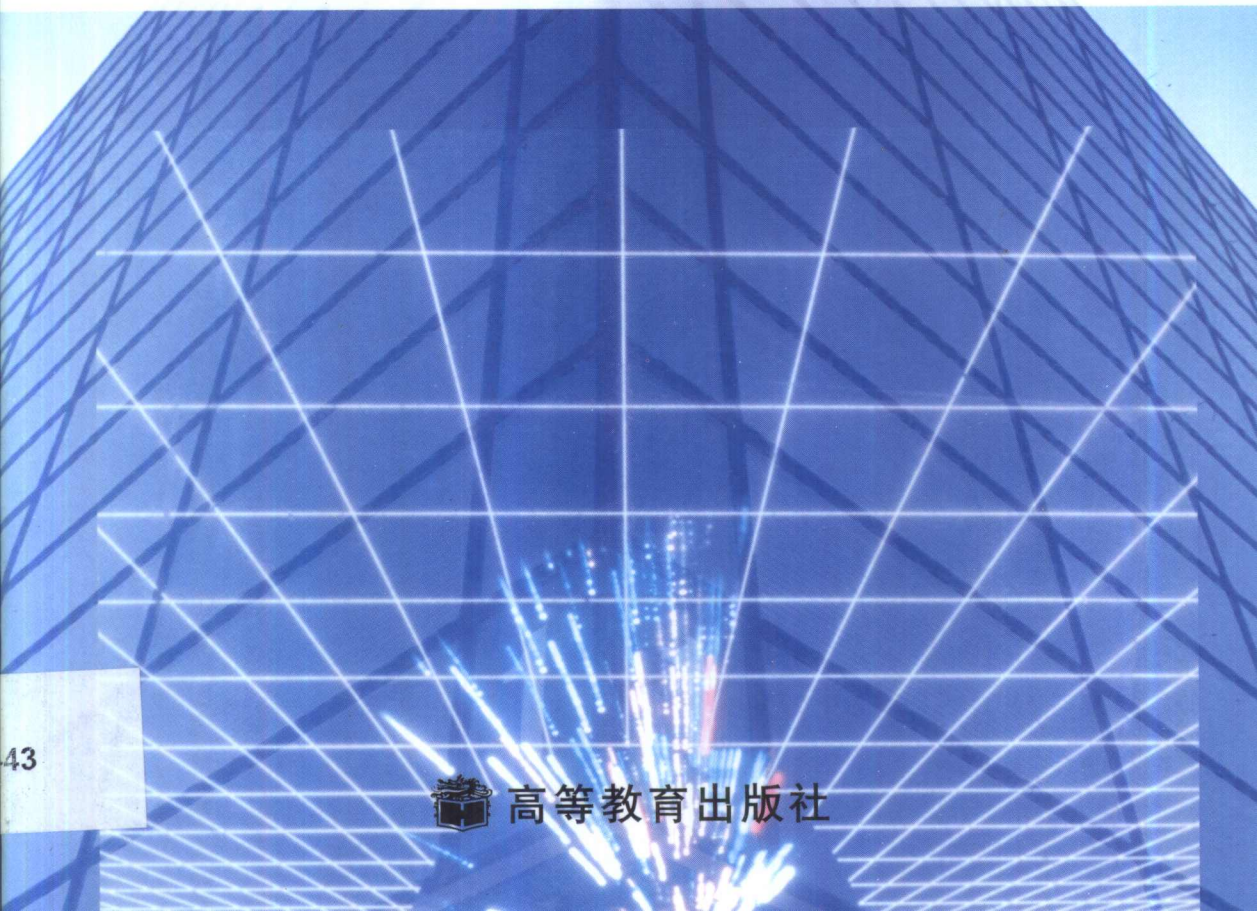
普通高等教育“十五”国家级规划教材

离散数学

孙吉贵　杨凤杰　欧阳丹彤　李占山



高等教育出版社

内容提要

本书是作者结合多年的教学实践，并参考了国内外多种同类教材编写而成的．为了更好地适应计算机学科发展的需要，增加了不少新知识、新内容以及演示性例子和应用实例．全书内容共分9章，主要包括：集合论基础、命题逻辑和谓词逻辑、图论与网络、数论基础、近世代数、格论与布尔代数基础知识以及计算机模型中语言、有限状态机和图灵机的内容．

