高等学校数学系列教材

近世代数基础

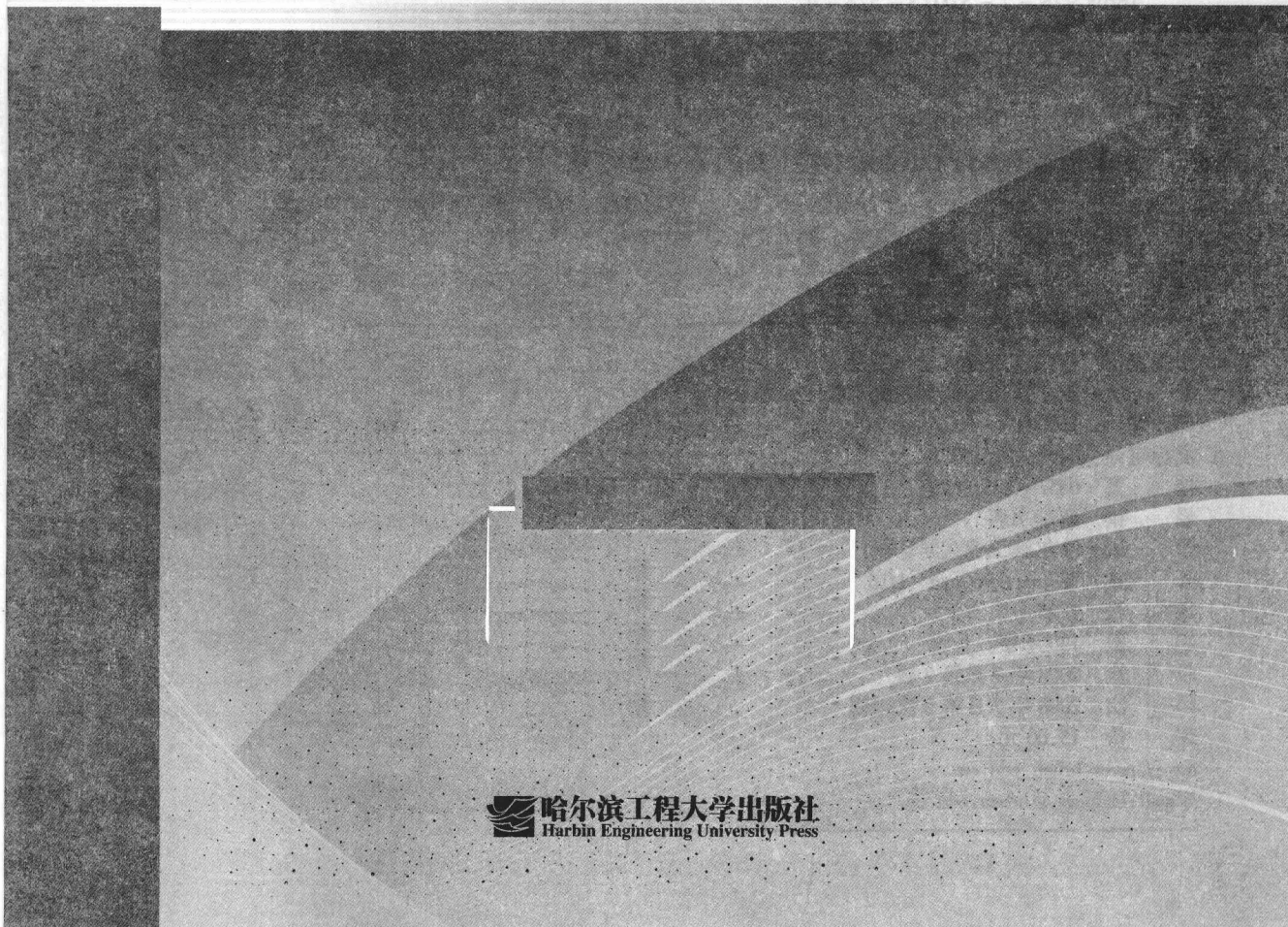
主编 / 范崇金

哈尔滨工程大学出版社
Harbin Engineering University Press

高等学校数学系列教材

近世代数基础

主编 / 范崇金



哈尔滨工程大学出版社
Harbin Engineering University Press

内容简介

本书作为工科院校研究生用的近世代数教材，介绍了代数运算、群、环、域及格与布尔代数的基础知识，内容简明扼要。

本书也可作为应用数学专业短学时的近世代数教材和参考书。

图书在版编目(CIP)数据

近世代数基础/范崇金主编.—哈尔滨：哈尔滨工程大学出版社，2003
ISBN 978-7-81073-528-4

Ⅰ.近… Ⅱ.范 Ⅲ.抽象代数-研究生-教材 Ⅳ.O153

中国版本图书馆 CIP 数据核字(2003)第 002536 号

出版发行 哈尔滨工程大学出版社
社　　址 哈尔滨市南岗区东大直街 124 号
邮政编码 150001
发行电话 0451-82519328
传　　真 0451-82519699
经　　销 新华书店
印　　刷 哈尔滨工业大学印刷厂
开　　本 787mm×960mm 1/16
印　　张 7.25
字　　数 130 千字
版　　次 2008 年 7 月第 2 版
印　　次 2008 年 7 月第 2 次印刷
定　　价 15.00 元
http://press.hrbeu.edu.cn
E-mail:heupress@hrbeu.edu.cn

