近世代数

高师函授教材

近　世　代　数

东北三省函授教材
《近世代数》协编组　编

吉林人民出版社

内 容 提 要

本书是由东北师大贺昌亭副教授等编写的。全书共分七章，前两章主要介绍代数体系等基本概念，后五章主要介绍几种基本的代数体系——群、环、域、模、格与布尔代数的基础知识。本书特点是由浅入深、通俗易懂，许多章节采用启发式、讨论式的写法，以揭示概念的实质和知识的规律性，书中选编相当数量的练习题和习题，并给出比较详细的解答，使读者从中体会近世代数的解题方法，便于自学。

本书适宜作高师函授院校、师范院校和电视大学、业余大学的教材或教学参考书。

高师函授教材
近世代数
东北三省函授教材《近世代数》协编组
*
吉林人民出版社出版　吉林省新华书店发行
通辽教育印刷厂印刷
*
787×1092毫米 32开本　16.75印张　2插页 373,000字
1983年8月第1版　1983年8月第1次印刷
印数：1—8,000册
统一书号：13091·144　定价：1.75元

说　明

本书是根据东北三省高师函授教材协作会议精神编写的。全书共分七章，前两章主要介绍代数体系等基本概念，后五章主要介绍几种基本的代数体系——群、环、域、模、格与布尔代数的基础知识。书中打星号部份可作为选学内容。

根据以往的经验，针对学员在学习这一课程时往往感到抽象，对概念不能很好理解，对解题不知如何下手的情况；又考虑到函授学员主要靠自学的特点，我们在编写中力求做到由浅入深，通俗易懂，总结规律，交待要领。在写法上，许多场合采用了启发式、讨论式，引导读者揭示概念的实质和知识的规律性；每个重要概念都列举了较多的实例，以增加感性认识，给上升到理性认识奠定基础；每一节都通过较多的例题来说明如何应用本节的概念与理论解题，每一章的末尾都写了习题选解用来说明如何综合运用本章的概念和理论解题，企图起到典型示范的作用，使读者从中体会近世代数的证题方法；本书选辑了相当数量的练习题与习题，并都作了较详细的解答以供参考。但切忌不经自己的独立思考就看解答。

本书是在1980年第一稿的基础上修改而成的。第一稿由东北师大贺昌亭编写了大部分章节，迟志敏编写了部分章节，孙保民和吉林省函授学院刘清祥参加了编写工作，东北师大高绪珏看了草稿，提出了有益的意见。第一稿在东北师大印刷并经试教两遍后，这次由贺昌亭主持作了全面修改。

迟志敏修改了大部分章节，孙保民修改了部分章节并解答了全部练习题与习题，刘清祥参加了修改工作，吉林省函授学院毛国平做了大量抄写工作。

本书是作为高师函授教材而写的，也可作为高师院校近世代数课程的参考书及中学教师自学的参考书。

由于编者水平所限，不妥之处在所难免，衷心希望批评指正。

东北三省高师函授教材协作编写组

1983年2月

目　　录

第一章 集合与映射

本章讲三个问题：

一、集合及有关术语；

二、映射、映射的类型及例子，变换；

三、集合的分类与等价关系.

第二个问题——映射是本章的重点，它在许多数学学科中都有用处. 等价关系的概念对初学者可能有些困难，但它是代数学中有份量的概念，不宜忽略.

学习本章最好能熟练地掌握一批例子，其实这也是学习近世代数的一种有效方法和手段——通过例子理解概念，运用例子掌握方法.

§1 集 合

首先介绍集合的概念与表述方法.

我们已经知道数集——任意一些数的总体——的概念. 因此，对于集合这一数学用语我们并不陌生，也不会很费解. 由于在数学上可能涉及的事物不限于数，而从事物的总体上考虑问题又是代数学的一个重要特点，因此有必要把"事物的总体"这样一个概念明确起来，这在数学上通常就是用集合这个术语来表达的. 于是我们可以说：

任何一些（没有重复的）事物的总体叫做集合（也简称为集）. 总体中的每个事物叫做元素.

