2008年6月20日

$A = \mathbf{R}[x]$ のイデアル $I = (x^2+1)$ を考え、同値関係

$$R = \{(a,b) \mid a \in A,\ b \in A,\ a-b \in I\}.$$

による商集合 A/R (A/I とも書く) に演算

$$+ : A/I \times A/I \to A/I, \quad + ([a],[b]) = [a+b],$$
$$\times : A/I \times A/I \to A/I, \quad \times ([a],[b]) = [ab].$$

を入れることにより、$\mathbf{R}[x]/I \cong \mathbf{C}$ となる。

同様のことを $\mathbf{R}$ の代わりに $\mathbf{Z}/3\mathbf{Z}$ でやってみる。$A = \mathbf{Z}/3\mathbf{Z}[x]$ のイデアル $I = (x^2+1)$ を考え、同値関係

$$R = \{(a,b) \mid a \in A,\ b \in A,\ a-b \in I\}.$$

による商集合 A/R (A/I とも書く) に演算

$$+ : A/I \times A/I \to A/I, \quad + ([a],[b]) = [a+b],$$
$$\times : A/I \times A/I \to A/I, \quad \times ([a],[b]) = [ab].$$

を入れる。$\mathbf{Z}/3\mathbf{Z}$ は3個の同値類 $[0],[1],[2]$ からなるので、A/I は以下の9個の同値類からなる：

$$[[0]],[[1]],[[2]],[[1]x],[[1]x+[1]],[[1]x+[2]],[[2]x],[[2]x+[1]],[[2]x+[2]]$$

これらを簡単に

$$0,1,2,x,x+1,x+2,2x,2x+1,2x+2$$

と書くことにする。加法は例えば、A において

$$(x+2)+(2x+2) = ([1]x+[2])+([2]x+[2]) = ([1]+[2])x+([2]+[2])$$
$$= [1+2]x+[2+2] = [0]x+[1] = [1] = 1$$

というように計算するので、A/I においては $[x+2]+[2x+2] = [1]$ となる。

乗法は例えば、A において

$$(x+2)(2x+2) = ([1]x+[2]) \times ([2]x+[2]) = [1][2]x^2+([1][2]+[2][2])x+[2][2]$$
$$= [2]x^2+[2+4]x+[4] = [2]x^2+[1] = 2x^2+1$$

というように計算するので、A/I においては $[x+2] \times [2x+2] = [2x^2+1] = [2(x^2+1)+2] = [2]$ となる。

体の定義

集合 A に 2 つの演算 $+$（加法）と $\times$（乗法）が定義されていて、下記の性質が成り立つとき、A は環であるという。

(1) $\forall a, b, c \in A,\ (a+b)+c = a+(b+c)$ （結合法則）

(2) $\forall a, b \in A,\ a+b = b+a$ （交換法則）

(3) $\exists 0 \in A,\ \forall a \in A,\ a+0 = a$ （零元の存在）

(4) $\forall a \in A,\ \exists b \in A,\ a+b = 0$ （加法に関する逆元の存在）

(5) $\forall a, b, c \in A,\ (a \times b) \times c = a \times (b \times c)$ （結合法則）

(6) $\exists 1 \in A,\ \forall a \in A,\ a \times 1 = 1 \times a = a$ （単位元の存在）

(7) $\forall a, b, c \in A,\ a \times (b+c) = (a \times b) + (a \times c),\ (b+c) \times a = (b \times a) + (c \times a)$ （分配法則）

環 A が次の条件を満たすとき、体という。

(1) $\forall a, b \in A,\ a \times b = b \times a$ （乗法に関する交換法則）

(2) $\forall a \in A - \{0\},\ \exists b \in A,\ ab = 1$ （乗法に関する逆元の存在）

例えば、$\mathbf{Q}, \mathbf{R}, \mathbf{C}$ は体である。$\mathbf{Z}$ は体ではない。また、一般に整域の商体は体であり、体は必ず整域である。

代数学の基本定理（定数でない複素数係数の 1 変数多項式は複素数の零点を必ず持つ）から、$\mathbf{R}[x]/(3\text{次以上の多項式})$ は整域にならない。ただし、$\mathbf{Q}[x]/(3\text{次以上の多項式})$ は体になることもある。因数分解できない多項式を既約という。

ユークリッドの互除法

以下 $A = \mathbf{Z}$ または $A = K[x]$ (ただし K は体) とする。

- $A = \mathbf{Z}$ のとき、$a \in A,\ b \in A,\ b > 0$ とすると、a を b で割った商と余りを求めることができる。すなわち、$a = bq + r,\ 0 \leq r < b$ となる $q, r \in A$ がただひとつ定まる。
- $A = K[x]$ のとき、$a(x) \in A,\ b(x) \in A,\ b(x) \neq 0$ とすると、$a(x)$ を $b(x)$ で割った商と余りを求めることができる。すなわち、$a(x) = b(x)q(x) + r(x),\ 0 \leq \deg r(x) < \deg b(x)$ または $r(x) = 0$ となる $q(x), r(x) \in A$ がただひとつ定まる。

以後、$a(x), b(x)$ の代わりに、a, b と書く。$A = \mathbf{Z}$, $A = K[x]$ いずれの場合にも、$r = 0$ となるとき、$b|a$ と書き、a は b で割り切れる、という。

$a, b \in A$ とし、a と b の少なくとも一方は 0 でないとする。a と b の最大公約数（最大公約元） d とは、以下の条件を満たすものである。

(1) $d > 0$ ($A = \mathbf{Z}$ の場合), d は最高次の係数が 1 ($A = K[x]$ の場合)

(2) $(d|a) \wedge (d|b)$

(3) $\forall e \in A,\ ((e|a) \wedge (e|b)) \implies e|d$

a と b の最大公約元を $\gcd(a, b)$ と書く。

$a, b \in A$ とし、a と b の少なくとも一方は 0 でないとする。今、0 でない方を b とし、$A = \mathbf{Z}$ の場合は $b' = |b|$ とする。$r_0 = a$, $r_1 = b'$ とおき、$k = 0, 1, \ldots$ に対して、r_k を r_{k+1} で割った商を q_{k+2}, 余りを r_{k+2} とおく。このとき

$$\begin{array}{ll} r_k > r_{k+1} & (A = \mathbf{Z}) \\ \deg r_k > \deg r_{k+1} & (A = K[x]) \end{array}$$

なので、$\exists n,\ r_n \neq 0,\ r_{n+1} = 0$ となる。すると r_{n+2} 以降は定義できない。

このとき、

$$\begin{aligned} r_n &= r_{n-2} - r_{n-1}q_n \\ &= r_{n-2} - (r_{n-3} - r_{n-2}q_{n-1})q_n \\ &= -r_{n-3}q_n + r_{n-2}(1 + q_{n-1}q_n) \\ &= \cdots \\ &= m_0 r_0 + m_1 r_1 \\ &= m_0 a + m_1 b' \\ &= m_0 a \pm m_1 b. \end{aligned}$$

これより、

$$\gcd(a, b) = \begin{cases} r_n & (A = \mathbf{Z}), \\ r_n \text{ をその最高次の係数で割ったもの} & (A = K[x]) \end{cases}$$

であり、しかも $\exists s, t \in A,\ sa + tb = \gcd(a, b)$ となる。