高等学校教学参考书

近世代数基础

(1978年修订本)

张禾瑞 著

人民教育出版社

内 容 提 要

本书是张禾瑞同志1952年著《近世代数基础》的修订本．内容除第一版中的基本概念、群论、环与域、整环里的因子分解等四章外，还增加了关于“扩域”的内容．

本书可作为综合大学数学系和高等师范院校有关专业的教学参考书．

高等学校教学参考书

近世代数基础

（1978年修订本）

张禾瑞著

*

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

*

1978年5月第1版

1978年9月第1次印刷

书号 13012·0124　　定价0.45元

修订本说明

本书第一版只假定读者有中等数学知识；修订本假定了读者学过我国高等学校的“高等代数”课程．但在修订本的前四章中，除极个别的例子和习题外，并没有用到“高等代数”的知识．所以没有学过高等代数的读者，读前四章还是没有什么困难的．

第一版对于“域”写得较少，所以修订本增加了关于“扩域”的第五章．第一版有加了＊号的“规则的等价关系”和“矩阵环”两节．前者内容比较抽象，有些超出这样一本篇幅小的书的限度；后者内容已见“高等代数”．所以修订本删去了这两节．除此以外，对于原有四章只做了不大的变动，主要是参照中国科学院编订的《数学名词》以及近年来的惯例，改动了某些名词和符号．

修订本的不妥之处，希望读者多提宝贵意见．

我的同事张益敏同志在修订本的抄写和校对方面帮了我的忙，我借此机会表示谢意．

张禾瑞

北京师范大学，一九七八年，三月．

第一版序

（一）本书根据1947—48，1949—50在北京大学教近世代数的材料编成.

（二）本书内容依据中央人民政府教育部1951课改草案，只介绍近世代数的初步理论同基本方法.

（三）本书如用作教本，讲授所需时间也符合上述草案的规定.

（四）我国数学著作多半用文言文. 本书不仅用语体文，并且尽可能用接近口语的语体文. 这是作者的一个尝试. 效果究竟如何，希望读者加以批评.

（五）本书只假定读者有中等数学知识.

（六）作者对于材料的选择，分布与处理，都曾加以特殊的注意. 希望因此可以使初学者对于理论易于了解，对于方法易于掌握，在最短时间内得到阅读近世代数方面较深书籍或文献的能力.

（七）本书差不多在每一章节开始都有一段小引，说明各该章节在全书里的地位. 这些小引能够帮助读者得到对于本书的全面了解.

（八）本书的例同习题都占极重要的地位；读者对于例不可忽略，对于习题越多做越好.

（九）本书第一章是全书的基础，读者必须特别加以注意，细心反复阅读. 这一章的内容虽然比较抽象，由于所包含的实例相当多，据经验一般大学生都能接受.

（十）本书的加＊的正文和习题初学者可以略去.

（十一）本书谈到前面定理，若是只说明定理数目，指的是本节的定理，若是加有其他数目，指的是其他章节的定理．如Ⅱ,3,定理1指的是第二章第三节的定理1.

（十二）本书用符号 $A\Longrightarrow B$ 表明由 A 可以得 B，$A\Longleftrightarrow B$ 表明由 A 可以得 B，由 B 可以得 A.

（十三）本书材料多取自各国在这一方面的标准著作，书名我不在这里一一列举了.

（十四）孙树本教授曾试教本书初稿，魏执权同志在本书的文字方面提了很多宝贵的意见，施惟枢同志在本书的抄写校对方面帮了我很大的忙．我在这里谢谢他们.

张禾瑞

北京大学，一九五二年，一月.

目　录

第一章 基本概念

在普通代数里，我们计算的对象是数，计算的方法是加、减、乘、除．数学渐渐进步，我们发现，可以对于若干不是数的事物，用类似普通计算的方法来加以计算．这种例子我们在高等代数里已经看到很多，例如对于向量、矩阵、线性变换等就都可以进行运算．近世代数（或抽象代数）的主要内容就是研究所谓代数系统，即带有运算的集合．近世代数在数学的其他分支和自然科学的许多部门里都有重要的应用．最近二十多年来，它的一些成果更被直接应用于某些新兴的技术．

我们在高等代数里已初步接触到的群、环、域是三个最基本的代数系统．在本书里我们要对这三个代数系统做略进一步的介绍．

在这一章里，我们先把常要用到的基本概念介绍一下．这些基本概念中的某一些，例如集合和映射，在高等代数里已经出现过．但为了完整起见，我们不得不有所重复．

§1. 集　合

若干个（有限或无限多个）固定事物的全体叫做一个**集合**（简称**集**）．

组成一个集合的事物叫做这个集合的**元素**（有时简称**元**）．

关于集合，我们常用到几个名词和符号，现在把它们说明一下．

首先我们要规定空集合这一个概念．

定义　一个没有元素的集合叫做**空集合**．

空集合好象没有什么意义，但我们的确有用得到这个概念的

地方. 这一点我们不久就会看到.

