群、环、域

§4.1 代数运算

习题 4.1

1. 判断下列集合对所给的二元运算是否封闭。

（1）集合 $n\mathbf{Z}=\{n\times z \mid z\in\mathbf{Z}\}$ 关于普通的加法和普通乘法运算，其中 n 是一个正整数。

（2）集合 $S=\{x \mid x=2n-1,\ n\in\mathbf{Z}^+\}$ 关于普通的加法和普通的乘法运算。

（3）集合 $S=\{0,\ 1\}$ 关于普通的加法和普通的乘法运算。

（4）集合 $S=\{x \mid x=2^n,\ n\in\mathbf{Z}^+\}$ 关于普通的加法和普通的乘法运算。

（5）所有 n 阶 $(n\geq 2)$ 实可逆矩阵集合 $\hat{\boldsymbol{M}}_n(\mathbf{R})$ 关于矩阵加法和矩阵乘法运算。

对于封闭的二元运算，判断它们是否满足交换律、结合律和分配律，并在存在的情况下求出它们的单位元、零元和所有可逆元素的逆元。

解：（1）任意 $a,b\in Z$，

$n\times a+n\times b\in nZ$，所以对普通的加法运算封闭。

$n\times a\times(n\times b)=n^2\times a\times b\in nZ$，所以对普通的乘法运算封闭。

（2）

2. 判断下列集合对所给的二元运算是否封闭。

（1）正实数集合 $\mathbf{R}^+$ 和*运算，其中*运算定义为：

$$\forall a,\ b\in\mathbf{R}^+,\ a*b=ab-a-b$$

（2）$A=\{a_1,\ a_2,\ \cdots,\ a_n\},\ n\geq 2$。*运算定义为：

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

对于封闭的二元运算，判断它们是否满足交换律、结合律和等幂律，并在存在的情况下求出它们的单位元、零元和所有可逆元素的逆元。

解：（1）不封闭。例如 $3*1=3\times1-1-3=3-1-3=-1$，$-1\notin R^+$ 。

（2）封闭。$\forall a,\ b\in A,\ a*b=b\in A$，所以*运算在 A 上是封闭的。

$\forall a,\ b,c\in\mathbf{R}^+$，　有：

$a*b=b$，而 $b*a=a$，因为 $a=b$ 不恒成立，即 $a*b\neq b*a$，
所以 $*$ 不满足交换律。

因为 $(a*b)*c=a*c=a$，$a*(b*c)=a*b=a$，

所以$(a*b)*c=a*(b*c)$，所以$*$满足结合律。

又因为$a*a=a$，所以$*$满足等幂律。

设e为单位元，则因有$\forall a\in A$，$a*e=e*a=a$，即$a=e=a$，由a的任意性可知，单位元不存在。

3. 设$S=\mathbf{Q}\times\mathbf{Q}$，这里$\mathbf{Q}$是有理数集合，$*$为$S$上的二元运算，$\forall<u，v>,<x，y>\in S$，

$$<u，v>*<x，y>=<ux，u\cdot y+v>$$

（1）$*$运算在S上是否可交换、可结合？是否为等幂的？

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

（3）$*$运算在S上是否满足消去律？

解：（1）$\forall<u，v>,<x，y>\in S$，

$<u，v>*<x，y>=<ux，u\cdot y+v>$

$<x，y>*<u，v>=<xu，xv+y>$

所以$<u，v>*<x，y>\neq<x，y>*<u,v>$，故$*$运算在$S$上不可交换。

又$\forall<u，v>,<x，y>,<a,b>\in S$，有

$(<a,b>*<u,v>)*<x,y>=<au,av+b>*<x,y>=<aux,auy+av+b>$

$<a,b>*(<u,v>*<x,y>)=<a,b>*<ux,uy+v>=<aux,auy+av+b>$

所以$(<a,b>*<u,v>)*<x,y>=<a,b>*(<u,v>*<x,y>)$，故$*$运算在$S$上可结合。

又$<x,y>*<x,y>=<xx,xy+y>\neq<x,y>$，所以$*$运算在$S$上不等幂。

（2）$*$运算在S上的单位元是$<1,0>$，存在逆元的元素$<x,y>$的逆元是$<x^{-1},-x^{-1}y>$，且$<x,y>$的可逆条件是$x\neq 0$，不存在零元。

（3）若$<a,b>*<u,v>=<a,b>*<x,y>$

即 $<au,av+b>=<ax,ay+b>$，

也即$au=ax,且av+b=ay+b$，所以$u=x,v=y$，也就是$<u,v>=<x,y>$，

故$<a,b>*<u,v>=<a,b>*<x,y>\Rightarrow<u,v>=<x,y>$，所以$*$满足左消去律，

同理可证$*$满足右消去律，故$*$满足消去律。

4. $\mathbf{R}$为实数集合，定义以下六个函数f_1，…，f_6。$\forall x，y\in\mathbf{R}$有

$f_1(<x，y>)=x+y$，　　$f_2(<x，y>)=x-y$，

$f_3(<x，y>)=|x-y|$，　　$f_4(<x，y>)=xy$，

$f_5(<x，y>)=\min(x，y)$，　　$f_6(<x，y>)=\max(x，y)$

（1）指出哪些函数是$\mathbf{R}$上的二元运算。

（2）若是$\mathbf{R}$上的二元运算，说明是否可交换的、可结合的、等幂的？

（3）若是**R**上的二元运算，求单位元、零元以及每一个可逆元素的逆元。

（4）若是**R**上的二元运算，说明是否满足消去律。

解：（1）这 6 个都是**R**上的二元运算。

（2）它们的可交换性、可结合性、等幂性、单位元、零元判断如下：

函数	交换	结合	等幂	单位元	零元
f_1	✓	✓	×	为 0	×
f_2	×	×	×	×	×
f_3	✓	×	×	×	×
f_4	✓	✓	×	为 1	为 0
f_5	✓	✓	✓	×	×
f_6	✓	✓	✓	×	×

（3）$x+y$的逆元为$-x-y$，xy的逆元为$1/(xy)$。

（4）略

5. 设$G=\{1，2，\cdots，10\}$，问下面定义的运算在G上是否封闭？对于封闭的二元运算，请说明运算*是否满足交换律、结合律，并在存在的情况下求出运算*的单位元、零元和所有可逆元素的逆元。

（1）$x*y=gcd(x，y)$，$gcd(x，y)$是x与y的最大公因数。

（2）$x*y=lcm(x，y)$，$lcm(x，y)$是x与y的最小公倍数。

（3）$x*y=$大于等于x和y的最小整数。

（4）$x*y=$质数p的个数，其中$x\le p\le y$。

解：（1）封闭。因为$\forall x,y\in G$，$gcd(x，y)$为x与y的因数，故$gcd(x，y)\in G$。交换律和结合律都满足。单位元没有，1 是零元。

（2）不封闭。例如，$lcm(2,7)=14$，$14\notin G$。

（3）封闭。交换律和结合律满足。单位元是 1，零元是 10。

（4）不封闭。例如，$8*10=0$，$0\notin G$。

§4.2 半群与群

1. 设G是所有形如

$$\begin{pmatrix} a_{11} & a_{12} \\ 0 & 0 \end{pmatrix}$$

的矩阵组成的集合，*表示矩阵乘法。试问$<G，*>$是半群吗？是有么半群吗？这里a_{11}、a_{12}是实数。

解：任取G的2个元素$A=\begin{pmatrix} a_{11} & a_{12} \\ 0 & 0 \end{pmatrix}$，$B=\begin{pmatrix} b_{11} & b_{12} \\ 0 & 0 \end{pmatrix}$

$$\because \quad A*B=\begin{pmatrix} a_{11} & a_{12} \\ 0 & 0 \end{pmatrix}*\begin{pmatrix} b_{11} & b_{12} \\ 0 & 0 \end{pmatrix}=\begin{pmatrix} a_{11}b_{11} & a_{11}b_{12} \\ 0 & 0 \end{pmatrix}\in G$$

