Ana I, Woche 6 Übung

0

18. Nov 2021

Agenda

Orga:

ÜB3: 1a; 1b; 3; | 2 → mod
4 →

Zu ÜB5:

- Konvergenz aus VL — unter |·|-Top? unter ≤-Top?
- hinreichende Bed. ⚡ Charakterisierung [S. 52]
- Divergenz gdw. ?? 0 Grenzwerte? ≥2 Grenzwerte?
- Rechenregeln
- Logik mit Quantoren (nur Übersetzungen)

Cauchy, Monoton, Leibniz, Sandwich, Quotient, Wurzel,

ÜB3 A2 (Skizze)

Sei $p \in \mathbb{P}$ (z.B. $p = 3$). Setze

$$\mathbb{F}_p = \{0, 1, \dots, p-1\} \subseteq \mathbb{Z}.$$

Definiere

$$m := \mathrm{mod}(\cdot, p) : \mathbb{Z} \longrightarrow \mathbb{F}_p$$

vermöge: $\mathrm{mod}(kp + r, p) = r$

für $k \in \mathbb{Z}$, $r \in \mathbb{F}_p$

Beachte

1) $m|_{\mathbb{F}_p} = \mathrm{id}_{\mathbb{F}_p}$, also

2) $m \circ m = m$

Setze $(\mathbb{F}_p, 0, 1; +_p, \cdot_p)$ wobei

$$r +_p r' := \mathrm{mod}(\underbrace{r + r'}_{\text{in } \mathbb{Z}}, p)$$

$$r \cdot_p r' := \mathrm{mod}(\overbrace{r \cdot r'}^{\text{in } \mathbb{Z}}, p)$$

1

Wohldefiniertheit

Operationen in $\mathbb{F}_p$ wohldefiniert, weil $\mathrm{mod}(\cdot, p) : \mathbb{Z} \longrightarrow \mathbb{F}_p$, $+$, $\cdot$ wohldefiniert sind

Kommutativität

Geht auf die Komm. von $+, \cdot$ in $\mathbb{Z}$ zurück:

$$r' +_p r \overset{\text{Def}^n}{=} m(r' + r) \overset{(\mathbb{Z},+)\text{ komm}}{=} m(r + r') \overset{\text{Def}^n}{=} r +_p r'$$

$$r' \cdot_p r \overset{\text{Def}^n}{=} m(r' \cdot r) \overset{(\mathbb{Z},\cdot)\text{ komm}}{=} m(r \cdot r') \overset{\text{Def}^n}{=} r \cdot_p r'$$

für alle $r, r' \in \mathbb{F}_p$.

Neutrale Elemente

$0_p = 0$ ist das additive und $1_p = 1$ das multiplikative Neutralel:

$$0_p +_p r = r +_p 0_p = m(r + 0) = m(r) \overset{1)}{=} r$$

$$1_p \cdot_p r = r \cdot_p 1_p = m(r \cdot 1) = m(r) \overset{1)}{=} r$$

für alle $r \in \mathbb{F}_p$.

Wir brauchen ein kleines Resultat

> **Proposition** Es gilt
> $$m(x+y) = m(m(x)+m(y))$$
> $$m(x\cdot y) = m(m(x)\cdot m(y))$$
> für alle $x, y \in \mathbb{Z}$.

(Beweis: kurze Übung)

Inverse Sei $r \in \mathbb{F}_p$. Dann ist $m(-r)$ das additive Inverse in $\mathbb{F}_p$, da

$$\begin{aligned} r +_p m(-r) &= m(r + m(-r)) \\ &= m(m(r) + m(-r)) \quad \text{nach 1)} \\ &= m(r + -r) \quad \text{wegen Prop.} \\ &= m(0) = 0 = 0_p \end{aligned}$$

und analog gilt $m(-r) +_p r = 0_p$.

Sei $r \in \mathbb{F}_p \setminus \{0_p\} = \mathbb{F}_p \setminus \{0\}$.

Resultat aus Zahlentheorie:

Da $0 < r < p$ und $p \in \mathbb{P}$, gilt $\mathrm{kgT}(r, p) = 1$.

2

Aus $\mathrm{kgT}(r,p)$ folgt:

$$\exists a, b \in \mathbb{Z}: \quad a\cdot r + b\cdot p = 1.$$

Dann ist $m(a)$ das multiplikative Inverse von r, da

$$\begin{aligned} m(a) \cdot_p r &= m(m(a)\cdot r) \\ &= m(m(a)\cdot m(r)) \text{ nach 1)} \\ &= m(a\cdot r) \quad \text{wegen Prop} \\ &\overset{*}{=} m(-b\cdot p + 1) \\ &= 1 = 1_p. \end{aligned}$$

und analog gilt $r \cdot_p m(a) = 1_p$.

