Vorlesung 12

F. 124 Bem. Satz 1

Sei $(G,\circ)$ eine assoziative alg. Strukt. $(G1, G2)$

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

"$\Rightarrow$": leichte Übung.

"$\Leftarrow$": [z.z.: $(G3)$, d.h.: $\exists e \in G\ \forall a \in G: e \circ a = a$]

Da $G \neq \emptyset$ ist, wähle $a_0 \in G$.

Nach ② finden wir eine Lösung für die Gl.

$x \circ a_0 = a_0$. Sei $x_1 \in G$ eine Lsg.

Setze $e := x_1 \in G$. Sei $a \in G$. Nach ①

finden wir eine Lsg. für die Gl. $a_0 \circ x = a$.

Sei $x_2 \in G$ eine Lsg. Es gilt:

$$e \circ a = x_1 \circ a = x_1 \circ (a_0 \circ x_2)$$

$$\underset{(G1)}{=} (x_1 \circ a_0) \circ x_2 = a_0 \circ x_2 = a.$$

[z.Z.: (GL), d.h.: $\forall a \in G \; \exists a' \in G : a' \circ a = e$] ②

Sei $a \in G$. Nach ② finden wir eine Lsg. für die Gl. $x \circ a = e$. Sei $x_1 \in G$ eine Lsg. Setze $a' := x_1 \in G$. Es gilt:

$$a' \circ a = x_1 \circ a = e. \; //$$

Bew. Satz 2

① [z.Z.: $\forall a,b \in G \; \forall x_1, x_2 \in G :$

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

Seien $a, b \in G$ und $x_1, x_2 \in G$. Es gelte:

$a \circ x_1 = b$ und $a \circ x_2 = b$. Nach Vor. gilt:

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

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

$$= e \circ x_2 = x_2 . \; //$$

② Analog. //

F. 191 Erläuterungen:

(3) $[a]_n \otimes [0]_n = [a \cdot 0]_n = [0]_n \neq [a]_n$

$[a]_n \otimes [1]_n = [a \cdot 1]_n = [a]_n$

(4) $[a]_n \otimes [0]_n = [a \cdot 0]_n = [0]_n \neq [1]_n$

F. 192

$3^{-1} = \frac{1}{3} \mod 5$

$[3]_5^{-1} = [2]_5$

F. 196 Ben. Satz

- Existenz wird auf F. 203 bewiesen.
- Eindeutigkeit folgt aus der Bem. von F. 196, da das Infimum eindeutig ist. //

F.197 Bew. Satz

Seien $a, b \in \mathbb{Z}$ nicht beide gleich 0 und $k \in \mathbb{Z}$.

Setze $g := ggT(a,b)$. (*)

[z.Zi. $g = ggT(a,b) = ggT(a, b+ka)$, d.h.:

(1) $g \mid a \wedge g \mid b+ka$

(2) $\forall c \in \mathbb{Z}: c \mid a \wedge c \mid b+ka \Rightarrow c \mid g$]

(1) Nach Vor. (*) gilt: $g \mid a$ und $g \mid b$.
Nach A5.1(2) in Modell gilt auch:

$g \mid b+ka$.

(2) Sei $c \in \mathbb{Z}$. Es gelte: $c \mid a$ und $c \mid b+ka$.
Nach A5.1(2) in Modell gilt auch

$c \mid b+ka+(-k)a = b$.

Nach Vor. (*) gilt: $c \mid g$. //

Bew. Folgerung:

Seien $a, b \in \mathbb{Z}$ mit $b \neq 0$. Nach dem Satz „Teilen mit Rest" ex. $q, r \in \mathbb{Z}$ mit

$$\underbrace{a = q \cdot b + r}_{\Leftrightarrow} \quad \text{und} \quad 0 \leq r < |b|.$$

$$r = a + (-q) \cdot b$$

Nach Satz im Text ergibt sich

$$ggT(b, r) = ggT(b, a + (-q)b) = ggT(b, a)$$

$$= ggT(a, b). \quad //$$