赵淼清 编著

近世代数

JINSHI DAISHU

浙江大学出版社

近世代数

赵森清 编著

浙江大學出版社

图书在版编目(CIP)数据

近世代数/赵淼清编著. —杭州：浙江大学出版社，2005.8

ISBN 7-308-04428-9

Ⅰ.近... Ⅱ.赵... Ⅲ.抽象代数 Ⅳ.0153

中国版本图书馆CIP数据核字(2005)第096935号

出版发行	浙江大学出版社
	(杭州天目山路148号 邮政编码310028)
	(E-mail：zjupress@sun.zu.edu.cn)
	(网址：http://www.zjupress.com)
责任编辑	沈国明
封面设计	刘依群
排　　版	杭州大漠照排印刷有限公司
印　　刷	杭州杭新印务有限公司
经　　销	浙江省新华书店
开　　本	889mm×1194mm 1/32
印　　张	8.625
字　　数	220千字
版 印 次	2005年8月第1版 2005年8月第1次印刷
书　　号	ISBN 7-308-04428-9/O·329
定　　价	12.00元

前 言

本书主要介绍了近世代数课程的基本内容和思想方法，全书共分五章，分别对群、环、域这三个最基本的代数系统进行了一些讨论。

由于学生在学习近世代数课程时，往往对一些抽象的概念不能很好地理解，因此本书在内容的叙述上力求简洁，对概念的建立与定理的证明尽可能地详细和严谨，使学生能够较好地理解和体会近世代数课程的基本内容和证题方法，同时给出一些具体的例子，以帮助对相关概念和内容的准确掌握和正确理解。

在每节后面都配有一些习题，以帮助学生提高和巩固每个章节的内容。这些习题大部分是比较容易的，对于那些真正掌握基本知识的学生来说，做这些习题应该没有什么困难。

由于编者水平所限，本书定有不妥之处，衷心希望读者指正。

编 者

2005 年 5 月

目　录

第一章　基本概念

近世代数的主要内容是研究所谓的代数系统，即带有代数运算的集合. 本教材主要讨论群、环、域这几个最基本的代数系统. 为了以后学习的便利以及教材的完整性，我们将在这一章中对集合、映射、等价关系、集合分类等几个基本概念作一个简单的介绍. 作为基础知识，这些内容将在以后的学习中经常被用到.

§1.1　集　合

一、集合的概念

在近代数学中，人们已经越来越广泛而深入地用到集合这个最基本的数学概念. 我们给"具有某种特定性质的事物之全体"一个名称，叫做**集合**. 组成一个集合的各个个体事物叫做这个集合的**元素**.

以后我们通常用大写字母 $A,B,C,\cdots$ 等表示集合，而用小写字母 $a,b,c,\cdots$ 等表示集合中的元素. 特别地，用 $\mathbf{N}$ 表示所有自然数所组成的集合（简称**自然数集**），用 $\mathbf{Z}$ 表示所有整数组成的集合（简称**整数集**），用 $\mathbf{Q}$ 表示所有有理数组成的集合（简称**有理数集**），用 $\mathbf{R}$ 表示所有实数组成的集合（简称**实数集**），用 $\mathbf{C}$ 表示所有复数组成的集合（简称**复数集**）. 这些数集合是我们经常用到的，以后如果没有特别的说明，则 $\mathbf{N},\mathbf{Z},\mathbf{Q},\mathbf{R},\mathbf{C}$ 就表示以上所述的数集.

对于一个集合 A 来说，某一事物 x 如果是集合 A 的元素，我们说元素 x 属于集合 A，记为 $x\in A$；如果 x 不是集合 A 的元素，

那么说 x 不属于 A，记为 $x\notin A$. 对于给定的集合 A 来说，任何事物，即元素 x，以上两种情形必居其一. 要确定一个集合 A，就是要明确哪些元素属于 A，而哪些元素不属于 A，即 A 中所含的元素是明确给定的.

设 A,B 是两个集合，如果集合 B 中的每一个元素都属于集合 A（即 $\forall x\in B$，可以得到 $x\in A$），那么，我们说 B 是 A 的**子集**（或称集合 B 包含在集合 A 中，或称集合 A 包含集合 B），记作 $B\subseteq A$.

若集合 B 是集合 A 的子集，而且至少有一个 A 的元素 x 不属于 B，即存在 $x\in A$，但 $x\notin B$，则称 B 是 A 的真子集，记作 $B\subsetneqq A$.