我们约定：不含任何事物的总体也叫集合，特别地，把它叫做空集合，记作ϕ。

用大写的拉丁字母A，B，C，…表示集合；小写的拉丁字母a，b，c，…表示元素。

如果a是集合A里的元素，就说a属于A或A含有a，记作$a\in A$；否则就说a不属于A或A不含有a，记作$a\notin A$。

如果两个集合A与B含有完全相同的元素：$x\in A\Longleftrightarrow x\in B$，则称$A$与$B$相等，记作$A=B$。（记号“$\Longleftrightarrow$”的含意是“当且仅当”）。

下面介绍表述一个集合A的方法，一般有三种方式：

（1）用语言说出集合A是由哪些元素组成的；

（2）在表示集合的字母后面点三个点，随后写出全部元素。例如A：0，-1。

（3）用符号$A=\{\cdots\}$表示A是由括号里的元素所组成的集合，而在括号中可以写出A的全部元素，也可以用适当的数学符号指明A的元素所应满足的条件。例如

$$A=\{1,\ -1\},\qquad B=\{x\,|\,x^2-1=0\}.$$

前者具体地写出A是由1，-1两个数组成，后者清楚地表明A是由二次方程$x^2-1=0$的根所组成。一般地，在括号中竖线后边指出A中元素所应具有的性质。显然它们都确切地描述了一个集合。这里是用不同方式描述了同一个集合，即$A=B$。

其次介绍子集、交集、并集、笛卡尔积集、幂集和补集。

设A，B为任意两个集合。

子集：若$x\in A\Longrightarrow x\in B$，则称$A$是$B$的子集，记作$A\subseteq B$。若$A\subseteq B$，但$A\neq B$，则称$A$是$B$的真子集，记作$A\subset B$。规定空集是任何集合的子集。

交集：集$\{x|x\in A$同时$x\in B\}$叫做A与B的交集，记作$A\cap B=\{x|x\in A$同时$x\in B\}$。如图1·1

并集：集$\{x|\in A$ 或 $x\in B\}$叫做A与B的并集，记作 $A\cup B=\{x|x\in A$或$x\in B\}$. 如图1·2

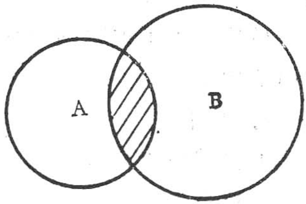

图1·1

笛卡尔积集：集$\{(a, b)|a\in A, b\in B\}$叫做$A$与$B$的笛卡尔积集，记作 $A\times B=\{(a,b)|a\in A, b\in B\}$.

幂集：集$\{X|X\subseteq A\}$叫做A的幂集，记作$P(A)$。

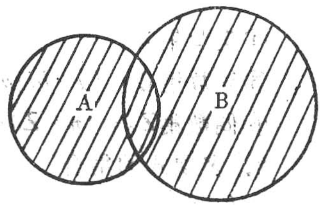

图1·2

为了定义补集，首先说明全集。一些集合常常是给定集合的子集，把这个给定集合叫做相对于那些子集的全集用符号I表示。就是说全集包含了所要研究的各个集合的全部元素。现在来定义补集。

补集：集$\{x|x\in I$ 但 $x\notin A\}$叫做集合A的补集，记作$A'=\{x|x\in I$，但$x\notin A\}$，如图1.3的长方形表示全集I，圆表示集合A，阴影部份表示集合A的补集A'。

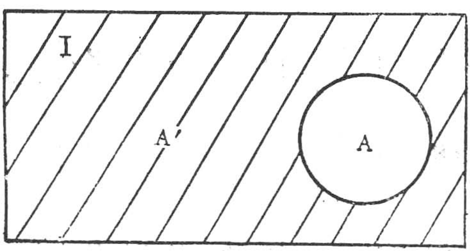

图1·3

由补集的定义，立即知A'是A的补集$\Longleftrightarrow$

$$A\cup A'=I,\ 且A\cap A'=\phi,$$

其中A为全集I的任一子集。

最后，为了说明问题和便于引述，现罗列一些大家熟习的例子如下：

1．数集

①自然数集$\mathbf{N}$：$1,\ 2,\ 3,\ \cdots,\ n,\ \cdots$；

②整数集$\mathbf{Z}$：$\cdots,\ -3,\ -2,\ -1,\ 0,\ 1,\ 2,\ 3,\ \cdots$；

③有理数集$\mathbf{Q}=\left\{\dfrac{a}{b}\,\middle|\,a,\ b\in\mathbf{Z},b\neq 0\right\}$；