$\therefore$ $<G，*>$是一个代数系统。又因为矩阵的乘法满足结合律，所以$<G，*>$是一个半群。

又因为，只要$a_{11}=1$，则

$$A*B=\begin{pmatrix} a_{11} & a_{12} \\ 0 & 0 \end{pmatrix}*\begin{pmatrix} b_{11} & b_{12} \\ 0 & 0 \end{pmatrix}=\begin{pmatrix} a_{11}b_{11} & a_{11}b_{12} \\ 0 & 0 \end{pmatrix}=\begin{pmatrix} b_{11} & b_{12} \\ 0 & 0 \end{pmatrix}=B,$$

对任何$B\in G$成立，即$\begin{pmatrix} 1 & a_{12} \\ 0 & 0 \end{pmatrix}$是左单位元（不论$a_{12}$取何值）。因此单位元不存在（若单位元则左右单位元都存在且相等还唯一），即$<G，*>$不是有么半群。事实上，右单位元确实不存在，因为不论b_{11},b_{12}取何值

$$A*B=\begin{pmatrix} a_{11} & a_{12} \\ 0 & 0 \end{pmatrix}*\begin{pmatrix} b_{11} & b_{12} \\ 0 & 0 \end{pmatrix}=\begin{pmatrix} a_{11}b_{11} & a_{11}b_{12} \\ 0 & 0 \end{pmatrix}=\begin{pmatrix} a_{11} & a_{11} \\ 0 & 0 \end{pmatrix}=A$$

不可能对任何$A\in G$成立，所以右单位元不存在。

因此单位元不存在$<G，*>$不是有么半群。

2. 在正实数集合$\mathbf{R}^+$上定义运算*如下

$$x*y=\frac{a+b}{1+ab}$$

试问$<\mathbf{R}^+，*>$是半群吗？是有么半群吗？

解： 任取$\mathbf{R}^+$中的3个元素$a,b,c\in\mathbf{R}^+$

$\because\ a*b=\dfrac{a+b}{1+ab}\in R^+$，所以$<\mathbf{R}^+,*>$是一个代数系统。

$$\because\quad (a*b)*c=\frac{a+b}{1+ab}*c=\frac{\dfrac{a+b}{1+ab}+c}{1+\dfrac{a+b}{1+ab}c}=\frac{a+b+c+abc}{1+ab+ac+bc}$$

$$a*(b*c)=a*\frac{b+c}{1+bc}=\frac{a+\dfrac{b+c}{1+bc}}{1+a\dfrac{b+c}{1+bc}}=\frac{a+b+c+abc}{1+ab+ac+bc}$$

$\therefore (a*b)*c=a*(b*c)$，即$<\mathbf{R}^+,*>$是一个半群。

如果存在单位元e，则$\forall x\in R^+$，$e*x=\dfrac{e+x}{1+ex}=x$，可得$e=0\notin R^+$，所以没有单位元，所以不是有幺半群。

3. 对自然数集合$\mathbf{N}$定义运算$\vee$和$\wedge$如下：

$$a\vee b=\max\{a，b\},\qquad a\wedge b=\min\{a，b\}$$

试问$<\mathbf{N},\vee>$和$<\mathbf{N},\wedge>$是半群吗？是有么半群吗？

解：显然都满足运算的封闭性，所以$<\mathbf{N},\vee>$和$<\mathbf{N},\wedge>$都是代数系统。

显然都满足运算的结合律，所以$<\mathbf{N},\vee>$和$<\mathbf{N},\wedge>$都是半群。

$<\mathbf{N},\vee>$有单位元“1”，所以是有么半群。

$<\mathbf{N},\wedge>$没有单位元，所以不是有么半群。

4. 设$<G,*>$是一个半群，它有一个左零元θ，令

$$G_\theta=\{x*\theta\mid x\in G\}$$

证明$<G_\theta,*>$也构成一个半群。

5. 在一个多于一个元素的有么半群中，证明一个右零元不可能有右逆元。

证：有么半群中的么元e显然不可能等于任一个右零元。

设有一个右零元θ_r，它的右逆元为θ_r^{-1}，则$\theta_r^{-1}*\theta_r=e$，因为$\theta_r*\theta_r=\theta_r$，

所以$\theta_r^{-1}*\theta_r*\theta_r=\theta_r^{-1}*\theta_r$，即$e*\theta_r=e$，$\theta_r=e$，导致矛盾，因此一个右零元不可能有右逆元。

6. 设G是一个多于一个元素的集合，G^G是G上所有函数组成的集合，证明有么半群$<G^G,\circ>$有多于一个的右零元，但没有左零元。这里$\circ$表示复合运算。

证： 因G至少含有2个元，不妨设$a,b\in G$，且$a\neq b$，定义如下两个映射$f_1,f_2\in G^G$：

$$f_1(x)=a,\forall x\in G,\qquad f_2(x)=b,\forall x\in G$$

则因为

$$f \circ f_1(x) = f_1(f(x)) = a, \qquad f \circ f_2(x) = f_2(f(x)) = b$$

所以 $f \circ f_1 = f_1$， $f \circ f_2 = f_2$，即 f_1 和 f_2 是 $< G^G, \circ >$ 的右零元，所以说 $< G^G, \circ >$ 有多于一个的右零元。

下面证明无左零元，用反证法，设有左零元 f_0，则 $\forall x \in G$ 有：

$$f_0(x) = f_0 \circ f_1(x) = f_1(f_0(x)) = a$$

$$f_0(x) = f_0 \circ f_2(x) = f_2(f_0(x)) = b$$

这与 $a \neq b$ 矛盾，所以 $< G^G, \circ >$ 无左零元。

7. 设 Z 为整数集合，在 Z 上定义二元运算 * 如下：

$$x * y = x + y - 2, \quad \forall x, \ y \in \mathbf{Z}$$

问 Z 关于 * 运算能否构成群？为什么？

解：易证 Z 关于 * 运算是封闭的，且对任意 $x, y, z \in Z$ 有

$$(x * y) * z = (x + y) - 2 + z - 2 = x + y + z - 4$$

$$x * (y * Z) = x * (y + z - 2) = x + (y + z - 2) - 2 = x + y + z - 4,$$

结合律成立。2 是 * 运算的么元。$\forall x \in Z$， $4 - x$ 是 x 关于 * 运算的逆元。纵上所述，$\langle Z, * \rangle$ 够成群。

8. $G = \{ f(x) = ax + b \mid a \neq 0, \ a, \ b \in \mathbf{R} \}$，证明 $< G, \circ >$ 是一个群，这里 $\circ$ 是复合运算。

证：$\forall a, b, c, d \in R$，且 $a, c \neq 0$，对于任意的 $x \in G$，有

$$(f_{c,d} \circ f_{a,b})(x) = f_{a,b}(cx + d) = a(cx + d) + b = acx + ad + b$$

又 $ac \neq 0, ac, ab + b \in G$，得 $f_{c,d} \circ f_{a,b} = f_{ac, ad+b} \in G$，故运算 $\circ$ 在 G 上是封闭的。