显然，集合的包含关系具有：

(1) 对于任意集合 A，有 $A\subseteq A$；

(2) 对于集合 A,B,C，如果 $A\subseteq B$，$B\subseteq C$，则 $A\subseteq C$.

特别地，当集合中不含任何元素时，我们称其为**空集**，记为 $\varnothing$. 我们规定空集是任何集合的子集.

若集合 A 和集合 B 所包含的元素完全一样，那么我们说集合 A 和 B **相等**，记为 $A=B$. 显然

$$A = B \quad \Leftrightarrow \quad A \subseteq B \text{ 且 } B \subseteq A.$$

如果集合 A 中所含的元素个数是一个有限数，即集合 A 是由有限个元素组成的，则称 A 为**有限集**，空集是有限集；否则称 A 为**无限集**. 集合 A 中的元素个数记为 $|A|$.

二、集合的运算

设 A,B 是任意两个集合，所有属于 A 或属于 B 的元素作成的集合称为 A 与 B 的**并集**，记为 $A\cup B$，即

$$A \cup B = \{x \mid x \in A \text{ 或 } x \in B\};$$

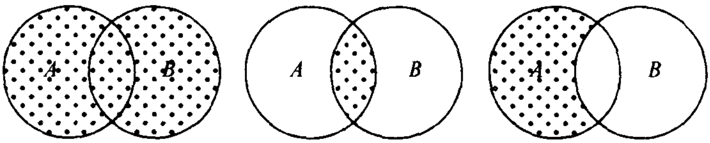
所有既属于 A 又属于 B 的元素作成的集合称为 A 与 B 的**交集**，记为 $A\cap B$，即

$$A \cap B = \{x \mid x \in A \text{ 且 } x \in B\};$$

所有属于 A 而不属于 B 的元素作成的集合称为 A 与 B 的**差集合**,记为 $A-B$,即

$$A - B = \{x \mid x \in A, \text{但 } x \notin B\}.$$

如果集合 A 和 B 给定,那么上述集合的三种运算 $A\cup B$,$A\cap B$,$A-B$ 所得的集合都完全被集合 A 与 B 所确定.关于上述定义的集合运算可用直观的图给出示意(阴影部分即为运算的结果).



$A\cup B$　　　$A\cap B$　　　$A-B$

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

$$A \cup B = \{1,2,3,4,5,6\},$$
$$A \cap B = \{3\}, \quad A - B = \{1,2\}.$$

当 A 作为全集 U 时,$A-B=U-B$ 就是 B 的补集 B'.因此,从某种意义上讲,补集可看作是差集的一种特殊情形.

关于多个集合的并集与交集完全可以用类似于上述方法给出其定义:

设集合族 A_i($i \in I$,其中 I 为某个指标集),则

$$\bigcup_{i\in I} A_i = \{x \mid \text{存在某个 } i \in I, \text{满足 } x \in A_i\};$$
$$\bigcap_{i\in I} A_i = \{x \mid x \in A_i, \forall\, i \in I\}.$$

设 S,A,B,C 为集合,不难证明,集合的交、并、差运算具有下面的性质:

1° 幂等律

$$A \cup A = A, A \cap A = A;$$

2° 交换律

$$A \cup B = B \cup A, A \cap B = B \cap A;$$

3° 结合律

$$(A \cup B) \cup C = A \cup (B \cup C),$$
$$(A \cap B) \cap C = A \cap (B \cap C);$$

4° 分配律

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C),$$
$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C),$$

5° 德·摩根定律

$$(S - A) \cup (S - B) = S - (A \cap B),$$
$$(S - A) \cap (S - B) = S - (A \cup B),$$

或者叙述成补集的形式：

$$A' \cup B' = (A \cap B)',$$
$$A' \cap B' = (A \cup B)'.$$

对于以上的性质，我们只证 5°中的 $A' \cup B' = (A \cap B)'$，以示范证明两个集合相等的通常思路，其余性质的证明由读者自行完成.

证明 设 $x \in (A \cup B)'$，则 $x \notin A \cup B$，因而 $x \notin A$ 且 $x \notin B$，从而 $x \in A'$ 且 $x \in B'$，故 $x \in A' \cap B'$，得 $(A \cup B) \subseteq A' \cap B'$；

反之，设 $x \in A' \cap B'$，则 $x \in A'$ 且 $x \in B'$，即 $x \notin A$ 且 $x \notin B$，于是有 $x \notin A \cup B$，即 $x \in (A \cup B)'$，故 $A' \cap B' \subseteq (A \cup B)'$.

