书面作业6.1 参考解答或提示

第1部分 基础

第2部分 理论

T1 实数集R上的二元运算*：a*b=a+b-a◦ b，+、-、◦ 为一般的加法、减法、乘法运算，请问代数结构<R; *>是否有单位元、零元与幂等元，如果有单位元，哪些元素有逆元?

1) 设e是单位元，则对a∈R, 有e*a=a*e=a。考虑e*a=a，即e*a=e+a-ea=a, 亦即e(1-a)=0, 由于a是任意的，故e=0.若e=0，即有0*a=a*0=a.因此，0是运算*的单位元.

2) 设z是零元，则对a∈R, 有z*a=a*z=z。考虑z*a=z，即z*a=z+a-za=z, 亦即 (1-z) a=0, 由a的任意性有z=1. 从而有1*a=a*1=1.因此, 1是运算*的零元.

3) 设a为幂等元, 则应有a*a=a, 即a*a=a+a-aa=a，亦即a(1-a)=0，则a=0或1. 因此，运算*的幂等元为0或1.

4) 由1)知单位元为0，设b是a的逆元，则应有a*b=0，即a+b-ab=0，则b=a/(a-1)，因此，对于R中除1以外的任何元素都有逆元a/(a-1).

T2 证明：有限半群存在幂等元.

提示：注意元素“有限”、“结合律”, 则可以构造出元素相等关系，从而可以进一步构造出幂等元.

设<S；*>是有限半群，需证 ∃a∈S，有a*a=a.

对∀b∈S，由运算封闭性，有b^2=b*b∈S,进一步可得: b^3，b^4，...∈S.

又S有限，故 ∃i，j∈N，j>i≥1 使得$b^i=b^j$.

从而利用半群的可结合性有 $b^i=b^j=b^{j-i}*b^i$.

现令p=j-i, 有 $b^i=b^p*b^i$

1) 若p=i, 则b^i即为幂等元.

2)若p>i, 则，$b^i*b^{p-i}=(b^p*b^i)*b^{p-i}$, 即：$b^p=b^p*b^p$.

于是 b^p为幂等元.

3) 若p<i,则可将$b^i=b^p*b^i$代入等式$b^i=b^p*b^i$右端的b^i 共计k-1次(k>1)，

得到等式：$b^i=b^{kp}*b^i$, 使得kp≥i. 于是有，kp=i或 kp>i，类似1) 2)证明方法，可得b^{kp}为幂等元.

综上，有限半群存在幂等元.

T3 设h是代数结构V_1=<S；o>到V_2=<S′；o′>的同态映射，h的同态像为h(S)⊆ S′, 证明:

(1) <h(S)；o′>为V_2的子代数;

(2) h是V_1到<h(S)；o′>的满同态映射;

(3) 如果V_1关于运算o有单位元e或零元z，则同态像h(S)中有关于o′的单位元h(e)或零元h(z).

(1) h是V_1到V_2的映射，h(S)⊆ S′，因此，h也是V1到h(S)的映射，且任意x∈h(S)，均有h下的原像x∈S，故h是V_1到h(S)的满射.

又h为V_1到V_2的同态映射，于是∀x,y∈S,h(xoy)=h(x)o′h(y),而h(x),h(y)∈h(S),故h也是V_1到<h(S)；o′>的同态映射.

所以，h是V_1到<h(S)；o′>的满同态映射.

(2) 首先注意到，h(S)⊆ S′，

对∀x′,y′∈h(S),有h下的原像x,y∈S,使得h(x)=x′,h(y)=y′,xoy∈S,

从而x′o′y′=h(x)o′h(y)=h(xoy)∈h(S)，

于是有V_2上的运算o′在h(S)上满足封闭性，

所以，<h(S)；o′>为V_2的子代数.

（3）h是V_1到<h(S)；o'>的满同态映射, e为V_1的单位元,

对∀x'∈h(S)，∃x∈S，使得x'=h(x),

于是，h(e)o'x'= h(e)o'h(x)=h(eox)=h(x),

且x'o'h(e)= h(x)o'h(e) =h(xoe)=h(x),

故h(e)o'x'= x'o'h(e)=x'.

