

# 近世代数概论

上册

[美] G. 伯克霍夫 著  
S. 麦克莱恩

王连祥 译  
徐广善

人民教育出版社

1979·北京

# 近世代数概论

## 上册

[美]G. 伯克霍夫 S. 麦克莱恩 著

王连祥 徐广善 译

\*

人民教育出版社出版

新华书店北京发行所发行

人民教育出版社印刷厂印装

\*

开本  $850 \times 1168$  1/32 印张 10.25 字数 246,000

1979 年 12 月第 1 版 1980 年 7 月第 1 次印刷

印数 00,001—14,000

书号 13012·0408 定价 0.90 元

## 第四版序言

在本书第一版写完以来的三十五年间，近世代数已成为世界上大学的标准课程，并且已有许多用于这门课程的著作。尽管如此，回顾一下我们的基本指导思想——也是现在这本书的基本指导思想——看来是可取的。

“我们始终力求表达各种常用的定义的构思背景。为此，我们尽可能用较多的熟悉的例子说明每个新术语。这在基础教科书里特别重要，因为它可以说明一切抽象概念都来源于对具体情况的分析。

“为了提高学生按照新概念独立思考的能力，每个课题里我们都编入广泛多样的习题。这些习题中，一些用来计算，一些用来进一步寻找新概念的例子，另一些给出附加的理论推导。后一种类型的习题对于学生熟悉正式证明的结构有重要的作用。习题的选择足够使讲授者改编课本，以适应在校大学生和研究生一年级学生不同程度的需要。

“近世代数也能够重新解释古典代数的结果，使它们具有更大的统一性和一般性。因此，我们并不省略这些结果，而努力把它们系统地编入近世代数的范围内。

“我们还力求不忽略如下事实：对于许多学生来说，代数学的意义在于它在其他领域的应用，这些领域如高等分析、几何学、物理学和哲学等等。这使我们强调实数域和复数域、同抽象群相对照的变换群、对称矩阵及其对角化、正交群下和欧几里得群下的二

次型分类,并使我们最后加上布尔代数、格论和超限数的内容。所有这些内容在数理逻辑和实函数近代理论中都很重要。”

详细地说,我们的第一、二、三章介绍交换环中线性方程和多项式方程理论,在强调普通的整数环、有理数域的同时,还强调了模 $n$ 整数环和相伴多项式环。第四、五章叙述实数域和复数域的基本代数性质,这对于几何学和物理学具有头等重要性。

第六章通过群这个最简单最基本的概念,引进非交换代数。在第七至十章里,群的概念系统地用到矢量空间和矩阵上。这里注意,代数学在欧几里得几何、仿射几何和射影几何中一直起着最显著最基础的作用。还讨论了对偶空间和张量积,但不考虑推广到环上加法群。

第十一章包含布尔代数和格论十分简单的介绍,后面第十二章,有关于超限数的简短讨论。最后的三章介绍了一般交换代数和算术:理想和商环、域的扩张、代数数及其因子分解以及伽罗瓦理论。

许多章是相互独立的。例如,群论一章可以紧接第一章之后介绍,而关于理想和域的内容(§ 13.1 和 § 14.1)可以直接在矢量空间后来研究。

这种独立性是为了使这本书既适用于只具备中学代数知识的学生的一年教程,又适用于各式各样的短期教程。例如包括线性代数的一学期或一学季的课程,可以以第六至十章为基础,实数域和复数域是要强调的。关于抽象代数的一学期课程,可以安排第一、二、三、六、七、八、十一、十三、十四章,还可以做其他安排。

我们希望本书不仅继续作为课本,而且为那些想要把近代代数的基本概念用于数学的其他领域(包括统计学和计算),用于物理学、化学和工程技术的读者作为方便的参考书。

在此愉快地向C. 贝尔, A. A. 波恩涅, E. 阿廷, F. A. 菲肯, J.

