东北师范大学

文库

袁秉成　等编

JINSHI DAISHU

近世代数

东北师范大学出版社

东北师范大学文库

近世代数

袁秉成　张永正
王仁发　游　宏　谷文祥　编

东北师范大学出版社
1995·长春

(吉)新登字 12 号

东北师范大学文库

近世代数

JINSHI DAISHU

袁秉成 等 编

责任编辑:杨述春　　封面设计:李冰彬　　责任校对:左　群

东北师范大学出版社出版　　吉林省新华书店发行

(长春市斯大林大街 110 号)　　吉林工学院印刷厂制版

(邮政编码:130024)　　吉新月历公司印刷分公司印刷

开本:850×1168 毫米 1/32　　1995 年 10 月第 1 版

印张:5.25　　1995 年 10 月第 1 次印刷

字数:130 千　　印数:0 001—1 000 册

ISBN 7 - 5602 - 1762 - 1/O • 88　　定价:7.00 元

本书系东北师范大学
图书出版基金项目

前　言

本书可作为高等师范院校数学系本科学生近世代数教材.

考虑到近世代数所具有的抽象性以及学生的实际接受能力，本书在写法上力求通俗易懂，推理与证明尽量详尽，同时列举了大量的实例，比如旋转群，平移群，正方形的对称群等，以增加学生的直观理解.

在内容选取上，除了编入了一般近世代数教材中群、环和域的基础知识外，还选进了更深入一些的并且与中学数学教学相关的内容，用近代数学的观点和知识解决一些初等数学不能解决的问题. 比如本书介绍了域上多元多项式因子分解的可行性与唯一性，用 Calois 理论证明了次数大于四的一元多项式不能用根号解的问题以及给出三四次多项式的根的解法. 本书还讨论了历史上的几何作图的三个不能问题（尺规作图不能问题），这是一个在中学数学教学中常使教师感到困扰的问题. 本书还证明了中国剩余定理，它是初等数论中整数的剩余定理的推广. 以上这些内容也是进一步学习代数学及现代数学的基础.

书中少数划 * 号的地方，表示该内容难度较大，可根据具体情况酌情删减.

本书的第一、二、三、六章依次由谷文祥、袁秉成、张永正、游宏编写，第四、五章由王仁发编写，全书最后由袁秉成、张永

正修改定稿. 由于编者水平有限，书中一定有不妥之处，希望得到读者的批评指正.

编　者

1994 年 12 月 21 日

目　录

第一章 集合 映射 关系

在这一章里，我们将介绍集合，映射，关系和分类等基本概念，它们在本书以后各章中都要被经常用到.

§1 集 合

人们在研究某种事物的时候，其研究对象一般总是隶属于某一确定的范围的. 我们把某一范围内的对象全体叫做一个集合，组成集合的每个对象叫做这个集合的元素. 今后我们用大写英文字母 $A,B,C\cdots$ 表示集合，用小写英文字母 $a,b,\cdots$ 来表示元素，当 a 是集合 A 的元素时，记为 $a\in A$ 或 $A\ni a$；当 a 不是 A 的元素时，记为 $a\overline{\in}A$（或 $a\notin A$），含有限个元素的集合叫做有限集，含无穷多个元素的集合叫做无限集.

我们可以用列举 A 的所有元素的办法来表示有限集合 A. 如 $A=\{1,2,3,4\}$.

当 A 是无限集时，我们可以用类似的方法来表示 A. 如自然数集 N 可表为

$N=\{1,2,3,\cdots\}$，

$N:1,2,3,\cdots$.

设 $P(x)$ 是某个与 x 有关的条件或法则，A 为满足 $P(x)$ 的一切 x 构成的集合，那么 A 可表为

$$A=\{x\mid P(x)\}.$$

例如　设 A 为 $x^2-5x+6=0$ 的根组成的集合. 则 A 可表为

$$A=\{x\mid x^2-5x+6=0\}.$$

若 B 为全体偶数组成的集合，则 B 可表为

$$B=\{x\mid x=2n, n \text{ 为整数}\}.$$

设 A，B 是两个集合，如果 A 的每个元素都属于 B，则说 A 是 B 的子集，记为 $A\subseteq B$；如果 A 是 B 的子集，并且至少存在一个 $b\in B$，但 $b\notin A$，则称 A 是 B 的真子集，记为 $A\subset B$.

显然，自然数集是整数集的子集，并且是真子集.

如果 $A\subseteq B$ 且 $B\subseteq A$，则称 A 与 B 相等，记为 $A=B$.

不包含任何元素的集合叫做空集，记为 ϕ，并规定 ϕ 是任何集合的子集.