所以<h(S)；o'>的存在单位元h(e).

类似地，

h是V_1到<h(S)；o'>的满同态映射, z为V_1的零元,

对∀x'∈h(S)，∃x∈S，使得x'=h(x),

于是，h(z)o'x'= h(z)o'h(x)=h(zox)=h(z),

且x'o'h(z)= h(x)o'h(z) =h(xoz)=h(z),

故h(z)o'x'= x'o'h(z)=h(z).

所以<h(S)；o'>的存在零元h(z).

T4 设f，g都是< S；*>到< S'；*'>的同态，并且*' 运算均满足交换律和结合律，证明:如下定义的函数h:

S→S'：h(x)=f(x)*'g(x)是<S；*>到<S'；*'>的同态.

由于 f，g 都是 S 到 S'的函数，*'是 S'上的运算， h(x) = f(x)*'g(x) ,

所以h是S到 S' 的函数.

又 x,y∈S， h(x*y)=f(x*y)*'g(x*y)=(f(x)*'f(y))*'(g(x)*'g(y))

=f(x)*'(f(y)*'g(x))*'g(y)

=f(x)*'(g(x))*'f(y))*'g(y)

=(f(x)*'g(x))*'(f(y)*'g(y))

=h(x) *'h(y)

h 是<S; *>到<S'; *'>的同态.

T5 给定代数结构 A=<X；∘ >、B=<Y；*> 和 C=<Z；×>.设 f：X→Y 是从A到B的同态，且 g：Y→Z 是从B到C的同态，试证明gof：X→Z必定是从A到C的同态, gof为函数f,g的复合.

f 是 X 到 Y 的映射，g 是从 X 到 Y 的映射，因此 f、g 的复合函数 gof 是 X 到 Z 的映射.而 gof(x1∘ x2) =g(f(x1)*f(x2))=g(f(x1))×g(f(x2))= gof (x1)×gof (x2).因此，gof： X→Z 是从 A 到 C 的同态.

T6 复数的加、乘运算可以转换为矩阵的加、乘运算，请从代数结构同构的角度进行证明.

提示：设复数的集合 C={a+bi|a+bi 为复数, a,b ∈ R}, 相应地可以定义 2×2 矩阵集合：

M={ $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ | a, b∈R }.

建立映射 f: C—>M, f(a+bi)= $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$,

容易证明 f 是从<C; +,*>到<M; +,*>的同构映射.

T7 代数结构间的同构关系是等价关系.

设〈X；°〉，〈Y；*〉，〈Z；+〉是任意的三个代数结构，并设同构关系用"≌"表示，下面 ≌ 证明满足自反性、对称性以及传递性.

(1) 自反性：显然有〈X；°〉≌〈X；°)，即是自反的.

(2) 对称性：如果〈X；°〉≌〈Y；*〉则必存在一个双射 g: X→Y，使得若x1，x2∈X，并有：

g(x1°x2)=g(x1)*g(x2)

根据双射的定义，必存在一个双射的逆映射g-1: Y→X.

现要证对g-1: Y→X，若y1，y2∈Y，必有:

g-1(y1*y2)=g-1(y1)°g-1(y2)

设对任意的y1，y2∈Y必存在x1，x2∈X，使得g(x1)=y1，g(x2)=y2，亦即g-1(y1)=x1，g-1(y2)=x2，故有：

g-1(y1*y2) = g-1(g(x1)*g(x2)) =g-1(g(x1°x2)) =x1°x2

又

g-1(y1)°g-1(y2)=x1°x2

所以

g-1(y1*y2)=g-1(y1)°g-1(y2)

因此，〈Y；*〉≌〈X；°〉，所以≌是对称的.

