本章教材习题全解

5－1　习题

1. 设集合 $A = \{1,2,3,\cdots,10\}$，问下面定义的二元运算 $*$ 关于集合 A 是否封闭？

a) $x * y = \max(x,y)$。

b) $x * y = \min(x,y)$。

c) $x * y = \mathrm{GCD}(x,y)$。

d) $x * y = \mathrm{LCM}(x,y)$。

e) $x * y =$ 质数 p 的个数，使得 $x \leqslant p \leqslant y$。

解：a) 封闭。b) 封闭。c) 封闭。d) 不封闭。例 $\mathrm{LCM}(3,6) = 18$。e) 不封闭，例 $6 * 6 = 0$。

2. 在表 5－7 所列出的集合和运算中，请根据运算的是否封闭，在相应的位置上填写“是”或“否”（其中 N 是自然数集合，I 是整数集合）。

表 5－7

是否封闭 / 集合	运算					
	$+$	$-$	$\lvert x-y \rvert$	max	min	$\lvert x \rvert$
I						
N						
$\{x \mid 0 \leqslant x \leqslant 10\}$						
$\{x \mid -10 \leqslant x \leqslant 10\}$						
$\{2x \mid x \in I\}$						

解:见表 5－8 所示。

表 5－8

是否封闭 / 集合	运算					
	+	－	$\vert x-y\vert$	max	min	$\vert x\vert$
I	是	是	是	是	是	是
N	是	否	是	是	是	是
$\{x \mid 0 \leqslant x \leqslant 10\}$	否	否	是	是	是	是
$\{x \mid -10 \leqslant x \leqslant 10\}$	否	否	否	是	是	是
$\{2x \mid x \in I\}$	是	是	是	是	是	是

3. 试列举你所熟悉的一些代数系统。

解:例如复数集合及其加法和复数乘法构成的代数系统$\langle C,+,\cdot\rangle$,整数集合 I 以及在该集合上的加法、乘法构成的代数系统$\langle I,+,\cdot\rangle$等。

5－2 习题

1. 对于实数集合 R,表 5－9 所列的二元运算是否具有左边一列中的那些性质,请在相应的位置上填写“是”或“否”。

表 5－9

	+	－	$\cdot$	max	min	$\vert x-y\vert$
可结合性						
可交换性						
存在幺元						
存在零元						

解:见表 5－10 所示。

表 5－10

	+	－	$\cdot$	max	min	$\vert x-y\vert$
可结合性	是	否	是	是	是	否
可交换性	是	否	是	是	是	是
存在幺元	是	否	是	否	否	否
存在零元	否	否	是	否	否	否

2. 设代数系统$\langle A,*\rangle$,其中$A=\{a,b,c\}$,$*$ 是 A 上的一个二元运算。对于由以下

几个表所确定的运算，试分别讨论它们的交换性、等幂性以及在 A 中关于 $*$ 是否有幺元。如果有幺元，那么 A 中的每个元素是否有逆元。

a)

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

b)

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

c)

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

d)

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

解：a) 可交换，不等幂，a 为幺元，a 以自身为逆元，b 与 c 互为逆元。

b) 可交换，不等幂，a 为幺元，a 和 b 均以自身为逆元，c 没有逆元。

c) 不可交换，等幂，没有幺元。

d) 可交换，不等幂，a 为幺元，a 以自身为逆元，b 和 c 没有逆元。

3. 证明定理 5－2.2。

证明：由左零元定义可知：$\theta_l * \theta_r = \theta_l$，由右零元定义可知：$\theta_l * \theta_r = \theta_r$，所以 $\theta_l = \theta_r = \theta$。

若有另一个零元 $\theta' = \theta' * \theta = \theta$，因此零元是唯一的。

4. 举日常生活的例子，分别说明幺元，零元和逆元。

解：例如：深颜色与浅颜色混合，则深颜色为零元，浅颜色为幺元。在钟表中，若将分针从零开始走了 t 分再走 s 分所指位置作为结果，若 $t+s\equiv\theta(\mathrm{mod}60)$，则 t 与 s 互为逆元。

5. 定义 I_+ 上的两个二元运算为：

$$\begin{cases} a * b = a^b \\ a \triangle b = a \cdot b, a, b \in I_+ \end{cases}$$

试证明：$*$ 对 $\triangle$ 是不可分配的。

证明：$a*(b\triangle c)=a^{b\cdot c}$，$(a*b)\triangle(a*c)=a^b\cdot a^c=a^{b+c}$，而 $b\cdot c$ 不一定等于 $b+c$，所以 $*$ 对 $\triangle$ 于是不可分配的。

5－3 习题

1. 对于正整数 k，$N_k=\{0,1,2,\cdots,k-1\}$，设 $*_k$ 是 N_k 上的一个二元运算，使得 $a *_k b =$ 用 k 除 $a\cdot b$ 所得的余数，这里 $a,b\in N_k$。

a) 当 $k=4$ 时，试造出 $*_k$ 的运算表。

b) 对于任意正整数 k，证明：$\langle N_k, *_k\rangle$ 是一个半群。

解:a) 当 $k=4$ 时,$*_4$ 的运算表见表 5－11 所示。

表 5－11

$*_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

b) 对于任意的 $a,b\in N_k$,$a*_kb=a\cdot b-nk=r$,其中 n 为 k 除 $a\cdot b$ 的商,r 为余数,$0\leqslant r\leqslant k-1$,所以 $*_k$ 在 N_k 上封闭的。

对于任意的 $a,b,c\in N_k$,有

$$\begin{aligned}(a*_kb)*_kc&=(a\cdot b-n_1k)*_kc\\&=(a\cdot b-n_1k)*c-n_2k\\&=a\cdot b\cdot c-(n_1c+n_2)k=r_1,\end{aligned}$$

$$\begin{aligned}a*_k(b*_kc)&=a*_k(b\cdot c-n_3k)\\&=a\cdot(b\cdot c-n_3k)-n_4k\\&=a\cdot b\cdot c-(an_3-n_4)k=r_2,\end{aligned}$$

因为 r_1,r_2 都为 $a\cdot b\cdot c$ 除以 k 所得的余数,所以 $r_1=r_2$,即 $(a*_kb)*_kc=a*_k(b*_kc)$,即 $*_k$ 满足结合律。

综上可知 $\langle N_k,*_k\rangle$ 是半群。

2. 设 $\langle S,*\rangle$ 是一个半群,$a\in S$,在 S 上定义一个二元运算 □,使得对于 S 中的任意元素 x 和 y,都有

$$x\square y=x*a*y$$

证明:二元运算 □ 是可结合的。

证明:因为 $\langle S,*\rangle$ 是一个半群,所以

$(x\square y)\square z=(x*a*y)\square z=(x*a*y)*a*z=x*a*y*a*z$,

$x\square(y\square z)=x\square(y*a*z)=x*a*(y*a*z)=x*a*y*a*z$,

所以 $(x\square y)\square z=x\square(y\square z)$,即二元运算 □ 是可结合的。

3. 设 $\langle R,*\rangle$ 是一个代数系统,$*$ 是 R 上的一个二元运算,使得对于 R 中的任意元素 a,b 都有

$$a*b=a+b+a\cdot b$$

证明:0 是幺元且 $\langle R,*\rangle$ 是独异点。

证明:任给 $a\in R$,$0*a=0+a+0\cdot a=a$,$a*0=a+0+a*0=a$,所以 $0*a=a\cdot 0=a$,即 0 是幺元;

任给 $a,b\in R$,因为在实数集上,"+"和"·"是封闭的,所以 $a*b=a+b+a\cdot b\in R$,$*$ 在 R 上封闭;

任给 $a,b,c\in R$,

$(a*b)*c=(a+b+a\cdot b)*c$
$=a+b+a\cdot b+c+(a+b+a\cdot b)\cdot c$
$=a+b+c+a\cdot b+a\cdot c+b\cdot c+a\cdot b\cdot c$
$a*(b*c)=a*(b+c+b\cdot c)$
$=a+b+c+b\cdot c+a\cdot(b+c+b\cdot c)$
$=a+b+c+a\cdot b+a\cdot c+b\cdot c+a\cdot b\cdot c$
所以$(a*b)*c=a*(b*c)$，
即 $*$ 在R上是可结合的，所以$\langle R,*\rangle$是独异点。

4. 设$X\neq\varnothing$，令$S=t(X)=\bigcup\limits_{n=0}^{\infty}X^n$，在$S$定义二元运算$\triangle$，对任意$\alpha=(x_1,x_2,\cdots,x_p)\in X^p$，$\beta=(y_1,y_2,\cdots,y_q)\in X^q$有

$$\alpha\triangle\beta=(x_1,x_2,\cdots,x_p,y_1,y_2,\cdots,y_q)\in X^{p+q}$$

证明：$\langle S,\triangle\rangle$是一个独异点。

证明：对于任意的$\alpha=(x_1,x_2,\cdots,x_p)$，$\beta=(y_1,y_2,\cdots,y_q)$，$\gamma=(z_1,z_2,\cdots,z_r)\in S$有$\alpha\triangle\beta=(x_1,x_2,\cdots,x_p,y_1,y_2,\cdots,y_q)\in X^{p+q}\in S$，即在$S$上封闭。

$(\alpha\triangle\beta)\triangle\gamma=(x_1,x_2,\cdots,x_p,y_1,y_2,\cdots,y_q)\triangle\gamma=(x_1,x_2,\cdots,x_p,y_1,y_2,\cdots,y_q,z_1,z_2,\cdots,z_r)$

$\alpha\triangle(\beta\triangle\gamma)=\alpha\triangle(y_1,y_2,\cdots,y_q,z_1,z_2,\cdots,z_r)=(x_1,x_2,\cdots,x_p,y_1,y_2,\cdots,y_q,z_1,z_2,\cdots,z_r)$

所以$(\alpha\triangle\beta)\triangle\gamma=\alpha\triangle(\beta\triangle\gamma)$，即$\triangle$在$S$上可结合。

设$\theta=()\in X^0\in S$，所以$\theta\triangle\alpha=\alpha\triangle\theta=\alpha=(x_1,x_2,\cdots,x_p)=X^p$，所以，$\theta$是幺元。

所以$\langle S,\triangle\rangle$是一个独异点。

5. 设$\langle A,*\rangle$是一个半群，而且对于A中的元素a和b，如果$a\neq b$必有$a*b\neq b*a$，试证明：

a) 对于A中的每个元素a，有$a*a=a$。

b) 对于A中任何元素a和b，有$a*b*a=a$。

c) 对于A中任何元素a，b和c，有$a*b*c=a*c$。

证明：由题意可知：若$a*b=b*a$，则必有$a=b$。

a) 因为$\langle A,*\rangle$是半群，所以 $*$ 满足结合律，即$(a*a)*a=a*(a*a)$，所以$a*a=a$。

b) 由 a) 知$a*a=a$，所以$a*(a*b*a)=(a*a)*(b*a)$
$=a*b*(a*a)=(a*b*a)*a$，所以$a*b*a=a$。

c) $(a*c)*(a*b*c)=(a*c*a)*(b*c)=a*(b*c)$
$=(a*b)*(c*a*c)=(a*b*c)*(a*c)$，所以$a*b*c=a*c$。

