近世代数与应用

杨振启　杨云雪　主 编

科学出版社

近世代数与应用

杨振启　杨云雪　主　编

科学出版社

北　京

内 容 简 介

本书介绍近世代数的理论和应用.

本书共 8 章, 分别介绍集合论、二元关系、同余与同余方程、二次剩余、代数系统的基础知识、群论、环论和域. 在讲解这些理论的同时也介绍了它们的应用. 在同余与同余方程一章介绍了离散对数 ElGamal 公钥密码算法体制、ElGamal 数据的加密和解密及 ElGamal 电子签名技术. 在群论一章介绍了著名的 RSA 公钥密码体制加密和解密方案及安全性讨论. 在域一章给出了通信中的线性码和循环码的编码与纠错方案以及这两种方案的编码和译码效率. 书中所有的应用都有详细的背景知识介绍, 应用理论涉及的每一个定理也都有详尽的证明过程.

本书可作为数学专业、信息与计算科学专业、电子通信等专业本科生教材, 也可供计算机科学技术、信息安全等专业研究生的应用数学教材及相关领域的科研人员和工程技术人员参考.

图书在版编目(CIP)数据

近世代数与应用/杨振启, 杨云雪主编. —北京: 科学出版社, 2017.11
ISBN 978-7-03-055074-3

Ⅰ. ①近… Ⅱ. ①杨… ②杨… Ⅲ. ①抽象代数-教材 Ⅳ. ①O153

中国版本图书馆 CIP 数据核字(2017) 第 269038 号

责任编辑: 邹 杰 / 责任校对: 郭瑞芝
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

2017 年 11 月第 一 版 开本: 787×1092 1/16
2018 年 1 月第二次印刷 印张: 15 1/2
字数: 360 000

定价: 49.00 元

(如有印装质量问题, 我社负责调换)

前　言

近世代数从它产生时起就明显有别于古典代数学. 它的主要研究对象不是代数结构中的元素特性, 而是各种代数结构本身和不同代数结构之间的相互联系. 掌握近世代数中所体现的丰富的数学思想和方法, 能提高人们解决问题和分析问题的能力.

近世代数最初是为了解决纯数学问题而建立的一套理论体系, 它首先作为大学数学学科的专业课程. 随着人们对其了解地不断深入, 如许多不同的物理结构, 具体有晶体结构和氢原子结构, 它们都可以用近世代数中的群理论的思想来建模, 特别是现代通信技术的发展、信息的加密/解密、数字认证、编码与纠错理论算法都是基于近世代数的理论开发的, 这就使得近世代数研究已从最初的数学领域扩展到了物理学、化学和信息科学等领域, 也使得传统的纯数学理论焕发出生机.

我们认为, 应用是体现数学理论价值的最好方式之一. 作为大学教学使用近世代数教材的内容, 也最好能体现这一原则. 目前, 不少数学专业包括非数学专业选用的近世代数教材, 还是沿用传统数学专业教材风格, 这些教材涉及的内容更多是数学知识本身, 应用方面的介绍很少. 部分学生学完该门课程后的印象不深或仅局限于抽象的逻辑符号, 难免会对近世代数的价值产生误解.

鉴于此, 本书的编写注意到了上述问题的存在, 有意识地使内容侧重于应用. 本书共 8 章, 分别是集合论、二元关系、同余与同余方程、二次剩余、代数系统的基础知识、群论、环论和域. 这些内容与市面上的近世代数教材没有多大差别. 除此之外, 用较大的篇幅介绍了近世代数在现代通信技术中的典型应用. 具体是第 3 章同余与同余方程中介绍了 ElGamal 公钥密码算法体制, ElGamal 数据的加密、解密及 ElGamal 电子签名. 第 6 章群论介绍了 RSA 公钥密码体制加密、解密的解决方案和对上述两种方案的安全性进行了讨论. 在第 8 章给出了通信中的线性码和循环码的编码与纠错方案, 包括对编码译码效率的讨论. 书中所有的应用都有详细的背景知识介绍, 应用理论涉及的每一个结论定理也都有详尽的证明过程, 读者在学习近世代数这门课程时都能够理解和掌握. 教学实践表明, 应用部分的学习能显著提高学习者的兴趣和取得良好的教学效果.

本书由国家自然科学基金重点项目（项目编号：NO.61232016）“云计算环境中数据安全的理论与关键技术研究”和江苏省研究生教育教学改革课题（课题编号：JGLX17_037）资助出版.

由于编者水平有限, 书中难免存在不足之处, 敬请读者批评指正, 谢谢!

作　者

2017 年 5 月

目　录

第1章 集 合 论

集合论简称集论. 这一数学分支是在 19 世纪初开始发展起来的. 德国数学家康托尔 (G. Cantor) 是集合论的奠基人.