前言

在我校研究生教材建设专项资金的资助下，本书得以出版。

随着计算机科学和信息科学的飞速发展，许多学科和领域要处理离散的数学结构——代数结构，有些学科甚至需要较深的近世代数知识。许多工科专业，特别是计算机科学专业的研究生急需开设近世代数课程。近世代数原为数学系一门较难的专业课。目前，绝大多数近世代数教材都是针对数学专业的。数学专业的教材以培养学生的数学素养、以数学研究为最终目的，追求纯数学的完美，篇幅浩大。显而易见，这样的教材是不适合工科研究生的。鉴于此，本书作者，在工科研究生教学和应用数学本科专业教学的基础上编写了此书。

编写教材，写厚容易，写薄难，对于一门36学时的课程更是如此。更难的是，如何使一门极其抽象的数学课程适合工科学生。鉴于本书的对象及学时所限，作者参阅了许多国内外优秀教材，以基础知识为本，尽力以最合理的安排和最新的处理使本教材简明扼要、通俗易懂、突出核心内容和骨干结构。近世代数的核心内容极其抽象，为使学生不致感到太枯燥，为增加学习兴趣，也为了展示近世代数应用的潜力，我们选择介绍了近世代数在几个方面的简单应用。

我校戴遗山教授和唐向浦教授审阅了本书的初稿，提出了非常好的建议，在此向他们表示由衷的感谢。限于作者的能力及知识视野，书中的不当之处在所难免，欢迎各方面的批评和建议。

全书授课时数需要约48学时；没标有☆号的内容可以构成一个36学时的简明教程。由于近世代数的习题较难，本书在最后对习题，特别是证明题给出了较详细的解答。标有*号的习题较难，只供有兴趣的学生练习。

哈尔滨工程大学理学院

编　者

目录

第1章　基本概念

在中学代数中，我们的运算对象是实数或复数．在大学的线性代数中，我们又将运算对象扩大到了向量和矩阵，而且我们已经注意到，这是很有意义的．随着许多新的科学领域的出现，及其数学本身的需要，我们必须将运算的对象进一步扩大．事实上，在现代代数学中，什么东西都可成为我们的运算对象．在本课程中，我们主要学习近世代数学中三个最主要的对象——群、环、域，它们都是在一个集合上定义一些运算律后而成的代数结构．为此，本章中我们介绍集合和运算的基本概念，为后几章中群、环、域的学习打基础．

1.1　集合与映射

1　集合

集合：一般我们将具有某种特性的事物的全体称为一个**集合**．通常我们用大写英文字母 A,B,C 等表示集合．集合中的事物称为元素．我们用 $a \in A$ 表示 a 是集合 A 中的**元素**，读“a 属于 A”；$a \notin A$ 表示 a 不是集合 A 中的元素，读“a 不属于 A”．

例如，$1 \in \{0,1\}$，$2 \notin \{0,1\}$．

我们用 $\mathbf{N},\mathbf{Z},\mathbf{Q},\mathbf{R},\mathbf{C}$ 分别表示自然数集合，整数集合，有理数集合，实数集合和复数集合．这些集合中去掉 0 后用 $\mathbf{N}^*,\mathbf{Z}^*,\mathbf{Q}^*,\mathbf{R}^*,\mathbf{C}^*$ 表示．

空集：我们称没有元素的集合为**空集**．空集的符号为 $\varnothing$．

例如，$\{x \in \mathbf{R} \mid x^2 + 1 = 0\} = \varnothing$

子集：若集合 B 中的元素都属于集合 A，我们称 B 是 A 的**子集**，记为 $B \subset A$．若 B 是 A 的子集，但 $B \neq A$，我们称 B 是 A 的真子集．

例如，若 $A = \{0,1,2\}$，$B = \{0,1\}$，则 $B \subset A$．

注意：对任何集合 A，有

$$\varnothing \subset A, A \subset A.$$

集合的并：对于集合 A,B，我们称集合

$$A \cup B \equiv \{c \mid c \in A \text{ 或 } c \in B\}$$

为 A,B 的**并集**．

例如，$\{0,1,2\} \cup \{1,2,3\} = \{0,1,2,3\}$．

注意:对于集合 A,B,有

$$A \subset A \cup B, B \subset A \cup B.$$

集合的差:对于集合 A,B,我们称集合

$$A - B \equiv \{c \mid c \in A \text{且} c \notin B\}$$

为 A 与 B 的**差集**.

例如,$\{0,1,2\} - \{1,2,3\} = \{0\}$.

集合的交:对于集合 A,B,我们称集合

$$A \cap B \equiv \{c \mid c \in A \text{且} c \in B\}$$

为 A,B 的**交集**.

例如,$\{0,1,2\} \cap \{1,2,3\} = \{1,2\}$.