本书可作为高等院校计算机及相关专业的教材，也可供从事计算机研究工作的人员参考．

图书在版编目（CIP）数据

离散数学/孙吉贵等．—北京：高等教育出版社，2002.8

教育部规划教材

ISBN 7-04-011248-5

Ⅰ.离… Ⅱ.孙… 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(2002)第048243号

离散数学

孙吉贵 杨凤杰 欧阳丹彤 李占山

出版发行	高等教育出版社	购书热线	010-64054588
社　　址	北京市东城区沙滩后街55号	免费咨询	800-810-0598
邮政编码	100009	网　　址	http://www.hep.edu.cn
传　　真	010-64014048		http://www.hep.com.cn
经　　销	新华书店北京发行所		
印　　刷	北京铭成印刷有限公司		
开　　本	787×960　1/16	版　　次	2002年8月第1版
印　　张	23.75	印　　次	2002年8月第1次印刷
字　　数	440 000	定　　价	27.30元

本书如有缺页、倒页、脱页等质量问题，请到所购图书销售部门联系调换．

前　言

离散数学是计算机科学与技术一级学科的核心课程，是整个计算机学科的专业基础课．目前，从总体看来国外离散数学教材深度和难度不及国内大部分离散数学教材，特别是国内重点计算机学科使用的教材．所以，在教育部吕福源副部长组织的第一次计算机学科英文原版教材引进讨论会上，与会者当时没有选出一本合适的离散数学原版教材．但国外教材中在离散数学应用方面阐述的内容多于国内教材．

离散数学在教给学生离散问题建模、数学理论、计算机求解方法和技术知识的同时，培养学生的数学抽象能力与严密的逻辑推理能力．通过本课程的学习，不仅使学生掌握进一步学习其他课程所必需的离散数学知识，而且可增强学生使用离散数学知识进行分析问题与解决实际问题的能力．

本次重新改编的《离散数学》是在三位恩师王湘浩院士、管纪文教授、刘叙华教授编写的《离散数学》（高等教育出版社 1983 年）的基础上，结合多年的教学实践，参考了国内外多种同名教材，对原教材内容进行了删改，添加了部分新知识与新内容，并增加了一定的演示性例子和应用实例，使之适应计算机学科发展的需要，希望能兼有国外教材与国内教材的优点．

作为评价一本好的教本的原则，我们十分赞同前辈闵嗣鹤先生所说的 3 个条件："第一是教材要选择得恰当，安排得自然；第二是说理要严格而清楚，深入浅出，也就是逻辑性与直观性要强；第三是要引人入胜，使人有'欲穷千里目，更上一层楼'之感，换句话说，问题的来源与发展都要交代清楚，使读者能从少许见多许，增加他们目前学习与今后钻研的兴趣"．对比这 3 个条件，我们的教材会有很多缺点．不过，我们参编人员结合多年的教学实践，在写作中还是朝着这个方向努力，力争使学习者在学习过程中能像欣赏丰美的食物那样，"品尝、咀嚼和消化"，过后还有"回味"之感．虽然我们做得很不够，也希望采用本书的教师能结合自己的经验和特长，随时弥补．

本书分为 9 章，主要内容为：

第一章介绍集合论基础知识，包括映射、关系、基数等知识．

第二章和第三章属于数理逻辑部分，主要介绍经典命题逻辑和谓词逻辑的基础知识．

第四章介绍图论与网络方面的基本知识，包括图与网络的数据结构，有向图与 Euler（欧拉）路，无向图与 Hamilton（哈密顿）路，平面图与二部图以

及网络优化算法.

第五章讨论数论基础知识，包括整除性、质因数分解、合同、一次同余式、二次同余式、数论在计算机通信安全中的应用.

第六章和第七章是抽象代数的群、环和域的基本内容，包括代数系统、半群与群、群的同构与同态、环的性质、环的同态与同构、域的特征、素域、多项式的整除性、多项式的根、有理域上的多项式、分圆多项式、有限域、计数问题和编码方法.

第八章介绍格论和布尔代数方面的基础知识，包括半序格与代数格、对偶原理、格的性质、格的同态与同构、有界格、有余格、分配格、模格、布尔代数的性质、有限布尔代数的表示理论、布尔代数的同态与同构、布尔表达式的化简问题（Quine 方法，Karnaugh 图方法），以及格与布尔代数在计算机科学中的应用.

第九章介绍了计算模型中 3 种类型的结构，即语法、有限状态机和图灵（Turing）机. 阐述了它们在语言识别方面的应用.

离散数学既是一门基础理论课程，又是一门与实际问题紧密相连的课程. 为此，本书强调基础理论，配有一定量的例题和习题，便于学生理解和掌握较抽象的理论和方法. 同时，吸收国外一些离散数学教材方面的经验，增加了可供学生应用的与本学科有关的实习题目，让学生感到学有所用，从而激发其学习兴趣，使学生获得尽可能好的学习效果.

为了便于教师讲授和学生学习，作为本书的补充，我们将在近期整理和编写配套的本教材的学习指导和较完整的习题解答，并将由高等教育出版社出版.

