

以下 d は素因数分解に平方因子を含まない整数とする. 環 $\mathbb{Z}[\sqrt{d}]$ を

$$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$$

と定義する. $\mathbb{Z}[\sqrt{d}]$ の元 $\alpha = a + b\sqrt{d}$ に対し, $\bar{\alpha} = a - b\sqrt{d}$ を α の**共役元**という. $\mathbb{Z}[\sqrt{d}]$ において α のノルム $N(\alpha)$ は,

$$N(\alpha) = \alpha\bar{\alpha} = a^2 - db^2$$

により定義される.

[1] $\alpha, \beta \in \mathbb{Z}[\sqrt{d}]$ とする. 次を示せ.

$$(1) N(\alpha\beta) = N(\alpha)N(\beta)$$

$$(2) \alpha \text{ が単元} \iff N(\alpha) = \pm 1$$

$$(3) N(\alpha) \text{ が } \mathbb{Z} \text{ の既約元ならば, } \alpha \text{ は } \mathbb{Z}[\sqrt{d}] \text{ の既約元である}$$

(解答)

$$(1) \alpha = a_1 + b_1\sqrt{d}, \beta = a_2 + b_2\sqrt{d} \text{ とする.}$$

$$\alpha\beta = (a_1 + b_1\sqrt{d})(a_2 + b_2\sqrt{d}) = (a_1a_2 + b_1b_2d) + (a_1b_2 + a_2b_1)\sqrt{d}$$

より

$$\begin{aligned} N(\alpha\beta) &= (a_1a_2 + b_1b_2d)^2 - d(a_1b_2 + a_2b_1)^2 \\ &= (a_1^2a_2^2 + 2a_1a_2b_1b_2d + b_1^2b_2^2d^2) - d(a_1^2b_2^2 + 2a_1a_2b_1b_2 + a_2^2b_1^2) \\ &= (a_1^2a_2^2 + b_1^2b_2^2d^2) - d(a_1^2b_2^2 + a_2^2b_1^2) \\ &= (a_1^2 - db_1^2)(a_2^2 - db_2^2) \\ &= N(\alpha)N(\beta). \end{aligned}$$

$$(2) \alpha \text{ を単元とすると, } \beta \in \mathbb{Z}[\sqrt{d}] \text{ が存在し, } \alpha\beta = 1 \text{ を満たす. 両辺のノルムをとれば,}$$

$$N(\alpha\beta) = N(\alpha)N(\beta) = 1$$

が成り立ち, $N(\alpha) \in \mathbb{Z}$ より $N(\alpha) = \pm 1$ を得る.

逆に $N(\alpha) = \pm 1$ ならば, $\alpha\bar{\alpha} = \pm 1$ を満たす. $\alpha^{-1} = \pm\bar{\alpha}$ が成り立つため, α は単元となる.

$$(3) \text{ 対偶を示す. } \alpha \text{ が可約元, すなわち既約元でないとする. このとき, 単元でない } \beta, \gamma \in \mathbb{Z}[\sqrt{d}] \text{ が存在し, } \alpha = \beta\gamma \text{ を満たす. 両辺のノルムを取ると}$$

$$N(\alpha) = N(\beta)N(\gamma)$$

が成り立つ. β, γ は単元でないので, (2) より

$$N(\beta) \neq \pm 1 \text{ かつ } N(\gamma) \neq \pm 1$$

となる. したがって $N(\alpha)$ は可約元である.

2 環 $\mathbb{Z}[\sqrt{5}]$ において、次の元が既約元かどうか判定せよ.

- (1) 2 (2) $2 - \sqrt{5}$ (3) $4 + \sqrt{5}$

(解答)

- (1) 非単元 $\alpha, \beta \in \mathbb{Z}[\sqrt{5}]$ が存在し $2 = \alpha\beta$ を満たすとする. 両辺のノルムを取ると

$$4 = N(2) = N(\alpha)N(\beta), \quad N(\alpha) \neq \pm 1, \quad N(\beta) = \pm 1$$

を満たす. したがって $N(\alpha) = \pm 2$ であることがわかる. $\alpha = a + b\sqrt{5}$ とおくと, 方程式

$$a^2 - 5b^2 = 2 \text{ または } a^2 - 5b^2 = -2$$

に整数解 (a, b) が存在するが, そのような整数解は存在しない. 任意の整数 x に対し法 4 の下で $x^2 \equiv 0$ または $x^2 \equiv 1$ であり, 両辺の mod 4 をとると, $a^2 - 5b^2 \equiv a^2 - b^2$ のため,

$$a^2 - 5b^2 \equiv 0 \pmod{4} \text{ または } a^2 - 5b^2 \equiv \pm 1 \pmod{4}$$

であることがわかる. 両者は矛盾するため 2 は $\mathbb{Z}[\sqrt{5}]$ において既約元である.

- (2) $N(2 - \sqrt{5}) = 2^2 - 5 = -1$. したがって $2 - \sqrt{5}$ は $\mathbb{Z}[\sqrt{5}]$ の単元である. 単元は既約元でないため, $2 - \sqrt{5}$ は既約元でない.

- (3) $N(4 + \sqrt{5}) = 16 - 5 = 11$ が素数になるので, $4 + \sqrt{5}$ は既約元である.

3 次の環 R において、指定された R の元 α が R の素元かどうか判定せよ.

- (1) $R = \mathbb{Z}, \alpha = 7$

- (2) $R = \mathbb{Z}[i]$ (R はガウス整数環, $i = \sqrt{-1}$), $\alpha = 2$

- (3) $R = \mathbb{Z}[\sqrt{-5}], \alpha = 3$

- (4) $R = \mathbb{Z}[\sqrt{5}], \alpha = 2 - \sqrt{5}$

(解答)

- (1) 素数 $p \in \mathbb{Z}$ と整数 $a, b \in \mathbb{Z}$ に対し,

$$p \mid ab \implies p \mid a \text{ または } p \mid b$$

が成り立ち, 7 は素数であるため, \mathbb{Z} において素元である.

- (2) $\mathbb{Z}[i]$ において,

$$2 = (1 + i)(1 - i)$$

かつ, $1 + i$ と $1 - i$ は単元でないため, 2 は $\mathbb{Z}[i]$ において既約元でない. 整域 R において

$$\alpha \in R \text{ が素元} \implies \alpha \in R \text{ は既約元}$$

である²ため, 2 は $\mathbb{Z}[i]$ の素元でない.³

- (3) $\mathbb{Z}[\sqrt{-5}]$ において,

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

がなりたち,

$$\frac{1 + \sqrt{-5}}{3} \notin \mathbb{Z}[\sqrt{-5}] \text{ かつ } \frac{1 - \sqrt{-5}}{3} \notin \mathbb{Z}[\sqrt{-5}]$$

より 3 は素元でない.

- (4) $\mathbb{Z}[\sqrt{5}]$ において, $\alpha = 2 - \sqrt{5}$ は単元である (2 の (2) 参照). 単元は素元でないため, $\alpha = 2 - \sqrt{5}$ は素元でない.

² R が一意分解整域のときは逆も正しい. ガウス整数環 $\mathbb{Z}[i]$ は単項イデアル整域であり, とくに一意分解整域であることが知られている.

³(3) と同様に $(1 \pm i)/2 \notin \mathbb{Z}[i]$ から 2 が素元でないことが従う.

³※この講義に関する情報はホームページを参照. <https://hirokazunasu.github.io/2025/alg2.html>