

多項式の既約性判定法

七条 彰紀

2017 年 9 月 6 日

定理 0.1 (Eisenstein's criterion)

$$f(x) = \sum_{0 \leq k \leq n} f_k x^k \in \mathbb{Z}[x]$$

について, ある素数 p が存在して, 整数 f_0, f_1, \dots, f_n が以下を満たすならば, $f(x)$ は $\mathbb{Q}[x]$ の既約元である.

1. $i \neq n$ の場合は f_i は p で割り切れる.
2. f_n は p で割り切れない.
3. f_0 は p^2 で割り切れない.

(証明). 多項式 g, h を $f(x) = g(x)h(x)$ を満たすものとおき, 多項式 f, g, h の各係数を

$$g(x) = \sum_{0 \leq i \leq n} g_i x^i, h(x) = \sum_{0 \leq j \leq n} h_j x^j$$

と置く. この時, 単純な計算で

$$f_k = \sum_{i+j=k} g_i h_j$$

が成り立つと分かる. 記法を簡単にするため, $P = (p) \subset \mathbb{Z}$ とおく. これが素イデアルであることを何度も使う.

■ $g_0 \in P, h_0 \notin P$. f_0 を考える.

$$f_0 = g_0 h_0$$

前提条件 1. より f_0 は p の倍数である. さらに前提条件 3. から, f_0 には素因数として p がただ一つ含まれる. その p は g_0 か h_0 のどちらか一方に含まれている. そこで前提条件に加えて (*) $g_0 \in P, h_0 \notin P$ を仮定する.

■ $g_0, g_1, \dots, g_{n-1} \in P$. 帰納法で $g_0, g_1, \dots, g_{n-1} \in P$ を示す. まず, $k = 1$ で示す.

$$f_1 = g_0 h_1 + g_1 h_0 \in P$$

P はイデアルだから $g_0 h_1 \in P, h_0 \notin P$. 特に P は素イデアルだから $g_1 \in P$. 次に, $0 \leq N+1 < n$ を満たす自然数 N について $g_0, g_1, \dots, g_N \in P$ が成り立つとする.

$$f_{N+1} = g_{N+1} h_0 + g_N h_1 + \sum_{1 \leq j \leq N+1} g_{N+1-j} h_j$$

そして前提条件 1. より $f_{N+1} \in P$ が成り立つ. 帰納法の仮定より, $g_N h_1, \sum_{2 \leq j \leq N+1} g_{N+1-j} h_j \in P$. 仮定 (*) より $h_0 \notin P$ だから $g_{N+1} \in P$.

■ $g_n \notin P$. さて、最後に f_n を考える.

$$f_n = g_n h_0 + \sum_{1 \leq j \leq n} g_{n-j} h_j$$

前提条件 2. より $f_n \notin P$. すでに示したとおり, $g_0, g_1, \dots, g_{n-1} \in P$ が成り立つ. したがって, 仮定 (*) と合わせて $g_n \notin P$ が成立する.

■ 結論: $\deg g = n$. $0 \in P$ だから, このことから $g_n \neq 0$. よって $\deg g = n, \deg h = n - n = 0$. これで f の既約性が示された. ■

これと命題を組み合わせると, 多くの多項式の既約性が示せる.

命題 0.2

多項式 $f(x) \in \mathbb{Z}[x]$ と任意の定数 a について, 「 $f(x+a)$ が既約」と「 $f(x)$ が既約」は同値.

(証明). $f(x)$ が既約だとする. 定数 a に対し, 1 次以上の多項式 g, h (これは a によって変化する) が存在して $f(x+a) = g(x)h(x)$ が成り立つ ($f(x+a)$ が既約でない) ならば, $f(x) = g(x-a)h(x-a)$ となり, $g(x-a), h(x-a)$ は 1 次以上の多項式. これは前提に矛盾. よって $f(x+a)$ も既約.

$f(x)$ が既約でないとする. すると 1 次以上の多項式 g, h が存在して $f(x) = g(x)h(x)$ が成り立つが, $f(x+a) = g(x+a)h(x+a)$ となり, $g(x+a), h(x+a)$ は 1 次以上の多項式. よって $f(x+a)$ も既約でない. ■

次は有限体への還元を用いた判定法である.

定理 0.3 (Reduction Criterion in S.Lang “Algebra”)

A, B を整域とし, $\phi: A \rightarrow B$ を準同型とする. さらに B の商体を L としておく. $f \in A[x]$ について以下が成り立つとき, f は $A[x]$ の既約元^{†1}である.

1. $\phi(f) \neq 0$.
2. $\deg \phi(f) = \deg f$.
3. $\phi(f)$ は $L[x]$ の既約多項式.

(証明). $f = gh$ ($g, h \in A[x]$) と分解できたとすると, $\phi(f) = \phi(g)\phi(h)$ となる. 前提条件 3. より $\deg \phi(g)$ or $\deg \phi(h) = \deg \phi(f)$ であり, かつ $\deg \phi(g) \leq \deg g, \deg \phi(h) \leq \deg h$. これらと前提条件 2. より $\deg g$ or $\deg h = \deg \phi(f) = \deg f$. 以上で主張が示せた. ■

系 0.4

\mathbb{F}_q を位数 q の有限体とし, 以下の準同型を定める.

$$\rho_q: \mathbb{Z}[x] \rightarrow \mathbb{F}_q[x]; \quad ax^n \mapsto (a \bmod q)x^n.$$

$f \in \mathbb{Q}[x]$ に適当に $d \in \mathbb{Z}^\times$ を掛けて $df \in \mathbb{Z}[x]$ とする. ある q について, $\rho_q(df)$ が既約ならば f は既約である.

^{†1} すなわち, $f = gh$ かつ $\deg g, \deg h > 1$ であるような $g, h \in A[x]$ が存在しない.

例 0.5

$n \in \mathbb{Z}^\times, f = x^3 - nx^2 + (n-3)x + 1 \in \mathbb{Z}[x]$ とする. $\rho_2(f) = x^3 + nx^2 + (n+1)x + 1$ であり, これが一次以上の因子を持つならば, そのうち少なくとも一つは 1 次式である. しかし $\rho_2(f)(0) = 1, \rho_2(f)(1) = 1$ だから $\rho_2(f)$ は 1 次式で割り切れない. これは矛盾であるから, $\rho_2(f)$ は $\mathbb{F}_2[x]$ の既約多項式である. そして系から, f は $\mathbb{Q}[x]$ の既約多項式である.

次もまた別の判定法である.

定理 0.6 (Cohn's Criterion)

$b \in \mathbb{Z}_{\geq 2}$ と $p(x) = a_k x^k + a_{k-1} x^{k-1} + \cdots + a_1 x + a_0$ は $0 \leq a_i \leq b-1$ を満たすとする. $p(b)$ が素数ならば, $p(x)$ は $\mathbb{Z}[x]$ の既約元である.

証明は難しい. 詳細は https://www.wikiwand.com/en/Cohn's_irreducibility_criterion を参照のこと.