经典数学的综合教材

H.B. GRIFFITHS
P.J. HILTON 著

第 三 册

贵阳师范学院数学系
一九八三年十月

肖荣圭赠

第三册 目录

第五部分

代数

第六部分

数系与拓扑

其它三册简目

第一册

序言

第一部份

数学语言

第一章 描述性集合论

第二章 函数：描述性理论

第三章 笛卡尔积

第四章 关系

第五章 数学归纳法

第二部份

集合论续

第六章 函数的集合

第七章 计数和超限算术

第八章 集合代数和命题演算

第二册

第三部份

算术

第九章 交换环和域

第十章 模 m 的算术

第十一章 具有整模的环

第十二章 分解质因数

第十三章 HCF理论的应用

第四部份

$\mathbb{R}^3$ 中的几何

第十四章 $\mathbb{R}^3$ 的向量几何

第十五章 线性代数和 $\mathbb{R}^3$ 内的测度

第十六章 几何的逻辑

第十七章 射影几何

第四册

第七部份

微积分

第二十六章 R^n 代数

第二十七章 极限过程

第二十八章 连续函数

第二十九章 可微函数

第三十章 积分

第七部份（续）

微积分的补充课题

第三十一章 指数函数与对数函数

第三十二章 微分方程

第三十三章 复变函数

第三十四章 逼近与迭代

第三十五章 多元实变函数

第三十六章 向量值函数

第三十七章 C^r 一函数

第八部份

基 础

第三十八章 范畴与函子

第三十九章 数理逻辑

第五部分

代数

要想说从哪个地方起，标术结束而代数开始，这是不容易的，而且该当如此。这部分的内容势必大量地牵涉到第三部分的林念和内容，但是我们提出问题的性质——以及大部分情况下给出的回答——并不是直接地从初等标术中导发出来的，因而我们十分广泛地涉及到第三部分有关整数中的整除问题以及与整数类似的系统，即整环内的整除问题。

这部分里我们再次地研究与整数类似的系统，但是我们的兴趣改变了，我们改察各种代数系统，其每个都来自于某个熟知的标术对象，但是我们现在研究的是一个特殊系统的成员即群的系统，并研究该系统怎样的一些成员是彼此相似，又怎样的一些成员是彼此不同的。因而，我们就涉及到把不同的群在所处结构的意义下进行分类的研究。我们还要涉及群的变换；这些变换仅当其传送群的结构才被认作群论允许的变换。(第十八章实际上是专属于群论的)

类似的说明也适用于向量空间和内积空间，十九章和二十章的主题也是来自于R^3的几何的启示。包含这样一些大学一年级课程水平的材料，在一定程度上说是这本书的一个革新，但是我们相信这个题材不仅有趣和重要而且提供给学生一个公理化方法的介绍，这种方法也许是最有力的，而且肯定的是近代数学的最大特征。当然，对学生来说要理解数学是什么，那是不会像理解数学做些什么来得那么快的。

第十一章引入了结构的一个更进一步的要素，就是次序关系，我们要求它与系统内所具有的代数性质是相容的。本章的一个特色是关于戴德金的实数定义的讨论以及关于布尔代数的一个简短

论述。读者可以适当选择他是否延迟对前者的研究，但我们却不劝告读者匆匆忙忙掌握后者，因为暂且不论其内在的兴趣和重要性，它还带来了重要的收益，代数不必非是关于数的。布尔代数是重要的，而且布尔代数的公理是易懂的，并且从教学的观点来看有其重要的特色，它与任何由整数标术所结合成的系统相违背。

这部分最后一章，我们给出多项式的严格定义，当然，它具有的林念，在以前的章节中，实际上已经突出地描述过了。我们讨论多项式方程的解，稍毫没有企图进行完备的解释，而主要的是为指出精确阐述的重要性，并把这个主要问题弄明白。

第十八章　群

18·1·　群的林念

在9·5的例子中我们早已遇到过阿贝尔群（或交换群）的林念，虽然这一章是独立的，读者将会发现重读9·5是有帮助的。在这一章里我们讨论的基本林念是群，而阿贝尔群则是这样的一个的群。在其中的群运称写成加法，而且是可交换的（见下面的G_4）事实上群的林念在代数和几何里起着根本的作用，而在微积分和数学分析里起着重要的作用。例如群论的产生（经由迦罗华，阿贝尔和其他人之手）是由于想了解为什么阶数≤4的方程可用标准的方法求解，而这些方法对于阶数≥5的方程就失效了，对于这样一个非常自然而又经典的问题进行成功地进军的历史，读者可以参阅E.T.Bell（丛书中的一本（[10]也许是最有吸引力的参考资料）关于方程的伽罗华理论的说明，读者可以参考Postnikov[103]，Birkhoff—Mac Lane[16]的有关章节，或者Artin的更多人为加工的教科书[6]。

