代数学の基本定理

Mr.

平成 15 年 8 月 7 日

1　一変数多項式

定義 1 (R-係数一変数多項式). R : 環, X : 不定元とする.
R-係数一変数多項式とは,

$$f(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n \quad (a_0, a_1, \ldots, a_n \in R).$$

$R[X] := \{f(X) | R$-係数一変数多項式 $\}$ は,

$$\text{和}: \quad \left(\sum_{i=0}^{m} a_iX^i\right) + \left(\sum_{i=0}^{n} b_iX^i\right) := \sum_{i=0}^{\max(m,n)} (a_i + b_i)X^i,$$

$$\text{積}: \quad \left(\sum_{i=0}^{m} a_iX^i\right)\left(\sum_{i=0}^{n} b_iX^i\right) := \sum_{i=0}^{m+n} c_iX^i, \quad c_i = \sum_{j+k=i} (a_j + b_k)$$

により, 環になる. $R[X]$ を R 上の一変数多項式環と呼ぶ.

定義 2 (次数). R : 環とする.

$$f(X) = a_0 + a_1X + a_2X^2 + \cdots + a_mX^m \in R[X], \quad a_m \neq 0$$

であるとき, f の次数は m であるといい, $\deg f = m$ と書く.
ここで, $\deg 0 = -\infty$ と約束する.

$f, g \in R[X]$ について,

(i) $\deg(f + g) \leq \max\{\deg f, \deg g\}$

(ii) $\deg(fg) \leq \deg f + \deg g$

がわかる.

註. (i), (ii) で $\leq$ を $=$ に代えたものは一般には成立しない.

(i) $f(X) = X, g(X) = -X + 1$ とすると,

$$\deg(f + g) = 0 < 1 = \max\{\deg f, \deg g\}.$$

(ii) $a, b \in R, a \neq 0, b \neq 0, ab = 0$ であるとき, $f(X) = aX, g(X) = bX$ とすると,

$$-\infty = \deg(fg) < \deg f + \deg g = 2.$$

定義 3 (整除). K : 可換体, $f, g \in K[X]$ とする.

$$f \text{ が } g \text{ で割り切れる} \quad \overset{\text{def}}{\iff} \quad \exists q \in K[X] \text{ s.t. } f = gq.$$

このとき, g を f の約式, f を g の倍式と言う.

以下，K は可換体とする．

定理 1.

$$f, g \in K[X],\ g \neq 0 \quad \Longrightarrow \quad \exists! q, \exists! r \in K[X] \text{ s.t. } f = gq + r,\ \deg r < \deg g.$$

証明:　＜一意性＞　$q, r \in K[X]$ 及び $q_1, r_1 \in K[X]$ がともに条件を満たすとすると，

$$g(X)(q(X) - q_1(X)) = r_1(X) - r(X).$$

$q(X) - q_1(X) \neq 0$ ならば，左辺の次数は $\deg g$ より小さくない．一方右辺の次数は $\deg g$ より小さいから，$q_1(X) = q(X)$ でなければならない．よって，$r(X) = r_1(X)$ となる．

＜存在＞　$f(X)$ ならば，$q(X) = r(X) = 0$ とすればよい．よって，$f(X) \neq 0$ とし，$\deg f$ に関する induction で示す．

$\deg f = 0$ の場合:　$\deg g = 0$ ならば，$q(X) = f(X)/g(X), r(X) = 0$;$\deg g > 0$ ならば，$q(X) = 0, r(X) = f(X)$ とすればよい．

$\deg f = n > 0$ とし，$\deg h < n$ なる $\forall h \in K[X]$ に関しては主張は正しいと仮定する．

$$f(X) = a_n X^n + \cdots + a_1 X + a_0,\ a_n \neq 0,$$

$$g(X) = b_n X^m + \cdots + b_1 X + b_0,\ b_m \neq 0$$

としよう．$\deg f < \deg g$ ならば，$q(X) = 0, r(X) = f(X)$ とすればよい．

$\deg f \geq \deg g$ のとき，

$$f_1(X) := f(X) - \frac{a_n}{b_m} X^{n-m} g(X)$$

と置けば，$f_1 \in K[X]$ かつ $\deg f_1 < n$ である．induction の仮定より，

$$\exists q_1, \exists r \in K[X] \text{ s.t. } f_1(X) = g(X)q_1(X) + r(X),\ \deg r < m.$$

$$q(X) = \frac{a_n}{b_m} X^{n-m} + q_1(X)$$

とすればよい．

証明終.

