Beweis: a) zz. $x^n \circ x^m = x^{n+m}$ $\quad n, m \in \mathbb{N}$

Induktion über m:

IA: $x^n \circ x^0 = x^n \circ e = x^n = x^{n+0}$ ✓

IS: Annahme: $x^n \circ x^m = x^{n+m}$ z.z.: $x^n \circ x^{m+1} = x^{n+m+1}$

$$x^n \circ x^{m+1} \underset{\text{Def.}}{=} x^n \circ (x^m \circ x) = (x^n \circ x^m) \circ x \underset{\text{Ind. Ann.}}{=}$$

$$= x^{n+m} \circ x \underset{\text{Def}}{=} x^{n+m+1} \qquad \square$$

$n < 0$ $m \in \mathbb{N}$ analog.

Falls $n \in \mathbb{Z}$ $m < 0$ Beweis gänzlich

IS: $x^n \circ x^{m-1} = x^n \circ (x^m \circ x^{-1}) = (x^n \circ x^m) \circ x^{-1} =$

$$= x^{n+m} \circ x^{-1} = x^{n+m-1}$$

Satz gilt also in der Tat für $n, m \in \mathbb{Z}$

b) z.z $(x^n)^m = x^{n \cdot m}$, Induktion über m

zunächst $m \in \mathbb{N}$.

IA: $(x^n)^0 = e = x^0 = x^{n \cdot 0}$ ✓

IS: $(x^n)^{m+1} \underset{\text{Def}}{=} (x^n)^m \circ x^n \underset{\text{IA}}{=} x^{n \cdot m} \circ x^n$

$$\underset{\text{P.G. a)}}{=} x^{n \cdot m + n} = x^{n(m+1)} \quad ✓$$

Für $m < 0$ benutzen wir $(x^n)^{-1} = x^{-n}$, denn:

$$x^n \circ x^{-n} \underset{\text{a)}}{=} x^0 \underset{\text{Def}}{=} e$$

Wegen Eindeutigkeit des Inversen ist also x^{-n} das Inverse von x^n, d.h.: $x^{-n} = (x^n)^{-1}$

(IA: $(x^n)^0 = e$ ✓)

IS: $(x^n)^{m-1} \underset{\text{Def.}}{=} (x^n)^m \circ (x^n)^{-1} \underset{\text{IA}}{=} x^{n \cdot m} \circ x^{-n}$

$$\underset{\text{a)}}{=} x^{n \cdot m - n} = x^{n(m-1)} \quad ✓$$

Bemerkung: Aus Schulzeiten ist das Gesetz $x^n \cdot y^n = (x \cdot y)^n$ bekannt. $(x, y \in \mathbb{R}^+, n \in \mathbb{R})$. Gilt das auch für $x, y \in G$ $n \in \mathbb{N}$ für bel. Gruppen G?

$(x \cdot y)^2 = x \cdot y \cdot x \cdot y = x y y x \ldots$ Kommut. Gesetz.

Das Gesetz gilt für kommutative Gruppen.

Im allgemeinen aber nicht.

Bsp: Betrachte die Menge der invertierbaren 2×2 Matrizen mit $\cdot$. Das ist Gruppe.

$$x = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad y = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$x^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad y^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad x^2 y^2 = \mathbb{E}_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$xy = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \qquad (xy)^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = x^2 \cdot y^2$$

Hat zu tun mit $xy \neq yx$.

Untergruppen

Definition: Sei $(G, \circ)$ eine Gruppe. Eine Teilmenge $U \subset G$ heißt Untergruppe von G (bzgl $\circ$) falls $(U, \circ)$ eine Gruppe ist.

Bemerkung zur Notation: Das $\circ$ wirkt nun auf $U \times U \subset G \times G$, ist also entsprechend eine andere Verknüpfung. Man schreibt daher auch $\circ|_{U\times U}$ "$\circ$ eingeschränkt auf $U \times U$". Dies lasse ich hier weg.

Bsp: Die Vielfachen von 7 : $7\mathbb{Z}$ bildet eine Untergruppe von $(\mathbb{Z}, +)$, $\quad 7\mathbb{Z} = \{\ldots -14, -7, 0, 7, 14 \ldots\}$

$U \neq \emptyset$

Satz: Sei $(G, \circ)$ Gruppe, $U \subset G$, Dann sind äquivalent:

a) U ist Untergruppe von G

b) Für alle $a, b \in U$ gilt: $a b^{-1} \in U$

c) Für alle $a, b \in U$ gilt: $a^{-1} \in U$ und $ab \in U$

d) Die Relation $a \sim b :\Leftrightarrow a b^{-1} \in U$ ist eine Äquivalenzrel $\circledast$ auf G

e) Falls $a \in U$ und $b \in G \setminus U \Rightarrow ab \notin U$. $(ab \in G \setminus U)$

$\circledast$ auf $G \times G$

Beweis: "$a \Rightarrow b$" Sei $(U, \circ)$ eine Gruppe $(U \subset G)$

z.z. $\forall\, a,b \in U$ ist $ab^{-1} \in U$.

Da U Gruppe ist $b^{-1} \in U$, also auch $ab^{-1} \in U$

$(\circ : U \times U \to U)$

"$b \Rightarrow c$": Es gelte: $\forall\, a,b \in U$ ist $ab^{-1} \in U$

z.z.: $\forall\, c,d \in U$ ist $c^{-1} \in U$ und $c \cdot d \in U$.

Zunächst ist nach Vorr. $e \in U$: Sei $a \in U$, wähle $b = a$

$\Rightarrow a a^{-1} = e \in U$.

Sei nun $c, d \in U$. Da auch $e \in U$ folgt n.V.: $e \cdot c^{-1} = c^{-1} \in U$

(a, b)

Außerdem ist $c((d)^{-1})^{-1} = cd \in U$

(a; $b \in U$ wegen 1. Teil.)

"$c \Rightarrow d$": Es gelte: $\forall\, a,b \in U$ gilt $a^{-1} \in U$ und $ab \in U$.

$a \sim b :\Leftrightarrow ab^{-1} \in U$. z.z. "$\sim$" ist ÄR auf $G \times G$.

1) Reflexivität "$a \sim a$": $a \sim a \Leftrightarrow a a^{-1} \in U \Leftrightarrow e \in U$

Wähle $x \in U$ beliebig $\Rightarrow x^{-1} \in U \Rightarrow x x^{-1} = e \in U$ (n.V.)

nach Vorr. folgt also $a \sim a$

2) Symmetrie "$a \sim b \Rightarrow b \sim a$": Sei $a \sim b$ z.z. $b \sim a$

d.h. z.z. $ba^{-1} \in U$

$\Rightarrow ab^{-1} \in U \Rightarrow (ab^{-1})^{-1} \in U$

$\Rightarrow ba^{-1} \in U$ ✓

Formel $a, b \in G$.

3) Transitivität: "$a \sim b$ und $b \sim c \Rightarrow a \sim c$".

Es gelte $a \sim b$ und $b \sim c$, d.h. $ab^{-1} \in U$ $bc^{-1} \in U$

$\overset{\text{Vorr.}}{\Rightarrow} ab^{-1} \cdot bc^{-1} \in U \Rightarrow ac^{-1} \in U \Rightarrow a \sim c$ ✓