大　学

数学系

自学丛书

近世代数

JINSHI DAISHU

大学数学系自学丛书

近 世 代 数

东北师范大学
高绪珏 主编

辽宁人民出版社

近世代数

Jinshi Daishu

高绪珏 主编

辽宁人民出版社出版　　辽宁省新华书店发行
（沈阳市南京街6段1里2号）　　朝阳六六七厂印刷

字数：380,000　　开本：850×1168 1/32　　印张：14 7/8
印数：1—14,000
1985年3月第1版　　1985年3月第1次印刷

责任编辑：俞晓群　　封面设计：安今生

统一书号：7090·299　　定价：2.85 元

出 版 说 明

为了适应广大在职人员和社会青年自学成才的需要，根据国家建立高等教育自学考试制度的精神，以满足学员自学教材的要求，由辽宁人民出版社出版一套大学数学系自学丛书。

本丛书是由东北师范大学数学系，根据教育部规定的普通高等院校本科必修课现行教学计划和教学大纲编写的。教材内容系统，数据充实，条理清晰，深入浅出；每章均有学习指导和习题解答，便于自学。经过刻苦自学，即可无师自通，达到本科毕业水平。

本丛书有：空间解析几何、高等代数、数学分析、高等几何、常微分方程、复变函数论、近世代数、实变函数论、微分几何、计算机与算法语言BASIC，概率论与数理统计、计算方法等。本丛书既可供自学应试之用，也可供大专院校的本科在校生和函授生及业余大学学生使用。

本丛书由于水平所限，不当之处在所难免，我们热诚希望广大自学读者批评指正。

目　录

第一部分　近世代数

第一章　基本概念

在这一章里，我们将介绍学习这门课程的预备知识以及近世代数的几个最基本的概念．近世代数的主要研究对象是代数体系，而代数体系是建立在集合概念基础之上的，所以我们从集合谈起．

§1 集　　合

人们观察某种客观事物，其观察对象一般总是隶属于某一确定的范围，所有观察对象都在该范围之内，而在该范围之外的则都不是．例如我们调查一个班级的学生的健康情况，那么这个班的每个学生都是调查对象；这个班以外的人都不是调查对象．我们把某一范围内的对象全体叫做一个**集合**，组成一个集合的每个对象叫做这个集合的**元素**（或**元**）．于是一个班级的学生全体是一个集合，这个班级的每个学生都是这个集合的元素．今后我们用大写拉丁字母A、B、C、…表示集合，小写拉丁字母a、b、c、…表示元素．当a是集合A的元素时，记为$a\in A$（读作a属于A）或$A\ni a$（读作A含着a）．当a不是A的元素时，记为$a\notin A$（读作a不属于A）或$A\not\ni a$（读作A不含着a）．

我们在以前的学习中，已经接触过大量的集合．例如：全体自然数组成一个集合，叫做自然数集，记为N；全体整数组

成一个集合，叫做整数集，记为Z；全体有理数组成一个集合，叫做有理数集，记为Q；全体实数组成一个集合，叫做实数集，记为R；全体复数组成一个集合，叫做复数集，记为C。

数域F上的全体n阶方阵组成集合$M_n(F)$，数域F上的全体多项式组成集合$F[x]$。

自然，四个数码1，2，3，4组成一个集合，甲、乙两个人组成一个集合。一般地，由有限个元素组成的集合叫做**有限集**；由无限多个元素组成的集合叫做**无限集**。

