ガウスの補題からアイゼンシュタインの既約判定法

定義 1 $f(x) \in \mathbb{Z}[x]$ とする[*1].

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

とするとき，$(a_0, a_1, a_2, \cdots, a_n) = 1$ である場合，$f(x)$ を**原始的 (primitive)** と呼ぶ.

定理 1 （**ガウスの補題**）$f(x), g(x)$ が原始的であれば $f(x)g(x)$ も原始的である.

［証明］$f(x), g(x)$ が原始的で，$f(x)g(x)$ が原始的でないと仮定すると，原始的な多項式 $h(x) \in \mathbb{Z}[x]$ と，0 や ± 1 でない整数 d を用いて

$$f(x)g(x) = dh(x)$$

と書ける．d の素因数の一つを p とし，

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

$$g(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_n x^n$$

とすると，$f(x)$ は原始的なので $a_0, a_1, a_2, \cdots, a_n$ のうち少なくとも一つは p の倍数ではない．また $b_0, b_1, b_2, \cdots, b_n$ についても同様である．$f(x)$ の各項の係数を a_0 から順に見て最初の p の倍数でない係数を a_k とする．同様に $g(x)$ の各項の係数を b_0 から順に見て最初の p の倍数でない係数を b_j とする．つまり a_k, b_j より前の係数は全て p で割り切れる．$f(x)g(x)$ を展開したときの x^{k+j} の係数は

$$a_0 b_{k+j} + a_1 b_{k+j-1} + a_2 b_{k+j-2} + \cdots + a_{k-1} b_{k+1} + \underline{a_k b_j} + a_{k+1} b_{j-1} + \cdots + a_{k+j-2} b_2 + a_{k+j-1} b_1 + a_{k+j} b_0$$

これらのうち $a_k b_j$（アンダーラインの部分）以外は全て p の倍数であるが，$a_k b_j$ は p の倍数でないのでこの x^{k+j} の係数は p の倍数でない．一方 $dh(x)$ の各項の係数は全て p で割り切れるので矛盾をきたす．よって $f(x), g(x)$ が原始的であれば $f(x)g(x)$ も原始的である．［証明おわり］

定理 2 原始多項式 $f(x) \in \mathbb{Z}[x]$ が $\mathbb{Q}[x]$ で可約ならば $\mathbb{Z}[x]$ でも可約である.

［証明］対偶「原始多項式 $f(x) \in \mathbb{Z}[x]$ が $\mathbb{Z}[x]$ で既約ならば $\mathbb{Q}[x]$ でも既約である.」を証明する.
$\mathbb{Z}[x]$ で既約な原始多項式 $f(x) \in \mathbb{Z}[x]$ が $\mathbb{Q}[x]$ で <u>可約</u> であると仮定すると,

$$f(x) = g(x)h(x) \qquad (g(x), h(x) \in \mathbb{Q}[x])$$

と因数分解できる.

$$g(x) = g_0 + g_1 x + g_2 x^2 + \cdots + g_n x^n$$

$$h(x) = h_0 + h_1 x + h_2 x^2 + \cdots + h_n x^n$$

$$(g_0, g_1, g_2, \cdots, g_n, h_0, h_1, h_2, \cdots, h_n \in \mathbb{Q})$$

とする．$g_0, g_1, g_2, \cdots, g_n$ を通分し共通分母を p. 通分した後の分子の最大公約数を c, 同様に $h_0, h_1, h_2, \cdots, h_n$ を通分し共通分母を q, 通分した後の分子の最大公約数を d とする．また $\dfrac{cd}{pq}$ を約分して既約分数 $\dfrac{A}{B}$ とすると,

[*1] 多項式全体の集合を，その係数の範囲によって $\mathbb{Z}[x], \mathbb{Q}[x], \mathbb{R}[x], \mathbb{C}[x]$ などと表す.

$$f(x) = \frac{A}{B}G(x)H(x) \qquad (\text{ただし } G(x), H(x) \in \mathbb{Z}[x] \text{ で原始的.})$$

