近世代数基础

（第二版）

毛 华 杨兰珍 编著

科学出版社

近世代数基础

（第二版）

毛　华　杨兰珍　编著

河北大学精品教材建设项目

科学出版社
北　京

内 容 简 介

本书是作者根据多年教学经验，结合第一版教学应用中出现的情况，以及这些年与课程内容有关的应用理论方面的发展情况，总结修改而成的. 作者在介绍近世代数课程的传统内容时，从以下几个方面进行了深入浅出的讲解：引入了泛代数研究的基本思想内容；较深入地介绍群、环的思想和内容；简单介绍了格论的思想内容；同时还指出了所介绍的几种代数结构的一些应用领域. 全书共 4 章. 第 1 章由泛代数基本研究结构引出近世代数应有的基本内容；第 2 章介绍群论基础；第 3 章介绍环的内容；第 4 章简单介绍格论. 每章配有适当数量的习题，难度适应多层次教学的需要.

本书可作为高等学校数学类和信息类专业的教材，也可供相关专业师生及科研人员参考使用.

图书在版编目（CIP）数据

近世代数基础/毛华，杨兰珍编著. —2 版. —北京：科学出版社，2018. 10
ISBN 978-7-03-058777-0

Ⅰ. ①近… Ⅱ. ①毛… ②杨… Ⅲ. ①抽象代数 Ⅳ. ①O153

中国版本图书馆 CIP 数据核字（2018）第 209296 号

责任编辑：王胡权／责任校对：张凤琴
责任印制：吴兆东／封面设计：迷底书装

科学出版社 出版
北京东黄城根北街 16 号
邮政编码：100717
http://www.sciencep.com

北京中石油彩色印刷有限责任公司 印刷
科学出版社发行 各地新华书店经销
*
2012 年 8 月第 一 版 开本：720 × 1000 1/16
2018 年 10 月第 二 版 印张：9 1/4
2019 年 1 月第二次印刷 字数：201 000

定价：38.00 元

（如有印装质量问题，我社负责调换）

第二版前言

本书第一版自 2012 年出版发行以来, 经河北大学等院校 6 年的教学使用, 反映良好, 获得了广大师生的认同与好评.

根据我们的教学实践和经验, 以及当前近世代数的发展与应用状况, 再版之前, 我们对全书进行了仔细且认真地修改与润色. 首先, 对第一版的结构与内容大体保留; 其次, 在本书内容的论证与计算的细节及表达方式上进行了必要地修正与精炼; 再次, 为了介绍近世代数近年来的发展, 第二版添加了模糊代数的一些相关内容, 例如模糊集合论、模糊群、模糊环、模糊格等内容; 最后, 第二版还添加了格的应用 —— 概念格, 介绍了概念格的理论发展新方法, 例如拟阵方法及其应用.

本书第二版的出版不仅得到了国家自然科学基金项目 (编号: 61572011) 和河北大学精品教材建设项目 (2017-BZ-JPJC24) 的资助. 也得到了河北大学学习本课程的广大同学的支持和帮助, 借此机会我们表示衷心感谢.

限于作者水平, 不妥与疏漏之处在所难免, 殷切地希望各位读者批评指正.

作　者

2018 年 6 月

第一版前言

有别于以因式分解、解方程、指数函数、对数函数等为主要研究内容的古典代数, 本书中所讲的内容为近世代数 (或称为抽象代数), 简单地说, 是研究带有一些运算的集合, 以及这些集合之间的映射. 近世代数作为一门学科, 一般认为是 20 世纪由 E. Noether 和 E. Artin 等数学家建立的.

作者在编写本书时, 根据多年讲授此课程的经验, 有以下一些考虑:

(1) 近世代数是数学类专业的一门重要课程, 随着编码理论、人工智能和数据分析的发展, 它也成为某些信息和通信类专业的课程. 理想的教学时长是一个学年, 但是由于种种现实原因, 课时较紧张, 仅能安排一个学期甚至多半个学期, 课时也只有 36~51 学时. 基于此, 为了使学生在较短的时间内掌握近世代数的基本研究对象和研究内容, 本书系统地介绍了泛代数的基本内容. 事实上, 大家可以看到这也是群、环、格等近世代数方面的主要研究对象、基本研究内容和研究方式. 读者掌握了第 1 章泛代数的思想, 对于后几章的学习将有很好的奠基指导作用.

