



普通高等教育“十一五”国家级规划教材

国家精品课程主讲教材

# 离散数学

屈婉玲 耿素云 张立昂

原书代数系统部分，仅供南京大学计算机科学与技术系、人工智能学院离散数学课程内部使用

请注意保护原作者版权



高等教育出版社  
Higher Education Press

普通高等教育“十一五”国家级规划教材

国家精品课程主讲教材

# 离散数学

屈婉玲 耿素云 张立昂

高等教育出版社

## 内容提要

本书起源于高等教育出版社 1998 年出版的《离散数学》,是教育部高等学校“九五”规划教材,2004 年作为“十五”规划教材出版了修订版。作为“十一五”规划教材,根据教育部计算机科学与技术专业教学指导委员会提出的《计算机科学与技术专业规范》(CCC2005)的教学要求,本教材对内容进行了较多的调整与更新。

本书分为数理逻辑、集合论、代数结构、组合数学、图论、初等数论等六个部分。全书既有严谨的、系统的理论阐述,也有丰富的、面向计算机科学技术发展的应用实例,同时选配了大量的典型例题与练习。各章内容按照模块化组织,可以适应不同的教学要求。与本书配套的电子教案和习题辅导用书随后将陆续推出。

本书可以作为普通高等学校计算机科学与技术专业不同方向的本科生的离散数学教材,也可以供其他专业学生和科技人员阅读参考。

## 图书在版编目(CIP)数据

离散数学 / 屈婉玲,耿素云,张立昂. —北京:高等教育出版社,2008.3

ISBN 978 - 7 - 04 - 023125 - 0

I. 离… II. ①屈…②耿…③张… III. 离散数学 - 高等学校 - 教材 IV. O158

中国版本图书馆 CIP 数据核字 (2008) 第 003713 号

策划编辑 刘 艳 责任编辑 张耀明 封面设计 于文燕 版式设计 马敬茹  
责任校对 王 超 责任印制 宋克学

出版发行 高等教育出版社  
社 址 北京市西城区德外大街 4 号  
邮政编码 100011  
总 机 010 - 58581000

经 销 蓝色畅想图书发行有限公司  
印 刷 高等教育出版社印刷厂

开 本 787 × 1092 1/16  
印 张 24.5  
字 数 550 000

购书热线 010 - 58581118  
免费咨询 800 - 810 - 0598  
网 址 <http://www.hep.edu.cn>  
<http://www.hep.com.cn>  
网上订购 <http://www.landaco.com>  
<http://www.landaco.com.cn>  
畅想教育 <http://www.widedu.com>

版 次 2008 年 3 月第 1 版  
印 次 2008 年 3 月第 1 次印刷  
定 价 30.50 元

本书如有缺页、倒页、脱页等质量问题,请到所购图书销售部门联系调换。

版权所有 侵权必究

物料号 23125 - 00

## 第九章 代数系统

### 9.1 二元运算及其性质

**定义 9.1** 设  $S$  为集合, 函数  $f: S \times S \rightarrow S$  称为  $S$  上的二元运算, 简称为二元运算.

例如  $f: \mathbf{N} \times \mathbf{N} \rightarrow \mathbf{N}, f(\langle x, y \rangle) = x + y$  就是自然数集合  $\mathbf{N}$  上的二元运算, 即普通的加法运算. 普通的减法不是自然数集合  $\mathbf{N}$  上的二元运算, 因为两个自然数相减可能得负数, 而负数不是自然数. 这时也称  $\mathbf{N}$  对减法运算不封闭. 验证一个运算是否为集合  $S$  上的二元运算主要考虑两点:

1.  $S$  中任何两个元素都可以进行这种运算, 且运算的结果是惟一的.
2.  $S$  中任何两个元素的运算结果都属于  $S$ , 即  $S$  对该运算是封闭的.

例如实数集合  $\mathbf{R}$  上不可以定义除法运算, 因为  $0 \in \mathbf{R}$ , 而  $0$  不能做除数. 但在  $\mathbf{R}^* = \mathbf{R} - \{0\}$  上就可以定义除法运算了, 因为  $\forall x, y \in \mathbf{R}^*,$  都有  $x/y \in \mathbf{R}^*.$

下面是一些二元运算的例子.

**例 9.1** (1) 自然数集合  $\mathbf{N}$  上的加法和乘法是  $\mathbf{N}$  上的二元运算, 但减法和除法不是.

(2) 整数集合  $\mathbf{Z}$  上的加法、减法和乘法都是  $\mathbf{Z}$  上的二元运算, 而除法不是.

(3) 非零实数集  $\mathbf{R}^*$  上的乘法和除法都是  $\mathbf{R}^*$  上的二元运算, 而加法和减法不是, 因为两个非零实数相加或相减可能得  $0$ .

(4) 设  $M_n(\mathbf{R})$  表示所有  $n$  阶 ( $n \geq 2$ ) 实矩阵的集合, 即

$$M_n(\mathbf{R}) = \left\{ \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix} \mid a_{ij} \in \mathbf{R}, 1 \leq i, j \leq n \right\}$$

则矩阵加法和乘法都是  $M_n(\mathbf{R})$  上的二元运算.

(5)  $S$  为任意集合, 则  $\cup, \cap, -, \oplus$  为  $S$  的幂集  $P(S)$  上的二元运算, 这里  $\cup$  和  $\cap$  是初级并和初级交.

(6)  $S$  为集合,  $S^S$  为  $S$  上的所有函数的集合, 则函数的复合运算  $\circ$  为  $S^S$  上的二元运算.

通常用  $\circ, *, \cdot$  等符号表示二元运算, 称为算符. 设  $f: S \times S \rightarrow S$  是  $S$  上的二元运算, 对任意的  $x, y \in S$ , 如果  $x$  与  $y$  的运算结果是  $z$ , 即

$$f(\langle x, y \rangle) = z$$

可利用算符  $\circ$  简记为

$$x \circ y = z$$

**例 9.2** 设  $\mathbf{R}$  为实数集合, 如下定义  $\mathbf{R}$  上的二元运算  $*$ :

$$\forall x, y \in \mathbf{R}, x * y = x$$

计算  $3 * 4, (-5) * 0.2, 0 * \frac{1}{2}$  等.

$$\text{解 } 3 * 4 = 3, (-5) * 0.2 = -5, 0 * \frac{1}{2} = 0$$

类似于二元运算, 也可以定义集合  $S$  上的一元运算.

**定义 9.2** 设  $S$  为集合, 函数  $f: S \rightarrow S$  称为  $S$  上的一个一元运算, 简称为一元运算.

下面是一些一元运算的例子.

**例 9.3** (1) 求一个数的相反数是整数集合  $\mathbf{Z}$ , 有理数集合  $\mathbf{Q}$  和实数集合  $\mathbf{R}$  上的一元运算.

(2) 求一个数  $x$  的倒数  $\frac{1}{x}$  是非零有理数集合  $\mathbf{Q}^*$ , 非零实数集合  $\mathbf{R}^*$  上的一元运算.

(3) 求一个复数的共轭复数是复数集合  $\mathbf{C}$  上的一元运算.

(4) 在幂集合  $P(S)$  上, 如果规定全集为  $S$ , 则求集合的绝对补运算  $\sim$  是  $P(S)$  上的一元运算.

(5) 设  $S$  为集合, 令  $A$  为  $S$  上所有双射函数的集合,  $A \subseteq S^S$ , 则求一个双射函数的反函数为  $A$  上的一元运算.

(6) 在  $n(n \geq 2)$  阶实矩阵的集合  $M_n(\mathbf{R})$  上, 求一个矩阵的转置矩阵是  $M_n(\mathbf{R})$  上的一元运算.

和二元运算一样, 也可以使用算符来表示一元运算. 若  $f: S \rightarrow S$  为  $S$  上的一元运算, 则  $f(x) = y$  可以用算符  $\circ$  记为

$$\circ(x) = y \text{ 或 } \circ x = y$$

其中  $x$  为参加运算的元素,  $y$  为运算的结果.

例如  $x$  的相反数  $-x$ 、集合  $A$  的绝对补集  $\sim A$  都是上述表示形式, 其中  $-$  和  $\sim$  都是算符.

对于有穷集  $S$  上的一元和二元运算, 除了可以使用函数  $f$  的表达式给出来以外, 还可以用运算表给出来. 表 9.1 和表 9.2 是一元运算表和二元运算表的一般形式, 其中  $a_1, a_2, \dots, a_n$  是  $S$  中的元素,  $\circ$  为算符.

表 9.1

$a_i$	$\circ a_i$
$a_1$	$\circ a_1$
$a_2$	$\circ a_2$
$\vdots$	$\vdots$
$a_n$	$\circ a_n$

表 9.2

$\circ$	$a_1$	$a_2$	$\dots$	$a_n$
$a_1$	$a_1 \circ a_1$	$a_1 \circ a_2$	$\dots$	$a_1 \circ a_n$
$a_2$	$a_2 \circ a_1$	$a_2 \circ a_2$	$\dots$	$a_2 \circ a_n$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$a_n$	$a_n \circ a_1$	$a_n \circ a_2$	$\dots$	$a_n \circ a_n$

例 9.4 设  $S = \{1, 2\}$ , 给出  $P(S)$  上的运算  $\sim$  和  $\oplus$  的运算表, 其中全集为  $S$ .

解 所求的运算表如表 9.3 和表 9.4.

表 9.3

$a_i$	$\sim a_i$
$\emptyset$	$\{1, 2\}$
$\{1\}$	$\{2\}$
$\{2\}$	$\{1\}$
$\{1, 2\}$	$\emptyset$

表 9.4

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

例 9.5 设  $S = \{1, 2, 3, 4\}$ , 定义  $S$  上的二元运算  $\circ$  如下:

$$x \circ y = (xy) \bmod 5, \quad \forall x, y \in S$$

求运算  $\circ$  的运算表.

解  $(xy) \bmod 5$  表示  $xy$  除以 5 的余数, 其运算表如表 9.5 所示.

表 9.5

$\circ$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

下面讨论二元运算的主要性质.

定义 9.3 设  $\circ$  为  $S$  上的二元运算. 如果对于任意的  $x, y \in S$  都有

$$x \circ y = y \circ x$$

则称运算  $\circ$  在  $S$  上是可交换的, 或者说运算  $\circ$  在  $S$  上适合交换律.

例如实数集合上的加法和乘法是可交换的, 但减法不可交换. 幂集  $P(S)$  上的  $\cup$ ,  $\cap$  和  $\oplus$  都是可交换的, 但是相对补运算不可交换.  $n$  阶 ( $n \geq 2$ ) 实矩阵集合  $M_n(\mathbb{R})$  上的矩阵加法是可交换的, 但矩阵乘法不是可交换的.  $A^A$  上函数的复合运算不是可交换的, 因为一般地说  $x \circ y \neq y \circ x$ .

**定义 9.4** 设 $\circ$ 为 $S$ 上的二元运算,如果对于任意的 $x, y \in S$ 都有

$$(x \circ y) \circ z = x \circ (y \circ z)$$

则称运算 $\circ$ 在 $S$ 上是可结合的,或者说运算 $\circ$ 在 $S$ 上适合结合律.

普通的加法和乘法在自然数集 $\mathbf{N}$ 、整数集 $\mathbf{Z}$ 、有理数集 $\mathbf{Q}$ 、实数集 $\mathbf{R}$ 和复数集 $\mathbf{C}$ 上都是可结合的. 矩阵的加法和乘法也是可结合的,集合的 $\cup, \cap$ 和 $\oplus$ 运算也是可结合的,还有函数的复合运算也是可结合的.

对于适合结合律的二元运算,在一个只由该运算的算符连接起来的表达式中,可以把所有表示运算顺序的括号去掉. 例如加法在实数集上是可结合的,对于任意实数 $x, y, z$ 和 $u$ ,可以写

$$(x + y) + (z + u) = x + y + z + u$$

**定义 9.5** 设 $\circ$ 为 $S$ 上的二元运算,如果对于任意的 $x, y \in S$ 都有

$$x \circ x = x$$

则称该运算 $\circ$ 适合幂等律.

如果 $S$ 中的某些 $x$ 满足 $x \circ x = x$ ,则称 $x$ 为运算 $x \circ x = x$ 的幂等元. 易见如果 $S$ 上的二元运算 $x \circ x = x$ 适合幂等律,则 $S$ 中的所有元素都是幂等元.

对于任何集合 $A$ ,有 $A \cup A = A$ 和 $A \cap A = A$ ,集合的并和交运算适合幂等律, $\oplus$ 运算和 $-$ 运算一般不适合幂等律,但 $\emptyset$ 是幂等元. 普通数的加法和乘法不适合幂等律,但 $0$ 是加法的幂等元, $0$ 和 $1$ 是乘法的幂等元.

以上性质都是对一个二元运算来说的. 下面的分配律和吸收律是对两个二元运算来说的.

**定义 9.6** 设 $\circ$ 和 $*$ 是 $S$ 上的两个二元运算,如果对任意的 $x, y, z \in S$ 有

$$x * (y \circ z) = (x * y) \circ (x * z) \quad (\text{左分配律})$$

$$(y \circ z) * x = (y * x) \circ (z * x) \quad (\text{右分配律})$$

则称运算 $*$ 对 $\circ$ 是可分配的,也称 $*$ 对 $\circ$ 适合分配律.

实数集 $\mathbf{R}$ 上的乘法对加法是可分配的,在 $n$ 阶( $n \geq 2$ )实矩阵的集合 $M_n(\mathbf{R})$ 上,矩阵乘法对于矩阵加法也是可分配的,而在幂集 $P(S)$ 上 $\cup$ 和 $\cap$ 是互相可分配的.

在讲到分配律时应该指明哪个运算对哪个运算可分配,不要笼统地讲它们适合分配律. 因为往往一个运算对另一个运算可分配,但反之不对. 例如,普通乘法对加法可分配,但普通加法对乘法不是可分配的.

使用归纳法不难证明,若 $*$ 对 $\circ$ 运算分配律成立,则 $*$ 对 $\circ$ 运算广义分配律也成立,即 $\forall x, y_1, y_2, \dots, y_n \in S$ 有

$$x * (y_1 \circ y_2 \circ \dots \circ y_n) = (x * y_1) \circ (x * y_2) \circ \dots \circ (x * y_n)$$

$$(y_1 \circ y_2 \circ \dots \circ y_n) * x = (y_1 * x) \circ (y_2 * x) \circ \dots \circ (y_n * x)$$

成立.

**定义 9.7** 设 $\circ$ 和 $*$ 是 $S$ 上两个可交换的二元运算,如果对于任意的 $x, y$ 都有

$$x * (x \circ y) = x$$

$$x \circ (x * y) = x$$

则称 $\circ$ 和 $*$ 满足吸收律.

例如幂集 $P(S)$ 上的 $\cup$ 和 $\cap$ 运算满足吸收律. 即 $\forall A, B \in P(S)$ 有

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

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

下面讨论有关二元运算的一些特异元素.

**定义 9.8** 设 $\circ$ 为 $S$ 上的二元运算, 如果存在 $e_l$ (或 $e_r$ )使得对任何 $x \in S$ 都有

$$e_l \circ x = x \quad (\text{或 } x \circ e_r = x)$$

则称 $e_l$ (或 $e_r$ )是 $S$ 中关于 $\circ$ 运算的一个左单位元(或右单位元). 若 $e$ 关于 $\circ$ 运算既是左单位元又是右单位元, 则称 $e$ 为 $S$ 上关于 $\circ$ 运算的单位元. 单位元也可以叫做幺元.

在自然数集 $\mathbf{N}$ 上, 0 是加法的单位元, 1 是乘法的单位元. 在 $M_n(\mathbf{R})$ 上( $n \geq 2$ )全 0 的 $n$ 阶矩阵是矩阵加法的单位元, 而 $n$ 阶单位矩阵是矩阵乘法的单位元. 在幂集 $P(S)$ 上,  $\emptyset$ 是 $\cup$ 运算的单位元,  $S$ 是 $\cap$ 运算的单位元.  $\emptyset$ 也是对称差运算 $\oplus$ 的单位元, 相对补运算没有单位元. 在 $A^A$ 上, 恒等函数 $I_A$ 是关于函数复合运算的单位元.

考虑非零实数的集合 $\mathbf{R}^*$ , 如下定义的二元运算 $\circ$ :

$$\forall a, b \in \mathbf{R}^*, a \circ b = a$$

则不存在 $e \in \mathbf{R}^*$ 使得 $\forall b \in \mathbf{R}^*$ 有 $e \circ b = e$ . 所以 $\circ$ 运算没有左单位元. 但对每一个 $a \in \mathbf{R}^*$ , 对任意 $b \in \mathbf{R}^*$ 都有 $b \circ a = b$ , 所以 $\mathbf{R}^*$ 中的每一个元素 $a$ 都是 $\circ$ 运算的右单位元.  $\mathbf{R}^*$ 中有无数多个右单位元, 但任何右单位元都不是左单位元,  $\mathbf{R}^*$ 中没有关于 $\circ$ 运算的单位元.

**定理 9.1** 设 $\circ$ 为 $S$ 上的二元运算,  $e_l$ 和 $e_r$ 分别为 $\circ$ 运算的左单位元和右单位元, 则有

$$e_l = e_r = e$$

且 $e$ 为 $S$ 上关于 $\circ$ 运算的唯一的单位元.

证  $e_l = e_l \circ e_r$  ( $e_r$ 为右单位元)

$$e_l \circ e_r = e_r \quad (e_l \text{ 为左单位元})$$

所以 $e_l = e_r$ .

把 $e_l = e_r$ 记作 $e$ , 则 $e$ 是 $S$ 中的单位元. 假设 $e'$ 是 $S$ 中的单位元, 则有

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

所以 $e$ 是 $S$ 中关于 $\circ$ 运算的唯一的单位元.

**定义 9.9** 设 $\circ$ 为 $S$ 上的二元运算, 若存在元素 $\theta_l$ (或 $\theta_r$ ) $\in S$ 使得对于任意的 $x \in S$ 有

$$\theta_l \circ x = \theta_l \quad (\text{或 } x \circ \theta_r = \theta_r)$$

则称 $\theta_l$ (或 $\theta_r$ )是 $S$ 上关于 $\circ$ 运算的左零元(或右零元). 若 $\theta \in S$ 关于 $\circ$ 运算既是左零元又是右零元, 则称 $\theta$ 为 $S$ 上关于 $\circ$ 运算的零元.

例如, 自然数集合上 0 是普通乘法的零元, 而加法没有零元.  $M_n(\mathbf{R})$ 上( $n \geq 2$ )矩阵乘法的零元是全 0 的 $n$ 阶矩阵, 而矩阵加法没有零元. 在幂集 $P(S)$ 上 $\cup$ 运算的零元是 $S$ ,  $\cap$ 运算的零元是

$\emptyset$ , 而对称差运算 $\oplus$ 没有零元. 在 $\mathbf{R}^*$ 上如果定义运算 $\circ$ , 使得对任意的 $a, b \in \mathbf{R}^*$ 有

$$a \circ b = a$$

那么 $\mathbf{R}^*$ 中的任何元素都是关于 $\circ$ 运算的左零元, 但没有右零元, 从而也没有零元.

和定理 9.1 类似地可以证明下面的定理.

**定理 9.2** 设 $\circ$ 为 $S$ 上的二元运算,  $\theta_l$  和  $\theta_r$  分别为 $\circ$ 运算的左零元和右零元, 则有

$$\theta_l = \theta_r = \theta$$

且 $\theta$ 是 $S$ 上关于 $\circ$ 运算的惟一的零元.

关于零元和单位元还有以下的定理.

**定理 9.3** 设 $\circ$ 为 $S$ 上的二元运算,  $e$  和  $\theta$  分别为 $\circ$ 运算的单位元和零元. 如果 $S$ 至少有两个元素, 则 $e \neq \theta$ .

**证** 用反证法. 假设 $e = \theta$ , 则 $\forall x \in S$ 有

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

与 $S$ 中至少含有两个元素矛盾.

**定义 9.10** 设 $\circ$ 为 $S$ 上的二元运算,  $e$  为 $\circ$ 运算的单位元, 对于 $x \in S$ , 如果存在 $y_l \in S$  (或 $y_r \in S$ ) 使得

$$y_l \circ x = e \quad (\text{或 } x \circ y_r = e)$$

则称 $y_l$  (或 $y_r$ ) 是 $x$ 的左逆元 (或右逆元). 若 $y \in S$ 既是 $x$ 的左逆元又是 $x$ 的右逆元, 则称 $y$ 是 $x$ 的逆元. 如果 $x$ 的逆元存在, 则称 $x$ 是可逆的.

在自然数集合 $\mathbf{N}$ 上只有0有加法逆元, 就是0自己. 在整数集合 $\mathbf{Z}$ 上加法的单位元是0. 对任何整数 $x$ , 它的加法逆元都存在, 即它的相反数 $-x$ . 在 $n$ 阶 ( $n \geq 2$ ) 实矩阵的集合 $M_n(\mathbf{R})$ 上,  $n$ 阶全0矩阵是矩阵加法的单位元. 对任何 $n$ 阶实矩阵 $M$ ,  $-M$ 是 $M$ 的加法逆元, 而 $n$ 阶单位矩阵是 $M_n(\mathbf{R})$ 上关于矩阵乘法的单位元. 只有 $n$ 阶实可逆矩阵 $M$ 存在乘法逆元 $M^{-1}$ . 在幂集 $P(S)$ 上, 对于 $\cup$ 运算,  $\emptyset$ 为单位元. 只有 $\emptyset$ 有逆元, 就是它自己, 其他的元素都没有逆元. 类似地, 对于 $\cap$ 运算,  $S$ 为单位元, 也只有 $S$ 有逆元, 即 $S$ 自己, 其他元素都没有逆元.

由上面的例子可以看出, 对于给定的集合和二元运算来说, 逆元和单位元、零元不同. 如果单位元或零元存在, 一定是惟一的. 换句话说, 整个集合只有一个. 而逆元能否存在, 还与元素有关. 有的元素有逆元, 有的元素没有逆元, 不同的元素对应着不同的逆元. 如果运算是可结合的, 那么对于集合中可逆的元素, 逆元是惟一的.

**定理 9.4** 设 $\circ$ 为 $S$ 上可结合的二元运算,  $e$  为该运算的单位元, 对于 $x \in S$  如果存在左逆元 $y_l$ 和右逆元 $y_r$ , 则有

$$y_l = y_r = y$$

且 $y$ 是 $x$ 的惟一的逆元.

**证** 由 $y_l \circ x = e$  和  $x \circ y_r = e$  得

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

令 $y_l = y_r = y$ , 则 $y$ 是 $x$ 的逆元. 假若 $y'$ 也是 $x$ 的逆元, 则

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

所以  $y$  是  $x$  的惟一的逆元.

由定理 9.4 可知, 对于可结合的二元运算来说, 可逆的元素  $x$  只有惟一的逆元, 通常把它记作  $x^{-1}$ .

最后再给出一条关于二元运算的算律——消去律.

**定义 9.11** 设  $\circ$  为  $S$  上的二元运算, 如果对于任意的  $x, y, z \in S$ , 满足以下条件:

(1) 若  $x \circ y = x \circ z$  且  $x \neq \theta$ , 则  $y = z$ ;

(2) 若  $y \circ x = z \circ x$  且  $x \neq \theta$ , 则  $y = z$ ;

那么称  $\circ$  运算满足消去律, 其中 (1) 称作左消去律, (2) 称作右消去律.

注意被消去的  $x$  不能是运算的零元  $\theta$ .

整数集合上的加法和乘法都满足消去律. 幂集  $P(S)$  上的并和交运算一般不满足消去律.  $\forall A, B, C \in P(S)$ , 由  $A \cup B = A \cup C$  不一定能得到  $B = C$ . 但对称差运算满足消去律.  $\oplus$  运算不存在零元,  $\forall A, B, C \in P(S)$ , 都有

$$A \oplus B = A \oplus C \Rightarrow B = C$$

$$B \oplus A = C \oplus A \Rightarrow B = C$$

**例 9.6** 对于下面给定的集合和该集合上的二元运算, 指出该运算的性质, 并求出它的单位元, 零元和所有可逆元素的逆元.

(1)  $\mathbf{Z}^+$ ,  $\forall x, y \in \mathbf{Z}^+$ ,  $x * y = \text{lcm}(x, y)$ , 即求  $x$  和  $y$  的最小公倍数.

(2)  $\mathbf{Q}$ ,  $\forall x, y \in \mathbf{Q}$ ,  $x * y = x + y - xy$

解 (1)  $*$  运算可交换, 可结合, 是幂等的.

$\forall x \in \mathbf{Z}^+$ ,  $x * 1 = x$ ,  $1 * x = x$ ,  $1$  为单位元.

不存在零元.

只有  $1$  有逆元, 是它自己, 其他正整数无逆元.

(2)  $*$  运算满足交换律, 因为  $\forall x, y \in \mathbf{Q}$ , 有

$$x * y = x + y - xy = y + x - yx = y * x$$

$*$  运算满足结合律, 因为  $\forall x, y, z \in \mathbf{Q}$ , 有

$$(x * y) * z = (x + y - xy) * z = x + y + z - xy - xz - yz + xyz$$

$$x * (y * z) = x * (y + z - yz) = x + y + z - xy - xz - yz + xyz$$

所以

$$x * (y * z) = x * (y * z)$$

$*$  运算不满足幂等律, 因为  $2 \in \mathbf{Q}$ , 但

$$2 * 2 = 2 + 2 - 2 \times 2 = 0 \neq 2$$

$*$  运算满足消去律, 因为  $\forall x, y, z \in \mathbf{Q}$ ,  $x \neq 1$  ( $1$  为零元), 有

$$x * y = x * z$$

$$\Rightarrow x + y - xy = x + z - xz$$

$$\Rightarrow (y-z) = x(y-z)$$

$$\Rightarrow y = z \quad (x \neq 1)$$

由于  $*$  是可交换的, 右消去律显然成立.

$\forall x \in Q$ , 有

$$x * 0 = x = 0 * x$$

0 是  $*$  运算的单位元.

$\forall x \in Q$ , 有

$$x * 1 = 1 = 1 * x$$

1 是  $*$  运算的零元.

$\forall x \in Q$ , 欲使  $x * y = 0$  和  $y * x = 0$  成立, 即

$$x + y - xy = 0$$

解得

$$y = \frac{x}{x-1} \quad (x \neq 1)$$

从而有  $x^{-1} = \frac{x}{x-1} \quad (x \neq 1)$ .

**例 9.7** 设  $A = \{a, b, c\}$ ,  $A$  上的二元运算  $*, \circ, \cdot$  如表 9.6 所示.

(1) 说明  $*, \circ$  和  $\cdot$  运算是否满足交换律、结合律、消去律和幂等律.

(2) 求出关于  $*, \circ$  和  $\cdot$  运算的单位元、零元和所有可逆元素的逆元.

表 9.6

$*$	$a$	$b$	$c$
$a$	$a$	$b$	$c$
$b$	$b$	$c$	$a$
$c$	$c$	$a$	$b$

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

$\cdot$	$a$	$b$	$c$
$a$	$a$	$b$	$c$
$b$	$a$	$b$	$c$
$c$	$a$	$b$	$c$

**解**  $*$  运算适合交换律、结合律和消去律, 不适合幂等律. 单位元是  $a$ , 没有零元, 且  $a^{-1} = a, b^{-1} = c, c^{-1} = b$ .

$\circ$  运算适合交换律、结合律和幂等律, 不适合消去律. 单位元是  $a$ , 零元是  $b$ . 只有  $a$  有逆元,  $a^{-1} = a$ .

$\cdot$  运算不适合交换律, 适合结合律和幂等律, 不适合消去律. 没有单位元, 没有零元, 没有可逆元素.

## 9.2 代数系统

**定义 9.12** 非空集合  $S$  和  $S$  上  $k$  个一元或二元运算  $f_1, f_2, \dots, f_k$  组成的系统称为一个代数系

统,简称代数,记作  $\langle S, f_1, f_2, \dots, f_k \rangle$ .

例如  $\langle \mathbf{N}, + \rangle$ ,  $\langle \mathbf{Z}, +, \cdot \rangle$ ,  $\langle \mathbf{R}, +, \cdot \rangle$  都是代数系统,其中  $+$  和  $\cdot$  分别表示普通加法和乘法.  $\langle M_n(\mathbf{R}), +, \cdot \rangle$  是代数系统,其中  $+$  和  $\cdot$  分别表示  $n$  阶 ( $n \geq 2$ ) 实矩阵的加法和乘法.  $\langle \mathbf{Z}_n, \oplus, \otimes \rangle$  是代数系统,其中  $\mathbf{Z}_n = \{0, 1, \dots, n-1\}$ ,  $\oplus$  和  $\otimes$  分别表示模  $n$  的加法和乘法,  $\forall x, y \in \mathbf{Z}_n$

$$x \oplus y = (x + y) \bmod n, \quad x \otimes y = (xy) \bmod n$$

$\langle P(S), \cup, \cap, \sim \rangle$  也是代数系统,其中含有两个二元运算  $\cup$  和  $\cap$  以及一个一元运算  $\sim$ .

