

# 近世代数

# 及其应用

(第二版)

阮传概 孙伟 编著



北京邮电大学出版社  
[www.buptpress.com](http://www.buptpress.com)

# 近世代数及其应用

(第二版)

阮传概 孙伟 编著

北京邮电大学出版社

·北京·

## 内 容 提 要

本书介绍了集合与映射、格、布尔代数、半群、群、环、有限域的基本内容和它们在逻辑电路与编码理论中的一些应用,以及与上述内容有关的一些多项式和线性同余式等知识。全书比较注重应用,条理清晰,论证详细,例题较多,每章末均附有习题。为了便于自学与参考,在本书的最后附有习题解答。

本书可作为通信理论、计算机科学、系统工程等有关专业的近世代数课程的教材,也可供从事工科有关各专业以及应用数学、应用物理等科技人员参考。

## 图书在版编目(CIP)数据

近世代数及其应用/阮传概,孙伟编著. 2版. —北京:北京邮电大学出版社,2001.8

ISBN 7-5635-0533-4

I. 近... II. ①阮...②孙... III. 抽象代数 IV. O153

中国版本图书馆 CIP 数据核字(2001)第 045092 号

- 
- 书 名: 近世代数及其应用(第二版)  
编 著: 阮传概 孙伟  
责任编辑: 徐凤琨  
出 版 者: 北京邮电大学出版社(北京市海淀区西土城路 10 号)  
邮 编: 100876 电 话: 62282185 62283578  
网 址: <http://www.buptpress.com>  
经 销: 各地新华书店  
印 刷: 北京源海印刷厂  
印 数: 1—3 000  
开 本: 850 mm×1 168 mm 1/32 印张: 13.625 字数: 351 千字  
版 次: 2001 年 9 月第 1 版 2001 年 9 月第 1 次印刷
- 

ISBN: 7-5635-0533-4/O·30

定价: 25.00 元

## 再版前言

近世代数的内容,不但在数学的各分支有很多应用,而且随着科学技术的发展,它在通信理论、计算机科学、系统工程等许多领域中也有广泛的应用。本书是为上述各专业的工科学生编写的,所以比较注重应用,例题较多,出版后受到读者的欢迎。这次再版时,根据读者的意见与建议,做了修改与补充。为了便于自学,增加了习题解答,可供读者做完习题后,作为参考。习题解答中的证明方法也不一定是唯一的,读者还可以想出更好的证明方法。

本书可作为通信理论、计算机科学、系统工程等有关专业的本科高年级学生或研究生的近世代数课程的教材,也可供从事工科各专业、应用数学、应用物理等科技人员参考。

我们向所有关心与支持本书的老师与读者表示衷心的感谢。在编写过程中,得到了北京邮电大学信息工程学院信息与计算中心的全体老师的支持与帮助,在此表示衷心的感谢。

这次再版一定还有不妥之处,殷切希望读者指出。

作 者

2001年5月

# 目 录

再版前言	1
第 1 章 集合与映射	1
§ 1-1 集合的概念	1
§ 1-2 集合的运算 集合元素的个数	3
§ 1-3 关系与等价关系	12
§ 1-4 映射 映射的计数 代数运算	17
§ 1-5 同态与同构	23
习题 1	29
第 2 章 格	33
§ 2-1 偏序集	33
§ 2-2 格的概念	36
§ 2-3 有补格与分配格	46
§ 2-4 模 格	51
习题 2	60
第 3 章 布尔代数与开关函数	65
§ 3-1 布尔代数的概念	65
§ 3-2 布尔代数的原子表示	73
§ 3-3 布尔表达式与布尔函数	77
§ 3-4 布尔函数的析取范式与极小乘积和	81
§ 3-5 素蕴涵 一致法	85
§ 3-6 开关函数	90
§ 3-7 逻辑门	98

