2008年6月27日

体の定義

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）

ユークリッドの互除法

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

$$\begin{array}{ll} r_k > r_{k+1} \geq 0 & (A = \mathbf{Z}) \\ \deg r_k > \deg r_{k+1} & (A = K[x]) \end{array}$$

なので、$\exists n,\ r_n \neq 0,\ r_{n+1} = 0$ となる。このとき、

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

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

体の例

p を素数とすると、$\mathbf{Z}/p\mathbf{Z}$ は体である。また、K を体とし、$f(x) \in K[x]$ を既約多項式とすると、$K[x]/(f(x))$ は体である。

体の元の位数

K を体とし、$0 \neq x \in K$ とする。

$$\exists n \in \mathbf{N},\ x^n = 1$$

が成り立つとき、このような最小の n を x の位数という。このような $n \in \mathbf{N}$ が存在しないときは、x の位数は無限であるという。$1 \in K$ の位数は 1 である。$-1 \in \mathbf{Q}$ の位数は 2 である。

$n \in \mathbf{N}$ とすると、

$$\zeta = e^{2\pi i/n} = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n} \in \mathbf{C}$$

の位数は n である。$\mathbf{C}$ における位数 n の元全体の集合は

$$\{\zeta^k \mid k \in \{1,\dots,n\},\ \gcd(k,n) = 1\}$$

である。この集合の元の個数、すなわち

$$|\{k \mid k \in \{1,\dots,n\},\ \gcd(k,n) = 1\}|$$

を $\varphi(n)$ で表し、φ をオイラーの関数という。例えば、$\varphi(1) = 1$ である。また、p が素数ならば

$$\varphi(p) = |\{1,2,\dots,p-1\}| = p-1$$

であり、一般には $\varphi(n) \leq n-1$ である。例えば $\varphi(12) = |\{1,5,7,9\}| = 4$ である。

有限体

K が体であり、しかも有限集合のとき、K を有限体という。例えば $\mathbf{Z}/p\mathbf{Z}$ は有限体である。また、$f(x) \in \mathbf{Z}/p\mathbf{Z}[x]$ が既約なら、$(\mathbf{Z}/p\mathbf{Z}[x])/(f(x))$ は有限体である。特に $(\mathbf{Z}/3\mathbf{Z}[x])/(x^2+1)$ は有限体である。

K を有限体とし、$0 \neq x \in K$ とすると、x の位数は有限でしかもそれは $|K|-1$ の約数である。例えば、$(\mathbf{Z}/3\mathbf{Z}[x])/(x^2+1)$ の 8 個の非零元の位数は、$1,2,4,8$ のいずれかである。実は、この逆も成り立つ。K を有限体とし、d を $|K|-1$ の約数とすると、K には位数 d の元が存在する。この事実の証明は次回の講義で行う。