Distributivität Seien $x, y, z \in \mathbb{F}_p$. Dann gilt

$$\begin{aligned} x \cdot_p (y +_p z) &\overset{\text{Def}^{\text{n}}}{=} m(x \cdot m(y+z)) \\ &= m(m(x)\cdot m(y+z)) \quad \text{nach 1)} \\ &= m(x\cdot(y+z)) \quad \text{wegen Prop} \\ &= m((x\cdot y) + (x\cdot z)) \\ &= m(m(x\cdot y) + m(x\cdot z)) \quad \text{nach 1)} \\ &\overset{\text{Def}^{\text{n}}}{=} (x\cdot_p y) +_p (x \cdot_p z) \end{aligned}$$

$(\mathbb{Z}, +, \cdot)$ distributiv

und analog gilt $(y +_p z)\cdot_p x = (y\cdot_p x) +_p (z\cdot_p x)$

Assoziativität Seien $x, y, z \in \mathbb{F}_p$.

Dann gilt

$$
\begin{aligned}
x +_p (y +_p z) &\overset{\text{Def}^{\text{n}}}{=} m(x + m(y+z)) \\
&= m(m(x) + m(y+z)) \quad \text{nach 1)} \\
&= m(x + (y+z)) \quad \text{wegen Prop.} \\
&= m((x+y)+z) \\
&= m(m(x+y)+m(z)) \quad \text{wegen Prop} \\
&= m(m(x+y)+z) \quad \text{nach 1)} \\
&\overset{\text{Def}^{\text{n}}}{=} (x +_p y) +_p z,
\end{aligned}
$$

$(\mathbb{Z}, +)$ assoz.

Analog gilt $x \cdot_p (y \cdot_p z) = (x \cdot_p y) \cdot_p z$.

Darum ist $(\mathbb{F}_p, +_p, \cdot_p, 0_p, 1_p)$ ein Körper.

(Und $\text{mod}(\cdot, p) : \mathbb{Z} \longrightarrow \mathbb{F}_p$ ist ein surjektiver Homomorphismus!)

$\mathbb{F}_p$ kann nicht angeordnet werden:

3

Angenommen nicht. Dann existiert eine Ordnungsrelation, $\leq$, für $\mathbb{F}_p$.

Beachte, dass $1 > 0$ per Definition.

Per Induktion lässt sich

$$n \cdot 1 := \underbrace{1 + 1 + \dots + 1}_{n \text{ Mal}} > \underbrace{0 + 0 + \dots + 0}_{n \text{ Mal}} = 0$$

für alle $n \in \mathbb{N}$ mit $n \geq 1$.

Insbesondere gilt

$$0 = \text{char}(\mathbb{F}_p) = p \cdot 1 > 0,$$

was ein Widerspruch ist.

Darum stimmt die o.s. Annahme nicht.

Anmerkung: Mittels dieser Argumentation wissen wir, dass sich kein Körper, K, mit $\text{char}(K) > 0$ anordnen lässt.

ÜB3 A3 a)

Seien $(K, \leq)$ ein ang. Körper, $a, b \in K$, $\lambda \in K^+$.

Z: $|ab| \leq \frac{1}{2\lambda} a^2 + \frac{\lambda}{2} b^2$

$2 = 1+1 \neq 0$, weil $\mathrm{char}(K) \neq 2$, weil K eine Anordnung hat

Da $|ab| = |a| \cdot |b|$ und $a^2 = |a|^2$, $b^2 = |b|^2$ gelten, können wir o.B.d.A. annehmen, dass $a, b \geq 0$

$\Rightarrow$ Z: $a \cdot b \leq \frac{1}{2\lambda} a^2 + \frac{\lambda}{2} b^2$

$$a \cdot b \leq \frac{1}{2\lambda} a^2 + \frac{\lambda}{2} b^2$$

$2, \lambda \neq 0$

$$\Longleftrightarrow \quad 2\lambda a b \leq a^2 + \lambda^2 b^2$$

$$\Longleftrightarrow \quad 2a \cdot (\lambda b) \leq a^2 + (\lambda b)^2$$

$$\Longleftrightarrow \quad 0 \leq a^2 + (\lambda b)^2 - 2a(\lambda b)$$

$$\Longleftrightarrow \quad 0 \leq (a - \lambda b)^2$$

Letzteres gilt, weil $\forall c \in K: c^2 \geq 0$.

Also gilt die erste Ungleichung.

4