

**Lösungsvorschläge zu Lineare Algebra für Informatiker und Statistiker**

**Blatt 6**

**Zu Aufgabe 21:**

Für die reellen Matrizen

$$A_1 = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & -1 \end{pmatrix}, \quad A_2 = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}, \quad A_3 = \begin{pmatrix} -1 & 2 & 3 \end{pmatrix}$$

sind alle möglichen Matrixprodukte  $A_i \cdot A_j$ ,  $i, j \in \{1, 2, 3\}$ , zu bestimmen.

Es sind

$$A_1 \in \mathbb{R}^{2 \times 3}, \quad A_2 \in \mathbb{R}^{3 \times 1}, \quad A_3 \in \mathbb{R}^{1 \times 3}$$

Damit das Matrixprodukt  $A_i \cdot A_j$  gemäß der in der Vorlesung gegebenen Definition ausführbar ist, muß gelten: Die Spaltenzahl des ersten Faktors  $A_i$  stimmt mit der Zeilenzahl des zweiten Faktors  $A_j$  überein:

$$A_i \in \mathbb{R}^{m \times n} \quad \mathbb{R}^{n \times r} \ni A_j$$

In diesem Fall gilt für  $A = (A_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$  und  $B = (B_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq r}}$ :

$$A \cdot B = (A \cdot B)_{\substack{1 \leq i \leq m \\ 1 \leq j \leq r}} \text{ mit } (A \cdot B)_{ij} = \sum_{k=1}^n A_{ik} \cdot B_{kj} \quad (1 \leq i \leq m, 1 \leq j \leq r) \text{ und die Produktmatrix}$$

$A \cdot B$  liegt in  $\mathbb{R}^{m \times r}$ .

Um alle möglichen Produkte zu untersuchen gehen wir alle Fälle durch, wo jeweils  $A_i$  der erste Faktor ist mit  $1 \leq i \leq 3$ :

**Erster Faktor  $A_1$ :**

- Die Spaltenzahl von  $A_1$  ist  $3 \neq 2$  = Zeilenzahl von  $A_1 \implies$  das Produkt aus  $A_1$  und  $A_1$  ist nicht bildbar.

- Die Spaltenzahl von  $A_1$  ist  $3 =$  Zeilenzahl von  $A_2 \implies A_1 \cdot A_2$  ist definiert und es gilt:

$$\mathbb{R}^{2 \times 1} \ni A_1 \cdot A_2 = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} = \begin{pmatrix} 7 \\ -1 \end{pmatrix}$$

- Die Spaltenzahl von  $A_1$  ist  $3 \neq 1$  = Zeilenzahl von  $A_3 \implies$  das Produkt aus  $A_1$  und  $A_3$  ist nicht bildbar.

**Erster Faktor  $A_2$  :**

- Die Spaltenzahl von  $A_2$  ist  $1 \neq 2 = \text{Zeilenzahl von } A_1 \implies$  das Produkt aus  $A_2$  und  $A_1$  ist nicht bildbar.
- Die Spaltenzahl von  $A_2$  ist  $1 \neq 3 = \text{Zeilenzahl von } A_2 \implies$  das Produkt aus  $A_2$  und  $A_2$  ist nicht bildbar.
- Die Spaltenzahl von  $A_2$  ist  $1 = \text{Zeilenzahl von } A_3 \implies A_2 \cdot A_3$  ist definiert und es gilt:

$$\mathbb{R}^{3 \times 3} \ni A_2 \cdot A_3 = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} \cdot \begin{pmatrix} -1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} -1 & 2 & 3 \\ -2 & 4 & 6 \\ -3 & 6 & 9 \end{pmatrix}$$

**Erster Faktor  $A_3$  :**

- Die Spaltenzahl von  $A_3$  ist  $3 \neq 2 = \text{Zeilenzahl von } A_1 \implies$  das Produkt aus  $A_3$  und  $A_1$  ist nicht bildbar.
- Die Spaltenzahl von  $A_3$  ist  $3 = \text{Zeilenzahl von } A_2 \implies A_3 \cdot A_2$  ist definiert und es gilt:

$$\mathbb{R}^{1 \times 1} \ni A_3 \cdot A_2 = \begin{pmatrix} -1 & 2 & 3 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} = \begin{pmatrix} 12 \end{pmatrix}$$

- Die Spaltenzahl von  $A_3$  ist  $3 \neq 1 = \text{Zeilenzahl von } A_3 \implies$  das Produkt aus  $A_3$  und  $A_3$  ist nicht bildbar.

