# Serie 8:
# Komposition und Matrixmultiplikation, Invertierbarkeit und Isomorphismen

**1.**

$$
\begin{aligned}
A(2B+3C) &= \begin{pmatrix} 1 & 3 \\ 2 & -1 \end{pmatrix} \left[ 2 \begin{pmatrix} 1 & 0 & -3 \\ 4 & 1 & 2 \end{pmatrix} + 3 \begin{pmatrix} 1 & 1 & 4 \\ -1 & -2 & 0 \end{pmatrix} \right] \\
&= \begin{pmatrix} 1 & 3 \\ 2 & -1 \end{pmatrix} \left[ \begin{pmatrix} 2 & 0 & -6 \\ 8 & 2 & 4 \end{pmatrix} + \begin{pmatrix} 3 & 3 & 12 \\ -3 & -6 & 0 \end{pmatrix} \right] \\
&= \begin{pmatrix} 1 & 3 \\ 2 & -1 \end{pmatrix} \begin{pmatrix} 5 & 3 & 6 \\ 5 & -4 & 4 \end{pmatrix} \\
&= \begin{pmatrix} 1\cdot 5 + 3\cdot 5 & 1\cdot 3 + 3\cdot(-4) & 1\cdot 6 + 3\cdot 4 \\ 2\cdot 5 + (-1)\cdot 5 & 2\cdot 3 + (-1)\cdot(-4) & 2\cdot 6 + (-1)\cdot 4 \end{pmatrix} \\
&= \begin{pmatrix} 20 & -9 & 18 \\ 5 & 10 & 8 \end{pmatrix} \\
(AB)D &= \left[ \begin{pmatrix} 1 & 3 \\ 2 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 & -3 \\ 4 & 1 & 2 \end{pmatrix} \right] \begin{pmatrix} 2 \\ -2 \\ 3 \end{pmatrix} \\
&= \begin{pmatrix} 13 & 3 & 3 \\ -2 & -1 & -8 \end{pmatrix} \begin{pmatrix} 2 \\ -2 \\ 3 \end{pmatrix} \\
&= \begin{pmatrix} 29 \\ -26 \end{pmatrix}
\end{aligned}
$$

und Assoziativität der Matrixmultiplikation impliziert $A(BD) = \left(\begin{smallmatrix} 29 \\ -26 \end{smallmatrix}\right)$.

**2.** **a)** Sei $A \in M_{n\times n}(\mathbb{K})$ invertierbar und seien $B, C \in M_{n\times n}(\mathbb{K})$ zwei Inverse von $A$, dann ist

$$C = I_n C = (BA)C = B(AC) = BI_n = B$$

und somit ist die Inverse eindeutig.

**b)** Wir zeigen zuerst, dass $L_A$ invertierbar ist. Da $AB = I_n$, gilt $\mathrm{Ker}(L_{AB}) = \mathrm{Ker}(I_n) = \{0\}$.

Daraus folgt bereits, dass $L_A$ invertierbar ist. Um das zu sehen, zeigen wir zuerst, dass $\mathrm{Ker}(L_B) = \{0\}$. Sei $v \in \mathrm{Ker}(L_B)$, dann ist

$$L_{AB}(v) = (L_A \circ L_B)(v) = L_A(L_B(v)) = L_A(0) = 0$$

also $v \in \mathrm{Ker}(L_A \circ L_B) = \mathrm{Ker}(L_{AB}) = \{0\}$ und folglich $\mathrm{Ker}(L_B) = \{0\}$. Da $L_B : \mathbb{K}^n \to \mathbb{K}^n$, ist $L_B$ bijektiv. Also ist $L_B$ invertierbar und somit

$$(L_B)^{-1} = L_{I_n} \circ (L_B)^{-1} = (L_A \circ L_B) \circ (L_B)^{-1} = L_A \circ (L_B \circ (L_B)^{-1}) = L_A$$

Da $L_B$ invertierbar ist, ist auch $L_A = (L_B)^{-1}$ invertierbar und wie in der Vorlesung gezeigt ist also $A$ invertierbar.

Es folgt

$$BA = I_n(BA) = (A^{-1}A)(BA) = A^{-1}(AB)A = A^{-1}I_nA = A^{-1}A = I_n$$

und somit $BA = AB = I_n$ und $B$ ist eine Inverse von $A$, sprich $B = A^{-1}$.

**c)**
- Berechne

$$((AB)^T)_{ij} = (AB)_{ji} = \sum_{k=1}^{n} A_{jk}B_{ki} = \sum_{k=1}^{n} (A^T)_{kj}(B^T)_{ik} = (B^TA^T)_{ij}$$

- Sei $A$ invertierbar und sei $B \in M_{n\times n}(\mathbb{K})$ mit $AB = BA = I_n$. Dann ist wegen dem soeben gezeigten

$$A^TB^T = (BA)^T = I_n^T = I_n \text{ und } B^TA^T = (AB)^T = I_n^T = I_n$$

  Also ist $A^T$ invertierbar und $(A^T)^{-1} = B^T = (A^{-1})^T$.
- Seien $A, B$ invertierbar, dann ist wegen der Assoziativität der Matrixmultiplikation

$$(B^{-1}A^{-1})AB = B^{-1}(A^{-1}A)B = B^{-1}I_nB = B^{-1}B = I_n$$

  und

$$AB(B^{-1}A^{-1}) = A(BB^{-1})A^{-1} = AI_nA^{-1} = AA^{-1} = I_n$$

  Also ist $AB$ invertierbar und $(AB)^{-1} = B^{-1}A^{-1}$.