III　如在17·11中所注明的，群的林念由克莱因所指出的是几何

的中心，因为它可以使人把几何意味着是什么描述得十分精确，于是我们可把坐标平面 $\mathbb{R}^2$ 看作是全体有序实数对 (x, y)，现在可以证明对任何集 X，全体双射变换 $X \to X$ 的集合 $Perm\ X$ 在变换的复合下成群（见下面的例 18.2.2(iii)），按照克莱因的思想，通过选择 $\mathbb{R}^2$ 的自身等价的群的一个子群 G，我们就得到一种几何，若 F 是一个几何图形，即是 $\mathbb{R}^2$ 的一个子集，如果当 g 跑遍 G 的元素时，F 的性质也是 F 的每个象 $g(F)$ 的性质，则 F 的性质是由 G 指定的几何的不变量。于是如果我们取 G 为由所有的平移，旋转和反射所生成的"欧几里德"运动群，则所得到的几何是平面欧几里德几何，关于群论在这方面的进一步讨论，见 Bell[12]。

在这个课本的三十二章我们将述说初等群论对线性微分方程理论的应用，我们希望这个简短的初级的予告将鼓动读者去研究这一部分，做了以后，他就会佩服群的林总在数学中的重要性，并以急切的心情去进一步探索它，如果是这样的话，我们介绍 Ledermann[80]，若不然，我们就劝告他重新考虑他和数学的关系。

18.2. 群的定义

我们将首先重述群的定义，在记号上和 9.5 中使用的有一点变化。我们说一个集合 G 和一个二元运算 $a \circ b$ 一起构成一个群，如它满足下列公理：

G_1：（结合律）：对所有的 a，b，$c \in G$，$a \circ (b \circ c) = (a \circ b) \circ c$

G_2：（中性元的存在性）：有一元素 e，使得对所有的 $a \in G$ 有 $e \circ a = a \circ e = a$

G_3：（逆元的存在性）：对每个 $a \in G$，有一元素 $\bar{a} \in G$，使得 $a \circ \bar{a} = \bar{a} \circ a = e$

18、2、1 注意：这要求在G_2内有$a\circ e=a$以及在G_3内有$a\circ\bar{a}=a$就已满足了需要；因为利用G_1可以推出$e\circ a=a$和$\bar{a}\circ a=e$，这是重要的，因为我们没有主张对所有$a,b\in G$ $a\circ b=b\circ a$

练习1：

证明e是唯一确定的；$\bar{a}$是由a唯一确定的；以及$\bar{e}=e$，$\overline{\bar{a}}=a$，$\overline{a\circ b}=\bar{b}\circ\bar{a}$，还说明若对某元素$a$有$ag=a$，则$g=e$[比较3、6]。

注：即函数$\circ: G\times G\to G$，但我们写作$g_1\circ g_2$来代替$\circ(g_1,g_2)$。

现在我们给出群的抽象的例子的一个目录，读者应验证所给的每个集合和指定的运算一起确实构成群

18、2、2 例

(i) $G=\mathbb{Z}$，$\circ=+$(则$e=0$，$\bar{a}=-a$)；

(ii) $G=m\mathbb{Z}$，$\circ=+$；

(iii) $G=\mathbb{Z}_m$，$\circ=+$($e=[0]$，$\bar{a}=[-a]$)；

(iv) $G=\mathbb{Q}$，$\circ=+$；

(v) $G=\mathbb{Z}_p-[0]$，$\circ=\times$，p是质数(这里$e=[1]$，又我们用欧拉定理(10、3.1)取$[\bar{a}]=[a]^{p-2}$)

(vi) $G=\mathbb{Q}-\{0\}$，$\circ=\times$($e=1$，$\frac{p}{q}$的逆元是$\frac{q}{p}$)；

(vii) $G=\mathbb{R}$，$\circ=+$；

(viii) $G=\mathbb{R}-\{0\}$，$\circ=\times$

(ix) $G=\mathbb{C}$，$\circ=+$；

(x) $G=\mathbb{C}-\{0\}$，$\circ=\times$；

(xi) $G=\mathbb{R}[x]$, $o=+$ (见例 9.2.4)

(xii) $G=\mathbb{R}^3$ 内将给定正方形变到它自身的欧氏变换的集合(即刚体运动), $o=$复合;