编 者

2002 年 3 月于吉林大学

目　录

第一章　集合论基础 …… 1
§1.1　集合的基本概念 …… 2
习题 1.1 …… 6
§1.2　关系 …… 7
1.2.1　关系的基本概念及其性质 …… 7
1.2.2　等价关系 …… 12
1.2.3　部分序关系 …… 16
习题 1.2 …… 18
§1.3　映射 …… 19
1.3.1　集合的基数 …… 20
1.3.2　可数集合 …… 21
1.3.3　不可数集合 …… 23
习题 1.3 …… 25
§1.4　集合在计算机科学中的应用 …… 25
1.4.1　关系在关系数据库中的应用 …… 25
1.4.2　关系代数与数据子语言 …… 30
1.4.3　等价关系在计算机中的应用 …… 32
1.4.4　序关系在项目管理中的应用 …… 33
第二章　命题逻辑 …… 35
§2.1　命题以及逻辑联结词 …… 36
2.1.1　命题 …… 36
2.1.2　逻辑联结词 …… 37
习题 2.1 …… 39
§2.2　命题公式 …… 39
2.2.1　公式 …… 39
2.2.2　解释 …… 40
习题 2.2 …… 41
§2.3　命题公式的等价关系和蕴涵关系 …… 42
2.3.1　公式的等价 …… 42
2.3.2　公式的蕴涵 …… 43
2.3.3　演绎 …… 44
2.3.4　公式蕴涵的证明方法 …… 46
习题 2.3 …… 47

§2.4 范式 …… 48
2.4.1 析取范式和合取范式 …… 48
2.4.2 主析取范式和主合取范式 …… 49
2.4.3 恒真恒假性的判定 …… 51
习题 2.4 …… 53
§2.5 命题逻辑在二值逻辑器件和语句逻辑中的应用 …… 53
第三章 谓词逻辑 …… 56
§3.1 谓词逻辑的基本概念 …… 56
3.1.1 谓词和量词 …… 56
3.1.2 改名规则 …… 58
习题 3.1 …… 59
§3.2 谓词公式 …… 60
3.2.1 公式 …… 60
3.2.2 解释 …… 60
习题 3.2 …… 62
§3.3 谓词公式的等价关系和蕴涵关系 …… 62
3.3.1 公式的等价和蕴涵 …… 62
3.3.2 谓词演算的推理理论 …… 64
习题 3.3 …… 66
§3.4 范式 …… 67
3.4.1 前束范式 …… 67
3.4.2 Skolem 范式 …… 68
习题 3.4 …… 70
§3.5 例 …… 71
习题 3.5 …… 74
§3.6 谓词逻辑的应用 …… 74
3.6.1 谓词逻辑与数据子语言 …… 74
3.6.2 谓词逻辑与逻辑程序设计语言 …… 76
第四章 图与网络 …… 84
§4.1 图 …… 85
4.1.1 图的基本概念 …… 85
4.1.2 权图 Dijkstra 算法 …… 89
习题 4.1 …… 92
§4.2 树 …… 93
4.2.1 树及其等价命题 …… 93
4.2.2 最优树 Kruskal 算法 …… 95
4.2.3 求最优树的其他算法 …… 97
习题 4.2 …… 99

§4.3　有向图　Euler路 …… 99
4.3.1　有向图与有向树 …… 100
4.3.2　Euler路　Euler图 …… 103
4.3.3　无向图　无向图中的Euler路 …… 107
习题4.3 …… 108
§4.4　Hamilton图 …… 109
4.4.1　Hamilton路　Hamilton图的必要条件 …… 110
4.4.2　Hamilton图的若干充分条件 …… 111
习题4.4 …… 117
§4.5　平面图 …… 117
4.5.1　平面图判定　Kuratowski判字准则 …… 117
4.5.2　平面图的Euler公式 …… 120
4.5.3　平面图的对偶图　Plato体 …… 122
4.5.4　平面图的着色 …… 124
习题4.5 …… 125
§4.6　匹配　二部图 …… 127
习题4.6 …… 132
§4.7　König无限性引理 …… 132
习题4.7 …… 135
§4.8　网络优化算法 …… 136
4.8.1　图与网络的数据结构 …… 136
4.8.2　单源最短路径问题具体算法及实现和比较 …… 139
4.8.3　最大流问题具体算法及实现和比较 …… 141
习题4.8 …… 152
第五章　数论基础 …… 153
§5.1　整除性　辗转相除 …… 154
5.1.1　整除及其性质 …… 154
5.1.2　辗转相除 …… 156
5.1.3　利用数的数码特征判别某些整除性 …… 159
习题5.1 …… 160
§5.2　互质　质因数分解 …… 161
5.2.1　整数互质 …… 161
5.2.2　质数与合数　算术基本定理 …… 163
习题5.2 …… 164
§5.3　合同　一次同余式 …… 166
5.3.1　合同及其性质 …… 166
5.3.2　剩余类　一次同余式 …… 168
习题5.3 …… 170