**Siehe nächstes Blatt!**

**3.** **a)** **Reflexivität:** Sei $V$ ein Vektorraum, dann ist $I_V : V \to V$ bijektiv – also invertierbar – und linear, folglich ist $V \cong V$.

**Symmetrie:** Seien $V, W$ Vektorräume über $\mathbb{K}$ und $V \cong W$, dann existiert $T \in \mathrm{Hom}(V,W)$ invertierbar. Wie in der Vorlesung gezeigt wurde, ist dann $T^{-1} \in \mathrm{Hom}(W,V)$. $T^{-1}$ ist invertierbar, folglich gilt $W \cong V$.

**Transitivität:** Seien $U, V, W$ Vektorräume über $\mathbb{K}$ und $U \cong V$, $V \cong W$. Dann existieren $T_1 \in \mathrm{Hom}(U,V)$, $T_2 \in \mathrm{Hom}(V,W)$ invertierbar oder (dazu äquivalent) bijektiv. Dann ist $T_2 \circ T_1 : U \to W$ ebenfalls bijektiv und, wie in der Vorlesung besprochen, linear. Also ist $T_2 \circ T_1 \in \mathrm{Hom}(U,W)$ invertierbar und folglich $U \cong W$.

**b)** 1. **"$\Rightarrow$":** Sei $T$ injektiv und sei $\{v_1, \ldots, v_n\}$ eine Basis von $V$. Für alle $i$ sei $w_i := T(v_i)$. Da $T$ injektiv ist, ist $\{w_1, \ldots, w_n\} \subset W$ linear unabhängig. Seien $w_{n+1}, \ldots, w_m \in W$ so dass $\{w_1, \ldots, w_m\}$ eine Basis von $W$ ist. Wie in der Vorlesung bewiesen, existiert genau ein $S \in \mathrm{Hom}(W,V)$, so dass

$$S(w_i) = \begin{cases} v_i & \text{falls } 1 \leq i \leq n \\ 0 & \text{sonst} \end{cases}$$

Für $1 \leq i \leq n$ gilt $(ST)(v_i) = S(T(v_i)) = S(w_i) = v_i$ und somit ist $ST = I_V$.

**"$\Leftarrow$":** Angenommen $S \in \mathrm{Hom}(W,V)$ mit $ST = I_V$. Sei $v \in \mathrm{Ker}(T)$, dann ist $v = I_V(v) = (ST)(v) = S(T(v)) = S(0) = 0$, folglich ist $T$ injektiv.

2. **"$\Rightarrow$":** Sei $T$ surjektiv und sei $\{w_1, \ldots, w_m\}$ eine Basis von $W$. Da $T$ surjektiv ist, finden wir $v_1, \ldots, v_m \in V$ so dass $w_i = T(v_i)$. Sei $S : W \to V$ die eindeutig bestimmte lineare Abbildung mit $S(w_i) = v_i$ – man sagt auch $S$ ist die lineare Erweiterung von $S(w_i) := v_i$ –, dann ist

$$(TS)(w_i) = T(S(w_i)) = T(v_i) = w_i$$

und somit ist $TS = I_W$.

**"$\Leftarrow$":** Sei $S \in \mathrm{Hom}(W,V)$ beliebig. Sei $w \in \mathrm{Im}(TS)$, dann existiert $\tilde{w} \in W$ mit $w = (TS)(\tilde{w}) = T(S(\tilde{w}))$ und somit $w \in \mathrm{Im}(T)$. Wir haben also gezeigt, dass $\mathrm{Im}(TS) \subset \mathrm{Im}(T)$.
Sei nun also $S \in \mathrm{Hom}(W,V)$ mit $TS = I_W$, dann ist

$$W = \mathrm{Im}(I_W) = \mathrm{Im}(TS) \subset \mathrm{Im}(T)$$

und folglich ist $T$ surjektiv.

**4.** **a)** Wie in der Vorlesung gezeigt, gilt für beliebige $A \in M_{m \times n}(\mathbb{K})$ und $B \in M_{n \times p}(\mathbb{K})$ die Gleichung

$$L_A \circ L_B = L_{AB}$$

**Bitte wenden!**

Folglich sind $L_A^2 = L_{A^2}$ und $L_A^3 = L_{A^3}$. Wir berechnen

$$A^2 = \begin{pmatrix} 2 & 2 & -10 \\ 1 & 2 & -7 \\ 0 & 2 & -4 \end{pmatrix} \begin{pmatrix} 2 & 2 & -10 \\ 1 & 2 & -7 \\ 0 & 2 & -4 \end{pmatrix} = \begin{pmatrix} 6 & -12 & 6 \\ 4 & -8 & 4 \\ 2 & -4 & 2 \end{pmatrix}$$
$$A^3 = \begin{pmatrix} 2 & 2 & -10 \\ 1 & 2 & -7 \\ 0 & 2 & -4 \end{pmatrix} \begin{pmatrix} 6 & -12 & 6 \\ 4 & -8 & 4 \\ 2 & -4 & 2 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Also ist $L_A^2 \neq 0$ (bspw. ist $L_A^2(e_1) = (6, 4, 2)^T$), und $L_A^3 = 0$.

