§10. 多項式の既約分解

(有理) 整数環 $\mathbb{Z}$ と体係数の 1 変数多項式環 $\mathbb{K}[X]$ は、環として見たときにたくさんの共通点 (類似点) を持っている。体ではないけれどもどちらも簡約法則が成り立つ点はその一例である。2 以上の整数は素数の積に分解することができたが、類似のことは多項式に対しても成り立つ。ここでは、素因数分解の多項式版について説明する。

● 10 - 1 : 既約多項式

整数における素数に対応する多項式は既約多項式と呼ばれる。

定義 10 - 1 - 1

$f \in \mathbb{K}[X]$ を X を不定元とする $\mathbb{K}$-係数多項式とする。次の条件を満たすとき、f は $\mathbb{K}$ 上**既約** (irreducible) であると呼ばれる。

(IP1) $\deg f \geq 1$ (つまり、f は定数多項式ではない).

(IP2) $f = gh$ $(g, h \in \mathbb{K}[X]) \implies g \in \mathbb{K}$ or $h \in \mathbb{K}$.

例 10 - 1 - 2

(1) 1 次多項式 $X - a$ $(a \in \mathbb{K})$ は $\mathbb{K}$ 上既約である。実際、$X - a$ が $\mathbb{K}$ 上既約でないとすると、$\deg p \geq 1,\ \deg q \geq 1$ を満たす $p, q \in \mathbb{K}[X] - \{0_{\mathbb{K}}\}$ を用いて、$X - a = pq$ と書ける。

$$1 = \deg(X - a) = \deg(pq) = \deg p + \deg q$$

となる。よって、$\deg p,\ \deg q$ のうち、一方は 1 で、もう一方は 0 である。これは $\deg p \geq 1,\ \deg q \geq 1$ に矛盾する。よって、$X - a$ は $\mathbb{K}$ 上既約である。

(2) 代数学の基本定理により、$f \in \mathbb{C}[X]$ に対して次が成り立つ：

$$f \text{ が } \mathbb{C} \text{ 上既約} \iff \deg f = 1.$$

注意：(1) は多項式の係数環 $\mathbb{K}$ が体であることから言えることであり、一般の環では成り立たない。例えば、$R = \mathbb{Z}/6\mathbb{Z}$ 係数の多項式 $f = \bar{2}X + \bar{5},\ g = \bar{3}X + \bar{5}$ について、

$$fg = \bar{6}X^2 + \overline{25}X + \overline{25} = X + \bar{1}$$

となる。つまり、1 次式 $X + \bar{1}$ が 2 つの 1 次式の積に分解されてしまう。

命題 10 - 1 - 3

$f \in \mathbb{R}[X]$ が $\mathbb{R}$ 上既約ならば、$\deg f = 1$ または $\deg f = 2$ である。

(**証明**)

代数学の基本定理により、$f \in \mathbb{R}[X]$ は $\mathbb{C}[X]$ において 1 次式の積に分解される。そこで、

$$f = a(X - \alpha_1) \cdots (X - \alpha_n) \qquad (a \in \mathbb{R},\ \alpha_1, \ldots, \alpha_n \in \mathbb{C})$$

と書く。f は実数係数なので、$\alpha \in \mathbb{C}$ を根に持てば、その共役複素数 $\overline{\alpha}$ も根に持つ。したがって、適当に番号を付け替えることにより、$\alpha_1, \ldots, \alpha_n$ のうち、最初の $2k$ 個は虚数であって、$\alpha_2 = \overline{\alpha_1}, \ldots, \alpha_{2k} = \overline{\alpha_{2k-1}}$ を満たし、残りの $(n - 2k)$ 個 $\alpha_{2k+1}, \ldots, \alpha_n$ は実数であるとしてよい ($k = 0$ の場合もあり得る)。このとき、

$$f = a(X^2 - 2\mathrm{Re}(\alpha_1)X + |\alpha_1|^2) \cdots (X^2 - 2\mathrm{Re}(\alpha_{2k-1})X + |\alpha_{2k-1}|^2)(X - \alpha_{2k+1}) \cdots (X - \alpha_n)$$