④实数集$\mathbf{R}$；

⑤复数集$\mathbf{C}=\{a+bi\mid a,b\in\mathbf{R}\}$；

⑥偶数集$\mathbf{Z}_0=\{n\in\mathbf{Z}\mid n=2q,\ q\in\mathbf{Z}\}$。

2．多项式的集合

①$F[x]=\{a_0+a_1x+\cdots+a_nx^n\mid a_i\in F,\ n\text{ 为非负整数}\}$；

②$F_n[x]=\{a_0+a_1x+\cdots+a_{n-1}x^{n-1}\mid a_i\in F,n\text{为确定的正整数}\}$，其中$F$为数域。

3．矩阵的集合．设$\mathbf{R}$为实数域．

①$M_2(\mathbf{R})=\left\{\begin{pmatrix}a&b\\c&d\end{pmatrix}\,\middle|\,a,\ b,\ c,\ d\in\mathbf{R}\right\}$；

②$GL_2(\mathbf{R})=\left\{\begin{pmatrix}a&b\\c&d\end{pmatrix}\,\middle|\,a,\ b,\ c,\ d\in\mathbf{R},\begin{vmatrix}a&b\\c&d\end{vmatrix}\neq 0\right\}$；

③$SL_2(\mathbf{R})=\left\{\begin{pmatrix}a&b\\c&d\end{pmatrix}\,\middle|\,a,\ b,\ c,\ d\in\mathbf{R},\begin{vmatrix}a&b\\c&d\end{vmatrix}=1\right\}$

④$O_2(\mathbf{R})=\left\{\begin{pmatrix}a&b\\c&d\end{pmatrix}\,\middle|\,a,\ b,\ c,\ d\in\mathbf{R},\begin{pmatrix}a&b\\c&d\end{pmatrix}'=\right.$

$$=\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1}\Big\}；$$

⑤$M_{m\times n}(\mathbf{R})=\{(a_{ij})|a_{ij}\in\mathbf{R},\ 1\leq i\leq m,\ 1\leq j\leq n\}$。

4。线性变换的集合.设V是实数域上的二维向 量空间。

① $L=\{\sigma|\sigma$为V上的线性变换$\}$；

② $GL_2(V)=\{\sigma\in L|\det\sigma$①$\neq 0\}$；

③ $SL_2(V)=\{\sigma\in L|\det\sigma=1\}$；

④ $RL_2(V)=\{\sigma\in L|\sigma x=kx,\ \forall x\in V\}$，$k$为任意的确定实数；

⑤ $O_2(V)=\{\sigma\in L|(\sigma x,\ \sigma y)=(x,y),\ \forall\ x、y\in V\}$。

5。有限集。含有限个元素的集叫有限集。

① $A=\{1,\ 2,\ 3,\ \cdots,\ n\}$；

② $B=\{a_1,\ a_2,\ a_3,\ \cdots,\ a_n\}$；

③ $C=\{0,\ 1\}$；

④ $D=\{1,\ -1\}$；

⑤ $C\cap D=\{1\}$，$C\cup D=\{0,1,-1\}$；

$C\times D=\{(0,1),\ (0,-1),\ (1,1),\ (1,-1)\}$；

$C\times C=\{(0,0),\ (0,1),\ (1,0),\ (1,1)\}$；

$P(C)=\{\{0\},\ \{1\},\ C,\ \phi\}$。

⑥$X=\{$偶，奇$\}$，$Y=\{$立正，向左转，向后转，向右转$\}$。

6。补集。

① 设$I=\{1,\ 2,\ 3,\ \cdots,\ n,\ \cdots\}$，$I_1=\{1,\ 3,\ 5,\ \cdots,\ 2n-1,\ \cdots\}$，$I_2=\{2,\ 4,\ 6,\ \cdots,\ 2n,\ \cdots\}$于是$I_1\cup I_2=I$，$I_1\cap I_2=\phi$，故$I_1$是$I_2$的补集，当然$I_2$也是$I_1$的补集，其实$I_1$与$I_2$是互为补集。

---

① $\det\sigma$表示σ在任意基底上的阵的行列式。

② 设$I=\mathbf{R}$（为实数集），$I_1=\{$有理数$\}$，$I_2=\{$无理数$\}$。于是$I_1\cup I_2=I$，$I_1\cap I_2=\phi$，故I_1是I_2的补集，I_2也是I_1的补集。

