第九章　半群与群

必备知识：第四章、第五章和第六章。

在 1.6 节已经介绍了数学结构的概念。在下面一些章节中，将展开讨论其他类型的数学体系，例如(命题，∧，∨，～)这样一些还没有给出明确名字的结构，但是其他一些结构如 B_n 已给出了名字，它是有 n 个元素的布尔代数。本章将认识另外几类数学结构——半群，群，环和域。在第十章学习有限状态机时将用到半群。对于群、环和域的一些基本概念也将展开讨论，并且将它应用到第十一章的编码理论中。

回　顾

*群*的术语最初是由 Evariste Galois(1811－1832)在 1830 年提出的，它应用于满足某些性质的一个有限集的一系列置换之中。Galois 生于并卒于法国巴黎。直到 12 岁他才进入了巴黎一所颇负名望的公立中学学习，在此之前，他在家里由母亲进行教育。在 16 岁的时候，他就完全沉浸在数学的学习之中，甚至忽略了其他课程。他两次参加有高度声誉的 École Polytechnique 的入学考试，但都没有通过，最后进入了一所较小的高等研究所 École Normale。他在这里的第一年就发表了四篇论文。其后不久他又写了三篇论文，但在他将论文交给一些著名的数学家，希望他们能够引见给科学院时，却都被弄丢了。1831 年，Galois 又写了一篇论文，仔细地描述了他的研究结果。但这篇论文却因为“难以理解”而被退回。在 1830 年法国革命期间，Galois 因指责其学校领导而被校方开除了。另外，他还因政治活动被捕入狱。1832 年 5 月 30 日，他在一场决斗中受了致命伤，并在第二天去世，年仅 20 岁。在决斗之前，Galois 留了一封信给他的一位朋友，信中详述了他的研究成果。他的成果对于同时代的人来说实在太超前了，因此直到 1870 年他的所有研究成果才完全展现在人们的面前。

大家都知道二次多项式求根公式。由于通过算术运算和开方就能得到根，因此称二次多项式是可通过根式求解的多项式。到 16 世纪，人们已经发现了通过系数求解三次和 4 次多项式有类似于求解二次多项式的公式。在此后三百多年中，数学家试图用求根公式解一般的 5 次多项式，但一直都没有成功。挪威数学家 Niels Henrik Abel(1802—1829)在 19 岁时证明了一般的 5 次或更高次数多项式不能通过根式求解。然而，许多特殊的 5 次或更高次的多项式可通过根式求解，因此确定哪些多项式具有这种性质就变得很重要了。Galois 通过研究与多项式相关的群的性质(现在称为*伽罗瓦群*)，发现了可通过根式求解的多项式的特征。

9.1 再论二元运算

本书在前面(见 1.6 节)定义了二元运算并且在 5.2 节提到二元运算可以用来定义一个函数。下面将把该过程反过来看，即把二元运算定义为具有某种性质的一个函数。

集合 A 上的二元运算是一个处处有定义的函数 $f: A\times A\to A$。注意二元运算必须满足下面的性质。

1．$\mathrm{Dom}(f)=A\times A$，所以 f 把 $A\times A$ 中每个有序对(a, b)对应于 A 中的一个元素 $f(a, b)$，即：二元运算必须为 A 的每个有序元素对而定义。

2．因为二元运算是一个函数，所以每个有序对仅对应 A 中惟一元素。

因此，可以说二元运算是把 A 中元素的每个有序对对应于 A 的惟一元素的一个法则。读者应该注意，此定义比第一章给出的定义有更多的限制，但是这样做简化了这一章的讨论。下面将给出大量的例子。

人们习惯上用一个符号如$*$而不是 f 来表示二元运算。用 $a*b$(而不是$*(a,b)$)表示对应于(a, b)的元素。应该强调的是如果 a 和 b 是 A 中的元素，那么 $a*b\in A$，并且常常把该性质说成是在运算$*$下 A 是**封闭的**。

例 1 设 $A=\mathbf{Z}$，定义 $a*b$ 为 $a+b$，那么$*$是 $\mathbf{Z}$ 上的一个二元运算。 ■

例 2 设 $A=\mathbf{R}$，定义 $a*b$ 为 a/b，那么$*$不是一个二元运算，因为 A 中元素的每个有序对并非都有定义，例如 $3*0$ 没有定义，因为不能用 0 作为除数。 ■

例 3 设 $A=\mathbf{Z}^+$，定义 $a*b$ 为 $a-b$，那么$*$不是一个二元运算，因为 A 中元素的每个有序对并不都对应于 A 中的一个元素，例如 $2*5\notin A$。 ■

例 4 设 $A=\mathbf{Z}$，定义 $a*b$ 为比 a 和 b 两者都小的一个数，那么$*$不是一个二元运算，因为 A 中元素的每个有序对并不都对应于 A 的*惟*一元素，例如 $8*6$ 可能是 5,4,3,1，等等。因此，在这种情况下，$*$是从 $A\times A$ 到 A 的一种关系，但不是一个函数。 ■

例 5 设 $A=\mathbf{Z}$，定义 $a*b$ 为 $\max\{a, b\}$，那么$*$是一个二元运算。例如，$2*4=4$，$-3*(-5)=-3$。 ■

例 6 设 $A=P(S)$，其中 S 是某个集合，如果 V 和 W 是 S 的子集，定义 $V*W$ 为 $V\cup W$，那么$*$是 A 上的一个二元运算。而且，如果定义 $V*'W$ 为 $V\cap W$，那么$*'$是 A 上的另一个二元运算。 ■

正如例 6 所示，在同一集合上可以定义多个二元运算。

例 7 设 M 是所有 $n\times n$(n 为固定值)布尔矩阵的集合，定义 $\boldsymbol{A}*\boldsymbol{B}$ 为 $\boldsymbol{A}\vee\boldsymbol{B}$(见 1.5 节)，那么$*$是一个二元运算。同样若定义 $\boldsymbol{A}*\boldsymbol{B}$ 为 $\boldsymbol{A}\wedge\boldsymbol{B}$，则$*$也是一个二元运算。 ■

例 8 设 L 是一个格，定义 $a*b$ 为 $a\wedge b$(a 和 b 的最大下界)，那么$*$是 L 上的一个二元运算。对于 $a\vee b$(a 和 b 的最小上界)，这也是正确的。 ■

表

如果 $A=\{a_1, a_2, \cdots, a_n\}$是一个有限集合，可通过图 9.1 所示的表在 A 上定义一个二元运算。在(i, j)位置上的值表示元素 a_i*a_j。

*	a_1	a_2	...	a_j	...	a_n
a_1						
a_2						
⋮						
a_i				a_i*a_j		
⋮						
a_n						

图 9.1

例 9 设 $A=\{0,1\}$，可以用下面的表定义二元运算∨和∧。

∨	0	1
0	0	1
1	1	1

∧	0	1
0	0	0
1	0	1

■

设 $A=\{a, b\}$，现在确定能够定义在 A 上的二元运算的个数。A 的每个二元运算*可以用下表描述。

*	a	b
a		
b		

因为每个空格可以用元素 a 或 b 填充，所以推出存在 $2\cdot2\cdot2\cdot2=2^4$ 即 16 种方法完成这张表。因此，在 A 上存在 16 种二元运算。

二元运算的性质

在 1.6 节中定义的二元运算的几条性质在本章具有特殊的重要性，对其重述如下。

如果对于 A 中的所有元素 a 和 b 有 $a*b=b*a$，则称集合 A 上的二元运算是交换的。

例 10 **Z** 上的加法二元运算(像例 1 中讨论的那样)是交换的。 ■

例 11 **Z** 上的减法二元运算不是交换的，因为 $2-3\neq3-2$。 ■

由一张表描述的二元运算是交换的当且仅当表中的值关于主对角线是对称的。

例 12 集合 $A=\{a, b, c, d\}$ 下述的哪个二元运算是交换的？

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

(a)

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

(b)

解 (a) 中的运算不是交换的，因为 $a*b$ 是 c 而 $b*a$ 是 b。(b) 中的运算是交换的，因为表中的值关于主对角线是对称的。■

如果对于 A 中所有元素 a, b 和 c，有

$$a*(b*c)=(a*b)*c$$

则称集合 A 上的二元运算是**结合的**。

例 13 **Z** 上的加法二元运算是结合的。■

例 14 **Z** 上的减法二元运算不是结合的，因为 $2-(3-5)\neq(2-3)-5$。■

例 15 设 L 是一个格，由 $a*b=a\wedge b$ 定义的二元运算(见例 8)是交换的和结合的。它还满足**幂等**性质 $a\wedge a=a$。此例的部分逆命题也是正确的，如例 16 所述。■

例 16 设*是集合 A 上的一个二元运算，假设*满足下面的性质：对于 A 中的任意 a，b 和 c，有

1. $a=a*a$　　幂等性质
2. $a*b=b*a$　　交换性质
3. $a*(b*c)=(a*b)*c$　　结合性质

那么在 A 上定义一个关系≤为：$a\leqslant b$ 当且仅当 $a=a*b$，证明：$(A,\leqslant)$是一个偏序集，并且对于 A 中的所有 a 和 b，有 $\mathrm{GLB}(a, b)=a*b$。

解 必须证明≤是自反的、反对称的和传递的。因为 $a=a*a$，所以对于 A 中的所有 a 有 $a\leqslant a$，从而≤是自反的。

现在假设 $a\leqslant b$ 且 $b\leqslant a$，那么由定义和性质 2 有

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

所以 $a=b$，因此≤是反对称的。

如果 $a\leqslant b$ 且 $b\leqslant c$，那么

$$a=a*b=a*(b*c)=(a*b)*c=a*c$$

所以 $a\leqslant c$，因此≤是传递的。

最后，必须证明对于 A 中的所有 a 和 b，有 $a*b=a\wedge b$(a 和 b 关于≤的最大下界)。因为 $a*b=a*(b*b)=(a*b)*b$，所以 $a*b\leqslant b$。用类似的方法可以证明 $a*b\leqslant a$，所以 $a*b$ 是 a 和 b 的一个下界。于是，如果 $c\leqslant a$ 且 $c\leqslant b$，那么由定义得 $c=c*a$ 和 $c=c*b$。因此，$c=(c*a)*b=c*(a*b)$，所以 $c\leqslant a*b$，这就证明了 $a*b$ 是 a 和 b 的最大下界。■

习 题 9.1

在第 1 题~第 8 题中，确定*的描述是否是已知集合上一个正确的二元运算的定义。

1. 在 $\mathbf{R}$ 上，$a*b$ 是 ab(普通乘法)。
2. 在 $\mathbf{Z}^+$ 上，$a*b$ 是 a/b。
3. 在 $\mathbf{Z}$ 上，$a*b$ 是 a^b。
4. 在 $\mathbf{Z}^+$ 上，$a*b$ 是 a^b。
5. 在 $\mathbf{Z}^+$ 上，$a*b$ 是 $a-b$。
6. 在 $\mathbf{R}$ 上，$a*b$ 是 $a\sqrt{b}$ 。
7. 在 $\mathbf{R}$ 上，$a*b$ 是比 ab 小的最大有理数。
8. 在 $\mathbf{Z}$ 上，$a*b$ 是 $2a+b$。

在第 9 题~第 19 题中，确定二元运算*是否是已知集合上交换的和结合的运算。

9. 在 $\mathbf{Z}^+$ 上，$a*b$ 是 $a+b+2$。
10. 在 $\mathbf{Z}$ 上，$a*b$ 是 ab。
11. 在 $\mathbf{R}$ 上，$a*b$ 是 $a\times|b|$。
12. 在非零实数集合上，$a*b$ 是 a/b。
13. 在 $\mathbf{R}$ 上，$a*b$ 是 a 和 b 中的最小值。
14. 在 $n\times n$ 布尔矩阵的集合上，$\boldsymbol{A}*\boldsymbol{B}$ 是 $\boldsymbol{A}\odot\boldsymbol{B}$(见 1.5 节)。
15. 在 $\mathbf{R}$ 上，$a*b$ 是 $ab/3$。
16. 在 $\mathbf{R}$ 上，$a*b$ 是 $ab+2b$。
17. 在一个格 A 上，$a*b$ 是 $a\vee b$。
18. 在 2×1 矩阵的集合上，有

$$\begin{bmatrix}a\\b\end{bmatrix}*\begin{bmatrix}c\\d\end{bmatrix}=\begin{bmatrix}a+c\\b+d+1\end{bmatrix}$$

19. 在有理数集合上，$a*b=\dfrac{a+b}{2}$ 。
20. 证明或反证：$\mathbf{Z}^+$ 上的二元运算 $a*b=\mathrm{GCD}(a,b)$有幂等性质。
21. 证明或反证：第 19 题中的二元运算有幂等性质。
22. 填写下表使得二元运算*是交换的。

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

23. 填写下表使得二元运算*是交换的并且有幂等性质。

*	a	b	c
a		c	
b			
c	c	a	

24. 考虑由下表定义在集合 $A=\{a, b, c\}$ 上的二元运算*。

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

(a) *是一个交换运算吗？

(b) 计算 $a*(b*c)$和$(a*b)*c$。

(c) *是一个结合运算吗？

25. 考虑由下表定义在集合 $A=\{a, b, c, d\}$ 上的二元运算*。

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

计算：

(a) $c*d$ 和 $d*c$。

(b) $b*d$ 和 $d*b$。

(c) $a*(b*c)$和$(a*b)*c$。

(d) *是交换运算吗？是结合运算吗？

在题 26 和 27 中，完成所给定的表，使得二元运算*是结合运算。

26.

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

27.