定理 1 における q を整商，r を余りという．

系 1 (剰余定理). $f \in K[X], \alpha \in K$ とする．
$f(X)$ を $X - \alpha$ で割った余りは $f(\alpha)$ に等しい．

証明:　$f(X) = (X - \alpha)q(X) + r\,(q \in K[X], r \in K)$ において，$X = \alpha$ とすればよい．

証明終.

2　代数学の基本定理

前節では環及び可換体の上で多項式を考えてきたが，この節では複素数体 $\mathbb{C}$ 上で多項式を考える．

定義 4 (代数方程式). $f \in \mathbb{C}, \deg f = n$ とする．このとき，$f(X) = 0$ を n 次代数方程式と言う．

$\alpha \in \mathbb{C}$ が $f(\alpha) = 0$ を満たすとき，α を代数方程式 $f(X) = 0$ の根であると言う．

定理 2 (代数学の基本定理). 一次以上の任意の代数方程式は少なくとも一つの根を持つ．

証明:　与えられた方程式を

$$f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n,\ \ a_0 \neq 0,\ \ n \geq 1$$

とする．

(i)　複素変数の実数値関数 $\varphi : x \mapsto |f(x)|$ は，$\mathbb{C}$ 上で最小値を持つ．

実際，$x \neq 0$ ならば，

$$f(x) = x^n \left(a_0 + \frac{a_1}{x} + \cdots + \frac{a_{n-1}}{x^{n-1}} + \frac{a_n}{x^n}\right)$$

と書ける．$R := \max\limits_{1\leq k\leq n} \sqrt[k]{\dfrac{2n(|a_k|+1)}{|a_0|}}$ とおくと，$|x| > R$ ならば，

$$\left|\frac{a_1}{x} + \cdots + \frac{a_n}{x^n}\right| \leq \sum_{k=1}^{n} \left|\frac{a_k}{x^k}\right| < \sum_{k=1}^{n} |a_k| \frac{|a_0|}{2n(|a_k|+1)} \leq \sum_{k=1}^{n} \frac{|a_0|}{2n} = \frac{|a_0|}{2},$$

$$|f(x)| = |x|^n \left|a_0 + \frac{a_1}{x} + \cdots + \frac{a_n}{x^n}\right| \geq |x|^n \left(|a_0| - \left|\frac{a_1}{x} + \cdots + \frac{a_n}{x^n}\right|\right) > |x|^n \frac{|a_0|}{2}$$

が成り立つ．よって，$R' =: \max\left(R, \sqrt[k]{2|f(0)|/|a_0|}\right)$ とおくと，$|x| > R'$ ならば，

$$|f(x)| > |x|^n \frac{|a_0|}{2} > |f(0)| \tag{1}$$

が成り立つ．複素変数の関数 $\varphi : \mathbb{C} \ni x \mapsto |f(x)| \in \mathbb{R}$ は，$\mathbb{C}$ 上連続であるから，compact 集合 $A := \{x | x \in \mathbb{C}, |x| \leq R'\}$ 上で最小値を持つ．(1) により，

$$|x| > R' \Longrightarrow |f(x)| > |f(0)| \geq \min A$$

であるから，$\min A$ は $\mathbb{C}$ 上での最小値である．

(ii) 一点 $\alpha \in \mathbb{C}$ において $f(\alpha) \neq 0$ ならば，$|f(\beta)| < |f(\alpha)|$ なる $\beta \in \mathbb{C}$ が存在する．

実際，$g(x) := f(x+\alpha)/f(\alpha)$ とすれば，$g(x)$ は n 次の多項式関数で，$g(0) = 1$ であるから，

$$g(x) = 1 + b_1x + b_2x^2 + \cdots + b_nx^n, \quad b_n \neq 0$$

と表される．

$m := \min\{k \in \mathbb{N} \mid b_k \neq 0\}$，$b_m := re^{i\theta}\ (r > 0,\ 0 \leq \theta < 2\pi)$ とし，$K := \max\limits_{m+1\leq k\leq n} |b_k|$ と置く．

