情報数学Ⅰ

第７回「代数構造-群、置換群」

3. 代数構造（群、環、体)

要素間にある一定の公理を満たす演算が定義されている集合を代数構造といい、群、環、体がある。

[集合上に演算が定義できるとは？]

$Z=\{1,i,-1,-i\}$上の演算を考える。ここで$i=\sqrt{-1}$である。

$\forall x,y\in Z$に対して

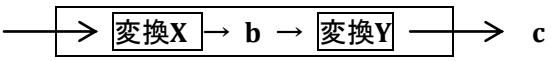
[加法] $x+y\notin Z$であるから、加法は定義できない

[減法] $x-y\notin Z$であるから、減法は定義できない

[乗法] $x\cdot y\in Z$であるから、乗法は定義できる

[除法] $x/y\in Z$であるから、除法は定義できる

[演算とは?]



変換の合成

$$\left.\begin{matrix}\mathbf{b}=\mathbf{X}\cdot\mathbf{a}\\ \mathbf{c}=\mathbf{Y}\cdot\mathbf{b}\end{matrix}\right\}\mathbf{c}=\mathbf{Y}\cdot\mathbf{X}\cdot\mathbf{a}=\mathbf{Z}\cdot\mathbf{a}$$

$$\mathbf{Z}=\mathbf{Y}\cdot\mathbf{X}$$

(意味) 変換**X**を施した後に変換**Y**を施したときの変換の合成は$\mathbf{Y}\cdot\mathbf{X}$となる。変換の合成$\cdot$は演算である。

3-1　群 (group)

(keywords)

① 群

　集合G上に１種類の２項演算$\cdot$が定義され、次の４つの条件を満たすならば、集合Gは演算$\cdot$に関して群であるという。

(1) 集合Gは演算に関して閉じている。

$\forall x,y\in G$に対して、$x\cdot y\in G$が成り立つとき、Gは２項演算$\cdot$に関して閉じている、という。

(2) 結合律を満たす。
$\forall x, y, z \in G$に対して、$(x \cdot y) \cdot z = x \cdot (y \cdot z)$が成り立つ。

(3) 単位元が存在する
$\forall x \in G$に対して、$x \cdot e = e \cdot x = x$を満たす単位元$e$が$G$に含まれる。すなわち、$e \in G$である。

(4) 逆元が存在する。
$\forall x \in G$に対して、$x \cdot y = y \cdot x = e$(単位元)となる$x$の逆元$y$が$G$に含まれる。

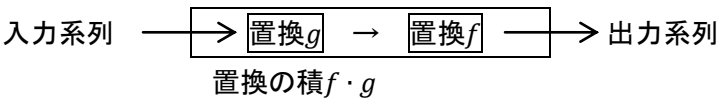
§置換群 (permutation group)
<keywords>
① 置換 (permutation)
自然数の有限集合$E = \{1,2,3,\cdots,n\}$からそれ自身E上への全単射、すなわち、1 対 1 写像fを置換といい、$f = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ f(1) & f(2) & f(3) & \cdots & f(n) \end{pmatrix}$で表す。ただし、$f(i) \neq f(j)$ $(i \neq j)$

(例)

入力 (a b c d e) → 置換 $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix}$ 出力 →(d a e b c)

置換とは記号列の記号の順序を並びかえる操作のことである。符号理論ではこの置換のことをインターリーブといい、アルゴリズムではこの置換のことをシャッフリングという。

② 置換の積
2 つの置換fとgの積$f \cdot g$を、iを$f(g(i))$ $(i = 1,2,\cdots,n)$に対応させる置換であるとする。すなわち、$f \cdot g$は置換gを施した後、置換fを施すことに等しい。



(例)

(a b c d e) → $g=\begin{pmatrix}1&2&3&4&5\\2&4&5&1&3\end{pmatrix}$ →(d a e b c)