对于一个集合A来说，如果能够把A的每个元素都确定出来，那么集合A就确定了。于是有时我们用列举A的所有元素的方法表记A。例如A是由元素a，b，c组成的，则将A表为

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

或

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

其中花括号里或“：”之后列入A的全部元素。当元素过多不便全部列入时，则先列入A的部分元素，再用删节号表示其余元素。比如可将自然数集N表为

$$N=\{1,\ 2,\ 3,\ \cdots\}$$

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

表示集合的另一种方法，是通过这个集合的元素所具有的属性去表示它。当集合A的每个元素都满足某个条件，而且不属于A的元素都不满足这个条件时，可用这个条件描述A。

$$A=\{\triangle\mid\ \boxed{\quad}\ \}$$

其中位置△记入表示A的元素的字母，位置$\boxed{\quad}$记入A的元素所满足的条件。如

$$A=\{x\mid x\in R,\ x^2-2=0\}$$

表明A是由满足方程式$x^2-2=0$的全体实数组成的集合，即二次方程$x^2-2=0$的所有实根的集合，亦即$A=\{\sqrt{2},-\sqrt{2}\}$。

为了减少冗长叙述，有时采用下列记号：“$\forall$”，读作“对于每个”，“$\Longrightarrow$”，读作“推得”，“$\Longleftrightarrow$”，读作“必

要而且只要”．这些记号也可读作其他的同义语．

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$A\subseteq B$（读作：A含在B里）或$B\supseteq A$（读作：B包含着A）．当A不是B的子集时，记为$A\nsubseteq B$．

显然$A\subseteq B\Longleftrightarrow\forall a\in A$有$a\in B$．例如$N$是$Z$的子集，$Z$也是$Z$的子集．

如果$A\subseteq B$且$B\subseteq A$，则说A与B**相等**，记为$A=B$．显然$A=B\Longleftrightarrow\forall a\in A$有$a\in B$，而且$\forall b\in B$有$b\in A$．

如果$A\subseteq B$且$A\neq B$，则说A是B的**真子集**，记为$A\subset B$．显然$A\subset B\Longleftrightarrow\forall a\in A$有$a\in B$，而且存在$b\in B$，使得$b\notin A$．例如$N$是$Z$的真子集．

定义1　不含任何元素的集合叫做空集，记为ϕ．规定ϕ是任一集合的子集．

例如，多项式$f(x)=x^2-2$的有理根的集合，速度超过光速的飞机的集合都是空集．

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$A\cap B=\{x|x\in A$且$x\in B\}$．易证，$A\cap B=A\Longleftrightarrow A\subseteq B$．事实上，如果$A\cap B=A$，则$\forall a\in A$有$a\in A\cap B$，从而$a\in B$，故$A\subseteq B$．反之，如果$A\subseteq B$，则一方面$\forall b\in A\cap B$有$b\in A$；另一方面$\forall c\in A$有$c\in B$，从而$c\in A\cap B$．于是$A\cap B=A$．

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，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$A\cup B=\{x|x\in A$或$x\in B\}$．

易证：$A\cup B=B\Longleftrightarrow A\subseteq B$．（证明留给读者）．

设A，B是两个集合，则由一切属于B但不属于A的元素组成的集合叫做A在B中的**余集**，记为$B\backslash A$，即$B\backslash A=\{x|x\in B$而$x\notin A\}$．

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

显然，$A\cup A'=B$，$A\cap A'=\phi$.

例如，设$A=\{1,2\}$,$B=\{1,3,4\}$,$C=\{3,4\}$ 时,则$A\cap B=\{1\}$，$A\cup B=\{1,2,3,4\}$，$B\backslash A=\{3,4\}$. C是B的子集，C在B中的补集$C'=\{1\}$. A与B相交，A与C不相交. 请注意集合$\{1\}$，它是由一个元素1组成的. 集合$\{1\}$和元素1有区别，对B来说，$\{1\}$是B的子集：$\{1\}\subset B$，而1是B的元素：$1\in B$.

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 $P(A)=\{X|X\subseteq A\}$. 这里要注意，X在A中是子集合，X在$P(A)$中则是元素. 例如，$A=\{1,2,3\}$，则$P(A)=\{\phi,\{1\},\{2\},\{3\},\{1,2\},\{1,3\},\{2,3\},A\}$.