§5.4 秦九韶定理 Euler 函数 …… 171
5.4.1 一次同余式组 秦九韶定理 …… 171
5.4.2 一元高次同余式的化简 …… 173
5.4.3 剩余系遍历 Euler 函数 …… 174
习题 5.4 …… 177
§5.5 一元高次同余式 二次剩余 …… 178
5.5.1 一元高次同余式的解 …… 178
5.5.2 二次同余式 二次剩余 …… 181
5.5.3 二次剩余的判定 Legendre 符号 …… 182
习题 5.5 …… 185
§5.6 数论在计算机通信安全中的应用 …… 187
5.6.1 密码系统 …… 187
5.6.2 凯撒密码 …… 188
5.6.3 Vigenere 密码 …… 189
5.6.4 Hill 加密算法 …… 189
5.6.5 RSA 公钥系统 …… 190
习题 5.6 …… 192
第六章 群与环 …… 193
§6.1 代数系统 …… 194
习题 6.1 …… 196
§6.2 群的定义 …… 197
6.2.1 半群 …… 197
6.2.2 群 …… 198
6.2.3 群的性质 …… 199
习题 6.2 …… 201
§6.3 置换群 …… 202
6.3.1 置换的定义 …… 202
6.3.2 置换的轮换表法 …… 203
6.3.3 置换的顺向圈表示 …… 205
6.3.4 置换的奇偶性 …… 206
习题 6.3 …… 208
§6.4 子群及其陪集 …… 209
6.4.1 子群的定义 …… 209
6.4.2 子群的判别条件 …… 209
6.4.3 循环群 …… 210
6.4.4 陪集 …… 213
习题 6.4 …… 215
§6.5 同构及同态 …… 216

6.5.1 同态映射 …… 216
6.5.2 同构映射 …… 217
6.5.3 同态核 …… 219
习题 6.5 …… 221
§6.6 环 …… 222
6.6.1 环的定义 …… 222
6.6.2 环的性质 …… 223
习题 6.6 …… 227
§6.7 环同态 …… 228
6.7.1 理想 …… 228
6.7.2 环中合同关系 …… 229
6.7.3 环同态与同构 …… 230
6.7.4 单纯环与极大理想 …… 232
习题 6.7 …… 233
§6.8 群与环在计算机科学中的应用 …… 234
6.8.1 计数问题 …… 234
6.8.2 纠错码 …… 239
第七章 多项式 有限域 …… 250
§7.1 域的特征 素域 …… 250
7.1.1 域的特征 …… 250
7.1.2 素域 …… 251
习题 7.1 …… 253
§7.2 多项式的整除性 …… 253
习题 7.2 …… 258
§7.3 多项式的根 …… 258
习题 7.3 …… 262
§7.4 有理域上的多项式 …… 263
习题 7.4 …… 266
§7.5 分圆多项式 …… 267
7.5.1 复数域上的分圆多项式 …… 267
7.5.2 任意域上的分圆多项式 …… 271
习题 7.5 …… 273
§7.6 有限域 …… 274
习题 7.6 …… 277
§7.7 多项式编码方法及其实现 …… 277
习题 7.7 …… 281
第八章 格与布尔代数 …… 282
§8.1 引言 …… 282

§8.2 格的定义 …… 283
习题 8.2 …… 287
§8.3 格的性质 …… 287
8.3.1 对偶原理 …… 287
8.3.2 格的其他性质 …… 289
8.3.3 格的同态与同构 …… 291
习题 8.3 …… 294
§8.4 几种特殊的格 …… 295
8.4.1 有界格 …… 295
8.4.2 有余格 …… 296
8.4.3 分配格 …… 297
8.4.4 模格 …… 298
习题 8.4 …… 301
§8.5 布尔代数 …… 302
8.5.1 布尔代数的定义及其性质 …… 302
8.5.2 有限布尔代数的表示理论 …… 307
8.5.3 布尔代数的同态与同构 …… 311
习题 8.5 …… 313
§8.6 布尔表达式的化简问题 …… 314
习题 8.6 …… 325
§8.7 格与布尔代数在计算机科学中的应用 …… 326
8.7.1 开关电路函数 …… 326
8.7.2 逻辑门 …… 328
8.7.3 全加器的逻辑设计 …… 328
第九章 语言和有限状态机 …… 331
§9.1 语言和语法 …… 331
9.1.1 语法结构 …… 333
9.1.2 语法结构的类型 …… 335
9.1.3 演绎树 …… 336
9.1.4 Backus－Naur form …… 337
习题 9.1 …… 338
§9.2 带有输出的有限状态机 …… 339
习题 9.2 …… 344
§9.3 没有输出的有限状态机 …… 345
习题 9.3 …… 350
§9.4 语言识别 …… 350
9.4.1 正则集合 …… 350
9.4.2 KLEENE 定理 …… 352

