環論 (第 15 回)

UFD 上の多項式環

今回は UFD 上の多項式環の性質について調べる. 目標は次を示すことである.

$$A \text{ は UFD} \Rightarrow A[x] \text{ も UFD} \tag{1}$$

(定理 15-6 を参照). 例えば, $\mathbb{Z}$ は UFD だったので, $\mathbb{Z}[x]$ も UFD となる. まずは, (1) を示すために必要な準備をする.

定義 15-1

整域 A の元 $a_1, a_2, ..., a_n$ はいずれかは 0 でないとする.

(1) $d \in A$ は $d \mid a_i$ $(i = 1, ..., n)$ をみたすとき, $a_1, ..., a_n$ の**公約元**という.

(2) $g \in A$ は $a_1, ..., a_n$ の公約元で, 任意の $a_1, ..., a_n$ の公約元 b に対して $b \mid g$ が成り立つとき, g を $a_1, ..., a_n$ の**最大公約元**といい, $\gcd(a_1, ..., a_n)$ で表す.

(3) $\gcd(a_1, ..., a_n) = 1$ のとき, $a_1, ..., a_n$ は**互いに素**という.

例えば, $\mathbb{Z}[x]$ の多項式 $f(x) = x^2 - 1$ と $g(x) = x^2 - 2x + 1$ は,

$$f(x) = (x-1)(x+1), \quad g(x) = (x-1)^2$$

と分解されるので, $\gcd(f(x), g(x)) = x - 1$ となる.

定理 15-1

A を UFD とし，$a_1, ..., a_n \in A$ はいずれかは 0 でないとする.

(1) $a_1, ..., a_n$ の最大公約元は存在する.

(2) g, g' がともに $a_1, ..., a_n$ の最大公約元ならば, g と g' は同伴である.

つまり, $a_1, ..., a_n$ の最大公約元は同伴の差を除き一意的に存在する.

[証明]

(1) $a_1, ..., a_n$ の順番を入れ替えて

$$a_1 \neq 0, ..., \ a_m \neq 0, \ a_{m+1} = 0, \ ..., \ a_n = 0$$

とする. A は UFD より $1 \leq i \leq m$ に対して

$$a_i = u_i \prod_{j=1}^{l} p_j^{\alpha_{ij}} \quad (\alpha_{ij} : \text{非負整数}, u_i \in A^\times, p_j : A \text{ の素元})$$

と表せる. ここで

$$g := \prod_{j=1}^{l} p_j^{\min\{\alpha_{1j}, ..., \alpha_{mj}\}}$$

とおくと, $g \mid a_i (i = 1, ..., n)$ である. また, $b \in A$ が $b \mid a_i$ $(i = 1, \ldots, n)$ を満たすとする. このとき,

$$b = v \prod_{j=1}^{l} p_j^{\beta_j} \quad (\ \beta_j : \text{非負整数}, v \in A^\times)$$

とかけて, さらに $b \mid a_1, ..., b \mid a_n$ より

$$\beta_j \leq \min\{\alpha_{1j}, ..., \alpha_{mj}\}.$$

従って $b \mid g$ を得る. よって g は $a_1, ..., a_n$ の最大公約元である.

(2) g, g' がともに $a_1, ..., a_n$ の最大公約元とする. g は $a_1, ..., a_n$ の公約元で g' は最大公約元だから $g \mid g'$. 同様に $g' \mid g$. よって $g \sim g'$.

□

問題 15-1 A を PID とし, $a, b \in A$ とする. このとき, $(\gcd(a, b)) = (a, b)$ を示せ.

定義 15-2 (原始多項式)
A を UFD とし,

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

とする. $\gcd(a_0, a_1, ..., a_n) = 1$ のとき, $f(x)$ を**原始多項式**という.

例えば, $f(x) = 6x^2 + 15x^2 + 10$ は $\gcd(6, 15, 10) = 1$ より $\mathbb{Z}[x]$ の原始多項式である.

定理 15-2 (ガウスの補題)
A を UFD とし, $f(x), g(x) \in A[x]$ はともに原始多項式とする. このとき, $f(x)g(x)$ も原始多項式である.