S. 弗雷姆, N. 雅各布森, W. 莱顿, G. 梅里曼, D. D. 米勒, I. 尼文  
以及许多其他朋友和同事致谢, 他们提供了有益的建议和改进。  
另外还要感谢 S. 麦克莱恩夫人, 前三版中她作了秘书工作。

*Cambridge, Mass.* G. 伯克霍夫

*Chicago, Illinois* S. 麦克莱恩

# 近世代数概论

下 册

[美] G. 伯克霍夫 著  
S. 麦克莱恩

人民教育出版社

1980 · 北京

# 目 录

|                         |           |
|-------------------------|-----------|
| <b>第一章 整数</b>           | <b>1</b>  |
| § 1.1 交换环·整环            | 1         |
| § 1.2 交换环的基本性质          | 3         |
| § 1.3 有序整环的性质           | 9         |
| § 1.4 良序原则              | 12        |
| § 1.5 数学归纳法·指数定律        | 14        |
| § 1.6 可除性               | 18        |
| § 1.7 欧几里得算法            | 19        |
| § 1.8 算术基本定理            | 25        |
| § 1.9 同余式               | 27        |
| § 1.10 环 $\mathbb{Z}_n$ | 32        |
| § 1.11 集合·函数·关系         | 35        |
| § 1.12 同构与自同构           | 39        |
| <b>第二章 有理数和域</b>        | <b>42</b> |
| § 2.1 域的定义              | 42        |
| § 2.2 有理数域的构造           | 47        |
| § 2.3 联立线性方程            | 53        |
| § 2.4 有序域               | 58        |
| * § 2.5 正整数公设           | 61        |
| * § 2.6 皮亚诺公设           | 65        |
| <b>第三章 多项式</b>          | <b>69</b> |
| § 3.1 多项式形式             | 69        |
| § 3.2 多项式函数             | 73        |
| § 3.3 交换环的同态            | 78        |
| * § 3.4 多元多项式           | 81        |

|            |             |            |
|------------|-------------|------------|
| § 3.5      | 辗转相除法       | 84         |
| § 3.6      | 单位与相伴       | 86         |
| § 3.7      | 不可约多项式      | 90         |
| § 3.8      | 唯一因子分解定理    | 92         |
| * § 3.9    | 其他唯一因子分解整环  | 97         |
| * § 3.10   | 爱森斯坦不可约判别准则 | 102        |
| * § 3.11   | 部分分式        | 104        |
| <b>第四章</b> | <b>实数</b>   | <b>110</b> |
| § 4.1      | 毕达哥拉斯二难推论   | 110        |
| § 4.2      | 上界与下界       | 112        |
| § 4.3      | 实数公设        | 115        |
| § 4.4      | 多项式方程的根     | 118        |
| * § 4.5    | 戴德金分割       | 122        |
| <b>第五章</b> | <b>复数</b>   | <b>127</b> |
| § 5.1      | 复数的定义       | 127        |
| § 5.2      | 复平面         | 130        |
| § 5.3      | 代数基本定理      | 134        |
| § 5.4      | 共轭数与实多项式    | 138        |
| * § 5.5    | 二次方程与三次方程   | 140        |
| * § 5.6    | 四次方程的根式解法   | 143        |
| * § 5.7    | 稳定型方程       | 145        |
| <b>第六章</b> | <b>群</b>    | <b>147</b> |
| § 6.1      | 正方形的对称      | 147        |
| § 6.2      | 变换群         | 149        |
| § 6.3      | 其他例子        | 155        |
| § 6.4      | 抽象群         | 157        |
| § 6.5      | 同构          | 162        |
| § 6.6      | 循环群         | 165        |
| § 6.7      | 子群          | 169        |
| § 6.8      | 拉格朗日定理      | 173        |
| § 6.9      | 置换群         | 176        |



|          |                  |     |
|----------|------------------|-----|
| § 6.10   | 偶置换与奇置换 .....    | 181 |
| § 6.11   | 同态 .....         | 183 |
| § 6.12   | 自同构 · 共轭元素 ..... | 186 |
| * § 6.13 | 商群 .....         | 190 |
| * § 6.14 | 等价关系与同余关系 .....  | 193 |

## 第七章 矢量与矢量空间 ..... 198

|          |                   |     |
|----------|-------------------|-----|
| § 7.1    | 平面矢量 .....        | 198 |
| § 7.2    | 推广 .....          | 199 |
| § 7.3    | 矢量空间与子空间 .....    | 202 |
| § 7.4    | 线性无关与维数 .....     | 207 |
| § 7.5    | 矩阵与行等价 .....      | 212 |
| § 7.6    | 线性相关的检验 .....     | 215 |
| § 7.7    | 矢量方程 · 齐次方程 ..... | 221 |
| § 7.8    | 基底与坐标系 .....      | 226 |
| § 7.9    | 内积 .....          | 233 |
| § 7.10   | 欧几里得矢量空间 .....    | 235 |
| § 7.11   | 标准正交基 .....       | 238 |
| § 7.12   | 商空间 .....         | 242 |
| * § 7.13 | 线性函数与对偶空间 .....   | 244 |

