近世代数基础

張禾瑞著

商务印書館

近世代数基础

張禾瑞著

（修訂本）

商务印書館

近 世 代 数 基 础

張 禾 瑞 著

商 务 印 書 館 出 版
北京东总布胡同 10 号
（北京市書刊出版業营業許可證出字第 107 号）
新 华 書 店 总 經 售
京华印書局印刷　第五裝訂生产合作社裝訂
統一書号 13017·175

1952 年 9 月初版	開本 850×1168 $^{1}/_{32}$
1958 年 7 月 5 版（修訂本）	字數 125,000
1958 年 7 月北京第 1 次印刷	印數 8,501—13,500
印張 5 $^{6}/_{16}$	定價（10）¥ 0.85

序

(一)本書根据 1947—48, 1949—50 在北京大學教近世代数的材料編成。

(二)本書內容依据中央人民政府教育部 1951 課改草案，只介紹近世代数的初步理論同基本方法。

(三)本書如用作教本，講授所需时間也符合上述草案的規定。

(四)我国数学著作多半用文言文。本書不仅用語体文，并且尽可能用接近口語的語体文。这是作者的一个尝試。效果究竟如何，希望讀者加以批評。

(五)本書只假定讀者有中等数学知識。

(六)作者对于材料的选擇，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論易于了解，对于方法易于掌握，在最短时間內得到閱讀近世代数方面較深書籍或文献的能力。

(七)本書差不多在每一章节开始都有一段小引，說明各該章节在全書里的地位。这些小引能够帮助讀者得到对于本書的全面了解。

(八)本書的例同習題都占極重要的地位；讀者对于例不可忽略，对于習題越多作越好。

(九)本書第一章是全書的基础，讀者必須特別加以注意，細心反复閱讀。这一章的內容虽然比較抽象，由于所包含的实例相当多，据經驗一般大学生都能接受。

(十)本書的加 * 的正文同習題初学者可以略去。

(十一)本書談到前面定理，若是只說明定理数目，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)本書用符号 $A \Longrightarrow B$ 表明由 A 可以得 B, $A \rightleftarrows B$ 表明由 A 可以得 B, 由 B 可以得 A。

(十三)本書材料多取自各国在这一方面的标准著作，書名我不在这里一一列举了。

(十四)孙树本教授曾試教本書初稿，魏执权同志在本書的文字方面提了很多宝貴的意見，施惟樞同志在本書的抄写校对方面帮了我很大的忙。我在这里謝謝他們。

張禾瑞

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，我們計算的对象是数目，計算的方法是加、减、乘、除。数学漸漸进步，我們發現，我們可以对于若干不是数目的东西，用些个类似普通計算法的方法来加以計算。这种例子越来越多，于是我們感覚到，只計算数目，而且只用加、减、乘、除来計算数目，实在有一点作茧自縛。近世代数就由这一个覚悟产生出来。在近世代数里，計算的对象不限于数目，計算的方法也不限于普通加、减、乘、除：以求能够得到尽可能一般的結果。这是近世代数与普通代数根本不同的地方。經过了这个根本的改变，近世代数里所用的方法，也就跟普通代数的方法有很大的不同。在这一章里，我們首先要把在近世代数里常用到的基本概念認識一下。

§1. 集合

在近世代数里，我們計算的对象是多方面的，可以是些个数，可以是些个函数，可以是一个平面的繞着一个定点的若干旋轉，也可以是其他的东西。为着不受束縛起見，我們替我們的計算对象起一个抽象的名字，叫作元素(有时就叫作元)。其实我們不用这个名字，而干干脆脆地說，我們的計算对象是些个东西，也未始不可。不过我們用这样一个特殊的名字，也沒有什么关系。在某种情形之下，比方說，在举例的时候，我們也常說明我們的元素是什么具体的东西。但一般，我們只說我們的計算对象是些个元素。

在我們的討論里，常有同时考察几組元素的必要。一組元素我們把它叫作一个集合。說詳細一点：

若干个(有限或無限多个)固定元素的全体，叫作一个集合。

这样，我們以后的計算，是在若干个集合里来进行的。集合是我們的討論所离不开的一个概念。

关于集合，我們常用到几个名詞同符号，現在把它們説明一下。

首先我們要規定空集合这一个名詞。

定义 一个沒有元素的集合叫作空集合。

空集合好像沒有什么意义，但我們的确有用得到这个概念的地方。这一点我們不久就会看到。

元素我們一般用小写字母 $a, b, c, \cdots$ 来表示，集合用大写字母 $A, B, C, \cdots$ 来表示。一个集合 A 若是由元素 $a, b, c\cdots$ 作成的，我們用符号