在某些代数系统中存在着一些特定的元素,它对该系统的一元或二元运算起着重要的作用,例如二元运算的单位元和零元. 在定义代数系统的时候,如果把含有这样的特定元素也作为系统的性质,比如规定系统的二元运算必须含有单位元,在这种情况下称这些元素为该代数系统的特异元素或代数常数. 有时为了强调某个代数系统是含有代数常数的系统,也可以把这些代数常数列到系统的表达式中,例如  $\langle \mathbf{Z}, + \rangle$  中的  $+$  运算有单位元  $0$ ,为了强调  $0$  的存在,将  $\langle \mathbf{Z}, + \rangle$  记作  $\langle \mathbf{Z}, +, 0 \rangle$ . 又如  $\langle P(S), \cup, \cap, \sim \rangle$  中的  $\cup$  和  $\cap$  运算存在单位元  $\emptyset$  和  $S$ ,当规定  $\emptyset$  和  $S$  是该系统的代数常数时,也可将它记为  $\langle P(S), \cup, \cap, \sim, \emptyset, S \rangle$ . 当然,在不发生混淆的情况下为了叙述的简便也常用集合的名字来标记代数系统,例如上述代数系统可以简记为  $\mathbf{Z}$  和  $P(S)$ .

**定义 9.13** 如果两个代数系统中运算的个数相同,对应运算的元数相同,且代数常数的个数也相同,则称这两个代数系统具有相同的构成成分,也称它们是同类型的代数系统.

例如

$$V_1 = \langle \mathbf{R}, +, \cdot, -, 0, 1 \rangle$$

$$V_2 = \langle P(B), \cup, \cap, \sim, \emptyset, B \rangle$$

是同类型的代数系统,它们都含有两个二元运算、一个一元运算和两个代数常数.

同类型的代数系统仅仅是构成成分相同,不一定具有相同的运算性质. 上述的  $V_1$  和  $V_2$  是同类型的代数系统,但它们的运算性质却很不一样,请看表 9.7.

表 9.7

$V_1$	$V_2$
$+$ 和 $\cdot$ 可交换,可结合 $\cdot$ 对 $+$ 可分配 $+$ 和 $\cdot$ 不遵从幂等律 $+$ 和 $\cdot$ 没有吸收律 $+$ 和 $\cdot$ 都有消去律	$\cup$ 和 $\cap$ 可交换,可结合 $\cup$ 和 $\cap$ 互相可分配 $\cup$ 和 $\cap$ 都有幂等律 $\cup$ 和 $\cap$ 有吸收律 $\cup$ 和 $\cap$ 一般没有消去律

在规定的了一个代数系统的构成成分,即集合、运算以及代数常数以后,如果再对这些运算所遵从的算律加以限制,那么满足这些条件的代数系统就具有完全相同的性质,从而构成了一类特

殊的代数系统. 例如代数系统  $V = \langle S, \circ \rangle$ , 其中  $\circ$  是一个可结合的二元运算, 就代表了一类特殊的代数系统——半群. 许多具体的代数系统, 如  $\langle \mathbf{Z}, + \rangle$ ,  $\langle \mathbf{R}, + \rangle$ ,  $\langle M_n(\mathbf{R}), \cdot \rangle$ ,  $\langle P(B), \cup \rangle$  等都是半群. 又如代数系统  $V = \langle S, \circ, * \rangle$ , 其中  $\circ$  和  $*$  是二元运算, 并满足交换律、结合律、幂等律和吸收律, 那么代表了另一类特殊的代数系统——格. 实际中的代数系统  $\langle \mathbf{Z}^+, \text{lcm}, \text{gcd} \rangle$ ,  $\langle P(B), \cup, \cap \rangle$  等都是格. 这里的  $\text{lcm}$  和  $\text{gcd}$  分别表示求两个正整数的最小公倍数和最大公约数的运算. 从代数系统的构成成分和遵从的算律出发, 将代数系统分类, 然后研究每一类代数系统的共同性质, 并将研究的结果运用到具体的代数系统中去. 这种方法就是抽象代数的基本方法, 也是代数结构课程的主要内容. 在给出了代数系统的一般概念以后, 后面我们将分别就几类重要的代数系统进行更深入的分析.

由已知的代数系统可以通过系统的方法构成新的代数系统, 即子代数和积代数. 这些代数系统能够保持或者基本上保持原有代数系统的良好性质.

**定义 9.14** 设  $V = \langle S, f_1, f_2, \dots, f_k \rangle$  是代数系统,  $B \subseteq S$ , 如果  $B$  对  $f_1, f_2, \dots, f_k$  都是封闭的, 且  $B$  和  $S$  含有相同的代数常数, 则称  $\langle B, f_1, f_2, \dots, f_k \rangle$  是  $V$  的子代数系统, 简称子代数. 有时将子代数系统简记为  $B$ .

例如  $\mathbf{N}$  是  $\langle \mathbf{Z}, + \rangle$  的子代数, 因为  $\mathbf{N}$  对加法运算  $+$  是封闭的.  $\mathbf{N}$  也是  $\langle \mathbf{Z}, +, 0 \rangle$  的子代数, 因为  $\mathbf{N}$  对加法运算  $+$  封闭, 且  $\mathbf{N}$  中含有代数常数  $0$ .  $\mathbf{N} - \{0\}$  是  $\langle \mathbf{Z}, + \rangle$  的子代数, 但不是  $\langle \mathbf{Z}, +, 0 \rangle$  的子代数, 因为  $\langle \mathbf{Z}, +, 0 \rangle$  的代数常数  $0 \notin \mathbf{N} - \{0\}$ .

从子代数定义不难看出, 子代数和原代数不仅具有相同的构成成分, 是同类型的代数系统, 而且对应的二元运算都具有相同的运算性质. 因为任何二元运算的性质如果在原代数上成立, 那么在它的子集上显然也是成立的. 在这个意义上讲, 子代数在许多方面与原代数非常相似, 不过可能小一些就是了.

对于任何代数系统  $V = \langle S, f_1, f_2, \dots, f_k \rangle$ , 其子代数一定存在. 最大的子代数就是  $V$  本身. 如果令  $V$  中所有代数常数构成的集合是  $B$ , 且  $B$  对  $V$  中所有的运算都是封闭的, 则  $B$  就构成了  $V$  的最小的子代数. 这种最大和最小的子代数称为  $V$  的平凡子代数. 若  $B$  是  $S$  的真子集, 则  $B$  构成的子代数称为  $V$  的真子代数.

**例 9.8** 设  $V = \langle \mathbf{Z}, +, 0 \rangle$ , 令

$$n\mathbf{Z} = \{nz \mid z \in \mathbf{Z}\}, \quad n \text{ 为自然数},$$

则  $n\mathbf{Z}$  是  $V$  的子代数.

**证** 任取  $n\mathbf{Z}$  中的两个元素  $nz_1, nz_2$  ( $z_1, z_2 \in \mathbf{Z}$ ), 则有

$$nz_1 + nz_2 = n(z_1 + z_2) \in n\mathbf{Z}$$

即  $n\mathbf{Z}$  对  $+$  运算是封闭的. 又

$$0 = n \cdot 0 \in n\mathbf{Z}$$

所以,  $n\mathbf{Z}$  是  $V$  的子代数.

当  $n=1$  和  $0$  时,  $n\mathbf{Z}$  是  $V$  的平凡子代数, 其他的都是  $V$  的非平凡的真子代数.

**定义 9.15** 设  $V_1 = \langle A, \circ \rangle$  和  $V_2 = \langle B, * \rangle$  是同类型的代数系统,  $\circ$  和  $*$  为二元运算, 在集

合  $A \times B$  上如下定义二元运算  $\cdot$ ,  $\forall \langle a_1, b_1 \rangle, \langle a_2, b_2 \rangle \in A \times B$ , 有

$$\langle a_1, b_1 \rangle \cdot \langle a_2, b_2 \rangle = \langle a_1 \circ a_2, b_1 * b_2 \rangle$$

称  $V = \langle A \times B, \cdot \rangle$  为  $V_1$  与  $V_2$  的积代数, 记作  $V_1 \times V_2$ . 这时也称  $V_1$  和  $V_2$  为  $V$  的因子代数.

**例 9.9** 设  $V_1$  和  $V_2$  分别为模 3 和模 2 加的代数系统, 给出  $V_1 \times V_2$  的运算表, 并说明它的运算是否具有交换律与结合律, 是否具有单位元.

**解** 运算表如表 9.8 所示.

表 9.8

$\oplus$	$\langle 0, 0 \rangle$	$\langle 0, 1 \rangle$	$\langle 1, 0 \rangle$	$\langle 1, 1 \rangle$	$\langle 2, 0 \rangle$	$\langle 2, 1 \rangle$
$\langle 0, 0 \rangle$	$\langle 0, 0 \rangle$	$\langle 0, 1 \rangle$	$\langle 1, 0 \rangle$	$\langle 1, 1 \rangle$	$\langle 2, 0 \rangle$	$\langle 2, 1 \rangle$
$\langle 0, 1 \rangle$	$\langle 0, 1 \rangle$	$\langle 0, 0 \rangle$	$\langle 1, 1 \rangle$	$\langle 1, 0 \rangle$	$\langle 2, 1 \rangle$	$\langle 2, 0 \rangle$
$\langle 1, 0 \rangle$	$\langle 1, 0 \rangle$	$\langle 1, 1 \rangle$	$\langle 2, 0 \rangle$	$\langle 2, 1 \rangle$	$\langle 0, 0 \rangle$	$\langle 0, 1 \rangle$
$\langle 1, 1 \rangle$	$\langle 1, 1 \rangle$	$\langle 1, 0 \rangle$	$\langle 2, 1 \rangle$	$\langle 2, 0 \rangle$	$\langle 0, 1 \rangle$	$\langle 0, 0 \rangle$
$\langle 2, 0 \rangle$	$\langle 2, 0 \rangle$	$\langle 2, 1 \rangle$	$\langle 0, 0 \rangle$	$\langle 0, 1 \rangle$	$\langle 1, 0 \rangle$	$\langle 1, 1 \rangle$
$\langle 2, 1 \rangle$	$\langle 2, 1 \rangle$	$\langle 2, 0 \rangle$	$\langle 0, 1 \rangle$	$\langle 0, 0 \rangle$	$\langle 1, 1 \rangle$	$\langle 1, 0 \rangle$

$V_1 \times V_2$  中的  $\oplus$  运算具有交换律、结合律, 单位元是  $\langle 0, 0 \rangle$ .

易见积代数与它的因子代数是同类型的代数系统, 可以证明积代数能够保持因子代数中的许多良好的性质.

**定理 9.5** 设  $V_1 = \langle A, \circ \rangle$  和  $V_2 = \langle B, * \rangle$  是同类型的代数系统,  $V_1 \times V_2 = \langle A \times B, \cdot \rangle$  是它们的积代数.

(1) 如果  $\circ$  和  $*$  运算是可交换(可结合、幂等)的, 那么  $\cdot$  运算也是可交换(可结合、幂等)的;

(2) 如果  $e_1$  和  $e_2$  ( $\theta_1$  和  $\theta_2$ ) 分别为  $\circ$  和  $*$  运算的单位元(零元), 那么  $\langle e_1, e_2 \rangle$  ( $\langle \theta_1, \theta_2 \rangle$ ) 也是  $\cdot$  运算的单位元(零元);

(3) 如果  $x$  和  $y$  分别为  $\circ$  和  $*$  运算的可逆元素, 那么  $\langle x, y \rangle$  也是  $\cdot$  运算的可逆元素, 其逆元就是  $\langle x^{-1}, y^{-1} \rangle$ .

**证** 这里只证明(1)中的结合律, (2)中的单位元, 其他性质的证明留作练习.

(1) 任取  $\langle a_1, b_1 \rangle, \langle a_2, b_2 \rangle, \langle a_3, b_3 \rangle \in V_1 \times V_2$ ,

$$\begin{aligned} & (\langle a_1, b_1 \rangle \cdot \langle a_2, b_2 \rangle) \cdot \langle a_3, b_3 \rangle = \langle a_1 \circ a_2, b_1 * b_2 \rangle \cdot \langle a_3, b_3 \rangle \\ & = \langle (a_1 \circ a_2) \circ a_3, (b_1 * b_2) * b_3 \rangle \\ & = \langle a_1 \circ (a_2 \circ a_3), b_1 * (b_2 * b_3) \rangle && \text{(因为 } \circ \text{ 和 } * \text{ 运算都满足结合律)} \\ & = \langle a_1, b_1 \rangle \cdot \langle a_2 \circ a_3, b_2 * b_3 \rangle = \langle a_1, b_1 \rangle \cdot (\langle a_2, b_2 \rangle \cdot \langle a_3, b_3 \rangle) \end{aligned}$$

(2) 任取  $\langle a, b \rangle \in V_1 \times V_2$ ,

$$\begin{aligned} \langle a, b \rangle \cdot \langle e_1, e_2 \rangle & = \langle a \circ e_1, b * e_2 \rangle = \langle a, b \rangle \\ \langle e_1, e_2 \rangle \cdot \langle a, b \rangle & = \langle e_1 \circ a, e_2 * b \rangle = \langle a, b \rangle \end{aligned}$$

因此  $\langle e_1, e_2 \rangle$  是关于  $\cdot$  运算的单位元.

积代数的定义可以推广到具有多个运算的同类型的代数系统. 在具有两个不同二元运算的情况下, 使用与定理 9.5 中类似的方法不难证明: 积代数也保留因子代数中的分配律和吸收律等性质. 但是消去律是一个例外. 请看下面的例子.

**例 9.10** 设  $Z_n = \{0, 1, \dots, n-1\}$ , 其中  $n$  是正整数,  $V_1 = \langle Z_4, \otimes_4 \rangle$ ,  $V_2 = \langle Z_3, \otimes_3 \rangle$  分别表示模 4 和模 3 乘法的代数系统. 那么  $V_1$  和  $V_2$  中的运算都满足消去律. 考虑积代数  $\langle V_1 \times V_2, \otimes \rangle$ , 这里的  $\otimes$  运算不满足消去律. 因为在  $V_1 \times V_2$  中有

$$\langle 2, 0 \rangle \otimes \langle 0, 2 \rangle = \langle 0, 0 \rangle = \langle 2, 0 \rangle \otimes \langle 0, 0 \rangle$$

$\langle 2, 0 \rangle$  不是零元, 在上式中用消去律将它消去, 就得到  $\langle 0, 2 \rangle = \langle 0, 0 \rangle$ , 显然这是错误的.

### 9.3 代数系统的同态与同构

实践中存在着很多不同的代数系统, 有些系统是同类型的, 有些不但是同类型的, 而且具有共同的运算性质, 因此是同种的. 在同种的代数系统中, 有些系统在结构上更为相似, 甚至完全一样. 例如代数系统  $V_1 = \langle Z_3, \oplus_3 \rangle$ ,  $V_2 = \langle A, \oplus_6 \rangle$ , 其中  $Z_3 = \{0, 1, 2\}$ ,  $A = \{0, 2, 4\}$ ,  $\oplus_3$  和  $\oplus_6$  分别表示模 3 和模 6 加. 那么这两个代数系统的运算表如下:

表 9.9

$\oplus_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

表 9.10

$\oplus_6$	0	2	4
0	0	2	4
2	2	4	0
4	4	0	2

把表 9.9 中的 1 和 2 分别替换成 2 和 4, 就可以得到表 9.10. 这个替换可以表示成函数:

$$f = \{ \langle 0, 0 \rangle, \langle 1, 2 \rangle, \langle 2, 4 \rangle \}$$

在双射函数  $f$  的作用下, 代数系统  $V_1$  转换成了  $V_2$ . 它们是同构的, 都是抽象代数系统  $\{a, b, c\}$  的实例.

**定义 9.16** 设  $V_1 = \langle A, \circ \rangle$  和  $V_2 = \langle B, * \rangle$  是同类型的代数系统,  $f: A \rightarrow B$ , 且  $\forall x, y \in A$  有

$$f(x \circ y) = f(x) * f(y)$$

则称  $f$  是  $V_1$  到  $V_2$  的同态映射, 简称同态.

根据同态映射的性质可以将同态分为单同态、满同态和同构. 即:  $f$  如果是单射, 则称为单同态; 如果是满射, 则称为满同态, 这时称  $V_2$  是  $V_1$  的同态像, 记作  $V_1 \sim V_2$ ; 如果是双射, 则称为同构, 也称代数系统  $V_1$  同构于  $V_2$ , 记作  $V_1 \cong V_2$ .

如果同态映射  $f$  是  $V$  到  $V$  的, 则称  $f$  为自同态. 类似地可以定义单自同态、满自同态和自

同构.

设  $f$  是  $V_1 = \langle A, \circ \rangle$  到  $V_2 = \langle B, * \rangle$  的同态映射, 那么  $f$  具有许多良好的性质. 首先, 如果  $\circ$  运算具有交换律、结合律、幂等律等, 那么在同态像  $f(V_1)$  中,  $*$  运算也具有相同的算律 (注意, 消去律可能有例外). 此外, 同态映射  $f$  恰好把  $V_1$  的单位元  $e_1$  映到  $V_2$  的单位元  $e_2$ , 即  $f(e_1) = e_2$ . 同样对于零元和可逆元也有

$$f(\theta_1) = \theta_2, \quad f(x^{-1}) = f(x)^{-1}$$

上述关于同态映射的定义可以推广到具有有限多个运算的代数系统. 例如, 对于具有两个二元运算的代数系统  $V_1 = \langle A, \circ_1, \circ_2 \rangle$  和  $V_2 = \langle B, *_1, *_2 \rangle$ ,  $f: A \rightarrow B$ , 如果  $\forall x, y \in A$  有

$$f(x \circ_1 y) = f(x) *_1 f(y) \text{ 和 } f(x \circ_2 y) = f(x) *_2 f(y)$$

那么  $f$  是  $V_1$  到  $V_2$  的同态映射.

**例 9.11** (1) 设代数系统  $V_1 = \langle \mathbf{Z}, + \rangle$ ,  $V_2 = \langle \mathbf{Z}_n, \oplus \rangle$ . 其中  $\mathbf{Z}$  为整数集合,  $+$  为普通加法;  $\mathbf{Z}_n = \{0, 1, \dots, n-1\}$ ,  $\oplus$  为模  $n$  加. 令

$$f: \mathbf{Z} \rightarrow \mathbf{Z}_n, f(x) = (x) \bmod n$$

那么  $f$  是  $V_1$  到  $V_2$  的满同态. 显然  $f$  是满射, 且  $\forall x, y \in \mathbf{Z}$  有

$$f(x + y) = (x + y) \bmod n = (x) \bmod n \oplus (y) \bmod n = f(x) \oplus f(y)$$

(2) 设  $V_1 = \langle \mathbf{R}, + \rangle$ ,  $V_2 = \langle \mathbf{R}^*, \cdot \rangle$ , 其中  $\mathbf{R}$  和  $\mathbf{R}^*$  分别为实数集与非零实数集,  $+$  和  $\cdot$  分别表示普通加法与乘法. 令

$$f: \mathbf{R} \rightarrow \mathbf{R}^*, f(x) = e^x$$

则  $f$  是  $V_1$  到  $V_2$  的单同态, 易见  $f$  是单射, 且  $\forall x, y \in \mathbf{R}$  有

$$f(x + y) = e^{x+y} = e^x \cdot e^y = f(x) \cdot f(y)$$

(3) 设  $V = \langle \mathbf{Z}, + \rangle$ , 其中  $\mathbf{Z}$  为整数集合,  $+$  为普通加法.  $\forall a \in \mathbf{Z}$ , 令

$$f_a: \mathbf{Z} \rightarrow \mathbf{Z}, f_a(x) = ax,$$

那么  $f_a$  是  $V$  的自同态. 因为  $\forall x, y \in \mathbf{Z}$ , 有

$$f_a(x + y) = a(x + y) = ax + ay = f_a(x) + f_a(y).$$

当  $a = 0$  时称  $f_0$  为零同态; 当  $a = \pm 1$  时, 称  $f_a$  为自同构; 除此之外其他的  $f_a$  都是单自同态.

**例 9.12** 设  $V = \langle \mathbf{Z}_n, \oplus \rangle$ , 其中  $\mathbf{Z}_n = \{0, 1, \dots, n-1\}$ ,  $\oplus$  为模  $n$  加. 证明恰含有  $n$  个  $V$  的自同态.

证 先证存在着  $n$  个  $V$  的自同态. 令

$$f_p: \mathbf{Z}_n \rightarrow \mathbf{Z}_n, f_p(x) = (px) \bmod n, p = 0, 1, \dots, n-1$$

则  $f_p$  是  $V$  的自同态, 因为  $\forall x, y \in \mathbf{Z}_n$  有

$$\begin{aligned} f_p(x \oplus y) &= (p(x \oplus y)) \bmod n \\ &= (px) \bmod n \oplus (py) \bmod n = f_p(x) \oplus f_p(y) \end{aligned}$$

由于  $p$  有  $n$  种取值, 不同的  $p$  确定了不同的映射  $f_p$ , 所以存在  $n$  个  $V$  的自同态.

下面证明任何  $V$  的自同态都是上述  $n$  个自同态中的一个. 设  $f$  是  $V$  的自同态, 且  $f(1) = i$ ,  $i \in \{0, \dots, n-1\}$ . 下面证明  $\forall x \in \mathbf{Z}_n$  有  $f(x) = (ix) \bmod n$ .

显然  $f(1) = i = (i \cdot 1) \bmod n$ . 假设对一切  $x \in \{1, 2, \dots, n-2\}$  有  $f(x) = (ix) \bmod n$  成立, 那么

$$\begin{aligned} f(x+1) &= f(x \oplus 1) = f(x) \oplus f(1) \\ &= (ix) \bmod n \oplus i = (ix + i) \bmod n \\ &= (i(x+1)) \bmod n \end{aligned}$$

最后有

$$\begin{aligned} f(0) &= f((n-1) \oplus 1) = f(n-1) \oplus f(1) \\ &= (i(n-1)) \bmod n \oplus i = (in) \bmod n \\ &= 0 \\ &= (i \cdot 0) \bmod n \end{aligned}$$

## 习 题 九

1. 列出以下运算的运算表:

(1)  $A = \{1, 2, 1/2\}$ ,  $\forall x \in A$ ,  $\circ x$  是  $x$  的倒数, 即  $\circ x = 1/x$ ;

(2)  $A = \{1, 2, 3, 4\}$ ,  $\forall x, y \in A$ , 有  $x \circ y = \max(x, y)$ ,  $\max(x, y)$  是  $x$  和  $y$  之中较大的数.

2. 设  $A = \{0, 1\}$ ,  $S = A^A$ ,

(1) 试列出  $S$  中的所有函数.

(2) 给出  $S$  上合成运算的运算表.

3. 设  $A = \{a, b, c\}$ ,  $a, b, c \in \mathbb{R}$ , 能否确定  $a, b, c$  的值使得

(1)  $A$  对普通乘法封闭.

(2)  $A$  对普通加法封闭.

4. 判断下列集合对所给的二元运算是否封闭:

(1) 整数集合  $\mathbb{Z}$  和普通的减法运算.

(2) 非零整数集合  $\mathbb{Z}^*$  和普通的除法运算.

(3) 全体  $n \times n$  实矩阵集合  $M_n(\mathbb{R})$  和矩阵加法及乘法运算, 其中  $n \geq 2$ .

(4) 全体  $n \times n$  实可逆矩阵集合关于矩阵加法和乘法运算, 其中  $n \geq 2$ .

(5) 正实数集合  $\mathbb{R}^+$  和  $\circ$  运算, 其中  $\circ$  运算定义为

$$\forall a, b \in \mathbb{R}^+, a \circ b = ab - a - b$$

(6)  $n \in \mathbb{Z}^+$ ,  $n\mathbb{Z} = \{nz \mid z \in \mathbb{Z}\}$ ,  $n\mathbb{Z}$  关于普通的加法和乘法运算.

(7)  $A = \{a_1, a_2, \dots, a_n\}$ ,  $n \geq 2$ .  $\circ$  运算定义如下:

$$\forall a, b \in A, a \circ b = b$$

(8)  $S = \{2x - 1 \mid x \in \mathbb{Z}^+\}$  关于普通的加法和乘法运算.

(9)  $S = \{0, 1\}$ ,  $S$  关于普通的加法和乘法运算.

(10)  $S = \{x \mid x = 2^n, n \in \mathbb{Z}^+\}$ ,  $S$  关于普通的加法和乘法运算.

5. 对于上题中封闭的二元运算判断是否适合交换律、结合律和分配律.

6. 对习题 4 中封闭的二元运算找出它的单位元、零元和所有可逆元素的逆元.

7. 设  $*$  为  $\mathbb{Z}^+$  上的二元运算,  $\forall x, y \in \mathbb{Z}^+$ ,

$$x * y = \min(x, y), \text{ 即 } x \text{ 和 } y \text{ 之中较小的数.}$$

(1) 求  $4 * 6, 7 * 3$ .

(2)  $*$  在  $\mathbb{Z}^+$  上是否满足交换律、结合律和幂等律?

(3) 求  $*$  运算的单位元、零元及  $\mathbb{Z}^+$  中所有可逆元素的逆元.

8.  $S = \mathbb{Q} \times \mathbb{Q}$ ,  $\mathbb{Q}$  为有理数集,  $*$  为  $S$  上的二元运算,  $\forall \langle a, b \rangle, \langle x, y \rangle \in S$  有

$$\langle a, b \rangle * \langle x, y \rangle = \langle ax, ay + b \rangle$$

(1)  $*$  运算在  $S$  上是否可交换、可结合? 是否为幂等的?

(2)  $*$  运算是否有单位元、零元? 如果有, 请指出, 并求  $S$  中所有可逆元素的逆元.

9.  $\mathbb{R}$  为实数集, 定义以下 6 个函数  $f_1, f_2, \dots, f_6$ .  $\forall x, y \in \mathbb{R}$  有

$$f_1(\langle x, y \rangle) = x + y, \quad f_2(\langle x, y \rangle) = x - y$$

$$f_3(\langle x, y \rangle) = x \cdot y, \quad f_4(\langle x, y \rangle) = \max(x, y)$$

$$f_5(\langle x, y \rangle) = \min(x, y), \quad f_6(\langle x, y \rangle) = |x - y|$$

(1) 指出哪些函数是  $\mathbb{R}$  上的二元运算;

(2) 对所有  $\mathbb{R}$  上的二元运算说明是否为可交换、可结合、幂等的;

(3) 求所有  $\mathbb{R}$  上二元运算的单位元、零元以及每一个可逆元素的逆元.

10. 令  $S = \{a, b\}$ ,  $S$  上有 4 个二元运算:  $*$ ,  $\circ$ ,  $\cdot$  和  $\square$ , 分别由表 9.11 确定.

表 9.11

$*$	$a$	$b$
$a$	$a$	$a$
$b$	$a$	$a$

$\circ$	$a$	$b$
$a$	$a$	$b$
$b$	$b$	$a$

$\cdot$	$a$	$b$
$a$	$b$	$a$
$b$	$a$	$a$

$\square$	$a$	$b$
$a$	$a$	$b$
$b$	$a$	$b$

(1) 这 4 个运算中哪些运算满足交换律、结合律、幂等律?

(2) 求每个运算的单位元、零元及所有可逆元素的逆元.

11. 设  $S = \{1, 2, \dots, 10\}$ , 问下面定义的运算能否与  $S$  构成代数系统  $\langle S, * \rangle$ ? 如果能构成代数系统则说明  $*$  运算是否满足交换律、结合律, 并求  $*$  运算的单位元和零元.

(1)  $x * y = \gcd(x, y)$ ,  $\gcd(x, y)$  是  $x$  与  $y$  的最大公约数;

(2)  $x * y = \text{lcm}(x, y)$ ,  $\text{lcm}(x, y)$  是  $x$  与  $y$  的最小公倍数;

(3)  $x * y =$  大于等于  $x$  和  $y$  的最小整数;

(4)  $x * y =$  质数  $p$  的个数, 其中  $x \leq p \leq y$ .

12. 设  $S = \{f | f \text{ 是 } [a, b] \text{ 上的连续函数}\}$ , 其中  $a, b \in \mathbb{R}, a < b$ , 问  $S$  关于下面每个运算是否构成代数系统? 如果能构成代数系统, 说明该运算是否适合交换律和结合律, 并求出单位元和零元.

(1) 函数加法, 即  $(f + g)(x) = f(x) + g(x), \forall x \in [a, b]$

(2) 函数减法, 即  $(f - g)(x) = f(x) - g(x), \forall x \in [a, b]$

(3) 函数乘法, 即  $(f \cdot g)(x) = f(x) \cdot g(x), \forall x \in [a, b]$

(4) 函数除法, 即  $(f/g)(x) = f(x)/g(x), \forall x \in [a, b]$

13. 设  $A = \{a, b\}$ , 试给出  $A$  上一个不可交换、也不可结合的二元运算.

14. 下面各集合都是  $\mathbf{N}$  的子集, 它们能否构成代数系统  $V = \langle \mathbf{N}, + \rangle$  的子代数:

(1)  $\{x | x \in \mathbf{N} \wedge x \text{ 的某次幂可以被 } 16 \text{ 整除}\}$ ;

(2)  $\{x | x \in \mathbf{N} \wedge x \text{ 与 } 5 \text{ 互素}\}$ ;

(3)  $\{x | x \in \mathbf{N} \wedge x \text{ 是 } 30 \text{ 的因子}\}$ ;

(4)  $\{x | x \in \mathbf{N} \wedge x \text{ 是 } 30 \text{ 的倍数}\}$ .

15. 设  $V = \langle \mathbf{Z}, +, \cdot \rangle$ , 其中  $+$  和  $\cdot$  分别代表普通加法和乘法, 对下面给定的每个集合确定它是否构成  $V$  的子代数, 为什么?

(1)  $S_1 = \{2n | n \in \mathbf{Z}\}$ ;

(2)  $S_2 = \{2n+1 | n \in \mathbf{Z}\}$ ;

(3)  $S_3 = \{-1, 0, 1\}$ .