**Zu Aufgabe 22:** Sei  $K$  ein Körper,  $m, n, r, s \in \mathbb{N}$ . Dann gilt:

- (a)  $A \in K^{m \times n} \wedge B, C \in K^{n \times r} \implies A \cdot (B + C) = A \cdot B + A \cdot C$   
 (b)  $A \in K^{m \times n}, B \in K^{n \times r}, C \in K^{r \times s} \implies (A \cdot B) \cdot C = A \cdot (B \cdot C)$

Beweis:

**Ad (a) :**

Zunächst verifizieren wir, daß alle Produkte und Summen wohldefiniert sind:

$B$  und  $C$  liegen im selben Matrizenraum  $K^{n \times r} \implies$  die Summenmatrix  $B + C$  ist definiert und liegt wieder in  $K^{n \times r}$ .

$A \in K^{m \times n}, K^{n \times r} \ni (B + C) \implies$  Spaltenzahl von  $A$  und Zeilenzahl von  $(B + C)$  stimmen überein  $\implies$  das Produkt  $A \cdot (B + C)$  ist definiert und liegt in  $K^{m \times r}$ .

$A \in K^{m \times n}, K^{n \times r} \ni B \implies$  die Spaltenzahl von  $A$  und die Zeilenzahl von  $B$  stimmen überein  $\implies$  das Produkt  $A \cdot B$  ist definiert und liegt in  $K^{m \times r}$ ; das gleiche gilt für das Produkt  $A \cdot C$ , da ja auch die Matrix  $C$  in  $K^{n \times r}$  liegt. Beide Summanden  $A \cdot B$  und  $A \cdot C$  liegen damit in  $K^{m \times r}$ , weshalb die Summe aus beiden wohldefiniert ist.

Nun zur Überprüfung der Formel:

Es sei wie in Aufgabe (21) :  $A = (A_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}, B = (B_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq r}}, C = (C_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq r}}.$

Ferner sei  $B + C = ((B + C)_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq r}}, A \cdot B = ((A \cdot B)_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq r}}, A \cdot C = ((A \cdot C)_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq r}}.$

Dann gilt für alle  $1 \leq i \leq m$  und alle  $1 \leq j \leq r$  :

$$\begin{aligned}
 (A \cdot (B + C))_{ij} & \stackrel{\substack{\text{Matrixprodukt} \\ A \text{ hat} \\ n \text{ Spalten}}}{=} \sum_{k=1}^n A_{ik} \cdot (B + C)_{kj} \\
 & \stackrel{\substack{\text{Def.} \\ \text{Summe}}}{=} \sum_{k=1}^n A_{ik} \cdot (B_{kj} + C_{kj}) \\
 & \stackrel{\substack{\text{Distrib.} \\ \text{in } K}}{=} \sum_{k=1}^n (A_{ik} \cdot B_{kj} + A_{ik} \cdot C_{kj}) \\
 & \stackrel{\substack{\text{Rechenregel} \\ (1.16) (a)}}{=} \underbrace{\sum_{k=1}^n A_{ik} \cdot B_{kj}}_{\substack{= (A \cdot B)_{ij} \\ \text{Matrixprodukt}}} + \underbrace{\sum_{k=1}^n A_{ik} \cdot C_{kj}}_{\substack{= (A \cdot C)_{ij} \\ \text{Matrixprodukt}}} \\
 & = (A \cdot B)_{ij} + (A \cdot C)_{ij} \\
 & \stackrel{\substack{\text{Def.} \\ \text{Summe}}}{=} (A \cdot B + A \cdot C)_{ij}
 \end{aligned}$$

Damit stimmen die Matrizen  $A \cdot (B + C)$  und  $A \cdot B + A \cdot C$  an allen Stellen  $(i, j)$  überein, also sind nach Definition diese beiden Matrizen identisch. q.e.d.