**b)** Seien $w := e_1$, $v := L_A(w)$ und $u := L_A(v)$. Wir müssen zeigen, dass $\{u, v, w\}$ linear unabhängig ist. Seien $\lambda, \mu, \nu \in \mathbb{R}$ und

$$0 = \lambda w + \mu v + \nu u = \lambda \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + \mu \begin{pmatrix} 2 \\ 1 \\ 0 \end{pmatrix} + \nu \begin{pmatrix} 6 \\ 4 \\ 2 \end{pmatrix} = \begin{pmatrix} \lambda + 2\mu + 6\nu \\ \mu + 4\nu \\ 2\nu \end{pmatrix}$$

dann folgt $\lambda = \mu = \nu = 0$ und folglich ist $\{u, v, w\}$ linear unabhängig. Es ist (wie bereits oben berechnet)

$$L_A(u) = \begin{pmatrix} 2 & 2 & -10 \\ 1 & 2 & -7 \\ 0 & 2 & -4 \end{pmatrix} \begin{pmatrix} 6 \\ 4 \\ 2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

wie gewünscht.

Es gilt

$$\begin{aligned} L_A(u) =& 0 = 0u + 0v + 0w \\ L_A(v) =& u = 1u + 0v + 0w \\ L_A(w) =& v = 0u + 1v + 0w \end{aligned}$$

und folglich

$$[L_A]_{(u,v,w)} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

**5. a)** Wir berechnen $({A_\mathcal{G}}^r)_{ij}$. Wir wissen, dass

$$({A_\mathcal{G}}^2)_{ij} = \sum_{k=1}^{n} (A_\mathcal{G})_{ik} (A_\mathcal{G})_{kj}$$

**Siehe nächstes Blatt!**

Angenommen $r \geq 2$ und

$$(A_{\mathcal{G}}{}^r)_{ij} = \sum_{k_1,\ldots,k_{r-1}=1}^{n} (A_{\mathcal{G}})_{ik_1} (A_{\mathcal{G}})_{k_{r-1}j} \prod_{l=1}^{r-2} (A_{\mathcal{G}})_{k_l k_{l+1}}$$

Dann ist

$$\begin{aligned}
(A_{\mathcal{G}}{}^{r+1})_{ij} &= \sum_{k=1}^{n} (A_{\mathcal{G}}{}^r)_{ik} (A_{\mathcal{G}})_{kj} \\
&= \sum_{k,k_1,\ldots,k_{r-1}}^{n} (A_{\mathcal{G}})_{ik_1} (A_{\mathcal{G}})_{k_{r-1}k} (A_{\mathcal{G}})_{kj} \prod_{l=1}^{r-2} (A_{\mathcal{G}})_{k_l k_{l+1}} \\
&= \sum_{k_1,\ldots,k_r}^{n} (A_{\mathcal{G}})_{ik_1} (A_{\mathcal{G}})_{k_r j} \prod_{l=1}^{r-1} (A_{\mathcal{G}})_{k_l k_{l+1}}
\end{aligned}$$

Nun ist

$$\begin{aligned}
&(A_{\mathcal{G}})_{ik_1} (A_{\mathcal{G}})_{k_{r-1}j} \prod_{l=1}^{r-2} (A_{\mathcal{G}})_{k_l k_{l+1}} \\
&\quad = \begin{cases} 1 & \text{falls } (A_{\mathcal{G}})_{ik_1} = (A_{\mathcal{G}})_{k_l k_{l+1}} = (A_{\mathcal{G}})_{k_{r-1}j} = 1 \\ 0 & \text{sonst} \end{cases}
\end{aligned}$$

Also ist $(A_{\mathcal{G}})_{ik_1} (A_{\mathcal{G}})_{k_{r-1}j} \prod_{l=1}^{r-1} (A_{\mathcal{G}})_{k_l k_{l+1}} = 1$ genau dann, wenn $(i, k_1, \ldots, k_{r-1}, j)$ ein Weg in $\mathcal{G}$ der Länge $r$ von $i$ nach $j$ ist und $0$ sonst.

Somit ist $(A_{\mathcal{G}}{}^r)_{ij} = m$ genau dann, wenn es genau $m$ Wege der Länge $r$ in $\mathcal{G}$ von $i$ nach $j$ gibt und die allgemeinere Äquivalenz folgt sofort.

**b)** Wir sagen $i \in V$ ist *dominant*, falls $(A_{\mathcal{G}} + A_{\mathcal{G}}{}^2)_{ij} > 0$ für alle von $i$ verschiedenen $j \in i$. Sei $i \in V$ beliebig und sei $j \in V$ mit $(A_{\mathcal{G}} + A_{\mathcal{G}}{}^2)_{ij} = 0$. Wir behaupten, dass jedes durch $i$ dominierte Element durch $j$ dominiert ist. Angenommen $i$ dominiert $k$ und $j$ dominiert $k$ *nicht*, dann ist $A_{ik} = 1$ und $A_{jk} = 0$, also $A_{kj} = 1$ und folglich

$$(A_{\mathcal{G}} + A_{\mathcal{G}}{}^2)_{ij} = A_{ij} + \sum_{l=1}^{n} A_{il} A_{lj} \geq A_{ik} A_{kj} = 1$$

im Widerspruch zur Annahme.