设A,B是两个集合,则A的每个元素a与B的每个元素b所做成的序对(a,b)的全体叫做A与B的**笛卡尔(Descartes)积**，记为 $A\times B$，即 $A\times B=\{(a,b)|a\in A,b\in B\}$. 例如，$A=\{a,b,c\}$，$B=\{x,y\}$，则 $A\times B=\{(a,x),(a,y),(b,x),(b,y),(c,x),(c,y)\}$. 实数集(实数轴)$R$与其自身的笛卡尔积$R\times R$就是实平面全体点的集合.

设 A_1，A_2，…，A_n 是n个集合，则它们的笛卡尔积是$A_1\times A_2\times\cdots\times A_n=\{(a_1,a_2,\cdots,a_n)|a_i\in A_i,\ i=1,2,\cdots,n\}$.

集合的交和并概念可推广到任意多个集合的情形. 为了容易分清层次，有时把由集合做为元素所组成的集合叫做族. 例如，A的幂集$P(A)$就是A的所有子集族. 设$\{A_i|i\in I\}$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(记作$\bigcap\limits_{i\in I}A_i$)规定为

$$\bigcap_{i\in I}A_i=\{x|\forall i\in I:x\in A_i\}$$

这个集合族的并(证作$\bigcup\limits_{i\in I}A_i$)规定为

$$\bigcup_{i\in I}A_i=\{x|\text{存在}j\in I\text{使}x\in A_j\}$$

习　　题

1　设 $A=\{1, 2, 3, 4\}$, $B=\{2, 4, 6, 8\}$, $C=\{2, 4\}$. 写出 $A\cap B$, $A\cup B$, $A\setminus B$, $B\setminus A$, $P(A)$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：$A\cap B=B\cap A$, $A\cup B=B\cup A$

（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）吸收律：$A\cup(A\cap B)=A$, $A\cap(A\cup B)=A$

§2 映　　射

上节讨论了集合的概念. 在我们的研究中所遇到的一些集合往往不是孤立的，它们之间存在着各种各样的关系. 现在我们来讨论在两个集合之间建立联系的一种手段——映射.

定义1　对于给定的集合A和B，如果存在一个法则φ，通过它，A中的每个元素a，都在B中确定唯一的元素a'，则法则φ叫做A到B的一个映射，记为

$$\varphi:\ A\longrightarrow B \text{ 或 } A\xrightarrow{\varphi} B$$

A叫做φ的定义域，B叫做φ的值域. 元素a'叫做a在φ之下的象，a叫做a'在φ之下的一个原象，记为

$$\varphi:\ a\longmapsto a' \text{ 或 } \varphi(a)=a'$$

例1　设 $y=f(x)$是定义在$[0, 1]$上的实值函数. 这是集合$[0, 1]$到实数集R的一个映射，用我们现在的表示法就是$f:[0, 1]\longrightarrow R$. 实际上，微积分中所见到的单值函数都是映射.

例2　设$A=\{x, y, z\}$, $B=\{a, b, c, d\}$.

$$\varphi_1:\ x\longmapsto a,\ y\longmapsto b,\ z\longmapsto c$$

是A到B的映射．注意，d在φ_1之下无原象．它表明，映射值域中的元素不必都有原象．

$$\varphi_2:\ x\longmapsto a,\ y\longmapsto a,\ z\longmapsto b$$

是A到B的映射．注意，x和y的象都是a．这说明，映射的定义域中的不同元素可以有相同的象．

$$\varphi_3:\ x\longmapsto a,\ x\longmapsto b,\ y\longmapsto c,\ z\longmapsto d$$