(2) 群和环是近世代数最基本的研究内容和研究对象, 在第 2 章和第 3 章中分别加以详细介绍. 本书采取由简至深、由一般到特殊的讲述方式, 这种方式有利于读者在今后的学习中更深入地进行研究.

1982 年, R. Wille 利用格论将哲学思想引入到形式概念分析中, 创立了概念格理论. 这种理论现在已经被广泛地应用于人工智能、网络物流、电子商务等诸多实际应用领域. 格作为与群、环结构不同的一种代数结构, 将在本书的第 4 章中予以简单介绍. 这可以使读者初步地接触到一个新的代数结构, 为将来的科学研究提供更广阔的思维方式.

本书对基本知识内容的介绍详细具体, 使读者比较容易读懂. 本书知识结构基本上是自封闭的. 对一些略去的证明, 大多可由读者根据已学知识自行完成. 为了读者能够在较短时间内掌握更多的基本内容, 书中没有过多的例子, 尽量以精要的例子为主, 说清问题. 对于主要内容的例子解释, 最多由 3 个例子加以说明, 读者可以根据书中内容或参看其他相应书籍, 举一反三列举出更多的例子.

本书第 2、3、4 章在介绍主要内容之前, 都简单讲述关于此内容在信息领域的某些应用, 并推荐给读者一些相关参考文献. 引发读者对书中内容的学习兴趣, 引导读者在应用上作出努力, 这也是我们教授课程的目的之一.

(3) 习题是重要的. 为了巩固课程的学习, 做习题是非常必要的. 本书习题数量适中, 难度有梯度性的变化, 可以适应不同层次的读者, 建议读者要尽量发掘自己

的创造力, 体验到数学推理的魅力, 进而扎实地掌握近世代数这门课程的精髓.

本书突出重点和难点, 讲思路、讲体会、讲方法, 作者试图用严密而朴素的方法 “讲述” 近世代数课程中基础而重要的知识和方法.

限于作者水平, 书中难免有不足之处, 敬请读者指正.

作　者

2012 年 6 月

目　　录

第 1 章　泛代数基础内容简介

在 19 世纪末 20 世纪初, 数学的研究方法发生了大的变革. 近世代数以一个崭新的思想出现于这个时期, 它是以研究代数结构为主题的一门数学学科, 主要研究对象有群、环、格, 另外, 还有代数结构以及相关的映射, 例如同态, 也是它的主要研究内容之一. 本章将简单地介绍泛代数的一些基本知识.

1.0　集合论基础知识

本节主要介绍集合论基础知识. 对于没有学习过集合论知识的读者, 可以先学习本节, 再学习 1.1~1.5 节. 对于学习过集合论知识的读者, 可以直接从 1.1 节开始学习. 对于教师而言, 可以根据学生的情况, 选讲此节内容. 建议学习过集合论知识的读者, 也不妨再读一下本节内容, 作为一个复习.

19 世纪末德国数学家康托尔 (Cantor) 为集合论做出了奠基工作, 自此以后, 集合论已经成为数学中不可缺少的基本工具, 集合已成为数学最为基本的概念.

集合论有两种体系组成: 一是朴素集合论体系, 也称为康托尔集合论体系, 二是公理集合论体系. 这里只介绍朴素集合论中的基本内容.

在朴素集合论中, 有些概念, 特别是关于集合的概念是不能精确定义的, 即使这样, 它丝毫不影响对集合的理解.

集合是具有一定属性的事物形成的一个集体, 根据这些属性可以区别一个事物属于或不属于这个集合. 一般地, 人们用大写英文字母 A, B, C, $\cdots$ 表示集合; 用小写英文字母 a, b, c, $\cdots$ 表示集合中的元素; 用 $a \in A$ 表示 a 为 A 的元素, 读作 a 属于 A; 用 $a \notin A$ 表示 a 不是 A 的元素, 读作 a 不属于 A.

