環論 (第 6 回)

6. イデアル (2)

前回に引き続きイデアルの解説をする. 今回はイデアルに対して演算を定義し, それらの計算方法について述べる. また最後にイデアルが導入された理由を紹介する.

定理 6-1
可換環 A のイデアル I, J に対して, 次の集合は A のイデアルとなる.

(1) $I \cap J := \{x \in A \mid x \in I$ かつ $x \in J\}$.

(2) $I + J := \{x + y \mid x \in I,\ y \in J\}$.

(3) $I \cdot J := \left\{ \sum_{i=1}^{n} x_i y_i \mid n \in \mathbb{N},\ \ x_i \in I,\ y_i \in J\ (i = 1, 2, ..., n) \right\}$.

$I \cap J$, $I + J$, $I \cdot J$ をそれぞれ I と J の**共通部分**, **和**, **積**という.

[証明]
(1) 問題 5-2 を参照.

(2) について.
(i) $z, w \in I + J$ とすると,

$$z = x_1 + y_1, \quad w = x_2 + y_2 \quad (x_1, x_2 \in I,\ y_1, y_2 \in J)$$

と表せる. I, J はイデアルより $x_1 - x_2 \in I$, $y_1 - y_2 \in J$. 従って

$$z - w = (x_1 - x_2) + (y_1 - y_2) \in I + J.$$

(ii) $a \in A$, $z \in I + J$ とすると,

$$z = x + y \ \ (x \in I,\ y \in J)$$

と表せる. I, J はイデアルより $ax \in I$, $ay \in J$. 従って

$$az = ax + ay \in I + J.$$

以上より $I + J$ は A のイデアル.

(3) 問題 6-1.

□

問題 6-1 定理 6-1 (3) を示せ.

例題 6-1
可換環 A のイデアル I, J に対して次を示せ.

$$I + J = A \Rightarrow I^2 + J^2 = A.$$

ただし, A のイデアル K と自然数 n に対して,

$$K^n := \underbrace{K \cdot K \cdots K}_{n\text{ 個}}$$

とする.

[**証明**]
問題 5-1 より $1_A \in I^2 + J^2$ を示せばよい. $1_A \in A = I + J$ より

$$1_A = x + y \quad (x \in I,\ y \in J)$$

と表せる. よって

$$1_A = 1_A^3 = (x+y)^3 = (x+3y)x^2 + (3x+y)y^2.$$

$x^2 \in I^2,\ y^2 \in J^2$ であり, $I^2,\ J^2$ はイデアルだから

$$(x+3y)x^2 \in I^2, \quad (3x+y)y^2 \in J^2.$$

よって $1_A \in I^2 + J^2$.

問題 6-2 可換環 A のイデアル I, J に対して次を示せ.

$$I + J = A \Rightarrow I \cap J = I \cdot J.$$

定理 6-2
可換環 A と $s_1, ..., s_m,\ t_1, ..., t_n \in A$ に対して,

$$I = (s_1, ..., s_m), \quad J = (t_1, ..., t_n)$$

とおく.

(1) $I + J = (s_1, ..., s_m,\ t_1, ..., t_n)$.

(2) イデアル $I \cdot J$ は

$$S = \{s_i t_j \mid 1 \leq s \leq m,\ 1 \leq t \leq n\}$$

で生成されたイデアルである.

[証明]

(1) $I \subseteq I+J$, $J \subseteq I+J$ より $s_1, ..., s_m,\ t_1, ..., t_n \in I+J$. よって

$$(s_1, ..., s_m,\ t_1, ..., t_n) \subseteq I+J.$$

逆に $z \in I+J$ とすると,

$$z = x + y \quad (x \in I,\ y \in J)$$

と表せる. また

$$x = \sum_{i=1}^{m} a_i s_i, \qquad y = \sum_{j=1}^{n} b_j t_j \qquad (a_i,\ b_i \in A)$$

と表せるので,

$$z = \sum_{i=1}^{m} a_i s_i + \sum_{j=1}^{n} b_j t_j \in (s_1, ..., s_m,\ t_1, ..., t_n).$$

よって $(s_1, ..., s_m,\ t_1, ..., t_n) \supseteq I+J$.

(2) K を S で生成されたイデアルとする. $I \cdot J$ の定義より $S \subseteq I \cdot J$ である. K は S を含む最小のイデアルなので

$$K \subseteq I \cdot J.$$

逆に $z \in I \cdot J$ とすると,

$$z = \sum_{u=1}^{l} x_u y_u \quad (x_u \in I,\ y_u \in J)$$

と表せる. また

$$x_u = \sum_{i=1}^{m} a_{u,i} s_i, \qquad y_u = \sum_{j=1}^{n} b_{u,j} t_j \qquad (a_{u,i},\ b_{u,j} \in A)$$

と表せるので

$$z = \sum_{i=1}^{m} \sum_{j=1}^{n} \left(\sum_{u=1}^{l} a_{u,i} b_{u,j} \right) s_i t_j \in K.$$

よって $I \cdot J \subseteq K$.