16. 设  $V_1 = \langle \{1, 2, 3\}, \circ, 1 \rangle$ , 其中  $x \circ y$  表示取  $x$  和  $y$  之中较大的数.  $V_2 = \langle \{5, 6\}, *, 6 \rangle$ , 其中  $x * y$  表示取  $x$  和  $y$  之中较小的数. 求出  $V_1$  和  $V_2$  的所有的子代数. 指出哪些是平凡子代数, 哪些是真子代数.

17.  $V = \langle \mathbf{R}^*, \cdot \rangle$ , 其中  $\mathbf{R}^*$  为非零实数集合,  $\cdot$  为普通乘法, 判断下面的哪些函数是  $V$  的同态? 是否为单自同态、满自同态和自同构? 计算  $V$  的同态像.

(1)  $f(x) = |x|$ ; (2)  $f(x) = 2x$ ; (3)  $f(x) = x^2$ ; (4)  $f(x) = 1/x$ ; (5)  $f(x) = -x$ ; (6)  $f(x) = x+1$ .

18.  $V_1 = \langle \mathbf{Z}, +, \cdot \rangle$ ,  $V_2 = \langle \mathbf{Z}_n, \oplus, \otimes \rangle$ , 其中  $\mathbf{Z}$  为整数集,  $+$ ,  $\cdot$  分别为普通加法与乘法,  $\mathbf{Z}_n = \{0, 1, \dots, n-1\}$ ,  $\oplus$  与  $\otimes$  分别为模  $n$  加法和模  $n$  乘法. 令  $f: \mathbf{Z} \rightarrow \mathbf{Z}_n$ ,  $f(x) = (x) \bmod n$ . 证明  $f$  为  $V_1$  到  $V_2$  的满同态映射.

19. 设  $V_1 = \langle A, \circ \rangle$ ,  $V_2 = \langle B, * \rangle$  为同类型代数系统,  $V_1 \times V_2$  是积代数, 定义函数  $f: A \times B \rightarrow A$ ,  $f(\langle x, y \rangle) = x$ , 证明  $f$  是  $V_1 \times V_2$  到  $V_1$  的同态映射.

# 第十章 群 与 环

## 10.1 群的定义及性质

半群与群都是具有一个二元运算的代数系统.

### 定义 10.1

(1) 设  $V = \langle S, \circ \rangle$  是代数系统,  $\circ$  为二元运算, 如果  $\circ$  是可结合的, 则称  $V$  为半群.

(2) 设  $V = \langle S, \circ \rangle$  是半群, 若  $e \in S$  是关于  $\circ$  运算的单位元, 则称  $V$  是幺半群, 也叫做独异点. 有时也将独异点  $V$  记作  $V = \langle S, \circ, e \rangle$ .

(3) 设  $V = \langle S, \circ \rangle$  是独异点,  $e \in S$  是关于  $\circ$  运算的单位元, 若  $\forall a \in S$ , 有  $a^{-1} \in S$ , 则称  $V$  是群. 通常将群记作  $G$ .

**例 10.1** (1)  $\langle \mathbf{Z}^+, + \rangle$ ,  $\langle \mathbf{N}, + \rangle$ ,  $\langle \mathbf{Z}, + \rangle$ ,  $\langle \mathbf{Q}, + \rangle$ ,  $\langle \mathbf{R}, + \rangle$ ,  $\langle \mathbf{C}, + \rangle$  都是半群,  $+$  是普通加法. 这些半群中除  $\langle \mathbf{Z}^+, + \rangle$  外都是独异点, 其中  $\langle \mathbf{Z}, + \rangle$ ,  $\langle \mathbf{Q}, + \rangle$ ,  $\langle \mathbf{R}, + \rangle$ ,  $\langle \mathbf{C}, + \rangle$  都是群, 分别叫做整数加群、有理数加群、实数加群和复数加群.

(2) 设  $n$  是大于 1 的正整数,  $\langle M_n(\mathbf{R}), + \rangle$  和  $\langle M_n(\mathbf{R}), \cdot \rangle$  都是半群, 也都是独异点,  $\langle M_n(\mathbf{R}), + \rangle$  也是群. 这里的  $+$  和  $\cdot$  分别表示矩阵加法和矩阵乘法.  $\langle M_n(\mathbf{R}), \cdot \rangle$  不是群, 因为不是每个  $n$  阶矩阵都有乘法逆元.

(3)  $\langle P(B), \oplus \rangle$  是半群, 也是独异点和群, 其中  $\oplus$  为集合的对称差运算.

(4)  $\langle \mathbf{Z}_n, \oplus \rangle$  是半群, 也是独异点和群, 其中  $\mathbf{Z}_n = \{0, 1, \dots, n-1\}$ ,  $\oplus$  为模  $n$  加法.

(5)  $\langle A^A, \circ \rangle$  为半群, 也是独异点, 其中  $\circ$  为函数的复合运算. 因为只有双射函数才有反函数, 请读者思考: 当  $A$  是什么集合时, 它能构成群?

(6)  $\langle \mathbf{R}^*, \circ \rangle$  为半群, 其中  $\mathbf{R}^*$  为非零实数集合,  $\circ$  运算定义如下:

$$\forall x, y \in \mathbf{R}^*, x \circ y = y$$

这个系统不构成独异点和群, 因为它没有单位元.

在半群、独异点和群中, 由于只有一个二元运算, 在不发生混淆的情况下, 经常将算符省去. 例如将  $x \circ y$  写作  $xy$ . 下面的讨论中我们将采用这种简略表示.

**例 10.2** 设  $G = \{a, b, c, d\}$ ,  $G$  上的运算由表 10.1 给出, 不难验证  $G$  是一个群. 由表中可以看出  $G$  的运算具有以下的特点:  $e$  为  $G$  中的单位元;  $G$  中的运算是可交换的; 每个元素的逆元就是它自己; 在  $a, b, c$  三个元素中, 任何两个元素运算的结果都等于另一个元素. 称这个群为 Klein

四元群,简称四元群.

表 10.1

	$e$	$a$	$b$	$c$
$e$	$e$	$a$	$b$	$c$
$a$	$a$	$e$	$c$	$b$
$b$	$b$	$c$	$e$	$a$
$c$	$c$	$b$	$a$	$e$

例 10.3 设  $\Sigma$  是有穷字母表,  $\forall k \in \mathbb{N}$ , 定义下述集合:

$$\Sigma_k = \{a_1 a_2 \cdots a_k \mid a_i \in \Sigma\}$$

是  $\Sigma$  上所有长度为  $k$  的串的集合. 当  $k=0$  时,  $\Sigma_0 = \{\lambda\}$ ,  $\lambda$  表示空串. 令  $\Sigma^* = \bigcup_{i=0}^{\infty} \Sigma_i$  表示  $\Sigma$  上所有有限长度的串的集合,  $\Sigma^+ = \Sigma^* - \{\lambda\}$  则表示  $\Sigma$  上所有长度至少为 1 的有限串的集合. 在  $\Sigma^*$  上可以定义串的连接运算,  $\forall \omega_1, \omega_2 \in \Sigma^*$ ,  $\omega_1 = a_1 a_2 \cdots a_m$ ,  $\omega_2 = b_1 b_2 \cdots b_n$  有

$$\omega_1 \omega_2 = a_1 a_2 \cdots a_m b_1 b_2 \cdots b_n$$

显然  $\Sigma^*$  关于连接运算构成一个独异点, 称为  $\Sigma$  上的字代数.  $\Sigma$  上的语言  $L$  (这里的语言指形式语言, 不是一般的自然语言) 就是  $\Sigma^*$  的一个子集.

例 10.4 某二进制码的码字  $x = x_1 x_2 \cdots x_7$  由 7 位构成, 其中  $x_1, x_2, x_3$  和  $x_4$  为数据位,  $x_5, x_6$  和  $x_7$  为校验位, 并且满足:

$$x_5 = x_1 \oplus x_2 \oplus x_3, \quad x_6 = x_1 \oplus x_2 \oplus x_4, \quad x_7 = x_1 \oplus x_3 \oplus x_4$$

这里的  $\oplus$  是模 2 加法. 设  $G$  为所有码字构成的集合, 在  $G$  上定义二元运算如下:

$$\forall x, y \in G, x \circ y = z_1 z_2 \cdots z_7, z_i = x_i \oplus y_i, i = 1, 2, \dots, 7$$

证明  $\langle G, \circ \rangle$  构成群.

证 任取  $x = x_1 x_2 \cdots x_7, y = y_1 y_2 \cdots y_7, x \circ y = z_1 z_2 \cdots z_7$ . 首先验证  $z_5 = z_1 \oplus z_2 \oplus z_3$ .

$$z_1 \oplus z_2 \oplus z_3 = (x_1 \oplus y_1) \oplus (x_2 \oplus y_2) \oplus (x_3 \oplus y_3)$$

$$= (x_1 \oplus x_2 \oplus x_3) \oplus (y_1 \oplus y_2 \oplus y_3) = x_5 \oplus y_5 = z_5$$

$z_6 = z_1 \oplus z_2 \oplus z_4$  和  $z_7 = z_1 \oplus z_3 \oplus z_4$  同理可证. 于是  $x \circ y = z \in G$ , 从而证明了封闭性.

任取  $x, y, z \in G$ , 令  $(x \circ y) \circ z = a_1 a_2 \cdots a_7, x \circ (y \circ z) = b_1 b_2 \cdots b_7$ . 下面证明  $a_i = b_i, i = 1, 2, \dots, 7$ . 由于  $\oplus$  运算满足结合律, 因此有

$$a_i = (x_i \oplus y_i) \oplus z_i = x_i \oplus (y_i \oplus z_i) = b_i$$

从而证明了  $G$  中满足结合律. 易见单位元为 0000000,  $\forall x \in G, x^{-1} = x$ . 综合上述,  $G$  构成群.

下面我们集中考虑群的一些重要的性质. 为此需要引入一些群论中常用的概念或术语.

#### 定义 10.2

(1) 若群  $G$  是有穷集, 则称  $G$  是有限群, 否则称为无限群. 群  $G$  的基数称为群  $G$  的阶.

(2) 只含单位元的群称为平凡群.

(3) 若群  $G$  中的二元运算是可交换的, 则称  $G$  为交换群或阿贝尔 (Abel) 群.

例如  $\langle \mathbf{Z}, + \rangle$  和  $\langle \mathbf{R}, + \rangle$  是无限群,  $\langle \mathbf{Z}_n, \oplus \rangle$  是有限群, 也是  $n$  阶群. Klein 四元群是 4 阶群.  $\langle \{0\}, + \rangle$  是平凡群. 上述所有的群都是交换群, 但  $n$  阶 ( $n \geq 2$ ) 实可逆矩阵的集合 (是  $M_n(\mathbf{R})$  的真子集) 关于矩阵乘法构成的群是非交换群, 因为矩阵乘法不满足交换律.

**定义 10.3** 设  $G$  是群,  $a \in G, n \in \mathbf{Z}$ , 则  $a$  的  $n$  次幂

$$a^n = \begin{cases} e, & n=0 \\ a^{n-1}a, & n>0 \\ (a^{-1})^m, & n<0, n=-m \end{cases}$$

元素的幂可以推广到半群和独异点. 但是幂指数  $n$  在半群中只能取正整数, 在独异点中只能取自然数, 只有在群中可以取负整数. 例如在  $\langle \mathbf{Z}_3, \oplus \rangle$  中有

$$2^{-3} = (2^{-1})^3 = 1^3 = 1 \oplus 1 \oplus 1 = 0$$

而在  $\langle \mathbf{Z}, + \rangle$  中有

$$3^{-5} = (3^{-1})^5 = (-3)^5 = (-3) + (-3) + (-3) + (-3) + (-3) = -15$$

**定义 10.4** 设  $G$  是群,  $a \in G$ , 使得等式  $a^k = e$  成立的最小正整数  $k$  称为  $a$  的阶 (或者周期), 记作  $|a| = k$ , 这时也称  $a$  为  $k$  阶元. 若不存在这样的正整数  $k$ , 则称  $a$  为无限阶元.

例如  $\langle \mathbf{Z}_6, \oplus \rangle$  中, 2 和 4 是 3 阶元, 3 是 2 阶元, 而 1 和 5 是 6 阶元, 0 是 1 阶元, 而在  $\langle \mathbf{Z}, + \rangle$  中, 0 是 1 阶元, 其他的整数都是无限阶元. 在 Klein 四元群中  $e$  为 1 阶元, 其他元素都是 2 阶元.

下面的定理给出了群的一些重要性质.

**定理 10.1** 设  $G$  为群, 则  $G$  中的幂运算满足:

- (1)  $\forall a \in G, (a^{-1})^{-1} = a.$
- (2)  $\forall a, b \in G, (ab)^{-1} = b^{-1}a^{-1}.$
- (3)  $\forall a \in G, a^n a^m = a^{n+m}, n, m \in \mathbf{Z}.$
- (4)  $\forall a \in G, (a^n)^m = a^{nm}, n, m \in \mathbf{Z}.$
- (5) 若  $G$  为交换群, 则  $(ab)^n = a^n b^n.$

**证** 只证(1)和(3), 其余留作练习.

(1)  $(a^{-1})^{-1}$  是  $a^{-1}$  的逆元, 而  $a$  也是  $a^{-1}$  的逆元. 根据逆元的惟一性有  $(a^{-1})^{-1} = a.$

(3) 先考虑  $n, m$  都是自然数的情况. 任意给定  $n$ , 对  $m$  进行归纳.

$m=0$  有  $a^n a^0 = a^n e = a^n = a^{n+0}$  成立.

假设对一切  $m \in \mathbf{N}$  有  $a^n a^m = a^{n+m}$  成立, 则有

$$a^n a^{m+1} = a^n (a^m a) = (a^n a^m) a = a^{n+m} a = a^{n+m+1}$$

由归纳法等式得证.

下面考虑存在负整数次幂的情况.

设  $n < 0, m \geq 0$ , 令  $n = -t, t \in \mathbf{Z}^+$ . 则

$$a^n a^m = a^{-t} a^m = (a^{-1})^t a^m = \begin{cases} a^{-(t-m)} = a^{m-t} = a^{n+m}, & t \geq m \\ a^{m-t} = a^{n+m}, & t < m \end{cases}$$

对于  $n \geq 0, m < 0$  以及  $n < 0, m < 0$  的情况同理可证.

定理 10.1(2) 中的结果可以推广到有限多个元素的情况, 即

$$(a_1 a_2 \cdots a_r)^{-1} = a_r^{-1} a_{r-1}^{-1} \cdots a_2^{-1} a_1^{-1}$$

注意上述定理中的最后一个等式只对交换群成立. 如果  $G$  是非交换群, 那么只有

$$(ab)^n = \underbrace{(ab)(ab)\cdots(ab)}_{n\uparrow}$$

**定理 10.2**  $G$  为群, 则  $G$  中适合消去律, 即对任意  $a, b, c \in G$  有

(1) 若  $ab = ac$ , 则  $b = c$ .

(2) 若  $ba = ca$ , 则  $b = c$ .

证明留作练习.

**例 10.5** 设  $G = \{a_1, a_2, \cdots, a_n\}$  是  $n$  阶群, 令

$$a_i G = \{a_i a_j \mid j = 1, 2, \cdots, n\}$$

证明  $a_i G = G$ .

**证** 由群中运算的封闭性有  $a_i G \subseteq G$ . 假设  $a_i G \subset G$ , 即  $|a_i G| < n$ . 必有  $a_j, a_k \in G$  使得

$$a_i a_j = a_i a_k \quad (j \neq k)$$

由消去律得  $a_j = a_k$ , 与  $|G| = n$  矛盾.

当  $G$  是  $n$  阶群的时候,  $a_i G$  恰好是  $G$  的运算表中第  $i$  行的全体元素. 例 10.5 说明  $G$  的运算表的每一行都是  $G$  中元素的一个排列. 不难看出, 对于每一列也有同样的性质. 如果一个代数系统的运算表不满足这个性质, 它肯定不是群. 但是, 满足这个性质的也可能不是群. 请读者给出一个反例.

**定理 10.3** 设  $G$  为群,  $a \in G$ , 且  $|a| = r$ . 设  $k$  是整数, 则

(1)  $a^k = e$  当且仅当  $r \mid k$  ( $r$  整除  $k$ )

(2)  $|a^{-1}| = |a|$

**证** (1) 充分性.

由于  $r \mid k$ , 必存在整数  $m$  使得  $k = mr$ , 所以有

$$a^k = a^{mr} = (a^r)^m = e^m = e$$

必要性. 根据带余除法, 存在整数  $m$  和  $i$  使得  $k = mr + i$ ,  $0 \leq i \leq r-1$ , 从而有

$$e = a^k = a^{mr+i} = (a^r)^m a^i = e a^i = a^i$$

因为  $|a| = r$ , 必有  $i = 0$ . 这就证明了  $r \mid k$ .

(2) 由  $(a^{-1})^r = (a^r)^{-1} = e^{-1} = e$  可知  $a^{-1}$  的阶是存在的. 令  $|a^{-1}| = t$ , 根据上面的证明有  $t \mid r$ . 这说明  $a$  的逆元的阶是  $a$  的阶的因子. 而  $a$  又是  $a^{-1}$  的逆元, 所以  $a$  的阶也是  $a^{-1}$  的阶的因子, 故有  $r \mid t$ . 从而证明了  $r = t$ , 即  $|a^{-1}| = |a|$ .

**例 10.6** 设  $G$  是群,  $a, b \in G$  是有限阶元. 证明:

$$(1) |b^{-1}ab| = |a|$$

$$(2) |ab| = |ba|$$

证 (1) 设  $|a| = r, |b^{-1}ab| = t$ . 则有

$$\begin{aligned} (b^{-1}ab)^r &= \underbrace{(b^{-1}ab)(b^{-1}ab)\cdots(b^{-1}ab)}_{r\uparrow} \\ &= b^{-1}a^rb = b^{-1}eb = e \end{aligned}$$

根据定理 10.3 得  $t|r$ .

另一方面, 由

$$a = b(b^{-1}ab)b^{-1} = (b^{-1})^{-1}(b^{-1}ab)b^{-1}$$

可知,  $(b^{-1})^{-1}(b^{-1}ab)b^{-1}$  的阶是  $b^{-1}ab$  的阶的因子, 即  $r|t$ . 从而有  $|b^{-1}ab| = |a|$ .

(2) 设  $|ab| = r, |ba| = t$ , 则有

$$\begin{aligned} (ab)^{r+1} &= \underbrace{(ab)(ab)\cdots(ab)}_{r+1\uparrow} = \underbrace{a(ba)(ba)\cdots(ba)}_{r\uparrow}b \\ &= a(ba)^rb = aeb = ab \end{aligned}$$

由消去律得  $(ab)^r = e$ , 从而可知  $r|t$ . 同理可证  $t|r$ . 因此  $|ab| = |ba|$ .

**例 10.7** 设  $G$  为有限群, 则  $G$  中阶大于 2 的元素有偶数个.

证 根据定理 10.2, 对于任意  $a \in G$  有

$$a^2 = e \Leftrightarrow a^{-1}a^2 = a^{-1}e \Leftrightarrow a = a^{-1}$$

因此对  $G$  中阶大于 2 的元素  $a$ , 必有  $a \neq a^{-1}$ . 又由于  $|a| = |a^{-1}|$ , 所以  $G$  中阶大于 2 的元素一定成对出现.  $G$  中若含有阶大于 2 的元素, 一定是偶数个. 若  $G$  中不含阶大于 2 的元素, 而 0 也是偶数.

## 10.2 子群与群的陪集分解

子群就是群的子代数.

**定义 10.5** 设  $G$  是群,  $H$  是  $G$  的非空子集, 如果  $H$  关于  $G$  中的运算构成群, 则称  $H$  是  $G$  的子群, 记作  $H \leq G$ . 若  $H$  是  $G$  的子群, 且  $H \subset G$ , 则称  $H$  是  $G$  的真子群, 记作  $H < G$ .

例如  $n\mathbb{Z}$  ( $n$  是自然数) 是整数加群  $\langle \mathbb{Z}, + \rangle$  的子群. 当  $n \neq 1$  时,  $n\mathbb{Z}$  是  $\mathbb{Z}$  的真子群.

对任何群  $G$  都存在子群.  $G$  和  $\{e\}$  都是  $G$  的子群, 称为  $G$  的平凡子群.

下面给出子群的三个判定定理.

**定理 10.4 (判定定理一)**

设  $G$  为群,  $H$  是  $G$  的非空子集.  $H$  是  $G$  的子群当且仅当下面的条件成立:

$$(1) \forall a, b \in H \text{ 有 } ab \in H.$$

$$(2) \forall a \in H \text{ 有 } a^{-1} \in H.$$

证 必要性是显然的. 为证明充分性, 只需证明  $e \in H$ .

因为  $H$  非空, 必存在  $a \in H$ . 由条件(2)可知  $a^{-1} \in H$ , 再使用条件(1)有  $aa^{-1} \in H$ , 即  $e \in H$ .

### 定理 10.5 (判定定理二)

设  $G$  为群,  $H$  是  $G$  的非空子集. 则  $H$  是  $G$  的子群当且仅当  $\forall a, b \in H$  有  $ab^{-1} \in H$ .

证 必要性. 任取  $a, b \in H$ , 由于  $H$  是  $G$  的子群, 必有  $b^{-1} \in H$ , 从而有  $ab^{-1} \in H$ .

充分性. 因为  $H$  非空, 必存在  $a \in H$ . 根据给定条件得  $aa^{-1} \in H$ , 即  $e \in H$ . 任取  $a \in H$ , 由  $e, a \in H$  得  $ea^{-1} \in H$ , 即  $a^{-1} \in H$ . 任取  $a, b \in H$ , 由刚才的证明知  $b^{-1} \in H$ . 再利用给定条件得  $a(b^{-1})^{-1} \in H$ , 即  $ab \in H$ .

综合上述, 根据判定定理一, 可知  $H$  是  $G$  的子群.

### 定理 10.6 (判定定理三)

设  $G$  为群,  $H$  是  $G$  的非空子集. 如果  $H$  是有穷集, 则  $H$  是  $G$  的子群当且仅当  $\forall a, b \in H$  有  $ab \in H$ .

证 必要性是显然的. 为证明充分性, 只需证明  $\forall a \in H$  有  $a^{-1} \in H$ .

任取  $a \in H$ , 若  $a = e$ , 则  $a^{-1} = e^{-1} = e \in H$ . 若  $a \neq e$ , 令  $S = \{a, a^2, \dots\}$ , 则  $S \subseteq H$ . 由于  $H$  是有穷集, 必有  $a^i = a^j (i < j)$ . 根据  $G$  中的消去律得  $a^{j-i} = e$ . 由  $a \neq e$  可知  $j-i > 1$ , 由此得

$$a^{j-i-1}a = e \text{ 和 } aa^{j-i-1} = e$$

从而证明了  $a^{-1} = a^{j-i-1}$ .

使用上述判定定理可以证明一些重要的子群.

**例 10.8** 设  $G$  为群,  $a \in G$ , 令

$$H = \{a^k \mid k \in \mathbb{Z}\}$$

即  $a$  的所有的幂构成的集合, 则  $H$  是  $G$  的子群, 称为由  $a$  生成的子群, 记作  $\langle a \rangle$ .

首先由  $a \in \langle a \rangle$  知道  $\langle a \rangle \neq \emptyset$ . 任取  $a^m, a^l \in \langle a \rangle$ , 则

$$a^m(a^l)^{-1} = a^m a^{-l} = a^{m-l} \in \langle a \rangle$$

根据判定定理二可知  $\langle a \rangle \leq G$ .

对于整数加群, 由 2 生成的子群是  $\langle 2 \rangle = \{2k \mid k \in \mathbb{Z}\} = 2\mathbb{Z}$ , 而在群  $\langle \mathbb{Z}_6, \oplus \rangle$  中, 由 2 生成的子群是  $\langle 2 \rangle = \{0, 2, 4\}$ . 对于 Klein 四元群  $G = \{e, a, b, c\}$  来说, 由它的每个元素生成的子群是:

$$\langle e \rangle = \{e\}, \langle a \rangle = \{e, a\}, \langle b \rangle = \{e, b\}, \langle c \rangle = \{e, c\}$$

**例 10.9** 设  $G$  为群, 令  $C$  是与  $G$  中所有的元素都可交换的元素构成的集合, 即

$$C = \{a \mid a \in G \wedge \forall x \in G (ax = xa)\}$$

则  $C$  是  $G$  的子群, 称为  $G$  的中心.

证 首先, 由  $e$  与  $G$  中所有元素的交换性可知  $e \in C$ .  $C$  是  $G$  的非空子集.

任取  $a, b \in C$ , 为证明  $ab^{-1} \in C$ , 只需证明  $ab^{-1}$  与  $G$  中所有的元素都可交换.  $\forall x \in G$ , 有

$$\begin{aligned} (ab^{-1})x &= ab^{-1}x = ab^{-1}(x^{-1})^{-1} = a(x^{-1}b)^{-1} \\ &= a(bx^{-1})^{-1} = (ax)b^{-1} = (xa)b^{-1} = x(ab^{-1}) \end{aligned}$$

由判定定理二可知  $C \leq G$ .

对于阿贝尔群  $G$ , 因为  $G$  中所有的元素互相都可交换,  $G$  的中心就等于  $G$ . 但是对某些非交换群  $G$ , 它的中心是  $\{e\}$ .

**例 10.10** 设  $G$  是群,  $H, K$  是  $G$  的子群. 证明:

(1)  $H \cap K$  也是  $G$  的子群.

(2)  $H \cup K$  是  $G$  的子群当且仅当  $H \subseteq K$  或  $K \subseteq H$ .

**证** (1) 由  $e \in H \cap K$  知  $H \cap K$  非空.

任取  $a, b \in H \cap K$ , 则  $a \in H, a \in K, b \in H, b \in K$ . 由于  $H$  和  $K$  是  $G$  的子群, 必有  $ab^{-1} \in H$  和  $ab^{-1} \in K$ . 从而推出  $ab^{-1} \in H \cap K$ . 根据判定定理二, 命题得证.

(2) 充分性是显然的. 只证必要性, 用反证法.

假设  $H \not\subseteq K$  且  $K \not\subseteq H$ , 那么存在  $h$  和  $k$  使得

$$h \in H \wedge h \notin K, k \in K \wedge k \notin H$$

这就推出  $hk \notin H$ . 若不然, 由  $h^{-1} \in H$  可得

$$k = h^{-1}(hk) \in H$$

与假设矛盾. 同理可证  $hk \notin K$ . 从而得到  $hk \notin H \cup K$ . 这与  $H \cup K$  是子群矛盾.

任取两个子群  $H_1, H_2$ , 一般说来  $H_1 \cup H_2$  不是  $G$  的子群, 而只是  $G$  的子集. 设  $B$  是  $G$  的子集, 将  $G$  的所有包含  $B$  的子群的交记作  $\langle B \rangle$ , 即

$$\langle B \rangle = \bigcap \{H \mid B \subseteq H \wedge H \leq G\}$$

易见  $\langle B \rangle$  是  $G$  的子群, 称为由  $B$  生成的子群. 不难证明  $\langle B \rangle$  中的元素恰为如下形式:

$$a_1 a_2 \cdots a_k, k \in \mathbb{Z}^+$$

其中  $a_i$  是  $B$  中的元素或者其逆元.

设  $G$  为群, 令  $S = \{H \mid H \text{ 是 } G \text{ 的子群}\}$  是  $G$  的所有子群的集合, 在  $S$  上定义关系  $R$  如下:

$$\forall A, B \in S, \quad ARB \Leftrightarrow A \text{ 是 } B \text{ 的子群}$$

那么  $\langle S, R \rangle$  构成偏序集, 称为群  $G$  的子群格. Klein 四元群  $G$  与模 12 加群  $\mathbb{Z}_{12}$  的子群格如图 10.1 所示.

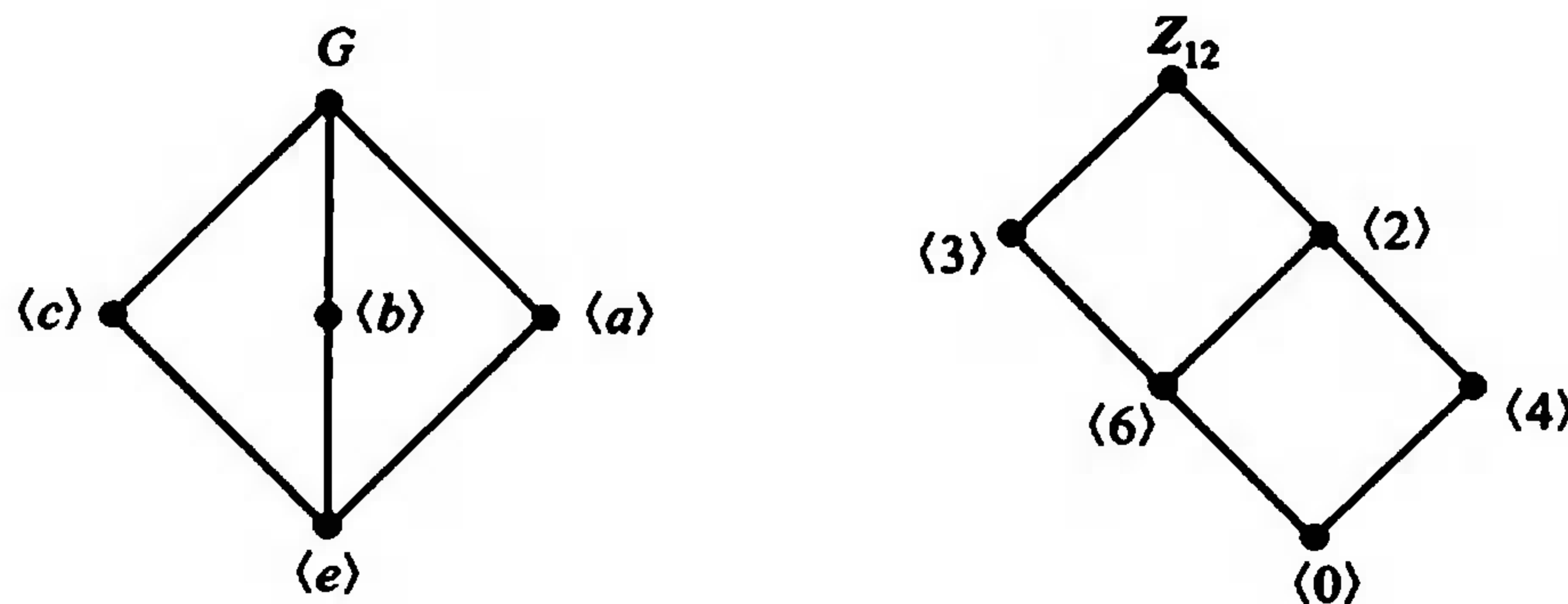


图 10.1

下面考虑群的分解. 先定义陪集.

