環論 (第 16 回)

多項式の既約性とアイゼンシュタインの定理

前回に引き続き, UFD 上の多項式環の性質をみます. 目標は多項式の既約判定で頻繁に用いられるアイゼンシュタインの定理を示すことです.

定義 16-1
A を整域とする. $f(x) \in A[x]$ $(\deg f(x) \geq 1)$ に対して,

$$f(x) = g_1(x)g_2(x), \ \deg g_1(x) \geq 1, \ \deg g_2(x) \geq 1$$

となる $g_1(x)$, $g_2(x) \in A[x]$ があるとき, $f(x)$ は A 上**可約**と言い, そうでないとき, A 上**既約**と言う.

つまり, $f(x)$ が A 上既約というのは, A 上ではそれ以上分解できないような多項式のことです. 例えば, $f(x) = x^2 + 1$ を考えます. $f(x)$ は $\mathbb{Q}$ 上ではそれ以上分解できないので, $\mathbb{Q}$ 上既約となります. 一方, $\mathbb{C}$ においては, $f(x) = (x + i)(x - i)$ とさらに分解できるので, $\mathbb{C}$ 上可約となります.

[**注意**]

(1) 定義から 1 次多項式は常に既約になります.

(2) K を体とし, $f(x) \in K[x]$ $(\deg f(x) \geq 1)$ とします. このとき, 次が成り立ちます.

$$f(x) \text{ が } K[x] \text{ の既約元} \iff f(x) \text{ が } K \text{ 上既約.} \quad \text{(eq1)}$$

問題 16-1 (eq1) を示せ.

定理 16-1
A を UFD とし, K をその商体とする. 原始多項式 $f(x) \in A[x]$ $(\deg f \geq 1)$ が A 上既約ならば, $f(x)$ は K 上既約でもある.

[**証明**]
対偶を示す. $f(x)$ が K 上可約とすると,

$$f(x) = g_1(x)g_2(x), \ \deg g_1(x) \geq 1, \ \deg g_2(x) \geq 1$$

となる $g_1(x)$, $g_2(x) \in K[x]$ がある. 各 $g_i(x)$ に対して, 定理 15-3 (1) から

$$g_i(x) = \alpha_i h_i(x)$$

をみたす $\alpha_i \in K^\times$ と $A[x]$ の原始多項式 $h_i(x)$ が取れる．このとき，

$$(\alpha_1\alpha_2)h_1(x)h_2(x) = f(x) \in A[x]$$

で，$h_1(x)h_2(x)$ は原始多項式だから，$\alpha_1\alpha_2 \in A$ となる (定理 15-2 (2) を参照)．よって $f(x)$ は A 上可約である．

□

問題 16-2　モニックな 3 次多項式 $f(x) \in \mathbb{Z}[x]$ は整数の根を持たなければ，$\mathbb{Q}$ 上既約であることを示せ．

定理 16-2 (アイゼンシュタインの定理)
A を UFD，K をその商体とする．原始多項式 $f(x) \in A[x]$ $(\deg f(x) \geq 1)$ を

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

で表す．このとき，

$$p \nmid a_n,\ \ p \mid a_{n-1},\ \ \ldots,\ \ p \mid a_0,\ \ p \nmid a_0^2$$

をみたす A の素元 p が存在すれば，$f(x)$ は K 上既約である．

[**証明**]
定理 16-1 より，$f(x)$ が A 上既約であることを示せばよい．仮に A 上可約だとすると，

$$f(x) = g_1(x)g_2(x),\ \ l := \deg g_1(x) \geq 1,\ \ m := \deg g_2(x) \geq 1$$

をみたす $g_1(x)$, $g_2(x) \in A[x]$ がある．ここで，

$$g_1(x) = \sum_{i=0}^{l} b_i x^i, \quad g_2(x) = \sum_{i=0}^{m} c_i x^i$$

と置く．$p^2 \nmid a_0$ より $p \nmid b_0$ または $p \nmid c_0$．ここでは，$p \nmid b_0$ の場合を考える．このとき，$p \mid a_0$ より $p \mid c_0$．また $p \nmid a_n$ より $p \nmid c_m$ に注意する．よって

$$p \mid c_0,\ \ p \mid c_1,\ \ \ldots,\ \ p \mid c_{i-1},\ \ p \nmid c_i$$

をみたす $0 < i \leq m$ がとれる．$f(x) = g_1(x)g_2(x)$ の両辺の i 次の係数を比較すると，

$$a_i = \underbrace{b_i c_0 + b_{i-1}c_1 + \cdots + b_1 c_{i-1}}_{p \text{ で割れる}} + \underbrace{b_0 c_i}_{p \text{ で割れない}}.$$

これより，$p \nmid a_i$ だが，$0 < i \leq m < n$ より a_i の条件に矛盾．$p \nmid c_0$ の場合も同様に矛盾．以上より $f(x)$ は A 上既約である．

□

例えば，$f(x) = x^3 + 4x^2 + 6x + 2 \in \mathbb{Z}[x]$ を考えます．このとき，$f(x)$ 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，$\mathbb{Q}$ 上既約となります．

例題 16-1

$f(x) = x^4 + 1$ が $\mathbb{Q}$ 上既約であることを示せ.

[**解答**]

$g(x) = f(x+1)$ と置く. このとき,

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

$g(x)$ 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. 従って $f(x) = g(x-1)$ も $\mathbb{Q}$ 上既約.

□

問題 16-3

(1) $f(x) = x^4 - 5x^2 + 10$ が $\mathbb{Q}$ 上既約であることを示せ.

(2) $g(x) = x^4 + x^3 + x^2 + x + 1$ が $\mathbb{Q}$ 上既約であることを示せ.

(3) $h(x) = x^2 + y^2 + xy^2 + xy - 1$ が $\mathbb{C}[y]$ 上既約であることを示せ.