ΣISAN SHUXUE XITI JI

离散数学习题集

抽象代数分册

张立昂 编著

北京大学出版社

离散数学习题集

抽象代数分册

张立昂　编著

北京大学出版社

内 容 简 介

本书为《离散数学习题集》抽象代数分册，包括群、环、域、格与布尔代数等内容，共有三章九节。全书分“内容提要、习题”和“习题解答”两大部分。“内容提要”给出了基本概念、主要性质和定理，包括了解答习题所需要的全部内容。习题有易有难、编排科学、解答详实、注重方法与能力的培养。全书共有习题430余道，书后附有名词索引及符号注释。

读者对象：大专院校计算机系、数学系及相关专业师生，有关专业科研工作者以及计算机科学或抽象代数的自学者、爱好者。

离散数学习题集

抽象代数分册

张立昂　编著

责任编辑：陈进元

*

北京大学出版社出版

（北京大学校内）

北京大学印刷厂印刷

新华书店北京发行所发行　各地新华书店经售

*

787×1092毫米　32开本　8.625印张　192千字

1990年8月第一版　1990年8月第一次印刷

印数：0001--4,000册

ISBN 7-301-01106-7/O·190

定价：3.85元

前　　言

随着计算机科学的迅速发展，作为计算机科学理论基础之一的离散数学，已成为计算机及有关专业的必修课。在广泛收集资料和多年教学积累的基础上，我们编写了这套《离散数学习题集》，以期对离散数学的教与学有所裨益。

习题集每分册分两大部分，第一部分是“内容提要”与“习题”，第二部分是“习题解答”．“内容提要”给出了基本概念、主要性质和定理，基本上划定了该节的取材范围。“习题”中的题目多数取自书后所列参考书，部分是笔者自编的。对于书中的解答，希望对读者掌握概念和解题技巧有所帮助。有些题目给出了多种解法，目的也在于扩大思路、掌握更多的技巧。我们在编写过程中，既考虑到高等院校有关专业的教学需要，也注意到自学者的需要。书中有些题目的内容或难度可能超出了教学大纲的要求，这部分可供学习能力较强、希望进一步钻研的学生学习和参考。

本书为《离散数学习题集》抽象代数分册，共分三章，包括 432 道习题。抽象代数的内容极其丰富，是离散数学的重要组成部分。但在内容的取舍方面，离散数学教材的各种版本之间存在着较大的差异。鉴于这种情况，这本书只包括了抽象代数的最基本的内容。因而，难免有些“应该”包括的内容没有包括进来，而有些问题的深度可能又“超过了”离散数学的要求。就基本内容而言，本书也可以用做数学、应用数学等专业作为公共基础课的抽象代数的教学参考书。

在本书的写作过程中，参考了不少离散数学以及抽象代数方面的教材与著作。在此，对责任编辑陈进元同志，对有关作者和单位，表示衷心地感谢。特别是王汝辑副教授对本书的初稿进行了认真仔细地审阅和修改，也在此向他致以衷心地感谢。

编写这样的习题与解答，对于我们来说还是初次尝试，可能有不少不妥或错误之处，恳请读者批评指正。

编著者

1989年9月于燕东园

目　　录

第一章　群

§1.1　基本概念及其性质

内 容 提 要

设 S 是一个非空集合，S^n 到 S 的一个映射 f 叫做 S 上的一个 **n 元运算**. 非空集合 S 连同它上面的若干个运算 $f_1, f_2, \cdots, f_k$ 称作一个**代数系统**，记作 $\langle S, f_1, \cdots, f_k\rangle$.

设 f 是 S 上的一个 n 元运算，T 是 S 的一个非空子集，如果对于任意的 $a_1, a_2, \cdots, a_n \in T$，恒有 $f(a_1, a_2, \cdots, a_n) \in T$，则称 f 在 T 上**是封闭的**. 此时，f 也是 T 上的一个 n 元运算.

设 f 是 S 上的二元运算，我们常把 $f(a,b)$ 记作 $a*b$，并把二元运算称作**乘法**，而 $*$ 称作**运算符号**. 在不会引起混淆时，常略去运算符号，把 $a*b$ 记作 ab.