Im Folgenden sei $d(i) := \{j \in V \mid i \text{ dominiert } j\}$. Sei $i_0 \in V$ beliebig. Falls $(A_{\mathcal{G}} + A_{\mathcal{G}}{}^2)_{i_0 j} > 0$ für alle von $i_0$ verschiedenen $j \in V$, dann sind wir fertig. Andernfalls existiert ein $i_1 \in V$ mit $(A_{\mathcal{G}} + A_{\mathcal{G}}{}^2)_{i_0 i_1} = 0$.

**Bitte wenden!**

Seien nun $i_0, \ldots, i_r \in V$ mit $(A_{\mathcal{G}} + A_{\mathcal{G}}{}^2)_{i_l i_{l+1}} = 0$ für $0 \leq l \leq r$. Wegen $(A_{\mathcal{G}} + A_{\mathcal{G}}{}^2)_{i_l i_{l+1}} = 0$ ist insbesondere $A_{i_{l+1} i_l} = 1$ und somit ist $d(i_l) < d(i_{l+1})$. Also ist $r \leq d(i_r)$. Falls $i_r$ dominant ist, sind wir fertig. Andernfalls existiert $i_{r+1} \in V$ mit $(A_{\mathcal{G}} + A_{\mathcal{G}}{}^2)_{i_r i_{r+1}} = 0$ und es gilt $r + 1 \leq d(i_{r+1})$. Da $d(i) \leq |V| - 1$, ist dies nur endlich viele Male möglich, d.h. die Konstruktion bricht irgendwann ab. Es existiert also ein $r^*$ so dass $(A_{\mathcal{G}} + A_{\mathcal{G}}{}^2)_{i_{r^*} j} > 0$ für alle von $i_{r^*}$ verschiedenene $j \in V$.

**6. a)** Die bilineare Fortsetzung heisst, dass für jedes $v \in V$ die Abbildung

$$\varphi_v : V \to V; w \mapsto v \cdot w$$

ein Endomorphismus, und dass die Abbildung $\varphi : V \to \mathrm{End}(V)$, $v \mapsto \varphi_v$ ein Homomorphismus ist. Wir bemerken, dass

$$(\varphi_u \circ \varphi_v)(w) = u \cdot (v \cdot w) \quad \text{und} \quad \varphi_{\varphi_u(v)}(w) = (u \cdot v) \cdot w$$

Das heisst, wir fordern $\varphi_u \circ \varphi_v = \varphi_{\varphi_u(v)}$. Wir nennen dies im Folgenden die *Assoziativität von* $\varphi$.

Im Folgenden sei $\mathcal{B} = \{\mathbf{1}, \mathbf{i}, \mathbf{j}, \mathbf{k}\}$.

Für jedes $v \in V$ ist ein $\varphi_v$ wie oben durch $(\varphi_v(\mathbf{1}), \varphi_v(\mathbf{i}), \varphi_v(\mathbf{j}), \varphi_v(\mathbf{k}))$ vollständig bestimmt und $\varphi$ ist durch $(\varphi_{\mathbf{1}}, \varphi_{\mathbf{i}}, \varphi_{\mathbf{j}}, \varphi_{\mathbf{k}})$. $\varphi_{\mathbf{1}} = I_V$ ist sicherlich wohldefiniert. Gegeben $\varphi_{\mathbf{1}}, \varphi_{\mathbf{i}}, \varphi_{\mathbf{j}}, \varphi_{\mathbf{j}} \in \mathrm{End}(V)$ wie in der Aufgabenstellung, d.h.

$$\begin{aligned} \varphi_{\mathbf{1}} =& I_V \\ \varphi_{\mathbf{i}}(\mathbf{1}) =& \mathbf{i}, \quad \varphi_{\mathbf{i}}(\mathbf{i}) = a\mathbf{1}, \quad \varphi_{\mathbf{i}}(\mathbf{j}) = \mathbf{k} \\ \varphi_{\mathbf{j}}(\mathbf{1}) =& \mathbf{j}, \quad \varphi_{\mathbf{j}}(\mathbf{i}) = -\mathbf{k}, \quad \varphi_{\mathbf{j}}(\mathbf{j}) = b\mathbf{1} \end{aligned} \tag{$\heartsuit$}$$

so dass $\varphi_v \circ \varphi_w = \varphi_{\varphi_v(w)}$ für alle $v, w \in \mathcal{B}$, dann folgt aus der Assoziativität und der Linearität von $\varphi$, dass

$$\begin{aligned} \varphi_{\mathbf{i}}(\mathbf{k}) =& (\varphi_{\mathbf{i}} \circ \varphi_{\mathbf{i}})(j) = \varphi_{\varphi_{\mathbf{i}}(i)}(\mathbf{j}) = \varphi_{a\mathbf{1}}(\mathbf{j}) \\ =& (a\varphi_{\mathbf{1}})(\mathbf{j}) = a\varphi_{\mathbf{1}}(\mathbf{j}) = a\mathbf{j} \\ \varphi_{\mathbf{j}}(\mathbf{k}) =& (\varphi_{\mathbf{j}} \circ \varphi_{-\mathbf{j}})(i) = \varphi_{\varphi_{\mathbf{j}}(-j)}(\mathbf{i}) = \varphi_{-b\mathbf{1}}(\mathbf{i}) \\ =& (-b\varphi_{\mathbf{1}})(\mathbf{i}) = -b\varphi_{\mathbf{1}}(\mathbf{i}) = -b\mathbf{i} \end{aligned}$$

sowie $\varphi_{\mathbf{k}} = \varphi_{\varphi_{\mathbf{i}}(\mathbf{j})} = \varphi_{\mathbf{i}} \circ \varphi_{\mathbf{j}}$. Also sind $\varphi_{\mathbf{1}}, \varphi_{\mathbf{i}}, \varphi_{\mathbf{j}}, \varphi_{\mathbf{k}}$ durch Annahme der Assoziativität und Linearität von $\varphi$ sowie Relationen in ($\heartsuit$) vollständig bestimt und somit auch die lineare Abbildung $\varphi$.

