离散数学基础习题答案

Answers to Exercises in Elementary Discrete Mathematics

周晓聪　　乔海燕

中山大学数据科学与计算机学院, 广州 510275

2021 年 1 月 19 日

目录

第十章　代数系统

练习 10.1 设集合$A=\{1,2,3,\cdots,10\}$，下面定义的二元运算$*$对于集合A是否封闭？其中gcd是求两个数的最大公约数，而lcm是求两个数的最小公倍数。

$$(1)\ x*y=\max(x,y) \qquad (2)\ x*y=\min(x,y)$$
$$(3)\ x*y=\gcd(x,y) \qquad (4)\ x*y=\mathrm{lcm}(x,y)$$

解答：(1) 显然$\max(x,y)\in\{x,y\}\subseteq A$，因此运算max对集合$A$封闭；
(2) 同样$\min(x,y)\in\{x,y\}\subseteq A$，因此运算min对集合$A$封闭；
(3) 显然$1\leq \mathrm{GCD}(x,y)\leq \min(x,y)$，因此运算GCD对集合$A$封闭；
(4) 显然$\mathrm{LCM}(3,8)=24\notin A$，因此运算LCM对集合$A$不封闭。

练习* 10.2 给定集合$A=\{a,b,c\}$，在A上定义运算$*$和$\circ$，其运算表如下：

$*$	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	a	c
c	c	c	c

试判断运算$*$和$\circ$是否满足交换律、结合律、幂等律、消去律，以及是否有单位元和零元，如果有单位元，进一步判断每个元素是否有逆元。最后确定$*$对$\circ$是否满足分配律，$\circ$对$*$是否满足分配律，如果$*$和$\circ$都满足交换律，判断$*$和$\circ$是否有吸收律。

解答：(1) 对于运算$*$，通过上述运算表可以看出：(i) 由于运算表关于主对角线对称，因此该运算满足交换律；(ii) 显然$b*b=c$，因此不满足幂等律；(iii) 由于每行每列中都没有相同元素，因此满足消去律；(iv) 显然a是单位元，但没有零元；(v) 显然a的逆元是a，而b和c互为逆元；(vi) 最后对于结合律，考虑对于任意的$x,y,z\in A$，如果x,y,z中有一个是单位元a，则必有$x*(y*z)=(x*y)*z$，否则若x,y,z中不出现a，则有以下情况，我们一一验证等式$x*(y*z)=(x*y)*z$：

$$b*(b*b)=b*c=a \qquad (b*b)*b=c*b=a \qquad //\ \text{不出现}c$$
$$b*(b*c)=b*a=b \qquad (b*b)*c=c*c=b \qquad //\ \text{出现一个}c\text{在最后}$$
$$b*(c*b)=b*a=b \qquad (b*c)*b=a*b=b \qquad //\ \text{出现一个}c\text{在中间}$$

$$c*(b*b)=c*c=b \qquad (c*b)*b=a*b=b \qquad \text{// 出现一个}c\text{在最前}$$
$$c*(c*b)=c*a=c \qquad (c*c)*b=b*b=c \qquad \text{// 出现一个}b\text{在最后}$$
$$c*(b*c)=c*a=c \qquad (c*b)*c=a*c=c \qquad \text{// 出现一个}b\text{在中间}$$
$$b*(c*c)=b*b=c \qquad (b*c)*c=a*c=c \qquad \text{// 出现一个}b\text{在最前}$$
$$c*(c*c)=c*b=a \qquad (c*c)*c=b*c=a \qquad \text{// 不出现}b$$

注意，这里确实罗列了所有情况，因为出现一个b相当于出现两个c，不出现b相当于全是c。

进一步根据以上等式可发现规律，当x,y,z全等于b或全等于c时，$(x*y)*z=a=x*(y*z)$，而当x,y,z中既有b又有c时，若$x\neq y$，则由$b*c=c*b=a$有$(x*y)*z=a*z=z$，若这时$y\neq z$，则$x=z$，从而$x*(y*z)=x*a=x=z$，若$y=z$，则$z\neq x$，则由$b*b=c$或$c*c=b$有$x*(y*z)=x*(z*z)=x*x=z$。同理，若$y\neq z$，则$(x*y)*z=x=x*(y*z)$。总之，我们得到$*$满足结合律。

(2) 对于运算$\circ$，通过上述运算表可以看出：(i) 由于运算表关于主对角线对称，因此该运算满足交换律；(ii) 显然$b*b=a$，因此不满足幂等律；(iii) 由于c是零元，因此不满足消去律；(iv) 显然a是单位元，而c是零元；(v) 显然a的逆元是a，而b的逆元是b，c是零元，因此没有逆元；(vi) 最后对于结合律，考虑对于任意的$x,y,z\in A$，如果x,y,z中有一个单位元a，则必有$x*(y*z)=(x*y)*z$，同理若x,y,z中有零元c，则必有$x*(y*z)=c=(x*y)*z$，而$b*(b*b)=b*a=b$，$(b*b)*b=a*b=b$。因此运算$\circ$满足结合律。

(3) 对于分配律，从下面的反例可以看出$*$对$\circ$没有分配律，且$\circ$对于$*$也没有分配律：

$$c*(c\circ c)=c*c=b \qquad (c*c)\circ(c*c)=b\circ b=a \qquad \text{// 表明}*\text{对}\circ\text{没有分配律}$$
$$c\circ(c*c)=c\circ b=c \qquad (c\circ c)*(c\circ c)=c*c=b \qquad \text{// 表明}\circ\text{对}*\text{没有分配律}$$

练习* 10.3 设$X=\mathbb{R}-\{0,1\}$，在X上定义如下函数$f_i,1\leq i\leq 6$，对任意的$x\in X$，

$$f_1(x)=x \qquad f_2(x)=x^{-1} \qquad f_3(x)=1-x$$
$$f_4(x)=(1-x)^{-1} \qquad f_5(x)=(x-1)x^{-1} \qquad f_6(x)=x(x-1)^{-1}$$

判断集合$F=\{f_1,f_2,f_3,f_4,f_5,f_6\}$对函数复合运算是否封闭，如封闭请给出$(F,\circ)$的运算表。

解答：由下面的运算表可得到F对函数复合运算$\circ$封闭：

$\circ$	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	f_4	f_3	f_6	f_5
f_3	f_3	f_5	f_1	f_6	f_2	f_4
f_4	f_4	f_6	f_2	f_5	f_1	f_3
f_5	f_5	f_3	f_6	f_1	f_4	f_2
f_6	f_6	f_4	f_5	f_2	f_3	f_1

注意，这里的复合$\circ$定义为$(g\circ f)(x)=g(f(x))$。

练习 10.4 对于集合X上所有关系构成的集合$\wp(X\times X)$，关系复合的单位元是恒等关系Δ_X，那么X上的哪些关系关于复合运算有逆元？逆元是什么？

解答：我们证明，对于X上的关系$R\subseteq X\times X$，R关于关系复合有逆元S当且仅当，对任意$x\in X$存在唯一的$y\in X$使得$\langle x,y\rangle\in R$，而且对任意$y\in X$存在唯一的$x\in X$使得$\langle x,y\rangle\in R$。

($\Longrightarrow$)：若R关于关系复合有逆元，也即存在关系S使得$R\circ S=\Delta_X$且$S\circ R=\Delta_X$。我们证明对任意$x\in X$都存在唯一的$y\in X$使得$\langle x,y\rangle\in R$，且对任意$y\in Y$存在唯一的$x\in X$使得$\langle x,y\rangle\in R$。

对任意$x\in X$，由于$S\circ R=\Delta_X$，从而$\langle x,x\rangle\in S\circ R$，从而存在$y\in X$使得$\langle x,y\rangle\in R$且$\langle y,x\rangle\in S$，这表明对任意$x\in X$，至少存在$y\in X$，使得$\langle x,y\rangle\in R$。进一步，若还存在$z\in X$，$z\neq y$且使得$\langle x,z\rangle\in R$，则由$\langle y,x\rangle\in S$，则有$\langle y,z\rangle\in R\circ S$，但$R\circ S=\Delta_X$，因此有$y=z$。这就表明对任意$x\in X$，存在唯一的$y\in X$使得$\langle x,y\rangle\in R$。同理可证，对任意$y\in X$，存在唯一的$x\in X$使得$\langle x,y\rangle\in R$。

($\Longleftarrow$)：若对任意$x\in X$存在唯一的$y\in X$使得$\langle x,y\rangle\in R$，而且对任意$y\in X$存在唯一的$x\in X$使得$\langle x,y\rangle\in R$，我们证明$R\circ R^{-1}=\Delta_X$及$R^{-1}\circ R=\Delta_X$。