所以，$A' \cup B' = (A \cap B)'$. ■

三、积集合与幂集合

设 $A_1, A_2, \cdots, A_n$ 是 n 个集合，由一切形如

$$(a_1, a_2, \cdots, a_n), a_i \in A_i, i = 1, 2, \cdots, n$$

的有序元素所组成的集合叫做集合 $A_1, A_2, \cdots, A_n$ 的**积集合**，或称集合 $A_1, A_2, \cdots, A_n$ 的**卡氏积**，记为

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \cdots, a_n) \mid a_i \in A_i, i = 1, 2, \cdots, n\}.$$

例如，$A = \{a, b\}, B = \{1, 2, 3\}$，则

$$A \times B = \{(a, 1), (a, 2), (a, 3), (b, 1), (b, 2), (b, 3)\};$$
$$B \times A = \{(1, a), (1, b), (2, a), (2, b), (3, a), (3, b)\}.$$

一般来说，卡氏积不可交换，即 $A \times B \neq B \times A$，只有当 $A = B$ 时，才有 $A \times B = B \times A$.

设 A 为集合，以 A 的所有子集作为元素所作成的集合称为 A 的**幂集合**，记为 2^A.

例如，$A = \{a, b, c\}$，则

$$2^A = \{\varnothing, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}.$$

习题 1.1

1. 设集合 $A = \{a, b, c, d\}, B = \{c, d, e\}$，求 $A \cup B, A \cap B, A - B, (A - B) \cup (B - A)$.

2. 设集合 $A = \{1, 2, 3, 4\}$，分别写出 $A \times A$ 与 2^A 中所含的所有元素.

3. 设 A, B 都为有限集，且 $|A| = m, |B| = n$，证明：

$$|A \times B| = mn.$$

4. 设 A 是有限集，证明：$|2^A| = 2^{|A|}$.

5. 具体证明集合的运算性质 4°，即证明

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C),$$
$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C).$$

§1.2 映 射

上节介绍了集合的概念,一般来说,在研究集合时,并不仅仅是孤立地考虑某个集合本身以及其中的元素,而是要建立某些集合与集合之间、元素与元素之间的相互联系,以达到进一步研究它们的目的.映射和代数运算则是建立这种联系的重要手段.

一、映射

定义 1 设 $A_1,A_2,\cdots,A_n,D$ 为集合,如果有一个法则 f,对于任意的 $(a_1,a_2,\cdots,a_n)\in A_1\times A_2\times\cdots\times A_n$,通过法则 f 在 D 中能得到唯一的元素 d 与它对应,那么法则 f 叫做由集合 $A_1\times A_2\times\cdots\times A_n$ 到集合 D 的一个**映射**;元素 d 叫做元素 $(a_1,a_2,\cdots,a_n)$ 在映射 f 下的**象**,而元素 $(a_1,a_2,\cdots,a_n)$ 叫做元素 d 在 f 下的一个**原象**.

对于映射我们常用以下符号来描述:

$$f:A_1\times A_2\times\cdots\times A_n\to D,$$
$$(a_1,a_2,\cdots,a_n)\mapsto d=f(a_1,a_2,\cdots,a_n).$$

要确定一个映射,则必须给定相应的集合和对应法则.也就是说,若要两个映射相等,那么这两个映射所联系着的集合必须分别相同,而且每一个元素所对应的象也必须是相等的.

例 1 设 $A_1=A_2=\cdots=A_n=D=\mathbf{R}$,

$$f:(a_1,a_2,\cdots,a_n)\mapsto a_1^2+a_2^2+\cdots+a_n^2,$$

是一个 $A_1\times A_2\times\cdots\times A_n$ 到 D 的映射.这里 A_i,D 都是相同的集合,映射的定义中并没有要求所给的集合要互不相同.

例 2 设 $A=\{a,b,c\},D=\{1,2,3,4\}$,

$$f:a\mapsto 1,b\mapsto 1,c\mapsto 2$$

是 A 到 D 的一个映射；

$$g: a \mapsto 1, b \mapsto 2, c \mapsto 3$$

也是 A 到 D 的一个映射；但

$$h: a \mapsto 1, b \mapsto 1$$

不是 A 到 D 的一个映射，因为 $c \in A$ 在 h 作用下没有象.

例 3　设 $A = \mathbf{Z}, D = \mathbf{Z}^+ = \{$全体正整数$\}$，

$$f: n \mapsto |n|$$

不是 A 到 D 的映射，因为 0 在 f 作用下的象不在 D 中；而

$$g: n \mapsto |n| + 1$$

是 A 到 D 的一个映射；再看

$$h: n \mapsto \begin{cases} 2(n+1) & \text{当 } n \geqslant 0 \text{ 时} \\ -2n-1 & n < 0 \text{ 时} \end{cases}$$

也是 A 到 D 的一个映射.