恒等变换 $I = f_{1,0} \in G$，从而 G 有单位元 I。

$\forall f_{a,b} \in G, a \neq 0, a, b \in R$，取 $f_{a^{-1}, -a^{-1}b} \in G$，有

$$f_{a,b} \circ f_{a^{-1}, -a^{-1}b} = f_{aa^{-1}, -aa^{-1}b + b} = f_{1,.0}$$

$$f_{a^{-1},-a^{-1}b} \circ f_{a,b} = f_{a^{-1}a,a^{-1}b-a^{-1}b} = f_{1.,0}$$

故 $f_{a,b}$ 可逆，且 $f_{a,b}^{-1} = f_{a^{-1},-a^{-1}b}$ 。所以$<G, \circ>$是一个群。

9. 设 $G=\{r, 1/r, 1-r, 1/(1-r), (r-1)/r, r/(r-1)\}$，证明$<G, *>$是一个群，这里，运算 $a*b$ 表示将 b 代换到 a 中 r 所在位置。

证：

$*$	r	$\frac{1}{r}$	$1-r$	$\frac{1}{1-r}$	$\frac{r-1}{r}$	$\frac{r}{r-1}$
r	r	$\frac{1}{r}$	$1-r$	$\frac{1}{1-r}$	$\frac{r-1}{r}$	$\frac{r}{r-1}$
$\frac{1}{r}$	$\frac{1}{r}$	r	$\frac{1}{1-r}$	$1-r$	$\frac{r}{r-1}$	$\frac{r-1}{r}$
$1-r$	$1-r$	$\frac{r-1}{r}$	r	$\frac{r}{r-1}$	$\frac{1}{r}$	$\frac{1}{1-r}$
$\frac{1}{1-r}$	$\frac{1}{1-r}$	$\frac{r}{r-1}$	$\frac{1}{r}$	$\frac{r-1}{r}$	r	$1-r$
$\frac{r-1}{r}$	$\frac{r-1}{r}$	$1-r$	$\frac{r}{r-1}$	r	$\frac{1}{1-r}$	$\frac{1}{r}$
$\frac{r}{r-1}$	$\frac{r}{r-1}$	$\frac{1}{1-r}$	$\frac{r-1}{r}$	$\frac{1}{r}$	$1-r$	r

从运算表上可以看出，运算具有封闭性，满足结合律，单位元为 r，每个元都有逆元，所以构成一个群。

10. 设 $A=\{x \mid x \in \mathbf{R} \wedge x \neq 0, 1\}$。在 A 上定义六个函数如下：

$f_1(x)=x$，　　$f_2(x)=x^{-1}$，

$f_3(x)=1-x$，　　$f_4(x)=(1-x)^{-1}$，

$f_5(x)=(x-1)x^{-1}$，　　$f_6(x)=x(x-1)^{-1}$

令 G 为这六个函数构成的集合，$\circ$是复合运算。

（1）给出$<G, \circ>$的运算表。　　（2）验证$<G, \circ>$是一个群。

证：（1）建造如下$<G, \circ>$的运算表

∘	$f_1(x)$	$f_2(x)$	$f_3(x)$	$f_4(x)$	$f_5(x)$	$f_6(x)$
$f_1(x)$	$f_1(x)$	$f_2(x)$	$f_3(x)$	$f_4(x)$	$f_5(x)$	$f_6(x)$
$f_2(x)$	$f_2(x)$	$f_1(x)$	$f_4(x)$	$f_3(x)$	$f_6(x)$	$f_5(x)$
$f_3(x)$	$f_3(x)$	$f_5(x)$	$f_1(x)$	$f_6(x)$	$f_2(x)$	$f_4(x)$
$f_4(x)$	$f_4(x)$	$f_6(x)$	$f_2(x)$	$f_5(x)$	$f_1(x)$	$f_3(x)$
$f_5(x)$	$f_5(x)$	$f_3(x)$	$f_6(x)$	$f_1(x)$	$f_4(x)$	$f_2(x)$
$f_6(x)$	$f_6(x)$	$f_4(x)$	$f_5(x)$	$f_2(x)$	$f_3(x)$	$f_1(x)$

（2）从表上可以看出，函数的复合运算∘在 G 上具有封闭性，有可结合性，有么元 $f_1(x)$，$f_2(x)$的逆元为 $f_2(x)$，$f_3(x)$的逆元为 $f_3(x)$，$f_6(x)$的逆元为 $f_6(x)$，$f_4(x)$与 $f_5(x)$互为逆元。故$<G,\circ>$是一个群。

11. 在群$<\mathbf{R},+>$中计算下列元素的幂：

$0.5^2=?$，　　$0.5^{10}=?$，

$0.5^0=?$，　　$\sqrt{4}^{\,2}=?$，

$\sqrt{4}^{\,10}=?$，　　$\sqrt{4}^{\,0}=?$

解： $0.5^2=1$，　　$0.5^{10}=5$，　　$0.5^0=0$，

$\sqrt{4}^{\,2}=2\sqrt{4}$，　　$\sqrt{4}^{\,10}=10\sqrt{4}$，　　$\sqrt{4}^{\,0}=0$

12　设$<G,*>$是一个群，证明

$$x^m * x^n = x^{m+n},\qquad (x^m)^n = x^{m\times n},\qquad \forall m,\ n\in\mathbf{Z}$$

13. 设$G=\{1,\ 2,\ 3,\ 4,\ 5,\ 6\}$，对于$G$上的二元运算“模 7 乘法$\times_7$”：

$$i\times_7 j=(i\times j)(\mathrm{mod}\ 7)$$

$<G,\times_7>$构成一个群。请

（1）给出$<G,\times_7>$的运算表。　　（2）给出每个元的逆元。

（3）给出每个元的次数。

解：（1）

$\times_7$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	3
4	4	1	5	2	6	3

5	5	3	1	6	4	2
6	6	5	4	3	2	1

（2）逆元： $1^{-1}=1$， $2^{-1}=4$， $3^{-1}=5$， $4^{-1}=2$， $5^{-1}=2$， $6^{-1}=6$。

（3）元素 1，2，3，4，5，6 的次数分别为 1，11，5，2，3，6。

14. 设 $G=\{1,\ 2,\ 4,\ 7,\ 8,\ 11,\ 13,\ 14,\}$，对于 G 上的二元运算“模 15 乘法 $\times_{15}$”：

$$i\times_{15} j=(i\times j)(\mathrm{mod}\,15)$$

$<G,\ \times_{15}>$构成一个群。请

（1）给出$<G,\ \times_{15}>$的运算表。　　（2）给出每个元的逆元。

（3）给出每个元的次数。

解：（1）

$\times_{15}$	1	2	4	7	8	11	13	14
1	1	2	4	7	8	11	13	14
2	2	4	8	14	1	7	11	13
4	4	8	1	13	2	14	7	11
7	7	14	13	4	11	2	1	8
8	8	1	2	11	4	13	14	7
11	11	7	14	2	13	1	8	4
13	13	11	7	1	14	8	2	2
14	14	13	11	9	7	4	2	1

（2）逆元：$1^{-1}=1,\ 2^{-1}=8,\ 4^{-1}=4,\ 7^{-1}=13,\ 8^{-1}=2,\ 11^{-1}=11,\ 13^{-1}=7,\ 14^{-1}=14$

（3）元素 1，2，4，7，8，11，13，14 的次数分别为 1，4，2，4，4，2，4，2。

§4.3　群的性质、循环群

1.　设$<G,\ *>$为群，若$\forall x\in G$有$x^2=e$，证明$<G,\ *>$为交换群。

证：$\forall x\in G$，因为有 $x^2=e$，所以有 $x=x^{-1}$，

因为 $x^2=x*x=x*x^{-1}=x^{-1}*x$，即 $x*x^{-1}=x^{-1}*x$，又因为$<G,\ *>$为群，所以$<G,\ *>$为交换群。