**Ad (b) :**

Wieder verifizieren wir, daß alle Produkte und Summen wohldefiniert sind:

$A \in K^{m \times \textcircled{n}}$  ,  $K^{\textcircled{n} \times r} \ni B \implies$  die Spaltenzahl von  $A$  und die Zeilenzahl von  $B$  stimmen überein  
 $\implies$  das Produkt  $A \cdot B$  ist definiert und liegt in  $K^{m \times r}$  ;

$A \cdot B \in K^{m \times \textcircled{r}}$  ,  $K^{\textcircled{r} \times s} \ni C \implies$  die Spaltenzahl von  $A \cdot B$  und die Zeilenzahl von  $C$  stimmen überein  
 $\implies$  das Produkt  $(A \cdot B) \cdot C$  ist definiert und liegt in  $K^{m \times s}$  ;

$B \in K^{n \times \textcircled{r}}$  ,  $K^{\textcircled{r} \times s} \ni C \implies$  die Spaltenzahl von  $B$  und die Zeilenzahl von  $C$  stimmen überein  
 $\implies$  das Produkt  $B \cdot C$  ist definiert und liegt in  $K^{n \times s}$  .

$A \in K^{m \times \textcircled{n}}$  ,  $K^{\textcircled{n} \times s} \ni B \cdot C \implies$  die Spaltenzahl von  $A$  und die Zeilenzahl von  $B \cdot C$  stimmen überein  
 $\implies$  das Produkt  $A \cdot (B \cdot C)$  ist definiert und liegt in  $K^{m \times s}$  .

Überprüfung der Formel: Für alle  $1 \leq i \leq m$  und für alle  $1 \leq j \leq s$  gilt:

$$\begin{aligned}
 ((A \cdot B) \cdot C)_{ij} & \stackrel{\substack{\text{Matrixprodukt} \\ AB \text{ hat} \\ r \text{ Spalten}}}{=} \sum_{k=1}^r (A \cdot B)_{ik} \cdot C_{kj} \\
 & \stackrel{\substack{\text{Matrixprodukt} \\ A \text{ hat} \\ n \text{ Spalten}}}{=} \sum_{k=1}^r \left( \sum_{l=1}^n (A_{il} \cdot B_{lk}) \right) \cdot C_{kj} \\
 & \stackrel{\substack{\text{Distrib.} \\ \text{in } K}}{=} \sum_{k=1}^r \left( \sum_{l=1}^n (A_{il} \cdot B_{lk}) \cdot C_{kj} \right) \\
 & \stackrel{\substack{\text{Rechenregel} \\ (1.16)(c)}}{=} \sum_{l=1}^n \left( \sum_{k=1}^r (A_{il} \cdot B_{lk}) \cdot C_{kj} \right) \\
 & \stackrel{\substack{\text{Assoz.} \\ \text{in } K}}{=} \sum_{l=1}^n \left( \sum_{k=1}^r A_{il} \cdot \underbrace{(B_{lk} \cdot C_{kj})}_{\substack{\text{unabhängig} \\ \text{von } k}} \right) \\
 & \stackrel{\substack{\text{Distrib.} \\ \text{in } K}}{=} \sum_{l=1}^n \left( A_{il} \cdot \underbrace{\sum_{k=1}^r (B_{lk} \cdot C_{kj})}_{\substack{= (B \cdot C)_{lj} \\ \text{(Matrixprodukt)}}} \right) \\
 & = \sum_{l=1}^n A_{il} \cdot (BC)_{lj} \\
 & \stackrel{\substack{\text{Matrixprodukt} \\ A \text{ hat } n \text{ Spalten}}}{=} (A \cdot (B \cdot C))_{ij}
 \end{aligned}$$

Damit stimmen die Einträge der Matrizen  $(A \cdot B) \cdot C$  und  $A \cdot (B \cdot C)$  an allen Stellen  $1 \leq i \leq m$  und  $1 \leq j \leq s$  überein, d.h. beide Matrizen sind gleich. q.e.d.

