大學叢書

近世代數基礎

張禾瑞著

商務印書館出版

序

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

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

（三） 本書如用作教本，講授所需時間也符合上述草案的規定。

（四） 我國數學著作多半用文言文。本書不僅用語體文，並且儘可能用接近口語的語體文。這是作者的一個嘗試。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數學知識。

（六） 作者對於材料的選擇，分佈與處理，都曾加以特殊的注意。希望因此可以使初學者對於理論易於了解，對於方法易於掌握，在最短時間內得到閱讀近世代數方面較深書籍或文獻的能力。

（七） 本書差不多在每一章節開始都有一段小引，說明各該章節在全書裏的地位。這些小引能够幫助讀者得到對於本書的全面了解。

（八） 本書的例同習題都佔極重要的地位；讀者對於例不可忽略，對於習題越多作越好。

（九） 本書第一章是全書的基礎，讀者必須特別加以注意，細心反覆閱讀。這一章的內容雖然比較抽象，由於所包含的實例相當多，

據經驗一般大學生都能接受。

（十） 本書的加 * 的正文同習題初學者可以略去。

（十一） 本書談到前面定理，若是只說明定理數目，指的是本節的定理，若是加有其他數目，指的是其他章節的定理。如 II,3, 定理 1 指的是第二章第三節的定理 1。

（十二） 本書用符號 $A\Longrightarrow B$ 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） 本書材料多取自各國在這一方面的標準著作，書名我不在這裏一一列舉了。

（十四） 孫樹本教授曾試教本書初稿，魏執權同志在本書的文字方面提了很多可寶貴的意見，施惟樞同志在本書的抄寫校對方面幫了我很大的忙。我在這裏謝謝他們。

張禾瑞

北京大學，一九五二年，一月。

目　錄

第一章　基本概念 …… 1

1. 集合 …… 1
2. 函數 …… 5
3. 結合法 …… 9
4. 結合律 …… 12
5. 交換律 …… 15
6. 分配律 …… 17
7. 對應、變換 …… 19
8. 同態對應 …… 24
9. 同構對應、自同構對應 …… 28
10. 等價關係與集合的分類 …… 32

第二章　羣　論 …… 38

1. 羣的定義 …… 38
2. 恆等元、逆元、消去律 …… 43
3. 有限羣的另一定義 …… 47
4. 羣的同態對應 …… 49
5. 變換羣 …… 53
6. 排列羣 …… 60
7. 循環羣 …… 66

8. 子羣……72
9. 子羣的陪集……76
10. 不變子羣、商羣……83
11. 同態對應與不變子羣……88
12.* 規則的等價關係……94

第三章 環與體……100

1. 加羣、環的定義……100
2. 交換律、單位元、零除元、整域……105
3. 除環、體……111
4. 無零除元環的特徵數……115
5. 子環、環的同態對應……119
6. 多項式環……124
7.* 矩陣環……133
8. 理想子環……139
9. 剩餘類環、同態對應與理想子環……144
10. 最大理想子環……148
11. 商體……151

第四章 整域裏的因子分解……158

1. 素元、單一分解……158
2. 單一分解域……164
3. 主理想子環域……170
4. 歐氏環……174
5. 多項式環的因子分解……177
6. 因子分解與多項式的根……185

近世代數基礎

第一章　基本概念

在普通代數裏，我們計算的對象是數目，計算的方法是加、減、乘、除。數學漸漸進步，我們發現，我們可以對於若干不是數目的東西，用些個類似普通計算法的方法來加以計算。這種例子越來越多，於是我們感覺到，只計算數目，而且只用加、減、乘、除來計算數目，實在有一點作繭自縛。近世代數就由這一個覺悟產生出來。在近世代數裏，計算的對象不限於數目，計算的方法也不限於普通加、減、乘、除：以求能够得到儘可能一般的結果。這是近世代數與普通代數根本不同的地方。經過了這個根本的改變，近世代數裏所用的方法，也就跟普通代數的方法有很大的不同。在這一章裏，我們首先要把在近世代數裏常用到的基本概念認識一下。

§1. 集　合

在近世代數裏，我們計算的對象是多方面的，可以是些個數，可以是些個函數，可以是一個平面的繞着一個定點的若干旋轉，也可以是其他的東西。爲着不受束縛起見，我們替我們的計算對象起一個