例如　$x^2+1=0$ 的实数根集合是空集.

又如，平面上两条平行线的交点集合是空集.

设 A，B 是两个集合，则由一切既属于 A 又属于 B 的元素组成的集合叫做 A 与 B 的交，记为 $A\cap B$. 即

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

由两个集合的交的定义，不难证明

$$A\cap B=A \text{ 当且仅当 } A\subseteq B.$$

事实上，如果 $A\cap B=A$，则每个 $x\in A$，都有 $x\in A\cap B$，从而 $x\in B$；反之，显然有 $A\cap B\subseteq A$，又每个 $x\in A$，由于 $A\subseteq B$，知 $x\in B$，因则 $x\in A\cap B$，故又能 $A\subseteq A\cap B$.

设 A，B 是两个集合，则由一切属于 A 或者属于 B 的元素组成的集合叫做 A 与 B 的并，记为 $A\cup B$. 即

$$A\cup B=\{x\mid x\in A \text{ 或者 } x\in B\}.$$

易证：$A\cup B=B$ 当且仅当 $A\subseteq B$.

设 A，B 是两个集合，则由一切属于 A 但不属 B 的元素组成的集合叫做 B 在 A 中的余集，记为 $A\setminus B$. 即

$$A\setminus B=\{x\mid x\in A \text{ 且 } x\notin B\}.$$

当 $B\subseteq A$ 时，$A\setminus B$ 叫做 B 在 A 中的补集，此时，把 $A\setminus B$ 记为 B'.

显然，$B\cap B'=\phi$，$B\cup B'=A$.

设 A，B 是两个集合，当 $A\cap B\neq\phi$ 时，则说 A 与 B 相交；当 $A\cap B=\phi$ 时，则说 A 与 B 不相交.

设 $A=\{a_1,a_2\}$，$B=\{a_1,a_3,a_4\}$，$C=\{a_3,a_4\}$，则 $A\cap B=\{a_1\}$，$A\cup B=\{a_1,a_2,a_3,a_4\}$，$B\setminus A=\{a_3,a_4\}$，$A\setminus B=\{a_2\}$，$C'=\{a_1\}$.

集合 A 的一切子集所组成的集合叫做 A 的幂集，记为 $P(A)$. 即

$$P(A)=\{B\mid B\subseteq A\}.$$

设 $A=\{1,2,3\}$，则

$$P(A)=\{\phi,\{1\},\{2\},\{3\},\{1,2\},\{1,3\},\{2,3\},A\}.$$

设 A，B 是两个集合，则称集合

$$\{(a,b)\mid a\in A,b\in B\}$$

为 A 与 B 的笛卡尔积集，记为 $A\times B$. 即

$$A\times B=\{(a,b)\mid a\in A,b\in B\}.$$

集合的交与并可以推广到任意多个集合的情形；为了容易分清层次，有时把以集合做为元素的集合叫做族. 例如，A 的幂集 $P(A)$ 就是 A 的所有子集族. 设 $\{A_i\mid i\in I\}$ 是任一集合族，其中每个 A_i 都是集合，I 是所有 A_i 的下标的集合. 于是，这个集合族的交规定为

$$\bigcap_{i\in I}A_i=\{x\mid x\in A_i,i\in I\}.$$

这个集合族的并规定为

$$\bigcup_{i\in I}A_i=\{x\mid \text{存在 } i\in I \text{ 使 } x\in A_i\}.$$

习　题

1　设 $A=\{1,2,3,4\}$，$B=\{2,4,6,8\}$，$C=\{2,4\}$，写出 $A\cap B$，$A\cup B$，

$A\backslash B$，$B\backslash A$ 以及 C 分别在 A 和 B 中的补集.

2 设 A，B，C 都是集合，证明下列等式：

(1) 幂等律：$A\cap A=A$，$A\cup A=A$.

(2) 结合律：$(A\cap B)\cap C=A\cap(B\cap C)$，

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

(3) 交换律：$A\cap B=B\cap C$，$A\cup B=B\cup C$.

(4) 分配律：$A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$，

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

(5) 吸收集：$A\cup(A\cap B)=A$，$A\cap(A\cup B)=A$.

3 如果 $A=\{0,1,2\}$，$B=\{1,2\}$，下列各种写法，哪些是对的？哪些不对？

$1\in A$，$0\notin B$，$\{1\}\in A$，$1\subset A$，$\{1\}\subseteq A$，$0\subseteq A$，$\{0\}\subseteq A$，$\{0\}\subset B$，$A=B$，$A\supseteq B$，$\varnothing\subset A$，$A\subset A$.