### Zu Aufgabe 23:

Wir wollen folgende, in den Tutorien bewiesene Aussage über Gruppen verwenden:

$$(\blacksquare) \left\{ \begin{array}{l} \text{Ist } (G, \circ) \text{ eine (abelsche) Gruppe, } H \text{ eine Menge und } * : H \times H \rightarrow H \text{ eine} \\ \text{Abbildung mit} \\ \forall a, b \in G : \varphi(a \circ b) = \varphi(a) * \varphi(b) \quad (\clubsuit). \\ \text{Dann ist auch } (H, *) \text{ eine (abelsche) Gruppe und (via } \varphi \text{ isomorph zu } (G, \circ). \end{array} \right.$$

### Beweis dafür:

- **assoziativ:** Seien  $\alpha, \beta, \gamma \in H$ . Zu zeigen ist:  $\alpha * (\beta * \gamma) = (\alpha * \beta) * \gamma$ .  
Da  $\varphi$  surjektiv ist, gibt es  $a, b, c \in G$  mit:  $\alpha = \varphi(a) \wedge \beta = \varphi(b) \wedge \gamma = \varphi(c)$ .  
Damit folgt:

$$\begin{array}{lll} \alpha * (\beta * \gamma) & \stackrel{\text{Substitution}}{=} & \varphi(a) * (\varphi(b) * \varphi(c)) \\ & = & \varphi(a) * \varphi(b \circ c) \\ & \stackrel{(\clubsuit)}{=} & \varphi(a \circ (b \circ c)) \\ & \stackrel{(\clubsuit)}{=} & \varphi((a \circ b) \circ c) \\ & \stackrel{(G, \circ)}{=} & \varphi(a \circ b) * \varphi(c) \\ & \stackrel{\text{asso.}}{=} & (\varphi(a) * \varphi(b)) * \varphi(c) \\ & \stackrel{(\clubsuit)}{=} & (\alpha * \beta) * \gamma \\ & \stackrel{\text{Rücksubstitution}}{=} & \end{array}$$

- **Existenz eines neutralen Elements:**

Da behauptet wird, daß  $\varphi$  ein Isomorphismus ist, muß, falls die Behauptung richtig ist, das neutrale Element  $e$  von  $(G, \circ)$  auf das neutrale Element von  $H$  abgebildet werden. Deshalb setzen wir für das (vermutete) neutrale Element  $\varepsilon$  von  $H$   $\varepsilon := \varphi(e)$  und verifizieren, daß dieses  $\varepsilon$  tatsächlich neutral in  $H$  bezüglich der Verknüpfung  $*$  ist:

Sei dazu wieder  $\alpha \in H$  und  $\alpha = \varphi(a)$  für ein geeignetes  $a \in G$ . Dann:

$$\alpha * \varepsilon \stackrel{\text{Def.}}{=} \alpha * \varphi(e) \stackrel{\text{Substitution}}{=} \varphi(a) * \varphi(e) = \varphi(a \circ e) \stackrel{(\clubsuit)}{=} \varphi(a) \stackrel{\text{neutral}}{=} \varphi(a) \stackrel{\text{Rücksubstitution}}{=} \alpha \quad \text{q.e.d.}$$

(Laut Vorlesung reicht es, die Existenz eines rechtsneutralen Elements nachzuweisen !)

- **Existenz inverser Elemente:**

Sei wieder  $\alpha \in H$  und  $\alpha = \varphi(a)$  für ein geeignetes  $a \in G$ . Wir zeigen, daß ein rechtsinverses Element  $\beta$  zu  $\alpha$  existiert. Wie oben vermuten wir, daß  $\beta := \varphi(a^{-1})$ , denn ein Homomorphismus bildet stets Inverse auf Inverse ab. Verifizierung:

$$\alpha * \beta \stackrel{\text{Substit.}}{=} \varphi(a) * \varphi(a^{-1}) = \varphi(a \circ a^{-1}) \stackrel{(\clubsuit)}{=} \varphi(e) \stackrel{\text{neutral}}{=} \varphi(e) \stackrel{\text{Def. des}}{=} \varepsilon \quad \text{q.e.d.}$$

- **Falls  $(G, \circ)$  abelsch:**

Seien  $\alpha, \beta \in H$  und  $\alpha = \varphi(a), \beta = \varphi(b)$  ( $a, b \in G$ ) (da  $\varphi$  surjektiv).

