近世代数及其应用

阮传概　编

北京邮电学院出版社

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有用的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。

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、应用数学、应用物理等科技人员参考。

近 世 代 数 及 其 应 用

编　　者　阮 传 概

责任编辑　阮 平 生

北京邮电学院出版社出版

新华书店北京发行所发行　各地新华书店经售

河北香河燃口印刷厂印刷

850×1168毫米　1/32　印张，9.4　字数，250千字

1988年6月第一版　1988年6月第一次印刷

印数，1—4000 册

ISBN 7—5635—0001—4/O 1　　定价，1.80元

前　言

近世代数课程不但在数学的各个分支有很多应用，而且随着计算技术的发展，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。近世代数的基本内容已成为这些领域中科技人员的基本工具。现在国内出版的近世代数的教科书，一般都是为数学专业的学生编写的，而通信理论、计算机科学、系统工程等一些专业的学生与数学专业的学生的数学基础不同，对近世代数内容的要求也不同，本书就是为这些专业的大学生及研究生编写的。

本书把集合与映射的概念作为预备知识首先介绍，然后介绍格、布尔代数、半群、群、环、有限域等几个代数系统的基本知识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有用的多项式和线性同余式等知识。本书从格、布尔代数开始讨论，目的在于使学生更早地看到应用，从而促进他们对近世代数学习的兴趣。由于本书是为工科学生编写的，所以比较注重应用，例题较多，每章末均附有习题。一般只要具有工科所要求的微积分与线性代数知识的人，就可学习本书。

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、应用数学、应用物理等科技人员参考。

本书是编者近年来在北京邮电学院多次讲授此课程的讲义的基础上修改而成，由于编者水平有限，定有不妥之处，殷切希望读者指正。本书在编写过程中，北京邮电学院童勤谟教授给予很大帮助，并详细地审阅全文，在此表示感谢。

编　者

1987.9.　于北京

目　录

第一章　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 $A,B,C,D,\cdots$ 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 $\boldsymbol{Z}$。以后我们把所有有理数所组成的集合，简称有理数集，记为 $\boldsymbol{Q}$；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 $\boldsymbol{R},\boldsymbol{C}$。组成一个集合的对象称为这集合的元素，通常用小写的英文字母 $a,b,c,d,\cdots$ 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：列表法和构造法。所谓列表法，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，$A=\{x\mid x\in\boldsymbol{Z},x>0\}$ 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ϕ；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

$$P(A)=\{\phi,\{a\},\{b\},A\}。$$

例 1-1-3 设 $A=\{a,b,c\}$，则

$$P(A)=\{\phi,\{a\},\{b\},\{c\},\{a,b\},\{a,c\},\{b,c\},A\}。$$

从上面例子可看出：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。可推出：n个元素的集合的幂集有2^n个元素，见（练习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”；B 表示“上物理课的学生”。如果这两门课安排在同一时间进行期终考试，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

$A\cap B=\{x|x\in U，x\in A$ 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 $A\cap B$。

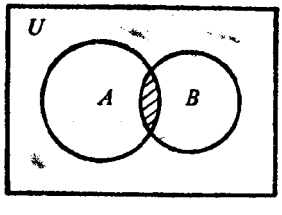

图 1-2-1

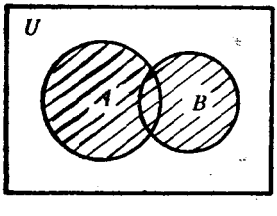

图 1-2-2

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

$$A\cap B=\{a,b,c\}。$$

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，ϕ 是空集。

（1） $A\cap A=A$；　　（2） $A\cap\phi=\phi$；

（3） $A\cap U=A$；　　（4） $A\cap B=B\cap A$；

（5） $A\cap(B\cap C)=(A\cap B)\cap C$。

下面我们证明（5）。

证 $(A\cap B)\cap C=\{x|x\in(A\cap B)$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$(x\in B$并且$x\in C)\}=\{x|x\in A$并且$x\in(B\cap C)\}=\{x|x\in A\cap(B\cap C)\}=A\cap(B\cap C)$。□

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

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

$$A\cup B=\{x|x\in A\text{ 或 }x\in B\}。$$

两个集的并的文氏图，为图 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，ϕ 是空集。

（1） $A\cup A=A$；　　（2） $A\cup U=U$；

（3） $A\cup\phi=A$；　　（4） $A\cup B=B\cup A$；

（5） $A\cup(B\cup C)=(A\cup B)\cup C$。

证 这些性质的证明，容易从定义得出。□

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） $A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$；

