



第10次作业 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 $*$: $a*b=a+b-a \circ b$, $+$ 、 $-$ 、 \circ 为一般的加法、减法、乘法运算, 请问代数结构 $\langle R; *$ 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 $a \in R$, 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 $a \in R$, 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 $\langle S; * \rangle$ 是有限半群, 需证 $\exists a \in S$, 有 $a*a=a$ 。

对 $\forall b \in S$, 由运算封闭性, 有 $b^2=b*b \in S$, 进一步可得: $b^3, b^4, \dots \in S$ 。

又 S 有限, 故 $\exists i, j \in \mathbb{N}, j > i \geq 1$ 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, $b^i*b^p=(b^p*b^i)*b^{p-i}$, 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 $kp \geq i$ 。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 $V_1=\langle S; \circ \rangle$ 到 $V_2=\langle S'; \circ' \rangle$ 的同态映射, h 的同态像为 $h(S) \subseteq S'$, 证明:

- (1) $\langle h(S); \circ' \rangle$ 为 V_2 的子代数;
 - (2) h 是 V_1 到 $\langle h(S); \circ' \rangle$ 的满同态映射;
 - (3) 如果 V_1 关于运算 \circ 有单位元 e 或零元 z , 则同态像 $h(S)$ 中有关于 \circ' 的单位元 $h(e)$ 或零元 $h(z)$ 。
- (1) h 是 V_1 到 V_2 的映射, $h(S) \subseteq S'$, 因此, h 也是 V_1 到 $h(S)$ 的映射, 且任意 $x \in h(S)$, 均有 h 下的原像 $x \in S$, 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 $\forall x, y \in S, h(xoy)=h(x)\circ'h(y)$, 而 $h(x), h(y) \in h(S)$, 故 h 也是 V_1 到 $\langle h(S); \circ' \rangle$ 的同态映射。

所以, h 是 V_1 到 $\langle h(S); \circ' \rangle$ 的满同态映射。

(2) 首先注意到, $h(S) \subseteq S'$,

对 $\forall x', y' \in h(S)$, 有 h 下的原像 $x, y \in S$, 使得 $h(x)=x', h(y)=y', xoy \in S$,

从而 $x'\circ'y'=h(x)\circ'h(y)=h(xoy) \in h(S)$,

于是有 V_2 上的运算 \circ' 在 $h(S)$ 上满足封闭性,

所以, $\langle h(S); \circ' \rangle$ 为 V_2 的子代数。



(3) h 是 V_1 到 $\langle h(S); o' \rangle$ 的满同态映射, e 为 V_1 的单位元,

对 $\forall x' \in h(S)$, $\exists x \in S$, 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 $\langle h(S); o' \rangle$ 的存在单位元 $h(e)$.

类似地,

h 是 V_1 到 $\langle h(S); o' \rangle$ 的满同态映射, z 为 V_1 的零元,

对 $\forall x' \in h(S)$, $\exists x \in S$, 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 $\langle h(S); o' \rangle$ 的存在零元 $h(z)$.

T4 设 f, g 都是 $\langle S; * \rangle$ 到 $\langle S'; *' \rangle$ 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 :

$S \rightarrow S'$: $h(x) = f(x) *' g(x)$ 是 $\langle S; * \rangle$ 到 $\langle S'; *' \rangle$ 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 $x, y \in S$, $h(x * y) = f(x * y) *' g(x * y) = (f(x) *' f(y)) *' (g(x) *' g(y))$

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

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

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

$= h(x) *' h(y)$

h 是 $\langle S; * \rangle$ 到 $\langle S'; *' \rangle$ 的同态.