Dann folgt:

$$\alpha * \beta \stackrel{\text{Substitution}}{=} \varphi(a) * \varphi(b) = \varphi(a \circ b) \stackrel{(G, \circ)}{=} \varphi(b \circ a) = \varphi(b) * \varphi(a) \stackrel{(\clubsuit)}{=} \beta * \alpha \quad \text{q.e.d.}$$

Also ist auch  $(H, *)$  abelsch.

Nun beweisen wir Aufgabe (23) :

**Ad (a)**  $(K, +, \cdot)$  sei ein Körper,  $L$  eine Menge auf der zwei Verknüpfungen

$$\oplus : L \times L \rightarrow L \quad \text{und}$$

$$\odot : L \times L \rightarrow L$$

definiert sind. Ferner gebe es eine bijektive Abbildung  $\varphi : K \rightarrow L$  mit der Eigenschaft:

$$\forall a, b \in K : \varphi(a + b) = \varphi(a) \oplus \varphi(b) \quad (1)$$

$$\varphi(a \cdot b) = \varphi(a) \odot \varphi(b) \quad (2)$$

Dann ist  $L$  ein Körper.

Beweis:

Wir müssen zeigen :

(i)  $(L, \oplus, \odot)$  ist ein Ring.

(ii)  $(L \setminus \{0_L\}, \odot)$  ist abelsche Gruppe.

(mit  $0_L$  das neutrale Element der Gruppe  $(L, \oplus)$  .

Für die Ringeigenschaft aus (i) brauchen wir:

( $\alpha$ )  $(L, \oplus)$  ist eine abelsche Gruppe.

( $\beta$ ) Die Multiplikation  $\odot$  ist assoziativ.

( $\gamma$ )  $\forall x, y, z \in L : (x \oplus y) \odot z = (x \odot z) \oplus (y \odot z) \quad \text{und}$   
 $z \odot (x \oplus y) = (z \odot x) \oplus (z \odot y)$

Wenn wir  $(G, \circ) := (K, +)$  setzen und  $H := L$ ,  $* := \oplus$ , so können wir (■) anwenden und erhalten unmittelbar:

$(L, \oplus)$  ist eine abelsche Gruppe (mit neutralem Element  $0_L = \varphi(0_K)$ ) und zudem (via  $\varphi$ ) isomorph zu  $(K, +)$ . Damit ist ( $\alpha$ ) bewiesen.

Um (ii) zu zeigen, müssen wir zuerst nachweisen, daß die eingeschränkte Operation

$\odot|_{(L \setminus \{0_L\}) \times (L \setminus \{0_L\})} : (L \setminus \{0_L\}) \times (L \setminus \{0_L\}) \rightarrow L \setminus \{0_L\}$  wohldefiniert ist; zu zeigen ist also:

$$\forall u, v \in L \setminus \{0_L\} : u \odot v \neq 0_L$$

Wegen  $\varphi$  surjektiv gibt es  $a, b \in K$ , so daß  $u = \varphi(a)$  und  $v = \varphi(b)$ . Weil  $0_L = \varphi(0_K)$

(da  $\varphi$  Gruppenhomomorphismus von  $(K, +)$  nach  $(L, \oplus)$  ist), gilt:

$$\left. \begin{array}{l} \varphi(a) = u \neq 0_L = \varphi(0_K) \xRightarrow[\text{Abbild.}]{\varphi} a \neq 0_K \\ \varphi(b) = v \neq 0_L = \varphi(0_K) \xRightarrow{\quad} b \neq 0_K \end{array} \right\} \xRightarrow[\text{nullteilerfrei}]{(K, +, \cdot)} a \cdot b \neq 0_K \xRightarrow[\text{injektiv}]{\varphi}$$

$$u \odot v = \varphi(a) \odot \varphi(b) \stackrel{(1)}{=} \varphi(a \cdot b) \neq \varphi(0_K) = 0_L . \quad \text{q.e.d.}$$

Damit können wir erneut (■) anwenden:

Setze  $(G, \circ) := (K \setminus \{0_K\}, \cdot)$ ,  $H := L \setminus \{0_L\}$  und  $* := \odot|_{(L \setminus \{0_L\}) \times (L \setminus \{0_L\})}$ .