习题 3 .....	103
<b>第 4 章 半群与群</b> .....	108
§ 4-1 半群与含幺半群 .....	108
§ 4-2 群的定义及其性质 .....	113
§ 4-3 子群 群同态 .....	120
§ 4-4 循环群 .....	126
§ 4-5 变换群与置换群 .....	131
习题 4 .....	142
<b>第 5 章 正规子群与商群</b> .....	146
§ 5-1 陪集 拉格朗日定理 .....	146
§ 5-2 正规子群 商群 .....	150
§ 5-3 群同态基本定理 .....	157
§ 5-4 群的直积 低阶群的构造 .....	162
§ 5-5 群对集合的作用 .....	169
习题 5 .....	177
<b>第 6 章 群码</b> .....	182
§ 6-1 数字通信与编码 .....	182
§ 6-2 线性码的生成矩阵与校验矩阵 .....	186
§ 6-3 群码 .....	192
习题 6 .....	197
<b>第 7 章 环</b> .....	200
§ 7-1 环的定义及其性质 .....	200
§ 7-2 整环 除环 布尔环 .....	205
§ 7-3 子环 环同态 .....	211
§ 7-4 由已知环构造新的环 .....	214
§ 7-5 分式域 .....	221
习题 7 .....	225
<b>第 8 章 商环与欧氏环</b> .....	229

§ 8-1 商环 环同态基本定理 .....	229
§ 8-2 素理想与极大理想 .....	235
§ 8-3 唯一分解环与主理想环 .....	237
§ 8-4 欧氏环 .....	243
§ 8-5 域上的既约多项式 .....	251
§ 8-6 线性同余式与孙子定理 .....	258
习题 8 .....	269
<b>第 9 章 有限域</b> .....	274
§ 9-1 扩域 .....	274
§ 9-2 极小多项式 多项式的分裂域 .....	280
§ 9-3 域的特征 有限域的构造 .....	284
§ 9-4 本原元与本原多项式 .....	292
§ 9-5 有限域上既约多项式的个数 .....	296
§ 9-6 循环码 .....	300
§ 9-7 有限域中的计算与伽罗瓦环 .....	305
习题 9 .....	309
<b>附录</b> .....	312
I 习题解答 .....	312
II 所用符号 .....	423
<b>参考文献</b> .....	426

# 第 1 章 集合与映射

近世代数的研究对象,主要是代数系统,即具有  $n$  元运算的集合.作为预备知识,在这章中,我们讨论数学中最基本的概念——集合与映射.

## § 1-1 集合的概念

集合的概念是数学中最基本的概念之一,是现代数学的重要基础,并且已深入到各种科学与技术的领域中.集合就是一些不同对象的总体.集合也简称集,通常用大写的英文字母  $A, B, C, D, \dots$  表示.例如,全体中国人是一个集合;所有整数也是一个集合,简称整数集,记为  $\mathbf{Z}$ .以后我们把所有有理数所组成的集合,简称有理数集,记为  $\mathbf{Q}$ ;把所有实数所组成的集合和所有复数所组成的集合分别记为  $\mathbf{R}, \mathbf{C}$ .组成一个集合的对象称为这个集合的元素,通常用小写的英文字母  $a, b, c, d, \dots$  表示.如果  $a$  是集  $A$  的元素,称为  $a$  属于  $A$ ,或  $A$  包含  $a$ ,记为  $a \in A$ ;如果  $a$  不是集合  $A$  的元素,称为  $a$  不属于  $A$ ,记为  $a \notin A$ .确定一个集合  $A$ ,就是要确定,哪些元素属于  $A$ ,哪些元素不属于  $A$ .

如果两个集合  $A, B$  包含的元素完全一样,则称  $A$  和  $B$  相等,记为  $A = B$ .

集合的表示方法主要有两种:列举法和构造法.所谓列举法,就是列出集合的元素.例如  $A = \{a, b, c, d, e\}$  是表示集合  $A$  由元素  $a, b, c, d, e$  组成.所谓构造法,就是描述出集合中元素适合的



条件. 例如,  $A = \{x | x \in \mathbf{Z}, x > 0\}$  表示集合  $A$  是由所有正整数组成.