6. 如果$\langle S,*\rangle$是半群，且 $*$ 是可交换的，称$\langle S,*\rangle$为可交换半群。证明：如果S中有元素a，b，使得$a*a=a$和$b*b=b$，则$(a*b)*(a*b)=a*b$。

证明：$\langle S,*\rangle$为可交换半群，所以 $*$ 运算在S上满足结合律和交换律，所以$(a*b)*(a*b)=a*(b*a)*b=a*(a*b)*b=(a*a)*(b*b)$
$=a*b$。

5—4 习题

1. 设 $X = R - \{0,1\}$，在 X 上定义 6 个函数如下：

对于任意 $x \in X$，$f_1(x) = x$；$f_2(x) = x^{-1}$；$f_3(x) = 1 - x$；$f_4(x) = (1-x)^{-1}$；$f_5(x) = (x-1)x^{-1}$；$f_6(x) = x(x-1)^{-1}$。

试证明：$\langle F, \circ \rangle$ 是一个群。其中 $F = \{f_1, f_2, f_3, f_4, f_5, f_6\}$，$\circ$ 是函数的复合运算。

证明：由函数的复合运算 $\circ$ 的定义 $f \circ g(x) = f(g(x))$，可写出 $\circ$ 在 F 上的运算表见表 5—12 所示。

表 5—12

$\circ$	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

从运算表 5—12 可知运算 $\circ$ 在 F 是封闭的、可结合的，且 f_1 是幺元，f_2, f_3, f_6 均以自身为逆元；f_4 与 f_5 互为逆元，由群的定义可知 $\langle F, \circ \rangle$ 是一个群。

2. 设 $\langle A, * \rangle$ 是半群，e 是左幺元且对每一个 $x \in A$，存在 $\hat{x} \in A$，使得 $\hat{x} * x = e$。

a) 证明：对于任意的 $a, b, c \in A$，如果 $a * b = a * c$，则 $b = c$。

b) 通过证明 e 是 A 中的幺元，证明：$\langle A, * \rangle$ 是群。

证明：a) 对于任意的 $a, b, c \in A$，由已知可得存在 $\hat{a}$，使得 $\hat{a} * a = e$，所以由 $a * b = a * c$。可得 $\hat{a} * (a * b) = \hat{a} * (a * c)$，因为 $\langle A, * \rangle$ 是半群，所以 $(\hat{a} * a) * b = (\hat{a} * a) * c$，即 $e * b = e * c$，因为 e 是左幺元，所以 $b = c$。

b) 对于任意的 $x \in A$，$\hat{x} * (x * e) = (\hat{x} * x) * e = e * e = e = \hat{x} * x$，由 a) 可知：$x * e = x$，所以 e 也是右幺元，即 e 为幺元；对任意 $x \in A$，有 $(x * \hat{x}) * x = x * (\hat{x} * x) = x * e = x = e * x$。所以 $x * \hat{x} = e$，故 $\hat{x} * x = x * \hat{x} = e$，所以对于任意的 x 均有逆元 $\hat{x}$，因此 $\langle A, * \rangle$ 是群。

3. 设 $\langle G, * \rangle$ 是群，对任一 $a \in G$，令 $H = \{y \mid y * a = a * y, y \in G\}$，试证明：$\langle H, * \rangle$ 是 $\langle G, * \rangle$ 的子群。

证明：由题意可知 $H \subseteq G$，运算 $*$ 在 H 中满足结合律。

对于任意的 $x, y \in H$，任意的 $a \in G$，$(x * y) * a = x * y * a = x * a * y = a * (x * y)$，所以 $x * y \in H$，$*$ 关于 H 封闭。因为 $e * a = a * e$，所以 $e \in H$。对于任意的 $x \in H$，由于 $x * a = a * x$，所以 $x^{-1} * (x * a) * x^{-1} = x^{-1} * (a * x) * x^{-1}$，所以 $a * x^{-1} = x^{-1} * a$，即 $x^{-1} \in H$。

综上可知,$\langle H, * \rangle$ 是 $\langle G, * \rangle$ 的子群。

4. 设 $\langle H, \cdot \rangle$ 和 $\langle K, \cdot \rangle$ 都是群 $\langle G, \cdot \rangle$ 的子群,令 $HK = \{h \cdot k \mid h \in H, k \in K\}$,证明:$\langle HK, \cdot \rangle$ 是 $\langle G, \cdot \rangle$ 的子群的充要条件是 $HK = KH$。

证明:必要性:对于任意的 $k \cdot h \in KH$,$(k \cdot h)^{-1} = h^{-1} \cdot k^{-1} \in HK$,因为 $\langle HK, \cdot \rangle$ 是群,所以 $((k \cdot h)^{-1})^{-1} \in HK$,即 $k \cdot h \in HK$,所以 $KH \subseteq HK$;

对于任意的 $h \cdot k \in HK$,$(h \cdot k)^{-1} \in HK$,令 $(h \cdot k)^{-1} = h_1 \cdot k_1$,则 $h \cdot k = (h_1 \cdot k_1)^{-1} = k_1^{-1} \cdot h_1^{-1} \in KH$,所以 $HK \subseteq KH$,总之 $HK = KH$。

充分性:对于任意的 $h_1 \cdot k_1 \in HK$,$h_2 \cdot k_2 \in HK$,$(h_2 \cdot k_2)^{-1} = k_2^{-1} \cdot h_2^{-1} \in KH$;又因为 $HK = KH$,所以必有 $h_3 \in H$,$k_3 \in K$,使得 $k_2^{-1} \cdot h_2^{-1} = h_3 \cdot k_3$,所以

$$\begin{aligned}(h_1 \cdot k_1) \cdot (h_2 \cdot k_2)^{-1} &= (h_1 \cdot k_1) \cdot (h_3 \cdot k_3) \\ &= h_1 \cdot (k_1 \cdot h_3) \cdot k_3 \\ &= h_1 \cdot (h_4 \cdot k_4) \cdot k_3 \\ &= (h_1 \cdot h_4) \cdot (k_4 \cdot k_3) \\ &= h_5 \cdot k_5 \in HK\end{aligned}$$

所以 $\langle HK, \cdot \rangle$ 是 $\langle G, \cdot \rangle$ 的子群。

5. 设 $\langle A, * \rangle$ 是群,且 $|A| = 2n, n \in I_+$。证明:在 A 中至少存在 $a \neq e$,使得 $a * a = e$,其中 e 是幺元。

证明:因为 $\langle A, * \rangle$ 是群,所以对于任意的 $x \in A$,均有 $x^{-1} \in A$,使得 $x * x^{-1} = x^{-1} * x = e$。因为互为逆元的两个不相等的元素是成对出现的,群中有唯一的幺元 e,以它为自身逆元,$|A| = 2n$,所以至少存在一个元素以自身为逆元的,即必存在 $a \in A, a \neq e$,使得 $a * a = e$。

5—5 习题

1. 设 $\langle G, * \rangle$ 是一个独异点,并且对于 G 中的每一个元素 x 都有 $x * x = e$,其中 e 是幺元,证明:$\langle G, * \rangle$ 是一个阿贝尔群。

证明:对于任意的 $x \in G$,有 $x * x = e$,所以 $x^{-1} = x$。

对于任意的 $a, b \in G$,$a * b = (a * b)^{-1} = b^{-1} * a^{-1} = b * a$。即运算 $*$ 是可交换的。

所以 $\langle G, * \rangle$ 是阿贝尔群。

2. 证明:任何阶数分别为 1,2,3,4 的群都是阿贝尔群,并举一个 6 阶群,它不是阿贝尔群。

证明:阶数为 1 的群,群中存在唯一的元素是幺元 e,$e * e = e * e$,显然为阿贝尔群。

阶数为 2 的群,群中除 e 外还有一个元素 $a \neq e$,a 的逆元是它本身,$a * a = e = a * a$,$e * a = a * e = a$,因此 $\langle \{a, e\}, * \rangle$ 是阿贝尔群。

阶数为 3 的群 $\langle \{a, b, e\}, * \rangle$,若 a 的逆元是 a,b 的逆元是 b,则 $a^2 = e$,$b^2 = e$,$a * b \neq e$,若 $a * b = a$ 或 $a * b = b$,得出 $b = e$ 或 $a = e$ 矛盾。所以 a 与 b 互为逆元,即 $a * b = b * a = e$ 满足交换性,$\langle \{a, b, e\}, * \rangle$ 是阿贝尔群。

阶数为 4 的群$\langle\{a,b,c,e\},*\rangle$有两种情况：

① 若 a,b,c 中有两个元素互为逆元，不妨设为 a,b，则 $a*b=b*a=e$，于是必有 $c*c=e, a*c\neq e$，所以 $a*c=b$，同样可证 $c*a=b$，故 $a*c=c*a$。同理可证 $b*c=c*b$，即 $*$ 满足交换性。

② 若 a,b,c 中每个元素都以自身为逆元，则有：$a*b=b*a=c, b*c=c*b=a, a*c=c*a=b$，$*$ 运算满足交换性。

综上两种情况，$*$ 运算都满足交换性，所以$\langle\{a,b,c,e\},*\rangle$是阿贝尔群。

下面构造一个 6 阶群，它不是阿贝尔群。

定义在集合 $S=\{a,b,c\}$ 上的所有双射函数为：

$f_0: f_0(a)=a, f_0(b)=b, f_0(c)=c$；

$f_1: f_1(a)=a, f_1(b)=c, f_1(c)=b$；

$f_2: f_2(a)=b, f_2(b)=a, f_2(c)=c$；

$f_3: f_3(a)=b, f_3(b)=c, f_3(c)=a$；

$f_4: f_4(a)=c, f_4(b)=a, f_4(c)=b$；

$f_5: f_5(a)=c, f_5(b)=b, f_5(c)=a$；

于是集合 $F=\{f_0,f_1,f_2,f_3,f_4,f_5\}$ 关于函数的复合运算 $\circ$ 构成 6 阶群，其运算表如表 5－13，运算表中元素关于对角线不对称，显然此 6 阶群不是阿贝尔群。