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

28. 设 A 是有 n 个元素的集合，则在 A 上可定义多少种二元运算？

29. 设 A 是有 n 个元素的集合，则在 A 上可定义多少种交换的二元运算？

30. 设 $A=\{a, b\}$。

(a) 为可定义在 A 上的 16 种二元运算制作一张表。

(b) 利用分题(a)确定 A 上交换的二元运算。

31. 设 $A=\{a, b\}$。

(a) 利用第 30 题确定 A 上结合的二元运算。

(b) 利用第 30 题确定 A 上满足幂等性质的二元运算。

32. 设$*$是集合 A 上的一个二元运算，假设$*$满足例 16 中讨论的幂等律、交换律和结合律，在 A 上用 $a\leqslant b$ 当且仅当 $b=a*b$ 定义一个关系$\leqslant$。证明：$(A, \leqslant)$是一个偏序集，并且对所有 a 和 b，$\mathrm{LUB}(a, b)=a*b$。

33. 描述集合 A 上二元运算的定义与 1.6 节给出的二元运算的定义有什么不同。同时根据 1.6 节的定义解释在一个集合上的二元运算是否是一个二元运算。

34. 在集合 S 上由 $a*b=b$ 定义一个二元运算。问$*$是结合运算吗？是交换运算吗？是幂等运算吗？

9.2 半 群

本节定义由集合以及一个二元运算所组成的一个简单数学结构，它有许多重要的应用。

半群就是非空集合 S 以及一个定义在 S 上的可结合的二元运算$*$，将用$(S,*)$表示半群，或者当运算$*$很清楚时可简记为 S。还可以把 $a*b$ 看成是 a 和 b 的**积**。如果$*$是一个交换运算，则称半群$(S,*)$是交换半群。

例 1 从 9.1 节得到 $(\mathbf{Z}, +)$是一个交换半群。 ■

例 2 集合 $P(S)$，其中 S 是一个集合，加上并运算，它是一个交换半群。 ■

例 3 集合 $\mathbf{Z}$ 以及减法二元运算就不是一个半群，因为减法不是可结合运算。 ■

例 4 设 S 是一个固定的非空集合，S^S 是所有函数 $f: S\to S$ 的集合。如果 f 和 g 是 S^S 的元素，定义 $f*g$ 为 $f\circ g$，即函数的合成。那么$*$是 S^S 上的一个二元运算。从 4.7 节得到$*$是结合的。因此，$(S^S,*)$是一个半群。半群 S^S 不是交换的。 ■

例 5 设$(L, \leqslant)$是一个格，在 L 上用 $a*b=a\vee b$ 定义一个二元运算，那么 L 是一个半群。 ■

例 6 设 $A=\{a_1, a_2, \cdots, a_n\}$是一个非空集合，从 1.3 节可知 A^*是 A 中元素的所有有限序列的集合，即 A^*是由 A 中字母表所形成的所有词组成的。设α和β是 A^*的元素，注意连接是 A^*上的一个二元运算 $\cdot$。回顾如果$\alpha=a_1a_2\cdots a_n$和$\beta=b_1b_2\cdots b_k$，那么$\alpha\cdot\beta=a_1a_2\cdots a_nb_1b_2\cdots b_k$。容易看到如果$\alpha$,$\beta$和$\gamma$是 A^*中的任意元素，那么

$$\alpha\cdot(\beta\cdot\gamma)=(\alpha\cdot\beta)\cdot\gamma$$

所以 $\cdot$ 是一个结合二元运算，从而$(A^*, \cdot)$是一个半群。称半群$(A^*, \cdot)$是由 A **产生的自由半群**。 ■

在半群$(S,*)$中，可以建立如下一般化的结合性质，其证明省略。

定理 1 如果 $a_1, a_2, \cdots, a_n (n\geqslant 3)$是半群中的任意元素，那么在由元素 $a_1, a_2, \cdots, a_n$ 形成的积中任意插入有意义的括号，积的结果都是相等的。 ■

例 7 定理 1 表明下面的积

$$((a_1*a_2)*a_3)*a_4,\quad a_1*(a_2*(a_3*a_4)),\quad (a_1*(a_2*a_3))*a_4$$

都是相等的。 ■

如果 $a_1, a_2, \cdots, a_n$ 是半群$(S, *)$中的元素，那么把它们的积写成 $a_1*a_2*\cdots*a_n$ 而省略括号。

半群$(S,*)$中的一个元素e如果对所有$a\in S$有$e*a=a*e=a$，那么称它为**单位元**。由1.6节的定理1可知，单位元一定是惟一的。

例8　半群$(\mathbf{Z},+)$中的数0是单位元。■

例9　半群$(\mathbf{Z}^+,+)$没有单位元。■

一个**幺半群**是有单位元的半群$(S,*)$。

例10　例2中定义的半群$P(S)$有单位元$\varnothing$，因为$\varnothing*A=\varnothing\cup A=A=A\cup\varnothing=A*\varnothing$对于任意$A\in P(S)$都成立，因此$P(S)$是一个幺半群。■

例11　例4中定义的半群S^S有单位元I_S，因为对任意$f\in S^S$，$I_S*f=I_S\circ f=f\circ I_S=f*I_S$，所以$S^S$是一个幺半群。■

例12　例6中定义的半群A^*实际上是一个具有单位元Λ(空序列)的幺半群，因为$\alpha\cdot\Lambda=\Lambda\cdot\alpha=\alpha$对所有$\alpha\in A^*$都成立。■

例13　集合A上所有关系的集合是在合成运算下的幺半群，单位元是相等关系Δ(见4.7节)。■

设$(S,*)$是一个半群，T是S的一个子集，如果T在运算$*$下是封闭的(即当a和b是T中的元素时，$a*b\in T$)，那么$(T,*)$称为$(S,*)$的**子半群**。类似地，设$(S,*)$是有单位元e的幺半群，T是S的一个非空子集，如果T在运算$*$下是封闭的，并且$e\in T$，那么$(T,*)$称为$(S,*)$的**子幺半群**。

注意到在半群的任意子集上结合性质成立，从而半群$(S,*)$的子半群$(T,*)$本身就是一个半群。类似地，幺半群的子幺半群本身是幺半群。

例14　如果T是所有偶数的集合，那么$(T,\times)$是幺半群$(\mathbf{Z},\times)$的子半群，其中$\times$是普通乘法，但它不是子幺半群，因为$\mathbf{Z}$的单位元(数1)不属于T。■

例15　如果$(S,*)$是一个半群，那么$(S,*)$是$(S,*)$的一个子半群。类似地，设$(S,*)$是一个幺半群，那么$(S,*)$是$(S,*)$的一个子幺半群，并且如果$T=\{e\}$，那么$(T,*)$也是$(S,*)$的一个子幺半群。■

假设$(S,*)$是一个半群，$a\in S$，对任意$n\in\mathbf{Z}^+$，递归定义幂a^n如下：

$$a^1=a,\quad a^n=a^{n-1}*a,\quad n\geqslant 2$$

而且如果$(S,*)$是一个幺半群，还可定义$a^0=e$。能够证明：如果m和n是非负整数，那么$a^m*a^n=a^{m+n}$。

例16　(a) 如果$(S,*)$是一个半群，$a\in S$，$T=\{a^i|i\in\mathbf{Z}^+\}$，那么$(T,*)$是$(S,*)$的一个子半群。

(b) 如果$(S,*)$是一个幺半群，$a\in S$，$T=\{a^i|i\in\mathbf{Z}^+$或$i=0\}$，那么$(T,*)$是$(S,*)$的一个子幺半群。■

同构和同态

两个偏序集之间的同构在6.1节是作为一一对应定义的，该对应保持序关系以及偏序集的主要特征。现在在保持二元运算的两个一一对应半群之间定义一个同构。一般地，在两个同类数学结构之间的同构应该保持结构的主要特征。

设$(S,*)$和$(T,*')$是两个半群，如果函数f：$S\to T$是从S到T的一个一一对应，并且对S中的所有a和b有$f(a*b)=f(a)*'f(b)$，则称f：$S\to T$是从$(S,*)$到$(T,*')$的一个**同构**。

如果 f 是从$(S,*)$到$(T,*')$的一个同构，那么因为 f 是一一对应的，所以从 5.1 节的定理 1 得到 f^{-1} 存在并且是从 T 到 S 的一一对应。现在证明 f^{-1} 是从$(T,*')$到$(S,*)$的一个同构。设 a'和 b'是 T的任意两个元素，因为 f 是满射，所以能够找到 S 中的元素 a 和 b，使得 $f(a)=a'$和 $f(b)=b'$。于是 $a=f^{-1}(a')$和 $b=f^{-1}(b')$。从而

$$f^{-1}(a'*'b')=f^{-1}(f(a)*'f(b))=f^{-1}(f(a*b))$$
$$=(f^{-1}\circ f)(a*b)=a*b=f^{-1}(a')*f^{-1}(b')$$

因此，f^{-1} 是一个同构。

此时称半群$(S,*)$和$(T,*')$是**同构的**并且记为 $S\simeq T$。

为了证明半群$(S,*)$与$(T,*')$是同构的，必须使用下述步骤。

步骤 1：定义一个函数 f：$S\to T$，Dom(f)=S。

步骤 2：证明 f 是单射。

步骤 3：证明 f 是满射。

步骤 4：证明 $f(a*b)=f(a)*'f(b)$。

例 17 设 T 是所有偶数的集合，证明半群$(\mathbf{Z},+)$与$(T,+)$是同构的。

解 **步骤 1**：定义函数 f：$\mathbf{Z}\to T$ 满足 $f(a)=2a$。

步骤 2：证明 f 是如下单射。假设 $f(a_1)=f(a_2)$，那么 $2a_1=2a_2$，所以 $a_1=a_2$，因此，f 是单射。

步骤 3：证明 f 是满射。假设 b 是任意偶数，那么 $a=b/2\in\mathbf{Z}$，且 $f(a)=f(b/2)=2(b/2)=b$，所以 f 是满射。

步骤 4：显然有 $f(a+b)=2(a+b)=2a+2b=f(a)+f(b)$。因此，$(\mathbf{Z},+)$和$(T,+)$是同构的半群。 ■

一般地，证明一个已知函数 f：$S\to T$ 是或不是一个同构是相当简单的。然而，证明两个半群是同构的一般来讲是很难的，因为人们必须创建同构 f。

同偏序集或格的同构情况一样，当两个半群$(S,*)$与$(T,*')$同构时，它们只是在元素的性质上可能不同，它们的半群结构是相同的。如果 S 和 T 是有限半群，那么它们各自的二元运算可用表给出。于是如果可以把 S 的元素重排并且重新标号，使得它的表与 T 的表是完全相同的，则 S 和 T 是同构的。

例 18 设 $S=\{a,b,c\}$，$T=\{x,y,z\}$，容易证明下面的运算表分别给出了 S 和 T 的半群结构。

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

*	x	y	z
x	z	x	y
y	x	y	z
z	y	z	x

设 $f(a)=y$，$f(b)=x$，$f(c)=z$，用它们的象取代 S 中的元素并且重排表格，恰好得到 T 的表。因此，S 和 T 是同构的。 ■

定理 2 设$(S,*)$和$(T,*')$是分别有单位元 e 和 e'的幺半群，f：$S\to T$ 是一个同构，那么 $f(e)=e'$。

证明 设 b 是 T 的任意一个元素，因为 f 是满射，所以在 S 中存在一个元素 a，使得 $f(a)=b$。于是 $a=a*e$，$b=f(a)=f(a*e)=f(a)*'f(e)=b*'f(e)$。类似地，因为 $a=e*a$，$b=f(e)*'b$，所以，对任

意 $b\in T$，$b=b*'f(e)=f(e)*'b$。这就推出 $f(e)$是 T 的一个单位元。因为单位元是惟一的，所以得到 $f(e)=e'$。■

如果$(S,*)$和$(T,*')$都是半群且 S 有单位元但 T 没有，那么由定理 2 得到$(S,*)$与$(T,*')$不可能是同构的。

例 19　设 T 是所有偶数的集合，×是普通乘法，那么半群$(\mathbf{Z},\ \times)$与$(T,\ \times)$不是同构的，因为 $\mathbf{Z}$ 有单位元而 T 没有。■

在两个半群同构的定义中去掉单射和满射的条件，可以得到比较两个半群的代数结构的另一个重要方法。

设$(S,*)$和$(T,*')$是两个半群，如果一个处处有定义的函数 f：$S\to T$ 对于 S 中的所有 a 和 b 有 $f(a*b)=f(a)*'f(b)$，则称 f 是从$(S,*)$到$(T,*')$的一个**同态**。如果 f 还是满射，则称 T 是 S 的**同态象**。

例 20　$A=\{0,1\}$，考虑半群$(A^*,\cdot)$和$(A,+)$，其中 · 是连接运算，+ 由下表定义：

+	0	1
0	0	1
1	1	0

定义函数 f：$A^*\to A$ 为

$$f(\alpha)=\begin{cases}1, & \alpha\text{ 有奇数个 }1\\ 0, & \alpha\text{ 有偶数个 }1\end{cases}$$

易证：如果α 和β 是 A^*的任意元素，那么

$$f(\alpha\cdot\beta)=f(\alpha)+f(\beta)$$

因此，f 是一个同态。函数 f 是满射，因为 $f(0)=0$，$f(1)=1$，但是 f 不是一个同构，因为它不是单射。■

同构与同态之间的差异是同构必须是单射和满射。同构与同态两者都有积的象是象的积。

下面定理的证明完全类似于定理 2 的证明，留给读者作为练习。

定理 3　设$(S,*)$和$(T,*')$分别是有单位元 e 和 e'的幺半群，f：$S\to T$ 是从$(S,*)$到$(T,*')$的一个同态且是满射，那么 $f(e)=e'$。■

定理 3 是一个比定理 2 更强或更一般的命题，因为结论只需要更少(更弱)的条件。

定理 3 以及下面的两个定理表明如果半群$(T,*')$是半群$(S,*)$的一个同态象，那么$(T,*')$在代数上很像$(S,*)$。

定理 4　设 f 是从半群$(S,*)$到半群$(T,*')$的一个同态，如果 S'是$(S,*)$的一个子半群，那么

$$f(S')=\{t\in T\mid t=f(s),\ \text{对 } s\in S'\}$$

即在 f 下 S'的象是$(T,*')$的一个子半群。

证明　如果 t_1 和 t_2 是 $f(S')$的任意两个元素，那么在 S'中存在 s_1 和 s_2 具有 $t_1=f(s_1)$和 $t_2=f(s_2)$，于是 $t_1*'t_2=f(s_1)*'f(s_2)=f(s_1*s_2)=f(s_3)$，其中 $s_3=s_1*s_2\in S'$，从而 $t_1*'t_2\in f(S')$。

因此，$f(S')$在运算$*'$下是封闭的。因为结合性质在T中成立，所以它在$f(S')$中也成立，因此，$f(S')$是$(T,*')$的一个子半群。■

定理5 如果f是从交换半群$(S,*)$到半群$(T,*')$的一个同态且是满射，那么$(T,*')$也是交换半群。

证明 设t_1和t_2是T的任意元素，那么在S中存在s_1和s_2使得

$$t_1=f(s_1),t_2=f(s_2)$$

所以

$$t_1*'t_2=f(s_1)*'f(s_2)=f(s_1*s_2)=f(s_2*s_1)=f(s_2)*'f(s_1)=t_2*'t_1$$

因此，$(T,*')$也是交换的。■

习 题 9.2

1. 设$A=\{a,b\}$，下面哪些表定义了A上的一个半群？哪些定义了A上的一个幺半群？

(a)

*	a	b
a	a	b
b	a	a

(b)

*	a	b
a	a	b
b	b	b

2. 设$A=\{a,b\}$，下面哪些表定义了A上的一个半群？哪些定义了A上的一个幺半群？

(a)

*	a	b
a	b	a
b	a	b

(b)

*	a	b
a	a	b
b	b	a

3. 设$A=\{a,b\}$，下面哪些表定义了A上的一个半群？哪些定义了A上的一个幺半群？

(a)

*	a	b
a	a	a
b	b	b

(b)

*	a	b
a	b	b
b	a	a

在第4题~第16题中，确定有二元运算的集合是否是一个半群、一个幺半群或者两者都不是。如果它是一个幺半群，指出它的单位元。如果它是一个半群或一个幺半群，确定它是否是交换的。

4. $\mathbf{Z}^+$，$*$定义为普通的乘法。
5. $\mathbf{Z}^+$，$a*b$定义为$\max\{a,b\}$。
6. $\mathbf{Z}^+$，$a*b$定义为$\mathrm{GCD}\{a,b\}$。
7. $\mathbf{Z}^+$，$a*b$定义为a。
8. 非零实数，$*$定义为普通乘法。
9. $P(S)$，S是一个集合，$*$定义为交。
10. 布尔代数B，$a*b$定义为$a\wedge b$。
11. $S=\{1,2,3,6,12\}$，$a*b$定义为$\mathrm{GCD}(a,b)$。
12. $S=\{1,2,3,6,9,18\}$，$a*b$定义为$\mathrm{LCM}(a,b)$。

13. $\mathbf{Z}$，$a*b=a+b-ab$。

14. 偶数集合，$a*b$ 定义为 $\dfrac{ab}{2}$。

15. 2×1 矩阵的集合，定义为

$$\begin{bmatrix} a \\ b \end{bmatrix} * \begin{bmatrix} c \\ d \end{bmatrix} = \begin{bmatrix} a+c \\ b+d+1 \end{bmatrix}$$

