7　代数系の基礎（4）–多項式環のイデアル–

K を体とする．つまり，K は和と積が定義されている可換環であって，零元 $0 \in K$ を除くすべての $a \in K$ が積に関する逆元をもつものであった．例えば，$K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ などを想定すれば良い．変数を X とするような K の元を係数に持つ一変数多項式全体の集合 $K[X]$ について，その性質や構造を考察していこう．

- **7-1 ： 割り算の原理**

多項式 $f(X) \in K[X]$ をとれば，

$$f(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0, \quad a_n, a_{n-1}, \ldots, a_0 \in K$$

という形でかける．このとき，n を $f(X)$ の **次数** といい，$\deg(f(X))$ で表す．

例 7-1　$f(X) = 3X^5 - 2X^4 + \dfrac{1}{4}X^3 + 1$ について，$\deg(f(X)) = 5$ である．また，定数関数 $g(X) = a_0$ $(a_0 \in K)$ については，$\deg(g(X)) = 0$ である．

定理 7.1 (割り算の原理)**.** 多項式 $f(X), g(X) \in K[X]$ $(\deg(g(X)) \geq 1)$ に対して，

$$f(X) = g(X)q(X) + r(X), \quad \deg(r(X)) < \deg(g(X))$$

となる $q(X), r(X) \in K[X]$ が一意的に存在する．

証明. $\deg(f(X)) = n$, $\deg(g(X)) = m$ とする．
（存在の証明） まず，$n < m$ ならば，$q(X) = 0$, $r(X) = f(X)$ とすればよい．
次に $n \geq m$ のときを考えよう．

$$f(X) = a_0 X^n + (\text{低次の項}), \quad g(X) = bX^m + (\text{低次の項}) \quad (a_0, b \in K)$$

としよう．このとき，

$$f_1(X) := f(X) - a_0 b^{-1} X^{n-m} g(X)$$

と定める．すると，$n_1 := \deg(f_1(X))$, $n_0 := n$ とおけば，$n_1 < n_0 = n$ である．もし $n_1 < m$ であれば，$q(X) = a_0 b^{-1} X^{n-m}$, $r(X) = f_1(X)$ とおけばよい．$n_1 \geq m$ のときを考える．

$$f_1(X) = a_1 X^{n_1} + (\text{低次の項})$$

と表されていたとして，

$$f_2(X) := f_1(X) - a_1 b^{-1} X^{n_1 - m} g(X)$$

と定める．すると，$n_2 := \deg(f_2(X))$ とおけば，$n_2 < n_1 < n$ である．このように帰納的に

$$f_k(X) = a_k X^{n_k} + (\text{低次の項})$$

と表されているときに，多項式 $f_{k+1}(X)$ を

$$f_{k+1}(X) := f_k(X) - a_k b^{-1} X^{n_k - m} g(X)$$

と定め，$n_{k+1} := \deg(f_{k+1}(X))$ と定義する．すると，

$$0 \leq n_{k+1} < n_k < n_{k-1} < \cdots < n_2 < n_1 < n_0 = n$$

担当：茨城大学 情報科学領域　宮本 賢伍

が成り立つ. すると, $m > 0$ だからどこかの ℓ で $n_\ell < m$ となるはずである. 今, 整数 ℓ で初めて $n_\ell < m$ となったとしよう. このとき,

$$r(X) := f_\ell(X), \quad q(X) := \sum_{i=0}^{\ell-1} a_i b^{-1} X^{n_i - m}$$

と定義すれば,

$$\begin{aligned} q(X)g(X) + r(X) &= \sum_{i=0}^{\ell-1} a_i b^{-1} X^{n_i-m} g(X) + f_\ell(X) \\ &= \sum_{i=0}^{\ell-2} a_i b^{-1} X^{n_i-m} g(X) + a_{\ell-1} b^{-1} X^{n_{\ell-1}-m} g(X) + f_\ell(X) \\ &= \sum_{i=0}^{\ell-2} a_i b^{-1} X^{n_i-m} g(X) + f_{\ell-1}(X) \\ &= \cdots \\ &= a_0 b^{-1} X^{n_0-m} g(X) + f_1(X) \\ &= f(X) \end{aligned}$$

となり, 求める表示を得ることができた.

（一意性の証明） $f(X)$ が 2 通りの表示

$$f(X) = q_1(X)g(X) + r_1(X) = q_2(X)g(X) + r_2(X), \quad \deg(r_1(X)), \deg(r_2(X)) < \deg(g(X))$$

を持ったとしよう. すると,

$$(q_1(X) - q_2(X))g(X) = r_1(X) - r_2(X)$$

となる. もし, $q_1(X) - q_2(X) \neq 0$ であれば,

$$\deg((q_1(X) - q_2(X))g(X)) \geq \deg(g(X))$$

であるが, $\deg(r_1(X)), \deg(r_2(X)) < \deg(g(X))$ だったので

$$\deg(r_1(X) - r_2(X)) < \deg(g(X))$$

となる. これは矛盾であるから $q_1(X) - q_2(X) = 0$, すなわち $q_1(X) = q_2(X)$ である. このとき,

$$r_1(X) = f(X) - q_1(X)g(X) = f(X) - q_2(X)g(X) = r_2(X)$$

となり, 一意性が示された. □

レポート 7-1 $f(X) = 2X^4 + 7X^3 + 3X^2 + 2X - 6$, $g(X) = 2X + 1$ とするとき,

$$f(X) = g(X)q(X) + r(X), \quad \deg(r(X)) < \deg(g(X))$$

となる $q(X), r(X) \in \mathbb{R}[X]$ を求めよ.

