2008年7月11日

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）

上の b は a^{-1} または $-a$ と書くことがある。

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。

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。無限巡回群は $\mathbf{Z}$ と同型である。位数 m の巡回群は $\mathbf{Z}/m\mathbf{Z}$ と同型である。

G を群とし、その単位元を 1 と書くことにする。$x \in G$ に対し、

$$\min\{n \mid n \in \mathbf{N},\ x^n = 1\}$$

を、元 x の位数という。ただし $\{n \mid n \in \mathbf{N},\ x^n = 1\} = \emptyset$ のときは位数無限という。K が体ならば、$K^\times$ は群になるので、すでに定義済みの $x \in K^\times$ の位数と上の定義は一致する。

群 G が有限集合のとき有限群という。$K^\times$ の場合と全く同様にして、$x \in G$ の位数は $|G|$ の約数であることがわかる。

$n \in \mathbf{N}$ とし、n 個の元からなる集合（例えば $X = \{1, 2, \ldots, n\}$）からそれ自身への全単射全体のなす集合を n 次対称群といい、S_n で表す。S_n は写像の合成に関して群をなす。単位元は恒等写像、逆元は逆写像である。恒等写像というのは、

$$\mathrm{id}(1) = 1, \quad \mathrm{id}(2) = 2, \ldots, \mathrm{id}(n) = n$$

で定義される X から X への写像である。一般には $|S_n| = n!$ である。例えば、$n = 3$, $X = \{1, 2, 3\}$ とすると、

$$f(1) = 2, \quad f(2) = 3, \quad f(3) = 1,$$
$$g(1) = 2, \quad g(2) = 1, \quad g(3) = 3$$

などが S_3 の元である。これらは順列と考えても良く、省略してそれぞれ 231, 213 と書くこともできる。写像の合成 $f \circ g$ とは $f \circ g(x) = f(g(x))$ によって定義される写像である。上記の f, g に対しては

$$f \circ g(1) = 3, \quad f \circ g(2) = 2, \quad f \circ g(3) = 1$$

となる。一般に、f, g が全単射ならば、$f \circ g$ も全単射である。したがって $\circ$ は S_n における演算となり、この演算に関して S_n は群になる。

S_n は線形代数学で習ったはず：$A = (a_{ij})$ を n 次正方行列とすると

$$\det A = \sum_{f \in S_n} \mathrm{sgn}(f) \prod_{i=1}^{n} a_{i,f(i)}$$

と表される。ここで

$$\mathrm{sgn}(f) = (-1)^{|\{(i,j)|i\in X,\, j\in X,\, i<j,\, f(i)>f(j)\}|}.$$

K を体とすると、K の元を成分とする n 次正方行列に、通常の行列の積を定義することができる。K が体であることから、K の元を成分とする行列の積は結合法則をみたし、K の単位元、零元から単位行列を作ることができる。また、K が体であることから、行列式の定義、それによる逆行列の公式が成り立つ。逆行列を持つ行列を正則行列といい、K の元を成分とする n 次正則行列全体の集合を $GL(n, K)$ と書く。$GL(n, K)$ は行列の積に関して群になる。

例えば、$n = 2$, $K = \mathbf{Z}/2\mathbf{Z}$ とすると

$$GL(2, \mathbf{Z}/2\mathbf{Z}) = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \right\}.$$

S_3 も $GL(2, \mathbf{Z}/2\mathbf{Z})$ も位数 6 の元を持たないので、$\mathbf{Z}/6\mathbf{Z}$ とは同型でない。

前回までに講義済みの内容

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	$\cdots$	$q-3$