Grupy

Definition

Zbiór G, w którym określone jest działanie $\circ$, nazywamy **grupą**, jeśli spełnione są warunki:

1. działanie $\circ$ jest *łączne*
2. istnieje *element neutralny*
3. dla każdego elementu, istnieje element do niego *odwrotny*

Własność skracania

Niech $(G, \circ)$, oraz $a, b, x, y \in G$, wtedy:

$$\begin{aligned} ax = ay &\implies x = y \quad \text{lewostronna własność skracania} \\ xb = yb &\implies x = y \quad \text{prawostronna własność skracania} \end{aligned}$$

Lemma

Niech $(S, \circ)$ będzie półgrupą, wtedy:

$$(S, \circ) \text{ is a group} \iff \forall a, b \in S \; \exists x, y \in S : ax = b, \; ya = b$$

Proof

$$\begin{aligned} (\Rightarrow) \quad & \text{Załóżmy że } (S, \circ) \text{ jest grupą.} \\ & \text{Dla danych } a, b \in S \text{ oznaczmy} \\ & x = a^{-1}b, \; y = ba^{-1} \end{aligned}$$

$$\begin{aligned} (\Leftarrow) \quad & \text{Dla danego } a \in S \; \exists x, y \in S : ax = a \wedge ya = a \\ & e := y : ea = a \\ & b \in S \implies \hat{x} \in S : a\hat{x} = b \\ & eb = e(a\hat{x}) = (ea)\hat{x} = a\hat{x} = b \implies e \text{ jest lewostronnie neutralne} \\ & \text{Dla danego } b \in S, \; \exists \hat{y} \in S : \hat{y}b = e \implies b \text{ jest lewostronnie odwraca} \end{aligned}$$

Theorem

Jeśli $(S, \circ)$ jest półgrupą i $\operatorname{ord}(S) < \infty$, to:

$$(S, \circ) \text{ jest grupą} \iff \text{obydwie własności skarcania są dla niej prawdziwe}$$

Proof

$$\begin{aligned}
&\forall f : S \to S : \\
&f \text{ jest injekcyjne} \iff f \text{ jest surjekcyjne} \\
\\
&\forall a \in S : \\
&f_a : S \to S,\ f_a(x) = ax \\
&g_a : S \to S,\ g_a(x) = xa
\end{aligned}$$

Obydwie własności skracania są prawdziwe

$$\begin{aligned}
\iff \forall a \in S : \quad & f_a(x) = f_a(y) \implies x = y \\
& g_a(x) = g_a(y) \implies x = y \\
\iff \forall a \in S : \quad & f_a \text{ i } g_a \text{ są injekcyjne} \\
\iff \forall a \in S : \quad & f_a \text{ i } g_a \text{ są surjekcyjne} \\
\iff \forall a \in S : \quad & \forall b \in S\ \exists x, y \in S : f_a(b) = b \wedge g_a(y) = b \\
\iff \text{Lemma} : \quad & (S, \circ) \text{ jest grupą}
\end{aligned}$$