对任意$x\in X$，因为存在$y\in X$使得$\langle x,y\rangle\in R$，从而$\langle y,x\rangle\in R^{-1}$，从而$\langle x,x\rangle\in R^{-1}\circ R$，这表明$\Delta_X\subseteq R^{-1}\circ R$。反之，对任意$\langle x,y\rangle\in R^{-1}\circ R$，则存在$z\in X$使得$\langle x,z\rangle\in R$且$\langle z,y\rangle\in R^{-1}$，从而$\langle x,z\rangle\in R$且$\langle y,z\rangle\in R$，但对$z$存在唯一的$x\in X$使得$\langle z,x\rangle\in R$，因此$x=y$，这表明$R^{-1}\circ R\subseteq\Delta_X$。综上有$R^{-1}\circ R=\Delta_X$，类似可证明这时也有$R\circ R^{-1}=\Delta_X$。

因此X上的二元关系R关于复合有逆元当且仅当，对任意$x\in X$，存在唯一的$y\in X$使得$\langle x,y\rangle\in R$，且对任意$y\in X$，存在唯一的$x\in X$使得$\langle x,y\rangle\in R$。而且这时R的逆元是R^{-1}。

练习* 10.5 设$\circ$是集合S上的二元运算，满足结合律，e是它的单位元，且对任意$x\in S$，x都可逆。这时任意元素的逆元都唯一，因此可定义一元运算$(-)^{-1}:S\to S$：对任意$x\in S$，x^{-1}是x关于运算$\circ$的唯一逆元。证明：

(1) 对任意$x,y\in S$，有$(x\circ y)^{-1}=y^{-1}\circ x^{-1}$；

(2) 对任意$x\in S$，及任意自然数$n\in\mathbb{N}$，$(x^n)^{-1}=(x^{-1})^n$。

证明 (1) 由于运算$\circ$满足结合律，因此我们有：

$$\begin{aligned}(x\circ y)\circ(y^{-1}\circ x^{-1}) &= x\circ(y\circ y^{-1})\circ x^{-1}=x\circ e\circ x^{-1}=x\circ x^{-1}=e\\ (y^{-1}\circ x^{-1})\circ(x\circ y) &= y^{-1}\circ(x^{-1}\circ x)\circ y=y^{-1}\circ e\circ y=y^{-1}\circ y=e\end{aligned}$$

这就表明$(x\circ y)$的逆元是$y^{-1}\circ x^{-1}$，即$(x\circ y)^{-1}=y^{-1}\circ x^{-1}$。

(2) 对n使用数学归纳法证明$(x^n)^{-1}=(x^{-1})^n$，当$n=0$时，注意到按定义$x^0=e$且$(x^{-1})^0=e$，而$e^{-1}=1$，因此等式成立。假设当$n=k$时等式成立，即有$(x^k)^{-1}=(x^{-1})^k$。考虑$n=k+1$时，我们有：

$$(x^{k+1})^{-1}=(x^k\circ x)^{-1}=x^{-1}\circ(x^k)^{-1}=x^{-1}\circ(x^{-1})^k=(x^{-1})^{k+1}$$

这里用到(1)证明的等式，以及幂运算的性质，即对任意自然数m,n，$x^m\circ x^n=x^{m+n}$。 □

练习 10.6 对于代数$(\mathbb{Z},+,\times)$和$(\mathbb{Z}_6,\oplus_6,\otimes_6)$，分别给出它们的一个子代数例子。注意，不要与例子10.12 给出的子代数相同。

解答：我们可类似例子10.12，考虑由3生成的子代数：对于代数$(\mathbb{Z},+,\times)$，令$T=\{3k\mid k\in\mathbb{Z}\}$，显然$T$对整数乘法和整数加法也封闭，因此$(T,+,\times)$是$(\mathbb{Z},+,\times)$子代数；而对代数$(\mathbb{Z}_6,\oplus_6,\otimes_6)$，3生成的子代数则是$(\{0,3\},\oplus_6,\otimes_6)$。

练习* 10.7 给定集合$\mathbb{Z}_{12}=\{0,1,2,3,4,5,6,7,8,9,10,11\}$，定义运算$\oplus_{12}$：$\forall x,y\in\mathbb{Z}_{12},x\oplus_{12}y=(x+y)\mod 12$，判断下面的集合$S_i,1\leq i\leq 4$是否是$(\mathbb{Z}_{12},\oplus_{12})$的子代数：

(1) $S_1=\{0,2,4,6,8,10\}$　　(2) $S_2=\{1,3,5,7,9,11\}$

(3) $S_3=\{0,3,6,9\}$　　(4) $S_4=\{0,5,10\}$

解答：(1) S_1是$\mathbb{Z}_{12}$的子代数，因为实际上$S_1=\{2k\mid k\in\mathbb{N},2k\in\mathbb{Z}_{12}\}$，对任意的$2k_1,2k_2\in S_1$，我们证明$(2k_1+2k_2)\mod 12\in S_1$，根据带余数除法，设$2k_1+2k_2=12s+r$，这里$0\leq r<12$，也即$r\in\mathbb{Z}_{12}$。另一方面$r=2(k_1+k_2-6s)$，也即存在$k=k_1+k_2-6s$使得$r=2k$，即$r\in S_1$，从而$(2k_1+2k_2)\mod 12=r\in S_1$，即$S_1$对运算$\oplus_{12}$封闭。

(2) S_2不是$\mathbb{Z}_{12}$的子代数，因为$5\oplus_{12}7=0\notin S_2$，也即$S_2$对运算$\oplus_{12}$不封闭。

(3) S_3是$\mathbb{Z}_{12}$的子代数，因为实际上$S_3=\{3k\mid k\in\mathbb{N},3k\in\mathbb{Z}_{12}\}$，对任意的$3k_1,3k_2\in S_1$，我们证明$(3k_1+3k_2)\mod 12\in S_3$，根据带余数除法，设$3k_1+3k_2=12s+r$，这里$0\leq r<12$，也即$r\in\mathbb{Z}_{12}$。另一方面$r=3(k_1+k_2-4s)$，也即存在$k=k_1+k_2-4s$使得$r=3k$，即$r\in S_3$，从而$(3k_1+3k_2)\mod 12=r\in S_3$，即$S_3$对运算$\oplus_{12}$封闭。

(4) S_4不是$\mathbb{Z}_{12}$的子代数，因为$5\oplus_{12}10=3\notin S_4$，也即$S_4$对运算$\oplus_{12}$不封闭。

练习 10.8 判断下面定义的$\mathbb{Z}$上的二元关系$R_i,1\leq i\leq 4$是否是代数系统$(\mathbb{Z},+)$（$+$是普通实数加法）上的同余关系？如果是同余关系，请写出代数系统$(\mathbb{Z},+)$关于该同余关系的商代数（即给出商代数的基集和运算的定义）。

(1) $\langle x,y\rangle\in R_1$当且仅当$(x\leq 0\wedge y\leq 0)\vee(x\geq 0\wedge y\geq 0)$；

(2) $\langle x,y\rangle\in R_2$当且仅当$|x-y|<10$；

(3) $\langle x,y\rangle\in R_3$当且仅当$(x=y=0)\vee(x\neq 0\wedge y\neq 0)$；

(4) $\langle x,y\rangle\in R_4$当且仅当$x\geq y$。

解答：(1) 显然$\langle -1,-1\rangle,\langle 0,2\rangle\in R_1$，但是$\langle -1+0,-1+2\rangle\notin R_1$，因此$R_1$不是同余关系。实际上，由于$\langle -1,0\rangle,\langle 0,1\rangle\in R_1$，而$\langle -1,1\rangle\notin R_1$，即$R_1$不传递，因此它根本不是等价关系。

(2) 显然$\langle 1,10\rangle,\langle 1,10\rangle\in R_2$，但是$\langle 1+1,10+10\rangle\notin R_2$，因此$R_2$不是同余关系。实际上，由于$\langle 1,9\rangle,\langle 9,18\rangle\in R_2$，而$\langle 1,18\rangle\notin R_2$，即$R_2$不传递，因此它根本不是等价关系。

(3) 显然$\langle -1,1\rangle,\langle 1,1\rangle\in R_3$，但是$\langle -1+1,1+1\rangle\notin R_3$，因此$R_3$不是同余关系。不过$R_3$是等价关系，$R_3$有两个等价类，即$\{0\}$和$\mathbb{Z}-\{0\}$。

(4) 显然R_4不是对称的，例如$\langle 3,2\rangle\in R_4$，可是$\langle 2,3\rangle\notin R_4$，因此$R_4$不是等价关系，当然也不是同余关系。不过对任意的$x_1,x_2,y_1,y_2$，如果$x_1\geq y_1$且$x_2\geq y_2$，显然$x_1+x_2\geq y_1+y_2$，即$R_4$对加法是可置换的。

练习* 10.9 判断下面定义的$\mathbb{R}$上的二元关系$R_i,1\leq i\leq 4$是否是代数系统$(\mathbb{R},*)$（$*$是普通实数乘法）上的同余关系？如果是同余关系，请写出代数系统$(\mathbb{R},*)$关于该同余关系的商代数（即给出商

代数的基集和运算的定义）。

(1) $R_1 = \{\langle x, y\rangle \mid x = y \vee x = -y\}$　(2) $R_2 = \{\langle x, y\rangle \mid x$和$y$同为零或同为正数或同为负数$\}$

(3) $R_3 = \{\langle x, y\rangle \mid x^2 + y^2 \geq 0\}$　(4) $R_4 = \Delta_{\mathbb{R}} \cup \{\langle 0, 1\rangle, \langle 1, 0\rangle\}$

