NIS2312-01 Fall 2023-2024

信息安全的数学基础 (1)

Answer 14

2023 年 11 月 17 日

Problem 1

证明: $\mathbf{Z}_{18}$ 的极大理想是 $\langle 2\rangle$ 与 $\langle 3\rangle$.

解: $\mathbf{Z}_{18}$ 有理想:

$$\{0\}, \mathbf{Z}_{18}, \langle 2\rangle, \langle 3\rangle, \langle 6\rangle, \langle 9\rangle,$$

不考虑平凡理想. 因为 $2 \mid 6$, 由此得到 $\langle 6\rangle \subset \langle 2\rangle$; 此外, $\langle 3\rangle$ 和 $\langle 9\rangle$ 均不包含 $\langle 2\rangle$, 故 $\langle 2\rangle$ 是极大理想; 同理 $\langle 3\rangle$ 也是极大理想.

Problem 2

设 p 是正整数. 证明: $\langle p\rangle$ 是 $\mathbf{Z}$ 的极大理想的充分必要条件是 p 是素数.

解: 证明必要性. 如果 p 不是素数, 则 $p = 1$ 或 p 是一个合数.

(1) 如果 $p = 1$, 则 $\langle p\rangle = \mathbf{Z}$ 不是 $\mathbf{Z}$ 的极大理想.

(2) 如果 p 是合数, 设 $p = ab(1 < a < p, 1 < b < p)$, 则 $\langle p\rangle \subseteq \langle a\rangle$. 因为 $a < p$, 所以 $a \notin \langle p\rangle$, 从而 $\langle p\rangle \subsetneq \langle a\rangle$. 又因为 $a\rangle 1$, 所以 $\langle a\rangle \subsetneq \mathbf{Z}$. 因此 $\langle p\rangle$ 也不是 $\mathbf{Z}$ 的极大理想.

这就证明了必要性.

充分性. 设 p 是素数, I 是 $\mathbf{Z}$ 的任一理想, 使 $\langle p\rangle \subsetneq I \subseteq \mathbf{Z}$, 则存在 $a \in I$, 使 $a \notin \langle p\rangle$. 从而 $p \nmid a$. 因为 p 是素数, 所以 $(a, p) = 1$. 从而存在 $u, v \in \mathbf{Z}$, 使 $au + pv = 1$. 于是, 对任意的 $z \in \mathbf{Z}$,

$$z = z \cdot 1 = zau + zpv \in I.$$

由此得 $I = \mathbf{Z}$. 所以 $\langle p\rangle$ 为 $\mathbf{Z}$ 的极大理想.

Problem 3

设 $R = 2\mathbf{Z}, I = 4\mathbf{Z}$ 为 R 的理想, 则 I 为 R 的极大理想, 但不是素理想.

解: 设 J 为 R 的任一理想且 $I \subsetneq J \subseteq R$, 则存在 $a \in J$ 且 $a \notin I$. 令 $a = 2b$, 则 $2 \nmid b$, 所以 $(4, a) = 2$. 从而存在 $u, v \in \mathbf{Z}$, 使 $au + 4v = 2$. 由此得 $2 \in J$, 所以 $J = 2\mathbf{Z} = R$, 从而 I 为 R 的极大理想.

又因为 $2 \notin I$, 但 $2 \cdot 2 = 4 \in I$, 所以 I 不是 R 的素理想.

Problem 4

设 R 是全体实函数的集合按通常函数的加法与乘法构成的一个环. 令

$$I = \{f(x) \in R | f(0) = 0\}.$$

证明: I 是 R 的极大理想.

解: 易知 I 为 R 的理想.

设 J 是 R 的任意真包含 I 的理想, 则存在 $h(x) \in J$ 使得 $h(0) \neq 0$. 令 $a = \frac{1}{h(0)}$ 且 $g(x) \equiv a$, 则 $g(x) \in R$. 又因为 $1 - g(0)h(0) = 1 - 1 = 0$, 所以 $1 - g(x)h(x) \in I$. 从而

$$1 = (1 - g(x)h(x) + g(x)h(x) \in J.$$

由此得 $J = R$. 所以 I 为 R 的极大理想.