**例 1-1-1**  $A = \{x | x \in \mathbf{Z}, x^2 - 3x + 2 = 0\}$ , 表示  $A$  的元素只有两个, 即  $x^2 - 3x + 2 = 0$  的两个根  $x = 1, x = 2$ .  $A = \{x | x \in \mathbf{Z}, x^2 - 3x + 2 = 0\} = \{1, 2\}$ .

设有两个集合  $A, B$ , 如果  $A$  的每个元素也是  $B$  的元素, 则称  $A$  为  $B$  的子集, 或称  $B$  包含  $A$ , 记为  $A \subseteq B$ . 如果  $A$  不是  $B$  的子集, 则记为  $A \not\subseteq B$ . 例如,  $A = \{a, b, c\}$  是  $B = \{a, b, c, d\}$  的子集, 集合  $A$  是自己的子集. 如果  $A \subseteq B$  并且  $A \neq B$ , 则称  $A$  是  $B$  的真子集, 记为  $A \subset B$ . 显然,  $A = B$  当且仅当  $A \subseteq B$  并且  $B \subseteq A$ . 我们把没有元素的集合称为空集, 记为  $\emptyset$ ; 只有一个元素的集合称为单点集. 例如,  $A = \{x | x \in \mathbf{Q}, x^2 = -1\}$  是空集;  $A = \{x | x = 3\} = \{3\}$  是单点集. 我们规定: 空集是任何集的子集.

如果一个集合包含了所要讨论的每一个集合, 则称这个集合为全集, 记为  $U$ . 例如, 在人口研究中, 全集就是包含全世界所有人的集合. 在研究平面上的点中, 全集就是包含平面上的所有点的集合.

**定义 1-1-1** 设  $A$  是给定的一个集合,  $A$  的所有子集构成的集合, 称为  $A$  的幂集, 记为  $P(A)$  或  $2^A$ , 即

$$P(A) = \{x | x \subseteq A\}.$$

**例 1-1-2** 设  $A = \{a, b\}$ , 则

$$P(A) = \{\emptyset, \{a\}, \{b\}, A\}.$$

**例 1-1-3** 设  $A = \{a, b, c\}$ , 则

$$P(A) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, A\}.$$

从上面例子可以看出: 2 个元素的集合的幂集有  $4 = 2^2$  个元素, 3 个元素的集合的幂集有  $8 = 2^3$  个元素. 可以推出:  $n$  个元素的集合的幂集有  $2^n$  个元素 (见习题 1-11).

## § 1-2 集合的运算 集合元素的个数

集合的运算就是以给定集合为对象,按照确定的规则,产生另外一些集合.例如, $A$ 表示“上数学课的学生集合”; $B$ 表示“上物理课的学生集合”.如果这两门课安排在同一时间进行期末考试,那么参加这两门课考试发生冲突的学生集合是什么?显然,该集合是同时上这两门课的学生的集合.如果在上数学课时和上物理课时分别宣布同一通知,那么知道这个消息的学生集合是什么?显然,这个集合是由上数学课或上物理课的学生组成.为了使这些概念一般化,我们定义集合的运算.

**定义 1-2-1** 设  $A, B$  是全集  $U$  的子集,由  $A$  和  $B$  的所有共同元素构成的集,称为  $A$  和  $B$  的交集,记为  $A \cap B$ ,即

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

两个集合的交可用所谓文氏图表示,见图 1-2-1,其中阴影部分就是  $A \cap B$ .

**例 1-2-1** 设  $A = \{a, b, c, d\}$ ,  $B = \{a, b, c, e, f\}$ , 则  $A \cap B = \{a, b, c\}$ .

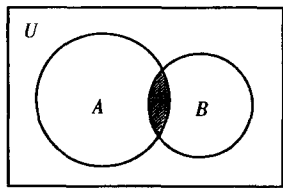


图 1-2-1

**定理 1-2-1** 集合的交运算满足下面性质,这里  $A, B, C$  是全集  $U$  的子集,  $\emptyset$  是空集.

- (1)  $A \cap A = A$ ;
- (2)  $A \cap \emptyset = \emptyset$ ;
- (3)  $A \cap U = A$ ;
- (4)  $A \cap B = B \cap A$ ;
- (5)  $A \cap (B \cap C) = (A \cap B) \cap C$ .

