北京大学计算机科学与技术系教材

代数结构与组合数学

离散数学三分册

▶ 屈婉玲 编著

北京大学出版社
PEKING UNIVERSITY PRESS

北京大学计算机科学与技术系教材　G605

代数结构与组合数学

（离散数学三分册）

屈婉玲　编著

北 京 大 学 出 版 社
北　　京

内 容 提 要

本书是离散数学的第三分册——代数结构与组合数学。全书由两部分组成。第一部分为代数结构，介绍代数系统的基本概念和几个重要的代数系统，包括半群、独异点、群、环、域、格与布尔代数；第二部分为组合数学，介绍组合存在性、组合计数、组合设计与编码以及组合最优化。全书体系严谨、内容丰富、配有大量的例题和习题，并与计算机科学的理论及实践密切结合。它不仅适用于计算机及相关专业的本科生或研究生，也可供计算机专业的科技人员使用或参考。

图书在版编目(CIP)数据

离散数学　三分册：代数结构与组合数学/屈婉玲编著. —北京：北京大学出版社，1998.2

ISBN 7-301-03588-8

Ⅰ.离…　Ⅱ.屈…　Ⅲ.①代数-高等学校-教材②组合数学-高等学校-教材　Ⅳ.015

书　　　名：代数结构与组合数学　离散数学三分册
著作责任者：屈婉玲
责 任 编 辑：沈承凤
标 准 书 号：ISBN 7-301-03588-8/TP・378
出　版　者：北京大学出版社
地　　　址：北京市海淀区中关村北京大学校内　100871
电　　　话：出版部 62752015　发行部 62559712　编辑部 62752032
排　印　者：国防科工委印刷厂印刷
发　行　者：北京大学出版社
经　销　者：新华书店
850×1168　32 开本　12.75 印张　331 千字
1998 年 2 月第一版　1998 年 2 月第一次印刷
定　　　价：21.00 元

前　言

离散数学是研究离散量的结构及相互关系的数学学科，是现代数学的一个重要分支，它在计算机科学与技术领域中有着广泛的应用。因此，离散数学是计算机专业学生的一门极为重要的专业基础课程。通过本课程的学习，可以使学生掌握处理离散结构的描述工具与方法，并能培养学生的抽象思维和严格的逻辑推理能力。

一般说来，离散数学包含数理逻辑、集合论、图论、代数结构、组合数学等内容。我们将以上内容分成三个分册出版：第一分册为数理逻辑，第二分册为集合论与图论，第三分册为代数结构与组合数学。本套教材体系严谨、内容丰富、配有大量的例题和习题，并与计算机科学的理论及实践紧密结合。它不仅适用于计算机及相关专业的本科生或研究生，也可供计算机专业的科技人员使用或参考。

本书为第三分册，其中第一章到第五章为代数结构部分，包括代数系统、半群与独异点、群、环与域、格与布尔代数。第六章到第十一章为组合数学部分，包括组合存在性定理、基本的计数公式、组合计数方法、组合计数定理、组合设计与编码、组合最优化问题等。

作者在编写本书过程中参阅了多种离散数学教材及有关资料，在此向作者们表示衷心的感谢。

在这里，我们还要特别感谢北大出版社、北大教学行政处以及计算机系领导对本套教材出版的大力支持与帮助。

最后，我们诚恳地期待读者对本套教材提出宝贵意见。

作　者

1996 年 12 月于北大

目　　录

第一篇　代数结构

此为试读,需要完整PDF请访问: www.ertongbook.com

第二篇　组合数学

第一篇
代 数 结 构

第一章 代数系统

§1.1 二元运算及其性质

定义 1.1 设 A 为集合，函数 $f: A\times A\rightarrow A$ 称为 A 上的一个**二元代数运算**，简称为**二元运算**．

对任意的 $x,y\in A$，如果 $f(\langle x,y\rangle)=c$，则称 x 和 y 是**运算数**，c 是 x 和 y 的**运算结果**．