不含任何元素的集合称为**空集**, 记作 “$\varnothing$”.

包含有限个元素的集合称为**有限集**, 否则称为**无限集**.

有限集 A 所包含的元素个数是一个非负整数, 记作 $|A|$, 特别地, $|\varnothing| = 0$.

一般有两种方法表示集合.

列举法　列举它的所有元素, 元素之间用逗号分开, 用花括号括起来.

例如, 设 A 是由 e, f, g 为元素的集合, B 是正奇数的集合, 则 $A = \{e, f, g\}, B = \{1, 3, 5, \cdots\}$.

描述法　用集合中的元素所具有的特殊性刻画.

例 1　(1) $D = \{x | x^2 - 9 = 0\}$ 表示方程 $x^2 - 9 = 0$ 的根所组成的集合.

(2) $T=\{y|y$ 是十进制数字$\}$ 表示 10 个十进制数字集合, 即 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 这 10 个数字组成的集合.

在本书中, 为了简便, 引入一些逻辑符号用于表达.

(1) "对于任意 $a\in S$" 表示为 "$\forall a\in S$";

(2) "存在一个 $a\in S$" 表示为 "$\exists a\in S$";

(3) "存在唯一的 $a\in S$" 表示为 "$\exists|a\in S$" (有人也用 "$\exists!a\in S$" 表示);

(4) 设 U,V 为两个命题,

"若 U 成立, 则V 成立" 表示为 "$U\Rightarrow V$";

"U 成立当且仅当 V 成立"表示为 "$U\Leftrightarrow V$".

对于集合应注意以下几点:

(1) 集合中的元素是各不相同的;

(2) 集合中的元素不规定顺序;

(3) 集合的两种表示法有时是可以相互转化的.

例如, 列举法中 $S=\{0,1,2,3,4,5,6,7,8,9\}$ 与描述法中的 T 是一样的.

下面讨论集合之间的关系.

定义 1.0.1 设 A,B 为两个集合.

(1) 若 $\forall a\in B\Rightarrow a\in A$, 则称 B 是 A 的**子集**, 也称 A 包含 B, 或 B 含于 A, 记作 $B\subseteq A$.

(2) 若 $B\subseteq A$ 且 $\exists a\in A$ 但 $a\notin B$, 则称 B 是 A 的**真子集**, 记作 $B\subset A$.

(3) 若 $B\subseteq A$ 且 $A\subseteq B$, 则称 A 与 B **相等**, 记作 $A=B$.

(4) 若限定所讨论的集合都是某一集合的子集, 则称该集合为**全集**, 常记作 E.

(5) 设 A 为一个集合, 称由 A 的所有子集组成的集合为 A 的**幂集**, 记作 $\wp(A)$(或 2^A).

(6) 若 B 不等于 A 并且不是 A 的子集, 则记作 $B\not\subseteq A$.

例 2 (1) 设 $A=\{a,b,c\},B=\{a,b,c,d\},C=\{a,b\}$, 则 $A\subseteq B$, $C\subseteq A$, $C\subseteq B$.

(2) 设 $A=\{2\},B=\{1,4\},C=\{x|x^2-5x+4=0\},D=\{x|x$ 为偶素数 $\}$, 则 $A=D$ 且 $B=C$.

(3) 设 $A=\{x|x^2+1=0$ 且 x 为实数 $\}$, 则 $A=\varnothing$.

(4) 用描述法表示 $\wp(A)$ 为 $\wp(A)=\{X|X\subseteq A\}$.

(5) 为了求出给定集合 A 的幂集, 可以求出 A 的由低到高的元的所有子集, 再将它们组成集合即可.

设 $A=\{a,b,c\}$, 求 $\wp(A)$ 的步骤如下:

0 元子集为: $\varnothing$;

1 元子集为: $\{a\}$, $\{b\}$, $\{c\}$;

2 元子集为: $\{a,b\}$, $\{a,c\}$, $\{b,c\}$;

3 元子集为: $\{a,b,c\}$;

A 的幂集 $\wp(A)=\{\varnothing, \{a\}, \{b\}, \{c\}, \{a,b\}, \{a,c\}, \{b,c\}, \{a,b,c\}\}$.

