近世代数及其应用

罗守山　陈　萍　编著

JINSHI DAISHU JIQI YINGYONG

北京邮电大学出版社
www.buptpress.com

近世代数及其应用

罗守山　陈　萍　编著

北京邮电大学出版社
www.buptpress.com

内 容 简 介

本书介绍了群、环、域的基本原理和方法，介绍了近世代数方法在编码、密码中的一些应用。本书的内容包括：集合与映射、关系与等价关系、多项式的表示与运算、群、环、域、群与纠错编码、环理论在密码学中的应用、有限域上的离散对数。为了增强学生对近世代数方法的理解，在每一章的最后，还介绍了相关数学知识在编码、密码中的应用。同时，各章还配有一定数量的习题，便于教学与自学。

本书可以作为通信、电子、计算机、信息安全等相关专业的研究生教材，也可供从事相关专业的教学、科研人员和工程技术人员参考。

图书在版编目(CIP)数据

近世代数及其应用 / 罗守山，陈萍编著. --北京：北京邮电大学出版社，2016.7
ISBN 978-7-5635-4734-0

Ⅰ.①近… Ⅱ.①罗…②陈… Ⅲ.①抽象代数 Ⅳ.①O153

中国版本图书馆 CIP 数据核字(2016)第 071971 号

书　　名：近世代数及其应用
著作责任者：罗守山　陈　萍　编著
责 任 编 辑：艾莉莎
出 版 发 行：北京邮电大学出版社
社　　址：北京市海淀区西土城路 10 号(邮编：100876)
发 行 部：电话：010-62282185　传真：010-62283578
E-mail：publish@bupt.edu.cn
经　　销：各地新华书店
印　　刷：保定市中画美凯印刷有限公司
开　　本：787 mm×1 092 mm　1/16
印　　张：12.25
字　　数：288 千字
版　　次：2016 年 7 月第 1 版　2016 年 7 月第 1 次印刷

ISBN 978-7-5635-4734-0　　定　价：26.00 元

前　言

近世代数是数学学科的一个重要分支，并且在通信中有重要的应用。近世代数课程也是很多高校研究生培养中的一门数理类公共基础课。

本书介绍了近世代数中的一些基本理论与方法，同时，也介绍了这些方法在可靠通信与保密通信中的应用。本书结构安排如下：

第 1 章预备知识，介绍了集合与映射、运算与同态映射、关系与等价关系、数论基础、多项式基础、密码学基础与同态密码算法等内容。

第 2 章群，介绍了群的定义与性质、子群与群的同态、循环群、变换群与置换群、正规子群与商群、群同态基本定理、群与纠错编码等内容。

第 3 章环，介绍了环的定义及其性质、子环、环同态基本定理、分式域、环的直积、矩阵环、多项式环、序列环、素理想与极大理想、唯一分解环、主理想环与欧氏环、环理论在密码学中的应用等内容。

第 4 章域，介绍了域的扩张、极小多项式、多项式的分裂域、有限域、有限域上的离散对数与密钥交换协议等内容。

通过对本书的学习，读者可以学习到近世代数中的一些基本知识与应用。通过对本书习题的思考，读者可以获得相关技能的训练。本书可以作为通信、电子、计算机、信息安全等相关专业的研究生教材。

本教材由北京邮电大学罗守山、陈萍共同编写。由于作者水平有限，在编写过程中难免出现错误与遗漏，请广大读者批评指正。

目　录

第1章　预备知识

In algebra, which is a broad division of mathematics, abstract algebra is a common name for the subarea that studies algebraic structures in their own right. Such structures include groups, rings, fields etc. The specific term abstract algebra was coined at the turn of the 20th century to distinguish this area from the other parts of algebra. The term modern algebra has also been used to denote abstract algebra.

As in other parts of mathematics, concrete problems and examples have played important roles in the development of algebra. Through the end of the nineteenth century many, perhaps most of these problems were in some way related to the theory of algebraic equations. Major themes include:

1. Solving of systems of linear equations, which led to matrices, determinants and linear algebra。

2. Attempts to find formulae for solutions of general polynomial equations of higher degree that resulted in discovery of groups as abstract manifestations of symmetry。

3. Arithmetical investigations of quadratic and higher degree forms and diophantine equations, that directly produced the notions of a ring and ideal。

Numerous textbooks in abstract algebra start with axiomatic definitions of various algebraic structures and then proceed to establish their properties. This creates a false impression that in algebra axioms had come first and then served as a motivation. The true order of historical development was almost exactly the opposite.