③ 设$I=M_2(\mathbf{R})$，$I_1=\left\{\begin{pmatrix}a & b\\ c & d\end{pmatrix}\middle| a, b, c, d\in\mathbf{R},\begin{vmatrix}a & b\\ c & d\end{vmatrix}\neq 0\right\}$，$I_2=\left\{\begin{pmatrix}a & b\\ c & d\end{pmatrix}\middle| a,b,c,d\in\mathbf{R},\begin{vmatrix}a & b\\ c & d\end{vmatrix}=0\right\}$，于是$I_1\cup I_2=I$，$I_1\cap I_2=\phi$，故$I_1$是$I_2$的补集，$I_2$也是$I_1$的补集。

最后介绍交集、并集、补集的性质。

L_1 幂等律 $A\cup A=A$，$A\cap A=A$；

L_2 交换律 $A\cup B=B\cup A$，$A\cap B=B\cap A$；

L_3 结合律 $(A\cup B)\cup C=A\cup(B\cup C)$，

$(A\cap B)\cap C=A\cap(B\cap C)$；

L_4 分配律 $A\cup(B\cap C)=(A\cup B)\cap(A\cup C)$，

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

L_5 吸收律 $A\cup(A\cap B)=A$，$A\cap(A\cup B)=A$；

L_6 对合律 $(A')'=A$，其中A是全集I的子集；

L_7 摩根法则 $(A\cup B)'=A'\cap B'$，

$(A\cap B)'=A'\cup B'$，

其中A，B是全集I的子集。

以上这些性质一般比较容易证明它的正确性，这里只选择L_4和L_7给出证明，其余留给读者。

证L_4。我们只证$A\cup(B\cap C)=(A\cup B)\cap(A\cup C)$，另一个可以类似证之。

任取 $x\in A\cup(B\cap C)$，那么$x\in A$或$x\in B\cap C$。

若$x\in A$，则$x\in A\cup B$，$x\in A\cup C$，故$x\in(A\cup B)\cap(A\cup C)$。

若$x\in B\cap C$，则$x\in B$，$x\in C$ 那么$x\in A\cup B$，$x\in A\cup C$，故

$x\in(A\cup B)\cap(A\cup C)$. 于是总有

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

另一方面，任取$x\in(A\cup B)\cap(A\cup C)$，那么$x\in A\cup B, x\in A\cup C$。因而必有$x\in A$或$x\in B$，$x\in A$或$x\in C$。当$x\in A$时，一定有$x\in A\cup(B\cap C)$；当$x\notin A$而$x\in B, x\in C$时有$x\in B\cap C$，故$x\in A\cup(B\cap C)$。于是总有

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

因此

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

再证L_7。我们只证明$(A\cup B)'=A'\cap B'$，另一个可类似证之。

因$(A\cup B)\cup(A'\cap B')\xlongequal{L_3}A\cup(B\cup(A'\cap B'))\xlongequal{L_4}A\cup((B\cup A')\cap(B\cup B'))=A\cup((B\cup A')\cap I)=A\cup(B\cup A')\xlongequal{L_2}A\cup(A'\cup B)\xlongequal{L_3}(A\cup A')\cup B=I\cup B=I$。即

$$(A\cup B)\cup(A'\cap B')=I \tag{1}$$

又因$(A\cup B)\cap(A'\cap B')\xlongequal{L_3}((A\cup B)\cap A')\cap B'\xlongequal{L_2}(A'\cap(A\cup B))\cap B'\xlongequal{L_4}((A'\cap A)\cup(A'\cap B))\cap B'=(A'\cap B)\cap B'\xlongequal{L_3}A'\cap(B\cap B')=A'\cap\phi=\phi$。 即

$$(A\cup B)\cap(A'\cap B')=\phi \tag{2}$$

于是由(1)与(2)知$(A\cup B)'=A'\cap B'$。

集合交、并的概念可以推广到任意多个集合上去。设集合族$\{A_\alpha|\alpha\in D$①$\}$

①D是有限集或无限集

集$\{x|x$属于每个$A_\alpha\}$叫做集合族$\{A_\alpha|\alpha\in D\}$的交集，记作$\bigcap\limits_{\alpha\in D}A_\alpha$。当$\bigcap\limits_{\alpha\in D}A_\alpha=\phi$时，说集合族$\{A_\alpha|\alpha\in D\}$是不相交的。

集$\{x|x$属于某一个$A_\alpha\}$叫做集合族$\{A_\alpha|\alpha\in D\}$的并集，记作$\bigcup\limits_{\alpha\in D}A_\alpha$.