不是A到B的映射．这是因为φ_3为x确定了两个不同元素a和b做为象，x的象不唯一，不符合映射定义．

$$\varphi_4:\ x\longmapsto a,\ y\longmapsto b$$

φ_4没有给z确定象，φ_4不是A到B的映射．

例 3 设$A=\boldsymbol{Z}$，$B=\{2n\mid n\in\boldsymbol{Z}\}$（所有偶数的集合），$\forall n\in\boldsymbol{Z}$定义

$$\varphi_1:\ n\longmapsto 2n$$

$$\varphi_2:\ n\longmapsto 4n$$

$$\varphi_3:\ n\longmapsto n,\ \text{当}2\mid n$$

$$n\longmapsto n+1,\ \text{当}2\nmid n$$

$$\varphi_4:\ n\longmapsto |n|,\ \text{当}2\mid n$$

$$n\longmapsto |n+1|,\ \text{当}2\nmid n$$

这四个法则都适合映射的定义，都是整数集$\boldsymbol{Z}$到偶数集$\boldsymbol{B}$的映射．

例 4 设$A=M_n(F)$（数域F上所有n阶方阵的集合），$B=\{0,\ 1,\ 2,\ \cdots,\ n\}$，则

$$\varphi:\ (a_{ij})\longmapsto \text{秩}(a_{ij})$$

是$M_n(F)$到B的映射．

例 5 设$A=F[x]$（数域F上所有多项式的集合），$B_1=\{0,\ 1,\ 2,\cdots\}$，$B_2=\{-\infty,\ 0,\ 1,\ 2,\ \cdots\}$，令

$$\varphi_1:\ f(x)\longmapsto \deg f(x)$$

$$\varphi_2:\ f(x)\longmapsto \deg f(x),\ \text{当}\ f(x)\neq 0$$

$$f(x)\longmapsto -\infty,\ \text{当}\ f(x)=0$$

由于零多项式$f(x)=0$在φ_1之下无象，所以φ_1不是$F[x]$到B_1的映射．而φ_2是$F[x]$到B_2的映射．

例6　设$A=B$，$\forall a\in A$令

$$\varphi:\ a\longmapsto a$$

则φ是A到A的一个映射．此映射叫做A的**恒等变换**，通常用I_A表示A的恒等变换．

设φ是A到B的映射，$S\subseteq A$，则称集合$T=\{\varphi(s)\mid s\in S\}$为$S$在$\varphi$之下的**象**，记为$\varphi(S)=T$．显然$\varphi(S)\subseteq B$．特别地，当$S=A$时，$\varphi(A)$叫做**映射$\varphi$的象**，记为$\mathrm{im}\varphi=\varphi(A)$．设$V\subseteq B$，则集合$U=\{u\mid\varphi(u)\in V\}$叫做$V$在$\varphi$之下的**完全原象**，记为$\varphi^{-1}(V)=U$．当$V=\{x\}$时，把$\varphi^{-1}(\{x\})$记作$\varphi^{-1}(x)$．显然$\varphi^{-1}(V)\subseteq A$，特别地，$\varphi^{-1}(B)=A$．请读者留意，符号$\varphi^{-1}(V)$中的$\varphi^{-1}$不表示映射，在后面另外场合还将采用这个符号，但涵义与此不同．

定义2　设φ，ψ都是A到B的映射，如果$\forall a\in A$均有$\varphi(a)=\psi(a)$，则说映射φ与映射ψ**相等**，记为$\varphi=\psi$．

例如，设$A=\{0,2\}$，$B=\{0,4\}$，$\forall x\in A$令

$$\varphi_1:\ x\longmapsto x^2,\quad \varphi_2:\ x\longmapsto 2x$$

显然φ_1，φ_2都是A到B的映射．尽管从形式上看，它们是不同的，但是对这里确定的A和B来说，由于$\varphi_1(0)=0=\varphi_2(0)$，$\varphi_1(2)=4=\varphi_2(2)$，所以$\varphi_1=\varphi_2$．

映射相等的定义表明，两个映射只要定义域不同或者值域不同，它们便是不同的映射．但是为了叙述简单起见，对下述两种情况，我们做例外的约定：设φ是A到B的映射，如果S是A的真子集，则把φ也看做是S到B的映射；如果$\mathrm{im}\varphi=C$是B的真子集，则把φ也看做是A到C的映射．