定理 1.0.2 (1) 空集是一切集合的子集.

(2) 空集是唯一的.

证明 (1) 显然.

(2) 是 (1) 的推论.

该定理说明: $\varnothing$ 是 "最小" 的集合.

给定两个集合, 除关心它们之间是否有包含或相等的关系外, 有时还要讨论如何由它们产生新集合, 即运算方面的问题.

定义 1.0.3 设 A,B 为两个集合.

(1) 称由 A 和 B 的所有元素组成的集合为 A 与 B 的**并集**, 记作 $A\cup B$, 即 $A\cup B=\{x|x\in A$ 或 $x\in B\}$.

(2) 称由 A 和 B 的公共元素组成的集合为 A 与 B 的**交集**, 记作 $A\cap B$, 即 $A\cap B=\{x|x\in A$ 且 $x\in B\}$.

(3) 称属于 A 而不属于 B 的全体元素组成的集合为 B 对 A 的**相对补集**, 记作 $A\backslash B$ (或 $A-B$), 即 $A\backslash B=\{x|x\in A$ 且 $x\notin B\}$.

(4) 称属于 A 而不属于 B, 或属于 B 而不属于 A 的全体元素组成的集合为 A 与 B 的**对称差**, 记作 $A\oplus B$, 即 $A\oplus B=\{x|x\in A$ 且 $x\notin B$, 或 $x\notin A$ 且 $x\in B\}$.

(5) 称 A 对全集 E 的相对补集为 A 的**绝对补集**, 记作 $E\backslash A$ 为 $\sim A$, 即

$$\sim A=\{x|x\in E \text{ 且 } x\notin A\}.$$

将以上各种运算 (将求集合的幂集也看做运算) 分成两类, 其中的绝对补、求幂集称为第 1 类运算, 而将并、交、补、对称差等运算称为第 2 类运算. 在第 1 类运算中, 按由右向左的顺序进行, 在第 2 类运算中, 顺序往往由括号来决定, 多个括号并排或无括号部分按由左向右的顺序进行.

集合的集中运算满足如下运算规律.

定理 1.0.4 设 A,B,C 为全集 E 的三个子集, 则有

(1) 幂等律 $A\cup A=A$; $A\cap A=A$.

(2) 交换律 $A\cup B=B\cup A$;

$A\cap B=B\cap A$.

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

$(A\cap B)\cap C=A\cap(B\cap C)$.

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

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

(5) 德・摩根律 $\sim(A\cup B)=\sim A\cap\sim B$;

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

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

$A\backslash(B\cap C)=(A\backslash B)\cup(A\backslash C)$.

(6) 吸收律 $A\cup(A\cap B)=A$;

$A\cap(A\cup B)=A$.

(7) 零律 $A\cup E=E$;　$A\cap\varnothing=\varnothing$.

(8) 同一律 $A\cup\varnothing=A$;　$A\cap E=A$.

(9) 排中律 $A\cup\sim A=E$.

(10) 矛盾律 $A\cap\sim A=\varnothing$.

(11) 补余律 $\sim\varnothing=E$;　$\sim E=\varnothing$.

(12) 双重否定律 (也称对合律) $\sim(\sim A)=A$.

(13) 补交转换律　$A-B=A\cap\sim B$.

证明　这里证明 (4) 作为例子, 其余留给读者.

对于任意的 x,

$$
\begin{aligned}
&x\in A\cup(B\cap C)\\
\Leftrightarrow\ &x\in A \text{ 或 } x\in(B\cap C)\\
\Leftrightarrow\ &x\in A \text{ 或 } (x\in B \text{ 且 } x\in C)\\
\Leftrightarrow\ &(x\in A \text{ 或 } x\in B) \text{ 且 } (x\in A \text{ 或 } x\in C)\\
\Leftrightarrow\ &x\in(A\cup B) \text{ 且 } x\in(A\cup C)\\
\Leftrightarrow\ &x\in(A\cup B)\cap x\in(A\cup C).
\end{aligned}
$$

所以 $A\cup(B\cap C)=(A\cup B)\cap(A\cup C)$.

