_1b_2]b_3,$$

此处圆括号内的乘积分别用 b_1,b_2 与 b_3 表示. (1.4) 式右边第二个因子由于归纳假设被分开之后,(1.4)式右边可以表示为

$$(a_1\cdots a_s)[(a_{s+1}\cdots a_r)(a_{r+1}\cdots a_n)]=b_1[b_2b_3].$$

由公理 II 我们得到

$$[b_1b_2]b_3=b_1[b_2b_3],$$

这就证明了(1.4)式. 因此我们完全可以省略括号而把每边表为

* 为纪念 N. H. Abel(1802—29)而命名.

$$a_1a_2\cdots a_n.$$

特别，当所有因子都相同时，象在普通代数中那样，我们就写成

$$aa = a^2,$$

$$(aa)a = a(aa) = a^3,$$

$$\cdots\cdots\cdots\cdots$$

因而，当 n 与 m 是正整数时，我们有

$$a^m a^n = a^n a^m = a^{m+n} \tag{1.5}$$

及

$$(a^m)^n = a^{mn}. \tag{1.6}$$

我们有趣地看到，熟知的指数定律(1.5)和(1.6) 最终是依靠乘法的结合律.

不过，当 a 与 b 不交换，通常会发现

$$(ab)^n \neq a^n b^n.$$

但是，当 a 与 b 交换时，

$$(ab)^n = abab\cdots ab = a^n b^n \tag{1.7}$$

及

$$a^m b^n = b^n a^m.$$

因为在这情况下我们可以任意地排列因子.

(ii) 公理 III 假定存在一个双边单位元素. 我们现在将证明只能有一个这样的元素. 因为假设1′是另一元素，具有与 1 相同的性质. 那么因为 1′作为右单位元素作用在 1上，$11' = 1$，又因为 1 作为左单位元素作用在 1′上而有 $11' = 1'$. 因此 $1 = 1'$.

(iii) 公理 IV 中所假设的(双边)逆元素是唯一的. 因为假设 $aa_1 = 1$，那么 $a^{-1}aa_1$ 可以用两种方法去计算，即

$$a^{-1}aa_1 = (a^{-1}a)a_1 = 1\ a_1 = a_1$$

及

$$a^{-1}aa_1 = a^{-1}(aa_1) = a^{-1}\ 1 = a^{-1},$$

从而 $a_1 = a^{-1}$. 类似地，方程 $a_2 a = 1$ 意味 $a_2 = a^{-1}$. 事实上，我们

已经证明 a 的任一左逆元素和 a 的任一右逆元素都等于 a^{-1}.

方程

$$ax=b, \quad ya=b$$

分别有解

$$x=a^{-1}b, \quad y=ba^{-1}.$$

一般情况中 $x\neq y$,我们必须区别用 a 左除与用 a 右除. 这些解是唯一的,因为假如

$$ax=ax_1=b,$$

那么,用 a^{-1} 左乘得出 $x=x_1$. 同样,如果

$$ya=y_1a=b,$$

我们推断出 $y=y_1$.

换句话说,我们有:在每一个群中,**消去律既对于左消去又对于右消去成立.**

显然

$$1=1^2=1^3=\cdots=1^n, \tag{1.8}$$

此处 n 是任一正整数. 因为 a 与 a^{-1} 交换,我们从(1.8)和(1.7)得到

$$1^n=1=(aa^{-1})^n=a^n(a^{-1})^n.$$

由于逆元素的唯一性,$(a^{-1})^n$ 是 a^n 的逆元素,通常写为

$$(a^n)^{-1}=(a^{-1})^n=a^{-n}. \tag{1.9}$$

对任一元素 a 令

$$a^0=1. \tag{1.10}$$

读者不难确信,当 m 与 n 是任何正整数,负整数或零时,法则(1.5)与(1.6)仍然是有效的. 特别,我们看到同一元素的两个幂永远交换,甚至指数是负或零时也如此,因此

$$a^ka^l=a^la^k. \tag{1.11}$$

假如 a 与 b 是任意两个元素,我们有

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

从而，由于逆元素的唯一性，

$$(ab)^{-1}=b^{-1}a^{-1}. \tag{1.12}$$

更一般地，有

$$(ab\cdots st)^{-1}=t^{-1}s^{-1}\cdots b^{-1}a^{-1}. \tag{1.13}$$

最后，我们说 1 是群的唯一的**幂等**元素，即方程

$$x^2=x \tag{1.14}$$

的唯一解是 $x=1$.

