環論 (第4回)

4. 多項式環

今回は多項式環の基本事項について解説する．また多項式環上の割り算の原理と応用について紹介する．

定義 4-1 (多項式環)
可換環 A に対して, x を変数とする A 係数多項式の集合

$$A[x] = \left\{ \sum_{i=0}^{n} a_i x^i \;\middle|\; a_i \in A, \quad n \in \mathbb{Z}_{\geq 0} \right\}$$

を考える．二つの多項式 $f(x) = \sum_{i=0}^{n} a_i x^i$, $g(x) = \sum_{i=0}^{m} b_i x^i \in A[x]$ が等しいことを

$$f(x) = g(x) \overset{\text{def}}{\iff} a_i = b_i \ \ (i = 0, 1, 2, ...)$$

で定める．また和と積を次で定義する．

$$\left(\sum_{i=0}^{n} a_i x^i\right) + \left(\sum_{i=0}^{m} b_i x^i\right) \ \ \overset{\text{def}}{=} \ \ \sum_{i=0}^{\max\{n,m\}} (a_i + b_i) x^i,$$

$$\left(\sum_{i=0}^{n} a_i x^i\right) \cdot \left(\sum_{i=0}^{m} b_i x^i\right) \ \ \overset{\text{def}}{=} \ \ \sum_{k=0}^{n+m} \left(\sum_{i+j=k} a_i b_j\right) x^k.$$

この演算により $A[x]$ は可換環となり, その零元と単位元はそれぞれ

$$0_{A[x]} = 0 + 0 \cdot x + 0 \cdot x^2 + \cdots, \qquad 1_{A[x]} = 1 + 0 \cdot x + 0 \cdot x^2 + \cdots$$

である．$A[x]$ を A **上の** 1 **変数多項式環**という．

[補足]

(1) A 係数多項式を $f(x) = \sum_{i} a_i x^i$ と表すこともある．この場合はある整数 $n \in \mathbb{Z}_{\geq 0}$ が存在して

$$f(x) = \sum_{i=0}^{n} a_i x^i$$

という意味である．

(2) $f(x) = \sum_{i} a_i x^i \in A[x]$ に対して,

$$f(x) = 0 \iff a_i = 0 \ (i = 0, 1, 2, ...).$$

(3) $a \in A$ と多項式 $a + 0 \cdot x + 0 \cdot x^2 + \cdots \in A[x]$ を同一視すると, A は $A[x]$ の部分環と見なせる．

(4) 自然数 $n \geq 2$ に対して, A 上の n 変数多項式環は帰納的に次で定義する.

$$A[x_1, x_2, ..., x_n] = (A[x_1, x_2, ..., x_{n-1}])[x_n].$$

定義 4-2 (多項式の次数)

可換環 A 上の多項式 $f(x) \in A[x]$ が

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n \quad (a_n \neq 0)$$

と表せるとき, $\deg f(x) := n$ とする. また $\deg 0 := -\infty$ とする. $\deg f(x)$ を $f(x)$ **の次数**という. 定義より,

$$\deg f(x) \geq 0 \iff f(x) \neq 0.$$

例えば, $\mathbb{Z}[x]$ において,

$$\deg(1 + x^3) = 3, \quad \deg(2 + 3x) = 1, \quad \deg 1 = 0$$

である.

定理 4-1

A を整域とする.

(1) $f(x),\ g(x) \in A[x]$ のとき,

$$\deg(f(x)g(x)) = \deg f(x) + \deg g(x).$$

(2) $A[x]$ は整域.

[証明]

(1) $f(x) = 0$ または $g(x) = 0$ のときは明らかなので, $f(x) \neq 0$ かつ $g(x) \neq 0$ のとき示す.

$$\begin{aligned} f(x) &= a_m x^m + a_{m-1} x^{m-1} + \cdots + a_0 \quad (a_m \neq 0), \\ g(x) &= b_n x^n + b_{n-1} x^{n-1} + \cdots + b_0 \quad (b_n \neq 0) \end{aligned}$$

と表すと,

$$f(x)g(x) = (a_m b_n) x^{m+n} \underbrace{+ \cdots + \cdots\cdots}_{n+m-1\ \text{次以下}}.$$

A は整域より $a_m b_n \neq 0$. 従って

$$\deg(f(x)g(x)) = m + n = \deg f(x) + \deg g(x).$$

(2) 問題 4-1.

□

問題 4-1　定理 4-1 (2) を示せ.

定理 4-2 (割り算の原理)

A を可換環とし,

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in A[x] \quad (a_n \in A^\times)$$

とする. このとき, $g(x) \in A[x]$ に対して,

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

を満たす $q(x), r(x) \in A[x]$ が一意的に存在する.

※ $q(x)$ を $g(x)$ **を** $f(x)$ **で割った商**, $r(x)$ を $g(x)$ **を** $f(x)$ **で割った余り**という.

[証明]

(存在) $n = 0$ の場合は

$$q(x) = a_0^{-1}g(x), \quad r(x) = 0$$

とすればよい.

次に $n \geq 1$ かつ $g(x) \neq 0$ の場合を $m := \deg g(x)$ に関する帰納法で証明する.

(i) $m < n$ の場合は

$$q(x) = 0, \quad r(x) = g(x)$$

とすればよい. 特に $m = 0$ のとき正しい.