常称以上 13 组集合等式为**集合恒等式**, 它们的正确性均可由相应的命题等值式证明.

关系一词是大家熟知并且在生活、学习和工作中经常遇到和处理的概念. 在诸多的关系中, 最基本的是涉及两个事物之间的关系, 即二元关系.

定义 1.0.5　(1) 一个有序 n $(n\geqslant 2)$ 元组是一个有序对, 它的第一个元素为有序的 $n-1$ 元组 $(a_1, a_2, \cdots, a_{n-1})$, 第二个元素为 a_n, 记为 $(a_1, a_2, \cdots, a_n)$.

n 维空间中点 M 的**坐标** $(x_1, x_2, \cdots, x_n)$ 为有序的 n 元组 $(x_1, x_2, \cdots, x_n)$.

(2) 设 A, B 为两个集合, 称集合$\{(x,y)|x\in A \text{ 且 } y\in B\}$为集合 A 与集合 B 的**直积, 或卡氏积, 或笛卡儿积** (Cartesian Product), 记作 $A\times B$.

(3) 设 $A_1, A_2, \cdots, A_n$ 为 n 个集合 ($n \geqslant 2$). 称集合

$$\{(x_1, x_2, \cdots, x_n) | x_j \in A_j, (j = 1, 2, \cdots, n)\}$$

为 **n维直积**, 记作 $A_1 \times A_2 \times \cdots \times A_n$.

若 $A_1 = A_2 = \cdots = A_n = A$ 时, 记 A 生成的 n 维直积为 A^n.

(4) 若集合 F 中的全体元素均为有序的 n ($n \geqslant 2$) 元组, 则称 F 为 n 元**关系**, 特别地, 当 n=2 时, 称 F 为二元关系.

对于二元关系 F, 若 $(x, y) \in F$, 常记为 xFy.

规定空集 $\varnothing$ 为 n 元关系, 当然也是二元空关系, 简称**空关系**.

(5) 设 A, B 为两个集合, $A \times B$ 的任何子集均称为 A 到 B 的**二元关系**, 特别地, 称 $A \times A$ 的子集 R 为 A 上的二元关系, 记作 $R \subseteq A \times A$.

(6) 称 $I_A=\{(x, x) | x \in A\}$为 A 上的**恒等关系**.

注意 (a, b) 是一个有序元素对, 从而, 一般来说, $B \times A$ 不等于 $A \times B$. 例如取 $A=\{1, 2, 3\}$, $B = \{4, 5\}$, 则 $A \times B \neq B \times A$.

定义 1.0.6 设 F, G, A 为三个集合.

(1) 称 $F^{-1} = \{(x, y) | (y, x) \in F\}$ 为 F 的**逆**.

(2) 称 $F \circ G = \{(x, y) | \exists z$ 使得 $(x, z) \in F$ 且 $(z, y) \in G\}$ 为 F 与 G 的**合成**(或复合).

(3) 称 $F|_A = \{(x, y) | (x, y) \in F$ 且 $x \in A\}$ 为 F 在 A 上的**限制**.

集合之间的合成满足以下性质.

定理 1.0.7 设 R_1, R_2, R_3 为三个集合, R 也为一个集合, 则

(1) $(R_1 \circ R_2) \circ R_3 = R_1 \circ (R_2 \circ R_3)$.

(2) $R_1 \circ (R_2 \cup R_3) = R_1 \circ R_2 \cup R_1 \circ R_3$.

(3) $(R_1 \cup R_2) \circ R_3 = R_1 \circ R_3 \cup R_2 \circ R_3$.

(4) $R_1 \circ (R_2 \cap R_3) \subseteq R_1 \circ R_2 \cap R_1 \circ R_3$.

(5) $(R_1 \cap R_2) \circ R_3 \subseteq R_1 \circ R_3 \cap R_2 \circ R_3$.

(6) $(R_1 \circ R_2)^{-1} = R_2^{-1} \circ R_1^{-1}$.

(7) $R|_{A \cup B} = (R|_A) \cup (R|_B)$.

