近世代数

Modern Algebra

邢伟 著

科学出版社
www.sciencep.com

近世代数

邢 伟 著

科学出版社
北京

内 容 简 介

本书前三章详细介绍了集合与整数、群和环的内容，最后一章介绍了域的内容。全书重点是群和环。本书内容丰富，叙述简练，论证详细，并且对群、环、域的结论（包括定理、引理、推论等）都给出了方法简练的证明。另外，本书也附加了大量例子以帮助读者很好地理解书中的概念。

本书可作为高等院校数学类各专业、计算机类相关专业、物理类相关专业、化学类相关专业，以及信息科学类相关专业的研究生教材或高年级本科生教材，也可供相关科学技术人员参考。

图书在版编目(CIP)数据

近世代数 / 邢伟著. —北京：科学出版社，2010

ISBN 978-7-03-029036-6

Ⅰ. 近… Ⅱ. 邢… Ⅲ. 抽象代数-高等学校-教材 Ⅳ. 0153

中国版本图书馆 CIP 数据核字(2010)第 184232 号

责任编辑：王志欣 汤 枫 潘继敏 / 责任校对：宋玲玲

责任印制：赵 博 / 封面设计：耕者设计工作室

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

丽源印刷厂 印刷

科学出版社发行 各地新华书店经销

*

2010 年 9 月第 一 版 开本：B5(720×1000)

2010 年 9 月第一次印刷 印张：16

印数：1—3 000 字数：304 000

定价：36.00 元

（如有印装质量问题，我社负责调换）

前　言

作为一门古老的数学分支，代数几乎在人类数学文明的诞生之初就出现了。在制作于公元前2000年左右的古巴比伦人的泥板上，在记载于公元前1650年左右，现今被称为“兰德纸草书(Rhind Papyrus)”和“莫斯科纸草书(Moscow Papyrus)”的古埃及人的数学文字中都出现了若干类型的代数方程(线性的或二次的)求解问题，并给出了解法。

阿拉伯数学家花拉子米(Mohammed ibn Musa al-Khowarizmi，780—850年)在公元825年左右所著的数学教程 *Al-jabr w-al-muqabala* 对后来代数学的发展产生了很大影响。其书名中的 al-jabr 是指解方程过程的移项，al-muqabala 是指解方程过程的化简(即两边消去相同项)。al-jabr 与 al-muqabala 后来演变成英文的数学术语“Algebra(代数)”(顺便指出，中文的“代数”一词是由我国清代数学家李善兰(1811—1882年)于1859年在汉译英文“Algebra”时首创)。由此可见，在历史上，代数学的主要研究对象是方程的求解问题。

一元一、二次方程的求解问题早已解决，三、四次方程的根式求解问题也已在16世纪的中后期分别获得了解决。但四次以上方程的根式求解问题却一直困扰着人们，直到1827年，才由年轻的挪威数学家阿贝尔(Niels Henrik Abel，1802—1829年)获得了重大突破。他第一次严格地证明了一般四次以上方程，即如下方程：

$$x^n + a_1^{n-1}x + \cdots + a_{n-1}x + a_n = 0$$

其中，$n>4$ 为正整数，没有根式解。但是，有些特殊的高次方程，如 $x^n-1=0$，其中，n 为素数，还是有根式解的。那么，一个方程有根式解的充分必要条件是什么呢？法国天才青年数学家伽罗瓦(Evariste Galois，1811—1832年)在1831年成功地解决了这个问题。他在解决这一问题的过程中，首次提出了群(即今天所称的置换群)的概念，并最终利用群与域扩张的方法彻底解决了根式求解问题。

伽罗瓦的方法是划时代的，它开辟了代数学的一个全新的巨大研究领域。从此，以研究代数方程为主的古典代数学走向了以研究集合的代数结构为主的近现代代数学。

在随后的19世纪以及整个20世纪里，人们建立并发展了众多的代数理论，其中对群、环、域等代数结构的研究获得了巨大成功，使得代数学成为20世纪最活跃的数学学科。堪称数学史上最伟大成就之一的有限单群分类定理，于1980年完成，期间先后有100多位数学家参与论证，耗时数十年，整个结果由500多篇论文

