巡回群
Cyclic Group

定義 1 群 G において，元の指数について次のように定義する．$n \in \boldsymbol{N}$

$$a^n = \overbrace{aaa\cdots a}^{n\text{ 個}}$$
$$a^0 = e$$
$$a^{-n} = (a^n)^{-1}$$

定理 1 群 G において，任意の整数 m, n に対し，指数法則が成り立つ．

$$(a^n)^{-1} = (a^{-1})^n$$
$$a^m a^n = a^{m+n}$$
$$(a^m)^n = a^{mn}$$

［証明略］

定義 2 群 G が G のある元 a を用いて

$$G = \{a^n \mid n \in \boldsymbol{Z}\}$$

と表せるとき，G を**巡回群**と呼ぶ．また a を G の**生成元**と呼び，

$$G = \langle a \rangle$$

と表す．

G の元を並べて書けば，

$$G = \{\cdots, a^{-2}, a^{-1}, e, a, a^2, \cdots\}$$

ということであるが，これらの元が全て異なるとは限らない．同じ元が多数あって，重複しないように並べたとき G の元が有限個となる場合もある．このような群を**有限巡回群**と呼び，それに対して元の個数が無限個（可付番無限個）であるものを**無限巡回群**と呼ぶ．また生成元は一つとは限らない．

定理 2 G が有限巡回群ならば，$\exists n \in \boldsymbol{N}$ を用いて

$$G = \{e, a, a^2, \cdots, a^{n-1}\}$$

と表せる．

［証明］巡回群の元のうち同じ元があるとする．その二つの元を a^i, a^j $(i > j)$ とする．

$$a^i = a^j$$

の右から a^{-j} をかけると，

$$a^i a^{-j} = a^j a^{-j}$$
$$a^{i-j} = e$$

つまり $a^k = e$ $(\exists k \in \boldsymbol{N})$ となる．このような k のうちで最小の自然数を n とすると，

$$e, a, a^2, \cdots, a^{n-1} \tag{1}$$

は全て異なる．なぜならば，もしこの中に同じものがあれば，$a^k = e$ となる最小の k が n であることと矛盾するからである．

さらに $\forall b \in G$ について

$$b = a^r \ (\exists r \in \boldsymbol{N}, 0 \leq r \leq n-1)$$

と表せる，なぜならば

$$b = a^m = a^{qn+r} = a^r$$

となるからである．つまり m を n で割った余りを r とすると，$0 \leq r \leq n-1$ となるのがその理由である．よって G の元は (1) が全てである． ［証明おわり］

定理 3 G が無限巡回群ならば

$$G = \{\cdots, a^{-2}, a^{-1}, e, a, a^2, \cdots\} \tag{2}$$

であり，これらの元は全て異なる．

［証明］仮に同じ元が一組でもあれば，それは前定理の証明の過程から明らかなように有限巡回群となるので，矛盾する．よって，(2) で表される G の元は全て異なる． ［証明おわり］

例 1 $G = \{1, -1\}$ は乗法について -1 を生成元とする有限巡回群である．つまり $G = \langle -1 \rangle$

例 2 $G = \{1, -1, i, -i\}$ は乗法について $i, -i$ を生成元とする有限巡回群である．つまり $G = \langle i \rangle = \langle -i \rangle$

参考文献

[1] 「ウィキペディア」<http://ja.wikipedia.org/wiki/>

[2] 「Wikipedia」<http://en.wikipedia.org/wiki/>

[3] 石村園子『すぐわかる代数』（東京図書，2003 年）