と書くことができる。ここで、複素数 α の実部を $\mathrm{Re}(\alpha)$ で表わしている。上の等式は $\mathbb{R}[X]$ における因数分解である。したがって、f が $\mathbb{R}[X]$ が既約ならば、f は 1 次かまたは 2 次でなければならない。 □

$\mathbb{R}$ 上既約な 2 次の実数係数多項式は次のように決定される。

例 10 - 1 - 4 実数係数の 2 次多項式 X^2+aX+b $(a,b\in\mathbb{R})$ について、

$$X^2+aX+b \text{ が } \mathbb{R} \text{ 上既約} \iff a^2-4b<0$$

となる。実際、X^2+aX+b が $\mathbb{R}$ 上既約でないならば、X^2+aX+b は $\mathbb{R}[X]$ において 1 次式の積に分解する。例えば、$X^2+aX+b=(X-\alpha)(X-\beta)$ $(\alpha,\beta\in\mathbb{R})$ と書ける。このとき、$a=-(\alpha+\beta)$, $b=\alpha\beta$ であるから、

$$a^2-4b=(\alpha+\beta)^2-4\alpha\beta=(\alpha-\beta)^2\geq 0$$

となる。この対偶をとって、「$a^2-4b<0$ ならば X^2+aX+b が $\mathbb{R}$ 上既約」となることがわかる。逆に、$a^2-4b\geq 0$ のときには、2 次方程式の解の公式から

$$X^2+aX+b=\left(X-\frac{-b+\sqrt{a^2-4b}}{2}\right)\left(X-\frac{-b-\sqrt{a^2-4b}}{2}\right)$$

のように $\mathbb{R}[X]$ において 1 次式の積に分解するので、X^2+aX+b は $\mathbb{R}$ 上既約でない。 □

[命題 10 - 1 - 3] と [例 10 - 1 - 4] により、実数係数の定数でない任意の多項式は、$\mathbb{R}[X]$ において次の形をした既約多項式の積に分解されることがわかる：

$$a(X^2+a_1X+b_1)\cdots(X^2+a_kX+b_k)(X-c_1)\cdots(X-c_l). \tag{10 - 1 a}$$

但し、$a,a_i,b_i,c_j\in\mathbb{R}$ $(i=1,\ldots,k,\ j=1,\ldots,l)$ であり、$a_i^2-4b_i<0$ である。

演習 10-1* (1) 多項式 X^3-2 を $\mathbb{R}[X]$ において既約な多項式の積に分解せよ。
(2) 多項式 X^3-2 を $\mathbb{C}[X]$ において既約な多項式の積に分解せよ。

● 10 - 2 ： 3 次以下の既約多項式の決定

3 次以下の既約多項式は因数定理に基づく次の補題を用いて決定することができる。

補題 10 - 2 - 1

$f(X)\in\mathbb{K}[X]$ を 2 次または 3 次の多項式とする。このとき、

$$f(X) \text{ が } \mathbb{K} \text{ 上既約でない} \iff f(\alpha)=0 \text{ となる } \alpha\in\mathbb{K} \text{ が存在する}$$

(**証明**)

「$\Longleftarrow$」の証明：因数定理により、$f(X)=(X-\alpha)q(X)$ を満たす $q(X)\in\mathbb{K}[X]$ が存在する。$\deg f=2,3$ より $q(X)$ は定数ではない。よって、$f(X)$ は $\mathbb{K}$ 上既約でない。

「$\Longrightarrow$」の証明：$f(X)$ が $\mathbb{K}$ 上既約でないとすると、定数でない 2 つのある多項式 $g,h\in\mathbb{K}[X]$ の積に分解される：$f=gh$. $\deg f\leq 3$ より、$g,h\in\mathbb{K}[X]$ の少なくとも一方は 1 次式である。例えば、$\deg g=1$ であったとすると $g=aX+b$ $(a,b\in\mathbb{K},\ a\neq 0)$ と表わされる。このとき、$\alpha=-a^{-1}b\in\mathbb{K}$ とおくと $f(\alpha)=g(\alpha)h(\alpha)=0h(\alpha)=0$ となる。 □