元素我们一般用小写拉丁字母 $a,b,c,\cdots$ 来表示，集合用大写拉丁字母 $A,B,C,\cdots$ 来表示. 一个集合 A 若是由元素 $a,b,c,\cdots$ 作成的，我们用符号

$$A=\{a,b,c,\cdots\}$$

来表示.

若 a 是集合 A 的一个元素，我们说，a 属于 A，或是说，A 包含 a，用符号

$$a\in A \quad 或是 \quad A\ni a$$

来表示.

若 a 不是集合 A 的元素，我们说，a 不属于 A，或是说，A 不包含 a，用符号

$$a\bar{\in}A \quad 或是 \quad A\bar{\ni}a$$

来表示.

定义 若集合 B 的每一个元都属于集合 A，我们说，B 是 A 的**子集**；不然的话，我们说，B 不是 A 的子集.

B 是 A 的子集，我们说，B 属于 A，或是说，A 包含 B，用符号

$$B\subset A \quad 或是 \quad A\supset B$$

来表示. B 不是 A 的子集，我们说，B 不属于 A，或是说，A 不包含 B，用符号

$$B\not\subset A \quad 或是 \quad A\not\supset B$$

来表示.

注意：空集合被认为是任何集合的子集.

定义 若集合 B 是集合 A 的子集，而且至少有一个 A 的元不属于 B，我们就说，B 是 A 的**真子集**；不然的话，我们说，B 不是 A 的真子集.

若集合 A 和集合 B 所包含的元完全一样，那么 A 和 B 表示的

是同一集合，这时我们说，A 等于 B，用符号

$$A=B$$

来表示. 显然

$$A=B\Longleftrightarrow A\subset B, B\subset A$$

一个元 a 若同时属于 A 和 B 两个集合，我们说，a 是 A 和 B 的共同元.

定义 集合 A 和集合 B 的所有共同元所组成的集合叫做 A 和 B 的**交集**.

A 和 B 的交集我们用符号

$$A\cap B$$

来表示.

例 1 $A=\{1,2,3\}, B=\{2,5,6\}$. 那么

$$A\cap B=\{2\}$$

$A=\{1,2,3\}, B=\{4,5,6\}$. 那么

$$A\cap B=\text{空集合}$$

这里，我们看到空集合这个概念的用处.

定义 由至少属于集合 A 和 B 之一的一切元素组成的集合叫做 A 和 B 的**并集**.

A 和 B 的并集我们用符号

$$A\cup B$$

来表示.

例 2 $A=\{1,2,3\}, B=\{2,4,6\}$. 那么

$$A\cup B=\{1,2,3,4,6\}$$

$A=\{1,2,3\}, B=\{4,5,6\}$. 那么

$$A\cup B=\{1,2,3,4,5,6\}$$

两个以上的集合 A_1, $A_2\cdots$ 的交集、并集的定义和上面完全类似.

定义 令$A_1, A_2, \cdots, A_n$是n个集合. 由一切从$A_1, A_2, \cdots, A_n$里顺序取出的元素组$(a_1, a_2, \cdots, a_n)$ $(a_i \in A_i)$所做成的集合叫做**集合** $A_1, A_2, \cdots, A_n$ **的积**, 记成

$$A_1 \times A_2 \times \cdots \times A_n$$

习 题

1. $B \subset A$, 但B不是A的真子集, 这个情况什么时候才能出现? $A = B$
2. 假定$A \subset B$. $A \cap B = A$ $A \cup B = B$

§2. 映 射

在高等代数里已经看到映射这一概念的重要性. 现在我们给出这一概念的一个比较一般的定义.

我们看n个集合$A_1, A_2, \cdots, A_n$和另外一个集合D.

