方正 主编

近世代数

哈尔滨地图出版社

近世代数

JINSHI DAISHU

主编 方 正

哈尔滨地图出版社

· 哈尔滨 ·

图书在版编目（CIP）数据

近世代数/方正主编.—哈尔滨：哈尔滨地图出版社，2006.4
ISBN 7-80717-305-X

Ⅰ.近... Ⅱ.方... Ⅲ.抽象代数 Ⅳ.O153

中国版本图书馆 CIP 数据核字（2006）第 036017 号

哈尔滨地图出版社出版发行
（地址：哈尔滨市南岗区测绘路 2 号 邮政编码：150086）
大庆师范学院印刷厂印刷
开本：850 mm×1 168 mm 1 / 32 印张：6.875 字数：170 千字
2006 年 4 月第 1 版 2006 年 4 月第 1 次印刷
印数：1～500 定价：20.00 元

前　言

本书是在大庆师范学院数学系多年讲授近世代数时所用的不断完善的讲义基础上，经反复修订而成的。因在教学计划中，近世代数的学时不多，不可能讲授太多、太深的内容，所以在编写过程中，在尽量保证知识的完整性与系统性的基础上，根据师范类本、专科学生实际情况，力求论述简明扼要、通俗易懂。

本书的习题按节配置，遵循循序渐进的原则，充分注意基本概念、基本方法和理论的讲解，并使学生能够透彻理解和熟练掌握所学内容。

在本书的编写过程中，曾得到史富贵教授、赵立军教授的热情鼓励和支持，在此表示诚挚的谢意。

由于编者学识水平有限，书中难免存在不妥之处，希望广大读者批评指正，使本书在教学实践中不断完善。

作　者

2006 年 4 月

目　　录

第一章　基本概念

近世代数的主要研究对象是带有运算的集合，即代数系统，本书的目的就是简略地介绍几个基本的代数系统——群、环、域、模及格的初步知识。为方便下面的学习，我们需回顾一些基本概念。

第一节　集合及其运算

集合是数学中最基本的概念之一，是现代数学的基础，集合就是一些对象的总体，例如，全体中国人是一个集合；所有自然数是一个集合，等等。集合也简称为集，常用大写字母 $A,B,C\cdots$ 来表示。

特别地，在本书中，我们用

N 表示所有自然数组成的集(简称自然数集)；

Z 表示所有整数组成的集(简称整数集)；

Q 表示所有有理数组成的集(简称有理数集)；

R 表示所有实数组成的集(简称实数集)；

C 表示所有复数组成的集(简称复数集)。

组成集的对象称为元素(简称元)，常用小写字母 $a,b,c\cdots$ 表示。若 a 是集 A 的元素，则称 a 属于 A 或 A 包含 a，记为 $a\in A$ 或 Aa。若 a 不是 A 的元素，则称 a 不属于 A 或 A 不包含 a，记为 $a\notin A$。

确定一个集合 A，就是要确定哪些元素属于 A，哪些元素不属于 A，标准必须明确。

下面这个特殊集合是常用的。

定义 1．1 一个没有任何元素的集合称为空集，记为 $\varnothing$。

集合的表示方法主要有两种：列举法和描述法。

所谓列举法就是列出集合的所有元素。例如，$A=\{a,b,c,d,e\}$ 表示集 A 由 a,b,c,d,e 组成。

所谓描述法就是描述出集合中元素适合的充要条件。例如，$A=\{x\in \mathrm{Z}|x\succ 0\}$ 表示集 A 是由所有正整数组成的集。

定义 1．2 如果两个集合 A 与 B 包含的元素完全一样，则称 A 与 B 相等，记为 $A=B$。否则记为 $A\neq B$。

定义 1．3 若集 A 的每个元素皆属于 B，则称 A 是 B 的子集，记为 $A\subset B$ 或 $B\supset A$，读做 A 含于 B 或 B 包含 A。若 A 不是 B 的子集，则记为 $A\not\subset B$。

定义 1．4 若 $A\subset B$ 且 $A\neq B$，则称 A 是 B 的真子集，记为 $A\underset{\neq}{\subset}B$。

对任意一集 A，均有 $\varnothing\subset A$，这是因为不属于 A 的元素均不在 $\varnothing$ 中。

定义 1．5 设 A 是一个集，由 A 的所有子集构成的集合称为 A 的幂集，记为 2^A。

例如，设 $A=\{1,\ 2,\ 3\}$，则

$$2^A=\{\varnothing,\{1\},\{2\},\{3\},\{1,2\},\{1,3\},\{2,3\},A\}。$$

一般地，若 A 有 n 个元，则 2^A 含有 2^n 个元。

设 X 是一个给定集，$A,B\in 2^X$。下面我们介绍集合的几种运算。

定义 1.6 由集 A 和 B 的所有共同元素组成的集合叫做 A 与 B 的交集，记为 $A\cap B$，即 $A\cap B=\{x\in X\mid x\in A且x\in B\}$。