例 10 - 2 - 2 $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ 係数の 3 次以下の既約多項式を決定しよう。$0 = [0]_2,\ 1 = [1]_2$ と略記する。

• $\mathbb{F}_2$ 係数の 1 次式は $X,\ X+1$ の 2 つだけであり、これらは [例 10 - 1 - 2(1)] により $\mathbb{F}_2$ 上既約である。

• $\mathbb{F}_2$ 係数の 2 次式は $X^2,\ X^2+1,\ X^2+X,\ X^2+X+1$ の 4 つである。このうち、X^2 と X^2+X は明らかに既約でない。$f_1(X) = X^2+1$ と $f_2(X) = X^2+X+1$ が $\mathbb{F}_2$ 上既約であるか否かを [補題 10 - 2 - 1] を用いて決定しよう。

$f_1(X) = X^2+1$ は、$f_1(1) = 0$ を満たすから、$X-1$ で割り切れる。実際、$f_1(X) = (X-1)^2$ と因数分解される。よって、$f_1(X)$ は $\mathbb{F}_2$ 上既約でない。一方、$f_2(X) = X^2+X+1$ については、$f_2(0) = 1 \neq 0,\ f_2(1) = 1 \neq 0$ であるから、$\mathbb{F}_2$ 上既約である。

• $\mathbb{F}_2$ 係数の 3 次式は $X^3 + aX^2 + bX + c\ (a,b,c \in \{0,1\})$ の形をしている。$c = 0$ なら既約でないから、既約なものは $X^3 + aX^2 + bX + 1\ (a,b \in \{0,1\})$ の形をしたものである。これを $f(X)$ とおくと $f(0) = 1 \neq 0,\ f(1) = a+b$ であるから、$f(X) = X^3 + aX^2 + bX + 1$ が既約になるのは $(a,b) = (1,0),(0,1)$ のときに限る。このようにして、$\mathbb{F}_2$ 上既約な 3 次式は X^3+X^2+1 と X^3+X+1 の 2 つであることがわかる。 □

演習 10-2 (1) $\mathbb{F}_5$ 上既約な $\mathbb{F}_5$ 係数の 2 次式であって、最高次係数が 1 で、かつ、定数項が 1 または 2 であるものをすべて求めよ。

(2) X^4+2 は $\mathbb{F}_5$ 上既約か否かを調べよ。

● 10 - 3 : 多項式の既約分解

2 以上の任意の整数は素数の積に順番を除いて一意的に表わすことができた。これと同じことが多項式に対しても成立する。2 以上の整数に相当するのが定数でない多項式であり、素数に相当するのが既約多項式である。

定理 10 - 3 - 1

$f \in \mathbb{K}[X]$ を次数が 1 以上の多項式とする。このとき、

$$f = p_1 \cdots p_k$$

となる既約多項式 $p_1, \ldots, p_k \in \mathbb{K}[X]$ が存在する。さらに、このような既約多項式 $p_1, \ldots, p_k$ は定数倍と順番を除いて一意的である。

この定理は、多項式の次数に関する数学的帰納法により、整数に対する素因数分解の存在と一意性の証明と同様にして証明することができるが、一意性を証明する際には、以下の [系 10 - 3 - 4] が必要になる。

命題 10 - 3 - 2

$p \in \mathbb{K}[X]$ が既約ならば、任意の多項式 $f \in \mathbb{K}[X]$ に対して $\gcd(f,p) = 1$ または $p|f$ が成り立つ。

(**証明**)

$d = \gcd(f,p)$ とおくと、$f = df_1,\ p = dp_1\ (f_1, p_1 \in \mathbb{K}[X])$ と書くことができる。p は既約であるから、$d \in \mathbb{K}$ または $p_1 \in \mathbb{K}$ となる。もし、$d \in \mathbb{K}$ ならば、最大公約数の定義から $d = 1$ である。$d \notin \mathbb{K}$ ならば、$p_1 \in \mathbb{K}$ である。p は既約なので $p \neq 0$. それゆえ、$p_1 \neq 0$ である。よって、$f = (pp_1^{-1})f_1 = p(p_1^{-1}f_1)$ と書けるので、$p|f$ とわかる。 □