表 5－13

$\circ$	f_0	f_1	f_2	f_3	f_4	f_5
f_0	f_0	f_1	f_2	f_3	f_4	f_5
f_1	f_1	f_0	f_4	f_5	f_2	f_3
f_2	f_2	f_3	f_0	f_1	f_5	f_4
f_3	f_3	f_2	f_5	f_4	f_0	f_1
f_4	f_4	f_5	f_1	f_0	f_3	f_2
f_5	f_5	f_4	f_3	f_2	f_1	f_0

3. 设$\langle G,*\rangle$是一个群，证明：如果对任意的 $a,b\in G$ 都有 $a^3*b^3=(a*b)^3$，$a^4*b^4=(a*b)^4$ 和 $a^5*b^5=(a*b)^5$，则$\langle G,*\rangle$是一个阿贝尔群。

证明：对于任意元素 $a,b\in G$，

因为 $a^3*b^3=(a*b)^3$，所以 $a^{-1}*(a^3*b^3)*b^{-1}=a^{-1}*(a*b)^3*b^{-1}$，即 $a^2*b^2=(b*a)^2$。

同理：由 $a^4*b^4=(a*b)^4$ 可得 $a^3*b^3=(b*a)^3$，

由 $a^5*b^5=(a*b)^5$ 可得 $a^4*b^4=(b*a)^4$，

所以 $a^3*b^3=(b*a)^2*(b*a)=a^2*b^2*(b*a)\Rightarrow a*b^3=b^3*a$，

$a^4*b^4=(b*a)^3*(b*a)=a^3*b^3*(b*a)\Rightarrow a*b^4=b^4*a$，

所以 $(a*b)*b^3 = a*b^4 = b^4*a = b*(b^3*a) = b*(a*b^3) = (b*a)*b^3$，故得 $a*b=b*a$。

所以 $\langle G,*\rangle$ 是阿贝尔群。

4. 设 $G=\{[1],[2],[3],[4],[5],[6]\}$，$G$ 上的二元运算 $\times_7$ 如表 5－14 所示。问 $\langle G,\times_7\rangle$ 是循环群吗？若是，试找出它的生成元。

表 5－14

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

解：$\langle G,\times_7\rangle$ 是循环群，生成元为[3]和[5]。

注意：判断一个群是不是循环群，即在 G 中看能否找到一个元素 a，使得 G 中的任意元素都有 a 的幂组成，一个循环群的生成元可以不是唯一的。

5. 证明：循环群的任何子群必定也是循环群。

证明：设 $\langle G,*\rangle$ 为循环群，其生成元是 a，设 $\langle S,*\rangle$ 是 $\langle G,*\rangle$ 的子群，若 $S=\{e\}$ 或 $S=G$ 时，显然 S 是循环群。

当 $S\neq\{e\}$ 且 $S\neq G$ 时，存在最小正整数 m，使得 $a^m\in S$，对于任意的 $a^l\in S$，必有 $l=tm+r, 0\leqslant r<m, t>0$，故 $a^r=a^{l-tm}=a^l*(a^m)^{-t}\in S$，因为 m 是 $a^m\in S$ 的最小正整数，所以只能有 $r=0$，即得 $a^l=(a^m)^t$，所以 S 中的任意元素都是 a^m 的乘幂，因此 $\langle S,*\rangle$ 是以 a^m 为生成元的循环群。

5－6 习题

1. 设有 $\{a,b,c,d,e\}$ 的置换如下：

$\alpha=\begin{pmatrix}a&b&c&d&e\\b&c&a&d&e\end{pmatrix}$，$\beta=\begin{pmatrix}a&b&c&d&e\\a&b&c&e&d\end{pmatrix}$，

$\gamma=\begin{pmatrix}a&b&c&d&e\\e&d&c&b&a\end{pmatrix}$，$\delta=\begin{pmatrix}a&b&c&d&e\\c&b&a&e&d\end{pmatrix}$。

试求：$\alpha\circ\beta,\beta\circ\alpha,\alpha\circ\alpha,\gamma\circ\beta,\delta^{-1},\alpha\circ\beta\circ\gamma$，并解方程 $\alpha\circ x=\beta, y\circ\gamma=\delta$。

解：$\alpha\circ\beta=\begin{pmatrix}a&b&c&d&e\\b&c&a&e&d\end{pmatrix}$；$\beta\circ\alpha=\begin{pmatrix}a&b&c&d&e\\b&c&a&e&d\end{pmatrix}$；

$\alpha\circ\alpha=\begin{pmatrix}a&b&c&d&e\\c&a&b&d&e\end{pmatrix}$；$\gamma\circ\beta=\begin{pmatrix}a&b&c&d&e\\e&d&c&a&b\end{pmatrix}$；

$$\delta^{-1}=\begin{pmatrix}a & b & c & d & e\\ c & b & a & e & d\end{pmatrix};\alpha\circ\beta\circ\gamma=\begin{pmatrix}a & b & c & d & e\\ d & e & a & c & b\end{pmatrix};$$

$$x=\alpha^{-1}\circ\beta=\begin{pmatrix}a & b & c & d & e\\ c & a & b & e & d\end{pmatrix};$$

$$y=\delta\circ\gamma^{-1}=\begin{pmatrix}a & b & c & d & e\\ c & b & a & e & d\end{pmatrix}\circ\begin{pmatrix}a & b & c & d & e\\ e & d & c & b & a\end{pmatrix}=\begin{pmatrix}a & b & c & d & e\\ d & e & a & b & c\end{pmatrix}$$

2. 设 p 是质数，证明：从 a 种颜色不同的珠子中选取 p 粒串成手镯，只有同色手镯保持旋转不变。

证明：由 p 粒珠子串成的手镯，其珠子颜色分别记为 $C_1,C_2,\cdots,C_p$，如图 5－7 所示。

顺时针方向旋转一粒珠子的位置后，若要不变，必有 $C_2=C_1,C_3=C_2,\cdots,C_p=C_{p-1},C_1=C_p$，即 $C_1=C_2=C_3=\cdots=C_p$，所以，只能用同色珠子串成的手镯才能保持旋转一粒珠子位置后不变。

由于 p 是质数，故不可能有 $k,1<k<p$，使得 p 是 k 的倍数，因此不可能实现：$C_1=C_k=C_{2k}=\cdots=$ 一种颜色，而 $C_2=C_{k+1}=C_{2k+1}=\cdots=$ 另一种颜色，…，即不可能用不同颜色的珠子串成的手镯，而使该 p 粒珠子串成的手镯保持旋转 k 粒珠子位置后不变，只有同色手镯才能保持旋转不变。

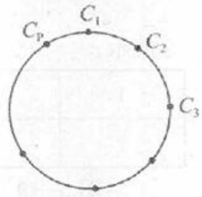

图 5－7

3. 哪些对称群是阿贝尔群？

解：$\langle S_1,\circ\rangle$ 和 $\langle S_2,\circ\rangle$ 是阿贝尔群。

$\langle S_3,\circ\rangle$ 中有置换 $\begin{pmatrix}a & b & c\\ b & a & c\end{pmatrix}$ 和 $\begin{pmatrix}a & b & c\\ b & c & a\end{pmatrix}$，而 $\begin{pmatrix}a & b & c\\ b & a & c\end{pmatrix}$。

$\begin{pmatrix}a & b & c\\ b & c & a\end{pmatrix}=\begin{pmatrix}a & b & c\\ a & c & b\end{pmatrix}$，$\begin{pmatrix}a & b & c\\ b & c & a\end{pmatrix}\circ\begin{pmatrix}a & b & c\\ b & a & c\end{pmatrix}=\begin{pmatrix}a & b & c\\ c & b & a\end{pmatrix}$，

所以 $\langle S_3,\circ\rangle$ 不是阿贝尔群。

对于任意的 $n,n\geqslant 4$，$\langle S_n,\circ\rangle$ 中总有置换 $\begin{pmatrix}a_1 & a_2 & a_3 & a_4 & \cdots & a_n\\ a_2 & a_1 & a_3 & a_4 & \cdots & a_n\end{pmatrix}$ 和 $\begin{pmatrix}a_1 & a_2 & a_3 & a_4 & \cdots & a_n\\ a_2 & a_3 & a_1 & a_4 & \cdots & a_n\end{pmatrix}$，而这两个置换之间的运算是不可交换的。因此，$\langle S_n,\circ\rangle,n\geqslant 4$，都不是阿贝尔群。

4. 用 4 种不同颜色中的一种或几种来涂一根六节的棍棒，问有多少种不同的涂法？

解：设棍棒第 i 节涂上 C_i 色，如图 5－8 所示。

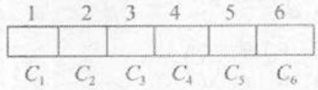

图 5－8

每一节上可以有 4 种涂色法，因此棍棒的所有涂色法共有 4^6 种。然而，只要是 C_1 色与 C_6 色相同，C_2 色与 C_5 色相同，C_3 色与 C_4 色相同，那么该棍棒倒向后的涂色情况不会改变的。因此，构造置换群 $\langle\{\pi_0,\pi_1\},\circ\rangle$ 其中 π_0 是幺置换，它将每一种涂色棍棒的情况 $C_1C_2C_3C_4C_5C_6$ 仍映照成 $C_1C_2C_3C_4C_5C_6$ 的情况，所以在 π_0 作用下的不变元个数为 4^6；而 π_1 是这样的一个置换，它将每一种涂色棍棒的情况 $C_1C_2C_3C_4C_5C_6$ 映照成 $C_6C_5C_4C_3C_2C_1$ 的情况，所在 π_1 作用下的不变元是 $C_1=C_6$，$C_2=C_5$，$C_3=C_4$ 的情况，故在 π_1 作用下的不变元个数为 4^3，因此由伯恩赛德定理可知，该棍棒不同涂色法的总数应是种 $\frac{1}{2}(4^6+4^3)=2080$ 种。

5. a) 2×2 的棋盘，用白色或黑色涂在每一个方格内，在考虑旋转等价的条件下，试确定每个方格涂上颜色的不同棋盘的数目。

b) 对于 4×4 的棋盘呢？

解：a) 设 2×2 的棋盘如图 5－9 所示。

1	3
2	4

图 5－9

令 C_i 表示棋盘中第 i 格所涂的颜色，现构造置换群为 $\langle\{\pi_0,\pi_1,\pi_2,\pi_3\},\circ\rangle$，其中 $\pi_i(0\leqslant i\leqslant 3)$ 是将棋盘映照到按顺时针方向旋转 $i\times 90°$ 所得的棋盘，那么，在 π_i 作用下，不变元的个数分别如下：