这里$\Delta_{\mathbb{R}}$是$\mathbb{R}$上的恒等关系。

解答：(1) R_1的直观含义是，$\langle x, y\rangle \in R_1$当且仅当$x$与$y$具有相同的绝对值，即$|x| = |y|$，因此$R_1$是等价关系。根据绝对值的定义，不难证明对任意的$x, y \in \mathbb{R}$，有$|x * y| = |x| * |y|$。从而对任意的$x_1, x_2, y_1, y_2$，如果$|x_1| = |y_1|$且$|x_2| = |y_2|$，则有

$$|x_1 * x_2| = |x_1| * |x_2| = |y_1| * |y_2| = |y_1 * y_2|$$

因此R_1是同余关系。而$\mathbb{R}/R_1 = \{\{x, -x\} \mid x \in \mathbb{R}\}$，也即对任意的$x \in \mathbb{R}$，等价类$[x]_{R_1} = \{x, -x\}$。商代数中的运算$\otimes$定义为：对任意的$x, y \in \mathbb{R}$，

$$[x]_{R_1} \otimes [y]_{R_1} = [x * y]_{R_1}$$

(2) 定义函数$\mathbf{Sig} : \mathbb{R} \to \{-1, 0, 1\}$为，对任意的$x \in \mathbb{R}$，

$$\mathbf{Sig}(x) = \begin{cases} -1 & \text{若 } x < 0 \\ 0 & \text{若 } x = 0 \\ 1 & \text{若 } x > 0 \end{cases}$$

也即$\mathbf{Sig}(x)$给出x的符号。从而R_2的直观含义是，$\langle x, y\rangle \in R_2$当且仅当$\mathbf{Sig}(x) = \mathbf{Sig}(y)$，因此$R_2$是等价关系。对任意的$x, y \in \mathbb{R}$，不难证明$\mathbf{Sig}(x * y) = \mathbf{Sig}(x) * \mathbf{Sig}(y)$，从而对任意的$x_1, x_2, y_1, y_2$，如果$\mathbf{Sig}(x_1) = \mathbf{Sig}(y_1)$且$\mathbf{Sig}(x_2) = \mathbf{Sig}(y_2)$，则有

$$\mathbf{Sig}(x_1 * x_2) = \mathbf{Sig}(x_1) * \mathbf{Sig}(x_2) = \mathbf{Sig}(y_1) * \mathbf{Sig}(y_2) = \mathbf{Sig}(y_1 * y_2)$$

因此R_2是同余关系。而$\mathbb{R}/R_2 = \{[-1]_{R_2}, [0]_{R_2}, [1]_{R_2}\}$，其中：

$$\begin{aligned} [-1]_{R_2} &= \{x \mid x \in \mathbb{R}, x < 0\} \\ [0]_{R_2} &= \{0\} \\ [1]_{R_2} &= \{x \mid x \in \mathbb{R}, x > 0\} \end{aligned}$$

商代数中的运算$\otimes$定义为：

$\otimes$	$[-1]_{R_2}$	$[0]_{R_2}$	$[1]_{R_2}$
$[-1]_{R_2}$	$[1]_{R_2}$	$[0]_{R_2}$	$[-1]_{R_2}$
$[0]_{R_2}$	$[0]_{R_2}$	$[0]_{R_2}$	$[0]_{R_2}$
$[1]_{R_2}$	$[-1]_{R_2}$	$[0]_{R_2}$	$[1]_{R_2}$

(3) 由于对任意的$x,y\in\mathbb{R}$都有$x^2+y^2\geq 0$，因此$R_3=\mathbb{R}\times\mathbb{R}$是全域关系，因此$R_3$是等价关系，而且肯定是同余关系，且$\mathbb{R}/R_2=\{\mathbb{R}\}$，商代数上的运算$\otimes$显然为$\mathbb{R}\otimes\mathbb{R}=\mathbb{R}$。

(4) 显然$\langle 0,1\rangle\in R_4$以及$\langle 3,3\rangle\in R_4$，但是$\langle 0*3,\ 1*3\rangle\notin R_4$，因此$R_4$不是同余关系。

练习 10.10 给定代数(A,Σ_A)上的同余关系R，证明商代数保持除消去律以外的运算性质，即设$+$和$\times$是(A,Σ_A)的两个二元运算，它们在商代数$(A/R,\Sigma_{A/R})$对应的运算分别是$\oplus$和$\otimes$：

(1) 若$\times$满足交换律、结合律和幂等律，则$\otimes$也满足交换律、结合律和幂等律；

(2) 若$\times$对$+$满足分配律，则$\otimes$对$\oplus$也满足分配律；

(3) 若$\times$和$+$有吸收律，则$\otimes$和$\oplus$也有吸收律；

(4) 若$e\in A$是A中关于$\times$的单位元，则$[e]_R$是A/R中关于$\otimes$的单位元；

(5) 若$\theta\in A$是A中关于$\times$的零元，则$[\theta]_R$是A/R中关于$\otimes$的零元；

(6) 设$\times$有单位元e，若$a\in A$关于$\times$的逆元是a^{-1}，则$[a]_R\in A/R$关于$\otimes$的逆元是$[a^{-1}]_R$。

证明 定义函数$\rho:A\to A/R$，对任意$a\in A$，$\rho(a)=[a]_R$，显然ρ是满函数，因为对任意的$[a]_R\in A/R$一定有原像a。而对于任意的$a,b\in A$和(A,σ_A)的任意运算σ_A，或者我们记为中缀运算符$\otimes$，它在商代数对应的运算$\sigma_{A/R}$记为$\otimes$，则有：对任意$a,b\in A$：

$$\rho(a\times b)=[a\times b]_R \qquad\qquad \rho(a)\otimes\rho(b)=[a]_R\otimes[b]_R=[a\times b]_R$$

这表明ρ是代数(A,Σ_A)到商代数$(A/R,\Sigma_{A/R})$的满同态，从而根据满同态保持消去律以外的性质立即得商代数也保持除消去律以外的运算性质。 □

【**讨论**】我们也可直接证明，例如对于结合律：对任意$[a]_R,[b]_R,[c]_R\in A/R$，

$$\begin{aligned}([a]_R\otimes[b]_R)\otimes[c]_R&=([a\times b]_R)\otimes[c]_R=[(a\times b)\times c]_R\\ [a]_R\otimes([b]_R\otimes[c]_R)&=[a]_R\otimes([b\times c]_R)=[a\times(b\times c)]_R\end{aligned}$$

由$\times$满足结合律，则有$a\times(b\times c)=(a\times b)\times c$，从而有$([a]_R\otimes[b]_R)\otimes[c]_R=[a]_R\otimes([b]_R\otimes[c]_R)$，即$\otimes$也满足结合律。

对于分配律，我们证明左分配等式：对任意$[a]_R,[b]_R,[c]_R\in A/R$，

$$\begin{aligned}[a]_R\otimes([b]_R\oplus[c]_R)&=[a]_R\otimes[b+c]_R=[a\times(b+c)]_R=[(a\times b)+(a\times c)]_R\\ ([a]_R\otimes[b]_R)\oplus([a]_R\otimes[c]_R)&=([a\times b]_R)\oplus([a\times c]_R)=[(a\times b)+(a\times c)]_R\end{aligned}$$

因此有$[a]_R\otimes([b]_R\oplus[c]_R)=([a]_R\otimes[b]_R)\oplus([a]_R\otimes[c]_R)$。右分配等式也可类似证明。

若$e\in A$是A中关于$\times$的单位元，则对任意$[a]_R$有：

$$[a]_R\otimes[e]_R=[a\times e]_R=[a]_R \qquad\qquad [e]_R\otimes[a]_R=[e\times a]_R=[a]_R$$

因此$[e]_R$是$\otimes$的单位元。

最后，设$\times$有单位元e，若$a\in A$关于$\times$的逆元是a^{-1}，则有：

$$[a^{-1}]_R\otimes[a]_R=[a^{-1}\times a]_R=[e]_R \qquad\qquad [a]_R\otimes[a^{-1}]_R=[a\times a^{-1}]_R=[e]_R$$

因此$[a]_R \in A/R$关于$\otimes$的逆元是$[a^{-1}]_R$。

练习 10.11 给定集合X，X上所有关系构成的集合是$\wp(X\times X)$，该集合与关系并和关系交构成代数$(\wp(X\times X),\cup,\cap)$。定义函数$f:\wp(X\times X)\to\wp(X\times X)$，对任意$R\subseteq X\times X$，$f(R)=R^{-1}$，证明$f:(\wp(X\times X),\cup,\cap)\longrightarrow(\wp(X\times X),\cup,\cap)$是同态。

证明 对任意关系R,S，我们有：

$$\begin{aligned} f(R\cup S) &= (R\cup S)^{-1} & f(R)\cup f(S) &= R^{-1}\cup S^{-1}\\ f(R\cap S) &= (R\cap S)^{-1} & f(R)\cap f(S) &= R^{-1}\cap S^{-1}\end{aligned}$$