Seien nun $\varphi_{\mathbf{1}}, \varphi_{\mathbf{i}}, \varphi_{\mathbf{j}}, \varphi_{\mathbf{k}}$ die eindeutigen Endomorphismen von $V$ von oben, d.h. $\varphi_{\mathbf{1}}$, $\varphi_{\mathbf{i}}$ und $\varphi_{\mathbf{j}}$ erfüllen die Relationen in ($\heartsuit$), $\varphi_{\mathbf{i}}(\mathbf{k}) = a\mathbf{j}$, $\varphi_{\mathbf{j}}(\mathbf{k}) = -b\mathbf{i}$ und

**Siehe nächstes Blatt!**

$\varphi_{\mathbf{k}} := \varphi_{\mathbf{i}} \circ \varphi_{\mathbf{j}}$. Wir definieren $\varphi \in \mathrm{Hom}(V, \mathrm{End}(V))$ als die eindeutige lineare Abbildung mit

$$\forall v \in \mathcal{B}: \ \varphi(v) = \varphi_v$$

Wir müssen zeigen, dass $\varphi$ assoziativ ist. Zuerst überprüft man explizit, dass für alle $u, v \in \mathcal{B}$ gilt

$$\varphi_u \circ \varphi_v = \varphi_{\varphi_u(v)}$$

Tatsächlich ist

$$\varphi_{\mathbf{1}} \circ \varphi_u = \varphi_u = \varphi_u \circ \varphi_{\mathbf{1}} \quad (u \in \mathcal{B})$$

und da $\varphi_{\mathbf{1}}(u) = \varphi_u(\mathbf{1}) = u$ für alle $u \in \mathcal{B}$, folgt die Assoziativität von $\varphi$ für Paare in $\mathcal{B}$, wo mindestens ein Element gleich $\mathbf{1}$ ist. In den anderen Fällen überprüft man explizit. So ist beispielsweise $\varphi_{\varphi_{\mathbf{j}}(\mathbf{k})} = -b\varphi_{\mathbf{i}}$ und folglich

$$\begin{aligned}
\varphi_{\mathbf{j}} \circ \varphi_{\mathbf{k}}(\mathbf{1}) =&\varphi_{\mathbf{j}}(\mathbf{k}) = -b\mathbf{i} \\
\varphi_{\mathbf{j}} \circ \varphi_{\mathbf{k}}(\mathbf{i}) =&\varphi_{\mathbf{j}} \circ \varphi_{\mathbf{i}} \circ \varphi_{\mathbf{j}}(\mathbf{i}) = -\varphi_{\mathbf{j}} \circ \varphi_{\mathbf{i}}(\mathbf{k}) = -a\varphi_{\mathbf{j}}(\mathbf{j}) = -ab\mathbf{1} \\
\varphi_{\mathbf{j}} \circ \varphi_{\mathbf{k}}(\mathbf{j}) =&\varphi_{\mathbf{j}} \circ \varphi_{\mathbf{i}} \circ \varphi_{\mathbf{j}}(\mathbf{j}) = b\varphi_{\mathbf{j}} \circ \varphi_{\mathbf{i}}(\mathbf{1}) = b\varphi_{\mathbf{j}}(\mathbf{i}) = -b\mathbf{k} \\
\varphi_{\mathbf{j}} \circ \varphi_{\mathbf{k}}(\mathbf{k}) =&\varphi_{\mathbf{j}} \circ \varphi_{\mathbf{i}} \circ \varphi_{\mathbf{j}}(\mathbf{k}) = -b\varphi_{\mathbf{j}} \circ \varphi_{\mathbf{i}}(\mathbf{i}) = -ab\varphi_{\mathbf{j}}(\mathbf{1}) = -ab\mathbf{j} \\
\varphi_{\varphi_{\mathbf{j}(\mathbf{k})}}(\mathbf{1}) =& - b\varphi_{\mathbf{i}}(\mathbf{1}) = -b\mathbf{i} \\
\varphi_{\varphi_{\mathbf{j}}(\mathbf{k})}(\mathbf{i}) =& - b\varphi_{\mathbf{i}}(\mathbf{i}) = -ab\mathbf{1} \\
\varphi_{\varphi_{\mathbf{j}}(\mathbf{k})}(\mathbf{j}) =& - b\varphi_{\mathbf{i}}(\mathbf{j}) = -b\mathbf{k} \\
\varphi_{\varphi_{\mathbf{j}}(\mathbf{k})}(\mathbf{k}) =& - b\varphi_{\mathbf{i}}(\mathbf{k}) = -ab\mathbf{j}
\end{aligned}$$

Dies beweist, dass $\varphi_{\mathbf{j}} \circ \varphi_{\mathbf{k}} = \varphi_{\varphi_{\mathbf{j}}(\mathbf{k})}$. Die anderen Fälle überprüft man analog.

