# LA Zettel 7

Bearbeitet von Leon Krasniqi, Christian Krause, Silas Gaschler (Tutorium: Gregor Teupke (Mi 16:15))

## Aufgabe 1

**a)**

(i) $(\mathbb{Z}_3, +_3, \cdot_2)$ Da 3 eine Primzahl ist, ist nach script $(\mathbb{Z}_3, +_3, \cdot_3)$ ein Körper.

**Bestimme Charakteristik**

$$\underbrace{(1+1)}_{2} + 1 = 0 \Rightarrow \operatorname{char}(\mathbb{Z}_3, +_3, \cdot_3) = 3$$

**Nullteilerfreiheit**

$\mathbb{Z}_3 = \{0, 1, 2\}$

$$0 * x = 0 \forall x \in \mathbb{Z}_3$$

$$1 * 2 = 2 * 1 = 2$$

$$2 * 2 = 1$$

$$1 * 1 = 1$$

$\Rightarrow$ Nullteilerfreiheit

**(ii)**

Bereits bewiesen

$$\forall A, B \in \mathcal{P}(X) :$$

$(\mathcal{P}(X), \Delta)$ ist abelsche Gruppe

$$A \cap (B \cap C) = (A \cap B) \cap C \in \mathcal{P}(X)$$

$\Rightarrow$ Es handelt sich um einen Ring Das Einselement ist $X$ da $A \cap X = A$ Das Nullelement ist $\emptyset$

**Nullteilerfreiheit**

Sei $A \in \mathcal{P}(X)$ und $\emptyset \neq A$ dann existiert ($\#X > 1$) eine zu $A$ disjunkte Menge $B \in \mathcal{P}(X)$ mit $B \neq \emptyset$

$$\Rightarrow A \cap B = \emptyset$$

$\Rightarrow$ Falls $\#X > 1$ ist der Ring nicht Nullteilerfrei.

Falls $\#X = 1$ existiert maximal eine von $A$ disjunkte Teilmenge, und zwar $\emptyset$. Also ist der Ring für $\#X = 1$ Nullteilerfrei

**Charakteristik**

**(iii)**

Angenommen $(\mathcal{P}(X), \Delta, \Delta)$ ist ein Ring, dann muss $\forall A, B, C \in X$ das Distributivgesetz gelten:

$$A\Delta(B\Delta C) = (A\Delta B)\Delta(A\Delta C)$$

Da $\Delta$ assoziativ sein muss, und die inversen Elemente für die verknüpfung $\Delta$ existieren müssen:

$$\Leftrightarrow (A\Delta B)\Delta C = (A\Delta B)\Delta(A\Delta C)$$

$$\Leftrightarrow (A\Delta B)\Delta C = (A\Delta B)\Delta(A\Delta C)$$

$$\Leftrightarrow C = A\Delta C \Leftrightarrow A = \emptyset$$

Das ist ein Wiederspruch, also ist $(\mathcal{P}(X), \Delta, \Delta)$ kein Ring

**(iv)**

Damit $(\mathbb{Q}^{\mathbb{R}}, +, \circ)$ ein Ring ist, muss das Distributivgesetz gelten. das heißt:

$$\forall f_1, f_2, f_3 \in \mathbb{Q}^{\mathbb{R}}; \forall x_2, x_3 \in \mathbb{R} :$$

$$f_1 \circ (f_2(x_2) + f_3(x_3)) = f_1 \circ f_2(x_2) + f_1 \circ f_3(x_3)$$

Wähle $f_1 = f_2 = f_3 : \mathbb{R} \ni x \mapsto 1 \in \mathbb{Q} :$

$$f_1(f_2(x_2) + f_3(x_3)) \neq f_1(f_2(x_2)) + f_1(f_3(x_3))$$

$$1 \neq 1 + 1$$

Das ist ein Wiederspruch. Es handelt sich also um keinen Ring

**b)**

**Lemma 0.1**:

Es sei $(R, +, \cdot)$ ein Ring und $a \cdot a$ für alle $a \in R$. Dann ist $(r, +, \cdot)$ kommutativ.