(xiii) $G=S_n$, 集 $(1,2,\cdots,n)$ 的置换的集合, $o=$复合(见下面的 18.2.3), S_n 称作 n 个符号上的对称群. 更一般地, 对任意集 A 我们定义在第八章里的所有双射 $A\to A$ 的集合为 $\mathrm{Perm}A$, 则 $\mathrm{Perm}A$ 关于复合成群; 因为若 $f,g\in \mathrm{Perm}A$, 则 $f\circ g\in \mathrm{Perm}A$, 故 $\mathrm{Perm}A$ 在复合下是封闭的, 由函数的可结合性(2.7.6)得出 $\mathrm{Perm}A$ 满足 G_1; G_2 要求的中性元是 $id: A\to A$ (由 2.7.3); 且定理 2.9.1 指出群的 f 的逆是 $f^{-1}: A\to A$, 在 $\mathrm{Perm}A$ 也是如此. 故 G_3 成立, 因而 $(\mathrm{Perm}A, o)$ 成群。

上面例(i)—(xi)与末两个例子不同. 这是因为它们是交换群的例子; 即群 (G,o) 使得 G_4 成立。

G_4: 对所有的 $a,b\in G$, $a\circ b=b\circ a$

如在 9.5 的注记中所说的那样, 这样的群又称作阿贝尔群, 这是在纪念大的挪威数学家阿贝尔之后而得名的, 但回忆一下, 这个术语应规地仅当群运标记作加法时才被使用。下面我们要说明例(xii)是非交换的, 而例(xiii)当 $n>2$ 是非交换的。18.2.2 中的例(i), (ii), (iv), (vi)—(xi)与其他的不同, 这是因为集合 G 在这些情况下是无限的, 而在其他情况下是有限的, 一般地, 一个群里元素的个数称作群的阶。在有限群的情况下, 我们可以写出群表, 它记下了二元运算。在 $G\times G$ 的元素上的所有值。这样的群表, 关于群 $(\mathbb{Z}_5,+)$ 的出现在例 10.1.5; 其他的在后面出现。

当群的运算标记作 $+$, 我们称这个群为加法的。而且我们称群

为乘法的，如果它是写作×或·或者简单地把两个元素并列在一起（即是说我们省去了运算符号，而把运算对于有序对(a, b)的作用简单地记为ab），我们也可以说群的运算可以写成加法方式或乘法的方式；当然群的运算写做加法或乘法是没有其自身的特性的，——这仅只是选择符号以表示群运算的问题。有个自然的习惯，若是用加法记号，就用0做中性元以及$-a$来做$\bar{a}$；类似地，若使用乘法记号，则习惯上用1做中性元（虽然有时也用e）而a^{-1}做$\bar{a}$。回忆那个约定，1是用来表示Id_X的，它是群$perm\,X$的中性元。这里读者当然不应当把1和e与数1和e相混淆。例(V)的群G，通常称作$\mathbb{Z}_p$的乘群；注意，它有$p-1$个元素。$\mathbb{Z}_5$的乘法群的群表，正示于例10.1.5。精确地说这个群是把所给乘法表限制于它的第一行和第一列的乘积而得到的。例18.2.2的(V)，(Vi)，(Viii)和(8)都是在域上的子集，而且每个都是所对应的域的乘法群；见命题9.6.2。

18.2.3　例　我们给出关于S_3的群表（见例18.2.2(Xiii)）

我们把S_3当做数1、2、3的置换所成的群，且在有序三数组$(1, 2, 3)$上用置换的结果来记S_3的一个元素，于是S_3的六个元素为：

$$(1\ 2\ 3),\ (1\ 3\ 2),\ (2\ 1\ 3),\ (2\ 3\ 1),$$
$$(3\ 1\ 2),\ (3\ 2\ 1)$$

把这些元素记为e，σ_1，σ_2，σ_3，σ_4 σ_5，则对于例$\sigma_1=(1,3,2)$是指$\sigma_1(1)=1$，$\sigma_1(2)=3$，$\sigma_1(3)=2$；现在易知e是S_3的中性元，则得群表：

	e	σ_1	σ_2	σ_3	σ_4	σ_5
e	e	σ_1	σ_2	σ_3	σ_4	σ_5
σ_1	σ_1	e	σ_3	σ_2	σ_5	σ_4
σ_2	σ_2	σ_4	e	σ_5	σ_1	σ_3
σ_3	σ_3	σ_5	σ_1	σ_4	e	σ_2
σ_4	σ_4	σ_2	σ_5	e	σ_3	σ_1
σ_5	σ_5	σ_3	σ_4	σ_1	σ_2	e