在关系一章我们已经证明$(R\cup S)^{-1}=R^{-1}\cup S^{-1}$，以及$(R\cap S)^{-1}=R^{-1}\cap S^{-1}$，因此$f$是同态。 □

练习* 10.12 给定实数集$\mathbb{R}$及其上的普通乘法$*$构成的代数$(\mathbb{R},*)$，试判断下面定义的函数$f_i:\mathbb{R}\to\mathbb{R}, 1\le i\le 4$是否是代数$(\mathbb{R},*)$的自同态（即该代数到它自己的同态）？如果是同态，是否是满同态、单同态或同构？

(1) $f_1(x)=|x|$　　(2) $f_2(x)=x^2$　　(3) $f_3(x)=2x$　　(4) $f_4(x)=-x$

解答：(1) 对于函数f_1，因为对任意的$x,y\in\mathbb{R}$，有$f_1(x*y)=|x*y|=|x|*|y|=f_1(x)*f_1(y)$，因此$f_1$是同态，由于$f_1$不是单函数（例如$f_1(3)=f_1(-3)=3$，也不是满函数（其值域是正实数），因此$f_1$既不是单同态，也不是满同态，当然也就不可能是同构；

(2) 对于函数f_2，因为对任意的$x,y\in\mathbb{R}$，有$f_2(x*y)=(x*y)^2=x^2*y^2=f_2(x)*f_2(y)$，因此$f_2$是同态，由于$f_2$不是单函数（例如$f_1(3)=f_1(-3)=9$，也不是满函数（其值域是正实数），因此$f_2$既不是单同态，也不是满同态，当然也就不可能是同构；

(3) 对于函数f_3，由于$f_3(3*3)=2*3*3=18$，而$f_3(3)*f_3(3)=2*3*2*3=36$，因此f_3不是同态；

(4) 对于函数f_4，由于$f_4(3*3)=-(3*3)=-9$，而$f_4(3)*f_4(3)=-3*-3=9$，因此f_4不是同态。

练习 10.13 代数系统$(\mathbb{R}-\{0\},*)$与$(\mathbb{R},+)$是否同构？为什么？这里$\mathbb{R}$是实数集，$*$是普通实数乘法，$+$是普通实数加法。

解答：我们用反证法证明这两者不同构，假设函数$\varphi:\mathbb{R}-\{0\}\to\mathbb{R}$是它们之间的同构，则根据$\varphi$是同态有$\varphi(1)=\varphi(1*1)=\varphi(1)+\varphi(1)=2\varphi(1)$，因此必有$\varphi(1)=0$。而另一方面由$0=\varphi(1)=\varphi(-1*-1)=\varphi(-1)+\varphi(-1)=2\varphi(-1)$，因此也必有$\varphi(-1)=0$，因此$\varphi$不可能是单函数，从而与函数$\varphi$是同构矛盾！

【**讨论**】也许有人认为$f:\mathbb{R}\to\mathbb{R}-\{0\}, x\mapsto e^x$是同构，但实际上虽然$f$是同态，却不是满函数（因为指数函数的值域是正实数），因此不是同构！

练习 10.14 对于代数$(\mathbb{Z}_6,\oplus_6,\otimes_6)$，利用代数同态证明$\oplus_6$和$\otimes_6$都满足交换律、结合律，以及$\otimes_6$对$\oplus_6$有分配律。

解答：可定义代数$(\mathbb{Z},+,\times)$到代数$(\mathbb{Z}_6,\oplus_6,\otimes_6)$的满同态$f:\mathbb{Z}\to\mathbb{Z}_6$：对任意整数$z$，$f(z)=z \bmod 6$。$f$显然是满函数，而且对任意整数$x,y$，不难证明有：

$$\begin{aligned} f(x+y) &= (x+y)\bmod 6 = ((x \bmod 6)+(y \bmod 6))\bmod 6 = f(x)\oplus 6 f(y) \\ f(x\times y) &= (x\times y)\bmod 6 = ((x \bmod 6)\times(y \bmod 6))\bmod 6 = f(x)\otimes 6 f(y) \end{aligned}$$

因此f确实是这两个代数之间的满同态，从而由$+,\times$都满足交换律、结合律以及$\times$对$+$有分配律立即得到$\oplus_6$和$\otimes_6$都满足交换律、结合律，以及$\otimes_6$对$\oplus_6$有分配律。

练习 10.15 举例说明一个同态不是满同态时它不保持运算的交换性，即给出两个同类型的代数$(A,\times)$和$(B,\circ)$，$\times$满足交换律，但$\circ$不满足交换律，且有同态$f:(A,\times)\to(B,\circ)$。

解答：我们可设$A=\{1,-1\}$，而$\times$是普通乘法，这样$(A,\times)$构成一个代数。设$B=\{a,b\}$，而运算$\circ$定义为：$a\circ a=a, a\circ b=a, b\circ a=b, b\circ b=b$，显然$\circ$不满足交换律（因为$a\circ b\neq b\circ a$），但我们可定义$f:A\to B$，$f(1)=f(-1)=a$，显然$f:(A,\times)\to(B,\circ)$是同态。

练习 10.16 在集合$\mathbb{Q}\times\mathbb{Q}$上定义二元运算$*$为：$\forall\langle a,b\rangle,\langle x,y\rangle\in\mathbb{Q}\times\mathbb{Q}$，$\langle a,b\rangle*\langle x,y\rangle=\langle a+x,ay+b\rangle$，这里$\mathbb{Q}$是有理数集，请判断$(\mathbb{Q}\times\mathbb{Q},\ *)$是否是半群，并说明理由。

解答：对任意的$\langle a,b\rangle,\langle x,y\rangle,\langle u,v\rangle\in\mathbb{Q}\times\mathbb{Q}$，

$$\begin{aligned} (\langle a,b\rangle*\langle x,y\rangle)*\langle u,v\rangle &= \langle a+x,ay+b\rangle*\langle u,v\rangle = \langle a+x+u,(a+x)v+ay+b\rangle \\ \langle a,b\rangle*(\langle x,y\rangle*\langle u,v\rangle) &= \langle a,b\rangle*\langle x+u,xv+y\rangle = \langle a+x+u,a(xv+y)+b\rangle \end{aligned}$$

显然不能对任意的a,x,v有$(a+x)v=axv$，因此运算$*$不满足结合律，因此$(\mathbb{Q}\times\mathbb{Q},\ *)$不是半群。

练习* 10.17 设$(S,*)$是半群，$a\in S$是S的一个固定的元素，在S上定义二元运算$\circ$：$\forall x,y\in S, x\circ y=x*a*y$，证明$(S,\circ)$是半群。

解答：对任意的$x,y,z\in S$，

$$\begin{aligned} (x\circ y)\circ z &= (x*a*y)\circ z = (x*a*y)*a*z \\ x\circ(y\circ z) &= x\circ(y*a*z) = x*a*(y*a*z) \end{aligned}$$

由$(S,*)$是半群，$*$满足结合律，因此

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

因此$\circ$也满足结合律，即$(S,\circ)$是半群。

练习 10.18 设$S=\{a,b\}$，$(S,*)$是半群，且$a*a=b$，证明$*$满足交换律，且b是$*$的幂等元。

证明 我们首先证明$a*b=b*a$，这是因为：由$a*a=b$可得：

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

由于显然有$a*a=a*a$及$b*b=b*b$，因此$*$满足交换律。

若$a*b=a=b*a$，则：

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

若$a*b=b=b*a$，则；

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

因为$a*b$不等于a就等于b，因此总有$b*b=b$。 □

练习 10.19 设$(G,e,*)$是独异点，且对G的任意元素$x\in G$都有$x*x=e$，证明$(G,*)$是交换群。

证明 因为对任意的$x\in G$，都有$x*x=e$，则x有逆元，就是它自己，即对任意的$x,x^{-1}=x$，因此$(G,*)$是群。进一步，对任意的x,y，

$$(x*y)*(y*x)=x*(y*y)*x=x*x=e$$

因此$y*x$是$x*y$的逆，但所有元素的逆都是它自己，因此$x*y=y*x$，即$(G,*)$是交换群。 □

练习 10.20 设G是群，e是其单位元，a和b是G的任意元素，证明：(1) a^{-1}的逆元是a；(2) $(ab)^{-1}=b^{-1}a^{-1}$；(3) 对任意整数n,m有$a^{m+n}=a^ma^n$，以及$(a^m)^n=a^{mn}$。

证明 (1) 因为$a^{-1}a=e$且$aa^{-1}=e$，因此a^{-1}的逆元就是a。

(2) 因为$(ab)(b^{-1}a^{-1})=a(bb^{-1})a^{-1}=aa^{-1}=e$且$(b^{-1}a^{-1})(ab)=b^{-1}(a^{-1}a)b=b^{-1}b=e$，因此$ab$的逆元是$b^{-1}a^{-1}$，即$(ab)^{-1}=b^{-1}a^{-1}$。

(3) 我们首先使用数学归纳法进行证明：对任意自然数n,m有$a^{m+n}=a^ma^n$，$(a^m)^n=a^{mn}$，以及$(a^n)^{-1}=(a^{-1})^n$。