*Proof*:

$$(a + b)$$

$$= (a + b) \cdot (a + b)$$

$$= (a + b) \cdot a + (a + b) \cdot b$$

$$= a \cdot a + b \cdot a + a \cdot b + b \cdot b$$

$$\Rightarrow a + b = b + b \cdot a + a \cdot b + a$$

$$\Rightarrow 0 = b \cdot a + a \cdot b$$

$$\Rightarrow \forall c \in R : c + c = c \cdot c + c \cdot c = 0$$

$$\Rightarrow \forall a, b \in R : a \cdot b + a \cdot b = 0 = b \cdot a + a \cdot b$$

$$\Rightarrow a \cdot b = b \cdot a$$

■

## Aufgabe 2

**a)**

**Lemma 0.2**: $(\mathbb{Z}_3, +_3, \cdot_3)$ ist ein Integritätsring, $(\mathcal{P}(X), \triangle, \cap)$ aber nicht.

**i)**

*Proof*:

1. $(\mathbb{Z}_3, \cdot_3)$ hat nur 3 Elemente und muss daher abelsch sein.
2. $(\mathbb{Z}_3, +_3, \cdot_3)$ ist ein Ring mit Eins, denn:

$$\forall x \in \mathbb{Z}_3 : 1 \cdot_3 x = x$$

3. $(\mathbb{Z}_3, +_3, \cdot_3)$ ist nullteilerfrei, denn:

$$1 \cdot_3 1 = 1 \neq 0$$

$$1 \cdot_3 2 \neq 0$$

$$2 \cdot_3 2 \neq 0$$

■

**ii)**

*Proof*:

1. Sei $A, B \subset X, A, B \neq \emptyset, A$ und $B$ sind disjunkt, dann gilt:

$$A \cap B = \emptyset$$

$\Rightarrow (\mathcal{P}(X), \triangle, \cap)$ ist nicht nullteilerfrei und somit kein Integritätsring. ■

**b)**

*Proof*:

$$\boldsymbol{(i) \Rightarrow (ii):}$$

$$(i) : \forall a \in R : a \neq 0_R \Rightarrow a \cdot b \neq 0_R$$

$$f : R \ni a \mapsto a \cdot b \in R$$

$$\mathrm{Kern}(f) = \{a | a \cdot b = 0_R\} = \{0_R\}$$

$$I : R/\{0_R\} \to \mathrm{Bild}(f)$$

$$a + \mathrm{Kern}(f) = [a] \mapsto f(a)$$

Homomorphiesatz für Ringe $\Rightarrow I$ ist ein Isomorphismus

$$\pi : R \ni a \to [a] \in R/\{0_R\}$$

Da

$$R/\{0_R\} = \{a + 0_R = [a] \square a \in R\} = \{a = [a] | \ a \in R\}$$

ist $\pi$ injektiv. Es gilt außerden, das:

$$f = I \circ \pi$$

Da $I, \pi$ injektiv $\Rightarrow f$ injektiv

$$\boldsymbol{(ii) \Rightarrow (iii)}$$

$$(ii) : (\forall a, c \in R : f(a) = f(c) \Rightarrow a = c)$$

$$\Leftrightarrow (\forall a, c \in R : a \cdot b = c \cdot b \Rightarrow a = c)$$

$$\boldsymbol{(iii) \Rightarrow (i)}$$

$$(iii) : (\forall a, b \in R : a \cdot b = c \cdot b \Rightarrow a = c)$$

Es gilt außerdem $0_R \cdot b = 0_R$

Sei $a \cdot b = 0_R = 0_R \cdot b \Rightarrow a = 0_R$

$\Rightarrow$ b ist kein Rechtsnullteiler

$\Rightarrow$ **$((i) \Rightarrow (ii) \Rightarrow (iii) \Rightarrow (i)) \Rightarrow$ Ringschluss**

■

## Aufgabe 3

**a)**

Es seien $(R_1, +_1, \cdot_1), (R_2, +_2, \cdot_2)$ Ringe und $f : R_1 \to R_2$ ein Homomorphisums.