因为对(1.14)左乘以 x^{-1}，我们得到

$$x^{-1}x^2=x^{-1}x,$$

因而

$$x=1.$$

假如 G 包含有限个元素，那么元素的个数称为 G 的**阶**；否则 G 称为无限阶的群. G 的阶，不论有限或无限，都用

$$|G|$$

来表示.

虽然对于群的元素的合成常采用乘法这一术语，但是有时为了方便，也采用另外的记号. 比如用

$$a\circ b$$

表示 a 与 b 的合成.

当群是阿贝尔群时(本书中只在这种情况下)经常喜欢用加法记号. 因此对于 a 与 b 的合成我们写成

$$a+b(=b+a),$$

结合律写成

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

单位元素(中性元素)用 0 表示，因此

$$a+0=0+a=a,$$

逆元素写成$(-a)$. 类似 a 的幂，现在就是

$$a+a+\cdots+a=na,$$

此处左边包含 n 个相同的项. 要注意右边的整数 n 通常不是群的元素,事实上,na 只是等式左边的缩写. "指数律"现在采取如下形式:

$$(n+m)a=na+ma,$$

$$n(ma)=(nm)a.$$

我们引入记号

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

因为是阿贝尔群,所以我们有更进一步的关系

$$n(a+b)=na+nb.$$

§ 3. 群的一些例子. 群在大多数数学分支中是屡见不鲜的. 这里我们搜集了几个群的例子,读者可能在别的地方遇见过它们.

(i) *所有正有理数集对于乘法形成一个群.* 的确,两个正有理数的积还是一个正有理数,单位元素是有理数 1,正有理数的逆元素也是正有理数. 结合律作为算术中的一个法则已为人们所知道. 这是一个无限阿贝尔群. 明显地,负有理数集不能形成群;正整数集也不能形成群,因为除 1 之外的每一个元素都没有逆元素.

(ii) *所有整数集对于加法形成一个阿贝尔群.* 这群通常以 Z 表示.

(iii) *围绕一固定点的旋转*: 假如一个三维的刚体相对于一固定点 O 自由转动,则刚体的每一位移相当于围绕经过 O 的一条线 l 转动一角度 α. 这样的位移将用(l,α)表示,或者更简单地用一个单一的字母 $a=(l,\alpha)$来表示. 假如 b 是另一个相对 O 的位移,乘积 ab 规定为这样一个位移,它是 b 跟随 a 之后的结果(按照这个次序——有些作者喜欢用相反的规定,依照那种规定,积必须从右向左念). 在这合成规则下,关于 O的所有位移的集形成一个非阿贝尔群. 单位元素的作用可以表示为$(l,0)$,此处 l 是任意的,(l,α)的逆元素是$(l,-\alpha)$. 根据转动是一种特殊的线性

变换这一事实可得出结合律.

我们通常只对使物体与自身重合的那些位移感兴趣,位移的这样的子集也形成一个群,它称为物体的**对称群**.

下面的实例说明交换律不总是能满足的. 设 1 2 3 4 表示一正方形薄板,最初放在(x,y)-平面内,如图 1 所示,z 轴与薄板平面成直角. 我们假设 $Oxyz$ 是一个右手参考系,它固定在空间中.

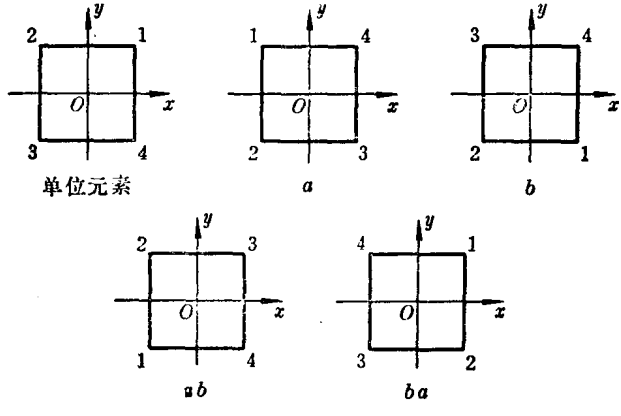

图 1

假如用上面的记号,则有

$$a=\left(Oz,\frac{1}{2}\pi\right),\qquad b=(Ox,\pi).$$

从最后的两个图可以看出 ab 与 ba 造成薄板的不同位置.

(iv) **矩阵群**:读者要熟悉基本的矩阵代数,特别要熟悉矩阵乘法. 群的一些最重要的例子是由矩阵的某些集提供的.

(a) 设 F 是一个域,例如实数域,考虑所有非奇异 $n\times n$ 矩阵,它的元素可从 F 中任意选择. 这个集在矩阵的乘法下形成一个群. 它用 $GL(n,F)$ 来表示,称为 F 上 n 次的**一般线性群**.

