高等师范专科学校试用教材

群环域基础

主编 晏能中
郭卫舵

高等师范专科学校试用教材

群环域基础

江苏工业学院图书馆
藏书章

主编 吴能中 郭卫鲸
副主编 潘杰 涂文艳

滇新登字07号

群环域基础

主编：晏能中　郭卫舵

责任编辑：李继毛

云南大学出版社出版发行
（云南大学校内）
云南师范大学印刷厂印刷

开本　787×1092/32　　印张　4.85　字数113千字
1992年3月第1版　　1992年3月第1次印刷

印数　0001—2200

ISBN 7—81025—185—6/O·7　定价：2.99元

前　言

《近世代数》是高等师范专科学校和教育学院数学专业的一门重要专业课程，各校都作为必修或选修课程开出。但，已经出版的近世代数教科书，一般都是为本科院校学生编写的。本书是专为师专和教院的学生而编写。为此，编写时力求做到科学性、系统性、思想性、通俗性和应用性，取材适当，条理清晰，由浅入深，通俗易懂，还配备了较多的例题和习题，以适应基础与本科生不同的师专和教院学生的学习，也能满足广大自学读者的需要。

本书在编写过程中，注意到师专和教院的近世代数课程都是在学习了《高等代数》后开出，课时一般不超过72个。为此，我们对常见近世代数教材中的内容做了较大调整，以保证在有限的课时内，让学生学习并掌握好该课程的主要内容。同时，为突出这一特点，还将本书定名为《群环域基础》。

显然，这仅仅是一种抛砖引玉的尝试。我们相信，经过全国师专、教院代数同行们的共同实践和努力，一定会有更多、更好的近世代数教材问世，本书也将随之得到完善和提高。

参与本书编写的有：四川达县师专晏能中（主编）、云南昆明师专郭卫舵（主编）、四川万县师专潘杰（副主编）、河南驻马店师专涂文彪（副主编）。本书在编写过程中，得到了吉林省数学会秘书长、吉林大学数学系牛凤文教授的指导，并审阅全文，写出了推荐意见。同时，还得到了四川宜宾师专数学系主任王国炳副教授的热情帮助，提供了不少有价值的修改意见。在此，谨向他们致以衷心的感谢。

编　者

一九九二年一月二十五日于昆明

目　录

此为试读，需要完整PDF请访问：www.ertongbook.com

第三章　域

第一章 群 论

群是一种代数体系，是近世代数的重要组成部分，它不仅是许多自然科学的基础理论，而且在一些应用学科中，也有着广泛的应用，如在自动机理论，编码理论和快速加法器的设计中都要用到它。

本章主要叙述群的一些基本性质和几种特殊的群——循环群、变换群、置换群以及正规子群和商群，最后讨论群的基本定理。

§1 代数运算与运算定律

我们把具有代数运算的集合，称为代数体系（或代数系统）。那么，什么叫代数运算呢？为此，先给出与代数运算有关的笛卡儿积的概念。

设A_1，A_2，…，A_n是任意n个集合，依次从A_1，A_2，…，A_n中，取出a_1，a_2，…，a_n。组成有序元素组$(a_1, a_2 \cdots, a_n)$所成的集合，叫做集合A_1，A_2，…，A_n的积。记为$A_1 \times A_2 \times \cdots \times A_n = \prod_{i=1}^{n} A_i = \{(a_1, a_2, \cdots, a_n) | a_i \in A_i, i = 1, 2 \cdots, n\}$。当$n=2$时，称$A_1 \times A_2 = \{(a_1, a_2) | a_i \in A_i, i = 1, 2\}$为$A_1$，$A_2$的笛卡儿积。

例1 实数集R（在本书中，R代表实数集，Q代表有理数

集，C代表复数集，Z代表整数集），$R\times R=\{(a,\ b)|a,\ b\in R\}$笛儿积，就是我们常说的笛卡儿平面。

为了给出代数运算，再介绍一下映射的概念。

设A_1，A_2，…，A_n为n个集合，D为另一个集合，规定一个法则φ，使个得对任何一$A_1\times A_2\times\cdots\times An$的元$(a_1,a_2,\ \cdots,\ an)$，都有D的唯一的一个元d与之对应。则称φ窗为集合$A_1\times A_2\times\cdots\times A_n$到集合D的一个映射。元素d称为元素$(a_1,\ a_2,\ \cdots,\ a_n)$在φ之下的象，元素$(a_1,\ a_2,\cdots,\ a_n)$称为元素d在φ之下的原象(逆象)，记为$\varphi((a_1,\ a_2,\ \cdots,\ a_n))=d$。