**i)**

**Lemma 0.3**: $\mathrm{Bild}(f)$ ist ein Unterring von $(R_2, +_2, \cdot_2)$.

Beweis durch das Unterringkriterium:

*Proof*:

1. $\text{Bild}(f) \neq \emptyset$, weil:

$$f\left(0_{R_1}\right) = 0_{R_2} \Rightarrow 0_{R_2} \in \text{Bild}(f)$$

2. $a_2, b_2 \in \text{Bild}(f) \land a_1, b_1 \in R_1$ :

$$a_2 +_2 (-b_2) = f(a_1) +_2 (-f(b_1))$$
$$= f(a_1) +_2 f(-b_1)$$
$$= f(a_1 +_1 (-b_1)) \in \text{Bild}(f)$$

3. $$a_2 \cdot_2 b_2^{-1} = f(a_1) \cdot_2 (f(b_1))^{-1}$$
$$= f(a_1) \cdot_2 f(b_1^{-1})$$
$$= f(a_1 \cdot_1 b_1^{-1}) \in \text{Bild}(f)$$

■

**ii)**

**Lemma 0.4**: $\text{Kern}(f)$ ist ein Unterring von $(R_1, +_1, \cdot_1)$.

Beweis durch das Unterringkriterium:

*Proof*:

1. $\mathrm{Kern}(f) \neq \emptyset$, weil:

$$f\left(0_{R_1}\right) = 0_{R_2} \Rightarrow 0_{R_1} \in \mathrm{Kern}(f)$$

2. $a_1, b_1 \in \mathrm{Kern}(f)$ :

$$f(a_1 +_1 (-b_1)) = f(a_1) +_2 f(-b_1)$$

$$= f(a_1) +_2 (-f(b_1))$$

$$= 0_{R_2} +_2 \left(-0_{R_2}\right)$$

$$= 0_{R_2} \in \mathrm{Kern}(f)$$

3.

$$f(a_1 \cdot_1 b_1^{-1}) = f(a_1) \cdot_2 f(b_1^{-1})$$

$$= f(a_1) \cdot_2 f(b_1^{-1})$$

$$= 0_{R_2} \cdot_2 f(b_1^{-1})$$

$$= 0_{R_2} \in \mathrm{Kern}(f)$$

■

**b)**

**Lemma 0.5**:

Seien $(R_1, +_1, \cdot_1)$ und $(R_2, +_2, \cdot_2)$ Ringe mit den Nullelementen $0_{R_1}$ bzw. $0_{R_2}$ und $f : R_1 \to R_2$ ein Homomorphismus, dann gilt die Äquivalenz foldender Aussagen:

- (i): $f$ ist injektiv
- (ii): $\mathrm{Kern}(f) = \left\{0_{R_1}\right\}$
- (iii): Die einzige Lösung der Gleichung $f(a) = 0_{R_2}$ ist $a = 0_{R_1}$

*Proof*:

**(i)⇒(ii)**

$$(i) : (\forall a, b \in R_1 : f(a) = f(b) \Rightarrow a = b)$$

$$\forall a_n \in R_1 : f(a_n) = f\left(a_n +_1 0_{R_1}\right) = f(a_n) +_2 f\left(0_{R_1}\right)$$

Da wir $+_2$ Kürzen dürfen

$$\Leftrightarrow 0_{R_2} = f\left(0_{R_1}\right)$$

$$\Rightarrow 0_{R_1} \in \text{Kern}(f)$$

$$\Rightarrow \forall b \in R_1 \text{ mit } f(b) = 0_{R_2} \Rightarrow f(b) = f\left(0_{R_1}\right) \Rightarrow b = 0_{R_1}$$

$$\Rightarrow \text{Kern}(f) = \left\{0_{R_1}\right\}$$

**(ii)⇒(iii)**

$$(ii) : \text{Kern}(f) = \left\{0_{R_1}\right\} = \left\{a \in R_1 |\ f(a) = 0_{R_2}\right\}$$

$$\Rightarrow \forall a \in R_1 \text{ mit } f(a) = 0_{R_2} \Rightarrow a \in \text{Kern}(f) \Rightarrow a = 0_{R_1}$$