2. 设$<G,\ *>$是群，证明G是交换群的充要条件是$\forall a,\ b\in G$有$(a*b)^2=a^2*b^2$。

证：充分性：

条件已知$(a*b)^2=a^2*b^2$，由于是群，运算满足结合律和消去律，有

$a*(b*a)*b=a*(a*b)*b$ ，故$a*b=b*a$，所以G是交换群。

必要性：

条件已知G是交换群，运算满足结合律和交换律，有

$(a*b)^2=(a*b)*(a*b)=a*(b*a)*b=a*(a*b)*b=(a*a)*(b*b)=a^2*b^2$，

即 $(a*b)^2=a^2*b^2$

证毕。

3. 设$<G,*>$为群，并且对任意的$a,b\in G$都有$(a*b)^3=a^3*b^3$，$(a*b)^5=a^5*b^5$，证明G是交换群。

证：$\forall a,b\in G$

因为$<G,*>$为群，所以运算满足消去律和结合律，又有$(a*b)^5=a^5*b^5$，

所以

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

从左边消去a和右边消去b后可得

$$(b*a)^4=a^4*b^4$$

即$a^4*b^4=(a*b)^4=(a*b)*(a*b)^3=(a*b)*a^3*b^3$

对上式使用消去律，有

$$a^3*b=b*a^3 \qquad (1)$$

$$a^5*b^5=(a*b)^5=(a*b)*(a*b)^5=a*b*a^4*b^4 \qquad (2)$$

由（1）和（2）可推出：

$$a^4*b=a*(a^3*b)=a*(b*a^3)=b*a^4$$

对$a*(a^3*b)=b*a^4$使用消去律，则有$a*b=b*a$。

所以G是交换群。

4. 设$<G,*>$为有限半群，且满足消去律，证明G是群。

证：对于$\forall a\in G$，考虑集合

$$G_a=\{a,a^2,a^3,\cdots,a^m,\cdots\}$$

由封闭性可知$G_a \subseteq G$，又由G的有限性，所以G_a也是有限集。故

必有$n,k>0$，使得

$$a^n = a^{n+k} \quad \text{即} \quad a^n * e = a^n * a^k$$

由消去律可得$a^k = e$，即有

$$a^{k-1} * a = a * a^{k-1} = a^k = e$$

可见，a的逆元$a^{-1} = a^{k-1}$。

因此，$<G,*>$是群。

5. 设$<G,*>$为群，a，b，$c \in G$，证明

$$|a*b*c| = |b*c*a| = |c*a*b|$$

6. 设$<G,*>$是群，a，$b \in G$且$a*b=b*a$。如果$|a|=n$，$|b|=m$且n与m互质，证明$|a*b|=n\times m$。

证：令$|a*b|=d$，由$a*b=b*a$可知

$$(a*b)^{n\times m} = (a^n)^m (b^m)^n = e^m * e^n = e$$

从而有$d \mid n\times m$。

又由$a^d * b^d = (a*b)^d = e$。可知

$$a^d = b^{-d}$$

即$|a^d| = |b^{-d}| = |b^d|$。再根据

$$(a^d)^n = (a^n)^d = e^d = e$$

得$|a^d| \parallel n$。同理有$|b^d| \parallel m$，又$|a^d| = |b^d|$。从而知道$|a^d|$是n和m的公因子。因为n与m互质，

所以$|a^d| = 1$。这就证明了$a^d = e$和$n \mid d$

同理可证$m \mid d$，即d是n和m的公倍数。由于n与m互质，必有$n\times m \mid d$。

综合前边的结果得$d = n\times m$。即$|a*b| = n\times m$。

7. 证明循环群一定是交换群，举例说明交换群不一定是循环群。

证：若$<G,*>$为循环群，则$\exists a \in G$，使得$G = \{a^k \mid k \in Z\}$，

所以$\exists b,c \in G$，使得$b = a^m, c = a^n$，$m,n \in Z$

所以$b*c = a^m * a^n = a^{m+n} = a^{n+m} = a^n * a^m = c*b$，即$<G,*>$满足交换律，也即

$<G,*>$是交换群。

不是所有的交换群都是循环群，例如：Klein 四元群是交换群，但不是循环群。

8. 证明由 1 的n次复根的全体所组成的集合与复数的乘法构成一个n阶循环群。

证：由代数的知识可知，1 的n次复根的全体所组成的集合为

$$G=\{e^{\frac{2k\pi}{n}i}\mid k=0,1,2,\cdots,n-1\}$$

$\forall e^{\frac{2p\pi}{n}i},e^{\frac{2q\pi}{n}i}\in G,p,q\in\{0,1,2,\cdots,n-1\}$，$e^{\frac{2p\pi}{n}i}\times e^{\frac{2q\pi}{n}i}=e^{\frac{2(p+q)\pi}{n}i}$

若$p+q<n$，则$e^{\frac{2(p+q)\pi}{n}i}\in G$；

若$p+q>=n$，则存在$k\in\{0,1,2,\cdots,n-1\}$，使得$p+q=n+k$，而

$e^{\frac{2(p+q)\pi}{n}i}=e^{\frac{2(n+k)\pi}{n}i}=e^{\frac{2k\pi}{n}i}\in G$。因此$G$关于数的乘法是封闭的。数的乘法运算满足结合律，$1=e^{\frac{2\times0\times\pi}{n}i}$是$G$的么元，因为$\forall e^{\frac{2k\pi}{n}i}\in G$，

$1\times e^{\frac{2k\pi}{n}i}=e^{\frac{2k\pi}{n}i}\times1=e^{\frac{2(k+0)\pi}{n}i}=e^{\frac{2k\pi}{n}i}$。 $\forall e^{\frac{2k\pi}{n}i}\in G$，都存在$e^{\frac{2(n-k)\pi}{n}i}\in G$，使得$e^{\frac{2k\pi}{n}i}\times e^{\frac{2(n-k)\pi}{n}i}=e^{\frac{2(n-k)\pi}{n}i}\times e^{\frac{2k\pi}{n}i}=e^{2\pi i}=e^{0\pi i}=e^{\frac{2\times0\times\pi}{n}i}$，所以$e^{\frac{2k\pi}{n}i}$的逆元存在。故$<G,\times>$是一个群。$e^{\frac{2\pi}{n}i}\in G$，都有$e^{\frac{2k\pi}{n}i}=[e^{\frac{2\pi}{n}i}]^k$，故$e^{\frac{2\pi}{n}i}$是群$G$的一个生成元，因此$G$是循环群。

9. 阶数为 5、6、14、15 的循环群的生成元分别有多少个？

解： 设a是阶数为 5 的循环群的生成元，则因在比 5 小的正整数中有且仅有2，3，4 与 5 互质，所以a^2， a^3， a^4也是生成元，因此生成元个数为 4。

设a是阶数为 6 的循环群的生成元，则因在比 6 小的正整数中有且仅有 5 与 6 互质，所以a^5也是生成元，因此生成元个数为 2。

设a是阶数为 14 的循环群的生成元，则因在比 14 小的正整数中有且仅有 3，5，9，11，13 与 14 互质，所以a^3， a^5， a^9 a^{11} a^{13}也是生成元，因此生成元个数为 6。

设a是阶数为 15 的循环群的生成元，则因在比 15 小的正整数中有且仅有 2，4，8，11，13，14 与 15 互质，所以a^2， a^4， a^8 a^{11} a^{13} a^{14}也是生成元，因此生成元个数为 7。

