Einführung in die Algebra
Übung 7

Beispiel 1.

a) Seien $n \in \mathbb{N}$ und $A, B, C \in M_n(\mathbb{R})$ und definiere

$$\mathbf{0} := \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{pmatrix}$$
$$\mathbf{1} := E_n$$

Überprüfe Ringeigenschaften:

- $A + \mathbf{0} = A$ ✓
- $A + (-A) = \mathbf{0}$ ✓
- $(A + B) + C = A + (B + C)$ ✓
- $A + B = B + A$ ✓
- Für $1 \leq i, j \leq n$:
  $[(A \cdot B) \cdot C]_{ij} = \sum\limits_{k=1}^{n} (A \cdot B)_{ik} C_{kj} = \sum\limits_{k=1}^{n} \left(\sum\limits_{l=1}^{n} A_{il} B_{lk} \right) C_{kj} = \sum\limits_{l=1}^{n} A_{il} \left(\sum\limits_{k=1}^{n} B_{lk} C_{kj} \right) =$
  $[A \cdot (B \cdot C)]_{ij}$, also $(A \cdot B) \cdot C = A \cdot (B \cdot C)$ ✓
- $A \cdot \mathbf{1} = A$ ✓
- $A \cdot (B + C) = A \cdot B + A \cdot C$ ✓
- $(B + C) \cdot A = B \cdot A + C \cdot A$ ✓

$A \cdot B = B \cdot A$ gilt nur für $n = 1$, da die Matrixmultiplikation für $n \geq 2$ nicht kommutativ ist.

b) K Körper $\Longrightarrow M_n(K)$ einfach.

Sei I ein Ideal von $M_n(K)$, das nicht gleich dem Nullideal ist, dann gibt es eine Matrix $A = (a_{ij}) \in I$ die zumindest einen nicht Nulleintrag in der k-ten Zeile und l-ten Spalte hat, also $a_{kl} \neq 0$. Aus den Idealeigenschaften folgt, dass für alle $M_1, M_2 \in M_n(K)$ und alle $A \in I$ gilt $M_1 \cdot A \in I$ und $A \cdot M_2 \in I$.

Wir definieren $M_{ij} = (m_{\alpha\beta})$ als die Matrix, dessen Eintrag $m_{ij} = 1$ ist und sonst nur Nulleinträge besitzt, weiter sei $N_{ij} = \operatorname{diag}(\frac{1}{a_{ij}}, \ldots, \frac{1}{a_{ij}})$.

Dann ist $M_{ik} A M_{lj} = a_{kl} M_{ij}$ in I, folglich ist auch $N_{kl} M_{ik} A M_{lj} = M_{ij}$ in I. Da alle M_{ii} in I liegt, so ist wegen der Idealeigenschaft auch die Summe der M_{ii} in I, $\sum_{i=1}^{n} M_{ii}$ ist jedoch die Einheitsmatrix, d.h. $I = M_n(K)$.

Somit besitzt $M_n(K)$ nur die Ideale $\{0\}$ und $M_n(K)$, d.h. $M_n(K)$ ist einfach.

Beispiel 2.

"$\Leftarrow$": Sei $I = I_1 \times I_2$ und $x = (x_1, x_2) \in I, y = (y_1, y_2) \in I$, dann gilt $x - y = (x_1 - y_1, x_2 - y_2) \in I$. Sei weiters $r = (r_1, r_2) \in R_1 \times R_2$, dann gilt $rx = (r_1 x_1, r_2 x_2) \in I$ sowie $xr = (x_1 r_1, x_2 r_2) \in I$. Also $I \trianglelefteq R_1 \times R_2$.

"$\Rightarrow$": Sei $I \trianglelefteq R_1 \times R_2$ und $x = (x_1, x_2) \in I, y = (y_1, y_2) \in I, r = (r_1, r_2) \in R_1 \times R_2$, dann gibt es Mengen $I_1 \subset R_1, I_2 \subset R_2 : I = I_1 \times I_2$ und es gilt

$$\begin{aligned} x - y &= (x_1 - y_1, x_2 - y_2) && \in I_1 \times I_2 \\ rx &= (r_1 x_1, r_2 x_2) && \in I_1 \times I_2 \\ xr &= (x_1 r_1, x_2 r_2) && \in I_1 \times I_2 \end{aligned}$$

Komponentenweise gelesen sind das die Idealeigenschaften für I_1, I_2, daher gilt $I_1 \trianglelefteq R_1, I_2 \trianglelefteq R_2$.

Beispiel 3. Wann ist $h : \mathbb{Z}_n \to \mathbb{Z}_m, [x]_n \mapsto [x]_m$ ein Homomorphismus?

Wir leiten zuerst eine notwendige Bedingung her, dass h überhaupt ein Homomorphismus sein kann. Wir nehmen also an, dass h wohldefiniert und ein Homomorphismus ist:

Das Element $[1]_n$ hat Ordnung n in $\mathbb{Z}_n$, dann hat $h([1]_n)$ höchstens Ordnung n in $\mathbb{Z}_m$, da $\underbrace{h([1]_n) + \ldots + h([1]_n)}_{n-\text{mal}} = h(\underbrace{[1]_n + \ldots + [1]_n}_{n-\text{mal}}) = h([0]_n) = [0]_m$. Wir wissen jedoch, dass $[1]_m = h([1]_n)$ Ordnung m hat, d.h. $m \mid n$.

Wir zeigen nun, dass h genau dann ein Homomorphismus ist, falls $m \mid n$.

- h ist wohldefiniert:
  Sei $[a]_n = [b]_n$, dann ist $a \equiv b \mod n$ oder anders ausgedrückt es existiert $k \in \mathbb{N}$, sodass $a - b = kn$, nach Voraussetzung gibt es $l \in \mathbb{N}$, sodass $n = lm$, insgesamt gilt also $a - b = kn = klm$, d.h. $a \equiv b \mod m$ und somit $[a]_m = [b]_m$ oder anders ausgedrückt $h([a]_n) = h([b]_n)$, also ist h wohldefiniert.
- h ist ein Homomorphismus:

$$h([a]_n + [b]_n) = h([a + b]_n) = [a + b]_m = [a]_m + [b]_m = h([a]_n) + h([b]_n)$$

- h ist genau dann ein Isomorphismus, wenn $n = m$.
- h ist genau dann ein Monomorphismus, wenn $n = m$.
- h ist immer ein Epimorphismus.

Beispiel 4. $h : R \to S$

a) $h(R) = \{h(r) \mid r \in R\} \leq S$

   Seien $a, b \in h(R)$ dann gibt es $x, y \in R$, sodass $h(x) = a, h(y) = b$.

   i) $0, 1 \in h(R)$, da $h(0_R) = 0_S$ und $h(1_R) = 1_S$

   ii) $a - b = h(x) - h(y) = h(x - y) \in h(R)$

   iii) $a \cdot b = h(x) \cdot h(y) = h(xy) \in h(R)$

b) $\ker h = \{r \in R \mid h(r) = 0\} \trianglelefteq R$

   i) $0 \in \ker h$

   ii) Seien $a, b \in \ker h$ dann gilt $h(a - b) = h(a) - h(b) = 0 - 0 = 0$ also $a - b \in \ker h$

   iii) Sei $a \in \ker h$ und $r \in R$, dann ist $h(r \cdot a) = h(r) \cdot h(a) = h(r) \cdot 0 = 0$, d.h. $ra \in \ker h$