例 4　设 $A_1 = A_2 = A_3 = \{$几何空间中以原点为起点的向量全体$\}$，$D = \mathbf{R}$，

$$f: (\alpha_1, \alpha_2, \alpha_3) \mapsto (\alpha_1 \times \alpha_2) \cdot \alpha_3,$$

其中 $(\alpha_1 \times \alpha_2) \cdot \alpha_3$ 表示向量 $\alpha_1, \alpha_2, \alpha_3$ 的混合积，那么 f 是 $A_1 \times A_2 \times A_3$ 到 D 的一个映射.

例 5　设 $A = D$，则

$$I_A: a \mapsto a, \ \forall a \in A$$

是 A 到 A 的一个映射，我们将这个映射 I_A 叫做集合 A 的**恒等映射**（或**单位映射**）.

注意：当 $A \neq B$ 时，I_A 与 I_B 是两个不同的映射.

由于 $A_1 \times A_2 \times \cdots \times A_n$ 仍是一个集合，因此，上述映射的定义等价于集合 A 到 D 的映射定义，即

定义 1′ 设 A,D 为集合，如果有一个法则 f，对于 $\forall a \in A$，通过法则 f 在 D 中能得到唯一的元素 d 与它对应，那么法则 f 叫做由集合 A 到集合 D 的一个**映射**.

以后我们可将这两种形式不同，但本质一样的映射定义按实际需要灵活运用.

定义 2 设 f 是 A 到 D 的一个映射. 如果对于 A 中的任意两个元素 x_1,x_2，当 $x_1 \neq x_2$ 时，必有 $f(x_1) \neq f(x_2)$，即 A 中任意两个不同的元素在 f 下的象也必定不同，那么，称 f 是 A 到 D 的一个**单射**；如果对于任意 $d \in D$，都存在 $a \in A$，使得 $f(a) = d$，即 D 中的每一个元素 d 在 f 下都有原象，那么，称 f 是 A 到 D 的一个**满射**；如果映射 f 既是单射，又是满射，则称 f 是 A 到 D 的一个**一一映射**.

例 1 中的 f 既不是单射，也不是满射；例 2 中的 g 是单射而不是满射；例 3 中的 g 是满射但不是单射；例 3 中的 h 和例 5 中的 I_A 都是一一映射.

设 f 是 A 到 D 的一个映射，任取 $S \subseteq A$，令

$$f(S) = \{f(x) \mid x \in S\},$$

这是 D 的一个子集，叫做 A 的子集 S 在映射 f 下的象. 特别地，当 $S = A$ 时，$f(A)$ 叫做**映射 f 的象**，通常记为

$$\mathbf{Im} f = f(A).$$

于是，一个 A 到 D 的映射 f 可以看作是 A 到 $\mathbf{Im} f$ 的一个满射.

任取 $T \subseteq D$，令

$$f^{-1}(T) = \{x \mid x \in A, f(x) \in T\},$$

这是 A 的一个子集，叫做 D 的子集 T 在映射 f 下的**完全原象**. 当 T 仅含有一个元素时，例如，$T = \{d\}$，则 $f^{-1}(\{d\})$ 通常记成 $f^{-1}(d)$.

注意：当 $T \neq \varnothing$ 时，可能 $f^{-1}(T) = \varnothing$. 例如在例 2 中，取 $T = \{4\}$，则 $f^{-1}(T) = \varnothing$. 另外，$f^{-1}(T)$ 仅是一个记号，要与后面将要学到的可逆映射的逆映射加以区别.

二、映射的合成

定义 3 设 A,B,C 为集合，有两个映射

$$f: A \to B,\ g: B \to C,$$

由 f,g 确定的 A 到 C 的映射

$$h: A \to C,\ a \mapsto g(f(a)),\ \forall a \in A$$

叫做**映射 f 和 g 的合成**，记为 $h = g \circ f$，有时也记为 $h = gf$，即

$$h(a) = (g \circ f)(a) = (gf)(a) = g(f(a)).$$

映射由 f 和 g 合成的 h 可用如下的图来表示：

$$\begin{tikzcd} A \arrow[rr, "g \circ f"] \arrow[dr, "f"'] & & C \\ & B \arrow[ur, "g"'] & \end{tikzcd}$$

对于的映射的合成我们有

定理 1 设 $f: A \to B, g: B \to C, h: C \to D$，则有

(1) $h \circ (g \circ f) = (h \circ g) \circ f$;

(2) $I_B \circ f = f,\ f \circ I_A = f$.