16. 形如 $3k+1$ 的整数的集合，$k \in \mathbf{Z}^+$，其中$*$是普通的乘法。

17. 下表定义了一个半群或幺半群吗？

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

18. 下表定义了一个半群或幺半群吗？

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

19. 完成下表使其成为一个半群。

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

20. 完成下表使其定义一个幺半群。

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

21. 设 $S=\{a, b\}$，为半群 S^S 写出运算表。此半群是交换的吗？

22. 设 $S=\{a,b\}$，为半群$(P(S),\cup)$写出运算表。

23. 设 $A=\{a,b,c\}$，考虑半群$(A^*, \cdot)$，其中 $\cdot$ 是连接运算。如果$\alpha=abac$，$\beta=cba$，$\gamma=babc$，计算

(a) $(\alpha \cdot \beta) \cdot \gamma$，　(b) $\gamma \cdot (\alpha \cdot \alpha)$　(c) $(\gamma \cdot \beta) \cdot \alpha$

24. 对一个半群中元素的一个子集，使其成为一个子半群有什么要求？

25. 对一个幺半群中元素的一个子集，使其成为一个子幺半群有什么要求？

26. 证明或反证：半群$(S,*)$的两个子半群的交是$(S,*)$的一个子半群。

27. 证明或反证：幺半群$(S,*)$的两个子幺半群的交是$(S,*)$的一个子幺半群。

28. 设$A=\{0,1\}$，考虑半群$(A^*,\cdot)$，其中$\cdot$是连接运算，设T是由奇数个1的所有序列所组成的A^*的子集，$(T,\cdot)$是$(A,\cdot)$的一个子半群吗？

29. 设$A=\{a,b\}$，存在两个不同构的半群$(A,*)$和$(A,*')$吗？

30. 幺半群中的一个元素x称作**幂等的**，如果它满足$x^2=x*x=x$。证明：在交换幺半群S中所有幂等元素的集合是S的一个子幺半群。

31. 设$(S_1,*_1)$，$(S_2,*_2)$和$(S_3,*_3)$是半群，f：$S_1\to S_2$和g：$S_2\to S_3$是同态，证明：$g\circ f$是从S_1到S_3的一个同态。

32. 设$(S_1,*)$，$(S_2,*')$和$(S_3,*'')$是半群，f：$S_1\to S_2$和g：$S_2\to S_3$是同构，证明：$g\circ f$：$S_1\to S_3$是一个同构。

33. 在定理2的证明中使用了f的哪些性质？

34. 解释为什么定理1的证明能够用来作为定理3的证明？

35. 设$\mathbf{R}^+$是所有正实数的集合，证明：由$f(x)=\ln x$所定义的函数f：$\mathbf{R}^+\to\mathbf{R}$是半群$(\mathbf{R}^+,\times)$到半群$(\mathbf{R},+)$上的一个同构，其中$\times$和$+$分别是普通乘法和加法。

36. 设$(S,*)$是一个半群，A是S的一个有限子集。定义$\hat{A}$是A中所有元素的有限乘积的集合。

(a) 证明：$\hat{A}$是$(S,*)$的一个子半群。

(b) 证明：$\hat{A}$是包含A的$(S,*)$的最小子半群。

9.3 半群的积与商

本节将从已有的半群得到新的半群。

定理1 如果$(S,*)$和$(T,*')$是半群，那么$(S\times T,*'')$是一个半群，其中$*''$由$(s_1,t_1)*''(s_2,t_2)=(s_1*s_2,t_1*'t_2)$定义。

证明 证明留作练习。 ■

从定理1可以得到如果S和T分别是有单位元e_S和e_T的幺半群，那么$S\times T$是有单位元(e_S,e_T)的一个幺半群。

下面讨论半群$(S,*)$上的等价关系。由于一个半群不仅仅是一个集合，所以将会发现半群上的某些等价关系给出了半群结构的一些附加信息。

半群$(S,*)$上的一个等价关系R称为一个**同余关系**，如果$a\,R\,a'$和$b\,R\,b'$推出$(a*b)R(a'*b')$。

例1 考虑半群$(\mathbf{Z},+)$和$\mathbf{Z}$上的等价关系R，它由$a\ R\ b$当且仅当$a\equiv b(\mathrm{mod}\ 2)$定义。回顾4.5节已讨论过这种等价关系。注意，如果a和b被2除时有相同的余数，那么$2|(a-b)$。现在证明这种关系是如下同余关系。

如果$a\equiv b(\mathrm{mod}\ 2)$和$c\equiv d(\mathrm{mod}\ 2)$，那么2整除$a-b$和2整除$c-d$，所以$a-b=2m$和$c-d=2n$，其中$m$和$n$属于$\mathbf{Z}$。此外，有

$$(a-b)+(c-d)=2m+2n$$

或

$$(a+c)-(b+d)=2(m+n)$$

所以

$$a+c\equiv b+d\ (\mathrm{mod}\ 2)$$

因此，关系是同余关系。 ■

例 2 设 $A=\{0,1\}$，考虑由 A 产生的自由半群$(A^*, \cdot)$，在 A 上定义下面的关系：

$\alpha R \beta$ 当且仅当α和β有相同个数的 1。

证明：R 是$(A^*, \cdot)$上的一个同余关系。

解 首先证明 R 是一个等价关系。我们有

1．对任意$\alpha \in A^*$，有$\alpha R \alpha$。

2．如果$\alpha R \beta$，那么α和β有相同个数的 1，所以$\beta R \alpha$。

3．如果$\alpha R \beta$且$\beta R \gamma$，那么α和β有相同个数的 1，β和γ有相同个数的 1，所以α和γ有相同个数的 1。因此，有$\alpha R \gamma$。

其次证明 R 是一个同余关系。假设$\alpha R \alpha'$且$\beta R \beta'$，那么α和α'有相同个数的 1,β和β'有相同个数的 1。因为在$\alpha \cdot \beta$中 1 的个数是α里 1 的个数和β里 1 的个数之和，所以推出$\alpha \cdot \beta$里 1 的个数同$\alpha' \cdot \beta'$里 1 的个数相等。因此，$(\alpha \cdot \beta) R (\alpha' \cdot \beta')$，从而 R 是一个同余关系。 ■

例 3 考虑半群$(\mathbf{Z}, +)$，其中+是普通加法。设 $f(x)=x^2-x-2$，在 $\mathbf{Z}$ 上定义下面的关系：$a R b$ 当且仅当 $f(a)=f(b)$。容易证明 R 是 $\mathbf{Z}$ 上的一个等价关系。然而，R 不是一个同余关系，因为有$-1\ R\ 2(f(-1)=f(2)=0)$和$-2\ R\ 3(f(-2)=f(3)=4)$，但是$(-1+(-2))\not R\ (2+3)$，因为 $f(-3)=10$ 和 $f(5)=18$。 ■

从 4.5 节易知，半群$(S,*)$上的等价关系 R 决定 S 的一个划分。设$[a]=R(a)$是包含 a 的等价类，S/R 表示所有等价类的集合。这种背景下更常用记号$[a]$，并且在计算中很少产生混淆。

定理 2 设 R 是半群$(S,*)$上的一个同余关系，考虑从 $S/R \times S/R$ 到 S/R 的关系⊛，它对于 S 中的 a 和 b，有序对$([a],[b])$与$[a*b]$有关。

(a) ⊛是从 $S/R \times S/R$ 到 S/R 的一个函数，像通常一样用$[a] \circledast [b]$表示 $\circledast([a],[b])$。因此，$[a] \circledast [b]=[a*b]$。

(b) $(S/R, \circledast)$是一个半群。

证明 假设$([a],[b])=([a'],[b'])$，那么 $a R a'$和 $b R b'$，所以一定有 $a*b R a'*b'$，因为 R 是一个同余关系。于是，$[a*b]=[a'*b']$，即⊛是一个函数。这意味着⊛是 S/R 上的一个二元运算。

其次，必须证明⊛是一个结合运算。我们有

$$\begin{aligned}[a] \circledast ([b] \circledast [c]) &= [a] \circledast [b*c] = [a*(b*c)] \\ &= [(a*b)*c] \qquad (\text{由 } S \text{ 中} * \text{的结合性质}) \\ &= [a*b] \circledast [c] = ([a] \circledast [b]) \circledast [c]\end{aligned}$$

因此 S/R 是一个半群。称 S/R 是**商半群或因子半群**。注意到⊛是 S/R 上的一类“商二元关系”，S/R 是由同余关系 R 从 S 上原来的二元关系*构造而来的。 ■

推论 1 设 R 是幺半群$(S,*)$上的一个同余关系，如果通过$[a] \circledast [b]=[a*b]$定义 S/R 中的运算⊛，那么$(S/R, \circledast)$是一个幺半群。

证明 如果 e 是$(S,*)$中的单位元，那么容易证明$[e]$是$(S/R, \circledast)$中的单位元。 ■

例 4 考虑例 2 中的情况。因为 R 是幺半群 $S=(A^*, \cdot)$上的一个同余关系，所以推出$(S/R, \odot)$

是一个幺半群，其中$[\alpha]\odot[\beta]=[\alpha\cdot\beta]$。 ■

例 5 如 4.5 节所指出的那样，可以用正整数 n 而不是 2 重复那一小节中的例 4，即在半群$(\mathbf{Z},+)$上定义下面的关系：

$$a\ R\ b \text{ 当且仅当 } a\equiv b(\mathrm{mod}\ n)$$

使用与 4.5 节的例 4 中完全相同的方法，可以证明 R 是一个等价关系，同 $n=2$ 这种情况一样，$a\equiv b(\mathrm{mod}\ n)$推出 $n|(a-b)$。因此，如果 n 是 4，那么

$$2\equiv 6\ (\mathrm{mod}\ 4)$$

即 4 整除(2−6)。将证明$\equiv(\mathrm{mod}\ n)$是 $\mathbf{Z}$ 上的一个同余关系留给读者。

现在设 $n=4$，计算由 $\mathbf{Z}$ 上的同余关系$\equiv(\mathrm{mod}\ 4)$所确定的等价类。可以得到

$$[0]=\{\cdots,-8,-4,0,4,8,12,\cdots\}=[4]=[8]=\cdots$$
$$[1]=\{\cdots,-7,-3,1,5,9,13,\cdots\}=[5]=[9]=\cdots$$
$$[2]=\{\cdots,-6,-2,2,6,10,14,\cdots\}=[6]=[10]=\cdots$$
$$[3]=\{\cdots,-5,-1,3,7,11,15,\cdots\}=[7]=[11]=\cdots$$

这些都是形成商集合 $\mathbf{Z}/\equiv(\mathrm{mod}\ 4)$的所有不同的等价类。习惯上用 Z_n 表示商集 $\mathbf{Z}/\equiv(\mathrm{mod}\ n)$；$Z_n$ 是有运算⊕和单位元[0]的一个幺半群。下面确定半群 Z_4 带运算⊕的加法表。

⊕	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

该表的元素是从$[a]\oplus[b]=[a+b]$得到的。因此

$$[1]\oplus[2]=[1+2]=[3],\ [1]\oplus[3]=[1+3]=[4]=[0]$$
$$[2]\oplus[3]=[2+3]=[5]=[1],\ [3]\oplus[3]=[3+3]=[6]=[2]$$

可以证明，Z_n 通常有 n 个等价类

$$[0],[1],[2],\cdots,[n-1]$$

且$[a]\oplus[b]=[r]$，其中 r 是当 $a+b$ 用 n 除时的余数。因此，如果 n 是 6，那么

$$[2]\oplus[3]=[5],\ [3]\oplus[5]=[2],\ [3]\oplus[3]=[0]$$ ■

下面考察在半群$(S,*)$与商半群$(S/R,\circledast)$结构之间的联系，其中 R 是$(S,*)$上的一个同余关系。

定理 3 设 R 是半群$(S,*)$上的一个同余关系，$(S/R,\circledast)$是对应的商半群，那么由 $f_R(a)=[a]$ 定义的函数 $f_R: S\to S/R$ 是一个同态，且是满射，称其为**自然同态**。

证明 如果$[a]\in S/R$，那么 $f_R(a)=[a]$，所以 f_R 是一个满射函数。此外，如果 a 和 b 是 S 的元素，那么

$$f_R(a*b)=[a*b]=[a]\circledast[b]=f_R(a)\circledast f_R(b)$$

所以 f_R 是一个同态。 ■

定理 4 (同态基本定理) 设 $f: S\to T$ 是半群$(S,*)$到半群$(T,*')$的一个同态，R 是 S 上的关系且定义为对于 S 中的 a 和 b，$a\,R\,b$ 当且仅当 $f(a)=f(b)$。那么

(a) R 是一个同余关系。

(b) $(T,*')$和商半群$(S/R, \circledast)$是同构的。

证明 (a) 证明 R 是一个等价关系。首先因为 $f(a)=f(a)$，所以对每个 $a\in S$，有 $a\,R\,a$。其次，如果 $a\,R\,b$，那么 $f(a)=f(b)$，所以 $b\,R\,a$。最后，如果 $a\,R\,b$ 且 $b\,R\,c$，那么 $f(a)=f(b)$和 $f(b)=f(c)$，所以 $f(a)=f(c)$，即 $a\,R\,c$。因此，R 是一个等价关系。现在假设 $a\,R\,a_1$ 且 $b\,R\,b_1$，那么

$$f(a)=f(a_1),\quad f(b)=f(b_1)$$

用 T 中的乘法，可得

$$f(a)*'f(b)=f(a_1)*'f(b_1)$$

因为 f 是同态的，所以上面的方程可以重写为

$$f(a*b)=f(a_1*b_1)$$

因此

$$(a*b)R(a_1*b_1)$$

所以 R 是一个同余关系。

(b) 现在考虑从 S/R 到 T 的关系 $\bar{f}$，它的定义如下：

$$\bar{f}=\{([a],\ f(a))\mid [a]\in S/R\}$$

首先证明 $\bar{f}$ 是一个函数。假设$[a]=[a']$，那么 $a\,R\,a'$，所以 $f(a)=f(a')$，这就推出 $\bar{f}$ 是一个函数。于是可以写出 $\bar{f}: S/R\to T$，其中对于 $[a]\in S/R$ 有 $\bar{f}([a])=f(a)$。

其次证明 $\bar{f}$ 是单射。假设 $\bar{f}([a])=\bar{f}([a'])$，那么 $f(a)=f(a')$。所以 $a\,R\,a'$，这就推出$[a]=[a']$。因此，$\bar{f}$ 是单射。

下面证明 $\bar{f}$ 是满射。假设 $b\in T$，因为 f 是满射，所以在 S 中存在某个元素 a 使得 $f(a)=b$，于是 $\bar{f}([a])=f(a)=b$，从而 $\bar{f}$ 是满射。

最后，有

$$\begin{aligned}\bar{f}([a]\circledast[b])&=\bar{f}([a*b])=f(a*b)=f(a)*'f(b)\\&=\bar{f}([a])*'\bar{f}([b])\end{aligned}$$