(3) 传递性：如果有〈X；°〉≌〈Y；*〉，且〈Y；*〉≌〈Z；+〉，要证明〈X；°〉≌〈Z；+〉.由条件亦即存在双射g: X→Y与h: Y→Z，使得对任意x1，x2∈X和y1，y2∈Y，必有：

g(x1°x2)=g(x1)*g(x2)， h(y1*y2)=h(y1)+h(y2)

下面证明存在一个双射f: X→Z，使得对任意x1，x2∈X，有f(x1°x2)=f(x1)+f(x2)，

现令f=h·g，即h与g的复合映射，由于g，h均是双射射，所以f亦是双射.

又 f(x1°x2) =h·g(x1°x2)=h(g(x1)*g(x2))=h(g(x1))+h(g(x2))

=h·g(x1)+h·g(x2)=f(x1)+f(x2)

所以，≌ 是传递的.

综上，≌ 是等价关系，即代数结构间的同构关系是等价关系.

T8 已知代数结构<Z; +>以及<C; $+_3$>，其中， Z 为整数集合，C={0, 1, 2}. +，$+_3$为 Z、C 上的一般加法、加模 3 运算. 请定义<Z; +>到<C; $+_3$>的同态映射φ，并按照同态基本定理，构造相应同态三角形，并给出解释.

定义φ: Z->C, ϕ(i)=i(mod3), i∈Z,

易证明ϕ为同态映射， 其中，同态映射的证明：φ(i+j)=(i+j)(mod 3), 而φ(i)+φ(j) =i (mod 3)$+_3$j (mod 3)=((i-3k_1)+(j-3k_2)) (mod 3)=(i+j-3(k_1+k_2)) (mod 3)=(i+j) (mod 3)，其中, k_1 k_2满足 0≤i-3k_1<3, 0≤j-3k_2<3；

定义ρ_ϕ：xρ_ϕy 当且仅当ϕ(x)=ϕ(y)；易证明ρ_ϕ为<Z; +>上同余关系，相应商代数为: <Z/ρ_ϕ, *>， Z/ρ_ϕ={[0]ρ_ϕ, [1]ρ_ϕ, [2]ρ_ϕ]}，[x]ρ_ϕ*[y]ρ_ϕ=[x+y]ρ_ϕ;

定义 h：Z->Z/ρ_ϕ : h(i)=[i]ρ_ϕ, i∈Z; 定义 f: Z/ρ_ϕ->C，f([x]ρ_ϕ)=ϕ(x), [x]ρ_ϕ∈Z/ρ_ϕ.

进而，可以证明h为Z到Z/ρ_ϕ的满同态映射，f为Z/ρ_ϕ到C的同构映射.

T9 If <A;+>is a algebraic structure, where the binary operation + is associative, and <A;+>has an identity, and its element has an inverse, then <A;+> is called a group(群).

A ring(环) is an algebra with the structure<A; +, *>, where <A;+> is a commutative group(交换群, i.e. , <A;+> is a group and the operation + is commutative），<A; *> is a monoid (独异点/单位半群), and the operation * distributes over + from the left and the right（即*对+满足左分配律）.

If <A; +, *> is a ring with the additional property that <A – {0}; *>is a commutative group, then it's called a field(域). Finite field, also known as Galois Field(named after Evariste Galois), refers to a field in which there exists finitely many elements. The most popular and widely used application of Galois Field is in Cryptography(密码学). Since each byte of data are represented as a vector in a finite field, encryption and decryption（加密与解密） using mathematical arithmetic is very straightforward and is easily manipulable.

Now, let N_5 = {0, 1, 2, 3, 4}, and let $+_5$ and $*_5$ be the two operations of addition mod 5（加模 5 求余）and multiplication mod 5（乘模 5 求余）, respectively. Please show that <N_5; $+_5$, $*_5$>is a field.

<N_5; $+_5$>是交换群：运算满足交换律、结合律，有单位元 0，0 的逆元是 0，1 与 4 互为逆元，2 与 3 互为逆元.

<N_5-{0}; $*_5$>是交换群：运算满足交换律、结合律，有单位元 1，1 的逆元是 1，2 与 3 互为逆元，4 的逆元为其自身.

可以验证，$*_5$对$+_5$是满足左右分配律的.

