環論 (第 11 回)

11 UFD

整数環 $\mathbb{Z}$ のように素因数分解できる整域を UFD という. 今回はまず可換環上で素数にあたる概念を定義し, さらに UFD の定義や性質について述べる.

定義 11-1(素元と既約元)
可換環 A と $a, b, \pi \in A$ $(\pi \neq 0,\ \pi \notin A^\times)$ を考える.

(1) $b = ua$ $(u \in A)$ と表せるとき, a **は** b **を割る**といい, $a \mid b$ で表す. $a \mid b$ でないとき, $a \nmid b$ で表す.

(2) $a = ub$ $(u \in A^\times)$ と表せるとき, a と b は **同伴**といい, $a \sim b$ で表す.

(3) 次の条件を満たすとき π を**素元**という.

$$\pi \mid xy \ \ (x, y \in A) \Rightarrow \pi \mid x \text{ または } \pi \mid y.$$

(4) 次の条件を満たすとき π を**既約元**という.

$$x \mid \pi \ \ (x \in A) \Rightarrow \pi \sim x \text{ または } x \in A^\times.$$

問題 11-1 A を整域とし, $a, b, \pi \in A \setminus \{0\}$ とする. このとき, 次を示せ.

(1) $a \sim b \iff (a) = (b)$.

(2) π が素元 $\iff$ (π) は素イデアル.

定理 11-1
整数環 $\mathbb{Z}$ において考える.

(1) $a \sim b \iff a = \pm b$.

(2) 素数 p は素元である.

(3) 素数 p は既約元である.

[**証明**]
(1) $\mathbb{Z}^\times = \{\pm 1\}$ より従う.

(2) 定理 9-2 より (p) は素イデアルである. 従って p は素元である.

(3) $x \mid p$ $(x \in \mathbb{Z})$ とすると, $x = \pm 1, \pm p$ のいずれか. $x = \pm 1$ なら $x \in \mathbb{Z}^\times$ であり, $x = \pm p$ なら $x \sim p$. よって p は既約元である.

□

定理 11-2
整域 A において素元は既約元である.

[証明]
π を素元とする. $x \mid \pi$ $(x \in A)$ とする. このとき, $\pi = xy$ $(y \in A)$ と表せる. π は素元なので $\pi \mid x$ または $\pi \mid y$.

(i) $\pi \mid x$ のとき. $x = \pi z$ $(z \in A)$ と表すと, $\pi = \pi yz$ である. A は整域より $1 = yz$ である. $z \in A^\times$ より $\pi \sim x$.

(ii) $\pi \mid y$ のとき. $y = \pi w$ $(w \in A)$ と表せるので, $\pi = \pi xw$ である. $1 = xw$ より $x \in A^\times$.

(i), (ii) より π は既約元である.

□

例題 11-1
整域 $A = \{a + b\sqrt{-1} \mid a, b \in \mathbb{Z}\}$ を考える. $A^\times = \{\pm 1, \pm\sqrt{-1}\}$ に注意する (例題 3-2).

(1) $1 + \sqrt{-1} \mid 2$ および $1 + \sqrt{-1} \nmid 2 + \sqrt{-1}$ を示せ.

(2) $1 + \sqrt{-1}$ が既約元であることを示せ.

(3) $1 + \sqrt{-1}$ が素元であることを示せ.

[証明]
(1) $2 = (1 + \sqrt{-1})(1 - \sqrt{-1})$ より $1 + \sqrt{-1} \mid 2$. また

$$\frac{2 + \sqrt{-1}}{1 + \sqrt{-1}} = \frac{3}{2} - \frac{1}{2}\sqrt{-1} \notin A$$

より $1 + \sqrt{-1} \nmid 2 + \sqrt{-1}$.

(2) $\alpha \mid 1 + \sqrt{-1}$ とする. $1 + \sqrt{-1} = \alpha\beta$ $(\beta \in A)$ と表せる. ここで,

$$\alpha = a + b\sqrt{-1}, \quad \beta = c + d\sqrt{-1} \quad (a, b, c, d \in \mathbb{Z})$$

と表す. 定理 3-2 の写像 $N : A \to \mathbb{Z}$ $(x + y\sqrt{-1} \mapsto x^2 + y^2)$ を考えると,

$$2 = N(1 + \sqrt{-1}) = N(\alpha)N(\beta) = (a^2 + b^2)(c^2 + d^2).$$

よって $a^2 + b^2$ は 1, 2 のいずれか.

(i) $a^2+b^2=1$ のとき, $(a,b)=(\pm1,0),\ (0,\pm1)$. よって $\alpha\in A^\times$.

(ii) $a^2+b^2=2$ のとき, $(a,b)=(1,\pm1),\ (-1,\pm1)$. このとき, α は $1\pm\sqrt{-1},\ -1\pm\sqrt{-1}$ のいずれかより,

$$(1+\sqrt{-1})u \quad (u\in A^\times)$$

の形でかける. よって $\alpha\sim 1+\sqrt{-1}$.

(i), (ii) より $1+\sqrt{-1}$ は A の既約元.

