

■ $p \geq 2$ を素数とし、整数の集合 \mathbb{Z} における二項関係 \sim を

$$n \sim m \iff n - m \text{ は } p \text{ で整除できる}$$

により定義するとき、二項関係 \sim は \mathbb{Z} における同値関係である（証明しなくてもよい）。また、二項関係 \sim による n を代表元とする \mathbb{Z} の同値類を $C(n)$ と表し、 \mathbb{Z}/\sim における演算 \oplus および \otimes をそれぞれ

$$C(n) \oplus C(m) = C(n + m), \quad C(n) \otimes C(m) = C(n \cdot m)$$

に定義するとき、演算 \oplus および \otimes は代表元の取り方に依存せずうまく定義できていることを示せ。

(解) $n \sim q$, $m \sim r$ とする。このとき、 $C(n) = C(q)$, $C(m) = C(r)$ であることと同値である。二項関係 \sim の定義より、ある整数 k_1, k_2 が取れて、 $n - q = k_1 \cdot p$, $m - r = k_2 \cdot p$ が成り立つので、

$$\begin{aligned} (n + m) - (q + r) &= (n - q) + (m - r) = k_1 \cdot p + k_2 \cdot p = (k_1 + k_2) \cdot p, \\ n \cdot m - q \cdot r &= (q + k_1 \cdot p) \cdot (r + k_2 \cdot p) - q \cdot r = p \cdot (k_1 \cdot r + k_2 \cdot q + k_1 \cdot k_2 \cdot p) \end{aligned}$$

となり、 $n + m \sim q + r$ および $n \cdot m \sim q \cdot r$ が得られる。したがって、演算 \oplus および \otimes は代表元の取り方に依存せずうまく定義できている。 ■