【例 1.1】

(1) 普通的加法和乘法是自然数集 N 上的二元运算，但减法和除法不是，因为 2 和 3 都是自然数，但 $2-3\notin N$，$2\div 3\notin N$. 此外，0 虽然是自然数，但 0 不可以做除数．

(2) 普通的加法，减法和乘法是整数集 Z，有理数集 Q，实数集 R 和复数集 C 上的二元运算，而除法不是这些集合上的二元运算．

(3) 普通的乘法和除法是非零实数集 R^* 上的二元运算，但加法和减法不是 R^* 上的运算．因为对于任意的 $x\in R^*$ 有 $x+(-x)=0$，$x-x=0$，而 $0\notin R^*$.

(4) 令 $M_n(R)$ 是 n 阶实矩阵的集合($n\geqslant 2$)，即

$$M_n(R)=\left\{\left.\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ & \cdots & & \\ a_{n1} & a_{n2} & \cdots & a_{nn}\end{pmatrix}\right| a_{ij}\in R\right\},$$

则矩阵加法和乘法是 $M_n(R)$ 上的二元运算.

(5) $P(B)$ 是集合 B 的幂集，则集合的并、交、相对补和对称差运算都是 $P(B)$ 上的二元运算.

(6) 令 $R(B)$ 表示集合 B 上的所有二元关系的集合，则关系的合成运算是 $R(B)$ 上的二元运算.

(7) $A^A = \{f \mid f; A \to A\}$，则函数的合成运算是 A^A 上的二元运算.

可以把二元运算的概念推广到 n 元运算.

定义 1.2 设 A 为集合，n 为正整数，$A^n = \underbrace{A \times A \times \cdots \times A}_{n个}$表示 A 的 n 阶笛卡儿积. 函数 f：$A^n \to A$ 称为 A 上的一个 **n 元代数运算**，简称为 **n 元运算**. 若 f 是 A 上的运算，也可以称 A 在运算 f 下是**封闭的**.

【例 1.2】

(1) 求一个数的相反数是整数集 Z，有理数集 Q，实数集 R 上的一元运算.

(2) 求一个 n 阶($n \geqslant 2$) 实矩阵的转置矩阵是 $M_n(R)$ 上的一元运算，而求逆阵不是 $M_n(R)$ 上的一元运算.

(3) 如果令 B 为全集，则集合的绝对补运算 $\sim$ 是 $P(B)$ 上的一元运算.

(4) 令 $R(B)$ 为集合 B 上的所有二元关系的集合，则关系的逆运算是 $R(B)$ 上的一元运算.

(5) 设 A 为集合，S 是所有从 A 到 A 的双射函数构成的集合，则求反函数的运算是 S 上的一元运算.

(6) R 为实数集，令 f：$R^n \to R$，$\forall \langle x_1, x_2, \cdots, x_n \rangle \in R^n$ 有 $f(\langle x_1, x_2, \cdots, x_n \rangle) = x_3$，则 f 是 R 上的 n 元运算. 它就是求一个 n 维向量的第三个分量的运算.

为了书写的方便，可以用**算符**来表示 n 元运算. 常用的算符有$\circ$，$*$，$\cdot$，$\square$，$\vartriangle$，…. 如果用算符$\circ$表示例 1.2(6) 中的 n 元运算，则有

$$\circ(x_1, x_2, \cdots, x_n) = x_3.$$

当$\circ$表示二元运算时，常将算符$\circ$放在两个运算数之间，把$\circ(x_1, x_2)$ 记为 $x_1 \circ x_2$. 而对于一元运算$\vartriangle$，通常将后面运算数 x 的括号省略，简记为 $\vartriangle x$.

