§9. 代入操作と因数定理

多項式 $a_0 + a_1X + \cdots + a_nX^n$ は「式」であるが、不定元 X のところに数 α を当てはめると、数 $a_0 + a_1\alpha + \cdots + a_n\alpha^n$ が得られる。特に、$a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$ となる数 α をその多項式の根という。この節では、多項式の代入操作から得られる諸結果を学ぶ。

● 9-1：代入

$\mathbb{K}'$ を $\mathbb{K} \subset \mathbb{K}'$ を満たす体とする。$\mathbb{K}' = \mathbb{K}$ の場合も含まれるが、$\mathbb{K}'$ としては、$\mathbb{K} = \mathbb{R}$ のとき $\mathbb{K}' = \mathbb{C}$ や $\mathbb{K} = \mathbb{Q}$ のとき $\mathbb{K}' = \mathbb{Q}(\sqrt{2})$ などを想定するとわかりやすい。このとき、多項式 $f = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{K}[X]$ と $\alpha \in \mathbb{K}'$ から、$\mathbb{K}'$ の元

$$f(\alpha) := a_0 + a_1\alpha + \cdots + a_n\alpha^n$$

を作ることを f に α を**代入する** (substitute) という。

例 9-1-1 $\mathbb{K} = \mathbb{R}$, $\mathbb{K}' = \mathbb{C}$ のときを考える。実数係数の多項式 $f(X) = X^2 - 3X - 2 \in \mathbb{R}[X]$ に複素数 $\alpha = 1 + i$ を代入すると、複素数

$$f(1+i) = (1+i)^2 - 3(1+i) - 2 = -i - 5$$

が得られる。 □

例 9-1-2 $\mathbb{C}[X]$ において、X^n を $X - i$ で割ったときの商 q と剰余 r を求めよう。定義より、

$$X^n = q(X - i) + r \quad (0 \leq \deg r < 1, \quad または \quad r = 0) \tag{9-1 a}$$

と書ける。r が 0 であると仮定すると矛盾がおきるから、r は 0 でない定数である。(9-1 a) の両辺に $X = i$ を代入することにより、$r = i^n$ とわかる。すると、

$$q(X - i) = X^n - i^n = (X - i)(X^{n-1} + iX^{n-2} + i^2X^{n-3} + \cdots + i^{n-1})$$

と書くことができ、$\mathbb{C}[X]$ において簡約法則が成り立つから、

$$q = X^{n-1} + iX^{n-2} + i^2X^{n-3} + \cdots i^{n-2}X + i^{n-1}$$

とわかる。 □

$\alpha \in \mathbb{K}'$ を代入する操作を表わす写像

$$\varphi_\alpha : \mathbb{K}[X] \longrightarrow \mathbb{K}', \quad \varphi_\alpha(f) = f(\alpha) \quad (f \in \mathbb{K}[X])$$

は次の性質を持っている：任意の $f, g \in \mathbb{K}[X]$ について、

(i) $\varphi_\alpha(f + g) = \varphi_\alpha(f) + \varphi_\alpha(g)$　　(ii) $\varphi_\alpha(fg) = \varphi_\alpha(f)\varphi_\alpha(g)$　　(iii) $\varphi_\alpha(1) = 1$

多項式 $f \in \mathbb{K}[X]$ に対して $f(\alpha) = 0$ となる $\alpha \in \mathbb{K}'$ を f の $\mathbb{K}'$ における **根**（こん）(root) という。

例 9-1-3 有理数係数の多項式 $f(X) = X^2 - 2 \in \mathbb{Q}[X]$ を考える。このとき、$f(\alpha) = 0$ となる有理数 α は存在しないので、$f(X) = X^2 - 2$ は $\mathbb{Q}$ において根を持たない。しかし、$f(\pm\sqrt{2}) = 0$ なので、$f(X)$ は $\mathbb{R}$ において根 $\pm\sqrt{2}$ を持つ。 □

例 9-1-4 $\alpha \in \mathbb{C}$ が多項式 $f \in \mathbb{R}[X]$ の根ならば、共役複素数 $\bar{\alpha}$ も f の根である。

(証明)

