第3版

离散数学

主　编　章炯民　陶增乐
副主编　柳银萍　李海晟　杨　沛

审　定　陈强璋　黄馥林

华东师范大学出版社

离散数学

（第 3 版）

主　编　章炯民　陶增乐
副主编　柳银萍　李海晟　杨　沛
审　定　陈强璋　黄馥林

华东师范大学出版社

图书在版编目(CIP)数据

离散数学/章炯民，陶增乐主编.—3版.—上海：华东师范大学出版社，2009
ISBN 978-7-5617-6765-8

Ⅰ.离… Ⅱ.①章…②陶… Ⅲ.离散数学—高等学校—教材 Ⅳ.0158

中国版本图书馆CIP数据核字(2009)第028253号

离散数学(第3版)

主　　编　章炯民　陶增乐
责任编辑　朱建宝
审读编辑　王春华
封面设计　黄惠敏

出版发行　华东师范大学出版社
社　　址　上海市中山北路3663号　邮编200062
电话总机　021-62450163转各部门　行政传真021-62572105
客服电话　021-62865537(兼传真)
门市(邮购)电话　021-62869887
门市地址　上海市中山北路3663号华东师范大学校内先锋路口
网　　址　www.ecnupress.com.cn

印 刷 者　江苏省句容市排印厂
开　　本　787×1092　16开
印　　张　15.5
字　　数　389千字
版　　次　2009年6月第1版
印　　次　2009年6月第1次
印　　数　3100
书　　号　ISBN 978-7-5617-6765-8/O·208
定　　价　28.00元

出 版 人　朱杰人

前　　言

现代社会与计算机日益密切地融合，而数字计算机本质上是一种“离散”的机器，并越来越多地用于处理离散的对象，从而使“离散数学”成为计算机科学不可或缺的理论基础和工具，并推动离散数学本身进一步发展和丰富。作为计算机专业最重要的必修课程之一，近年来离散数学越来越受到重视，它不仅是学习后继课程的基础，更是培养学生的思维、提高分析问题和解决问题的能力的重要途径。

本书第一版成书于 1985 年，11 年后，为了适应计算机学科的迅速发展作了一次修订。如今，距第二版成书又过去了 13 年。期间，不仅计算机学科本身又有了许多重大进展，而且目前的社会环境、高校和学生的情况都与以往大不一样。正是基于这样的背景，我们对第二版再次作了全面修订，以适应学科的发展和教学的需要。

第三版的内容组织主要依据教育部计算机科学与技术专业教学指导分委员会制定的《高等学校计算机科学与技术专业发展战略研究报告暨专业规范》，并参考了美国计算机学会 ACM 的 *Computing Curricula 2005*。与第二版相比较，第三版的涵盖面有所扩大，增加了初等数论、组合数学等方面的内容；与计算机科学的结合更紧密，增加了离散数学应用的内容；压缩了某些较抽象、实际应用中较少涉及的内容，如集合的基数等。

本书前两版的显著特点是：简洁、条理清晰。第三版在保持这两个特点的基础上，把离散数学与计算机科学有机地联系起来，力图将本教材编写成“面向计算机科学的”离散数学。一方面加强学生对基本内容的掌握，培养分析问题和解决问题的能力；另一方面，进一步激发学生的学习兴趣。此外，第三版对学生的实际情况也作了充分考虑，对难点和重点的讨论尽可能地做到直观、循序渐进、详尽，并适当地作了一些学习指导。

第三版包含的内容较多，一般需要两个学期才能全部覆盖。教师可根据具体的专业方向、教学目标、学生的情况等进行适当组合。本书在内容的组织上已经充分考虑到这样的需要，尽可能地保持各章节内容的自含，以便于取舍。

第三版第一章、第五至八章、第十四由章炯民执笔，第二章、第十一至十三章由柳银萍执笔，第三章、第四章由杨沛执笔，第九章、第十章由李海晟执笔。限于编者的水平，书中疏漏和不妥之处难免，恳请读者指正。