## 第八章 矩阵代数 ..... 251

|          |                           |     |
|----------|---------------------------|-----|
| § 8.1    | 线性变换与矩阵 .....             | 251 |
| § 8.2    | 矩阵加法 .....                | 258 |
| § 8.3    | 矩阵乘法 .....                | 260 |
| § 8.4    | 对角矩阵 · 置换矩阵 · 三角形矩阵 ..... | 266 |
| § 8.5    | 长方矩阵 .....                | 269 |
| § 8.6    | 逆矩阵 .....                 | 275 |
| § 8.7    | 秩与零度 .....                | 281 |
| § 8.8    | 初等矩阵 .....                | 284 |
| § 8.9    | 等价与标准型 .....              | 290 |
| * § 8.10 | 双线性函数与张量积 .....           | 293 |
| * § 8.11 | 四元数 .....                 | 298 |

|             |     |
|-------------|-----|
| 数学符号表 ..... | 303 |
| 索引 .....    | 305 |

# 目 录

|                              |     |
|------------------------------|-----|
| <b>第九章 线性群</b> .....         | 319 |
| § 9.1 基底的变换 .....            | 319 |
| § 9.2 相似矩阵与特征矢量 .....        | 322 |
| § 9.3 全线性群与仿射群 .....         | 328 |
| § 9.4 正交群与欧几里得群 .....        | 333 |
| § 9.5 不变量与标准型 .....          | 338 |
| § 9.6 线性型与双线性型 .....         | 342 |
| § 9.7 二次型 .....              | 345 |
| § 9.8 全线性群之下的二次型 .....       | 349 |
| § 9.9 全线性群之下的实二次型 .....      | 351 |
| § 9.10 正交群之下的二次型 .....       | 356 |
| § 9.11 仿射群和欧几里得群之下的二次型 ..... | 361 |
| *§ 9.12 酉矩阵与埃尔米特矩阵 .....     | 366 |
| *§ 9.13 仿射几何 .....           | 371 |
| *§ 9.14 射影几何 .....           | 379 |
| <b>第十章 行列式与标准型</b> .....     | 386 |
| § 10.1 行列式的定义和基本性质 .....     | 386 |
| § 10.2 行列式的乘积 .....          | 392 |
| § 10.3 作为体积的行列式 .....        | 396 |
| § 10.4 特征多项式 .....           | 402 |
| § 10.5 极小多项式 .....           | 407 |
| § 10.6 凯莱-哈密顿定理 .....        | 412 |
| § 10.7 不变子空间与可约性 .....       | 414 |
| § 10.8 第一分解定理 .....          | 419 |
| § 10.9 第二分解定理 .....          | 422 |
| § 10.10 有理标准型与若当标准型 .....    | 425 |

|                          |     |
|--------------------------|-----|
| <b>第十一章 布尔代数与格</b> ..... | 429 |
| § 11.1 基本定义 .....        | 429 |
| § 11.2 定律: 同算术定律类比 ..... | 431 |
| § 11.3 布尔代数 .....        | 434 |
| § 11.4 其他基本定律的推导 .....   | 437 |
| § 11.5 布尔多项式的标准型 .....   | 441 |
| § 11.6 半序 .....          | 445 |
| § 11.7 格 .....           | 448 |
| § 11.8 集合表示 .....        | 452 |
| <b>第十二章 超限算术</b> .....   | 457 |
| § 12.1 数与集合 .....        | 457 |
| § 12.2 可数集 .....         | 460 |
| § 12.3 其他基数 .....        | 463 |
| *§ 12.4 基数的加法与乘法 .....   | 467 |
| *§ 12.5 取幂 .....         | 470 |
| <b>第十三章 环与理想</b> .....   | 473 |
| § 13.1 环 .....           | 473 |
| § 13.2 同态 .....          | 477 |
| § 13.3 商环 .....          | 482 |
| *§ 13.4 理想的代数 .....      | 486 |
| § 13.5 多项式理想 .....       | 490 |
| *§ 13.6 线性代数中的理想 .....   | 494 |
| § 13.7 环的特征 .....        | 496 |
| § 13.8 域的特征 .....        | 499 |
| <b>第十四章 代数数域</b> .....   | 501 |
| § 14.1 代数扩张与超越扩张 .....   | 501 |
| § 14.2 域上的代数元素 .....     | 504 |
| § 14.3 根的添加 .....        | 507 |
| § 14.4 次数与有限扩张 .....     | 511 |
| § 14.5 多重代数扩张 .....      | 514 |
| § 14.6 代数数 .....         | 519 |