代数学是博大的数学学科中的一个研究领域。作为代数学的一个分支，抽象代数主要研究群、环、域等代数结构。在20世纪初，为了区别于代数学中的其他分支，“抽象代数”这个词开始出现。抽象代数也称为近世代数。

与数学中的其他分支一样，在代数学的发展过程中，具体问题和实例起着重要的作用。到19世纪末，也许大部分的数学问题与代数方程有关。这包括：

1. 通过对求解线性方程组问题的研究，人们归纳出了矩阵、行列式、线性代数的知识。

2. 通过对一般高阶多项式方程求根公式的探索，人们归纳出用群表示对称的方法。

3. 通过对二次、高次及丢番图方程的探索，人们提出了环与理想的概念。

很多抽象代数教材都是从不同代数系统的定义出发，然后再给出它们的性质。这样会导致一个错误印象：代数公理在前，其次才是解决一些实际问题。实际上，代数发展的过程恰恰相反。

——W. Keith Nicholson, Introduction to Abstract Algebra, 4th edition, John Wiley & Sons, 2012, ISBN 978-1-118-13535-8。

近世代数也称为抽象代数。它主要研究各种代数系统的运算性质，并利用这些性质来解决数学、其他科学以及工程技术中的问题。在本章中，我们将学习近世代数的一些预备知识，包括：集合与映射、运算与同态映射、关系与等价关系、数论基础、多项式基础、密码学基础与同态密码算法等内容。

1.1 集合与映射

集合与映射，都是数学中的一些基本概念。在本节中，我们对这些概念做一个复习。

1.1.1 集合

1. 集合的概念

首先，我们给出集合的概念。

集合是一个不定义的数学概念。所谓集合就是具有一定属性的事物组成的整体（或集体）。通常用英文大写字母 $A,B,C,\cdots$ 表示。集合由元素构成，元素指的是组成一个集合的事物。元素一般用小写字母 $a,b,c,\cdots$ 表示。如果 a 是集合 A 的元素，称 a 属于 A，记为 $a\in A$；如果 a 不是集合 A 的元素，称 a 不属于 A，记为 $a\notin A$，或 $a\in\!\!\!/\, A$。对任何元素 a 和任何集合 A，或者 $a\in A$，或者 $a\notin A$，两者恰居其一。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。几个常用的数集：**N**（自然数集），**Z**（整数集），**Q**（有理数集），**R**（实数集），**C**（复数集）。空集 $\varnothing$ 表示没有元素的集合。

如果 A 和 B 是两个集合，$A=B$ 读为 A 等于 B，表示它们是由相同的元素构成的集合，即 A 的每一个元素都是 B 的元素，并且 B 的每一个元素也都是 A 的元素。

如果集合 A 的每一个元素都是集合 B 的元素，即若元素 x 属于 A，那么 x 属于 B，则可以记作 $A\subseteq B$（或 $B\supseteq A$），读作“A 包含于 B”（或“B 包含 A”）。我们把 A 称作是 B 的子集。A 不是 B 的子集用 $A\not\subset B$ 来表示。如果 $A\subseteq B$ 且 $A\neq B$，则称 A 是 B 的真子集。“A 是 B 的真子集”记为 $A\subset B$。

集合 S 的幂集是指由 S 的全体子集组成的集合。记作 2^S。

例 设集合 $A=\{1,2,3\}$，试写出集合 A 的幂集。

解：$2^A=\{\varnothing,\{1\},\{2\},\{3\},\{1,2\},\{1,3\},\{2,3\},\{1,2,3\}\}$。

2. 集合的运算

设 A,B 是两集合，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 $A \cup B = \{x \mid x \in A$ 或 $x \in B\}$。

集合并的运算具有以下性质：

(1) $A \cup A = A$；

(2) $A \cup \varnothing = A$；

(3) $A \subseteq B \Leftrightarrow A \cup B = B$

对于多个集合的并，我们可以记为：$W = A_1 \cup A_2 \cup \cdots \cup A_n = \bigcup_{i=1}^{n} A_i$。

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 $A \cap B = \{x \mid x \in A$ 且 $x \in B\}$。

集合交集的运算具有以下性质：

(1) $A \cap A = A$；

(2) $A \cap \varnothing = \varnothing$；

(3) $A \subseteq B \Leftrightarrow A \cap B = A$。

当研究集合与集合间的关系时，在某些情况下，这些集合都是某一个给定集合的子集，这个给定的集合就称为全集 I。也就是说，全集含有我们所要研究的各个集合的全体元素。

已知全集 I，集合 $A \subseteq I$，由 I 中所有不属于 A 的元素组成的集合，成为集合 A 在 I 中的补集，记作 $\overline{A}$，即 $\overline{A} = \{x \mid x \in I$ 且 $x \notin A\}$。