编　者

2009 年 4 月

目　录

第一章

集 合 论

集合是数学的基本概念，很多数学家都认为，所有的数学都可以用集合论的术语来表示。集合论的起源可以追溯到 16 世纪末，但它的创立是在 19 世纪末由德国数学家康托尔(G. Cantor)完成的。最初，为了建立微积分学的严格的理论基础，人们对数集进行了研究，直到 1876～1883 年，康托尔对任意元素的集合进行了系统的研究，提出了基数、序数和良序集等理论，从而奠定了集合论的基础。这样的集合论基于直观的集合概念，称为朴素集合论。1900 年前后，由于各种悖论的发现，特别是 1901 年罗素(B. Russell)悖论的发现，使集合论的发展一度受阻。1908 年，策墨罗(E. Zermelo)提出了第一个集合论的公理系统，使数学哲学中产生的一些矛盾基本上得到统一。在此基础上，集合论与逻辑学相互融合并迅速发展，逐步形成了各种公理集合论。现在，集合论不仅作为一门纯数学成为数理逻辑的一个主要分支，而且作为精确、严谨而又简便的语言，已经渗透到现代数学的各个领域，成为整个数学的基础。

计算机科学对集合论感兴趣，是因为它在计算机科学中被广泛地应用，是建立数学模型以及进行深入探讨的有力工具。比如，在形式语言、编译理论、信息检索、数据结构、程序设计、算法分析、数据库、有限自动机、人工智能等等许多领域中，集合论都是不可缺少的理论工具，起着重要的作用。

本书仅限于讨论朴素集合论。本章介绍集合的基础知识，主要包括集合的概念、集合运算及其基本性质、n 元组和笛卡儿乘积等等，这些基本概念是离散数学的基础，将贯穿整个课程。集合论的其他重要内容，如关系、函数、基数等等，将在第五章和第六章中讲述。

1.1 集合的概念和术语

1.1.1 集合的基本概念和表示

集合是最基本的数学概念，没有更基本的可用来定义集合的其他数学概念了，它的严谨描述属于数学的一个分支——公理集合论的研究范畴，这里只给出集合的直观描述。把某些对象汇集在一起，视为一个整体，这个整体就是一个**集合**，其中的对象(也就是各个个体)称为集合的**元素**。集合也常简称为**集**。

例如，所有的整数组成一个集合，这个集合含有整数…、-2、-1、0、1、2、…，但是不含有 6.8、π、$\sqrt{2}$…非整数；中国的所有大学也构成一个集合，北京大学、清华大学、华东师范大学等等都是这个集合的元素，但是，哈佛大学、麻省理工学院等等都不是这个集合的元素。还有大家熟悉的自然数集、有理数集和实数集等等，都是集合的例子。

通常，集合用大写英文字母表示，集合中的元素用小写英文字母表示，并且约定 $\mathbf{N}$、$\mathbf{Z}$、$\mathbf{Q}$ 和 $\mathbf{R}$ 分别表示自然数集、整数集、有理数集和实数集，$\mathbf{Z}^+$、$\mathbf{Q}^+$ 和 $\mathbf{R}^+$ 分别表示正整数集(即自然数集 $\mathbf{N}$)、正有理数集和正实数集，$\mathbf{Z}^-$、$\mathbf{Q}^-$ 和 $\mathbf{R}^-$ 分别表示负整数集、负有理数集和负实数集。

若 x 是集合 A 中的元素，那么称 x **属于** A，记为 $x \in \mathbf{A}$。反之，若 x 不是 A 的元素，称 x **不属于** A，记为 $x \notin \mathbf{A}$。例如，$3 \in \mathbf{N}$，$0 \notin \mathbf{N}$，$\sqrt{2} \notin \mathbf{Q}$，$\sqrt{2} \in \mathbf{R}$。

除了用符号表示集合及其元素以外，列举法、概括法和文氏图也是常用的描述集合的方法。

(1) 列举法

在花括号{ }中列举出集合的所有元素，或者将集合中的所有元素按某种显而易见的规律罗列出来。例如，$\{1, 2, \{4\}\}$ 表示一个集合，这个集合中有 3 个元素，分别是 1、2 和 $\{4\}$；$\{1, 2, 3, \cdots\}$ 表示所有正整数的集合 $\mathbf{Z}^+$，也就是自然数集 $\mathbf{N}$。

