2013年7月2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、$a \in K$ を $f(x)$ に「代入」することができるので、それを $f(a)$ で表す。「因数定理」は実は任意の体で成り立つ。定理1の後半の証明には、次の一般的事実を使う。

$$a, b \in K, ab = 0 \implies a = 0 \text{ または } b = 0.$$

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。

定理 1. *K を体とし、$f(x) \in K[x]$ を多項式とする。$a \in K$ に対して、*

$$f(a) = 0 \iff \exists g(x) \in K[x],\ f(x) = (x - a)g(x).$$

特に、$|\{a \in K \mid f(a) = 0\}| \leq \deg f(x)$.

証明. 前半は多項式 $f(x)$ を $x - a$ で割った余りを考えれば明か。後半は、$\deg f(x)$ に関する帰納法を用いる。$f(x) = (x - a)g(x)$ で $f(b) = 0$ ならば $g(b) = 0$ でなければならないこと、$\deg g(x) = \deg f(x) - 1$ であることからわかる。 □

以下、K を有限体とし、$q = |K|$ とする。$K^\times = K - \{0\}$ と書く。$a \in K^\times$ とすると、$a, a^2, a^3, \ldots$ を考えるとこれらすべて相異なることはない。$a^i = a^j$ $(i < j)$ とすると、$a^{j-i} = 1$ となる。すなわち、$\{n \in \mathbb{N} \mid a^n = 1\} \neq \emptyset$ である。そこで、この集合の最小値を a の位数とよぶ。すなわち、a の位数が n であるとは

$$\begin{aligned} &a^n = 1, \\ &\forall m \in \{1, \ldots, n-1\},\ a^m \neq 1. \end{aligned}$$

となることを言うのである。

補題 1. *K を有限体、$|K| = q$ とし、$a \in K^\times$ の位数が n とすると、$n | q - 1$.*

証明.

$$\{1, a, a^2, \ldots, a^{n-1}\} \subseteq K^\times.$$

である。ここで等号が成り立てば $n = q-1$ だが、等号が成り立たなければ $\exists b \in K^\times$, $b \notin \{1, a, a^2, \ldots, a^{n-1}\}$ となる。このとき

$$\{1, a, a^2, \ldots, a^{n-1}\} \cup \{b, ab, a^2b, \ldots, a^{n-1}b\} \subseteq K^\times.$$

この操作を繰り返すと、$\exists b_1, \ldots, b_m \in K^\times$,

$$\bigcup_{j=1}^{m} \{b_j, ab_j, a^2b_j, \ldots, a^{n-1}b_j\} = K^\times \quad \text{(disjoint)}$$

となるので $q-1 = mn$ となって n は $q-1$ の約数であることがわかる。 □

実は、補題1 の逆も成り立つ。n を $q-1$ の約数とすると、K には位数 n の元が存在する。これを示すために補題を準備する。

補題 2. $a \in K^\times$ の位数が n とすると、$m \in \mathbb{N}$ に対して、$a^m = 1 \iff n|m$ である。特に、$a^{q-1} = 1$.

証明. 明らかに、$n|m$ ならば $a^m = 1$ である。逆に $a^m = 1$ とすると、m を n で割って $m = ns + r$, $0 \leq r < n$ とすると、$1 = a^m = (a^n)^q a^r = a^r$ となる。n の最小性より $r = 0$ を得る。後半は、補題1 と前半よりわかる。 □

補題 3. $\forall n \in \mathbb{N}$, $n|q-1 \implies |\{a \mid a \in K^\times,\ a^n = 1\}| = n$.

