离散数学复习题

代数系统部分

1、设$<H, *>$和$<K, *>$都是交换群$<G, *>$的子群，

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

证明：$<HK, *>$是$<G, *>$的子群。

2、写出群$<Z_{30}, \oplus>$的所有生成元和生成子群，并画出子群格。

3、Klein四元群 G 和$<Z_6, \oplus>$的子群格。

4、在Z^+上定义二元运算 ：

$$\forall x, y \in Z,\quad x \circ y = x + y + 2xy,$$

① 二元运算∘是否满足交换律、结合律和幂等律？

② 求二元运算∘在Z中的单位元、零元和所有可逆元素的逆元。

5、求群<N6,＋6>的所有非平凡子群。

6、设 σ, τ 是五元置换 $\sigma = (1\ 5)(2\ 3\ 4)$,

$$\tau = (1\ 4\ 2\ 5\ 3)$$

求 $\sigma\tau, \tau\sigma$ 和 $\tau^{-1}\sigma$ 。

7、设 I 是整数集合，＋是普通加法，

$\langle I,+,0\rangle$ 是代数系统，设 $B=\{x \mid x=2n \wedge n\in I\}$，

证明：$\langle B,+,0\rangle$ 是 $\langle I,+,0\rangle$ 的子代数。

8、设R为实数集，＋和×分别为R上的加法和乘法运算，证明$<R,+>$与$<R,\times>$同态。

9、设$<G,*>$是n阶阿贝尔群，令f是从G到G的一个映射，定义为：$f(x)=x^{-1}$，验证f是自同构。

10、设f为由代数系统$<A,*>$到代数系统$<B,\circ>$的一个同态映射。

⑴如果$<A,*>$是半群，则同态像$<f(A),\circ>$也是半群。

⑵如果$<A,*>$是独异点，则同态像$<f(A),\circ>$也是独异点。

⑶如果$<A,*>$是群，则同态像$<f(A),\circ>$也是群。

答案

1、设$<H, *>$和$<K, *>$都是交换群$<G, *>$的子群，令

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

证明：$<HK, *>$是$<G, *>$的子群。

证：

① 因为$<H, *>$和$<K, *>$都是$<G, *>$的子群，所以$e\in H\wedge e\in K$，

因此$e = e*e\in HK$，所以HK为G的非空子集。

②$\forall x,y\in HK$，则一定存在$h_1, h_2\in H \wedge k_1, k_2\in K$，使得$x = h_1 * k_1, y = h_2 * k_2$，（2分）从而

$$x * y^{-1} = (h_1 * k_1) *(h_2 * k_2)^{-1}= (h_1 * k_1) *(k_2^{-1} * h_2^{-1})$$