(i). **归纳基**：$n=0$时，注意到$a^0=e$，因此显然成立；

(ii). **归纳步**：设$n=k$时成立，$a^{m+k}=a^ma^k$，以及$(a^m)^k=a^{mk}$，以及$(a^k)^{-1}=(a^{-1})^k$，对于$n=k+1$，我们有：

$$\begin{aligned}
a^{m+k+1} &= a^{m+k}a=a^ma^ka=a^ma^{k+1}\\
(a^m)^{k+1} &= (a^m)^ka^m=(a^{mk})a^m=(a^{mk+m})=a^{m(k+1)}\\
(a^{k+1})^{-1} &= (a^ka)^{-1}=a^{-1}(a^k)^{-1}=a^{-1}(a^{-1})^k=(a^{-1})^{k+1}
\end{aligned}$$

根据数学归纳法，对任意自然数n,m有$a^{m+n}=a^ma^n$，$(a^m)^n=a^{mn}$以及$(a^n)^{-1}=(a^{-1})^n$。从而，进一步，若$n,m<0$，则有：

$$\begin{aligned}
a^{m+n} &= (a^{-1})^{|m|+|n|}=(a^{-1})^{|m|}+(a^{-1})^{|n|}=a^m+a^n\\
(a^m)^n &= ((a^{-1})^{|m|})^n=(((a^{-1})^{|m|})^{-1})^{|n|}=(((a^{-1})^{-1})^{|m|})^{|n|}=a^{|m||n|}=a^{mn}
\end{aligned}$$

而若m和n只有一个负数，不妨设$m \geq 0, n < 0$，则若$m+n<0$，则有$m+n=-(|n|-m)$，从而有：

$$\begin{aligned} a^{m+n} &= a^{-(|n|-m)} = (a^{-1})^{(|n|-m)} \\ a^m a^n &= a^m (a^{-1})^{|n|} = a^m ((a^{-1})^m (a^{-1})^{(|n|-m)}) = a^m (a^m)^{-1} (a^{-1})^{(|n|-m)} = (a^{-1})^{(|n|-m)} \end{aligned}$$

因此$a^{m+n}=a^m a^n$。而若$m+n \geq 0$，则这时$m+n=m-|n|$，从而有：

$$a^{m+n} = a^{(m-|n|)} \qquad a^m a^n = a^{(m-|n|)} a^{|n|} (a^{-1})^{|n|} = a^{(m-|n|)} a^{|n|} (a^{|n|})^{-1} = a^{(m-|n|)}$$

因此也有$a^{m+n}=a^m a^n$。而当$m \geq 0, n < 0$时有：

$$(a^m)^n = ((a^m)^{-1})^{|n|} = ((a^{-1})^m)^{|n|} = (a^{-1})^{m|n|} \qquad a^{mn} = (a^{-1})^{|mn|} = (a^{-1})^{|m||n|} = (a^{-1})^{m|n|}$$

因此有$(a^m)^n = a^{mn}$。

综上，我们证明了对任意整数n, m有$a^{m+n}=a^m a^n$，以及$(a^m)^n = a^{mn}$。 □

练习 10.21 证明：群中以下每组中的元素有相同的阶，其中a, b, c都是任意元素

(1) a, a^{-1}, cac^{-1} (2) ab, ba (3) abc, bca, cab

证明 (1) 设$|a|=n, |a^{-1}|=m, |cac^{-1}|=k$，则由于：

$$a^m = ((a^{-1})^{-1})^m = ((a^{-1})^m)^{-1} = e^{-1} = e$$

从而$m \mid n$，另一方面：$(a^{-1})^n = (a^n)^{-1} = e^{-1} = e$，从而$n \mid m$，从而$m=n$。

进一步，我们使用数学归纳法证明对任意的自然数p，有$(cac^{-1})^p = ca^p c^{-1}$，显然$p=0,1$时成立，假设对任意的自然数$p=q$成立，考虑$p=q+1$，我们有：

$$(cac^{-1})^{q+1} = (cac^{-1})^q (cac^{-1}) = (ca^q c^{-1})(cac^{-1}) = ca^{q+1}c^{-1}$$

这就证明了对任意的p有$(cac^{-1})^p = ca^p c^{-1}$。从而：$(cac^{-1})^n = ca^n c^{-1} = cec^{-1} = e$，从而$k \mid n$，另一方面：

$$a^k = c^{-1} ca^k c^{-1} c = c^{-1} (cac^{-1})^k c = c^{-1} ec = e$$

从而$n \mid k$，即$n=k$。

(2) 因为$ab = a(ba)a^{-1}$，所以由上一小题知

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

(3) 因为$abc = a(bc),\ bca = (bc)a = b(ca),\ cab = (ca)b$，因此由上一小题有

$$|abc| = |a(bc)| = |(bc)a| = |bca| = |b(ca)| = |(ca)b| = |cab|$$

□

练习* 10.22 求模14加群Z_{14}和群$U(14)$中每个元素的阶。

解答：(1) 首先$Z_{14}=\{0,1,2,3,4,5,6,7,8,9,10,11,12,13\}=\langle 1\rangle$，对任意的$a\in Z_{14}$，$a=a\cdot 1$。注意到$|1|=14$，从而根据阶的性质有，若$a\neq 0$，则$|a|=\dfrac{14}{(14,a)}$。从而：

$$\begin{array}{lllll} |0|=1 & |1|=14 & |2|=7 & |3|=14 & |4|=7 \\ |5|=14 & |6|=7 & |7|=2 & |8|=7 & |9|=14 \\ |10|=7 & |11|=14 & |12|=7 & |13|=14 & \end{array}$$

(2) 首先$U(14)=\{1,3,5,9,11,13\}$，而且：

$$3^2=9 \qquad 3^3=13 \qquad 3^4=11 \qquad 3^5=5 \qquad 3^6=1$$

因此$U(14)=\langle 3\rangle$，再根据阶的性质，容易得到：

$$|1|=1 \qquad |3|=6 \qquad |5|=6 \qquad |9|=3 \qquad |11|=3 \qquad |13|=2$$

练习 10.23 给出群$U(18)$的阶，以及它的每个元素的阶。

解答：注意到$U(18)=\{1,5,7,11,13,17\}$，因此群$U(18)$的阶是6，而且：

$$5^2=7 \qquad 5^3=17 \qquad 5^4=13 \qquad 5^5=11 \qquad 5^6=1$$

因此$U(18)=\langle 5\rangle$，再根据阶的性质，容易得到：

$$|1|=1 \qquad |5|=6 \qquad |7|=3 \qquad |11|=6 \qquad |13|=3 \qquad |17|=2$$

练习* 10.24 设$G=\{\varphi:\mathbb{R}\to\mathbb{R}\mid \varphi:x\mapsto ax+b,a,b\in\mathbb{R},a\neq 0\}$，即$G$是所有形如$\varphi(x)=ax+b$的函数$\varphi$构成的集合。

(1). 证明G以函数复合运算构成群；

(2). 设$S=\{\varphi:\mathbb{R}\to\mathbb{R}\mid \varphi:x\mapsto x+b,b\in\mathbb{R}\}$，证明$S$是$G$的子群；

(3). 设$T=\{\varphi:\mathbb{R}\to\mathbb{R}\mid \varphi:x\mapsto ax,a\in\mathbb{R},a\neq 0\}$，证明$T$是$G$的子群。

证明 (1) 对于G的任意两个函数$\varphi_1(x)=a_1x+b_1$和$\varphi_2(x)=a_2x+b_2$，显然有

$$(\varphi_1\circ\varphi_2)(x)=\varphi_1(a_2x+b_2)=a_1(a_2x+b_2)+b_1=a_1a_2x+(a_1b_2+b_1)$$

因此$\varphi_1\circ\varphi_2$也属于G，即G对函数复合封闭。显然恒等函数$\mathbf{id}(x)=x$属于G，它是G的单位元。而对任意函数$\varphi(x)=ax+b$，因为$a\neq 0$，因此它的逆可定义为$\varphi^{-1}(x)=x/a-b/a$，不难看到有：

$$(\varphi\circ\varphi^{-1})(x)=\varphi(x/a-b)=x \qquad (\varphi^{-1}\circ\varphi)(ax+b)=x$$

即$\varphi\circ\varphi^{-1}=\mathbf{id}$且$\varphi^{-1}\circ\varphi=\mathbf{id}$，即$\varphi^{-1}$确实是$\varphi$的逆元。因此$G$构成群。

