体論 (第2回)

2. 多項式の既約性

今回は1変数多項式の既約性を判定する方法について述べる.

定義 2-1
A を整域とし, $f(x) \in A[x]$ はモニックかつ $\deg f \geq 1$ とする.

(1) $\deg g_1 \geq 1$, $\deg g_2 \geq 1$ かつ $g_1(x)g_2(x) = f(x)$ を満たす $g_1(x), g_2(x) \in A[x]$ が存在するとき, $f(x)$ を A 上**可約**と言う.

(2) $f(x)$ が A 上可約でないとき, $f(x)$ を A 上**既約**と言う. 言い換えると,

$$f(x) = g_1(x)g_2(x) \Rightarrow \deg g_1 = 0 \text{ または } \deg g_2 = 0$$

が成り立つ.

[補足] モニック1次多項式 $f(x) \in A[x]$ は A 上既約である.

x^2+1 は $\mathbb{Q}$ 上でこれ以上分解できないので $\mathbb{Q}$ 上既約である. 一方, $\mathbb{C}$ においては,

$$x^2 + 1 = (x+i)(x-i)$$

と分解できるので $\mathbb{C}$ 上可約である.

定理 2-1
$f(x) \in \mathbb{Z}[x]$ をモニックかつ $\deg f \geq 1$ とする. このとき, 次は同値である.

(1) $f(x)$ は $\mathbb{Z}$ 上既約である.

(2) $f(x)$ は $\mathbb{Q}$ 上既約である.

[証明]
参考文献 [1] 命題 1.11.34 を参照のこと.

□

定理 2-2

$f(x) \in \mathbb{Z}[x]$ をモニックかつ $\deg f = 2, 3$ とする．このとき，$f(x)$ が整数の根を持たなければ，$f(x)$ は $\mathbb{Q}$ 上既約である．

[証明]

定理 2-1 より $f(x)$ が $\mathbb{Z}$ 上既約であることを示せばよい．$f(x)$ が $\mathbb{Z}$ 上可約と仮定すると，$\deg f = 2, 3$ なので，

$$f(x) = (x - a)g(x) \quad (g(x) \in \mathbb{Z}[x],\ a \in \mathbb{Z})$$

と表せる．このとき，$f(a) = 0$ であるから仮定に矛盾する．従って，$f(x)$ は $\mathbb{Z}$ 上既約である．

□

[補足] 定理 2-2 は $f(x)$ が 4 次以上だと成立しない．例えば，$f(x) = (x^2 + 1)^2$ は $\mathbb{Q}$ 上可約であるが，整数の根を持たない．

例 2-1

(1) $f(x) = x^3 - 2$ は $\mathbb{Q}$ 上既約である．

(2) $\alpha = \sqrt[3]{2}$ は無理数である．

[証明]

(1) $y = f(x)$ のグラフを考えると，$f(x)$ は整数の根を持たないことが分かる．従って，定理 2-2 より $f(x)$ は $\mathbb{Q}$ 上既約である．

(2) $\alpha \in \mathbb{Q}$ と仮定する．因数定理より

$$x^3 - 2 = (x - \alpha)g(x) \quad (g(x) \in \mathbb{Q}[x])$$

と表せる．これは $f(x)$ が $\mathbb{Q}$ 上既約であることに矛盾する．従って，α は無理数である．

□

定理 2-3 (アイゼンシュタインの定理)

素数 p と多項式

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$$

に対して，

$$p \mid a_0,\ p \mid a_1,\ \ldots, p \mid a_{n-1},\ p^2 \nmid a_0 \qquad (*)$$

が成り立てば，$f(x)$ は $\mathbb{Q}$ 上既約である．

例えば，多項式 $f(x) = x^2 + 6x + 2$ は $p = 2$ で $(*)$ をみたすので $\mathbb{Q}$ 上既約である．

[定理 2-3 の証明]

$f(x)$ が $\mathbb{Z}$ 上可約と仮定する．このとき,

$$f(x) = (x^s + b_{s-1}x^{s-1} + \cdots + b_0)(x^t + c_{t-1}x^{t-1} + \cdots + c_0) \quad (a_i, b_i \in \mathbb{Z},\ 1 \leq s, t < n) \qquad (**)$$

と分解できる．$a_0 = b_0c_0$ であり, また $p \mid a_0$ より $p \mid b_0$ または $p \mid c_0$ である．$p \mid b_0$ としておく．すると, $p^2 \nmid a_0$ より $p \nmid c_0$ が分かる．ここで,

$$p \mid b_0,\ p \mid b_1, \ldots, p \mid b_{i_0-1},\ p \nmid b_{i_0}$$

をみたす $1 \leq i_0 \leq s$ をとる．式 $(**)$ の i_0 次の項を比較すると,

$$a_{i_0} = b_{i_0}c_0 + b_{i_0-1}c_1 + \cdots + b_1c_{i_0-1} + b_0c_{i_0}$$

を得る．このとき, 左辺は仮定から p で割れるが, 右辺は p で割れない ($p \nmid b_{i_0}c_0$ に注意)．よって矛盾．従って, $f(x)$ は $\mathbb{Z}$ 上既約であり, 定理 2-1 から $\mathbb{Q}$ 上既約でもある．

□

問題 2-1

(1) $f(x) = x^3 - 3x + 1$ が $\mathbb{Q}$ 上既約であることを示せ.

(2) $\alpha = \sqrt{2 + \sqrt{2}}$ が無理数であることを示せ.

例 2-2

$f(x) = x^4 + 1$ は $\mathbb{Q}$ 上既約である.

[証明]

$g(x) = f(x+1)$ と置く．このとき,

$$g(x) = (x+1)^4 + 1 = x^4 + 4x^3 + 6x^2 + 4x + 2$$

は $p = 2$ でアイゼンシュタインの定理の条件を満たすので, $\mathbb{Q}$ 上既約である．従って, 下の問題 2-2 より, $f(x) = g(x-1)$ も $\mathbb{Q}$ 上既約である.

□

問題 2-2 モニック多項式 $f(x) \in \mathbb{Q}[x]$ $(\deg f \geq 1)$ と $a \in \mathbb{Q}$ を考える．このとき, $f(x)$ が $\mathbb{Q}$ 上既約ならば, $f(x+a)$ も $\mathbb{Q}$ 上既約であることを示せ.

問題 2-3 $x^5 + 4$ が $\mathbb{Q}$ 上既約であることを示せ.

問題 2-4 p を素数とする.

(1) ${}_pC_k$ $(k = 1, 2, ..., p-1)$ が p で割れることを示せ.

(2) $f(x) = x^{p-1} + x^{p-2} + \cdots + 1$ は $\mathbb{Q}$ 上既約であることを示せ.

参考文献

[1] 雪江明彦, 代数学 2 環と体とガロア理論, 日本評論社, 2010.