群論

Lexington Whalen

January 2023

1　巡回群

1.1　巡回群の部分群はまた巡回群になる。

Gを元gによって生成された巡回群とし、HをGの任意の部分群とする。

もし$H = \langle e \rangle$であれば、Hは元eによって生成された巡回群となるので、この場合では主張は正しい。

$H \neq \langle e \rangle$の場合を考えましょう。その時、Hの任意の元ｈを取り、そのｈを$h = g^k$と表すことができる。ここでkを$h = g^k \in H$となる最小の自然数とする。我々が目指しているのは$\langle g^k \rangle = H$であることを証明すること。

Hは群なので、$\langle a^k \rangle \subset H$である。次に、Hの任意の元$b = g^i$を取る。割り算の定義により、

$$i = kq + r, 0 \leq r < m, q, r \in \mathbb{Z}$$

となる。これを踏まえて、次のように書くこともできる：

$$a^i = a^{kq+r}, a^r = a^i \times (a^k)^{-q}$$

ここでｋはa^kとなる最小の自然数であったので、$r = 0$が言える。
よって、$\langle a^k \rangle = H$となる。

■