[証明]
$h(x) = f(x)g(x)$ とし,

$$f(x) = \sum_i a_i x^i, \quad g(x) = \sum_i b_i x^i, \quad h(x) = \sum_i c_i x^i$$

と表す. $h(x)$ が原始多項式でないとすると,

$$p \mid c_i \quad (i = 0, 1, 2, ...) \tag{2}$$

をみたす A の素元 p が存在する．一方，

$$p \mid a_0,\ \ldots,\ p \mid a_{i_0-1},\ p \nmid a_{i_0},$$
$$p \mid b_0,\ \ldots,\ p \mid b_{j_0-1},\ p \nmid b_{j_0}$$

をみたす i_0, j_0 がとれる．ここで，$h(x) = f(x)g(x)$ の両辺の $i_0 + j_0$ 次の項を比較すると，

$$c_{i_0+j_0} = \underbrace{a_0 b_{i_0+j_0} + \cdots + a_{i_0-1} b_{j_0+1}}_{p \text{ で割れる}} + a_{i_0} b_{j_0} + \underbrace{a_{i_0+1} b_{j_0-1} + \cdots + a_{i_0+j_0} b_0}_{p \text{ で割れる}}.$$

$p \nmid a_{i_0} b_{j_0}$ より $p \nmid c_{i_0+j_0}$ となる．これは (2) に反する．よって $h(x)$ は原始多項式である．

□

定理 15-3

UFD A とその商体 K を考える．

(1) $f(x) \in K[x] \setminus \{0\}$ に対して，$f(x) = \alpha g(x)$ をみたす $\alpha \in K^\times$ と $A[x]$ の原始多項式 $g(x)$ が存在する．

(2) $\alpha, \beta \in K^\times$ と $A[x]$ の原始多項式 $f(x), g(x)$ に対して，$\alpha f(x) = \beta g(x)$ ならば $\beta\alpha^{-1} \in A^\times$ が成り立つ．

[証明]

(1) まず，

$$f(x) = \frac{a_n}{b_n} x^n + \frac{a_{n-1}}{b_{n-1}} x^{n-1} + \cdots + \frac{a_0}{b_0} \quad (a_i, b_i \in A)$$

と表す．$b = b_0 \cdots b_n$ と置くと，$ba_i \in A\,(0 \le i \le n)$ となる．$c = \gcd(ba_0, \ldots, ba_n)$ と置くと，

$$g(x) := \frac{a_n b}{c} x^n + \cdots + \frac{a_0 b}{c} \in A[x]$$

は原始多項式で，$f(x) = \dfrac{c}{b} g(x)$ をみたす．

(2) $\alpha = \dfrac{a}{b},\ \beta = \dfrac{c}{d}\ (a, b, c, d \in A)$ と置くと，

$$adf(x) = bcg(x)$$

となる．$f(x), g(x)$ は原始多項式より $adf(x), bcg(x)$ のそれぞれの係数の最大公約元は ad, bc である．定理 15-1 (2) より $adu = bc\,(u \in A^\times)$ と表せる．よって

$$\beta\alpha^{-1} = u \in A^\times.$$

□

[補足]　定理 15-3 (1) において，

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

のときは

$$c = \gcd(a_0, a_1, ..., a_n), \quad g(x) := \frac{1}{c} f(x) \in A[x]$$

とすればよい.

定理 15-4

A を UFD，K をその商体とし，$f(x)$ を $A[x]$ の原始多項式とする.

(1) $g(x) \in A[x]$ とする. $K[x]$ において $f(x) \mid g(x)$ ならば, $A[x]$ において $f(x) \mid g(x)$ である.

(2) 次が成り立つ.

$$f(x) \text{ が } K[x] \text{ の素元} \iff f(x) \text{ が } A[x] \text{ の素元.}$$

[証明]

(1) $f(x) \mid g(x)$ とすると,

$$g(x) = f(x)h(x) \quad (\ h(x) \in K[x]\ )$$

と表せる. 定理 15-3 (1) とその補足から

$$g(x) = \alpha g_1(x), \quad h(x) = \beta h_1(x)$$

を満たす $\alpha \in A$, $\beta \in K^\times$ と $A[x]$ の原始多項式 $g_1(x), h_1(x)$ がとれる. このとき,

$$\alpha g_1(x) = \beta f(x) h_1(x)$$

であり, 定理 15-2 から $f(x)h_1(x)$ は $A[x]$ の原始多項式となる. よって, 定理 15-3 (2) より $\beta\alpha^{-1} \in A$. よって $\beta \in A$. これより $h(x) \in A[x]$ となる.