$$=(h_1 * h_2^{-1}) *(k_1 * k_2^{-1})$$

因为$<H, *>$是$<G, *>$的子群, 所以$h_1 * h_2^{-1}\in H$，

同理，因为，$<K, *>$是$<G, *>$的子群,

所以$k_1 * k_2^{-1}\in K$，从而$x * y^{-1}\in HK$，因此HK是$<G, *>$的子群。

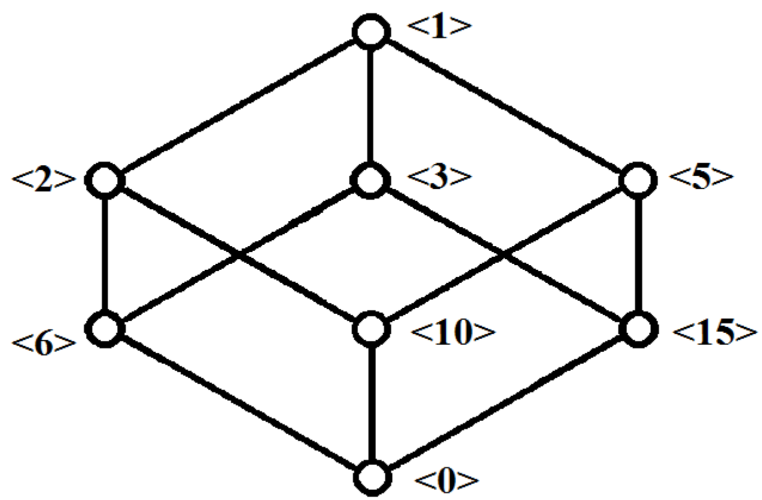
答案

2、写出群$<Z_{30}, \oplus>$的所有生成元和生成子群，并画出子群格。

解：生成元：1、7、11、13、17、19、23、29

生成子群：<0>、<1>、<2>、<3>、<5>、<6>、<10>、<15>

子群格：



答案

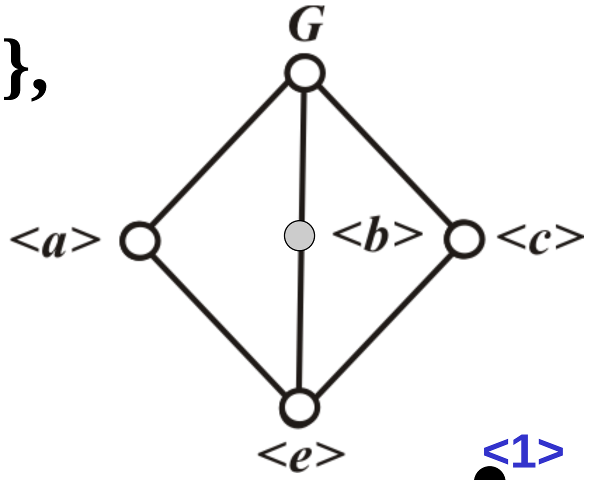
3、Klein四元群 *G* 和$\langle Z_6,\oplus\rangle$的子群格。

解：（1）Klein四元群G={e, *a*, *b*, *c*}, 单位元为*e*，

它的所有子群是： *G*，$\langle e\rangle = \{ e \}$,

$\langle a\rangle = \{ e, a \}$, $\langle b\rangle = \{ e, b \}$,

$\langle c\rangle = \{ e, c \}$.



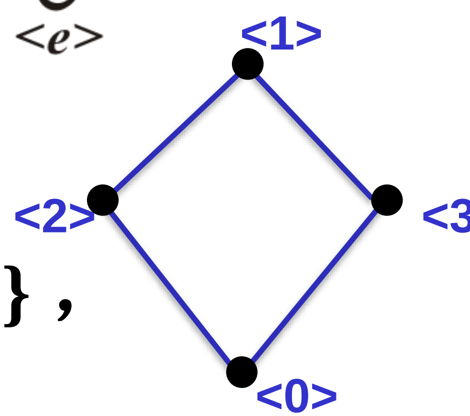
子群格如右图所示：

（2） $\langle Z_6,\oplus\rangle$单位元是0，

它的所有子群是： Z_6 , $\langle 0\rangle = \{0\}$,

$\langle 1\rangle= Z_6 = \{0,1,2,3,4,5\}$, $\langle 2\rangle=\langle 4\rangle= \{0,2,4\}$，

$\langle 3\rangle=\langle 6\rangle= \{0,3,6\}$



子群格如右图所示：

答案

4、在Z^+上定义二元运算 ∘：

$$\forall x, y \in Z,\quad x \circ y = x + y + 2xy,$$

① 二元运算∘是否满足交换律、结合律和幂等律？

② 求二元运算∘在Z中的单位元、零元和所有可逆元素的逆元。

证明：交换律：$\forall x, y \in Z,\quad x \circ y = x + y + 2xy = y \circ x,$ 满足交换律

结合律：$\forall x, y, z \in Z,\quad (x \circ y) \circ z = (x + y + 2xy) \circ z$

$$= x + y + z + 2xy + 2xz + 2yz + 4xyz$$

$x \circ (y \circ z) = x \circ (y + z + 2yz) = x + y + z + 2xy + 2xz + 2yz + 4xyz$ 满足结合律