定义3　设$\varphi:\ A\to B$，如果$\forall a,b\in A$，$a\neq b$，有$\varphi(a)\neq\varphi(b)$，则φ叫做**单射**；如果$\mathrm{im}\varphi=B$，则φ叫做**满射**；如果φ既是单射又是满射，则φ叫做**双射**．

φ是单射时，表明B的每个元素在A中的原象不能多于1

个；φ是满射时表明，B的每个元素必在A中有原象；φ是双射时，表明A的全体元素可与B的全体元素一个对一个地对应起来．特别是，当A、B之一是有限集时，另一个也必是有限集，而且A与B的元素个数相等．双射是一种重要映射，后面将做进一步讨论．

例3中的φ_1是双射，φ_2是单射但不是满射，φ_3是满射但不是单射，φ_4既不是单射也不是满射．例6中的恒等变换I_A是双射．

定义4 设A，B，C是三个集合，φ：$A\to B$，ψ：$B\to C$，则A到C的映射γ：$a\longmapsto\psi(\varphi(a))$，$\forall a\in A$，叫做$\varphi$与$\psi$的合成，记为$\psi\varphi=\gamma$．

例7 设$A=\{a,b\}$，$B=\{1,2,3,4\}$，$C=\{x,y,z\}$，

φ：$a\longmapsto 1$，$b\longmapsto 3$

ψ：$1\longmapsto x$，$2\longmapsto y$，$3\longmapsto z$，$4\longmapsto z$

则φ和ψ分别是A到B和B到C的映射，它们的合成是

$$\psi\varphi:\ a\longmapsto\psi(\varphi(a))=\psi(1)=x$$
$$b\longmapsto\psi(\varphi(b))=\psi(3)=z$$

值得注意的是，不是任何两个映射都可以做合成，能做合成的两个映射必须而且只须第一个映射的值域与第二个映射的定义域相同．还应注意，为了便于计算，在合成的记号$\psi\varphi$中，把第一个映射φ列在第二个映射ψ的右边．参加合成的两个映射的顺序一般不可颠倒，尽管$\psi\varphi$是映射合成，但是可能$\varphi\psi$无意义（ψ的值域不等于φ的定义域）例7便是如此．有时虽然$\varphi\psi$有意义，但$\varphi\psi\neq\psi\varphi$．所以一般的映射合成不满足交换律．然而映射合成满足结合律．

定理1 设$A\xrightarrow{\varphi}B\xrightarrow{\psi}C\xrightarrow{\gamma}D$，则

$$\gamma(\psi\varphi)=(\gamma\psi)\varphi$$

证明 首先，由所给条件知$\gamma(\psi\varphi)$和$(\gamma\psi)\varphi$是具有相同定义域A和相同值域D的两个映射．

其次证明这两个映射对A的每个元素的作用效果相同.

$\forall a\in A$有

$$[\gamma[\psi\varphi)](a)=\gamma[(\psi\varphi)(a)]=\gamma[\psi(\varphi(a))]$$

$$[(\gamma\psi)\varphi](a)=(\gamma\psi)(\varphi(a))=\gamma[\psi(\varphi(a))]$$

即

$$[\gamma(\psi\varphi)](a)=[(\gamma\psi)\varphi](a)$$

由映射相等的定义得

$$\gamma(\psi\varphi)=(\gamma\psi)\varphi$$

证完.

关于映射合成，还有两个明显的性质：其一是，$A\xrightarrow{\varphi}B\xrightarrow{\psi}C$，则当$\varphi$、$\psi$都是单射时，$\psi\varphi$必是单射；当$\varphi$、$\psi$都是满射时，$\psi\varphi$必是满射；从而，当$\varphi$、$\psi$都是双射时，$\psi\varphi$必是双射. 其二是，设$\varphi$：$A\longrightarrow B$，则$\varphi I_A=\varphi$，$I_B\varphi=\varphi$，其中$I_A$和$I_B$分别是$A$和$B$的恒等变换.