当n＝2时，$A_1\times A_2$到D的映射，称为$A_1\times A_2$到D的代数运算。

当$A_1=A_2=D=A$时，就称$A_1\times A_2$到D的代数运算为二元运算。当然$A\times A\times\cdots\times A$到A的映射，就称为n元运算。

由于代数运算是特殊的映射，我们就用特殊的记号来表示，常用“o”表示，因此，$A\times A$到D的代数运算用

$o:(a,\ b)\longrightarrow d=o(a,\ b)=aob$表示。有时为了方便表$o(a,\ b)$写成ab，

即 $$o:(a,\ b)\longrightarrow d=ab.$$

例2 R为实数集，R*为非零实数集，令

$$o:\ R\times R^*\longrightarrow R,(a,\ b)\longrightarrow\frac{a}{b},$$

其中$(a,b)\in R\times R^*(a\in R,b\in R^*)$，$\frac{a}{b}$有意义，所以“o”是$R\times R^*$到R的代数运算，这就是常见的普通数的除法。

整数集的加法，减法，乘法就是Z的二元运算，取负元就

是一元运算。在有理数集Q中，加法和乘法是二元运算，而取逆元不是Q的一元运算，因为不是Q的一切元都有逆元。如果Q^*表示非零有理数集则Q，*的除法是二元运算，取逆元是一元运算，但加法和减法不是Q^*的二元运算，因$a+(-a)=0\in Q^*$，$a-a=0\in Q^*$。

设“o”是集合A的一个代数运算，把A与“o”当成一个整体，叫做代数体系(或代数系统)，记为$<A, o>$，如果A有两个代数运算o_1，o_2，代数体系记为$<A, O_1, O_2>$，如$<R, +>$，$<R, \cdot>$，$<R, +, \cdot>$都是代数体系。$<M_n(R), +>$，$<Mn(R), +, \cdot>$（$M_n(R)$）表示实数集R上的n阶矩阵集合，“+”表示矩阵加法，“·”表示矩阵乘法）也是代数体系。

下面，我们研究代数体系的一些运算定律。

定义1　给定代数体系$<A, O>$，$\forall$（$\forall$表示任意）a，$b\in A$，如果$ao(boc)=(aob)oc$成立，则称代数运算“o”满足结合律。

定义2　给定代数体系$<A, o>$，$\forall a, b\in A$，如果$aob=boa$，则称代数运算“o”满足交换律。

设$\oplus$，$\odot$是集合A的两个不同的代数运算，其中$\oplus$称为A的加法，$\odot$称为A的乘法，于是有

定义3　给定代数体系$<A, \oplus, \odot>$，$\forall a, b, c\in A$，如果

$$a\odot(b\oplus c)=(a\odot b)\oplus(a\odot c)$$

$$(b\oplus c)\odot a=(b\odot a)\oplus(c\odot a)$$

都成立，则称$\odot$对$\oplus$满足分配律。如果只有前一个等式成立，就称$\odot$对$\oplus$满足左分配律，如果只有后一个等式成立，则称$\odot$

对⊕满足右分配律。

例3　代数体系$<Z, +, \cdot>$，代数运算“+”，“·”都满足结合律和交换律，乘法“·”对“+”满足分配律。但代数体系$<Z, ->$，减法不满足结合律，也不满足交换律，例如$(3-2)-1 \neq 3-(2-1)$，$5-3 \neq 3-5$。

下面研究结合律，交换律，分配律究竟有什么实际意义。

在代数体系$<A, o>$中，$\forall a, b \in A$，有唯一的$aob \in A$。因此，对A中任意$n(n \geq 2)$个元素，通过代数运算能得到唯一的一个元素。但是，我们知道，对$\forall a, b, c \in A$，就有两种不同计算方式算出结果来：

$(aob)oc$和$ao(boc)$。

对$\forall a, b, c, d \in A$(限定a，b，c，d这样的顺序)，就有五种不同的计算方式算出结果来：

$((aob)oc)od$，$(aob)o(cod)$，$(ao(boc))od$，

$ao((boc)od)$，$ao(bo)(cod)$。

我们要问这种五种不同的计算方式（或五种不同的加括号方法）算出的结果会一样吗？

更一般地是$Aa_1, a_2, \cdots a_n \in A$（元素的顺序不变）共有$\frac{(2n-2)!}{n!\,(n-1)!}$种计算方式，其结果会一样吗？下面将证明，如果结合律成立，则不论按照那种计算方式，其结果是一样的。