**(iii)⇒(i)**

$$(iii) : f(a) = 0_{R_2} \Rightarrow a = 0_{R_1}$$

Sei $c, d \in R_1$ und $f(c) = f(d)$

$$\Rightarrow 0_{R_2} = f(c) - f(d)$$

$$\Rightarrow f(c - d) = 0_{R_2}$$

$$\Rightarrow c - d = 0_{R_1}$$

$$\Rightarrow c = d$$

$$\boldsymbol{\Rightarrow ((i) \Rightarrow (ii) \Rightarrow (iii) \Rightarrow (i)) \Rightarrow ((i) \Leftrightarrow (ii) \Leftrightarrow (iii))}$$

■

**c)**

**Lemma 0.6**:

Es sei $(R, +, \cdot)$ ein Ring mit Eins und $\text{char}(R) = 0$, dann enthält $R$ einen Unterring, der isomorph zu $\mathbb{Z}$ ist.

*Proof*:

$$f : \mathbb{Z} \ni n \to \begin{cases} 0_R \text{ falls } n = 0 \\ n1 \text{ falls } n > 0 \\ |n|(-1_R) \text{ falls } n < 0 \end{cases} \in R$$

$$a \in \mathbb{Z}$$

$$a > 0 : f(-a) = a(-1_R) = \underbrace{(-1_R - ... - 1_R)}_{a \text{ mal}} = -\underbrace{(1 + .. + 1)}_{a \text{ mal}} = -(a1_R)$$

$$\text{In folgendem nutze wir} : -(a1_R) \mathrel{\hat{=}} -a1_R = \underbrace{(1 + ... + 1)}_{-a \text{ mal}}$$

$$a, b \in \mathbb{Z}$$

$$f(a) + f(b) = a1_R + b1_R = \underbrace{(1_R + ... + 1_R)}_{a \text{ mal}} + \underbrace{(1_R + ... + 1_R)}_{b \text{ mal}} = (a + b)1_R = f(a + b)$$

$$f(a) \cdot f(b) = \underbrace{(1_R + ... + 1_R)}_{a \text{ mal}} \cdot \underbrace{(1_R + ... + 1_R)}_{b \text{ mal}} = \underbrace{(b1 + ... + b1)}_{a \text{ mal}} = (a \cdot b)1_R = f(a \cdot b)$$

$$\Rightarrow f \text{ ist Homomorphismus}$$

Als nächstes zeigen wir, das $f$ injektiv ist:

$$\text{Sei } f(a) = f(b) \Rightarrow a1_R = b1_R$$

$$\Rightarrow (a - b)1_R = 0_R \Rightarrow a - b = \operatorname{char}(R) = 0 \Rightarrow a = b$$

Schränken wir R auf das Bild von $f$ ein, so bekommen wir den Isomorphismus:

$$g : \mathbb{Z} \ni n \to \begin{cases} 0_R \text{ falls } n = 0 \\ n1 \text{ falls } n > 0 \\ |n|(-1_R) \text{ falls } n < 0 \end{cases} \in \operatorname{Bild}(f)$$

Es bleibt zu zeigen, das das Bild von $f$ ein Unterring von $R$ ist:

$$\forall a, b \in \mathbb{Z} :$$

$$\text{Es gilt: } a - b \in \mathbb{Z} \text{und } a \cdot b \in \mathbb{Z} \text{ und } 0_R \in \operatorname{Bild}(f) \Rightarrow \operatorname{Bild}(f) \neq \emptyset$$

$$g(a) - g(b) = g(a) + g(-b) = g\left(\underbrace{a - b}_{\in \mathbb{Z}}\right) \in \operatorname{Bild}(g) = \operatorname{Bild}(f)$$

$$g(a) \cdot g(b) = g(a \cdot b) \in \operatorname{Bild}(f)$$

$\Rightarrow \mathbb{Z}$ ist isomorph zum Bild($f$), welcher ein Unterring von $R$ ist. ■

## Aufgabe 4

### a)

### i)

$\mathbb{N}$ bildet kein Ideal in $(\mathbb{Z}, +, \cdot)$, da $\mathbb{N}$ kein Unterring ist (nicht unter additiver Inversbildung abgeschlossen). $-42 \notin \mathbb{N}$

