一意分解整域とその商体における Eisenstein の既約判定法

石井 大海（@mr_konn）

2018-12-15

1 はじめに

$\mathbb{Q}[X]$ や $\mathbb{Z}[X]$ の既約元を判定する方法として，次の **Eisenstein の既約判定法**は広く知られています：

定理 1 (Eisenstein の既約判定法《整数・有理係数版》). $\mathbb{Z}$-係数の一変数多項式 $f(X) = a_n X^n + \cdots + a_1 X + a_0 \in \mathbb{Z}[X]$ について，次を満たす素数 p が存在するとする：

(1) $p \nmid a_n$
(2) $p \mid a_j \quad (j = 0, \ldots, n-1)$
(3) $p^2 \nmid a_0$

この時，$f(X)$ は $\mathbb{Z}$ および $\mathbb{Q}$ 上既約である．

実は，Eisenstein の既約判定法は，係数環が一般の UFD やその商体の場合にも使うことが出来ます[*1)]．これにより，多変数多項式の既約性を簡単に判定することが出来る場合があります．

2 UFD 版の証明と応用例

Def. 2 (一意分解整域；UFD).

- $u \in D$ が**単元** $\overset{\text{def}}{\iff}$ ある $i \in D$ があって $ui = 1$ となる．
- D の単元全体を $D^\times$ と書く．
- $d \in D$ が**既約元** $\overset{\text{def}}{\iff}$ d は単元や零元ではなく，もし $d = pq$ と書けるなら $p \in D^\times$ または $q \in D^\times$
- 整域 D が**一意分解整域** (*unique factorization domain, UFD*) である
  $\overset{\text{def}}{\iff}$ 任意の $x \in D$ について，x が単元でも零元でもないなら，既約元 $p_1, \ldots, p_n$ が存在して，$x = p_1 \ldots p_n$ の形に単元倍の差を除いて一意に書ける．

[*1)] この事実は 2013 年度のゼミで教えて貰いました．後半の同型による判定法はゼミ同期の広川くんの方法を参考にしました．

補題 3. D を整域とする．$Q(D)$ を D の商体とする時，$f \in D[X]$ が $Q(D)[X]$ の元として既約 $\Leftrightarrow$ $D[X]$ の元として既約

定理 4 (Eisenstein の既約判定法). R を UFD とし，$f(X) = a_n X^n + \cdots + a_1 X + a_0 \in R[X]$ とする．次を満たすような R の既約元 $p \in R$ が存在するとする：

(1) $p \nmid a_n$
(2) $p \mid a_j \quad (j = 0, \ldots, n-1)$
(3) $p^2 \nmid a_0$

この時，$f(X)$ は R および $Q(R)$ 上既約である．

Proof. 補題より f が R 上既約であれば $Q(R)$ 上でも既約となるので，R 上既約であることを示せば十分である．

そこで，f が R 上可約であるとして矛盾を導く．$f = gh \quad (g, h \in R[X] \setminus R[X]^\times)$ とする．$g = b_m X^m + \cdots + b_0, h = c_{n-m} X^\ell + \ldots c_0$ とおこう．条件より $m < n$ でなくてはならない．このとき，$p \mid a_0 = b_0 c_0$ より既約元の基本性質から $p \mid b_0$ または $p \mid c_0$ の少なくとも一方が成立する．また，条件 3 より $p^2 \nmid b_0 c_0$ なので，b_0 か c_0 のどちらか一方のみが p で割り切れることがわかる．よって，$p \mid b_0$ としても一般性を失わない．以下，各 $k \leq m$ について $p \mid b_k$ を帰納法により示す．

$i < k$ について $p \mid b_i$ が成立するとする．$k \leq m < n$ なので，仮定から $a_k = b_k c_0 + b_{k-1} c_1 + \cdots + b_0 c_k$ は p で割り切れる．この時，帰納法の仮定により第二項目以降はすべて p で割り切れる．最初の仮定から $p \nmid c_0$ なので，$p \mid b_k$ でなくてはならない．よって帰納法により $k \leq m$ について $p \mid b_k$ が成立することがわかった．

さて，この時先頭項係数は $a_n = b_m c_{n-m}$ である．上の議論から $p \mid b_m$ であるので $p \mid a_n$ となるが，これは仮定に反する．よって f は R 上既約である．

これを応用して多変数多項式の既約判定をしてみよう．

簡単な例ではありますが，$f(x, y) = x^2 + 2y \in \mathbb{Q}[x, y]$ を考えてみましょう．これは $\mathbb{Q}[x, y] = (\mathbb{Q}[y])[x]$ と思えば，$\mathbb{Q}[y]$ は UFD ですから一般化 Eisenstein 判定法が使えそうです．そこで，$p = y$ とおいてみれば，$y \nmid 1, y \mid 2y, y^2 \nmid 2y$ なので前提条件を満たします．よって f は既約となります．

もうちょっと混み入った例を考えてみましょう．$g(x, y) = x^2 + xy + y^2 - 3x - 4y + 4$ を考えてみます．これは，$g(x, y) \in (\mathbb{Q}[y])[x]$ と見て降冪の順に並べてみると $g(x) = x^2 + (y-3)x + (y-2)^2$ となりますが，このままでは p は見付かりそうにありません．そこで，$h(y) \in \mathbb{Q}[y]$ として次の同型を考えてみます：

$$\begin{array}{rcl} (\mathbb{Q}[y])[x] & \to & (\mathbb{Q}[y])[x] \\ f(x) & \mapsto & f(x + h(y)) \end{array}$$

これは代入による準同型の特別な場合で，同型になることもすぐにわかります．同型は既約元を保ちますので，うまい変換を見付けてその後で既約判定法に持ち込めないか考えてみましょう．ここで，

$$g(x + h(y)) = x^2 + (y + 2h(y) - 3)x + y^2 + (h(y) - 4)y + (h(y)^2 - 3h(y) + 4)$$

です．二次以上ですと既約判定が大変になってくるので，$h(y) = t \in \mathbb{Q}$ の場合をまずは考えてみましょう．

$$g(x+t) = x^2 + (y+2t-3)x + y^2 + (t-4)y + (t^2 - 3t + 4)$$

Eisenstein 既約判定法を使いたいので，「定数項」$y^2 + (t-4)y + (t^2 - 3t + 4)$ が $(y + 2t - 3)$ で割り切れるように t を選べるか？ ということが問題になります．係数を比較すれば，$t = 1, \frac{1}{3}$ が t の候補になります．分数は面倒なので $t = 1$ の場合を考えてみると，

$$g(x+1) = x^2 + (y-1)x + (y-1)(y-2)$$

となります．よって，$p = y-1$ とおけば $y-1 \nmid 1, y-1 \mid y-1, y-1 \mid (y-1)(y-2)$ かつ $(y-1)^2 \nmid (y-1)(y-2)$ すので，Eisenstein の判定法より $g(x+1)$ は既約になります．よって，上の同型 $x \mapsto x+1$ によって元の $g(x) = g(x, y)$ も $\mathbb{Q}[x, y]$ で既約であることがわかりました．このように，文字を $\mathbb{Q}[x]$ の分だけ平行移動してやったり，$\mathbb{Q}[x]$ の単元倍してやったりしても元の多項式環と同型になることを使えば，2 変数以上の多項式の場合も既約判定を行うことが出来るようになります[*2)]．

[*2)] 勿論，あくまで十分条件でしかないので，これでも判定出来ない場合はあるかと思います．