第2章　複素数と代数学の基本定理

以下では $\mathbf{K}$ で $\mathbf{R}$ または $\mathbf{C}$ を表します．また $\mathbf{K}[x]$ は $\mathbf{K}$ を係数とする多項式全体の集合を表します．

2.3　多項式

2.3.3　多項式の次数

1. $P(x) \in \mathbf{K}[x]$ が $P(x) \neq 0$ であるとします．

$$P(x) = a_n x^n + \cdots + a_1 x + a_0,\ a_j \in \mathbf{K}(j = 0, \cdots, n), a_n \neq 0 \tag{2.1}$$

とします．このとき P の次数として

$$\deg(P) = n$$

と定めます．
2. $P(x) \in \mathbf{K}[x]$ が $P(x) = 0$ であるとします．このとき

$$\deg(P) = -\infty$$

と定めます．
3. $P, Q \in \mathbf{K}[x]$ のとき

$$\deg(PQ) = \deg(P) + \deg(Q)$$

が成立します．これは P が (2.1)

$$Q(x) = b_m x^m + \cdots + b_1 x + b_0,\ b_k \in \mathbf{K}(k = 0, \cdots, m), b_m \neq 0 \tag{2.2}$$

で与えられているとき

$$(P \cdot Q)(x) = a_n b_m x^{m+n} + \cdots + c_\ell x^\ell + \cdots + c_1 x + c_0$$

$$c_\ell = \sum_{i+j=\ell} a_i b_j$$

となることから示せます．
4. **（剰余定理）**

定理 2.1. $P, D \in \mathbf{K}[x]$ で $\deg(D) \geq 1$ とします．このとき

$$P(x) = D(x)Q(x) + R(x)$$

$$\deg(R(x)) < \deg(D(x))$$

を満たす $Q(x), R(x) \in \mathbf{K}[x]$ がただ一つ存在します．

Proof. **（存在）**　**(i)** $\deg(P) < \deg(D)$ の場合

$$P(x) = 0 \cdot D(x) + P(x),\ \deg(P(x)) < \deg(D(x))$$

となりますから，$Q(x) = 0,\ R(x) = P(x)$ として成立します．
(ii) $n = \deg(P) \geq \deg(D) = m$ の場合を考えます．帰納法を用いるとして，$\deg(P) \leq n-1$ の場合は定理（存在について）が示されているとします．

$$D(x) = b_m x^m + \cdots + b_1 x + b_0,\ b_k \in \mathbf{K}(k = 0, \cdots, m), b_m \neq 0$$

$$P(x) = a_n x^n + \cdots + a_1 x + a_0,\ a_j \in \mathbf{K}(j = 0, \cdots, n), a_n \neq 0$$

とします．ここで

$$S(x) := P(x) - a_n b_m^{-1} x^{n-m} D(x)$$

とすると

$$\deg(S(x)) \leq n - 1$$

となります．帰納法の仮定を用いると

$$S(x) = Q_1(x)D(x) + R(x), \quad \deg(R(x)) < \deg(D(x))$$

を満たす $Q_1,\ R \in \mathbf{K}[x]$ が存在します．このとき

$$P(x) = (a_n b_m x^{n-m} + Q_1(x))D(x) + R(x)$$

より

$$Q(x) = a_n b_m x^{n-m} + Q_1(x)$$

として定理（存在について）が成立することが分かります．
（一意性）

$$P(x) = Q(x)D(x) + R(x) = Q_0(x)D(x) + R_0(x)$$

$$\deg(R(x)) < \deg(D(x)),\ \deg(R_0(x)) < \deg(D_0(x))$$

が成立するとします．このとき

$$(Q(x) - Q_0(x))D(x) = R_0(x) - R(x)$$

が成立しますが，$R \neq R_0$ とすると $Q(x) - Q_0(x) \neq 0$ が従います[1] ．このことから

$$\deg(D) > \deg(R_0 - R_1) = \deg(Q - Q_0) + \deg(D) \geq \deg(D)$$

から矛盾が生じます．よって $R = R_0$ が導かれます．さらに $D \neq 0$ から $Q = Q_0$ も従います． □

定理 2.1（剰余定理）を用いると次の定理 2.2（因数定理）を証明できます.

定理 2.2.（因数定理） $P(x) \in \mathbf{K}[x]$, $\alpha \in$ ‘K のとき

$$P(\alpha) = 0 \ \Leftrightarrow \ x - \alpha\text{は}P(x)\text{を割切ります}$$

Proof. （⇒ ）$P(x)$ を $x - \alpha$ で割ります．すなわち

$$P(x) = (x - \alpha)Q(x) + \beta$$

を満たす $Q(x) \in \mathbf{K}[x]$, $\beta \in \mathbf{K}$ が存在します．この両辺に $x = \alpha$ を代入すると

$$0 = P(\alpha) = 0 \cdot Q(\alpha) + \beta = \beta$$

から $\beta = 0$ が分かりますから，$P(x) = (x - \alpha)Q(x)$ が導けます.
（⇐ ）これは明らかでしょう. □

定理 2.2（因数定理）の応用として次の定理 2.3 を証明します.