(2) $f(x)$ を $K[x]$ の素元と仮定する. このとき,

$$f(x) \mid g(x)h(x) \quad (g(x), h(x) \in A[x])$$

とすると, $K[x]$ において

$$f(x) \mid g(x) \quad \text{または} \quad f(x) \mid h(x).$$

(1) より $A[x]$ において

$$f(x) \mid g(x) \quad \text{または} \quad f(x) \mid h(x)$$

が成り立つ. よって $f(x)$ は $A[x]$ の素元である.

逆に $f(x)$ を $A[x]$ の素元とする. $K[x]$ は UFD だから, $f(x)$ が $K[x]$ の既約元であることを示せばよい. $f(x)$ は $A[x]$ の素元かつ原始多項式なので $\deg f(x) \geq 1$ となる. 特に $f(x) \notin K^\times$ である. 次に, $g(x) \in K[x]$ を $f(x)$ の約元とし, $\alpha \in K^\times$ と $A[x]$ の原始多項式 $g_1(x)$ を用いて $g(x) = \alpha g_1(x)$ と表す. $K[x]$ で $g_1(x) \mid f(x)$ だから, $A[x]$ でも $g_1(x) \mid f(x)$ である. $f(x)$ は $A[x]$ の既約元だから,

$$g_1(x) \in A[x]^\times = A^\times \quad \text{または} \quad A[x] \text{ で } f(x) \sim g_1(x).$$

従って

$$g(x) \in K^\times \quad \text{または} \quad K[x] \text{ で } f(x) \sim g(x).$$

従って $f(x)$ は $K[x]$ の既約元である. □

定理 15-5
可換環 A の素元は $A[x]$ の素元でもある.

[**証明**] 問題 15-2.

□

問題 15-2 可換環 A の素元 p を考える.

(1) 次の同型を示せ.

$$A[x]/pA[x] \simeq (A/(p))[x].$$

(2) p は $A[x]$ の素元であることを示せ.

□

以上を踏まえて, 目標であった (1) の証明をする.

定理 15-6
A が UFD ならば, $A[x]$ も UFD である.

[**証明**]
K を A の商体とする. $f(x) \in A[x]$ $(f(x) \notin A[x]^\times,\ f(x) \neq 0)$ とすると, $K[x]$ は UFD より

$$f(x) = f_1(x) \cdots f_s(x) \quad (f_i(x) : K[x] \text{ の素元})$$

と表せる. 定理 15-3 より

$$f_i(x) = c_i g_i(x) \quad (c_i \in K^\times,\ g_i(x) \in A[x] : \text{原始多項式})$$

と表せる. 定理 15-4 (2) より各 $g_i(x)$ は $A[x]$ の素元である. また

$$(c_1 \cdots c_s) g_1(x) \cdots g_s(x) = f(x) \in A[x]$$

で, $g_1(x) \cdots g_s(x)$ は原始多項式なので $c := c_1 \cdots c_s \in A$ となる. $c \in A^\times$ ならば,

$$f(x) = (cg_1(x)) g_2(x) \cdots g_s(x)$$

が $f(x)$ の素元分解である. $c \notin A^\times$ ならば, A は UFD より

$$c = p_1 \cdots p_t \quad (p_i : A \text{ の素元})$$

と表せる. 定理 15-5 より各 p_i は $A[x]$ の素元であるから,

$$f(x) = p_1 \cdots p_t \cdot g_1(x) \cdots g_s(x)$$

が $f(x)$ の素元分解である.

□

[**コメント**] 定理 15-6 を繰り返し使うと, A が UFD のとき, $A[x_1, \ldots, x_n]$ も UFD であることが分かる.

問題 15-3 PID ではない UFD の例を一つ挙げよ.