**ii)**

$2\mathbb{Z} = \{2k \mid k \in \mathbb{Z}\}$

**Lemma 0.7**: Die ganzen geraden Zahlen $2\mathbb{Z}$ bilden ein Ideal in $(\mathbb{Z}, +, \cdot)$.

*Proof*: Die ganzen geraden Zahlen sind ein Unterring von $(\mathbb{Z}, +, \cdot)$:
Zu zeigen: $a - b \in 2\mathbb{Z}, \forall a, b \in 2\mathbb{Z}$. Gilt, da $\exists k_a \in \mathbb{Z}, a = 2k, \forall a \in 2\mathbb{Z}$.

$$2k_a - 2k_b = 2(k_a - k_b) \in 2\mathbb{Z}$$

Zu zeigen: $a \cdot b \in 2\mathbb{Z}, \forall a, b \in 2\mathbb{Z}$. Gilt, da

$$2k_a \cdot 2k_b = 2 \cdot (2 \cdot k_a \cdot k_b) \in 2\mathbb{Z}$$

Zu zeigen: $z \cdot a \in 2\mathbb{Z} \wedge a \cdot z \in 2\mathbb{Z}, \forall a \in 2\mathbb{Z}, z \in \mathbb{Z}$

$$z \cdot a = z \cdot 2k_a = 2(z \cdot k_a) \in 2\mathbb{Z}$$

$$a \cdot z = 2k_a \cdot z = 2(k_a \cdot z) \in 2\mathbb{Z}$$

■

## iii)

TODOTODOTODOTDOTODOTODO

## b)

**Lemma 0.8**: Es sei $(R, +, \cdot)$ ein Ring und $E \subseteq R$.

$$(E) = \left\{ \sum_i^n a_i \mid \exists n \in \mathbb{N}_0, \forall i = 1, ..., n \quad (a_i \in E \cup -E \cup RE \cup ER \cup RER) \right\} = M$$

(Wir nennen die Menge rechts ab sofort M). Sei außerdem $M_0 = E \cup -E \cup RE \cup ER \cup RER$.

*Proof*:

1. Zu zeigen $(E) \subseteq M$. Es genügt zu zeigen, dass $M$ ein Ideal in $R$ ist und $E \subseteq M$.

Zu zeigen: $a - b \in M, \forall a, b \in M$.

$$a - b = \left(\sum_i^n a_i\right) - \left(\sum_j^m b_j\right)$$
$$= \left(\sum_i^n a_i\right) + \left(\sum_j^m -b_j\right)$$
$$\text{Sei} \quad a_{i+n} = -b_j \quad \forall j \in [\![1, m]\!]$$
$$= \sum_i^{n+m} a_i$$

Zu zeigen: $-b_j \in M_0 \quad \forall b_j \in M_0$

1. $b_j \in E \Rightarrow -b_j \in -E$
2. $b_j \in -E \Rightarrow -b_j \in E$
3. $b_j \in RE \Rightarrow \exists r \in R, \exists e \in E, b_j = r \cdot e$
$$-b_j = -(r \cdot e) = -r \cdot e \in RE \quad \text{da } -r \in R$$
4. $b_j \in ER \Rightarrow \exists r \in R, \exists e \in E, b_j = e \cdot r$
$$-b_j = -(e \cdot r) = e \cdot (-r) \in R \quad \text{da } -r \in R$$
5. $b_j \in RER \Rightarrow \exists r_1, r_2 \in R, \exists e \in E, b_j = r_1 \cdot e \cdot r_2$
$$-b_j = -(r_1 \cdot e \cdot r_2) = -r_1 \cdot e \cdot r_2 \in R \quad \text{da } -r_1 \in R$$

Zu zeigen: $r \cdot m \in M \land m \cdot r \in M \quad \forall m \in M \forall r \in R$.