(2) 概括法

通过指出集合中的元素所具有的性质来表示集合。如果集合 A 中的元素都具有性质 p[①]，而不在 A 中的元素都不具有性质 p，也就是说，集合 A 由所有具有性质 p 的元素组成，那么应用概括法集合 A 可表示为

$$\{x \mid p(x)\}。$$

例如，

$$\{x \mid x \in \mathbf{R} \text{ 且 } 0 < x < 1\}$$

表示开区间 $(0, 1)$ 上的所有实数组成的集合；

$$\{x \mid x \text{ 是 } 10 \text{ 以内的质数}\}$$

表示一个集合，这个集合中有 4 个元素，它们分别是 2、3、5 和 7，也即 $\{2, 3, 5, 7\}$。

不难看出，集合

$$\{x \mid x \in \mathbf{R} \text{ 且 } x^2 + 1 = 0\}$$

不含任何元素。不含任何元素的集合称为**空集**，记为 $\varnothing$。

在特定的讨论范围内，由所关心的全体对象所组成的集合称为**全集**，全集常用 U 来表示。比如，在微积分中，我们的讨论范围是全体实数，全集是实数集 $\mathbf{R}$；在数论中，全集是整数集 $\mathbf{Z}$，因为数论只关心整数的性质，而不关心小数和无理数。所以，相应于不同的领域，全集也不尽相同，这一点需要特别注意。

(3) 文氏图

文氏图是以英国数学家 John Venn 的名字命名的，它可以形象地表示集合，尤其是集合之间的关系(参见 1.1.2 小节)。虽然这种表示方法并不精确，但它可以极大地帮助我们直

① 在数理逻辑中，个体对象的性质可用一个谓词 $p(x)$ 表示，所以概括法也称为**谓词法**。

观地分析问题。

文氏图把集合表示成几何图形，主要是矩形和圆(或椭圆)，其中，矩形表示全集，圆或其他图形表示一般集合，有时也用点来表示集合中特定的元素。

在图 1.1.1 所展示的文氏图中，全集 U 是由 26 个小写英文字母组成的集合，集合 V 由 5 个小写的元音字母构成。在文氏图 1.1.2 中，全集 U 是实数集 $\mathbf{R}$，三个集合 $\mathbf{R}$、$\mathbf{Q}$ 和 $\mathbf{N}$ 相互之间的“大小”关系在图中得到了直观的展示。

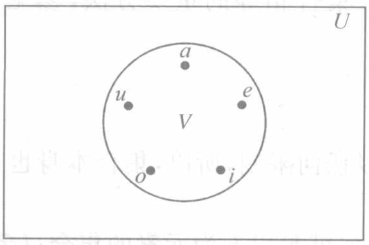

图 1.1.1 $U=\{a, b, c, \cdots, z\}$, $V=\{a, e, i, o, u\}$

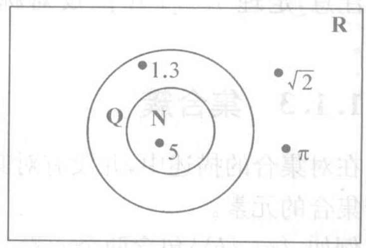

图 1.1.2 $U=\mathbf{R}$

1.1.2 集合之间的关系

定义 1.1.1 若集合 A 和 B 包含相同的元素，则称 **A 和 B 相等**，记为 $A=B$。

例如，$\mathbf{Z}^{+}=\mathbf{N}$。

由上述定义，集合仅由组成它的元素所决定，而与元素在集合中出现的顺序和次数无关。例如：

$$\{3, 4, 5\}=\{5, 4, 3\}=\{5, 5, 4, 4, 4, 3\}, \{x \mid x^{2}-1=0\}=\{-1, 1\}。$$

定义 1.1.2 若集合 A 中的元素均属于集合 B，则称 A **是** B **的子集**，B **包含** A，A **包含于** B，记为 $A \subseteq B$ 或 $B \supseteq A$。特别地，若 $A \subseteq B$ 但 $A \neq B$，则称 A **是** B **的真子集**，B **真包含** A，A **真包含于** B，记为 $A \subset B$ 或 $B \supset A$。

例如，因为每个自然数都是整数，而有些整数不是自然数，所以，$\mathbf{N}$ 是 $\mathbf{Z}$ 的真子集，亦即 $\mathbf{N} \subset \mathbf{Z}$。注意，集合 $\{a, b\}$ 不是集合 $\{\{a\}, b\}$ 的子集，当然也不是它的真子集。