组成，其最后证明的总长度达15000页之多！

在1930年与1931年，荷兰数学家范德瓦尔登(Bartel Leendert van der Waerden，1903—1996年)先后出版了两卷本的德文专著 *Moderne Algebra*（近世代数）。该书系统地总结了自伽罗瓦时代以来，特别是进入20世纪以来人们所建立起来的众多代数学的新理论与新方法，在代数学领域产生了深远影响。虽然该书在1955年第四版中已改名为 *Algebra*（代数），但“近世代数”的称谓却流传了下来。

目前，近世代数的理论、思想与方法已经浸透到数学的许多领域，并成为整个现代数学的主要组成部分。与此同时，近世代数的理论、思想与方法也在数学以外的其他领域获得了大量应用，例如，在近代物理、近代化学、计算机科学、编码理论、自动机理论等领域都有着重要应用。

近世代数中的群、环、域等概念是用公理化体系建立起来的，其形式优美，结构清晰，非常有利于数学思维与数学能力的培养与提高。

因为后面内容的需要，本书在第1章中先介绍了集合论的一些初步知识以及整数上的算术理论；第2章与第3章重点介绍了群论与环论的一些内容；最后在第4章介绍了域扩张理论的初步内容。在使用本书时，如果时间紧，每章后面的几节内容可以跳过，另外，每节内容也可以有挑选地读。在阅读本书过程中，如能将重点放在对概念的理解与对方法的掌握上，那将不失为事半功倍的好方法。本书力求叙述简练、论证详细、深入浅出。原则上，阅读本书不需要预备的数学知识，但一些适当数学能力还是需要的。

本书的写作与出版，先后得到了“东北大学研究生院教材建设项目”和科学出版社的大力支持，作者在此向他们表达诚挚的谢意。

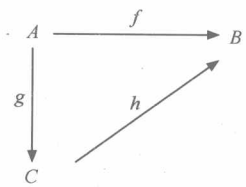
由于时间较紧，尽管做了很大努力，但恐有不当、遗漏之处，恳请读者批评指正或给出您的宝贵建议(联系方式 E-mail：awxing@mail.neu.edu.cn)。

邢　伟
于东北大学理学院
2010年8月17日

书中常用符号说明

符　号	意　义
$\forall$	任意
$\exists$	存在
$\exists 1$	唯一存在，存在唯一的
$\Rightarrow$	蕴含，推得
$\Leftrightarrow$	充分必要，等价于
$:=$	定义式
$\mathbb{N}$	自然数集；$\mathbb{N}=\{0,1,2,\cdots\}$
$\mathbb{Z}$	整数集，整数环；$\mathbb{Z}=\{0,\pm1,\pm2,\cdots\}$
$\mathbb{Z}^+$	正整数集；$\mathbb{Z}^+=\{1,2,3,\cdots\}$
$\mathbb{Q}$	有理数集，有理数域；$\mathbb{Q}=\left\{\frac{m}{n} \mid m,n\in\mathbb{Z},n\neq 0\right\}$
$\mathbb{R}$	实数集，实数域
$\mathbb{C}$	复数集，复数域；$\mathbb{C}=\{a+b\sqrt{-1} \mid a,b\in\mathbb{R}\}$
$\mathbb{Z}_n$	模 n 的剩余类集，模 n 整数加群，模 n 整数环； $\mathbb{Z}_n=\{\bar{0},\bar{1},\cdots,\overline{n-1}\}$，其中 $n\in\mathbb{Z}^+$
$\mathbb{Z}_n^*$	模 n 的单位群，有限域； $\mathbb{Z}_n^*=\{\bar{a}\in\mathbb{Z}_n \mid (a,n)=1\}$，其中 $n\in\mathbb{Z}^+$
$a \mid b$	整数或环中元的整除，等价于 $\exists c$ 使得 $b=ac$
(a,b)	二集合的笛卡儿积的元素，或整数 a,b 的最大公因子
$(a,b)=1$	整数 a,b 互素
$[a,b]$	整数 a,b 的最小公倍数
$a\equiv b \pmod n$	整数 a,b 模 n 同余，等价于 $n \mid (a-b)$
$\varnothing$	空集
$P(S)$	集合 S 的幂集，即 S 的所有子集组成的集合
$f:A\to B$	f 是集合 A 到集合 B 的映射； 当 A 和 B 都具有群(或环等)结构时，f 也表示群(或环等)的同态或同构
$f:A\to B,\quad a\mapsto f(a)$	同上，并且 f 将 $a\in A$ 映射为 $f(a)\in B$