因此，$\bar{f}$ 是一个同构。 ■

例 6 设 $A=\{0,1\}$，考虑在连接运算下由 A 所产生的自由半群 A^*。注意 A^*是由空字符串Λ作为单位元的一个幺半群。设 $\mathbf{N}$ 是所有非负整数的集合，那么 $\mathbf{N}$ 是在普通加法运算下的一个半群，用$(\mathbf{N}, +)$表示。函数 $f: A^*\to\mathbf{N}$ 定义为

$$f(\alpha)=\alpha\text{ 中含 }1\text{ 的个数}$$

容易验证它是一个同态。设 R 是 A^*上由下面定义的关系：

$$\alpha\,R\,\beta\text{ 当且仅当 }f(\alpha)=f(\beta)$$

即$\alpha R\beta$当且仅当α和β有相同个数的1。定理4推出在下面定义的同构映射$\bar{f}$：$A^*/R\to\mathbf{N}$

$$\bar{f}([\alpha])=f(\alpha)=\alpha\text{中含1的个数}$$

中有$A^*/R\simeq\mathbf{N}$。■

定理4(b)可用图9.2给出的图解描述，其中f_R是自然同态。从f_R和$\bar{f}$的定义得到

$$\bar{f}\circ f_R=f$$

因为$(\bar{f}\circ f_R)(a)=\bar{f}(f_R(a))=\bar{f}([a])=f(a)$。

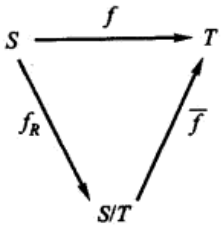


图 9.2

习 题 9.3

1. 设$(S,*)$和$(T,*')$是交换半群，证明：$S\times T$(见定理1)也是一个交换半群。
2. 设$(S,*)$和$(T,*')$是幺半群，证明：$S\times T$也是一个幺半群，$S\times T$的单位元是(e_S,e_T)。
3. 设$(S,*)$和$(T,*')$是半群，证明：由$f(s,t)=s$所定义的函数f：$S\times T\to S$是半群$S\times T$到半群S上的一个同态且是满射。
4. 设$(S,*)$和$(T,*')$是半群，证明：$S\times T$和$T\times S$是同构的半群。
5. 证明定理1。

在第6题~第16题中，确定半群S上的关系R是否是一个同余关系。

6. $S=\mathbf{Z}$，在普通的加法运算下，$a\,R\,b$当且仅当2不能整除$a-b$。
7. $S=\mathbf{Z}$，在普通的加法运算下，$a\,R\,b$当且仅当$a+b$是偶数。
8. S是任意半群，$a\,R\,b$当且仅当$a=b$。
9. S是所有有理数在加法运算下的集合，$a/b\,R\,c/d$，当且仅当$ad=bc$。
10. S是所有有理数在乘法运算下的集合，$a/b\,R\,c/d$当且仅当$ad=bc$。
11. $S=\mathbf{Z}$，在普通的加法运算下，$a\,R\,b$当且仅当$a\equiv b(\mathrm{mod}\ 3)$。
12. $S=\mathbf{Z}$，在普通的加法运算下，$a\,R\,b$当且仅当a和b都是偶数或者a和b都是奇数。
13. $S=\mathbf{Z}^+$，在普通的乘法运算下，$a\,R\,b$当且仅当$|a-b|\leqslant 2$。
14. $A=\{0,1\}$且$S=A^*$，即在连接运算下由A产生的自由半群，$\alpha\ R\ \beta$当且仅当α和β都有偶数个1或者都有奇数个1。
15. $S=\{0,1\}$，在由下表定义的运算$*$下，

*	0	1
0	0	1
1	1	0

$a\,R\,b$当且仅当$a*a=b*b$。(提示：注意如果x是S中任意一个元素，那么$x*x=0$。)

16. $S=\{3k+1,\ k\in\mathbf{Z}^+\}$，在普通的乘法运算下，$a\,R\,b$当且仅当$a\equiv b(\mathrm{mod}\ 5)$。
17. 描述第16题中所给的S和R的商半群。
18. 证明：半群上的两个同余关系的交是一个同余关系。
19. 证明：半群上的两个同余关系的合成不一定是一个同余关系。
20. 描述第10题中所给的S和R的商半群。

21. 描述第 11 题中所给的 S 和 R 的商半群。

22. 描述第 12 题中所给的 S 和 R 的商半群。

23. 设 $S=\mathbf{Z}$，具有普通的加法运算，R 定义为：$a\,R\,b$ 当且仅当 $a\equiv b(\mathrm{mod}\ 5)$，描述 S 和 R 的商半群。

24. 设半群 $S=\{a,b,c,d\}$，它有下面的运算表。

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

考虑 S 上的同余关系

$$R=\{(a,a),(a,b),(b,a),(b,b),(c,c),(c,d),(d,c),(d,d)\}$$

(a) 写出商半群 S/R 的运算表。

(b) 描述自然同态 f_R：$S\to S/R$。

25. 考虑有下面运算表的幺半群 $S=\{e,a,b,c\}$。

*	e	a	b	c
e	e	a	b	c
a	a	e	b	c
b	b	c	b	c
c	c	b	b	c

设 S 上的同余关系为

$$R=\{(e,e),(e,a),(a,e),(a,a),(b,b),(b,c),(c,b),(c,c)\}$$

(a) 写出商幺半群 S/R 的运算表。

(b) 描述自然同态 f_R：$S\to S/R$。

26. 设 $A=\{0,1\}$，考虑在连接运算下由 A 产生的自由半群 A^*，设 N 是在普通加法运算下的所有非负整数的半群。

(a) 验证：函数 f：$A^*\to N$ 是一个同态，f 定义为

$$f(\alpha)=\alpha \text{ 中数字的个数}$$

(b) 设 R 是 A^* 上的下述关系：$\alpha\,R\,\beta$ 当且仅当 $f(\alpha)=f(\beta)$，证明：R 是 A^* 上的一个同余关系。

(c) 证明：A^*/R 和 N 是同构的。

27. 证明或反证：Z_2 与第 22 题中的半群是同构的。

28. 证明或反证：Z_4 与第 24 题中的半群是同构的。

29. 描述定理 4 证明的策略，概述证明。

30. 设 S 是一个非空集合且有 $a*b=b$，证明：S 上的任意等价关系是一个同余关系。

9.4 群

本节将考查一类特殊的幺半群，它称为群，在每一个存在对称的领域中都有它的应用。关于群的应用可以在数学、物理、化学以及还不太明显的领域如社会学中找到。近来，令人激动

因为对于 G 中所有的 a 和 b 有 $a*b=b*a$，所以推出 G 是一个阿贝尔群。 ■

在列举另外一些群的例子之前，对于在任意群 G 中所满足的几条重要性质展开讨论。

定理 1 设 G 是一个群，则 G 中的每个元素 a 在 G 中仅有一个逆元。

证明 设 a' 和 a'' 都是 a 的逆，那么

$$a'(aa'')=a'e=a'$$
$$(a'a)a''=ea''=a''$$

因此，由结合性可知 $a'=a''$。 ■

从现在起，将用 a^{-1} 表示 a 的逆。因此，在群 G 中有 $aa^{-1}=a^{-1}a=e$。

定理 2 设 G 是一个群，a,b 和 c 是 G 的元素，那么

(a) $ab=ac$ 推出 $b=c$ (**左消去性质**)。

(b) $ba=ca$ 推出 $b=c$ (**右消去性质**)。

证明

(a) 假设 $ab=ac$，用 a^{-1} 左乘该方程的两边，得到

$$\begin{aligned} a^{-1}(ab)&=a^{-1}(ac) \\ (a^{-1}a)b&=(a^{-1}a)c && \text{由结合性} \\ eb&=ec && \text{由逆的定义} \\ b&=c && \text{由单位元的定义} \end{aligned}$$

(b) 证明类似于上述(a)。 ■

推论 1 设 G 是一个群且 $a\in G$。定义一个函数 $M_a:G\to G$ 满足公式：$M_a(g)=ag$，那么 M_a 是单射。

证明 它是定理 2 的一个直接结果。 ■

定理 3 设 G 是一个群，a 和 b 是 G 的元素，那么

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

证明 (a) 证明 a 是 a^{-1} 的逆：

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

因为一个元素的逆元是惟一的，所以得到 $(a^{-1})^{-1}=a$。

(b) 容易验证：

$$(ab)(b^{-1}a^{-1})=a(b(b^{-1}a^{-1}))=a((bb^{-1})a^{-1})=a(ea^{-1})=aa^{-1}=e$$

类似地，有

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

所以

$$(ab)^{-1}=b^{-1}a^{-1}$$ ■

定理 4 设 G 是一个群，a 和 b 是 G 的元素，那么

(a) 方程 $ax=b$ 在 G 中有惟一解。

(b) 方程 $ya=b$ 在 G 中有惟一解。

证明

(a) 因为 $a(a^{-1}b)=(aa^{-1})b=eb=b$，所以元素 $x=a^{-1}b$ 是方程 $ax=b$ 的一个解。现在假设 x_1 和 x_2 是方程 $ax=b$ 的两个解，那么

$$ax_1=b, \quad ax_2=b$$

因此

$$ax_1=ax_2$$

由定理 2 推出 $x_1=x_2$。

(b) 证明类似于上述(a)。 ■

从幺半群的讨论中可以知道，如果群 G 具有有限元素，那么它的二元运算可以通过某个表给出，通常称作**乘法表**。一个群 $G=\{a_1,a_2,\cdots,a_n\}$在二元运算$*$下的乘法表一定满足下面的性质：

1．用 e 标号的行一定是

$$a_1, a_2, \cdots, a_n$$

用 e 标号的列一定是

$$\begin{matrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{matrix}$$

2．由定理 4 可知群中的每个元素 b 一定在表的每行和每列中恰好出现一次。因此，每一行和列是 G 中元素 $a_1, a_2, \cdots, a_n$ 的排列，并且每行(每列)决定不同的排列。

如果 G 是具有有限元素的一个群，则称 G 是**有限群**，G 的**阶**是 G 中元素的个数$|G|$。下面将确定阶为 1、2、3 和 4 的所有非同构群的乘法表。

如果 G 是一个 1 阶群，那么 $G=\{e\}$并且有 $ee=e$。现在设 $G=\{e,a\}$是阶为 2 的一个群，那么得到一个需要填充空格的乘法表(表 9.1)。空格能够用 e 或 a 填充。因为在任意行或列中不能存在重复的元素，所以必须在空格里填 e。表 9.2 所给出的乘法表满足结合性质和群的其余性质，所以它是 2 阶群的乘法表。

表 9.1

	e	a
e	e	a
a	a	

表 9.2

	e	a
e	e	a
a	a	e

其次设 $G=\{e,a,b\}$是阶为 3 的群，有一个必须填充 4 个空格的乘法表(表 9.3)。少量试验表明只能完成表 9.4 给出的这种表。可以证明(冗长乏味的工作)表 9.4 满足结合性质和群的其余性质。因此，它是 3 阶群的乘法表。注意，阶为 1、2 和 3 的群也是阿贝尔群，并且对于元素的固定标号来说，每个阶刚好存在一个群。

现在讨论阶为 4 的群 $G=\{e, a, b, c\}$。不难证明 G 的可能的乘法表如表 9.5~表 9.8 所示。能

够证明这些表中每一个都满足结合性和群的其余性质。因此，对于阶为 4 的群存在 4 种可能的乘法表，而且注意阶为 4 的群是阿贝尔群。本节的末尾将再次讨论阶为 4 的群，在那里会看到只存在两个而不是 4 个不同的 4 阶非同构群。

表 9.3

	e	a	b
e	e	a	b
a	a		
b	b		

表 9.4

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

表 9.5

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

表 9.6

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

表 9.7

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

表 9.8

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

例 5 设 $B=\{0,1\}$，+是如下表定义在 B 上的运算。

+	0	1
0	0	1
1	1	0

那么 B 是一个群。在该群中每个元是它自身的逆。 ■

下面给出群的一个很重要的例子。

例 6 考虑图 9.3 给出的具有顶点 1、2 和 3 的等边三角形。三角形(或任意几何图形)的**对称性**是从形成三角形点的集合(几何图形)到其本身邻接点之间保持距离的一一对应。因为三角形是由顶点决定的，所以三角形的对称性只是邻接点之间保持距离的顶点置换。设 l_1，l_2 和 l_3 是图 9.3 所示的对应角的角平分线，O 是它们的交点。

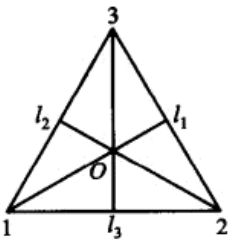


图 9.3

现在开始描述该三角形的对称性。首先，存在三角形关于 O 的 120° 逆时针旋转 f_2，那么 f_2 能够写成置换(见 5.3 节)

$$f_2=\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}$$

其次，获得关于 O 的 240°逆时针旋转 f_3，它能够写成置换

$$f_3=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$$

最后，存在关于 O 的 360° 逆时针旋转 f_1，它能够写成置换

$$f_1=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$$

当然，f_1 也能看成三角形关于 O 旋转 0°的结果。

还可以分别通过关于角平分线 l_1，l_2 和 l_3 的反射 g_1，g_2 和 g_3 获得三角形的另外三个对称性。把这些反射表示成下面的置换：

$$g_1=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix},\quad g_2=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix},\quad g_3=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$$

注意三角形的所有对称性的集合可以通过集合{1,2,3}的置换的集合来描述，它已在 5.3 节讨论过并且用 S_3 表示。因此

$$S_3=\{f_1, f_2, f_3, g_1, g_2, g_3\}$$

通过在集合 S_3 上引进运算*(*依次序定义*)可获得如表 9.9 所示的乘法表。

表 9.9

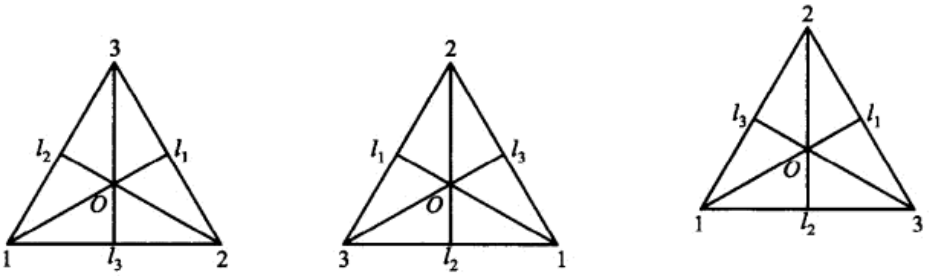
*	f_1	f_2	f_3	g_1	g_2	g_3
f_1	f_1	f_2	f_3	g_1	g_2	g_3
f_2	f_2	f_3	f_1	g_3	g_1	g_2
f_3	f_3	f_1	f_2	g_2	g_3	g_1
g_1	g_1	g_2	g_3	f_1	f_2	f_3
g_2	g_2	g_3	g_1	f_3	f_1	f_2
g_3	g_3	g_1	g_2	f_2	f_3	f_1

该表中的每个元可用代数或几何方法之一获得。例如，假设要用几何方法计算 f_2*g_2，可以像图 9.4 那样进行。注意上面提到的“依次序定义”是指几何次序。为了用代数方法计算 f_2*g_2，计算 $f_2\circ g_2$ 如下：

$$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\circ\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}=g_1$$

从而得到 $f_2*g_2=g_1$。

因为函数的合成是可结合运算，所以*是 S_3 上的结合运算。注意 f_1 是 S_3 中的单位元并且 S_3 中每个元在 S_3 中有惟一逆。例如，$f_2^{-1}=f_3$。因此，群 S_3 称为**三角形的对称群**。注意 S_3 是这里给出的群中不是阿贝尔群的第一个例子。 ■