$$r \cdot m = r \cdot \left(\sum_i^n m_i\right) = \sum_i^n r \cdot m_i$$

Zu zeigen: $r \cdot m_i \in M_0 \quad \forall m_i \in M_0$

1. $m_i \in E \Rightarrow r \cdot m_i \in RE$
2. $m_i \in -E \Rightarrow \exists e \in E, m_i = (-e), \quad r \cdot m_i = r \cdot (-e) = -r \cdot e \in RE \quad \text{da } -r \in R$
3. $m_i \in RE \Rightarrow \exists r_1 \in R, \exists e \in E, r \cdot m_i = r \cdot (r_1 \cdot e) = (r \cdot r_1) \cdot e \in RE \quad \text{da } r \cdot r_1 R$
4. $m_i \in ER \Rightarrow \exists r_1 \in R, \exists e \in E, r \cdot m_i = r \cdot \left(e \cdot_{r_1}\right) = r \cdot e \cdot r_1 \in RER \quad \text{da } r, r_1 \in R$
5. $m_i \in RER \Rightarrow \exists r_1, r_2 \in R, \exists e \in E, r \cdot m_i = r \cdot (r_1 \cdot e \cdot r_2) = (r \cdot r_1) \cdot e \cdot r_2 \in RER$

Da $E \subseteq M$ trivial ist, wissen wir nun, dass M ein Ideal in R mit $E \subseteq M$ ist, d.h. nach der Definition eines erzeugten Integrals gilt $(E) \subseteq M$

---

Zu zeigen: $M \subseteq (E)$ d.h. $\forall a_i \in M_0, \sum_i^n a_i \in (E)$. Da $(E)$ unter endlicher Addition abgeschlossen sein muss, genügt es zu zeigen, dass alle $a_i \in M_0$ in $(E)$ enthalten sind.

1. $a_i \in E \Rightarrow \text{trivial}$
2. $a_i \in -E \Rightarrow a_i \in (E) \quad \text{da } (E) \text{ unter additiver inversbildung abgeschlossen sein muss}$
3. $a_i \in RE, \exists r_1 \in R, \exists e \in E, a_i = r \cdot e \in (E) \quad \text{folgt aus kriterium für ideale}$
4. $a_i \in ER, \exists r_1 \in R, \exists e \in E, a_i = e \cdot r \in (E) \quad \text{folgt aus kriterium für ideale}$
5. $a_i \in RER, \exists r_1, r_2 \in R, \exists \in E, a_i = r \cdot e \cdot r \in (E) \quad \text{folgt aus kriterium für ideale (zweimal)}$

---

Da wir nun beide Richtungen der Inklusion gezeigt haben folgt: $(E) = M$ ■

In einem Ring mit 1 gilt:

$$E \cup -E \cup RE \cup ER \cup RER = RER$$

da
1. $E = 1 \cdot E \cdot 1$
2. $-E = -1 \cdot E \cdot 1$
3. $RE = R \cdot E \cdot 1$
4. $ER = 1 \cdot E \cdot R$
5. $RER$ ist sowieso enthalten

In einem kommutativen Ring gilt:

$$E \cup -E \cup RE \cup ER \cup RER = E \cup -E \cup RE$$

1. $E$, $-E$ und $RE$ sind sowieso enthalten.
2. $ER = RE$
3. $RER = RRE = RE$

**c)**
Sei $(R, +, \cdot)$ ein unitärer, kommutativer Ring.

**Lemma 0.9**: Folgende Aussagen sind equivalent:
1. $(R, +, \cdot)$ ist ein Körper
2. $(R, +, \cdot)$ hat genau die trivialen Ideale (die übereinstimmen)

*Proof*: "⇒" $(R, +, \cdot)$ ist ein Körper. Ein Ideal $I$ muss die Bedingung $RI = I$ erfüllen. $I$ kann nun entweder das Nullideal $I = \{0\}$ oder das Ideal des ganzen Körpers $I = R$ sein. Zu zeigen:

$$RI = I \Rightarrow I = \{0\} \vee I = R$$

Entweder gilt, $I\# < 1$, dann gilt $I = \{0\}$.
Sei im folgenden $\#I > 0$. Zu zeigen $RI = R$. Dafür genügt es zu zeigen $RI \supseteq R$, also

$$r \in R \Rightarrow \exists r_1 \in R, i \in I, r_1 \cdot i = r$$

Sei $r_1 = i^{-1} \cdot r$ (Multiplikatives Invers existiert in dem Körper).
Es gilt $r_1 \cdot i = i^{-1} \cdot r \cdot i = r$.

