Lösung 8: Komposition, Matrixmultiplikation, Invertierbarkeit, Isomorphismen

1. a) Seien $u_1, u_2 \in U$ und $\lambda \in \mathbb{K}$ beliebig. Aus der Linearität von S und T folgt

$$\begin{aligned}(S \circ T)(u_1 + \lambda u_2) &= S(T(u_1 + \lambda u_2)) \\ &= S(T(u_1) + \lambda T(u_2)) \\ &= S(T(u_1)) + \lambda S(T(u_2)) \\ &= (S \circ T)(u_1) + \lambda (S \circ T)(u_2)\end{aligned}$$

und es folgt die Linearität von $S \circ T$.

b) Sei $v \in U$ beliebig, dann gelten nach Definition

$$\begin{aligned}(S \circ (\lambda T))(v) &= S((\lambda T)(v)) = S(\lambda T(v)) = \lambda S(T(v)) = \lambda (S \circ T)(v) \\ &= (\lambda (S \circ T))(v), \\ ((\lambda S) \circ T)(v) &= (\lambda S)(T(v)) = \lambda S(T(v)) = \lambda (S \circ T)(v) = (\lambda (S \circ T))(v).\end{aligned}$$

Da $v \in V$ beliebig war, stimmen also $S \circ (\lambda T)$, $(\lambda S) \circ T$ und $\lambda(S \circ T)$ punktweise überein und damit folgt die Behauptung.

c) Wir wissen aus der Vorlesung, dass $\mathrm{Hom}(V, W)$ ein Vektorraum ist bezüglich punktweiser Addition und punktweiser skalarer Multiplikation, mit Nullelement $\mathbf{0} : V \to W$ gegeben durch $\mathbf{0}(v) = 0_W$ für alle $v \in V$. Insbesondere ist also $\mathrm{End}(V)$ versehen mit der punktweisen Addition eine abelsche Gruppe mit neutralem Element $\mathbf{0}$.

Aus Teilaufgabe 1.a) wissen wir, dass die Komposition eine wohldefinierte Abbildung $\circ : \mathrm{End}(V) \times \mathrm{End}(V) \to \mathrm{End}(V)$ ist, und wir wissen aus der Diskussion der Mengenlehre (siehe Beispiel 1.36 im Analysisskript), dass diese Verknüpfung assoziativ ist.

Wir zeigen zuerst, dass $\mathrm{End}(V)$ ein Einselement bezüglich $\circ$ enthält. Nach Aufgabe 1.a aus Serie 7 ist id_V ein Element in $\mathrm{End}(V)$, sodass für alle $T \in \mathrm{End}(V)$ gilt $\mathrm{id}_V \circ T = T$. Sei nämlich $v \in V$, dann ist

$$(\mathrm{id}_V \circ T)(v) = \mathrm{id}_V(T(v)) = T(v)$$

und da $v \in V$ beliebig war, stimmen $\mathrm{id}_V \circ T$ und T punktweise überein und somit gilt $\mathrm{id}_V \circ T = T$. Da $T \in \mathrm{End}(V)$ beliebig war, ist also id_V ein Einselement bezüglich Komposition. Man beachte, dass im Spezialfalle $V = \{0_V\}$ die Abbildungen **0** und id_V punktweise übereinstimmen, also ist Körperaxiom (K9) nicht erfüllt. Dieses wird allerdings für Ringe nicht verlangt.

Es verbleibt nur noch, die Distributivität der Komposition über der Addition zu überprüfen, also Körperaxiom (K8). Seien $S, T_1, T_2 \in \mathrm{End}(V)$ und sei $v \in V$, dann berechnet man

$$\begin{aligned}
(S \circ (T_1 + T_2))(v) &= S((T_1 + T_2)(v)) = S(T_1(v) + T_2(v)) \\
&= S(T_1(v)) + S(T_2(v)) \\
&= (S \circ T_1)(v) + (S \circ T_2)(v) \\
&= ((S \circ T_1) + (S \circ T_2))(v), \\
((T_1 + T_2) \circ S)(v) &= (T_1 + T_2)(S(v)) \\
&= T_1(S(v)) + T_2(S(v)) \\
&= (T_1 \circ S)(v) + (T_2 \circ S)(v) \\
&= ((T_1 \circ S) + (T_2 \circ S))(v).
\end{aligned}$$