由补集的定义可知，对于任何集合 A，有

$$A \cup \overline{A} = I, \quad A \cap \overline{A} = \varnothing, \quad \overline{\overline{A}} = A。$$

就象我们熟悉的加减乘除运算一样，集合的运算也有它的一些规律，现在我们就来简要的概括一下这些运算规律。

定理　设 A, B, C 为任意集合，$*$ 代表运算 $\cup$ 或 $\cap$，那么

(1) $A * A = A$　　(等幂律)

(2) $A * B = B * A$　　(交换律)

(3) $A * (B * C) = (A * B) * C$　　(结合律)

(4) $A \cup \varnothing = A, A \cup I = I, A \cap \varnothing = \varnothing, A \cap I = A$

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

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

$A - B$ 称为 A 与 B 的差集，定义为：$A - B = \{x \mid x \in A$ 且 $x \notin B\}$

集合的笛卡儿积是多个集合之间的一种运算。

定义　设 $A_1, A_2, \cdots, A_n$ 是 n 个集合，则集合 $A_1, A_2, \cdots, A_n$ 的笛卡儿积定义为集合：$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \cdots, a_n) \mid a_i \in A_i\}$。即由一切从 $A_1, A_2, \cdots, A_n$ 里顺序取出元素组成的元素组 $(a_1, a_2, \cdots, a_n) a_i \in A_i$ 组成的集合。

例　$A = \{1, 2, 3\}$，$B = \{4, 5\}$，求如下形式的笛卡儿积：$A \times B, B \times A$。

解：$A \times B = \{(1,4), (1,5), (2,4), (2,5), (3,4), (3,5)\}$，

$$B \times A = \{(4,1), (4,2), (4,3), (5,1), (5,2), (5,3)\}$$

由该例能够看出，一般地，$A \times B \neq B \times A$。

3. 集合中元素的计数

计算集合中元素的数量，成为集合的计数。

摩根律：

设全集为 I，集合 A 的补集记为$\overline{A}$，即：$\overline{A}=\{x|x\in I \text{ 且 } x\notin A\}$。则：

1. $\overline{A\cup B}=\overline{A}\cap\overline{B}$

2. $\overline{A\cap B}=\overline{A}\cup\overline{B}$

推广：

设 $A_1,A_2,\cdots,A_n$ 是全集 I 的子集，则：

1. $\overline{A_1\cup A_2\cup\cdots\cup A_n}=\overline{A_1}\cap\overline{A_2}\cap\cdots\cap\overline{A_n}$

2. $\overline{A_1\cap A_2\cap\cdots\cap A_n}=\overline{A_1}\cup\overline{A_2}\cup\cdots\cup\overline{A_n}$

容斥原理(两个集合)：

$$|A\cup B|=|A|+|B|-|A\cap B|$$

这里，$|A|$表示集合 A 中元素的个数。

3 个集合时的容斥原理的形式为：

$$|A\cup B\cup C|=|A|+|B|+|C|-|A\cap B|-|A\cap C|-|B\cap C|+|A\cap B\cap C|$$

可以采用图 1-1 表示。

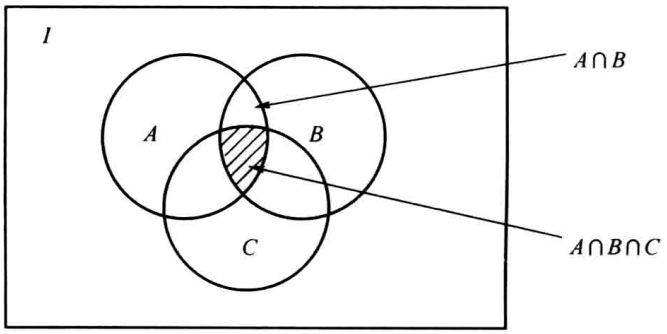

图 1-1　3 个集合时的容斥原理图示

一般地，n 个集合时的容斥原理形式如下。

容斥原理：

设：$A_1,A_2,\cdots,A_n$ 是有限集合，则

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

又：

$$|\overline{A}|=N-|A|$$

其中 N 是全集 I 中的元素个数，即：不属于 A 的元素的个数等于 N 减去 A 中元素的个数。

由上面的知识，可以推出容斥原理的另一种形式。

容斥原理：

$$|\overline{A}_1 \cap \overline{A}_2 \cap \cdots \cap \overline{A}_n| = |\overline{A_1 \cup A_2 \cup \cdots \cup A_n}|$$
$$= N - |A_1 \cup A_2 \cup \cdots \cup A_n| =$$
$$N - \sum_{i=1}^{n} |A_i| + \sum_{i=1}^{n} \sum_{j>i} |A_i \cap A_j| -$$
$$\sum_{i=1}^{n} \sum_{j>i} \sum_{k>j} |A_i \cap A_j \cap A_k| + \cdots +$$
$$(-1)^n |A_i \cap A_j \cap \cdots \cap A_n|$$