π_0：不转，不变元的个数是 2^4。

π_1：顺时针转 $90°$，只有当 $C_1=C_2=C_3=C_4$ 时为不变元，所以不变元的个数是 2。

π_2：顺时针转 $180°$，只有当 $C_1=C_3$，$C_2=C_4$ 时为不变元，所以不变元的个数是 2^2。

π_3：顺时针转 $270°$，只有当 $C_1=C_4=C_3=C_2$ 时为不变元，所以不变元的个数是 2。

因此，由伯恩赛德定理可知，不相同的 2×2 棋盘数是 $\frac{1}{4}(2^4+2+4+2)=6$。

b) 设 4×4 的棋盘如图 5－10 所示。

图 5－10

类似于 a)，构造置换群 $\langle\{\pi_0,\pi_1,\pi_2,\pi_3\},\circ\rangle$，那么在 π_i 作用下，不变元的个数分别如下：

π_0：不转，不变元的个数是 2^{16}。

π_1：顺时针转 $90°$，不变元要求 $C_1=C_4=C_7=C_{10}$，

$C_2 = C_5 = C_8 = C_{11}$，$C_3 = C_6 = C_9 = C_{12}$，$C_{一} = C_{二} = C_{三} = C_{四}$，故不变元的个数应等于四组涂两色的个数，即为 2^4。

π_2：顺时针转 $180°$，不变元要求 $C_1 = C_7$，$C_2 = C_8$，$C_3 = C_9$，$C_4 = C_{10}$，$C_5 = C_{11}$，$C_6 = C_{12}$，$C_{一} = C_{二}$，$C_{三} = C_{四}$，故不变元的个数应等于八组涂两色的个数，即为 2^8。

π_3：顺时针转 $270°$，不变元要求 $C_1 = C_{10} = C_7 = C_4$，$C_2 = C_{11} = C_8 = C_5$，$C_3 = C_{12} = C_9 = C_6$，$C_{一} = C_{四} = C_{三} = C_{二}$，故不变元的个数应等于四组涂两色的个数，即为 2^4

因此，由伯恩赛德定理可知，不相同的 4×4 棋盘数是 $\frac{1}{4}(2^{16}+2^4+2^8+2^4) = 16456$。

5—7 习题

1. 设 $G = \{\varphi \mid \varphi : x \to ax+b$，其中 $a,b \in R$ 且 $a \neq 0, x \in R\}$，二元运算 $\circ$ 是映射的复合。

a) 证明 $\langle G, \circ\rangle$ 是一个群。

b) 若 S 和 T 分别是由 G 中 $a=1$ 和 $b=0$ 的所有映射构成的集合，证明：$\langle S,\circ\rangle$ 和 $\langle T,\circ\rangle$ 都是子群。

c) 写出 S 和 T 在 G 中所有的左陪集。

证明：a) ① 对于任意的 $\varphi_1, \varphi_2 \in G$，设 $\varphi_1(x) = a_1x+b_1$，$a_1 \neq 0$，$\varphi_2(x) = a_2x+b_2$，$a_2 \neq 0$，$\varphi_1\circ\varphi_2(x) = \varphi_1(\varphi_2(x)) = \varphi_1(a_2x+b_2) = a_1(a_2x+b_2)+b_1 = (a_1a_2)x+a_1b_2+b_1$，因为 $a_1a_2 \in R$，$a_1b_2+b_1 \in R$ 且 $a_1a_2 \neq 0$。所以 $\varphi_1\circ\varphi_2 \in G$ 满足封闭性。

② 对于任意的 $\varphi_1,\varphi_2,\varphi_3 \in G$ 有 $(\varphi_1\circ\varphi_2)\circ\varphi_3(x) = (\varphi_1\circ\varphi_2)(\varphi_3(x)) = \varphi_1(\varphi_2(\varphi_3(x)))$，而 $\varphi_1\circ(\varphi_2\circ\varphi_3)(x) = \varphi_1(\varphi_2\circ\varphi_3(x)) = \varphi_1(\varphi_2(\varphi_3(x)))$，所以 $(\varphi_1\circ\varphi_2)\circ\varphi_3 = \varphi_1\circ(\varphi_2\circ\varphi_3)$ 满足结合性。

③ 设 $\varphi_e = x$，对于任意的 $\varphi \in G$，设 $\varphi(x) = ax+b$，则 $\varphi_e\circ\varphi(x) = \varphi_e(ax+b) = ax+b$，$\varphi\circ\varphi_e(x) = \varphi(x) = ax+b$，所以 $\varphi_e\circ\varphi = \varphi\circ\varphi_e$，所以 $\varphi_e = x$ 是幺元。

④ 对于任意的 $\varphi \in G$，设 $\varphi(x) = ax+b$，$a\neq 0$，于是存在 $\varphi^{-1}\in G$，使得 $\varphi^{-1}(x) = \frac{1}{a}x - \frac{b}{a}$，$\varphi\circ\varphi^{-1}(x) = \varphi(\varphi^{-1}(x)) = \varphi\left(\frac{1}{a}x-\frac{b}{a}\right) = a\left(\frac{1}{a}x-\frac{b}{a}\right)+b = x$，$\varphi^{-1}\circ\varphi(x) = \varphi^{-1}(ax+b) = \frac{1}{a}(ax+b)-\frac{b}{a} = x$，所以 $\varphi^{-1}\circ\varphi = \varphi\circ\varphi^{-1} = \varphi_e$，逆元存在，

综上可知 $\langle G,\circ\rangle$ 是一个群。

b) 对于任意的 $\varphi_1,\varphi_2 \in S$，$\varphi_1(x) = x+b_1$，$\varphi_2(x) = x+b_2$，有 $\varphi_2^{-1}(x) = x-b_2$，$\varphi_1\circ\varphi_2^{-1}(x) = \varphi_1(\varphi_2^{-1}(x)) = x-b_2+b_1 = x+(b_1-b_2) \in S$，即 $\varphi_1\circ\varphi_2^{-1}(x) \in S$。

因此，$\langle S, \circ\rangle$ 是 $\langle G, \circ\rangle$ 是子群。

对于任意的 $\varphi_1,\varphi_2 \in T$，设 $\varphi_1(x)=a_1x,\varphi_2(x)=a_2x,a_1\neq 0,a_2\neq 0$，于是 $\varphi_2^{-1}(x)=\dfrac{1}{a_2}x,\varphi_1\circ\varphi_2^{-1}(x)=\varphi_1(\varphi_2^{-1}(x))=\varphi_1\left(\dfrac{1}{a_2}x\right)=a_1\dfrac{1}{a_2}x=\dfrac{a_1}{a_2}x,\dfrac{a_1}{a_2}\neq 0$，所以 $\varphi_1\circ\varphi_2^{-1}\in T$，因此 $\langle T, \circ\rangle$ 也是 $\langle G, \circ\rangle$ 的子群。

c) S 的左陪集应为：$\varphi\circ S,\varphi\in G$，对于任意的 $\varphi\in G$，设 $\varphi(x)=ax+b,a\neq 0$，那么

$$\begin{aligned}\varphi\circ S&=\{\varphi\circ\varphi'\mid\varphi'\in S\}\\&=\{\varphi\circ\varphi'\mid\varphi':x\to x+b',b'\in R,x\in R\}\\&=\{\bar{\varphi}\mid\bar{\varphi}:x\to a(x+b')+b,a\in R\text{且}a\neq 0,b\in R,b'\in R,x\in R\}\\&=\{\bar{\varphi}\mid\bar{\varphi}:x\to ax+c,a\in R\text{且}a\neq 0,c\in R,x\in R\}\end{aligned}$$

所以，S 在 G 中的所有左陪集为：$\{\bar{\varphi}\mid\bar{\varphi}:x\to ax+c,a\in R\text{且}a\neq 0,c\in R,x\in R\}$。

T 的左陪集应为：$\varphi\circ T,\varphi\in G$，对于任意的 $\varphi\in G$，设 $\varphi(x)=ax+b,a\neq 0$，那么

$$\begin{aligned}\varphi\circ T&=\{\varphi\circ\varphi'\mid\varphi'\in T\}\\&=\{\varphi\circ\varphi'\mid\varphi':x\to a'x,a'\in R,x\in R\}\\&=\{\bar{\varphi}\mid\bar{\varphi}:x\to a(a'x)+b,a\in R\text{且}a\neq 0,b\in R,a'\in R,x\in R\}\\&=\{\bar{\varphi}\mid\bar{\varphi}:x\to cx+b,c\in R\text{且}c\neq 0,b\in R,x\in R\}\end{aligned}$$

所以，T 在 G 中的所有左陪集为：$\{\bar{\varphi}\mid\bar{\varphi}:x\to cx+b,c\in R\text{且}c\neq 0,b\in R,x\in R\}$。

2. 设 $\langle Z_6, +_6\rangle$ 是一个群，这里 $+_6$ 是模6加法，$Z_6=\{[0],[1],[2],[3],[4],[5]\}$，试写出 $\langle Z_6, +_6\rangle$ 中每个子群及其相应的左陪集。

解：子群有：$\langle\{[0]\},+_6\rangle$，$\langle\{[0],[3]\},+_6\rangle$，$\langle\{[0],[2],[4]\},+_6\rangle$ 和 $\langle Z_6, +_6\rangle$。

$\{[0]\}$ 的左陪集为：$\{[0]\},\{[1]\},\{[2]\},\{[3]\},\{[4]\},\{[5]\}$，

$\{[0],[3]\}$ 的左陪集为：$\{[0],[3]\},\{[1],[4]\},\{[2],[5]\}$，

$\{[0],[2],[4]\}$ 的左陪集为：$\{[0],[2],[4]\},\{[1],[3],[5]\}$，

Z_6 的左陪集就是 Z_6 本身。

3. 设 $\langle G, *\rangle$ 是任一群，定义 $R\subseteq G\times G$ 为 $R=\{\langle\sigma,\varphi\rangle\mid\text{存在}\theta\in G\text{使得}\varphi=\theta*\sigma*\theta^{-1}\}$，验证 R 是 G 上的等价关系。

证明：设 $\langle G, *\rangle$ 是任一群，e 为幺元，对于任意的 $a\in G$，有 $a=e*a*e^{-1}$，所以 $\langle a,a\rangle\in R$，即 R 是自反的。

若 $\langle a,b\rangle\in R$，由 R 的定义可知，存在 $\theta\in R$，使得：$b=\theta*a*\theta^{-1}$ 所以有 $a=\theta^{-1}*b*\theta=\theta^{-1}*b*(\theta^{-1})^{-1}$，说明 $\langle b,a\rangle\in R$，即 R 是对称的。

若 $\langle a,b\rangle\in R$ 且 $\langle b,c\rangle\in R$，则存在 θ_1,θ_2，使得 $b=\theta_1*a*\theta_1^{-1},c=\theta_2*b*\theta_2^{-1}$

所以 $c=\theta_2*b*\theta_2^{-1}=\theta_2*(\theta_1*a*\theta_1^{-1})*\theta_2^{-1}=(\theta_2*\theta_1)*a*(\theta_2*\theta_1)^{-1}$

