Zahlkörper

Verknüpfung auf A

$f: A \times A \to A$

$f(a_1, a_2) \in A$

$+ : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$

$+(x_1, x_2) = x_1 + x_2$

Def Ein **Körper** ist ein Tripel $(K, +, \cdot)$ aus einer Menge K mit ≥ 2 El., einer Verknüpfung

$+ : K \times K \to K$ ("Addition")

und einer Verknüpfung

$\cdot : K \times K \to K$ ("Multiplikation")

derart, dass

(A1) $(a+b)+c = a+(b+c)$

$\forall a, b, c \in K$ ("Assoziativgesetz")

(A2) $a+b = b+a \quad \forall a, b \in K$

"Kommutativgesetz"

(A3) $\exists\, 0 \in K : \forall a \in K :$

$$a + 0 = a$$

Bem 0 ist eindeutig.

Beweis Wenn $\forall a \in K : a + 0' = a$ (*)

dann $0' \overset{(A3)}{=} 0' + 0$

$\overset{(A2)}{=} 0 + 0'$

$\overset{(*)}{=} 0$. □

(A4) $\forall a \in K : \exists\, \tilde{a} \in K : a + \tilde{a} = 0$

Bem $\tilde{a}$ ist eind.

Beweis Wenn $a + \tilde{a}' = 0$,

dann $\tilde{a}' \overset{(A3)}{=} \tilde{a}' + 0$

$\overset{(A2)}{=} 0 + \tilde{a}'$

$\overset{(A4)}{=} (a + \tilde{a}) + \tilde{a}'$

$\overset{(A2)}{=} (\tilde{a} + a) + \tilde{a}'$

$\overset{(A1)}{=} \tilde{a} + (a + \tilde{a}')$

$\overset{\text{Vor.}}{=} \tilde{a} + 0$

$\overset{(A3)}{=} \tilde{a}$. □

(M1) $(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \forall a, b, c \in K$

(M2) $a \cdot b = b \cdot a \quad \forall a, b \in K$

(M3) $\exists 1 \in K : \forall a \in K : a \cdot 1 = a.$

Bem 1 ist eind.

Beweis Wenn $\forall a \in K : a \cdot 1' = a$,

dann $1' \overset{(M3)}{=} 1' \cdot 1$

$\overset{(M2)}{=} 1 \cdot 1'$

$= 1.$ □

(M4) $\forall a \in K \setminus \{0\} \; \exists \hat{a} \in K : a \cdot \hat{a} = 1.$

Bem $\hat{a}$ ist eind.

Bew Wenn $a \cdot \hat{a}' = 1$

dann $\hat{a}' = \hat{a}' \cdot 1$

$= 1 \cdot \hat{a}'$

$= (a \cdot \hat{a}) \cdot \hat{a}'$

$= (\hat{a} \cdot a) \cdot \hat{a}'$

$= \hat{a} \cdot (a \cdot \hat{a}')$

$= \hat{a} \cdot 1$

$= \hat{a}.$ □

(D) $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$
$\forall a, b, c \in K$ "Distributivgesetz"

Ende der Def. "Körper".

Notation: $\widehat{a} =: -a$

$\widehat{a} =: a^{-1} = \frac{1}{a}$

Bsp $\mathbb{R}, \mathbb{C}, \mathbb{Q}$ Körper

$\mathbb{Z}, \mathbb{N}$ keine Körper

Verknüpfungen

Def $A^B := \{f : B \to A\}$

(vgl. $A^N \cong A^{\{1 \dots N\}}$)

Proposition Auf $M^M = \{f : M \to M\}$ definiert die Verkettung

$(f \circ g)(x) = f(g(x))$

stets eine assoziative Verkn.

Beweis

$((f \circ g) \circ h)(x) = (f \circ g)(h(x)) = f(g(h(x)))$.

$(f \circ (g \circ h))(x) = f((g \circ h)(x)) = f(g(h(x)))$ □

Gruppen

Def Eine Gruppe ist ein Paar $(G, \circ)$ aus einer Menge $G \neq \emptyset$ und einer Verkn. $\circ : G \times G \to G$ derart, dass

(G1) $(g \circ h) \circ j = g \circ (h \circ j)$ $\forall g, h, j \in G$

(G2) $\exists e \in G \ \forall g \in G$:

$g \cdot e = g$ und $e \cdot g = g$.

~~(G2)~~ Bem: e ist eind.

(G3) $\forall g \in G \ \exists g^{-1} \in G$:

$g \cdot g^{-1} = e$ und $g^{-1} \cdot g = e$.

Bem: g^{-1} ist eind.

Def Eine Gruppe heißt abelsch oder kommutativ falls $g \circ h = h \circ g$ $\forall g, h \in G$.

Bem Für Körper $(K, +, \cdot)$ ist

$(K, +)$ eine abelsche Gruppe

$(K \setminus \{0\}, \cdot)$ ist eine abelsche Gr.

Bsp $(\mathbb{Z}, +)$ abelsche Gruppe!

$(\mathbb{R}^n, +)$ ist abelsche Gruppe für

$(x_1 \dots x_n) + (y_1 \& \dots y_n)$

$:= (x_1 + y_1, \dots, x_n + y_n)$.

Bem Wenn für $(G, \circ)$ gilt

1) Asso. (G1)

2) $\exists$ linksneutrales $e \in G$,

d.h. $\exists e \in G : \forall g \in G : e \cdot g = g$

3) $\forall g \in G \; \exists g' \in G : g' \circ g = e$

(linksinv. zu diesem linksneutr.)

dann ist $(G, \circ)$ bereits eine Gruppe.

Justes. linksneutr. e sind, rechtsneutr. $g \cdot e = g$

linksinv. zu g sind. und rechtsinv., $g \circ g' = e$.

Beweis: $g'' \circ g' = e$ also

$$g \cdot g' \overset{2}{=} (e \cdot g) \cdot g' \overset{1}{=} e \cdot (g \cdot g')$$
$$\overset{3}{=} (g'' \circ g') \circ (g \cdot g') \overset{1}{=} g'' \cdot (g' \cdot (g \cdot g'))$$
$$\overset{1}{=} g'' \circ ((g' \cdot g) \cdot g') \overset{3}{=} g'' \cdot (e \cdot g')$$
$$\overset{2}{=} g'' \circ g' = e$$

$$g \cdot e = g \cdot (g' \circ g) \overset{1}{=} (g \cdot g') \cdot g$$
$$\overset{\text{oben}}{=} e \cdot g \overset{2}{=} g$$

Also sind (G2) und (G3) erfüllt. □

Bem 1), 2) $\not\Rightarrow$ e rechtsneutral

Bem (G1), (G2), nicht $\forall g \in G$ $\exists$ linksinv

$\not\Rightarrow$ linksinv = rechtsinv.

Bem $(M^M, \circ)$ ist keine Gruppe.

denn nicht alle $f: M \to M$

besitzen Inverse (nur die bijektiven).