Übungszettel 11

Henning Lehmann, Darya Nemtsava

Afg. 11.1

a) 1. Ist $(F, +_F)$ abelsche Gruppe?

1.a: Ist $+_F$ assoziativ?

$$((f +_F g) +_F h)(m) = (f(m) +_R g(m)) +_R h(m)$$
$$\overset{*}{=} f(m) +_R (g(m) +_R h(m))$$
$$= (f +_F (g +_F h))(m) \checkmark$$

1.b: Ist $+_F$ kommutativ?

$$(f +_F g)(m) = f(m) +_R g(m) \overset{*}{=} g(m) +_R f(m) = (g +_F f)(m) \checkmark$$

$*$ $(R, +_R, \cdot_R)$ Ring $\Rightarrow$ $(R, +_R)$ abelsche Gruppe $\Rightarrow$ $+_R$ assoz. & $+_R$ kommut.

1.c: Hat $(F, +_F)$ neutrales Element?

Sei 0_R neutrales Element von $(R, +_R)$. Da $(R, +_R)$ abelsche Gruppe, existiert ein solches Element.

Sei $0_F \in F$ mit $0_F(m) = 0_R$ für alle $m \in M$.

$$(f +_F 0_F)(m) \underset{+_F \text{ kommut.}}{=} (0_F +_F f)(m) = 0_R +_R f(m) = f(m)$$

$\Rightarrow 0_F$ ist neutr. Elem. von $(F, +_F)$. ✓

1.d: Hat jedes $f \in F$ inverses Element?

Sei $-f \in F$ mit $f(m) +_R (-f(m)) = 0_R$. Da $(R, +_R)$ abelsche Gruppe, existiert inverses Element zu $f(m)$.

$$(f +_F (-f))(m) = (-(f) +_F f)(m) = -f(m) +_R f(m) = 0_R = 0_f(m)$$

$\Rightarrow -f$ ist invers zu f bzgl. $+_F$. ✓ (1a, 1b, 1c, 1d) $\Rightarrow$ $(F, +_F)$ ist abelsche Gruppe.

2. Ist $\cdot_F$ assoziativ?

$$((f \cdot_F g) \cdot_F h)(m) = (f(m) \cdot_R g(m)) \cdot_R h(m)$$

$(R, +_R, \cdot_R)$ Ring $\Rightarrow \cdot_R$ assoz.

$$= f(m) \cdot_R (g(m) \cdot_R h(m))$$
$$= (f \cdot_F (g \cdot_F h))(m) \checkmark$$

3. Gelten die Distributivgesetze?

$$(f \cdot_F (g +_F h))(m) = f(m) \cdot_R (g +_F h)(m)$$
$$= f(m) \cdot_R (g(m) +_R h(m))$$

$(R, +_R, \cdot_R)$ Ring $\Rightarrow$ Dist.g. gelten

$$= (f(m) \cdot_R g(m)) +_R (f(m) \cdot_R h(m))$$
$$= (f \cdot_F g)(m) +_R (f \cdot_F h)(m)$$
$$= ((f \cdot_F g) +_F (f \cdot_F h))(m) \checkmark$$

Rechte Distributivität analog.

$(1, 2, 3) \Rightarrow (F, +_F, \cdot_F)$ ist Ring.

b) $(R, +_R, \cdot_R)$ ist Körper $\Rightarrow (R \setminus \{0_R\}, \cdot_R)$ ist abelsche Gruppe.

D.h. es ex. $1\!\!1_R \in R$ mit $r \cdot_R 1\!\!1_R = 1\!\!1_R \cdot_R r = r$, und

jedes Element $r \in R \setminus \{0_R\}$ besitzt $r^{-1} \in R$ mit $r \cdot_R r^{-1} = 1\!\!1_R$.

Z.Z.: $(F, +_F, \cdot_F)$ ist Körper.

Sei $1\!\!1_F$ neutrales Element von $(F, \cdot_F)$ mit $1\!\!1_F(m) = 1\!\!1_R$.

$$(1\!\!1_F \cdot_F f)(m) = (f \cdot_F 1\!\!1_F)(m) = f(m) \cdot_R 1\!\!1_R = f(m) \checkmark$$

Seien $s \in R \setminus \{0_R\}$ und $n \in M$ beliebig aber fest, und sei

$f(m) := \begin{cases} 0_R, & \text{wenn } m = n, \\ s & \text{sonst.} \end{cases}$ Es gilt: $f \neq 0_F$ und daher $f \in F \setminus \{0_F\}$.

Sei f^{-1} Inverses Element zu f mit $(f \cdot_F f^{-1})(m) = f(m) \cdot_R f(m)^{-1}$

$$= 1_F(m) = 1_R$$

$(f \cdot_F f^{-1})(n) = f(n) \cdot_R f^{-1}(n) = 0_R \cdot_R (0_R)^{-1}$ ↯, da 0 kein multiplikatives Inverses besitzt.

$\Rightarrow ((R, +_R, \cdot_R)$ ist Körper$) \Rightarrow (F, +_F, \cdot_F)$ ist Ring mit Eins, aber <u>kein</u> Körper.

<u>Afg. 11.2</u>

Beweis via vollst. Induktion:

IA.: Sei $k = 2$.

In erster Iteration: $x_2 = x_0 \bmod x_1 = f_3 \bmod f_2$

$$= 2 \bmod 1 = 0$$

Da nun $i = 2$, terminiert der Algorithmus (nach $k-1 = 1$ Iteration).

IV.: Der Algorithmus terminiert für alle $2 \leq k < n$ nach genau $k-1$ Iterationen, n beliebig aber fest.

IS.: Betrachte 1. Iteration für $k+1 = n$

$$x_2 = x_0 \bmod x_1 = f_{n+1} \bmod f_n$$
$$= (f_{n-1} + f_n) \bmod f_n$$
$$= f_{n-1} \bmod f_n = f_{n-1}, \text{ da } f_{n-1} < f_n \text{ für alle } n > 2.$$

Daher gilt: $x_3 = x_1 \bmod x_2 = f_n \bmod f_{n-1} = f_{k+1} \bmod f_k$

Diese Berechnung ist äquivalent zur ersten Iteration für (f_{k+1}, f_k).

Gemäß IV werden hierfür $k-1$ Schritte benötigt, d.h. für (f_{n+1}, f_n) werden $(k-1)+1 = k = n-1$ Schritte benötigt.

$\Rightarrow$ IV gilt für $k = n$. $\square$