抽象的名字，叫作元素(有時就叫作元)。其實我們不用這個名字，而乾乾脆脆地說，我們的計算對象是些個東西，也未始不可。不過我們用這樣一個特殊的名字，也沒有什麼關係。在某種情形之下，比方說，在舉例的時候，我們也常說明我們的元素是什麼具體的東西。但一般，我們只說我們的計算對象是些個元素。

在我們的討論裏，常有同時考察幾組元素的必要。一組元素我們把它叫作一個集合。說詳細一點：

定義 若干個(有限或無限多個)固定元素的全體，叫作一個集合。

這樣，我們以後的計算，是在若干個集合裏來進行的。集合是我們的討論所離不開的一個概念。

關於集合，我們常用到幾個名詞同符號，現在把它們說明一下。

首先我們要規定空集合這一個名詞。

定義 一個沒有元素的集合叫作空集合。

空集合好像沒有什麼意義，但我們的確有用得到這個概念的地方。這一點我們不久就會看到。

元素我們一般用小寫字母 $a,b,c,\cdots$ 來表示，集合用大寫字母 $A,B,C,\cdots$ 來表示。一個集合 A 若是由元素 $a,b,c,\cdots$ 作成的，我們用符號

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

來表示。

若是 a 是集合 A 的一個元素，我們說，a 屬於 A，或是說，A 包含 a，用符號

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

來表示。

若是 a 不是集合 A 的元素，我們說，a 不屬於 A，或是說，A 不包含 a，用符號

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

來表示。

定義 若是集合 B 的每一個元都屬於集合 A，我們說，B 是 A 的部份集合；不然的話，我們說，B 不是 A 的部份集合。

B 是 A 的部份集合，我們說，B 屬於 A，或是說，A 包含 B，用符號

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

來表示。B 不是 A 的部份集合，我們說，B 不屬於 A，或是說，A 不包含 B，用符號

$$B \not\subseteq A, \quad \text{或是} \quad A \not\supseteq B$$

來表示。

定義 若是集合 B 是集合 A 的部份集合，而且至少有一個 A 的元不屬於 B，我們說，B 是 A 的眞正部份集合；不然的話，我們說，B 不是 A 的眞正部份集合。

B 是 A 的眞正部份集合，我們用符號

$$B \subset A, \quad \text{或是} \quad A \supset B$$

來表示。B 不是 A 的眞正部份集合，我們用符號

$$B \not\subset A, \quad \text{或是} \quad A \not\supset B$$

來表示。

若是集合 A 同集合 B 所包含的元完全一樣，那麼 A 同 B 表示的是同一集合，這時，我們說，A 等於 B，用符號

$$A=B$$

來表示。顯然，

$$A=B \iff A\subseteq B,\ B\subseteq A。$$

一個元 a 若是同時屬於 A, B 兩個集合，我們說 a 是 A, B 的共同元。

定義 集合 A 與集合 B 的所有共同元所作成的集合，叫作 A 與 B 的相交集合。

A 與 B 的相交集合我們用符號

$$A\cap B$$

來表示。

例 1. A：1,2,3; B：2,5,6。那麼，

$$A\cap B：2。$$

A：1,2,3; B：4,5,6。那麼，

$$A\cap B=空集合。$$

這裏，我們看到空集合這個概念的用處。

定義 一個集合叫作集合 A 與 B 的聯合集合，假如這個集合的每一個元素不屬於 A 卽屬於 B。

A 與 B 的聯合集合我們用符號

$$A\cup B$$

來表示。

例 2. A：1,2,3; B：2,4,6。那麼，

$$A\cup B：1,2,3,4,6。$$

A：1,2,3; B：4,5,6。那麼，

$$A\cup B：1,2,3,4,5,6。$$

兩個以上的集合 $A_1, A_2, \cdots$ 的相交集合同聯合集合的定義同上面完全類似。

習 題

1. $B \subset A$, $B \subseteq A$ 什麼時候才能成立?
2. 假定 $A \subseteq B$, $A \cap B = ?$ $A \cup B = ?$