即 $\langle a,c\rangle\in R$，即 R 满足传递性。

综上可知，R 是 G 上的等价关系。

4. 设 S_n 是一个对称群，G 是保持某一个元素不变的置换群，求出 G 在 S_n 中的所有

左陪集。

解：设G是使第i个元素不变的置换群，因为$|S_n|=n!$，$|G|=(n-1)!$，由拉格朗日定理可知G在S_n中的左陪集共有n个，即为G以及$\pi_k \cdot G$
$=\left\{\begin{pmatrix}1 & 2\cdots & i\cdots n\\ k_1 & k_2\cdots k\cdots & k_n\end{pmatrix}\middle| k_1,k_2,\cdots,k_{i-1},k_{i+1},\cdots,k_n\right.$是$1,2,\cdots,k-1,k+1,$
$\cdots,n$的任一置换排列$\left.(k=1,2,\cdots,i-1,i+1,\cdots,n)\right\}$

5. 设$\langle H,*\rangle$是群$\langle G,*\rangle$的一个子群，如果$A=\{x \mid x\in G, x*H*x^{-1}=H\}$，证明：$\langle A,*\rangle$是$\langle G,*\rangle$的一个子群。

证明：显然$A\subseteq G$，对于任意的$a,b\in A$，有$a*H*a^{-1}=H$，$b*H*b^{-1}=H$。由$b*H*b^{-1}=H$可得$b^{-1}*H*b=H$，所以$(a*b^{-1})*H*(a*b^{-1})^{-1}=a*(b^{-1}*H*(b^{-1})^{-1})*a^{-1}=a*H*a^{-1}=H$，即$a*b^{-1}\in A$，因此$\langle A,*\rangle$是$\langle G,*\rangle$的一个子群。

6. 证明：在由群$\langle G,*\rangle$的一个子群$\langle S,*\rangle$所确定的陪集中，只有一个陪集是子群。

证明：任取元素$a\in G$，aS是a所确定的左陪集，取a为G中幺元e，即$a=e$，则$aS=eS=S$，S是一个陪集。
假设另外一个元素$a\neq e$，由a确定的左陪集aS也是G的子群，则$e\in aS$，由陪集定义，存在s_1，使得：$a*s_1=e$，即$a=s_1^{-1}$。
下证$aS=S$，对于任意的$a*s\in aS$，则$a*s=s_1^{-1}*s\in S$，即有$aS\subseteq S$。反之，对于任意的$s\in S$，有$s=a*a^{-1}*s=a*(a^{-1}*s)=a*(s_1*s)\in aS$，即有$S\subseteq aS$，所以$aS=S$。即$S$的左陪集中只有一个是子群，即$S$本身。

7. 设aH和bH是H在G中的两个左陪集，证明：要么$aH\cap bH=\varnothing$，要么$aH=bH$。

证明：对于aH和bH，具有两种情况：
①$aH\cap bH=\varnothing$，
②$aH\cap bH\neq\varnothing$，则必存在h_1和h_2，使得$ah_1=bh_2$，即$a=bh_2h_1^{-1}$，对于任意的$ah\in aH$，有$ah=bh_2h_1^{-1}h=bh_3\in bH$，故有$aH\subseteq bH$，同理可证$bH\subseteq aH$。所以$aH=bH$。

8. 设p是质数，证明：p^m阶群中一定包含着一个p阶子群。

证明：设p^m阶群为$\langle G,*\rangle$，对于任意$a\in G, a\neq e$，若a的阶数为n，即$a^n=e$，则$n\mid p^m$，因为p是质数，所以$n=p^t(t\geqslant 1, t$为整数)。
若$t=1$，则$n=p$，即循环群$\langle\{a,a^2,\cdots,a^n\},*\rangle$是$\langle G,*\rangle$的$p$阶子群。
若$t>1$，则令$b^p=(a^{p^{t-1}})^p=a^{p^t}=a^n=e$，所以循环群$\langle\{b,b^2,\cdots,b^p\},*\rangle$是$\langle G,*\rangle$的$p$阶子群。

9. 设$\langle S,*\rangle$和$\langle T,*\rangle$分别是群$\langle G,*\rangle$的s阶和t阶子群，并且$S\cap T$和$S\cup T$的阶分别为μ和v，证明：$st>\mu v$。

证明：由包含排斥原理得：$|S\cup T|=|S|+|T|-|S\cap T|$，即$v=s+t-\mu$，因为$|S\cap T|\leqslant|S|$，$|S\cap T|\leqslant|T|$，即$\mu\leqslant s$，$\mu\leqslant t$，因此$\mu v=\mu(s+$

$t-\mu) = \mu(s-\mu) - t(s-\mu) + st = st - (t-\mu)(s-\mu) \leqslant st$，即 $st \geqslant \mu\nu$。

5－8 习题

1. 证明：如果 f 是由 $\langle A, \bigstar \rangle$ 到 $\langle B, * \rangle$ 的同态映射，g 是由 $\langle B, * \rangle$ 到 $\langle C, \triangle \rangle$ 的同态映射，那么，$g \circ f$ 是由 $\langle A, \bigstar \rangle$ 到 $\langle C, \triangle \rangle$ 的同态映射。

证明：因为 f 是由 $\langle A, \bigstar \rangle$ 到 $\langle B, * \rangle$ 的同态映射，g 是由 $\langle B, * \rangle$ 到 $\langle C, \triangle \rangle$ 的同态映射，

所以 $g \circ f(a \bigstar b) = g(f(a \bigstar b)) = g(f(a) * f(b)) = g(f(a)) \triangle g(f(b)) = g \circ f(a) \triangle g \circ f(b)$

因此，$g \circ f$ 是由 $\langle A, \bigstar \rangle$ 到 $\langle C, \triangle \rangle$ 的同态映射。

2. 设 $\langle G, * \rangle$ 是一个群，而 $a \in G$，如果 f 是从 G 到 G 的映射，使得对于每一个 $x \in G$，都有

$$f(x) = a * x * a^{-1},$$

试证明：f 是一个从 G 到 G 上的自同构。

证明：对于任意 $x, y \in G$，若 $x \neq y$，则 $f(x) = a * x * a^{-1} \neq a * y * a^{-1} = f(y)$，即 f 是入射。

对于任意 $y \in G$，由封闭性得 $a^{-1} * y * a \in G$，令 $a^{-1} * y * a = x$，因为 $\langle G, * \rangle$ 是群，所以有 $y = a * x * a^{-1}$，所以对于任意 $y \in G$ 都能找到一个 x，使得 $y \in f(x)$，即 f 是 G 上的满射。

所以 f 是 G 上的双射。

另外，对于任意的 $x, y \in G$，有

$$\begin{aligned} f(x * y) &= a * (x * y) * a^{-1} = (a * x * a^{-1}) * (a * y * a^{-1}) \\ &= f(x) * f(y)。\end{aligned}$$

因此，f 是从 G 到 G 的一个自同构。

3. 试证由表 5－15 所给出的两个群 $\langle G, \bigstar \rangle$ 和 $\langle S, * \rangle$ 是同构的。

表 5－15

$\bigstar$	p_1	p_2	p_3	p_4
p_1	p_1	p_2	p_3	p_4
p_2	p_2	p_1	p_4	p_3
p_3	p_3	p_4	p_1	p_2
p_4	p_4	p_3	p_2	p_1

$\langle G, \bigstar \rangle$

$*$	q_1	q_2	q_3	q_4
q_1	q_3	q_4	q_1	q_2
q_2	q_4	q_3	q_2	q_1
q_3	q_1	q_2	q_3	q_4
q_4	q_2	q_1	q_4	q_3

$\langle S, * \rangle$

证明:作 G 到 S 的映射 f 为:$f(p_1)=q_3$,$f(p_2)=q_2$,$f(p_3)=q_1$,$f(p_4)=q_4$。

由表 5-15 可知 f 是一个双射。

易证:$f(p_1★p_1)=f(p_1)=q_3=q_3*q_3=f(p_1)*f(p_1)$,

$f(p_1★p_2)=f(p_2)=q_2=q_3*q_2=f(p_1)*f(p_2)$,

$f(p_3★p_2)=f(p_4)=q_4=q_1*q_2=f(p_3)*f(p_2)$,

$f(p_4★p_2)=f(p_3)=q_1=q_4*q_2=f(p_4)*f(p_2)$,

等等,其余可类似验证。

所以 $\langle G,★\rangle$ 和 $\langle S,*\rangle$ 同构。

4. 设 f_1,f_2 都是从代数系统 $\langle A,★\rangle$ 到代数系统 $\langle B,*\rangle$ 的同态。设 g 是从 A 到 B 的一个映射,使得对任意 $a\in A$,都有 $g(a)=f_1(a)*f_2(a)$。

证明:如果 $\langle B,*\rangle$ 是一个可交换半群,那么 g 是一个由 $\langle A,★\rangle$ 到 $\langle B,*\rangle$ 的同态。

证明:因为对于任意的 $a,b\in A$,都有

$$\begin{aligned}g(a★b)=f_1(a★b)*f_2(a★b)&=f_1(a)*f_1(b)*f_2(a)*f_2(b)\\&=f_1(a)*f_2(a)*f_1(b)*f_2(b)\\&=g(a)*g(b)\end{aligned}$$

所以,g 是 $\langle A,★\rangle$ 到 $\langle B,*\rangle$ 的同态。

5. $\langle R,+\rangle$ 是实数集上的加法群,设 $f:x\rightarrow e^{2\pi ix}$,$x\in R$,$f$ 是同态否?如果是,请写出同态象和同态核。

解:由定义可知:f 是实数集 R 到复数 C 的一个映射。

对于任意 $a,b\in R$,有 $f(a+b)=e^{2\pi i(a+b)}=e^{2\pi ia}\cdot e^{2\pi ib}=f(a)\cdot f(b)$

所以 f 是 $\langle R,+\rangle$ 到 $\langle C,\cdot\rangle$ 是同态,这里的 $\langle C,\cdot\rangle$ 是复数集上的乘法群。

因为 $f(R)=\{e^{2\pi ix}\mid x\in R\}=\{\cos 2\pi x+i\sin 2\pi x\mid x\in R\}$

所以 f 的同态象为 $\langle\{\cos 2\pi x+i\sin 2\pi x\mid x\in R\},\cdot\rangle$,它是一个群,其幺元为 1。

所以同态核为 $Ker(f)=\{x\mid x\in R$ 且 $\cos 2\pi x+i\sin 2\pi x=1\}$,即有 $\cos 2\pi x=1$,$\sin 2\pi x=0$。因此 $2\pi x=2k\pi$(k 为整数),所以当 x 为整数时,$f(x)=1$,即 f 的同态核为整数集 I。

6. 证明:循环群的同态象必定是循环群。

证明:设代数系统 $\langle A,\cdot\rangle$ 为循环群,生成元为 a,同态映射为 f,同态象为 $\langle f(A),*\rangle$。

则对任意的 $a^n,a^m\in A$,有 $f(a^n\cdot a^m)=f(a^n)*f(a^m)$,$n,m\geqslant 0$ 且为整数,

下用数学归纳法证明 $f(a^n)=f^n(a)$,$n\in N$。

$n=2$ 时,$f(a^2)=f(a\cdot a)=f(a)*f(a)=f^2(a)$。

假设 $n=k-1$ 时,$f(a^{k-1})=f^{k-1}(a)$。

则当 $n=k$ 时,$f(a^k)=f(a^{k-1}\cdot a)=f^{k-1}(a)*f(a)=f^k(a)$。

所以 $f(A)$ 中的每个元素都可以表示为 $f^n(a)$,$\langle f(A),*\rangle$ 是以 $f(a)$ 为生成元的循环群。

7. $\langle R-\{0\},\times\rangle$ 与 $\langle R,+\rangle$ 同构吗?