定义 假如通过一个法则ϕ, 对于任何一个$A_1 \times A_2 \times \cdots \times A_n$的元$(a_1, a_2, \cdots, a_n)$$(a_i \in A_i)$, 都能得到一个唯一的$D$的元$d$, 那么这个法则$\phi$叫做集合$A_1 \times A_2 \times \cdots \times A_n$到集合$D$的一个**映射**; 元$d$叫做元$(a_1, a_2, \cdots, a_n)$在映射$\phi$之下的**象**; 元$(a_1, a_2, \cdots, a_n)$叫做元$d$在$\phi$下的一个**逆象**.

一个映射我们常用以下符号来描写,

$$\phi: \quad (a_1, a_2, \cdots, a_n) \longrightarrow d = \phi(a_1, a_2, \cdots, a_n)$$

这里, ϕ代表所给的法则, 也就是所给的映射;

$$(a_1, a_2, \cdots, a_n) \longrightarrow d$$

表示ϕ替$(a_1, a_2, \cdots, a_n)$这个元规定的象是d; 至于$\phi(a_1, a_2, \cdots, a_n)$只是一个符号, 就是说, 我们有时把$d$这个元写成$\phi(a_1, a_2, \cdots, a_n)$. 但这个符号也不是毫无意义的. 这个符号暗示, d是把ϕ应用到$(a_1, a_2, \cdots, a_n)$上所得的结果.

在以上的定义中, 有几点应该特别加以注意, 我们用下面的几

个例来说明一下.

例 1 $A_1=A_2=\cdots=A_n=D=$所有实数作成的集合.

ϕ: $(a_1,a_2,\cdots,a_n)\longrightarrow a_1^2+a_2^2+\cdots+a_n^2=\phi(a_1,a_2,\cdots,a_n)$

是一个 $A_1\times A_2\times\cdots\times A_n$ 到 D 的映射. 这里, A_i 和 D 都是相同的集合, 但这没有什么关系, 因为映射的定义并没有说, $A_1,A_2,\cdots,A_n$, D 这几个集合中不许有相同的.

例 2 $A_1=\{$东, 西$\}$, $A_2=\{$南$\}$, $D=\{$高, 低$\}$.

ϕ_1: (西, 南)$\longrightarrow$高$=\phi_1$(西, 南)

不是一个 $A_1\times A_2$ 到 D 的映射. 因为, 这个 ϕ_1 只替(西, 南)这一个元规定了一个象; 但我们从 $A_1\times A_2$ 里还可以取出另一个元来, 就是(东, 南), 替这一个元, ϕ_1 并没有规定什么象. 这和定义中一个映射必须替每一个元规定一个象的要求不合.

假如 ϕ_2 是如下的一个法则

ϕ_2: (西, 南)$\longrightarrow$高, (东, 南)$\longrightarrow$低

那么 ϕ_2 是一个 $A_1\times A_2$ 到 D 的映射.

在例 1 里, $A_1=A_2=\cdots=A_n$. 对于那里的映射 ϕ 来说, A_i 的次序没有什么关系, 比方说, ϕ 也是 $A_2\times A_1\times\cdots\times A_n$ 到 D 的映射. 但对例 2 里的映射 ϕ_2 来说, A_1 和 A_2 的次序不能变动, ϕ_2 不是一个 $A_2\times A_1$ 到 D 的映射. 因为 ϕ_2 只替(西, 南)和(东, 南)各规定了一个象, 但并没有替(南, 西)和(南, 东)规定什么象.

例 3 $A_1=D=$所有实数作成的集合.

ϕ: $a\longrightarrow a$, 若是 $a\neq 1$

$1\longrightarrow b$, 这里 $b^2=1$

不是一个 A_1 到 D 的映射. 因为, 这个 ϕ 固然替每一个不等于 1 的 a 规定了一个唯一的象; 但通过这个 ϕ, 我们不能决定 b 是 1 还是 -1, 这就是说, ϕ 没有替 1 规定一个唯一的象; 这是与定义不合的.

例 4 $A_1=D=$所有正整数作成的集合.

ϕ: $\qquad a\longrightarrow a-1$

不是一个 A_1 到 D 的映射. 因为这个 ϕ 固然替每一个 $a\neq 1$ 规定了一个唯一的值 $a-1$; 但当 $a=1$ 的时候, $a-1\bar{\in}D$: 这是与定义不合的.