Seien nun $u_1, u_2, v_1, v_2 \in V$ gegeben, so dass $\varphi_{u_i} \circ \varphi_{v_j} = \varphi_{\varphi_{u_i}(v_j)}$ für $i, j = 1, 2$. Dann ist für $\lambda_1, \lambda_2, \mu_1, \mu_2 \in \mathbb{K}$

$$\begin{aligned}
\varphi_{\lambda_1 u_1 + \lambda_2 u_2} \circ \varphi_{\mu_1 v_1 + \mu_2 u_2} =&(\lambda_1 \varphi_{u_1} + \lambda_2 \varphi_{u_2}) \circ (\mu_1 \varphi_{v_1} + \mu_2 \varphi_{v_2}) \\
=&\sum_{i,j=1}^{2} \lambda_i \mu_j (\varphi_{u_i} \circ \varphi_{v_j}) = \sum_{i,j=1}^{2} \lambda_i \mu_j \varphi_{\varphi_{u_i}(v_j)} \\
=&\sum_{i=1}^{2} \lambda_i \varphi_{\varphi_{u_i}(\mu_1 v_1 + \mu_2 v_2)} \\
=&\varphi_{\lambda_1 \varphi_{u_1}(\mu_1 v_1 + \mu_2 v_2)} + \varphi_{\lambda_2 \varphi_{u_2}(\mu_1 v_1 + \mu_2 v_2)} \\
=&\varphi_{\varphi_{\lambda_1 u_1 + \lambda_2 u_2}(\mu_1 v_1 + \mu_2 v_2)}
\end{aligned}$$

Also gilt die Assoziativität von $\varphi$ für Linearkombinationen zweier Elemente in $\mathcal{B}$. Das Argument nochmals angewendet auf solche Linearkombination, liefert die Assoziativität für Linearkombinationen von vier Elementen in $\mathcal{B}$ und da letzteres eine Basis ist, folgt Assoziativität von $\varphi$ für alle Paare in $V \times V$, d.h.

$$\varphi_u \circ \varphi_v = \varphi_{\varphi_u(v)} \quad (u, v \in V)$$

**Bitte wenden!**

| $\overline{u\cdot v}$ | $\mathbf{1}$ | $\mathbf{i}$ | $\mathbf{j}$ | $\mathbf{k}$ |
|---|---|---|---|---|
| $\mathbf{1}$ | $\mathbf{1}$ | $-\mathbf{i}$ | $-\mathbf{j}$ | $-\mathbf{k}$ |
| $\mathbf{i}$ | $-\mathbf{i}$ | $a\mathbf{1}$ | $-\mathbf{k}$ | $-a\mathbf{j}$ |
| $\mathbf{j}$ | $-\mathbf{j}$ | $\mathbf{k}$ | $b\mathbf{1}$ | $b\mathbf{i}$ |
| $\mathbf{k}$ | $-\mathbf{k}$ | $a\mathbf{j}$ | $-b\mathbf{i}$ | $-ab\mathbf{1}$ |

Tabelle 1: Tabelle der $\overline{u\cdot v}$ für $u, v \in \mathcal{B}$.

**b)** Seien $\lambda \in \mathbb{K}$ und $v, w \in V$ mit

$$\begin{aligned} v =& x_1\mathbf{1} + x_2\mathbf{i} + x_3\mathbf{j} + x_4\mathbf{k} \\ w =& y_1\mathbf{1} + y_2\mathbf{i} + y_3\mathbf{j} + y_4\mathbf{k} \end{aligned}$$

Dann ist

$$\begin{aligned} \overline{v+\lambda w} =& (x_1+\lambda y_1)\mathbf{1} - (x_2+\lambda y_2)\mathbf{i} - (x_3+\lambda y_2)\mathbf{j} - (x_4+\lambda y_4)\mathbf{k} \\ =& (x_1\mathbf{1} - x_2\mathbf{i} - x_3\mathbf{j} - x_4\mathbf{k}) + \lambda(y_1\mathbf{1} - y_2\mathbf{i} - y_3\mathbf{j} - y_4\mathbf{k}) = \overline{v} + \lambda\overline{w} \end{aligned}$$

Sei $T_{\mathcal{B}} : V \to V$ die Abbildung

$$v \mapsto [v]_{(\mathbf{1},\mathbf{i},\mathbf{j},\mathbf{k})} \quad (v \in V)$$

Sei $A \in M_{4\times 4}(\mathbb{K})$ gegeben durch

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

Dann ist $\overline{v} = (T_{\mathcal{B}}^{-1} \circ L_A \circ T_{\mathcal{B}})(v)$ (man überprüft dies auf den Elementen von $\mathcal{B}$) und wegen $L_{A^2} = L_{I_4} = I_{\mathbb{K}^4}$ ist somit

$$\begin{aligned} \overline{\overline{v}} =& (T_{\mathcal{B}}^{-1} \circ L_A \circ T_{\mathcal{B}}) \circ (T_{\mathcal{B}}^{-1} \circ L_A \circ T_{\mathcal{B}})(v) \\ =& (T_{\mathcal{B}}^{-1} \circ L_A \circ L_A \circ T_{\mathcal{B}})(v) \\ =& (T_{\mathcal{B}}^{-1} \circ L_{A^2} \circ T_{\mathcal{B}})(v) = v \end{aligned}$$