例　求 1～500 的正整数中能被 3 或 5 整除的数有多少？

解：

设：A 为 1～500 中能被 3 整除的数的集合，B 为 1～500 中能被 5 整除的数的集合，用符号$\lfloor X \rfloor$表示不超过 X 的最大整数。则有：

$$|A| = \left\lfloor \frac{500}{3} \right\rfloor = 166, \quad |B| = \left\lfloor \frac{500}{5} \right\rfloor = 100, \quad |A \cap B| = \left\lfloor \frac{500}{15} \right\rfloor = 33$$
$$|A \cup B| = |A| + |B| - |A \cap B| = 166 + 100 - 33 = 233$$

即：1～500 的正整数中能被 3 或 5 整除的数有 233 个。

例　求由 a,b,c,d 4 个字母构成的 n 位符号串，a,b,c 均至少出现一次的符号串的数目？

解：“均”的含义为“且”，可以考虑采用“$\cap$”形式的容斥原理。

设：A 为 n 位符号串中不出现 a 的字串的集合；

B 为 n 位符号串中不出现 b 的字串的集合；

C 为 n 位符号串中不出现 c 的字串的集合。

下面，只需求出$|\overline{A} \cap \overline{B} \cap \overline{C}|$。

$$N = 4^n, |A| = |B| = |C| = 3^n$$
$$|A \cap B| = 2^n = |A \cap C| = |B \cap C|$$
$$|A \cap B \cap C| = 1$$
$$|\overline{A} \cap \overline{B} \cap \overline{C}| = N - \{|A| + |B| + |C|\} + \{|A \cap B| + |B \cap C| + |A \cap C|\} - |A \cap B \cap C| =$$
$$4^n - 3 \cdot 3^n + 3 \cdot 2^n - 1$$

故，a,b,c 均至少出现一次的符号串的数目为 $4^n - 3 \cdot 3^n + 3 \cdot 2^n - 1$。

例　欧拉函数 $\varphi(n)$是指小于 n 且与 n 互素的数的个数。已知 n 分解式：

$n = p_1^{a_1} \cdot p_2^{a_2} \cdot \cdots \cdot p_k^{a_k}$，其中 $p_1, p_2, \cdots, p_k$ 均为质数，求 $\varphi(n) = ?$。

解：两个正整数 a,b 互素，指 a 与 b 除 1 之外没有公因子。如 $n=7$，小于且与 7 互素的数为：1,2,3,4,5,6，所以，$\varphi(7) = 6$。按照题意，所求的数均不为 $p_1, p_2, \cdots, p_k$ 的倍数。

设：A_1 表示 1～n 中是 p_1 的倍数的数的集合；

A_2 表示 1～n 中是 p_2 的倍数的数的集合；

…

A_n 表示 1～n 中是 p_n 的倍数的数的集合。

按照题意，只需求出：$|\overline{A}_1 \cap \overline{A}_2 \cap \cdots \cap \overline{A}_k|$

$$n=p_1^{a_1}\cdot p_2^{a_2}\cdot\cdots\cdot p_k^{a_k},|A_i|=\frac{n}{p_i},\quad i=1,2,\cdots,k$$

$$|A_i\cap A_j|=\frac{n}{p_i\cdot p_j},\quad i=1,2,\cdots,k,j\neq i$$

$$\varphi(n)=|\overline{A}_1\cap\overline{A}_2\cap\cdots\cap\overline{A}_k|=n-\left\{\frac{n}{p_1}+\frac{n}{p_2}+\cdots+\frac{n}{p_n}\right\}+$$

$$\left\{\frac{n}{p_1\cdot p_2}+\frac{n}{p_1\cdot p_3}+\cdots+\frac{n}{p_{k-1}\cdot p_k}\right\}-\cdots+(-1)^k\frac{n}{p_1p_2\cdots p_n}=$$

$$n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)$$

如：$n=60=2\times3\times5$，则 $\varphi(60)=60\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)=16$。