证明 (1) 按照两个映射相等的意义，需要证明与这两个映射 $h \circ (g \circ f)$，$(h \circ g) \circ f$ 相关的集合分别是一样的，根据映射合成的定义，我们可知它们都是由 A 到 D 的映射. 其次，还需要证明法则相同，即 $\forall a \in A$，有

$$[h \circ (g \circ f)](a) = [(h \circ g) \circ f](a).$$

由映射合成的定义，对于 $\forall a \in A$，我们有

$$[h\circ(g\circ f)](a)=h[(g\circ f)](a)=h[g(f(a))],$$
$$[(h\circ g)\circ f](a)=(h\circ g)(f(a))=h[g(f(a))],$$

即得
$$h\circ(g\circ f)=(h\circ g)\circ f.$$

(2) $I_B\circ f$ 与 f 都是 A 到 B 的映射，并且 $\forall a \in A$，有

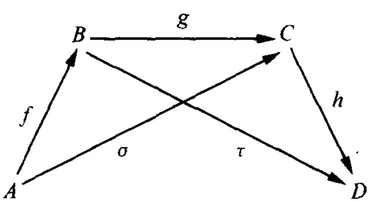
$$(I_B\circ f)(a)=I_B(f(a))=f(a),$$

即
$$I_B\circ f=f.$$

同理可证
$$f\circ I_A=f.$$ ■

如果在一个映射图中，任意两个集合之间经过不同途径（如果不同途径存在的话）所得的结果是相同的，则称这个**图可交换**．例如，要使下图可交换，则必须满足：

$$A\to D:\ h\circ g\circ f=h\circ\sigma=\tau\circ f,$$
$$A\to C:\ g\circ f=\sigma,$$
$$B\to D:\ h\circ g=\tau.$$



定理 2 设 f 是 A 到 B 的一个一一映射，那么由 f 可以诱导出唯一的一个 B 到 A 的一一映射 f^{-1}，使

$$f\circ f^{-1}=I_B,\ f^{-1}\circ f=I_A.$$

证明 首先利用 f 来作 B 到 A 的映射

$$f^{-1}:b\mapsto a,\ 假如\ b=f(a).$$

由于 f 是 A 到 B 的一个一一映射，任意给出一个 $b\in B$，有且仅有

一个 $a \in A$ 能够满足条件 $f(a)=b$,即 B 中的任何元素 b 在 f^{-1} 下都存在象 a,且其象唯一.也就是说,这样定义的映射 f^{-1} 是合理的.

再来证 f^{-1} 也是一一映射. $\forall a \in A$,有 $b \in B$,使 $f(a)=b$,也就是说 $f^{-1}(b)=a$,即 f^{-1} 为满射;

若 $b_1, b_2 \in B$,如果 $b_1 \neq b_2$,那么必有 $f^{-1}(b_1) \neq f(b_2)$.如果不然,即 $f^{-1}(b_1)=f^{-1}(b_2)=a$,那么 b_1 与 b_2 是同一个元素 a 在 f 下的象,得 $b_1=b_2$,矛盾,从而证得 f^{-1} 为单射.

根据 f^{-1} 的定义,容易得到

$$f \circ f^{-1}=I_B, \quad f^{-1} \circ f=I_A.$$

最后,证明满足条件的映射是唯一的.如果还有 $g: B \to A$,使

$$f \circ g=I_B, \quad g \circ f=I_A.$$

则

$$g=I_A \circ g=(f^{-1} \circ f) \circ g=f^{-1} \circ (f \circ g)=f^{-1} \circ I_B=f^{-1}.$$

■

当 f 为一一映射时,也称 f 为**可逆映射**,称 f^{-1} 为 f 的**逆映射**.

三、变换

对于映射 $f: A \to D$,它是联系着两个集合 A 与 D 的,但映射的定义中并没有要求 A 与 D 必须是两个不同的集合.当这两个集合 A 与 D 相同时,我们有

定义 4 一个 A 到 A 的映射叫做 A 的一个**变换**,如果这个 A 到 A 的映射还是单射、满射、一一映射,那么这个变换分别叫做 A 的**单变换**、**满变换**、**一一变换**.

例 6 设 $A=\mathbf{R}$,

$$\sigma: x \mapsto e^x, \ \forall x \in A$$