アイゼンシュタインの既約判定法

定義. 整数係数の多項式が**原始的**であるとは，全ての係数の最大公約数が 1 である時をいう．

定理. 原始的な整数係数の多項式

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \qquad (a_n \neq 0)$$

に対して，次の条件を満たす素数 p が存在する時，$f(x)$ は因数分解（下の注意を参照）できない．

- p は，a_n の約数でない．
- p は，a_i $(i = 0, 1, \cdots, n-1)$ の約数である．
- p^2 は，a_0 の約数でない．

注意. 上の定理において「因数分解できない」とは，正確には，「整数係数の多項式の積の形に変形できない」ということである．これは，整数係数の 1 変数多項式全体の中で $f(x)$ は「**既約**」ということなので，既約判定法という名前が付けられている．

例えば，2 次多項式 $f(x) = x^2 - 2x - 2$ は，$f(x) = (x - 1 + \sqrt{3})(x - 1 - \sqrt{3})$ というように，1 次式の積の形に変形することができるが，$x - 1 \pm \sqrt{3}$ は実数係数の 1 次式である．このような場合を，上では「因数分解できない」と呼んでいる．

下の証明では，次の記号を用いる．

- $p \mid a$ ： p は a の約数である．（a は p の倍数である．a は p で割れる．）
- $p \nmid a$ ： p は a の約数でない．（a は p の倍数でない．a は p で割れない．）

証明. $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ を整数係数の n 次式とし，定理の条件を満たす素数が p が存在するとする．さらに，2 つの $n-1$ 次以下の整数係数多項式

$$g(x) = b_s x^s + b_{s-1}x^{s-1} + \cdots + b_1 x + b_0 \quad , \quad h(x) = c_t x^t + c_{t-1}x^{t-1} + \cdots + c_1 x + c_0$$

が存在して，

$$f(x) = g(x)h(x)$$

が成り立つと仮定する（背理法）．$f(x)$ は原始的であるという仮定から，$s \neq 0$ かつ，$t \neq 0$ である．また，明らかに $s + t = n$ であるから，$s, t < n$ が成り立つ．

まず，定数項を比較することにより，$b_0 c_0 = a_0$ である．仮定から，$p \mid b_0 c_0$ であるが，$p^2 \nmid b_0 c_0$ なので $p \mid b_0$，$p \nmid c_0$ または，$p \nmid b_0$，$p \mid c_0$ である．記号の付け方を変えればどちらも同じなので，$p \mid b_0$，$p \nmid c_0$ を仮定する．次に x の係数を考えることにより，$b_0 c_1 + b_1 c_0 = a_1$ である．仮定より，$p \mid a_1$，$p \mid b_0$ なので，$p \mid b_1 c_0$ であるが，$p \nmid c_0$ を仮定しているので，$p \mid b_1$ である．

同様にして，$1 \leqq k \leqq s$ である k に対して，x^k の係数を比較することで，等式，

$$\sum_{i+j=k} b_i c_j = \sum_{i=0}^{k} b_i c_{k-i} = a_k$$

を得る．$b_0, b_1, \cdots b_{k-1}$ が全て p の倍数であるとすると，$p \mid a_k$，$p \mid b_k c_0$ であるが，$p \nmid c_0$ を仮定しているので，$p \mid b_k$ である．数学的帰納法により，$b_0, b_1, \cdots b_s$ が全て p の倍数であることがわかる．$g(x)$ の係数は全て p の倍数なので，ある s 次多項式 $g'(x)$ が存在して，$g(x) = pg'(x)$ と因数分解できる．したがって，$f(x) = g(x)h(x) = pg'(x)h(x)$ とかけるが，これは，$f(x)$ が原始的であるという仮定に矛盾である．よって結果が従う． □

例. 1. 多項式 $x^3+3x^2+6x+15$ が因数分解できないことを示せ.

(解) $p=3$ とすると，$p \mid 3$，$p \mid 6$，$p \mid 15$ であるが，$p \nmid 1$，$p^2 \nmid 15$ である．よって，アイゼンシュタインの既約判定法に必要な素数の存在が確認できた．したがって，与えられた多項式は因数分解できない.

2. p を素数とする．多項式 $x^{p-1}+x^{p-2}+\cdots+x+1$ が因数分解できないことを示せ.

(解) まず多項式 $f(x)$ と任意の整数 k に対して，明らかに次がなり立つ.

$$f(x) \text{ が因数分解できる.} \quad \Longleftrightarrow \quad f(x+k) \text{ が因数分解できる.}$$

よって，$f(x)=x^{p-1}+x^{p-2}+\cdots+x+1$ とおくと，$f(x+1)$ が因数分解できないことを示せば良い.

$$f(x)=\frac{x^p-1}{x-1}$$

なので，$f(x+1)$ は,

$$f(x+1)=\frac{(x+1)^p-1}{x}=\frac{1}{x}\left\{\sum_{k=0}^{p}\binom{p}{k}x^k-1\right\}=\sum_{k=1}^{p}\binom{p}{k}x^{k-1}$$

と計算できる．ここで，$\binom{p}{k}={}_pC_k=\dfrac{p!}{(p-k)!k!}$ は，二項係数である.

(i) x^{p-1} の係数は，$\binom{p}{p}=1$ であり，p で割れない.

(ii) $1 \leqq k \leqq p-1$ に対して，x^{k-1} の係数は，$\binom{p}{k}$ であり，p で割れる.（下の補題を参照）

(iii) 定数項は，$\binom{p}{1}=p$ であり，p^2 で割れない.

以上より，アイゼンシュタインの既約判定法から，主張が従う.

補題. $1 \leqq k \leqq p-1$ に対して，$\binom{p}{k}$ は，p で割れる.

証明. $\binom{p}{k}=\dfrac{p!}{(p-k)!k!}$ であった．明らかに，$p!$ は p で割れる．$1 \leqq k \leqq p-1$ という仮定から，$p-k<p$ かつ $k<p$ である．p は素数なので，$p \nmid (p-k)!$ かつ $p \nmid k!$ である．以上より，主張が従う. □

注意. 二項係数 $\binom{m}{n}={}_mC_n=\dfrac{m!}{(m-n)!n!}$ $(m \geqq n \geqq 0)$ は整数である．これは，$\binom{m}{n}$ の定義を ${}_mC_n$ とみると，コンビネーションの定義（m 個から n 個を選ぶ組み合わせの数）から明らかであるが，m に関数する数学的帰納法を用いて，次のようにも証明できる.
$m=1$ の時は，$\binom{1}{1}=\binom{1}{0}=1$ から成り立つ．$m=k$ の時，$k \geqq \ell \geqq 0$ である ℓ について，$\binom{k}{\ell}$ が全て整数であると仮定すると，二項係数の基本公式 $\binom{k+1}{\ell'}=\binom{k}{\ell'}+\binom{k}{\ell'-1}$ から，$k \geqq \ell' \geqq 1$ となる ℓ' に対して，$\binom{k+1}{\ell'}$ は整数である．最後に，$\binom{k+1}{k+1}=\binom{k+1}{0}=1$ は整数なので，$m=k+1$ の時も主張が成り立つ.