9.4.3　其他几种类型的有限状态机 …… 358
习题 9.4 …… 358
§9.5　Turing 机 …… 360
习题 9.5 …… 365
参考文献 …… 367

第一章　集合论基础

20 世纪数学中最为深刻的活动，是关于数学基础的探讨．这不仅涉及到数学的本性，也涉及到演绎数学的正确性．数学中若干悖论的发现，引发了数学史上的第三次危机，这种悖论在将要讲到的集合论中尤为突出．集合论最初是一门研究数学基础的学科，它从一个比“数”更简单的概念——集合出发，定义数及其运算，进而发展到整个数学领域，在这方面它取得了极大的成功．

集合论的起源可以追溯到 19 世纪末期．1874 年，29 岁的德国数学家康托尔（Georg Cantor）在“数学杂志”上发表了关于无穷集合论的第一篇革命性文章，从 1874 至 1884 年间，Cantor 的系列有关集合的文章，奠定了集合论的基础．同时 Cantor 的思想也引起了当时权威数学家 Kronecker（克罗内克）的敌视，粗暴地攻击他的思想达十年之久．Poincare（庞加莱）也把集合论当作一个有趣的“病理学”，并预测：后一代人将把 Cantor 的集合论当作一种疾病，而人们已经从中恢复过来了．康托尔开创的集合论被称为朴素集合论，因为他没有对集合论做完整形式的刻画，从而导致了理论的不一致（产生了悖论）．在集合论的若干悖论中，最通俗易懂的是 Russell（罗素）的理发师悖论：一个乡村理发师，自夸本村无人可与相比，宣称他当然不给自己刮脸的人刮脸，但却给本村所有自己不刮脸的人刮脸．一天他发生了疑问，他是否应当给自己刮脸？但 Cantor 的工作为数学开辟了广泛的研究领域．他所提出的问题及其解决过程至少影响了数学半个世纪的发展，如连续统假设．1930 年，Godel（哥德尔）给出了连续统假设与选择公理是相容的，从而证明了连续统假设不会错．1963 年，Cohen（科恩）证明了选择公理与连续统假设是相互独立的，从而给出了：证明连续统假设成立是不可能的．由此得到，在使用的公理系统中，连续统假设是不能判定的．19 世纪末到 20 世纪初，数学各个分支的一个普遍的思潮就是建立公理化系统．为了弥补 Cantor 集合论的不足，德国数学家 Ernst Zermelo（策梅洛）承担了集合论的公理化任务，建立了形式集合论．Zermelo 相信悖论起因于 Cantor 对集合的概念未加以限制，所以他所建立的公理系统只包含公理本身叙述所定义的基本概念和关系，并把选择公理作为其中的一条公理．然而此公理化集合论的相容性当时并没有证明．关于这一相容性问题，Poincare 评论说：为了防备狼，羊群已经用篱笆圈起来了，但却不知道羊圈内有没有狼．

集合论既然有这么多的欠缺和不足，为什么还仍然把它作为数学的基础

呢？早在集合论刚建立不久的 1897 年，在苏黎世举行的第一次国际数学家大会上，Hurwitz（胡尔维茨）与 Hadamard（阿达马）就指出了超限数理论在分析中的重要应用，进一步的应用不久就在测度论和拓扑学方面开展起来．目前已经知道，整个分析数学是建立在集合论的基础上的，集合论的概念已深入到现代科学的各个方面，成为表达各种严谨科学概念的必不可少的数学语言．Hilbert（希尔伯特）在 1926 年曾说到："没有人能把我们从 Cantor 为我们创造的乐园中开除出去"，称 Cantor 的超限算术为"数学思想的最惊人的产物，在纯粹理性的范畴中人类活动的最美观的表现之一"．Russell 把 Cantor 的工作描述为"可能是这个时代所能夸耀的最巨大的工作"．

我们这里学习集合论，更是因为计算机科学及其应用的研究也和集合论有着极其密切的关系．集合不仅可以用来表示数及其运算，更可以用于非数值信息的表示和处理．如数据的增加、删除、修改、排序，以及数据间关系的描述，有些很难用传统的数值计算来处理，但可以用集合运算来处理．因此集合论在程序语言、数据结构、编译原理、数据库与知识库、形式语言和人工智能等领域中都得到了广泛的应用，并且还得到了发展，如 Zadeh（扎德）的模糊集理论和 Pawlak 的粗糙集理论．本章对集合论本身及其公理化系统不作深入探讨，主要是介绍有关集合论的基础知识．在讲授上力求直观易懂，而非严格的形式化．若想深入学习，请阅读集合论方面著作．