**定义 10.6** 设  $H$  是群  $G$  的子群,  $a \in G$ . 令

$$Ha = \{ha \mid h \in H\}$$

称  $Ha$  是子群  $H$  在  $G$  中的右陪集. 称  $a$  为  $Ha$  的代表元素.

**例 10.11** 设  $G = \{e, a, b, c\}$  是 Klein 四元群,  $H = \{e, a\}$  是  $G$  的子群. 那么  $H$  的所有的右陪集是:

$$He = \{e, a\} = H = Ha$$

$$Hb = \{b, c\} = Hc$$

不同的右陪集只有两个, 即  $H$  和  $\{b, c\}$ .

下面考虑右陪集的性质.

**定理 10.7** 设  $H$  是群  $G$  的子群, 则

$$(1) He = H$$

$$(2) \forall a \in G \text{ 有 } a \in Ha.$$

证 (1)  $He = \{he \mid h \in H\} = \{h \mid h \in H\} = H$

(2) 任取  $a \in G$ , 由  $a = ea$  和  $ea \in Ha$  得  $a \in Ha$ .

**定理 10.8** 设  $H$  是群  $G$  的子群, 则  $\forall a, b \in G$  有

$$a \in Hb \Leftrightarrow ab^{-1} \in H \Leftrightarrow Ha = Hb$$

证 先证  $a \in Hb \Leftrightarrow ab^{-1} \in H$ .

$$\begin{aligned} a \in Hb &\Leftrightarrow \exists h(h \in H \wedge a = hb) \\ &\Leftrightarrow \exists h(h \in H \wedge ab^{-1} = h) \Leftrightarrow ab^{-1} \in H \end{aligned}$$

再证  $a \in Hb \Leftrightarrow Ha = Hb$ .

充分性. 若  $Ha = Hb$ , 由  $a \in Ha$  可知必有  $a \in Hb$ .

必要性. 由  $a \in Hb$  可知存在  $h \in H$  使得  $a = hb$ , 即  $b = h^{-1}a$ . 任取  $h_1 a \in Ha$ , 则有

$$h_1 a = h_1(hb) = (h_1 h)b \in Hb$$

从而得到  $Ha \subseteq Hb$ . 反之, 任取  $h_1 b \in Hb$ , 则有

$$h_1 b = h_1(h^{-1}a) = (h_1 h^{-1})a \in Ha$$

从而得到  $Hb \subseteq Ha$ . 综合上述,  $Ha = Hb$  得证.

定理 10.8 给出了两个右陪集相等的充分必要条件, 并且说明在右陪集中的任何元素都可以作为它的代表元素.

**定理 10.9** 设  $H$  是群  $G$  的子群, 在  $G$  上定义二元关系:  $\forall a, b \in G$ ,

$$\langle a, b \rangle \in R \Leftrightarrow ab^{-1} \in H$$

则  $R$  是  $G$  上的等价关系, 且  $[a]_R = Ha$ .

证 为证明  $R$  是等价的, 只需证明  $R$  的自反、对称、传递的性质. 这个证明留给读者思考. 这里只证明  $\forall a \in G, [a]_R = Ha$ . 任取  $b \in G$ , 则有

$$b \in [a]_R \Leftrightarrow \langle a, b \rangle \in R \Leftrightarrow ab^{-1} \in H$$

根据定理 10.8 有

$$ab^{-1} \in H \Leftrightarrow Ha = Hb \Leftrightarrow b \in Ha$$

这就推出  $b \in [a]_R \Leftrightarrow b \in Ha$ , 从而证明了  $[a]_R = Ha$ .

**推论** 设  $H$  是群  $G$  的子群, 则

$$(1) \forall a, b \in G, Ha = Hb \text{ 或 } Ha \cap Hb = \emptyset$$

$$(2) \cup \{Ha \mid a \in G\} = G$$

**证** 由定理 10.9 和 7.14 可得.

根据以上定理和推论可以知道, 给定群  $G$  的一个子群  $H$ ,  $H$  的所有右陪集的集合  $\{Ha \mid a \in G\}$  恰好构成  $G$  的一个划分, 而且可进一步证明, 这个划分的所有划分块都与  $H$  等势.

以上已经对子群  $H$  的右陪集及其性质进行了讨论, 类似地, 也可以定义  $H$  的左陪集,

$$aH = \{ah \mid h \in H\}, a \in G$$

并证明关于左陪集的下述性质:

$$1. eH = H$$

$$2. \forall a \in G, a \in aH$$

$$3. \forall a, b \in G, a \in bH \Leftrightarrow b^{-1}a \in H \Leftrightarrow aH = bH$$

4. 若在  $G$  上定义二元关系  $R$ ,

$$\forall a, b \in G, \langle a, b \rangle \in R \Leftrightarrow b^{-1}a \in H$$

则  $R$  是  $G$  上的等价关系, 且  $[a]_R = aH$ .

$$5. \forall a \in G, H \approx aH$$

一般说来, 对于群  $G$  的子群  $H$  和元素  $a$  不能保证  $Ha = aH$ . 如果对于所有的  $a \in G$  都有  $aH = Ha$ , 那么称  $H$  为  $G$  的正规子群或不变子群. 记作  $H \triangleleft G$ . 任何群  $G$  都有正规子群, 因为它的两个平凡子群  $\{e\}$  和  $G$  都是正规的.

尽管  $H$  的右陪集  $Ha$  和左陪集  $aH$  可能不一样, 但  $H$  在  $G$  中的右陪集的个数和左陪集的个数却是相等的. 令

$$S = \{Ha \mid a \in G\} \quad \text{和} \quad T = \{aH \mid a \in G\}$$

分别表示  $H$  的右陪集和左陪集的集合, 定义函数

$$f: S \rightarrow T, f(Ha) = a^{-1}H, \forall a \in G$$

不难证明  $f$  是  $S$  到  $T$  的双射函数. 由于  $H$  在  $G$  中的右陪集数和左陪集数相等, 今后不再区分右陪集数和左陪集数, 而统称  $H$  在  $G$  中的陪集数, 也叫做  $H$  在  $G$  中的指数, 记作  $[G:H]$ .

对于有限群  $G$ ,  $H$  在  $G$  中的指数  $[G:H]$  和  $|G|$  及  $|H|$  有着密切的关系, 这就是著名的拉格朗日定理.

**定理 10.10 (拉格朗日定理)** 设  $G$  是有限群,  $H$  是  $G$  的子群, 则

$$|G| = |H| \cdot [G:H]$$

**证** 设  $[G:H] = r$ ,  $a_1, a_2, \dots, a_r$  分别是  $H$  的  $r$  个右陪集的代表元素. 根据定理 10.9 的推论有

$$G = Ha_1 \cup Ha_2 \cup \dots \cup Ha_r$$

由于这  $r$  个右陪集是两两不交的, 所以有

$$|G| = |Ha_1| + |Ha_2| + \cdots + |Ha_r|$$

因为  $|Ha_i| = |H|, i = 1, 2, \cdots, r$ . 将这些等式代入上式得

$$|G| = |H| \cdot r = |H| \cdot [G:H]$$

**推论 1** 设  $G$  是  $n$  阶群, 则  $\forall a \in G, |a|$  是  $n$  的因子, 且有  $a^n = e$ .

**证** 任取  $a \in G$ , 则  $\langle a \rangle$  是  $G$  的子群. 由拉格朗日定理知  $\langle a \rangle$  的阶是  $n$  的因子. 另一方面,  $\langle a \rangle$  是由  $a$  生成的子群, 若  $|a| = r$ , 则

$$\langle a \rangle = \{a^0 = e, a^1, a^2, \cdots, a^{r-1}\}$$

这说明  $\langle a \rangle$  的阶与  $|a|$  相等, 所以  $|a|$  是  $n$  的因子. 根据定理 10.3(1) 必有  $a^n = e$ .

**推论 2** 设  $G$  是素数阶的群, 则存在  $a \in G$  使得  $G = \langle a \rangle$ .

**证** 设  $|G| = p, p$  是素数. 由  $p \geq 2$  知  $G$  中必存在非单位元. 任取  $a \in G, a \neq e$ , 则  $\langle a \rangle$  是  $G$  的子群. 根据拉格朗日定理,  $\langle a \rangle$  的阶是  $p$  的因子, 即  $\langle a \rangle$  的阶是  $p$  或 1. 显然  $\langle a \rangle$  的阶不等于 1. 这就推出  $G = \langle a \rangle$ .

拉格朗日定理对分析有限群中元素的阶很有用. 但注意到这个定理的逆命题并不为真. 尽管有时候  $r$  是  $n$  的因子, 但  $n$  阶群  $G$  中不一定含有  $r$  阶元. 例如 Klein 四元群中就没有 4 阶元.

**例 10.12** 证明 6 阶群中必含有 3 阶元.

**证** 设  $G$  是 6 阶群, 由拉格朗日定理的推论 1 可知  $G$  中的元素只可能是 1 阶, 2 阶, 3 阶或 6 阶元.

若  $G$  中含有 6 阶元, 设这个 6 阶元是  $a$ , 则  $a^2$  是 3 阶元.

若  $G$  中不含 6 阶元, 下面证明  $G$  中必含有 3 阶元. 如若不然,  $G$  中只含 1 阶和 2 阶元, 即  $\forall a \in G$ , 有  $a^2 = e$ . 由本章练习第 15 题可知  $G$  是阿贝尔群. 取  $G$  中两个不同的 2 阶元  $a$  和  $b$ , 令

$$H = \{e, a, b, ab\}$$

易证  $H$  是  $G$  的子群, 但  $|H| = 4, |G| = 6$ , 与拉格朗日定理矛盾.

**例 10.13** 证明阶小于 6 的群都是阿贝尔群.

**证** 1 阶群是平凡的, 显然是阿贝尔群. 2、3 和 5 都是素数. 由拉格朗日定理的推论 2 可知 2 阶、3 阶和 5 阶群都是由一个元素生成的群. 它们都是阿贝尔群(见习题十第 26 题).

设  $G$  是 4 阶群. 若  $G$  中含有 4 阶元, 比如说  $a$ , 则  $G = \langle a \rangle$ , 由刚才的分析可知  $G$  是阿贝尔群, 若  $G$  中不含 4 阶元, 根据拉格朗日定理,  $G$  中只含 1 阶和 2 阶元. 由本章练习第 15 题可知  $G$  也是阿贝尔群.

下面给出一个群分解的实际例子——Slepian 译码表.

考虑计算机通信中的一种编码  $C$ .  $C$  中的一个码字  $v = a_1 a_2 \cdots a_n (a_i \in \{0, 1\})$  可以看作  $\{0, 1\}$  集合上的  $n$  维向量, 所有  $2^n$  个  $n$  维向量构成  $n$  维线性空间  $F_2^n$ .  $F_2^n$  的一个  $k$  维子空间称作  $\{0, 1\}$  集合上的一个  $k$  维线性码, 记作  $[n, k]$  码. 由于  $C$  是  $k$  维的, 因此存在  $k$  个线性独立的向量  $v_1, v_2, \cdots, v_k$  作为  $C$  的一组基, 任意  $v \in C$  都可以唯一地表示成  $v = x_1 v_1 + x_2 v_2 + \cdots + x_k v_k, x_i \in \{0, 1\}, i = 1, 2, \cdots, k$ . 于是  $|C| = 2^k$ . 设  $C$  是  $\{0, 1\}$  集合上的  $[n, k]$  码, 因为  $C$  关于向量加法封闭, 向量加

法满足结合律,单位元是  $n$  维 0 向量,向量  $v$  的加法逆元就是自身,于是  $C$  关于向量加法构成群,且是  $F_2^n$  的子群. 考虑  $C$  在  $F_2^n$  中的陪集  $C + a, a \in F_2^n$ . 根据拉格朗日定理,不同的陪集有  $2^{n-k}$  个.

前面的例 10.4 中的编码就是一种  $[7,4]$  码,我们把这个码记作  $C_1$ .  $C_1$  有  $2^4 = 16$  个码字,它们的前 4 位恰好从 0000 到 1111,后 3 个校验位根据公式由前 3 位确定. 即:

$$C_1 = \{0000000, 0001011, 0010101, 0011110, 0100110, 0101101, 0110011, 0111000, \\ 1000111, 1001100, 1010010, 1011001, 1100001, 1101010, 1110100, 1111111\}$$

不难验证 1000111, 0100110, 0010101, 0001011 是  $C_1$  的一组基.  $C_1$  在  $F_2^7$  中有 8 个不同的陪集.

下面考虑译码. 因为在信息传输中有干扰,有时候发送的码字是  $v$ ,但接收到的向量  $u$  可能根本不是  $C$  中的码字. 这时候需要对  $u$  进行纠错,一般将它译成  $C$  中与它最接近的码字(即不同的位数最少的码字,这个原则称为最近距离译码原则).  $C$  的译码阵列由  $F_2^n$  中的全体向量构成,每个陪集占一行,共有  $2^{n-k}$  行  $2^k$  列. 构成规则如下:第一行由  $C$  中的全体码字构成;第二行是陪集  $C + a_1$ ,其中  $a_1$  是  $F_2^n - C$  中 1 的个数最少且数值最小的向量;第三行是陪集  $C + a_2$ ,其中  $a_2$  是  $F_2^n - C - (C + a_1)$  中 1 的个数最少且数值最小的向量;... 称这个译码阵列为 Slepian 译码表. 假若接收到的  $u$  属于陪集  $C + a_j$ ,由阵列的构成知道  $a_j$  恰好排在这一行的第一列,这时将  $u$  译作  $u + a_j$ . 因为  $a_j + a_j = 0$  (这里的 0 指 0 向量),因此  $u = v + a_j \Leftrightarrow v = u + a_j$ . 我们把译码表的第一列称作错误向量. 可以证明这种译码方法符合最近距离译码原则.

下面以一个简单的码  $C = \{0000, 0110, 1001, 1111\}$  来说明这种译码方法. 码  $C$  是一个  $[4,2]$  码,它的一组基是  $\{0110, 1001\}$ . 整个向量空间  $F_2^4$  有 16 个向量,  $C$  在  $F_2^4$  中有 4 个陪集,因此  $C$  的 Slepian 译码表有 4 行,如表 10.2 所示,第一行恰好就是码  $C$ .

表 10.2

	错误 向量			
$C$	0000	0110	1001	1111
$C + 0001$	0001	0111	1000	1110
$C + 0010$	0010	0100	1011	1101
$C + 0011$	0011	0101	1010	1100

如果接收到的是 1001,那么它就是  $C$  中的码字,在译码时就译作 1001;如果接收到的是 1101,这不是  $C$  中的码字,通过在表中查找,知道 1101 属于  $C + 0010$ ,找到错误向量 0010,于是将 1101 译作  $1101 + 0010 = 1111$ ,而 1111 恰好是 1101 所在列的第一个元素,这正是一个距它最近的码字.

### 10.3 循环群与置换群

下面介绍两类重要的群:循环群和置换群. 先考虑循环群.

**定义 10.7** 若存在  $a \in G$  使得  $G = \langle a \rangle$ , 则称  $G$  是循环群, 称  $a$  为  $G$  的生成元.

循环群  $G = \langle a \rangle$  根据生成元  $a$  的阶可以分成两类:  $n$  阶循环群和无限循环群. 设  $G = \langle a \rangle$  是循环群, 若  $a$  是  $n$  阶元, 则

$$G = \{a^0 = e, a^1, a^2, \dots, a^{n-1}\}$$

那么  $|G| = n$ , 称  $G$  为  $n$  阶循环群. 若  $a$  是无限阶元, 则

$$G = \{a^{\pm 0} = e, a^{\pm 1}, a^{\pm 2}, \dots\}$$

这时称  $G$  为无限循环群.

例如整数加群  $\langle \mathbb{Z}, + \rangle$  是无限循环群, 它的生成元是 1 和 -1. 而模 6 整数加群  $\langle \mathbb{Z}_6, \oplus \rangle$  是 6 阶循环群, 它的生成元是 1 和 5.

对于循环群  $G = \langle a \rangle$ , 它的生成元可能不止一个, 怎样求出它的所有生成元呢? 请看下面的定理.

**定理 10.11** 设  $G = \langle a \rangle$  是循环群.

(1) 若  $G$  是无限循环群, 则  $G$  只有两个生成元, 即  $a$  和  $a^{-1}$ .

(2) 若  $G$  是  $n$  阶循环群, 则  $G$  含有  $\phi(n)$  个生成元<sup>①</sup>. 对于任何小于  $n$  且与  $n$  互素的自然数  $r$ ,  $a^r$  是  $G$  的生成元.

**证** (1) 显然  $\langle a^{-1} \rangle \subseteq G$ . 为证明  $G \subseteq \langle a^{-1} \rangle$ , 只需证明对任意  $a^k \in G$ ,  $a^k$  都可以表成  $a^{-1}$  的幂. 由定理 10.1 有

$$a^k = (a^{-1})^{-k}$$

从而得到  $G = \langle a^{-1} \rangle$ ,  $a^{-1}$  是  $G$  的生成元.

再证明  $G$  只有  $a$  和  $a^{-1}$  这两个生成元. 假设  $b$  也是  $G$  的生成元, 则  $G = \langle b \rangle$ . 由  $a \in G$  可知存在整数  $t$  使得  $a = b^t$ . 又由  $b \in G = \langle a \rangle$  知存在整数  $m$  使得  $b = a^m$ . 从而得到

$$a = b^t = (a^m)^t = a^{mt}$$

由  $G$  中的消去律得

$$a^{mt-1} = e$$

因为  $G$  是无限群, 必有  $mt - 1 = 0$ . 从而证明了  $m = t = 1$  或  $m = t = -1$ , 即  $b = a$  或  $b = a^{-1}$ .

(2)  $n = 1$  时显然成立, 因此只需证明: 对任何正整数  $r$  ( $r < n, n > 1$ ),  $a^r$  是  $G$  的生成元当且仅当  $n$  与  $r$  互素.

充分性. 设  $r$  与  $n$  互素, 且  $r < n$ , 那么存在整数  $u$  和  $v$  使得

$$ur + vn = 1 \quad (\text{见数论部分定理 19.8})$$

因此由定理 10.1 和  $a^n = e$  有

$$a = a^{ur+vn} = (a^r)^u (a^n)^v = (a^r)^u$$

这就推出  $\forall a^k \in G, a^k = (a^r)^{uk} \in \langle a^r \rangle$ , 即  $G \subseteq \langle a^r \rangle$ . 另一方面, 显然有  $\langle a^r \rangle \subseteq G$ . 所以  $a^r$  是  $G$  的生成元.

<sup>①</sup>  $\phi(n)$  是欧拉函数, 表示  $0, 1, \dots, n-1$  中与  $n$  互素的数的个数 (见例 6.6).

必要性. 设  $a'$  是  $G$  的生成元, 则  $|a'| = n$ . 令  $r$  与  $n$  的最大公约数为  $d$ , 则存在正整数  $t$  使得  $r = dt$ . 因此有

$$(a')^{\frac{n}{d}} = (a^{dt})^{\frac{n}{d}} = (a^n)^t = e$$

根据定理 10.3 知  $|a'|$  是  $n/d$  的因子, 即  $n$  整除  $n/d$ . 从而证明了  $d = 1$ .

**例 10.14** (1) 设  $G = \langle \mathbb{Z}_9, \oplus \rangle$  是模 9 的整数加群, 则  $\phi(9) = 6$ . 小于或等于 9 且与 9 互素的数是 1, 2, 4, 5, 7, 8. 根据定理 10.11,  $G$  的生成元是 1, 2, 4, 5, 7 和 8.

(2) 设  $G = 3\mathbb{Z} = \{3z | z \in \mathbb{Z}\}$ ,  $G$  上的运算是普通加法. 那么  $G$  只有两个生成元: 3 和 -3.

下面考虑循环群的子群, 一般说来, 求一个有限群的子群不是一件容易的事. 但对于循环群来说可以直接求出它的所有的子群. 请看下面的定理.

### 定理 10.12

(1) 设  $G = \langle a \rangle$  是循环群, 则  $G$  的子群仍是循环群.

(2) 若  $G = \langle a \rangle$  是无限循环群, 则  $G$  的子群除  $\{e\}$  以外都是无限循环群.

(3) 若  $G = \langle a \rangle$  是  $n$  阶循环群, 则对  $n$  的每个正因子  $d$ ,  $G$  恰好含有一个  $d$  阶子群.

**证** (1) 设  $H$  是  $G = \langle a \rangle$  的子群, 若  $H = \{e\}$ , 显然  $H$  是循环群; 否则取  $H$  中的最小正方幂元  $a^m$ , 下面证明  $a^m$  是  $H$  的生成元.

易见  $\langle a^m \rangle \subseteq H$ . 为证明  $H \subseteq \langle a^m \rangle$ , 只需证明  $H$  中的任何元素都可以表成  $a^m$  的整数次幂. 任取  $a^l \in H$ , 由除法可知存在整数  $q$  和  $r$ , 使得  $l = qm + r$ , 其中  $0 \leq r < m$ , 因此有

$$a^l = a^{l - qm} = a^l (a^m)^{-q}$$

由  $a^l, a^m \in H$  且  $H$  是  $G$  的子群可知  $a^l \in H$ , 因为  $a^m$  是  $H$  中最小正方幂元, 必有  $r = 0$ . 这就推出

$$a^l = (a^m)^q \in \langle a^m \rangle$$

(2) 设  $G = \langle a \rangle$  是无限循环群,  $H$  是  $G$  的子群. 若  $H \neq \{e\}$ , 根据上面证明可知  $H = \langle a^m \rangle$ , 其中  $a^m$  为  $H$  中最小正方幂元. 假若  $|H| = t$ , 则  $|a^m| = t$ , 从而得到  $a^{mt} = e$ . 这与  $a$  为无限阶元矛盾.

(3) 设  $G = \langle a \rangle$  是  $n$  阶循环群, 则

$$G = \{a^0 = e, a^1, \dots, a^{n-1}\}$$

根据拉格朗日定理,  $G$  的每个子群的阶都是  $n$  的因子. 下面证明对于  $n$  的每个正因子  $d$  都存在一个  $d$  阶子群. 易见  $H = \langle a^{n/d} \rangle$  是  $G$  的  $d$  阶子群. 假设  $H_1 = \langle a^m \rangle$  也是  $G$  的  $d$  阶子群, 其中  $a^m$  为  $H_1$  中的最小正方幂元. 则由  $(a^m)^d = e$  可知,  $n$  整除  $md$ , 即  $n/d$  整除  $m$ . 令  $m = (n/d) \cdot l$ ,  $l$  是整数, 则有

$$a^m = (a^{n/d})^l \in H$$

这就推出  $H_1 \subseteq H$ . 又由于  $|H_1| = |H| = d$ , 得  $H_1 = H$ .

根据这个定理的证明不难得到求循环群子群的方法, 如果  $G = \langle a \rangle$  是无限循环群, 那么  $\langle a^m \rangle$  是  $G$  的子群, 其中  $m$  是自然数, 并且容易证明对于不同的自然数  $m$  和  $t$ ,  $\langle a^m \rangle$  和  $\langle a^t \rangle$  是不同的子群. 如果  $G = \langle a \rangle$  是  $n$  阶循环群, 先求出  $n$  的所有的正因子. 对于每个正因子  $d$ ,  $\langle a^{n/d} \rangle$  是  $G$  的惟一的  $d$  阶子群.

**例 10.15** 设  $G_1$  是整数加群,  $G_2$  是模 12 加群, 求出  $G_1$  与  $G_2$  的所有子群.

**解**  $G_1$  的生成元为 1 和 -1. 易见  $1^m = m, m \in \mathbf{N}$ . 所以  $G_1$  的子群是  $m\mathbf{Z}, m \in \mathbf{N}$ . 即

$$\langle 0 \rangle = \{0\} = 0\mathbf{Z}$$

$$\langle m \rangle = \{mz | z \in \mathbf{Z}\} = m\mathbf{Z}, m > 0$$

$G_2$  是 12 阶循环群. 12 的正因子是 1, 2, 3, 4, 6 和 12, 因此  $G_2$  的子群是:

$\langle 12 \rangle = \langle 0 \rangle = \{0\}$	1 阶子群
$\langle 6 \rangle = \{0, 6\}$	2 阶子群
$\langle 4 \rangle = \{0, 4, 8\}$	3 阶子群
$\langle 3 \rangle = \{0, 3, 6, 9\}$	4 阶子群
$\langle 2 \rangle = \{0, 2, 4, 6, 8, 10\}$	6 阶子群
$\langle 1 \rangle = \mathbf{Z}_{12}$	12 阶子群

下面考虑另一类重要的群——置换群. 先定义  $n$  元置换和置换的乘法.

**定义 10.8** 设  $S = \{1, 2, \dots, n\}$ ,  $S$  上的任何双射函数  $\sigma: S \rightarrow S$  称为  $S$  上的  $n$  元置换. 一般将  $n$  元置换  $\sigma$  记为

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

例如  $S = \{1, 2, 3, 4, 5\}$ , 则

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 1 & 5 \end{pmatrix}, \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 4 & 5 \end{pmatrix}$$

都是 5 元置换.

**定义 10.9** 设  $\sigma, \tau$  是  $n$  元置换,  $\sigma$  和  $\tau$  的复合  $\sigma \circ \tau$  也是  $n$  元置换, 称为  $\sigma$  与  $\tau$  的乘积, 记作  $\sigma\tau$ .

例如上面的 5 元置换  $\sigma$  和  $\tau$  有

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 3 & 5 \end{pmatrix}, \tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 1 & 5 \end{pmatrix}$$

**定义 10.10** 设  $\sigma$  是  $S = \{1, 2, \dots, n\}$  上的  $n$  元置换. 若

$$\sigma(i_1) = i_2, \sigma(i_2) = i_3, \dots, \sigma(i_{k-1}) = i_k, \sigma(i_k) = i_1$$

且保持  $S$  中的其他元素不变, 则称  $\sigma$  为  $S$  上的  $k$  阶轮换, 记作  $(i_1 i_2 \cdots i_k)$ . 若  $k=2$ , 称  $\sigma$  为  $S$  上的对换.

设  $S = \{1, 2, \dots, n\}$ , 对于任何  $S$  上的  $n$  元置换  $\sigma$  一定存在着一个有限序列  $i_1, i_2, \dots, i_k, k \geq 1$ , 使得

$$\sigma(i_1) = i_2, \sigma(i_2) = i_3, \dots, \sigma(i_{k-1}) = i_k, \sigma(i_k) = i_1$$

令  $\sigma_1 = (i_1 i_2 \cdots i_k)$ . 它是从  $\sigma$  中分解出来的第一个轮换. 根据函数的复合定义可将  $\sigma$  写作  $\sigma_1 \sigma'$ , 其中  $\sigma'$  作用于  $S - \{i_1, i_2, \dots, i_k\}$  上的元素. 继续对  $\sigma'$  进行类似的分解. 由于  $S$  中只有  $n$  个元素, 经过有限步以后, 必得到  $\sigma$  的轮换分解式

$$\sigma = \sigma_1 \sigma_2 \cdots \sigma_l$$

不难看出,在上述分解式中任何两个轮换都作用于不同的元素上,我们称它们是不交的.因此,可以说:任何  $n$  元置换都可以表示成不交的轮换之积.

**例 10.16** 设  $S = \{1, 2, \dots, 8\}$

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 3 & 6 & 4 & 2 & 1 & 8 & 7 \end{pmatrix}$$

是 8 元置换. 考虑  $\sigma$  的分解式. 观察到

$$\sigma(1) = 5, \sigma(5) = 2, \sigma(2) = 3, \sigma(3) = 6, \sigma(6) = 1$$

所以从  $\sigma$  中分解出来的第一个轮换是  $(1\ 5\ 2\ 3\ 6)$ ,  $S$  中剩下的元素是 4, 7, 8. 由  $\sigma(4) = 4$  得到 1 阶轮换  $(4)$ , 它是从  $\sigma$  中分解出来的第二个轮换. 对于剩下的元素 7 和 8 有  $\sigma(7) = 8, \sigma(8) = 7$ . 这样就得到第三个轮换  $(7\ 8)$ . 至此为止,  $S$  中的元素都被分解完毕. 因此可以写出  $\sigma$  的轮换表示式

$$\sigma = (1\ 5\ 2\ 3\ 6) (4) (7\ 8)$$

为了使得轮换表示式更为简洁,通常省略其中的 1 阶轮换,例如  $\sigma$  可以写作  $(1\ 5\ 2\ 3\ 6) (7\ 8)$ . 如果  $n$  元置换的轮换表示式中全是 1 阶轮换,例如 8 元恒等置换  $(1) (2) \cdots (8)$ , 只能省略其中的 7 个 1 阶轮换,而将它简记为  $(1)$ .