注意:对于集合 A,B,有

$$A \cap B \subset A, A \cap B \subset B.$$

集合的积:对于集合 A,B,我们称集合

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

为 A,B 的**积**.

例如,

$$\{0,1,2\} \times \{a,b\} = \{(0,a),(0,b),(1,a),(1,b),(2,a),(2,b)\};$$

$\mathbf{R}^2 \equiv \mathbf{R} \times \mathbf{R}$ 为平面点集.

2 映射

约定:以后,若无特别声明,集合都不是空集.

定义 对两个集合 A,B.若一个法则 σ 使得 A 中**任何一个元素** a 都对应 B 中**唯一的一个元素** b,则我们称 σ 为集合 A 到集合 B 的一个**映射**;元素 b 称元素 a 在映射 σ 下的**像**,记为 $\sigma(a) = b$;元素 a 称元素 b 在映射 σ 之下的一个**原像**;若 $A' \subset A$,集合

$$\sigma(A') \equiv \{\sigma(a) \mid a \in A'\} \subset B$$

称 A' 在 σ 下的**像集**;若 $B' \subset B$,集合

$$\sigma^{-1}(B') \equiv \{a \in A \mid \sigma(a) \in B'\} \subset A$$

称 B' 在映射 σ 下的**原像集**.

例 1 设 $A = \{0,1,2,3\}, B = \{a,b,c\}$.

若令

$$\alpha: 0 \mapsto a, 1 \mapsto b, 2 \mapsto a, 3 \mapsto b, 0 \mapsto c$$

则 α 不是 A 到 B 的映射,因为 $0 \in A$ 对应的元素不唯一.

若令

$$\beta: 0 \mapsto a, 1 \mapsto b, 2 \mapsto c$$

则 β 不是 A 到 B 的映射,因为 $3 \in A$ 不对应 B 中的任何元素.

若令

$$\gamma: 0 \mapsto a, 1 \mapsto b, 2 \mapsto a, 3 \mapsto b,$$

则 γ 是 A 到 B 的映射;此时

$$\gamma(A) = \{a,b\}, \gamma(\{0,2\}) = \{a\}, \gamma(\{0\}) = \{a\},$$
$$\gamma^{-1}(\{a\}) = \{0,2\}, \gamma^{-1}(\{c\}) = \varnothing$$

例 2 $\sigma: (m,n) \mapsto m+n$ 为 $\mathbf{Z} \times \mathbf{Z}$ 到 $\mathbf{Z}$ 的一个映射.

例 3 令 $M_{m\times n}(\mathbf{R})$ 为一切 $m \times n$ 实矩阵构成的集合,则

$$\sigma: (A,B) \mapsto AB$$

为 $M_{l\times m}(\mathbf{R}) \times M_{m\times n}(\mathbf{R})$ 到 $M_{l\times n}(\mathbf{R})$ 的一个映射.

定义 设 σ 为集合 A 到集合 B 的一个映射.

(1) 若 $\sigma(A) = B$,即 B 中每个元素在映射 σ 下都至少有一个原像,则我们称 σ 为**满射**;

(2) 若 A 中任何两个不同的元素 a_1, a_2 的像 $\sigma(a_1), \sigma(a_2)$ 也不同,则我们称 σ 为**单射**;

(3) 若 σ 既是单射又是满射,则称 σ 为**双射**.此时我们称 A 与 B **一一对应**;

(4) 集合 A 到自身的映射称 A 的一个**变换**.同理,变换有**单变换、满变换**和**一一变换**之分.

例 4 设 $S = \{0,1,2\}, B = \{a,b\}, C = \{a,b,c\}, D = \{a,b,c,d\}$.令

$$\beta: S \to B, 0 \mapsto a, 1 \mapsto b, 2 \mapsto a;$$
$$\gamma: S \to C, 0 \mapsto a, 1 \mapsto b, 2 \mapsto c;$$
$$\delta: S \to D, 0 \mapsto a, 1 \mapsto b, 2 \mapsto c.$$

则 β 是满射,不是单射;γ 是双射,δ 是单射,不是满射.

例 5 设 $A = \{0,1,2,\cdots\}, B = \{0,2,4,\cdots\}$,则 $\sigma: n \mapsto 2n$ 为 A 到 B 的一个双射,即 A 与 B 一一对应.

例 6 设 $A = [0,2\pi), B = \{(x,y) \in \mathbf{R} \times \mathbf{R} \mid x^2 + y^2 = 1\}$,则

$$\sigma: \theta \mapsto (\cos\theta, \sin\theta)$$

为 A 到 B 的一个双射.

例 7 集合 A 的一一变换 $1_A: a \mapsto a$ 称 A 的**恒同变换**.

3 映射的复合

定义 给定两个映射 $\alpha: A \to B$ 和 $\beta: B \to C$,则对应

$$\beta\alpha: A \to C, a \mapsto \beta(\alpha(a))$$

为 A 到 C 的映射,称其为 α 与 β 的**复合(映射)**.