如果对于任意的 $a, b \in S$ 都有 $a*b=b*a$，则称二元运算 $*$ **是可交换的**或 $*$ **遵守交换律**. 如果对于任意的 $a, b, c \in S$ 都有 $(a*b)*c=a*(b*c)$，则称 $*$ **是可结合的**或 $*$ **遵守结合律**. 设 $e_l \in S$ ($e_r \in S$)，如果对于任意的 $a \in S$ 都有 $e_l*a=a$ ($a*e_r=a$)，则称 e_l (e_r) 是 S 中关于运算 $*$ 的**左(右)幺元**. 如果 S 中的元素 e 既是左幺元又是右幺元，则称 e 是 S 中关于运算 $*$ 的**幺元**. (左、右)幺元又叫做(左、右)单位元.

设 e 是 S 中关于二元运算 $*$ 的单位元. 对于 $a \in S$，如果

存在 $b\in S$ 使得 $b*a=e$ $(a*b=e)$，则称 b 是 a 的左(右)逆元。如果元素$b\in S$既是 a 的左逆元又是 a 的右逆元，则称 b 是 a 的逆元，通常记作a^{-1}。如果元素 a 具有逆元，则称 a是可逆的或 a 是正则元。

设 G 是一个非空集合，$*$是 G 上的二元运算，如果 $*$ 是可结合的，则称$\langle G,*\rangle$是一个半群。含有幺元的半群称作独异点。

所有元素都可逆的独异点称作群，即设 G 是一个非空集合，$*$ 是 A 上的二元运算，如果满足下述三条：

(1) 结合律成立：$(a*b)*c=a*(b*c)$，$\forall a,b,c\in G$；

(2) 有单位元$e\in G$：$a*e=e*a=a$，$\forall a\in G$；

(3) G 的每一个元素a都有逆元 a^{-1}：$a*a^{-1}=a^{-1}*a=e$。

则称$\langle G,*\rangle$是一个群。

当不会引起混淆时，我们常把(半)群$\langle G,*\rangle$说成(半)群 G。

设$\langle G,*\rangle$是一个(半)群，$A\subseteq G$ 且 $A\neq\varnothing$，如果$\langle A,*\rangle$也构成一个(半)群，则称$\langle A,*\rangle$是$\langle G,*\rangle$的子(半)群。

设$\langle G,*\rangle$是一个群，e 是单位元。那么，$\langle\{e\},*\rangle$和$\langle G,*\rangle$本身都是$\langle G,*\rangle$的子群，称作 G 的平凡子群。G 的非平凡子群叫做 G 的真子群。

交换群 运算是可交换的群称作交换群或 Abel 群。交换群中的运算通常叫做加法，运算符号记作 $+$。交换群中的单位元又称作零元，记作 0。元素 a 的逆元又称作 a 的负元，记作 $-a$。

只含有有限个元素的群称作有限群，否则称作无限群。有限群中的元素个数称作有限群的阶数。有限群 $\langle G,*\rangle$的阶数用 $|G|$ 表示。

设$\langle G,*\rangle$是一个群，$a\in G$，使$a^m=e$的最小自然数m叫做a的周期(或a的阶数)。如果不存在这样的m，则说a的周期是无限的。

设$\langle G,*\rangle$是一个群，A和B是G的两个非空子集。称G的子集

$$AB=\{a*b\mid a\in A,b\in B\}$$

为A和B的乘积。

定理1.1.1 如果代数系统$\langle A,*\rangle$既有左单位元e_l又有右单位元e_r，则$e_l=e_r$是$\langle A,*\rangle$的唯一的单位元。

定理1.1.2 设$\langle A,*\rangle$是一个独异点，$a,b\in A$。

(1) 如果a有左逆元a'，又有右逆元a''，则$a'=a''$是a的逆元；

(2) 如果a是可逆的，则a的逆元是唯一的；

(3) 如果a是可逆的，则a^{-1}也可逆且$(a^{-1})^{-1}=a$；

(4) 如果a,b可逆，则$a*b$也可逆且$(a*b)^{-1}=b^{-1}*a^{-1}$。

定理1.1.3 设$\langle G,*\rangle$是一个群，$a,b,c\in G$。则

(1) 方程$a*x=b$和$x*a=b$有解且解是唯一的，

(2) 消去律成立，即$a*b=a*c$或$b*a=c*a\Rightarrow b=c$。

定理1.1.4 设$\langle G,*\rangle$是一个群，H是G的非空子集，则$\langle H,*\rangle$为$\langle G,*\rangle$的子群的充分必要条件是

(1) 运算$*$在H上是封闭的，即$x*y\in H$，$\forall x,y\in H$，

(2) $x^{-1}\in H$，$\forall x\in H$。

定理1.1.5 设$\langle G,*\rangle$是一个群，H是G的非空子集。如果H是有限集且$*$在H上是封闭的，则$\langle H,*\rangle$是$\langle G,*\rangle$的子群。

定理1.1.6 设$\langle G,*\rangle$是一个群，H是G的非空子集。如果对于任意的$x,y\in H$都有$x*y^{-1}\in H$，则$\langle H,*\rangle$是$\langle G,*\rangle$的子

群。

定理1.1.7 群G的任意多个子群的交仍是G的子群.