4 已知集合 $A=\{a,3,2,4\}$，$B=\{1,3,5,b\}$. 若 $A\cap B=\{1,2,3\}$，求 a 和 b.

5 设集合 $A=\{$北京，上海$\}$，$B=\{$南京，广州，深圳$\}$. 求 $A\times B$ 与 $B\times A$.

§2 映射与交换图

映射是近世代数中又一个非常重要的概念. 利用映射来揭示事物间的联系是常用的手段.

定义 1 设 A 与 B 是任意两个集合. 如果存在一个法则 σ，使得对于 A 中每一个元素 a，按照法则 σ，都能在 B 中确定唯一的一个元素 a'，记作 $\sigma:a\longrightarrow a'$（或 $\sigma(a)=a'$）. 这样就说（法则）σ 是 A 到 B 的一个映射. a' 叫做 a 在 σ 下的像，a 叫做 a' 在 σ 下的一个原像.

常用以下符号来表示 σ 是 A 到 B 的映射：

$$\sigma:A\longrightarrow B$$
$$a\longrightarrow a'=\sigma(a).$$

例 1 设 $A=\{a,b,c,d\}$，$B=\{1,2,3\}$，

$$\sigma_1:\begin{array}{l}a\longrightarrow 1\\ b\longrightarrow 2\\ c\longrightarrow 3\\ d\longrightarrow 3.\end{array}$$

易知 σ_1 是 A 到 B 的一个映射；

再令

$$\sigma_2:\begin{array}{l}a\longrightarrow 1\\ b\longrightarrow 2\\ c\longrightarrow 1\\ d\longrightarrow 1.\end{array}$$

σ_2 也是 A 到 B 的一个映射.

若令

$$\sigma_3:\begin{array}{l}a\longrightarrow 2\\ b\longrightarrow 3\\ d\longrightarrow 1.\end{array}$$

由于 A 中的 c 在 σ_3 之下没有像，故 σ_3 不是 A 到 B 的映射.

例 2 设 $A=N$ 为自然数集，$B=Z$ 为整数集.

令 $\sigma:n\longrightarrow n,n\in N$，

易知 σ 是 A 到 B 的映射.

例 3 设 $A=\left\{\begin{pmatrix}a & 0\\ 0 & a\end{pmatrix}\middle|\, a\in R\right\}$，$B=R$.

$$\sigma_1:\begin{pmatrix}a & 0\\ 0 & a\end{pmatrix}\longrightarrow a,$$

$$\sigma_2:\begin{pmatrix}a & 0\\ 0 & a\end{pmatrix}\longrightarrow a^2,$$

$$\sigma_3:\begin{pmatrix}a & 0\\ 0 & a\end{pmatrix}\longrightarrow 0.$$

易知 $\sigma_1,\sigma_2,\sigma_3$ 都是 A 到 B 的映射.

定义 2 设 σ 为 A 到 B 的映射. 如果 B 中每个元素，通过 σ

在 A 中都有原像，则称 σ 为 A 到 B 的满射.

如例 1 的 σ_1，例 3 的 σ_1，σ_2 都是 A 到 B 的满射.

定义 3 设 σ 为 A 到 B 的映射. 如果 A 中任意两个不同的元素，在 σ 之下的像也不同，则称 σ 为 A 到 B 的单射.

例 2 的 σ，例 3 的 σ_1 都是单射.

定义 4 设 σ 是 A 到 B 的映射. 如果 B 中每一元素通过 σ 在 A 中都有原像，并且 A 中任何不同的两个元素，在 σ 之下的像也不同，则称映射 σ 为 A 到 B 的双射.

显然双射既是满射又是单射. 例 3 的 σ_1 是双射.

例 4 设 $A=F[x]=\{f(x)\mid f(x)$是数域 F 上的多项式$\}$，$B_1=\{0,1,2,3,\cdots\}$，$B_2=\{-\infty,0,1,2,\cdots\}$，

令 $\sigma_1: f(x)\longrightarrow \deg f(x)$，

$\sigma_2: f(x)\longrightarrow \deg f(x)$，当 $f(x)\neq 0$ 时；

$f(x)\longrightarrow -\infty$，当 $f(x)=0$ 时；

则由于 $f(x)=0$ 在 σ_1 之下没有像，所以 σ_1 不是 $F[x]$ 到 B_1 的映射，而 σ_2 是 $F[x]$ 到 B_2 的映射，而且是满射，但不是单射.

例 5 设 $A=B$. 令

$$\sigma: a\longrightarrow a, a\in A.$$

则 σ 是 A 到 A 的一个映射. 此映射叫做 A 的恒等映射，通常用 ε_A 来表示 A 的恒等映射.