T5 给定代数结构 $A = \langle X; \circ \rangle$, $B = \langle Y; * \rangle$ 和 $C = \langle Z; \times \rangle$. 设 $f: X \rightarrow Y$ 是从 A 到 B 的同态, 且 $g: Y \rightarrow Z$ 是从 B 到 C 的同态, 试证明 $g \circ f: X \rightarrow Z$ 必定是从 A 到 C 的同态, $g \circ f$ 为函数 f, g 的复合.

f 是 X 到 Y 的映射, g 是从 Y 到 Z 的映射, 因此 f, g 的复合函数 $g \circ f$ 是 X 到 Z 的映射. 而 $g \circ f(x_1 \circ x_2) = g(f(x_1) * f(x_2)) = g(f(x_1)) \times g(f(x_2)) = g \circ f(x_1) \times g \circ f(x_2)$. 因此, $g \circ f: X \rightarrow Z$ 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 $C = \{a + bi \mid a + bi \text{ 为复数}, a, b \in \mathbb{R}\}$, 相应地可以定义 2×2 矩阵集合:

$$M = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \mid a, b \in \mathbb{R} \right\}.$$

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

容易证明 f 是从 $\langle C; +, * \rangle$ 到 $\langle M; +, * \rangle$ 的同构映射.

T7 代数结构间的同构关系是等价关系.

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

(1) 自反性: 显然有 $\langle X; \circ \rangle \cong \langle X; \circ \rangle$, 即是自反的.

(2) 对称性: 如果 $\langle X; \circ \rangle \cong \langle Y; * \rangle$ 则必存在一个双射 $g: X \rightarrow Y$, 使得若 $x_1, x_2 \in X$, 并有:

$$g(x_1 \circ x_2) = g(x_1) * g(x_2)$$

根据双射的定义, 必存在一个双射的逆映射 $g^{-1}: Y \rightarrow X$.

现要证对 $g^{-1}: Y \rightarrow X$, 若 $y_1, y_2 \in Y$, 必有:



$$g^{-1}(y_1 * y_2) = g^{-1}(y_1) \circ g^{-1}(y_2)$$

设对任意的 $y_1, y_2 \in Y$ 必存在 $x_1, x_2 \in X$, 使得 $g(x_1) = y_1, g(x_2) = y_2$, 亦即 $g^{-1}(y_1) = x_1, g^{-1}(y_2) = x_2$, 故有:

$$g^{-1}(y_1 * y_2) = g^{-1}(g(x_1) * g(x_2)) = g^{-1}(g(x_1 \circ x_2)) = x_1 \circ x_2$$

又

$$g^{-1}(y_1) \circ g^{-1}(y_2) = x_1 \circ x_2$$

所以

$$g^{-1}(y_1 * y_2) = g^{-1}(y_1) \circ g^{-1}(y_2)$$

因此, $\langle Y; * \rangle \cong \langle X; \circ \rangle$, 所以 \cong 是对称的.

(3) 传递性: 如果有 $\langle X; \circ \rangle \cong \langle Y; * \rangle$, 且 $\langle Y; * \rangle \cong \langle Z; + \rangle$, 要证明 $\langle X; \circ \rangle \cong \langle Z; + \rangle$. 由条件亦即存在双射 $g: X \rightarrow Y$ 与 $h: Y \rightarrow Z$, 使得对任意 $x_1, x_2 \in X$ 和 $y_1, y_2 \in Y$, 必有:

$$g(x_1 \circ x_2) = g(x_1) * g(x_2), \quad h(y_1 * y_2) = h(y_1) + h(y_2)$$

下面证明存在一个双射 $f: X \rightarrow Z$, 使得对任意 $x_1, x_2 \in X$, 有 $f(x_1 \circ x_2) = f(x_1) + f(x_2)$,

现令 $f = h \circ g$, 即 h 与 g 的复合映射, 由于 g, h 均是双射, 所以 f 亦是双射.

$$\text{又 } f(x_1 \circ x_2) = h \cdot g(x_1 \circ x_2) = h(g(x_1) * g(x_2)) = h(g(x_1)) + h(g(x_2))$$

$$= h \cdot g(x_1) + h \cdot g(x_2) = f(x_1) + f(x_2)$$

所以, \cong 是传递的.