Also ist $\bar{\cdot}$ eine Involution. Man überprüft für Elemente von $\mathcal{B}$ leicht, dass $\bar{\cdot}$ antimultiplikativ ist (vgl. Tabellen 1 und 2). Nun argumentiert man wie bei der Assoziativität von $\varphi$: Angenommen $u_1, u_2, v_1, v_2 \in V$, so dass $\overline{u_i \cdot v_j} = \overline{v_j} \cdot \overline{u_i}$, und $\lambda_1, \lambda_2, \mu_1, \mu_2 \in \mathbb{K}$. Dann ist

$$\overline{(\lambda_1 u_1 + \lambda_2 u_2)\cdot(\mu_1 v_1 + \mu_2 v_2)} = \overline{\sum_{i,j=1}^{2} \lambda_i \mu_j u_i \cdot v_j} = \sum_{i,j=1}^{2} \lambda_i \mu_j \overline{v_j} \cdot \overline{u_i}$$

**Siehe nächstes Blatt!**

| $\overline{v}\cdot\overline{u}$ | $\mathbf{1}$ | $\mathbf{i}$ | $\mathbf{j}$ | $\mathbf{k}$ |
|---|---|---|---|---|
| $\mathbf{1}$ | $\mathbf{1}\cdot\mathbf{1}=\mathbf{1}$ | $\overline{\mathbf{i}}\cdot\mathbf{1}=-\mathbf{i}$ | $\overline{\mathbf{j}}\cdot\mathbf{1}=-\mathbf{j}$ | $\overline{\mathbf{k}}\cdot\mathbf{1}=-\mathbf{k}$ |
| $\mathbf{i}$ | $\mathbf{1}\cdot\overline{\mathbf{i}}=-\mathbf{i}$ | $\overline{\mathbf{i}}\cdot\overline{\mathbf{i}}=a\mathbf{1}$ | $\overline{\mathbf{j}}\cdot\overline{\mathbf{i}}=-\mathbf{k}$ | $\overline{\mathbf{k}}\cdot\overline{\mathbf{i}}=-a\mathbf{j}$ |
| $\mathbf{j}$ | $\mathbf{1}\cdot\overline{\mathbf{j}}=-\mathbf{j}$ | $\overline{\mathbf{i}}\cdot\overline{\mathbf{j}}=\mathbf{k}$ | $\overline{j}\cdot\overline{j}=b\mathbf{1}$ | $\overline{k}\cdot\overline{j}=b\mathbf{i}$ |
| $\mathbf{k}$ | $\mathbf{1}\cdot\overline{\mathbf{k}}=-\mathbf{k}$ | $\overline{\mathbf{i}}\cdot\overline{\mathbf{k}}=a\mathbf{j}$ | $\overline{\mathbf{j}}\cdot\overline{\mathbf{k}}=-b\mathbf{i}$ | $\overline{k}\cdot\overline{k}=-ab\mathbf{1}$ |

Tabelle 2: Tabelle der $\overline{v}\cdot\overline{u}$ für $u,v\in\mathcal{B}$.

Andererseits ist

$$\begin{aligned}\overline{\mu_1 v_1+\mu_2 v_2}\cdot\overline{\lambda_1 u_1+\lambda_2 u_2} =&(\mu_1\overline{v_1}+\mu_2\overline{v_2})\cdot(\lambda_1\overline{u_1}+\lambda_2\overline{u_2})\\ =&\sum_{i,j=1}^{2}\lambda_i\mu_j\overline{v_j}\cdot\overline{u_i}\end{aligned}$$

Dies beweist, dass $\bar{\cdot}$ für Linearkombinationen von zwei Elementen in $\mathcal{K}$ antimultiplikativ ist. Dasselbe Argument nochmals angewendet auf Paare solcher Linearkombinationen impliziert, dass $\bar{\cdot}$ für beliebige Linearkombinationen von Elementen in $\mathcal{B}$ antimultiplikativ ist.

**c)** Wir bemerken, dass $\overline{N(x)}=\overline{x\cdot\overline{x}}=\overline{\overline{x}}\cdot\overline{x}=x\cdot\overline{x}=N(x)$. Es reicht also zu zeigen, dass $x\in\langle\mathbf{1}\rangle$ genau dann, wenn $\overline{x}=x$.

**"$\Rightarrow$":** Falls $x\in\langle\mathbf{1}\rangle$, dann ist $x=\lambda\mathbf{1}$ für ein $\lambda\in\mathbb{K}$ und also per definitionem $\overline{x}=\lambda\mathbf{1}=x$.

**"$\Leftarrow$":** Sei $x=x_1\mathbf{1}+x_2\mathbf{i}+x_3\mathbf{j}+x_4\mathbf{k}$, und sei $x=\overline{x}$, dann ist

$$0=x-\overline{x}=2x_2\mathbf{i}+2x_3\mathbf{j}+2x_4\mathbf{k}$$

und folglich sind $0=x_2=x_3=x_4$ und $x\in\langle\mathbf{1}\rangle$.