已知三角形　　应用 f_2 后得到的三角形　　对左边的三角形应用 g_2 后得到的三角形

图 9.4

例 7　n 个元素的所有置换的集合在合成运算下是一个阶为 $n!$的群，称这个群为 ***n* 个字母上的对称群**，用 S_n 表示。已经看到，S_3 还表示等边三角形的对称群。 ■

同例 6 一样，同样可以考虑一个正方形的对称群。然而，得出这个群的阶为 8，所以它与群 S_4 不一样，S_4 的阶是 4!=24。

例 8　在 9.3 节讨论过幺半群 Z_n，现在证明 Z_n 是如下的一个群。设$[a]\in Z_n$，那么可以假设 $0\leqslant a<n$，而且$[n-a]\in Z_n$。因为

$$[a]\oplus[n-a]=[a+n-a]=[n]=[0]$$

所以推出$[n-a]$是$[a]$的逆。因此，如果 n 是 6，那么[2]是[4]的逆。注意 Z_n 是一个阿贝尔群。 ■

下面主要讨论群的重要子集。设 H 是群 G 的一个子集，使得

(a) G 的单位元 e 属于 H。

(b) 如果 a 和 b 属于 H，那么 $ab\in H$。

(c) 如果 $a\in H$，那么 $a^{-1}\in H$。

则称 H 为 G 的一个**子群**。(a)和(b) 说明 H 是 G 的子幺半群。因此 G 的子群可看成是具有性质 (a) 和(c) 的一个子幺半群。

注意，如果 G 是一个群，H 是 G 的一个子群，那么 H 也是关于 G 中运算的一个群，因为 G 中的结合性质在 H 中也成立。

例 9　设 G 是一个群，那么 G 和 $H=\{e\}$是 G 的子群，称它们为 G 的**平凡子群**。 ■

例 10　考虑等边三角形的对称群 S_3，它的乘法表如表 9.9 所示。容易证明 $H=\{f_1, f_2, f_3\}$是 S_3 的一个子群。 ■

例 11　设 A_n 是群 S_n 中所有偶置换的集合(见 5.4 节)，从偶置换的定义能够证明 A_n 是 S_n 的一个子群，称它为 ***n* 个字母的交错群**。 ■

例 12　设 G 是一个群，$a\in G$，因为群是一个幺半群，在 9.2 节对 $n\in\mathbf{Z}^+$，a_n 定义为 $aa\cdots a$ (n 个因子)，a^0 定义为 e。如果 n 是一个负整数，那么定义 a^{-n} 为 $a^{-1}a^{-1}\cdots a^{-1}$($n$ 个因子)。于是，如果 n 和 m 是任意整数，那么有 $a^n a^m=a^{n+m}$。容易证明

$$H=\{a^i|i\in\mathbf{Z}\}$$

是 G 的一个子群。 ■

设$(G,*)$和$(G',*')$是两个群，因为群也是半群，所以可考虑从$(G,*)$到$(G',*')$的同构和同态。

因为一个同构必须是单射和满射的函数，所以，阶不相等的两个群不可能是同构的。

例 13 设 G 是在加法运算下的实数群，G'是在乘法运算下的正实数群，$f:G\to G'$由 $f(x)=e^x$ 定义，现在证明 f 是一个同构。

如果 $f(a)=f(b)$，那么 $e^a=e^b$，于是 $a=b$。因此，f 是单射。如果 $c\in G'$，那么 $\ln c\in G$，$f(\ln c)=e^{\ln c}=c$，所以 f 是满射。最后

$$f(a+b)=e^{a+b}=e^a e^b=f(a)\,f(b)$$

因此 f 是一个同构。 ■

例 14 设 G 是 n 个字母的对称群，G'是例 5 中定义的群 B，$f:G\to G'$定义如下：对于 $p\in G$，有

$$f(p)=\begin{cases}0, & p\in A_n(G\text{ 中所有偶置换的子群})\\ 1, & p\notin A_n\end{cases}$$

那么 f 是一个同态。 ■

例 15 设 G 是在加法运算下的整数群，G'是例 8 中讨论的群 Z_n，f：$G\to G'$定义如下：如果 $m\in G$，那么 $f(m)=[r]$，其中 r 是当 m 被 n 除时的余数。下面证明 f 是 G 到 G'的一个同态且是满射。

设$[r]\in Z_n$，那么可以假设 $0\leqslant r<n$，所以

$$r=0\cdot n+r$$

这意味着当 r 用 n 除时余数是 r。因此，$f(r)=[r]$，从而 f 是满射。

其次，设 a 和 b 是 G 的元素，它们可表示为

$$a=q_1n+r_1,\quad 0\leqslant r_1<n,\ r_1\text{ 和 }q_1\text{ 是整数} \tag{1}$$

$$b=q_2n+r_2,\quad 0\leqslant r_2<n,\ r_2\text{ 和 }q_2\text{ 是整数} \tag{2}$$

并且使得 $f(a)=[r_1]$，$f(b)=[r_2]$，那么

$$f(a)+f(b)=[r_1]+[r_2]=[r_1+r_2]$$

为了找出$[r_1+r_2]$，需要当 r_1+r_2 用 n 除时的余数。记

$$r_1+r_2=q_3n+r_3,\quad 0\leqslant r_3<n,\ r_3\text{ 和 }q_3\text{ 是整数}$$

因此

$$f(a)+f(b)=[r_3]$$

此外，有

$$a+b=q_1n+q_2n+r_1+r_2=(q_1+q_2+q_3)n+r_3$$

所以

$$f(a+b)=[r_1+r_2]=[r_3]$$

因此

$$f(a+b)=f(a)+f(b)$$

这就推出 f 是一个同态。

当 n 是 2 时，f 指定每个偶数为[0]且每个奇数为[1]。 ■

定理 5 设$(G,*)$和$(G',*')$是两个群，f：$G\to G'$是从 G 到 G'的一个同态。

(a) 如果 e 是 G 的单位元，e'是 G'的单位元，那么 $f(e)=e'$。

(b) 如果 $a\in G$，那么 $f(a^{-1})=(f(a))^{-1}$。

(c) 如果 H 是 G 的一个子群，那么

$$f(H)=\{f(h)|h\in H\}$$

是 G'的一个子群。

证明 (a) 设 $x=f(e)$，那么

$$x*'x=f(e)*'f(e)=f(e*e)=f(e)=x$$

所以 $x*'x=x$。用 x^{-1} 右乘等式两边，得到

$$x=x*'x*'x^{-1}=x*'x^{-1}=e'$$

因此 $f(e)=e'$。

(b) 因为 $a*a^{-1}=e$，所以 $f(a*a^{-1})=f(e)=e'$(由(a))或者因为 f 是一个同态，所以 $f(a)*'f(a^{-1})=e'$。类似地，$f(a^{-1})*'f(a)=e'$。因此，$f(a^{-1})=(f(a))^{-1}$。

(c) 从 9.2 节的定理 4、上述(a)和(b)得到结论。 ■

例 16 群 S_3 和 Z_6 都是 6 阶群，然而 S_3 不是阿贝尔群而 Z_6 是阿贝尔群。因此，它们不是同构的。记住同构保持由群运算所定义的所有性质。 ■

例 17 在本节的开始对 4 阶群求出了 4 种可能的乘法表(表 9.5~表 9.8)，现在证明乘法表为表 9.6、表 9.7 和表 9.8 的群是如下同构的。设 $G=\{e,a,b,c\}$是乘法表为表 9.6 的群，$G'=\{e',a',b',c'\}$是乘法表为表 9.7 的群，其中在表 9.7 的每个元上放上符号“′”。设 f：$G\to G'$定义为 $f(e)=e'$，$f(a)=b'$，$f(b)=a'$，$f(c)=c'$，那么可以验证在这些元素重新命名的意义下，两个表变得完全相同，所以对应的群是同构的。类似地，设 $G''=\{e'',a'',b'',c''\}$是乘法表为表 9.8 的群，其中在表 9.8 的每个元上放上符号“″”。设 g：$G\to G''$是由 $g(e)=e''$，$g(a)=c''$，$g(b)=b''$，$g(c)=a''$定义的，那么可以验证在这些元素重新命名的意义下，两个表变成完全一致，所以对应的群是同构的，即由表 9.6、表 9.7 和表 9.8 给出的群是同构的。

现在怎样才能确定表 9.5 和表 9.6 不生成同构的群呢？注意，如果 x 是由表 9.5 确定的群中的任意元素，那么 $x^2=e$。如果群是同构的，那么由表 9.6 确定的群有相同性质。然而事实并非如此，所以推得这两个群不是同构的。因此，确实存在两个阶为 4 的非同构群。

由乘法表 9.5 给出的群称为 **Klein 四元群**，用 V 表示。由乘法表 9.6、表 9.7 和表 9.8 给出的群用 Z_4 表示，因为 Z_4 的元素重新标号后可得到这些乘法表。 ■

习 题 9.4

在第 1 题~第 11 题中，确定集合辅以二元运算是否是一个群。如果它是一个群，确定它是否是阿贝尔群，指出单位元和元素 a 的逆。

1. $\mathbf{Z}$，$*$是普通乘法。
2. $\mathbf{Z}$，$*$是普通减法。
3. 所有有理数的集合 $\mathbf{Q}$ 在加法运算下。
4. 所有有理数的集合 $\mathbf{Q}$ 在乘法运算下。
5. $\mathbf{R}$，在乘法运算下。
6. $\mathbf{R}$，$a*b=a+b+2$。
7. $\mathbf{Z}^+$，在加法运算下。
8. 不等于–1 的实数，满足 $a*b=a+b+ab$。
9. 奇数集合在乘法运算下。
10. 所有 $m\times n$ 矩阵的集合在矩阵加法运算下。
11. 如果 S 是一个非空集合，集合 $P(S)$，$A*B=A\oplus B$(见 1.2 节)。
12. 设 $S=\{x\mid x$ 是一个实数且 $x\neq 0$，$x\neq -1\}$，考虑下列函数 f_i：$S\to S(i=1,2,\cdots,6)$：

$$f_1(x)=x,\quad f_2(x)=1-x,\quad f_3(x)=\frac{1}{x},\quad f_4(x)=\frac{1}{1-x},\quad f_5(x)=1-\frac{1}{x},\quad f_6(x)=\frac{x}{x-1}$$

证明：$G=\{f_1,f_2,f_3,f_4,f_5,f_6\}$是在合成运算下的一个群。给出 G 的乘法表。

13. 考虑等边三角形的对称群 S_3 和第 12 题中的群，证明或反证：这两个群是同构的。
14. 证明：例 14 中的映射是一个同态。
15. 设 G 是例 4 中所定义的群，求解下列方程：

(a) $3*x=4$　　(b) $y*5=-2$

16. 设 $i=\sqrt{-1}$，证明：$S=\{1,-1,i,-i\}$ 在复数乘法的运算下是一个群。该群是阿贝尔群吗？
17. 求第 16 题中群的所有子群。
18. 设 G 是有单位元 e 的一个群，证明：如果对 G 中所有的 a 有 $a^2=e$，那么 G 是阿尔贝群。
19. 考虑图 9.5 所示的正方形，此正方形的对称性是分别通过旋转 0°，90°，180°和 270°的 f_1，f_2，f_3 和 f_4 得到的，f_5 和 f_6 分别是关于线段 v 和 h 的反射，f_7 和 f_8 分别是关于对角线 d_1 和 d_2 的反射。写出正方形对称群 D_4 的乘法表。

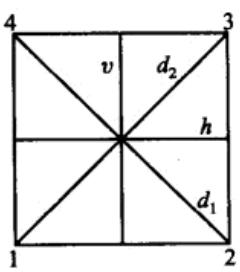


图 9.5

20. 设 G 是一个群，证明：如果 $g\in G$ 有性质 $gg=g$，那么 g 是 G 的单位元。
21. 设 G 是有单位元 e 的一个有限群，a 是 G 的任意一个元素，证明：存在非负整数 n，使得 $a^n=e$。
22. 设 G 是在乘法运算下的非零整数群，$H=\{3^n\mid n\in\mathbf{Z}\}$。问 H 是 G 的一个子群吗？
23. 设 G 是在加法运算下的整数群，$H=\{3k\mid k\in\mathbf{Z}\}$。问 H 是 G 的一个子群吗？
24. 设 G 是具有单位元 e 的阿贝尔群，$H=\{x\mid x^2=e\}$。证明：H 是 G 的一个子群。
25. 设 G 是一个群，$H=\{x\mid x\in G$，对所有 $y\in G$，$xy=yx\}$。证明：H 是 G 的一个子群。
26. 设 G 是一个群，$a\in G$，定义 $H_a=\{x\mid x\in G$，$xa=ax\}$。证明：H_a 是 G 的一个子群。
27. 设 A_n 是 S_n 中所有偶置换的集合，证明：A_n 是 S_n 的一个子群。
28. 设 H 和 K 是群 G 的一个子群。

(a) 证明：$H\cap K$ 是 G 的一个子群。

(b) 证明：$H\cup K$ 不一定是 G 的一个子群。

29. 求出第 19 题中群的所有子群。

30. 设 G 是一个阿贝尔群，n 是固定的整数。证明：对于 $a\in G$，由 $f(a)=a^n$ 定义的函数 f：$G\to G$ 是一个同态。

31. 证明：函数 $f(x)=|x|$ 是从非零实数群 G 到正实数群 G' 的一个同态，其中群 G 和 G' 中的运算是乘法。

32. 设 G 是具有单位元 e 的一个群。证明：对所有 $a\in G$，由 $f(a)=e$ 定义的函数 f：$G\to G$ 是一个同态。

33. 设 G 是一个群。证明：由 $f(a)=a^2$ 定义的函数 f：$G\to G$ 是一个同态当且仅当 G 是阿贝尔群。

34. 设 G 是一个群。证明：由 $f(a)=a^{-1}$ 定义的函数 f：$G\to G$ 是一个同构当且仅当 G 是阿贝尔群。

35. 设 G 是一个群，a 是 G 中的一个固定元素。证明：对于 $x\in G$，由 $f_a(x)=axa^{-1}$ 定义的函数 f_a：$G\to G$ 是一个同构。

36. 设 $G=\{e,a,a^2,a^3,a^4,a^5\}$ 是在运算 $a^ia^j=a^r$，$i+j\equiv r(\bmod 6)$ 下的一个群，证明：G 和 Z_6 是同构的。

37. 设 G 是一个群，用数学归纳法证明：如果 $ab=ba$，那么对于 $n\in\mathbf{Z}^+$，$(ab)^n=a^nb^n$。

38. 证明：在一个群的乘法表中，每个元素在每行和每列恰好只出现一次。

39. 证明：第 38 题中的条件是必要的，但对于这样的群的乘法表而言，条件不是充分的。

9.5 群的积与商

在这一节，将通过使用积和商的概念从已知的群得到新的群。因为群比半群有更多的结构，所以本节结果比 9.3 节讨论的半群中的类似结果更深刻。

定理 1 如果 G_1 和 G_2 是群，那么 $G=G_1\times G_2$ 是二元运算由 $(a_1,b_1)(a_2,b_2)=(a_1a_2,b_1b_2)$ (式(1)) 定义的群。

证明 由 9.3 节的定理 1 可知 G 是一个半群，单位元和逆元的存在性很容易通过验证得到。■

例 1 设 G_1 和 G_2 是群 Z_2，为简化记号，将 Z_2 中的元素分别写成 $\bar{0}$ 和 $\bar{1}$ 而不是[0]和[1]。那么 $G=G_1\times G_2$ 的乘法表由表 9.10 给出。