集合的概念在现实世界中有广泛的背景, 每个人对集合都有一定的朴素印象. 把人们直观上或思维上的那些确定的、与其他事物有明显区别的对象汇集在一起就可以说是一个集合.

集合论研究集合的性质、集合间的关系和运算等. 集合论的概念和研究方法已经渗透到所有的数学分支, 并且改变了它们的面貌.

本章主要对集合论作简单介绍.

1.1 基 本 概 念

数学中的概念有两种定义形式. 其中, 一种概念可以用严格的数学逻辑形式来定义, 称为可定义概念. 另一种则不能用严格形式来定义, 而只能用语言对它进行大致的描述, 称为不可定义概念. **集合**便属于后一种. 虽然我们不能给集合以确切的定义, 但是一提到一个集合, 我们便都清楚所指的是什么, 这是因为所提集合中的事物都具有某种共同的性质.

定义 1.1 把具有某种共同属性的事物的全体称为一个集合.

通常用大写字母 $A, B, C, \cdots, M$ 等表示集合. 集合中的每一个事物称为集合的元素. 常用小写字母 $a, b, c, \cdots, m$ 等表示集合中的元素.

上面对集合给出了一个描述性的定义. 在研究具体问题时, 还需把集合具体表示出来. 集合的常用表示法有三种.

列举法: 把集合中的元素一一列举出来, 两端用花括号括起来.

例 1.1 小于 5 的所有非负整数组成的集合.

$$A = \{0, 1, 2, 3, 4\}$$

例 1.2 全体正奇数集合.

$$B = \{1, 3, 5, 7, 9, \cdots\}$$

描述法: 若集合中元素 x 具有某种性质 $p(x)$, 可在花括号内用语言叙述, 即表示成 $\{x \mid x$具有性质$p(x)\}$, 简记为 $\{x \mid p(x)\}$.

例 1.3 全体有理数的集合.

$$A = \{x \mid x\text{是有理数}\}$$

例 1.4 方程 $x^2 - 1 = 0$ 的解的集合.

$$B = \{x \mid x\text{是}x^2 - 1 = 0\text{的解}\}$$

图示法：文氏图是用图形表示集合最常见的方法. 文氏图 (或称维恩图) 是以英国数学家 John Venn 的名字命名的, 他在 1881 年介绍了这种图的使用. 我们把所考虑的所有对象的集合记为 U, U 称为全集. 在文氏图中, 全集用长方形表示. 在长方形内部, 用圆或其他几何图形表示集合, 用点来表示集合中的特定的元素. 文氏图的优点是能形象和直观地表示集合与集合之间的关系.

下面的例子解释了怎样用文氏图表示集合.

例 1.5　画一个表示英文字母中元音字母集合 V 的文氏图.

解　此种情况下, 可以认为全集 U 为考虑的所有 26 个英文字母组成的集合, 画一个长方形表示全集 U. 在长方形内部画一个圆表示元音字母集合 V, 在圆中用点表示集合 V 的五个元素, 参见图 1.1.

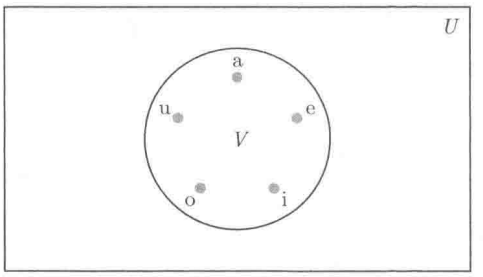

图 1.1　英文元音字母的文氏图

例 1.6　在有理数集合内讨论它的一些元素所成的集合, 如自然数集合、整数集合、奇数集合、方程 $x^2-1=0$ 的解集等, 都是一些有理数组成的集合. 全体有理数构成的集合包含了我们所考虑对象的全体元素, 在这个例子中的全集 U 就是所有有理数构成的集合.

例 1.5 和例 1.6 中的全集显然是不同的. 因为我们总是在一定的环境中考虑全集, 故全集的概念是相对的.

与全集相对应, 一个不包含任何元素的集合称为空集合, 简称**空集**, 空集用 $\varnothing$ 来表示.

例 1.7　方程 $x^2+1=0$ 的实数解的集合便是空集.

注 1　所谓给出一个集合, 就是规定了这个集合是由哪些元素组成的. 并且对于任意一个元素 a, 都能明确判断 a 是这个集合的元素, 或者 a 不是这个集合的元素, 二者必居其一.