例如，这里出现的σ_1，它在标有σ_3的那一行和标有σ_2那一列，这就告诉我们，如果我们做出置换σ_3，接着又做出置换σ_2，就得到置换$\sigma_1=\sigma_2\circ\sigma_3$。

通过观察群表，我们可以立即察觉到一个有限群是否是可交换的——当且仅当该表关于它的主对角线为对称时，这个群是可交换的，于是S_3是不可交换的（$\sigma_2\sigma_2\neq\sigma_2\sigma_1$）

练习2

(i)当$n\geq 3$时推出S_n是不可交换的。

(ii)证明在S_3中，$\sigma_3^3=e$且$\sigma_3^2=\sigma_4$，在S_3中是否其它元素有"平方根"？

(iii)在集S_3上定义一个新运算$*$，其规则为$a*b=b\circ a$，证明$(S_3,*)$成群，其乘法表可将上表对主对角线$e\cdots e$，做一个反射而得到〔主对角线是左上方指向右下方的〕如果沿着对角线$S_5\cdots S_5$做反射，我们是否得到一个群呢？

18、2、4 例 我们给出例18、2、2(8ii)的群的表，我们记正方形的四个顶点为ABCD，显然$\mathbb{R}^3$的任何欧几里德运动（即刚体运动）将正方形映射到它自身，其效果相当于把顶点做了

一个置换，而一个给定的置换，也可以通过至多一个运动来达到[这在直观上是显然的；但是其证明需要一些线性代数]，于是剩下的就是要列出那些由此得出的置换。

我们可以得到A、B、C、D的任何循环置换：

$(A\ B\ C\ D)$，$(B\ C\ D\ A)$，$(C\ D\ A\ B)$，$(D\ A\ B\ C)$

我们可以做出沿着其中一条对角线（譬如说由左上到右下的）的反射；于是得到：

$(C\ B\ A\ D)$，$(D\ C\ B\ A)$，$(A\ D\ C\ B)$，$(B\ A\ D\ C)$

我们当然不能得到这样的置换，即它仅是把相邻两顶点进行交换；由此得一个容易推出上云八个元素的目录表，就是群的元素的完全的目录表

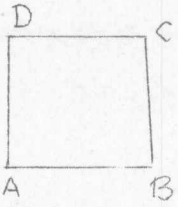

图18·1

因而群的阶数为8；把这些元素（依上云的顺序记为 e，t_1、t_2，…，t_7 我们求得群表为：

·	e	t_1	t_2	t_3	t_4	t_5	t_6	t_7
e	e	t_1	t_2	t_3	t_4	t_5	t_6	t_7
t_1	t_1	t_2	t_3	e	t_7	t_4	t_5	t_6
t_2	t_2	t_3	e	t_1	t_6	t_7	t_4	t_5
t_3	t_3	e	t_1	t_2	t_5	t_6	t_7	t_4
t_4	t_4	t_5	t_6	t_7	e	t_1	t_2	t_3
t_5	t_5	t_6	t_7	t_4	t_3	e	t_1	t_2
t_6	t_6	t_7	t_4	t_5	t_2	t_3	e	t_1
t_7	t_7	t_4	t_5	t_6	t_1	t_2	t_3	e

这个群是非交换的（因为，例如说 $t_1 t_4 \neq t_4 t_1$）。请读者仔细地研究这个例子并实际地核对这个群表。

练习3

(i) 证明元素 e，t_1，t_2，t_3 构成一交换群，并解释这一事实。

(ii) 为求得，譬如说 t_1 的逆，我们沿"t_1"列往下看找到 e；因而 $t_3 = t_1^{-1}$，求出所有其他元素的逆。

现在我们给出群论的某些基本事实和概念。自然地，我们不是以完备为目标的，〔见 lederman [80] 以及载有进一步知识的教科书〕。我们的第一个结论给出群的可供选择的特征，而且还以有系统的方式介绍关于方程的概念。（比较命题 9.5.5）

18.2.5 定理 设 (G, o) 是一非空集且有一个可结合的二元运算 o，则 G 成群当且仅当对每个 $a, b \in G$，方程 $a o x = b$，$y o a = b$ 在 G 内有一个解。

（注意我们所说的"G 成群"是一个标准的省略语，以后都要经常用的，在合适的地方我们还许可把群写成乘法形式）

证：设 G 成群，则 $a(a^{-1}b) = (aa^{-1})b = eb = b$，故方程 $ax = b$ 有一解。类似地，$y = ba^{-1}$ 是方程 $ya = b$ 的一个解。