例 8 设 $A = \mathbf{R}, B = \mathbf{R}^+$ (正实数的集合).令

$$\alpha: A \to B, x \mapsto e^x; \beta: B \to A, y \mapsto \ln y,$$

则

$$\beta\alpha: A \to A, x \mapsto e^x \mapsto \ln(e^x) = x,$$
$$\alpha\beta: B \to B, y \mapsto \ln y \mapsto e^{\ln y} = y,$$

即 $\beta\alpha = 1_A, \alpha\beta = 1_B$.

定理 映射 $\alpha: A \to B$ 是双射 $\Leftrightarrow$ 存在映射 $\beta: B \to A$ 使

$$\alpha\beta = 1_B, \quad \beta\alpha = 1_A.$$

证明 ($\Rightarrow$) 由于 α 是满射,又是单射,因而对任意 $b \in B$,在 A 中存在唯一一个元素 a 使 $\alpha(a) = b$.令 $\beta: b \mapsto a$,即

$$\beta(b) = a \Leftrightarrow \alpha(a) = b,$$

此时,直接验证可得到 $\alpha\beta = 1_B, \beta\alpha = 1_A$.

($\Leftarrow$) 对任意 $b \in B$,我们有 $(\alpha\beta)(b) = 1_B(b) \Rightarrow \alpha(\beta(b)) = b$,这说明 α 是满射;又

$$\alpha(a_1) = \alpha(a_2) \Rightarrow \beta(\alpha(a_1)) = \beta(\alpha(a_2)) \Rightarrow (\beta\alpha)(a_1) = (\beta\alpha)(a_2)$$
$$\Rightarrow 1_A(a_1) = 1_A(a_2) \Rightarrow a_1 = a_2,$$

这说明 α 是单射.总之,α 是双射.

习题 1 – 1

1.若 $A \subset B$,求 $A \cap B, A \cup B$.

2.试证有理数集合 $\mathbf{Q}$ 与整数集合 $\mathbf{Z}$ 一一对应.

3.试建立一个由区间(0,1) 到区间$(-\infty, +\infty)$ 的一一对应.

4.证明集合运算律:$U - (A \cup B) = (U - A) \cap (U - B)\ (A, B \subset U)$.

5.若集合 A 有 n 个不同的元素,证明 A 有 2^n 个不同的子集.

1.2 代数结构

1 代数运算

我们知道对于二维向量有两个运算,一个是数乘向量:

$$k \circ (a, b) = (ka, kb);$$

另一个是向量与向量的加法:

$$(a, b) \oplus (c, d) = (a + c, b + d).$$

事实上,我们可将数乘向量视为一个由 $\mathbf{R} \times \mathbf{R}^2$ 到 $\mathbf{R}^2$ 的映射:

$$\circ: (k, (a, b)) \mapsto (ka, kb),$$

只要将 $\circ(k, (a, b))$ 记为 $k \circ (a, b)$;同样,可将向量与向量的加法视为一个由 $\mathbf{R}^2 \times \mathbf{R}^2$ 到 $\mathbf{R}^2$ 的映射:

$$\oplus: ((a, b), (c, d)) \mapsto (a + c, b + d),$$

只要将 $\oplus((a,b),(c,d))$ 记为 $(a,b)\oplus(c,d)$.

定义 (1) 我们称映射 $\circ: A\times B\to D$ 为 $A\times B$ 到 D 的一个**代数运算**.为了方便,我们用 $a\circ b$ 表示 $\circ(a,b)$;

(2) 由 $A\times A$ 到 A 的一个代数运算 $\circ$ 称为 A 上的一个**二元运算**,此时我们说 $(A,\circ)$ 是一个**代数结构**.

例 1 令 $\circ:(m,n)\mapsto\frac{m}{n}$,则 $\circ$ 为由 $\mathbf{Z}\times\mathbf{Z}^*$ 到 $\mathbf{Q}$ 的一个代数运算,也就是普通的整数除法.

例 2 $\oplus:(m,n)\mapsto m+n$ 为 $\mathbf{Z}$ 上的一个二元运算,也就是普通的整数加法.

例 3 若 $p(A)=\{B\mid B\subset A\}$,则集合的并($\cup$)和交($\cap$)为 $p(A)$ 上的两个二元运算.

2 运算表

当 $A=\{a_1,\cdots,a_n\}$, $B=\{b_1,\cdots,b_m\}$ 为有限集时,若 $\circ$ 为 $A\times B$ 到 D 的代数运算,$a_i\circ b_j=d_{ij}\in D$,我们可用下表表示这个代数运算:

$\circ$	b_1	b_2	$\cdots$	b_m
a_1	d_{11}	d_{12}	$\cdots$	d_{1m}
a_2	d_{21}	d_{22}	$\cdots$	d_{2m}
$\vdots$	$\vdots$	$\vdots$		$\vdots$
a_n	d_{n1}	d_{n2}	$\cdots$	d_{nm}

例 4 $A=\{N,Y\}$.在 A 上如下定义两个二元运算 $\otimes$ 和 $\oplus$:

$$Y\otimes Y=Y,Y\otimes N=N,N\otimes Y=N,N\otimes N=N;$$

$$Y\oplus Y=Y,Y\oplus N=N,N\oplus Y=N,N\oplus N=N;$$

它们用运算表表示如下:

$\otimes$	N	Y
N	N	N
Y	N	Y

$\oplus$	N	Y
N	N	Y
Y	Y	Y

例 5 令 $\varepsilon_1=\cos\frac{2\pi}{3}+\mathrm{i}\sin\frac{2\pi}{3}$, $\varepsilon_2=\varepsilon_1^2$, $U_3=\{1,\varepsilon_1,\varepsilon_2\}$,则 U_3 对于复数的乘法构成一个代数结构,其运算表如下:

·	1	ε_1	ε_2
1	1	ε_1	ε_2
ε_1	ε_1	ε_2	1
ε_2	ε_2	1	ε_1

习题 1 – 2

1.设 $A = \{a, b, c\}$,规定 A 的两个不同的二元运算.

2.$U_6 \equiv \{z \in \mathbf{C} \mid z^6 = 1\}$,写出代数结构$(U_6, \cdot)$的乘法表,这里运算是复数的乘法.

3.$A = \{a, b\}$,写出代数结构$(p(A), \cup)$和$(p(A), \cap)$的运算表.

4.$A = \{0,1,2\}$.对任意 $a, b \in A$,定义 $a \oplus b$ 为 $a + b$ 被 3 除得到的余数;定义 $a \otimes b$ 为 $a \cdot b$ 被 3 除得到的余数.写出代数结构$(A, \oplus)$和$(A, \otimes)$的运算表.

1.3 运 算 律

由上一节我们看到,定义一个代数结构是很容易的,代数运算也是多种多样的,但不是任何一个都是很有意义的.我们仅对一些有意义的代数结构感兴趣,这首先要求其运算满足一些重要的运算律,如结合律、交换律和分配律.

1 结合律

定义 $(A, \circ)$为一个代数结构,我们称运算$\circ$**满足结合律**,假若对于任何 $a, b, c \in A$,都有$(a \circ b) \circ c = a \circ (b \circ c)$.

例如,$(\mathbf{C}, +)$,$(\mathbf{C}, \cdot)$都满足结合律,但$(\mathbf{C}, -)$不满足结合律.

对于代数结构$(A, \circ)$中的元素 $a_1, a_2, \cdots, a_n$,通过加括号可使 $a_1 \circ a_2 \circ \cdots \circ a_n$ 有意义,但从表面上看,不同的方式得到的运算结果可能是 A 中不同的元素.但是下面的定理告诉我们,对于满足结合律的运算不会发生这种现象,即 $a_1 \circ a_2 \circ \cdots \circ a_n$ 是有意义的.

定理 1 若代数结构$(A, \circ)$满足结合律,则对 A 中任何 n $(n \geqslant 3)$ 个元素 $a_1, a_2, \cdots, a_n$,以任何方式加括号得到的有意义的结果都相等.

证明 首先,对于 A 中的元素,我们归纳定义一个标准乘积:

$$\prod_{i=1}^{1} a_i = a_1, \quad \prod_{i=1}^{2} a_i = a_1 \circ a_2, \cdots, \prod_{i=1}^{n} a_i = \left(\prod_{i=1}^{n-1} a_i\right) \circ a_n.$$

现在我们用 $\pi(a_1 \circ a_2 \circ \cdots \circ a_n)$ 表示 $a_1 \circ a_2 \circ \cdots \circ a_n$ 通过加括号得到的一个有意义的结果.下面我们对元素的个数用归纳法证明此定理.

(1) 当元素的个数是 3 时,由结合律的定义知

$$\pi(a_1 \circ a_2 \circ a_3) = \prod_{i=1}^{3} a_i .$$

(2) 假设元素的个数小于 n 时结论正确,则乘积都等于标准积.

(3) 由归纳假设和加括号的运算过程知

$$\begin{aligned}\pi(a_1 \circ a_2 \circ \cdots \circ a_n) &= (\prod_{i=1}^{m} a_i) \circ (\prod_{i=m+1}^{n} a_i) \\ &= (\prod_{i=1}^{m} a_i) \circ [(\prod_{i=m+1}^{n-1} a_i) \circ a_n] \\ &= [(\prod_{i=1}^{m} a_i) \circ (\prod_{i=m+1}^{n-1} a_i)] \circ a_n \\ &= (\prod_{i=1}^{n-1} a_i) \circ a_n = \prod_{i=1}^{n} a_i \quad (1 \leqslant m < n).\end{aligned}$$

由归纳原理知定理命题成立.

2 交换律

定义 $(A, \circ)$ 为一个代数结构,我们称运算 $\circ$ 满足**交换律**,即假若对于任何 $a, b \in A$,都有 $a \circ b = b \circ a$.

例如,$(\mathbf{C}, +)$,$(\mathbf{C}, \cdot)$ 都满足交换律,但$(\mathbf{C}, -)$ 不满足交换律.

定理2 若代数结构满$(A, \circ)$ 足结合律和交换律,则对 A 中任何$n(n \geqslant 2)$ 个元素 $a_1, a_2, \cdots, a_n, a_1 \circ a_2 \circ \cdots \circ a_n$ 中的元素可以任意调换(结果不变).