可以证明将  $n$  元置换分解为不交的轮换之积时,它的表示式是惟一的. 这里的惟一性是说:若

$$\sigma = \sigma_1 \sigma_2 \cdots \sigma_l \quad \text{和} \quad \sigma = \tau_1 \tau_2 \cdots \tau_s$$

是  $\sigma$  的两个轮换表示式,则有

$$\{\sigma_1, \sigma_2, \dots, \sigma_l\} = \{\tau_1, \tau_2, \dots, \tau_s\}$$

换句话说,由于分解式中的任意两个轮换都作用于  $S$  的不同元素上,根据函数复合的性质可以证明,交换轮换的次序以后得到的仍是相等的  $n$  元置换. 因此在不考虑表示式中轮换的次序的情况下,该表示式是惟一的.

设  $S = \{1, 2, \dots, n\}$ ,  $\sigma$  是  $S$  上的  $k$  阶轮换,那么  $\sigma$  可以进一步表成对换之积. 不难证明

$$(i_1\ i_2 \cdots i_k) = (i_1\ i_2) (i_1\ i_3) \cdots (i_1\ i_k)$$

回顾关于  $n$  元置换的轮换表示,任何  $n$  元置换都可以惟一地表示成不交的轮换之积,而任何轮换又可以进一步表示成对换之积,所以任何  $n$  元置换都可以表成对换之积. 例如 8 元置换

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 3 & 6 & 4 & 2 & 1 & 8 & 7 \end{pmatrix}$$

的轮换和对换表示式分别为

$$\sigma = (1\ 5\ 2\ 3\ 6) (7\ 8) = (1\ 5) (1\ 2) (1\ 3) (1\ 6) (7\ 8)$$

对换表示与轮换表示都是  $n$  元置换的表示式. 它们的不同点在于:轮换表示式中的轮换是不交的,而对换表示式中的对换是允许有交的. 轮换表示式是惟一的,而对换表示式是不惟一的. 例

如 4 元置换  $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$  可以有下面不同的对换表示:

$$\sigma = (1\ 2)(1\ 3) \text{ 和 } \sigma = (1\ 4)(2\ 4)(3\ 4)(1\ 4)$$

尽管  $n$  元置换的对换表示式是不惟一的,但可以证明表示式中所含对换个数的奇偶性是不变的.例如上面的 4 元置换只能表示成偶数个对换之积,而 4 元置换  $\tau = (1\ 3\ 2\ 4)$  只能表示成奇数个对换之积.如果  $n$  元置换  $\sigma$  可以表成奇数个对换之积,则称  $\sigma$  为奇置换,否则称为偶置换,在偶置换和奇置换之间存在一一对应,因此奇置换和偶置换各有  $n!/2$  个.

考虑所有的  $n$  元置换构成的集合  $S_n$ .任何两个  $n$  元置换之积仍旧是  $n$  元置换,所以  $S_n$  关于置换的乘法是封闭的.置换的乘法满足结合律.恒等置换  $(1)$  是  $S_n$  中的单位元(见定理 8.3).对于任何  $n$  元置换  $\sigma \in S_n$ ,逆置换  $\sigma^{-1} \in S_n$  是  $\sigma$  的逆元(见定理 8.5).这就证明了  $S_n$  关于置换的乘法构成一个群,称为  $n$  元对称群.

**例 10.17** 设  $S = \{1, 2, 3\}$ , 则 3 元对称群  $S_3 = \{(1), (12), (13), (23), (123), (132)\}$ , 其运算表如表 10.3 所示.

表 10.3

	(1)	(12)	(13)	(23)	(123)	(132)
(1)	(1)	(12)	(13)	(23)	(123)	(132)
(12)	(12)	(1)	(123)	(132)	(13)	(23)
(13)	(13)	(132)	(1)	(123)	(23)	(12)
(23)	(23)	(123)	(132)	(1)	(12)	(13)
(123)	(123)	(23)	(12)	(13)	(132)	(1)
(132)	(132)	(13)	(23)	(12)	(1)	(123)

下面考虑  $S_n$  的子群. 设  $A_n$  是所有的  $n$  元偶置换的集合. 使用子群的判定定理不难证明  $A_n$  是  $S_n$  的子群, 称为  $n$  元交错群.

例如  $S_3 = \{(1), (12), (13), (23), (123), (132)\}$ . 其中的偶置换是  $(1), (123)$  和  $(132)$ . 因此 3 元交错群  $A_3 = \{(1), (123), (132)\}$ .

对于  $S_n$  来说, 它的所有子群都叫做  $n$  元置换群,  $n$  元对称群  $S_n$ ,  $n$  元交错群  $A_n$  都是  $n$  元置换群的特例.

以  $S_3$  为例, 除了  $S_3$  和  $A_3$  以外, 它的其他子群是:

$\{(1), (12)\}$	2 阶子群
$\{(1), (13)\}$	2 阶子群
$\{(1), (23)\}$	2 阶子群
$\{(1)\}$	1 阶子群

这三个 2 阶子群都不是正规子群. 两个平凡子群和  $A_3$  是正规子群.

置换群经常出现在具有对称结构的实际系统中. 考虑下面一个着色问题的例子.

使用黑白两种颜色对图 10.2 中的方格图形进行着色, 每个方格一种颜色. 如果允许方格图

形围绕中心点旋转,问不同的着色方案有多少种? 如果不考虑图形的运动,每个方格有 2 种可能的颜色选择,总计有 16 个着色方案. 围绕中心逆时针旋转有 4 种可能:0 度、90 度、180 度、270 度. 这些旋转作用在方格上,由于方格上的文字被置换,从而导致了对着色方案的置换. 令  $N = \{1, 2, 3, 4\}$  代表 4 个方格的集合,4 种旋转的集合  $G = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$  恰好构成  $N$  上的一个置换群. 如果一种方案在  $G$  中置换作用下变成另一种方案,就说这两个方案属于同一个轨道. 那么,我们的问题是:在  $G$  作用下对  $N$  上方格的着色方案被分解成多少个不同的轨道?

1	2
4	3

图 10.2

解决这个计数问题的定理叫做 Polya 定理,是组合学的基本定理之一,它与拉格朗日定理有着密切的关系. 限于篇幅,我们不加证明,而直接给出相关的结果. 后面我们还会看到它在证明费马小定理中的应用.

**定理 10.13** 设  $N = \{1, 2, \dots, n\}$  是被着色物体的集合,  $G = \{\sigma_1, \sigma_2, \dots, \sigma_g\}$  是  $N$  上的置换群. 用  $m$  种颜色对  $N$  中的元素进行着色,则在  $G$  的作用下不同的着色方案数是

$$M = \frac{1}{|G|} \sum_{k=1}^g m^{c(\sigma_k)}$$

其中  $c(\sigma_k)$  是置换  $\sigma_k$  的轮换表示式中包含 1-轮换在内的轮换个数.

考虑上面的方格着色问题. 群  $G$  中的所有置换是:

$$\sigma_1 = (1), \sigma_2 = (1\ 2\ 3\ 4), \sigma_3 = (1\ 3)(2\ 4), \sigma_4 = (1\ 4\ 3\ 2)$$

因此  $c(\sigma_1) = 4, c(\sigma_2) = 1, c(\sigma_3) = 2, c(\sigma_4) = 1$ . 代入 Polya 定理得

$$M = \frac{1}{4}(2^4 + 2^1 + 2^2 + 2^1) = 6$$

图 10.3 给出了这 6 种不同的着色方案.

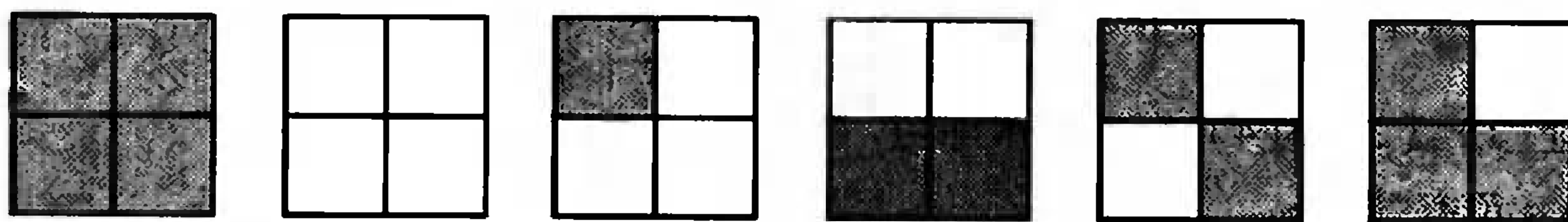


图 10.3

代数系统的同态定义同样适合于群,有关的性质在群中也成立. 这里不再重复.

## 10.4 环 与 域

环是具有两个二元运算的代数系统,它和群及半群有着密切的联系. 先给出环的定义.

**定义 10.11** 设  $\langle R, +, \cdot \rangle$  是代数系统,  $+$  和  $\cdot$  是二元运算,如果满足以下条件:

(1)  $\langle R, + \rangle$  构成交换群;

(2)  $\langle R, \cdot \rangle$  构成半群;

(3)  $\cdot$  运算关于  $+$  运算适合分配律,

则称  $\langle R, +, \cdot \rangle$  是一个环.

为了区别环中的两个运算,通常称  $+$  运算为环中的加法,  $\cdot$  运算为环中的乘法.

**例 10.18** (1) 整数集,有理数集,实数集和复数集关于普通的加法和乘法构成环,分别称为整数环  $\mathbf{Z}$ ,有理数环  $\mathbf{Q}$ ,实数环  $\mathbf{R}$  和复数环  $\mathbf{C}$ .

(2)  $n(n \geq 2)$  阶实矩阵的集合  $M_n(\mathbf{R})$  关于矩阵的加法和乘法构成环,称为  $n$  阶实矩阵环.

(3) 集合的幂集  $P(B)$  关于集合的对称差运算和交运算构成环.

(4) 设  $\mathbf{Z}_n = \{0, 1, \dots, n-1\}$ ,  $\oplus$  和  $\otimes$  分别表示模  $n$  的加法和乘法,则  $\langle \mathbf{Z}_n, \oplus, \otimes \rangle$  构成环,称为模  $n$  的整数环.

为了今后叙述上的方便,将环中加法的单位元记作  $0$ ,乘法的单位元记作  $1$  (对于某些环中的乘法不存在单位元),对任何环中的元素  $x$ ,称  $x$  的加法逆元为负元,记作  $-x$ ,若  $x$  存在乘法逆元的话,则将它称为逆元,记作  $x^{-1}$ ,类似地,针对环中的加法,用  $x - y$  表示  $x + (-y)$ ,  $nx$  表示  $\underbrace{x + x + \dots + x}_{n \uparrow x}$ ,即  $x$  的  $n$  次加法幂,并且用  $-xy$  表示  $xy$  的负元.

下面考虑环的运算性质.

**定理 10.14** 设  $\langle R, +, \cdot \rangle$  是环,则

(1)  $\forall a \in R, a0 = 0a = 0$

(2)  $\forall a, b \in R, (-a)b = a(-b) = -ab$

(3)  $\forall a, b, c \in R, a(b - c) = ab - ac, (b - c)a = ba - ca$

(4)  $\forall a_1, a_2, \dots, a_n, b_1, b_2, \dots, b_m \in R \quad (n, m \geq 2)$

$$\left( \sum_{i=1}^n a_i \right) \left( \sum_{j=1}^m b_j \right) = \sum_{i=1}^n \sum_{j=1}^m a_i b_j$$

证 只证(1),(2)和(4),(3)留作练习.

(1)  $\forall a \in R$  有

$$a0 = a(0 + 0) = a0 + a0$$

由环中加法的消去律得  $a0 = 0$ . 同理可证  $0a = 0$ .

(2)  $\forall a, b \in R$ , 有

$$(-a)b + ab = (-a + a)b = 0b = 0$$

$$ab + (-a)b = (a + (-a))b = 0b = 0$$

因此  $(-a)b$  是  $ab$  的负元. 由负元的惟一性可知

$$(-a)b = -ab$$

同理可证  $a(-b) = -ab$ .

(4) 先证  $\forall a_1, a_2, \dots, a_n$  有

$$\left( \sum_{i=1}^n a_i \right) b_j = \sum_{i=1}^n a_i b_j$$

对  $n$  进行归纳.

当  $n=2$  时, 由环中乘法对加法的分配律, 等式显然成立.

假设  $\left(\sum_{i=1}^n a_i\right)b_j = \sum_{i=1}^n a_i b_j$ , 则有

$$\begin{aligned}\left(\sum_{i=1}^{n+1} a_i\right)b_j &= \left(\sum_{i=1}^n a_i + a_{n+1}\right)b_j \\ &= \left(\sum_{i=1}^n a_i\right)b_j + a_{n+1}b_j \\ &= \sum_{i=1}^n a_i b_j + a_{n+1}b_j = \sum_{i=1}^{n+1} a_i b_j\end{aligned}$$

由归纳法命题得证.

同理可证,  $\forall b_1, b_2, \dots, b_m$  有

$$a_i \left(\sum_{j=1}^m b_j\right) = \sum_{j=1}^m a_i b_j$$

于是

$$\left(\sum_{i=1}^n a_i\right)\left(\sum_{j=1}^m b_j\right) = \sum_{i=1}^n a_i \left(\sum_{j=1}^m b_j\right) = \sum_{i=1}^n \sum_{j=1}^m a_i b_j$$

**例 10.19** 在环中计算  $(a+b)^3, (a-b)^2$

解

$$\begin{aligned}(a+b)^3 &= (a+b)(a+b)(a+b) \\ &= (a^2 + ba + ab + b^2)(a+b) \\ &= a^3 + ba^2 + aba + b^2a + a^2b + bab + ab^2 + b^3 \\ (a-b)^2 &= (a-b)(a-b) = a^2 - ba - ab + b^2\end{aligned}$$

按照代数系统的子代数和同态定义可以定义子环以及环同态与同构, 这里不再赘述. 下面考虑特殊的环: 整环和域.

**定义 10.12** 设  $\langle R, +, \cdot \rangle$  是环,

(1) 若环中乘法  $\cdot$  适合交换律, 则称  $R$  是交换环.

(2) 若环中乘法  $\cdot$  存在单位元, 则称  $R$  是含幺环.

(3) 若  $\forall a, b \in R, ab=0 \Rightarrow a=0 \vee b=0$ , 则称  $R$  是无零因子环.

(4) 若  $R$  既是交换环、含幺环, 也是无零因子环, 则称  $R$  是整环.

(5) 设  $R$  是整环, 且  $R$  中至少含有两个元素. 若  $\forall a \in R^* = R - \{0\}$ , 都有  $a^{-1} \in R$ , 则称  $R$  是域.

**例 10.20** (1) 整数环  $\mathbf{Z}$ 、有理数环  $\mathbf{Q}$ 、实数环  $\mathbf{R}$ 、复数环  $\mathbf{C}$  都是交换环、含幺环、无零因子环和整环, 其中有理数环  $\mathbf{Q}$ 、实数环  $\mathbf{R}$ 、复数环  $\mathbf{C}$  是域.

(2) 令  $2\mathbf{Z} = \{2z \mid z \in \mathbf{Z}\}$ , 则  $2\mathbf{Z}$  关于普通的加法和乘法构成交换环和无零因子环, 但不是含幺环和整环, 因为  $1 \notin 2\mathbf{Z}$ .

(3) 设  $n$  是大于或等于 2 的正整数, 则  $n$  阶实矩阵的集合  $M_n(\mathbf{R})$  关于矩阵加法和乘法构成

环,它是含么环,但不是交换环和无零因子环,也不是整环.

(4)  $\mathbb{Z}_6$  关于模 6 加法和乘法构成环,它是交换环、含么环,但不是无零因子环和整环,因为  $2 \otimes 3 = 0$ ,但 2 和 3 都不是 0,称 2 为  $\mathbb{Z}_6$  中的左零因子,3 为右零因子,类似地,又有  $3 \otimes 2 = 0$ ,所以 3 也是左零因子. 2 也是右零因子,它们都是零因子. 可以证明  $\mathbb{Z}_n$  是域当且仅当  $n$  是素数.

**例 10.21** 设  $p$  为素数,证明  $\mathbb{Z}_p$  是域.

**证**  $p$  为素数,  $p \geq 2$ , 所以  $|\mathbb{Z}_p| \geq 2$ .

易见  $\mathbb{Z}_p$  关于模  $p$  乘法可交换,单位元是 1,且对于任意的  $i, j \in \mathbb{Z}_p, i \neq 0$  有

$$i \otimes j = 0 \Rightarrow p \text{ 整除 } ij \Rightarrow p | j \Rightarrow j = 0$$

所以  $\mathbb{Z}_p$  中无零因子,  $\mathbb{Z}_p$  为整环.

$\mathbb{Z}_p$  关于乘法  $\otimes$  构成有限半群,且  $\mathbb{Z}_p$  关于  $\otimes$  适合消去律,任取  $i \in \mathbb{Z}_p, i \neq 0$ , 令

$$i \otimes \mathbb{Z}_p = \{i \otimes j \mid j \in \mathbb{Z}_p\}$$

则  $i \otimes \mathbb{Z}_p = \mathbb{Z}_p$ , 否则  $\exists j, k \in \mathbb{Z}_p$ , 使得

$$i \otimes j = i \otimes k$$

由消去律得  $j = k$ . 这是矛盾的. 由于  $1 \in \mathbb{Z}_p$ , 存在  $i' \in \mathbb{Z}_p$ , 使得  $i \otimes i' = 1$ . 由于  $\otimes$  运算的交换性可知  $i'$  就是  $i$  的逆元, 从而证明了  $\mathbb{Z}_p$  是域.

类似于子环,也可以定义子整环和子域,请读者试给出相关的定义.

信息安全是关系国计民生的重大问题,也是计算机科学和数学的一个重要的研究领域. 有限域的理论在密码学中有着重要的应用. 密码学,特别是公开密钥密码学常常要用到大的素数,但是目前还没有找到好的素数测试算法. 著名的费马(Fermat)小定理给出了素数测试的必要条件,但不是充分条件,满足这个条件的也可能是合数. 概率算法是目前大量使用的效率比较高的算法,下面先给出费马小定理的组合证明,然后简单介绍素数测试的概率算法. 有关费马小定理的其他的知识将在第十九章给予介绍.

### 定理 10.15 费马(Fermat)小定理

如果  $p$  为素数,则对所有的  $n \not\equiv 0 \pmod{p}$  有  $n^{p-1} \equiv 1 \pmod{p}$ .

**证** 对于费马小定理有一个简单的组合证明. 考虑用  $n$  种颜色对具有  $p$  颗珠子的手镯进行着色. 这些珠子标记为  $1, 2, \dots, p$ , 等距离地顺序排列在圆环上,图 10.4 给出了 5 个珠子的一个实例. 令  $\theta = 2\pi/p$ , 当手镯旋转的角度分别等于  $\theta, 2\theta, \dots, p\theta$  时就对应于  $p$  个置换作用于珠子上. 比如旋转  $\theta$  角的置换可表示为轮换  $(12 \dots p)$ . 由于  $p$  是素数,除了  $p\theta = 2\pi$  对应于恒等置换之外,其他  $p-1$  个置换都由一个  $p$  阶轮换构成. 根据 Polya 定理,不同的着色方案数是

$$M = \frac{1}{p} [n^p + (p-1)n^1] = \frac{1}{p} (n^p - n) + n$$

因为  $M$  和  $n$  是正整数,因此  $n^p - n = n(n^{p-1} - 1)$  能够被  $p$  整除,即

$$n^{p-1} \equiv 1 \pmod{p}$$

由于满足费马小定理的数也可能是合数,为了减少出错,下面再给出另一个测试条件,这里要用到有限域的知识.

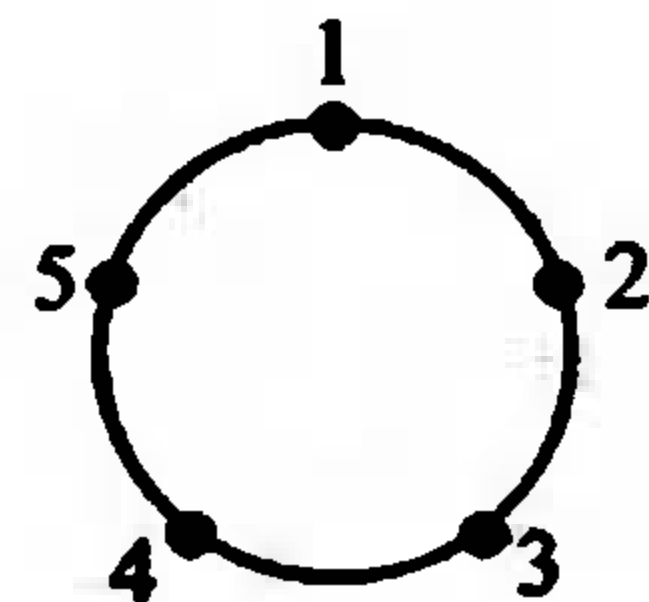


图 10.4

一个有限域  $F$  是具有有限个元素的代数系统, 其中  $F$  与加法构成 Abel 群,  $F^* = F - \{0\}$  与乘法也构成 Abel 群. 当  $n$  为素数时,  $\langle \mathbb{Z}_n, \oplus, \otimes \rangle$  就是含有  $n$  个元素的有限域, 简记为  $\mathbb{Z}_n$ .

**命题** 如果  $n$  为素数, 则在域  $\mathbb{Z}_n$  中方程  $x^2 \equiv 1 \pmod{n}$  的根只有两个, 即  $x=1, x=n-1$ .

**证**

$$\begin{aligned} x^2 &\equiv 1 \pmod{n} \Leftrightarrow x^2 - 1 \equiv 0 \pmod{n} \\ &\Leftrightarrow (x-1)(x+1) \equiv 0 \pmod{n} \\ &\Leftrightarrow x-1 \equiv 0 \pmod{n} \vee x+1 \equiv 0 \pmod{n} \quad (\text{域中没有零因子}) \\ &\Leftrightarrow x=1 \vee x=n-1 \end{aligned}$$

称  $x \neq 1$  和  $n-1$  的根为非平凡的. 例如  $n=12$ ,

$$x^2 \pmod{12} \equiv 1 \Leftrightarrow x=1 \text{ 或 } x=11 \text{ 或 } x=5 \text{ 或 } x=7$$

上式中 5 和 7 是非平凡的根. 根据命题, 如果方程有非平凡根, 则  $n$  为合数. 素数判断的问题就归结为方程是否存在非平凡根的问题. 不幸的是, 目前也没有解决这个问题的好的确定型算法.

设  $n$  为奇素数, 根据除法, 存在正整数  $q$  和  $m$ , 其中  $q > 1, m$  为奇数, 使得  $n-1 = 2^q m$ . 给定正整数  $a$ , 令  $k=0, 1, \dots, q$ , 从而得到通项公式为  $a^{2^k m} \pmod{n}$  的序列:

$$a^m \pmod{n}, a^{2^m} \pmod{n}, a^{4^m} \pmod{n}, \dots, a^{2^{q^m}} \pmod{n}$$

该序列的最后一项为  $a^{n-1} \pmod{n}$ , 而且每一项是前面一项的平方. 根据费马小定理, 对于素数  $n$ , 一定有  $a^{n-1} \equiv 1 \pmod{n}$ . 因此上述序列的最后一项, 即  $k=q$  的项应该等于 1. 根据命题, 它的前一项, 也就是  $k=q-1$  的项应该等于 1 或  $n-1$ . 如果这项等于 1, 那么  $k=q-2$  的项也应该等于 1 或  $n-1$ . 照此进行, 依次检查序列的各项, 判断  $a^{2^k m} \pmod{n}$  是否为 1 和  $n-1$ , 且它的后一项是否为 1. 如果存在某一项, 比如第  $k$  项, 不等于 1 和  $n-1$ , 但是第  $k+1$  项等于 1, 从而知道  $n$  不是素数. 例如  $n=561$ , 那么  $n-1=560=2^4 \cdot 35$ , 假设  $a=7$ , 构造的序列为

$$7^{35} \pmod{561} = 241, 7^{70} \pmod{561} = 298, 7^{2^{235}} \pmod{561} = 166,$$

$$7^{2^{335}} \pmod{561} = 67, 7^{2^{435}} \pmod{561} = 1$$

第 5 项为 1, 但是第 4 项等于 67, 它既不等于 1 也不等于 560, 是个非平凡的根, 因此可以判定  $n$  为合数. 根据这个思想设计的计算机算法称为 Miller-Rabin 算法, 它随机选择正整数  $a \in \{2, 3, \dots, n-1\}$ , 然后进行上述测试.

**算法** Miller-Rabin( $n$ )

1. 令  $n-1 = 2^q m, q \geq 1, m$  为奇数
2.  $a \leftarrow \text{Random}(2, n-1)$  (随机选择  $a \in \{2, \dots, n-1\}$ )
3.  $x_0 \leftarrow a^m \pmod{n}$
4. for  $i \leftarrow 1$  to  $q$  do
5.      $x_i \leftarrow x_{i-1}^2 \pmod{n}$
6.     if  $x_i = 1$  and  $x_{i-1} \neq 1$  and  $x_{i-1} \neq n-1$
7.         then return composite
8. if  $x_q \neq 1$  then return composite

## 9. return prime

由于  $a$  是随机选择的, 这种测试不能保证检查到所有可能出现非平凡根的情况, 这种出错是由于对  $a$  的选择不当而引起的. 可以证明: 在  $n$  为奇合数的情况下, 出错的概率小于  $1/2$ . 证明涉及较多的群论和数论的知识, 这里不再详细阐述, 只是介绍一下证明的主要思想.

根据费马小定理, 有  $a^{n-1} \equiv 1 \pmod{n}$ , 从而有  $aa^{n-2} \equiv 1 \pmod{n}$ , 因此存在整数  $u, v$  使得

$$au + nv = 1$$

这是  $a$  与  $n$  互素的充要条件(见第十九章定理 19.8), 于是  $(a, n) = 1$ . 这说明所有出现错误的  $a$  都属于集合

$$T = \{x \mid x \in \mathbb{Z}_n, (x, n) = 1\}$$

根据习题十第 12 题, 这个集合关于模  $n$  乘法构成 Abel 群, 且  $|T| = \phi(n)$ , 这里的  $\phi(n)$  是欧拉函数的值. 定义集合

$$B = \{x \mid x \in T, x^{2^k} \equiv 1 \pmod{n} \vee x^{2^k} \equiv n-1 \pmod{n}\}$$

利用群和数论的知识, 可以证明  $B$  构成  $T$  的真子群. 再根据拉格朗日定理,  $|B|$  小于  $\phi(n)$  且整除  $\phi(n)$ , 因此至多是  $(n-1)/2$ . 由于  $B$  中含有 1, 而  $a \neq 1$ , 因此使得算法出错的  $a$  的个数少于  $(n-1)/2$ . 这就证明了算法对于素数测试得到正确结果的概率大于  $1/2$ .

对这个算法重复运行  $k$  次, 可以将出错概率降到至多  $2^{-k}$ . 令  $k = \lceil \log n \rceil$ , 出错的概率小于等于  $2^{-k} \leq 1/n$ . 即算法给出正确答案的概率为  $1 - 1/n$ . 换句话说, 如果  $n$  为素数, 则算法输出素数; 如果  $n$  为合数, 则算法以  $1 - 1/n$  的概率输出“合数”. 考虑到算法比较高的效率, 在实际当中 Miller-Rabin 算法是一个较好的算法.

## 习 题 十

1. 设  $A = \{0, 1\}$ , 试给出半群  $\langle A^+, \circ \rangle$  的运算表, 其中  $\circ$  为函数的复合运算.
2. 判断下列集合关于指定的运算是否构成半群, 独异点和群:
  - (1)  $a$  是正实数,  $G = \{a^n \mid n \in \mathbb{Z}\}$ , 运算是普通乘法;
  - (2)  $\mathbb{Q}^+$  为正有理数集, 运算是普通乘法;
  - (3)  $\mathbb{Q}^+$  为正有理数集, 运算是普通加法;
  - (4) 一元实系数多项式的集合关于多项式的加法;
  - (5) 一元实系数多项式的集合关于多项式的乘法;
  - (6)  $U_n = \{x \mid x \in \mathbb{C} \wedge x^n = 1\}$ ,  $n$  为某个给定的正整数,  $\mathbb{C}$  为复数集合, 运算是复数乘法.
3. 在  $\mathbb{R}$  中定义二元运算  $*$  使得  $\forall a, b \in \mathbb{R}$ ,

$$a * b = a + b + ab$$

证明  $\langle \mathbb{R}, * \rangle$  构成独异点.

4.  $S = \{a, b, c\}$ ,  $*$  是  $S$  上的二元运算, 且  $\forall x, y \in S, x * y = x$ .
  - (1) 证明  $S$  关于  $*$  运算构成半群;
  - (2) 试通过增加最少的元素使得  $S$  扩张成一个独异点.

5. 设  $V = \langle \{a, b\}, * \rangle$  是半群, 且  $a * a = b$ , 证明:

$$(1) a * b = b * a;$$

$$(2) b * b = b.$$

6. 设  $V = \langle S, * \rangle$  是可交换半群, 若  $a, b$  是  $V$  中的幂等元, 证明  $a * b$  也是  $V$  中的幂等元.

