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） $P(x) \in \mathbf{K}[x]$, $\alpha \in \mathbf{K}$ 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 公約式・最大公約式

多項式 $f(t), g(t) \in \mathbf{K}[t]$ が与えられているとします．f が g で**割り切れる**とは，f を g で割った剰余が 0 ということです．すなわち

$$f(t) = g(t)h(t)$$

を満たす $h(t) \in \mathbf{K}[t]$ が存在することです．このとき g を f の**因子** (divisor) と呼び

$$g(t)|f(t)$$

と記します．

多項式 $f_1(t), \cdots, f_\ell(t) \in \mathbf{K}[t]$ すべての因子である $g(t) \in \mathbf{K}[t]$ を**公約式**と呼びます：

$$g(t)|f_1(t),\ \cdots, g(t)|f_\ell(t)$$

このとき次数について

$$\deg(g(t)) \leq \deg(f_i(t)) \quad (i = 1, \ddots, \ell)$$

が成立するので，最大次数の公約式 $d(t)$ が存在することが分かり． **最大公約式**と呼びます．証明を考えるときに，$1 \in \mathbf{K}[t]$ が公約式になることにも注意しよう．ここで最高次の係数が 1 とすると[2]最大公約式はただ一つ存在することが示ます．そのための道はいろいろありますが，ここでは**（拡張）ユークリッドの互除法**を用いることにします[3]．

2.5 （拡張）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 **（拡張）ユークリッドの互除法**を解説します．まず拡張版でない互除法についてです．

まず $f_0 := f,\ f_1 := g$ として，以下のように割り算を繰り返します．

$f_0(x) = f(x)$ を $f_1(x) = g(x)$ で割るとき	商：$q_1(x)$	剰余：$f_2(x)$
$f_1(x) = g(x)$ を $f_2(x)$ で割るとき	商：$q_2(x)$	剰余：$f_3(x)$
$f_2(x)$ を $f_3(x)$ で割るとき	商：$q_3(x)$	剰余：$f_4(x)$
$f_3(x)$ を $f_4(x)$ で割るとき	商：$q_4(x)$	剰余：$f_5(x)$
	⋮	
$f_{k-2}(x)$ を $f_{k-1}(x)$ で割るとき	商：$q_{k-1}(x)$	剰余：$f_k(x)$
	⋮	

[2]最高次数の係数が 1 である多項式 $t^m + a_{m-1}t^{m-1} + \ddots + a_1 t + a_0$ のことをモニック (monic) な多項式と呼びます．

[3]線型代数学の教科書にはイデアル（Ideal）を用いる流れを示してあります．

とします．このとき

$$f_0(x) = q_1(x)f_1(x) + f_2(x) \tag{0}$$
$$f_1(x) = q_2(x)f_2(x) + f_3(x) \tag{1}$$
$$f_2(x) = q_3(x)f_3(x) + f_4(x) \tag{2}$$
$$\vdots$$
$$f_{j-2}(x) = f_{j-1}(x)q_{j-1}(x) + f_j(x) \tag{j}$$
$$\vdots$$

となります．剰余の次数に着目すると

$$\deg(f_1) > \deg(f_2) > \deg(f_3) > \cdots$$

と 1 以上小さくなっていきますから，ある時点で

$$\deg(f_{k+1}) = -\infty$$

従って

$$f_{k-1}(t) = q_k(t)f_k(t)$$

となります．以上のプロセスで

$$f_{j-2}(x) = q_{j-1}(x)f_{j-1}(x) + f_j(x)$$

において f_{j-2} と f_{j-1} の共通因子であることと f_{j-1} と f_j の共通因子であることは必要十分です．従って f_0 と f_1 の共通因子と f_{k-1} と f_k の共通因子は一致します．f_k が f_{k-1} と f_k の最大公約式なので，f_0 と f_1 の最大公約式であることが従います．