现证明，如果$A\xrightarrow{\varphi}B\xrightarrow{\psi}C$，则当$\varphi$，$\psi$都是单射时，$\psi\varphi$必是单射（其余的证明留给读者.）事实上，$\forall a$，$b\in A$，如果$a\neq b$，则因$\varphi$是单射，有$\varphi(a)\neq\varphi(b)$. 再因$\psi$是单射，有$\psi(\varphi(a))\neq\psi(\varphi(b))$，即$(\psi\varphi)(a)\neq(\psi\varphi)(b)$. 于是$\psi\varphi$是单射.

下面利用映射合成给出映射是双射的判定条件，为此先给出逆映射的概念.

定义5 设φ：$A\longrightarrow B$，如果存在ψ：$B\longrightarrow A$，使得$\psi\varphi=I_A$且$\varphi\psi=I_B$，则ψ叫做φ的逆映射. 具有逆映射的映射叫做可逆映射.

初等函数中的指数函数，对数函数，线性代数中的可逆线性变换，本节例3中的φ_1，例6中的恒等变换I_A都是可逆映射.

由逆映射的定义可直接推得：若ψ是φ：$A\longrightarrow B$的逆映射，则对于任意的$a\in A$，$a'\in B$有：$\varphi(a)=a'\Longleftrightarrow\psi(a')=a$.

事实上，如果$\varphi(a)=a'$，则$\psi(\varphi(a))=\psi(a')$，即$I_A(a)=$

$\psi(a')$，所以，$a=\psi(a')$．反之，如果$\psi(a')=a$，则$\varphi(\psi(a'))=\varphi(a)$，即$I_B(a')=\varphi(a)$，得$a'=\varphi(a)$．

由逆映射的定义还可直接推得：如果φ：$A\longrightarrow B$是可逆的，则φ的逆映射唯一．

事实上，设ψ、ψ'都是φ的逆映射，则有

$$\psi\varphi=I_A=\psi'\varphi,\quad \varphi\psi=I_B=\varphi\psi'$$

于是

$$\psi=I_A\psi=(\psi'\varphi)\psi=\psi'(\varphi\psi)=\psi' I_B=\psi'$$

现把可逆映射φ的唯一的逆映射记为φ^{-1}．

由逆映射的定义还可看出，如果φ是可逆映射，那么φ^{-1}也是可逆的，而且φ就是φ^{-1}的逆映射，即

$$(\varphi^{-1})^{-1}=\varphi$$

现在我们来证明，双射与可逆映射本质上的一致性．

定理2　φ：$A\longrightarrow B$**是可逆映射必要而且只要**φ**是双射．**

证明　充分性．假设φ是双射，$\forall a'\in B$，当$\varphi(a)=a'$，$a\in A$，令

$$\psi:\ a'\longmapsto a,\ \text{即}\ \psi(a')=a$$

下面说明ψ是B到A的映射．按上面规定，B中的元素a'在ψ之下的象是a'在φ之下的原象a．因为φ是双射，所以B中的任意元a'在A中必有原象，而且唯一．因此，ψ是B到A的映射．下面证明ψ是φ的逆映射．

显然$\psi\varphi$和I_A的定义域和值域都是A，$\varphi\psi$和I_B的定义域和值域都是B．而且，

$$\psi\varphi((a))=\psi(\varphi(a))=\psi(a')=a=I_A(a),\quad \forall a\in A$$

所以，$\psi\varphi=\mathrm{I}_A$．$\forall a'\in B$有

$$\varphi\psi(a')=\varphi(\psi(a'))=\varphi(a)=a'=I_B(a')$$

故

$$\varphi\psi=I_B$$

因此ψ是φ的逆映射．