续表

符　号	意　义
$f(S)$	当 $f:A\to B$ 为映射，$S\subset A$ 时，$f(S)$ 为 S 在 f 下的像，即 $f(S)=\{f(a)\mid a\in S\}$
$\mathrm{Im}f$	映射 f 的像，即若 $f:A\to B$，则 $\mathrm{Im}f=f(A)$
$f^{-1}(T)$	当 $f:A\to B$ 为映射，$T\subset B$ 时，$f^{-1}(T)$ 为 T 在 f 下的逆像，即 $f^{-1}(T)=\{a\in A\mid f(a)\in T\}$
$f\mid_S$	限制映射，即当 $f:A\to B$，$S\subset A$ 时，$f\mid_S:S\to B$，$s\mapsto f(s)$
	交换图，表示三映射 f,g,h 满足条件：$hg=f$
1_A	单位映射(恒等映射，单位变换)，即 $1_A:A\to A$，　$a\mapsto a$
$\mid S\mid$，$\mid S\mid<\infty$，$\mid S\mid=\infty$	分别表示集合 S 的基数，“S 是有限集”，“S 是无限集”
$\mathbf{H}\leqslant\mathbf{G}$	$\mathbf{H}$ 为群 $\mathbf{G}$ 的子群
$[\mathbf{G}:\mathbf{H}]$	子群 $\mathbf{H}$ 在 $\mathbf{G}$ 中的指数，$[\mathbf{G}:\mathbf{H}]=\mid\{\mathbf{H}a\mid a\in\mathbf{G}\}\mid$
$\mathbf{H}\lhd\mathbf{G}$	$\mathbf{H}$ 是 $\mathbf{G}$ 的正规子群
$\mathbf{G}/\mathbf{N}$	群 $\mathbf{G}$ 关于其正规子群 $\mathbf{N}$ 的商群
$\langle X\rangle$	由群的子集 X 在群中生成的子群
$\langle e\rangle$	单位元群，即 e 生成的子群，$\langle e\rangle=\{e\}$
$\mid a\mid$	群中元 a 的阶，$\mid a\mid=\mid\langle a\rangle\mid$
$\ker f$	f 的同态核，即当 $f:\mathbf{A}\to\mathbf{B}$ 为群同态时，$\ker f=\{a\in\mathbf{A}\mid f(a)=e_{\mathbf{B}}\}$； 当 f 为环同态时，$\ker f=\{a\in\mathbf{A}\mid f(a)=0\}$
$1_{\mathbf{R}}$	环 $\mathbf{R}$ 的单位元
$\mathrm{char}\,\mathbf{R}$	环 $\mathbf{R}$ 的特征
$\mathbf{R}/\mathbf{I}$	环 $\mathbf{R}$ 关于其理想 $\mathbf{I}$ 的商环
$[X]$	环的子集 X 在环中生成的子环
(X)	环的子集 X 在环中生成的理想
(0)	零理想，或零元 0 生成的理想，$(0)=\{0\}$
$\mathbf{R}[S]$	$\mathbf{R}'$ 为环 $\mathbf{R}$ 的扩环，$S\subset\mathbf{R}'$，$\mathbf{R}[S]$ 为 $\mathbf{R}$ 与 S 在 $\mathbf{R}'$ 中生成的子环，它是 $\mathbf{R}'$ 中包含 $\mathbf{R}$ 与 S 的最小子环

续表

符　号	意　义
$\mathbf{R}[x],\mathbf{R}[x_1,x_2,\cdots,x_n]$	环 $\mathbf{R}$ 上关于未定元 x 或 $x_1,x_2,\cdots,x_n$ 的多项式环
$\mathbf{K}/\mathbf{F}$	域扩张，即域 $\mathbf{K}$ 是域 $\mathbf{F}$ 的扩域
$\mathbf{F}(S)$	在域扩张 $\mathbf{K}/\mathbf{F}$ 中，$S\subset\mathbf{K}$，$\mathbf{F}(S)$ 为 $\mathbf{F}$ 与 S 在 $\mathbf{K}$ 中生成的子域，它是 $\mathbf{K}$ 中包含 $\mathbf{F}$ 与 S 的最小子域
$\mathbf{A}\cong\mathbf{B}$	表示具有代数结构的两个集合之间的同构关系（如群同构、环同构等）
□	定理或引理或推论（包括其证明）的结束处
◇	例子的结束处

