§3. 巡回群

定義　群 G が有限集合からなるとき，G を有限群といい，そうでないとき**無限群**という．群 G が有限群であるとき，その元の個数を G の**位数**という．無限群 G に対してもその濃度を G の位数ということがある．

定義　群 G の元 x に対して，$x^n = e$ をみたす最小の $n \in \mathbb{N}$ が存在するとき，それを x の**位数**という．

命題 3.1　群 G の元 x の位数が n であるとする．

(1) n 個の元　$e, x, x^2, \cdots, x^{n-1}$　はどの二つも相異なる．

(2) 自然数 m について，$x^m = e$ ならば $n|m$ である．

定義　G を群とする．ある $g \in G$ が存在して，任意の $x \in G$ に対して $x = g^n$ をみたす $n \in \mathbb{Z}$ がとれるとき，G を**巡回群**という．すなわち，G が巡回群であるとは，

$$G = \{\ g^n \mid n \in \mathbb{Z}\ \}$$

をみたす g が存在することである（このような g を巡回群 G の生成元という）．

定理 3.2　巡回群はアーベル群である．また，巡回群の部分群は巡回群である．

定理 3.3　G を位数 n の有限群とするとき，次の (i), (ii) は同値である．

(i) G は巡回群である．

(ii) G は位数 n の元をもつ．

系 3.4　群 G の元 g に対して，次の (i), (ii) は同値である．

(i) $\left\{\, g^k \,|\, k \in \mathbb{Z} \,\right\}$ は位数 n の部分群である．

(ii) g の位数は n である．

定理 3.5　G を位数 n の巡回群とする．

(1) G の任意の元について，その位数は n の約数である．

(2) G の任意の部分群について，その位数は n の約数である．

(3) n の任意の正の約数 m に対して，G は位数 m の元をもつ．

(4) n の任意の正の約数 m に対して，G は位数 m の部分群をもつ．

定理 3.6　前定理 (4) の部分群は，各 m に対して一意的に定まる．