即小于 60 且与 60 互素的数有 16 个：1,7,11,13,17,19,23,29,31,37,41,43,47,49,53,59。

1.1.2 映射

1. 映射的概念

定义 设 A,B 是两个集合。若有一个对应法则 ϕ，使 $\forall a\in A$，通过 ϕ，存在唯一的元素 $b\in B$ 与之对应。则称 ϕ 是 A 到 B 的一个映射，b 称为 a 在映射 ϕ 下的像，记为 $b=\phi(a)$，a 称为 b 在映射 ϕ 下的一个逆像(原像)，A 称为 ϕ 的定义域，B 称 ϕ 为的值域。记作

$$\phi:A\to B;a\mapsto b=\phi(a),\forall a\in A;$$

一般情形下，将 A 换成集合的积 $A_1\times A_2\times\cdots\times A_n$，则有：

$$\phi:A_1\times A_2\times\cdots\times A_n\to B;$$

$$(a_1,a_2,\cdots,a_n)\mapsto b=\phi(a_1,a_2,\cdots,a_n),\quad\forall(a_1,a_2,\cdots,a_n)\in A_1\times A_2\times\cdots\times A_n。$$

例 设集合 $A_1=A_2=\cdots=A_n=B=R$，对 $\forall(a_1,a_2,\cdots,a_n)\in A_1\times A_2\times\cdots\times A_n$，规定：$\phi:A_1\times A_2\times\cdots\times A_n\to B;(a_1,a_2,\cdots,a_n)\mapsto b=a_1^2+\cdots+a_n^2$，则 ϕ 是一个 $A_1\times A_2\times\cdots\times A_n$ 到 B 的映射。

需要注意的是，一般情形中，$A_1,A_2,\cdots,A_n,B$ 中可以有相同的集合。当 $A_1,A_2,\cdots,A_n$ 不相同时，$A_1,A_2,\cdots,A_n$ 的次序不能调换。

例 设 $A=B=\mathbf{Z}^+$(正整数集)，则 $\phi:\mathbf{Z}^+\to\mathbf{Z}^+;a\mapsto a-1$ 不是一个映射。因为 $a=1$ 时，$\phi(1)=0\notin\mathbf{Z}^+$。

定义 设 ϕ_1,ϕ_2 是 A 到 B 的两个映射，若对 $\forall a\in A,\phi_1(a)=\phi_2(a)$，则称 ϕ_1,ϕ_2 是相等的。记作 $\phi_1=\phi_2$。

下面给出单射、满射、双射的概念，它们都是一些特殊的映射。

定义 设 ϕ 是集合 A 到 $\overline{A}$ 的一个映射。

若对 $\forall a,b\in A$，当 $a\neq b$ 时，有 $\phi(a)\neq\phi(b)$，则称 ϕ 是 A 到 $\overline{A}$ 的一个单射；

若对 $\forall\overline{a}\in\overline{A},\exists a\in A$，使得 $\phi(a)=\overline{a}$，则称 ϕ 是 A 到 $\overline{A}$ 的一个满射；

若 ϕ 是满射又是单射，则称 ϕ 是 A 到 $\overline{A}$ 的一个双射(一一映射)。

特别地，一个 A 到 A 间的映射 ϕ 称作 A 的一个变换。

设 $\phi: A \to B; a \mapsto b = \phi(a), \forall a \in A$，集合 C 是 A 的子集。则 ϕ 诱导一个从 C 到 B 的映射 ϕ_1。定义如下：$\forall a \in C$，令 $\phi_1(a) = \phi(a)$。此时，称映射 ϕ_1 为映射 ϕ 在集合 C 上的限制。

若 ϕ_1 是从集合 C 到 B 的映射，此时 $C \subseteq A$。设 $\phi: A \to B; a \mapsto b = \phi(a)$。如果 $\forall a \in C$，都有 $\phi_1(a) = \phi(a)$。则称映射 ϕ 是映射 ϕ_1 在集合 A 上的扩张。易知，限制是唯一的，扩张可能不是唯一的。

设 $f: A \to B; a \mapsto b = f(a); g: B \to C; b \mapsto c = g(b)$，则由映射 f 与 g 可以诱导出一个 $A \to C$ 的映射 h。h 的定义如下：$\forall a \in A, h(a) = g(f(a))$。并称映射 h 为映射 f 与 g 的合成。记为 $h = g \circ f$。可以采用图 1-2 表示。

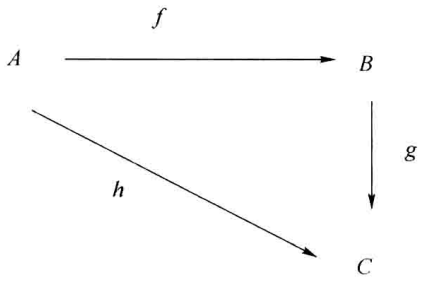

图 1-2　映射的合成

关于映射的合成，有如下结论。

定理　设 $f: A \to B; a \mapsto b = f(a); g: B \to C; b \mapsto c = g(b); h: C \to D; c \mapsto d = h(c)$，则有：$h \circ (g \circ f) = (h \circ g) \circ f$。

