

**定理 2.17**  $\langle G, * \rangle$  を群とする。 $\langle G, * \rangle$  が可換群である必要十分条件は任意の要素  $a, b \in G$  に対して、 $(a * b) * (a * b) = (a * a) * (b * b)$  が成り立つことである。

【証明】

“ $\Rightarrow$ ” :  $\langle G, * \rangle$  は可換群であるとする。 $G$  の任意の要素  $a$  と  $b$  に対して、

$$\begin{aligned} a * b &= b * a \text{ から, } (a * b) * (a * b) = a * (b * a) * b \\ &= a * (a * b) * b \\ &= (a * a) * (b * b) \end{aligned}$$

が成り立つ。

“ $\Leftarrow$ ” :  $G$  の任意の要素  $a$  と  $b$  に対して、 $(a * b) * (a * b) = (a * a) * (b * b)$  より、

$$\begin{aligned} a * b &= (a^{-1} * a) * (a * b) * (b * b^{-1}) \\ &= a^{-1} * ((a * a) * (b * b)) * b^{-1} \\ &= a^{-1} * ((a * b) * (a * b)) * b^{-1} \\ &= (a^{-1} * a) * (b * a) * (b * b^{-1}) \\ &= b * a \end{aligned}$$

すなわち、 $*$  は可換演算である。ゆえに、 $\langle G, * \rangle$  が可換群である。