$$A: a, b, c, \cdots$$

来表示。

若是 a 是集合 A 的一个元素，我們説，a 屬于 A，或是説，A 包含 a，用符号

$$a \in A, \text{ 或是 } A \ni a$$

来表示。

若是 a 不是集合 A 的元素，我們説，a 不屬于 A，或是説，A 不包含 a，用符号

$$a \overline{\in} A, \text{ 或是 } A \overline{\ni} a$$

来表示。

定义 若是集合 B 的每一个元都屬于集合 A，我們説，B 是 A 的部分集合；不然的話，我們説，B 不是 A 的部分集合。

B 是 A 的部分集合，我們説，B 屬于 A，或者説，A 包含 B，用符号

$$B \subseteq A, \text{ 或是 } A \supseteq B$$

来表示。B 不是 A 的部分集合，我們説，B 不屬于 A，或是説，A

不包含 B，用符号

$$B \not\subseteq A,\ 或是\ A \not\supseteq B$$

来表示。

注意：空集合是任何集合的部分集合。

定义 若是集合 B 是集合 A 的部分集合，而且至少有一个 A 的元不属于 B，我們說，B 是 A 的眞正部分集合；不然的話，我們說，B 不是 A 的眞正部分集合。

B 是 A 的眞正部分集合，我們用符号

$$B \subset A,\ 或是\ A \supset B$$

来表示。B 不是 A 的眞正部分集合，我們用符号

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

来表示。

若是集合 A 同集合 B 所包含的元完全一样，那么 A 同 B 表示的是同一集合，这时，我們說，A 等于 B，用符号

$$A = B$$

来表示。显然 $A = B \rightleftarrows A \subseteq B,\ B \subseteq A.$

一个元 a 若是同时属于 A, B 两个集合，我們說 a 是 A, B 的共同元。

定义 集合 A 与集合 B 的所有共同元所作成的集合，叫作 A 与 B 的相交集合。

A 与 B 的相交集合我們用符号

$$A \cap B$$

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，

$$A \cap B = 空集合。$$

这里，我們看到空集合这个概念的用处。

定义 由至少屬于集合 A 与 B 之一的一切元素組成的集合叫作集合 A 与 B 的联合集合。

A 与 B 的联合集合我們用符号

$$A \cup B$$

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 $A_1 A_2, \cdots$ 的相交集合同联合集合的定义同上面完全类似。

習 題

1. $B \not\subseteq A$, $B \subseteq A$ 什么时候才能成立？

2. 假定 $A \subseteq B$, $A \cap B =$？ $A \cup B =$？

§2. 函数

在上一节已經說过，我們以后要在若干个集合里来計算。要計算，就需要有計算的方法，計算的方法我們把它叫作代数运算。以下我們首先要作的事，就是要規定，什么叫作代数运算。要作到这一点，最好是用一般函数的概念。函数这一个概念我們在其他的地方也还要用到。

我們看 n 个集合 $A_1, A_2, \cdots, A_n$ 同另外一个集合 D。

定义 一个法則 ϕ 叫作一个 $A_1 A_2 \cdots A_n$ 到 D 里面的函数，假如我們能够經由这个法則，对于任何一組从 $A_1, A_2, \cdots, A_n$ 里順序取出来的元 $a_1, a_2, \cdots, a_n (a_i \in A_i)$ 得到一个惟一的 D 的元 d。这时，d

叫作 $a_1, a_2, \cdots, a_n$ 这一組元在函数 ϕ 之下的值。

一个函数我們常用以下符号来描写，

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

这里，ϕ 代表我們的規則，也就是我們的函数；

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

表示 ϕ 替 $(a_1, \cdots, a_n)$ 这一組元規定的値是 d；至于 $\phi(a_1, \cdots, a_n)$ 只是一个符号，就是說，我們有时也把 d 这个元写作 $\phi(a_1, \cdots, a_n)$。但这个符号也不是毫無意义的。这个符号暗示，d 是把 ϕ 应用到 $a_1, a_2, \cdots, a_n$ 上所得的結果。

在以上的定义中，有几点应該特別加以注意，我們用下面的几个例来說明一下。

例 1. $A_1 = A_2 = \cdots = A_n = D =$ 所有实数作成的集合。

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

是一个 $A_1A_2\cdots A_n$ 到 D 里面的函数。这里，A_i 同 D 都是相同的集合，但这沒有什么关系，因为我們的定义并沒有說，$A_1, A_2, \cdots, A_n$ 同 D 这几个集合中不許有兩个相同的。

例 2. A_1：东，西；A_2：北；D：山，水。

$$\phi_1: \qquad (\text{东},\text{北}) \longrightarrow \text{水} = \phi_1(\text{东},\text{北})$$

不是一个 A_1A_2 到 D 里面的函数。因为，这个 ϕ_1 只替(东，北)这一組元規定了一个値；但我們从 A_1, A_2 里还可以取出另一組元来，就是(西，北)，替这一組元，ϕ_1 并沒有規定什么値。这与定义中一个函数必須替每一組元規定一个値的要求不合。

