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。

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

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

となることを言うのである。

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

証明.

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

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 $\exists y \in K^\times$, $y \notin \{1, x, x^2, \ldots, x^{n-1}\}$ となる。このとき

$$\{1, x, x^2, \ldots, x^{n-1}\} \cup \{y, xy, x^2y, \ldots, x^{n-1}y\} \subseteq K^\times.$$

この操作を繰り返すと、$\exists y_1, \ldots, y_m \in K^\times$,

$$\bigcup_{j=1}^{m} \{y_j, xy_j, x^2y_j, \ldots, x^{n-1}y_j\} = K^\times \quad \text{(disjoint)}$$

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

証明. 明らかに、$n|m$ ならば $x^m = 1$ である。逆に $x^m = 1$ とすると、m を n で割って $m = ns + r$, $0 \leq r < n$ とすると、$1 = x^m = (x^n)^q x^r = x^r$ 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. *$\forall n \in \mathbb{N}$, $n|q-1 \implies |\{x \mid x \in K^\times,\ x^n = 1\}| = n$.*

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、

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

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

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

□

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

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

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、

$$\begin{aligned} &\sum_{\substack{d \in \mathbb{N} \\ d|n}} \varphi(d) = n && \text{(補題 4 より)} \\ &= |\{x \mid x \in K^\times,\ x^n = 1\}| && \text{(補題 3 より)} \end{aligned}$$

$$= \sum_{\substack{d\in\mathbb{N}\\ d|n}} \alpha(d) \qquad \text{(補題 2 より)}$$

$$= \sum_{\substack{d\in\mathbb{N}\\ d|n\\ d\neq n}} \alpha(d) + \alpha(n)$$

$$= \sum_{\substack{d\in\mathbb{N}\\ d|n\\ d\neq n}} \varphi(d) + \alpha(n) \qquad \text{(帰納法の仮定より).}$$

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	$\cdots$	$q-3$