此为试读，需要完整PDF请访问：www.ertongbook.com

当 A 为有穷集时，A 上的一元和二元运算可以用**运算表**来给出. 设 $A=\{a_1,a_2,\cdots,a_n\}$，$\circ$ 和 $\triangle$ 分别为 A 上的二元和一元运算，它们的运算表给在表 1.1.

表 1.1

$\circ$	a_1	a_2	$\cdots$	a_n
a_1	$a_1\circ a_1$	$a_1\circ a_2$	$\cdots$	$a_1\circ a_n$
a_2	$a_2\circ a_1$	$a_2\circ a_2$	$\cdots$	$a_2\circ a_n$
$\vdots$				
a_n	$a_n\circ a_1$	$a_n\circ a_2$	$\cdots$	$a_n\circ a_n$

$\triangle$	$\triangle a_i$
a_1	$\triangle a_1$
a_2	$\triangle a_2$
$\vdots$	$\vdots$
a_n	$\triangle a_n$

【例 1.3】 设 $B=\{1,2\}$，$P(B)$ 上的二元运算 $\oplus$ 和一元运算 $\sim$ 的运算表如表 1.2 所示。

表 1.2

$\oplus$	$\varnothing$	$\{1\}$	$\{2\}$	$\{1,2\}$
$\varnothing$	$\varnothing$	$\{1\}$	$\{2\}$	$\{1,2\}$
$\{1\}$	$\{1\}$	$\varnothing$	$\{1,2\}$	$\{2\}$
$\{2\}$	$\{2\}$	$\{1,2\}$	$\varnothing$	$\{1\}$
$\{1,2\}$	$\{1,2\}$	$\{2\}$	$\{1\}$	$\varnothing$

$\sim$	
$\varnothing$	$\{1,2\}$
$\{1\}$	$\{2\}$
$\{2\}$	$\{1\}$
$\{1,2\}$	$\varnothing$

下面讨论二元运算的性质.

定义 1.3 设 A 为集合，$\circ$ 为 A 上的二元运算.

(1) 若 $\forall x,y\in A$ 有 $x\circ y=y\circ x$，则称 $\circ$ 运算在 A 上是**可交换的**，也称 $\circ$ 运算在 A 上满足**交换律**.

(2) 若 $\forall x,y,z\in A$ 有 $(x\circ y)\circ z=x\circ(y\circ z)$，则称 $\circ$ 运算在 A 上是**可结合的**，也称 $\circ$ 运算在 A 上满足**结合律**.

(3) 若 $\forall x\in A$ 有 $x\circ x=x$，则称 $\circ$ 运算在 A 上是**幂等的**，也称 $\circ$ 运算在 A 上满足**幂等律**.

【例 1.4】

(1) 实数集 R 上的加法和乘法是可交换的、可结合的，而减法不满足交换律和结合律.

(2) $M_n(R)(n \geqslant 2)$ 上的矩阵加法是可交换的、可结合的，而矩阵乘法是可结合的，但不是可交换的.

(3) $P(B)$ 上的并、交，对称差运算是可交换的、可结合的.

(4) A^A 上的函数合成运算是可结合的，但一般不是可交换的.

以上所有的运算中只有集合的并和交运算满足幂等律，其它的运算一般说来都不是幂等的.

某些二元运算$\circ$尽管不满足幂等律，但存在着某些元素 x 满足 $x \circ x = x$，称这样的 x 是关于$\circ$运算的**幂等元**. 例如实数集中，0 是加法的幂等元，0 和 1 是乘法的幂等元. 不难看出，如果集合中的所有元素都是关于$\circ$运算的幂等元，则$\circ$运算满足幂等律.

定义 1.4 设$\circ$为 A 上的二元运算，如果对于 A 中任取的 n 个元素 $a_1, a_2, \cdots, a_n, n \geqslant 3$，在 $a_1 \circ a_2 \circ \cdots \circ a_n$ 中任意加括号所得的运算结果都相等，则称$\circ$运算在 A 上是**广义可结合的**，或称$\circ$运算在 A 上适合**广义结合律**.