注 2　集合里有若干相同的元素时, 这些相同的元素只能算作一个, 只用一个符号表示出来. 例如, $M=\{1,1,1,2\}$, 元素 1 在集合 M 中虽出现了三次, 但元素 1 只能算作集合 M 的一个元素, 通常写成 $M=\{1,2\}$.

注 3　在集合里, 不考虑元素的顺序. 例如, $\{a,b,c\},\{b,c,a\},\{a,c,b\}$ 集合虽然元素顺序不同, 但都认为是同一个集合.

注 4　对于某个元素 a, 由于 a 或者是集合 A 的元素, 或者不是集合 A 的元素, 元素与集合的这种关系称为从属关系.

若 a 是集合 A 中的元素, 就说 a 属于 A, 记为 $a\in A$. "$\in$" 读作 "属于".

若 a 不是集合 A 的元素, 就说 a 不属于 A, 记为 $a\notin A$ 或 $a\overline{\in}A$. "$\notin$" 或 "$\overline{\in}$" 读作 "不属于".

例 1.8 $A=\{x \mid x$是自然数$\}$, 则 $3 \in A$, $10 \in A$, $199 \in A$, 而 $-5 \notin A$.

1.2 集合间的关系

集合之间也有许多特定的关系, 下面分别讨论.

定义 1.2 如果集合 A 与 B 的元素相同, 则称这两个集合是**相等**的. 记为 $A=B$, 否则称这两个集合**不相等**, 记为 $A \neq B$.

例 1.9 集合 $A=\{1,2\}$ 与集合 $B=\{x \mid x$是方程$x^2-3x+2=0$的解$\}$, 有相同的元素, 所以 $A=B$.

例 1.10 集合 $A=\{1,2,3,4\}$ 与集合 $B=\{5,6,7,8\}$ 是两个不相等集合, 即 $A \neq B$.

定义 1.3 设有集合 A、B, 若对于任一 $a \in A$, 都有 $a \in B$, 则称集合 A 是集合 B 的**子集**, 我们说集合 A 包含于集合 B, 或者说 B 包含 A, 记为

$$A \subseteq B \text{ 或 } B \supseteq A$$

$\subseteq$ 读作包含于, $\supseteq$ 读作包含.

若 $B \supseteq A$ 且有 $b \in B$, $b \notin A$, 则称 A 是 B 的**真子集**, 或者说 B 真包含 A, 记为

$$B \supset A \text{ 或 } A \subset B$$

$\supset$ 读作真包含, $\subset$ 读作真包含于. 也可以记作 $A \subsetneqq B$ 或 $B \supsetneqq A$.

若 A 不包含于 B, 或者 B 不包含 A, 记作

$$A \nsubseteq B \text{ 或 } B \nsupseteq A$$

A 是 B 的真子集的文氏图表示方法, 如图 1.2 所示.

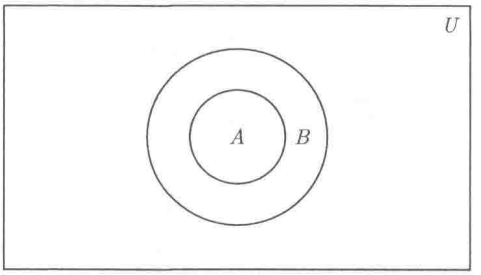

图 1.2 A 是 B 的真子集

下面再给出一个例子.

例 1.11 设 $A=\{a,b,b,c\}$, $B=\{a,b,c\}$, 则 $A=B$; 设 $A=\{1,2,3,\cdots,100\}$, 则 $A \subseteq \mathbf{N}$ 且有 $A \subset \mathbf{N}$ (这里 $\mathbf{N}$ 是全体自然数组成的集合); 设 $B=\{x \geqslant 0\}$, 则 $A \subseteq B$ 且有 $A \subset B$.

下面的几个结论都比较明显.

定理 1.1 *对任意集合 A, 必有 $\varnothing \subseteq A$.*

证明 假设 A 不包含 $\varnothing$, 按照符号 $\subseteq$ 的定义, 则至少存在一个元素 x, $x \in \varnothing$; 且 $x \notin A$, 但 $\varnothing$ 中没有元素, 故 $x \notin \varnothing$, 这与空集中没有元素相矛盾, 这个矛盾说明必有 $\varnothing \subseteq A$, 证毕.

定理 1.2 *对任意集合 A, 都有 $U \supseteq A$.*

证明　因为对于任意 $x \in A$, 都有 $x \in U$, 所以 $A \subseteq U$.

定理 1.3　*对任意集合 A, 必有 $\varnothing \subseteq A \subseteq U$.*

证明　将上面的两个定理合在一起便知.

