2119116s 佐野海徳

HW51

巡回群 G の生成元を a, 単位元を 1 で表す。G の部分群を H と書く。H の元はすべて生成元のべき $a^i(i \in \mathbb{Z})$ で書ける。a = 1, つまり G が単位元だけでなる群のときは自明。また、H が単位元 1 のみからなる G の部分群であるとき、H は巡回群。$a \neq 1$ として H は単位元 1 の他にも元を持つとすると、$S = \{i \in \mathbb{Z} | i > 0 \& a^i \in H\}$ となる集合 S を考える。H についての仮定と $a^{-i} \in H \Leftrightarrow a^i \in H$ から $S \neq \emptyset$ がわかる。したがって S は最小元 m をもつ。このとき $H =< a^m >$ が成り立つ。このとき $< a^m > \subseteq H$ は明らか。逆に $a^n(n \in \mathbb{Z})$ とする。n を m で割ると $n = mq + r$ となるある整数の組 m,r0 $\leq r < m$ が一意的に存在し、$a^r = a^n a^{-mq}$ inH。m の最小性により r = 0, 故に n = mq。これより $a^n = a^{mq} \in < a^m >$。よって $H \subseteq < a^m >$。