此定理的证明与上述定理的证明类似, 留作练习.

3 分配律

许多有意义的代数结构上有两个代数运算,而且它们是有机结合的,一个运算对另一个有分配律就是一种重要的结合.以下,我们假设 $\otimes$ 是 $B \times A$ 到A 的运算, $\oplus$ 是 A 上的二元运算.

定义 我们称 $\otimes$ 对 $\oplus$ 满足**左分配律**,假若对于任何 $b \in B, a_1, a_2 \in A$,都有

$$b \otimes (a_1 \oplus a_2) = (b \otimes a_1) \oplus (b \otimes a_2).$$

同样我们可定义 $\otimes$ 对 $\oplus$ 满足**右分配律**.

例如,数乘向量满足左分配律;数的乘法对加法满足左分配律和右分配律,而数的减法对加法不满足左分配律和右分配律.

由归纳法我们可以很容易证明如下定理.

定理3 若 $\oplus$ 满足结合律,而且 $\otimes$ 对 $\oplus$ 满足左分配律,则对于任何 $b \in B, a_1, a_2, \cdots, a_n \in A$ 我们有

$$b \otimes (a_1 \oplus a_2 \oplus \cdots \oplus a_n) = (b \otimes a_1) \oplus (b \otimes a_2) \oplus \cdots \oplus (b \otimes a_n).$$

习题 1 – 3

1.$(\mathbf{R}^*, \div)$ 满足结合律吗?

2.对任意 $a, b \in \mathbf{R}$,定义 $a \circ b = a + 2b$,$(\mathbf{R}, \circ)$ 满足结合律吗?

3.在你已知的非数的运算中找出一个不满足结合律,也不满足交换律的运算.

4.设 $\oplus$ 满足结合律,且 $\otimes$ 对 $\oplus$ 满足左分配律和右分配律,证明

$$(a_1 \otimes b_1) \oplus (a_1 \otimes b_2) \oplus (a_2 \otimes b_1) \oplus (a_2 \otimes b_2)$$
$$= (a_1 \otimes b_1) \oplus (a_2 \otimes b_1) \oplus (a_1 \otimes b_2) \oplus (a_2 \otimes b_2)$$

1.4 同态与同构

在代数学中,我们主要关心的是代数结构的抽象运算,而元素用什么表示,运算用何符号无关紧要,因此我们就要建立两个代数结构的比较方法. 我们观察两个极其简单的代数结构 $(A, \cdot)$ 与 $(B, \otimes)$,$A = \{N, Y\}$,$B = \{0, 1\}$,运算由下表定义:

$\cdot$	N	Y
N	N	N
Y	N	Y

$\otimes$	0	1
0	0	0
1	0	1

我们自然会说 $(A, \cdot)$ 与 $(B, \otimes)$ 本质上没有什么不同,我们是靠直观做出判断的.但当代数结构很复杂时,如何做出这样的判断?另一方面,当两个代数结构不完全相同时,我们如何探讨它们某个侧面的相同性?同态与同构就是我们将采取的有效手段.

定义 设 $(A, \circ)$,$(\bar{A}, \bar{\circ})$ 为代数结构,σ 为 A 到 $\bar{A}$ 的映射.

(1) 若对于任何 $a, b \in A$,有 $\sigma(a \circ b) = \sigma(a) \bar{\circ} \sigma(b)$,则我们说 σ 是 A 到 $\bar{A}$ 的**同态**;

(2) 若 σ 是单射同态,我们称 σ 为**单同态**;

(3) 若 σ 是满射同态,我们称 σ 为**满同态**,称 A 与 $\bar{A}$ 同态,记为 $A \geqslant \bar{A}$;

(4) 若 σ 是双射同态,我们称 σ 为**同构**,并称 A 与 $\bar{A}$ 同构,记为 $A \cong \bar{A}$.

(5) 若 σ 是 A 到 A 自身的同态(同构),我们称 σ 为 A 的**自同态(同构)**.

例 1 对于本节开头的两个代数结构 $(A, \cdot)$ 与 $(B, \otimes)$,定义

$$\sigma: N \longmapsto 0, Y \longmapsto 1,$$

则 σ 为 A 到 B 的同构.

例 2 对于 $(\mathbf{Z}, +)$ 和 $(U_3, \cdot)$,$\sigma: n \longmapsto \varepsilon_1^n$ 为 $\mathbf{Z}$ 到 U_3 的满同态.

例 3 若令 $\sigma: z \longmapsto \bar{z}$,这里 $\bar{z}$ 为复数 z 的共轭,则 σ 为双射是明显的,又

$$\sigma(z_1 + z_2) = \overline{z_1 + z_2} = \bar{z}_1 + \bar{z}_2 = \sigma(z_1) + \sigma(z_2),$$
$$\sigma(z_1 \cdot z_2) = \overline{z_1 \cdot z_2} = \bar{z}_1 \cdot \bar{z}_2 = \sigma(z_1) \cdot \sigma(z_2),$$

故 σ 为$(\mathbf{C},\cdot)$和$(\mathbf{C},+)$的自同构.

