Satz Sei $(G, \cdot, e)$ endliche Gruppe und U eine nichtleere, in G enthaltene Menge. Dann gilt:

$$(\forall a, b \in U: \;\; a \cdot b \in U) \quad \to \quad U \leq G.$$

Beweis

(1) Zu zeigen: $e \in U$

$U \neq \emptyset \quad \to \quad \exists\, a \in U \overset{Voraussetzung}{\to} \forall\, k \in \mathbb{N} : a^k \in U$

Da G endlich $\quad \to \quad$ U endlich $\quad \to \quad \exists\, k_1, k_2 \in \mathbb{N}$ mit $k_1 < k_2$ und $\quad a^{k_1} = a^{k_2}$

G ist Gruppe $\quad \to \quad (a^{k_1})^{-1} \in G$ und $(a^{k_1})^{-1} = a^{-k_1}$

$\to \quad e = a^{k_1} \cdot a^{-k_1} = a^{k_2} \cdot a^{-k_1} = a^{k_2 - k_1} \in U$ da $k_2 - k_1 \in \mathbb{N}$

(2) Zu zeigen: $a \in U \quad \to \quad a^{-1} \in U$

Sei $a \in U$ mit $a^{k_1} = a^{k_2}, \quad k_1 < k_2$

1.Fall: $k_2 = k_1 + 1$

$\to \quad e = a^{k_2 - k_1} = a^1 = a \quad \to \quad a^{-1} \in U$

2.Fall: $k_2 > k_1 + 1$, d.h. $k_2 - k_1 - 1 \in \mathbb{N}$

$\to \quad a^{k_2 - k_1 - 1} \in U$

$a^{k_2 - k_1 - 1} \cdot a = a^{k_2 - k_1} = e$

$\Rightarrow \quad a^{-1} = a^{k_2 - k_1 - 1} \in U$

$\square$