10. 设$G=\{1，5，7，11\}$，对于G上的二元运算“模 12 乘法$\times_{12}$”：

$$i\times_{12}j=(i\times j)(\mathrm{mod}\,12)$$

（1）证明$<G，\times_{12}>$构成一个群。 （2）求G中每个元素的次数。

（3）$<G，\times_{12}>$是循环群吗？

（1）**证**：$\forall i,j,k\in G$，

$$(i\times_{12}j)\times_{12}k=(i\times j)(\mathrm{mod}12)\times_{12}k=(i\times j\times k)(\mathrm{mod}12)$$

$$i\times_{12}(j\times_{12}k)=i\times_{12}((j\times k)(\mathrm{mod}12))=(i\times j\times k)(\mathrm{mod}12)$$

所以 $(i\times_{12} j)\times_{12} k = i\times_{12}(j\times_{12} k)$

即 $\times_{12}$ 满足结合律。

又由下表

$\times_{12}$	**1**	**5**	**7**	**11**
1	**1**	**5**	**7**	**11**
5	**5**	**1**	**11**	**7**
7	**7**	**11**	**1**	**5**
11	**11**	**7**	**5**	**1**

得单位元 1，$1\in G$，

而且每个元素都存在逆元，$1^{-1}=1$，$5^{-1}=5$，$7^{-1}=7$，$11^{-1}=11$，

综上可知 $<G, \times_{12}>$ 构成一个群。

(2) 1,5,7,11 的次数分别为 1，5，7，11。

(3)

§4.4 子群、置换群

1. 给出群 $<\mathbf{Z}_8, +_8>$ 的全部子群。

解：群 $<\mathbf{Z}_8, +_8>$ 的平凡子群两个：$<\{[0]\}, +_8>$ 和 $<\mathbf{Z}_8, +_8>$

非平凡子群两个：$<\{[0],[2],[4],[6]\}, +_8>$

$<\{[0],[4]\}, +_8>$

子群 $\{[0]\}$ 的左陪集有 8 个：

$\{[0]\}$，$\{[1]\}$，$\{[2]\}$，$\{[3]\}$，$\{[4]\}$，$\{[5]\}$，$\{[6]\}$，$\{[7]\}$

这 8 个左陪集构成了 Z_8 的一个划分。

子群 Z_8 的左陪集有 1 个：Z_8

这 1 个左陪集构成了 Z_8 的一个划分。

子群 $\{[0],\ [2],\ [4],\ [6]\}$ 的左陪集有 2 个：

$\{[0],\ [2],\ [4],\ [6]\}$，$\{[1],\ [3],\ [5],\ [7]\}$

这 2 个左陪集构成了 Z_8 的一个划分。

子群 $\{[0],\ [4]\}$ 的左陪集有 4 个：

$\{[0],\ [4]\}$，$\{[1],\ [5]\}$，$\{[2],\ [6]\}$，$\{[3],\ [7]\}$

这 4 个左陪集也构成了 Z_8 的一个划分。

2. 设$G=\{1，5，7，11\}$，对G上的二元运算“模12乘法$\times_{12}$”：

$$i\times_{12} j=(i\times j)(\mathrm{mod}\,12)$$

$<G，\times_{12}>$构成一个群，请求出$<G，\times_{12}>$的所有子群。

3. 设$<G，*>$是群，H是其子群，任给$a\in H$，令

$$aHa=\{a*h*a^{-1}\mid h\in H\}$$

证明aHa^{-1}是G的子群（称为H的**共轭子群**）

证：由于H非空，可知aHa^{-1}非空。

$\forall b,c\in aHa^{-1}$，即存在$h_1,h_2\in H$使得$b=ah_1a^{-1},c=ah_2a^{-1}$，有

$$bc^{-1}=(ah_1a^{-1})(ah_2a^{-1})^{-1}=ah_1a^{-1}(a^{-1})^{-1}h_2a^{-1}=a(h_1h_2^{-1})a^{-1}$$

因为H为子群，有$h_1h_2^{-1}\underline{\Delta}h\in H$，从而$bc^{-1}=aha^{-1}\in aHa^{-1}$。

所以aHa^{-1}是G的子群。

4. 设$<G，*>$是群，H和K是其子群，证明HK和KH是$<G，*>$的子群当且仅当$HK=KH$，其中

$$HK=\{h*k\mid h\in H\wedge k\in K\},\qquad KH=\{k*h\mid k\in K\wedge h\in H\}$$

证：（1）充分性。假设$HK=KH$，需要证明HK是子群。因$e\in H,e\in K$，故$e=ee\in HK$，从而HK非空。$\forall x=hk,y=h_1k_1\in HK$，这里$h,h_1\in H,k,k_1\in K$，有

$$xy^{-1}=(hk)(h_1k_1)^{-1}=h(kk_1^{-1})h_1^{-1}，\text{记}\ k_2=kk_1^{-1}\in K$$

由$HK=KH$可知，$\exists h_3\in H,k_3\in K$，使得$k_2h_1^{-1}=h_3k_3$，从而

$$xy^{-1}=h(h_3k_3)=(hh_3)k_3\in HK$$

由子群的判定定理，HK是$<G，*>$的子群。

（2）必要性。已知HK是$<G，*>$的子群，需要证明$HK=KH$。

对于$\forall x\in HK$，因HK是子群，故$x^{-1}\in HK$。于是$\exists h\in H,k\in K$，使得$x^{-1}=hk$，从而$x=k^{-1}h^{-1}$。因$k^{-1}\in K,h^{-1}\in H$，故$x=KH$。证得$HK\subseteq KH$。

同理可证$KH\subseteq HK$。

从而有$HK=KH$。

故HK是$<G，*>$的子群当且仅当$HK=KH$。

同理可证KH是$<G，*>$的子群当且仅当$HK=KH$。

5. 设$<G，*>$是群，H是G的子集，证明H是G的子群当且仅当$H^2=H，H^{-1}=H$，这里

$$H^2=\{h_1*h_2\mid h_1，h_2\in H\},\quad H^{-1}=\{h^{-1}\mid h\in H\}$$

证：（1）根据H^2，H^{-1}的定义：

$$H^2=\{h_1*h_2\mid h_1,\ h_2\in H\},\quad H^{-1}=\{h^{-1}\mid h\in H\}$$

因为H是G的子集，所以显然有：$H^2\subseteq H, H^{-1}\subseteq H$。又因为$H$中任意元素$h$可以写成$e*h$，所以$H\subseteq H^2$，还因为$H$中任意元素$h$可以写成$(h^{-1})^{-1}$，所以$H\subseteq H^{-1}$，因此

$$H^2=H,\ H^{-1}=H$$

（2）$\forall h_1, h_2\in H$，因为$H^2=H,\ H^{-1}=H$，所以

$$h_1*h_2^{-1}=h_1*h_3=h_4\in H$$

由子群的判定定理知，H是G的子集。

6. 某一通讯编码的码字$x=(x_1,\ x_2,\ \cdots,\ x_7)$，其中$x_1$，$x_2$，$x_3$和$x_4$为数据位，$x_5$，$x_6$和$x_7$为校验位（$x_1$，$x_2$，$\cdots$，$x_7$都是0或1），并且满足

$$x_5=x_1+_2x_2+_2x_3,\quad x_6=x_1+_2x_2+_2x_4,\quad x_7=x_1+_2x_3+_2x_4$$

这里$+_2$是模2加法。设H是所有这样的码字构成的集合。在H上定义二元运算如下：

$$\forall x,\ y\in H,\ x*y=(x_1+_2y_1,\ x_2+_2y_2,\ \cdots,\ x_7+_2y_7)$$

证明$<H,*>$构成一个群，且是$<G,*>$的子群，其中G是长度为7的位串构成的集合。

7. 设H和K分别是群$<G,*>$的r，s阶子群，若r，s互质，证明$H\bigcap K=\{e\}$。

证：假设不然，则存在$x\in H\bigcap K$，且$x\neq e$。于是x也是H的生成元，从而$(x)=H\subseteq K$，所以与r，s互质矛盾。