显然，空集是任何集合的子集，每个集合又都是全集的子集，即

$$\varnothing \subseteq A \subseteq U。$$

另外，任何集合都是其本身的子集，但不是其本身的真子集。所以，对于任意集合 A，称 $\varnothing$ 和 A 为它的**平凡子集**。

文氏图 1.1.3 和 1.1.4 形象地表示了 $A \subseteq B$ 和 $A \not\subseteq B$。

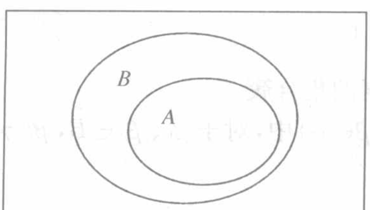

图 1.1.3 $A \subseteq B$

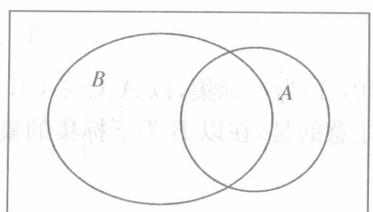

图 1.1.4 $A \not\subseteq B$

集合之间的包含关系满足下列性质。

定理 1.1.1 对于任意集合 A、B 和 C：

(1) $A \subseteq A$（自反性）；

(2) 若 $A \subseteq B$，且 $B \subseteq A$，则 $A = B$（反对称性）；

(3) 若 $A \subseteq B$，且 $B \subseteq C$，则 $A \subseteq C$（传递性）。

定理 1.1.1 的证明留作练习，请读者自行完成。

注意，定理 1.1.1 中的反对称性是证明两个集合相等的重要方法，参见 1.2 和 1.3 小节。

1.1.3 集合簇

在对集合的描述中，并没有对其中的元素加以任何限制，所以，集合本身也可以作为另一个集合的元素。

例如，$\{a, \{b\}\}$ 包含两个元素，其中一个元素 $\{b\}$ 就是以 b 为元素的集合；$\{\varnothing\}$ 是以空集 $\varnothing$ 为元素的单元素集。容易看出，

$$\{a, \{b\}\} \neq \{a, b\},$$

$$\{a, \{b\}\} \subseteq \{a, b, \{b\}\},$$

$$\{\varnothing\} \neq \varnothing,$$

$$\varnothing \subseteq \{\varnothing\}。$$

特别地，一个集合的所有元素可以都是集合。为了避免过多地使用集合这个词，把由若干集合组成的集合称为**集合簇**。

例如，$\{\varnothing\}$ 和 $\{\varnothing, \{b\}\}$ 都是集合簇。当 $A_1 = \{1\}$，$A_2 = \{2\}$ 时，称 $\{A_1, A_2\}$ 是以 $\{1, 2\}$ 为下标集，以 A_1 和 A_2 为元素的集合簇。

一般地，若 B 是集合，且对任意 $\beta \in B$，A_β 是一个集合，那么称

$$\{A_\beta \mid \beta \in B\}$$

为以 B 为下标集，以所有 $A_\beta(\beta \in B)$ 为元素的集合簇。

例如，对任意自然数 n，若定义 $A_n = \{x \mid 0 < x < 1 + \frac{1}{n}\}$，则

$$\{A_n \mid n \in \mathbf{N}\}$$

是以自然数集 $\mathbf{N}$ 为下标集，以 $A_n(n \in \mathbf{N})$ 为元素的集合簇。对任意 $x \in (0, 1)$，若令 $A_x = \{x\}$，则

$$\{A_x \mid x \in (0, 1)\}$$

是以集合 $(0, 1)$ 为下标集，以 $A_x(x \in (0, 1))$ 为元素的集合簇。

值得注意的是，在以 B 为下标集的集合簇 $\{A_\beta | \beta \in B\}$ 中，对于 β_1、$\beta_2 \in B$，$\beta_1 \neq \beta_2$，允许 $A_{\beta_1} = A_{\beta_2}$。

1.2 集合的运算

1.2.1 集合的基本运算

对实数可以进行加、减、乘和除等等基本运算，结果得到其他实数。类似地，集合上也有并、交、差和补等基本运算，运算结果是其他新的集合。

定义 1.2.1 设 A 和 B 是集合，由 A 和 B 的所有元素所组成的集合称为 A 和 B 的**并集**，记为 $A \cup B$；由 A 和 B 的公共元素所组成的集合称为 A 和 B 的**交集**，记为 $A \cap B$；属于 A 但不属于 B 的元素所组成的集合称为 A 关于 B 的**差集**，记为 $A-B$。特别地，称 $U-A$ 为 A 的**补集**，记为 $\overline{A}$。也就是说

$$A \cup B = \{x \mid x \in A \text{或} x \in B\},$$
$$A \cap B = \{x \mid x \in A \text{且} x \in B\},$$
$$A - B = \{x \mid x \in A \text{但} x \notin B\},$$
$$\overline{A} = \{x \mid x \notin A\}。$$