7. 设  $G = \{a + bi \mid a, b \in \mathbb{Z}\}$ ,  $i$  为虚数单位, 即  $i^2 = -1$ . 验证  $G$  关于复数加法构成群.

8. 设  $S = \{0, 1, 2, 3\}$ ,  $\otimes$  为模 4 乘法, 即

$$\forall x, y \in S, x \otimes y = (xy) \bmod 4$$

问  $\langle S, \otimes \rangle$  构成什么代数系统(半群, 独异点, 群)? 为什么?

9. 设  $\mathbb{Z}$  为整数集合, 在  $\mathbb{Z}$  上定义二元运算  $\circ$  如下:

$$\forall x, y \in \mathbb{Z}, x \circ y = x + y - 2.$$

问  $\mathbb{Z}$  关于  $\circ$  运算能否构成群? 为什么?

10. 设  $A = \{x \mid x \in \mathbb{R} \wedge x \neq 0, 1\}$ , 在  $A$  上定义 6 个函数如下:

$$\begin{aligned} f_1(x) &= x, & f_2(x) &= x^{-1}, & f_3(x) &= 1 - x, \\ f_4(x) &= (1 - x)^{-1}, & f_5(x) &= (x - 1)x^{-1}, & f_6(x) &= x(x - 1)^{-1} \end{aligned}$$

令  $F$  为这 6 个函数构成的集合,  $\circ$  运算为函数的复合运算.

(1) 给出  $\circ$  运算的运算表;

(2) 验证  $\langle F, \circ \rangle$  是一个群.

11. 设  $G = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \right\}$ , 证明  $G$  关于矩阵乘法构成一个群.

12.  $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$ , 定义

$$T = \{x \mid x \in \mathbb{Z}_n \text{ 且 } (x, n) = 1\}$$

这里的  $(x, n)$  表示  $x$  与  $n$  的最大公约数, 证明  $T$  关于模  $n$  乘法构成 Abel 群.

13. 证明定理 10.1 的(2)、(4) 和 (5), 即设  $G$  为群, 证明

$$(2) \forall a, b \in G, (ab)^{-1} = b^{-1}a^{-1};$$

$$(4) \forall a \in G, (a^n)^m = a^{nm};$$

$$(5) \text{ 若 } G \text{ 为交换群, 则 } (ab)^n = a^n b^n.$$

14. 证明定理 10.2, 即证明群  $G$  中运算适合消去律.

15. 设  $G$  为群, 若  $\forall x \in G$  有  $x^2 = e$ , 证明  $G$  为交换群.

16. 设  $G$  为群, 证明  $e$  为  $G$  中惟一的幂等元.

17. 设  $G$  为群,  $a, b, c \in G$ , 证明

$$|abc| = |bca| = |cab|$$

18. 证明偶数阶群必含 2 阶元.

19. 设  $G$  为非 Abel 群, 证明  $G$  中存在非单位元  $a$  和  $b$ ,  $a \neq b$ , 且  $ab = ba$ .

20. 设  $G$  为  $M_n(\mathbb{R})$  上的加法群,  $n \geq 2$ , 判断下述子集是否构成子群.

(1) 全体对称矩阵;

(2) 全体对角矩阵;

(3) 全体行列式大于等于 0 的矩阵;

(4) 全体上(下)三角矩阵.

21. 设  $G$  为群,  $a$  是  $G$  中给定元素,  $a$  的正规化子  $N(a)$  表示  $G$  中与  $a$  可交换的元素构成的集合, 即

$$N(a) = \{x \mid x \in G \wedge xa = ax\}$$

证明  $N(a)$  是  $G$  的子群.

22. 设  $H$  是群  $G$  的子群,  $x \in G$ , 令

$$xHx^{-1} = \{xhx^{-1} \mid h \in H\}$$

证明  $xHx^{-1}$  是  $G$  的子群, 称为  $H$  的共轭子群.

23. 画出群  $\langle \mathbb{Z}_{18}, \oplus \rangle$  的子群格.

24. 设  $H$  和  $K$  分别为群  $G$  的  $r, s$  阶子群, 若  $r$  和  $s$  互素, 证明  $H \cap K = \{e\}$ .

25. 对以下各小题给定的群  $G_1$  和  $G_2$ , 以及  $f: G_1 \rightarrow G_2$ , 说明  $f$  是否为群  $G_1$  到  $G_2$  的同态, 如果是, 说明是否为单同态、满同态和同构. 求同态像  $f(G_1)$ .

(1)  $G_1 = \langle \mathbb{Z}, + \rangle, G_2 = \langle \mathbb{R}^*, \cdot \rangle$ , 其中  $\mathbb{R}^*$  为非零实数集合,  $+$  和  $\cdot$  分别表示数的加法和乘法.

$$f: \mathbb{Z} \rightarrow \mathbb{R}^*, f(x) = \begin{cases} 1 & x \text{ 是偶数} \\ -1 & x \text{ 是奇数} \end{cases}$$

(2)  $G_1 = \langle \mathbb{Z}, + \rangle, G_2 = \langle A, \cdot \rangle$ , 其中  $+$  和  $\cdot$  分别表示数的加法和乘法,  $A = \{x \mid x \in \mathbb{C} \wedge |x| = 1\}$ , 其中  $\mathbb{C}$  为复数集合.

$$f: \mathbb{Z} \rightarrow A, f(x) = \cos x + i \sin x$$

(3)  $G_1 = \langle \mathbb{R}, + \rangle, G_2 = \langle A, \cdot \rangle$ ,  $+$  和  $\cdot$  以及  $A$  的定义同(2)

$$f: \mathbb{R} \rightarrow A, f(x) = \cos x + i \sin x$$

26. 证明循环群一定是阿贝尔群, 说明阿贝尔群是否一定是循环群, 并证明你的结论.

27. 设  $G_1$  为循环群,  $f$  是群  $G_1$  到  $G_2$  的同态, 证明  $f(G_1)$  也是循环群.

28. 设  $G = \langle a \rangle$  是 15 阶循环群.

(1) 求出  $G$  的所有生成元;

(2) 求出  $G$  的所有子群.

29. 设  $\sigma, \tau$  是 5 元置换, 且

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix}, \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix}$$

(1) 计算  $\sigma\tau, \tau\sigma, \sigma^{-1}, \tau^{-1}, \sigma^{-1}\tau\sigma$ ;

(2) 将  $\sigma\tau, \tau^{-1}, \sigma^{-1}\tau\sigma$  表成不交的轮换之积;

(3) 将(2)中的置换表示成对换之积, 并说明哪些为奇置换, 哪些为偶置换.

30. 如果允许立方体在空间任意转动, 用  $n$  种颜色着色立方体的 6 个面, 证明不同的着色方案数是  $\frac{1}{24}(n^6 + 8n^2 + 12n^3 + 3n^4)$ .

31. 一个圆环上等距地镶有 6 颗珠子, 每颗珠子可以是红、蓝、黄三种颜色, 问有多少种不同的镶嵌方案?

32. 设  $A = \{a + bi \mid a, b \in \mathbb{Z}, i^2 = -1\}$ , 证明  $A$  关于复数加法和乘法构成环, 称为高斯整数环.

33. 设  $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n, a_0, a_1, \cdots, a_n$  为实数, 称  $f(x)$  为实数域上的  $n$  次多项式, 令

$$A = \{f(x) \mid f(x) \text{ 为实数域上的 } n \text{ 次多项式}, n \in \mathbb{N}\}$$

证明  $A$  关于多项式的加法和乘法构成一个环, 称为实数域上的多项式环.

34. 判断下列集合和给定运算是否构成环、整环和域, 如果不能构成, 说明理由.

(1)  $A = \{a + bi \mid a, b \in \mathbb{Q}\}$ , 其中  $i^2 = -1$ , 运算为复数加法和乘法;

- (2)  $A = \{2z + 1 \mid z \in \mathbf{Z}\}$ , 运算为实数加法和乘法;  
 (3)  $A = \{2z \mid z \in \mathbf{Z}\}$ , 运算为实数加法和乘法;  
 (4)  $A = \{x \mid x \geq 0 \wedge x \in \mathbf{Z}\}$ , 运算为实数加法和乘法;  
 (5)  $A = \{a + b\sqrt[4]{5} \mid a, b \in \mathbf{Q}\}$ , 运算为实数加法和乘法.

35. 在域  $\mathbf{Z}_5$  中解下列方程和方程组:

(1)  $3x = 2$ ;

(2) 
$$\begin{cases} x + 2z = 1 \\ z + 2x = 2 \\ 2x + y = 1 \end{cases}$$

36. 设  $a$  和  $b$  是含么环  $R$  中的两个可逆元, 证明:

- (1)  $-a$  也是可逆元, 且  $(-a)^{-1} = -a^{-1}$ ;  
 (2)  $ab$  也是可逆元, 且  $(ab)^{-1} = b^{-1}a^{-1}$ .

37. 设  $R$  是环, 令

$$C = \{x \mid x \in R \wedge \forall a \in R (xa = ax)\}$$

$C$  称作  $R$  的中心, 证明  $C$  是  $R$  的子环.

38. 证明定理 10.14 (3), 即设  $R$  是环, 则  $\forall a, b, c \in R$ , 有

$$a(b - c) = ab - ac, \quad (b - c)a = ba - ca$$

# 第十一章 格与布尔代数

## 11.1 格的定义与性质

格与布尔代数是具有两个二元运算的代数系统,它们与同样具有两个二元运算的代数系统——环具有完全不同的性质.格或布尔代数在逻辑电路设计、软件形式方法、数据仓库等各方面都有重要的应用.下面先给出格的定义和基本性质.

首先说明,本章出现的 $\wedge$ 和 $\vee$ 的符号不再代表逻辑上的合取与析取,而是格中的运算符,涉及合取和析取,我们将使用自然语言加以叙述.下面给出格作为偏序集的第一个定义.

**定义 11.1** 设 $\langle S, \leq \rangle$ 是偏序集,如果 $\forall x, y \in S, \{x, y\}$ 都有最小上界和最大下界,则称 $S$ 关于偏序 $\leq$ 作成一个格.

由于最小上界和最大下界的惟一性,可以把求 $\{x, y\}$ 的最小上界和最大下界看成 $x$ 与 $y$ 的二元运算 $\vee$ 和 $\wedge$ ,即 $x \vee y$ 和 $x \wedge y$ 分别表示 $x$ 与 $y$ 的最小上界和最大下界.

**例 11.1** 设 $n$ 是正整数, $S_n$ 是 $n$ 的正因子的集合. $D$ 为整除关系,则偏序集 $\langle S_n, D \rangle$ 构成格. $\forall x, y \in S_n, x \vee y$ 是 $\text{lcm}(x, y)$ ,即 $x$ 与 $y$ 的最小公倍数. $x \wedge y$ 是 $\text{gcd}(x, y)$ ,即 $x$ 与 $y$ 的最大公约数.图 11.1 给出了格 $\langle S_8, D \rangle, \langle S_6, D \rangle$ 和 $\langle S_{30}, D \rangle$ .

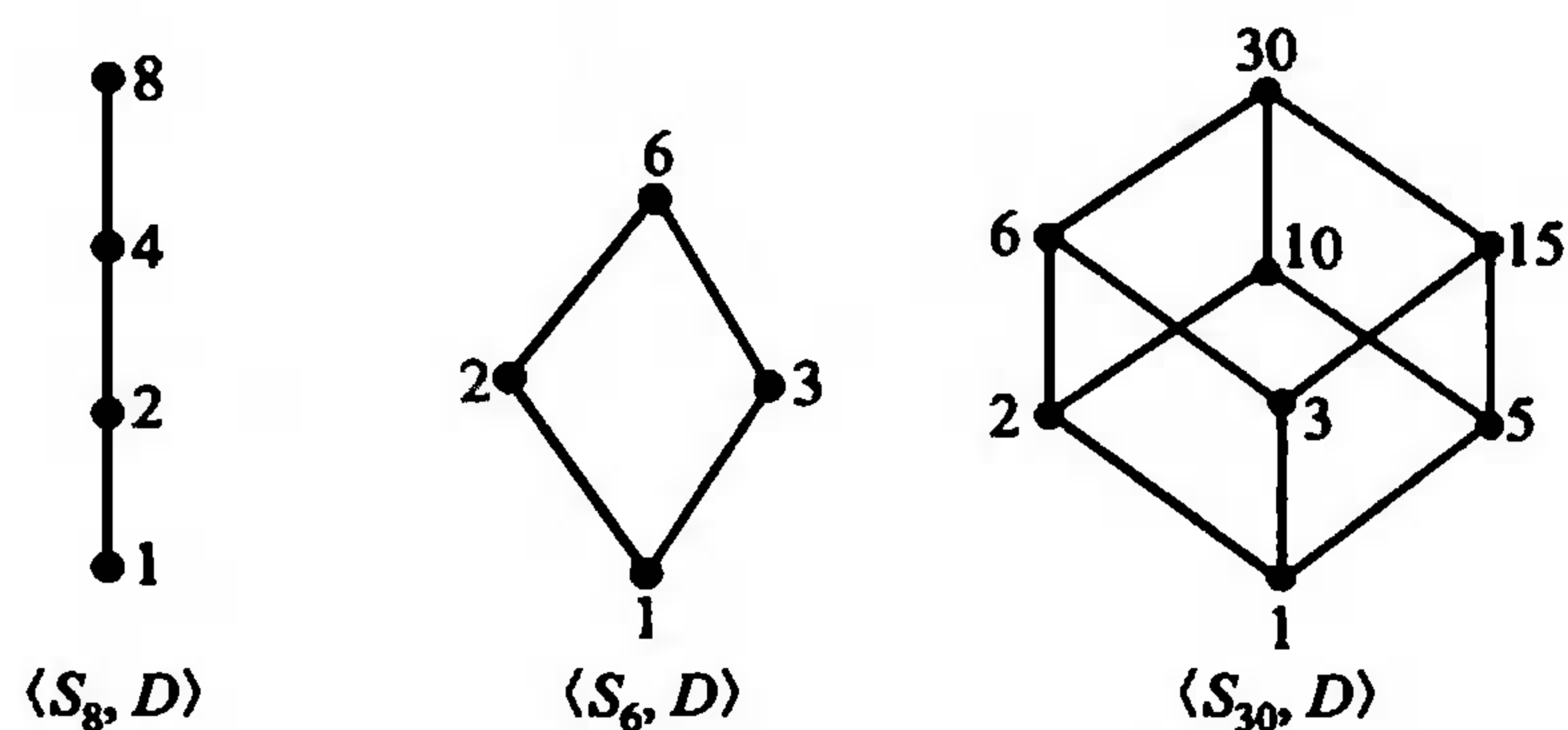


图 11.1

**例 11.2** 判断下列偏序集是否构成格,并说明理由.

- (1)  $\langle P(B), \subseteq \rangle$ , 其中 $P(B)$ 是集合 $B$ 的幂集.
- (2)  $\langle \mathbb{Z}, \leq \rangle$ , 其中 $\mathbb{Z}$ 是整数集, $\leq$ 为小于或等于关系.

(3) 偏序集的哈斯图分别在图 11.2 给出.

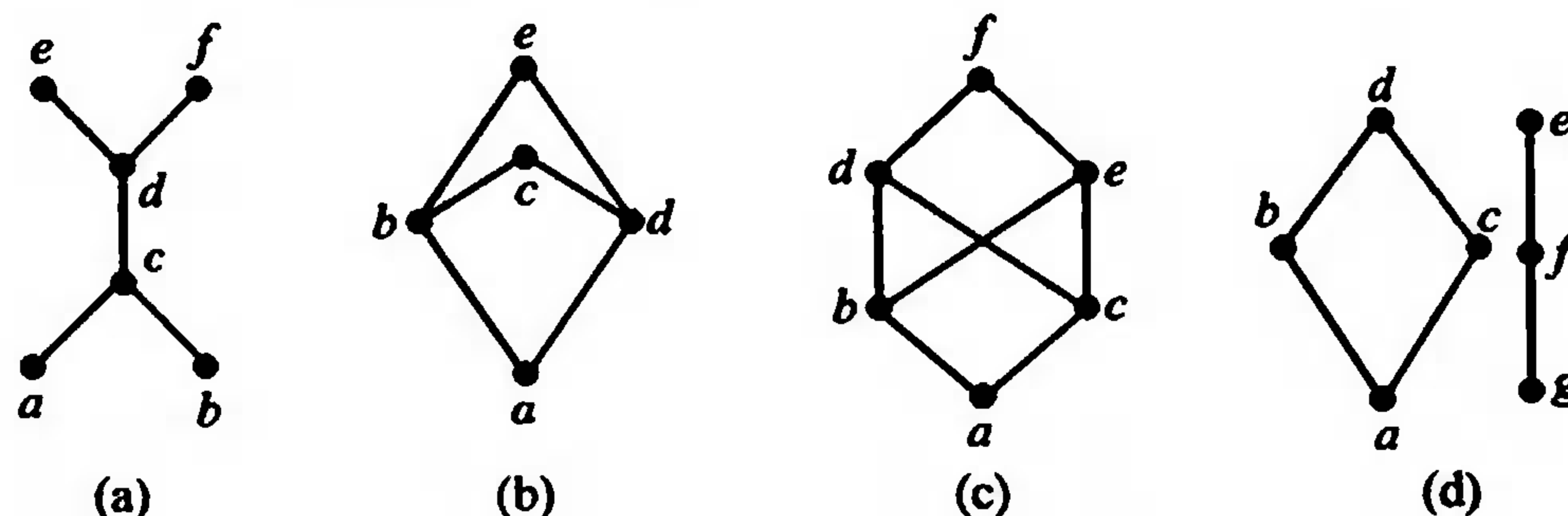


图 11.2

解 (1) 是格.  $\forall x, y \in P(B), x \vee y$  就是  $x \cup y, x \wedge y$  就是  $x \cap y$ . 由于  $\cup$  和  $\cap$  运算在  $P(B)$  上是封闭的, 所以  $x \cup y, x \cap y \in P(B)$ . 称  $\langle P(B), \subseteq \rangle$  为  $B$  的幂集格.

(2) 是格.  $\forall x, y \in \mathbb{Z}, x \vee y = \max(x, y), x \wedge y = \min(x, y)$ , 它们都是整数.

(3) 都不是格. (a) 中的  $\{a, b\}$  没有最大下界. (b) 中的  $\{b, d\}$  有两个上界  $c$  和  $e$ , 但没有最小上界. (c) 的  $\{b, c\}$  有三个上界  $d, e$  和  $f$ , 但没有最小上界. (d) 中的  $\{a, g\}$  没有最大下界.

例 11.3 设  $G$  是群,  $L(G)$  是  $G$  的所有子群的集合, 即

$$L(G) = \{H \mid H \leq G\}$$

对任意的  $H_1, H_2 \in L(G), H_1 \cap H_2$  也是  $G$  的子群, 而  $\langle H_1 \cup H_2 \rangle$  是由  $H_1 \cup H_2$  生成的子群 (见节 10.2). 在  $L(G)$  上定义包含关系  $\subseteq$ , 则  $L(G)$  关于包含关系构成一个格, 称为  $G$  的子群格. 易见在  $L(G)$  中,  $H_1 \wedge H_2$  就是  $H_1 \cap H_2, H_1 \vee H_2$  就是  $\langle H_1 \cup H_2 \rangle$ .

例 11.4 数据仓库中的视图格<sup>①</sup>.

数据仓库中的数据空间可以看成是一个多维的“立方体”, 比如一个汽车销售的数据仓库的模式可能是:

Sales(serialNo, date, dealer, price)

Autos(serialNo, model, color)

Dealers(name, city, phone)

其中涉及销售的属性有汽车型号、销售日期、代理商、价格等; 涉及汽车的属性有型号、类型、颜色等; 涉及代理商的属性有名称、城市、电话等. 在决策查询中可能需要某段指定时间的销售情况. 比如

SELECT city, AVG(prices)

FROM Sales, Dealers

WHERE Sales.dealer = Dealers.name AND

Data > = '2005 - 01 - 01'

GROUP BY city;

① 这个例子改写自 Hector Garcia - Molina, etc. 的“Database Systems - the Complete Book”一书.

这个查询将返回 2005 年 1 月 1 号以后各个城市的每种汽车的平均销售价格.

数据仓库可以分成日期维,汽车维(轿车、越野车和可转换汽车),代理商维(西部地区、东部地区)等.可以对它进行切块和切片查询,这种查询会涉及在某一维上进行切片,而在其他维上进行切块.图 11.3 中的阴影部分就是在日期维切片,而在汽车和代理商维进行切块的分割.

面对数据仓库的海量数据,在联机分析处理(OLAP)中,为了加快查询速度,可以将数据按照维进行聚集,比如沿时间维将每种汽车、每个代理商的数据聚集到一起,也可以沿代理商维将每个日期、每种汽车的所有代理商的数据聚集起来.如果在这两个维度上进行聚集,那么就得到每种汽车在所有时间和代理商的数据.当限制查询只能是完全聚集或不聚集,那么这种聚集才是有用的.但是实际的大量查询可能涉及部分聚集的数据,比如我们需要查询省会城市在大众汽车的销售情况.如果每次查询都从原始数据查找,效率是很低的,为此需要建立物化视图.被选择进行物化的视图是一些典型的聚集结果.可以事先将这些视图存

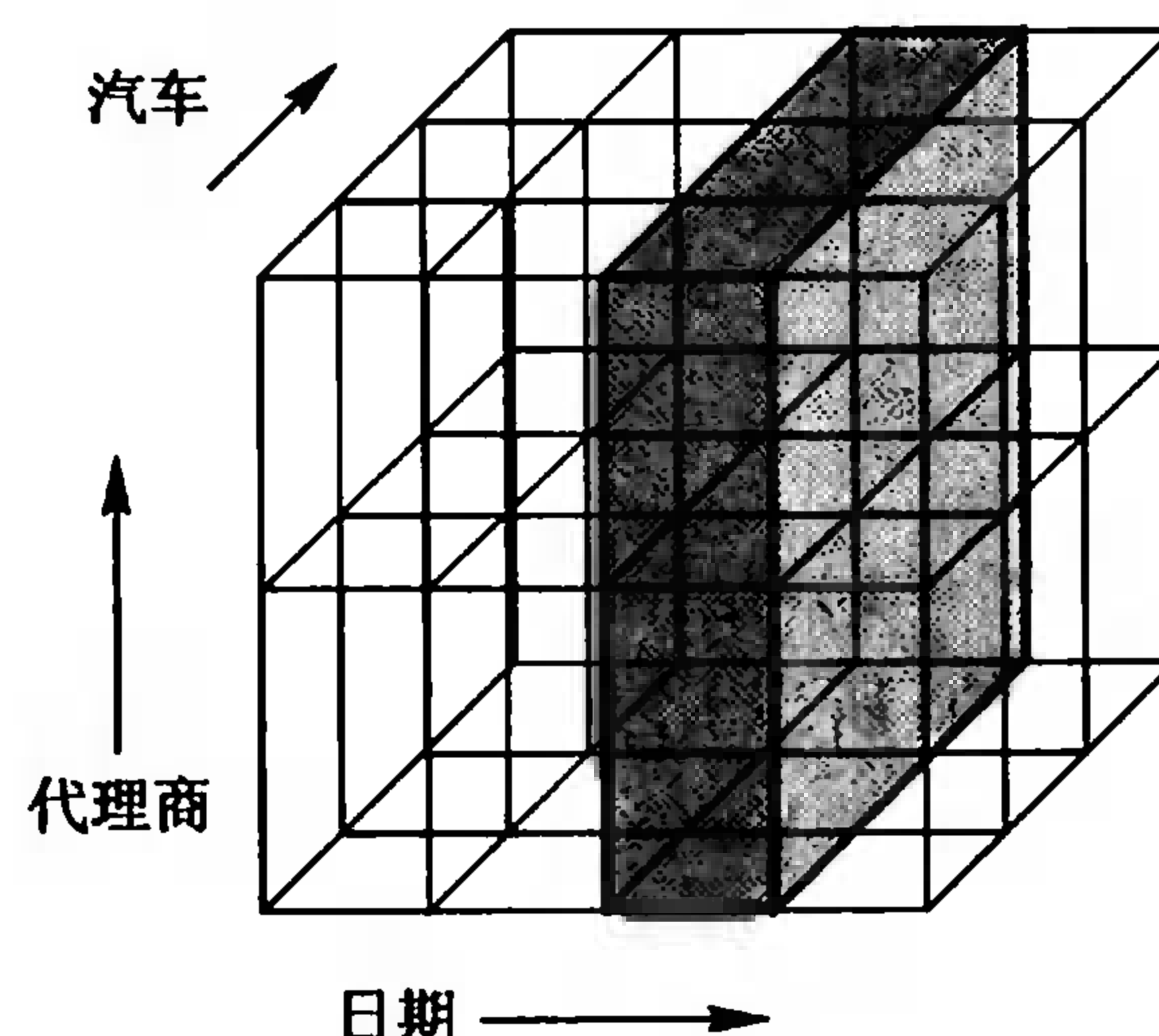


图 11.3

放在数据库中,根据用户的查询要求进行选择使用.在这个例子中,一个可能的物化视图  $V_1$  可以按月对时间分组,按城市对代理商分组.另一个物化视图  $V_2$  可能是按周对时间分组,按省对代理商分组,还可以有许多其他的方案.

如何选择物化视图的分组方案,使得占用较小的空间,同时尽可能满足更多的查询要求?这里就用到格的构造.

每维上的数据构成集合,对它的一种分组就是对这个集合的划分.对同维上的两个划分  $P_1$  和  $P_2$ ,如果  $P_1$  的每个划分块都是  $P_2$  的某个划分块的子集,就称  $P_1$  是  $P_2$  的加细,记作  $P_1 \leq P_2$ .比如在时间维上,  $P_1$  把数据按周划分,  $P_2$  把数据按月划分,那么  $P_1$  就是  $P_2$  的加细.显然加细是偏序关系.如果把维上的所有分组的集合记作  $X$ ,那么  $X$  关于加细关系构成格.图 11.4 给出了时间维和代理商维对应的两个格.

如果数据立方体的每个维都有一个格,那么可以为数据立方体的所有可能的物化视图定义一个格(第七章习题 48 断定偏序集的 2 阶笛卡儿积仍旧是偏序,这里则是高维的),这个格称为视图格.如果  $V_1$  和  $V_2$  是两个物化视图,它们通过在每一维上选择一种划分构成.那么  $V_1 \leq V_2$  就意味着:在每一维上  $V_1$  对应的划分都是  $V_2$  对应划分的加细.上述数据仓库中物化视图  $V_1$  和  $V_2$  构成的格(整个格的一部分)如图 11.5 所示.其中  $Q_1, Q_2$  和  $Q_3$  代表三个不同的查询.  $Q_1$  既可以从视图  $V_1$  得到回答,也可以从视图  $V_2$  得到回答,而  $Q_3$  只能从 Sales 中得到回答,视图  $V_1$  和  $V_2$  不支持  $Q_3$  查询,但是 Sales 也是视图,它在每一维上的划分都是最细的,它可以支持所有的查询.

根据偏序集的性质不难证明格的重要性质,即格的对偶原理.

**定义 11.2** 设  $f$  是含有格中元素以及符号  $=, \leq, \geq, \vee$  和  $\wedge$  的命题.令  $f^*$  是将  $f$  中的  $\leq$  替换

成 $\geq$ ,  $\geq$ 替换成 $\leq$ ,  $\vee$ 替换成 $\wedge$ ,  $\wedge$ 替换成 $\vee$ 所得到的命题. 称 $f^*$ 为 $f$ 的对偶命题.

