2008年7月4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。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 の位数は有限でしかもそれは $q-1$ の約数である。実際、x の位数を n とすると、

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

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、この逆も成り立つ。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 1. $x \in K^\times$ の位数が n とすると、$m \in \mathbf{N}$ に対して、$x^m = 1 \iff n|m$ である。

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 $m = ns + r$, $0 \le r < n$ 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。 □

補題 2. $\forall n \in \mathbf{N}$, $n|q-1 \implies |\{x \mid x \in K^\times,\ x^n = 1\}| = n$.

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1 より、

$$X^{q-1} - 1 = \prod_{x \in K^\times} (X - x)$$

となるので、

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

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 3. $\forall n \in \mathbf{N}$

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

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

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

よって $\varphi(n) = \alpha(n)$ を得る。 □

例えば、$\mathbf{Z}/13\mathbf{Z}$ 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	$\cdots$	$q-3$

群

集合 G に演算 $*: G \times G \to G$ が定義されていて、次の性質を満たすとき、$(G, *)$ は群であるという。

(1) $\forall a, b, c \in G,\ (a * b) * c = a * (b * c)$ （結合法則）

(2) $\exists e \in G,\ \forall a \in G,\ a * e = e * a = a$ （単位元の存在）

(3) $\forall a \in G,\ \exists b \in G,\ a * b = b * a = e$ （逆元の存在）

もし $*$ を指定しなくても他の演算と混乱することがないときは、単に G は群であるという。e を 1 または 0 と書くこともある。上の b は a^{-1} または $-a$ と書くことがある。

任意の環 A は、その加法 $+$ に関して群になる。体 K に対して、$K^\times$ は乗法に関して群になる。実数を成分とする n 次正則行列全体は行列の積に関して群になる。

二つの群 $(G_1, *_1)$, $(G_2, *_2)$ に対して、全単射 $f: G_1 \to G_2$ が存在して $\forall x, y \in G_1$, $f(x *_1 y) = f(x) *_2 f(y)$ が成り立つとき、G_1 と G_2 は同型であるといい、$G_1 \cong G_2$ と書く。例えば $(\mathbf{Z}/3\mathbf{Z}[x])/(x^2+1), \times) \cong (\mathbf{Z}/8\mathbf{Z}, +)$, $(\mathbf{R}_{>0}, \times) \cong (\mathbf{R}, +)$ である。

群 G に対して、$\exists a \in G,\ G = \{a^n \mid n \in \mathbf{Z}\}$ が成り立つとき、G は巡回群であるという。ここで、

$$a^n = \begin{cases} a * a * \cdots * a \quad (n \text{ 個}) & (n \in \mathbf{N}) \\ e & (n = 0) \\ a^{-1} * a^{-1} * \cdots * a^{-1} \quad (n \text{ 個}) & (-n \in \mathbf{N}) \end{cases}$$

このとき指数法則が成り立つ。定理 1 より、任意の有限体 K に対して $K^\times$ は巡回群である。任意の $m \in \mathbf{N}$ に対して、$(\mathbf{Z}/m\mathbf{Z}, +)$ は巡回群である。有限巡回群の乗積表は上図のようになる。$(\mathbf{Z}, +)$ は巡回群であるが、$(\mathbf{Q}, +)$ は巡回群ではない。任意の無限巡回群は $(\mathbf{Z}, +)$ と同型である。

前回までに講義済みの内容

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）

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。オイラーの関数とは

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

で定義される関数 $\varphi : \mathbf{N} \to \mathbf{N}$ のことである。