定理1　在代数体系$<A, O>$中，“○”满足结合律，对$Aa_1, a_2, \cdots, a_n \in A$（它们的顺序不变）用任何方式计算的结果是一样的。

证明 $\prod_{i=1}^{n} a_i$ 表示 $a_1, a_2, \cdots, a_n$ 按顺序计算的结果，即

$$\prod_{i=1}^{n} a_i = (((a_1 o a_2) o a_3) o \cdots o a_{n-1}) o a_n .$$

用归纳法，证明n个元素的任何一种计算方式都等于 $\prod_{i=1}^{n} a_i$ 即可。

$n = 3$ 时，命题成立。

假定 $k < n$ 时，命题成立。

当n个元素的任一种计算方式，最后一步，总归结为两个元素的计算：aob，设a表示m个元素 $a_1, a_2, \cdots, a_m$ 的计算结果，b表示n－m个元素 $a_{m+1}, a_{m+2}, \cdots, a_n$ 的计算结果，$1 \leq m < n$，由归纳假设没有：

$$a = \prod_{i=1}^{m} a_i, \quad b = \prod_{j=1}^{n-m} a_{m+j} .$$

现在只需证：$aob = \prod_{i=1}^{n} a_i$ 即可。

事实上，

$$aob = \left(\prod_{i=1}^{m} a_i\right) o \left(\prod_{j=1}^{n-m} a_{m+j}\right)$$

$$= \left(\prod_{i=1}^{m} a_i\right) o \left(\prod_{j=1}^{n-m-1} a_{m+j} a_n\right)$$

$$= \left(\prod_{i=1}^{m} a_i o \prod_{j=1}^{n-m-1} a_{m+j}\right) o a_n$$

$$= \left(\prod_{i=1}^{n-1} a_i\right) o a_n = \prod_{i=1}^{n} a_i .$$

证毕

此为试读，需要完整PDF请访问：www.ertongbook.com

在代数体系$<A, o>$中，只要“o”满足结合律，对任意n（$n \geqslant 3$）个元，不论那种方式括加号，计算出来的结果是一样的，但元素的次序不能改变，否则运算结果一般不一样。如果运算满足交换律，这种限制就没有必要了，这是因为有

定理2　在代数体系$<A, o>$中，如果“o”同时满足结合律和交换律，那么在$a_1 o a_2 o \cdots o a_n$中，元素的次序可以掉换。

证明　对n作归纳法，$n=2$时，命题成立。假定元素个数$<n$时，命题成立，要证元素个数为n时，命题亦成立。

令$i_1, i_2, \cdots, i_n$是1，2，…，n的任意一个排列，如能证得$a_{i_1} o a_{i_2} o \cdots o a_{i_n} = a_1 o a_2 o \cdots o a_n$即可。

在$i_1, i_2, \cdots, i_n$中，必有一个n，不妨设，$i_k = n$，于是有

$$\begin{aligned} & a_{i_1} o a_{i_2} o \cdots o a_{i_k} o \cdots o a_{i_n} \\ &= a_{i_1} o \cdots o a_n o \cdots o a_{i_n} \\ &= (a_{i_1} o \cdots o a_{i_{k-1}}) o (a_n o (a_{i_{k+1}} o \cdots o a_{i_n})) \\ &= (a_{i_1} o \cdots o a_{i_{k-1}}) o (a_{i_{k+1}} o \cdots o a_{i_n}) o a_n \\ &= (a_1 o \cdots o a_{n-1}) o a_n = a_1 o \cdots o a_{n-1} o a_n . \end{aligned}$$

证毕

在代数体系$<M_n(F), o>$中，代数运算“o”就是矩阵的法，它不满足交换律，因此定理2在$<M_n(F), o>$中，不成立。

下面讨论分配律

定理3．在代数体系$<A, \oplus, \odot>$中，$\oplus$满足结合律，$\odot$对$\oplus$满足分配律，那么

$$\begin{aligned} & a \odot (b_1 \oplus b_2 \oplus \cdots \oplus b_n) \\ &= (a \odot b_1) \oplus (a \odot b_2) \oplus \cdots \oplus (a \odot b_n) . \\ & (b_1 \oplus b_2 \oplus \cdots \oplus b_n) \odot a \\ &= (b_1 \odot a) \oplus (b_2 \odot a) \oplus \cdots \oplus (b_n \odot a) . \end{aligned}$$