因为 G 是一个 4 阶群，所以它一定同构于 V 或 Z_4(见 9.4 节)，即仅有的 4 阶群。通过查看乘法表可知由 $f(e)=(\bar{0},\bar{0})$，$f(a)=(\bar{1},\bar{0})$，$f(b)=(\bar{0},\bar{1})$，$f(c)=(\bar{1},\bar{1})$ 所定义的函数 f：$V\to Z_2\times Z_2$ 是一个同构。■

表 9.10 $Z_2\times Z_2$ 的乘法表

	$(\bar{0},\bar{0})$	$(\bar{1},\bar{0})$	$(\bar{0},\bar{1})$	$(\bar{1},\bar{1})$
$(\bar{0},\bar{0})$	$(\bar{0},\bar{0})$	$(\bar{1},\bar{0})$	$(\bar{0},\bar{1})$	$(\bar{1},\bar{1})$
$(\bar{1},\bar{0})$	$(\bar{1},\bar{0})$	$(\bar{0},\bar{0})$	$(\bar{1},\bar{1})$	$(\bar{0},\bar{1})$
$(\bar{0},\bar{1})$	$(\bar{0},\bar{1})$	$(\bar{1},\bar{1})$	$(\bar{0},\bar{0})$	$(\bar{1},\bar{0})$
$(\bar{1},\bar{1})$	$(\bar{1},\bar{1})$	$(\bar{0},\bar{1})$	$(\bar{1},\bar{0})$	$(\bar{0},\bar{0})$

如果用 Z_2 和 Z_3 重复例 1，可得到 $Z_2\times Z_3\simeq Z_6$。一般地，可以证明 $Z_m\times Z_n\simeq Z_{mn}$ 当且仅当

GCD$(m, n)=1$，即：当且仅当 m 和 n 互素。

显然，定理 1 可推广为：如果 $G_1,G_2,\cdots,G_n$ 是群，那么 $G=G_1\times G_2\times\cdots\times G_n$ 也是一个群。

例 2 设 $B=\{0,1\}$ 是 9.4 节例 5 中定义的群，这里的+定义如下：

+	0	1
0	0	1
1	1	0

那么 $B^n=B\times B\times\cdots\times B$($n$ 个因子)是一个群，它的运算 $\oplus$ 定义为

$$(x_1, x_2, \cdots, x_n)\oplus(y_1, y_2, \cdots, y_n)=(x_1+y_1, x_2+y_2, \cdots, x_n+y_n)$$

B^n 的单位元是$(0,0,\cdots,0)$并且每一个元素是它自身的逆。该群基本上同 6.4 节定义的布尔代数 B_n 相同，但是二元运算同$\wedge$和$\vee$是完全不同的。 ■

在一个群上的同余关系就是当该群被看成半群时的一个同余关系。下面讨论由群上的同余关系所决定的商结构。

定理 2 设 R 是群$(G,*)$上的一个同余关系，那么半群$(G/R, \circledast)$是一个群，其中运算$\circledast$定义在 G/R 上且满足$[a]\circledast[b]=[a*b]$(见 9.3 节)(式(2))。

证明 因为群是幺半群，从 9.3 节的推论 1 可知 G/R 是一个幺半群，需要证明 G/R 的每个元素有一个逆。设$[a]\in G/R$，那么$[a^{-1}]\in G/R$，$[a]\circledast[a^{-1}]=[a*a^{-1}]=[e]$，所以$[a]^{-1}=[a^{-1}]$。因此，$(G/R,\circledast)$是一个群。 ■

因为群的同态、同构以及同余的定义仅仅包含群的半群和幺半群的结构，所以下面的推论是 9.3 节定理 3 和定理 4 的直接结果。

推论 1 (a) 如果 R 是群 G 上的一个同余关系，那么由 $f_R(a)=[a]$给出的函数 f_R：$G\to G/R$ 是群的同态。

(b) 如果 f：$G\to G'$是从群$(G,*)$到群$(G',*')$上的一个同态且是满射，R 是定义在 G 上的关系，满足 $a\,R\,b$ 当且仅当对 G 中的 a 和 b 有 $f(a)=f(b)$，那么

1．R 是一个同余关系。

2．由 $\overline{f}([a])=f(a)$ 给出的函数 $\overline{f}$：$G/R\to G'$是从群$(G/R,\circledast)$到群$(G',*')$的一个同构且是满射。 ■

群上的同余关系有非常特殊的形式，下面进一步讨论。设 H 是群 G 的一个子群，$a\in G$，由 a 决定的 G 中 H 的**左陪集**是集合 $aH=\{ah|h\in H\}$，由 a 决定的 G 中 H 的**右陪集**是集合 $Ha=\{ha|h\in H\}$。最后，如果对 G 中所有的 a 有 $aH=Ha$，则称 G 的子群 H 是**正规子群**。

警告 如果 $Ha=aH$，由此并*不能*得到：对于 $h\in H$ 和 $a\in G$，有 $ha=ah$，而只能得到 $ha=ah'$，其中 h'是 H 中的某个元素。

如果 H 是 G 的一个子群，那么需要在某些应用里计算 G 中 H 的所有左陪集。首先，假设 $a\in H$，因为 H 是 G 的一个子群，所以 $aH\subseteq H$，而且如果 $h\in H$，那么 $h=ah'$，其中 $h'=a^{-1}h\in H$，所以 $H\subseteq aH$。因此，如果 $a\in H$，那么 $aH=H$，也就是说，当寻找 H 的所有陪集时，对于 $a\in H$，

则不需要计算 aH，因为它总是 H。

例 3 设 G 是 9.4 节例 6 中讨论的对称群 S_3，子集 $H=\{f_1, g_2\}$ 是 G 的一个子群，计算 G 中 H 的所有不同的左陪集。

解 如果 $a\in H$，那么 $aH=H$。因此

$$f_1H=g_2H=H$$

同样

$$f_2H=\{f_2, g_1\},\ f_3H=\{f_3, g_3\},\ g_1H=\{g_1, f_2\}=f_2H,\ g_3H=\{g_3, f_3\}=f_3H$$

G 中 H 的不同左陪集是 H，f_2H 和 f_3H。 ■

例 4 设 G 和 H 是例 3 中给出的，那么右陪集 $Hf_2=\{f_2, g_3\}$。在例 3 中看到 $f_2H=\{f_2, g_1\}$，从而得到 H 不是 G 的一个正规子群。 ■

例 5 说明如果 G 是一个阿贝尔群，那么 G 的每个子群都是一个正规子群。

解 设 H 是 G 的一个子群，$a\in G$ 且 $h\in H$，那么 $ha=ah$，所以 $Ha=aH$，这就推出 H 是 G 的一个正规子群。 ■

定理 3 设 R 是群 G 上的一个同余关系，$H=[e]$，即包含单位元的等价类，那么 H 是 G 的一个正规子群，并且对每个 $a\in G$，$[a]=aH=Ha$。

证明 设 a 和 b 是 G 中任意元素，因为 R 是一个等价关系，$b\in[a]$当且仅当$[b]=[a]$。此外，由定理 2 可知 G/R 是一个群，所以$[b]=[a]$当且仅当$[e]=[a]^{-1}[b]=[a^{-1}b]$。因此，$b\in[a]$当且仅当 $H=[e]=[a^{-1}b]$，即 $b\in[a]$当且仅当 $a^{-1}b\in H$ 或 $b\in aH$，这就证明了对每个 $a\in G$，$[a]=aH$。类似地，可证明 $b\in[a]$当且仅当 $H=[e]=[b][a]^{-1}=[ba^{-1}]$，这等价于语句$[a]=Ha$。因此，$[a]=aH=Ha$，故 H 是正规子群。 ■

结合定理 3 与推论 1 可以看到在这种情况下商群 G/R 是由 $N=[e]$的所有左陪集所组成的，G/R 中的运算由

$$(aN)(bN)=[a]\circledast[b]=[ab]=abN$$

给出，并且由 $f_R(a)=aN$ 所定义的函数 f_R：$G\to G/R$ 是从 G 到 G/R 的一个同态且是满射。正因如此，常把 G/R 写成 G/N。

下面考虑这样一个问题，对于某个同余关系，群 G 中的每个正规子群是否是 G 的单位元的等价类。

定理 4 设 N 是群 G 的一个正规子群，R 是 G 上的下述关系：$a\ R\ b$ 当且仅当 $a^{-1}b\in N$。那么

(a) R 是 G 上的同余关系。

(b) N 是关于 R 的等价类$[e]$，其中 e 是 G 的单位元。

证明 (a) 设 $a\in G$，因为 $a^{-1}a=e\in N$，所以 $a\,R\,a$，从而 R 是自反的。其次，假设 $a\,R\,b$ 使得 $a^{-1}b\in N$，那么$(a^{-1}b)^{-1}=b^{-1}a\in N$，所以 $b\,R\,a$，因此 R 是对称的。最后，假设 $a\,R\,b$ 和 $b\,R\,c$，那么 $a^{-1}b\in N$ 和 $b^{-1}c\in N$，于是$(a^{-1}b)(b^{-1}c)=a^{-1}c\in N$，所以 $a\,R\,c$，因此 R 是传递的。从而得到 R 是 G 上的一个等价关系。

下面证明 R 是 G 上的一个同余关系。假设 $a\,R\,b$ 和 $c\,R\,d$，那么 $a^{-1}b\in N$ 和 $c^{-1}d\in N$。因为 N 是正规子群，所以 $Nd=dN$，即对任意 $n_1\in N$，存在某个 $n_2\in N$，使得 $n_1d=dn_2$。特别地，因为 $a^{-1}b\in N$，所以对某个 $n_2\in N$，有 $a^{-1}bd=dn_2$，于是

$$(ac)^{-1}bd=(c^{-1}a^{-1})(bd)=c^{-1}(a^{-1}b)d=(c^{-1}d)n_2\in N$$

从而 $ac\,R\,bd$，因此 R 是 G 上的一个同余关系。

(b) 假设 $x\in N$，那么因为 N 是一个子群，从而 $x^{-1}e=x^{-1}\in N$，所以 $x\ R\ e$，即 $x\in[e]$，因此 $N\subseteq[e]$。反之，如果 $x\in[e]$，那么 $x\,R\,e$，所以 $x^{-1}e=x^{-1}\in N$，于是 $x\in N$ 和 $[e]\subseteq N$，因此 $N=[e]$。 ■

从定理 3 和定理 4 可以看到，如果 G 是任意一个群，那么 G 上的同余关系的等价类总是 G 的某个正规子群的陪集。反之，G 的任意一个正规子群的陪集恰好是关于 G 上某个同余关系的等价类。所以，现在可以把推论 1(b)做如下解释：设 f 是从群$(G,*)$到群$(G',*')$上的同态并且是满射，f 的**核**记做 $\ker(f)$，定义为

$$\ker(f)=\{a\in G\mid f(a)=e'\}$$

那么

(a) $\ker(f)$是 G 的一个正规子群。

(b) 商群 $G/\ker(f)$与 G'是同构的。

从推论 1 和定理 3 很容易证明上述结论，因为如果 R 是 G 上的同余关系并且已知

$$a\,R\,b \quad \text{当且仅当 } f(a)=f(b)$$

那么易证 $\ker(f)=[e]$。

例 6 考虑从 $\mathbf{Z}$ 到 Z_n 上由 $f(m)=[r]$所定义的一个同态和满射 f，其中 r 是当 m 用 n 除时的余数(见 9.4 节的例 15)。求 $\ker(f)$。

解 $\mathbf{Z}$ 中的整数 m 属于 $\ker(f)$当且仅当 $f(m)=[0]$，即当且仅当 m 是 n 的倍数。因此 $\ker(f)=n\mathbf{Z}$。 ■

习 题 9.5

1. 写出群 $Z_2\times Z_3$ 的乘法表。
2. 证明：如果 G 和 G'是阿贝尔群，那么 $G\times G'$是一个阿贝尔群。
3. 设 G_1 和 G_2 是群，证明：$G_1\times G_2$ 和 $G_2\times G_1$ 是同构的。
4. 设 G_1 和 G_2 是群，证明：函数 f：$G_1\times G_2\to G_1$ 是一个同态，其中 f 定义为对 $a\in G_1$ 和 $b\in G_2$，有 $f(a,b)=a$。
5. 确定商群 $\mathbf{Z}/3\mathbf{Z}$ 的乘法表，其中 $\mathbf{Z}$ 有运算+。
6. 设 $\mathbf{Z}$ 是在加法运算下的整数群。证明：由 $f(a,b)=a+b$ 定义的函数 f：$\mathbf{Z}\times\mathbf{Z}\to\mathbf{Z}$ 是一个同态。
7. 已知第 4 题中的函数 f，求 $\ker(f)$是什么?
8. 已知第 6 题中的函数 f，求 $\ker(f)$是什么?
9. 设 $G=Z_4$，求 G 中 $H=\{[0]\}$的所有左陪集。
10. 设 $G=Z_4$，求 G 中 $H=\{[0],[2]\}$的所有左陪集。

11. 设 $G=Z_4$，求 G 中 $H=\{[0],[1],[2],[3]\}$ 的所有左陪集。

12. 设 $S=\{1,-1,i,-i\}, i=\sqrt{-1}$，$G=(S,$ 复数乘法)。

(a) 证明：$H=\{1,-1\}$ 是 G 的一个子群。

(b) 确定 H 的所有左陪集。

13. 证明或反证：第 12 题中的 G 与 Z_4 是同构的。

14. 设 $G=S_3$，求 G 中 $H=\{f_1,g_1\}$ 的所有左陪集。

15. 设 $G=S_3$，求 G 中 $H=\{f_1,g_3\}$ 的所有左陪集。

16. 设 $G=S_3$，求 G 中 $H=\{f_1,f_2,f_3\}$ 的所有左陪集。

17. 设 $G=S_3$，求 G 中 $H=\{f_1\}$ 的所有左陪集。

18. 设 $G=S_3$，求 G 中 $H=\{f_1, f_2, f_3, g_1, g_2, g_3\}$ 的所有左陪集。

19. 设 $G=Z_8$，求 G 中 $H=\{[0],[4]\}$ 的所有左陪集。

20. 设 $G=Z_8$，求 G 中 $H=\{[0],[2],[4],[6]\}$ 的所有左陪集。

21. 设 $\mathbf{Z}$ 是在加法运算下的整数群，$G=\mathbf{Z}\times\mathbf{Z}$，考虑 G 的子群 $H=\{(x,y)|x=y\}$，描述 G 中 H 的左陪集。

22. 设 N 是群 G 的一个子群，$a\in G$，定义

$$a^{-1}Na=\{a^{-1}na|n\in N\}$$

证明：N 是 G 的一个正规子群当且仅当对所有 $a\in G$，$a^{-1}Na=N$。

23. 设 N 是群 G 的一个子群，证明：N 是 G 的一个正规子群当且仅当对所有 $a\in G$，$a^{-1}Na\subseteq N$。

24. 求 S_3 的所有正规子群。

25. 求 D_4(见 9.4 节的第 19 题)的所有正规子群。

26. 设 G 是一个群，$H=\{x|x\in G,$ 对所有 $a\in G,$ $xa=ax\}$。证明：H 是 G 的一个正规子群。

27. 设 H 是群 G 的一个子群，证明：H 的每个左陪集 aH 和 H 有相同数目的元素，即证明由 $f_a(h)=ah$，$h\in H$ 定义的函数 f_a：$H\to aH$ 是单射和满射。