Für $u,v\in\mathcal{B}$ ist genau dann $u\cdot v\in\langle\mathbf{1}\rangle$, wenn $u=v$. Daraus und aus $N(x)\in\langle\mathbf{1}\rangle$ folgt

$$\begin{aligned}N(x)=&x_1^2\mathbf{1}\cdot\mathbf{1}-x_2^2\mathbf{i}\cdot\mathbf{i}-x_3^2\mathbf{j}\cdot\mathbf{j}-x_2^2\mathbf{k}\cdot\mathbf{k}\\ =&(x_1^2-ax_2^2-bx_3^2+abx_4^2)\mathbf{1}\end{aligned}$$

Für die Multiplikativität berechnen wir

$$N(x\cdot y)=x\cdot y\cdot\overline{x\cdot y}=x\cdot y\cdot\overline{y}\cdot\overline{x}=x\cdot N(y)\cdot\overline{x}=x\cdot\overline{x}\cdot N(y)=N(x)\cdot N(y)$$

da $\lambda\mathbf{1}\cdot v=v\cdot\lambda\mathbf{1}$ für alle $v\in V$.

Wir zeigen, dass $x\in V$ genau dann invertierbar ist, wenn $N(x)\neq 0$. Angenommen $x\in V$ ist invertierbar, d.h. es gibt $y\in V$, so dass $xy=\mathbf{1}$. Dann ist

$$\mathbf{1}=N(\mathbf{1})=N(xy)=N(x)N(y)$$

**Bitte wenden!**

und folglich ist $N(x) \neq 0$. Für die andere Richtung sei $N(x) \neq 0$, d.h. es gibt $\lambda \in \mathbb{K} \setminus \{0\}$, so dass $N(x) = \lambda \mathbf{1}$. Dann gilt

$$x \cdot (\lambda^{-1}\overline{x}) = \lambda^{-1}(x \cdot \overline{x}) = \lambda^{-1}N(x) = \mathbf{1}$$

**d)** Wir wissen von oben, dass für ein Element $x \in H_{-1,-1}(\mathbb{R})$ gilt

$$N(x) = (x_1^2 + x_2^2 + x_3^2 + x_4^2)\mathbf{1}$$

Somit ist $N(x) = 0$ genau dann, wenn $x = 0$ und $H_{-1,-1}(\mathbb{R})$ ist ein Schiefkörper.

**e)** Wir müssen zeigen, dass für $x \in \mathbb{Q}^4$ gilt

$$x_1^2 - ax_2^2 - px_3^2 + apx_4^2 = 0 \Rightarrow x = 0$$

Sei $x \in \mathbb{Q}^4$ wie oben. Schreibe $x_i = \frac{r_i}{s_i}$ mit $r_i \in \mathbb{Z}$ und $s_i \in \mathbb{N}$. Dann ist

$$\begin{aligned} 0 =& s_1^2 s_2^2 s_3^2 s_4^2 (x_1^2 - ax_2^2 - px_3^2 + apx_4^2) \\ =& (r_1 s_2 s_3 s_4)^2 - a(s_1 r_2 s_3 s_4)^2 - p(s_1 s_2 r_3 s_4)^2 + ap(s_1 s_2 s_3 r_4)^2 \end{aligned}$$

Das heisst, es reicht zu zeigen, dass für $x \in \mathbb{Z}^4$ gilt

$$x_1^2 - ax_2^2 - px_3^2 + apx_4^2 = 0 \Rightarrow x = 0$$

Sei also $x \in \mathbb{Z}^4 \setminus \{0\}$ so dass

$$x_1^2 - ax_2^2 - px_3^2 + apx_4^2 = 0$$

Beachte, dass wir o.B.d.A. annehmen können, dass die $x_i$ alle teilerfremd sind, d.h. $n \in \mathbb{Z}$ und $n \mid x_i$ für $1 \leq i \leq 4$ impliziert $n = \pm 1$. Es ist

$$x_1^2 - ax_2^2 \equiv 0 \mod p$$

Falls $x_2^2 \not\equiv 0 \mod p$, dann ist $x_2^2$ invertierbar $\mod p$ und folglich auch $x_2$, d.h. es gibt $n \in \mathbb{Z}$ so dass $nx_2 \equiv 1 \mod p$ und also

$$a \equiv n^2 a x_2^2 \equiv (nx_1)^2 \mod p$$

Da aber nach Annahme $a$ kein Quadrat ist $\mod p$, folgt dass $x_2^2 \equiv 0 \mod p$, also $p \mid x_2$. Des Weiteren $x_1^2 \equiv 0 \mod p$ und folglich $p \mid x_1$. Also existieren $y_1, y_2 \in \mathbb{Z}$, so dass

$$p^2 y_1^2 - ap^2 y_2^2 - px_3^2 + apx_4^2 = 0$$

und folglich

$$py_1^2 - apy_2^2 - x_3^2 + ax_4^2 = 0$$

Also ist $ax_4^2 \equiv x_3^2 \mod p$. Falls $x_4 \neq 0 \mod p$, dann folgt wieder ein Widerspruch zur Annahme, dass $a$ kein Quadrat ist $\mod p$ und wir finden mit demselben Argument wie bereits zuvor, dass $p \mid x_3$ und $p \mid x_4$. Das impliziert aber, dass $p \mid x_i$ für $1 \leq i \leq 4$, im Widerspruch zur Teilerfremdheit der $x_i$.