§2. 函 數

在上一節已經說過，我們以後要在若干個集合裏來計算。要計算，就需要有計算的方法，計算的方法我們把它叫作結合法。以下我們首先要作的事，就是要規定，什麼叫作結合法。要作到這一點，最好是用一般函數的概念。函數這一個概念我們在其他的地方也還要用到。

我們看 n 個集合 $A_1, A_2, \cdots, A_n$ 同另外一個集合 D。

定義 一個法則 ϕ 叫作一個 $A_1 A_2 \cdots A_n$ 到 D 裏面的函數，假如我們能够經由這個法則，對於任何一組從 $A_1, A_2, \cdots, A_n$ 裏順序取出來的元 $a_1, a_2, \cdots, a_n$ $(a_i \in A_i)$ 得到一個惟一的 D 的元 d。這時，d 叫作 $a_1, a_2, \cdots, a_n$ 這一組元在函數 ϕ 之下的值。

一個函數我們常用以下符號來描寫，

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

這裏，ϕ 代表我們的規則，也就是我們的函數；

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

表示 ϕ 替 $(a_1, \cdots, a_n)$ 這一組元規定的值是 d；至於 $\phi(a_1, \cdots, a_n)$ 只是一個符號，就是說，我們有時也把 d 這個元寫作 $\phi(a_1, \cdots, a_n)$。但這個符

號也不是毫無意義的。這個符號暗示，d 是把 ϕ 應用到 $a_1,a_2,\cdots,a_n$ 上所得的結果。

在以上的定義中，有幾點應該特別加以注意，我們用下面的幾個例來說明一下。

例 1. $A_1=A_2=\cdots=A_n=D=$ 所有實數作成的集合。

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

是一個 $A_1A_2\cdots A_n$ 到 D 裏面的函數。這裏，A_i 同 D 都是相同的集合，但這沒有什麼關係，因爲我們的定義並沒有說，$A_1,A_2,\cdots,A_n$ 同 D 這幾個集合中不許有兩個相同的。

例 2. A_1：這，那；A_2：個；A_3：東；A_4：西；D：好，壞。

ϕ_1: (這，個，東，西)$\longrightarrow$好$=\phi_1$(這，個，東，西)

不是一個 $A_1A_2A_3A_4$ 到 D 裏面的函數。因爲，這個 ϕ_1 只替(這，個，東，西)這一組元規定了一個值；但我們從 A_1,A_2,A_3,A_4 裏還可以取出另一組元來，就是(那，個，東，西)；替這一組元，ϕ_1 並沒有規定什麼值。這與定義中一個函數必須替每一組元規定一個值的要求不合。

假如 ϕ_2 是如下的一個規則，

ϕ_2: (這，個，東，西)$\longrightarrow$好，

(那，個，東，西)$\longrightarrow$壞，

那麼 ϕ_2 是一個 $A_1A_2A_3A_4$ 到 D 裏的函數。

在例 1 裏，$A_1=A_2=\cdots=A_n$。對於那裏的函數 ϕ 來講，A_i 的次序沒有什麼關係，比方說，ϕ 也是 $A_2A_1\cdots A_n$ 到 D 裏的函數。但對例 2 裏的函數 ϕ_2 來講，A_1,A_2,A_3,A_4 的次序不能變動，比方說，ϕ_2 不是一個 $A_2A_1A_4A_3$ 到 D 裏的函數。因爲，ϕ_2 只替(這，個，東，西)以

及(那,個,東,西)各規定了一個值，但並沒有替(個,這,西,東)以及(個,那,西,東)規定了什麼值。

例 3. $A_1=D=$ 所有實數作成的集合。

ϕ: $a\longrightarrow a$, 若是 $a\neq 1$;

$1\longrightarrow b$, 這裏 $b^2=1$

不是一個 A_1 到 D 裏面的函數。因爲,這個 ϕ 固然替每一個不等於 1 的 a 規定了一個惟一的值;但由於這個 ϕ,我們不能決定 b 是 1 還是 -1,這就是說，ϕ 沒有替 1 規定一個惟一的值:這是與定義不合的。

例 4. $A_1=D=$ 所有實數作成的集合。

ϕ: $a\longrightarrow +\sqrt{a}$

不是一個 A_1 到 D 裏面的函數。因爲這個 ϕ 固然替每一個 a 規定了一個惟一的值 $+\sqrt{a}$;但當 a 是負數的時候，$+\sqrt{a}\in D$: 這是與定義不合的。