(ii) $m - 1$ まで正しいと仮定する. (i) より $m \geq n$ の場合だけ考えればよい.

$$g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_0$$

と表す. このとき,

$$h(x) = g(x) - b_m a_n^{-1} f(x) x^{m-n} \quad \text{(eq1)}$$

とおくと, $\deg h(x) \leq m - 1$. 帰納法の仮定から

$$h(x) = q_0(x)f(x) + r_0(x), \quad \deg r_0(x) < \deg f(x) \quad \text{(eq2)}$$

を満たす $q_0(x), r_0(x) \in A[x]$ が存在する. 式 (eq1), (eq2) より

$$g(x) = \{q_0(x) + b_m a_n^{-1} x^{m-n}\} f(x) + r_0(x), \quad \deg r_0(x) < \deg f(x).$$

これで m のときも正しいことが分かった.

(一意性) 2 通りで表せたとする.

$$\begin{aligned} g(x) &= q_1(x)f(x) + r_1(x), \quad \deg r_1(x) < \deg f(x) \quad (q_1(x), r_1(x) \in A[x]), \\ g(x) &= q_2(x)f(x) + r_2(x), \quad \deg r_2(x) < \deg f(x) \quad (q_2(x), r_2(x) \in A[x]). \end{aligned}$$

このとき,

$$(q_1(x)-q_2(x))f(x)=r_2(x)-r_1(x).$$

$q_1(x)-q_2(x)\neq 0$ と仮定すると,

$$\deg f(x)\leq \deg f(x)+\deg(q_1(x)-q_2(x))=\deg(r_2(x)-r_1(x))\leq \max\{\deg r_1(x),\ \deg r_2(x)\}.$$

これは $\deg r_i(x)<\deg f(x)$ $(i=1,2)$ に矛盾. 従って $q_1(x)=q_2(x)$ であり, $r_1(x)=r_2(x)$.

□

$f(x)=x^2-1,\ g(x)=x^3+1\in\mathbb{C}[x]$ とする. このとき,

$$g(x)=xf(x)+(x+1).$$

よって $g(x)$ を $f(x)$ で割った商は x, 余りは $x+1$.

[補足] 定理 4-2 で $a_n\in A^\times$ の条件に注意. $f(x)=2x+1$ と $g(x)=x^2+1$ に対して,

$$g(x)=\left(\frac{1}{2}x-\frac{1}{4}\right)f(x)+\frac{5}{4}$$

となり, $\mathbb{Z}[x]$ において $g(x)$ は $f(x)$ で割り算できない ($\mathbb{Q}[x]$ では可能).

例題 4-1.

$f(x)\in\mathbb{R}[x]$ を考える. $f(\sqrt{-1})=0$ のとき, $x^2+1\mid f(x)$ を示せ.

※ $p(x)\mid q(x)$ は「$q(x)$ は $p(x)$ の倍数」の意味.

[解答]

$\mathbb{R}[x]$ で $f(x)$ を x^2+1 で割ると,

$$f(x)=(x^2+1)q(x)+ax+b\ \ (q(x)\in\mathbb{R}[x],\ \ a,b\in\mathbb{R})$$

と表せる. このとき,

$$0=f(\sqrt{-1})=a\sqrt{-1}+b.$$

$a,b\in\mathbb{R}$ より, $a=b=0$. 従って $x^2+1\mid f(x)$.

□

[補足] 例題 4-1 は $\mathbb{R}[x]$ で割り算しているところがポイント. $\mathbb{C}[x]$ で割り算を行うと, $a,b\in\mathbb{C}$ となり, 上の議論はうまくいかない.

問題 4-2 $f(x)\in\mathbb{R}[x]$ とする. $f(1)=f(-1)=1$ のとき, $f(x)$ を x^2-1 で割った余りを求めよ.

問題 4-3 A を可換環とし, $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0\in A[x]$ $(a_n\in A^\times)$ とする. $g_1(x),\ g_2(x)\in A[x]$ を $f(x)$ で割った余りをそれぞれ $r_1(x),r_2(x)$ とするとき, 次の同値を示せ.

$$r_1(x)=r_2(x)\iff f(x)\mid(g_1(x)-g_2(x)).$$

定理 4-3

A を整域とし, $f(x) \in A[x]$ $(f(x) \neq 0)$ とする. また, $\alpha_1, \alpha_2, ..., \alpha_s \in A$ を $f(x)$ の相異なる根とする.

(1) $f(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_s)q(x)$ を満たす $q(x) \in A[x]$ が存在する.

(2) $\deg f \geq s$.

[証明]

(1) s に関する帰納法で示す. $s=0$ のときは $q(x)=f(x)$ とすればよい. 次に $s \geq 1$ のときを考える. $f(x)$ を $x-\alpha_1$ で割ると, 定理 4-2 より

$$f(x) = (x-\alpha_1)q_1(x) + a, \quad (q(x) \in A[x],\ a \in A)$$

と表せる. $0 = f(\alpha_1) = a$ より, $f(x) = (x-\alpha_1)q_1(x)$. また $i = 2, 3, ..., s$ に対して,

$$0 = f(\alpha_i) = (\alpha_i - \alpha_1)q_1(\alpha_i), \quad \alpha_i - \alpha_1 \neq 0$$

であり, A は整域であるから $q_1(\alpha_i) = 0$. 帰納法の仮定から

$$q_1(x) = (x-\alpha_2)(x-\alpha_3)\cdots(x-\alpha_s)q(x) \quad (q(x) \in A[x])$$

と表せる. 以上より $f(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_s)q(x)$.

(2) (1) と定理 4-1 より $\deg f = s + \deg q \geq s$.

□

問題 4-4 A を整域とし, $f(x), g(x) \in A[x]$ $(n = \deg f \geq \deg g)$ とする. また $\alpha_1, \alpha_2, ..., \alpha_{n+1} \in A$ は相異なるとする. $f(\alpha_i) = g(\alpha_i)$ $(i = 1, 2, ..., n+1)$ ならば, $f(x) = g(x)$ を示せ.