§1.1 集合的基本概念

集合是数学中最基本的概念．既然是最基本的概念，它就不那么好定义，一般只是说明，正像数学中"点"那样．最基本的东西就是大家都知道的东西．要说明什么是集合，有多种描述方法："所要讨论的一类对象的整体"；"具有同一性质单元的集体"等．当我们讨论某一类对象的时候，就把这一类对象的整体称为集合．而集合中的对象就称为该集合中的元素．

Cantor 是这样描述集合的：所谓集合，是指我们无意中或思想中将一些确定的，彼此完全不同的客体的总和而考虑为一个整体．这些客体叫做该集合的元素．

设 A 是一个集合，a 是集合 A 中的元素，今后将这一事实记为 $a \in A$，读做 a 属于 A；若 a 不是集合 A 中的元素，则记为 $a \notin A$，读做 a 不属于 A．

例如，这间教室里所有桌子的整体就构成一个桌子集合．每个桌子都属于这个集合，每个椅子都不属于这个集合．

又如，世界上所有哺乳动物的整体构成一个哺乳动物集合．每一条狗每一只猫都属于这个集合，而每一只鸡都不属于这个集合．

又如，平面上的所有点的整体构成平面点集；所有连续函数的整体构成连续函数集等.

有限个元素 a_1，…，a_n 构成的集合，称为有穷集（有限集），记为 $\{a_1, \cdots, a_n\}$；无限个元素构成的集合，称为无穷集. 有穷集中元素的个数称为该集合的元素数，记为 $|A|$.

特别，不含元素的集合称为空集，记为 $\varnothing$，一个元素 a 构成的集合，记为 $\{a\}$.

定义 1.1.1 当 A，B 两个集合的元素完全一样，即 A，B 两个集合实际上是同一集合时，则称集合 A，B 相等，记为 $A=B$.

定义 1.1.2 设 A，B 是两个集合. 若 A 的元素都是 B 的元素，则称 B 包含 A，或称 A 是 B 的子集，记为 $A\subseteq B$. 若 $A\subseteq B$，且 $A\neq B$，则称 A 是 B 的真子集，记为 $A\subset B$.

例如，所有狗构成的狗的集合就是哺乳动物集合的真子集.

显然，空集是任何集合的子集且空集惟一.

当我们所讨论的集合都是某一集合的子集时，这个集合就称为全集，记为 E.

由定义，下面的结论是显然的：对于任意两个集合 A 和 B，$A=B$ 的充要条件是 $A\subseteq B$ 且 $B\subseteq A$. 这一结论是证明两个集合相等时最常用的方法.

定义 1.1.3 设 A 是集合，A 的所有子集为元素构成的集合称为 A 的幂集，记为 $\rho(A)$ 或 2^A.

显然，若 A 为有穷集，元素数为 n，则 2^A 的元素数为

$$C_n^0+C_n^1+\cdots+C_n^n=2^n.$$

幂集具有以下性质：

(1) 设 A，B 是两个集合，$A\subseteq B$ 当且仅当 $\rho(A)\subseteq\rho(B)$；

(2) $x\in\rho(A)$ 当且仅当 $x\subseteq A$.

定义 1.1.4 设 C 是一个集合. 若 C 的元素都是集合，则称 C 为集合族. 若集合族 C 可表示为 $C=\{S_d\mid d\in D\}$，则称 D 为集合族 C 的标志（索引）集.

显然，2^A 是一个集合族. 设 A_1，A_2，A_3，…，是集合的序列，且两两之间互不相同，则集合 $\{A_1, A_2, A_3, \cdots\}$ 是一个集合族，可表示为 $\{A_i\mid i\in\mathbf{N}_+\}$，其中 $\mathbf{N}$ 是自然数集合（除去 0），是该集合的标志集合.

定义 1.1.5 设 A，B 是两个集合. 属于集合 A 而不属于集合 B 的所有元素组成的集合，称为 A 与 B 的差集，记为 $A-B$，或 $A\setminus B$.

例如，令 $A=\{a,b,c,d\}$，$B=\{b,c,e,f\}$，于是 $A-B=\{a,d\}$，$B-A=\{e,f\}$.

定义 1.1.6　设 A，B 是两个集合. 所有属于 A 或者属于 B 的元素构成的集合，称为 A 和 B 的并集，记为 $A\cup B$.

例如，令 $A=\{a,b,c,d\}$，$B=\{b,d,e,f\}$，于是 $A\cup B=\{a,b,c,d,e,f\}$.

可以把定义 1.1.6 推广到多个集合的并集.

定义 1.1.7　设 A，B 是两个集合. 由属于 A 又属于 B 的元素构成的集合，称为 A 和 B 的交集，记为 $A\cap B$.