下面证明(5).

**证**  $(A \cap B) \cap C = \{x \mid x \in (A \cap B) \text{ 并且 } x \in C\} = \{x \mid (x \in A \text{ 并$

且  $x \in B$  并且  $x \in C$  } = {  $x | x \in A$  并且 (  $x \in B$  并且  $x \in C$  ) } = {  $x | x \in A$  并且  $x \in (B \cap C)$  } = {  $x | x \in A \cap (B \cap C)$  } =  $A \cap (B \cap C)$ .  $\square$

如果集合  $A, B$  没有共同的元素, 则称  $A, B$  不相交, 记为  $A \cap B = \emptyset$ .

**定义 1-2-2** 设  $A, B$  是全集  $U$  的子集, 所有属于  $A$  或属于  $B$  的元素构成的集, 称为  $A$  和  $B$  的并集, 记为  $A \cup B$ , 即

$$A \cup B = \{x | x \in U, x \in A \text{ 或 } x \in B\}.$$

两个集的并集的文氏图为图 1-2-2.

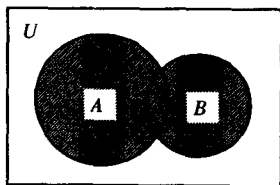


图 1-2-2

**例 1-2-2** 设  $A = \{a, b, c\}$ ,  $B = \{b, c, d, e\}$ , 则

$$A \cup B = \{a, b, c, d, e\}.$$

**定理 1-2-2** 集合的并运算满足下面性质, 这里  $A, B, C$  是全集  $U$  的子集,  $\emptyset$  是空集.

- |   |                             |
|---|-----------------------------|
| (1) $A \cup A = A$ ;                          | (2) $A \cup U = U$ ;        |
| (3) $A \cup \emptyset = A$ ;                  | (4) $A \cup B = B \cup A$ ; |
| (5) $A \cup (B \cap C) = (A \cup B) \cup C$ . |                             |

**证** 这些性质的证明, 容易从定义得出.  $\square$

**定理 1-2-3** 集合的交、并运算满足下面性质, 这里  $A, B, C$  是全集  $U$  的子集.

- |  |       |
|--|-------|
| (1) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ ;                   | (分配律) |
| (2) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ ;                   |       |
| (3) $A \cup (A \cap B) = A$ ;  | (吸收律) |
| (4) $A \cap (A \cup B) = A$ ;  |       |
| (5) 若 $A \subseteq C$ , 则 $A \cup (B \cap C) = (A \cup B) \cap C$ . (模律) |       |

下面证明(5).

**证** 设  $x \in A \cup (B \cap C)$ , 则  $x \in A$  或  $x \in B \cap C$ . 当  $x \in A$  时,  $x$

$\in A \cup B$ . 又因为  $A \subseteq C$ , 故  $x \in C$ , 即  $x \in (A \cup B) \cap C$ ; 当  $x \in (B \cap C)$  时, 则  $x \in A \cup B$  并且  $x \in C$ , 即  $x \in (A \cup B) \cap C$ . 因此,  $A \cup (B \cap C) \subseteq (A \cup B) \cap C$ ; 反之, 设  $x \in (A \cup B) \cap C$ , 则  $x \in (A \cup B)$  并且  $x \in C$ . 若  $x \in A$ , 则  $x \in A \cup (B \cap C)$ ; 若  $x \in B$ , 则  $x \in B \cap C$ , 从而  $x \in A \cup (B \cap C)$ . 于是  $A \cup (B \cap C) \supseteq (A \cup B) \cap C$ . 因此, 在  $A \subseteq C$  的条件下, 有

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

集合的交与并的概念还可以推广到全集  $U$  的任意多个集合上去.

**定义 1-2-3** 设  $A, B$  是全集  $U$  的子集, 所有属于  $A$  而不属于  $B$  的一切元素构成的集, 称为  $B$  关于  $A$  的余集或补集, 记为  $A - B$ , 即

$$A - B = \{x \mid x \in U, x \in A \text{ 并且 } x \notin B\}.$$

$A - B$  也称为集合  $A$  和  $B$  的差, 文氏图为图 1-2-3.