书中出现的外国姓氏中英互译
（按中文姓氏汉语拼音排序）

中　文	英　文	年　代	所在国
阿贝尔	Niels Henrik Abel	1802—1829	挪威
埃尔米特	Charles Hermite	1822—1901	法国
艾森斯坦	Ferdinand Gotthold Eisenstein	1823—1852	德国
比左	Etienne Bezout	1730—1783	法国
伯恩斯坦	Felix Bernstein	1878—1956	德国
布尔	George Boole	1815—1864	英国
策梅洛	Ernst Zermelo	1871—1953	德国
戴德金	Richard Dedekind	1831—1916	德国
笛卡儿	Rene Descartes	1596—1650	法国
范德蒙德	Alexandre-Théophile Vandermonde	1735—1796	法国
费尔马	Pierre de Fermat	1601—1665	法国
哈密顿	William Rowan Hamilton	1805—1865	爱尔兰
高斯	Carl Friderich Gauss	1777—1855	德国
凯莱	Arthur Cayley	1821—1895	英国
康托尔	Georg Cantor	1845—1918	德国
克莱因	Felix Christian Klein	1849—1925	德国
柯西	Augustin-Louis Cauchy	1789—1857	法国
拉格朗日	Joseph Louis Lagrange	1736—1813	意大利，德国，法国
林德曼	Ferdinand Lindemann	1852—1939	德国
刘维尔	Joseph Liouville	1809—1882	法国
罗素	Bertrand Russell	1872—1970	英国
欧几里得	Euclid	约公元前 330—前 275	希腊
欧拉	Leonhard Paul Euler	1707—1783	瑞士
施罗德	Ernst Schroeder	1841—1902	德国
韦达	Francois Viete	1540—1603	法国
希尔伯特	David Hilbert	1862—1943	德国
西罗	Peter Ludwig Mejdell Sylow	1832—1918	挪威
佐恩	Max August Zorn	1906—1993	德国，美国

目　录

第 1 章　集合与整数

1.1　集　　合

集合是数学的最基本概念之一。它既普通，又不平凡。说它普通，是因为集合一词经常出现在人们的日常生活中；说它不平凡，则是因为集合曾经引起了轰动 20 世纪初叶的“第三次数学危机”。

当作为一个最基本的数学概念时，集合没有严格的数学定义，只有对它的描述。集合论创始人康托尔认为：集合是一些确定的、不同的东西的总体，这些东西人们能意识到，并且能判断一个给定的东西是否属于这个总体。也就是说，集合(set)是一些具有一定属性的对象所组成的一个整体，该属性能够区别一个对象是否属于该集合。集合中的对象被称为集合的元素(element)，一个集合是由它的所有元素组成的。设 S 为一个集合，当元素 a 属于 S 时，记 $a \in S$，否则记 $a \notin S$。

例 1.1.1　所有整数组成的集合被称为整数集(set of integers)，记为$\mathbb{Z}$，即

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \cdots, \pm n, \cdots\}$$

所有有理数组成的集合被称为有理数集(set of rational numbers)，记为$\mathbb{Q}$，即

$$\mathbb{Q} = \left\{ \frac{m}{n} \mid m, n \in \mathbb{Z},\ n \neq 0 \right\}$$

所有实数组成的集合被称为实数集(set of real numbers)，记为$\mathbb{R}$。

所有复数组成的集合被称为复数集(set of complex numbers)，记为$\mathbb{C}$，即

$$\mathbb{C} = \{a + b\sqrt{-1} \mid a, b \in \mathbb{R}\}$$

通常，也称非负整数为自然数(natural number)。所有自然数组成的集合被称为自然数集(set of natural numbers)，记为$\mathbb{N}$，即

$$\mathbb{N} = \{n \in \mathbb{Z} \mid n \geqslant 0\} = \{0, 1, 2, \cdots, n, \cdots\}$$

