代数学 IA NO.3 要約

群とは操作の集まりでした。演算が定義されるということ、(つまり、演算について閉じていること)、「何もしない」という操作、各操作の逆操作がその集まりに含まれるという事が大事なのでした。

今日のテーマ 《有限群》

- 元の数が有限であるような群を、有限群と言う。
- 群 G の元の個数を、G の位数と言い、$|G|$ で表す。

有限群の重要な例として、有限対称群、有限巡回群、二面体群がある。

置換

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

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

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

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 3.1. 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**と呼ぶ。

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 3.1. n 次の対称群の位数は $n!$ である。

「一つの元から生成されていて、元の数が有限である巡回群を、有限巡回群という」というのが正統的な定義なのだが、ここでは「生成する」の定義を後回しにして、つぎのような間に合わせな的な定義をしておくことにする。

定義 3.2. $\mathfrak{S}_n$ の元 a を $a = (1\ 2\ \ldots\ n-1\ n)$ で定義する。このとき、

$$C_n = \{e, a, a^2, a^3, a^4, \ldots, a^{-1}, a^{-2}, \ldots\}$$

を位数 n の有限巡回群と呼ぶ。

注意

上の元 a について、

$$a(k) = \begin{cases} k+1 & (k \neq n \text{ のとき}) \\ 1 & (k = n \text{ のとき}) \end{cases}$$

と書ける。だが、場合分けをするより、もっと楽な方法がある。n を決めておいて、$1 \leq k \leq n$ の範囲では、k のかわりに $[k]$ という記号を導入する。(どの n を考えて

いるかはっきりさせたい時には $[k]_n$ と書くこともある。) つぎに、一般の整数について、順繰りに、

$$[n+1]=[1],[n+2]=[2],[n+3]=[3],\dots,$$
$$[0]=[n],[-1]=[n-1],[-2]=[n-2],\dots$$

等と約束する。例えば、$n=13$ ならば、

$$[14]=[1],[15]=[2],[16]=[3],\dots,$$
$$[0]=[13],[-1]=[12],[-2]=[10],\dots,$$
$$[128]=[10],[-128]=[2],\text{etc}$$

$[k]=[l]$ かどうかは、 $k-l$ が n で割り切れるかどうかで判断できることに注意しておこう。

以上のようにしておいて、C_n は $\{[1],[2],[3],\dots,[n]\}$ の置換だとみなすと、

$$a([k])=[k+1]$$

と書ける。これは以後の定理の証明に非常に有効である。

定理 3.2. 上の C_n を考え、$a=(1\ 2\ \dots\ n-1\ n)$ とおく。このとき、

(1) $a^n=e$ である。*(e は恒等置換)*

(2) 整数 k,l に対して、
$$a^k=a^l$$
が成り立つということと、$k-l$ は n の倍数であるということとは、同値である。

(3) C_n の位数は n である。

正 n 角形をそれ自身に重ねあわせる操作のなす群を二面体群と言う。これをここでは次のように導入する。

定義 3.3. n は 3 以上の整数であるとする。

$\mathfrak{S}_n$ のなかで、$a=(1\ 2\ \dots\ n-1\ n)$ と、

$$b=\begin{pmatrix}1 & 2 & 3 & \dots & n-1 & n\\ n & n-1 & n-2 & \dots & 2 & 1\end{pmatrix}$$

とで生成された群を $\mathbb{D}_n$ と書き、二面体群と言う。

注意

等式
$$b(k)=n-k+1$$
が成り立つ。さらに、 先ほど述べた $[k]$ という記号を用いると、
$$b([k])=[-k+1]$$
が成り立つ。

定理 3.3.

(1) 等式 $a^n=e,b^2=e,bab^{-1}=a^{-1}$ が成り立つ。

(2) $a^kba^l=a^{k-l}b$ が全ての整数 k,l について成り立つ。

(3) $\mathbb{D}_n$ の元は
$$e,a,a^2,a^3,\dots,a^{n-1},b,ab,a^2b,a^3b,\dots,a^{n-1}b$$
の $2n$ 個ある。特に、$\mathbb{D}_n$ の位数は $2n$ である。

※レポート問題

次の中から一問を選んで、レポートとして提出しなさい。

(期限：次の講義の終了時まで。)

(I) $a^k(b(a^l([x])))$ および $a^{k-l}(b([x]))$ を計算することにより、定理 5.3 の 2. を証明しなさい。