8. 设$G=<a>$是循环群，$H=<a^s>$和$K=<a^t>$是它的两个子群。证明$H\bigcap K=<a^u>$，这里$u=\gcd(s,\ t)$是s和t的最小公倍数。

9. 设5阶置换为

$$\alpha=\begin{pmatrix}1&2&3&4&5\\2&3&1&5&4\end{pmatrix},\qquad \beta=\begin{pmatrix}1&2&3&4&5\\1&3&4&5&2\end{pmatrix}$$

计算$\alpha\beta$，$\beta\alpha$，α^{-1}，$\alpha^{-1}\beta\alpha$，$\beta^{-1}\alpha\beta$。

解：

$$\alpha\beta=\begin{pmatrix}1&2&3&4&5\\3&4&1&2&5\end{pmatrix}$$

$$\beta\alpha=\begin{pmatrix}1&2&3&4&5\\2&1&5&4&3\end{pmatrix}$$

$$\alpha^{-1}=\begin{pmatrix}1&2&3&4&5\\3&1&2&5&4\end{pmatrix}$$

$$\alpha^{-1}\beta\alpha=\begin{pmatrix}1&2&3&4&5\\5&2&1&3&4\end{pmatrix}$$

$$\beta^{-1}\alpha\beta=\begin{pmatrix}1&2&3&4&5\\3&5&4&1&2\end{pmatrix}$$

10. 设$S=\{1,\ 2,\ 3,\ 4\}$，写出S上的所有4元置换。

11. 列出 4 元对称群$<S_4,\circ>$的运算表，求出单位元，每个元的逆元，每个元的次数以及它的所有子群。

§4.5 陪集与商群

习题 4.5

1. 集合$\mathbf{Z}_{20}=\{0,\ 1,\ 2,\ \cdots,\ 19\}$在“模 20 加法$+_{20}$”下构成一个群。设$H$是由 5 生成的$\mathbf{Z}_{20}$的一个子群。

（1）求出H的每个元素及其次数。　　（2）求H在$\mathbf{Z}_{20}$中的所有左陪集。

2. 求 12 阶循环群$G=\{e,\ a,\ a^2,\ a^3,\ a^4,\ \cdots,\ a^{11}\}$的子群$H=\{e,\ a^4,\ a^8\}$在$G$中的所有左陪集。

证：$H=eH$是一个左陪集；取$c\in G$且$c\notin H$,则$cH=\{c,c^5,c^9\}$又是一个左陪集；取不属于$H\bigcup cH$的G中的元素，如c^2，则$c^2H=\{c^2,c^6,c^{10}\}$又是左陪集；取不属于$H\bigcup cH\bigcup c^2H$在G中元素，如c^3，则$c^3H=\{c^3,c^7,c^{11}\}$又是左陪集。于是$G=H\bigcup cH\bigcup c^2H\bigcup c^3H$，即$H$在$G$中的所有左陪集有$H,cH,c^2H,c^3H$。

3. 设H是群$<G,\ *>$的子群，证明H的所有不同左陪集（右陪集）中有且仅又一个在$*$下构成$<G,\ *>$的子群。

证：设G中的么元为e。因为$eH=H$，所以H是一个陪集。

若另一个陪集aH也是G的子群，那么$e\in aH$，故必有$h_1\in H$，使得$a*h_1=e$，即有$a=h_1^{-1}$。对于$\forall a*h\in aH$，有$a*h=h_1^{-1}*h\in H$，所以$aH\subseteq H$；反之，对于$\forall h\in H$，有

$$h=a*a^{-1}*h=a*(a^{-1}*h)=a*((h_1^{-1})^{-1}*h)=a*(h_1*h)\in aH$$

因此，$aH\subseteq H$。这就表明左陪集只有一个是子群，即H本身。

同理可证右陪集只有一个是子群，即H本身。

4. 证明 6 阶群必含有 3 次元。

证：设G是6阶群。根据推论1，G中只可能存在1阶，2阶，3阶和6阶元。

若G含有6阶元，比如说是a，则a^2就是G中的3阶元。

若G中不含有6阶元，则G中的非单位元只可能为2阶或3阶元。下面用反证法证明G中必含有3阶元。若不然，则G中的所有元素a都满足$a^2=e$，即$a=a^{-1}$。任取$a,b\in G$，则有

$$ab=(ab)^{-1}=b^{-1}a^{-1}=ba。$$

所以G是交换群。取G中非单位元a和b，令$H=\{e,a,b,ab\}$，易证H是G的子群。

但$|H|\nmid|G|$，与拉格朗日定理矛盾。

5. 证明偶数阶群必含2次元。

证：由下一题（第6题）可知有限群中，周期大于2的元素的个数是偶数。群的么元周期为1，群的阶又是偶数，因此，至少存在一个周期为2的元素。

6. 证明在有限群中次数大于2的元素的个数必定是偶数。

证：有限群为G，e为其么元，$a,b,c\in G$，对$\forall k\in Z$，$a^k=e$，则$(a^{-1})^k=e$，

由此可知a的是无限的当且仅当a^{-1}的周期是无限的。又可知，若a的周期为n，a^{-1}的周期为m，由定理得，$m|n,n|m$，所以，$n=m$。如果b的周期大于2的元素，则$b^{-1}\neq b$，因为如果$b^{-1}=b$，从而$b^2=e$，这与b的周期大于2矛盾。由于群的元素的逆元是唯一的，故不同的元素有不同的逆元。因此，周期大于2的元素与它的逆元成对出现，所以有限群中，次数大于2的元素的个数是偶数。

7. 设$<G,*>$是一个阶数为p的有限群，其中p是质数，证明G是循环群并求它的所有子群。

证：由$p\geq 2$，G中必存在$a\in G,a\neq e$。令$H=<a>$，则H是G的子群，根据拉格朗日定理$|H|=1$或$|H|=p$。

若$|H|=1$，则$|a|=|H|=1$，与$a\neq e$矛盾，所以$|H|=p$。又由于$|G|=p$，必有$H=G$，G是循环群。

下略。

8. 证明循环群的子群仍是循环群。

证：设循环群$G=(a)$，a是生成元。H是G的子群。当$H=\{e\}$时，H是循环群。

设$H\neq\{e\}$。注意到$a^n\in H\Leftrightarrow a^{-n}\in H$，又知$\{n|n\in Z^+,a^n\in H\}$非空，故可令

$$k=\min\{n|n\in Z^+,a^n\in H\}$$

下面证明$H=(a^k)$。

首先，$a^k \in H$，则有$(a^k) \subseteq H$。

其次，对于任一$a^n \in H$，设$n=sk+l, 0 \le l \le k$。于是

$$a^l = a^{n-sk} = a^n (a^k)^{-s}$$

又因

$$a^n, a^k \in H \Rightarrow a^l \in H$$

根据k的定义，必有$l=0$。证得$k \mid n \Rightarrow a^n \in (a^k)$。从而$H \subseteq (a^k)$，故有$H=(a^k)$。故$H$为循环群。所以循环群的子群仍是循环群。

9. 设i为虚数单位，即$i^2=-1$，令

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

则G与矩阵乘法构成群$<G, \times>$，请

（1）给出G的运算表。　　（2）试找出G的所有子群。

（3）证明G的所有子群都是正规子群。

解： （1）略

（2）它的子群除了两个平凡群外还有：

$$H_1=\left\{\pm\begin{pmatrix}1&0\\0&1\end{pmatrix}\right\};$$

$$H_2=\left\{\pm\begin{pmatrix}1&0\\0&1\end{pmatrix}, \pm\begin{pmatrix}i&0\\0&-i\end{pmatrix}\right\}$$

$$H_3=\left\{\pm\begin{pmatrix}1&0\\0&1\end{pmatrix}, \pm\begin{pmatrix}0&i\\i&0\end{pmatrix}\right\}$$

$$H_4=\left\{\pm\begin{pmatrix}1&0\\0&1\end{pmatrix}, \pm\begin{pmatrix}0&1\\-1&0\end{pmatrix}\right\}$$