定理 1.4　*设有集合 A、B, 则 $A = B$ 的充要条件是 $A \supseteq B$ 且 $B \supseteq A$.*

证明　($\Leftarrow$) 设 $A \supseteq B$ 且 $B \supseteq A$. 假设 $A \neq B$, 由定义 1.2 可知, A 与 B 的元素不相同, 那么存在元素 x 属于 A, 而 x 不属于 B 或者存在元素 y 属于 B, 而元素 y 不属于 A. 不失一般性设为前者, 即 $x \in A$, $x \notin B$; 但由于 $A \subseteq B$, 故当 $x \in A$ 时必有 $x \in B$, 与 $x \notin B$ 矛盾, 这个矛盾表明 $A = B$.

($\Rightarrow$) 设 $A = B$. 若 $A \supseteq B$ 和 $B \supseteq A$ 至少有一个不成立; 不妨设 $B \supseteq A$ 不成立, 则必至少存在一个 $x \in A$ 且 $x \notin B$, 这与 $A = B$ 是矛盾的, 故 $A \supseteq B$ 且 $B \supseteq A$ 成立, 证毕.

1.3　集合的运算

集合的运算就是从已知的集合产生新的集合的方法.

1.3.1　集合的基本运算

定义 1.4　由集合 A、B 的所有元素合并组成的集合称为集合 A 与 B 的**并集**, 记作 $A \cup B$. 即

$$A \cup B = \{\, x \mid x \in A \text{ 或 } x \in B \,\}$$

图 1.3 的文氏图表示了集合 A 和集合 B 的并集, 代表集合 A 的圆圈和代表 B 的圆圈内的阴影区域表示 A 和 B 的并集.

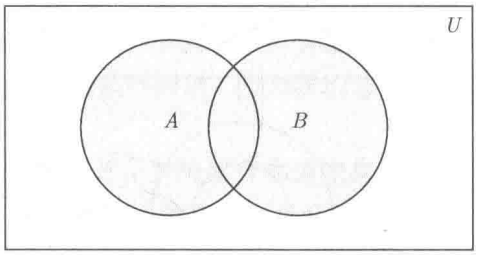

图 1.3　集合 A 与 B 的并集

例 1.12　若 $A = \{\, a, b, c, d \,\}, B = \{\, c, d, e, f \,\}$, 则

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

例 1.13　$A = \{x | x$ 是有理数 $\}$, $B = \{x | x$ 是无理数 $\}$, $C = A \cup B = \{x | x$ 是实数 $\}$.

注 5　两个集合的公共元素在并集中只能出现一次.

定义 1.5　由集合 A、B 所有的公共元素所组成的集合称为集合 A 与 B 的交集, 记作 $A \cap B$. 即

$$A \cap B = \{\, x \mid x \in A \wedge x \in B \,\}$$

图 1.4 的文氏图表示了集合 A 和集合 B 的**交集**, 代表集合 A 的圆圈和代表 B 的圆圈内公共的阴影区域表示 A 和 B 的交集.

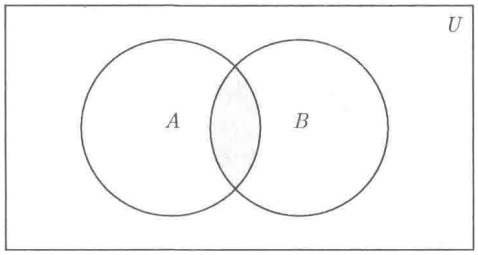

图 1.4 集合 A 与 B 的交集

例 1.14 若 $A=\{1,2,3,4\}$, $B=\{2,4,6,8\}$, 则 $A\cap B=\{2,4\}$.

例 1.15 若 $A=\{x\mid x\geqslant 3\}$, $B=\{x\mid x\leqslant 7\}$, 则 $A\cap B=\{x\mid 3\leqslant x\leqslant 7\}$.

定义 1.6 集合 A、B 若满足 $A\cap B=\varnothing$, 则称 A、B 是分离的, 也称 A、B 不相交.

例 1.16 $A=\{1,2,3\}$, $B=\{a,b,c\}$, 则 $A\cap B=\varnothing$, 即 A 与 B 是分离的.

定义 1.7 由集合 A、B 中所有属于 A 而不属于 B 的元素所组成的集合称为 A 与 B 的**差集**, 记作 $A-B$, A 和 B 的差集, 也称为 B 对于 A 的**补集**. 即

$$A-B=\{x\mid x\in A\wedge x\notin B\}$$

图 1.5 的文氏图表示了集合 A 和集合 B 的差集, 在代表集合 A 的圆圈内部和代表 B 的圆圈外的阴影区域表示 A 和 B 的差集.