總括起來說,我們對於函數的定義應當注意以下幾點:

1. 集合 $A_1,A_2\cdots,A_n,D$ 中可能有幾個是相同的;
2. 一般，$A_1,A_2,\cdots,A_n$ 的次序不能掉換;
3. 函數 ϕ 一定要替每一組元$(a_1,a_2,\cdots,a_n)$規定一個值 d;
4. 一組元$(a_1,a_2,\cdots,a_n)$只能有一個惟一的值;
5. 所有的值都必須是 D 的元。

給了一個 $A_1A_2\cdots A_n$ 到 D 裏面的函數 ϕ,D 的元未必被 ϕ 用光，換一句話說，D 的某些個元可能不是任何一組元 $a_1,\cdots,a_n$ 的值,比方說,在第一例裏 D 的負數就不是任何 $a_1,\cdots,a_n$ 的值。但在特殊函數之下,當然可能 D 的每一個元都是某些 $a_1,\cdots,a_n$ 的值,比方說,例 2 的函數就有這個性質。這種特殊的函數對於我們非常重要，我們給

它一個名字。

定義 一個 $A_1\cdots A_n$ 到 D 裏面的函數叫作一個 $A_1\cdots A_n$ 到 D 上面的函數，假如 D 的每一個元 d 都至少是某一組元 $a_1,\cdots,a_n$ 的值。

我們再舉一個例。

例 5. $A_1=A_2=\cdots=A_n=$ 所有實數作成的集合，

$D=$ 所有大於或等於零的實數作成的集合。

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

是一個 $A_1A_2\cdots A_n$ 到 D 上面的函數。

給了集合 $A_1,A_2,\cdots A_n,D$，一般來講，有各種不同的法則可以替每一組元 $a_1,a_2,\cdots a_n$ 規定一個值。有時兩個法則雖然不同，但它們替每一組元所規定的值却永遠相同。

定義 我們說，$A_1A_2\cdots A_n$ 到 D 裏面的兩個函數 ϕ_1，ϕ_2 是相同的，假如對於任何一組元 $a_1,a_2,\cdots,a_n$ 來講，

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

我們所以這樣規定的原因是，兩個函數本身是不是相同對於我們並不重要，重要的是它們的效果是不是相同。

例 6. $A=D=$ 所有實數的集合。

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

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

這裏替每一個 a 規定值的法則，換一句話說，我們的函數，本身並不相同。但照我們的定義這兩個函數是相同的。

習 題

1. A：1,2,3,$\cdots$,100。找一個 AA 到 A 裏面的函數。

2. 你在習題 1 裏所找到的函數是不是 AA 到 A 上面的函數?

§3. 結合法

有了函數的概念，我們很容易規定結合法這一個概念。我們看兩個集合 A B 同另外一個集合 D。

定義 一個 AB 到 D 裏面的函數，叫作一個 AB 到 D 裏面的結合法。

按照我們的定義，一個結合法只是一種特殊的函數。在一般函數的定義裏，一方面有 n 個集合 $A_1, A_2, \cdots, A_n$ 出現，另一方面有一個集合 D 出現，這裏 n 可以是任何正整數。假如我們有一個特殊的函數，他一方面只同兩個集合 A, B, 另一方面同一個集合 D 發生關係，我們就把它叫作一個結合法。讓我們看一看，我們爲什麼要把這樣的一個特殊函數叫作結合法。假定我們有一個 AB 到 D 的結合法；按照我們的定義，給了一個 A 的任意元 a，一個 B 的任意元 b，就可以由於我們的結合法，得到一個 D 裏的元 d。我們也可以說，我們的結合法能够把 a 同 b 結合起來，而得到一個結果 d。這正是普通的計算法的特徵，比方說，普通加法也不過是能够把任意兩個數加起來，而得到另一個數。

結合法既是一種特殊的函數，我們描寫它的符號，也可以特殊一點。一個結合法我們用 $\circ$ 來表示，用以前的符號，我們可以寫

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

我們說過，$\circ(a,b)$完全是一個符號；現在我們爲方便起見，不寫$\circ(a,b)$，而寫 $a \circ b$ 這樣，我們描寫結合法的符號，就變成