|                    |                    |            |
|--------------------|--------------------|------------|
| § 14.7             | 高斯整数 .....         | 523        |
| § 14.8             | 代数整数 .....         | 527        |
| § 14.9             | 代数整数的和与积 .....     | 530        |
| § 14.10            | 二次代数整数的因子分解 .....  | 534        |
| <b>第十五章</b>        | <b>伽罗瓦理论 .....</b> | <b>538</b> |
| § 15.1             | 方程的根域 .....        | 538        |
| § 15.2             | 唯一性定理 .....        | 541        |
| § 15.3             | 有限域 .....          | 543        |
| § 15.4             | 伽罗瓦群 .....         | 546        |
| § 15.5             | 可分多项式与不可分多项式 ..... | 552        |
| § 15.6             | 伽罗瓦群的性质 .....      | 555        |
| § 15.7             | 子群与子域 .....        | 559        |
| § 15.8             | 三次不可约方程 .....      | 563        |
| § 15.9             | 五次方程的不可解性 .....    | 568        |
| <b>文献目录</b> .....  |                    | <b>574</b> |
| <b>数学符号表</b> ..... |                    | <b>578</b> |
| <b>索引</b> .....    |                    | <b>580</b> |

# 第一章 整 数

## § 1.1 交换环·整环

近世代数第一次揭示了数学系统的多变性和丰富性。我们将构造并研究许多这样的系统，但是它们中最基本的是最古老的数学系统——由所有正整数(全体)组成的系统。与其有关的，稍大一点的系统是由所有整数  $0, \pm 1, \pm 2, \pm 3, \dots$  组成的集合  $\mathbf{Z}$ 。因为它与近世代数中的其他系统极为相似，所以我们的讨论就从它开始。

整数具有许多有趣的代数性质。在这一章里，我们将假定一些象公设那样特别明显的性质，并通过逻辑推理由它们导出许多别的性质。

我们首先假定加法和乘法的八个公设。这些公设不仅对于整数成立，而且对于许多其他数系都成立，例如所有有理数(分数)、所有实数(无限小数)和所有复数。这些公设对于多项式和任意已知区间上的连续实函数也成立。对于系统  $R$ ，当这八个公设成立时，我们称  $R$  为交换环。

**定义** 设  $R$  是由元素  $a, b, c, \dots$  组成的集合，在  $R$  上定义了任意两个元素  $a$  与  $b$  (不同或相同) 的和  $a+b$  及积  $ab$ 。如果下列公设 (i)~(viii) 成立，那么  $R$  称为交换环：

- (i) 封闭性。若  $a$  与  $b$  在  $R$  中，则和  $a+b$  及积  $ab$  在  $R$  中。
- (ii) 唯一性。若  $R$  中  $a=a'$  且  $b=b'$ ，则
$$a+b=a'+b' \text{ 以及 } ab=a'b'.$$
- (iii) 交换律。对  $R$  中一切  $a$  与  $b$ ，
$$a+b=b+a, \quad ab=ba.$$

(iv) 结合律. 对  $R$  中一切  $a, b, c$ ,

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

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

(v) 分配律. 对  $R$  中一切  $a, b, c$ ,

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

(vi) 零.  $R$  包含元素  $0$ , 使得

$$a + 0 = a, \text{ 对 } R \text{ 中一切 } a \text{ 成立.}$$

(vii) 单位元素.  $R$  包含元素  $1 \neq 0$ , 使得

$$a1 = a, \text{ 对 } R \text{ 中一切 } a \text{ 成立.}$$

(viii) 加法逆元素. 对  $R$  中每个  $a$ , 方程

$$a + x = 0 \text{ 在 } R \text{ 中有解 } x.$$

所有整数的集合  $\mathbf{Z}$  满足这些公设, 这是我们熟知的. 例如, 交换律和结合律是这么熟悉, 以致在平常应用时无须明确提及它们, 就把  $a + b + c$  表示相等的数  $a + (b + c)$  和  $(a + b) + c$ . (vi) 中指出的  $0$  的性质是数零的特性; 类似地, (vii) 中指出的  $1$  的性质是数  $1$  的特性. 因为这两个公设形式上是类似的, 所以我们可以说,  $0$  和  $1$  分别是加法和乘法的“单位元素”. (vii) 中的假定  $1 \neq 0$  排除了平凡的情形 (否则, 交换环将是仅由整数  $0$  所组成的集合).