証明. $f(x) = x^n - 1 \in K[x]$ とおくと、$n|q-1$ より $\exists g(x) \in K[x]$, $x^{q-1} - 1 = f(x)g(x)$ となる。補題2 の後半より、

$$\begin{aligned}
q - 1 = |K^\times| &= |\{a \mid a \in K^\times,\ a^{q-1} - 1 = 0\}| \\
&= |\{a \mid a \in K^\times,\ f(a) = 0 \text{ or } g(a) = 0\}| \\
&\leq |\{a \mid a \in K^\times,\ f(a) = 0\}| + |\{a \mid a \in K^\times,\ g(a) = 0\}| \\
&\leq \deg f(x) + \deg g(x) \\
&= n + (q - 1 - n) = q - 1.
\end{aligned}$$

したがって、$f(x) = 0$ は n 個の相異なる解を $K^\times$ に持つ。 □

補題 4. $\forall n \in \mathbb{N}$

$$n = \sum_{\substack{d \in \mathbb{N} \\ d|n}} \varphi(d).$$

証明. $N = \{1, 2, \ldots, n\}$, $D = \{d \mid d \in \mathbb{N},\ d|n\}$ とし、

$$S = \{(k, d) \mid (k, d) \in N \times D,\ d = \gcd(k, n)\}$$

とおく。すると

$$\begin{aligned} n = |N| &= \sum_{k \in N} 1 = \sum_{k \in N} |\{d \mid d \in D,\ d = \gcd(k, n)\}| \\ &= |S| = \sum_{d \in D} |\{k \mid k \in N,\ d = \gcd(k, n)\}| \end{aligned}$$

全単射

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

$k \mapsto \frac{k}{d}$ が存在するから

$$\begin{aligned} n &= \sum_{d \in D} |\{k' \mid k' \in \{1, \ldots, \frac{n}{d}\},\ 1 = \gcd(k', \frac{n}{d})\}| \\ &= \sum_{d \in D} \varphi(\frac{n}{d}). \end{aligned}$$

全単射 $D \to D$, $d \mapsto \frac{n}{d}$ が存在するから

$$n = \sum_{e \in D} \varphi(e).$$

□

定理 2. K を有限体、$n \in \mathbb{N}$ を $|K| - 1$ の約数とすると、

$$|\{a \mid a \in K^\times,\ a \text{ の位数は } n\}| = \varphi(n).$$

証明. 左辺を $\alpha(n)$ とおくと、$\alpha(1) = \varphi(1)$ は明らか。ある n より小さい d について $\alpha(d) = \varphi(d)$ が成立すると仮定すると、

$$\begin{aligned} \sum_{\substack{d \in \mathbb{N} \\ d|n}} \varphi(d) &= n && \text{(補題 4 より)} \\ &= |\{a \mid a \in K^\times,\ a^n = 1\}| && \text{(補題 3 より)} \\ &= \sum_{\substack{d \in \mathbb{N} \\ d|n}} \alpha(d) && \text{(補題 2 より)} \\ &= \sum_{\substack{d \in \mathbb{N} \\ d|n \\ d \neq n}} \alpha(d) + \alpha(n) \\ &= \sum_{\substack{d \in \mathbb{N} \\ d|n \\ d \neq n}} \varphi(d) + \alpha(n) && \text{(帰納法の仮定より)}. \end{aligned}$$

よって $\varphi(n) = \alpha(n)$ を得る。 □

例えば、$\mathbb{Z}/13\mathbb{Z}$ は体であり、位数 12 の元は $2, 6, 7, 11$ で、確かに $\varphi(12) = 4$ 個である。位数 6 の元は $4, 10$ で、確かに $\varphi(6) = 2$ 個である。

一般に、$|K| = q$ である体 K には、位数 $q-1$ の元の存在が保証されているので、そのような元のひとつを α とすると、$K^\times$ の乗積表は、次のようになる。

$\times$	1	α	α^2	$\cdots$	α^{q-1}
1	1	α	α^2	$\cdots$	α^{q-1}
α	α	α^2	α^3	$\cdots$	1
α^2	α^2	α^3	α^4	$\cdots$	α
$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$
α^{q-2}	α^{q-2}	1	α	$\cdots$	α^{q-3}

指数だけ書けば

$+$	0	1	2	$\cdots$	$q-1$
0	0	1	2	$\cdots$	$q-1$
1	1	2	3	$\cdots$	0
2	2	3	4	$\cdots$	1
$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$
$q-2$	$q-2$	0	1	$\cdots$	$q-3$