所有正整数组成的集合被称为正整数集(set of positive integers)，记为$\mathbb{Z}^+$，即

$$\mathbb{Z}^+ = \{n \in \mathbb{Z} \mid n > 0\} = \{1, 2, \cdots, n, \cdots\}$$ ◇

例 1.1.2　任意一个集合，比如 S，它可以不是它自己的元素(即 $S \notin S$)，它也可以是自己的元素(即 $S \in S$)。这样一来，我们可以将集合分成两类：第一类的集合 S 都满足 $S \notin S$，第二类的集合 S 都满足 $S \in S$。第一类的集合是经常遇见的，如正整数集合$\mathbb{Z}^+$就是第一类集合，因为$\mathbb{Z}^+$本身已不是正整数了，即$\mathbb{Z}^+ \notin \mathbb{Z}^+$；又如方程 $x^2 - 1 = 0$ 的解集合

$$\Gamma = \{x \in \mathbb{C} \mid x^2 - 1 = 0\} = \{1, -1\}$$

也是第一类集合，因为 Γ 本身不是方程的解，即 $\Gamma \notin \Gamma$。属于第二类的集合也是大量存在的，如 $\forall i \in \mathbb{Z}^+$，令

$$A_i := \{S \mid S\text{为集合且}S\text{所含元素个数} > i\}$$

及 $\forall k \in \mathbb{N}$，令

$$B_i^{(k)} := \{x \in \mathbb{N} \mid k \leqslant x \leqslant k + i\}$$

则因 $B_i^{(k)}(k = 0,1,2,\cdots)$ 所含元素个数都为 $i+1$，故集合

$$B_i^{(0)}, B_i^{(1)}, \cdots, B_i^{(i)}, B_i^{(i+1)} \in A_i$$

这说明集合 A_i 所含元素的个数也是大于 i 的，于是有 $A_i \in A_i$。

现在考虑集合 $M := \{S \mid S\text{为集合且}S \notin S\}$（即 M 是由所有第一类集合作为元素所组成的集合）。我们面对的问题是，作为一个集合，M 应该属于第几类呢？根据集合 M 的定义即知：若 $M \notin M$，则 $M \in M$；若 $M \in M$，则 $M \notin M$。

由此产生了一个逻辑“怪圈”，这个逻辑怪圈就是著名的罗素悖论(Russell's paradox)，它是由集哲学家、逻辑学家、数学家于一身的罗素于 1902 年提出来的。罗素悖论的出现在数学的历史上引发了一场危机，史称“第三次数学危机”。 ◇

为了避免上述集合悖论的产生，人们建立了公理集合论。在公理集合论中，为了避免悖论的出现，人们引进了类的概念，而将集合视为一种特殊的类。类(class)可以理解为具有一定属性的一些对象的全体。若对象 x 属于类 C，则记为 $x \in C$，否则记为 $x \notin C$。对于类 S，若存在类 C，使得 $S \in C$，则称 S 为集合。当一个类不是集合时，称这样的类为真类(proper class)。在例 1.1.2 中的 M 就不是一个集合而是一个真类。

本书所要讨论的主要内容是具有一定代数运算的集合，这些集合分别是群、环、域。

设 A、B 为集合，若 $\forall a \in A$，都有 $a \in B$，则称集合 A 是集合 B 的子集(subset)，并记为 $A \subset B$（有时也记为 $A \subseteq B$）。当 $A \subset B$ 时，也称集合 A 包含在集合 B 中，或集合 B 包含集合 A。若 $A \subset B$ 且 $B \subset A$，则称集合 A 与 B 相等(equality)，记为 $A = B$。也就是说，两个集合相等的充分必要条件是它们互相包含。当 $A \subset B$ 但 $A \neq B$ 时，有时记为 $A \subsetneq B$。

空集(empty set)是不含任何元素的集合，将空集记为 $\varnothing$。事实上，$\varnothing = \{x \mid x \neq x\}$。由于对于任何元素 x，都有 $x \notin \varnothing$，也即 $x \in \varnothing$ 总是假的，故对于任意集合 S，语句“ $\forall x \in \varnothing$，都有 $x \in S$ ”为真，于是 $\varnothing \subset S$，即空集是任意集合的子集。