---

"⇐"
Wenn $(R, +, \cdot)$ nur die zwei trivialen Ideale hat, dann folgt

$$(r) = R \vee (r) = (0) \quad \forall r \in R \text{ mit } r \neq 0$$

$(r) = (0)$ ist aber nicht möglich, da $r \notin (0) \quad \forall r \in R$ mit $r \neq 0$. Es gilt also:

$$(1) = (r) = R \quad \forall r \in R$$

Zu zeigen ist: Für jedes $r \in R$ existiert ein Multiplikatives Inverses $r^{-1}$ mit $r \cdot r^{-1} = r^{-1} \cdot r = 1$.
Da $(1) = (r)$ gilt, wissen wir $\exists r_1 \in R, r_1 \cdot r = 1$, was für jedes $r$ ein Multiplikatives Invers erzeugt.

■

## Aufgabe 5

a)

**Lemma 0.10**: Jeder Körper $(K, +, \cdot)$ ist Nullteilerfrei.

*Proof*:

Angenommen es existiert ein Linksnullteiler $a \neq 0_K$

$$\exists b \neq 0_K \in K :$$

$$ab = 0_K$$

$$ab = a0_K$$

$$\Leftrightarrow a^{-1} \cdot a \cdot b = a^{-1} \cdot a \cdot 0_K$$

$$\Leftrightarrow b = 0_K$$

Das ist ein Wiederspruch $\Rightarrow$ Jeder Körper ist Nullteilerfrei

■

**Lemma 0.11**: Es sei $(K, +, \cdot)$ ein Körper und $a, b \in K$.

$$(a - x) \cdot (b - x) = 0_K \Rightarrow x = a \lor x = b$$

*Proof*:

Wir haben bereit gezeigt, das jeder Körper Nullteilerfrei ist. Daraus folgt:

$$\underbrace{(a - x)}_{\in K} \cdot \underbrace{(b - x)}_{\in K} = 0_K \Rightarrow a - x = 0_K \lor b - x = 0_K$$

$$\Leftrightarrow x = a \lor x = b$$

■

### b)

Wir beweisen zunächst einige Hilfslemmas. Zur besseren lesbarkeit wird verwendt: $1_K \mathrel{\hat{=}} 1$

**Lemma 0.12**: Sei $(K, +, \cdot)$ ein Körper mit $\operatorname{char}(K) = 0$, dann gilt

$$\forall a, b \in \mathbb{N} : a1 = b1 \Rightarrow a = b$$

*Proof*:

Falls

$$a \geq b$$

$$a1 = b1 \Leftrightarrow b1 + (a-b)1 = b1 \Rightarrow a - b = \operatorname{char}(K) = 0 \Rightarrow a = b$$

Falls

$$a \leq b$$

$$b1 = a1 \Leftrightarrow a1 + (b-a)1 = a1 \Rightarrow b - a = \operatorname{char}(K) = 0 \Rightarrow a = b$$

■

**Lemma 0.13**: Sei $(K, +, \cdot)$ ein Körper mit $\operatorname{char}(K) = 0$, dann gilt:

$$a1 + b1 = (a+b)1$$

$$a1 + b(-1) = (a-b)1$$

$$a1 \cdot b1 = (a \cdot b)1$$

$$(a1)^{-1} \cdot (b1)^{-1} = ((a \cdot b)1)^{-1}$$

*Proof*:

$$a1 + b1 = \underbrace{(1 + ... + 1)}_{a \text{ mal}} + \underbrace{(1 + ... + 1)}_{b \text{ mal}} = (a+b)1$$

$$1 + b1 = \underbrace{(1 + ... + 1)}_{a \text{ mal}} + \underbrace{(-1 - ... - 1)}_{b \text{ mal}} = \underbrace{(1 + ... + 1)}_{a - b \text{ mal}} + \underbrace{(0_K + ... + 0_K)}_{b \text{ mal}} = (a-b)1$$

