18.10.2011

Lineare Algebra I. Vortrag 1.

Definition: (i) Eine Verknüpfung (auf eine Menge G) ist (oder binäre Operation) eine Funktion:

$$* : G \times G \longrightarrow G.$$

Bezeich.: $*(g, h) := g * h$

(ii) Sei $G \neq \emptyset$

Das Paar $(G, *)$ ist eine Gruppe wenn

Assoziativ. – $(g * h) * k = g * (h * k) \quad \forall g, h, k \in G$

Neutrales Element – $\exists\, e \in G$ s.d.

$$e * g = g = g * e \qquad \forall g \in G$$

$\exists$ von Inversen – $\forall g \in G \ \exists\, h \in G$ s.d.

$$g * h = e = h * g$$

NB: Eindeutigkeit von neutralem Element und Inversen; siehe ÜB.

kommutativ oder abelsch – $g * h = h * g \quad \forall h, g$

Bezeich: $\mathbb{Z} :=$ Menge der ganzen Zahlen, $\mathbb{Q}$ (rationale),

Bezeich. $\mathbb{R} := $ die Menge der reellen Zahlen.

Beisp. I) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ $\square$

II) $(\mathbb{Q}^{\times}, \cdot)$, $(\mathbb{R}^{\times}, \cdot)$ $\square$

Bezeich. $\mathbb{Q}^{\times} = \mathbb{Q} \setminus \{0\}$

$\mathbb{R}^{\times} = \mathbb{Q} \setminus \{0\}$.

III) $\mathcal{F} := \{ f \mid f : \mathbb{R} \to \mathbb{R} \}$

Verknüpfung: $f, g \in \mathcal{F}$ definiere

$f + g : \mathbb{R} \longrightarrow \mathbb{R}$ mit

$(f+g)(r) := f(r) + g(r) \quad \forall r \in \mathbb{R}$.

Neutrales. $Z : \mathbb{R} \longrightarrow \mathbb{R}$

$Z(r) = 0 \quad \forall r \in \mathbb{R}$.

Inverse $-f : \mathbb{R} \longrightarrow \mathbb{R}$

$(-f)(r) := -(f(r)) \quad \forall r \in \mathbb{R}$. $\square$

Diese sind abelsche (siehe ÜB für nicht abelsche) und unendliche Gruppen.

Wir konstruieren nun Beispiele von endlichen Gruppen.

Bezeich. $\mathbb{N} := \{1, 2, \ldots\}$ die Menge der natürlichen Zahlen

$\mathbb{N}_0 := \{0, 1, \ldots\} = \{0\} \cup \mathbb{N}$.

$\mathbb{Z} :=$ die Menge der natur. Zahlen

Divisionsalgorithmus:

Seien $a, b \in \mathbb{Z}$; $b > 0$.

$\exists!$ $q, r \in \mathbb{Z}$ mit $0 \leq r < b$

und $a = bq + r$.

Beweis Betrachte zunächst den Fall $a > 0$

Falls $0 < a < b$ setze $r := a$ ✓

sonst $a \geq b$ betrachte die Menge

$$S := \{s \in \mathbb{N} ; sb \leq a\}$$

$1 \in S$ also $S \neq \emptyset$, und S ist endlich.

Setze $q := \max S$.

$r := a - qb$.

(also $r = 0$ gdw $a = qb$)

 18. 10. 2011

Beh $0 \leq r < b$. Widerspruchsbeweis:

$r \geq 0$ gilt per Definition ✓

Wenn $r \geq b$ dann

$$a - qb \geq b$$

i.e. $a \geq qb + b$

i.e. $a \geq (q+1)b$

also $q+1 \in S$ aber

$q+1 > q$. ↯.

Eindeutigkeit:

$$\left.\begin{aligned} a &= q_1 b + r_1 \\ b &= q_2 b + r_2 \end{aligned}\right\} (\dagger)$$

Also von $(\dagger)$: $0 = (q_2 - q_1) b + (r_2 - r_1)$

Widerspruchsbeweis: Wenn $r_1 > r_2$

dann $(r_1 - r_2) > 0$

Also $0 < (r_1 - r_2) \underset{\text{aus } (\dagger)}{=} \underbrace{(q_2 - q_1) b}_{b > 0}$ (*)

also $(q_2 - q_1) > 0$

also $(q_2 - q_1) b \geq b$

andererseits:

$r_1 < b$ und $r_2 < b$ also

$$(r_1 - r_2) < (b - r_2) \leq b$$

mit (*) erhält man einen Widerspruch:

linke Seite in (*): $< b$

rechte Seite in (*): $\geq b$. $\lightning$. $\boxed{1}$

Also $r_1 = r_2$ und mit (†) bekommt man auch
$q_1 = q_2$. $\boxed{2}$

Sei nun $c \in \mathbb{Z}$; $c \leq 0$

Wenn $c = 0$ setze $q := 0$ und $r := c$

$$c = 0 = 0b + 0 \quad \checkmark.$$

Wenn $c < 0$ setze $a := (-c)$ $a > 0$

Also $\exists!\ q, r$ mit $0 \leq r < b$ und

$$a = bq + r$$

$r = 0 \Rightarrow c = -a = b(-q)$ $\checkmark$

$r \neq 0 \Rightarrow c = -a = b(-q) + (-r)$
$= b(-q) - b + (b - r)$

$$= b(-q-1) + (b-r)$$

$$= b[-(q+1)] + \underbrace{(b-r)}$$

$$0 \leq r < b$$

also $0 \geq -r > -b$

also $b > (b-r) > 0$ $\blacksquare$