习 题

1.1.1 数的加、减、乘、除运算是否为下述集合上的二元运算：

1）实数集R；

2）非零实数集$R^* = R - \{0\}$；

3）正整数集Z^+；

4）$A = \{2n+1 \mid n \in Z\}$，其中$Z$是整数集；

5）$B = \{2^K \mid K \in Z\}$。

1.1.2 数的加法和乘法在下述集合上是否封闭：

1）$A = \{0,1\}$；

2）$B = \{-1,1\}$；

3）$C = \{a\sqrt{2} + b \mid a,b \in Z\}$；

4）$D = \{x \mid x为素数\}$；

5）$E = \{x \mid x 为复数且 |x| = 1\}$。

1.1.3 下述二元运算$\circ$在实数集R上是否为可结合的，是否为可交换的：

1）$a \circ b = a + 2b$；

2）$a \circ b = a + b - ab$；

3）$a \circ b = b$；

4）$a \circ b = |a + b|$。

1.1.4 在下述代数系统$\langle A, * \rangle$中，是否存在左单位元、右单位元、单位元。如果存在的话，请给出：

1）A为实数集，

$$a * b = a + b - ab；$$

2) A 为实数集，

$$a*b=b;$$

3) A 为正整数集，

$$a*b=a^b;$$

4) A 为正整数集，

$$a*b=\gcd(a,b);$$

这里gcd(a,b)表示 a 和 b 的最大公约数。

5) A 为正整数集，

$$a*b=\mathrm{lcm}(a,b);$$

这里lcm(a,b)表示 a 和 b 的最小公倍数。

1.1.5 设代数系统$\langle A,*\rangle$，其中$A=\{a,b,c,d\}$，$*$由乘法表定义如下。问运算$*$是否是可交换的；A是否有单位元；如果有单位元，指出哪些元素是可逆的，并给出它们的逆元。

1)

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

2)

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

1.1.6 设代数系统$\langle A,*\rangle$，$\theta_l,\theta_r\in A$。对于所有的$x\in A$都有$\theta_l*x=\theta_l$，$x*\theta_r=\theta_r$，试证$\theta_l=\theta_r$并且这样的元素是唯一的。

1.1.7 设A是一个非空集合，定义

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

试证明$\langle A,\circ\rangle$是一个半群.

1.1.8 设G表示平面上所有点的集合，对任意两点a，$b\in G$，定义$a\circ b$为线段a,b的中点。问$\circ$是不是G上的一个二元运算？$\langle G,\circ\rangle$是不是一个半群？

1.1.9 设S是非空集合A的所有二元关系组成的集合，试证明S关于二元关系的合成"$\circ$"构成一个有单位元的半群。

1.1.10 设A是一个非空集合，A^A是A到A的所有映射组成的集合。试证明A^A关于映射的合成"$\circ$"构成一个有单位元的半群。

1.1.11 设$A=\{0,1\}$，试给出半群$\langle A^A,\circ\rangle$的乘法表，这里"$\circ$"是映射的合成。

1.1.12 给定正整数k，$N_k=\{0,1,\cdots,k-1\}$。对于任意的$a,b\in N_k$，定义$a*b$等于用k除ab得到的余数。

1）当$k=6$时，给出$*$的乘法表。

2）证明$\langle N_k,*\rangle$是一个半群。

1.1.13 设S是一个半群，且左、右消去律成立，即$\forall a$，$b,c\in S$，$ab=ac$或$ba=ca\Rightarrow b=c$。证明S是交换半群当且仅当$\forall a,b\in S$，$(ab)^2=a^2b^2$。

1.1.14 设S是一个有单位元e的半群，$a,b\in S$，b是正则元且$ab=ba$。证明$ab^{-1}=b^{-1}a$。

1.1.15 设$\langle Z^+,*\rangle$，其中Z^+为正整数集，$*$为求最小公

倍数. 即 $a*b=\mathrm{lcm}(a,b)$, $\forall a,b\in Z^+$. 问 $\langle Z^+,*\rangle$ 是否是半群? $*$ 是可交换的吗? Z^+ 有没有单位元? 如果有单位元, 给出所有的可逆元素.