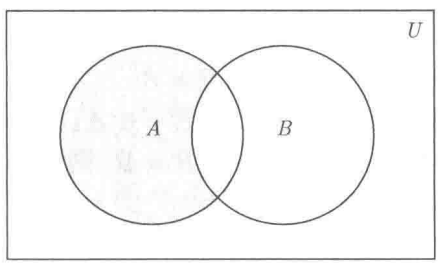

图 1.5 集合 A 与 B 的差集

例 1.17 $A=\{a,b,c,d\}$ 和 $B=\{b,c,e\}$, 则 $A-B=\{a,d\}$, $B-A=\{e\}$.

定义 1.8 全集 U 与其子集 A 的差集称为集合 A 的补集, 记作 $\overline{A}$, 于是 $\overline{A}=U-A$.

图 1.6 中代表集合 A 的圆圈外面的阴影区域表示 $\overline{A}$.

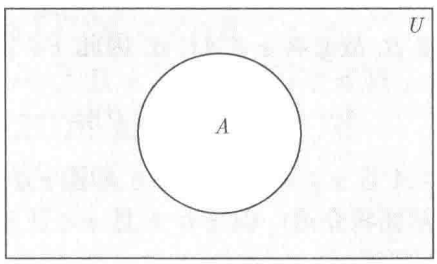

图 1.6 集合 A 的补集

例 1.18　设 $U=\{0,1,2,3,\cdots\}$,$A=\{0,2,4,6,\cdots\}$, 则

$$\overline{A}=\{1,3,5,\cdots\}$$

定义 1.9　集合 A、B 的**对称差**记作 $A\oplus B$, 定义为

$$A\oplus B=(A-B)\cup(B-A)=\{x\mid(x\in A\wedge x\notin B)\vee(x\in B\wedge x\notin A)\}$$

例 1.19　$A=\{1,2,3,4\}$,$B=\{3,4,5,6\}$, 则

$$A\oplus B=\{1,2,5,6\}$$

前面我们定义了两个集合的交集. 两个集合的交集是由两个集合中公共元素组成的集合. 而对称差与之正好相反, 它恰是去掉两个集合的所有公共元素, 由剩下的所有元素组成的集合.

下面介绍几个集合运算的重要公式.

定理 1.5　对于任意的集合 A、B, 有

$$A\cap B\subseteq A,\quad A\cap B\subseteq B$$

$$A\subseteq A\cup B,\quad B\subseteq A\cup B$$

证明　$A\subseteq A\cup B$, $B\subseteq A\cup B$ 显然成立. 其次, 如果 $x\in A\cap B$, 则 $x\in A$ 且 $x\in B$, 故 $A\cap B\subseteq A$ 且 $A\cap B\subseteq B$, 证毕.

定理 1.6　若 $A\subsetneqq B$, 则 $A\cup B=B$, $A\cap B=A$.

证明　设 $x\in A\cup B$, 则 $x\in A$ 或 $x\in B$. 若 $x\in A$, 则由 $A\subsetneqq B$ 可知 $x\in B$, 总之有 $A\cup B\subseteq B$. 根据定理 1.5 有 $B\subseteq A\cup B$, 故 $A\cup B=B$. 同理 $A\cap B\subseteq A$, 证毕.

定理 1.7　设 A、B 为任意集合, 则有

$$A-B=A\cap\overline{B}$$

$$A-B=A-A\cap B$$

证明　$x\in A-B\Leftrightarrow x\in A$ 且 $x\notin B\Leftrightarrow x\in A$ 且 $x\in\overline{B}$, 故

$$A-B=A\cap\overline{B}$$

设 $x\in A-B$, 即 $x\in A$ 且 $x\notin B$, 故必有 $x\notin A\cap B$, 因此 $x\in[A-(A\cap B)]$, 即

$$A-B\subseteq[A-(A\cap B)]$$

又设 $x\in[A-(A\cap B)]$, 则 $x\in A$ 且 $x\notin A\cap B$, 即 $x\in A$ 且 $x\in(\overline{A\cap B})$; 即 $x\in A$ 且 [$x\in\overline{A}$ 或 $x\in\overline{B}$] (注: $(\overline{A\cap B})=\overline{A}$ 后面将介绍). 但 $x\in A$ 且 $x\in\overline{A}$ 是不可能的, 故只能有 $x\in A$ 且 $x\in\overline{B}$. 即 $x\in A-B$, 从而得到 $A-(A\cap B)\subseteq A-B$. 因此

$$A-B=A-(A\cap B)$$

定理 1.8 设 A、B 为两个集合, 若 $A \subseteq B$, 则

$$\overline{B} \subseteq \overline{A}$$
$$(B-A) \cup A = B$$

证明 若 $x \in A$, 则 $x \in B$, 因此 $x \notin B$ 必有 $x \notin A$, 故 $x \in \overline{B}$, 必有 $x \notin \overline{A}$, 即 $\overline{B} \subseteq \overline{A}$.