定义 1.7 由至少属于集 A 与集 B 之一的所有元素组成的集合叫做 A 与 B 的并集，记为 $A\cup B$，即

$$A\cup B=\{x\in X\mid x\in A或x\in B\}。$$

定义 1.8 由所有属于 A 但不属于 B 的元素组成的集合叫做 B 在 A 中的补集，记为 $A\setminus B$，特别地，B 在 X 中的补集简称为 B 的补集，记为 B'。

下面的运算性质是显然的，证明略。

性质 1.1 取定集 X，则对 X 的任意子集 A，B，C 而言，运算“$\cap,\cup,'$”满足下面结论：

(1) $A\cap A=A$，$A\cup A=A$（幂等律）；

(2) $A\cap B=B\cap A$，$A\cup B=B\cup A$（交换律）；

(3) $(A\cap B)\cap C=A\cap(B\cap C)$，

$(A\cup B)\cup C=A\cup(B\cup C)$（结合律）；

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

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

(5) $A\cap X=A$，$A\cup X=X$，

$A\cup\varnothing=A$，$A\cap\varnothing=\varnothing$（单位律）；

(6) $A\cup A'=X$，$A\cap A'=\varnothing$（补余律）；

(7) $(A')'=A$（对合律）；

(8) $(A\cap B)'=A'\cup B'$，

$(A\cup B)'=A'\cap B'$（对偶律或笛莫根律）。

集合的交、并也可推广到任意多个集合的情形。

定义 1．9 设 A_i（$i\in I$）是集 X 的一族子集，定义集族 $\{A_i\mid i\in I\}$ 的交、并如下：

$$\bigcap_{i\in I}A_i=\bigcap\{A_i\mid i\in I\}=\{x\in X\mid \forall i\in I,x\in A_i\},$$

$$\bigcup_{i\in I}A_i=\bigcup\{A_i\mid i\in I\}=\{x\in X\mid \exists i\in I,x\in A_i\}$$，这里“$\forall$”表示“任意”，“$\exists$”表示“存在”，I 叫做指标集。当 $I=\varnothing$ 时，我们约定

$$\bigcap_{i\in I}A_i=X,\ \bigcup_{i\in I}A_i=\varnothing。$$

最后，我们引入集的卡氏集的概念。

定义 1．10 设 $A_1,A_2,\cdots,A_n$ 是 n 个集，称所有 n 元有序组 $(a_1,a_2,\cdots,a_n)$ 构成的集为 $A_1,A_2,\cdots,A_n$ 的卡氏集，简称积，其中每个 $a_i\in A_i$，$i\in\{1,2,\cdots,n\}$；并记为 $A_1\times A_2\times\cdots\times A_n$ 或 $\prod_{i=1}^{n}A_i$。

习题 1——1

1. 试证本节中的对偶律。

2. 设 A，B 是给定集 X 的子集，定义集 $A\Delta B$ 如下：

$$A\Delta B=(A\cup B)\setminus(A\cap B)。$$

$A\Delta B$ 称为 A 与 B 的对称差，试证：

（1）$A\Delta B=B\Delta A$；　　（2）$A\Delta\varnothing=A$；

（3）$A\Delta A=\varnothing$；　　（4）$(A\Delta B)\Delta C=A\Delta(B\Delta C)$。

3. 试证下列事实成立：

（1）$A\times(B\cup C)=(A\times B)\cup(A\times C)$；

（2）$A\times(B\cap C)=(A\times B)\cap(A\times C)$；

（3）$(A\times B)\cap(C\times D)=(A\cap C)\times(B\cap D)$。

第二节　二元关系、等价关系、集的分类

定义 2.1　积集 $A\times B$ 的一个子集 R 称做 A，B 间的一个二元关系。当 $(a,b)\in R$ 时，称 a 与 b 有关系 R，记为 aRb。当 $(a,b)\notin R$ 时，称 a，b 没有关系 R，记为 $aR'b$。A 与 A 间的二元关系也称为 A 的二元关系。