（2） $A\cup(B\cap C)=(A\cup B)\cap(A\cup C)$　（分配律）；

（3） $A\cup(A\cap B)=A$；

（4） $A\cap(A\cup B)=A$　（吸收律）；

（5） 若 $A\subseteq C$，则 $A\cup(B\cap C)=(A\cup B)\cap C$（模律）。

下面我们证明（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

$A\cup(B\cap C)=(A\cup B)\cap C$。□

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

$A-B=\{x|x\in A$ 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。

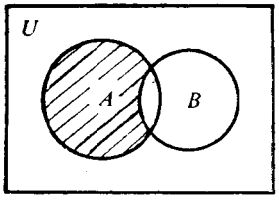

图 1-2-3

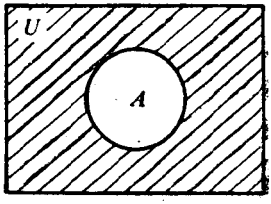

图 1-2-4

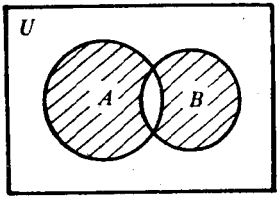

图 1-2-5

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

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

$A'=\{x|x\in U$ 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，ϕ是空集。

（1） $(A')'=A$；　　（2） $U'=\phi$；

（3） $\phi'=U$；　　（4） $A\cup A'=U$；

（5） $A\cap A'=\phi$；　　（6） $(A\cup B)'=A'\cap B'$；

（7） $(A\cap B)'=A'\cup B'$。

下面我们证明（6）。

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

$=\{x|x\in A'$ 并且 $x\in B'\}=A'\cap B'$。□

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。

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，ϕ 是空集。

（1） $A\oplus B=B\oplus A$；　　（2） $A\oplus\phi=A$；

（3） $A\oplus A=\phi$；

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

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

下面我们证明（4）、（5）。

证

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

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

这表示 A，B，C 是对称的，于是

$$A\oplus(B\oplus C)=(A\oplus B)\oplus C)。\ \square$$

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$\#A$。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 我们从图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

$$\#(A\cup B)=\#A+\#B-\#(A\cap B)。\qquad \square$$

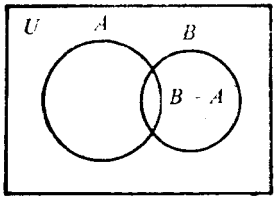

图 1-2-6

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

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

证　$\#(A\cup B\cup C)=\#[(A\cup B)\cup C]$
$$=\#(A\cup B)+\#C-\#[(A\cup B)\cap C]$$
$$=\#A+\#B+\#C-\#(A\cap B)$$
$$-\#[(A\cap C)\cup(B\cap C)]$$
$$=\#A+\#B+\#C-\#(A\cap B)$$
$$-\#(A\cap C)-\#(B\cap C)$$
$$+\#(A\cap B\cap C)。\quad \square$$

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

$$\#(A_1\cup A_2\cup\cdots\cup A_n)=\sum_{i=1}^{n}\#A_i-\sum_{1\leqslant i<j\leqslant n}\#(A_i\cap A_j)$$
$$+\sum_{1\leqslant i<j<k\leqslant n}\#(A_i\cap A_j\cap A_k)-\cdots$$
$$+(-1)^{n-1}\#(A_1\cap A_2\cap\cdots\cap A_n)。$$

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

$$\#(A_1\cup A_2\cup\cdots\cup A_{n-1})=\sum_{i=1}^{n-1}\#A_i-\sum_{1\leqslant i<j\leqslant n-1}\#(A_i\cap A_j)$$
$$+\sum_{1\leqslant i<j<k\leqslant n-1}\#(A_i\cap A_j\cap A_k)$$
$$-\cdots(-1)^n\#(A_1\cap A_2\cap\cdots\cap A_{n-1})。$$

$$\#(A_1\cup A_2\cup\cdots\cup A_{n-1}\cup A_n)=\#[(A_1\cup A_2\cup\cdots\cup A_{n-1})\cup A_n]$$

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

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

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

因此

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

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，我们有

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

于是 $\#A' = u - \#A$。一般有

推论 1-2-1

$$\#(A_1' \cap A_2' \cap \cdots \cap A_n') = u - \#(A_1 \cup A_2 \cup \cdots \cup A_n)$$

$$= u - \sum_{i=1}^{n} \#A_i + \sum_{1 \leqslant i < j \leqslant n} \#(A_i \cap A_j)$$

$$- \sum_{1 \leqslant i < j < k \leqslant n} \#(A_i \cap A_j \cap A_k) + \cdots$$

$$+ (-1)^n \#(A_1 \cap A_2 \cap \cdots \cap A_n) \ ,$$

这里 u 是有限全集 U 的元素个数。

例 1-2-8　设 n 为正整数，欧拉(Euler)函数 $\varphi(n)$ 是小于 n 且与 n 互素的正整数的个数，求 $\varphi(n)$。

解　把 n 分解成素数幂的乘积

$$n = p_1^{a_1} p_2^{a_2} \cdots p_m^{a_m}$$

这里 $p_1, p_2, \cdots, p_m$ 为素数；$\alpha_1, \alpha_2, \cdots, \alpha_m$ 为正整数。设 1 到 n 的 n 个正整数中为 p_i 倍数的数构成集 A_i，$i = 1, 2, \cdots, m$，则

$$\#A_i = \frac{n}{p_i}, \quad i = 1, \ 2, \ \cdots, \ m;$$

$$\#(A_i \cap A_j) = \frac{n}{p_i p_j}, \quad i, j = 1, 2, \cdots, m; \ j > i;$$

$$\#(A_i \cap A_j \cap A_k) = \frac{n}{p_i p_j p_k}, \quad i, j, k = 1, 2, \cdots, m; \ k > j > i$$

$\cdots\cdots$。

因此，

$$\varphi(n) = \#(A_1' \cap A_2' \cap \cdots \cap A_m')$$

$$= n - \sum_{i=1}^{m} \#A_i + \sum_{1 \leqslant i < j \leqslant m} \#(A_i \cap A_j)$$

$$- \sum_{1 \leqslant i < j < k \leqslant m} \#(A_i \cap A_j \cap A_k) + \cdots$$

$$+ (-1)^m \#(A_1 \cap A_2 \cap \cdots \cap A_m)$$