设 $x \in (B-A) \cup A$, 则 $x \in B-A$ 或 $x \in A$. 若 $x \in B-A$, 则 $x \in B$; 若 $x \in$ A, 由已知 $A \subseteq B$, 应有 $x \in B$. 因此, $(B-A) \cup A \subseteq B$.

反之, 设 $x \in B$, 由 $A \subseteq B$ 有, 或者是 $x \in A$, 或者是 $x \in B-A$, 总之有 $x \in (B-A) \cup A$, 即 $B \subseteq (B-A) \cup A$. 因此

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

证毕.

1.3.2 集合的运算律

前面定义了集合的并、交、差等运算, 这些运算还可以混合进行, 且遵循一定的规律, 下面列举一些.

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

(2) $(A \cup B) \cup C = A \cup (B \cup C)$, $(A \cap B) \cap C = A \cap (B \cap C)$ (结合律)

(3) $A \cup B = B \cup A$, $A \cap B = B \cap A$ (交换律)

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

(5) $A \cup \varnothing = A$, $A \cap \varnothing = \varnothing$

(6) $A \cup E = E$, $A \cap E = A$

(7) $A \cup \overline{A} = E$, $A \cap \overline{A} = \varnothing$

(8) $A \cup (A \cap B) = A$, $A \cap (A \cup B) = A$ (吸收律)

(9) $\overline{(A \cup B)} = \overline{A} \cap \overline{B}$, $\overline{(A \cap B)} = \overline{A} \cup \overline{B}$ (德·摩根律)

(10) $\overline{\varnothing} = E$, $\overline{E} = \varnothing$

(11) $\overline{\overline{A}} = A$

这 11 个等式, 除最后一个外, 其他的都是成对出现的.

我们现在来证明其中的公式 (9) 德·摩根律, 其他略.

先证 $\overline{(A \cup B)} = \overline{A} \cap \overline{B}$. 设 $x \in \overline{(A \cup B)}$, 则 $x \notin (A \cup B)$, 因此 $x \notin A$ 且 $x \notin B$, 从而 $x \in \overline{A}$ 且 $x \in \overline{B}$, 即 $x \in \overline{A} \cap \overline{B}$, 从而 $\overline{(A \cup B)} \subseteq \overline{A} \cap \overline{B}$.

反之, 设 $x \in \overline{A} \cap \overline{B}$, 则 $x \in \overline{A}$ 且 $x \in \overline{B}$, 从而 $x \notin A$ 且 $x \notin B$, 还有 $x \notin A \cup B$, 于是必有 $x \in \overline{(A \cup B)}$, 即 $\overline{A} \cap \overline{B} \subseteq \overline{(A \cup B)}$, 故 $\overline{(A \cap B)} = \overline{A} \cup \overline{B}$.

$\overline{(A \cap B)} = \overline{A} \cup \overline{B}$ 同理可证, 证毕.

1.3.3 例题

前面介绍了集合的运算及运算律, 现在通过几个例子, 我们来观察一下, 集合的运算律在运算过程及实际中的应用.

例 1.20　化简 $(A\cup B)\cap(A\cup\overline{B})$.

解

$$\begin{aligned}&(A\cup B)\cap(A\cup\overline{B})\\=&A\cup(B\cap\overline{B})\ (\text{分配律})\\=&A\cup\varnothing\ (\text{公式 (7)})\\=&A\ (\text{公式 (5)})\end{aligned}$$

例 1.21　化简 $(A\cup B)\cup(\overline{A}\cap B)$.

解

$$\begin{aligned}&(A\cup B)\cup(\overline{A}\cap B)\\=&[(A\cup B)\cup\overline{A}]\cap[(A\cup B)\cup B]\ (\text{分配律})\\=&[A\cup B\cup\overline{A}]\cap[A\cup B\cup B]\ (\text{结合律})\\=&(E\cup B)\cap(A\cup B)\ (\text{交换律、公式 (7)、幂等律})\\=&E\cap(A\cup B)\ (\text{公式 (6)})\\=&A\cup B\ (\text{公式 (6)})\end{aligned}$$

例 1.22　证明若 $A\cup B=A\cap B$, 则 $A=B$.