总括起来说, 我们对于映射的定义应当注意以下几点:

1. 集合 $A_1, A_2, \cdots, A_n, D$ 中可能有几个是相同的;
2. 一般, $A_1, A_2, \cdots, A_n$ 的次序不能掉换;
3. 映射 ϕ 一定要替每一个元 $(a_1, a_2, \cdots, a_n)$ 规定一个象 d;
4. 一个元 $(a_1, a_2, \cdots, a_n)$ 只能有一个唯一的象;
5. 所有的象都必须是 D 的元.

给了集合 $A_1, A_2, \cdots, A_n, D$, 一般来说, 有各种不同的法则可以替每一个元 $(a_1, a_2, \cdots, a_n)$ 规定一个象. 有时两个法则虽然不同, 但它们替每一个元所规定的象却永远相同.

定义 我们说, $A_1\times A_2\times\cdots\times A_n$ 到 D 的两个映射 ϕ_1 和 ϕ_2 是相同的, 假如对于任何一个元 $(a_1, a_2, \cdots, a_n)$ 来说,

$$\phi_1(a_1, a_2, \cdots, a_n)=\phi_2(a_1, a_2, \cdots, a_n)$$

我们所以这样规定的原因是, 两个映射本身是不是相同对于我们并不重要, 重要的是它们的效果是不是相同.

例 5 $A=D=$所有正整数的集合.

ϕ_1: $\qquad a\longrightarrow 1=\phi_1(a)$

ϕ_2: $\qquad a\longrightarrow a^0=\phi_2(a)$

这里替每一个 a 规定象的法则, 换一句话说, 我们的映射, 本身并不相同. 但照我们的定义这两个映射是相同的.

习 题

1. $A=\{1, 2, 3, \cdots, 100\}$. 找一个 $A\times A$ 到 A 的映射.

2. 在你为习题1所找到的映射之下，是不是A的每一个元都是$A\times A$的一个元的象？

§3. 代数运算

在本章开头已经说过，我们要研究带有运算的集合. 现在我们利用映射的概念，来定义代数运算这一个概念. 我们看两个集合A, B和另一个集合D.

定义 一个$A\times B$到D的映射叫做一个$A\times B$到D的**代数运算**.

按照我们的定义，一个代数运算只是一种特殊的映射. 在一般映射的定义里，一方面有n个集合$A_1, A_2, \cdots, A_n$出现，另一方面有一个集合D出现，这里n可以是任何正整数. 假如我们有一个特殊的映射，它一方面只和两个集合A, B，另一方面和一个集合D发生关系，就把它叫做一个代数运算. 让我们看一看，为什么把这样的一个特殊映射叫做代数运算. 假定我们有一个$A\times B$到D的代数运算，按照定义，给了一个A的任意元a和一个B的任意元b，就可以通过这个代数运算，得到一个D的元d. 我们也可以说，所给代数运算能够对a和b进行运算，而得到一个结果d. 这正是普通的计算法的特征，比方说，普通加法也不过是能够把任意两个数加起来，而得到另一个数.

代数运算既是一种特殊的映射，描写它的符号，也可以特殊一点. 一个代数运算我们用$\circ$来表示，用以前的符号，就可以写

$$\circ:\quad (a,b)\longrightarrow d=\circ(a,b)$$

我们说过，$\circ(a,b)$完全是一个符号，现在为方便起见，不写$\circ(a,b)$，而写$a\circ b$. 这样，我们描写代数运算的符号，就变成

$$\circ:\quad (a,b)\longrightarrow d=a\circ b$$

我们举几个例.

例 1 $A=\{$所有整数$\}$，$B=\{$所有不等于零的整数$\}$，$D=\{$所有有理数$\}$.

$\circ$：
$$(a,b)\longrightarrow\frac{a}{b}=a\circ b$$
是一个 $A\times B$ 到 D 的代数运算，也就是普通的除法.

例 2 令 V 是数域 F 上一个向量空间. 那么 F 的数与 V 的向量间的乘法是一个 $F\times V$ 到 V 的代数运算.

例 3 $A=\{1\}$，$B=\{2\}$，$D=\{$奇，偶$\}$.

$\circ$：
$$(1,2)\longrightarrow\text{奇}=1\circ 2$$
是一个 $A\times B$ 到 D 的代数运算.

例 4 $A=\{1,2\}$，$B=\{1,2\}$，$D=\{$奇，偶$\}$.

$\circ$：
$$(1,1)\longrightarrow\text{奇}，\ (2,2)\longrightarrow\text{奇}$$
$$(1,2)\longrightarrow\text{奇}，\ (2,1)\longrightarrow\text{偶}$$
是一个 $A\times B$ 到 D 的代数运算.