证明　易知，映射 $h \circ (g \circ f)$ 与 $(h \circ g) \circ f$ 都是 $A \to D$ 的映射。

又：　$\forall a \in A, (h \circ (g \circ f))(x) = h((g \circ f)(x)) = h(g(f(x)))$

$((h \circ g) \circ f)(x) = (h \circ g)(f(x)) = h(g(f(x)))$。

由映射相等的定义，知 $h \circ (g \circ f) = (h \circ g) \circ f$。

2. 映射的计数

下面，我们介绍两个有限集合之间的一些特殊映射的数量。

定理　设有限集合 A, B，且 $|A| = n, |B| = m$，则：

(1) 映射 $f: A \to B$ 的个数为 m^n；

(2) 当 $m \geqslant n$ 时，单射 $g: A \to B$ 的个数为 $m(m-1)(m-2)\cdots(m-n+1)$；

(3) 当 $m = n$ 时，双射 $g: A \to B$ 的个数为 $m!$。

证明　(1) 由映射的定义，有限集合 A 中的每一个元素在集合 B 中有唯一的像。将集合 A 中的元素记作 $a_1, a_2, \cdots, a_n$。元素 a_1 在集合 B 中的像有 m 种选择方法，元素 a_2 在集合 B 中的像有 m 种选择方法，……，元素 a_n 在集合 B 中的像也有 m 种选择方法。因此，映射 $f: A \to B$ 的个数为 m^n。

(2) 由单射的定义，有限集合 A 中的不同元素在集合 B 中有不同的像。因此，元素 a_1 在集合 B 中的像有 m 种选择方法，元素 a_2 在集合 B 中的像有 $m-1$ 种选择方法，……，元素 a_n 在集合 B 中的像也有 $m-n+1$ 种选择方法。因此，单射 $g: A \to B$ 的个数为 $m(m-1)(m-2)\cdots(m-n+1)$。

(3) 由双射的定义及(2),可知,双射 $g:A\to B$ 的个数为 $m!$

定理,设有限集合 A,B,且 $|A|=n,|B|=m$,当 $n\geqslant m$ 时,则满射 $f:A\to B$ 的个数为:

$$m^n-\binom{m}{1}(m-1)^n+\binom{m}{2}(m-2)^n-\cdots+(-1)^{m-1}\binom{m}{m-1}$$

证 设 $A=\{x_1,x_2,\cdots,x_n\},B=\{y_1,y_2,\cdots,y_m\}$。设 A_i 表示 A 到 B 的一些映射的集合,满足 y_i 不是 A 中任何一个元素的像。即:$A_i=\{f:A\to B\mid y_i\notin \mathrm{Im}\, f\},(i=1,2,\cdots,m)$。

依题意,只需求出:$|\overline{A_1}\cap\overline{A_2}\cap\cdots\cap\overline{A_m}|$。

由容斥原理,

$$|\overline{A}_1\cap\overline{A}_2\cap\cdots\cap\overline{A}_n|=N-\sum_{i=1}^{n}|A_i|+\sum_{i=1}^{n}\sum_{j>i}|A_i\cap A_j|-$$
$$\sum_{i=1}^{n}\sum_{j>i}\sum_{k>j}|A_i\cap A_j\cap A_k|+\cdots+$$
$$(-1)^n|A_i\cap A_j\cap\cdots\cap A_n|$$

此时,$N=m^n$,$|A_i|=(m-1)^n$,$|A_i\cap A_j|=(m-2)^n$。

一般地,$|A_{i_1}\cap A_{i_2}\cap\cdots\cap A_{i_l}|=(m-l)^n$,则:

$$|\overline{A_1}\cap\overline{A_2}\cap\cdots\cap\overline{A_m}|=m^n-\binom{m}{1}(m-1)^n+\binom{m}{2}(m-2)^n-\cdots+(-1)^{m-1}\binom{m}{m-1}$$

在本节中,我们复习了集合与映射的一些概念。这些概念包括:集合的交、并、笛卡儿乘积等运算,满射、单射、双射的定义,映射的扩张与限制。同时,我们还学习了集合中元素的计数方法,即容斥原理。应用容斥原理,我们还可以对两个有限集合之间的映射个数进行计数。

1.2 运算与同态映射

在数学概念上,映射是运算的基础。运算能够满足一些运算律。在本节中,我们将学习二元运算的概念,及运算满足的结合律、交换律、分配律。进一步,我们还将学习同态映射的知识。