幂等律：$1 \in Z,\quad 1 \circ 1 = 1 + 1 + 2 \times 1 \times 1 \neq 1,$ 不满足幂等律

单位元：设$e \in Z$为单位元, $\forall x \in Z$, 则 $e \circ x = x \circ e = e + x + 2ex = x \Rightarrow e = 0$

零元：设$\theta \in Z$为零元, $\forall x \in Z$, 则$\theta \circ x = x \circ \theta = \theta + x + 2\theta x = \theta \Rightarrow \theta = -1/2 \notin Z$ 无零元

逆元：$\forall x \in Z$, 设$x^{-1} \in Z$为x的逆元，则

$x^{-1} \circ x = x \circ x^{-1} = x + x^{-1} + 2xx^{-1} = 0 \Rightarrow x^{-1} = -x/(1 + 2x)$

从而，$x = 0$的逆元$x^{-1} = 0$，$x = -1$的逆元$x^{-1} = -1$，其它元素无逆元。

答案

5、求群<N6,＋6>的所有非平凡子群。

解: 作N_6={0,1,2,3,4,5}上模6加法$+_6$的运算表，如右表所示。取N_6的子集S_1={0,2,4}和S_2={0,3}，它们的运算表如下表所示。从表中可以看出,模6加法$+_6$在S_1和S_2上封闭。子群判定定理三，有限群的子群判定。

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$+_6$	0	3
0	0	3
3	3	0

$+_6$	0	2	4
0	0	2	4
2	2	4	0
4	4	0	2

答案

6、设 σ, τ 是五元置换 $\sigma = (1\ 5)(2\ 3\ 4)$,

$\tau = (1\ 4\ 2\ 5\ 3)$

求 $\sigma\tau, \tau\sigma$ 和 $\tau^{-1}\sigma$。

解:

$$\sigma\tau = (1\ 3\ 2)(4\ 5);$$

$$\tau\sigma = (1\ 2)(3\ 5\ 4);$$

$$\tau^{-1}\sigma = (1\ 4\ 5\ 3)(2);$$

答案

7、设I是整数集合，＋是普通加法，

$<I,+,0>$是代数系统，设$B=\{x|x=2n\wedge n\in I\}$，

证明：$<B,+,0>$是$<I,+,0>$的子代数。

证明： 任取B的两个元素$2n_1$和$2n_2$，$n_1\in I$，$n_2\in I$。

$2n_1+2n_2=2(n_1+n_2)\in B$　　$n_1+n_2\in I$

所以，加法＋在B上封闭。

又　$0=2\times 0\in B$

所以$<B,+,0>$ 是$<I,+,0>$的子代数。

答案

8、设R为实数集，＋和×分别为R上的加法和乘法运算，证明<R,＋>与<R,×>同态。

证明： $\forall x\in R$，设$f(x)=2^x$，对任意$y, z\in R$有

$$f(y+z)=2^{y+z}=2^y\times 2^z=f(y)\times f(z)$$

故<R,＋>与<R,×>同态。

9、设<G,*>是n阶阿贝尔群，令f是从G到G的一个映射，定义为：$f(x)=x^{-1}$，验证f是自同构。

证明： $\forall x,y\in G$，$f(x*y)=(x*y)^{-1}=y^{-1}*x^{-1}=x^{-1}*y^{-1}=f(x)*f(y)$

当$x\neq y$时，如果$x^{-1}=y^{-1}$，则$x=(x^{-1})^{-1}=(y^{-1})^{-1}=y$，矛盾。所以$x^{-1}\neq y^{-1}$，即$f(x)\neq f(y)$，$f$是单同态。

$\forall x\in G$，$x=(x^{-1})^{-1}$，$x^{-1}\in G$，使$f(x^{-1})=(x^{-1})^{-1}=x$，故$f$是满同态。

