NIS2312-01 Fall 2023-2024

信息安全的数学基础 (1)

Answer 13

2023 年 11 月 10 日

Problem 1

设 $\phi : \mathbf{Z}_6 \to \mathbf{Z}_2$ 使 $\phi(x + \langle 6 \rangle) = x + \langle 2 \rangle$. 证明: ϕ 是 $\mathbf{Z}_6$ 到 $\mathbf{Z}_2$ 的环同态并求 $ker(\phi)$.
解:

(1) 如果 $x + \langle 6 \rangle = y + \langle 6 \rangle$, 则有 $x - y \in \langle 6 \rangle \subseteq \langle 2 \rangle$, 故 $x + \langle 2 \rangle = y + \langle 2 \rangle$, 即 $\phi(x + \langle 6 \rangle) = \phi(y + \langle 6 \rangle)$, 故 ϕ 是一个映射.

(2) 对任意 $x + \langle 6 \rangle, y + \langle 6 \rangle \in \mathbf{Z}_6$, 都有

$$\begin{aligned}
\phi((x + \langle 6 \rangle) + (y + \langle 6 \rangle)) = \phi((x + y) + \langle 6 \rangle) = (x + y) + \langle 2 \rangle &= (x + \langle 2 \rangle) + (y + \langle 2 \rangle) \\
&= \phi(x + \langle 6 \rangle) + \phi(y + \langle 6 \rangle) \\
\phi((x + \langle 6 \rangle)(y + \langle 6 \rangle)) = \phi(xy + \langle 6 \rangle) = xy + \langle 2 \rangle &= (x + \langle 2 \rangle)(y + \langle 2 \rangle) \\
&= \phi(x + \langle 6 \rangle)\phi(y + \langle 6 \rangle),
\end{aligned}$$

因此 ϕ 是一个环同态映射.

(3)

$$\begin{aligned}
ker(\phi) &= \{x + \langle 6 \rangle | x + \langle 2 \rangle = \langle 2 \rangle\} \\
&= \{x + \langle 6 \rangle | x \in \langle 2 \rangle\} \\
&= \{x + \langle 6 \rangle | x \mid 2\} \\
&= 2\mathbf{Z}_6.
\end{aligned}$$

Problem 2

设 ϕ 是环 R 到环 R' 同态. 证明 ϕ 是单同态的充分必要条件是 $ker(\phi) = \{0\}$.
解:

必要性: 设 $x \in ker(\phi)$, 则 $\phi(x) = 0 = \phi(0)$. 由于 ϕ 是单同态, 因此 $x = 0$, 故 $ker(\phi) = \{0\}$.

充分性: 设 $x, y \in R$ 满足 $\phi(x) = \phi(y)$, 则 $\phi(x - y) = \phi(x) - \phi(y) = 0$. 因此 $x - y \in ker(\phi)$. 又因为 $ker(\phi) = \{0\}$, 则 $x - y = 0$, 即 $x = y$, ϕ 是单同态.

Problem 3

设 m 与 n 是互素的正整数. 证明: 存在环同构 $\mathbf{Z}_{mn} \cong \mathbf{Z}_m \oplus \mathbf{Z}_n$.

解:

$$\begin{aligned}\phi: \quad \mathbf{Z}_{mn} &\longrightarrow \mathbf{Z}_m \oplus \mathbf{Z}_n \\ \overline{x} &\longmapsto ([x]_m, [x]_n).\end{aligned}$$

(1) 如果 $\overline{x} = \overline{y}$, 则 $mn \mid x-y$, 于是 $m|(x-y), n|(x-y)$. 所以 $([x]_m, [x]_n) = ([y]_m, [y]_n)$, 因此 ϕ 为 $\mathbf{Z}_{mn}$ 到 $\mathbf{Z}_m \oplus \mathbf{Z}_n$ 的映射.

(2) 设 $\overline{x}, \overline{y} \in \mathbf{Z}_{mn}$, 如果 $\phi(\overline{x}) = \phi(\overline{y})$, 即 $([x]_m, [x]_n) = ([y]_m, [y]_n)$, 则 $m|(x-y), n|(x-y)$. 由于 $(m, n) = 1$, 因此 $mn \mid (x-y)$, 从而 $\overline{x} = \overline{y} \in \mathbf{Z}_{mn}$. 这说明 ϕ 是 $\mathbf{Z}_{mn}$ 到 $\mathbf{Z}_m \oplus \mathbf{Z}_n$ 的单映射. 又因为 $|\mathbf{Z}_{mn}| = mn = |\mathbf{Z}_m \oplus \mathbf{Z}_n|$, 所以 $\phi(\mathbf{Z}_{mn}) = \mathbf{Z}_m \oplus \mathbf{Z}_n$, 因此 ϕ 也是 $\mathbf{Z}_{mn}$ 到 $\mathbf{Z}_m \oplus \mathbf{Z}_n$ 的满映射.

(3) 对任意的 $\overline{x}, \overline{y} \in \mathbf{Z}_{mn}$, 有

$$\begin{aligned}\phi(\overline{x} + \overline{y}) &= \phi(\overline{x+y}) = (\overline{x+y}, \overline{x+y}) = ([x]_m, [x]_n) + ([y]_m, [y]_n) = \phi(\overline{x}) + \phi(\overline{y}), \\ \phi(\overline{x} \cdot \overline{y}) &= \phi(\overline{xy}) = ([xy]_m, [xy]_n) = ([x]_m, [x]_n)([y]_m, [y]_n) = \phi(\overline{x}) \cdot \phi(\overline{y}),\end{aligned}$$

所以 ϕ 为 $\mathbf{Z}_{mn}$ 到 $\mathbf{Z}_m \oplus \mathbf{Z}_n$ 环同构. 即

$$\mathbf{Z}_{mn} \cong \mathbf{Z}_m \oplus \mathbf{Z}_n.$$

Problem 4

设 R 是一个有单位元的交换环, I, J 是 R 的两个理想, 满足 $I + J = R$. 证明:

(1) $\phi : R \to R/I \times R/J$, 其中 $\phi(r) = (r + I, r + J)$ 是环同态映射;

(2) 利用环同态基本定理证明 $R/I \cap J \cong R/I \times R/J$.

解:

(1) $\forall a, b \in R$ 我们有

$$\begin{aligned}\phi(a + b) &= (a + b + I, a + b + J) = (a + I, a + J) + (b + I, b + J) = \phi(a) + \phi(b) \\ \phi(ab) &= (ab + I, ab + J) = (a + I, a + J) \times (b + I, b + J) = \phi(a)\phi(b),\end{aligned}$$

故是一个环同态映射;

(2) 验证 ϕ 是满同态: 由于 $R = I + J$, 我们有结果 $\exists i \in I, j \in J$ 满足 $i + j = e$. 因此 $\forall (a + I, b + J) \in R/I \times R/J$, 我们有原象 $ai + bj \in R$,

$$\phi(aj + bi) = (aj + I, bi + J) = (a(e - i) + I, b(e - j) + J) = (a + I, b + J),$$

故 ϕ 是一个满同态;

最后我们计算 ϕ 的核空间 $\forall r \in R, \phi(r) = (r + I, r + J) = (I, J)$, 这说明 $r \in I$ 以及 $r \in J$, 从而有 $r \in I \cap J$. 反过来, 如果 $r \in I \cap J$, 我们有 $\phi(r) = (r+I, r+J) = (I, J)$. 所以 $ker(\phi) = I \cap J$.

(3) 由环同态基本定理可得 $R/I \cap J \cong R/I \times R/J$