（3）尽管G不是交换群，因为

$$\begin{pmatrix}i&0\\0&-i\end{pmatrix}\begin{pmatrix}0&1\\-1&0\end{pmatrix}=\begin{pmatrix}0&i\\i&0\end{pmatrix},$$

$$\begin{pmatrix}0&1\\-1&0\end{pmatrix}\begin{pmatrix}i&0\\0&-i\end{pmatrix}=\begin{pmatrix}0&-i\\-i&0\end{pmatrix}$$

单它的所有子群都是正规子

10. 设$<G,*>$是群，H和K是其子群，若H或K是正规子群，则$HK=KH$，其中

$$HK=\{h*k\mid h\in H\wedge k\in K\},\qquad KH=\{k*h\mid k\in K\wedge h\in H\}$$

证：不妨假设H为正规子群。

对于$h*k\in HK,h\in H,k\in K$，因为H是正规子群，所以必存在$h_1\in H$使得

$$k^{-1}*h*k=h_1$$，于是就有

$$h*k=k*k^{-1}*h*k=k*h_1\in KH$$

故有$HK\subseteq KH$。

同理可证$KH\subseteq HK$。

因此，$HK=KH$。

11. 设$<G,*>$是群，H是其子群，证明H是正规子群当且仅当对任意的$a\in G$，都有$aHa^{-1}=H$。

证：若H是正规子群，则$aH=Ha,\forall a\in G$。有$aHa^{-1}=H$，则

$$\forall h\in H,aha^{-1}\in H$$

若对于$\forall a\in G,h\in H$，$aha^{-1}\in H$，则有$aHa^{-1}\subseteq H$。

另一方面，对于$\forall h\in H$，有

$$h=a(a^{-1}ha)a^{-1}$$

其中$a\in G$，从而$a^{-1}\in G$，根据条件有$a^{-1}ha\in H$，从而

$$h=a(a^{-1}ha)a^{-1}\in aHa^{-1}$$

有$H\subseteq aHa^{-1}$。证得$aHa^{-1}=H$。H是正规子群。

12. 令$G=<\mathbf{Z},+>$是整数加群。求商群$\mathbf{Z}/4\mathbf{Z}$，$\mathbf{Z}/12\mathbf{Z}$和$4\mathbf{Z}/12\mathbf{Z}$，其中，集合$4\mathbf{Z}=\{4\times z\mid z\in\mathbf{Z}\}$，$12\mathbf{Z}=\{12\times z\mid z\in\mathbf{Z}\}$。

解：$4\mathbf{Z}$是$\mathbf{Z}$的正规子群，左陪集有4个：$\{4\times z\mid z\in\mathbf{Z}\}$，$\{4\times z+1\mid z\in\mathbf{Z}\}$，$\{4\times z+2\mid z\in\mathbf{Z}\}$，$\{4\times z+3\mid z\in\mathbf{Z}\}$，所以

$$\mathbf{Z}/4\mathbf{Z}=\{\{4\times z\mid z\in\mathbf{Z}\},\{4\times z+1\mid z\in\mathbf{Z}\},\{4\times z+2\mid z\in\mathbf{Z}\},\{4\times z+3\mid z\in\mathbf{Z}\}\}$$

$12\mathbf{Z}$是$4\mathbf{Z}$的正规子群，左陪集有：

$$0(12Z)=\{12\times z\mid z\in\mathbf{Z}\},4(12Z)=\{12\times z+4\mid z\in\mathbf{Z}\},8(12Z)=\{12\times z+8\mid z\in\mathbf{Z}\},$$

所以$4\mathbf{Z}/12\mathbf{Z}=\{0(12Z),4(12Z),8(12Z)\}$

§4.6 同态与同构

习题 4.6

1. 对以下各小题给定的群G_1和G_2以及φ，说明φ是否为群G_1到G_2的同态。如果是，说明是否为单同态，满同态和同构，并求同态像$\varphi(G_1)$和同态核$\ker(\varphi)$。

（1）$G_1=<\mathbf{Z},+>$，$G_2=<\mathbf{R}^*,\times>$，其中$\mathbf{R}^*$为非零实数的集合，＋和×分别表示数的加法和乘法。

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

（2）$G_1=<\mathbf{Z},+>$，$G_2=<A,\times>$，其中$A=\{x\mid x\in\mathbf{C}\wedge|x|=1\}$，$\mathbf{C}$为复数集合，＋和×分别表示数的加法和乘法。

$$\varphi:\ \mathbf{Z}\to A,\ \ \varphi(x)=\cos x+i\sin x$$

（3）$G_1=<\mathbf{R},+>$，$G_2=<A,\times>$，其中A，＋和×的定义同（2）。

$$\varphi:\ \mathbf{R}\to A,\ \ \varphi(x)=\cos x+i\sin x$$

2. $<\mathbf{Z},\times>$，$<A,\times>$都是有么半群，其中$A=\{0,\ 1\}$，×表示数的乘法。

$$\varphi:\ \mathbf{Z}\to A,\ \ \varphi(x)=\begin{cases}1 & \text{当}x=2^k(k\in\mathbf{N})\text{时}\\ 0 & \text{其它情况}\end{cases}$$

证明φ是从$\mathbf{Z}$到A的同态映射。

证：显然φ是从$\mathbf{Z}$到A的映射，$\forall x,y\in Z$，下面分两种情况讨论：

（1）当$x=2^m,y=2^n(m,n\in N)$时，有$\varphi(x)=1,\varphi(y)=1$，于是

$$\varphi(x\times y)=1=1\times1=\varphi(x)\times\varphi(y)。$$

（2）当x,y至少有一个不能表示为$2^k(k\in N)$时，$x\times y$就不能表示为$2^k(k\in N)$的形式，$\varphi(x),\varphi(y)$至少有一个为0，于是

$$\varphi(x\times y)=0=\varphi(x)\times\varphi(y)。$$

因此，$\forall x,y\in Z$，$\varphi(x\times y)=\varphi(x)\times\varphi(y)$，即$\varphi$是从$\mathbf{Z}$到$A$的同态映射。

3. $<\mathbf{R},+>$，$<\mathbf{R},\times>$都是有么半群，＋和×分别表示数的加法和乘法。

$$\varphi:\ \mathbf{R}\to\mathbf{R},\ \ \varphi(x)=10^x$$

证明φ是从$<\mathbf{R},+>$到$<\mathbf{R},\times>$的单同态，但不是同构。

证：对$\forall x,y\in R$，有$\varphi(x+y)=10^{x+y}=10^x\times10^y=\varphi(x)\times\varphi(y)$，

所以φ是$<\mathbf{R},+>$到$<\mathbf{R},\times>$的同态映射。

对$\forall x,y\in R$，若$x\neq y$，显然有$10^x\neq 10^y$，即$\varphi(x)\neq\varphi(y)$，

从而φ是R上的单射；然而对$-1\in R$，不存在满足$\varphi(x)=-1$的$x\in R$，

从而φ不是R上的满射；因此φ不是R的双射。

故，φ是从$<\mathbf{R},+>$到$<\mathbf{R},\times>$的单同态，但不是同构。

4. $<\mathbf{Z},+>$是整数加法群，$<G,*>$是任意一个群，对于G中的任一固定元素a，令$g(n)=a^n(n\in\mathbf{Z})$，证明g是从$\mathbf{Z}$到G的同态映射，并求同态核。