→ $f=\begin{pmatrix}1&2&3&4&5\\5&3&1&2&4\end{pmatrix}$ →(e b a c d)

$$f\cdot g=\begin{pmatrix}1&2&3&4&5\\5&3&1&2&4\end{pmatrix}\begin{pmatrix}1&2&3&4&5\\2&4&5&1&3\end{pmatrix}=\begin{pmatrix}1&2&3&4&5\\3&2&4&5&1\end{pmatrix}$$

$$g\cdot f=\begin{pmatrix}1&2&3&4&5\\2&4&5&1&3\end{pmatrix}\cdot\begin{pmatrix}1&2&3&4&5\\5&3&1&2&4\end{pmatrix}=\begin{pmatrix}1&2&3&4&5\\3&5&2&4&1\end{pmatrix}$$

[定理] 一般に置換の積$\cdot$は交換律を満たさない。すなわち、$f\cdot g\neq g\cdot f$が成り立つ。

③ 置換群

集合$E=\{1,2,3,\cdots,n\}$上の置換全体は、$n!$個ある。この置換の集合をS_nとすると、S_nは積$\cdot$に関して群となる。これをn次対称群という。($|S_n|=n!$である)

置換群

(例) 3 次対称群

$E=\{1,2,3\}$上の置換全体の集合$S_3=\{e,r,s,t,u,v\}$が積に関して群をなすことを示せ。

ただし、$e=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$, $r=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$, $s=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$,

$t=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$, $u=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$, $v=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$

(解) 群の 4 つの条件を満たすことを示せばよい。

$x\setminus y$	e	r	s	t	u	v
e	e	r	s	t	u	v
r	r	e	v	u	t	s
s	s	t	u	v	e	r
t	t	s	r	e	v	u
u	u	v	e	r	s	t
v	v	u	t	s	r	e

(1) $\forall x,y\in S_3$に対して、$x\cdot y\in S_3$

(2) いま、$f(i),g(i),h(i)\in\{1,2,3\}$ $(i=1,2,3)$を考える。ここで、$f(i)\neq f(j)$ $(i\neq j)$、$g(i)\neq g(j)$ $(i\neq j)$、$h(i)\neq h(j)$ $(i\neq j)$である。

$$\left(\begin{pmatrix}1 & 2 & 3\\ f(1) & f(2) & f(3)\end{pmatrix}\cdot\begin{pmatrix}1 & 2 & 3\\ g(1) & g(2) & g(3)\end{pmatrix}\right)\cdot\begin{pmatrix}1 & 2 & 3\\ h(1) & h(2) & h(3)\end{pmatrix}$$

$$=\begin{pmatrix}1 & 2 & 3\\ f(g(1)) & f(g(2)) & f(g(3))\end{pmatrix}\cdot\begin{pmatrix}1 & 2 & 3\\ h(1) & h(2) & h(3)\end{pmatrix}$$

$$=\begin{pmatrix}1 & 2 & 3\\ f\left(g(h(1))\right) & f\left(g(h(2))\right) & f\left(g(h(3))\right)\end{pmatrix}\quad\cdots(1)$$

$$\begin{pmatrix}1 & 2 & 3\\ f(1) & f(2) & f(3)\end{pmatrix}\cdot\left(\begin{pmatrix}1 & 2 & 3\\ g(1) & g(2) & g(3)\end{pmatrix}\cdot\begin{pmatrix}1 & 2 & 3\\ h(1) & h(2) & h(3)\end{pmatrix}\right)$$

$$=\begin{pmatrix}1 & 2 & 3\\ f(1) & f(2) & f(3)\end{pmatrix}\cdot\begin{pmatrix}1 & 2 & 3\\ g(h(1)) & g(h(2)) & g(h(3))\end{pmatrix}$$

$$=\begin{pmatrix}1 & 2 & 3\\ f\left(g(h(1))\right) & f\left(g(h(2))\right) & f\left(g(h(3))\right)\end{pmatrix}\quad\cdots(2)$$

(1)(2)より、積に関して結合律を満たす。

(3) 単位元$e \in S_3$である。

(4) $\forall x \in S_3$に対して、その逆元$x^{-1} \in S_3$である。
$e\cdot e=e,\ r\cdot r=e,\ s\cdot u=e,\ t\cdot t=e, u\cdot s=e, v\cdot v=e$であるので、
$e^{-1}=e, r^{-1}=r, s^{-1}=u, t^{-1}=t, u^{-1}=s, v^{-1}=v$である。

よって、S_3は積に関して、(1),(2),(3),(4)の 4 つの群であるための条件を満たすので、群である。