(3) $1+\sqrt{-1}\mid\alpha\beta$ $(\alpha,\beta\in A)$ とする. ここで,

$$\alpha=a+b\sqrt{-1},\quad \beta=c+d\sqrt{-1}\quad (a,b,c,d\in\mathbb{Z})$$

と置く. このとき

$$2=N(1+\sqrt{-1})\mid N(\alpha)N(\beta)=(a^2+b^2)(c^2+d^2).$$

よって $2\mid(a^2+b^2)$ または $2\mid(c^2+d^2)$.

仮に $2\mid a^2+b^2$ とする. このとき, a,b の偶奇は一致する. a,b が共に偶数のとき, $(a,b)=(2s,2t)$ $(s,t\in\mathbb{Z})$ と表すと,

$$\alpha=2(s+t\sqrt{-1})=(1+\sqrt{-1})(1-\sqrt{-1})(s+t\sqrt{-1}).$$

よって $1+\sqrt{-1}\mid\alpha$ である. a,b が共に奇数のとき, $(a,b)=(2s+1,2t+1)$ $(s,t\in\mathbb{Z})$ と表すと,

$$\alpha=(1+\sqrt{-1})+2(s+t\sqrt{-1})=(1+\sqrt{-1})+(1+\sqrt{-1})(1-\sqrt{-1})(s+t\sqrt{-1})$$

より, $1+\sqrt{-1}\mid\alpha$ である.

$2\mid c^2+d^2$ の場合も同様に $1+\sqrt{-1}\mid\beta$ が分かる. 以上より $1+\sqrt{-1}$ は素元である.

□

[補足] $1+\sqrt{-1}$ が既約元かつ素元であることは次のようにも示せる. $(1+\sqrt{-1})$ は A の素イデアルである (定理 9-1 と問題 9-3). よって $1+\sqrt{-1}$ は素元で, また定理 11-2 より既約元でもある.

問題 11-2

整域 $A=\{a+b\sqrt{-5}\mid a,b\in\mathbb{Z}\}$ を考える.

(1) $1+\sqrt{-5}\mid 6$ および $1-\sqrt{-5}\nmid 1+\sqrt{-5}$ を示せ.

(2) $A^\times=\{\pm1\}$.

(3) $1+\sqrt{-5}$ は既約元であることを示せ.

(4) $1+\sqrt{-5}$ は素元でないことを示せ

定義 11-2 (UFD)

A を整域とする. 任意の $x\in A$ $(x\notin A^\times\cup\{0\})$ が素元の積で表せるとき, A を **UFD** という.

整数環 $\mathbb{Z}$ の場合を考える. 任意の整数 $x \in \mathbb{Z}$ $(x \notin \{0, \pm 1\})$ は次の形で表せる.

$$x = \delta p_1 p_2 \cdots p_k \quad (\delta \in \{\pm 1\},\ p_i\text{: 素数}).$$

例 11-1 より $(\delta p_1),\ p_2, ..., p_k$ は素元である. よって $\mathbb{Z}$ は UFD である.

定理 11-3 (素元分解の一意性)
A を UFD とする. $x \in A$ $(x \notin A^\times \cup \{0\})$ が

$$x = p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_t \quad (\ p_i,\ q_j\text{: 素元})$$

と 2 通りに表せたとする. このとき, $s = t$ であり, $p_1, ..., p_s$ 順番を入れ替えると

$$p_i \sim q_i \quad (i = 1, 2, ..., s).$$

つまり, 素元の積への表し方は同伴の差を除いて一意的である.

[証明]
s に関する帰納法で示す.

(I) $s = 1$ のとき. つまり,

$$x = p_1 = q_1 q_2 \cdots q_t$$

とする. $t \geq 2$ と仮定する. p_1 は素元より既約元でもある. $q_1 \mid p_1$ より $q_1 \in A^\times$ または $p_1 \sim q_1$ である. q_1 は素元より $p_1 \sim q_1$. 従って $q_1 = u p_1$ $(u \in A^\times)$ と表せる. よって

$$1 = u q_2 \cdots q_t.$$

このとき, $q_2 \in A^\times$ となり矛盾. 従って $t = 1$ であり, $p_1 = q_1$ となる. 特に $p_1 \sim q_1$ である.

(II) $s - 1$ まで正しいと仮定し,

$$x = p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_t$$

とする. p_s は素元より, $p_s \mid q_j$ となる j がある. $j = t$ として問題ない. (I) と同様の議論で $q_t = u p_s$ $(u \in A^\times)$ と表せる. よって

$$p_1 p_2 \cdots p_{s-1} = q_1 q_2 \cdots (u q_{t-1}).$$

帰納法の仮定より $s - 1 = t - 1$ $(\Rightarrow s = t)$ であり, 順番を入れ替えると

$$p_i \sim q_i \quad (i = 1, 2, ..., s-2), \quad p_{s-1} \sim u q_{s-1} \sim q_{s-1}.$$

また $p_s \sim q_s$ である. よって s のときも正しい.

□

問題 11-3　UFD において, 既約元は素元であることを示せ.