解:设 f 是 $\langle R,+\rangle$ 与 $\langle R-\{0\},\times\rangle$ 的同构映射。

则对于任意的 $a\in R$,有 $f(a)=f(0+a)=f(0)\times f(a)=f(a)\times f(0)$

所以，$f(0)$ 是 $\langle R-\{0\},\times\rangle$ 中的幺元，$f(0)=1$。

对于 $-1\in R-\{0\}$，必存在 $b\in R$，使得 $f(b)=-1$，则有 $f(b+b)=f(b)\times f(b)=-1\times(-1)=1$，所以有 $b+b=0$，即 $b=0$，也就是 $f(0)=-1$，这与 $f(0)=1$ 矛盾。

所以 $\langle R,+\rangle$ 与 $\langle R-\{0\},\times\rangle$ 不可能同构。

8. 证明：一个集合上任意两个同余关系的交也是一个同余关系。

证明：设 $\langle A,*\rangle$ 上的任意两个同余关系为 R_1 和 R_2，即对于任意 $\langle a_1,b_1\rangle\in R_1$，$\langle a_2,b_2\rangle\in R_1$，有 $\langle a_1*a_2,b_1*b_2\rangle\in R_1$；对于任意 $\langle c_1,d_1\rangle\in R_2$，$\langle c_2,d_2\rangle\in R_2$，有 $\langle c_1*c_2,d_1*d_2\rangle\in R_2$。

所以，对于任意的 $\langle a,b\rangle\in R_1\cap R_2$，$\langle c,d\rangle\in R_1\cap R_2$，有 $\langle a,b\rangle\in R_1$，$\langle c,d\rangle\in R_1$ 且 $\langle a,b\rangle\in R_2$，$\langle c,d\rangle\in R_2$，所以 $\langle a*c,b*d\rangle\in R_1$ 且 $\langle a*c,b*d\rangle\in R_2$，即 $\langle a*c,b*d\rangle\in R_1\cap R_2$。

因此，一个集合上任意两个同余关系的交仍是一个同余关系。

9. 证明：定理 5-8.4 中在 B 上所定义的二元运算 $*$ 是唯一确定的。

证明：对于任意的 $A_i,A_j\in B$，任取 $a_1\in A_i$，$a_2\in A_j$，若 $a_1\bigstar a_2\in A_k$，则定义 $A_i*A_j=A_k$。

另取 $a_1'\in A_i$，$a_2'\in A_j$，则有 $\langle a_1,a_1'\rangle\in R$ 和 $\langle a_2,a_2'\rangle\in R$，又因 R 是 A 上的同余关系，所以 $\langle a_1\bigstar a_2,a_1'\bigstar a_2'\rangle\in R$，因此可知，若 $a_1\bigstar a_2\in A_k$，则 $a_1'\bigstar a_2'\in A_k$，这表明，不论怎样选取 $a_1\in A_i$，$a_2\in A_j$，总有 $a_1\bigstar a_2\in A_k$。

因此上述在 B 上定义的二元运算 $*$ 是唯一确定的。

10. 考察代数系统 $\langle I,+\rangle$，以下定义在 I 上的二元关系 R 是同余关系吗？

a) $\langle x,y\rangle\in R$ 当且仅当 $(x<0\wedge y<0)\vee(x\geqslant 0\wedge y\geqslant 0)$。

b) $\langle x,y\rangle\in R$ 当且仅当 $|x-y|<10$。

c) $\langle x,y\rangle\in R$ 当且仅当 $(x=y=0)\vee(x\neq 0\wedge y\neq 0)$。

d) $\langle x,y\rangle\in R$ 当且仅当 $x\geqslant y$。

解：a) 因为 $\langle -3,-1\rangle\in R$，$\langle 2,5\rangle\in R$，但 $\langle -3+2,-1+5\rangle=\langle -1,4\rangle\notin R$，所以 R 不是同余关系。

b) 因为 $\langle 1,5\rangle\in R$，$\langle 2,10\rangle\in R$（因为 $|1-5|=4<10$，$|2-10|=8<10$），但 $\langle 1+2,5+10\rangle=\langle 3,15\rangle\notin R$。$|3-15|=12>10$，所以 R 不是同余关系。

c) 因为 $\langle -3,2\rangle\in R$ 且 $\langle 3,4\rangle\in R$，但 $\langle -3+3,2+4\rangle=\langle 0,6\rangle\notin R$，所以 R 不是同余关系。

d) $\langle 4,1\rangle\in R$，但 $\langle 1,4\rangle\notin R$，对称性不成立，$R$ 不是等价关系，必不是同余关系。

注意：若 R 是代数系统 $\langle A,\bigstar\rangle$ 上的同余关系，则必满足 ①R 是 A 上的等价关系。② 当 $\langle a_1,a_2\rangle\in R$，$\langle b_1,b_2\rangle\in R$ 时，$\langle a_1\bigstar b_1,a_2\bigstar b_2\rangle\in R$。

11. 设 f 和 g 都是群 $\langle G_1,\bigstar\rangle$ 到群 $\langle G_2,*\rangle$ 的同态，证明：$\langle C,\bigstar\rangle$ 是 $\langle G_1,\bigstar\rangle$ 的一个子群，其中 $C=\{x\mid x\in G_1$ 且 $f(x)=g(x)\}$。

证明：显然 $C\subseteq G_1$，对于任意的 $a,b\in C$，有 $f(a)=g(a)$，$f(b)=g(b)$。

因为 f 和 g 都是同态映射，所以有，$f(b^{-1})=f(b)^{-1}$，$g(b^{-1})=g(b)^{-1}$，又因

$f(b)=g(b)$，所以 $f(b)^{-1}=g(b)^{-1}$，即 $f(b^{-1})=g(b^{-1})$，由此可得 $f(a\bigstar b^{-1})=f(a)*f(b^{-1})=g(a)*g(b^{-1})=g(a\bigstar b^{-1})$，即 $a\bigstar b^{-1}\in C$，因此 $\langle C,\bigstar\rangle$ 是 $\langle G_1,\bigstar\rangle$ 的子群。

12. 设 f 为从群 $\langle G_1,*\rangle$ 到 $\langle G_2,\triangle\rangle$ 的同态映射，则 f 为入射当且仅当 $Ker(f)=\{e\}$。其中，e 是 G_1 中的幺元。

证明：必要性，设 f 是入射。因为 $f(e)=e$，所以 $e\in Ker(f)$。
设存在 $a\in G_1, a\neq e$，使得 $f(a)=e$，则 $f(e)=f(a)$ 与 f 是入射相矛盾，所以 $Ker(f)=\{e\}$。
充分性，设 $Ker(f)=\{e\}$，对于任意 $a,b\in G_1$，若 $f(a)=f(b)$，因为 f 是同态映射，则有 $f(a*b^{-1})=f(a)\triangle f(b)^{-1}=f(b)\triangle f(b^{-1})=f(e)$，即 $a*b^{-1}=e$，则 $a=b$，因此 f 是入射。

5—9 习题

1. 已知一个环 $\langle\{a,b,c,d\},+,\cdot\rangle$，它的运算由表 5—16 给出：

表 5—16

+	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

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

它是一个交换环吗？它有乘法幺元吗？这个环中的零元是什么？并求出每个元素的加法逆元。

解：因为·运算是对称的，所以环 $\langle\{a,b,c,d\},+,\cdot\rangle$ 是交换环，没有乘法幺元，环中零元是 a，a 和 c 以自身为加法逆元，b 和 d 互为加法逆元。

2. 试证 $\langle I,\triangle\!\!\!\cdot,\triangle\rangle$ 是有幺元的交换环，其中，运算 $\triangle\!\!\!\cdot$ 和 $\triangle$ 分别定义为：对任意的 $a,b\in I$，$a\triangle\!\!\!\cdot b=a+b-1$，$a\triangle b=a+b-a\cdot b$。

证明：先证明 $\langle I,\triangle\!\!\!\cdot\rangle$ 为阿贝尔群。
对于任意 $a,b\in I$，$a\triangle\!\!\!\cdot b=a+b-1\in I$，满足封闭性；
$a\triangle\!\!\!\cdot b=a+b-1=b+a-1=b\triangle\!\!\!\cdot a$，满足交换性；
对于任意 $a,b,c\in I$，

$$\begin{aligned}(a\triangle\!\!\!\cdot b)\triangle\!\!\!\cdot c&=(a+b-1)\triangle\!\!\!\cdot c\\&=a+b-1+c-1\\&=a+b+c-2\end{aligned}$$

$$\begin{aligned}a\triangle\!\!\!\cdot(b\triangle\!\!\!\cdot c)&=a\triangle\!\!\!\cdot(b+c-1)\\&=a+b+c-1-1\\&=a+b+c-2\end{aligned}$$

所以$(a \blacktriangle b) \blacktriangle c = a \blacktriangle (b \blacktriangle c)$,满足结合性;

对于任意$a \in I$,存在$1 \in I$,使得

$1 \blacktriangle a = 1 + a - 1 = a = a + 1 - 1 = a \blacktriangle 1$,

所以1是I中关于$\blacktriangle$的幺元;

对于任意$a \in I$,存在$2 - a \in I$,使得

$a \blacktriangle (2-a) = a + 2 - a - 1 = 1$,

$(2-a) \blacktriangle a = 2 - a + a - 1 = 1$,

所以$a \blacktriangle (2-a) = (2-a) \blacktriangle a = 1$,$2-a$是$a$的逆元;

因此$\langle I, \blacktriangle \rangle$是阿贝尔群。

再证明$\langle I, \triangle \rangle$是半群

对于任意$a,b \in I$,$a \triangle b = a + b - a \cdot b \in I$,满足封闭性;