显然，A 的恒等映射是 A 的双射.

设 σ 是 A 到 B 的映射，S 是 A 的子集，则称集合 $T=\{\sigma(x)\mid x\in S\}$ 为 S 在 σ 之下的像，记为 $\sigma(S)=T$. 显然，$\sigma(S)\subseteq B$. 特别地，当 $S=A$ 时，$\sigma(A)$ 叫做映射 σ 的像，记为 $\mathrm{im}\sigma=\sigma(A)$. 设 $V\subseteq B$，则集合 $U=\{x\mid \sigma(x)\in V\}$ 叫做 V 在 σ 之下的完全原像集，记为 $\sigma^{-1}(V)=U$. 当 $V=\{x\}$ 时，$\sigma^{-1}(\{x\})$ 记为 $\sigma^{-1}(x)$.

不难证明，A 到 B 的映射 σ 是满射当且仅当 $\mathrm{im}\sigma=\sigma(A)=B$.

设 σ,τ 都是 A 到 B 的映射，如果对于任意 $x\in A$，总有 $\sigma(x)=\tau(x)$，则称 σ 与 τ 相等，记作 $\sigma=\tau$.

例如，设 $A=\{0,2\}$，$B=\{0,4\}$，

令 $\sigma_1: x \longrightarrow x^2, x \in A$.

$\sigma_2: x \longrightarrow 2x, x \in A$.

显然 σ_1, σ_2 都是 A 到 B 的映射. 虽然从形式上看它们有很大差别，但是，由于 $\sigma_1(0)=0=\sigma_2(0)$，$\sigma_1(2)=4=\sigma_2(2)$，所以 $\sigma_1=\sigma_2$.

定义 5 设 A, B, C 是三个集合，$\sigma: A \longrightarrow B$，$\tau: B \longrightarrow C$，则 A 到 C 的映射 $\mu: a \longrightarrow \tau(\sigma(a)), a \in A$，叫做 σ 与 τ 的合成，记为 $\mu=\tau\sigma$，即 $(\tau\sigma)(a)=\tau(\sigma(a))$.

例 6 设 $A=\{a.b\}$，$B=\{1,2,3,4\}$，$C=\{x, y, z\}$，

$\sigma: a \longrightarrow 1, b \longrightarrow 3$.

$\tau: 1 \longrightarrow x, 2 \longrightarrow y, 3 \longrightarrow z, 4 \longrightarrow z$.

则 σ, τ 分别是 A 到 B，B 到 C 的映射，它们的合成是

$\tau\sigma: a \longrightarrow \tau(\sigma(a))=\tau(1)=x$，

$b \longrightarrow \tau(\sigma(b))=\tau(3)=z$.

值得注意的是，一般的映射合成不满足交换律. 然而映射的合成满足结合律.

定理 1 设 $\sigma: A \longrightarrow B$，$\tau: B \longrightarrow C$，$\mu: C \longrightarrow D$，则

$$(\mu\tau)\sigma=\mu(\tau\sigma).$$

证明 首先，由所给条件知 $\mu(\tau\sigma)$ 与 $(\mu\tau)\sigma$ 都是 A 到 D 的映射，又对于每个 $a \in A$，有

$$((\mu\tau)\sigma)(a)=(\mu\tau)(\sigma(a))=\mu(\tau(\sigma(a)))$$

$$(\mu(\tau\sigma))(a)=\mu((\tau\sigma)(a)=\mu(\tau(\sigma(a))),$$

即

$$((\mu\tau\sigma)(a)=(\mu(\tau\sigma))(a).$$

由两个映射相等的定义，有

$$(\mu\tau)\sigma=\mu(\tau\sigma).$$

我们不难证明：若 σ 与 τ 都是单射，则 $\tau\sigma$ 也是单射；若 σ, τ 都是满射，则 $\tau\sigma$ 也是满射；若 σ, τ 都是双射，$\tau\sigma$ 也是双射.

定义 6 设 σ 是 A 到 B 的映射，如果存在 B 到 A 的映射 τ，使

得

$$\tau\sigma=\varepsilon_A \text{且 } \sigma\tau=\varepsilon_B,$$

则称 τ 为 σ 的逆映射. 具有逆映射的映射叫做可逆映射.

例 6 中的恒等映射是可逆映射.