5. $<\mathbf{R},+>$是实数加法群，$<\mathbf{C}_1,\times>$是模为1的复数对于乘法运算的群，这两个群同态吗？同构吗？请说明理由。

6. $<\mathbf{Z}^+,+>$和$<\mathbf{Z}^+,\times>$分别是正整数对于加法和乘法构成的半群，问从$<\mathbf{Z}^+,+>$到$<\mathbf{Z}^+,\times>$，和从$<\mathbf{Z}^+,\times>$到$<\mathbf{Z}^+,+>$都存在同态映射吗？说明理由。

7. 设f是从群$<G,*>$到群$<H,\bullet>$的同态映射，g是从群$<H,\bullet>$到群$<K,\Diamond>$的同态映射，证明复合函数$f\circ g$是从群$<G,*>$到群$<K,\Diamond>$的同态映射。

8. 设$<G,*>$、$<H,\bullet>$是代数系统，$*,\bullet$都是二元运算，ϕ是从G到H的同态映射，则

（1）$\bullet$是$\phi(G)$上的运算，即$<\varphi(G),\bullet>$是代数系统。

（2）如果$*$在G上满足交换律，则$\bullet$在$\phi(G)$上也满足交换律。

（3）如果$*$在G上满足结合律，则$\bullet$在$\phi(G)$上也满足结合律。

（4）如果$*$在G上满足等幂律，则$\bullet$在$\phi(G)$上也满足等幂律。

（5）如果θ是$<G,*>$的零元，则$\phi(\theta)$是$<\varphi(G),\bullet>$的零元。

9. 设$<G,*,*'>$、$<H,\bullet,\bullet'>$是代数系统，$*,*',\bullet,\bullet'$都是二元运算，ϕ是从G到H的同态映射，证明如果在G上，$*$和$*'$满足吸收律，则在$\phi(G)$上，$\bullet$和$\bullet'$也满足吸收律。

10. 设$<G,*>$是一个群，定义映射φ：$G\to G$为$\varphi(x)=x^{-1}$，证明φ是G的自同构当且仅当G是交换群。

11. 设φ是从群$<G,*>$到群$<H,\bullet>$的同态映射，证明若G是循环群，则$\varphi(G)$也是循环群。

证：因为G是循环群，于是对于$\forall a^n,a^m\in G$，都有

$$\varphi(a^n\bullet a^m)=\varphi(a^n)*\varphi(a^m)$$

对于$n=1$时，有$\varphi(a)=\varphi(a)$。

对于$n=2$时，有$\varphi(a^2)=\varphi(a\bullet a)=\varphi(a)*\varphi(a)=\varphi(a)^2$。

若$n=k-1$时，有$\varphi(a^{k-1})=\varphi(a)^{k-1}$，那么，对$n=k$时有

$$\varphi(a^k)=\varphi(a^{k-1}\bullet a)=\varphi(a^{k-1})*\varphi(a)=\varphi(a)^{k-1}*\varphi(a)=\varphi(a)^k$$

这表明，$\varphi(G)$中的每一个元素都可以表示为$\varphi(a)^n$，所以$\varphi(G)$是以生成元为$\varphi(a)$的循环群。

12. 设$<G,*>$和$<H,\bullet>$分别是m阶群和n阶群，若从G到H存在单同态，证明$m|n$，即m是n的因子。

证：设g是群G到H的单一同态，则g的同态象$g(G)$是H的子群，显然g是G到$g(G)$的双射，于是$g(G)$是一个m阶群，由拉格朗日定理可知，$m|n$。

13. 设φ是从群$<G,*>$到群$<H,\bullet>$的同态映射，对任意的$a\in G$，记$b=\varphi(a)$，试问b和a的次数是否一定相同？如果不同，它们之间有何关系？

14. 给出群$<\mathbf{Z}_6,+_6>$的全部自同态。

解：若f是一个自同态映射，则$\forall[x],[y]\in Z_6$，有：

$$f([x]+_6[y])=f([x])+_6\ f([y]) \qquad (1)$$

$$f([x]\times_6[y])=f([x])\times_6\ f([y]) \qquad (2)$$

（1） 令$[x]=[y]=[0]$，则由(1)式可得：$f([0])=f([0])+_6\ f([0])$，因为$<\mathbf{Z}_6,+_6>$是群，所以消去律成立，所以有$f([0])=[0]$。

（2） 令$[x]=[y]=[1]$，记$[a]=f([1])$则由2式得：$[a]=[a^2]$，

即$a^2=6k+a,k\geq 0$为整数。

$a=0$ ：即$f([1])=[0]$，再加上（1）式，推出：$f([x])=[0],x=1,2,3,4,5$；

$a=1$ ：即$f([1])=[1]$，再加上（1）式，推出：$f([x])=[x],x=1,2,3,4,5$；

$a=2$ ：推出$k=1/3$与k是整数矛盾；

$a=3$ ：即$f([1])=[3]$，再加上（1）式，推出：$f([1])=[3]$，$f([2])=[0]$

$f([3])=[3]$，$f([4])=[0]$，$f([5])=[3]$；

$a=4$ ：即$f([1])=[4]$，再加上（1）式，推出：$f([1])=[4]$，$f([2])=[2]$

$f([3])=[0]$，$f([4])=[4]$，$f([5])=[2]$；

$a=5$ ：推出$k=10/3$与k是整数矛盾；

由上面的（1）和（2），我们得到如下4个自同态映射：

$f([x])=[0],\forall[x]\in Z_6$

$f([x])=[x],\forall[x]\in Z_6$

$f([0])=[0]$，$f([1])=[3]$，$f([2])=[0]$ ，$f([3])=[3]$，$f([4])=[0]$，$f([5])=[3]$

$f([0])=[0]$，$f([1])=[4]$，$f([2])=[2]$ ，$f([3])=[0]$，$f([4])=[4]$，$f([5])=[2]$

§4.7 环与域

习题 4.7

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

2. 设 $f(x)=a_0+a_1x+a_2x^2+\cdots+a_nx^n$，$a_1$，$a_2$，…，$a_n$ 为实数，称 $f(x)$ 为实数域上的 n 次多项式，令

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

证明 A 关于多项式的加法和乘法构成环，称为**实数域上的多项式环**。

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

（1）$A=\{a+bi \mid a，\ b\in \mathbf{Q}，\ i^2=-1\}$，运算为复数的加法和乘法。

（2）$A=\{2z+1 \mid z\in \mathbf{Z}\}$，运算为实数的加法和乘法。

（3）$A=\{2z \mid z\in \mathbf{Z}\}$，运算为实数的加法和乘法。

（4）$A=\{x \mid x\geq 0\wedge x\in \mathbf{Z}\}$，运算为实数的加法和乘法。

（5）$A=\{a+b\sqrt[4]{5} \mid a，\ b\in \mathbf{Q}\}$，运算为实数的加法和乘法。

4. 设 $<R,+,\times>$ 是环，证明

（1）$\forall a\in R，\ a0=0a=0$

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

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

5. 设 $<R,+,\times>$ 是环，令

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

C 称作环 R 的**中心**，证明 C 是 R 的子环。

6. 设 a 和 b 是含么环中的两个逆元，证明：

（1）$-a$ 也是可逆元，且 $(-a)^{-1}=-a^{-1}$

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

7. 在域 $<\mathbf{Z}_5,+_5,\times_5>$ 中解下列方程和方程组：

（1）$3x=2$

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

8. 类似于子环，给出**子整环**和**子域的**定义。