证明 (1) 式说明集合之间的合成运算满足结合律, 我们只对 (1) 给予证明, 其余留给读者.

$$\begin{aligned}
&\forall (x, y),\\
&(x, y) \in (R_1 \circ R_2) \circ R_3\\
\Leftrightarrow\ &\exists z,\ 使得 (x, z) \in R_3\ 且\ (z, y) \in R_1 \circ R_2
\end{aligned}$$

$$\Leftrightarrow \exists z, \text{ 有 } (x,z)\in R_3 \text{ 且 } \exists t \text{ 有 } (z,t)\in R_2 \text{ 使得 } (t,y)\in R_1$$

$$\Leftrightarrow \exists z, \exists t, \text{ 有 } (x,z)\in R_3, (z,t)\in R_2, (t,y)\in R_1$$

$$\Leftrightarrow \exists t, (\exists z, (x,z)\in R_3, (z,t)\in R_2), (t,y)\in R_1$$

$$\Leftrightarrow \exists t, (x,t)\in R_2\circ R_3 \text{ 且} (t,y)\in R_1$$

$$\Leftrightarrow (x,y)\in R_1\circ(R_2\circ R_3).$$

所以 $(R_1\circ R_2)\circ R_3=(R_1\circ R_2)\circ R_3$.

下面讨论非空集合上的二元关系的性质.

定义 1.0.8　设 A 为一集合, $R\subseteq A\times A$.

(1) 若对于任意的 $x\in A$ 均有 xRx, 则称 R 是 A 上**自反的**二元关系 (也称自身性).

(2) 若对于任意的 $x\in A$ 均有 xRx 不成立 (即 $(x,x)\notin R$), 则称 R 是 A 上**反自反的**二元关系.

(3) 对于任意 $x,y\in A$, 若 xRy, 必有 yRx, 则称 R 是 A 上**对称的**二元关系.

(4) 对于任意的 $x,y\in A$, 若 xRy 且 $x\neq y$, 必有 $(y,x)\notin R$, 则称 R 是 A 上**反对称的**二元关系.

(5) 对于任意的 $x,y,z\in A$, 若 xRy, yRz, 必有 xRz, 则称 R 是 A 上**传递的**二元关系.

设 A 为一个非空集合, A 上的关系 R 不一定具有讨论过的 5 种性质中的某些性质. 下面讨论最小的包含 R 的关系 R', 使它具有所要求的性质, 这就是关系的闭包.

定义 1.0.9　设 $A\neq\varnothing, R\subseteq A\times A, R$ 的**自反闭包**(**对称闭包**、**传递闭包**)R' 满足如下条件:

(1) R' 是自反的 (对称的、传递的).

(2) $R\subseteq R'$.

(3) A 上任意的自反的 (对称的、传递的) 关系 R'', 若 $R\subseteq R''$, 则 $R'\subseteq R''$.

常用 $r(R)$, $s(R)$, $t(R)$ 分别表示 R 的自反闭包、对称闭包、传递闭包.

定理 1.0.10　设 $R\subseteq A\times A$ 且 $A\neq\varnothing$, 则

(1) R 是自反的当且仅当 $r(R)=R$.

(2) R 是对称的当且仅当 $s(R)=R$.

(3) R 是传递的当且仅当 $t(R)=R$.

本定理的证明简单, 这里不再赘述.

定义 1.0.11　设 $R\subseteq A\times A$ 且 $A\neq\varnothing$. 若 R 是自反的、对称的和传递的, 则称 R 为 A 上的**等价关系**, 简称等价关系.

例 3 (1) 设 A 为实数集合 $\mathbf{R}$, 则 $R_1=\{(a,b)|(a,b)\in\mathbf{R}\times\mathbf{R},\ a=b\}$ 为实数间的 "相等" 关系, 并且是 $\mathbf{R}$ 上的一个等价关系.

(2) 设 A 为某班学生的集合.

$$R_2=\{(x,y)|x,y\in A,\quad \text{并且 } x \text{ 与 } y \text{ 同姓}\}$$

为一个等价关系.

$$R_3=\{(x,y)|x,y\in A, x \text{ 的年龄不比 } y \text{ 小}\}$$

无对称性, 所以不是等价关系.

集合 A 上的等价关系与集合 A 的分类之间有着本质的联系.