由逆映射的定义可直接推得:若 τ 是 $\sigma:A\longrightarrow B$ 的逆映射,则对于任意的 $a\in A$,$a'\in B$ 有:

$$\sigma(a)=a' \text{当且仅当 } \tau(a')=a.$$

事实上,如果 $\sigma(a)=a'$,则 $\tau(\sigma(a))=\tau(a')$. 但 $\tau\sigma=\varepsilon_A$,所以 $\tau(a')=\varepsilon_A(a)=a$. 反之,如果 $\tau(a')=a$,则 $\sigma(a)=\sigma(\tau(a'))=(\sigma\tau)(a')=\varepsilon_B(a')=a'$.

由逆映射的定义还可直接推得:如果 $\sigma:A\longrightarrow B$ 是可逆映射,则 σ 的逆映射只有一个.

事实上,若 τ_1,τ_2 都是 σ 的逆映射,则

$$\tau_1\sigma=\varepsilon_A=\tau_2\sigma,\sigma\tau_1=\varepsilon_B=\sigma\tau_2.$$

于是

$$\tau_1=\varepsilon_A\tau_1=(\tau_2\sigma)\tau_1=\tau_2(\sigma\tau_1)=\tau_2\varepsilon_B=\tau_2.$$

以后我们把可逆映射 σ 的唯一的逆映射记为 σ^{-1}.

由逆映射的定义还可看出,如果 σ 是可逆映射,那么 σ^{-1} 也是可逆的,而且 σ 就是 σ^{-1} 的逆映射. 即 $(\sigma^{-1})^{-1}=\sigma$.

现在我们来证明,双射与可逆映射本质上是一致的.

定理 2 $\sigma:A\longrightarrow B$ 是可逆映射当且仅当 σ 是双射.

证明 充分性 假设 σ 是双射. 对于任意 $a'\in B$,规定

$$\tau:a'\longrightarrow a \text{,如果 } \sigma(a)=a',$$

则 τ 显然是 B 到 A 的映射. 而且

$$(\tau\sigma)(a)=\tau(\sigma(a))=\tau(a')=a=\varepsilon_A(a),a\in A.$$

$$(\sigma\tau)(a')=\sigma(\tau(a'))=\sigma(a)=a'=\varepsilon_B(a'),a'\in B.$$

因而

$$\sigma\tau=\varepsilon_B,\tau\sigma=\varepsilon_A.$$

所以 τ 是 σ 的逆映射.

必要性　假设 σ 是可逆的，则存在逆映射 σ^{-1} 使 $\sigma^{-1}\sigma=\varepsilon_A$，$\sigma\sigma^{-1}=\varepsilon_B$. 对于任意 $a'\in B$，有 $\sigma^{-1}(a')=a\in A$，

$$\sigma(a)=\sigma(\sigma^{-1}(a'))=(\sigma\sigma^{-1})(a')=\varepsilon_B(a')=a'.$$

这说明 σ 是满射. 又对于任意 $a,b\in A$，若

$$\sigma(a)=\sigma(b),$$

则

$$\sigma^{-1}(\sigma(a))=\sigma^{-1}(\sigma(b)),\varepsilon_A(a)=\varepsilon_A(b),a=b.$$

这说明 σ 是单射. 从而知 σ 是单射.

为了在讨论问题时使思路清晰，还可以用图形来表示映射合成：其中多边形顶点表示集合，有箭头的线段表示映射，由始点集合 A 到终点集合 B 经历的各条线路所组成的映射合成都相等. 图 1-1 说明

$$\mu=\tau\sigma,$$

此时也说图形是交换的. 再如图 1-2 表示 $\tau\sigma=\omega\mu$.

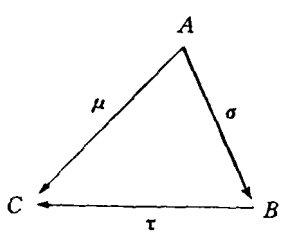

图 1-1

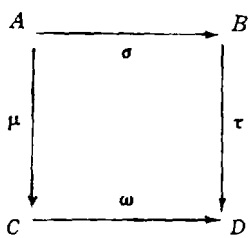

图 1-2

在本节的最后，我们讨论一类特殊的映射.

定义 7　A 到 A 的映射 σ 叫做 A 的一个变换. 当 σ 分别是单射、满射、双射时，则 σ 分别叫做 A 的单变换、满变换、双变换. A 到 A 的恒等映射叫做 A 的恒等变换.

几何中的平移、旋转都是变换.

前面对于映射的讨论自然地适用于变换. 特别是 A 的任意两个变换 σ,τ 都可以做合成，而且它们的合成 $\tau\sigma$ 仍然是 A 的变换. 如果 σ,τ 分别是 A 的单变换，满变换，双变换，那么 $\tau\sigma$ 也分别是单