$f = a_0 + a_1X + \cdots + a_nX^n$ $(a_0, a_1, \ldots, a_n \in \mathbb{R})$ とおくと、仮定より $f(\alpha) = 0$ である：

$$0 = f(\alpha) = a_0 + a_1\alpha + \cdots + a_n\alpha^n.$$

両辺の複素共役をとると、

$$\begin{aligned} 0 = \overline{0} &= \overline{a_0 + a_1\alpha + \cdots + a_n\alpha^n} \\ &= \overline{a_0} + \overline{a_1}\,\overline{\alpha} + \cdots + \overline{a_n}\,\overline{\alpha^n} \\ &= a_0 + a_1\overline{\alpha} + \cdots + a_n(\overline{\alpha})^n \quad (\because a_i \in \mathbb{R}\ (i = 0, 1, \ldots, n)) \end{aligned}$$

となる。これは $f(\overline{\alpha}) = 0$ であることを意味する。 □

● 9 - 2 : 因数定理

次の補題 (因数定理) は、定数でない多項式 $f \in \mathbb{K}[X]$ が $\mathbb{K}$ 内に根 α を持てば、f は $\mathbb{K}[X]$ において $X - \alpha$ で割り切れるということを主張している。

補題 9 - 2 - 1 (因数定理)
$\deg f \geq 1$ の多項式 $f(X) \in \mathbb{K}[X]$ と $\alpha \in \mathbb{K}$ について、$f(\alpha) = 0$ ならば、$f(X) = (X-\alpha)q(X)$ を満たす $q(X) \in \mathbb{K}[X]$ が存在する。

(証明)

除法の定理より、$f(X) = (X - \alpha)q(X) + r$ を満たす $q(X) \in \mathbb{K}[X]$ と $r \in \mathbb{K}$ が存在する。$f(\alpha) = 0$ であるから、$r = 0$ とわかる。 □

例 9 - 2 - 2 $f(X) = 2X^3 + 2X^2 - X - 1 \in \mathbb{Q}[X]$ に対して $f(-1) = 0$ となるから、$f(X)$ は $X + 1$ で割り切れる。実際、割り算を実行すると、$f(X) = (X + 1)(2X^2 - 1)$ であることがわかる。よって、$f(X)$ は $\mathbb{R}[X]$ において $f(X) = (X + 1)(\sqrt{2}X + 1)(\sqrt{2}X - 1)$ のように 1 次式の積に分解される。 □

1 次多項式 $f = aX + b \in \mathbb{K}[X]$ $(a \neq 0)$ は $X = -ba^{-1}$ を唯一の根に持つ。では、2 次方程式 $f = aX^2 + bX + c \in \mathbb{K}[X]$ $(a \neq 0)$ の場合はどうであろうか。$\mathbb{K} = \mathbb{R}$ の場合、判別式により、$D = b^2 - 4ac$ の値が 0 以上なら解の公式から f は $\mathbb{R}[X]$ において重解を込みで 2 個の解を持つことがわかる。因数定理の応用として、より一般に次がわかる。

系 9 - 2 - 3
自然数 n に対して、n 次多項式 $f \in \mathbb{K}[X]$ の $\mathbb{K}$ における根の個数は重複解を込みで n 個以下である。

(証明)

n に関する数学的帰納法で証明する。

I. $n = 1$ のとき、f は $f = a + bX$ $(a, b \in \mathbb{K},\ b \neq 0)$ の形をしている。$b \neq 0$ より、f は $\mathbb{K}$ において唯一の根 $\alpha = -\frac{a}{b}$ を持つ。よって、1 次多項式について系の主張が成り立つ。

II. $n \in \mathbb{N}$ とし、$\mathbb{K}$-係数の任意の n 次多項式の $\mathbb{K}$ における根の個数は重複解を込みで n 個以下であると仮定する。

$f \in \mathbb{K}[X]$ を $(n + 1)$ 次多項式とする。

もし、f が $\mathbb{K}$ 内に根を持たないならば、f の $\mathbb{K}$ における根の個数は 0 個以下であり、系の主張は成立する。そこで、f が $\mathbb{K}$ 内に根を持つ場合を考える。α を f の $\mathbb{K}$ における根とする。すると、因数定理 ([定理 9-2-1]) により、f は

$$f = (X-\alpha)g \qquad (g \in \mathbb{K}[X])$$

と表わされる。[補題 7-6-1] により $\deg g = n$ であるから、g に対して帰納法の仮定を適用して、g の $\mathbb{K}$ における根の個数は重複解を込みで n 個以下であることがわかる。

