代数学 IA NO.7 要約

今日のテーマ: **置換群 ・ 整数の加法群**

置換

$$a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

は、$1,2,3,4$ がそれぞれ《変身》して $2,3,4,1$ になると言う操作であって、これを、

$$a(1) = 2, a(2) = 3, a(3) = 4, a(4) = 1$$

というようにも書く。

二つの置換の結合 (演算) は通常《後ろから読》む。たとえば、

$$a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \quad b = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$$

の掛け算 ab は、

$$ab = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix}$$

つまり、例えば 1 は b で 3 に化けて、次に a で 3 は 4 に化けるので、結果として 1 は ab によって 4 に化けることになる。

いくつかの元 $\{a_1, a_2, \ldots, a_r\}$ を順繰りに変える置換、すなわち

$$\begin{pmatrix} a_1 & a_2 & \ldots & a_{r-1} & a_r \\ a_2 & a_3 & \ldots & a_r & 1 \end{pmatrix}$$

のことを**巡回置換**と呼び、$(a_1, a_2, \ldots a_r)$ と書き表す。

定義 7.1. 集合 S が与えられたとする。このとき S から S への全単射の全体は写像の合成に関して群をなす。これを S 上の**対称群**と言う。有限集合上の対称群を有限対称群と呼ぶ。n 個の元からなる集合 $\{1, 2, \ldots, n\}$ の上の対称群を、n **次の対称群**と呼び、$\mathfrak{S}_n$ で書き表す。

要は、n 個の元 $1, \ldots, n$ の置換全体のなす群が n 次の対称群である。

定理 7.2. n 次の対称群の位数は $n!$ である。

定義 7.3. 対称群 $\mathfrak{S}_n$ の部分群のことを**置換群**という。

任意の置換は互いに同じ文字を含まない巡回置換の積として表すことができる。例えば、置換

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 5 & 7 & 6 & 2 & 1 & 8 & 9 & 3 \end{pmatrix}$$

をよくみてみると、次のような変身の様子が分かる。

$$3 \overset{\sigma}{\mapsto} 7 \overset{\sigma}{\mapsto} 8 \overset{\sigma}{\mapsto} 9 \overset{\sigma}{\mapsto} 3 \qquad 1 \overset{\sigma}{\mapsto} 4 \overset{\sigma}{\mapsto} 6 \overset{\sigma}{\mapsto} 1 \qquad 2 \overset{\sigma}{\mapsto} 5 \overset{\sigma}{\mapsto} 2$$

したがって、

$$\sigma = (3\ 7\ 8\ 9)(1\ 4\ 6)(2\ 5)$$

であることが分かる。

置換の概念および記号は、$\{1, 2, 3 \ldots, n\}$ のような集合だけではなく、他の集合でも使える。

たとえば、$\mu_n(\mathbb{C})$ の元を一斉に $\{\zeta_n\}$ 倍することは

$$(1\ \zeta\ \zeta^2\ \zeta^3\ \ldots \zeta^{n-1})$$

なる置換に対応する。

$(\mathbb{Z}, +)$ は可換群なのであった。演算としては加法 $+$ を用いる。$(\mathbb{Z}, +)$ に対してももちろん群の一般論が使える。ただし、記法に関しては注意が必要である。

補題 7.4. 任意の $n \in Z_{\leq 0}$ に対し、 $n\mathbb{Z}$ は $(\mathbb{Z}, +)$ の部分群であり、逆に、$(\mathbb{Z}, +)$ の部分群はこのようにして得られるものに限る。

$\mathbb{Z}$ の部分集合 $n\mathbb{Z}$ を考えよう。話を見えやすくするために $n = 12$ とし、$\mathbb{Z} \subset 12\mathbb{Z}$ を考える。群の一般論により、剰余集合 $\mathbb{Z}/12\mathbb{Z}$ が存在する。それは、

$$a \equiv b \Leftrightarrow a - b \in 12\mathbb{Z}$$

により整数を類別したものである。

12 を法とした剰余類というのを高校で習った人もいるかもしれない。それらの人にとっては、$a \equiv_{12\mathbb{Z}} b$ というのは $a \equiv b \pmod{12}$ と同義である。

$\mu_{12}(\mathbb{C})$ と $\mathbb{Z}/12\mathbb{Z}$ の間に

$$\zeta^k \leftrightarrow [k] \qquad (k \text{ のクラス})$$

という一対一対応があることにも注意しておこう。