問. 環 $\mathbb{Z}[\sqrt{10}] = \{a + b\sqrt{10} \mid a, b \in \mathbb{Z}\}$ において, 2 は既約元であるが素元ではないことを示せ.

解答例.（2 が既約元であること）

$$2 = (a + b\sqrt{10})(c + d\sqrt{10}) \tag{1}$$

とする．ただし, $a, b, c, d \in \mathbb{Z}$. (1) より $(ac + 10bd - 2) + (ad + bc)\sqrt{10} = 0$. 従って, $ac + 10bd = 2,\ ad + bc = 0$ であるから

$$(a - b\sqrt{10})(c - d\sqrt{10}) = (ac + 10bd) - (ad + bc)\sqrt{10} = 2. \tag{2}$$

(1), (2) より

$$(a^2 - 10b^2)(c^2 - 10d^2) = 4.$$

$a^2 - 10b^2 = \pm 2$ とすると $a^2 \equiv \pm 2 \pmod 5$, すなわち, $a^2 \equiv 2, 3 \pmod 5$ であるが, $\forall a \in \mathbb{Z}$ に対して $a^2 \equiv 0, 1, 4 \pmod 5$ であるから矛盾．従って, $a^2 - 10b^2 = \pm 1$ または $c^2 - 10d^2 = \pm 1$ である．$a^2 - 10b^2 = \pm 1$ のとき $a + b\sqrt{10}$ の逆元は $\pm(a - b\sqrt{10})$（複号同順）だから $a + b\sqrt{10}$ は単元（単数）である．$c^2 - 10d^2 = \pm 1$ のときも同様にして $c + d\sqrt{10}$ は単元（単数）である．よって, 2 は既約元である.

（2 は素元ではないこと）
$2|6 = (4 + \sqrt{10})(4 - \sqrt{10})$ であるが $2 \nmid (4 \pm \sqrt{10})$ だから 2 は素元ではない.（解答例終り）

参考. $m \in \mathbb{Z},\ m \neq 1$ とし, m は平方数で割り切れないとする．$x, y \in \mathbb{Z}$ に対し $|x^2 - my^2|$ が素数ならば, $x + y\sqrt{m}$ と $x - y\sqrt{m}$ は環 $\mathbb{Z}[\sqrt{m}] = \{a + b\sqrt{m} \mid a, b \in \mathbb{Z}\}$ の既約元である．以下, このことを証明する.

$$x + y\sqrt{m} = (a + b\sqrt{m})(c + d\sqrt{m}) \tag{3}$$

とする．ただし, $a, b, c, d \in \mathbb{Z}$. (3) より $(ac + bdm - x) + (ad + bc - y)\sqrt{m} = 0$. 従って, $ac + bdm = x,\ ad + bc = y$ であるから

$$(a - b\sqrt{m})(c - d\sqrt{m}) = (ac + bdm) - (ad + bc)\sqrt{m} = x - y\sqrt{m}. \tag{4}$$

(3), (4) より

$$(a^2 - mb^2)(c^2 - md^2) = x^2 - my^2.$$

$|x^2 - my^2|$ は素数だから, $a^2 - mb^2 = \pm 1$ または $c^2 - md^2 = \pm 1$ である．$a^2 - mb^2 = \pm 1$ のとき $a + b\sqrt{m}$ の逆元は $\pm(a - b\sqrt{m})$（複号同順）だから $a + b\sqrt{m}$ は単元（単数）である．$c^2 - md^2 = \pm 1$ のときも同様にして $c + d\sqrt{m}$ は単元（単数）である．よって, $x + y\sqrt{m}$ は既約元である．同様にして, $x - y\sqrt{m}$ が既約元であることも分かる.