28. 设 H 和 K 是 G 的正规子群，证明：$H\cap K$ 是 G 的一个正规子群。

29. 设 G 是一个群，H 是 G 的一个子群，S 是 G 中 H 的所有左陪集集合，T 是 G 中 H 的所有右陪集集合。证明：由 $f(aH)=Ha^{-1}$ 定义的函数 f：$S\to T$ 是单射和满射。

30. 设 G_1 和 G_2 是群，f：$G_1\times G_2\to G_2$ 是从 $G_1\times G_2$ 到 G_2 上的一个同态且是满射，其中 $f((g_1,g_2))=g_2$。计算 $\ker(f)$。

31. 设 f 是从群 G_1 到群 G_2 上的一个同态，且是满射，假设 G_2 是阿贝尔群，证明：$\ker(f)$包含了所有形如 $aba^{-1}b^{-1}$ 的 G_1 的元素，其中 a 和 b 是 G_1 中的任意元素。

32. 设 G 是一个阿贝尔群，N 是 G 的一个子群，证明：G/N 是一个阿贝尔群。

33. 设 H 是有限群 G 的一个子群，假设在 G 中只存在 H 的两个左陪集，证明：H 是 G 的一个正规子群。

34. 设 H 和 N 是群 G 的子群。证明：如果 N 是 G 的一个正规子群,那么 $H\cap N$ 是 H 的一个正规子群。

35. 设 f：$G\to G'$ 是群的同态。证明：f 是单射当且仅当 $\ker(f)=\{e\}$。

36. 设 $S=\{1,3,7,9\}$,$G=(S,$ 乘法 mod 10)。

(a) 证明：G 是一个群。

(b) 确定子群$\{1,9\}$的所有左陪集。

37. 设 G 是一个有限群，H 是 G 的一个子群。证明：H 的所有不同左陪集的集合是 G 的一个划分。

38. 使用题 27 和 37 的结果，描述 H 的阶和 G 的阶之间的关系。

9.6 其他数学结构

环

在以前的章节中，已看到过很多情况，在一个集合 S 上定义了两种二元运算。现在将更详细地学习这种结构。特别地，令 S 是一个非空集合，在它上面定义了两种二元运算＋和*使得(S，＋)是一个阿贝尔群，而*对于＋满足分配律。(这两种运算符号与人们最熟悉的实数运算结构相同。)如果*满足结合律，那么结构(S，＋，*)称作一个**环**。如果*同时满足结合律和交换律，则称(S，＋，*)为**交换环**。如果(S，*)是一个幺半群，则称(S，＋，*)为**含幺环**。*的单位元通常用 1 表示，＋的单位元通常用 0 表示。

例 1 令 S=**Z**，**Z** 是整数集合，令＋和*为普通的整数加法和乘法，则(S，＋，*)为可交换的含幺环。 ■

例 2 设 S 是所有 2×2 矩阵的集合，令＋和*是 1.5 节中定义的矩阵的加法和乘法运算。根据 1.5 节所证明的定理可知(S，＋，*)是一个非交换环。令 $\boldsymbol{I}=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$，则 $\boldsymbol{I}$ 是矩阵乘法运算的一个单位元，即对 S 中的所有元素 $\boldsymbol{A}$ 有 $\boldsymbol{AI}=\boldsymbol{IA}=\boldsymbol{A}$。因此，($S$，＋，*)是一个不可交换的含幺环。 ■

前面提到过，如果 a，b 和 n 是整数且 $n>1$，$a-b$ 是 n 的倍数，或者说 a 和 b 除 n 的余数相同，则称 a 和 b 关于模 n 同余，记为 $a\equiv b(\mathrm{mod}\ n)$。9.4 节中已经证明关于模 n 的同余在整数上是一个等价关系，由所有这样的等价类所构成的集合 Z_n 是关于加法模 n 的一个阿贝尔群。如果整数 a 的等价类表示为表达式 $\overline{a}$，则 $Z_n=\{\overline{0},\ \overline{1},\ \overline{2},\ \cdots,\ \overline{n-1}\}$，并满足 $\overline{a}+\overline{b}=\overline{a+b}$。

现在在 Z_n 上定义乘法。假设 a，b，x 和 y 都是整数，$a\equiv x(\mathrm{mod}\ n)$，$b\equiv y(\mathrm{mod}\ n)$，这些假设推出对于某个整数 s 和 t 有 $a=x+sn, b=y+tn$。于是 $ab=xy+xtn+ysn+stn^2$，这就推出 $ab-xy=n(xt+ys+stn)$，所以 $ab\equiv xy(\mathrm{mod}\ n)$。故可以定义 $\overline{a}*\overline{b}$ 为 $\overline{ab}$。该定义并不依赖于表示每个等价类所选取的整数。

例 3 集合 Z_n 上定义了关于模 n 的加法和上面定义的乘法，它是一个可交换含幺环。由于

$$(\overline{a}*\overline{b})*\overline{c}=\overline{ab}*\overline{c}=\overline{(ab)c}=\overline{a(bc)}=\overline{a}*\overline{bc}=\overline{a}*(\overline{b}*\overline{c})$$

且

$$\overline{a}*(\overline{b}+\overline{c})=\overline{a}*\overline{(b+c)}=\overline{a(b+c)}=\overline{ab+ac}=\overline{ab}+\overline{ac}=(\overline{a}*\overline{b})+(\overline{a}*\overline{c})$$

表明乘法满足结合律且乘法对于加法满足分配律。同样可以证明乘法满足结合律，乘法的单位元为 $\overline{1}$。 ■

一般地，把＋和*看成加法和乘法，甚至它们不是通常意义下的加法和乘法运算时也如此认为。

整数环的许多性质对于任意可交换含幺环也成立。下面的定理给出两个例子。

定理 1 设 R 是可交换含幺环，加法单位元为 0，乘法单位元为 1。则

(a) 对于 R 中的任意元素 x，有 $0*x=0$。

(b) 对于 R 中的任意元素 x，有 $-x=(-1)*x$。

证明 (a) 设 y 表示元素 $0*x$。由于 R 是一个环，所以有

$$y+y=0*x+0*x=(0+0)*x=0*x=y$$

而$(R, +)$是一个阿贝尔群，所以

$$0=(-y)+y=(-y)+(y+y)=[(-y)+y]+y=0+y=y$$

从而(a) 得证。

(b) 由于 $x+((-1)*x)=(1*x)+((-1)*x)=(1+(-1))*x=0*x=0$，所以(b) 得证。 ■

在定理 1(b) 的证明过程中，使用了阿贝尔群中的逆元是惟一的特性，因此，如果一个元素要作为一个逆元表现，则它必是一个逆元。

对于有单位元 1 的可交换环 R 中的一个非零元 x，如果有元素 y 满足 $x*y=y*x=1$，则称 y 是 x 的一个乘法逆元。如果这样的 y 存在，则它是惟一的(1.6 节的定理 1)。因此称之为 x 的乘法逆，用 x^{-1} 或有时用 $1/x$ 表示。

整数集 **Z** 中有乘法逆元的只有整数 1 和–1。但在环 Z_n 中情形是不同的。能够证明如果 a 和 n 互素，即 $\mathrm{GCD}(a,n)=1$，那么 $\overline{a}$ 在 Z_n 中有一个乘法逆元。事实上，根据 1.4 节的定理 4(a)，存在整数 k 和 s 满足方程 $ak+ns=1$，或者 $1-ak=ns$，这就推出 $\overline{1}=\overline{ak}=\overline{a}*\overline{k}$，于是 $\overline{a}$ 有乘法逆元 $\overline{k}$。

例 4 整数 25 和 384 互素，于是 $\overline{25}$ 在 Z_{384} 中有一个乘法逆元。为了求出这个元素，利用 1.4 节中的欧几里得算法计算可得

$$384=15\times 25+9$$
$$25=2\times 9+7$$
$$9=1\times 7+2$$
$$7=3\times 2+1$$

通过连续的替代，有

$$\begin{aligned}1&=7-3\cdot 2=7-3(9-7)=(4\cdot 7)-(3\cdot 9)\\&=4(25-2\cdot 9)-(3\cdot 9)=(4\cdot 25)-(11\cdot 9)\\&=(4\cdot 25)-11(384-15\cdot 25)=(169\cdot 25)-(11\cdot 384)\end{aligned}$$

因此，$169\cdot 25\equiv 1(\mathrm{mod}\ 384)$。所以 $\overline{25}$ 在 Z_{384} 中的乘法逆元为 $\overline{169}$。 ■

域

假设 F 是一个可交换的含幺环。如果 F 中的每个非零元 x 都有一个乘法逆元，则称 F 是一个**域**。下面总结了域 F 的一些性质。

域的性质

F 有两种二元运算：加法+和乘法*，另外有两个特殊的元 0 和 1，使得对于 F 中的任意元

素 x，y 和 z，有

(1) $x+y=y+x$　　(2) $x*y=y*x$

(3) $(x+y)+z=x+(y+z)$　　(4) $(x*y)*z=x*(y*z)$

(5) $x+0=x$　　(6) $x*1=x$

(7) $x*(y+z)=(x*y)+(x*z)$　　(8) $(y+z)*x=(y*x)+(z*x)$

(9) 对于 F 中的任一元素 x，在 F 中都有惟一元素 $-x$，使得 $x+(-x)=0$。

(10) 对于 F 中的任一元素 $x\neq 0$，在 F 中都有惟一元素 x^{-1}，使得 $x*x^{-1}=1$。

例 5 所有实数的集合 $\mathbb{R}$ 以及普通的加法和乘法运算构成一个域。这里 $x^{-1}=1/x$。上面列出的域的性质就是算术运算的标准规则。 ■

例 6 有理数集合 $\mathbb{Q}$ 以及普通的加法和乘法运算构成一个域。 ■

上面的一些例子是典型的域。域事实上符合算术和代数运算中的所有类似的规则，大多数代数技巧都可以用于域中。值得注意的是，存在只有有限个元素的域。下面的定理介绍一些有限域，它们在以后的讨论中是非常重要的。

定理 2 当 n 是一个素数时，环 Z_n 是一个域。

证明 回顾 n 如果除了它本身和 1 之外没有其他除数，那么 n 是一个素数。如果 $\bar{a}$ 是 Z_n 的任意一个非零元，则 a 不能被 n 整除，从而 $\mathrm{GCD}(a,n)=1$。根据前面例 4 的结论，$\bar{a}$ 有一个乘法逆元，因此 Z_n 是一个域。 ■

例 7 根据定理 2，$Z_5=\{\bar{0},\bar{1},\bar{2},\bar{3},\bar{4}\}$ 是一个域。因为 $2+3=5$，所以 $\bar{2}+\bar{3}=\bar{0}$，故 $-\bar{2}=\bar{3},-\bar{3}=\bar{2}$。类似地，$-\bar{4}=\bar{1},-\bar{1}=\bar{4}$。为了表示方便，将该域中的一个非零元 $\bar{a}$ 的乘法逆元表示为 $\frac{1}{\bar{a}}$，将 $\bar{a}$ 和 $\bar{b}$ 的积用 $\bar{a}\cdot\bar{b}$ 表示。这样，由于 $2\cdot 3=6=1\cdot 5+1$，所以 $\bar{2}\cdot\bar{3}=\bar{1}$。于是 $\frac{1}{\bar{2}}=\bar{3},\frac{1}{\bar{3}}=\bar{2}$。类似地，由于 $4\cdot 4=16=3\cdot 5+1$，所以 $\frac{1}{\bar{4}}=\bar{4}$，并且同实数域中一样，$\bar{1}$ 的乘法逆元是它自身。在实数域中使用的一些运算方法对该域同样适用。例如，假设要同时求解如下方程组：

$$\begin{cases}\bar{3}x+\bar{2}y=\bar{4}\\ \bar{2}x+\bar{4}y=\bar{2}\end{cases}$$

开始可以先将第一个方程两边乘上 $\frac{1}{\bar{3}}=\bar{2}$，得到 $x+\bar{4}y=\bar{3}$（因为 $\bar{2}\cdot\bar{4}=\bar{3}$），或者 $x=\bar{3}-\bar{4}y=\bar{3}+(-\bar{4})y=\bar{3}+y$。根据定理 1(b)把 x 代入第二个方程，得到

$$\bar{2}\cdot(\bar{3}+y)+\bar{4}y=\bar{1}+y=\bar{2}$$

这里利用了 $\bar{2}\cdot\bar{3}=\bar{1},\bar{2}+\bar{4}=\bar{1}$ 的事实。于是 $y=\bar{1}$，从而 $x=\bar{4}$。 ■

读者可以将结果代入原方程组进行检验。

费尔马小定理

域 F 的一个重要性质是 F 中的非零元所组成的集合 F^* 关于乘法是一个阿贝尔群。需要证明

F关于乘法运算是一个闭集，也就是说，F中非零元之积也是非零元。从域的性质(2)、(4)、(6)和(10)中可以推出这个结果。假设在F中，$a*b=0$，如果a不等于0，那么可以在等式$a*b=0$两边乘上a^{-1}，根据定理1(a)得到

$$b=a^{-1}*0=0$$

因此a或b中必有一个为0。从而证明了F中的非零元之积也是非零元。于是F关于乘法是闭集，故它是一个阿贝尔群。

下面的结果在数学上有很多用途，而(b)和(c)将用在第十一章的公钥密码算法中。

定理3 (a) 如果$G=\{g_1, g_2,\ldots, g_n\}$是一个有限阿贝尔群，单位元记为$e$，$a$是$G$中的任意一个元素，则$a^n=e$。

(b) **费尔马小定理**：如果p是一个素数，且$\mathrm{GCD}(a, p)=1$，则

$$a^{p-1}\equiv 1(\mathrm{mod}\ p)$$

(c) 如果p是一个素数，a是任意整数，那么$a^p\equiv a(\mathrm{mod}\ p)$。

证明 (a) 根据9.4节中的推论1，群中的一个元的乘法运算是一对一的函数，所以，积$ag_1, ag_2, \cdots, ag_n$各不相同且它们只是元素$g_1, g_2, \cdots, g_n$以不同次序的一个排列。由此和G中乘法的可交换性得

$$g_1g_2\cdots g_n=(ag_1)(ag_2)\cdots(ag_n)=g_1g_2\cdots g_n(a^n)$$

在上式两端左乘$(g_1g_2\cdots g_n)^{-1}$，则(a)得证。

(b) 如果p是一个素数，则由定理2可知Z_p是一个域，于是非零元关于乘法运算构成了一个阿贝尔群。该群的单位元为$\overline{1}$。由于该群中有$p-1$个元素，所以根据(a)的结果推出如果$\overline{a}\neq\overline{0}$，则$[\overline{a}]^{p-1}=\overline{1}$。这与(b)是等价的。

(c) 如果a不被p整除，那么可以运用费尔马小定理，在两边乘上a的同余，就可以得到(c)的结果。如果a能被p整除，则$a^p\equiv 0(\mathrm{mod}\ p), a\equiv 0(\mathrm{mod}\ p)$，所以$a^p$和$a$相互同余。■

例8 根据费尔马小定理，$12^{30}\equiv 1(\mathrm{mod}\ 31)$, $74^{83}\equiv 74(\mathrm{mod}\ 83)$。■

例9 53除4^{900}的余数是多少？

解 根据费尔马小定理，$4^{52}\equiv 1(\mathrm{mod}\ 53)$。由于

$$900=(17\times 52)+16$$

可以得到

$$4^{900}=4^{(17\times 52)+16}=(4^{52})^{17}4^{16}\equiv 4^{16}(\mathrm{mod}\ 53)$$