证明

$$\begin{aligned}A=&A\cup(A\cap B)\ (\text{吸收律})\\=&A\cup(A\cup B)\ (\text{已知条件})\\=&(A\cup A)\cup B\ (\text{公式 (2)})\\=&A\cup B\ (\text{公式 (1)})\end{aligned}$$

而

$$\begin{aligned}B=&B\cup(B\cap A)\ (\text{吸收律})\\=&B\cup(B\cup A)\ (\text{已知条件})\\=&(B\cup B)\cup A\ (\text{公式 (2)})\\=&A\cup B\ (\text{公式 (1)})\end{aligned}$$

故得 $A=B$, 证毕.

1.4　包含排斥原理

1.4.1　两个集合的包含排斥原理

集合广泛应用于计数问题. 先给出集合基数的概念.

定义 1.10　设 A 是一个集合, n 是非负整数, 若 A 中恰有 n 个不同的元素, 则称 A 是**有限集合**, n 是 A 的基数, A 的基数用 $|A|$ 表示.

例 1.23　若 A 是小于 10 的正奇数的集合, 那么 $|A|=5$.

例 1.24　由于空集没有元素, 所以 $|\varnothing|=0$.

例 1.25 设 S 是所有英文字母组成的集合, 则 $|S|=26$.

定义 1.11 当集合不是有限集合时, 就称为**无限集合**.

例 1.26 正整数组成的集合是无限集合.

设 A_1、A_2 为有限集合, 其基数分别为 $|A_1|$、$|A_2|$, 从集合 A_1 和 A_2 并集、交集、差集和对称差集的文氏图上不难验证以下各式成立.

(1) $|A_1 \cup A_2| \leqslant |A_1| + |A_2|$

(2) $|A_1 \cap A_2| \leqslant \min\{|A_1|, |A_2|\}$

(3) $|A_1 - A_2| \geqslant |A_1| - |A_2|$

(4) $|A_1 \oplus A_2| = |A_1| + |A_2| - 2|A_1 \cap A_2|$

在有限集的元素计数问题中, 下述定理有广泛的应用.

定理 1.9 设 A_1、A_2 为有限集合, 其元素个数分别为 $|A_1|$、$|A_2|$, 则

$$|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$$

证明 若 A_1 与 A_2 不相交, 即 $A_1 \cap A_2 = \varnothing$, 则

$$|A_1 \cup A_2| = |A_1| + |A_2|$$

若 $A_1 \cap A_2 \neq \varnothing$, 则

$$|A_1| = |A_1 \cap \overline{A}_2| + |A_1 \cap A_2|$$

$$|A_2| = |\overline{A}_1 \cap A_2| + |A_1 \cap A_2|$$

所以

$$|A_1| + |A_2| = |A_1 \cap \overline{A}_2| + |\overline{A}_1 \cap A_2| + 2|A_1 \cap A_2|$$

但

$$|A_1 \cap \overline{A}_2| + |\overline{A}_1 \cap A_2| + |A_1 \cap A_2| = |A_1 \cup A_2|$$

故

$$|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$$

定理 1.9 称作两个集合的包含排斥原理.

例 1.27 假设在 10 名青年中有 5 名是工人, 7 名是学生, 其中兼具有工人与学生双重身份的青年有 3 名, 问既不是工人又不是学生的青年有几名?

解 设工人的集合为 W, 学生的集合为 S, 则根据题设有 $|W|=5$, $|S|=7$, $|W \cap S|=3$. 又因为 $|\overline{W} \cap \overline{S}| + |W \cup S| = 10$, 则

$$\begin{aligned} |\overline{W} \cap \overline{S}| = 10 - |W \cup S| &= 10 - (|W| + |S| - |W \cap S|) \\ &= 10 - (5 + 7 - 3) \\ &= 1 \end{aligned}$$

所以既不是工人又不是学生的青年有一名.

1.4.2　三个集合的包含排斥原理

可以将定理 1.9 中的两个集合推广到三个集合的情形, 相应的结果为

$$|A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| + |A_1 \cap A_2 \cap A_3|$$

这个公式可以通过图 1.7 予以验证.

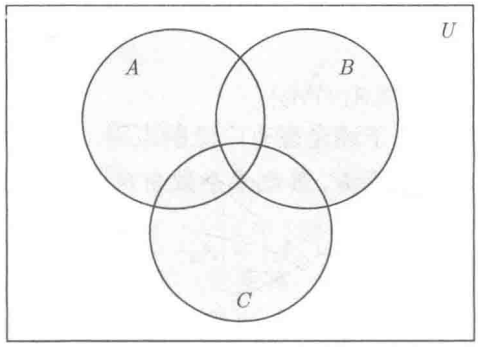

图 1.7　三个集合 A、B 和 C 的并集

例 1.28　在某工厂装配 30 辆汽车, 可供选择的设备有收音机、空气调节器和对讲机. 已知其中 15 辆汽车有收音机, 8 辆有空气调节器, 6 辆有对讲机, 而且其中 3 辆汽车这三样设备都有. 我们希望知道至少有多少辆汽车没有提供任何设备.