综上, \cong 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 $\langle Z; + \rangle$ 以及 $\langle C; +_3 \rangle$, 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 $\langle Z; + \rangle$ 到 $\langle C; +_3 \rangle$ 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 $\phi: Z \rightarrow C, \phi(i) = i \pmod{3}, i \in Z$,

易证明 ϕ 为同态映射, 其中, 同态映射的证明: $\phi(i+j) = (i+j) \pmod{3}$, 而 $\phi(i) + \phi(j) = i \pmod{3} + j \pmod{3} = ((i-3k_1) + (j-3k_2)) \pmod{3} = (i+j-3(k_1+k_2)) \pmod{3} = (i+j) \pmod{3}$, 其中, k_1, k_2 满足 $0 \leq i-3k_1 < 3, 0 \leq j-3k_2 < 3$;

定义 $\rho_\phi: x \rho_\phi y$ 当且仅当 $\phi(x) = \phi(y)$; 易证明 ρ_ϕ 为 $\langle Z; + \rangle$ 上同余关系, 相应商代数为: $\langle Z/\rho_\phi, * \rangle$, $Z/\rho_\phi = \{[0]_{\rho_\phi}, [1]_{\rho_\phi}, [2]_{\rho_\phi}\}$, $[x]_{\rho_\phi} * [y]_{\rho_\phi} = [x+y]_{\rho_\phi}$;

定义 $h: Z/\rho_\phi \rightarrow C: h([i]_{\rho_\phi}) = i \pmod{3}, i \in Z$; 定义 $f: Z/\rho_\phi \rightarrow C, f([x]_{\rho_\phi}) = \phi(x), [x]_{\rho_\phi} \in Z/\rho_\phi$.

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 $\langle A; + \rangle$ is an algebraic structure, where the binary operation $+$ is associative, and $\langle A; + \rangle$ has an identity, and its element has an inverse, then $\langle A; + \rangle$ is called a group(群).

A ring(环) is an algebra with the structure $\langle A; +, * \rangle$, where $\langle A; + \rangle$ is a commutative group(交换群, i.e., $\langle A; + \rangle$ is a group and the operation $+$ is commutative), $\langle A; * \rangle$ 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 $\langle A; +, * \rangle$ is a ring with the additional property that $\langle A - \{0\}; * \rangle$ 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 $\langle N_5; +_5, *_5 \rangle$ is a field.

$\langle N_5; +_5 \rangle$ 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.

$\langle N_5 - \{0\}; *_5 \rangle$ 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 .

- $\langle A; \circ \rangle$ is a group (群的定义请参考 T8) .
- $\langle A; \circ \rangle$ is a monoid but not a group.
- $\langle A; \circ \rangle$ is a semigroup(半群) but not a monoid.

\circ	a	b
a	a	b
b	b	a

a.

\circ	a	b
a	a	b
b	b	b

b.

\circ	a	b
a	b	b
b	b	b

c.

\circ	a	b
a	a	b
b	a	b

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: $f_{two}(b_k b_{k-1} \dots b_1 b_0) = 2^k b_k + 2^{k-1} b_{k-1} + \dots + 2^1 b_1 + 2^0 b_0$, 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 $\langle B; +_{bi} \rangle$ 到 $\langle N; + \rangle$ 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 $\langle N_3; +_3 \rangle$ to the algebra $\langle N_6; +_6 \rangle$ 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 $\langle N_8; +_8 \rangle$ to itself, where $+$ 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 $x, y \in N_8$.

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

$$\begin{aligned} \text{如: } f(3 +_8 4) &= f(1 +_8 1 +_8 1 +_8 1 +_8 1 +_8 1) \\ &= f(1) +_8 f(1) +_8 f(1) +_8 f(1) +_8 f(1) +_8 f(1) \\ &= [f(1) +_8 f(1) +_8 f(1)] +_8 [f(1) +_8 f(1) +_8 f(1)] \\ &= f(1 +_8 1 +_8 1) +_8 f(1 +_8 1 +_8 1) \\ &= f(3) +_8 f(4). \end{aligned}$$

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

第3部分 综合应用