$\forall(a,b)\in A\times B$，要么 $(a,b)\in R$，要么 $(a,b)\notin R$，二者有且

仅有一个成立。

一个二元关系就是把 A 中某些元与 B 中某些元的相关性给以形式化。

例 2．1 设 $A=\{a_1,a_2,a_3,a_4\}$ 表示 4 个学生的集合，$B=\{b_1,b_2,b_3,b_4,b_5,b_6\}$ 表示 6 门课程的集合，则 $A\times B$ 给出了学生和课程之间的所有配对，共有 24 个元，设 $R=\{(a_1,b_2),(a_2,b_2),(a_2,b_4),(a_3,b_2),(a_3,b_3),(a_3,b_5),(a_4,b_3),(a_4,b_6)\}$，则 R 表示学生们与选学课程间的一个二元关系。如 $(a_2,b_4)\in R$ 表明学生 a_2 选学课程 b_4，$(a_2,b_3)\notin R$ 表明学生 a_2 不选学课程 b_3。

例 2．2 在有理数集 Q 中，大于关系“$\succ$”就是下面集合 $R=\{(x,y)\mid x,y\in \mathrm{Q},x\succ y\}$。$(3,2)\in R$ 表明 $3\succ 2$，$(2,3)\notin R$ 表明 $2\not\succ 3$，即 $2\leq 3$。

例 2．3 设 $A=\mathbf{R}$，令

$$R_1=\{(a,b)\mid a,b\in \mathrm{R},a=2b\}\ ,$$

$$R_2=\{(a,b)\mid a,b\in \mathrm{R},a^2+b^2=1\}\ .$$

$\forall a,b\in \mathrm{R}$，$aR_1b\Leftrightarrow (a,b)$ 在直线 $x=2y$ 上，$aR_2b\Leftrightarrow (a,b)$ 在单位圆上。

例 2．4 设 $Z_n=\{(a,b)\mid a,b\in Z,n\mid a-b\}$，这里 n 是非零整

数，$\forall a,b\in\mathbf{Z}$，$aZ_nb\Leftrightarrow a-b=kn$ （$k\in\mathbf{Z}$）。当$\forall a,b\in Z_n$时，

我们称a,b关于模n同余，记为$a\equiv b(n)$，Z_n称为同余关系。

二元关系有各种不同的类型，其中等价关系占有很重要的地位，下面我们介绍其定义。

定义 2．2 集A的一个二元关系R叫做一个等价关系，如果R满足下面条件：

(1)反身性：$\forall a\in A$，aRa；

(2)对称性：$aRb\Rightarrow bRa$；

(3)传递性：aRb，$bRc\Rightarrow aRc$。

为别于其它关系，以后常以“～”表示等价关系。

若$a\sim b$，则称a与b等价。

例 2．5 （1）设A表示一学院在校学生之集合，R是A中的一个二元关系，此时我们规定：

$\forall a,b\in A$，$aRb\Leftrightarrow a$和b住同一宿舍，则R是A中的一个等价关系。

(2)整数集$\mathbf{Z}$中的同余关系Z_n是一个等价关系。

一个集合中的等价关系与集合的分类这一概念密切相关。

定义 2．3 若一个集合A能写成非空且互不相交的若干子集A_i（$i\in I$）的并，则称$\{A_i\mid i\in I\}$为A的一个分类，而称每个A_i为一个类。

例 2．6 一副扑克牌中有花色的共有52张，按花色分类，可分为四个类，按数的大小分，可分为13类。

定义 2．4 设～是集A的一个等价关系，$\forall a\in A$，令

$[a]=\{x\in A\mid x\sim a\}$，则$[a]$是非空集，称$[a]$为$A$的一个等价类。

引理 2．1 等价类具有下列性质：

(1) $\forall a\in A$，$a\in[a]$；

(2)$\forall b,c\in[a]\Rightarrow b\sim c$；

(3) $b\in[a]$，$b\sim c\Rightarrow c\in[a]$。

证 (1)是显然的；由$b,c\in[a]\Rightarrow b\sim a,a\sim c\Rightarrow b\sim a,c\sim a$

$\Rightarrow b\sim c$，知(2)成立；再由$b\in[a]$，$b\sim c\Rightarrow b\sim a,b\sim c\Rightarrow$