例如，上面集合 A 和 B 的 $A\cap B=\{b,d\}$.

同样，可以把定义 1.1.7 推广到多个集合的交集.

定义 1.1.8　设 A,B 是两个集合，所有序偶 (x,y) 构成的集合（其中 $x\in A,y\in B$），称为 A,B 的直乘积（笛卡儿积），记为 $A\times B$.

直乘积符号表示为 $A\times B=\{(x,y)\mid x\in A \text{ 且 } y\in B\}$.

例如，令 A 是直角坐标系中 x 轴上的点集，B 是 y 轴上的点集，于是 $A\times B$ 就和平面点集一一对应.

由排列组合的基本常识不难证明，如果集合 A 的元数 $|A|=m$，集合 B 的元数 $|B|=n$，则 $A\times B$ 中有 mn 个元素.

直乘积运算有以下性质：

(1) 对任意集合 A，根据定义有 $A\times\varnothing=\varnothing$，$\varnothing\times A=\varnothing$；

(2) 一般地说，直乘积运算不满足交换律，即 $A\times B\neq B\times A$（当 $A\neq\varnothing$，$B\neq\varnothing$ 且 $A\neq B$ 时）；

(3) 直乘积运算不满足结合律，即 $(A\times B)\times C\neq A\times(B\times C)$（当 $A\neq\varnothing,B\neq\varnothing$ 且 $C\neq\varnothing$ 时）；

(4) 直乘积运算对并和交运算满足分配律，即

$A\times(B\cup C)=(A\times B)\cup(A\times C)$，　$(B\cup C)\times A=(B\times A)\cup(C\times A)$，

$A\times(B\cap C)=(A\times B)\cap(A\times C)$，　$(B\cap C)\times A=(B\times A)\cap(C\times A)$；

(5) 设 A，B，C，D 是集合，则有：

若 $A\subseteq C$ 且 $B\subseteq D$，则 $A\times B\subseteq C\times D$.

定理 1.1.1　设 A_1，A_2，…，A_n 是 n 个集合，则

$$\left|\bigcup_{i=1}^{n}A_i\right|=\sum_{i=1}^{n}|A_i|-\sum_{i<j}|A_i\cap A_j|+\sum_{i<j<k}|A_i\cap A_j\cap A_k|+\cdots$$
$$+(-1)^{n-1}|A_1\cap A_2\cap\cdots\cap A_n|$$

称为包含排斥原理，简称容斥原理.

定义 1.1.9　设 A 是一个集合，全集 E 与 A 的差集称为 A 的余集或补集，记为 $\sim A$（或用 $\overline{A}$，但不是国家标准）.

例如，令 $E=\{a,b,c,d,e,f\}$，$A=\{b,c\}$，于是 $\sim A=\{a,d,e,f\}$.

定义 1.1.10　设 A,B 是两个集合. 则 A 与 B 的环和（对称差）定义为 $A\oplus$

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

A 与 B 的对称差还有一个等价的定义，即 $A\oplus B=(A\cup B)-(A\cap B)$.

定义 1.1.11 设 A,B 是两个集合，则 A 与 B 的环积定义为 $A\otimes B=\complement(A\oplus B)$.

不难证明，对于任意集合 A,B,C 有如下算律：

1. $A\cap A=A, A\cup A=A$. （等幂律）
2. $A\cap B=B\cap A, A\cup B=B\cup A$. （交换律）
3. $(A\cap B)\cap C=A\cap(B\cap C)$,
   $(A\cup B)\cup C=A\cup(B\cup C)$. （结合律）
4. $A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$,
   $A\cup(B\cap C)=(A\cup B)\cap(A\cup C)$. （分配律）
5. $A\cap(A\cup B)=A, A\cup(A\cap B)=A$. （吸收律）
6. $A\cap\complement A=\varnothing, A\cup\complement A=E, \complement\complement A=A$.
7. $\complement(A\cap B)=\complement A\cup\complement B$,
   $\complement(A\cup B)=\complement A\cap\complement B$. （De Morgan 律）
8. $E\cap A=A, E\cup A=E$.
9. $\varnothing\cap A=\varnothing, \varnothing\cup A=A$.

例 1.1.1 证明：$A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$.

证明 任取 $a\in A\cap(B\cup C)$，即 $a\in A$ 并且 $a\in B\cup C$，亦即 $a\in A$ 并且 $a\in B$ 或 $a\in C$. 于是 $a\in A\cap B$ 或者 $a\in A\cap C$，故 $a\in(A\cap B)\cup(A\cap C)$. 即证得 $A\cap(B\cup C)\subseteq(A\cap B)\cup(A\cap C)$.