反之，假定对每个 $a, b \in G$，方程 $ax = b$，$ya = b$，在 G 内有一解，于是特别地，方程 $ax = a$ 有一解，譬如说是 $x = e_a$，我们必明 e_a 是关于 G 的中性元。对任何 $b \in G$，存在着 $y \in G$，使有 $ya = b$，于是 $be_a = (ya)e_a = y(ae_a) = ya = b$，因而 $e = a_a$ 是 G 内的一个右中性元（即对所有的 $b \in G$，$be = b$）。类似地，在 G 内存在一个左中性元 e'，然则

$$e'e = e' \quad (\text{因为 } e \text{ 是一个右中性元})$$
$$= e \quad (\text{因为 } e' \text{ 是一个左中性元})$$

于是 $e=e'$，是 G 内的一个中性元且满足了公理 G_2，公理 G_3 也是满足的，因为存在元素 a'，a'' 使得 $a'a=e$，$aa''=e$，然则 $a'=a'e=a'(aa'')=(a'a)a''=ea''=a''$。故有 $a'=a''=a^{-1}$ 是 G 内 a 的逆。 ▣

按照注位 18·2·1 的说明，上面的证明是不必要的精密，因为指出方程 $ax=b$，$ya=b$ 有解就足以保证了左中性元和左逆元的存在。

练习 4

(i) 证明方程 $ax=b$，$ya=b$ 在 G 内有惟一解，在 G 内解方程 $axb=e$。

(ii) 在例 18·2·4 的群内解方程 $xt_1x=t_3$，〔利用乘法表〕

(iii) 在例 18·2·3 的群 S_3 内解方程 $x^2S_3=S_4$

18·3 指数；子群

研究属于一个群 G 的元素 a，利用乘法记号，自然要把 aa 写成 a^2，一般地把元素 a 的 n 连乘积写成 a^n。类似地把 $(a^{-1})^n$ 写作 a^{-n}，而且通常的指数律在 G 内成立，那即是说约定 $a^0=e$。

18·3·1 $a^m a^n=a^{m+n}$，$(a^m)^n=a^{mn}$，$(a\in G, m,n\in\mathbb{Z})$

18·3·1 的证明，正如 a^n，$n\in\mathbb{N}$ 的定义是用归纳法，读者可以详细地证明它从而得到练习。注意，如果我们在 18·3·1 的第二个方程里令 $n=-1$ 则得到 $(a^m)^{-1}=a^{-m}$。

现在设 H 是 G 的具有下列性质的非空子集

$\mathfrak{P}$：若 $a,b\in H$，则 $ab^{-1}\in H$

读者不难验证 H 成群，反之设 H 是 G 的一个子集，且又是关

于定义群G的二元运算。成群的，则H有性质(P)。我们称这样一个子集H为G的子群。例如，G和单元集{e}就是G的子群，下列的命题是显然的。

18·3·2 命题 设G成群且设a∈G，则a的所有的幂的总集构成G的一个子群。

我们称这个子群为由a产生的子群。若这个子群是G的全体，则G称作由a产生的循环群。当然若G是由a产生的，则G也是由a^{-1}产生的，读者应当在加法记号下研究这些注释。例如，做为$a^2=aa$的代替，我们有$2a=a+b$，而18·3·1的第二个方程变成$n(ma)=mna$，则由a产生的子群是集合

$$\{0, \pm a, \pm 2a, \cdots\}$$

特别地，Z是循环的，它是由$a=1$（或$a=-1$）产生的。

练习5

(i) 说出例18·2·2中的群哪些是循环的并指出其生成元。

(ii) 证明上面的注，单元集{e}是G的一个子群，其中e是中性元。

现在设G是a生成的循环群，则G可能是有限的或无限的。如果G是有限的，a的所有正幂不可能全不相同。假定$e, a, \cdots, a^{n-1}$是全不相同的，而a^n则等于它们中的一个。譬如说有某个q，$0\leq q\leq n-1$，$a^n=a^q$，则$a^{n-q}=e$；但是$e, a, \cdots, a^{n-1}$是全不相同的，我们必有$q=0$，$a^n=e$，现在我们注意到G的每个元素必然和元素$e, a, \cdots, a^{n-1}$中的一个相等。对于G的任意元素有a^k的形式，其中k是一个整数，今由Z的欧几里德性质(11·1.5)我们可写$k=qn+r$ 其中$0\leq r\leq n-1$，则利用