$b\sim a,c\sim b\Rightarrow c\sim a\Rightarrow c\in[a]$，可证(3)。

由引理 2．1 可知，当$b\in[a]$时，$[a]=[b]$，即等价类可由其中的任意一元素作为代表，也就是说，等价类与其代表的选择无关。

定理 2．1 设$\sim$是集A的一个等价关系，则

(1) $A=\cup\{[a]\mid a\in A\}$。

(2) $\forall a,b\in A$，或者$[a]\cap[b]=\varnothing$，或者$[a]=[b]$，即$\sim$决定A的一个分类。

反之，若$\{A_i\mid i\in I\}$是A的一个分类，则其决定A的一个等价关系。

证 设$\sim$是A的一个等价关系，则(1)显然成立。$\forall a,b\in A$，

由

$[a]\cap[b]\neq\varnothing \Rightarrow c\in[a]\cap[b] \Rightarrow c\sim a, c\sim b \Rightarrow [a]=[b]$，可知(2)成立。

反之，$\{A_i \mid i\in I\}$是A的一个分类。当$a,b\in A_i$时，规定$a\sim b$，则$\forall a\in A$，$a\sim a$是显然的；若$a\sim b$，则a,b属于同一类，当然$b\sim a$；再者，若$a\sim b$，$b\sim c$，则a,b属于同一类，b,c属于同一类，当然a,c也在同一类，从而$a\sim c$，故$\sim$是A的一个等价关系。

在例 2．4 中，等价关系Z_n所决定的 Z 的分类为：

$$[0]=\{kn \mid k\in \mathrm{Z}\},\quad [1]=\{kn+1 \mid k\in \mathrm{Z}\},$$

$$[2]=\{kn+2 \mid k\in \mathrm{Z}\},\ \cdots,\ [n-1]=\{(k+1)n-1 \mid k\in \mathrm{Z}\}。$$

这样得来的类叫做模n的剩余类。

在例 2．6 中，如按花色分为四类，则决定的等价关系就是同种花色；如按大小分类，则决定的等价关系是大小相同。

定义 2．5 集A的一个等价关系$\sim$所决定的等价类的集合$\{[a] \mid a\in A\}$，常以$A/\sim$记之，称为A关于$\sim$的商集。

显然$A/\sim \subset 2^A$。

习题 1——2

1. 设 $A=\{a,b,c\}$，下列关系是否具有反身性、对称性与传递性？

(1) $R=\{(a,a)\}$；　　(2) $R=\{(a,b),(b,a)\}$；

(3) $R=\varnothing$；　　(4) $R=\{(a,a),(b,b),(a,b)\}$。

2. 设 A 为平面上所有直线之集，R 是 $A\times A$ 中满足下面条件的子集，

$$R=\{(l_1,l_2)\mid l_1,l_2\in A,l_1 /\!/ l_2 \text{或} l_1=l_2\}。$$

试证 R 是 A 中的等价关系，试决定相应的等价类。

3. 设 $A=\{1,2,3,4\}$，R 是 $2^A\times 2^A$ 中满足下面条件的子集，$R=\{(B,C)\mid B,C\in 2^A,B,C\text{含有相同个数的元}\}$，试证 R 是等价关系，写出商集 A/R。

4. 设 R_1，R_2 是集 A 的两个等价关系，那么 $R_1\cap R_2$，$R_1\cup R_2$ 是不是 A 的二元关系？是不是等价关系？为什么？

第三节　映射、代数运算

定义 3.1　设 A，B 是两个集，f 是 A，B 间的二元关系，如

果$\forall x \in A$，都有惟一的$y \in B$使得$(x,y) \in f$，则称关系f为A到B的映射，记为$f:A \to B$，我们也常以$y=f(x)$来表示$(x,y) \in f$。

若$(x,y) \in f$，则称x为自变元，y为x在f下的象，x也称为y在f下的原象。A称为定义域、B称为值域。

一个映射$f:A \to B$实际上是由三元组(A,B,f)决定的，若$g:A_1 \to B_1$是另一映射，则当且仅当$A=A_1$，$B=B_1$，$f=g$时，我们才认为$f:A \to B$与$g:A_1 \to B_1$相同，此时仍记为$f=g$。

例3.1 (1)设$A=\mathrm{Z}$，$B=\mathrm{R}$。我们规定A，B间的关系f为$f=\{(x,x^2) \mid x \in \mathrm{Z}\}$，则$f$是$A$到$B$的映射，可记为$f:A \to B$，$f(x)=x^2$。

(2)设$A=B=\mathrm{N}$，我们规定N的二元关系f为$f=\{(n,n-1) \mid n \in \mathrm{N}, n \geq 2\}$，则$f$不是$A$到$B$的映射，因为当$n=1$时，找不到N中元素$m$，使$(n,m) \in f$。