解　设 A_1、A_2、A_3 分别表示配有收音机、空气调节器和对讲机的汽车集合. 因此 $|A_1| = 15|$, $|A_2| = 8$, $|A_3| = 6$, 并且 $|A_1 \cap A_2 \cap A_3| = 3$, 故

$$\begin{aligned} |A_1 \cup A_2 \cup A_3| &= 15 + 8 + 6 - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| + 3 \\ &= 32 - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| \end{aligned}$$

因为

$$|A_1 \cap A_2| \geqslant |A_1 \cap A_2 \cap A_3|$$

$$|A_1 \cap A_3| \geqslant |A_1 \cap A_2 \cap A_3|$$

$$|A_2 \cap A_3| \geqslant |A_1 \cap A_2 \cap A_3|$$

我们得到

$$|A_1 \cup A_2 \cup A_3| \leqslant 32 - 3 - 3 - 3 = 23$$

即至多有 23 辆汽车有一个或几个供选择的设备, 因此, 至少有 7 辆汽车不提供任何可选择的设备.

1.4.3　多个集合的包含排斥原理

继续将包含排斥原理推广到 n $(n > 3)$ 个集合的情况, 有下述结论.

定理 1.10 设 $A_1, A_2, \cdots, A_n$ 为有限集合, 其元素个数分别为 $|A_1|, |A_2|, \cdots, |A_n|$, 则

$$\begin{aligned}|A_1 \cup A_2 \cup \cdots \cup A_n| = &\sum_{i=1}^{n} |A_i| - \sum_{1 \leqslant i < j \leqslant n} |A_i \cap A_j| \\ &+ \sum_{1 \leqslant i < j < k \leqslant n} |A_i \cap A_j \cap A_k| \\ &+ \cdots + (-1)^{n-1} |A_1 \cap A_2 \cap A_3 \cap \cdots \cap A_n| \end{aligned} \tag{1.1}$$

证明 用归纳法.

(1) $n = 2$, 则 $|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$, 结论成立.

(2) 设 $r - 1$ 个集合时结论成立.

对于 r 个集合 $A_1, A_2, \cdots, A_{r-1}, A_r$, 因为两个集合时结论成立, 则有

$$\begin{aligned}|A_1 \cup A_2 \cup \cdots \cup A_{r-1} \cup A_r| &= |A_1 \cup A_2 \cup \cdots \cup A_{r-1}| + |A_r| \\ &\quad - |A_r \cap (A_1 \cup A_2 \cup \cdots \cup A_{r-1})| \\ &= |A_1 \cup A_2 \cup \cdots \cup A_{r-1}| + |A_r| \\ &\quad - |(A_r \cap A_1) \cup (A_r \cap A_2) \cup \cdots \cup (A_r \cap A_{r-1})| \end{aligned} \tag{1.2}$$

对于 $r - 1$ 个集合 $A_r \cap A_i (i = 1, 2, \cdots, r-1)$, 由归纳假设可知

$$\begin{aligned}&|(A_r \cap A_1) \cup (A_r \cap A_2) \cup \cdots \cup (A_r \cap A_{r-1})| \\ =&\sum_{i=1}^{r-1} |A_r \cap A_i| - \sum_{1 \leqslant i < j \leqslant r-1} |(A_r \cap A_i) \cap (A_r \cap A_j)| \\ &+ \cdots + (-1)^{r-2} |(A_r \cap A_1) \cap (A_r \cap A_2) \cap \cdots \cap (A_r \cap A_{r-1})| \\ =&\sum_{i=1}^{r-1} |A_r \cap A_i| - \sum_{1 \leqslant i < j \leqslant r-1} |(A_r \cap A_i \cap A_j)| \\ &+ \cdots + (-1)^{r-2} |A_1 \cap A_2 \cap \cdots \cap A_{r-1} \cap A_r| \end{aligned} \tag{1.3}$$

另外对 $r - 1$ 个集合 $A_i (i = 1, 2, \cdots, r-1)$, 由归纳假设有

$$\begin{aligned}|A_1 \cup A_2 \cup \cdots \cup A_{r-1}| = &\sum_{i=1}^{r-1} |A_i| - \sum_{1 \leqslant i < j \leqslant r-1} |A_i \cap A_j| + \sum_{1 \leqslant i < j < k \leqslant r-1} |A_i \cap A_j \cap A_k| \\ &+ \cdots + (-1)^{r-2} |A_1 \cap A_2 \cap \cdots \cap A_{r-1}| \end{aligned} \tag{1.4}$$