既約多項式

$f \in R$ が単元ではない 2 つの元 $a, b \in R$ が存在し $f = ab$ とかけるとき、f を可約といい、そのような $a, b \in R$ が存在しないとき f を既約という。

例えば、単項式 $2x$ は $\mathbb{Z}[x]$ において $2x = 2 \times x$ であり、$2, x \in \mathbb{Z}[x]$ は単元ではない。つまり、$2 \times \alpha = 1$ や $x \times \beta = 1$ となる α, β は $\mathbb{Z}[x]$ に存在しない。その為、$2x$ は $\mathbb{Z}[x]$ において可約である。

同様に $2x \in \mathbb{Q}[x]$ は単元でない物の積に表せない。よって、$2x$ は $\mathbb{Q}[x]$ において既約である。

単元でないことが意味を持つのは次のような無限の表現を持つものを排除するためである。

$$2x \;=\; 2 \cdot 2^{-1} \cdot 2 \cdot x \;=\; 2 \cdot 2^{-1} \cdot 2 \cdot 2^{-1} \cdot 2x \;= \cdots \tag{1}$$

$f \in \mathbb{Z}[x]$ を以下のように定める。f が $\mathbb{Z}[x]$ と $\mathbb{Q}[x]$ それぞれにおいて既約であるか否か判定せよ。

1. $-x - 1$
2. $4x$
3. $2x^2 + 4$
4. $x^2 + 2x + 4$
5. $x^3 + 5x + 6$
6. $7x^3 + 10x^2 + 20$
7. $x^{13} - 1$
8. $\sum_{i=0}^{17} x^i$
9. $\sum_{i=13}^{22} x^i$
10. $187x^{80} - 306x^{39} + 204$

	$\mathbb{Z}[x]$	$\mathbb{Q}[x]$
$-x - 1$	既約	既約
$4x$	可約	既約
$2x^2 + 4$	可約	既約
$x^2 + 2x + 4$	既約	既約
$x^3 + 5x + 6$	可約	可約
$7x^3 + 10x^2 + 20$	既約	既約
$x^{13} - 1$	可約	可約
$\sum_{i=0}^{17} x^i$	可約	可約
$\sum_{i=13}^{22} x^i$	可約	可約
$187x^{80} - 306x^{39} + 204$	可約	既約

1. $-x - 1$

   $-x - 1$ は 1 次式である為、$-x - 1 = ab$ となる a, b があれば $\deg a = 0, \deg b = 1$ となる。$b = \alpha x + \beta$ とすれば $a\alpha = -1$ を満たすような a となるが、$a \times (-\alpha) = 1$ を満たす為に a は単元となる。

   よって、$-x - 1$ は $\mathbb{Z}[x]$ において既約である。

   $-x - 1$ は 1 次式である為 $\mathbb{Q}[x]$ においても既約である。

2. $4x$

   $4 \in \mathbb{Z}$ は単元ではないので、$4x = 4 \times x$ である為、$4x$ は $\mathbb{Z}[x]$ において可約である。

   $4x$ は 1 次式である為 $\mathbb{Q}[x]$ において既約である。

3. $2x^2 + 4$

   $2x^2 + 4 = 2(x^2 + 2)$ であるので、$2x^2 + 4$ は $\mathbb{Z}[x]$ において可約である。

   x^2+2 がある $f, g \in \mathbb{Q}[x]$ を用いて $x^2+2 = fg$ とかけたとする。$\deg f = \deg g = 1$ となる式があれば可約となる。

   最高次の項の係数が 1 である (モニック多項式) ので、$f = x + \alpha, g = x + \beta$ となる式を用いれば $x^2 + 2 = fg = (x + \alpha)(x + \beta) = x^2 + (\alpha + \beta)x + \alpha\beta$ である。つまり、α, β は $\alpha + \beta = 0, \alpha\beta = 2$ の 2 式を満たす。

   しかし、これを満たす有理数は存在しないので $x^2 + 2$ は $\mathbb{Q}[x]$ において既約である。これより、$2x^2 + 4$ も $\mathbb{Q}[x]$ において既約である。

4. $x^2 + 2x + 4$

   $x^2 + 2x + 4$ はモニック多項式であり、2 次式であるので $x^2 + 2x + 4 = fg$ となる多項式が $\deg f = 0, \deg g = 2$ となるのであれば f は単元となる。この場合、可約とはならない。