**例 1-2-3** 设  $A$  表示“上数学课的学生集合”,  $B$  表示“这门课考试及格的学生集合”, 则  $A - B$  表示“上数学课的学生中考试不及格的学生集合”.

**例 1-2-4** 设  $A$  是素数集合,  $B$  是奇数集合, 则  $A - B = \{2\}$ .

**例 1-2-5** 设  $A = \{a, b, c, d\}$ ,  $B = \{a, e\}$ , 则  $A - B = \{b, c, d\}$ ,  $B - A = \{e\}$ .

上面例子说明:  $A - B \neq B - A$ .

**定义 1-2-4** 设  $A$  是全集  $U$  的子集, 集合  $A$  关于  $U$  的余集  $U - A$ , 称为集合  $A$  的余, 记为  $A'$  或  $\bar{A}$ , 即

$$A' = \{x \mid x \in U \text{ 并且 } x \notin A\}.$$

集合  $A$  的余的文氏图为图 1-2-4. 显然,  $A - B = A \cap B'$ .

**定理 1-2-4** 集合的余的运算满足下面性质, 这里  $A, B$  是全集  $U$  的子集,  $\emptyset$  是空集.

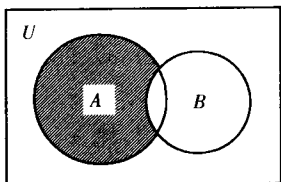


图 1-2-3

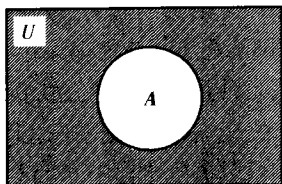


图 1-2-4

- (1)  $(A')' = A$ ;                      (2)  $U' = \emptyset$ ;  
 (3)  $\emptyset' = U$ ;                        (4)  $A \cup A' = U$ ;  
 (5)  $A \cap A' = \emptyset$ ;                (6)  $(A \cup B)' = A' \cap B'$ ;  
 (7)  $(A \cap B)' = A' \cup B'$ .

下面证明(6).

证  $(A \cup B)' = \{x | x \in (A \cup B)'\} = \{x | x \notin A \text{ 并且 } x \notin B\}$   
 $= \{x | x \in A' \text{ 并且 } x \in B'\} = A' \cap B'$ .                       $\square$

**定义 1-2-5** 设  $A, B$  是全集  $U$  的子集,  $A$  和  $B$  的对称差为集合  $S$ , 其元素属于  $A$  或属于  $B$ , 但不能既属于  $A$  又属于  $B$ , 记为  $A \oplus B$  或  $A \triangle B$ , 即

$$S = A \oplus B = (A \cup B) - (A \cap B).$$

两个集的对称差的文氏图为图 1-2-5.

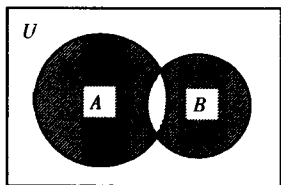


图 1-2-5

**例 1-2-6** 设  $A$  表示“主机有故障的计算机集合”,  $B$  表示“外

部设备有故障的计算机集合”，则  $A \oplus B$  表示“主机有故障与外部设备有故障中，只有一种故障的计算机集合”。

**定理 1-2-5** 集合的对称差满足下面性质，这里  $A, B, C$  是全集  $U$  的子集， $\emptyset$  是空集。

$$(1) A \oplus B = B \oplus A; \quad (2) A \oplus \emptyset = A;$$

$$(3) A \oplus A = \emptyset;$$

$$(4) A \oplus B = (A \cap B') \cup (A' \cap B) = (A - B) \cup (B - A);$$

$$(5) (A \oplus B) \oplus C = A \oplus (B \oplus C).$$

下面证明(4),(5)。

证

$$\begin{aligned} (4) A \oplus B &= (A \cup B) - (A \cap B) \\ &= (A \cup B) \cap (A \cap B)' \\ &= (A \cup B) \cap (A' \cup B') \\ &= (A \cap A') \cup (A \cap B') \cup (B \cap A') \cup (B \cap B') \\ &= (A \cap B') \cup (A' \cap B) \\ &= (A - B) \cup (B - A); \end{aligned}$$