T10 (定义满足某些性质的二元运算) Let A = {a, b}. For each of the following problems, find an operation table satisfying the given condition for a binary operation $\circ$ on A.

a. <A; $\circ$> is a group（群的定义请参考 T8）.

b. <A; $\circ$> is a monoid but not a group.

c. <A; $\circ$> is a semigroup(半群) but not a monoid.

∘	a	b
a	a	b
b	b	a

a.

∘	a	b
a	a	b
b	b	b

b.

∘	a	b
a	b	b
b	b	b

∘	a	b
a	a	b
b	a	b

c.

T11 Show that there is an epimorphism(满同态) between the set B of binary numerals(二进制数) with the usual binary addition(一般二进制加法) defined on B and the set N of natural numbers with the usual addition on N.（提示：注意到二进制与十进制之间的对应关系）

设$+_{bi}$、+分别为 B、N 上二进制加法与普通加法运算，显然, 容易证明运算满足封闭性. 进一步可以定义 f_{two}为 B 到 N 的映射: $f_{two}(b_k\ b_{k-1} \ldots b_1b_0) = 2^kb_k+2^{k-1}b_{k-1} + \ldots + 2^1b_1+ 2^0b_0$., 可以证明 f_{two} 为满射，且满足同态方程: $f_{two}(x+_{bi}y)=f_{two}(x)+f_{two}(y)$. 故代数结构 <B; $+_{bi}$>到 <N; +>存在满同态关系.

T12 Find the three homomorphisms(定义 3 个同态映射) that exist from the algebra <N_3; $+_3$> to the algebra <N_6; $+_6$> where , where $+_3$,$+_6$ is the operation of addition mod 3 or 6.（提示：$+_3$,$+_6$是加模 3，加模 6 运算，注意定义需要满足同态方程）

3 个同态映射分别为 f, g, and h:

f(0) = 0, f(1) = 0, f(2) = 0;

g(0) = 0, g(1) = 2, g(2) = 4;

h(0) = 0, h(1) = 4, h(2) = 2.

T13 Suppose we need a function f : $N_8 \rightarrow N_8$ with the property that f (1) = 3; and also, f must be a homomorphism(同态) from the algebra <N_8; $+_8$> to itself, where $+_8$ is the operation of addition mod 8. Please finish the definition of f. (提示：利用需要满足的同态方程来定义)

假设 f 是同态映射，0 为的单位元，易得 f(0)=0. 注意到 f(2) = f(1 $+_8$ 1) = f(1) $+_8$ f(1) = 3 $+_8$ 3 = 6. 于是 f(3) = f(1 $+_8$ 2) = f(1) $+_8$ f(2) = 3 $+_8$ 6 = 1. 类似地, 有: f(4) = 4, f(5) = 7, f(6) = 2, and f(7) = 5.

下面证明，上述定义下，f满足同态方程：f(x $+_8$ y) = f(x) $+_8$ f(y) for all x, y ∈ N_8.

事实上，可以验证：f(1$+_8$ ... $+_8$ 1) = f(1)$+_8$ ... $+_8$ f(1) , n次$+_8$运算，0≤n≤7. 从而可以证明同态方程成立,

如：f(3 $+_8$ 4) = f(1 $+_8$ 1 $+_8$ 1 $+_8$ 1 $+_8$ 1 $+_8$ 1 $+_8$ 1)

= f(1) $+_8$ f(1) $+_8$ f(1) $+_8$ f(1) $+_8$ f(1) $+_8$ f(1) $+_8$ f(1)

= [f(1) $+_8$ f(1) $+_8$ f(1)] $+_8$ [f(1) $+_8$ f(1) $+_8$ f(1) $+_8$ f(1)]

= f(1 $+_8$ 1 $+_8$ 1) $+_8$ f(1 $+_8$ 1 $+_8$ 1 $+_8$ 1)

= f(3) $+_8$ f(4).

（另一方面，注意到，f(x)=3x (mod 8),可证明f(x$+_8$y)=f(x)$+_8$f(y)，即：3(x$+_8$y) mod 8=3x mod 8$+_8$3y mod 8 ）

第3部分 综合应用