   $x^2+2x+4 = (x+\alpha)(x+\beta)$ となる場合を考える。$(x+\alpha)(x+\beta) = x^2+(\alpha+\beta)x+\alpha\beta$ であるので α, β は $\alpha + \beta = 2, \alpha\beta = 4$ を満たす。

   $\mathbb{Z}$ で考えれば、$\alpha\beta = 4$ より $(\alpha, \beta) = (1, 4), (2, 2), (4, 1)$ とその -1 倍したものとなるが、これらはすべて $\alpha+\beta = 2$ を満たさない。よって、$x^2+2x+4 = (x+\alpha)(x+\beta)$ となることはなく、$x^2 + 2x + 4$ は $\mathbb{Z}[x]$ において既約である。

   有理数の範囲で考えても α, β は $\alpha + \beta = 2, \alpha\beta = 4$ を満たすので、$\beta = 2 - \alpha$ を $\alpha\beta = 4$ に代入して出来る $\alpha^2-2\alpha+4 = 0$ を満たす。この方程式の解は $\alpha = 1\pm\sqrt{3}i$ となり有理数ではない。よって、$x^2 + 2x + 4$ は $\mathbb{Q}[x]$ においても既約である。

5. $x^3 + 5x + 6$

   $x^3 + 5x + 6 = (x + 1)\big(x^2 - x + 6\big)$ である。

   $x+1,\ x^2-x+6 \in \mathbb{Z}[x]$ であり、$x+1,\ x^2-x+6 \in \mathbb{Q}[x]$ であるので、x^3+5x+6 は $\mathbb{Z}[x]$ でも $\mathbb{Q}[x]$ でも可約である。

6. $7x^3 + 10x^2 + 20$

   7 は 5 で割り切れないが、10 と 20 は 5 で割り切れる。また、20 は 5^2 で割り切れない。アイゼンシュタインの既約判定法により $7x^3 + 10x^2 + 20$ は $\mathbb{Q}[x]$ で既約である。

   $7, 10, 20$ は互いに素であるので、$7x^3 + 10x^2 + 20$ は原始多項式である。原始多項式が $\mathbb{Z}[x]$ で可約なら $\mathbb{Q}[x]$ で可約である。その為、その対偶をとれば $\mathbb{Q}[x]$ で既約

なら $\mathbb{Z}[x]$ で既約である。よって、$7x^3+10x^2+20$ は $\mathbb{Q}[x]$ で既約であるので、$\mathbb{Z}[x]$ で既約である。

7. $x^{13}-1$
   $x^{13}-1=(x-1)\left(\sum_{i=0}^{12}x^i\right)$ である。$x-1$ や $\left(\sum_{i=0}^{12}x^i\right)$ は $\mathbb{Z}[x]$ や $\mathbb{Q}[x]$ の元であるので、$x^{13}-1$ は $\mathbb{Z}[x]$ でも $\mathbb{Q}[x]$ でも可約である。
8. $\sum_{i=0}^{17}x^i$
   $x=-1$ のとき、$\sum_{i=0}^{17}x^i=0$ であるので、$x+1$ で割り切れる。具体的には次のようになる。
   $$\sum_{i=0}^{17}x^i=(x+1)\left(\sum_{i=0}^{8}x^{2i}\right) \tag{2}$$
   よって、$\sum_{i=0}^{17}x^i$ は $\mathbb{Z}[x]$ でも $\mathbb{Q}[x]$ でも可約である。
9. $\sum_{i=13}^{22}x^i$
   $\sum_{i=13}^{22}x^i=x^{13}\sum_{i=0}^{9}x^i$ である。x^{13} や $\sum_{i=0}^{9}x^i$ は $\mathbb{Z}[x]$ や $\mathbb{Q}[x]$ の元であるので、$\sum_{i=13}^{22}x^i$ は $\mathbb{Z}[x]$ でも $\mathbb{Q}[x]$ でも可約である。
10. $187x^{80}-306x^{39}+204$
    $187x^{80}-306x^{39}+204=17(11x^{80}-18x^{39}+12)$ である。よって、$187x^{80}-306x^{39}+204$ は $\mathbb{Z}[x]$ において可約である。
    $11x^{80}-18x^{39}+12$ は 18 や 12 が 3 で割り切れるが、11 は 3 で割り切れない。また、12 は 3^2 でも割り切れない。アイゼンシュタインの既約判定法より、$11x^{80}-18x^{39}+12$ は $\mathbb{Q}[x]$ において可約である。

定数倍を除けば $\mathbb{Z}[x]$ と $\mathbb{Q}[x]$ の既約、可約は一致すると思われる。