

代数学 IA NO.4 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 (続き)》

- 元の数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。

「一つの元から生成されていて、元の数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的な定義をしておくことにする。

定義 4.1. C_n の元 a を $a = (1\ 2\ \dots\ n-1\ n)$ で定義する。このとき、

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

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。) つぎに、一般の整数について、順繰りに、

$$\begin{aligned} [n+1] &= [1], [n+2] = [2], [n+3] = [3], \dots, \\ [0] &= [n], [-1] = [n-1], [-2] = [n-2], \dots \end{aligned}$$

等と約束する。例えば、 $n = 13$ ならば、

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

$[k] = [l]$ 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 4.1. 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 4.2. n は 3 以上の整数であるとする。

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 4.2.

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