(2) 对S的任意函数$\varphi_1(x)=x+b_1$，$\varphi_2(x)=x+b_2$，则$\varphi_2^{-1}(x)=x-b_2$，从而有：

$$(\varphi_1\circ\varphi_2^{-1})=\varphi(x-b_2)=x+(b_1-b-2)$$

从而有$\varphi_1\circ\varphi_2^{-1}\in S$，从而根据子群判定定理有$S$是$G$的子群。

(3) 对T的任意函数$\varphi_1(x)=a_1x$，$\varphi_2(x)=a_2x$，这里$a_1\neq 0$且$a_2\neq 0$，则$\varphi_2^{-1}(x)=x/a_2$，从而有：

$$(\varphi_1\circ\varphi_2^{-1})=\varphi(x/a_2)=(a_1/a_2)x$$

从而有$\varphi_1\circ\varphi_2^{-1}\in T$，从而根据子群判定定理有$T$是$G$的子群。 □

练习 10.25 求循环群Z_{14}和$U(14)$的所有子群。

解答：(1) 我们知道$Z_{14}=\langle 1\rangle$，根据循环群的性质，当$a\in Z_{14}$是14的因子时，$\langle a\rangle$是Z_{14}的子群，这样Z_{14}的所有子群包括：

$$\begin{aligned}\langle 1\rangle &= Z_{14}\\ \langle 2\rangle &= \{2,4,6,8,10,12,0\}\\ \langle 7\rangle &= \{7,0\}\\ \langle 0\rangle &= \{0\}\end{aligned}$$

(2) 们知道$U(14)=\langle 3\rangle$，根据循环群的性质，对于任意的$a=3^k\in U(14)$，当k是$|U(14)=6$的因子时，$\langle a\rangle$是$U(14)$的子群，这样$U(14)$的所有子群包括：

$$\begin{aligned}\langle 3\rangle &= U(14)\\ \langle 3^2\rangle &= \{3^2,3^4,3^0\}=\{9,11,1\}\\ \langle 3^3\rangle &= \{3^3,3^0\}=\{13,1\}\\ \langle 3^6\rangle &= \{1\}\end{aligned}$$

练习* 10.26 考虑群$U(30)$，给出子群$\langle 7\rangle$的所有左陪集，这里$\langle 7\rangle$表示7生成的$U(30)$的子群。

解答：首先$U(30)=\{1,7,11,13,17,19,23,29\}$，而子群$\langle 7\rangle=\{1,7,19,13\}$，因此它的所有陪集是：

$$\begin{aligned}1\cdot\langle 7\rangle &= \{1,7,19,13\} & 7\cdot\langle 7\rangle &= \{1,7,19,13\}\\ 11\cdot\langle 7\rangle &= \{11,17,23,29\} & 13\cdot\langle 7\rangle &= \{1,7,19,13\}\\ 17\cdot\langle 7\rangle &= \{11,17,23,29\} & 19\cdot\langle 7\rangle &= \{1,7,19,13\}\\ 23\cdot\langle 7\rangle &= \{11,17,23,29\} & 29\cdot\langle 7\rangle &= \{11,17,23,29\}\end{aligned}$$

实际上，由于$|\langle 7\rangle|=4$，而$|U(30)|=8$，因此$\langle 7\rangle$只有两个陪集：$\{1,7,13,19\}$和$\{11,17,23,29\}$。

练习 10.27 设H是群G的子群，证明：(1) 对任意$a\in G$，$|H|=|Ha|=|aH|$；(2) 证明H的所有左陪集构成的集合G/H和所有右陪集构成的集合$G\backslash H$等势，即$|G/H|=|G\backslash H|$。

证明 (1) 定义$\psi: H\to Ha$为$\forall h\in H$，$\psi(h)=ha\in Ha$，由群的消去律我们有：$\forall h_1,h_2\in H$

$$\psi(h_1)=\psi(h_2)\Longrightarrow h_1a=h_2a\Longrightarrow h_1=h_2$$

因此ψ是单函数，另一方面由Ha的定义，任意$b\in Ha$都必然存在$h\in H$使得$b=ha$，因此ψ也是满函数，从而h是双函数，即$|Ha|=|H|$。

类似定义$\psi': H\to aH$为$\forall h\in H$，$\psi'(h)=ah\in aH$，不难证明$|aH|=|H|$。

(2) 我们可定义函数$\varphi: H\backslash G\to G/H$, $\forall a\in G$, $\varphi(Ha)=a^{-1}H$，我们证明φ是G/H到$H\backslash G$的双函数。

由于对$a,b\in G$，$a\neq b$但可能$Ha=Hb$，因此我们必须证明φ的定义是合适的，即$\forall a,b\in G$，$Ha=Hb$蕴含$\varphi(Ha)=\varphi(Hb)$，这可验证如下：

$$Ha=Hb\iff ab^{-1}\in H\iff (ab^{-1})^{-1}=(b^{-1})^{-1}a^{-1}\in H\iff b^{-1}H=a^{-1}H$$

上式也表明φ是单函数。而对于任意的$Hb\in H\backslash G$，显然有$b^{-1}H\in G/H$使得

$$\varphi(b^{-1}H)=H(b^{-1})^{-1}=Hb$$

这表明φ也是满函数，从而φ是双函数，从而$|G/H|=|G\backslash H|$。 □

练习* 10.28 设H是群G的子群，证明H是G的正规子群当且仅当对任意$a\in G$，有$aHa^{-1}=H$。注意，这里$aHa^{-1}=\{aha^{-1}\mid h\in H\}$。

证明 (1) 设H是G的正规子群，我们证明对任意$a\in G$，有$aHa^{-1}=H$。首先对任意$h\in H$，由于H是正规子群，即有$Ha=aH$，因此存在$h'\in H$使得$ha=ah'$，从而$h=ah'a^{-1}\in aHa^{-1}$，即$H\subseteq aHa^{-1}$。反之，对任意$x\in aHa^{-1}$，即存在$h\in H$使得$x=aha^{-1}$，而$aH=Ha$，因此存在h'使得$ah=h'a$，从而$x=h'aa^{-1}=h'\in H$，这表明$aHa^{-1}\subseteq H$，因此当H是G的正规子群时，对任意$a\in G$都有$aHa^{-1}=H$¿

(2) 反之，设对任意$a\in G$有$aHa^{-1}=H$，我们证明G是正规子群，即要证明对任意$a\in G$有$aH=Ha$。首先对任意$x\in aH$，即存在$h\in H$使得$x=ah$，由于$H=aHa^{-1}$，因此$aha^{-1}\in H$，因此$x=ah=ah(a^{-1}a)=(aha^{-1})a\in Ha$，这表明$aH\subseteq Ha$。反之，对任意$x\in Ha$，即存在$h\in H$使得$x=ha$，由于$H$是子群，因此$h^{-1}\in H$，从而$ah^{-1}a^{-1}\in aHa^{-1}$，而$H=aHa^{-1}$是子群，所以也有$(ah^{-1}a^{-1})^{-1}\in H$，从而$x=ha=aa^{-1}ha=a(ah^{-1}a^{-1})^{-1}\in aH$，这就得到$Ha\subseteq aH$。综上有$aH=Ha$，因此$H$是正规子群。 □

练习 10.29 设$G=\{(a,b)\mid a,b\in\mathbb{R},a\neq 0\}$，在$G$上定义运算，对任意的$(a,b),(c,d)\in G$，

$$(a,b)(c,d)=(ac,\ ad+b)$$

证明G关于该运算构成群。又令$K=\{(1,b)\mid b\in\mathbb{R}\}\subseteq G$，证明$K$是$G$的正规子群，并给出商群$G/K$的元素和运算。

证明 (1) 对任意的$(a,b),(c,d),(e,f)\in G$，

$$((a,b)(c,d))(e,f)=(ac,\ ad+b)(e,f)=(ace,acf+ad+b)$$
$$(a,b)((c,d)(e,f))=(a,b)(ce,\ cf+d)=(ace,a(cf+d)+b)$$

因此G的运算满足结合律。

(2) G的运算存在单位元$(1,0)$，显然$(a,b)(1,0)=(a,b)=(1,0)(a,b)$。

(3) 对G的每个元素(a,b)，它有逆元$(1/a,-b/a)$，显然：

$$(a,b)(\frac{1}{a},\frac{-b}{a})=(1,0)=(\frac{1}{a},\frac{-b}{a})(a,b)$$

由(1),(2),(3)得到G是群。

(4) 对于任意的$(1,b_1),(1,b_2)\in K$，

$$(1,b_1)(1,b_2)^{-1}=(1,b_1)(1,-b_2)=(1,b_1-b_2)$$

显然$(1,b_1-b_2)\in K$，因此由子群判定定理2有K是G的子群。又对任意的$(a,c)\in G,(1,b)\in K$，

$$(a,c)(1,b)(a,c)^{-1}=(a,ab+c)(1/a,-c/a)=(1,ab)\in K$$

因此K是G的正规子群。

(5) 商群的基集$G/K=\{(a,c)K\mid(a,c)\in G\}=\{\{(a,b)\mid b\in\mathbb{R}\}\mid a\in\mathbb{R}^*\}$，这里$\mathbb{R}^*$是非零实数构成的集合，也即$G/K$的每个元素实际上是一个集合，这个集合是实数对的集合，且每个实数对的第一个非零实数相同，换句话说，G/K实际上与$\mathbb{R}^*$一一对应。

商群G/K的二元运算$\circ$定义为，对$(a,c)K,(b,d)K\in G/K$，$(a,c)K\circ(b,d)K=(ab,ad+b)K$，注意，$(ab,ad+b)K$中的有序对都是第一个元素是$ab$的实数对，因此运算$\circ$实际上相当于非零实数集上的乘法运算。