1.2.1 运算

我们首先给出代数运算的概念。

定义 设 A,B,D 是 3 个非空集合。从 $A\times B$ 到 D 的映射称作一个 $A\times B$ 到 D 的二元代数运算;当 $A=B=D$ 时,$A\times A$ 到 A 的映射简称 A 上的代数运算或二元运算。

一个代数运算可以用$\circ$表示,并将(a,b)在$\circ$下的像记作 $a\circ b$。若$\circ$是 A 上的代数运算 $\Leftrightarrow\forall a,b\in A,a\circ b\in A$。

设:$A=\{a_1,a_2,\cdots,a_n\},B=\{b_1,b_2,\cdots,b_m\}$,则 $A\times B$ 到 D 的一个代数运算 $a_i\circ b_j=d_{ij}$ 可以表示为

∘	b_1	b_2	…	b_m
a_1	d_{11}	d_{12}	…	d_{1m}
a_2	d_{21}	d_{22}	…	d_{2m}
⋮	⋮	⋮		⋮
a_n	d_{n1}	d_{n2}	…	d_{nm}

定义　设 A 是一个非空集合，n 是自然数，$A\times A\times\cdots\times A$（$n$ 个 A 的笛卡儿积）到 A 的映射 f，称为 A 的一个 n 元运算。

例　设 $\mathbf{Q}^*$ 为非 0 有理数的集合，每个非 0 有理数的倒数还是有理数，故倒数运算是 $\mathbf{Q}^*$ 的一元运算。此时，

$$f:\mathbf{Q}^*\to\mathbf{Q}^*,\quad f(a)=\frac{1}{a},\quad \forall a\in\mathbf{Q}^*$$

一般地，一个二元运算可能会满足一些运算律，如：结合律、交换律、分配律。下面，依次介绍这些概念。

定义　设∘是集合 A 的一个代数运算。如果对任意 $a,b,c\in A$，有 $(a\circ b)\circ c=a\circ(b\circ c)$，则称代数运算∘适合结合律，并且统一记成 $a\circ b\circ c$。

需要注意的是，对于 A 中 n 个元素 $a_1,a_2,\cdots,a_n$，当元素的排列顺序不变时（如按下标的自然顺序），可以有 $\dfrac{(2n-2)!}{n!\ (n-1)!}=N$ 种不同的加括号方法。对于不同的加括号的方法，其计算结果未必相同。如 $n=3$，$N=2$，即有 2 种加括号的方法：$(a\circ b)\circ c$，$a\circ(b\circ c)$。而 $n=4$，$N=5$，即有 5 种加括号方法：$(a_1\circ a_2)\circ(a_3\circ a_4)$，$((a_1\circ a_2)\circ a_3)\circ a_4$，$(a_1\circ(a_2\circ a_3))\circ a_4$，$a_1\circ((a_2\circ a_3)\circ a_4)$，$a_1\circ(a_2\circ(a_3\circ a_4))$。不妨用 $\pi_1(a_1\circ a_2\circ\cdots\circ a_n)$，$\pi_2(a_1\circ a_2\circ\cdots\circ a_n)$，$\cdots$，$\pi_N(a_1\circ a_2\circ\cdots\circ a_n)$ 来表示这些加括号方法。

定理　对于 A 中 n 个元素 $a_1,a_2,\cdots,a_n$，共有 $\dfrac{(2n-2)!}{n!\ (n-1)!}$ 种不同的加括号方法。

证明　用 $d(n)$ 表示 n 个元素 $a_1,a_2,\cdots,a_n$ 的各种不同加括号方法的数量。知：$d(1)=1,d(2)=1,d(3)=2$。经过分析，可知 $d(1),d(2),\cdots,d(n)$ 满足：

$$d(n)=d(n-1)d(1)+d(n-2)d(2)+\cdots+d(1)d(n-1)$$

采用组合数学中母函数的方法求 $d(n)$。设序列 $d(1),d(2),\cdots,d(n),\cdots$ 对应的母函数为：

$$f(x)=d(1)x+d(2)x^2+\cdots d(n)x^n+\cdots$$

计算可得：

$$f(x)^2=d(1)d(1)x^2+[d(2)d(1)+d(1)d(2)]x^3+\cdots[d(n-1)d(1)+d(n-2)d(2)+\cdots+d(1)d(n-1)]x^n+\cdots$$