证明　用数学归纳法，当$n=2$时，命题成立。假设b的个

数小于n 时，命题成立。于是有

$$\begin{aligned} & a\odot(b_1\oplus b_2\oplus\cdots\oplus b_n) \\ &= a\odot((b_1\oplus\cdots\oplus b_{n-1})\oplus b_n) \\ &= a\odot(b_1\oplus\cdots\oplus b_{n-1})\oplus(a\odot b_n) \\ &= (a\odot b_1)\oplus\cdots\oplus(a_1\odot b_{n-1})\oplus(a\odot b_n) \end{aligned}$$

同理可证第二个分配律。 证毕

在代数体系$<A, o>$中，集合A的非空子集B，对A的代数运算“o”，B亦构成一个代数体系$<B,o>$，我们称$<B, o>$为$<A,o>$的子代数体系。例如$<R^+,o>$是代数体系$<R,o>$的子代数体系(R 表示正实数集)。

习 题 一

1．R^+为正实数集，Q 为正有理数集，证明$<R^+, \oplus, \odot>$构成一个代数体系其中

$$a\oplus b=\frac{a+b}{2},\quad a\odot b=\sqrt{ab}\ .$$

$<Q^+, \oplus, \odot>$对上面规定的加和乘是否构成代数体系，是否为$<R^+, \oplus, \odot>$的子代数体系。

2．$<R^*, o>$，其中$aob=\frac{a}{b}$，是否适合结合律。

3．$R=\{实数\}$，$aob=a+2b$，“o”是否为R的代数运算，如果是，适不适合结合律？

4．$R=\{实数\}$，$aob=a-b$是否为R的代数运算，如果是，适不适合交换律？

5．$A=\{a,b,c,d\}$，由表

o	a	b	c	d
a	**a**	b	c	**d**
b	b	d	a	c
c	c	a	b	d
d	d	c	a	b

所给的代数运算，适不适合交换律？

§2 集合的分类与等价关系

研究代数体系，就是对规定有代数运算的集合进行研究，对这样的集合进行研究的方法，往往是从局部去研究整体，即通过子代数系统去了解掌握整个代数系统。为此先介绍集合的分类，再介绍等价关系。

例1 $A=\{(x,y)|(x,y)\in R\times R$

$R_1=\{(x,y)\in R\times R|x^2+y^2=1\}$.

$R_2=\{(x,y)\in R\times R|x^2+y^2<1\}$.

$R_3=\{(x,y)\in R\times R|x^2+y^2>1\}$.

显然，(1)$R_i\neq\phi$. $i=1,2,3$.

(2) $\bigcap_{i=1}^{3} R_i=\phi$.

(3) $A=\bigcap_{i=1}^{3} R_i$.

这样就把平面上的点分为三类，而且平面上的点(x,y)属

于一类而且只属于一类。

例2 $Z=\{\cdots,-2,-1,0,1,2,\cdots\}$

$R_0=\{n\in Z\mid n=4k\}$.

$R_1=\{n\in Z\mid n=4k+1\}$.

$R_2=\{n\in Z\mid n=4k+2\}$.

$R_3=\{n\in Z\mid n=4k+3\}$.

显然 (1) $R_i\neq\phi$. $i=0,1,2,3$.

(2) $\bigcap_{i=0}^{3}R_i=\phi$.

(3) $\bigcup_{i=0}^{3}R_i=Z$.

这样把整数集Z分成四类,而且Z的每一个元素属于一类而且只属于一类。

由此,我们给出集合分类的概念。

定义1 设A为任意集合,$T=\{R_\alpha\mid\alpha\in I\}$,其中$R_\alpha$是A的一些子集,I是$R_\alpha$的下标组成的集合,如果有

(1) $\forall\alpha\in I, R_\alpha\neq\phi$,

(2) $\forall\alpha,\beta\in I,\alpha\neq\beta$,有$R_\alpha\cap R_\beta\neq\phi$,

(3) $\bigcup_{\alpha\in I}R_\alpha=A$,

那么称T是集合A的一个分类,称R_α为集合A的一个类。

在研究一个集合的子集时,往往遇着集合的两个元素同属于一个子集,或不同属于一个子集,二者必居其一,这就是一个集合的元素间的一个二元关系,上面给出二元关系概念。

定义2　$A\times A$的一个子集R称为A的元素间的一个二元关系，即如果$A\times A$的一个元$(a,b)\in R$，就说a,b具有关系R，记为aRb。如果$(a,b)\in R$，就说a，b不具有系R，记为$a\overline{R}b$。