□

定理 6-2 より次が従う.

系 6-1

可換環 A と $s_1, s_2, t_1, t_2 \in A$ を考える.

(1) $(s_1) + (t_1) = (s_1, t_1)$.

(2) $(s_1) \cdot (t_1) = (s_1 t_1)$.

(3) $(s_1, s_2) + (t_1, t_2) = (s_1, s_2, t_1, t_2)$.

(4) $(s_1, s_2) \cdot (t_1, t_2) = (s_1 t_1,\ s_1 t_2,\ s_2 t_1,\ s_2 t_2)$.

例えば, 整数環 $\mathbb{Z}$ において,

$$\begin{aligned}&(2)+(4)=(2,4)=(2)\cdot(1,2)=(2),\\&(2)\cdot(4)=(2\cdot 4)=(8)\end{aligned}$$

と計算できる. 次に, $(2,4)\cdot(3,6)$ を計算する.

$$(2,4)\cdot(3,6)=(2\cdot 3,\ 2\cdot 6,\ 4\cdot 3,\ 4\cdot 6)=(6,\ 12,\ 12,\ 24)=(6)\cdot(1,\ 2,\ 2,\ 4).$$

$1\in(1,\ 2,\ 2,\ 4)$ より $(1,\ 2,\ 2,\ 4)=(1)$. 従って

$$(2,4)\cdot(3,6)=(6)\cdot(1)=(6).$$

問題 6-3 $A=\mathbb{Z}[x]$ とそのイデアル $I=(x),\ J=(2,x-1),\ K=(3,x+1)$ に対して次を示せ.

$$I+J\cdot K=A.$$

例題 6-2

可換環 $A=\{a+b\sqrt{-5}\mid a,b\in\mathbb{Z}\}$ において次を示せ.

$$(3)=(3,1+\sqrt{-5})\cdot(3,1-\sqrt{-5}).$$

[証明]

$$\begin{aligned}&\quad (3,\ 1+\sqrt{-5})\cdot(3,1-\sqrt{-5})\\&=\big(\,3\cdot 3,\ 3\cdot(1-\sqrt{-5}),\ (1+\sqrt{-5})\cdot 3,\ (1+\sqrt{-5})\cdot(1-\sqrt{-5})\,\big)\\&=\big(9,\ 3(1-\sqrt{-5}),\ 3(1+\sqrt{-5}),\ 6\,\big)\\&=(3)\cdot\big(3,\ 1-\sqrt{-5},\ 1+\sqrt{-5},\ 2\,\big)\\&=(3)\cdot(1)\qquad\big(\because 1=3-2\in\big(3,\ 1-\sqrt{-5},\ 1+\sqrt{-5},\ 2\,\big)\,\big)\\&=(3).\end{aligned}$$

□

問題 6-4 可換環 $A=\{a+b\sqrt{-5}\mid a,b\in\mathbb{Z}\}$ において次を示せ.

$$(2)=(2,\ 1+\sqrt{-5})^2.$$

[イデアルが導入された理由]

整数環 $\mathbb{Z}$ では素因数分解の一意性が成立する. 例えば, 6 の素因数分解は本質的には

$$6 = 2 \times 3$$

しかない. 一方, 可換環

$$A = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$$

で考えると,

$$6 = 2 \times 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5}) \qquad \text{(eq1)}$$

と 2 通りの既約元分解を持ち (既約元は可換環の素数にあたるもの), 分解の一意性が成り立たない. イデアルはこの不都合を解消するために 19 世紀の数学者デデキントにより導入された. A のイデアル

$$P = (2,\ 1 + \sqrt{-5}), \quad Q = (3,\ 1 + \sqrt{-5}), \quad R = (3,\ 1 - \sqrt{-5})$$

を考える. このとき, P, Q, R は A の素イデアル (=イデアルの素数みたいなもの) であり, これらを使うと A のイデアル (6) は

$$(6) = P^2QR$$

と素イデアル分解され, また分解はこれしかないことが証明できる. さらに

$$(2) = P^2, \quad (3) = QR, \quad (1 + \sqrt{-5}) = PQ, \quad (1 - \sqrt{-5}) = PR$$

であり, 等式 (eq1) の数の世界の 2 通りの分解はイデアルの立場で考えると,

$$(6) = P^2 \cdot QR = (2) \cdot (3), \qquad (6) = PQ \cdot PR = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$$

と, P, Q, R の掛け方の違いで生じていることが分かる.

可換環 A の (0) ではないイデアルはすべて素イデアルの積に一意的に分解できることが示せる. このような性質を持つ環をデデキント環という.

★「既約元」や「素イデアル」については後々の授業ノートで解説する.