现在

$$4^3=64\equiv 11(\mathrm{mod}\ 53)$$
$$4^6\equiv 11^2\equiv 15(\mathrm{mod}\ 53)$$
$$4^{12}\equiv 15^2\equiv 13(\mathrm{mod}\ 53)$$
$$4^{16}\equiv 4^{12}\cdot 128\equiv 13\cdot 22\equiv 21(\mathrm{mod}\ 53)$$

所以53除4^{900}的余数是21。■

习 题 9.6

在第 1 题~第 6 题中，确定已知的数学结构是一个环、一个交换环还是一个含幺环。

1．(2×2 矩阵，+，*)

2．($n\times n$ 对角矩阵，+，*)

3．$n\times n$ 布尔矩阵，其中+是$\vee$，*是$\wedge$。

4．S={0，1}，其中+和*由下表定义：

+	0	1
0	0	1
1	1	0

*	0	1
0	0	0
1	0	1

5．$S=\{a+b\sqrt{2},\ a,\ b\in\mathbf{Z}\}$，其中+和*是通常的加法和乘法。

6．S={$a+b\sqrt{5}$，a，$b\in\mathbf{Z}$}，其中+和*是通常的加法和乘法。

一个环 R，如果在 R 中存在元素 a 和 b 使得 $a\neq0$，$b\neq0$ 且 $a*b=0$，那么 R 有**零因子**。

7．证明：(2×2 矩阵，+，*)是一个有零因子的环。

8．证明：Z_{10} 是一个有零因子的环。

一个环 R 的元素 r 称为 R 的一个**单位**，如果在 R 中 r 有一个乘法逆 r^{-1}。在第 9 题~第 12 题中，给出已知环的所有单位。

9．Z_4　　10．Z_7　　11．Z_{10}　　12．Z_{11}

如果(T，+)是(R，+)的一个子群并且(T，*)是(R，*)的一个子半群，则 T 是环 R 的一个**子环**。

13．证明：形如$\begin{bmatrix}0 & a\\ 0 & b\end{bmatrix}$的 2×2 矩阵的集合是第 1 题中环的一个子环。

14．证明：整数集合是第 5 题中所给环的一个子环。

15．对于第 1 题~第 6 题中的每一个结构，确定结构是否是一个域。解释你的决定。

16．在域 Z_7 中，求下面每一个元素。

(a) $-\bar{3}$　(b) $-\bar{2}$　(c) $-\bar{6}$　(d) $\frac{\bar{1}}{\bar{2}}$　(e) $\frac{\bar{2}}{\bar{3}}$

17．在 Z_{196} 中求 $\overline{55}$ 的乘法逆。

18．在 Z_{196} 中求 $\overline{29}$ 的乘法逆。

19．在 Z_5 中求解下面的方程组。

$$\begin{cases}\bar{4}x-\bar{3}y=\bar{1}\\ \bar{2}x+y=\bar{3}\end{cases}$$

20．在 Z_7 中求解下面的方程组。

$$\begin{cases}\bar{4}x-\bar{3}y=\bar{1}\\ \bar{2}x+\bar{4}y=\bar{2}\end{cases}$$

21．在 Z_7 中，求下面方程的所有解。

(a) $x^2+\bar{2}x+\bar{3}=\bar{4}$ (b) $x^2+\bar{4}x+\bar{1}=\bar{3}$

22. 在 Z_5 中，求下面方程的所有解。

(a) $x^2+\bar{2}x+\bar{3}=\bar{4}$ (b) $x^2+\bar{4}x+\bar{1}=\bar{3}$

23. 当 3^{850} 用 17 除，余数是多少？

24. 当 5^{219} 用 17 除，余数是多少？

25. 域 Z_2 与 6.5 节定义的有限布尔代数 B 可以等同，其中+和*是由第 4 题中的表给出的运算。如果把这些表看成是真值表，那么每一个表有表达它的一个布尔函数。

(a) 求布尔函数 f 使得 $f(x,y)=x+y$。

(b) 求布尔函数 g 使得 $g(x,y)=x*y$。

26. 证明：一个域不能有任何零因子。

27. 对于一个环 R 的单位的集合，有什么条件才能保证 R 是一个域？

28. 证明：如果 n 不是一个素数，那么 Z_n 不是一个域。

29. 证明：Z_n 是一个域当且仅当 n 是一个素数。

证明知识小结

本章中的证明大部分是一些简单的直接证明，从某种程度来讲是由于介绍了几种新的数学结构(半群、幺群、群、阿贝尔群、环和域)。首先用新的数学结构考察了所定义的一些简单结果，例如 9.2 节的定理 1。然而，像 9.4 节中定理 1 和定理 4 那样的惟一性证明往往是间接的。

在本章中，子结构概念出现了几次。一般来说，要证明一个子集形成一个数学结构的一个子结构，必须证明该子集合以及其上的运算满足这种类型结构的定义。但是任何整体性质，例如结合律，子集合都是会继承的，因此，只需检验封闭性和涉及某些特殊元素的性质。所以，证明一个子集合是一个子群，只需验证乘法的封闭性，单位元属于子集合，子集合中的每一个元素的逆元属于该子集合。

同构是证明命题的一个强有力的工具，因为粗略地说，如果在两个结构之间建立了一个同构，则允许将其中一个结构的性质转到另一个结构上，如 9.2 节的定理 4 所示。

主要概念复习

- A 上的二元运算：处处有定义的函数 $f:A\times A\to A$。
- 可交换二元运算：$a*b=b*a$。
- 可结合二元运算：$a*(b*c)=(a*b)*c$。
- 半群：非空集合 S 加上一个定义在 S 上的可结合二元运算*。
- 幺半群：具有单位元的半群。
- 半群$(S,*)$的子半群$(T,*)$：T 是 S 的一个非空子集并且当 a 和 b 属于 T 时，$a*b\in T$。
- 幺半群$(S,*)$的子幺半群$(T,*)$：T 是 S 的非空子集，$e\in T$，当 a 和 b 属于 T 时，$a*b\in T$。
- 同构：见 9.2 节。

- 同态：见 9.2 节。
- 定理：设$(S,*)$和$(T,*')$分别是具有单位元 e 和 e'的幺半群，假设 $f: S\to T$ 是一个同构，那么 $f(e)=e'$。
- 定理：如果$(S,*)$ 和$(T, *')$是半群，那么$(S\times T, *'')$是一个半群，其中$*''$ 定义为
$$(s_1, t_1)*'' (s_2, t_2)=(s_1*s_2, t_1*'t_2)$$
- 半群$(S,*)$上的同余类系 R：等价关系 R 使得 $a\,R\,a'$ 和 $b\,R\,b'$推出$(a*b)R(a'*b')$。
- 定理：设 R 是半群$(S,*)$上的一个同余关系，定义 S/R 中的运算⊛如下：
$$[a]\circledast[b]=[a*b]$$
那么$(S/R, \circledast)$是一个半群。
- 商半群或因子半群 S/R：见 9.3 节。
- Z_n：见 9.3 节。
- 定理(同态基本定理)：设 $f: S\to T$ 是半群$(S, *)$到半群$(T, *')$上的一个同态且是满射，R 是 S 上的关系且定义为 $a\,R\,b$ 当且仅当对于 S 中的 a 和 b 有 $f(a)=f(b)$，那么
(a) R 是一个同余关系。(b) T 与 S/R 是同构的。
- 群$(G, *)$：具有单位元 e 的幺半群，使得对每个 $a\in G$，存在 $a'\in G$ 具有性质 $a*a'=a'*a=e$。
- 定理：设 G 是一个群，a, b 和 c 是 G 的元素，那么
(a) $ab=ac$ 推出 $b=c$(左消去性质)。
(b) $ba=ca$ 推出 $b=c$ (右消去性质)。
- 定理：设 G 是一个群，a 和 b 是 G 的元素，那么
(a) $(a^{-1})^{-1}=a$。　　(b) $(ab)^{-1}=b^{-1}a^{-1}$。
- 群 G 的阶：$|G|$，G 中元素的个数。
- S_n：n 个字母上的对称群。
- 子群：见 9.4 节。
- 定理：设 R 是群$(G, *)$上的一个同余关系，那么半群$(G/R, \circledast)$是一个群，其中在 G/R 中的运算⊛定义为
$$[a]\circledast[b]=[a*b]$$
- 由 a 确定的 G 中 H 的左陪集 aH：$\{ah|b\in H\}$。
- 正规子群：子群 H，使得对 G 中所有的 a 有 $aH=Ha$。
- 定理：设 R 是群 G 上的一个同余关系，$H=[e]$(即包含单位元的等价类)，那么 H 是 G 的正规子群并且对每个 $a\in G$,$[a]=aH=Ha$。
- 定理：设 N 是群 G 的一个正规子群，R 是 G 上的如下关系：$a\ R\ b$ 当且仅当 $a^{-1}b\in N$，那么
(a) R 是 G 上的一个同余关系。
(b) N 是关于 R 的等价类$[e]$，其中 e 是 G 的单位元。
- 环$(S, +, *)$：非空集合 S 使得$(S, +)$是一个阿贝尔群，$*$是可结合的，$*$关于+是可分配的。

- 交换环：运算*是可交换的环。
- 定理：设 R 是有加法单位元 0 和乘法单位元 1 的一个交换环，那么
  (a) 对 R 中的任意 x，有 $0*x=0$。
  (b) 对 R 中的任意 x，有 $-x=(-1)*x$。
- 域：具有单位元的交换环并且每个非零元有一个乘法逆。
- 定理：当 n 是一个素数时，环 Z_n 是一个域。
- 定理：(a) 如果 $G=\{g_1, g_2, \cdots, g_n\}$ 是一个有单位元 e 的有限阿贝尔群，a 是 G 中的任意一个元素，那么 $a^n=e$。
  (b) (费尔马小定理) 如果 p 是一个素数，$\mathrm{GCD}(a, p)=1$，那么 $a^{p-1}\equiv 1(\mathrm{mod}\ p)$。
  (c) 如果 p 是一个素数且 a 是任意一个整数，那么 $a^p\equiv a(\mathrm{mod}\ p)$。

回 顾 问 题

1. 说一个集合关于二元运算是封闭的，其含义是什么？
2. 半群同构与偏序集同构有何不同？群的同构与偏序集同构有何相同？
3. 定义一个同余关系的性质是什么？
4. 为什么说群比半群有更多的结构？
5. 一个域与一个环有何不同？

第九章自测题

1. 对于下面每一个分题，判断*的描述是否是已知集合上一个二元运算的正确定义。
(a) 2×2 布尔矩阵集合，$\boldsymbol{A}*\boldsymbol{B}=[(a_{ij}+b_{ij})\ (\mathrm{mod}\ 2)]$。
(b) 偶数集合，$a*b=a+b$。
(c) $\mathbf{Z}^+$ 上的运算，$a*b=2^{ab}$。
2. 完成下面的运算表使得*是一个交换的和幂等的二元运算。

*	a	b	c
a		c	
b			
c		b	

3. 设 $\mathbf{Q}$ 是有理数集合，定义 $a*b=a+b-ab$。
(a) $(\mathbf{Q}, *)$是一个幺半群吗？证明你的答案。
(b) 如果$(\mathbf{Q}, *)$是一个幺半群，$\mathbf{Q}$ 的哪些元素有一个逆元？
4. 判断第 1 题中所给的集合和运算是否是一个半群、一个幺半群或者两者都不是。
5. 设 $A=\{0, 1\}$，考虑半群$(A^*, \cdot)$，其中 $\cdot$ 是连接运算，定义该半群上的关系 R 为$\alpha\ R\ \beta$当且仅当α和β有相同的长度。证明：R 是一个同余关系。

6. 设 G 是一个群，定义 $f: G\to G$ 为 $f(a)=a^{-1}$。问 f 是一个同态吗？证明你的答案。

7. 设 G 是一个群，它的乘法表如下所示，H 是子群 $\{c, d, e\}$。

*	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	e	c	b	f	d
b	b	d	e	f	a	c
c	c	f	a	d	e	b
d	d	b	f	e	c	a
f	f	c	d	a	b	e

在 G 中找 H 的右陪集。

8. 设 f: $G_1\to G_2$ 是从群 $(G_1, *_1)$ 到群 $(G_2, *_2)$ 上的一个同态满射，如果 N 是 G_1 的一个正规子群，证明：它的像 $f(N)$ 是 G_2 的一个正规子群。

9. 设 G 是具有单位元 e 的一个群，证明：如果 $x^2=x$ 对 G 中某个 x 成立，则 $x=e$。

10. 设 G 是在加法运算下的整数群，G' 是在加法运算下的所有偶数的群，证明：由 $f(a)=2a$ 定义的函数 f: $G\to G'$ 是一个同构。

11. 设 H_1，H_2，…，H_k 是群 G 的子群，证明：$\bigcap_{i=1}^{k} H_i$ 也是 G 的一个子群。

12. 证明：如果 $\sqrt{n}$ 是一个无理数，那么所有形如 $a+b\sqrt{n}$ 的数的集合以及普通的加法和乘法运算是一个域，其中 a 和 b 是整数。

编码练习

对于下面各题，用伪码(见附录 A 描述)或你所熟悉的程序设计语言写出符合要求的程序或子程序，通过手工记录或计算机运行来检验你的编码。

设 Z_n 是 9.3 节中所定义的集合。

1. 写一个函数 SUM 使得取 Z_n 的两个元素[x]和[y]，返回它们的和[x]+[y]，并且用户能够输入对 n 的选择。
2. 设 H={[0]，[2]}，写一个计算 Z_6 中 H 的左陪集的子程序。
3. 设 H={[0]，[2]，[4]，[6]}，写一个计算 Z_8 中 H 的右陪集的子程序。
4. 写一个程序使得已知一个有限的运算表，确定该运算是否满足结合性质。
5. 写一个程序使得已知一个有限群 G 和一个子群 H，确定 H 是否是 G 的一个正规子群。

实验九

本实验的目的是考察群、子群和元素之间的关系。在考察中将给出 5 个群的例子，当然你也可以决定寻找其他群以检验你的猜想。

S_3 是{1，2，3}的置换群，运算为合成。它也是一个三角形的对称群(见 9.4 节)。

D_4 是一个正方形的对称群(见 9.4 节的第 19 题所示)。

S_4 是{1，2，3，4}的置换群，运算为合成。

G_1 是乘法表如表 1 所示的群。

G_2 是乘法表如表 2 所示的群。

写出 S_3，D_4 和 S_4 的乘法表也许对你是有帮助的。

表 1

	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	5	4	7	6	1	8	3
3	3	8	5	2	7	4	1	6
4	4	3	6	5	8	7	2	1
5	5	6	7	8	1	2	3	4
6	6	1	8	3	2	5	4	7
7	7	4	1	6	3	8	5	2
8	8	7	2	1	4	3	6	5

表 2

	1	2	3	4	5
1	1	2	3	4	5
2	2	3	4	5	1
3	3	4	5	1	2
4	4	5	1	2	3
5	5	1	2	3	4

1．指出上面 5 个群的单位元 e。

2．对于上面 5 个群，做下面的事情：对于群中的每个元 g，求满足 $g^k=e$(单位元)的最小 k，该数 k 称为 g 的阶。

3．在群的元素阶与群的阶(群的阶是其元素的个数)之间有什么关系？

4．对于上面 5 个群中的每一个群找出群的所有子群。

5．如果群的元素是某个元素的方幂，则称该群是循环群。确定每个群的子群中的循环群。

6．在子群的阶和群的阶之间有什么关系？

7．G_1 和 D_4 都是阶为 8 的群，它们同构吗？解释你的理由。