環論 (第 13 回)

13. ガウス整数環

前回は PID について解説し, さらに「PID⇒ UFD」を示した. 今回は PID の例としてガウス整数環を取り上げる. $\mathbb{C}$ の部分環

$$A = \{a + bi \mid a, b \in \mathbb{Z}\}$$

を**ガウス整数環**と呼ぶ. ただし, $i = \sqrt{-1}$ である. また写像

$$N : A \to \mathbb{Z} \ \ (a + bi \mapsto a^2 + b^2)$$

を A の**ノルム**と呼ぶ. 定義から

$$N(\alpha) = |\alpha|^2 = \alpha\overline{\alpha} \quad (\alpha \in A).$$

ここで, $\overline{\alpha}$ は α の複素共役である.

定理 13-1

$\alpha, \beta \in A$ とする.

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

(2) A において $\alpha \mid \beta$ ならば, $\mathbb{Z}$ において $N(\alpha) \mid N(\beta)$ が成り立つ.

(3) $\alpha \in A^\times \iff N(\alpha) = 1$.

(4) $A^\times = \{\pm 1, \pm i\}$.

(5) $\alpha \sim \beta$ のとき, $N(\alpha) = N(\beta)$.

[証明]

(1), (3) は定理 3-2 より従う. また (2), (4), (5) は (1), (3) より従う.

□

次の定理はガウス整数環での割り算の原理に相当する.

定理 13-2

$\alpha, \beta \in A$ $(\alpha \neq 0)$ とする. このとき,

$$\beta = \gamma\alpha + \delta, \quad N(\delta) < N(\alpha)$$

を満たす γ, $\delta \in A$ がある.

[証明]

$\frac{\beta}{\alpha} = a + bi$ $(a, b \in \mathbb{R})$ と表す. また,

$$|a - c| \leqq \frac{1}{2}, \quad |b - d| \leqq \frac{1}{2}$$

を満たす $c, d \in \mathbb{Z}$ をとり, $\gamma = c + di$ とおく. このとき, $\gamma \in A$ であり,

$$\left|\frac{\beta}{\alpha} - \gamma\right|^2 = (a - c)^2 + (b - d)^2 < 1.$$

$\delta = \beta - \gamma\alpha \in A$ と置けば, $\beta = \gamma\alpha + \delta$ であり,

$$N(\delta) = |\delta|^2 = |\alpha|^2 \cdot \left|\frac{\beta}{\alpha} - \gamma\right|^2 < |\alpha|^2 = N(\alpha).$$

□

定理 13-3

A は PID である.

[証明]

I を (0) でない A のイデアルとする. α を $I \setminus \{0\}$ に含まれるノルムが最小の元とする. このとき, $\alpha \in I$ より $(\alpha) \subseteq I$ である. 逆に $\beta \in I$ とすると, 定理 13-2 から

$$\beta = \gamma\alpha + \delta, \quad N(\delta) < N(\alpha)$$

を満たす γ, $\delta \in A$ が取れる. $\delta = \beta - \gamma\alpha \in I$ より, $N(\alpha)$ の最小性から $\delta = 0$. よって $\beta = \alpha\gamma \in (\alpha)$. よって $I \subseteq (\alpha)$ であり, $I = (\alpha)$ を得る. よって A は PID である.

□

定理 12-3 と定理 13-3 より, A は UFD である. また定理 12-2 から, $\alpha \in A$ に対して,

$$\alpha\text{が既約元} \iff \alpha \text{ が素元}$$

が成り立つ.

定理 13-4

$\alpha, \beta \in A \setminus \{0\}$ とする.

(1) $\alpha \mid \beta$ かつ $N(\alpha) = N(\beta)$ のとき, $\alpha \sim \beta$ である.

(2) $N(\alpha)$ が素数のとき, α は A の既約元 (素元) である.

[証明]
(1) $\alpha \mid \beta$ より $\beta = \gamma\alpha$ $(\gamma \in A)$ と表せる. 仮定より

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

よって $N(\gamma) = 1$ より $\gamma \in A^\times$. 従って $\alpha \sim \beta$.

(2) $p = N(\alpha)$ (p : 素数) とする. このとき, $\alpha \neq 0$ かつ $\alpha \notin A^\times$ に注意する. $\beta \mid \alpha$ とすると,

$$N(\beta) \mid N(\alpha) = p.$$

よって $N(\beta)$ は 1 または p である. $N(\beta) = 1$ のとき, $\beta \in A^\times$ である. $N(\beta) = p$ のとき, $\beta \mid \alpha$ かつ $N(\beta) = N(\alpha)$ より $\beta \sim \alpha$. よって α は既約元である.

□

例題 13-1
ガウス整数環 A において考える.

(1) $2 - i$ と $2 + i$ は素元であることを示せ.

(2) $2 - i$ と $2 + i$ は同伴でないことを示せ.

(3) 3 は素元である.

[証明]
(1) $N(2 \pm i) = 5$ は素数. 定理 13-4 (2) より, $2 \pm i$ は素元.

(2) $2 + i$ に $A^\times = \{\pm 1, \pm i\}$ の元をかけても $2 - i$ にならない. 従って $2 + i$ と $2 - i$ は同伴でない.

(3) $a + bi \mid 3$ とする. このとき,

$$N(a + bi) \mid N(3) = 9.$$

よって $N(a+bi)$ は $1, 3, 9$ のいずれか. $N(a+bi) = 1$ のときは $a + bi \in A^\times$ である. $N(a+bi) = 9$ のとき, $N(a+bi) = N(3)$ より $a + bi \sim 3$. また

$$a^2 + b^2 = N(a + bi) = 3$$

となる整数の組 (a, b) はないので, $N(a + bi) = 3$ の場合は起きない. よって 3 は A の既約元であり, 素元でもある.

□

例題 13-2
39 の A 上での素元分解を求めよ.

[**証明**]

$N(2 \pm 3i) = 13$ であるので $2 \pm 3i$ は素元である. また $2+3i$ に $A^\times = \{\pm 1,\ \pm i\}$ の元をかけても $2-3i$ にならない. 従って $2+3i$ と $2-3i$ は同伴でない. また例題 13-1 より 3 は A の素元である. 以上より, 39 の A における素元分解は

$$39 = 3 \cdot 13 = 3 \cdot (2+3i) \cdot (2-3i)$$

であり, また $3, 2+3i, 2-3i$ は互いに同伴ではない. □

問題 13-1

(1) $1+i$ は A の素元であることを示せ.

(2) 7 は A の素元であることを示せ.

(3) $\alpha = 9-2i$ の A での素元分解を求めよ.

問題 13-2 π が A の素元のとき, $N(\pi)$ は素数または素数の 2 乗であることを示せ.

最後に, ガウス整数環における素数の素元分解に関する結果を紹介しておく.

定理 13-5

素数 p は A 上で次のように素元分解される.

(1) $p = 2$ のとき,

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

と素元分解される. ここで, $1+i$ と $1-i$ は同伴である.

(2) $p \equiv 1 \pmod 4$ のとき,

$$p = \pi\bar{\pi}$$

と素元分解される. ここで, $\bar{\pi}$ は π の複素共役で, π と $\bar{\pi}$ は同伴ではない.

(3) $p \equiv 3 \pmod 4$ のとき, p は A の素元である.

[**証明**]

参考文献 [1] の定理 5.45 を参照のこと. □

参考文献

[1] 青木昇, 素数と 2 次体の整数論, 共立出版, 2012.