$\beta \in \mathbb{K}$ を f の根とすると、

$$0 = f(\beta) = (\beta-\alpha)g(\beta)$$

となるので、$\beta-\alpha = 0$ または $g(\beta) = 0$ でなければならない。つまり、f の $\mathbb{K}$ における根は α かまたは g の $\mathbb{K}$ における根のいずれかでなければならない。これは、f の $\mathbb{K}$ における根の個数は $(n+1)$ 個以下であることを意味する。これで、任意の $(n+1)$ 次多項式についても $\mathbb{K}$ における根の個数は重複解を込みで $(n+1)$ 個以下であることがわかり、帰納法が完成した。 □

上の証明の途中で現れた考察は重要なので補題としてまとめておこう。

補題 9-2-4

$f(X) \in \mathbb{K}[X]$ を次数が 2 以上の多項式とし、$\alpha, \beta \in \mathbb{K}$ を相異なる 2 元とする。$f(\alpha) = f(\beta) = 0$ ならば、$f(X) = (X-\alpha)(X-\beta)q(X)$ を満たす多項式 $q(X) \in \mathbb{K}[X]$ が存在する。

(**証明**)

$f(\alpha) = 0$ より因数定理から $f = (X-\alpha)g$ となる $g \in \mathbb{K}[X]$ が存在する。$0 = f(\beta) = (\beta-\alpha)g(\beta)$ となるが、$\alpha \neq \beta$ なので $g(\beta) = 0$ であることがわかる。$\deg f \geq 2$ より $\deg g \geq 1$ であるから、因数定理より $g = (X-\beta)h$ となる $h \in \mathbb{K}[X]$ が存在する。結局、$f = (X-\alpha)(X-\beta)h$ $(h \in \mathbb{K}[X])$ のように表わされる。 □

[例 9-1-4] と [補題 9-2-4] を合わせて次が得られる。

例 9-2-5 次数が 2 以上の実係数多項式 $f(X)$ は $\alpha \in \mathbb{C} - \mathbb{R}$ を根に持つものとする。このとき、$f(X) = (X^2 - (\alpha+\overline{\alpha})X + \alpha\overline{\alpha})q(X)$ を満たす $q(X) \in \mathbb{R}[X]$ が存在する。

● 9-3：ラグランジュの補間式

[系 9-2-3] により、n 次式 $f, g \in \mathbb{K}[X]$ が $\mathbb{K}$ に属する相異なる $(n+1)$ 個の元 $\alpha_0, \alpha_1, \ldots, \alpha_n$ に対して、$f(\alpha_i) = g(\alpha_i)$ $(i = 0, 1, \ldots, n)$ を満たすならば、多項式として $f = g$ であることがわかる。つまり、n 次式は相異なる $(n+1)$ 個の値によって決まってしまう。$(n+1)$ 個の元 $\beta_0, \beta_1, \ldots, \beta_n \in \mathbb{K}$ が与えられたとき、$f(\alpha_i) = \beta_i$ $(i = 0, 1, \ldots, n)$ を満たす n 次以下の多項式 $f \in \mathbb{K}[X]$ は具体的に次の式で与えられる。この式を**ラグランジュの補間式** (Lagrange's interpolation polynomial) と呼ぶ。

$$f := \beta_0 \frac{f_0(X)}{f_0(\alpha_0)} + \beta_1 \frac{f_1(X)}{f_1(\alpha_1)} + \cdots + \beta_n \frac{f_n(X)}{f_n(\alpha_n)}.$$