(b) 所有 F 上 n 阶正交矩阵在矩阵乘法下形成一个群.

(c) 元素是整数的非奇异 $n\times n$ 矩阵集在乘法下是封闭的，但是这样的矩阵的逆元素一般不属于这个集，因为这个逆元素的形成需要用行列式去除. 可是，行列式是 ± 1 的整数矩阵集的确形成一个群，它称为 n 次幺模群*.

(v) 剩余类：设 m 是大于 1 的固定整数，在本文中 m 称为模. 假如 $x-y$ 可以被 m 整除，那么两个整数 x 与 y 就称为关于模 m 同余，或者称为模 m 同余，这用符号写成

$$x\equiv y(\mathrm{mod}\,m). \tag{1.15}$$

这相当于说：存在一个整数 k 使得

$$x=y+km. \tag{1.16}$$

例如，$3\equiv 18(\mathrm{mod}\ 5)$，$-2\equiv 14(\mathrm{mod}\ 8)$，$12\equiv 0(\mathrm{mod}\ 3)$.

任何一个整数都恰与集

$$Z_m, 0,1,2,\cdots(m-2),(m-1) \tag{1.17}$$

中的某一个整数模 m 同余. 因而 Z_m 被称为模 m 的完全剩余集. 事实上这些数是模 m 的最小非负剩余.

容易检验下面关于同余的法则：

假如 $x_1\equiv y_1(\mathrm{mod}\,m)$ 及 $x_2\equiv y_2(\mathrm{mod}\,m)$，那么

$$x_1+x_2\equiv y_1+y_2\ (\mathrm{mod}\,m) \tag{1.18}$$

及

$$x_1x_2\equiv y_1y_2\ (\mathrm{mod}\,m). \tag{1.19}$$

由于(1.18)，我们能用下面的规定赋予 (1.17) 一个加法群结构，这个规定是：$a+b$ 是(1.17)中与 $a+b$ 模 m 同余的元素，换句话说，元素的合成是普通的加法，假如和大于 m，就将元素的和约化到模 m 的最小非负剩余. 单位元素是零，a 的逆元素是 $(m-$

* 有些作者只对行列式等于 1 的矩阵用这名词.

a). 因而 Z_m 是一个群;它称为模 m 剩余类的加法群. 例如,当 $m=5, 1+2=3, 3+4=2, 2+3=0$ 等等.

也许会问,是否可以用相似的方法利用(1.19)在剩余集中引入一个乘法群结构. 但是不久就会明白,即使我们略去零剩余——它明显地不能是阶大于 1 的乘法群的元素——我们也将要陷入困境. 象我们在§ 2 中所看到的那样,消去律要求假如 $cx=cy$ 则 $x=y$. 但是,例如,我们有 $22\equiv 4(\mathrm{mod}\ 6)$,而 $11\not\equiv 2(\mathrm{mod}\ 6)$,所以消去律对于模 m 的乘法一般并不成立. 尽管如此,我们将看到,同余式中的消去律在某些情况下是容许的. 为了分析这种情况,我们需要从初等数论中借用一些结果和记号,a 与 b 的最大公约数用 (a,b) 表示;特别,当 $(a,b)=1$ 时,我们说 a 与 b 互素. 如果 a 能整除 b,我们写成 $a|b$. 下面的事实只引用不证明.

(i) 假如 $m|kc$ 及 $(m,k)=1$,那么 $m|c$.

(ii) 假如 $(m,a)=1$ 及 $(m,b)=1$,那么 $(m,ab)=1$.

(iii) 假如 $(m,a)=1$. 那么存在整数 u 与 v 使得 $au+mv=1$.

现在我们可以说:假如 $(k,m)=1$,那么由于同余式

$$kx\equiv ky(\mathrm{mod}\, m) \tag{1.20}$$

可得 $x\equiv y(\mathrm{mod}\, m)$. 因为 (1.20) 相当于 $m|k(x-y)$,从而由 (i),$m|(x-y)$. 即 $x\equiv y(\mathrm{mod}\, m)$. 因此假如某一因子与模互素. 它就可以消去.

在集

$$1, 2\cdots, m$$

中那些与 m 互素的整数个数用 $\phi(m)$(欧拉函数)表示.例如,$\phi(9)=6$,因为有 6 个整数 n 使得 $1\leqslant n\leqslant 9$ 及 $(n,9)=1$. 当 p 是素数时,在集 $1, 2,\cdots, p$ 的所有整数中,除最后一个整数外,