# Vorlesung 11

F. 168 Bew. Satz $\otimes \subseteq (\mathbb{Z}_m \times \mathbb{Z}_m) \times \mathbb{Z}_m$

[z.z.: $\otimes : \mathbb{Z}_m \times \mathbb{Z}_m \to \mathbb{Z}_m,\ ([a]_m, [b]_m) \mapsto [a \cdot b]_m$

ist wohldefiniert, d.h. $\otimes$ ist r.e., d.h.:

$$\forall \left(([a]_m, [b]_m), [a \cdot b]_m\right), \left(([a']_m, [b']_m), [a' \cdot b']_m\right) \in \otimes :$$

$$([a]_m, [b]_m) = ([a']_m, [b']_m) \Rightarrow [a \cdot b]_m = [a' \cdot b']_m]$$

Seien $\left(([a]_m, [b]_m), [a \cdot b]_m\right), \left(([a']_m, [b']_m), [a' \cdot b']_m\right) \in \otimes$.

Es gilt: $([a]_m, [b]_m) = ([a']_m, [b']_m)$.

[z.z.: $[a \cdot b]_m = [a' \cdot b']_m$, d.h.: $a \cdot b \equiv_m a' \cdot b'$, d.h.:

$m \mid a' \cdot b' - a \cdot b$, d.h.:

$\exists c \in \mathbb{Z} : \ m \cdot c = a' \cdot b' - a \cdot b$ ]

Nach Vor. gilt: $[a]_m = [a']_m$ und $[b]_m = [b']_m$.

D.h. $a \equiv_m a'$ und $b \equiv_m b'$, d.h.:

$m \mid a' - a$ und $m \mid b' - b$, d.h.:

es ex. $c', c'' \in \mathbb{Z}$ mit

(I) $\underbrace{m \cdot c' = a' - a}_{\Leftrightarrow\ a' = a + m \cdot c'}$ und (II) $\underbrace{m \cdot c'' = b' - b}_{\Leftrightarrow\ b' = b + m \cdot c''}$.

Multiplikation der Gl. (I) und (II) liefert:

$$a' \cdot b' = (a + m \cdot c')(b + m \cdot c'') = ab + mc''a + mc'b + m^2 c'c''$$

$\Leftrightarrow$

$$\text{(III)}\quad m(c''a + c'b + mc'c'') = mc''a + mc'b + m^2c'c'' = a'b' - ab.$$

Setze $c := c''a + c'b + mc'c'' \in \mathbb{Z}$. Es gilt mit (III):

$$m \cdot c = m \cdot (c''a + c'b + mc'c'') \underset{\text{(III)}}{=} a'b' - ab.$$

F. 170 Bew. Satz

① $[a]_m \oplus [b]_m = [a+b]_m = [b+a]_m = [b]_m \oplus [a]_m$

② – ④ analog beweisen.

F. 17]

$$[a]_n \oplus x = [b]_n \qquad | \oplus [-a]_n$$

$$\iff [a]_n \oplus [-a]_n \oplus x = [b]_n \oplus [-a]_n$$

$$\iff [a+(-a)]_n \oplus x = [b+(-a)]_n$$

$$\iff [0]_n \oplus x = [b-a]_n$$

$$\iff x = [b-a]_n$$

$$[5]_6 \oplus x = [2]_6$$

Lsg.: $x = [2-5]_6 = [-3]_6 = [3]_6$

F. 18]

① [z.z.: $\forall a, a' \in G$: $a' \circ a = e \implies a \circ a' = e$]

Seien $a, a' \in G$. Es gelte: $a' \circ a = e$.

Nach (G4) ex. ein $a'' \in G$ mit $a'' \circ a' = e$.

Es gilt:

④

$$a \circ a' \underset{(G1, G3)}{=} e \circ (a \circ a') \underset{(G4)}{=} (a'' \circ a') \circ (a \circ a')$$

$$\underset{(G2)}{=} a'' \circ (a' \circ a) \circ a' \underset{(G3)}{=} a'' \circ e \circ a'$$

$$\underset{(G3)}{=} a'' \circ a' \underset{(G4)}{=} e.$$

② [z.z.: $\forall a \in G: e \circ a = a \Rightarrow a \circ e = a$]

Sei $a \in G$. Es gelte: $e \circ a = a$.

Nach (G4) ex. ein $a' \in G$ mit $a' \circ a = e$.

Es gilt:

$$a \circ e \underset{(G4)}{=} a \circ (a' \circ a) \underset{(G2)}{=} (a \circ a') \circ a$$

$$\underset{①}{=} e \circ a \underset{(G3)}{=} a.$$

③ [z.z.: $\forall e, e' \in G$: $e, e'$ neu. El. $\Rightarrow e = e'$]

Sei $e, e' \in G$. Es gelte: $e, e'$ sind neu. El.

Es gilt: $e = e \circ e' = e'$.

5

(4) [Z.z.: $\forall a \in G \ \forall a', a'' \in G$: $a', a''$ inv. El. von $a$
$\Rightarrow a' = a''$]

Sei $a \in G$. Seien $a', a'' \in G$. Es gelte: $a', a''$ sind inv. El. von $a$. Es gilt:

$$a'' \underset{(2)}{=} a'' \circ e \underset{(1)}{=} a'' \circ (a \circ a')$$
$$\underset{(G2)}{=} (a'' \circ a) \circ a' \underset{(G4)}{=} e \circ a' \underset{(G3)}{=} a'.$$

(5) [Z.z.: $\forall a \in G$: $(a^{-1})^{-1} = a$]

Sei $a \in G$. Es gilt:

$$(a^{-1})^{-1} \circ a^{-1} = e \quad \text{und} \quad a \circ a^{-1} = e$$

Nach (4) gilt: $(a^{-1})^{-1} = a$.

(6) [Z.z.: $\forall a, b \in G$: $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$]

Seien $a, b \in G$. Es gilt:

$$(b^{-1} \circ a^{-1}) \circ (a \circ b) \underset{(G2)}{=} b^{-1} \circ (a^{-1} \circ a) \circ b$$

$$\underset{(G4)}{=} b^{-1} \circ e \circ b \underset{(G3)}{=} b^{-1} \circ b \underset{(G4)}{=} e$$

und

$$(a \circ b)^{-1} \circ (a \circ b) = e .$$

Nach ④ gilt: $b^{-1} \circ a^{-1} = (a \circ b)^{-1}$. //

F. 174 Bew. Satz 1

Sei $(G, \circ)$ ein assoziative alg. Struktur. (G1, G2)

[7.7.: (G3) und (G4) $\Leftrightarrow$ $G \neq \emptyset$ und ① und ② ]

„$\Rightarrow$": Es gilt: (G3) und (G4).

Da $G$ Gruppe ist, besitzt $G$ ein neutrales El. $e \in G \neq \emptyset$.

[7.7.: $\forall a, b \in G \; \exists x_1, x_2 \in G$:

$a \circ x_1 = b \;\wedge\; x_2 \circ a = b$ ]

Seien $a, b \in G$. Setze $x_1 := a^{-1} \circ b \in G$ und $x_2 := b \circ a^{-1} \in G$. Es gilt:

$$a \circ x_1 = a \circ (a^{-1} \circ b) = (a \circ a^{-1}) \circ b$$
$$= e \circ b = b$$

und

$$x_2 \circ a = (b \circ a^{-1}) \circ a = b \circ (a^{-1} \circ a)$$
$$= b \circ e = b.$$

„$\Leftarrow$" nächste Vl.