商群G/K的单位元就是K，对$(a,c)K\in G/K$，它的逆元是$(1/a,-c/a)K$，也即所有以$1/a$为第一个元素的实数对构成的集合。

总的来说，商群G/K实际上与非零实数集以乘法构成的群同构。 □

练习 10.30 给定集合$A=\{1,2,3,4\}$，定义运算$\otimes_5$为：$\forall x,y\in A$，$x\otimes_5 y=(x*y)\mod 5$，这里$*$是普通乘法，为验证$\otimes_5$确实是集合A上的运算请给出该运算的运算表，然后证明代数$(A,\otimes_5)$与模4加群$(\mathbb{Z}_4=\{0,1,2,3\},\oplus_4)$同构。

解答：$\otimes_5$在集合A上的运算表：

$\otimes_5$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

为了考察它是否与$(\mathbb{Z}_4,\oplus_4)$同构，下面列出$\oplus_4$的运算表：

$\oplus$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

定义函数$\varphi:A\to\mathbb{Z}_4,\varphi(1)=0,\varphi(2)=1,\varphi(3)=3,\varphi(4)=2$，重排$\oplus_4$的运算表：

$\oplus$	0	1	3	2
0	0	1	3	2
1	1	2	0	3
3	3	0	2	1
2	2	3	1	0

不难看到φ是同构。

练习* 10.31 设G是正有理数乘群，$\mathbb{Z}$是整数加群，证明每个正有理数$q\in\mathbb{G}$，都存在惟一的$n\in\mathbb{Z}$，使得$q=2^n\cdot\dfrac{b}{a}$，其中a,b是互素的正奇数，从而可定义函数$\varphi:G\to\mathbb{Z}$，为$\varphi(2^n\cdot\dfrac{b}{a})=n$，证明$\varphi$是满同态。

证明 首先，根据算术基本定理，对每个正整数m，都存在唯一的自然数n使得$m=2^n\cdot a$，这里a是正奇数，实际上，n是m的质因子分解中2的幂（指数），而a是其他质因子的乘积，显然是正奇数。

而对每个正有理数q，都存在正整数m_1,m_2使得$q=\dfrac{m_1}{m_2}$，而m_1,m_2分别存在唯一的自然数n_1,n_2使得$m_1=2^{n_1}\cdot b$，$m_2=2^{n_2}\cdot a$，从而$q=2^{n_1-n_2}\dfrac{b}{a}$，即存在唯一的整数$n=n_1-n_2$使得$q=2^n\dfrac{b}{a}$（当$a,b$不是互素时，从可以化简为互素的两个奇数）。

对任意正有理数p,q，假定分别存在唯一的整数m,n使得$p=2^m\dfrac{b}{a}$，$q=2^n\dfrac{d}{c}$，从而

$$\varphi(p\cdot q)=\varphi(2^m\frac{b}{a}\cdot 2^n\frac{d}{c})=\varphi(2^{m+n}\frac{bd}{ac})=m+n=\varphi(2^m\frac{b}{a})+\varphi(2^n\frac{d}{c})=\varphi(p)+\varphi(q)$$

这表明φ是群同态。注意，这里由于b,a和d,c都是正奇数，因此有

$$2^m\frac{b}{a}\cdot 2^n\frac{d}{c}=2^{m+n}\frac{bd}{ac}$$

其中bd,ac都不会有2的因子，当这两者不互素时可化简为互素的两个数。

显然φ是满函数，例如对任意整数n，有正有理数$q=2^n\cdot\dfrac{3}{5}$，使得$\varphi(q)=n$，因此φ是满同态。□

练习 10.32 补充问题10.46 的证明，即对于从偏序角度定义的格$(L,\wedge,\vee)$，证明$\wedge$满足结合律。

证明 证明$\wedge$满足结合律，即要证明，对L的任意元素a,b,c，有$a\wedge(b\wedge c)=(a\wedge b)\wedge c$。我们分别证明$a\wedge(b\wedge c)\preceq(a\wedge b)\wedge c$和$(a\wedge b)\wedge c\preceq a\wedge(b\wedge c)$。

对于$a \wedge (b \wedge c) \preceq (a \wedge b) \wedge c$我们只要证明$a \wedge (b \wedge c)$也是$a \wedge b$和$c$的下界即可，即只需证明$a \wedge (b \wedge c) \preceq a \wedge b$和$a \wedge (b \wedge c) \preceq c$，后者由

$$a \wedge (b \wedge c) \preceq b \wedge c \preceq c$$

立即可得，而前者又只需证明$a \wedge (b \wedge c) \preceq a$以及$a \wedge (b \wedge c) \preceq b$即可，这里前者显然成立，而后者由

$$a \wedge (b \wedge c) \preceq b \wedge c \preceq b$$

可得。这就证明了$a \wedge (b \wedge c) \preceq (a \wedge b) \wedge c$。

对于$(a \wedge b) \wedge c \preceq a \wedge (b \wedge c)$，只需证明$(a \wedge b) \wedge c \preceq a$以及$(a \wedge b) \wedge c \preceq (b \wedge c)$即可，前者由

$$(a \wedge b) \wedge c \preceq a \wedge b \preceq a$$

立即可得，而对于后者又只需证明$(a \wedge b) \wedge c \preceq b$且$(a \wedge b) \wedge c \preceq c$，后者显然成立，而前者由

$$(a \wedge b) \wedge c \preceq a \wedge b \preceq b$$

可得。这就证明$(a \wedge b) \wedge c \preceq a \wedge (b \wedge c)$。

综上我们得到，$\wedge$满足结合律，即对L的任意元素a, b, c，有$a \wedge (b \wedge c) = (a \wedge b) \wedge c$。 □

练习 10.33 设a和b是格$(A, \preceq)$中的两个元素，证明$a \wedge b \prec b$和$a \vee b \prec a$当且仅当a与b是不可比较的，这里对任意的$x, y \in A$，$x \prec y$当且仅当$x \preceq y$且$x \neq y$。

证明 设$a \wedge b \prec b$及$a \wedge b \prec a$，若a与b可比较，则有$a \preceq b$或$b \preceq a$，从而$a \wedge b = a$或$a \wedge b = b$，与假设矛盾!

反之，若a与b不可比较，则显然$a \wedge b \preceq a$且$a \wedge b \preceq b$，且$a \wedge b \neq a$（否则$a \preceq b$）及$a \wedge b \neq b$（否则$b \preceq a$）。 □

练习* 10.34 设a, b, c是格$(L, \preceq)$的任意元素，证明$a \preceq b \implies a \vee (b \wedge c) \preceq b \wedge (a \vee c)$。

证明 若$a \preceq b$，则由$b \wedge c \preceq b$及$b \wedge c \preceq c \preceq a \vee c$有$b \wedge c \preceq b \wedge (a \vee c)$，从而$b \wedge (a \vee c)$是$a$与$b \wedge c$的上界，根据上确界的性质就有$a \preceq b \implies a \vee (b \wedge c) \preceq b \wedge (a \vee c)$。 □

练习* 10.35 设$(L, \preceq)$是格，证明对任意的$a, b, c \in L$，若$a \preceq b$，则：

$$\begin{aligned}(a \vee (b \wedge c)) \vee c &= (b \wedge (a \vee c)) \vee c \\ (b \wedge (a \vee c)) \wedge c &= (a \vee (b \wedge c)) \wedge c\end{aligned}$$

证明 (1) 我们证明

$$(a \vee (b \wedge c)) \vee c \preceq (b \wedge (a \vee c)) \vee c \quad 及 \quad (b \wedge (a \vee c)) \vee c \preceq (a \vee (b \wedge c)) \vee c$$

对于前者，由练习10.34，当$a \preceq b$，有$(a \vee (b \wedge c)) \preceq (b \wedge (a \vee c))$，而$c \preceq c$，由$\vee$的保序性，前一个不等式确实成立。对于后者，由于显然有$c \preceq (a \vee (b \wedge c)) \vee c$，因此只要证明$(b \wedge (a \vee c)) \preceq (a \vee (b \wedge c)) \vee c$，这可由$b \wedge (a \vee c) \preceq a \vee c \preceq (a \vee (b \wedge c)) \vee c$得到。

(2) 我们证明：

$$(b\wedge(a\vee c))\wedge c\preceq(a\vee(b\wedge c))\wedge c\quad 及\quad (a\vee(b\wedge c))\wedge c\preceq(b\wedge(a\vee c))\wedge c$$

同样地，由练习10.34及$\wedge$的保序性得后一个不等式。而对于前一个不等式，则由于显然有$(b\wedge(a\vee c))\wedge c\preceq c$，只需证明$(b\wedge(a\vee c))\wedge c\preceq(a\vee(b\wedge c))$，而这可由$(b\wedge(a\vee c))\wedge c\preceq b\wedge c\preceq a\vee(b\wedge c)$得到。 □