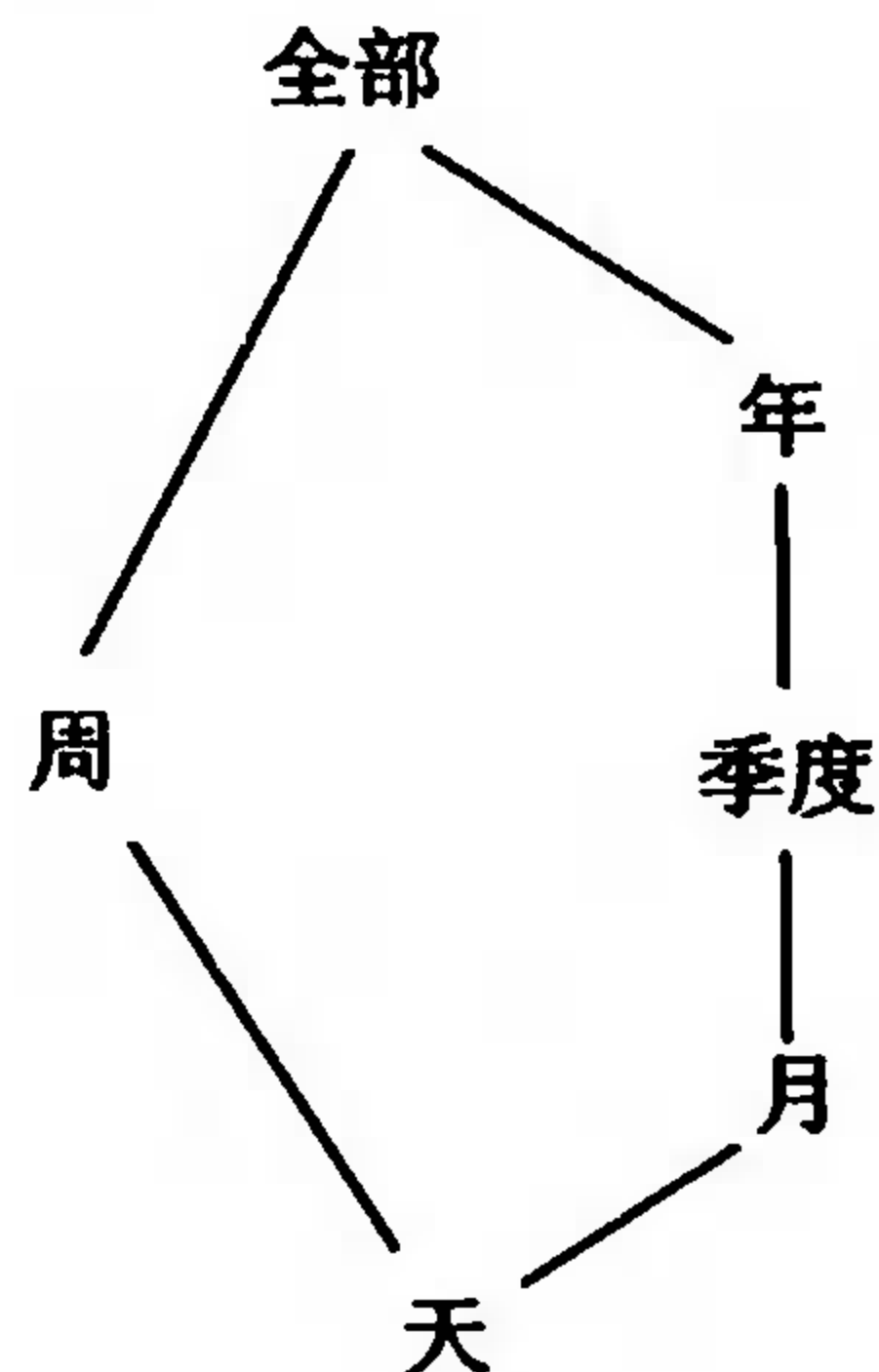


图 11.4

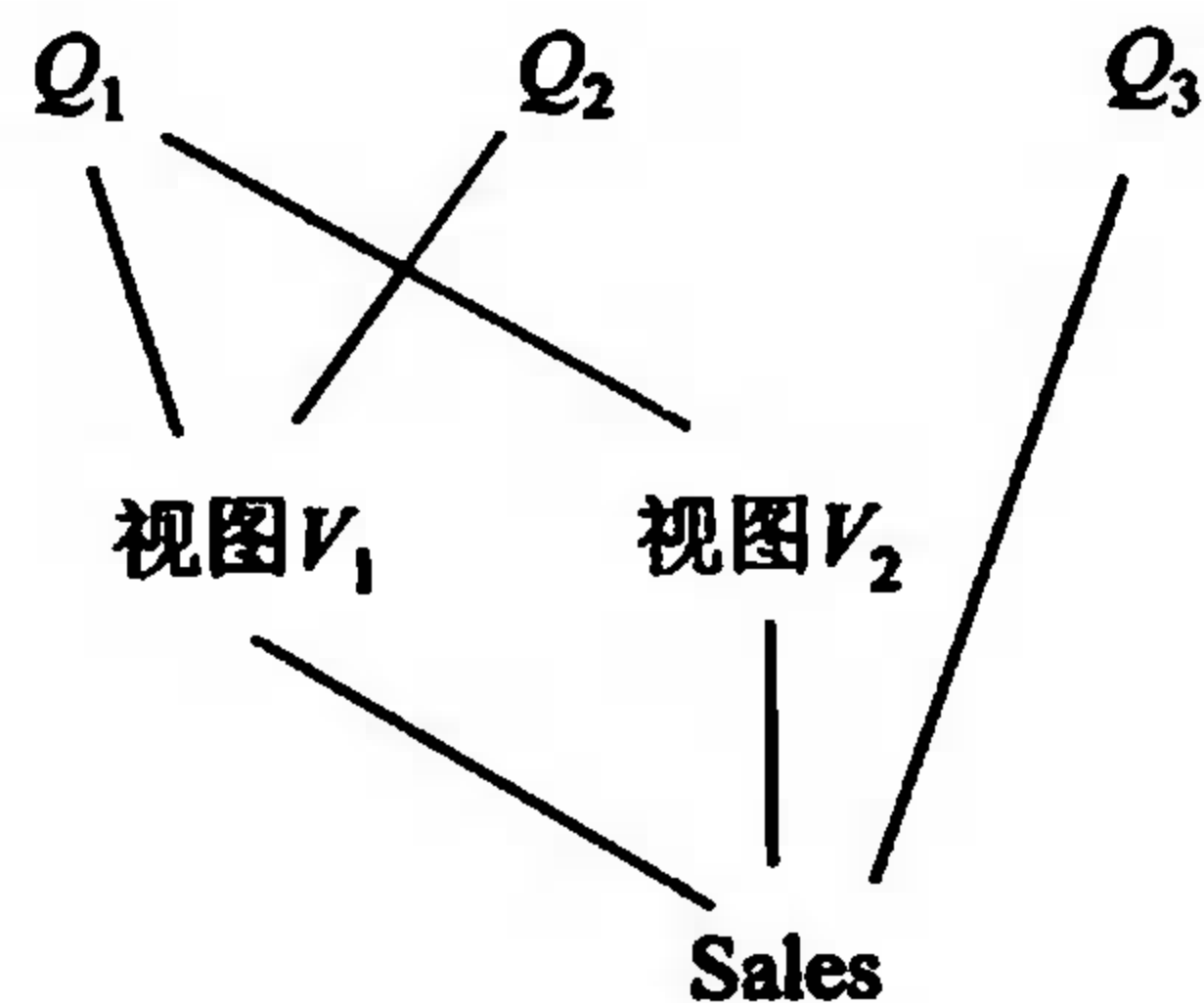


图 11.5

例如, 在格中令 $f$ 是 $(a \vee b) \wedge c \leq c$ , 则 $f^*$ 是

$$(a \wedge b) \vee c \geq c$$

**格的对偶原理** 设 $f$ 是含有格中元素以及符号 $=, \leq, \geq, \vee$ 和 $\wedge$ 等的命题. 若 $f$ 对一切格为真, 则 $f$ 的对偶命题 $f^*$ 也对一切格为真.

例如, 若对一切格 $L$ 都有

$$\forall a, b \in L, a \wedge b \leq a$$

那么对一切格 $L$ 都有

$$\forall a, b \in L, a \vee b \geq a$$

许多格的性质都是互为对偶命题的, 有了格的对偶原理, 在证明格的性质时, 只需证明其中的一个命题就可以了.

**定理 11.1** 设 $\langle L, \leq \rangle$ 是格, 则运算 $\vee$ 和 $\wedge$ 适合交换律、结合律、幂等律和吸收律, 即

(1)  $\forall a, b \in L$  有

$$a \vee b = b \vee a, \quad a \wedge b = b \wedge a$$

(2)  $\forall a, b, c \in L$  有

$$(a \vee b) \vee c = a \vee (b \vee c), \quad (a \wedge b) \wedge c = a \wedge (b \wedge c)$$

(3)  $\forall a \in L$  有

$$a \vee a = a, \quad a \wedge a = a$$

(4)  $\forall a, b \in L$  有

$$a \vee (a \wedge b) = a, \quad a \wedge (a \vee b) = a$$

**证** (1)  $a \vee b$  和  $b \wedge a$  分别是  $\{a, b\}$  的最小上界和  $\{b, a\}$  的最小上界. 由于  $\{a, b\} = \{b, a\}$ , 所以  $a \vee b = b \vee a$ .

由对偶原理,  $a \wedge b = b \wedge a$  得证.

(2) 由最小上界的定义有

$$(a \vee b) \vee c \geq a \vee b \geq a \quad (11.1)$$

$$(a \vee b) \vee c \geq a \vee b \geq b \quad (11.2)$$

$$(a \vee b) \vee c \geq c \quad (11.3)$$

由式(11.2)和(11.3)有

$$(a \vee b) \vee c \geq b \vee c \quad (11.4)$$

由式(11.1)和(11.4)有

$$(a \vee b) \vee c \geq a \vee (b \vee c)$$

同理可证

$$(a \vee b) \vee c \leq a \vee (b \vee c)$$

根据偏序的反对称性有

$$(a \vee b) \vee c = a \vee (b \vee c)$$

由对偶原理,  $(a \wedge b) \wedge c = a \wedge (b \wedge c)$  得证.

(3) 显然  $a \leq a \vee a$ , 又由  $a \leq a$  可得  $a \vee a \leq a$ , 根据反对称性有

$$a \vee a = a$$

由对偶原理,  $a \wedge a = a$  得证.

(4) 显然

$$a \vee (a \wedge b) \geq a \quad (11.5)$$

又由  $a \leq a, a \wedge b \leq a$  可得

$$a \vee (a \wedge b) \leq a \quad (11.6)$$

由式(11.5)和(11.6)可得

$$a \vee (a \wedge b) = a$$

根据对偶原理,  $a \wedge (a \vee b) = a$  得证.

由定理 11.1 可知, 格是具有两个二元运算的代数系统  $\langle L, \wedge, \vee \rangle$ , 其中运算  $\wedge$  和  $\vee$  满足交换律, 结合律, 幂等律和吸收律. 那么能不能像群、环、域一样, 通过规定运算及其基本性质来给出格的定义呢? 回答是肯定的.

**定理 11.2** 设  $\langle S, *, \circ \rangle$  是具有两个二元运算的代数系统, 且对于  $*$  和  $\circ$  运算适合交换律、结合律、吸收律, 则可以适当定义  $S$  中的偏序  $\leq$ , 使得  $\langle S, \leq \rangle$  构成一个格, 且  $\forall a, b \in S$  有  $a \wedge b = a * b, a \vee b = a \circ b$ .

**证** (1) 先证在  $S$  中  $*$  和  $\circ$  运算都适合幂等律.

$\forall a \in S$ , 由吸收律得

$$a * a = a * (a \circ (a * a)) = a$$

同理有

$$a \circ a = a$$

(2) 在  $S$  上定义二元关系  $R, \forall a, b \in S$  有

$$\langle a, b \rangle \in R \Leftrightarrow a \circ b = b$$

下面证明  $R$  是  $S$  上的偏序.

根据幂等律,  $\forall a \in S$  都有  $a \circ a = a$ , 即  $\langle a, a \rangle \in R$ , 所以  $R$  在  $S$  上是自反的.

$\forall a, b \in S$  有

$$\begin{aligned} aRb \text{ 且 } bRa &\Leftrightarrow a \circ b = b \text{ 且 } b \circ a = a \\ &\Rightarrow a = b \circ a = a \circ b = b \text{ (由于 } a \circ b = b \circ a) \end{aligned}$$

这就证明了  $R$  在  $S$  上是反对称的.

$\forall a, b, c \in S$  有

$$\begin{aligned} aRb \text{ 且 } bRc &\Rightarrow a \circ b = b \text{ 且 } b \circ c = c \\ &\Rightarrow a \circ c = a \circ (b \circ c) && \text{(由于 } b \circ c = c) \\ &\Rightarrow a \circ c = (a \circ b) \circ c && \text{(结合律)} \\ &\Rightarrow a \circ c = b \circ c = c && \text{(由于 } a \circ b = b, b \circ c = c) \\ &\Rightarrow aRc \end{aligned}$$

这就证明了  $R$  在  $S$  上是传递的.

综上所述,  $R$  为  $S$  上的偏序. 以下把关系  $R$  记作  $\leq$ .

(3) 证明  $\langle S, \leq \rangle$  构成格.

$\forall a, b \in S$  有

$$\begin{aligned} a \circ (a \circ b) &= (a \circ a) \circ b = a \circ b \\ b \circ (a \circ b) &= a \circ (b \circ b) = a \circ b \end{aligned}$$

这就推出  $a \leq a \circ b$  和  $b \leq a \circ b$ , 所以  $a \circ b$  是  $\{a, b\}$  的上界.

假设  $c$  为  $\{a, b\}$  的上界, 则有  $a \circ c = c$  和  $b \circ c = c$ , 从而有

$$(a \circ b) \circ c = a \circ (b \circ c) = a \circ c = c$$

这就证明了  $a \circ b \leq c$ , 所以  $a \circ b$  是  $\{a, b\}$  的最小上界, 即

$$a \vee b = a \circ b$$

为证  $a * b$  是  $\{a, b\}$  的最大下界, 先证

$$a \circ b = b \Leftrightarrow a * b = a \quad (11.7)$$

首先由  $a \circ b = b$  可知

$$a * b = a * (a \circ b) = a$$

反之由  $a * b = a$  可知

$$a \circ b = (a * b) \circ b = b \circ (b * a) = b$$

再由式(11.7)有  $a \leq b \Leftrightarrow a * b = a$ , 依照前边的证明, 类似地可证  $a * b$  是  $\{a, b\}$  的最大下界, 即  $a \wedge b = a * b$ .

根据定理 11.2, 可以给出格的另一个等价定义.

**定义 11.3** 设  $\langle S, *, \circ \rangle$  是代数系统,  $*$  和  $\circ$  是二元运算, 如果  $*$  和  $\circ$  满足交换律、结合律和吸收律, 则  $\langle S, *, \circ \rangle$  构成一个格.

读者可能会注意到, 格中运算满足四条算律, 还有一条幂等律(见定理 11.1), 但幂等律可以

由吸收律推出(见定理 11.2 证明 (1)), 所以上述定义中只需满足三条算律即可.

以后我们不再区别是偏序集定义的格, 还是代数系统定义的格, 而统称为格  $L$ . 下面继续考虑格的性质.

**定理 11.3** 设  $L$  是格, 则  $\forall a, b \in L$  有

$$a \leq b \Leftrightarrow a \wedge b = a \Leftrightarrow a \vee b = b$$

**证** 先证  $a \leq b \Leftrightarrow a \wedge b = a$ .

由  $a \leq a$  和  $a \leq b$  可知  $a$  是  $\{a, b\}$  的下界, 故  $a \leq a \wedge b$ , 显然又有  $a \wedge b \leq a$ . 根据偏序关系的反对称性得  $a \wedge b = a$ .

再证  $a \wedge b = a \Rightarrow a \vee b = b$ , 根据吸收律有

$$b = b \vee (b \wedge a)$$

由  $a \wedge b = a$  得  $b = b \vee a$ , 即  $a \vee b = b$ .

最后证  $a \vee b = b \Rightarrow a \leq b$ . 由  $a \leq a \vee b$  得

$$a \leq a \vee b = b$$

**定理 11.4** 设  $L$  是格,  $\forall a, b, c, d \in L$ , 若  $a \leq b$  且  $c \leq d$ , 则  $a \wedge c \leq b \wedge d$ ,  $a \vee c \leq b \vee d$ .

**证**

$$a \wedge c \leq a \leq b$$

$$a \wedge c \leq c \leq d$$

因此  $a \wedge c \leq b \wedge d$ .

同理可证  $a \vee c \leq b \vee d$ .

**例 11.5** 设  $L$  是格, 证明  $\forall a, b, c \in L$  有

$$a \vee (b \wedge c) \leq (a \vee b) \wedge (a \vee c)$$

**证** 由  $a \leq a$ ,  $b \wedge c \leq b$  得

$$a \vee (b \wedge c) \leq a \vee b$$

由  $a \leq a$ ,  $b \wedge c \leq c$  得

$$a \vee (b \wedge c) \leq a \vee c$$

从而得到

$$a \vee (b \wedge c) \leq (a \vee b) \wedge (a \vee c)$$

例 11.5 说明在格中分配不等式成立. 一般说来, 格中的  $\vee$  和  $\wedge$  运算并不是互相满足分配律的.

下面考虑格的子代数.

**定义 11.4** 设  $\langle L, \wedge, \vee \rangle$  是格,  $S$  是  $L$  的非空子集, 若  $S$  关于  $L$  中的运算  $\wedge$  和  $\vee$  仍构成格, 则称  $S$  是  $L$  的子格.

**例 11.6** 设格  $L$  如图 11.6 所示. 令  $S_1 = \{a, e, f, g\}$  和  $S_2 = \{a, b, e, g\}$ , 则  $S_1$  不是  $L$  的子格,  $S_2$  是  $L$  的子格. 因为对  $e$  和  $f$ , 有  $e \wedge f = c$ , 但  $c \notin S_1$ .

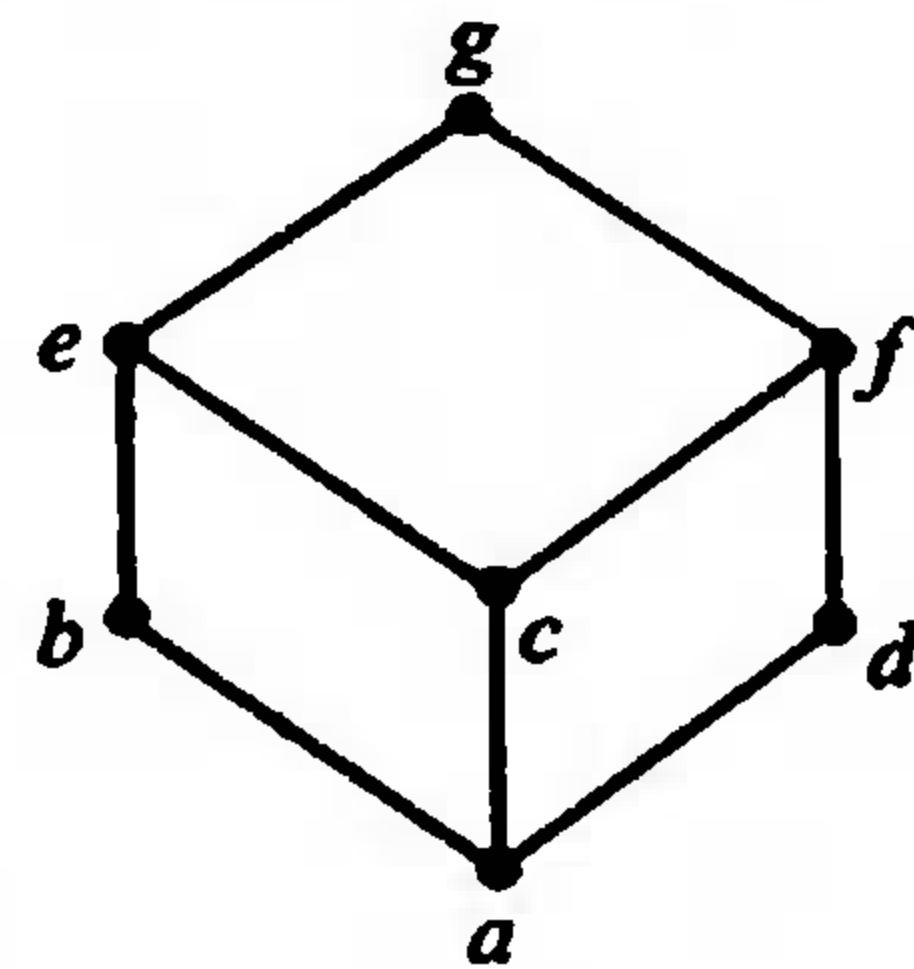


图 11.6

## 11.2 分配格、有补格与布尔代数

下面讨论一些特殊的格——分配格与有补格.

**定义 11.5** 设  $\langle L, \wedge, \vee \rangle$  是格, 若  $\forall a, b, c \in L$ , 有

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$$

$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$$

成立, 则称  $L$  为分配格.

不难证明, 以上两个等式中只要成立一个, 另一个也一定成立.

**例 11.7** 参见图 11.7.

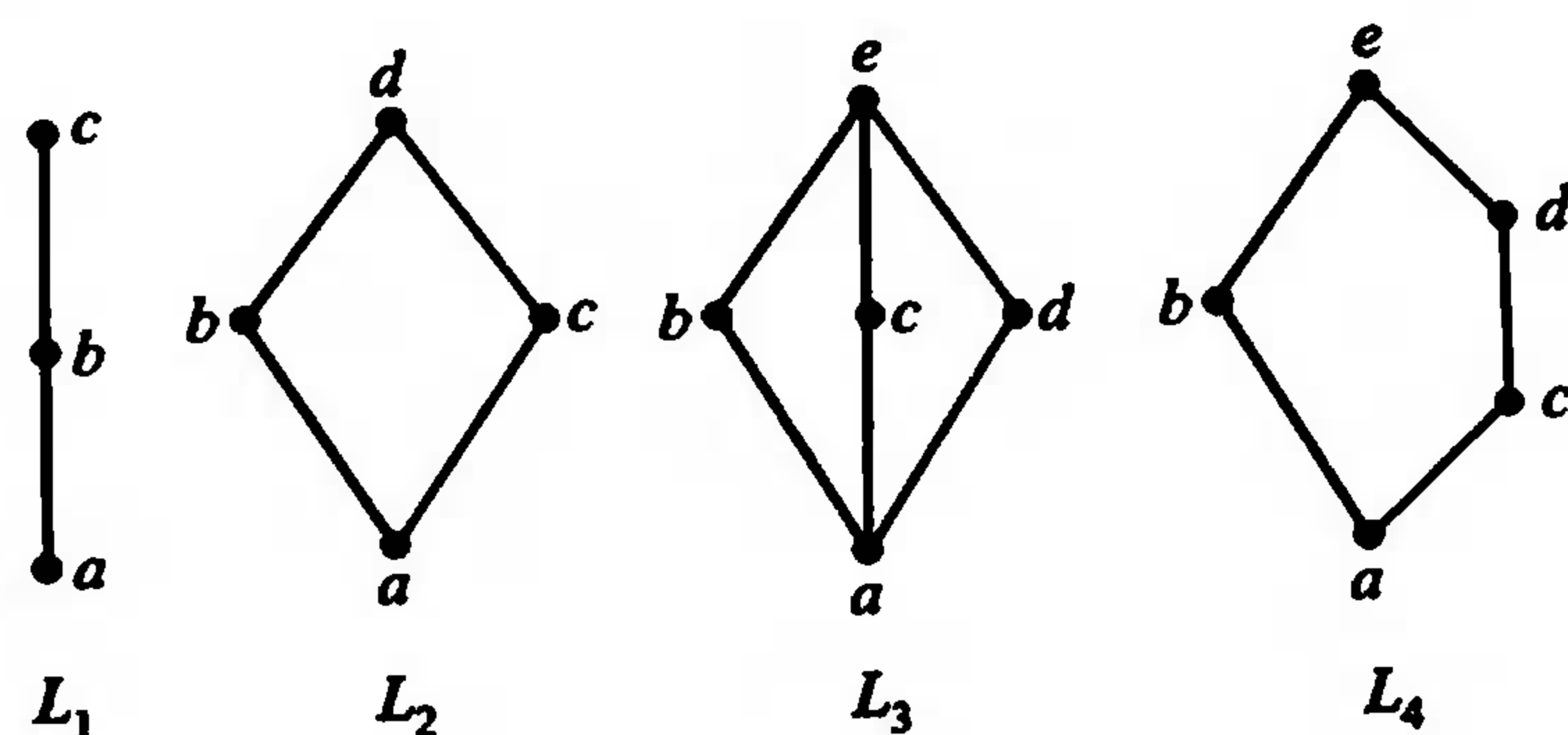


图 11.7

$L_1$  和  $L_2$  是分配格,  $L_3$  和  $L_4$  不是分配格. 在  $L_3$  中,

$$b \wedge (c \vee d) = b \wedge e = b$$

$$(b \wedge c) \vee (b \wedge d) = a \vee a = a$$

而在  $L_4$  中,

$$c \vee (b \wedge d) = c \vee a = c$$

$$(c \vee b) \wedge (c \vee d) = e \wedge d = d$$

称  $L_3$  为钻石格,  $L_4$  为五角格.

下面给出一个格是分配格的充分必要条件.

**定理 11.5** 设  $L$  是格, 则  $L$  是分配格当且仅当  $L$  中不含有与钻石格或五角格同构的子格.

由于该定理的证明比较繁, 故此略去, 读者只要掌握它的应用就行了.

**推论** (1) 小于五元的格都是分配格.

(2) 任何一条链都是分配格.

**例 11.8** 说明图 11.8 中的格是否为分配格, 为什么?

**解**  $L_1, L_2$  和  $L_3$  都不是分配格, 因为  $\{a, b, c, d, e\}$  是  $L_1$  的子格, 并且同构于钻石格,  $\{a, b, c,$

$e, f\}$  是  $L_2$  的子格, 并且同构于五角格.  $\{a, c, b, e, f\}$  是  $L_3$  的子格, 也同构于钻石格.

下面考虑另一种特殊的格——有补格. 先引入有界格的概念.

**定义 11.6** 设  $L$  是格, 若存在  $a \in L$  使得  $\forall x \in L$  有  $a \leq x$ , 则称  $a$  为  $L$  的全下界. 若存在  $b \in L$  使得  $\forall x \in L$  有  $x \leq b$ , 则称  $b$  为  $L$  的全上界.

可以证明, 格  $L$  若存在全下界或全上界, 一定是惟一的, 以全下界为例, 假若  $a_1$  和  $a_2$  都是格  $L$  的全下界, 则有  $a_1 \leq a_2$  和  $a_2 \leq a_1$ . 根据偏序关系  $\leq$  的反对称性必有  $a_1 = a_2$ . 由于全下界和全上界的惟一性, 一般将格  $L$  的全下界记为 0, 全上界记为 1.

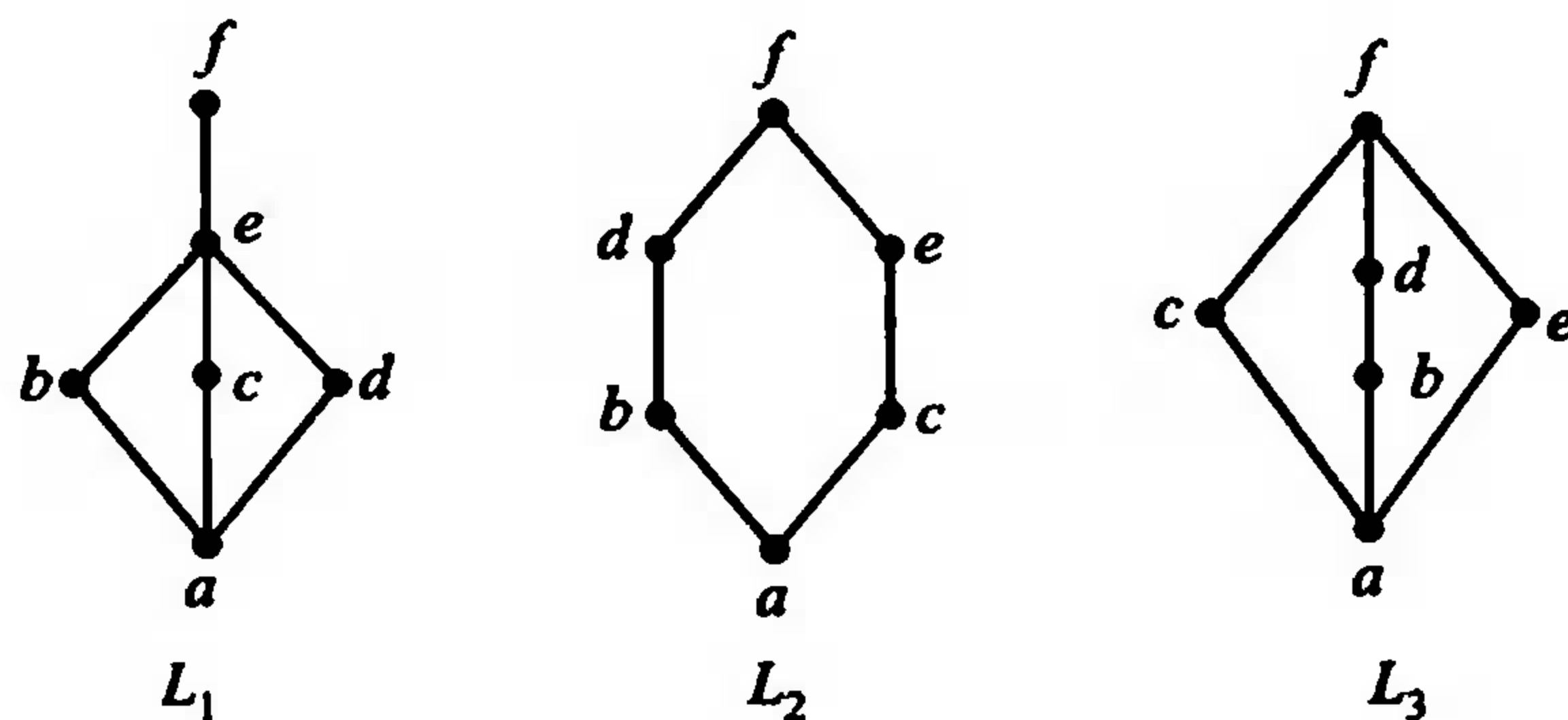


图 11.8

**定义 11.7** 设  $L$  是格, 若  $L$  存在全下界和全上界, 则称  $L$  为有界格, 并将  $L$  记为  $\langle L, \wedge, \vee, 0, 1 \rangle$ .

不难看出, 有限格  $L$  一定是有界格. 设  $L$  是  $n$  元格, 且  $L = \{a_1, a_2, \dots, a_n\}$ , 那么  $a_1 \wedge a_2 \wedge \dots \wedge a_n$  就是  $L$  的全下界, 而  $a_1 \vee a_2 \vee \dots \vee a_n$  就是  $L$  的全上界. 因此  $L$  是有界格. 对于无限格  $L$  来说, 有的是有界格, 有的不是有界格. 如集合  $B$  的幂集格  $\langle P(B), \cap, \cup \rangle$ , 不管  $B$  是有穷集还是无穷集, 它都是有界格. 它的全下界是空集  $\emptyset$ , 全上界是  $B$ . 而整数集  $\mathbb{Z}$  关于通常数的小于或等于关系  $\leq$  构成的格不是有界格, 因为不存在最小和最大的整数.

