定義

アーベル群

ある群の演算が可換である時、その群を可換群またはアーベル群という。

巡回群

G を群とし、$g \in G$ に対し、g^n $(n \in \mathbb{Z})$ となるもののみで構成される群を巡回群という。

巡回群はアーベル群であることを示せ。

.....

巡回群 G の任意の元は g^n $(g \in \mathbb{Z})$ とかける。これは次の式を省略して書いたものである。$\circ$ は演算を表している。

$$g^n = g \circ g \circ g \circ \cdots \circ g \quad (n\text{個の積}) \tag{1}$$

ここで、2 つの元 $g^n,\ g^m$ $(n, m \in \mathbb{Z})$ の演算を考える。

$$\begin{aligned}
g^n \circ g^m =& (g \circ g \circ g \circ \cdots \circ g) \circ (g \circ g \circ g \circ \cdots \circ g) && n\text{個と}m\text{個の積} && (2)\\
=& g \circ g \circ g \circ \cdots \circ g \circ g \circ g \circ g \circ \cdots \circ g && n+m\text{個の積} && (3)\\
=& (g \circ g \circ g \circ \cdots \circ g) \circ (g \circ g \circ g \circ \cdots \circ g) && m\text{個と}n\text{個の積} && (4)\\
=& g^m \circ g^n && && (5)
\end{aligned}$$

よって、$g^n \circ g^m = g^m \circ g^n$ より巡回群はアーベル群である。