定理 2.3. $P(x) \in \mathbf{K}[x]$ が n 次以下とします．そして $\alpha_1, \cdots, \alpha_n, \alpha_{n+1} \in \mathbf{K}$ が条件

$$\alpha_i \neq \alpha_j \ (i \neq j), \ P(\alpha_i) = 0 \ (1 \leq i \leq n+1)$$

を満たすとします．このとき

$$P(x) = 0$$

が成立します.

Proof. 因数定理によって $P(\alpha_1) = 0$ から

$$P(x) = (x - \alpha_1)P_1(x)$$

を満たす $P_1(x) \in \mathbf{K}[x]$ が存在します．さらに $P(\alpha_2) = 0$ と $\alpha_1 \neq \alpha_2$ が成立しますから

$$0 = P(\alpha_2) = (\alpha_2 - \alpha_1)P_1(\alpha_2)$$

[1] $P_1, P_2 \in \mathbf{K}[x]$ において $P_1 P_2 = 0$ ならば $P_1 = 0$ または $P_2 = 0$ となることを用いています.

から $P_1(\alpha_2)=0$ が従います．よって因数定理を用いると

$$P_1(x)=(x-\alpha_2)P_2(x),\ \text{従って}\ P(x)=(x-\alpha_1)(x-\alpha_2)P_2(x)$$

を満たす $P_2(x)\in\mathbf{K}[x]$ が存在することが分かります．このプロセスを繰り返します．すなわち，いま $i\leq n-1$ を満たす i に対して

$$P(x)=(x-\alpha_1)\cdots(x-\alpha_i)P_i(x)$$

を満たす $P_i(x)\in\mathbf{K}[x]$ が存在するとします．$x=\alpha_{i+1}$ を代入すると

$$0=P(\alpha_{i+1})=(\alpha_{i+1}-\alpha_1)\cdots(\alpha_{i+1}-\alpha_i)P_i(\alpha_{i+1})$$

が従います．さらに $\alpha_{i+1}\neq\alpha_k$ $(k=1,\cdots,i)$ から

$$P_i(\alpha_{i+1})=0$$

を得ます．よって因数定理から

$$P_i(x)=(x-\alpha_{i+1})P_{i+1}(x)\ \text{従って}\ P(x)=(x-\alpha_1)\cdots(x-\alpha_{i+1})P_{i+1}(x)$$

を満たす $P_{i+1}(x)\in\mathbf{K}[x]$ が存在することが分かります．特に $i=n-1$ のとき

$$P(x)=(x-\alpha_1)\cdots(x-\alpha_n)P_n(x)$$

となります．この両辺の次数を考えると

$$n\geq\deg(P)=n+\deg(P_n)$$

から

$$\deg(P_n)\leq 0$$

が分かります．すなわち $P_n(x)=\alpha\in\mathbf{K}$ であることが導かれました．

$$P(x)=(x-\alpha_1)\cdots(x-\alpha_n)\alpha$$

に $x=\alpha_{n+1}$ を代入すると

$$0=P(\alpha_{n+1})=(\alpha_{n+1}-\alpha_1)\cdots(\alpha_{n+1}-\alpha_n)\alpha$$

から $\alpha=0$ であることがが結論できます．以上で $P(x)=0$ であることが証明できました．

□

2.4 ユークリッドの互除法

定理 2.1（剰余定理）の応用として，2 つの多項式 $f(x), g(x) \in \mathbf{K}[x]$ の最大次数の共通因子を求める**ユークリッドの互除法**を解説します．以下のように割り算を繰り返します．

$f(x)$ を $g(x)$ で割るとき	商：$q_1(x)$	剰余：$r_1(x)$
$g(x)$ を $r_1(x)$ で割るとき	商：$q_2(x)$	剰余：$r_2(x)$
$r_1(x)$ を $r_2(x)$ で割るとき	商：$q_3(x)$	剰余：$r_3(x)$
$r_2(x)$ を $r_3(x)$ で割るとき	商：$q_4(x)$	剰余：$r_4(x)$
	⋮	
$r_{k-2}(x)$ を $r_{k-1}(x)$ で割るとき	商：$q_k(x)$	剰余：$r_k(x)$
	⋮	

とします．このとき

$$\begin{aligned} f(x) &= q_1(x)g(x) + r_1(x) \\ g(x) &= q_2(x)r_1(x) + r_2(x) \\ r_1(x) &= q_3(x)r_2(x) + r_3(x) \\ &\vdots \\ r_{k-2}(x) &= q_k(x)r_{k-1}(x) + r_k(x) \\ &\vdots \end{aligned}$$

となります．剰余の次数に着目すると

$$\deg(r_1) > \deg(r_2) > \deg(r_3) > \cdots$$

と 1 以上小さくなっていきますから，ある時点で

$$\deg(r_k) = 0 \quad \text{または} \quad \deg(r_k) = -\infty$$

となります．
$\deg(r_k) = 0$のときは，$r_k = c \neq 0$ と $c \in \mathbf{K}$ が最大次数の共通因子となりますから f と g は互いに素であることが分かります．
$\deg(r_k) = -\infty$のときは，$r_k = 0$ となりますから $r_{k-1}(x)$ が f と g の最大次数の共通因子となります．