$$\begin{aligned} (5) A \oplus (B \oplus C) &= [A \cap (B \oplus C)'] \cup [A' \cap (B \oplus C)] \\ &= \{A \cap [(B \cap C') \cup (B' \cap C)]'\} \\ &\quad \cup \{A' \cap [(B \cap C') \cup (B' \cap C)]\} \\ &= \{A \cap [(B' \cup C) \cap (B \cup C')]\} \\ &\quad \cup \{(A' \cap B \cap C') \cup (A' \cap B' \cap C)\} \\ &= (A \cap B' \cap B) \cup (A \cap B' \cap C') \\ &\quad \cup (A \cap B \cap C) \cup (A \cap C \cap C') \\ &\quad \cup (A' \cap B \cap C') \cup (A' \cap B' \cap C) \\ &= (A \cap B \cap C) \cup (A \cap B' \cap C') \\ &\quad \cup (A' \cap B \cap C') \cup (A' \cap B' \cap C). \end{aligned}$$

这表示  $A, B, C$  是对称的，于是

$$A \oplus (B \oplus C) = (A \oplus B) \oplus C. \quad \square$$

下面讨论集合的元素的个数问题. 集合  $A$  中不同元素的个数, 称为集合  $A$  的阶或基, 记为  $\#A$  或  $|A|$ . 如果  $\#A$  是有限的, 称  $A$  为有限集; 如果  $\#A$  是无限的, 称  $A$  为无限集.

如果  $A$  和  $B$  都是有限集, 并且不相交. 显然,

$$\#(A \cup B) = \#A + \#B.$$

**定理 1-2-6** 设任意两个有限集  $A, B$ , 则

$$\#(A \cup B) = \#A + \#B - \#(A \cap B).$$

**证** 从图 1-2-6 中看出:  $A \cup B$  可表为不相交的  $A$  和  $B - A$  的并.  $B$  可表为不相交的  $B - A$  和  $A \cap B$  的并. 于是

$$\#(A \cup B) = \#A + \#(B - A),$$

$$\#B = \#(B - A) + \#(A \cap B).$$

由此可得

$$\#(A \cup B) = \#A + \#B - \#(A \cap B). \quad \square$$

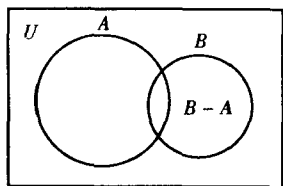


图 1-2-6

**例 1-2-7** 假设在 12 本书的集合中, 其中有 6 本小说. 1988 年出版的有 7 本书, 其中有 3 本小说. 设  $A$  为小说的集合,  $B$  为 1988 年出版的书的集合, 即  $\#A = 6$ ,  $\#B = 7$ , 于是  $A \cup B$  表示或是小说或是 1988 年出版的书的集合.

$$\#(A \cup B) = \#A + \#B - \#(A \cap B) = 6 + 7 - 3 = 10,$$

即有 10 本书或是小说或是 1988 年出版的书.

**定理 1-2-7** 设任意三个有限集  $A, B, C$ , 则

$$\begin{aligned} \#(A \cup B \cup C) &= \#A + \#B + \#C - \#(A \cap B) - \#(A \cap C) \\ &\quad - \#(B \cap C) + \#(A \cap B \cap C). \end{aligned}$$

证  $\#(A \cup B \cup C) = \#[(A \cup B) \cup C]$

$$\begin{aligned} &= \#(A \cup B) + \#C - \#[(A \cup B) \cap C] \\ &= \#A + \#B + \#C - \#(A \cap B) \\ &\quad - \#[(A \cap C) \cup (B \cap C)] \\ &= \#A + \#B + \#C - \#(A \cap B) \\ &\quad - \#(A \cap C) - \#(B \cap C) \\ &\quad + \#(A \cap B \cap C). \end{aligned}$$