若 $A \subsetneq B$ 但 $A \neq \varnothing$，则称 A 是 B 的真子集(proper subset)。

设 S 为集合，则 S 的所有子集也构成了一个集合，称其为 S 的幂集(power set)，记为 $P(S)$。$P(S) = \{A \mid A \subset S\}$，其中 $\varnothing \in P(S)$。

设 I 为集合，若 $\forall i \in I$，都对应一集合 A_i，则称 $\{A_i \mid i \in I\}$ 为集族(family of set)，其中 I 被称为该集族的指标集(index set)。集族 $\{A_i \mid i \in I\}$ 的并(union)定义为

$$\bigcup_{i \in I} A_i := \{x \mid \exists j \in I, x \in A_j\}$$

集族 $\{A_i \mid i \in I\}$ 的交(intersection)定义为

$$\bigcap_{i \in I} A_i := \{x \mid \forall j \in I, x \in A_j\}$$

集族的并与交也都是集合。特别的，当 $I = \{1,2,\cdots,n\}$ 时，分别记

$$A_1 \cup A_2 \cup \cdots \cup A_n := \bigcup_{i \in I} A_i$$

$$A_1 \cap A_2 \cap \cdots \cap A_n := \bigcap_{i \in I} A_i$$

当二集合 A 与 B 的交为空集，即 $A \cap B = \varnothing$ 时，称 A 与 B 不相交(disjoint)。

设 A 和 B 为集合，则

$$A \backslash B := \{a \in A \mid a \notin B\}$$

也是集合，称 $A \backslash B$ 为 A 与 B 的差(difference)，或称 B 在 A 中的相对补(relative complement)。当所讨论的集合 A 是集合 U 的子集时，称 $\overline{A} := U \backslash A$ 为 A 的补(complement)。

集合的并、交以及差是集合之间的三种基本运算。设集合 A 和 B 都是集合 U 的子集，即 $A, B \subset U$，则 A 和 B 的并、交以及差可以通过图 1.1.1 直观表示。

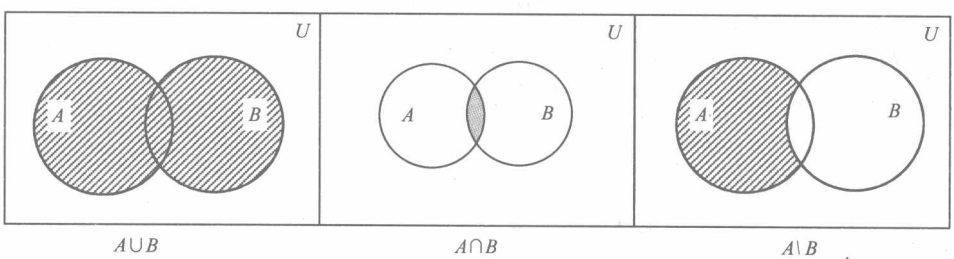


图 1.1.1　A 和 B 的并、交以及差

定理 1.1.1　集合的运算具有下列基本性质：

1) $A \cup A = A, A \cap A = A$。(idempotent law，幂等律)

2) $A \cup B = B \cup A, A \cap B = B \cap A$。(commutative law，交换律)

3) $(A \cup B) \cup C = A \cup (B \cup C), (A \cap B) \cap C = A \cap (B \cap C)$。(associative law，结合律)

4) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C), A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$。(distributive law，分配律)

$A \cup \bigcap_{i \in I} B_i = \bigcap_{i \in I} (A \cup B_i), A \cap \bigcup_{i \in I} B_i = \bigcup_{i \in I} (A \cap B_i)$。(generalized distributive law，广义分配律)

5) $A \cup (A \cap B) = A$, $A \cap (A \cup B) = A$。(absorption law,吸收律)

6) 若 $A \subset C$, 则 $A \cup (B \cap C) = (A \cup B) \cap C$。(modular law,模律)

设 $A \subset U, \overline{A} = U \backslash A$, 则

7) $\overline{(\overline{A})} = A$。(involution law,对合律)

8) $A \cup \varnothing = A, A \cap U = A$。(identity law,同一律)

9) $A \cup \overline{A} = U, A \cap \overline{A} = \varnothing$。(complement law,补律)

10) $A \cup U = U, A \cap \varnothing = \varnothing$。(domination law,控制律)