系 10 - 3 - 3
$p \in \mathbb{K}[X]$ を既約多項式とする。多項式 $f, g \in \mathbb{K}[X]$ に対して次が成り立つ：

$$p|fg \implies p|f \text{ または } p|g.$$

(**証明**)

$p|fg$ より、$fg = pq$ $(q \in \mathbb{K}[X])$ と書くことができる。$p \nmid f$ であるとすると、[命題 10 - 3 - 2] より、$\gcd(f, p) = 1$ である。したがって、$af + bp = 1$ を満たす $a, b \in \mathbb{K}[X]$ が存在する。このとき、

$$g = (af + bp)g = afg + bpg = apq + bpg = p(aq + bg)$$

となる。これは $p|g$ を意味する。 □

上の結果を繰り返し用いて次が示される。

系 10 - 3 - 4
$p \in \mathbb{K}[X]$ を既約多項式とする。多項式 $f_1, \ldots, f_k \in \mathbb{K}[X]$ に対して次が成り立つ：

$$p|(f_1 \cdots f_k) \implies \exists\, i \in \{1, \ldots, k\} \text{ s.t. } p|f_i.$$

● 10 - 4 : アイゼンシュタインの既約判定法

前述のように、多項式が $\mathbb{C}$ 上既約か否か、$\mathbb{R}$ 上の既約か否かは簡単にわかるが、$\mathbb{Q}$ 上既約かどうかを判定することはやさしくないが、次の判定法が知られている。

定理 10 - 4 - 1 (アイゼンシュタインの既約判定法)
定数でない整数係数多項式 $f = a_0 + a_1X + \cdots + a_nX^n$ の係数はある素数 p に対して次の条件を満たしているとする：

$$p|a_i \ (0 \le i < n), \quad p \nmid a_n, \quad p^2 \nmid a_0.$$

このとき、f は $\mathbb{Q}$ 上既約である。

上の定理の証明は代数学や整数論の教科書を参照してほしい。上の定理を使うと、素数 p に対して $X^n - p$ は $\mathbb{Q}$ 上既約なことがわかる。したがって、いくらでも次数の高い $\mathbb{Q}$ 上既約な多項式が存在する。次の例もアイゼンシュタインの既約判定法を使って示される。

例 10 - 4 - 2 任意の素数 p に対して $f(X) = 1 + X + X^2 + \cdots + X^{p-1}$ は $\mathbb{Q}$ 上既約である。

このことを示すために、$f(X)$ における X に $1 + X$ を代入して得られる多項式 $g(X) := f(1 + X) \in \mathbb{Z}[X]$ を考える。$g(X)$ が $\mathbb{Q}$ 上既約であれば、$f(X)$ も $\mathbb{Q}$ 上既約になるので、$g(X)$ が $\mathbb{Q}$ 上既約となることをアイゼンシュタインの既約判定法を用いて示す。

$X^p - 1 = (X - 1)f(X)$ であるから、$(X + 1)^p - 1 = Xf(X + 1) = Xg(X)$ が成り立つ。

$$(X + 1)^p - 1 = \sum_{i=1}^{p} \binom{p}{i} X^i = X \sum_{i=1}^{p} \binom{p}{i} X^{i-1}$$

であるから、

$$g(X) = \sum_{i=1}^{p} \binom{p}{i} X^{i-1} = 1 + \binom{p}{1} X + \binom{p}{2} X^2 + \cdots + \binom{p}{p} X^{p-1}$$

と書けることがわかる。したがって、$g(X)$ は最高次以外の係数は p で割り切れ、定数項は p^2 では割り切れないことがわかる (p は素数であることに注意)。アイゼンシュタインの既約判定法により、$g(X)$ は $\mathbb{Q}$ 上既約である。 □