□

**定理 1-2-8** 设任意  $n$  个有限集合  $A_1, A_2, \dots, A_n$ , 则

$$\begin{aligned} &\#(A_1 \cup A_2 \cup \dots \cup A_n) \\ &= \sum_{i=1}^n \#A_i - \sum_{1 \leq i < j \leq n} \#(A_i \cap A_j) \\ &\quad + \sum_{1 \leq i < j < k \leq n} \#(A_i \cap A_j \cap A_k) - \dots \\ &\quad + (-1)^{n-1} \#(A_1 \cap A_2 \cap \dots \cap A_n). \end{aligned}$$

证 对  $n$  用数学归纳法.

当  $n=2$  时, 有  $\#(A_1 \cup A_2) = \#A_1 + \#A_2 - \#(A_1 \cap A_2)$ , 即定理成立.

假定

$$\begin{aligned} &\#(A_1 \cup A_2 \cup \dots \cup A_{n-1}) \\ &= \sum_{i=1}^{n-1} \#A_i - \sum_{1 \leq i < j \leq n-1} \#(A_i \cap A_j) \\ &\quad + \sum_{1 \leq i < j < k \leq n-1} \#(A_i \cap A_j \cap A_k) \\ &\quad - \dots (-1)^n \#(A_1 \cap A_2 \cap \dots \cap A_{n-1}). \end{aligned}$$



$$\begin{aligned}
& \#(A_1 \cup A_2 \cup \cdots \cup A_{n-1} \cup A_n) \\
&= \#[(A_1 \cup A_2 \cup \cdots \cup A_{n-1}) \cup A_n] \\
&= \#(A_1 \cup A_2 \cup \cdots \cup A_{n-1}) + \#A_n \\
&\quad - \#[(A_1 \cup A_2 \cup \cdots \cup A_{n-1}) \cap A_n],
\end{aligned}$$

但

$$(A_1 \cup A_2 \cup \cdots \cup A_{n-1}) \cap A_n = (A_1 \cap A_n) \cup (A_2 \cap A_n) \cup \cdots \cup (A_{n-1} \cap A_n),$$

于是

$$\begin{aligned}
& \#[(A_1 \cup A_2 \cup \cdots \cup A_{n-1}) \cap A_n] \\
&= \#[(A_1 \cap A_n) \cup (A_2 \cap A_n) \cup \cdots \cup (A_{n-1} \cap A_n)] \\
&= \#(A_1 \cap A_n) + \#(A_2 \cap A_n) + \cdots + \#(A_{n-1} \cap A_n) \\
&\quad - \#(A_1 \cap A_2 \cap A_n) - \#(A_1 \cap A_3 \cap A_n) - \cdots \\
&\quad - \#(A_{n-2} \cap A_{n-1} \cap A_n) + \cdots + (-1)^n \#(A_1 \cap A_2 \cap \cdots \cap A_n) \\
&= \sum_{i=1}^{n-1} \#(A_i \cap A_n) - \sum_{1 \leq i < j \leq n-1} \#(A_i \cap A_j \cap A_n) + \cdots \\
&\quad + (-1)^n \#(A_1 \cap A_2 \cap \cdots \cap A_n).
\end{aligned}$$

因此

$$\begin{aligned}
& \#(A_1 \cup A_2 \cup \cdots \cup A_{n-1} \cup A_n) \\
&= \sum_{i=1}^n \#A_i - \sum_{1 \leq i < j \leq n} \#(A_i \cap A_j) \\
&\quad + \sum_{1 \leq i < j < k \leq n} \#(A_i \cap A_j \cap A_k) \\
&\quad - \cdots - (-1)^{n-1} \#(A_1 \cap A_2 \cap \cdots \cap A_n). \quad \square
\end{aligned}$$

从定理 1-2-8 中, 得出求  $n$  个有限集的并的元素个数的公式.

如果  $u$  是有限全集  $U$  的元素个数, 有

$$\#U = \#(A \cup A') = \#A + \#A' - \#(A \cap A') = \#A + \#A'.$$

于是  $\#A' = u - \#A$ . 一般有