2008年6月27日

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。

実際、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。

r_n の作り方から $r_{n+1} = 0$ より、r_{n-1} は r_n で割り切れている。r_{n-2} を r_{n-1} で割った余りが r_n であるということから r_{n-2} も r_n で割り切れている。同様に r_{n-3} も r_n で割り切れている。続けていくと r_1, r_0 も r_n で割り切れている。したがって r_n は a, b 両方を割り切っている。

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

とおくと、上で示したように、d は a, b 両方を割り切っている。

また、$e|a$ かつ $e|b$ とすると、$e|r_0$ かつ $e|r_1$ である。r_2 は r_0 を r_1 で割った余りなので $e|r_2$ となる。r_3 は r_1 を r_2 で割った余りなので $e|r_1$, $e|r_2$ より $e|r_3$ となる。同様に続けていくと $e|r_n$ がわかる。よって $e|d$ となる。

以上より、$d = \gcd(a, b)$ が言えた。