文氏图 1.2.1、1.2.2、1.2.3 和 1.2.4 中的阴影区域分别表示了 $A \cup B$、$A \cap B$、$A-B$ 和 $\overline{A}$。

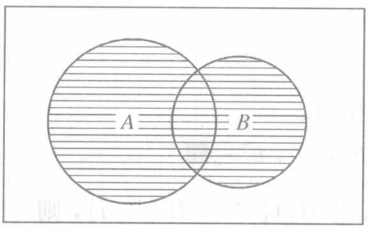

图 1.2.1 $A \cup B$

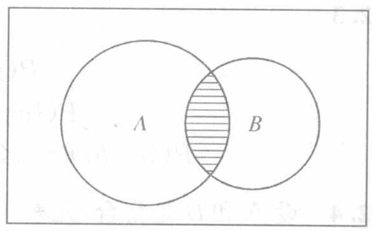

图 1.2.2 $A \cap B$

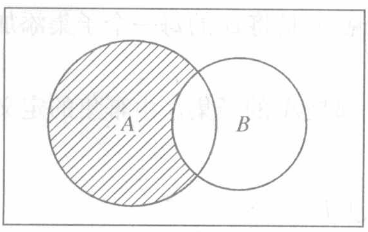

图 1.2.3 $A-B$

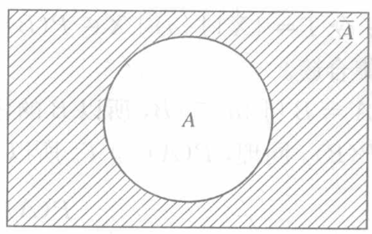

图 1.2.4 $\overline{A}$

例 1.2.1

$$\{1, 2\} \cup \{5, 6\} = \{1, 2, 5, 6\},$$
$$\{1, 2\} \cup \{2, 3\} = \{1, 2, 3\},$$
$$\{1, 2\} \cap \{2, 3\} = \{2\},$$
$$\{1, 2\} \cap \{5, 6\} = \varnothing,$$
$$\{1, 2\} - \{2, 3\} = \{1\},$$
$$\{1, 2\} - \{5, 6\} = \{1, 2\},$$

$$\{1, 2\} - \{1, 2, 3\} = \varnothing。$$

若全集 U 为 $\mathbf{N}$,则

$$\overline{\{1, 2\}} = \mathbf{N} - \{1, 2\} = \{3, 4, 5, 6, \cdots\}。■$$

当集合 A 和 B 满足 $A \cap B = \varnothing$ 时,称 A 和 B **互不相交**。

1.2.2 幂集

定义 1.2.2 设 A 是集合,由 A 的所有子集所组成的集合称为 A 的**幂集**,记为 $P(A)$。也就是说

$$P(A) = \{X \mid X \subseteq A\}。$$

由定义可知:$\varnothing \in P(A)$;$A \in P(A)$;$X \in P(A)$ 当且仅当 $X \subseteq A$。

例 1.2.2 $P(\mathbf{N})$表示自然数集 $\mathbf{N}$ 的幂集,所以

$$\{1\} \in P(\mathbf{N}),$$
$$\{2, 4\} \in P(\mathbf{N}),$$
$$\{1, 3, 5, 7, \cdots, 2n-1, \cdots\} \in P(\mathbf{N}),$$
$$\{\{1\}, \{2, 4\}, \{1, 3, 5, 7, \cdots\}\} \subseteq P(\mathbf{N})。■$$

例 1.2.3

$$P(\varnothing) = \{\varnothing\},$$
$$P(\{a\}) = \{\varnothing, \{a\}\},$$
$$P(\{a, b\}) = \{\varnothing, \{a\}, \{b\}, \{a, b\}\}。■$$

例 1.2.4 设 A 和 B 是集合,元素 $a \in A$,但 $a \notin B$,且 $A = B \cup \{a\}$,则

$$P(A) = P(B) \cup \{X \cup \{a\} \mid X \in P(B)\}。$$

证明: 令 $T = \{X \cup \{a\} \mid X \in P(B)\}$,也就是说,$T$ 是将 B 的每一个子集添加元素 a 之后得到的集合簇。