11) $\overline{A \cup B} = \overline{A} \cap \overline{B}, \overline{A \cap B} = \overline{A} \cup \overline{B}$。(De Morgan's law,德摩根律)

12) $\overline{(\bigcup\limits_{i \in I} A_i)} = \bigcap\limits_{i \in I} \overline{A_i}, \overline{(\bigcap\limits_{i \in I} A_i)} = \bigcup\limits_{i \in I} \overline{A_i}$。(generalized De Morgan's laws,广义德摩根律)

证明 略。 □

另外,不难证明集合还具有下列诸性质。

定理 1.1.2 设 A, B, C 和 U 均为集合。

1) 若 $A, B \subset C$, 则 $A \cup B \subset C$。

2) 若 $C \subset A, B$, 则 $C \subset A \cap B$。

3) 若 $A, B \subset U$, 且有 $A \cup B = U, A \cap B = \varnothing$, 则 $B = \overline{A}$。特别的, $\overline{\varnothing} = U$, $\overline{U} = \varnothing$。

4) $A \subset B \Leftrightarrow A \cap B = A \Leftrightarrow A \cup B = B \Leftrightarrow A \backslash B = \varnothing \Leftrightarrow \overline{B} \subset \overline{A}$。

5) $C \backslash (A \cap B) = (C \backslash A) \cup (C \backslash B)$。

6) $C \backslash (A \cup B) = (C \backslash A) \cap (C \backslash B)$。

7) $C \backslash (B \backslash A) = (A \cap C) \cup (C \backslash B)$。

8) $(B \backslash A) \cap C = (B \cap C) \backslash A = B \cap (C \backslash A)$。

9) $(B \backslash A) \cup C = (B \cup C) \backslash (A \backslash C)$。

10) $B \backslash A = \overline{A} \cap B$。

11) $\overline{(B \backslash A)} = A \cup \overline{B}$。

证明 略。 □

习题 1.1

1. 写出以下各集合的表达式。

1) 所有偶数组成的集合,所有奇数组成的集合。

2) 所有能被 7 整除的整数组成的集合,所有不能被 7 整除的整数组成的集合。

3) 所有有理数组成的集合,所有复数组成的集合。

4) 平面上的所有点组成的集合,单位圆圆周上的所有点组成的集合,单位圆

所有圆内的点组成的集合。

5) 齐次线性方程组 $Ax=0$ 与 $Bx=0$ 的所有公共解组成的集合。

2. 设

$$A=\{x\in\mathbb{R}\mid |x|\geqslant 3\},\quad B=\{x\in\mathbb{R}\mid -5<x<0\}$$

求：$A\cup B, A\cap B, A\backslash B, B\backslash A, (A\backslash B)\cup(B\backslash A)$。

3. 设 $A=\{1,2,3,4,5\}$，求 A 的幂集 $P(A)$。

4. $\forall n\in\mathbb{Z}^+$，令

$$A_n=\{x\in\mathbb{R}\mid |x|<n\},\quad B_n=\{x\in\mathbb{R}\mid |x|<n^{-1}\}$$

1) 证明：$A_1\subset A_2\subset\cdots\subset A_n\subset\cdots, B_1\supset B_2\supset\cdots\supset B_n\supset\cdots$。

2) 求：$\bigcup\limits_{n\in\mathbb{Z}^+}A_n$，$\bigcap\limits_{n\in\mathbb{Z}^+}B_n$。

5. 设 A,B 为二集合，称集合

$$A\Delta B:=(A\backslash B)\cup(B\backslash A)$$

为 A 与 B 的对称差(symmetric difference)。证明：

1) $A\Delta B=B\Delta A$; 2) $A\Delta\varnothing=A$;3) $A\Delta A=\varnothing$;4)$(A\Delta B)\Delta C=A\Delta(B\Delta C)$。