练 习 一

1. 设$A=\{1,2,3,4\}$，$B=\{2,4,6,8\}$，求$A\cap B$，$A\cup B$。并写出$P(A)$，$P(B)$。

2. 设$I=\{a,b,c,d,e,f\}$，$A=\{a,c,d\}$，$B=\{b,d,e\}$，求A'，B'，$A'\cup B'$，$A'\cap B'$，$(A\cup B)'$，$(A\cap B)'$。

3. 证明：$A\subseteq B\Longleftrightarrow A\cap B=A\Longleftrightarrow A\cup B=B$。

4. 证明：$A=B\Longleftrightarrow A\cup B=A\cap B$。

5. 令$A-B=\{x|x\in A$但$x\notin B\}$，证明：

$$A-B=A-(A\cap B),\quad A-(A-B)=A\cap B.$$

6. 证明L_3，L_5，L_6。

§2 映 射

任何事物，不论是个别的或总体的，都不是孤立的、静止的，它的内部和相互之间无不存在一定的联系，不了解这种联系就不了解事物的规律性．因此，分析事物的相互联系，从中找出规律性的东西，是人们认识事物的必由之路，也是分析问题解决问题的基本方法．着眼于事物的变化和相互关联，从事物的变化和相互关联中寻求分析问题的门径，找出解决问题的线索和方法是代数学的一个重要特点．这种方法在数学上的体现，就是把所要研究的对象——这里把它叫做

集合，对它的元素进行比较，从中发现其间的某些联系，这就是下面要定义的重要概念——集合的映射。

设A、B为任二集合。

定义1 对集合A与B给定一种规则（方法）φ，使得A中每一元素a，按照给定的规则φ，能在B中确定唯一的一个元素a'，记作φ：$a \longmapsto a'$（或$\varphi(a)=a'$），这样就说（规则）φ是A到B的一个映射．a'叫做a在φ之下的象，a叫做a'在φ之下的原象．

常用以下符号来表示φ是A到B的映射：

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

例1 设$A=\{a,b,c,d\}$，$B=\{1,2,3\}$

$$\varphi_1\text{：}\quad \begin{aligned} a &\longmapsto 1 \\ b &\longmapsto 2 \\ c &\longmapsto 3 \\ d &\longmapsto 3. \end{aligned}$$

易知φ_1是A到B的一个映射；

再令

$$\varphi_2\text{：}\quad \begin{aligned} a &\longmapsto 1 \\ b &\longmapsto 2 \\ c &\longmapsto 1 \\ d &\longmapsto 1. \end{aligned}$$

φ_2也是A到B的一个映射；

若令

$$\varphi_3\text{：}\quad \begin{aligned} a &\longmapsto 2 \\ b &\longmapsto 3 \\ d &\longmapsto 1. \end{aligned}$$

由于A中的c在φ_3之下没有象，故φ_3不是A到B的映射.

例 2 设$A=\{$甲，乙，丙，丁$\}$，$B=\{$张，王，李，赵$\}$

令

φ_1: 甲$\longmapsto$张

乙$\longmapsto$李

丙$\longmapsto$赵

丁$\longmapsto$王.

易知φ_1是A到B的一个映射；

再令

φ_2: 甲$\longmapsto$李

乙$\longmapsto$李

丙$\longmapsto$张

丁$\longmapsto$赵

丁$\longmapsto$王

由于A中的丁在φ_2之下有两个象赵与王，故φ_2不是A到B的映射.

例 3 设$A=\mathbf{N}$，$B=\mathbf{Z}$

令 φ: $n\longmapsto n$，$n\in\mathbf{N}$.

易知φ是A到B的映射.

例 4 设$A=\left\{\begin{pmatrix} a & o \\ o & a \end{pmatrix}\middle| a\in\mathbf{R}\right\}$，$B=\mathbf{R}$.

$$\varphi_1: \begin{pmatrix} a & o \\ o & a \end{pmatrix}\longmapsto a,$$

$$\varphi_2: \begin{pmatrix} a & o \\ o & a \end{pmatrix}\longmapsto a^2,$$