定义 1.0.12 设 R 是非空集合 A 上的等价关系.

(1) $\forall x\in A$, 令 $[x]_R=\{y|y\in A \text{ 且 } xRy\}$, 则称 $[x]_R$ 为 x 的关于 R 的**等价类**, 简称为 x 的等价类. 有时在不引起混淆时, 记 $[x]_R$ 为 $[x]$.

类里任何一个元素称为这个类的一个**代表**.

(2) 以关于 R 的全体不同的等价类为元素的集合, 称为 A 关于 R 的**商集**, 简称 A 的商集, 记作 A/R.

(3) A 的非空子集族 $C=\{A_i|i\in I\}$ 是 A 的一个**分类**(也称**划分**) 当且仅当其满足

(3.1) $\cup_{i\in I}A_i=A$;

(3.2) 当 $i\neq j$ 时, $A_i\cap A_j=\varnothing$.

定理 1.0.13 (1) 设 $S=\{A_i|i\in I\}$ 是 A 的一个分类, 规定 $\approx$ 为

$$a\approx b\Leftrightarrow a \text{ 与 } b \text{ 属于同一个类},$$

则 $\approx$ 是 A 上的一个等价关系.

(2) 设 $\approx$ 是 A 上的一个等价关系, 对于 $a\in A$, 令 $[a]=\{x|x\in A,\ x\approx a\}$, 则 A 的子集族 $S=\{[a]|a\in A\}$ 是 A 的一个分类.

本定理的证明简单, 留给读者.

上面的定理 1.0.13 说明, 非空集合 A 上的等价关系与 A 的划分是一一对应的, 于是 A 上有多少个不同的等价关系, 就产生同样个数的不同的划分, 反之亦然.

给定 $n(n\geqslant 1)$ 元集合 A, 若能求出 A 上的全部划分, 也就求出了 A 上的全部等价关系, 那么如何求出 A 的全部划分, 可参见组合数学中相关内容.

例 4 设 A 为整数集合 $\mathbf{Z}$, m 为自然数, 令

$$R_m=\{(a,b)|a,b\in\mathbf{Z}, m|a-b\},$$

则 R_m 是整数集合 $\mathbf{Z}$ 上的一个等价关系.

这是由于: 显然 R_m 是 $\mathbf{Z}\times\mathbf{Z}$ 的子集, 可以验证 R_m 满足自身性、对称性、传递性, 并且 R_m 确定的等价类为

$$\begin{aligned}
&[0]=\{\cdots,-2m,-m,0,m,2m,\cdots\},\\
&[1]=\{\cdots,-2m+1,-m+1,1,m+1,2m+1,\cdots\},\\
&\cdots\cdots\\
&[m-1]=\{\cdots,-m-1,-1,m-1,\cdots\},
\end{aligned}$$

称 R_m 为**模 m 的同余关系**, 由 R_m 所确定的等价类称为**模 m 剩余类**.

练　　习

1. 用列举法表示.

(1) 偶素数集合;

(2) 24 的素因子集合.

2. 用描述法表示.

(1) 八进制数字集合;

(2) $x^2+y^2=z^2$ 的非负整数解集.

3. 证明对于任意的集合 A, B, C, 若 $A\in B$ 且 $B\in C$, 不一定有 $A\in C$ 成立.

4. 列出下列集合的子集, 并求幂集.

(1) $\{1, \{2, 3\}\}$;

(2) $\{\varnothing, \{\varnothing\}\}$.

5. 化简下列集合.

(1) $\cup\{\{3, 4\}, \{\{3\}, \{4\}\}, \{3, \{4\}\}, \{\{3\}, 4\}\}$;

(2) $\cap\{\wp\wp\wp(\varnothing), \wp\wp(\varnothing), \wp(\varnothing)\}$.

6. 化简下列式子.

(1) $(A\cap B)\cup(A\backslash B)$;

(2) $A\cup(B\backslash A)\backslash A$.

7. 设 $A=\{a,b,c,d\}$, 在 $\wp(A)$ 中, 规定二元关系 $\approx$ 为

$$B\approx C\Leftrightarrow |B|=|C|,$$

证明 $\approx$ 是 $\wp(A)$ 上的一个等价关系, 并写出商集 $\wp(A)/\approx$.