1.1.16 设 $\langle S,\circ\rangle$ 是一个有单位元 e 的半群, 令 $G=S^S$, 对任意的 $f,g\in G$, 规定

$$(f*g)(x)=f(x)\circ g(x),\quad \forall x\in S.$$

证明 $\langle G,*\rangle$ 是一个有单位元的半群.

1.1.17 设 S 是一个半群, $G=\{f_a \mid a\in S,\ f_a(x)=ax,\ \forall x\in S\}$, 证明 $\langle G,\circ\rangle$ 是 $\langle S^S,\circ\rangle$ 的子半群. 这里 "$\circ$" 是映射的合成.

1.1.18 设 $\langle S,*\rangle$ 是一个半群, 如果对所有的 $a,b\in S$, 只要 $a\neq b$, 必有 $a*b\neq b*a$. 证明

1) $\forall a\in S$, 有 $a*a=a$;

2) $\forall a,b\in S$, 有 $a*b*a=a$;

3) $\forall a,b,c\in S$, 有 $a*b*c=a*c$.

1.1.19 设 S 是交换半群, $a,b\in S$, 且 $a^2=a$, $b^2=b$, 试证明 $(ab)^2=ab$.

1.1.20 设 $\langle S,*\rangle$ 是一个半群, S 是一个有限集. 试证明存在 $a\in S$ 使 $a^2=a$.

1.1.21 设 $\langle S,*\rangle$ 是一个半群, $a\in S$, 在 S 上定义 $\circ$ 如下:

$$x\circ y=x*a*y,\quad \forall x,y\in S.$$

证明 $\langle S,\circ\rangle$ 也是一个半群.

1.1.22 下列集合关于指定的运算是否构成群?

1) 给定 $a>0$ 且 $a\neq 1$, 集合 $G=\{a^n \mid n\in Z\}$, 关于数的乘法;

2) 非负整数集 N, 关于数的加法;

3）正有理数集Q^+，关于数的乘法；

4）整数集Z，关于数的减法；

5）给定正整数n，集合$U_n=\{z|z\in C,z^n=1\}$，关于数的乘法；

6）$U=\{z|z\in C,\ z^n=1,n\in Z^+\}$，关于数的乘法；

7）正实数集R^+，关于数的除法；

8）一元实系数多项式集合，关于多项式加法；

9）一元实系数多项式集合，关于多项式乘法；

10）n维线性空间，关于向量加法。

1.1.23　设G表示有理数域Q到Q的线性变换

$$f_{a,b}(x)=ax+b,\ a\neq0,\ a,b\in Q$$

构成的集合。试证明G关于变换的合成构成群。

1.1.24　给定正整数m，令$G=\{km|k\in Z\}$，证明$\langle G,+\rangle$是一个群。

1.1.25　设$G=\{x|x\in Q$且$x\neq1\}$，定义

$$x\circ y=x+y-xy,\quad \forall x,y\in G.$$

证明$\langle G,\circ\rangle$是一个群。

1.1.26　设$\langle A,*\rangle$是一个群，对每一个元素$a\in A$，作映射σ_a：

$$\sigma_a(x)=a*x,\quad \forall x\in A.$$

记$G=\{\sigma_a|a\in A\}$。证明G关于映射的合成构成一个群。

1.1.27　给定一个n阶实对称矩阵A，$O(A)$是所有满足$P'AP=A$的可逆矩阵P组成的集合。证明$O(A)$关于矩阵乘法组成一个群。这里P'是P的转置矩阵。

1.1.28　设$G=\{a+bi|a,b\in Z\}$，其中i是虚数单位。证明$\langle G,+\rangle$是一个群。

1.1.29　设$X=\{x|x\in R,x\neq0,1\}$，在X上定义6个函

数如下：$f_1(x)=x$，$f_2(x)=x^{-1}$，$f_3(x)=1-x$，$f_4(x)=(1-x)^{-1}$，$f_5(x)=(x-1)x^{-1}$，$f_6(x)=x(x-1)^{-1}$。试证明$\langle F,\circ\rangle$是一个群，其中$F=\{f_i|1\leqslant i\leqslant 6\}$，$\circ$是函数的复合运算。

1.1.30 设$\langle S,\circ\rangle$是一个半群。在$S\times S$上定义：

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

证明$\langle S\times S,*\rangle$构成一个半群，并且当$\langle S,\circ\rangle$有单位元时，$\langle S\times S,*\rangle$也有单位元；当$\langle S,\circ\rangle$是群时，$\langle S\times S,*\rangle$也是群。