所有整数的系统  $\mathbf{Z}$  具有另一个不能由上述公设推出的性质, 即若  $\mathbf{Z}$  中  $c \neq 0$  且  $ca = cb$ , 则必有  $a = b$  ((ii) 中后一部分的逆性质). 但是交换环不一定都具有这个性质, 例如由已知区间上的全体实函数组成的集合, 虽然它们构成交换环, 但并不满足上述性质. 因此, 全体整数不仅构成交换环, 而且构成按下述意义定义的整体环.

**定义** 满足下面附加公设的交换环是整环:

(ix) 消去律. 若  $c \neq 0$ , 且  $ca = cb$ , 则  $a = b$ .

整环  $\mathbf{Z}[\sqrt{2}]$ . 由所有形为  $a + b\sqrt{2}$  的数组成的整环是数论

所感兴趣的, 这里  $a$  和  $b$  是普通整数(在  $\mathbf{Z}$  中). 在  $\mathbf{Z}[\sqrt{2}]$  中,  $a+b\sqrt{2}=c+d\sqrt{2}$  当且仅当  $a=c$ ,  $b=d$ . 加法和乘法分别定义为

$$\begin{aligned}(a+b\sqrt{2})+(c+d\sqrt{2}) &= (a+c)+(b+d)\sqrt{2}, \\ (a+b\sqrt{2})(c+d\sqrt{2}) &= (ac+2bd)+(ad+bc)\sqrt{2}.\end{aligned}$$

对于这些运算, 唯一性和交换律是容易验证的, 而  $0+0\sqrt{2}$  相当于零, 并且  $1+0\sqrt{2}$  相当于单位元素.  $a+b\sqrt{2}$  的加法逆元素是  $(-a)+(-b)\sqrt{2}$ . 结合律和分配律的验证稍长一些, 消去律的验证将放到 § 1.2 末尾.

## § 1.2 交换环的基本性质

在初等代数中, 人们常常认为上述公设及其基本推论是允许的. 倘若对照特殊的例子检验代数运算时, 一般不会发生大的错误. 然而, 当我们想要得到对于整个代数系统都正确的结论(例如, 一般地, 对一切整环都成立)时, 必须多加小心. 我们必须确信, 所有证明只用到明显列出的公设和一般逻辑法则, 其中最基本的逻辑法则是相等关系的三个基本定律:

自反律  $a=a$ .

对称律 若  $a=b$ , 则  $b=a$ .

传递律 若  $a=b$  且  $b=c$ , 则  $a=c$ ,

对一切  $a, b$  和  $c$  都成立.

现在我们列出几个在任意交换环  $R$  中都成立的法则, 并给出它们正式证明.

**法则 1** 对  $R$  中一切  $a, b, c$ , 有

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

这法则可称为右分配律. 与公设 (v) 对比, 公设 (v) 是左分配律.



**证明** 对  $R$  中一切  $a, b, c$ , 有

- 1°  $(a+b)c = c(a+b)$  (乘法交换律)
- 2°  $c(a+b) = ca+cb$  (分配律)
- 3°  $(a+b)c = ca+cb$  (1°, 2°, 传递律)
- 4°  $ca=ac, cb=bc$  (乘法交换律)
- 5°  $ca+cb=ac+bc$  (4°, 加法唯一性)
- 6°  $(a+b)c=ac+bc$  (3°, 5°, 传递律)

**法则 2** 对  $R$  中一切  $a, 0+a=a$ , 且  $1a=a$ .

**证明** 对  $R$  中一切  $a$ , 有

- 1°  $0+a=a+0$  (加法交换律)
- 2°  $a+0=a$  (零的性质)
- 3°  $0+a=a$  (1°, 2°, 传递律)

$1a=a$  的证明类似.

**法则 3** 如果  $R$  中的  $z$  具有性质“对  $R$  中一切  $a, a+z=a$ ”, 那么  $z=0$ .

这个法则表明,  $R$  仅包含一个 0 元素, 它可以起加法单位元素的作用.

**证明** 因为  $a+z=a$  对一切  $a$  都成立, 所以当  $a$  为 0 时等式也成立.

- 1°  $0+z=0$
- 2°  $0=0+z$  (1°, 对称律)
- 3°  $0+z=z$  (法则 2, 当  $a$  为  $z$ )
- 4°  $0=z$  (2°, 3°, 传递律)

在以后的这类证明中, 相等的对称律和传递律的反复运用, 我们都不必写出.

**法则 4** 对  $R$  中一切  $a, b, c$  成立:

由  $a+b=a+c$ , 可推出  $b=c$ .