注意：跟一般映射的情形一样，当 $A=B$ 的时候，A,B 的次序对于一个 $A\times B$ 到 D 的代数运算来说没有什么关系，一个 $A\times B$ 到 D 的代数运算也是一个 $B\times A$ 到 D 的代数运算. 但 A 和 B 的次序可以掉换并不是说，对于 A 的任意元 a，B 的任意元 b，有
$$a\circ b=b\circ a$$
因为 A 和 B 的次序可以掉换只是说，$a\circ b$ 和 $b\circ a$ 都有意义，并不是说，$a\circ b=b\circ a$. 比方说，例 4 的 A,B 就是相等的集合，但
$$1\circ 2=\text{奇}$$
$$2\circ 1=\text{偶}$$

在 A 和 B 都是有限集合的时候，一个 $A\times B$ 到 D 的代数运算，我们常用一个表，叫做运算表来说明. 假定 A 有 n 个元 $a_1,\cdots,a_n$，B 有 m 个元 $b_1,\cdots,b_m$，

$\circ$：
$$(a_i,b_j)\longrightarrow d_{ij}$$
是所给的代数运算. 我们先画一垂线，在这垂线上端画一向右的

横线．把A的元$a_1, a_2, \cdots, a_n$依次写在垂线的左边，把B的元$b_1, b_2, \cdots, b_m$依次写在横线的上边，然后把对a_i和b_j进行运算后所得结果d_{ij}写在从a_i右行的横线和从b_j下行的垂线的交点上：

	b_1	b_2	$\cdots$	b_m
a_1	d_{11}	d_{12}	$\cdots$	d_{1m}
a_2	d_{21}	d_{22}	$\cdots$	d_{2m}
$\vdots$		$\cdots\cdots\cdots\cdots$		
a_n	d_{n1}	d_{n2}	$\cdots$	d_{nm}

比方说，例4的代数运算的运算表是

	1	2
1	奇	奇
2	偶	奇

用运算表来说明一个代数运算，常比用箭头或用等式的方法省事，并且清楚．

$A\times B$到D的一般代数运算用到的时候比较少．最常用的代数运算是$A\times A$到A的代数运算．在这样的一个代数运算之下，可以对A的任意两个元加以运算，而且所得结果还是在A里面．所以我们有

定义 假如$\circ$是一个$A\times A$到A的代数运算，我们就说，集合A对于代数运算$\circ$来说是闭的，也说，$\circ$是A的代数运算或**二元运算**．

习　题

1．$A=\{$所有不等于零的偶数$\}$．找一个集合D，使得普通除法是$A\times A$到D的代数运算．是不是找得到一个以上的这样的D？

2．$A=\{a, b, c\}$．规定A的两个不同的代数运算．

§4. 结 合 律

从上一节的3,4两例,我们可以看出,一个代数运算是可以相当任意规定的,并不一定有多大意义. 假如我们任意取几个集合,任意给它们规定几个代数运算,我们很难希望,可以由此算出什么好的结果来. 所以以下将遇到的代数运算都适合某些从实际中来的规律. 常见的这种规律的第一个,就是结合律.

我们看一个集合 A,一个 $A\times A$ 到 A 的代数运算 $\circ$.

在 A 里任意取出三个元 a,b,c 来,假如我们写下符号

$$a\circ b\circ c$$

那么这个符号没有什么意义,因为代数运算只能对两个元进行运算. 但是我们可以先对 a 和 b 进行运算,而得到 $a\circ b$,因为 $\circ$ 是 $A\times A$ 到 A 的代数运算,$a\circ b\in A$,所以我们又可以把这个元同 c 来进行运算,而得到一个结果. 这样得来的结果,普通用加括号的方法来表示,所用的步骤也就叫做加括号的步骤. 由上面所描写的步骤得来的结果,用加括号的方法写出来,就是

$$(a\circ b)\circ c$$

但我们还有另外一种加括号的步骤,它的结果用加括号的方法写出来是

$$a\circ(b\circ c)$$

在一般情形之下,由这两个不同的步骤所得的结果也未必相同. 我们举一个例.

例 $A=\{$所有整数$\}$. 代数运算是普通减法. 那么

$$(a-b)-c\neq a-(b-c),\quad \text{除非 } c=0$$

现在我们下一个

定义 我们说,一个集合 A 的代数运算 $\circ$ 适合**结合律**,假如对于 A 的任何三个元 a,b,c 来说,都有