1.1.31 有单位元且适合消去律的有限半群一定是群。

1.1.32 设$\langle G,*\rangle$是一个半群，且对所有的$a,b\in G$，方程$a*x=b$，$x*a=b$有解。试证明$\langle G,*\rangle$是一个群。

1.1.33 设$\langle G,*\rangle$是一个半群，并且满足下述条件：

1）存在右单位元，即存在$e\in G$使$a*e=a$，$\forall a\in G$，

2）G中的每个元素都有右逆元，即$\forall a\in G$，存在$b\in G$使$a*b=e$。

试证明$\langle G,*\rangle$是一个群。

1.1.34 设G是一个群，$a,b,c\in G$。证明

$$xaxba=xbc$$

在G中有且仅有一个解。

1.1.35 设G是一个群，$x,y\in G$，k是一个正整数。证明$(x^{-1}yx)^k=x^{-1}yx$的充分必要条件是$y^k=y$。

1.1.36 设G是一个群，$a,b\in G$且$(ab)^2=a^2b^2$。证明$ab=ba$。

1.1.37 设$\langle G,\circ\rangle$是一个群，$u\in G$。定义

$$a*b=a\circ u^{-1}\circ b,\quad \forall a,b\in G。$$

证明$\langle G,*\rangle$也是一个群。

1.1.38　在整数集 Z 上定义

$$a\circ b = a + b - 2,\quad \forall a,b\in Z.$$

证明 $\langle Z,\circ\rangle$ 是一个群。

1.1.39 试证明

$$G=\left\{\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix},\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix},\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix},\begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix}\right\}$$

关于矩阵乘法构成群。

1.1.40　设 $M=\{\langle a,b\rangle \mid a,b\in R, a\neq 0\}$，在 M 上定义运算如下：

$$\langle a,b\rangle\circ\langle c,d\rangle = \langle ac, ad+b\rangle.$$

试验证 $\langle M,\circ\rangle$ 构成一个群。

1.1.41　设 $G=\{a,b,c\}$，在 G 上定义二元运算 $\circ$ 如表 1.1.1

表 1.1.1

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

试证明 $\langle G,\circ\rangle$ 是一个群，并且任意 3 个元素的群的乘法表，在不计元素的记号和顺序时必为上述形式。

1.1.42　证明 $H=\{f_{1,b} \mid b\in Q\}$ 是题1.1.23中 Q 上线性交换群 G 的子群。

1.1.43　设 $G=\{\langle x_1,x_2,x_3,x_4\rangle \mid x_i=0,1, 1\leqslant i\leqslant 4\}$。对任意的 $x=\langle x_1,x_2,x_3,x_4\rangle$，$y=\langle y_1,y_2,y_3,y_4\rangle\in G$，定义

$$x\oplus y=\langle x_1\veebar y_1, x_2\veebar y_2, x_3\veebar y_3, x_4\veebar y_4\rangle,$$

其中$\forall$定义如表1.1.2。

表 1.1.2

$\forall$	0	1
0	0	1
1	1	0

试证明：1) $\langle G,\oplus\rangle$是一个群，

2) $\langle H,\oplus\rangle$ 是 $\langle G,\oplus\rangle$ 的子群，其中$H=\{\langle 0,0,0,0\rangle,\langle 1,1,1,1\rangle\}$。

1.1.44 证明 $H=\{x\mid x\in C,x^n=1,n\in Z^+\}$ 是非零复数乘法群C^*的子群。

1.1.45 设S是非空集合，$\langle G,+\rangle$是一个交换群。对任意的$f,g\in G^S$ 规定

$$(f+g)(x)=f(x)+g(x),\quad \forall x\in S$$

试证明$\langle G^S,+\rangle$是一个交换群。

1.1.46 设$G=\{2^m3^n\mid m,n\in Z\}$。证明$G$关于普通数的乘法构成一个群。

1.1.47 设$\langle G,*\rangle$是一个群，令

$$R=\{\langle a,b\rangle\mid a,b\in G,\text{存在}\theta\in G\text{使}b=\theta*a*\theta^{-1}\}。$$

验证R是G上的等价关系，若$\langle a,b\rangle\in R$，则称b是a的共轭元素。R在G上诱导的等价类称作共轭元素类。

1.1.48 设G是一个群。$\sim$是G的元素之间的等价关系，并且$\forall a,x,y\in G$。

$$ax\sim ay\Rightarrow x\sim y。$$

证明$H=\{x\mid x\in G,x\sim e\}$是$G$的子群，其中$e$是$G$的单位元。

1.1.49 设H和K都是群G的子群，令