对于任意$a,b,c \in I$,

$$\begin{aligned}(a \triangle b) \triangle c &= (a + b - a \cdot b) \triangle c \\ &= (a + b - a \cdot b) + c - (a + b - a \cdot b) \cdot c \\ &= a + b + c - a \cdot b - a \cdot c - b \cdot c + a \cdot b \cdot c\end{aligned}$$

$$\begin{aligned}a \triangle (b \triangle c) &= a \triangle (b + c - b \cdot c) = a + b + c - b \cdot c - a \cdot (b + c - b \cdot c) \\ &= a + b + c - b \cdot c - a \cdot b - a \cdot c + a \cdot b \cdot c\end{aligned}$$

所以$a \triangle (b \triangle c) = (a \triangle b) \triangle c$,满足结合性;

所以$\langle I, \triangle \rangle$是半群。

又因为$a \triangle b = a + b - a \cdot b = b + a - b \cdot a = b \triangle a$,满足交换性,

又因为$0 \triangle a = 0 + a - 0 \cdot a = a$,$a \triangle 0 = a + 0 - a \cdot 0 = a$,所以0是关于运算$\triangle$的幺元

因此$\langle I, \triangle \rangle$是含幺元可交换半群。

对于任意$a,b,c \in I$,有

$$\begin{aligned}a \triangle (b \blacktriangle c) &= a \triangle (b + c - 1) \\ &= a + b + c - 1 - a \cdot (b + c - 1) \\ &= 2 \cdot a + b + c - a \cdot b - a \cdot c - 1,\end{aligned}$$

$$\begin{aligned}a(\triangle b) \blacktriangle (a \triangle c) &= (a + b - a \cdot b) \blacktriangle (a + c - a \cdot c) \\ &= a + b - a \cdot b + a + c - a \cdot c - 1 \\ &= 2 \cdot a + b + c - a \cdot b - a \cdot c - 1,\end{aligned}$$

即有$a \triangle (b \blacktriangle c) = (a \triangle b) \blacktriangle (a \triangle c)$,

同理可证$(b \blacktriangle c) \triangle a = (b \triangle a) \blacktriangle (c \triangle a)$,即运算$\triangle$关于运算$\blacktriangle$是可分配的。

因此$\langle I, \blacktriangle, \triangle \rangle$,是有幺元的交换环。

3. 设$\langle R, +, \cdot \rangle$是一个环,证明:如果$a,b \in R$,则$(a+b)^2 = a^2 + a \cdot b + b \cdot a + b^2$。其中,$x^2 = x \cdot x$。

证明:$$\begin{aligned}(a+b)^2 &= (a+b) \cdot (a+b) \\ &= (a+b) \cdot a + (a+b) \cdot b\end{aligned}$$

$= a \cdot a + b \cdot a + a \cdot b + b \cdot b$

$= a^2 + a \cdot b + b \cdot a + b^2$

4. 设$\langle A, +, \cdot \rangle$是一个代数系统，其中$+$，$\cdot$为普通的加法和乘法运算，$A$为下列集合：

a) $A = \{x \mid x = 2n, n \in I\}$。

b) $A = \{x \mid x = 2n+1, n \in I\}$。

c) $A = \{x \mid x \geqslant 0 \text{ 且 } x \in I\}$。

d) $A = \{x \mid x = a + b\sqrt[4]{5}, a, b \in R\}$。

e) $A = \{x \mid x = a + b\sqrt{3}, a, b \in R\}$。

问$\langle A, +, \cdot \rangle$是整环吗？为什么？

解：a) 没有乘法幺元，不是整环。

b) 对于加法不封闭，不是整环。

c) 对于任意$x \neq 0$，不存在加法逆元，不是整环。

d) 是整环。

e) 是整环。

5. 证明：$\langle \{0,1\}, \oplus, \odot \rangle$是一个整环，其中运算$\oplus$和$\odot$由表5－17定义。

表5－17

$\oplus$	0	1
0	0	1
1	1	0

$\odot$	0	1
0	0	0
1	0	1

证明：先证$\langle \{0,1\}, \oplus \rangle$是阿贝尔群。

由$\oplus$的运算表可知运算满足封闭性，可交换性，且幺元为0，0和1均以自身为逆元。

$(0 \oplus 0) \oplus 0 = 0 \oplus (0 \oplus 0)$，$(0 \oplus 0) \oplus 1 = 0 \oplus (0 \oplus 1)$，

$(0 \oplus 1) \oplus 0 = 1 = 0 \oplus (1 \oplus 0)$…… 其余类似可验证，结合性成立。

所以$\langle \{0,1\}, \oplus \rangle$是阿贝尔群。

再考察$\langle \{0,1\}, \odot \rangle$。

由$\odot$的运算表可知运算满足封闭性、交换性、结合性，幺元为1，所以$\langle \{0, 1\}, \odot \rangle$是可交换独异点，又因为$1 \odot 1 = 1 \neq 0$，故满足是无零因子条件。

另外，对于任意的$x, y \in \{0,1\}$。

$0 \odot (x \oplus y) = 0 = 0 \oplus 0 = (0 \odot x) \oplus (0 \odot y)$

对于$1 \odot (x \oplus y)$，若$x = y$，则$1 \odot (x \oplus y) = 1 \odot 0 = 0 = \begin{cases} 0 \oplus 0 \\ 1 \oplus 1 \end{cases}$

$= \begin{cases} (1 \odot 0) \oplus (1 \odot 0) \\ (1 \odot 1) \oplus (1 \odot 1) \end{cases} = (1 \odot x) \oplus (1 \odot y)$，

若$x \neq y$，则$1 \odot (x \oplus y) = 1 \odot 1 = 1 = \begin{cases} 1 \oplus 0 \\ 0 \oplus 1 \end{cases} = \begin{cases} (1 \odot 1) \oplus (1 \odot 0) \\ (1 \odot 0) \oplus (1 \odot 1) \end{cases} =$

$(1\odot x)\oplus(1\odot y)$,

所以对于任意 $x,y,z\in\{0,1\}$,都有 $z\odot(x\oplus y)=(z\odot x)\oplus(z\odot y)$,

同理可证,$(x\oplus y)\odot z=(x\odot z)\oplus(y\odot z)$,所以运算 $\odot$ 对于运算 $\oplus$ 是可分配的。

因此 $\langle\{0,1\},\oplus,\odot\rangle$ 是整环。

6. 设 $\langle A,+,\cdot\rangle$ 是一个环,并且对于任意的 $a\in A$,都有 $a\cdot a=a$,证明:

a) 对于任意的 $a\in A$,都有 $a+a=\theta$,其中 θ 是加法幺元。

b) $\langle A,+,\cdot\rangle$ 是可交换环。

证明:a) 对于任意 $a\in A$,都有 $a+a\in A$,又因 $a\cdot a=a$,所以 $(a+a)\cdot(a+a)=a+a$,即 $a\cdot a+a\cdot a+a\cdot a+a\cdot a=a+a$,即有 $a+a+a+a=a+a+\theta$,因为 $\langle A,+\rangle$ 是群,所以 $a+a=\theta$。

b) 对于任意 $a,b\in A$,$a+b\in A$,有 $(a+b)\cdot(a+b)=a+b$,所以 $a\cdot a+a\cdot b+b\cdot a+b\cdot b=a+b$,即 $a+a\cdot b+b\cdot a+b=a+b$,所以 $a\cdot b+b\cdot a=\theta$,即 $a\cdot b=-b\cdot a$,由 a) 可知 $b\cdot a+b\cdot a=\theta$,即 $b\cdot a=-b\cdot a$,所以 $a\cdot b=b\cdot a$。即 $\langle A,+,\cdot\rangle$ 是可交换环。

7. 设 $\langle A,+,\cdot\rangle$ 是一个代数系统,其中 $+,\cdot$ 为普通的加法和乘法运算,A 为下列集合:

a) $A=\{x\mid x\geqslant 0,x\in I\}$。

b) $A=\{x\mid x=a+b\sqrt{3},a,b$ 均为有理数$\}$。

c) $A=\{x\mid x=a+b\sqrt[3]{5},a,b$ 均为有理数$\}$。

d) $A=\{x\mid x=a+b\sqrt{5},a,b$ 均为有理数$\}$。

c) $A=\{x\mid x=\frac{a}{b},a,b\in I_+$ 且 $a\neq k\cdot b\}$。

问 $\langle A,+,\cdot\rangle$ 是域否?为什么?

解:a) 对于任何 $x>0$,没有加法逆元,所以不是域。

b) 易证 $\langle A,+,\cdot\rangle$ 是环,又因乘法幺元是 1,$a+b\sqrt{3}$ 的乘法逆元是 $\frac{a-\sqrt{3}b}{a^2-3b^2}$,所以 $\langle A,+,\cdot\rangle$ 是域。

c) $b\neq 0$ 时 $a+b\sqrt[3]{5}$ 的乘法逆元不存在,因此不是域。

d) 易证 $\langle A,+,\cdot\rangle$ 是环,乘法幺元是 1,$a+b\sqrt{5}$ 的乘法逆元是 $\frac{a-\sqrt{5}b}{a^2-5b^2}$,所以 $\langle A,+,\cdot\rangle$ 是域。

e) 无乘法幺元,不是域。

8. 设 $\langle F,+,\cdot\rangle$ 是一个域,$S_1\subseteq F$,$S_2\subseteq F$,且 $\langle S_1,+,\cdot\rangle$,$\langle S_2,+,\cdot\rangle$ 都构成域,证明:$\langle S_1\cap S_2,+,\cdot\rangle$ 也构成一个域。

证明:因为 $\langle S_1,+\rangle$,$\langle S_2,+\rangle$ 都是 $\langle F,+\rangle$ 的子群,且都为阿贝尔群。$\langle S_1,\cdot\rangle$,$\langle S_2,\cdot\rangle$ 都是 $\langle F,\cdot\rangle$ 的子群,且都为阿贝尔群。所以 $\langle S_1\cap S_2,+\rangle$ 和 $\langle S_1\cap S_2,\cdot\rangle$ 分别是 $\langle F,+\rangle$ 和 $\langle F,\cdot\rangle$ 的子群,且为阿贝尔群。

在$\langle S_1,+,\cdot\rangle$中，运算·对于运算＋是可分配的，在$\langle S_2,+,\cdot\rangle$中运算·对于运算＋是可分配的，所以在$\langle S_1 \cap S_2,+,\cdot\rangle$中，运算·对于运算＋是可分配的。

因此$\langle S_1 \cap S_2,+,\cdot\rangle$构成域。

9. 设$\langle A,\bigstar,*\rangle$是一个关于运算★和＊分别具有幺元$e_1$和$e_2$的代数系统，并且运算★和＊彼此之间是可分配的，证明：对于A中所有的x，式$x\bigstar x = x*x = x$成立。