と表せる．$G(x)H(x) = F(x)$ とすると，ガウスの補題により $F(x)$ も原始的である．つまり $F(x)$（展開した多項式）の各係数は公約数（1 以外）を持たず，$B \neq 1$ で約分できない．しかし左辺すなわち $f(x)$ は整数係数なので $p = 1$ である．

$$\therefore f(x) = AG(x)H(x)$$

$f(x)$ は原始的なので $A = 1$．つまり

$$f(x) = G(H)H(x)$$

と整数係数で因数分解できて仮定と矛盾した．よってこの定理は証明された．［証明おわり］

この定理の逆「原始多項式 $f(x) \in \mathbb{Z}[x]$ が $\mathbb{Z}[x]$ で可約ならば $\mathbb{Q}[x]$ でも可約である．」は当然真なので結局のところ，「原始多項式 $f(x) \in \mathbb{Z}[x]$ が $\mathbb{Z}[x]$ で可約であることと $\mathbb{Q}[x]$ で可約であることは同値である．」さらに必ずしも原始的であることは必要ではない．

定理 3 （アイゼンシュタインの既約判定法）$f(x) \in \mathbb{Z}[x]$ が

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$$

と表せるとする．ある素数 p が a_0〜a_{n-1} の全てを割り切り，a_n を割り切らない．また p^2 が a_0 を割り切らないとき $f(x)$ は $\mathbb{Q}[x]$ で既約である．

［証明］$f(x)$ が $\mathbb{Z}[x]$ で 可約 であると仮定すると，

$$f(x) = g(x)h(x) \qquad (g(x), h(x) \in \mathbb{Z}[x])$$

と因数分解できる．

$$\begin{aligned} g(x) &= g_0 + g_1x + g_2x^2 + \cdots + g_mx^m \\ h(x) &= h_0 + h_1x + h_2x^2 + \cdots + h_{n-m}x^{n-m}(1 \leq m \leq n-1) \end{aligned}$$

とすると，

$$a_0 = g_0h_0, a_1 = g_0h_1 + g_1h_0, a_2 = g_0h_2 + g_1h_1 + g_2h_0, \cdots, a_n = g_mh_{n-m}$$

a_0 は p で割り切れて p^2 で割り切れないので g_0, h_0 のうちのどちらかが p で割り切れない．どちらが p で割り切れないとしても差し支えないので，g_0 が p で割り切れて，h_0 が p で割り切れないとする．a_n は p で割り切れないので g_m も p で割り切れない．つまり g_0〜g_m の全てが p で割り切れるということは無い．g_0 の方から順に見て行って，最初に p で割り切れない係数を $g_k(1 \leq k \leq m)$ とすると，

$$a_k = g_0h_k + g_1h_{k-1} + g_2h_{k-2} + \cdots + g_kh_0$$

上式の最後の項 g_kh_0 は p で割り切れず，それ以外は全て p で割り切れる．よって a_k は p で割り切れない．つまり a_1〜a_{n-1} のうちで p で割り切れないものがあることになり，矛盾をきたす．よって $f(x)$ は $\mathbb{Q}[x]$ で既約で，前定理より $\mathbb{Q}[x]$ でも既約である．［証明おわり］

定理 4 素数 p について

$$f(x) = x^{p-1} + x^{p-2} + x^{p-3} + \cdots + 1 = \frac{x^p - 1}{x - 1}$$

は $\mathbb{Q}[x]$ 上既約な多項式である．

［証明］変数を 1 だけずらし $g(x) = f(x+1)$ とすると，

$$g(x) = \frac{(x+1)^{p-1}}{x} = x^p +_p \mathrm{C}_1 x^{p-2} +_p \mathrm{C}_2 x^{p-3} + \cdots {}_p\mathrm{C}_{p-1}$$

${}_p\mathrm{C}_1$〜${}_p\mathrm{C}_{p-1}$ は p で割り切れ，${}_p\mathrm{C}_{p-1} = p$ は p^2 の倍数ではないので，アイゼンシュタインの既約判定法より $g(x)$ は既約である．よって $f(x)$ も既約である． ［証明おわり］

補題 1 素数 p について，${}_p\mathrm{C}_r (1 \leq r \leq p-1)$ は p の倍数である．

［証明］

$${}_p\mathrm{C}_r = \frac{p!}{r!(p-r)!}$$

$r < p, p-r < p$ より分母に因数 p を持ち得ない．よって分子の p を約分により消すことはできないので，結果 p の倍数である． ［証明おわり］

補題 2 $f(x)$ が既約ならば $f(x+1)$ も既約である．

［証明］$f(x+1) = g(x)h(x)$ とすると，$f(x) = g(x-1)h(x-1)$ となり $f(x)$ が可約となってしまい矛盾する． ［証明おわり］

参考文献

[1] 草場公邦『ガロワと方程式』（朝倉書店，すうがくブックス 7，1991 年）
[2] 上野健爾『代数入門 1』（岩波書店，岩波講座 現代数学への入門 7，1995 年）