[美] G. 伯克霍夫　　S. 麦克莱恩著

近世代数概论

上　册

王连祥
徐广善　译

人民教育出版社

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
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 850×1168 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全年教程，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世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

目　录

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 $0,\pm1,\pm2,\pm3,\cdots$ 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 $a,b,c,\cdots$ 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，

$$a+b=b+a, \qquad ab=ba.$$

(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

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

(vii) 单位元素. R 包含元素 $1\neq 0$, 使得

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

(viii) 加法逆元素. 对 R 中每个 a, 方程

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

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

$$(a+b\sqrt{2})+(c+d\sqrt{2})=(a+c)+(b+d)\sqrt{2},$$

$$(a+b\sqrt{2})(c+d\sqrt{2})=(ac+2bd)+(ad+bc)\sqrt{2}.$$

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，并给出它们正式的证明.

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 $b=c$.

这个法则称为加法消去律.

证明 根据公设(viii),对元素a,存在元素x,使 $a+x=0$. 因此

1° $x+a=a+x=0$ (加法交换律,传递律)

2° $x=x, a+b=a+c$ (自反律,假设)

3° $x+(a+b)=x+(a+c)$ (2°,加法唯一性)

4° $b=0+b=(x+a)+b$

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

$=(x+a)+c=0+c=c$

(补上4°中每步的理由!)

法则5 对每个a,R包含方程$a+x=0$的唯一解x.

这个解通常用$x=-a$表示. 因此这法则可被引述为$a+(-a)=0$. 通常,符号$a-b$表示$a+(-b)$.

证明 根据公设(viii),存在解x. 如果y是第二个解,那么根据传递律和对称律,$a+x=0=a+y$. 因此由法则4,$x=y$. 证毕

法则6 对R中给定的a和b,在R中存在唯一的x,使$a+x=b$.

这个法则表明,减法是可能的而且差是唯一的.

证明 取$x=(-a)+b$. 则(给出理由!)

$$a+x=a+[(-a)+b]=[a+(-a)]+b=0+b=b.$$

如果y是第二个解,那么根据传递律$a+x=b=a+y$,因此由法则4,$x=y$. 证毕

法则7 对R中一切a,$a\cdot 0=0=0\cdot a$.

证明

1° $a=a, a+0=a$ (自反律,公设(vi))

2° $a(a+0)=aa$ (1°,乘法唯一性)

3° $aa+a\cdot 0=a(a+0)=aa$ (分配律等)

$$=aa+0$$

4° $a\cdot 0=0$ (3°, 法则 4)

5° $0\cdot a=a\cdot 0=0$ (乘法交换律, 4°)

法则 8 如果 R 中的 u 具有性质"对 R 中一切 a, $au=a$", 那么 $u=1$.

这个法则表明乘法单位元素 1 的唯一性. 证明类似于法则 3, 留作习题.

法则 9 对 R 中一切 a 和 b, $(-a)(-b)=ab$.

这个法则的特殊情形是"玄"律 $(-1)(-1)=1$.

证明 考察三重和(结合律!)

1° $[ab+a(-b)]+(-a)(-b)=ab+[a(-b)+(-a)(-b)]$.

由分配律, $-a$的定义, 法则 7 和公设(vi)得

2° $$ab+[a(-b)+(-a)(-b)]=ab+[a+(-a)](-b)$$
$$=ab+0(-b)=ab.$$

同理, 有

3° $$[ab+a(-b)]+(-a)(-b)=a[b+(-b)]+(-a)(-b)$$
$$=a\cdot 0+(-a)(-b)=(-a)(-b).$$

因此, 根据相等的传递律和对称律, 从 1°, 2°和 3°得出结论.

其他各种简单而熟悉的法则, 都是我们公设的推论, 其中一些在下面习题中叙述.

另一个基本的代数定律是用在解二次方程. 比如, 由 $(x+2)(x-3)=0$ 推出或者 $x+2=0$ 或者$x-3=0$, 就用到这个定律, 它的一般形式就是断语:

若 $ab=0$, 则或者 $a=0$ 或者 $b=0$. (1)

这个断语不是对一切交换环都成立的. 但是在任意整环 D 中, 根据消去律, 这个断语是正确的. 因为假设第一个因子不为零, 则 $ab=0=a0$, 并且 a 可以消去, 因此 $b=0$. 反之, 在任意交换环 R

中，从断语(1)可得到消去律．因为如果 $a\neq 0, ab=ac$，则有 $ab-ac=a(b-c)=0$，由(1)得 $b-c=0$．因此，我们有

定理 1 *在交换环中，乘法消去律等价于"非零因子之积不为零"这个命题．*

使乘积 $ab=0$ 的非零元素 a 和 b 有时称为"零因子"，因此，交换环 R 中的消去律等价于"R 不包含零因子"．

定理 1 可以用来证明 § 1.1 末尾定义的整环 $\mathbf{Z}[\sqrt{2}]$ 的消去律，如下所述．假定 $\mathbf{Z}[\sqrt{2}]$ 包含零因子，使

$$(a+b\sqrt{2})(c+d\sqrt{2})=(ac+2bd)+(ad+bc)\sqrt{2}=0.$$

由定义可推出 $ac+2bd=0, ad+bc=0$．用 d 乘第一个等式，用 c 乘第二个等式，而后相减，得到 $b(2d^2-c^2)=0$，所以或者 $b=0$，或者 $c^2=2d^2$．如果 $b=0$，则上述两个方程给出 $ac=ad=0$，因此，根据定理 1，不是 $a=0$ 就是 $c=d=0$．但是第一种情形 $a=0$ 意味着 $a+b\sqrt{2}=0$(因为 $b=0$)；第二种情形意味着 $c+d\sqrt{2}=0$，所以这两种情形中，都没有零因子．

现在余下 $c^2=2d^2$ 的情形，这意味着 $\sqrt{2}=\frac{c}{d}$ 是有理数，这是不可能的，在 § 3.7 定理 10 中将给出它的证明．

如果承认 $\sqrt{2}$ 是实数，而且承认所有实数的集合构成整环，那么借助于下面子整环的概念可以非常容易地证明 $\mathbf{Z}[\sqrt{2}]$ 是整环．

定义 *整环 D 的子整环是 D 的子集，它对于同一种加法和乘法运算也是整环．*

显然，子集 S 是子整环的充分必要条件是：S 包含 0 和 1；S 包含其中任意元素 a 的加法逆元素；S 包含其中任意两个元素 a 与 b 的和 $a+b$ 及积 ab．