但し、各 $i = 0, 1, \ldots, n$ に対して $f_i(X) \in \mathbb{K}[X]$ は $\prod_{j=0}^{n}(X-\alpha_j)$ から因子 $X-\alpha_i$ を削除して得られる n 次式 $f_i(X) = \frac{\prod_{j=0}^{n}(X-\alpha_j)}{X-\alpha_i}$ を表わす。

演習 9-1 3 次の実数係数多項式 f であって、$f(1)=1,\ f(2)=\sqrt{2},\ f(3)=\sqrt{3},\ f(4)=2$ を満たすものを求めよ。

● 9-4：代数学の基本定理

ここでは、$\mathbb{K}=\mathbb{C}$ (複素数体) に限定して考える。[系 9-2-3] は任意の体 $\mathbb{K}$ に対して成立するから、n 次多項式 $f \in \mathbb{C}[X]$ は $\mathbb{C}$ 内に重複解を込みで高々 n 個の根を持つ。実は、任意の n 次多項式 $f \in \mathbb{C}[X]$ は重複解を込みで n 個の解を持つ。この結果は、ガウスによって厳密な証明が与えられ、広く知られるようになった代数学の基本定理から導かれる。

定理 9-4-1 (代数学の基本定理)
$n \geq 1$ を整数とする。任意の複素数係数の n 次方程式

$$a_0 + a_1X + a_2X^2 + \cdots + a_nX^n = 0 \qquad (\text{但し、} a_n \neq 0,\ a_0, a_1, a_2, \ldots, a_n \text{ は複素数})$$

は必ず複素数内に解を持つ。

代数学の基本定理の証明にはいくつかの方法が知られている。そのいずれもかなりの準備を必要とし、ここで証明を与えることは出来ない。

注意 9-4-2 代数学の基本定理を使わなくても、2 次方程式 $aX^2+bX+c=0\ (a \neq 0)$ の解は「解の公式」を用いて、いつでも求めることができるから、2 次方程式は必ず $\mathbb{C}$ 内に解をもつ。3 次方程式や 4 次方程式に対しても複雑であるが、解の公式が存在するので、$n=3,4$ のときにも n 次方程式は必ず $\mathbb{C}$ に解をもつ。では、$n \geq 5$ に対してはどうであろうか。実は、与えられた 5 次方程式の解を、その係数を用いて求めることのできる一般的な公式、すなわち、「解の公式」を作ることができないことが証明されている。解を求めるための公式がない以上、解をどのように求めればよいのか (一般には) わからないのだが、代数学の基本定理は、どんな代数方程式も (複素数の中に) 解を持つことは真である、ということを主張している。

系 9-4-3
$n \geq 1$ を整数とする。任意の複素数係数の n 次方程式

$$a_0 + a_1X + a_2X^2 + \cdots + a_nX^n = 0 \qquad (\text{但し、} a_n \neq 0,\ a_0, a_1, a_2, \ldots, a_n \text{ は複素数})$$

は複素数の範囲内で

(9-4 a) $$f(X) = a_n(X-\alpha_1)(X-\alpha_2)\cdots(X-\alpha_n) \quad (\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{C})$$

のように一次式の積に分解される。

(証明)

$f(X)=a_0+a_1X+a_2X^2+\cdots+a_nX^n$ とおくと、代数学の基本定理から、$f(\alpha)=0$ となる $\alpha \in \mathbb{C}$ が存在する。したがって、$f(X)$ は $X-\alpha$ で割り切れる。よって、ある $(n-1)$ 次の複素数係数多項式 $g(X)$ を用いて $f(X)=(X-\alpha)g(X)$ と書ける。方程式 $g(X)=0$ に対して再び代数学の基本定理を適用すると、$g(\beta)=0$ となる $\beta \in \mathbb{C}$ が存在する。よって、ある $(n-2)$ 次の複素数係数多項式 $h(X)$ を用いて $g(X)=(X-\beta)h(X)$ と書ける。以下、これを繰り返していくことにより、$f(X)$ は (9-4 a) のように一次式の積に分解されることがわかる。 □

演習 9-2 3 次の複素係数多項式 X^3+aX^2+bX+c は α, β, γ を根に持つとする。このとき、$2\alpha, 2\beta, 2\gamma$ を根に持つ 3 次多項式を作れ。