假如 ϕ_2 是如下的一个規則，

$$\phi_2: \qquad \begin{aligned} (\text{东},\text{北}) &\longrightarrow \text{水}, \\ (\text{西},\text{北}) &\longrightarrow \text{山}, \end{aligned}$$

那么 ϕ_2 是一个 A_1A_2 到 D 里的函数。

在例 1 里，$A_1 = A_2 = \cdots = A_n$。对于那里的函数 ϕ 来講，A_i 的

次序没有什么关系，比方說，ϕ 也是 $A_2A_1\cdots A_n$ 到 D 里的函数。但对例 2 里的函数 ϕ_2 来講，A_1, A_2 的次序不能变动，ϕ_2 不是一个 A_2A_1 到 D 里的函数。因为，ϕ_2 只替（东，北）以及（西，北）各规定了一个值，但并没有替（北，东）以及（北，西）規定什么值。

例 3. $A_1=D=$所有实数作成的集合。

$$\phi: \quad a \longrightarrow a, \quad \text{若是 } a \neq 1;$$
$$1 \longrightarrow b, \quad \text{这里 } b^2=1$$

不是一个 A_1 到 D 里面的函数。因为，这个 ϕ 固然替每一个不等于 1 的 a 規定了一个惟一的値；但由于这个 ϕ，我們不能决定 b 是 1 还是 -1，这就是說，ϕ 没有替 1 規定一个惟一的値：这是与定义不合的。

例 4. $A_1=D=$所有正整数作成的集合。

$$\phi: \quad a \longrightarrow a-1$$

不是一个 A_1 到 D 里面的函数。因为这个 ϕ 固然替每一个 $a\neq 1$ 規定了一个惟一的値 $a-1$；但当 $a=1$ 的时候，$a-1 \overline{\in} D$：这是与定义不合的。

总括起来說，我們对于函数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，$A_1A_2, \cdots, A_n$ 的次序不能掉换；
3. 函数 ϕ 一定要替每一組元 $(a_1, a_2, \cdots, a_n)$ 規定一个値 d；
4. 一組元 $(a_1, a_2, \cdots, a_n)$ 只能有一个惟一的値；
5. 所有的値都必須是 D 的元。

給了一个 $A_1A_2\cdots A_n$ 到 D 里面的函数 ϕ，D 的元未必被 ϕ 用光，換一句話說，D 的某些个元可能不是任何一組元 $a_1, \cdots, a_n$ 的値，比方說，在第一例里 D 的負数就不是任何 $a_1, \cdots, a_n$ 的値。但在特殊函数之下，当然可能 D 的每一个元都是某些 $a_1, \cdots, a_n$ 的値，比方說，例 2 的函数就有这个性質。这种特殊的函数对于我們

非常重要，我們給它一个名字。

定义 一个 $A_1\cdots A_n$ 到 D 里面的函数叫作一个 $A_1\cdots A_n$ 到 D 上面的函数，假如 D 的每一个元 d 都至少是某一組元 $a_1, \cdots, a_n$ 的值。

我們再举一个例。

例 5. $A_1=A_2=\cdots=A_n=$所有实数作成的集合，

$D=$所有大于或等于零的实数作成的集合。

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

是一个 $A_1A_2\cdots A_n$ 到 D 上面的函数。

給了集合 $A_1, A_2, \cdots A_n, D$，一般来講，有各种不同的法則可以替每一組元 $a_1, a_2, \cdots, a_n$ 規定一个值。有时两个法則虽然不同，但它們替每一組元所規定的值却永远相同。

定义 我們說，$A_1A_2\cdots A_n$ 到 D 里面的两个函数 ϕ_1, ϕ_2 是相同的，假如对于任何一組元 $a_1, a_2, \cdots, a_n$ 来講，