综上，f既是单同态又是满同态，因此是自同构。

答案

10、设f为由代数系统$<A,*>$到代数系统$<B,\circ>$的一个同态映射。

(1)如果$<A,*>$是半群，那么同态像$<f(A),\circ>$也是半群。

证明：(1) 设$<A,*>$是半群，$\forall a,b\in f(A)$，必有$x,y\in A$，使

$$f(x)=a,\quad f(y)=b$$

因为$<A,*>$是半群，必有$x*y\in A$，于是

$$a\circ b=f(x)\circ f(y)=f(x*y)\in f(A)$$，即$\circ$在$f(A)$上封闭。

$\forall a,b,c\in f(A)$，必有$x,y,z\in A$，使得$f(x)=a$，$f(y)=b$，$f(z)=c$

$$(a\circ b)\circ c=(f(x)\circ f(y))\circ f(z)=f(x*y)\circ f(z)=f((x*y)*z)=f(x*(y*z))$$

$$=f(x)\circ f(y*z)=f(x)\circ(f(y)\circ f(z))=a\circ(b\circ c)$$

即$\circ$在$f(A)$上满足结合律。

所以$<f(A),\circ>$是半群。

答案

10、设f为由代数系统$<A,*>$到代数系统$<B,\circ>$的一个同态映射。

⑵如果$<A,*>$是独异点，那么同态像$<f(A),\circ>$也是独异点。

证明：

(2) 设$<A,*>$是独异点，e是A中的幺元。

$\forall a \in f(A)$，必有$x \in A$，使得$f(x)=a$，于是

$$a \circ f(e)=f(x) \circ f(e)=f(x*e)=f(x)=a$$

$$f(e) \circ a=f(e) \circ f(x)=f(e*x)=f(x)=a$$

即$f(e)$是$f(A)$中的幺元。

因此$<f(A),\circ>$是独异点。

答案

10、设f为由代数系统$<A,*>$到代数系统$<B,\circ>$的一个同态映射。

⑶ 如果$<A,*>$是群，那么同态像$<f(A),\circ>$也是群。

证明：

⑶设$<A,*>$是群，$\forall a\in f(A)$，必有$x\in A$，使得$f(x)=a$，

因为$<A,*>$是群，$x^{-1}\in A$且$f(x^{-1})\in f(A)$，于是

$$a\circ f(x^{-1})=f(x)\circ f(x^{-1})=f(x*x^{-1})=f(e)$$

$$f(x^{-1})\circ a=f(x^{-1})\circ f(x)=f(x^{-1}*x)=f(e)$$

所以$a^{-1}= f(x)^{-1}=f(x^{-1})\in f(A)$。

因此$<f(A),\circ>$是群。

（补充）证明阶数小于6的群都是阿贝尔群。

Lagrange定理：设$<G,*>$是有限群，$<H,*>$是$<G,*>$的子群。则$|H|$是$|G|$的因子。

证明：设$<G,*>$是阶小于6的群。

若$|G|=1$，则群$<G,*>$是平凡的，显然是阿贝尔群。

若$|G|$是素数，即$|G|$是2，3和5。由推论2知

$G=\{a,a^2,\cdots,a^k\}$，其中$k=2,3,5$。$\forall a^i \in G$，$\forall a^j \in G$，

$a^i*a^j= a^{i+j}=a^j*a^i$，所以$<G,*>$ 阿贝尔群。

若$|G|=4$，若G中含有4阶元，比如说a，则$G=\{a,a^2, a^3,a^4\}$。由刚才的分析可知$<G,*>$是阿贝尔群。若G中不含4阶元，根据Lagrange定理，G中只含1阶和2阶元，即$\forall a \in G$，有$a^2=e$。则$(a*b)*(a*b)=e=e*e=(a*a)*(b*b)$，根据拉格朗日定理，$G$是阿贝尔群。