次に上で求めた $f(t)$ と $g(t)$ の最大公約式 $d(t) = f_k(t)$ に対して

$$a(t)f(t) + b(t)g(t) = d(t)$$

を満たす $a(t), b(t) \in \mathbf{K}[t]$ を求めることを考えましょう．ここでは上で求めた $f_0, f_1, \ddots, f_k$ に対して順次

$$a(t)_i f(t) + b_i(t)g(t) = f_i(t)$$

を満たす $a_i(t), b_i(t)$ を定めていく形で $a(t) = a_k(t), b(t) = b_k(t)$ を求めていきます．

最初に

$$a_0 = 1,\ b_0 = 0, a_1 = 0, b_1 = 1$$

と定めます．すると $f = f_0, g = g_1$ と (0),(1) に注意すると

$$a_0 f + b_0 g = f_0, \quad a_1 f + b_1 g = f_1$$

が成立します. 帰納的に

$$a(t)_i f(t) + b_i(t)g(t) = f_i(t)$$

が $i = 0, 1, \ddots, j$ に対しているとして

$$a_{j+1} := a_{j-1} - q_j a_j, \quad b_{j+1} := b_{j-1} - q_j b_j$$

と定めると (j-1) によって

$$\begin{aligned} f_{j+1} &= f_{j-1} - q_j f_j \\ &= (a_{j-1}f + b_{j-1}g) - q_j(a_j f + b_j g) \\ &= (a_{j-1} - q_j a_j)f + (b_{j-1} - q_j b_j) \\ &= a_{j+1}f + b_{j+1}g \end{aligned}$$

となります. これを繰り返していくと

$$a_k f + b_k g = f_k$$

となります. $a(t) = a_k(t),\ b(t) = b_k(t)$ と定めると

$$a(t)f(t) + b(t)g(t) = d(t) \tag{2.3}$$

が成立することが分かります.

定理 2.4.

$$(f, g) := \{h_1(t)f(t) + h_2(t)g(t) \in \mathbf{K}[t];\ h_1(t), h_2(t) \in \mathbf{K}[t]\}$$

$$(d) := \{d(t)h(t) \in \mathbf{K}[t];\ h(t) \in \mathbf{K}[t]\}$$

と定めると

$$(f, g) = (d)$$

が成立します.

Proof. 任意の $p \in (f, g)$ を取ります. すると

$$p(t) = h_1(t)f(t) + h_2(t)g(t),\ h_1(t), h_2(t) \in \mathbf{K}[t]$$

と表されます. $d(t)$ は $f(t)$ と $g(t)$ の公約数ですから

$$f(t) = p_1(t)d(t), \quad g(t) = p_2(t)d(t)$$

がある $p_1(t), p_2(t) \in \mathbf{K}[t]$ に対して成立します. このとき

$$p(t) = h_1(t)p_1(t)d(t) + h_2(t)p_2(t)d(t) = (h_1(t)p_1(t) + h_2(t)p_2(t))d(t) \in (d)$$

から $(f,g)\subset(d)$ であることが分かります.

逆に $p(t)\in(d)$ をとると，ある $q(t)\in\mathbf{K}[t]$ に対して

$$p(t)=d(t)q(t)=(a(t)f(t)+b(t)g(t))q(t)=a(t)q(t)f(t)+b(t)q(t)g(t)\in(f,g)$$

となりますから $(d)\subset(f,g)$ であることが分かります. □

(d) を $d(t)$ が生成する**イデアル**, (f,g) を $f(t)$ と $g(t)$ が生成するイデアルと呼びます.

定理 2.5. $c(t)\in\mathbf{K}[t]$ が $f(t)$ と $g(t)$ の公約式であるとします：

$$c(t)|f(t),c(t)|g(t)$$

このとき $c(t)|d(t)$ が成立します.

Proof. 仮定から

$$f(t)=q_1(t)c(t),\ g(t)=q_2(t)c(t)$$

がある $q_1(t),q_2(t)\in\mathbf{K}[t]$ に対して成立します. この状況で

$$d(t)=a(t)f(t)+b(t)g(t)=a(t)q_1(t)c(t)+b(t)q_2(t)c(t)=(a(t)q_1(t)+b(t)q_2(t))c(t)$$

となりますから，$c|d$ が分かります. □

ここで $c(t)$ として $f(t)$ と $g(t)$ に別の最大公約式 $d'(t)$ を考えます. $d'(t)$ は $f(t)$ と $g(t)$ の公約式なので定理 2.5 を用いると

$$d(t)=d'(t)\alpha$$

を満たす $\alpha\in\mathbf{K}^*:=\mathbf{K}\setminus\{0\}$ が存在します. これが**最大公約式の一意性**です.