任取 $a\in(A\cap B)\cup(A\cap C)$，即 $a\in A\cap B$ 或者 $a\in A\cap C$，亦即 $a\in A$ 并且 $a\in B$，或者 $a\in A$ 并且 $a\in C$，总之，$a\in A$，且 $a\in B$ 或者 $a\in C$，即 $a\in A$ 且 $a\in B\cup C$，故 $a\in A\cap(B\cup C)$，即证得 $(A\cap B)\cup(A\cap C)\subseteq A\cap(B\cup C)$. 综上可得 $A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$.

例 1.1.2 证明：$\complement(A\cup B)=\complement A\cap\complement B$.

证明 任取 $a\in\complement(A\cup B)$，即 $a\notin A\cup B$，亦即 $a\notin A$ 且 $a\notin B$，于是 $a\in\complement A$ 且 $a\in\complement B$，故 $a\in\complement A\cap\complement B$，即证得了 $\complement(A\cup B)\subseteq\complement A\cap\complement B$.

另一方面，任取 $a\in\complement A\cap\complement B$，即 $a\in\complement A$ 且 $a\in\complement B$，亦即 $a\notin A$ 且 $a\notin B$，于是 $a\notin A\cup B$，故 $a\in\complement(A\cup B)$，这就证得了 $\complement A\cap\complement B\subseteq\complement(A\cup B)$. 总之，我们证得了 $\complement(A\cup B)=\complement A\cap\complement B$.

现在我们利用这一结果证明 $\complement(A\cap B)=\complement A\cup\complement B$.

由上面的结果我们知道 $\complement(\complement A\cup\complement B)=\complement\complement A\cap\complement\complement B=A\cap B$，这样，$\complement[\complement(\complement A\cup\complement B)]=\complement(A\cap B)$，因为 $\complement[\complement(\complement A\cup\complement B)]=\complement A\cup\complement B$，也就是 $\complement(A\cap B)=\complement A\cup\complement B$.

一个集合 S 实际上就确定了一个性质 P，例如，规定性质 P 如下：若 $x\in S$，则称 x 有性质 P；否则，x 无性质 P.

反之，一个性质 P 实际上也确定了一个集合 S. 例如，令集合 S 由所有具有性质 P 的元素组成，因此，集合 S 可以用如下方式表示：

$$S=\{x\mid x \text{ 具有性质 } P\}.$$

例如，在直角坐标系中，以坐标原点为心的单位圆圆周上所有点构成的集合 S 可表示如下，

$$S=\{(x,y)\mid x^2+y^2=1\}.$$

又如，设 A，B 是两个集合，A 和 B 的交集可表示如下：

$$A\cap B=\{x\mid x\in A \text{ 并且 } x\in B\}.$$

集合的表示方法主要有 5 种：

1. 上面表示集合的方法 $S=\{x\mid x \text{ 具有性质 } P\}$，称为属性表示法，或称描述法.

2. 列举法，表示一个集合 A 时，将 A 中元素一一列举，或列出足够多的元素以反映 A 中成员的特征，例如：

$$A=\{a_1,a_2,\cdots,a_n\} \quad 或 \quad A=\{a_1,a_2,a_3,\cdots\}.$$

3. 递归指定集合，通过计算规则定义集合中的元素，例如：

设 $a_0=1,a_1=1,a_{n+1}=a_n+a_{n-1}$，于是 $A=\{a_0,a_1,a_2,\cdots\}=\{a_k\mid k\geqslant 0\}$.

4. 巴科斯范式 BNF 表示法

BNF 常常用来定义高级程序设计语言的标识符或表达式集合.

5. 文氏图法（John Venn），首先画一个大矩形表示全集，其次在矩形内画一些圆，用圆的内部表示集合，集合之间的相互关系和有关的运算可以用文氏图给予形象的描述. 一般情况下，表示集合的圆应该是相交的. 如果已知某两个集合是不相交的，则表示它们的圆就彼此相离.

习 题 1.1

1. 设 $S=\{2,a,\{3\},4\}$，$R=\{\{a\},3,4,1\}$ 指出下列写法哪些是对的？哪些是错的？

$\{a\}\in S,\{a\}\in R,\{a,4,\{3\}\}\subseteq S,\{\{a\},1,3,4\}\subset R,R=S,\{a\}\subseteq S,\{a\}\subseteq R,\varnothing\subseteq R,\varnothing\subseteq\{\{a\}\}\subseteq R\subseteq E,\{\varnothing\}\subseteq S,\varnothing\in R,\varnothing\subseteq\{\{3\},4\}$.

2. 写出下列集合的幂集合

$\{a,\{b\}\}$，$\{1,\varnothing\}$，$\{a,b,c\}$.

3. 对任意集合 A，B 证明：

(1) $A\subseteq B$ 当且仅当 $\rho(A)\subseteq\rho(B)$；