对于适合广义结合律的二元运算$\circ$，通常用 $a_1 \circ a_2 \circ \cdots \circ a_n$ 来表示 $a_1, a_2, \cdots, a_n$ 的运算结果.

定理 1.1 设$\circ$为 A 上的二元运算，若$\circ$运算适合结合律，则$\circ$运算适合广义结合律.

证 任取 A 中 n 个元素 $a_1, a_2, \cdots, a_n$，令

$$b = ((\cdots(((a_1 \circ a_2) \circ a_3) \circ a_4) \circ \cdots) \circ a_{n-1}) \circ a_n.$$

我们只须证明在 $a_1 \circ a_2 \circ \cdots \circ a_{n-1} \circ a_n$ 中任意加括号所得的运算结果都等于 b. 施归纳于 n.

$n = 3$，由结合律有 $(a_1 \circ a_2) \circ a_3 = a_1 \circ (a_2 \circ a_3)$.

假设小于 n 时结论为真，对于 $a_1 \circ a_2 \circ \cdots \circ a_{n-1} \circ a_n$ 任意加括号后所得的运算结果是 c，且最后一次运算是在 α 和 β 两部分之间进行的. 根据归纳假设有 $\beta = (\cdots) \circ a_n$，代入 c 得

$$c = \alpha \circ ((\cdots) \circ a_n).$$

由结合律 $c = (\alpha \circ (\cdots)) \circ a_n$. 再使用归纳假设得

$$\alpha\circ(\cdots) = (\cdots((a_1\circ a_2)\circ a_3)\circ\cdots)\circ a_{n-1}.$$

所以有

$$c = ((\cdots((a_1\circ a_2)\circ a_3)\circ\cdots)\circ a_{n-1})\circ a_n. \quad \blacksquare$$

以上讨论的运算性质只涉及一个二元运算. 下面考虑与两个二元运算相关的性质,即分配律和吸收律.

定义 1.5　设$\circ$和 $*$ 是集合 A 上的二元运算.

(1) 若$\forall x,y,z\in A$ 有 $x\circ(y*z)=(x\circ y)*(x\circ z)$ 和 $(y*z)\circ x=(y\circ x)*(z\circ x)$ 成立,则称$\circ$运算对 $*$ 运算是**可分配的**,或称$\circ$运算对 $*$ 运算满足**分配律**.

(2) 若$\circ$和 $*$ 满足交换律且 $\forall x,y\in A$ 有 $x\circ(x*y)=x$ 和 $x*(x\circ y)=x$ 成立,则称$\circ$和 $*$ 运算是**可吸收的**,或称$\circ$和 $*$ 运算满足**吸收律**.

【例 1.5】

(1) 实数集 R 上的乘法对加法是可分配的,但加法对乘法不满足分配律.

(2) n 阶($n\geqslant 2$)实矩阵集合 $M_n(R)$ 上的矩阵乘法对矩阵加法是可分配的.

(3) 幂集 $P(B)$ 上的并和交是互相可分配的,并且满足吸收律.

除了算律以外,还有一些和二元运算有关的特异元素,如单位元、零元、逆元等.

定义 1.6　设$\circ$为集合 A 上的二元运算.

(1) 若存在$e_l\in A$(或$e_r\in A$)使得$\forall x\in A$都有$e_l\circ x=x$(或$x\circ e_r=x$),则称 e_l(或 e_r)是 A 中关于$\circ$运算的**左(或右)单位元**. 若 $e\in A$ 关于$\circ$运算既为左单位元又为右单位元,则称 e 为 A 中关于$\circ$运算的**单位元**①.

(2) 若存在$\theta_l\in A$(或$\theta_r\in A$)使得$\forall x\in A$都有$\theta_l\circ x=\theta_l$(或$x\circ\theta_r$

---

① 在有的书中称单位元为幺元.