$\forall a, b\in A$，那么(a, b)在R之中，或(a, b)不在R之中，二者必居其一，故有关aRb或$a\overline{R}b$。

例3　$A=R=\{$实数$\}$。

$$R_1=\{(a,b)\mid(a,b)\in R\times R,\ a=b\}.$$

显然，$a, b\in R$，$(a,b)\in R_1$，当且仅当$a=b$，即aR_1b，当且仅当$a=b$，或者当a，b相等时，就称a与b具有R_1关系，因此，R_1是R的元素间的一个相等关系。

$$R_2=\{(a, b)\mid(a, b)\in R\times R,\ a\leqslant b\}。$$

$a, b\in R$，如果$(a, b)\in R_2$即aR_2b当且仅当$a\leqslant b$。称R_2是R的元素间“小于等于”关系。

$$R_3=\{(a, b)\mid(a, b)\in Z\times Z,\ a=2b\},$$

$a, b\in R$，$(a, b)\in R_3$，即aR_3b当且仅当(a, b)在直线$x=2y$上，称R_3表示R的两个元素在直线$x=2y$上的关系。

例4　$A=Z=\{\cdots, -2, -1, 0, 1, 2, \cdots\}$。

$R_m=\{(a, b)\mid(a, b)\in Z\times Z,\ m\mid a-b\}$。（注）

$a, b\in Z$，$(a, b)\in R$，即aR_mb当且仅当$m\mid a-b$，即aR_nb当且仅当$a-b=mk$ $(k\in Z)$，故R_m是Z的元素间的一个关系，常称R是Z的元素间的同余关系。

上面研究的集合A的元素间的二元关系，往往具有某种特殊关系——等价关系。

定义3　集合A上的元素间的一个二元关系R称为等价关系，如果下列三条被满足：

注：“$m\mid a-b$”表示“m能整除$a-b$”

（1）反身性：$\forall a \in A$，有aRa。

（2）对称性：$\forall a, b \in A$，$aRb \Longrightarrow bRa$（$\Longrightarrow$表示能推出）。

（3）传递性：$\forall a, b, c \in R$，aRb，bRc，$\Longrightarrow aRc$。

等价关系记为“$\sim$”。

例5　在例3中，R_1是一个等价关系。R_2不是等价关系，因R_2不具有对称性。R_3也不是等价关系，因不具有对称性。在例4中，R_m是一个等价关系：（1）$\forall a \in Z$，有aR_ma当且仅当$m|a-a$。（2）$\forall a, b \in Z$，若$aR_mb \Longrightarrow m|a-b=-(b-a)$，$\Longrightarrow m|b-a \Longrightarrow bR_ma$。（3）$\forall a, bc \in Z$，若$aR_mb$，$R_mc$，$\Longrightarrow m|a-b, m|b-c$，$\Longrightarrow m|(a-b)+(b-c)=a-c$，$\Longrightarrow aR_mc$。故R是Z的元素间的一个关等阶系。

下面研究集合A的分类与等价关系之间的联系。

设$\sim$是集合A的一个等价关系，$a \in A$，令$\overline{a}=\{x \in A | x \sim a\}$，即$\overline{a}$表示A中与a个价的元素所组成的集合，则$\overline{a}$是A的一个非空子集，因$a \sim a$，故$a \in \overline{a}$，即$\overline{a}$至少含有一元a。称$\overline{a}$为A的一个等价元素类，或称a所在的等价类，而a为类$\overline{a}$的代表。

引理　a所在的等价类$\overline{a}$具有以下性质：

（1）$a \in \overline{a}$。

（2）同属一类的元素等价，即$b, c \in \overline{a}$，有$b \sim c$。

（3）等价的元素同属一类，即$b \in \overline{a}$，且$x \sim b$，有$x \in \overline{a}$。

证明　（1）因$a \sim a$，$\Longrightarrow a \in \overline{a}$。

（2）若$b, c \in \overline{a}$，$\Longrightarrow b \sim a, c \sim a$，$\Longrightarrow b \sim a$，$a \sim c$，$\Longrightarrow b \sim c$。

（3）因$b \in \overline{a}$，$\Longrightarrow b \sim a$，因$x \sim b$，$\Longrightarrow x \sim a$，$\Longrightarrow x \in \overline{a}$。

证毕

此为试读，需要完整PDF请访问：www.ertongbook.com