例 4 $\sigma: x \longmapsto \mathrm{e}^x$ 为代数结构$(\mathbf{R},+)$到$(\mathbf{R}^+,\cdot)$的同构.事实上,σ 为双射是明显的,且

$$\sigma(x_1+x_2)=\mathrm{e}^{x_1+x_2}=\mathrm{e}^{x_1}\mathrm{e}^{x_2}=\sigma(x_1)\cdot\sigma(x_2).$$

定理 假设$(A,\circ)\geqslant(\bar{A},\bar{\circ})$,则我们有下列结论:

(1) 若$(A,\circ)$满足结合律,则$(\bar{A},\bar{\circ})$也满足结合律;

(2) 若$(A,\circ)$满足交换律,则$(\bar{A},\bar{\circ})$也满足交换律.

证明 我们仅证(1).设 σ 为 A 到 $\bar{A}$ 的满同态.任取 $\bar{a},\bar{b},\bar{c}\in\bar{A}$,由于 σ 为满同态,故存在 $a,b,c\in A$ 使$\sigma(a)=\bar{a},\sigma(b)=\bar{b},\sigma(c)=\bar{c}$,因而

$$\begin{aligned}(\bar{a}\,\bar{\circ}\,\bar{b})\,\bar{\circ}\,\bar{c}&=(\sigma(a)\,\bar{\circ}\,\sigma(b))\,\bar{\circ}\,\sigma(c)=\sigma(a\circ b)\,\bar{\circ}\,\sigma(c)=\sigma((a\circ b)\circ c)\\&=\sigma(a\circ(b\circ c))=\sigma(a)\,\bar{\circ}\,(\sigma(b\circ c))=\sigma(a)\,\bar{\circ}\,(\sigma(b)\,\bar{\circ}\,\sigma(c))\\&=\bar{a}\,\bar{\circ}\,(\bar{b}\,\bar{\circ}\,\bar{c}),\end{aligned}$$

即$(\bar{A},\bar{\circ})$满足结合律.

习题 1 – 4

1.以下映射是不是代数结构$(\mathbf{R},\cdot)$的自同态?

(1) $x\longmapsto|x|$; (2) $x\longmapsto 2x$; (3) $x\longmapsto x^2$; (4) $x\longmapsto -x$.

2.证明$(A,\circ)\cong(A,\circ)$.

3.若$(A,\circ)\geqslant(B,*)$,$(B,*)\geqslant(C,\cdot)$,证明$(A,\circ)\geqslant(C,\cdot)$.

4. $A=\{a,b,c\}$,其上的运算由下表定义:

$\cdot$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

证明,$(A,\cdot)$满足结合律,且与 1.2 例 5 中的$(U_3,\cdot)$同构.

5.找$(\mathbf{Q},+)$的一个非恒同的自同构.

6.在 $\mathbf{R}^2$ 上定义两个二元运算 $\oplus$, $\otimes$ 使得

$$(\mathbf{R}^2,\oplus)\cong(\mathbf{C},+),\quad(\mathbf{R}^2,\otimes)\cong(\mathbf{C},\cdot).$$

7.证明$(\mathbf{Q},+)$不与$(\mathbf{Q}^*,\cdot)$同构.

1.5 等价关系与集合的分类

在代数学中除了要比较两个代数结构,当然也要研究一个代数 结构自身的性质.但有时又难以以结构中的元素作为对象直接处理,即我们难以得到此结构中最低层的性质.此时我们

不得不寻找此结构中上层的性质.这样我们要将结构(一个集合)中的元素分类处理,即将一个集合分割成互不相同的子集,以这些子集作为一个新的代数结构中的对象来处理.将一个集合分割成互不相同的子集又与此集合元素间的一个重要关系——等价关系相呼应.

1 等价关系

我们在日常生活中常常谈到各种各样的关系,如"父子关系"、"同事关系"和"同学关系"等.但这些关系如何用数学语言描述呢?我们以"同班同学关系"为例来看.若 S 表示某大学的全部学生,令 $R = \{(s_1, s_2) \in S \times S \mid s_1, s_2 \text{ 在同一个班级中}\}$,则 s_1 与 s_2 有同班同学关系就相当于 $(s_1, s_2) \in R$.

定义 $A \times A$ 上的任何一个非空子集 R 称 A 上的一个**关系**.若 $(a, b) \in R$,我们称 a 与 b 有 R **关系**,改记为 aRb.

一个集合会有许许多多的关系,但在代数学中我们最关心的是"等价关系"和"偏序关系".本章中我们仅讨论前者.

定义 令 $\sim$ 是集合上的一个关系.若 $\sim$ 满足下列三条,我们则称 $\sim$ 为 A 上的一个**等价关系**:

(Ⅰ)**反身性**:$a \in A \Rightarrow a \sim a$;

(Ⅱ)**对称性**:$a \sim b \Rightarrow b \sim a$;

(Ⅲ)**传递性**:$a \sim b, b \sim c \Rightarrow a \sim c$.

若 $a \sim b$,我们说 a **与** b **等价**.