Da $v \in V$ beliebig war, folgen

$$\begin{aligned}
S \circ (T_1 + T_2) &= (S \circ T_1) + (S \circ T_2), \\
(T_1 + T_2) \circ S &= (T_1 \circ S) + (T_2 \circ S).
\end{aligned}$$

Dies beweist, dass Axiom (K8) gilt.

d) Seien $r, s \in R^\times$ beliebig, dann existieren nach Voraussetzung $\tilde{r}, \tilde{s} \in R$, sodass gilt $\tilde{r} \cdot r = 1_R$ und $\tilde{s} \cdot s = 1_R$, wobei $1_R \in R$ das Einselement bezüglich Multiplikation ist, d.h. für alle $r \in R$ gilt $1_R \cdot r = r$. Unter Verwendung der Assoziativität der Multiplikation, folgt

$$(\tilde{s} \cdot \tilde{r}) \cdot (r \cdot s) = \tilde{s} \cdot (\tilde{r} \cdot (r \cdot s)) = \tilde{s} \cdot ((\tilde{r} \cdot r) \cdot s) = \tilde{s} \cdot (1_R \cdot s) = \tilde{s} \cdot s = 1_R$$

und somit ist $r \cdot s \in R^\times$. Da $r, s \in R^\times$ beliebig waren, liefert die Restriktion der Multiplikation auf $R^\times$ eine wohldefinierte Verknüpfung $\cdot : R^\times \times R^\times \to R^\times$.

Aus der Definition eines Ringes wissen wir, dass die Verknüpfung $\cdot : R \times R \to R$, $(r, s) \mapsto r \cdot s$ assoziativ ist, und somit gilt dies auch für die Restriktion auf

Siehe nächstes Blatt!

$R^\times \times R^\times$. Nach Voraussetzung erfüllt das Einselement $1_R \in R$ für alle $r \in R$ die Gleichung $1_R \cdot r = r$. Insbesondere gilt also $1_R \cdot 1_R = 1_R$ und somit ist $1_R \in R^\times$. Also enthält $R^\times$ ein neutrales Element bezüglich Multiplikation.

Per definitionem existiert für alle $r \in R^\times$ in R eine Inverse bezüglich Multiplikation. Das heisst, es bleibt nur zu zeigen, die Inverse ebenfalls eine Einheit ist. Dies folgt aber sofort aus der Symmetrie der Definition, denn die Inverse s hat die Inverse r und somit ist per definitionem $s \in R^\times$.

e) Wir zeigen, dass gilt $\mathrm{GL}(V) = \mathrm{End}(V)^\times$.

$\subseteq$: Sei $T \in \mathrm{GL}(V)$, dann ist T bijektiv und somit existieren $S_1, S_2 \in V^V$, sodass gilt $S_1 \circ T = T \circ S_2 = \mathrm{id}_V$, d.h. T hat eine Links- und eine Rechtsinverse. Man berechnet unter Verwendung von Beispiel 1.36 aus dem Analysisskript

$$S_1 = S_1 \circ \mathrm{id}_V = S_1 \circ (T \circ S_2) = (S_1 \circ T) \circ S_2 = \mathrm{id}_V \circ S_2 = S_2.$$

Das heisst, T besitzt eine beidseitige Inverse S. Wir zeigen, dass $S \in \mathrm{End}(V)$ gilt. Seien $v_1, v_2 \in V$, $\lambda \in \mathbb{K}$, und wähle $w_1, w_2 \in V$ mit $T(w_i) = v_i$. Dann folgt

$$\begin{aligned} S(v_1 + \lambda v_2) &= S(T(w_1) + \lambda T(w_2)) = S(T(w_1 + \lambda w_2)) \\ &= w_1 + \lambda w_2 = S(T(w_1)) + \lambda S(T(w_2)) \\ &= S(v_1) + \lambda S(v_2). \end{aligned}$$

Dies zeigt, dass gilt

$$\mathrm{GL}(V) \subseteq \{T \in \mathrm{End}(V) \mid \exists S \in \mathrm{End}(V) : S \circ T = T \circ S = \mathrm{id}_V\} = \mathrm{End}(V)^\times.$$

$\supseteq$: Sei $T \in \mathrm{End}(V)^\times$. Dann existiert per definitionem $S \in \mathrm{End}(V)$, sodass gilt $S \circ T = T \circ S = \mathrm{id}_V$. Es folgt aus Übung 1.44 im Analysisskript, dass $T \in \mathrm{GL}(V)$ gilt.