由于 $A = B \cup \{a\} \supseteq B$,所以 B 的任何子集也都是 A 的子集。由幂集的定义,显然有,$P(A) \supseteq P(B)$。同理,$P(A) \supseteq T$。所以

$$P(A) \supseteq P(B) \cup T。$$

反之,对于任意 $X \in P(A)$,由幂集的定义,X 是 A 的子集。若 $a \notin X$,则 $X \subseteq B$,X 是 B 的子集,从而 $X \in P(B)$;若 $a \in X$,则 $X = (X - \{a\}) \cup \{a\}$,且 $X - \{a\} \in P(B)$,从而 $X \in T$。总之,$X \in P(B) \cup T$。因此

$$P(A) \subseteq P(B) \cup T。$$

综上,由集合间包含关系的反对称性可知:

$$P(A) = P(B) \cup \{X \cup \{a\} \mid X \in P(B)\}。■$$

例 1.2.4 实际上提示了一种罗列出有限集合所有子集的方法(参见习题 17)。

1.2.3 n 元组和笛卡儿乘积

集合是由若干对象构成的一个整体，其中对象的顺序无关紧要，即使重新排列集合中的元素，只要集合中所包含的元素不变，作为整体的集合就保持不变。然而，在很多情况下，我们也确实需要考虑对象构成整体的顺序，仅变换个体对象的顺序就可能导致另一个新的整体。

在笛卡儿直角坐标系下，$(4, 2)$和$(2, 4)$表示平面上两个不同的点，所以平面上的笛卡儿坐标可表示为两个实数组成的序列，而不能表示为集合。类似地，英语单词可视为由若干个字母组成的序列，pin 和 nip 是两个不同的单词。

数学上，对象的序列表示为多元组。

定义 1.2.3 设 n 是自然数，则由 n 个对象组成的序列 $a_1a_2\cdots a_n$ 称为 **n 元组**，记为$(a_1, a_2, \cdots, a_n)$，其中，$a_i(1\leqslant i\leqslant n)$ 称为该 n 元组的第 i 个**坐标**。如果两个 n 元组对应的坐标均相同，那么称这两个 **n 元组相等**，即 $(a_1, a_2, \cdots, a_n)=(b_1, b_2, \cdots, b_n)$ 当且仅当 $a_i=b_i(1\leqslant i\leqslant n)$。

从定义可知，$(1, 2)\neq(1, 3)$，$(1, 2)\neq(1, 2, 3)$。

定义 1.2.4 设 n 是自然数，D_1、D_2、…、D_n 是 n 个集合，由 n 元组组成的集合$\{(d_1, d_2, \cdots, d_n)\mid$对任意$i(1\leqslant i\leqslant n)$, $d_i\in D_i\}$ 称为 D_1、D_2、…、D_n 的笛卡儿乘积，记为 $D_1\times D_2\times\cdots\times D_n$。

也就是说，从 n 个集合 D_1、D_2、…、D_n 中依次各取出一个元素构成n 元组，所有这样的 n 元组所组成的集合就是 D_1、D_2、…、D_n 的笛卡儿乘积。

特别地，$\underbrace{D\times D\times\cdots\times D}_{n个}$记为$D^n$。

例 1.2.5 若集合 $A=\{1, 2, 3\}$, $B=\{a, b\}$，则

$A\times B=\{(1, a), (2, a), (3, a), (1, b), (2, b), (3, b)\}$;
$B\times A=\{(a, 1), (a, 2), (a, 3), (b, 1), (b, 2), (b, 3)\}$;
$A^2=\{(1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (2, 3), (3, 1), (3, 2), (3, 3)\}$;
$B^2=\{(a, a), (a, b), (b, a), (b, b)\}$。■

例 1.2.6 $\mathbf{R}^2$ 表示笛卡儿平面，$\mathbf{Q}^2$ 表示笛卡儿平面上坐标是有理数的点组成的集合。■

*1.2.4 广义并和广义交

定义 1.2.5 设 A 是集合簇。

(1) 由所有 A 的元素中的元素所组成的集合称为集合簇 A 的**广义并**，记为$\bigcup A$，即

$$\bigcup A=\{x\mid 存在\ X\in A, 使\ x\in X\}。$$

(2) 由 A 中所有元素的共公元素所组成的集合称为集合簇 A 的**广义交**，记为$\bigcap A$，即

$$\bigcap A=\{x\mid 对任意\ X\in A, 有\ x\in X\}。$$

例 1.2.7 设集合簇 $A=\{\{1, 2\}, \{2, \{3\}\}, \{1, 2, \{\{3\}\}\}\}$，则有

$$\bigcup A=\{1, 2, \{3\}, \{\{3\}\}\},$$