$\rho := \min\left(\dfrac{1}{3}, \dfrac{r}{r+K+1}, \dfrac{1}{\sqrt[m]{3r}}, \dfrac{1}{\sqrt[m+1]{3(r+K)}}\right)$ なる $\rho > 0$ をとれば，

$$\rho \leq \frac{1}{\sqrt[m]{3r}} < \frac{1}{\sqrt[m]{r}} \implies 1 - r\rho^m > 0,$$

$$\rho \le \frac{r}{r+K+1} < \frac{r}{r+K} \implies 0 < (1-\rho)r - K\rho \implies 0 < r\rho^m - \frac{K\rho^{m+1}}{1-\rho},$$

$$\rho + r\rho^m - (r+K)\rho^{m+1} < \rho + r\rho^m + (r+K)\rho^{m+1} \le \frac{1}{3} + r\frac{1}{3r} + (r+K)\frac{1}{3(r+K)} = 1$$
$$\implies (1-\rho)r\rho^m - K\rho^{m+1} < 1-\rho \implies r\rho^m - \frac{K\rho^{m+1}}{1-\rho} < 1$$

すなわち,

$$1 - r\rho^m > 0, \quad 0 < r\rho^m - \frac{K\rho^{m+1}}{1-\rho} < 1$$

が成り立つ．ここで，$\gamma := \rho e^{\frac{\pi-\theta}{m}i}$ と置けば，$b_m\gamma^m = -r\rho^m$ となり,

$$\begin{aligned} |g(\gamma)| &\le |1 - r\rho^m| + |b_{m+1}||\gamma|^{m+1} + \cdots + |b_n||\gamma|^n \le |1 - r\rho^m| + K(\rho^{m+1} + \cdots + \rho^n) \\ &\le 1 - r\rho^m + \frac{K\rho^{m+1}}{1-\rho} < 1 \end{aligned}$$

が成り立つ．$\beta := \gamma + \alpha$ とすれば $|f(\beta)| < |f(\alpha)|$ となる．

(iii)　$|f(x)|$ の最小値は 0 である．

$f(\alpha) := \min_{x\in\mathbb{C}} |f(x)|$ とする．$f(\alpha) \neq 0$ ならば，$\exists\beta \in \mathbb{C}$ s.t. $|f(\beta)| < |f(\alpha)|$　(by (ii))．これは $|f(\alpha)|$ が最小値であることに反する．よって，$|f(\alpha)| = 0$ すなわち $f(\alpha) = 0$ でなければならない．

証明終.

系 2. $\deg f = n \ge 1$ なる $\forall f \in \mathbb{C}[X]$ は $\mathbb{C}[X]$ において一次式の積に分解される：

$$f(X) = a_0(X - \alpha_1)(X - \alpha_2)\cdots(X - \alpha_n). \tag{2}$$

証明:　$f(X) = 0$ の一つの根を α_1 とすれば，剰余定理により，$f(X)$ は $X - \alpha_1$ で割り切れる:

$$f(X) = (X - \alpha_1)f_1(X).$$

f_1 は $n-1$ 次多項式である．この操作を続ければ (2) に達する．

証明終.

α が $f(X) = 0$ の根であるとき，分解 (2) に現れる因数 $X - \alpha$ の個数を，根 α の重複度と言う．重複度 1 の根を単根，重複度 k の根を k 重根と言う．

次は系 2 と同値である．

系 3. n 次代数方程式は，重複度を込めてちょうど n 個の根を持つ.

線型代数学では，行列を $\mathbb{R}$ 上で考えるよりも，$\mathbb{C}$ 上で考えたほうが色々と上手くいく．それは，系 3 によって，任意の n 次正方行列の固有多項式が $\mathbb{C}$ に重複度を込めてちょうど n 個の零点を持つ，すなわち，任意の n 次正方行列は，重複度を込めてちょうど n 個の固有値を持つということからわかる．固有値が存在するというのは非常に有意義なことで，これにより，固有ベクトルが必ず存在し，Jordan の標準形などの理論にも大きく貢献することとなる．

実数 $\mathbb{R}$ 上の多項式が必ずしも $\mathbb{R}$ に零点を持たないことは容易にわかるであろう．実際，2 次方程式 $ax^2 + bx + c = 0$ $(a, b, c \in \mathbb{R}, a \neq 0)$ の良く知られた次の公式がある．

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

この公式において，$b^2 - 4ac < 0$ ならば，$x \notin \mathbb{R}$ である．この公式は私の頃の教育課程では中学 3 年生で習うものである．ここで，平方根の中身が負にしてもいいのではないか？と思う生徒もいるはずである．しかし，現行の教育課程では，数学 B の「複素数」を習うことなく高校を卒業する人も居る．これは実に残念なことに思われる．

最後に，代数学の基本定理の証明に使った Euler の公式を補足として挙げておく．$\theta \in \mathbb{R}$ として，

$$e^{i\theta} = \cos\theta + i\sin\theta.$$