Die Aussage folgt nun aus Teilaufgaben 1.c) und 1.d).

2.

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

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

3. **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

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

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.

Siehe nächstes Blatt!

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

4. **a)** **Reflexivität:** Sei V ein Vektorraum, dann ist $\mathrm{id}_V : V \to V$ 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 **“ $\Longrightarrow$ ”:** 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 $\{w_1, \ldots, w_n\} \subseteq W$ 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 $ST = \mathrm{id}_V$.

Bitte wenden!

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

2 **“ $\Longrightarrow$ ”:** 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 $TS = \mathrm{id}_W$.

“$\Leftarrow$”: 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 $\mathrm{Im}(TS) \subseteq \mathrm{Im}(T)$.
Sei nun also $S \in \mathrm{Hom}(W, V)$ mit $TS = \mathrm{id}_W$, dann ist

$$W = \mathrm{Im}(\mathrm{id}_W) = \mathrm{Im}(TS) \subseteq \mathrm{Im}(T)$$

und folglich ist T surjektiv.

5. 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

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

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)

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

Siehe nächstes Blatt!

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

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

c) Wir wissen aus der vorangehenden Teilaufgabe, dass $\langle\{u\}\rangle \subseteq \operatorname{Ker}(L_A)$ und $\langle\{u,v\}\rangle \subseteq \operatorname{Im}(L_A) = \operatorname{Im}(A)$. Wir wissen aus der Dimensionsformel, dass

$$3 = \dim(\operatorname{Ker}(A)) + \dim(\operatorname{Im}(A)) \geq \dim(\langle\{u\}\rangle) + \dim(\langle\{u,v\}\rangle) = 3,$$

und somit ist $\operatorname{Ker}(A) = \langle\{u\}\rangle$ und $\operatorname{Im}(A) = \langle\{u,v\}\rangle$.

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 $\varphi : V \to \operatorname{End}(V)$, $v \mapsto \varphi_v$ 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* φ.

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

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

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

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 φ, 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 φ sowie Relationen in ($\heartsuit$) vollständig bestimt und somit auch die lineare Abbildung φ.

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

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

Wir müssen zeigen, dass φ 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 φ 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 $\lambda_1, \lambda_2, \mu_1, \mu_2 \in \mathbb{K}$

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

Siehe nächstes Blatt!

Also gilt die Assoziativität von φ 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 φ für alle Paare in $V \times V$, d.h.

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

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 $A \in M_{4\times4}(\mathbb{K})$ 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 $L_{A^2} = L_{I_4} = \mathrm{id}_{\mathbb{K}^4}$ 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 $\overline{\cdot}$ eine Involution. Man überprüft für Elemente von $\mathcal{B}$ leicht, dass $\overline{\cdot}$ antimultiplikativ ist (vgl. Tabellen 1 und 2). Nun argumentiert man wie bei der Assoziativität von φ: 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

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

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 $u, v \in \mathcal{B}$.

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

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 $\overline{x} = x$.

“ $\Longrightarrow$ ”: 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

$$\begin{aligned}N(x) =& x_1^2 \mathbf{1} \cdot \mathbf{1} - x_2^2 \mathbf{i} \cdot \mathbf{i} - x_3^2 \mathbf{j} \cdot \mathbf{j} - x_2^2 \mathbf{k} \cdot \mathbf{k} \\ =& (x_1^2 - a x_2^2 - b x_3^2 + ab x_4^2) \mathbf{1}\end{aligned}$$

Siehe nächstes Blatt!

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

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

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

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

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

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

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

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

Bitte wenden!

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

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

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.