$= \theta_r$)，则称 θ_l（或 θ_r）是 A 中关于$\circ$运算的**左**（或**右**）**零元**. 若 $\theta \in A$ 关于$\circ$运算既为左零元又为右零元，则称 θ 为 A 中关于$\circ$运算的**零元**.

【例 1.6】

(1) 整数集 Z 中关于加法的单位元是 0，没有零元，关于乘法的单位元是 1，零元是 0.

(2) n 阶（$n \geqslant 2$）实矩阵集合 $M_n(R)$ 中关于矩阵加法的单位元是 n 阶全 0 矩阵，没有零元，而关于矩阵乘法的单位元是 n 阶单位矩阵，零元是 n 阶全 0 矩阵.

(3) 幂集 $P(B)$ 中关于并运算的单位元是$\varnothing$，零元是 B，而关于交运算的单位元是 B，零元是$\varnothing$.

(4) A^A 中关于函数合成运算的单位元是 A 上的恒等函数 I_A，$I_A: A \to A, I_A(x) = x, \forall x \in A$. 没有零元.

(5) $A = \{a_1, a_2, \cdots, a_n\}$，$n \geqslant 2$. 定义 A 上的二元运算$\circ$，$\forall a_i, a_j \in A$ 有 $a_i \circ a_j = a_i$. 则 A 中的每个元素都是$\circ$运算的右单位元，但没有左单位元，所以 A 中没有单位元. 同样地，A 中每个元素都是$\circ$运算的左零元，但没有零元.

关于单位元和零元存在以下定理.

定理 1.2 设$\circ$是集合 A 上的二元运算，若存在 $e_l \in A$ 和 $e_r \in A$ 满足 $\forall x \in A$ 有 $e_l \circ x = x$ 和 $x \circ e_r = x$，则 $e_l = e_r = e$，且 e 就是 A 中关于$\circ$运算的唯一的单位元.

证 因为 e_r 是右单位元，所以有 $e_l = e_l \circ e_r$，又由于 e_l 是左单位元，因此有 $e_l \circ e_r = e_r$. 由这两个等式可得 $e_l = e_r$，把这个单位元记作 e. 假设关于$\circ$运算存在另一个单位元 e'，则有

$$e' = e' \circ e = e,$$

所以 e 是关于$\circ$运算的唯一的单位元. ∎

定理 1.3 设$\circ$为集合 A 上的二元运算，若存在 $\theta_l \in A$ 和 $\theta_r \in A$ 使得 $\forall x \in A$ 有 $\theta_l \circ x = \theta_l$ 和 $x \circ \theta_r = \theta_r$，则 $\theta_l = \theta_r = \theta$，且 θ 是 A 中关于$\circ$运算的唯一的零元.

证明留作练习.

定理 1.4　设集合 A 至少含有两个元素，e 和 θ 分别为 A 中关于 $\circ$ 运算的单位元和零元，则 $e \neq \theta$.

证　假设 $e = \theta$，则 $\forall x \in A$ 有

$$x = x \circ e = x \circ \theta = \theta,$$

与 A 中至少含有两个元素矛盾. ∎

定义 1.7　设 $\circ$ 是集合 A 上的二元运算，$e \in A$ 是关于 $\circ$ 运算的单位元. 对于 $x \in A$ 若存在 $y_l \in A$(或 $y_r \in A$) 使得 $y_l \circ x = e$(或 $x \circ y_r = e$) 则称 y_l(或 y_r) 是 x 关于 $\circ$ 运算的**左**(或**右**) **逆元**. 若 $y \in A$ 既是 x 关于 $\circ$ 运算的左逆元，又是 x 关于 $\circ$ 运算的右逆元，则称 y 是 x 关于 $\circ$ 运算的**逆元**.

【例 1.7】

(1) 在整数集 Z 中，任何整数 n 关于加法的逆元是 $-n$. 关于乘法只有 1 和 -1 存在逆元，就是它们自己，其它整数没有乘法逆元.