例 1 "等于"关系是等价关系.

例 2 若 $\sim$ 为"同班同学关系",则 $\sim$ 是一个学校全体学生之集的等价关系.

2 集合的分类

我们可以将一个学校的全体学生按班级分类,即两个学生在同一个班中等同于这两个学生有同班同学关系.

定义 $p(A)$ 的子集 $\Pi = \{A_i \subset A \mid i \in I\}$ 称集合 A 的一个**分类**,假若 A 中每一个元素属于且只属于 A_i 之一,即下面两项同时成立:

(1) $A = \bigcup\limits_{i \in I} A_i$;

(2) 对任何 $i, j \in I$,有 $A_i \cap A_j = \varnothing$ 或 $A_i = A_j$.

例如,一个学校的全体班级是学校全体学生的一个分类,每个学生必在一个班级中,且仅在一个班级中.

定理 集合 A 的一个分类决定 A 的元素间的一个等价关系;反之,A 的元素间的一个等价关系也决定 A 的一个分类.

证明 设 $\Pi = \{A_i \subset A \mid i \in I\}$ 是集合 A 一个分类.定义 A 上的关系 $\sim$:

$$a \sim b \Leftrightarrow a, b \in A_i(\text{对某个 } i \in I).$$

我们说 $\sim$ 是 A 上的等价关系. 事实上,

(Ⅰ) $a \in A = \bigcup_{i \in I} A_i \Rightarrow a, a \in A_i \Rightarrow a \sim a$;

(Ⅱ) $a \sim b \Rightarrow a, b \in A_i \Rightarrow b, a \in A_i \Rightarrow b \sim a$;

(Ⅲ) $a \sim b, b \sim c \Rightarrow a, b \in A_i; b, c \in A_j \Rightarrow b \in A_i \cap A_j \neq \varnothing \Rightarrow a, c \in A_i = A_j \Rightarrow a \sim c$.

反之,设 $\sim$ 是 A 上的等价关系.我们称 A 的子集 $\bar{a} \equiv \{b \in A \mid b \sim a\}$ 为 a **所代表的等价类**.我们说 $\Pi = \{\bar{a} \mid a \in A\}$ 是 A 的分类.

等价类的基本性质:

(1) $a \in \bar{a}$;

(2) $a \sim b \Leftrightarrow a \in \bar{b}$;

(3) $a \sim b \Leftrightarrow b \in \bar{a}$;

(4) $a \sim b \Leftrightarrow \bar{a} = \bar{b}$.

证明 (1),(2),(3) 明显成立.我们仅证明(4).

事实上,$\bar{a} = \bar{b} \Rightarrow a \in \bar{a} = \bar{b} \Rightarrow a \sim b$.反之,设 $a \sim b$.此时,

$$c \in \bar{a} \Rightarrow c \sim a, a \sim b \Rightarrow c \sim b \Rightarrow c \in \bar{b} \Rightarrow \bar{a} \subset \bar{b};$$

再由对称性,$\bar{b} \subset \bar{a}$.因此,$a \sim b \Rightarrow \bar{a} = \bar{b}$.

现在,我们推得:

(Ⅰ) $a \in A \Rightarrow a \sim a \Rightarrow a \in \bar{a} \Rightarrow A = \bigcup_{a \in A} \bar{a}$;

(Ⅱ) $\bar{a} \cap \bar{b} \neq \varnothing \Rightarrow$ 存在 $c \in \bar{a}, \bar{b} \Rightarrow c \sim a, c \sim b \Rightarrow a \sim c, c \sim b \Rightarrow a \sim b \Rightarrow \bar{a} = \bar{b}$,

这就证明了 $\Pi = \{\bar{a} \mid a \in A\}$ 是 A 的分类.

若 $\sim$ 是 A 上的等价关系,我们将它如上决定的分类 $\{\bar{a} \mid a \in A\}$ 记为 $A/\sim$,称为 A 的等价类集合.请记住 $A/\sim \subset p(A)$.

3 整数的同余关系与同余类

现在我们介绍在代数学中重要的整数同余关系与同余类.

同余关系: n 为一个取定的正整数.对于任何 $a, b \in \mathbf{Z}$,我们在 $\mathbf{Z}$ 上定义模 n **的同余关系** $\sim$:

$$a \sim b \Leftrightarrow n \mid (a - b).$$

评注:(1) 这里,$p \mid q$ 表示 p 整除 q;$n \mid (a - b)$ 等同于 a, b 被 n 除时,余数相同,即"a 与 b 模 n 同余";a 与 b 模 n 同余的通用写法为同余式 $a \equiv b(\mathrm{mod}n)$;

(2) 容易证明同余式有下列性质:

① $a \equiv a(\mathrm{mod}n)$;

② $a \equiv b(\mathrm{mod}n) \Rightarrow b \equiv a(\mathrm{mod}n)$;

③ $a \equiv b, b \equiv c(\mathrm{mod}n) \Rightarrow a \equiv c(\mathrm{mod}n)$;

④ $a \equiv b, c \equiv d(\mathrm{mod}n) \Rightarrow a + c \equiv b + d$,