$$a1 \cdot b1 = \underbrace{(1 + ... + 1)}_{a \text{ mal}} \cdot b1 = \underbrace{(b1 + ... + b1)}_{a \text{ mal}} = (a \cdot b)1$$

$$(a1)^{-1} \cdot (b1)^{-1} \cdot a1 \cdot b1 = 1 \Leftrightarrow (a1)^{-1} \cdot (b1)^{-1} \cdot (a \cdot b)1 = 1$$

$$\Rightarrow (a1)^{-1} \cdot (b1)^{-1} = ((a \cdot b)1)^{-1}$$

■

**Lemma 0.14**:

Sei $(K, +, \cdot)$ ein Körper mit $\operatorname{char}(K) = 0$, dann enthält $K$ einen Unterkörper, der isomorph zu $\mathbb{Q}$ ist.

*Proof*:

Wir verwenden aus dem script:

Jeder Homomorphismus zwischen Körpern ist injektiv

Wir definieren:

$$f : \mathbb{Q} \to K$$

$$\frac{a}{b} \mapsto \begin{cases} a1 \cdot (b1)^{-1} \text{ falls } \ a > 0 \\ 0_K \text{ falls } a = 0 \\ |a|(-1) \cdot (b1)^{-1} \text{ falls } \ a < 0 \end{cases}$$

Wir zeigen, das $f$ ein Homomorphismus ist Zur besseren Lesbarkeit schreiben wir $n1 \mathrel{\hat{=}} n$ und $(n1)^{-1} \mathrel{\hat{=}} n^{-1}$

$$f\left(\frac{a}{b}\right) + f\left(\frac{c}{d}\right) = a \cdot b^{-1} + c \cdot d^{-1}$$

$$= b^{-1}(a + c \cdot b \cdot d^{-1}) = b^{-1} \cdot d^{-1} \cdot (a \cdot d + c \cdot b) = (b \cdot d)^{-1} \cdot (a \cdot d + c \cdot b) = f\left(\frac{ad + cb}{bd}\right) = f\left(\frac{a}{b} + \frac{b}{c}\right)$$

$$f\left(\frac{a}{b}\right) \cdot f\left(\frac{c}{d}\right) = a \cdot b^{-1} \cdot c \cdot d^{-1} = (a \cdot b) \cdot (b \cdot d)^{-1} = f\left(\frac{a}{b} \cdot \frac{c}{d}\right)$$

$$\Rightarrow f \text{ ist ein Homomorphismus}$$

$$\Rightarrow f \text{ ist injektiv Wir definieren}$$

$$g : \mathbb{Q} \to \mathrm{Bild}(f)$$

$$\frac{a}{b} \mapsto \begin{cases} a1 \cdot (b1)^{-1} \text{ falls } \ a > 0 \\ 0_K \text{ falls } a = 0 \\ |a|(-1) \cdot (b1)^{-1} \text{ falls } \ a < 0 \end{cases}$$

$$\Rightarrow \text{g ist ein Isomorphismus}$$

Es gilt außerdem, da $\mathrm{Bild}(f) \subseteq K$, dass das $\mathrm{Bild}(f)$ einen zu $\mathbb{Q}$ isomorphen Unterkörper in $K$ bildet

■

## c)

**Lemma 0.15**:

Kein endlicher Körper kann geordnet werden

*Proof*:

In einem geordneten Körper gilt:

$$0_K < 1_K$$

$$\alpha \leq \beta \Rightarrow \alpha + \gamma \leq \beta + \gamma$$

Angenommen es existiert ein endlicher geordneter Körper $(K, +, \cdot)$, dann

$$\exists m = \max(K)$$

Es gilt $\forall a \in K$

$$a + 1_K \leq m$$

Wähle $a = m$

$$\Rightarrow m + 1_K \leq m \Leftrightarrow m + 1_K \leq m + 0_K$$

$$\Rightarrow 1_K \leq 0_K$$

Das Wiederspricht den Rechenregeln in einem Körper

∎