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

我們所以这样規定的原因是，两个函数本身是不是相同对于我們并不重要，重要的是它們的效果是不是相同。

例 6. $A=D=$所有正整数的集合。

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

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

这里替每一个 a 規定值的法則，换一句話說，我們的函数，本身并不相同。但照我們的定义这两个函数是相同的。

習　題

1. A：1, 2, 3, …, 100。找一个 AA 到 A 里面的函数。

2. 你在習題 1 里所找到的函数是不是 AA 到 A 上面的函数？

§3. 代数运算

有了函数的概念，我們很容易規定代数运算这一个概念。我們看兩个集合 A, B 同另外一个集合 D。

定义 一个 AB 到 D 里面的函数，叫作一个 AB 到 D 里面的代数运算。

按照我們的定义，一个代数运算只是一种特殊的函数。在一般函数的定义里，一方面有 n 个集合 $A_1, A_2, \cdots, A_n$ 出現，另一方面有一个集合 D 出現，这里 n 可以是任何正整数。假如我們有一个特殊的函数，他一方面只同兩个集合 A, B，另一方面同一个集合 D 發生关系，我們就把它叫作一个代数运算。讓我們看一看，我們为什么要把这样的一个特殊函数叫作代数运算。假定我們有一个 AB 到 D 的代数运算；按照我們的定义，給了一个 A 的任意元 a，一个 B 的任意元 b，就可以由于我們的代数运算，得到一个 D 里的元 d。我們也可以說，我們的代数运算能够把 a 同 b 結合起来，而得到一个結果 d。这正是普通的計算法的特征，比方說，普通加法也不过是能够把任意兩个数加起来，而得到另一个数。

代数运算既是一种特殊的函数，我們描写它的符号，也可以特殊一点。一个代数运算我們用 $\circ$ 来表示，用以前的符号，我們可以写

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

我們說过，$\circ(a, b)$ 完全是一个符号；現在我們为方便起見，不写 $\circ(a, b)$，而写 $a \circ b$ 这样，我們描写代数运算的符号，就变成

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

我們举几个例。

例 1. A：所有整数；B：所有不等于零的整数；D：所有有理数。

$$\circ: \qquad (a, b) \longrightarrow \frac{a}{b} = a \circ b$$

是一个 AB 到D里的代数运算，也就是普通的除法。

例 2. A ∶ 1；B ∶ 2；D ∶ 奇，偶。

$$\circ: \qquad (1, 2) \longrightarrow 奇 = 1 \circ 2$$

是一个 AB 到D里的代数运算。

例 3. A ∶ 1, 2；B ∶ 1, 2；D ∶ 奇偶。

$$\circ: \qquad \begin{aligned} &(1, 1) \longrightarrow 奇, \\ &(2, 2) \longrightarrow 奇, \\ &(1, 2) \longrightarrow 奇, \\ &(2, 1) \longrightarrow 偶。 \end{aligned}$$

是一个 AB 到D里的代数运算。

注意：跟一般函数的情形一样，当 $A=B$ 的时候，A, B 的次序对于一个 AB 到D的代数运算来講沒有什么关系：一个 AB 到D的代数运算也是一个 BA 到D的代数运算。但A同B的次序可以掉换并不是說，对于A的任意元 a, B 的任意元 b 来講，

$$a \circ b = b \circ a.$$

因为A同B的次序可以掉换只是說，$a \circ b$ 同 $b \circ a$ 都有意义，并不是說，$a \circ b = b \circ a$。比方說，例 3 的 A, B 就是相等的集合，但

$$1 \circ 2 = 奇,$$
$$2 \circ 1 = 偶。$$

在A同B都是有限集合的时候，一个 AB 到D的代数运算，我們常用一个表，叫作結合表，来說明。假定A有 n 个元 $a_1, \cdots, a_n$，B 有 m 个元 $b_1, \cdots, b_m$，

$$\circ: \qquad (a_i, b_j) \longrightarrow d_{ij}$$

是我們的代数运算。我們先画一垂綫，在这垂綫上端画一向右的横綫。我們把A的元 $a_1, a_2, \cdots, a_n$ 依次写在垂綫的左边，把B的元

$b_1, b_2, \cdots, b_m$ 依次写在横綫的上边，然后把 a_i 同 b_j 結合后的值 b_{ij} 写在从 a_i 右行以及 b_j 下行的兩条綫的交点上：

$$\begin{array}{c|cccc} & b_1 & b_2 & \cdots & b_m \\ \hline a_1 & d_{11} & d_{12} & \cdots & d_{1m} \\ a_2 & d_{21} & d_{22} & \cdots & d_{2m} \\ \vdots & \cdots & \cdots & \cdots & \cdots \\ a_n & d_{n1} & d_{n2} & \cdots & d_{nm}. \end{array}$$

比方說，例 3 的代数运算的結合表是

$$\begin{array}{c|cc} & 1 & 2 \\ \hline 1 & 奇 & 奇 \\ 2 & 偶 & 奇. \end{array}$$

用結合表来說明一个代数运算，常比用箭头或用等式的方法省事，并且清楚。

AB 到 D 的一般代数运算用到的时候比較少。我們最常用的代数运算是 AA 到 A 的代数运算。在这样的一个代数运算之下，A 的任意兩个元可以被結合起来，而且所得的值还是在 A 里面。所以我們有

定义 假如 $\circ$ 是一个 AA 到 A 里面的代数运算，我們說，集合 A 对于代数运算 $\circ$ 来講是关閉的，或是說，$\circ$ 是 A 的代数运算。

習 題

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

2. A：a, b, c。規定兩个不同的 AA 到 A 里的代数运算。