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

我們舉幾個例。

例1. A：所有整數；B：所有不等於零的整數；D：所有有理數。

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

是一個 AB 到 D 裏的結合法，也就是普通的除法。

例2. A：1；B：2；D：牛，羊。

$\circ$：
$$(1,2)\longrightarrow 牛=1\circ 2$$

是一個 AB 到 D 裏的結合法。

例3. A：1, 2；B：1, 2；D：牛，羊。

$\circ$：
$$(1,1)\longrightarrow 牛,$$
$$(2,2)\longrightarrow 牛,$$
$$(1,2)\longrightarrow 牛,$$
$$(2,1)\longrightarrow 羊$$

是一個 AB 到 D 裏的結合法。

注意：跟一般函數的情形一樣，當 $A=B$ 的時候，A, B 的次序對於一個 AB 到 D 的結合法來講沒有什麼關係：一個 AB 到 D 的結合法也是一個 BA 到 D 的結合法。但 A 同 B 的次序可以掉換並不是說，對於 A 的任意元 a，B 的任意元 b 來講，

$$a\circ b=b\circ a。$$

因爲 A 同 B 的次序可以掉換只是說，$a\circ b$ 同 $b\circ a$ 都有意義，並不是說，$a\circ b=b\circ a$。比方說，例3的 A, B 就是相等的集合，但

$$1\circ 2=牛,$$
$$2\circ 1=羊。$$

在 A 同 B 都是有限集合的時候，一個 AB 到 D 的結合法，我們常用一個表，叫作結合表，來說明。假定 A 有 n 個元 $a_1,\cdots,a_n$，B 有 m 個元 $b_1,\cdots,b_m$，

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

是我們的結合法。我們先畫一垂線，在這垂線上端畫一向右的橫線。我們把 A 的元 $a_1,a_2,\cdots,a_n$ 依次寫在垂線的左邊，把 B 的元 $b_1,b_2,\cdots,b_m$ 依次寫在橫線的上邊，然後把 a_i 同 b_j 結合後的值 d_{ij} 寫在從 a_i 右行以及 b_j 下行的兩條線的交點上：

	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}

比方說，例 3 的結合法的結合表是

	1	2
1	牛	牛
2	羊	牛。

用結合表來說明一個結合法，常比用箭頭或用等式的方法省事，並且清楚。

AB 到 D 的一般結合法用到的時候比較少。我們最常用的結合法是 AA 到 A 的結合法。在這樣的一個結合法之下，A 的任意兩個元可以被結合起來，而且所得的值還是在 A 裏面。所以我們有

定義 假如 $\circ$ 是一個 AA 到 A 裏面的結合法，我們說，集合 A

對於結合法○來講是關閉的，或是說，○是 A 的結合法。

習 題

1. A：所有不等於零的雙數。找一個集合 D，使得普通除法是 AA 到 D 裏的結合法。是不是找得到一個以上的這樣的 D？

2. A：a, b, c。規定兩個不同的 AA 到 A 裏的結合法。

§4. 結 合 律

從上一節的 2,3 兩例，我們可以看出，一個結合法是可以相當任意規定的，並不一定有多大意義。假如我們任意取幾個集合，任意給它們規定幾個結合法，我們很難希望，可以由此算出什麼好的結果來。所以我們對於結合法，需要加以相當的限制，要求它們適合某些合理的規律。常見的這種規律的第一個，就是結合律。

我們看一個集合 A，一個 AA 到 A 的結合法○。

我們在 A 裏任意取出三個元 a, b, c 來。假如我們寫下符號

$$a \circ b \circ c,$$

那麼這個符號沒有什麼意義，因爲我們的結合法只能把兩個元結合起來。但是我們可以先把 a 同 b 結合起來，而得到 $a \circ b$，因爲○是 AA 到 A 的結合法，$a \circ b \in A$，所以我們又可以把這個元同 c 來結合，而得到一個結果。這樣得來的結果，普通用加括弧的方法來表示，所用的步驟也就叫作加括弧的步驟。由我們剛才所描寫的步驟得來的結果，用加括弧的方法寫出來，就是

$$(a \circ b) \circ c。$$

但我們還有另外一種加括弧的步驟，他的結果用加括弧的方法寫出