2012年7月3日

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、p を素数とするとき $\mathbb{Z}/p\mathbb{Z}$ は体である。また、$(\mathbb{Z}/p\mathbb{Z})[x]$ において $f(x)$ は既約ならば、$(\mathbb{Z}/p\mathbb{Z})[x]/(f(x))$ も体になる。これらはいずれもユークリッドの互除法を用いて証明される。

実際、$[a] \in \mathbb{Z}/p\mathbb{Z}$ を 0 でないとすると a は p で割り切れないから $\gcd(a,p) = 1$ である。すると、ある $s,t \in \mathbb{Z}$ が存在して $sa + tp = 1$ となるが、これは $[s][a] = [1]$ を意味する。すなわち、$[a]$ は逆元を持つ。

また、$[g(x)] \in (\mathbb{Z}/p\mathbb{Z})[x]/(f(x))$ を 0 でないとすると $g(x)$ は $f(x)$ で割り切れない。$f(x)$ が既約だから、これは $\gcd(g(x), f(x)) = 1$ を意味する。すると、ある $s(x), t(x) \in (\mathbb{Z}/p\mathbb{Z})[x]$ が存在して $s(x)g(x) + t(x)f(x) = 1$ となるが、これは $[s(x)][g(x)] = [1]$ を意味する。すなわち、$[g(x)]$ は逆元を持つ。

K を体とし、$f(X) \in K[X]$ を多項式とする。このとき、$x \in K$ を $f(X)$ に「代入」することができるので、それを $f(x)$ で表す。

一般に $a, b \in K$ に対して、$ab = 0$ ならば $a = 0$ または $b = 0$ である。実際、$a \neq 0$ とすると a の逆元 c が存在する、すなわち $ac = 1$ となる。このとき $b = 1b = acb = c(ab) = c0 = 0$ となる。

全単射

$$\{k \mid k \in N,\ d = \gcd(k,n)\} \to \{k' \mid k' \in \{1, \ldots, \frac{n}{d}\},\ 1 = \gcd(k', \frac{n}{d})\}$$

$k \mapsto \frac{k}{d}$ がある。

全単射 $D \to D,\ d \mapsto \frac{n}{d}$ がある。