(2) n 阶($n \geqslant 2$) 实矩阵集合 $M_n(R)$ 中任何矩阵 M 的加法逆元为 $-M$. 而对于矩阵乘法只有实可逆矩阵 M 存在乘法逆元 M^{-1}.

(3) 幂集 $P(B)$ 中关于并运算只有空集 $\varnothing$ 有逆元，就是 $\varnothing$ 本身，B 的其它子集没有逆元.

关于逆元存在以下定理.

定理 1.5　设 $\circ$ 为集合 A 上可结合的二元运算且单位元为 e. 对于 $x \in A$ 若存在 y_l 和 $y_r \in A$ 使得 $y_l \circ x = e$ 和 $x \circ y_r = e$，则 $y_l = y_r = y$，且 y 是 x 关于 $\circ$ 运算的唯一的逆元.

证　$y_l = y_l \circ e = y_l \circ (x \circ y_r) = (y_l \circ x) \circ y_r = e \circ y_r = y_r$.

令 $y = y_l = y_r$，则 y 是 x 关于 $\circ$ 运算的逆元.

假设 y' 也是 x 关于 $\circ$ 运算的逆元，则有

$$y' = y' \circ e = y' \circ (x \circ y) = (y' \circ x) \circ y = e \circ y = y.$$

所以 y 是 x 关于 $\circ$ 运算的唯一的逆元. ∎

根据这个定理，对于任意 $x \in A$，如果存在关于二元运算的逆

元，则是唯一的．可将这个唯一的逆元记作 x^{-1}．

【例1.8】 设$\circ$为实数集 R 上的二元运算，$\forall x \in R$ 有 $x \circ y = x + y - 2xy$，说明$\circ$运算是否为可交换的、可结合的、幂等的，然后确定关于$\circ$运算的单位元，零元和所有可逆元素的逆元．

解 $\circ$运算是可交换的、可结合的，但不是幂等的．

假设 e 和 θ 分别为$\circ$运算的单位元和零元，则 $\forall x \in R$ 有

$$x + e - 2xe = x \text{ 和 } x + \theta - 2x\theta = \theta,$$

即

$$(1 - 2x)e = 0 \text{ 和 } x(1 - 2\theta) = 0.$$

要使这些等式对一切实数 x 都成立，只有 $e = 0$ 和 $\theta = \frac{1}{2}$．

任取 $x \in R$，设 y 为 x 关于$\circ$运算的逆元，则有 $x + y - 2xy = 0$，从而解得 $y = \frac{-x}{1-2x}\ (x \neq \frac{1}{2})$．

通过上面的分析可知 0 是$\circ$运算的单位元，$\frac{1}{2}$ 是$\circ$运算的零元，$\forall x \in R(x \neq \frac{1}{2})$ 有 $x^{-1} = \frac{-x}{1-2x}$．

【例1.9】 设 A 上的二元运算$\circ$由表1.3所确定．求 A 中关于$\circ$运算的单位元、零元和所有可逆元素的逆元．

表 1.3

$\circ$	a	b	c	d
a	a	b	c	d
b	b	a	d	d
c	c	a	a	d
d	d	d	d	d

解 由表1.3不难看出 a 是$\circ$运算的单位元，d 是$\circ$运算的零元．a,b,c 为可逆元素，且 $a^{-1} = a,\ b^{-1} = b,\ c^{-1} = c$．

下面给出关于二元运算的最后一条算律 —— 消去律．

定义1.8 设$\circ$为集合 A 上的二元运算，若对于任意的 $a,b,c \in A$（a 不是$\circ$运算的零元）都有

$$a \circ b = a \circ c \Rightarrow b = c,$$

$$b \circ a = c \circ a \Rightarrow b = c.$$

则称$\circ$运算在 A 中适合**消去律**．

此为试读，需要完整PDF请访问：www.ertongbook.com