将上式代入，得：　$f(x)^2=d(2)x^2+d(3)x^3+\cdots+d(n)x^n+\cdots$

故有：　$f(x)^2-f(x)+x=0$。

解得：$$f(x)=\frac{1\pm\sqrt{1-4x}}{2}。$$

考虑 $f(x)=\frac{1+\sqrt{1-4x}}{2}$。代入 $x=0$，得 $f(0)=1$。而由 $f(x)=d(1)x+d(2)x^2+\cdots d(n)x^n+\cdots$，得：$f(0)=0$。故 $f(x)=\frac{1+\sqrt{1-4x}}{2}$ 为增根。所以 $f(x)=\frac{1-\sqrt{1-4x}}{2}$。

利用展开式：$(1+x)^m=1+mx+\frac{m(m-1)}{2!}x^2+\cdots+\frac{m(m-1)(m-2)\cdots(m-n+1)}{n!}+\cdots$

可得：$f(x)=\frac{1-\sqrt{1-4x}}{2}=\sum_{n=1}^{\infty}\frac{1\cdot3\cdot5\cdot\cdots\cdot(2n-3)}{n!}\cdot2^{n-1}x^n$。

因此，由 $f(x)$ 的表达式：$f(x)=d(1)x+d(2)x^2+\cdots d(n)x^n+\cdots$，知：$d(n)=\frac{1\cdot3\cdot5\cdot\cdots\cdot(2n-3)}{n!}2^{n-1}$。

又：

$$\begin{aligned}(2n-2)!&=(2n-2)(2n-3)(2n-4)\cdot\cdots\cdot6\cdot5\cdot4\cdot3\cdot2\cdot1\\&=[1\cdot3\cdot5\cdot\cdots\cdot(2n-3)]\cdot[(2n-2)(2n-4)\cdot\cdots\cdot6\cdot4\cdot2]\\&=[1\cdot3\cdot5\cdot\cdots\cdot(2n-3)]\cdot2^{n-1}(n-1)!\end{aligned}$$

故：$d(n)=\frac{(2n-2)!}{n!\ (n-1)!}$。

定理 设集合 A 的一个代数运算$\circ$为，当$\circ$适合结合律时，则对任意 $a_1,a_2,\cdots,a_n\in A$，$n\geqslant2$，所有的 $\pi(a_1\circ a_2\circ\cdots\circ a_n)$ 都相等，并将其结果统一记为：$a_1\circ a_2\circ\cdots\circ a_n$。

证 用数学归纳法证明任何一种加括号方法计算所得结果都等于按自然顺序依次加括号计算所得的结果〔即：$(\cdots(a_1\circ a_2)\circ\cdots)\circ a_n$〕。

(1) $n=3$，$N=2$，由已知条件，知定理成立。

(2) 假定对 $k<n$ 时，定理成立，下面证明 n 的情形。

n 个元素的任意一种计算方法，最后一步总是 $u\circ v$ 的形式，其中 u 表示 m 个元素 $a_1,a_2,\cdots,a_m$ 的计算结果，而 v 表示 $n-m$ 个元素 $a_{m+1},a_{m+2},\cdots,a_n$ 的计算结果，$1\leqslant m<n$。

由归纳假设，于是有 $u=(\cdots(a_1\circ a_2)\circ\cdots)\circ a_m$，$v=(\cdots(a_{m+1}\circ a_{m+2})\circ\cdots)\circ a_n$。因此

$$u\circ v=[(\cdots(a_1\circ a_2)\circ\cdots)\circ a_m][(\cdots(a_{m+1}\circ a_{m+2})\circ\cdots)\circ a_n]。$$

若将 $((\cdots(a_{m+1}\circ a_{m+2})\circ\cdots\circ)a_{n-1})$ 看成 v_1，由结合律，可以得到：

$$\begin{aligned}u\circ v&=[(\cdots(a_1\circ a_2)\circ\cdots\circ)a_m\circ((\cdots(a_{m+1}\circ a_{m+2})\circ\cdots\circ)a_{n-1})]\circ a_n\\&\xlongequal{\text{归纳假设}}((\cdots(a_1\circ a_2)\circ\cdots)\circ a_{n-1})\circ a_n\end{aligned}$$

故得证。

定义 设$\circ$是 $A\times A$ 到 D 的代数运算。如果 $\forall a,b\in A$，有 $a\circ b=b\circ a$ 成立，则称运算$\circ$满足交换律。

定理 假设一个集合 A 的代数运算$\circ$同时适合结合律与交换律，那么在 $a_1\circ a_2\circ\cdots a_n$ 中，元素的次序可以互换。证明略。

设$\odot:B\times A\to A$ 是代数运算，$\oplus:A\times A\to A$ 是 A 上的一个代数运算。显然，对任意 $b\in B$，$a_1,a_2\in A$，$b\odot(a_1\oplus a_2)$ 和 $(b\odot a_1)\oplus(b\odot a_2)$ 均有意义，但是二者未必相等。