8. 设 R 是非空集合 A 上的二元关系, 对 $\forall x,y,z\in A$, 如果 xRy 且 yRz, 那么 xRz 不成立, 这时称 R 是 A 上**反传递的**二元关系. 证明, R 是反传递的充要条件为 $R^2\cap R=\varnothing$, 其中 $R^2=R\circ R$.

9. 设 $A=\{1,2,\cdots,20\}$, $R=\{(x,y)|x,y\in A$ 并且 $x\equiv y(\mathrm{mod}5)\}$, 证明 R 为 A 上的等价关系, 求 A/R 诱导出 A 的划分.

10. 设 A,B 为两个集合, 已知 $A\cap B\neq\varnothing$, 又已知 $\pi_1=\{A_1, A_2, \cdots, A_n\}$为 A 的划分, 设在 $A_i\cap B(i=1, 2, \cdots, n)$ 中有 m 个是非空的 ($m\geqslant 1$ 是显然的), 设 $B_{i_k}=A_{i_k}\cap B\neq\varnothing$, $k=1, 2, \cdots, m$, 证明 $\pi_2=\{B_{i_1}, B_{i_2},\cdots, B_{i_m}\}$为 $A\cap B$ 的划分.

11. 设 A,B,C 为三个集合, $f:A\to B, g:B\to C$ 为两个映射, 则有下列结论成立.

(1) f,g 是单射 $\Rightarrow gf$ 是单射.

(2) f,g 是满射 $\Rightarrow gf$ 是满射.

(3) gf 是单射 $\Rightarrow f$ 是单射.

(4) gf 是双射 $\Rightarrow g$ 是双射.

(5) f 是单射 $\Leftrightarrow$ 存在一个映射 $h:B\to A$ 使得 $hf=I_A$.

(6) f 是双射 $\Leftrightarrow$ 存在一个映射 $\pi:B\to A$ 使得 $f\pi=I_B$.

以上 I_A, I_B 分别为 A,B 上的单位映射.

1.1 代　数

对本书中常用集合约定使用下面记号: 自然数集合 $\mathbf{N}$; 正整数集合 $\mathbf{Z}^+$; 整数集合 $\mathbf{Z}$; 有理数集合 $\mathbf{Q}$; 实数集合 $\mathbf{R}$; 复数集合 $\mathbf{C}$.

“泛代数” 是研究代数的一般性的定理和性质, 这些代数是有唯一值和广泛的定义、有限算子等, 这些概念下面会分别给出.

本书讨论的是**近世代数** (modern algebra), 所以首先引入代数的定义.

定义 1.1.1　一个**代数**(algebra)A 是一个对 (S, F), 其中 S 是一个非空集合, F 是一些运算的集合, 其中每个 $f_\alpha\in F$ 为 S 到 S 内的一个幂集 $S^{n(\alpha)}$ 的映射, 这里 $n(\alpha)$ 为一个适当的非负有限整数.

也可表述为, 给每个算子 f_α 指定 S 中元素的 $n(\alpha)$-对 $(x_1, \cdots, x_{n(\alpha)})$, 有 S 中的一个值 $f_\alpha(x_1, \cdots, x_{n(\alpha)})$, 即 f_α 在序列 $x_1, \cdots, x_{n(\alpha)}$ 完成运算.

若 $n(\alpha)=0$, 则运算 f_α 称为**空运算**(nullary), 它选取 S 中的一个固定元 (例如群的单位元, 或格中的最小元, 或最大元).

若 $n(\alpha)=1$, 则运算 f_α 称为**一元运算**(unary).

若 $n(\alpha)=2$, 则运算 f_α 称为**二元运算**(binary).

若 $n(\alpha)$=3, 则运算 f_α 称为**三元运算**(ternary).

以此类推.

例 5　(1) 令 $\mathbf{R}$ 为全体实数, “+” 为通常意义下的实数加法, 则 “+” 为 $\mathbf{R}$ 上的一个二元运算, 并且 $(\mathbf{R},+)$ 为一个代数.