练习 10.36 设$(L,\preceq)$是格，对任意的$a,b,c\in L$，证明：

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

证明 (1) 由于$a\wedge b\preceq(a\wedge b)\vee(a\wedge c)$及$a\wedge b\preceq(a\wedge b)\vee(b\wedge c)$，因此$a\wedge b\preceq((a\wedge b)\vee(a\wedge c))\wedge((a\wedge b)\vee(b\wedge c))$。

(2) 因此剩下需要证明$((a\wedge b)\vee(a\wedge c))\wedge((a\wedge b)\vee(b\wedge c))\preceq a\wedge b$，这只需证明$(a\wedge b)\vee(a\wedge c)\preceq a$及$(a\wedge b)\vee(b\wedge c)\preceq b$即可，这由$a\wedge b\preceq a$及$a\wedge c\preceq a$和$a\wedge b\preceq b$和$b\wedge c\preceq b$可得。 □

练习 10.37 设$(L,\vee,\wedge)$是格，证明对任意的$a,b\in L$有$a\wedge b=a\vee b$蕴含$a=b$。

证明 因为$a\preceq a\vee b=a\wedge b\preceq b$及$b\preceq a\vee b=a\wedge b\preceq a$。 □

练习 10.38 设$(S,\preceq)$是格，$\vee$和$\wedge$是求上下确界运算，证明对任意$a,b,c\in S$，有分配律不等式：

$$a\vee(b\wedge c)\preceq(a\vee b)\wedge(a\vee c)\qquad (a\wedge b)\vee(a\wedge c)\preceq a\wedge(b\vee c)$$

证明 对于$a\vee(b\wedge c)\preceq(a\vee b)\wedge(a\vee c)$，我们只需证明$a\vee(b\wedge c)\preceq(a\vee b)$且$a\vee(b\wedge c)\preceq(a\vee c)$即可，而前者只需证明$a\preceq a\vee b$及$b\wedge c\preceq a\vee b$即可，这里$a\preceq a\vee b$显然成立，而由$b\wedge c\preceq b\preceq a\vee b$可得$b\wedge c\preceq a\vee b$。对于后者类似只需证明$a\preceq a\vee c$及$b\wedge c\preceq a\vee c$，这里$a\preceq a\vee c$显然成立，而由$b\wedge c\preceq c\preceq a\vee c$可得$b\wedge c\preceq a\vee c$。

对于$(a\wedge b)\vee(a\wedge c)\preceq a\wedge(b\vee c)$，我们只需证明$(a\wedge b)\vee(a\wedge c)\preceq a$且$(a\wedge b)\vee(a\wedge c)\preceq b\vee c$即可，前者又只需证明$a\wedge b\preceq a$及$a\wedge c\preceq a$，这显然成立，后者又只需证明$a\wedge b\preceq b\vee c$及$a\wedge c\preceq b\vee c$，这分别由$a\wedge b\preceq b\preceq b\vee c$和$a\wedge c\preceq c\preceq b\vee c$可得。 □

练习 10.39 补充定理10.19 的证明，即证明其中二元运算$*$满足结合律。注意，这时需要先证明对任意$a,b\in B$，若$a\circ b=a\circ c$且$(\neg a)\circ b=(\neg a)\circ c$，则$b=c$。

证明 我们首先证明对任意$a,b\in B$，若$a\circ b=a\circ c$且$(\neg a)\circ b=(\neg a)\circ c$，由分配律，$a*(\neg a)=\mathbf{0}$以及$\mathbf{0}$是$\circ$的单位元有：

$$\begin{aligned}b&=\mathbf{0}\circ b=(a*(\neg a))\circ b=(a\circ b)*((\neg a)\circ b)\\&=(a\circ c)*((\neg a)\circ c)=(a*(\neg a))\circ c=\mathbf{0}\circ c=c\end{aligned}$$

于是要证明$*$满足结合律，即要证明对任意$a,b,c\in B$, $(a*b)*c=a*(b*c)$，只要证明

$$a\circ((a*b)*c)=a\circ(a*(b*c)) \tag{10.1}$$

$$(\neg a)\circ((a*b)*c)=(\neg a)\circ(a*(b*c)) \tag{10.2}$$

对于(10.1)式，注意到由吸收律有$a\circ(a*(b*c))=a$，且由分配律和吸收律有：

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

这就证明了(10.1)式。对于(10.2)式，由分配律，$\mathbf{1}$是$*$的单位元，以及$a\circ\neg a=\neg a\circ a=\mathbf{1}$有：

$$(\neg a)\circ(a*(b*c))\ =(\neg a\circ a)*(\neg a\circ(b*c))=\mathbf{1}*(\neg a\circ(b*c))=\neg a\circ(b*c)$$

另一方面，同样由分配律，$\mathbf{1}$是$*$的单位元，以及$\neg a\circ a=\mathbf{1}$有：

$$\begin{aligned}(\neg a)\circ((a*b)*c)\ &=(\neg a\circ(a*b))*(\neg a\circ c)=((\neg a\circ a)*(\neg a\circ b))*(\neg a\circ c)\\&=(\mathbf{1}*(\neg a\circ b))*(\neg a\circ c)=(\neg a\circ b)*(\neg a\circ c)=\neg a\circ(b*c)\end{aligned}$$

因此(10.2)式的等号两边都等于$\neg a\circ(b*c)$，这就证明了(10.2)式。 □

练习* 10.40 设$(S,\vee,\wedge)$是布尔代数，$x,y\in S$，证明$x\preceq y$当且仅当$\neg y\preceq\neg x$

证明 对任意的$x,y\in S$，

$$x\preceq y\iff x\wedge y=x\iff\neg(x\wedge y)=\neg x\iff\neg x\vee\neg y=\neg x\iff\neg y\preceq\neg x$$

□

练习* 10.41 证明在布尔代数中，$b\wedge\neg c=0$当且仅当$b\preceq c$。

证明 (1) 若$b\wedge\neg c=0$，则$b\wedge c=(b\wedge c)\vee 0=(b\wedge c)\vee(b\wedge\neg c)=b\vee(c\wedge\neg c)=b\vee 0=b$，从而$b\preceq c$；

(2) 反之，若$b\preceq c$，则$b\wedge c=b$，从而$b\wedge\neg c=(b\wedge c)\wedge\neg c=b\wedge 0=0$。 □

练习 10.42 试证明在任意的布尔代数中有：(1) $a=b$当且仅当$(a\wedge\neg b)\vee(\neg a\wedge b)=0$；(2) $a\preceq b$蕴含$a\vee(b\wedge c)=b\wedge(a\vee c)$。

证明 (1) 若$a=b$，则显然$(a\wedge\neg b)\vee(\neg a\wedge b)=(a\wedge\neg a)\vee(\neg a\wedge a)=0\vee 0=0$。反之，若$(a\wedge\neg b)\vee(\neg a\wedge b)=0$，则必有$a\wedge\neg b=0$且$\neg a\wedge b=0$（实际上，对任意的$x,y$，若$x\vee y=0$，必有$x=0$且$y=0$）。从而$a\wedge\neg b=0$及$a\wedge\neg b=1$，即$\neg b$是$a$的补元，由补元的惟一性得$a=\neg(\neg b)=b$。

(2) 当$a\preceq b$时有$a\vee b=b$，再由分配律有：$a\vee(b\wedge c)=(a\vee b)\wedge(a\vee c)=b\wedge(a\vee c)$ □

练习 10.43 试编写计算机程序判断一个集合上的某个运算是否满足交换律、结合律、幂等律，是否有单位元、零元，每个元素是否有逆元，并判断两个运算之间是否有分配律、吸收律。可假定集合是数字的集合或字母的集合，运算使用运算表定义。

练习 10.44 试编写计算机程序生成群$U(n)$的运算表，这里$U(n)$是所有小于n且与n互质的正整数构成的集合，以模n乘为运算。进一步实现下面一些功能：

(1) 判断$U(n)$是否是循环群，即是否存在元素a，使得$U(n)$的每个元素都能表示成a^i的形式；

(2) 计算$U(n)$的每个元素的阶；

(3) 生成$U(n)$的所有子群，并计算每个子群的所有陪集（这个群是交换群，因此每个元素的左右陪集相同）。

练习 10.45 试编写计算机程序，给定集合$S = \{1, 2, \cdots, n\}$，生成以S上的所有双函数为基集，以函数复合为运算的群的运算表，我们记这个群为$(\mathbf{S}_n, \circ)$，并进一步实现下面一些功能：

(1) 判断$(\mathbf{S}_n, \circ)$是否是循环群；

(2) 计算$(\mathbf{S}_n, \circ)$中每个元素（即每个双函数）的阶；

(3) 给出$(\mathbf{S}_n, \circ)$的所有子群，并计算每个子群的所有陪集，并判断是否是正规子群，如果是则给出它所导出的商群。

练习 10.46 试编写计算机程序，判断对任意正整数n，F_n以整除关系为偏序集是否是布尔代数，这里F_n是n的所有正因子构成的集合。

练习 10.47 试编写计算机程序，判断给定集合上的关系是否是偏序，进一步判断它是否是格、有界格、有补格、分配格或布尔代数。可假定集合是数字或字母的集合，集合上的关系可使用有序对列表、关系矩阵或关系图的邻接表表示。