• 7-2 : 既約多項式

定義 7.2. K を体とする. このとき, 定数でない $f(X) \in K[X]$ が K 上の **既約多項式** であるとは,

$$f(X) = g(X)h(X), \quad \deg(g(X)), \deg(h(X)) \geq 1$$

となるような多項式 $g(X), h(X) \in K[X]$ が存在しないときをいう. つまり, これ以上因数分解できないような多項式である. 既約多項式ではないような多項式は **可約** と呼ばれる.

担当：茨城大学 情報科学領域　宮本 賢伍

例 7-2　$f(X) = X^2 + 1$ を考えれば, これは $\mathbb{R}$ の範囲でこれ以上因数分解できないので $\mathbb{R}$ 上の既約多項式である. 一方, $f(X) = X^2 + 1$ は $\mathbb{C}$ の範囲で

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

と因数分解できるので, $\mathbb{C}$ 上の既約多項式ではない.

- **7-3 : 多項式環 $K[X]$ のイデアル**

多項式 $f(X) \in K[X]$ の生成するイデアルは

$$(f(X)) = \{f(X)g(X) \mid g(X) \in K[X]\}$$

であった. つまり, 「$f(X)$ の多項式倍」全体からなる集合である. このようなイデアルを単項イデアルと呼んだが, $\mathbb{Z}$ の場合（**命題 6.6** を参照せよ）と同様にして, $K[X]$ のイデアルは $(f(X))$ のようなものしか存在しないことを観察しよう.

命題 7.3. 環 $K[X]$ のイデアルはすべて単項イデアルとなる. つまり, $K[X]$ の任意のイデアル I に対して, ある $f(X) \in K[X]$ が存在して, $I = (f(X))$ とできる.

証明. $K[X]$ のイデアル I を任意にとる. $I = \{0\}$ ならば, **命題 6.2** より $I = (0)$ で単項イデアルだから, $I \neq (0)$ と仮定する. また, $I = K[X]$ ならば,

$$K[X] = \{1 \cdot f(X) \mid f(X) \in K[X]\} = (1)$$

なので, $I \neq K[X]$ としてもよい. すると, **命題 6.5** より定数でないような多項式を I は含む. このような I に属する定数でない多項式のなかで, 最も次数の低いものを一つ取り, これを $f(X)$ とおく. 以下, $I = (f(X))$ を証明しよう.

任意の $h(X) \in (f(X))$ をとれば, $h(X) = g(X)f(X)$ となる多項式 $g(X) \in K[X]$ がとれる. $f(X) \in I$ だから (ID2) より $g(X)f(X) \in I$. 従って $h(X) \in I$ となり, $(f(X)) \subset I$ が示された.

次に任意の $h(X) \in I$ をとる. 割り算の原理より

$$h(X) = f(X)q(X) + r(X), \quad \deg(r(X)) < \deg(f(X))$$

となるような $q(X), r(X) \in K[X]$ が存在する. このとき, $r(X) = h(X) - f(X)q(X)$ だが, $h(X) \in I$ であり, $f(X)q(X) \in (f(X)) \subset I$ だから (ID1) より $r(X) \in I$ となる. $f(X)$ は I のなかで定数でないような次数が最小の多項式であったから, $\deg(r(X)) < \deg(f(X))$ より $r(X)$ は定数でなければならない. $r(X) \neq 0$ ならば, $r(X) \in K$ で可逆となり $I = K[X]$ となり不合理である. よって $r(X) = 0$ だから

$$h(X) = f(X)q(X) \in (f(X))$$

がわかる. 故に $I \subset (f(X))$ が示されたので $I = (f(X))$ である. □

命題 7.4. 環 $K[X]$ の 2 つのイデアル $(f(X))$, $(g(X))$ について, $(f(X)) \subset (g(X))$ であることと, $g(X)$ が $f(X)$ を割り切ることは同値である.

証明. **（必要条件）** $f(X) \in (f(X)) \subset (g(X))$ より, ある $h(X) \in K[X]$ が存在して $f(X) = g(X)h(X)$ とかけるので $g(X)$ は $f(X)$ を割り切る.

（十分条件） $g(X)$ が $f(X)$ を割り切るとき, ある $h(X) \in K[X]$ が存在して $f(X) = g(X)h(X)$ で表せる. 従って $f(X) \in (g(X))$ である. ところで, 任意の $p(X) \in (f(X))$ をとれば, ある $q(X) \in K[X]$ が存在して $p(X) = f(X)q(X)$ とかけるので,

$$p(X) = f(X)q(X) = g(X)h(X)q(X)$$

担当：茨城大学 情報科学領域　宮本 賢伍

となり, $p(X) \in (g(X))$ がわかる. よって, $(f(X)) \subset (g(X))$ がわかった. □

命題 7.3 と**命題 7.4** によって, $K[X]$ のイデアルの中で包含に関して “極大” となっているは, 既約多項式 $f(X)$ が生成する単項イデアルであることがわかった.

レポート 7-2　$f(X) = (X+1)(X+2)(X+3)(X+6) - 3X^2 \in \mathbb{R}[X]$ を考える. $\mathbb{R}$ 上の既約多項式 $g(X) \in \mathbb{R}[X]$ であって, $f(X) \in (g(X))$ となるような多項式 $g(X)$ をすべて求めよ.

担当：茨城大学 情報科学領域　宮本 賢伍