不难看出, 在有界格中, 全下界 0 是关于  $\wedge$  运算的零元,  $\vee$  运算的单位元. 而全上界 1 是关于  $\vee$  运算的零元,  $\wedge$  运算的单位元. 对于涉及有界格的命题, 如果其中含有全下界 0 或全上界 1, 在求该命题的对偶命题时, 必须将 0 替换成 1, 而将 1 替换成 0.

下面定义有界格中的补元和有补格.

**定义 11.8** 设  $\langle L, \wedge, \vee, 0, 1 \rangle$  是有界格,  $a \in L$ , 若存在  $b \in L$  使得

$$a \wedge b = 0 \text{ 和 } a \vee b = 1$$

成立, 则称  $b$  是  $a$  的补元.

由这个定义不难看出, 若  $b$  是  $a$  的补元, 那么  $a$  也是  $b$  的补元. 换句话说,  $a$  和  $b$  互为补元.

**例 11.9** 考虑图 11.7 中的四个格.

$L_1$  中的  $a$  与  $c$  互为补元, 其中  $a$  为全下界,  $c$  为全上界,  $b$  没有补元.

$L_2$  中的  $a$  与  $d$  互为补元, 其中  $a$  为全下界,  $d$  为全上界,  $b$  与  $c$  也互为补元.

$L_3$  中的  $a$  与  $e$  互为补元, 其中  $a$  为全下界,  $e$  为全上界,  $b$  的补元是  $c$  和  $d$ ,  $c$  的补元是  $b$  和  $d$ ,  $d$  的补元是  $b$  和  $c$ .  $b, c, d$  每个元素都有两个补元。

$L_4$  中的  $a$  与  $e$  互为补元, 其中  $a$  为全下界,  $e$  为全上界,  $b$  的补元是  $c$  和  $d$ ,  $c$  的补元是  $b$ ,  $d$  的补元是  $b$ .

不难证明, 在任何有界格中, 全下界  $0$  与全上界  $1$  总是互补的. 而对于其他的元素, 可能存在补元, 也可能不存在补元. 如果存在补元, 可能是惟一的, 也可能是多个补元. 但对于有界分配格, 如果它的元素存在补元, 则一定是惟一的.

**定理 11.6** 设  $\langle L, \wedge, \vee, 0, 1 \rangle$  是有界分配格, 若  $a \in L$ , 且对于  $a$  存在补元  $b$ , 则  $b$  是  $a$  的惟一补元.

**证** 假设  $c \in L$  也是  $a$  的补元, 则有  $a \vee c = 1$  和  $a \wedge c = 0$ . 又知  $b$  是  $a$  的补元, 也有  $a \vee b = 1$  和  $a \wedge b = 0$ , 从而得到

$$a \vee c = a \vee b, a \wedge c = a \wedge b$$

由于  $L$  是分配格, 从而有

$$\begin{aligned} b &= b \wedge (b \vee a) = b \wedge (c \vee a) = (b \wedge c) \vee (b \wedge a) \\ &= (b \wedge c) \vee (a \wedge c) = (b \vee a) \wedge c = (a \vee c) \wedge c = c \end{aligned}$$

**定义 11.9** 设  $\langle L, \wedge, \vee, 0, 1 \rangle$  是有界格, 若  $\forall a \in L$ , 在  $L$  中都有  $a$  的补元存在, 则称  $L$  是有补格.

例如图 11.7 中的  $L_2, L_3$  和  $L_4$  是有补格,  $L_1$  不是有补格, 图 11.8 中的  $L_2$  和  $L_3$  是有补格,  $L_1$  不是有补格, 因为  $b, c, d, e$  都不存在补元.

**定义 11.10** 如果一个格是有补分配格, 则称它为布尔格或布尔代数.

根据定理 11.6, 在分配格中, 如果一个元素存在补元, 则是惟一的. 因此, 在布尔代数中, 每个元素都存在着惟一的补元, 可以把求补元的运算看做是布尔代数中的一元运算. 从而可以把一个布尔代数标记为  $\langle B, \wedge, \vee, ', 0, 1 \rangle$ , 其中  $\wedge, \vee, 0, 1$  和有界格一样,  $'$  为求补运算,  $\forall a \in B, a'$  是  $a$  的补元.

**例 11.10** (1) 设  $S_{110} = \{1, 2, 5, 10, 11, 22, 55, 110\}$  是 110 的正因子集合. 令  $\gcd, \text{lcm}$  分别表示求两个数的最大公约数和最小公倍数的运算. 则  $\langle S_{110}, \gcd, \text{lcm} \rangle$  构成布尔代数.

(2) 设  $B$  为任意集合, 可以证明  $B$  的幂集格  $\langle P(B), \cap, \cup, \sim, \emptyset, B \rangle$  构成布尔代数, 称为集合代数.

(3) 数理逻辑中的命题代数是布尔代数.

(4) 数字电路中的逻辑代数也是布尔代数.

下面考虑布尔代数的性质.

**定理 11.7** 设  $\langle B, \wedge, \vee, ', 0, 1 \rangle$  是布尔代数, 则

$$(1) \quad \forall a \in B, (a')' = a$$

$$(2) \quad \forall a, b \in B, (a \wedge b)' = a' \vee b', (a \vee b)' = a' \wedge b'$$

**证**  $(a')'$  是  $a'$  的补元,  $a$  也是  $a'$  的补元, 由补元的惟一性得  $(a')' = a$ .

现证明(2),对任意  $a, b \in B$  有

$$\begin{aligned}(a \wedge b) \vee (a' \vee b') &= (a \vee a' \vee b') \wedge (b \vee a' \vee b') \\ &= (1 \vee b') \wedge (a' \vee 1) = 1 \wedge 1 = 1 \\ (a \wedge b) \wedge (a' \vee b') &= (a \wedge b \wedge a') \vee (a \wedge b \wedge b') \\ &= (0 \wedge b) \vee (a \wedge 0) = 0 \vee 0 = 0.\end{aligned}$$

所以  $a' \vee b'$  是  $a \wedge b$  的补元,根据补元的惟一性有

$$(a \wedge b)' = a' \vee b'$$

同理可证  $(a \vee b)' = a' \wedge b'$ .

定理 11.7 的(1)称为双重否定律,(2)称为德摩根律.命题代数与集合代数的双重否定律与德摩根律实际上是这个定理的特例.可以证明德摩根律对有限个元素也是正确的.

布尔代数中各条算律不是彼此独立的,下面的定义告诉我们,只需验证交换律、分配律、同一律和补元律就可以证明一个代数系统是布尔代数了.

**定义 11.11** 设  $\langle B, *, \circ \rangle$  是代数系统,  $*$  和  $\circ$  是二元运算.若  $*$  和  $\circ$  运算满足:

(1) 交换律,即  $\forall a, b \in B$  有

$$a * b = b * a, \quad a \circ b = b \circ a$$

(2) 分配律,即  $\forall a, b, c \in B$  有

$$\begin{aligned}a * (b \circ c) &= (a * b) \circ (a * c) \\ a \circ (b * c) &= (a \circ b) * (a \circ c)\end{aligned}$$

(3) 同一律,即存在  $0, 1 \in B$ ,使得  $\forall a \in B$  有

$$a * 1 = a, a \circ 0 = a$$

(4) 补元律,即  $\forall a \in B$ ,存在  $a' \in B$  使得

$$a * a' = 0, a \circ a' = 1$$

则称  $\langle B, *, \circ \rangle$  是一个布尔代数.

以上定义中的同一律是说  $1$  是  $*$  运算的单位元, $0$  是  $\circ$  运算的单位元.可以证明  $1$  和  $0$  分别也是  $\circ$  和  $*$  运算的零元.  $\forall a \in B$  有

$$\begin{aligned}a \circ 1 &= (a \circ 1) * 1 && \text{(同一律)} \\ &= 1 * (a \circ 1) && \text{(交换律)} \\ &= (a \circ a') * (a \circ 1) && \text{(补元律)} \\ &= a \circ (a' * 1) && \text{(分配律)} \\ &= a \circ a' && \text{(同一律)} \\ &= 0 && \text{(补元律)}\end{aligned}$$

同理可证  $a * 0 = 0$ .

为证明以上定义的  $\langle B, *, \circ \rangle$  是布尔代数,只需证明它是一个格,即证明  $*$  和  $\circ$  运算满足吸收律和结合律.限于篇幅,这里不再赘述,有兴趣的读者可以自己尝试给出证明.

最后,我们不加证明,只是给出与有限布尔代数结构有关的结果.

**定义 11.12** 设  $L$  是格,  $0 \in L, a \in L$ , 若  $\forall b \in L$  有

$$0 < b \leq a \Leftrightarrow b = a$$

则称  $a$  是  $L$  中的原子.

考虑图 11.9 中的几个格. 其中  $L_1$  的原子是  $a$ ,  $L_2$  的原子是  $a, b, c$ ,  $L_3$  的原子是  $a$  和  $b$ . 若  $L$  是正整数  $n$  的全体正因子关于整除关系构成的格, 则  $L$  的原子恰为  $n$  的全体素因子. 若  $L$  是集合  $B$  的幂集格, 则  $L$  的原子就是由  $B$  中元素构成的单元集.

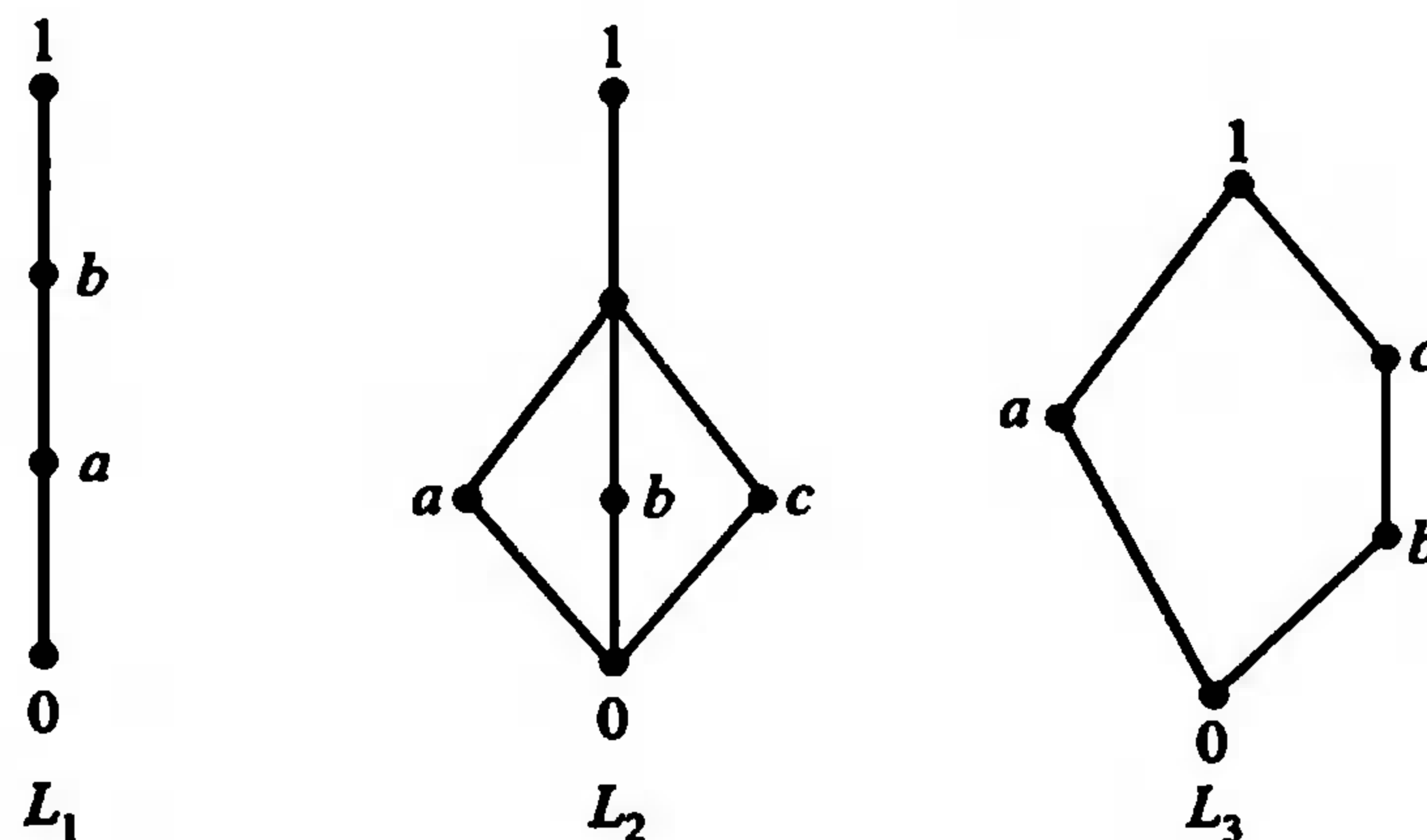


图 11.9

下面的定理说明有限布尔代数有着良好的结构. 限于篇幅, 这里只给出相关的结果, 不再加以证明.

**定理 11.8 (有限布尔代数的表示定理)** 设  $B$  是有限布尔代数,  $A$  是  $B$  的全体原子构成的集合, 则  $B$  同构于  $A$  的幂集代数  $P(A)$ .

**推论 1** 任何有限布尔代数的基数为  $2^n, n \in \mathbf{N}$ .

**证** 设  $B$  是有限布尔代数,  $A$  是  $B$  的所有原子构成的集合. 且  $|A| = n, n \in \mathbf{N}$ . 由定理 11.8 得  $B \cong P(A)$ , 而  $|P(A)| = 2^n$ , 所以  $|B| = 2^n$ .

**推论 2** 任何等势的有限布尔代数都是同构的.

根据这个定理, 有限布尔代数的基数都是 2 的幂, 同时在同构的意义上对于任何  $2^n, n$  为自然数, 仅存在一个  $2^n$  元的布尔代数. 图 11.10 给出了 1 元、2 元、4 元和 8 元的布尔代数.

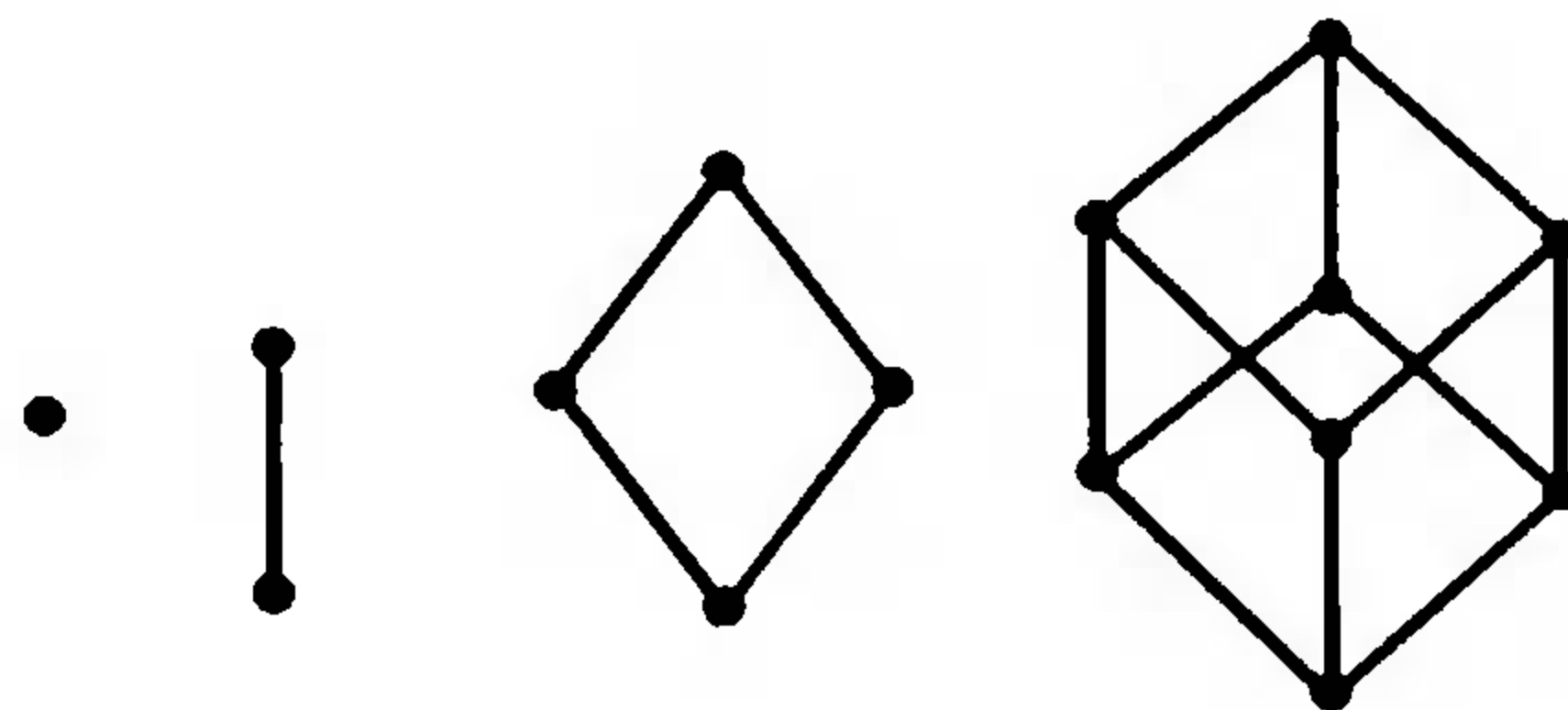


图 11.10

## 习题十一

1. 图 11.11 给出了 6 个偏序集的哈斯图. 判断其中哪些是格. 如果不是格, 说明理由.

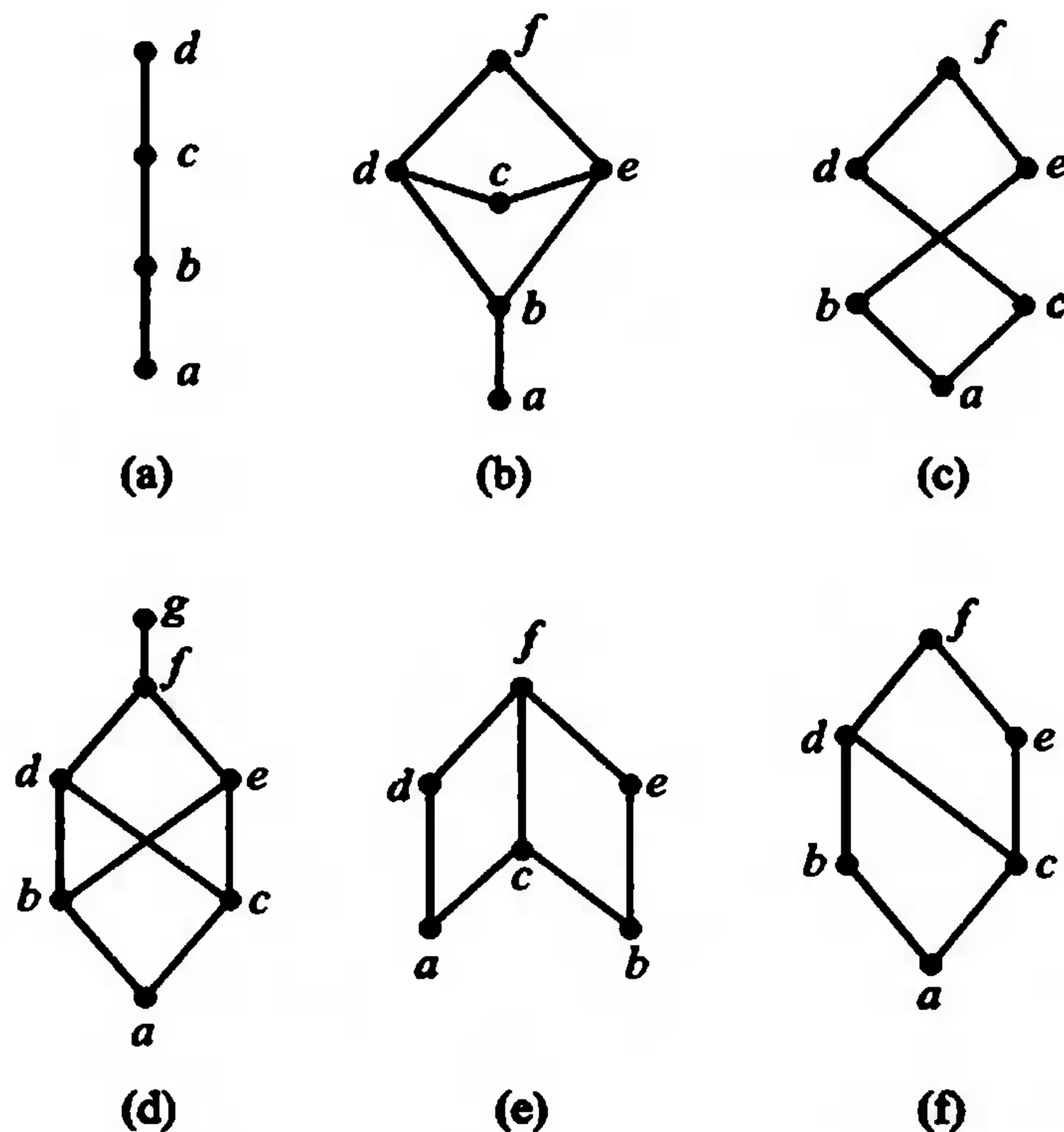


图 11.11

2. 下列各集合对于整除关系都构成偏序集, 判断哪些偏序集是格.

- (1)  $L = \{1, 2, 3, 4, 5\}$ ;
- (2)  $L = \{1, 2, 3, 6, 12\}$ ;
- (3)  $L = \{1, 2, 3, 4, 6, 9, 12, 18, 36\}$ ;
- (4)  $L = \{1, 2, 2^2, \dots, 2^n \mid n \in \mathbb{Z}^+\}$ .

3. (1) 画出  $\langle \mathbb{Z}_{16}, \oplus \rangle$  的子群格;

(2) 画出 3 元对称群  $S_3$  的子群格.

4. 设  $L$  是格, 求以下公式的对偶式:

- (1)  $a \wedge (a \vee b) \leq a$ ;
- (2)  $a \vee (b \wedge c) \leq (a \vee b) \wedge (a \vee c)$ ;
- (3)  $b \vee (c \wedge a) \leq (b \vee c) \wedge a$ .

5. 设  $*$  为集合  $S$  上可交换、可结合的二元运算, 若  $a$  和  $b$  是  $S$  上关于  $*$  运算的幂等元, 证明  $a * b$  也是关于  $*$  运算的幂等元.

6. 设  $L$  是格,  $a, b, c \in L$ , 且  $a \leq b \leq c$ , 证明:  $a \vee b = b \wedge c$ .

7. 针对图 11.7 中的格  $L_2$ , 求出  $L_2$  的所有子格.

8. 设  $\langle L, \leq \rangle$  是格, 任取  $a \in L$ , 令

$$S = \{x \mid x \in L \wedge x \leq a\}$$

证明  $\langle S, \leq \rangle$  是  $L$  的子格.

9. 针对图 11.11 中的每个格, 如果格中的元素存在补元, 则求出这些补元.

10. 说明图 11.11 中的每个格是否为分配格、有补格和布尔格, 并说明理由.

11. 设  $\langle L, \wedge, \vee, 0, 1 \rangle$  是有界格, 证明  $\forall a \in L$ , 有

$$a \wedge 0 = 0, a \vee 0 = a, a \wedge 1 = a, a \vee 1 = 1$$

12. 对以下各小题给定的集合和运算判断它们是哪一类代数系统(半群、独异点、群、环、域、格、布尔代数), 并说明理由.

(1)  $S_1 = \left\{1, \frac{1}{2}, 2, \frac{1}{3}, 3, \frac{1}{4}, 4\right\}$ ,  $*$  为普通乘法;

(2)  $S_2 = \{a_1, a_2, \dots, a_n\}$ ,  $\forall a_i, a_j \in S_2, a_i * a_j = a_i$ , 这里的  $n$  是给定的正整数, 且  $n \geq 2$ ;

(3)  $S_3 = \{0, 1\}$ ,  $*$  为普通乘法;

(4)  $S_4 = \{1, 2, 3, 6\}$ ,  $\forall x, y \in S_4, x \circ y$  和  $x * y$  分别表示求  $x$  和  $y$  的最小公倍数和最大公约数;

(5)  $S_5 = \{0, 1\}$ ,  $*$  表示模 2 加法,  $\circ$  为模 2 乘法.

13. 设  $B$  是布尔代数,  $B$  中的表达式  $f$  是

$$(a \wedge b) \vee (a \wedge b \wedge c) \vee (b \wedge c)$$

(1) 化简  $f$ ;

(2) 求  $f$  的对偶式  $f^*$ .

14. 设  $B$  是布尔代数,  $\forall a, b \in B$ , 证明

$$a \leq b \Leftrightarrow a \wedge b' = 0 \Leftrightarrow a' \vee b = 1.$$

15. 对于  $n = 1, 2, 3, 4, 5$ , 给出所有不同构的  $n$  元格, 并说明其中哪些是分配格、有补格和布尔格.

16. 设  $\langle B, \wedge, \vee, ', 0, 1 \rangle$  是布尔代数, 在  $B$  上定义二元运算  $\oplus$ ,  $\forall x, y \in B$  有

$$x \oplus y = (x \wedge y') \vee (x' \wedge y)$$

问  $\langle B, \oplus \rangle$  能否构成代数系统? 如果能, 指出是哪一种代数系统. 为什么?

17. 设  $B$  是布尔代数,  $\forall a, b, c \in B$ , 若  $a \leq c$ , 则有

$$a \vee (b \wedge c) = (a \vee b) \wedge c$$

称这个等式为模律, 证明布尔代数适合模律.

18. 设  $B$  是布尔代数,  $a_1, a_2, \dots, a_n \in B$ , 证明:

(1)  $(a_1 \vee a_2 \vee \dots \vee a_n)' = a_1' \wedge a_2' \wedge \dots \wedge a_n'$ ;

(2)  $(a_1 \wedge a_2 \wedge \dots \wedge a_n)' = a_1' \vee a_2' \vee \dots \vee a_n'$ .

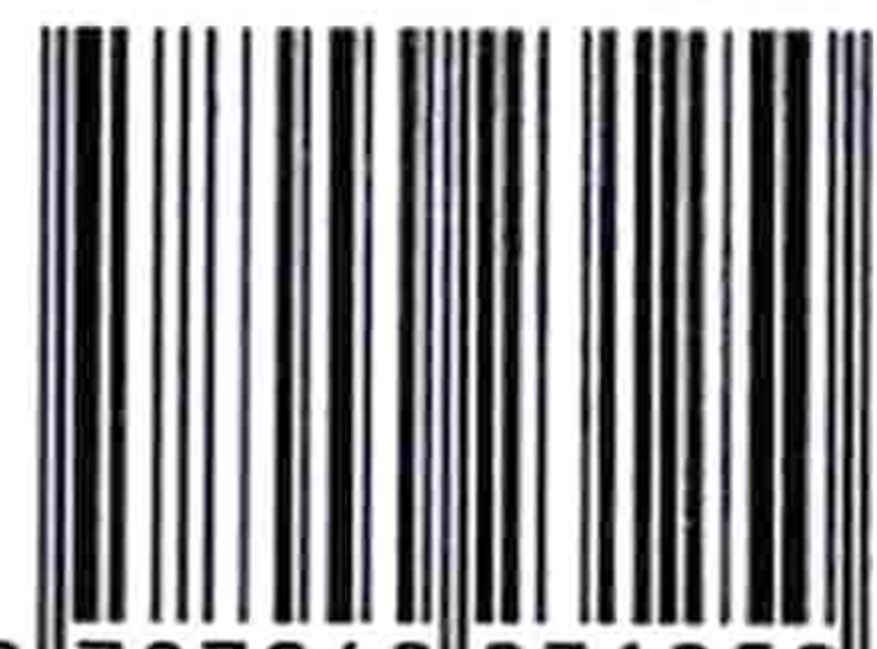
19. 设  $B_1, B_2, B_3$  是布尔代数, 证明: 若  $B_1 \cong B_2, B_2 \cong B_3$ , 则  $B_1 \cong B_3$ .

# 离散数学

## 本书特色：

- ◆ 以教育部计算机科学与技术教学指导委员会制订的计算机科学与技术专业规范为指导，内容涵盖计算机科学技术中常用离散结构的数学基础。
- ◆ 紧密围绕离散数学的基本概念、基本理论精炼选材，体系严谨，内容丰富；面向计算机科学技术，介绍了很多离散数学在计算机科学技术中的应用。
- ◆ 强化描述与分析离散结构的基本方法与能力的训练，配有丰富的例题和习题；例题有针对性，分析讲解到位；习题难易结合，适合学生课后练习。
- ◆ 知识体系采用模块化结构，可以根据不同的教学要求进行调整；语言通俗易懂，深入浅出，突出重点、难点，提示易于出错的地方。
- ◆ 辅助教学资源丰富，配有用于习题课、包含上千道习题的教学辅导用书《离散数学学习指导与习题解析》，PPT 电子教案，教学资源库等。

ISBN 978-7-04-023125-0



9 787040 231250 >

定价 30.50 元