证明：因为$e_2 = e_1\bigstar e_2 = (e_1 * e_2)\bigstar e_2 = (e_1\bigstar e_2)*(e_2\bigstar e_2) = e_2*(e_2\bigstar e_2) = e_2\bigstar e_2$，

$e_1 = e_2 * e_1 = (e_2\bigstar e_1)*e_1 = (e_2*e_1)\bigstar(e_1*e_1) = e_1\bigstar(e_1*e_1) = e_1*e_1$，

所以对于A中任意x，有$x\bigstar x = (x*e_2)\bigstar(x*e_2) = x*(e_2\bigstar e_2) = x*e_2 = x$，

$x*x = (x\bigstar e_1)*(x\bigstar e_1) = x\bigstar(e_1*e_1) = x\bigstar e_1 = x$，

所以$x\bigstar x = x*x = x$成立。

10. 设$\langle A,\bigstar,*\rangle$是一个代数系统，且对于任意的$a\in A$，有$a\bigstar b = a$，证明：二元运算＊对于★是可分配的。

证明：对于任意$a,b,c\in A$，$a*(b\bigstar c) = a*b = (a*b)\bigstar(a*c)$，

$(a\bigstar b)*c = a*c = (a*c)\bigstar(b*c)$，

即二元运算＊对于★是可分配的。

历年考研真题评析

1. 设f和g都是$\langle G_1,\bigstar\rangle$到$\langle G_2,*\rangle$的群同态，且$H_1=\{x \mid x\in G_1 \wedge f(x)=g(x)\}$，试证$\langle H_1,\bigstar\rangle$是$\langle G_1,\bigstar\rangle$的子群。（大连理工大学考研真题）

【分析】 判断子群有三种方法：

第一种：1) H是一个有限子集；2) 运算★在H上封闭。

第二种：子集H中的任意元素a和b有$a\bigstar b^{-1}\in H$。

第三种：根据子群的定义，即证明子集H上的代数结构$\langle H,\bigstar\rangle$是一个群。

证明：显然$H_1\subseteq G_1$，(1) 对于任意的$a,b\in H_1$，有$f(a)=g(a)$，$f(b)=g(b)$。因为f和g都是群同态映射，所以有$f(a\bigstar b) = f(a)*f(b) = g(a)*g(b) = g(a\bigstar b)$，所以$a\bigstar b\in H_1$，运算封闭；

(2) H_1是G_1的子集，所以在H_1上保持可结合性；

(3) 设e是G_1的幺元，e'是G_2的幺元，则有$f(e)=e'=g(e)$，所以$e\in H_1$，即e是H_1的幺元；

(4) 对于任意的$a\in H_1$，有$f(a)=g(a)$，所以$f(a)^{-1}=g(a)^{-1}$，即$f(a^{-1}) = g(a^{-1})$，即$a^{-1}\in H_1$，存在逆元；

综上所述，$\langle H_1, \bigstar\rangle$ 是 $\langle G_1, \bigstar\rangle$ 的子群。

2. 设 $\langle G, *\rangle$ 为群，R 为 G 上等价关系且对任意 $x, y, z \in G$，若 $(x*z)R(y*z)$，则 xRy，设 $H=\{h \mid h \in G$ 且 $hRe\}$，求证 $\langle H, *\rangle$ 为 $\langle G, *\rangle$ 的子群。其中 e 是 $\langle G, *\rangle$ 的幺元。（山东大学考研真题）

【分析】 判断子群有三种方法：

第一种：1) H 是一个有限子集；2) 运算 $*$ 在 H 上封闭。

第二种：子集 H 中的任意元素 a 和 b 有 $a*b^{-1} \in H$。

第三种：根据子群的定义，即证明子集 H 上的代数结构 $\langle H, *\rangle$ 是一个群。

证明：显然 H 是 G 的子集，任给 $h_1, h_2 \in H$，则有 h_1Re 和 h_2Re，因为 R 是等价关系，则有 eRh_2，即有 h_1Rh_2，即 $h_1 * h_2^{-1} * h_2 Re * h_2$，则有 $h_1 * h_2^{-1} Re$，所以 $h_1 * h_2^{-1} \in H$，因此 $\langle H, *\rangle$ 为 $\langle G, *\rangle$ 的子群。

3. G 是奇数阶的 Abel 群，证明 G 中所有元素之积为单位元。（南京大学考研真题）

【分析】 群 G 的阶为奇数设为 $2m+1$，G 的所有元素之积中，只有 a 与 a^{-1} 是不同元素才能消掉 a，因此需要判断 a 与其逆元。

证明：由于 G 为奇数阶交换群，由拉格朗日定理知，不存在元素 a 满足 $a^2=e$，因此任给 $a \in G$ 且 $a \neq e$，则有 $a \neq a^{-1}$，即 a 与 a^{-1} 是两个不同的元素，G 为交换群，群 G 的阶设为 $2m+1$，因此 G 的所有元素之积 $=e*a_1*a_1^{-1}*a_2*a_2^{-1}*\cdots*a_m*a_m^{-1}=e$，其中 $a_1 \in G-\{e\}, a_2 \in G-\{e\}, \cdots, a_m \in G-\{e\}$。

4. ①$\langle G, *\rangle$ 是个群，H, K 是其子群，在 G 上定义二元关系 R：$\forall a, b \in G, aRb \Leftrightarrow$ 存在 $h \in H, k \in K$，使得 $b=h*a*k$，证明：R 是 G 上的等价关系。

② 在 ① 中，若 $|H|=m, |K|=n, |G|=mn$，m 与 n 互素，且 R 的某个等价类在 G 的乘法运算下构成 G 的一个子群，则 $R=G\times G$。（中科院计算机技术研究所考研真题）

【分析】 证明一个关系为等价关系，即需要证明这个关系满足自反性，对称性和传递性。

证明：①(1) 任给 $a \in G$，有 $a=e*a*e$，其中 e 为 G 中单位元，而 H, K 为 G 的子群，从而 $e \in H, e \in K$，所以有 aRa，满足自反性；

(2) 若 $aRb \Rightarrow$ 存在 $h \in H, k \in K$，使得 $b=h*a*k \Rightarrow a=h^{-1}*b*k^{-1}$，由于 H, K 为 G 的子群，所以 $h^{-1} \in H, k^{-1} \in K$，所以有 bRa，满足对称性；

(3) 若 $aRb, bRc \Rightarrow$ 存在 $h_1, h_2 \in H, k_1, k_2 \in K$，使得 $b=h_1*a*k_1, c=h_2*b*k_2$，由于 H, K 为 G 的子群，所以 $h_2*h_1 \in H, k_1*k_2 \in K$，使得 $c=(h_2*h_1)*a*(k_1*k_2)$，所以 aRc，满足传递性；

综上所述，R 是等价关系。

② 设是 G 的子群的那个 R 的等价类为 $[a]_R=\{x \mid x \in G \wedge aRx\}=\{x \mid x \in G$ 且存在 $h \in H, k \in K$，使 $x=h*a*k\}=\{h*a*k \mid h \in H, k \in K\}$，由于该等价类为 G 的子群，故对任意的 $h_1, h_2 \in H$，有 $(h_1*a*k_1)*(h_2*a*k_2)^{-1} \in [a]_R$，取 $k_1=k_2$，则得 $\forall h_1, h_2 \in H$ 有 $h_1*a^2*h_2^{-1} \in [a]_R$，从而可以从中推出 $h_1*a^{2r}*h_2^{(-1)} \in [a]_R$，由于 G 为有限群，必存在某个 r 使 $a^{2r}=e$，此时，有 $\forall h_1, h_2 \in H, h_1*h_2^{(-1)} \in [a]_R$，即 H

为 $[a]_R$ 的子群。

同理,K 为$[a]_R$ 的子群,所以 $m \mid |[a]_R|$,$n \mid |[a]_R|$,而 m 与 n 互 $\Rightarrow mn \mid |[a]_R|$,即 $|G| \mid |[a]_R|$,又$[a]_R$为 G 的子群,因此 $|[a]_R| \mid |G|$,从而 $|G| = |[a]_R|$,从而$[a]_R = G$,即 $\forall g \in G$。有 aRg,而 R 为等价关系,$\forall g_1, g_2 \in G$,由对称性 $aRg_1 \Rightarrow g_1Ra$。由传递性,$aRg_1 \wedge aRg_2 \Rightarrow g_1Ra \wedge aRg_2 \Rightarrow g_1Rg_2$。所以 $R = G \times G$。

5. G 为群,$a,b,c \in G, ab = cba, ac = ca, bc = cb$。

(1) 证明:若 a,b 的阶分别为 m,n,则 c 的阶整除 m 与 n 的最大公因子(m,n)。

(2) 若 a,b,c 的阶均为 2,给出集合 $S = \{a,b,c\}$ 的生成子群。(中国科学院软件研究所考研真题)

(1) 证明:由于 $ac = ca, bc = cb$,所以 c 与 a、b 均可交换,又由于 $ab = cba$,则等式右边同时乘 $n-1$ 次 b 得,$ab^n = cbab^{n-1} = cbcbab^{n-2} = c^2b^2ab^{n-2} = \cdots = c^nb^na$,从而 $c^n = e$,

同理,左乘 $m-1$ 次 a 得,$a^mb = c^mba^m$,因此 $c^m = e$,由于 c 的阶 k 是满足 $c^k = e$ 的最小正整数,可推得 $k \mid m, k \mid n$,即 $k \mid (m,n)$。

(2) 解:$S = \{e,a,b,c,ab,ac,bc,abc\}$。

6. $\langle G,*\rangle$ 是群,$\langle H,*\rangle$ 是$\langle G,*\rangle$ 的子群,对于任意的 $a \in G$,有 $aH = Ha$ 的充要条件是对于任意的 $a \in G, h \in H$,有 $a^{-1} * h * a \in H$。(上海交通大学考研真题)

证明:(1) 若有 $aH = Ha$,则对于任意的 $a \in G, h \in H$,有 $h * a \in aH = Ha$,则存在 $h_1 \in H$ 使得 $h * a = a * h_1$,即 $a^{-1} * h * a = h_1$,也就有 $a^{-1} * h * a \in H$;

(2) 若对于任意的 $a \in G, h \in H$,若 $h * a \in Ha$,而 $a^{-1} * h * a \in H$,设 $a^{-1} * h * a = h_1 \in H$,则 $h * a = a * h_1 \in aH$,即 $Ha \subseteq aH$;

若 $a * h \in aH$,而 $a * h * a^{-1} \in H$,设 $a * h * a^{-1} = h_2 \in H$,则 $a * h = h_2 * a \in Ha$,即 $aH \subseteq Ha$;

即 $aH = Ha$。