6. 证明定理 1.1.1。

7. 证明定理 1.1.2。

1.2　映　　射

映射是数学的另一个最基本的概念，也是数学的一个最重要的概念。它建立在集合之上，并有着广泛的含义与应用背景。例如，我们所熟悉的各种函数以及各种运算，通常都是映射。

映射的概念可以利用集合的语言来严格定义(见 1.3 节)。在这里，我们采用更为习惯的方式来给出映射的定义。

定义 1.2.1　设 A 与 B 为二非空集合。A 到 B 的映射(map) f 是指一个对应，使得 $\forall a\in A,\exists 1 b\in B$，$b$ 与 a 对应(或者说，b 通过 f 被 a 唯一确定)。称 b 是 f 在 a 处的值(value)，并记 $f(a)=b$，称集合 A 是 f 的定义域(domain)，集合 B 是 f 的值域(range)。特别的，当 $B=A$ 时，称 A 到 A 的映射为 A 上的变换(transformation)。

上面所定义的由集合 A 到集合 B 的映射 f 通常表示为

$$f:A\to B,\quad a\mapsto b$$

设 $f,g:A\to B$ 都是映射，若 $\forall a\in A$，都有 $f(a)=g(a)$，则称 f 与 g 是相等的(equal)，并记为 $f=g$。

设 $f:A\to B$ 为映射，$\varnothing\neq S\subset A$，称映射

$$S\to B,\quad s\mapsto f(s)$$

为 f 在 S 上的限制(restriction),也记为 $f|_S: S \to B$。设 A 为非空集合,称映射

$$A \to A, \quad a \mapsto a$$

为 A 上的单位映射(或恒等映射,或单位变换)(identity map, identity transformation),并记为 1_A 或 1。设 $S \subset A$,称映射

$$i: S \to A, \quad s \mapsto s$$

为包含映射(inclusion map)。

设二映射 $f: A \to B, g: B \to C$,则称映射

$$A \to C, \quad a \mapsto g(f(a))$$

为 f 与 g 的合成(composite),也称 f 与 g 的积(product),记为 $g \circ f$ 或 gf。

定理 1.2.1 1)设三映射 $f: A \to B, g: B \to C, h: C \to D$,则

$$(hg)f = h(gf)$$

即映射的合成满足结合律。

2) 设映射 $f: A \to B$,则 $f \circ 1_A = f, 1_B \circ f = f$。

证明 1) 因 $(hg)f$ 与 $h(gf)$ 都是集合 A 到集合 D 的映射,且 $\forall a \in A$,有

$$((hg)f)(a) = (hg)(f(a)) = h(g(f(a))) = h((gf)(a)) = (h(gf))(a)$$

故有 $(hg)f = h(gf)$。

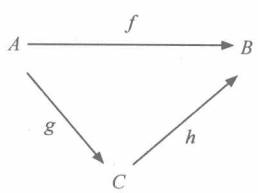


图 1.2.1 交换图

2) 注意 $f \circ 1_A$ 也是集合 A 到集合 B 的映射,而 $\forall a \in A, (f \circ 1_A)(a) = f(1_A(a)) = f(a)$,故 $f \circ 1_A = f$。同理可证,$1_B \circ f = f$。 □

设 $f: A \to B, g: A \to C, h: C \to B$ 为三个映射,如果 $hg = f$,则称图 1.2.1 是交换图(commutative)。

设 $f: A \to B$ 为映射,$S \subset A$,称

$$f(S) := \{f(s) \mid s \in S\}$$

为 S 在 f 下的像(image of S under f)。特别的,称 $\mathrm{Im} f := f(A)$ 为 f 的像(image of f)。设 $T \subset B$,称

$$f^{-1}(T) := \{a \in A \mid f(a) \in T\}$$

为 T 在 f 下的逆像(inverse image of T under f)。特别的,若 $b \in B$,记

$$f^{-1}(b) := \{a \in A \mid f(a) = b\}$$

定理 1.2.2 设 $f: A \to B$ 为映射,则

1) 当 $S \subset A$ 时,$S \subset f^{-1}(f(S))$。

2) 当 $T \subset B$ 时,$f(f^{-1}(T)) \subset T$。

3) 当 $\{T_i \mid i \in I\}$ 为 B 的子集族时,$f^{-1}\left(\bigcup\limits_{i \in I} T_i\right) = \bigcup\limits_{i \in I} f^{-1}(T_i)$,$f^{-1}\left(\bigcap\limits_{i \in I} T_i\right) = \bigcap\limits_{i \in I} f^{-1}(T_i)$。

证明 1) 记 $T := f(S)$。$\forall s \in S$,因 $f(s) \in f(S) = T$,故 $s \in f^{-1}(T) =$