Dann gilt mit (■) :

$(L \setminus \{0_L\}, \odot)$  ist eine abelsche Gruppe und (via  $\varphi$ ) isomorph zu  $(K \setminus \{0_K\}, \cdot)$ .

Damit ist (ii) gezeigt und fast die gesamte Aussage ( $\beta$ ) :

$$\forall x, y, z \in L \setminus \{0_L\} : x \odot (y \odot z) = (x \odot y) \odot z$$

gilt wegen (ii). Wir müssen also nur noch den Fall untersuchen, daß eines der  $x, y, z$  gleich  $0_L$  ist.

Wenn  $y \in L$  beliebig und  $y = \varphi(b)$  ( $b \in K$ ), so gilt:

$$0_L \odot y = \varphi(0_K) \odot \varphi(b) \stackrel{(2)}{=} \varphi(0_K \cdot b) \stackrel{\text{Rechenregel (1.15)(a)}}{=} \varphi(0_K) \stackrel{\text{Def.}}{=} 0_L.$$

Ist also in  $x \odot (y \odot z)$  einer der Faktoren  $0_L$ , so ist das Produkt gleich  $0_L$ ; das gilt auch im Produkt  $(x \odot y) \odot z$ , weshalb die Assoziativität in  $(\beta)$  bewiesen ist.

Es bleibt noch  $(\gamma)$  zu beweisen.

Weil wir bereits wissen, daß die Multiplikation für  $x, y \in L \setminus \{0_L\}$  kommutativ ist und wie eben  $x \odot y = 0_L = y \odot x$ , wenn einer der Faktoren gleich  $0_L$  ist, brauchen wir nur eine der beiden in  $(\gamma)$  geforderten Gleichungen nachzuweisen.

Seien also  $x, y, z \in L$  und mit  $\varphi$  surjektiv  $a, b, c \in K$ , sodaß  $x = \varphi(a)$ ,  $y = \varphi(b)$ ,  $z = \varphi(c)$  ist. Dann:

$$\begin{aligned} (x \oplus y) \odot z & \stackrel{\text{Substitution}}{=} (\varphi(a) \oplus \varphi(b)) \odot \varphi(c) \\ & \stackrel{(1)}{=} \varphi(a + b) \odot \varphi(c) \\ & \stackrel{(2)}{=} \varphi((a + b) \cdot c) \\ & \stackrel{\text{Distrib.gesetz in } (K, +, \cdot)}{=} \varphi(a \cdot c + b \cdot c) \\ & \stackrel{(1)}{=} \varphi(a \cdot c) \oplus \varphi(b \cdot c) \\ & \stackrel{(2)}{=} (\varphi(a) \odot \varphi(c)) \oplus (\varphi(b) \odot \varphi(c)) \\ & \stackrel{\text{Rücksubstitution}}{=} (x \odot z) \oplus (y \odot z) \end{aligned}$$

Damit ist alles gezeigt.

**Ad (b)**  $L := \left\{ \begin{pmatrix} x & -y \\ y & x \end{pmatrix} \mid x, y \in \mathbb{R} \right\}$  ist zusammen mit der Matrizenaddition und der Matrizenmultiplikation ein zu  $\mathbb{C}$  isomorpher Körper.

Beweis:

Wir wollen den Beweis führen, indem wir Teil (a) verwenden. Aus der Vorlesung und aus Aufgabe (19) ist bekannt, daß  $\mathbb{C} = (\mathbb{R}^2, +, \cdot)$  ein Körper ist. Wenn wir also eine bijektive Abbildung  $\varphi$  von  $\mathbb{C}$  nach  $L$  finden, die bezüglich der Matrizenaddition „+“ und -multiplikation „ $\cdot$ “ als Verknüpfungen auf  $L$  die Bedingungen (1) und (2) aus Aufgabenteil (a) erfüllt, so wissen wir, daß  $(L, +, \cdot)$  ein Körper ist und (mit der in Teil (a) angegebenen Definition) zudem  $\varphi$  ein Körperisomorphismus ist, wenn es nur zusätzlich noch der Bedingung  $\varphi(1_{\mathbb{C}}) = 1_L = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$  genügt.

Wir definieren:

$$\varphi : \mathbb{C} \rightarrow L, \quad (x, y) = x + iy \mapsto \begin{pmatrix} x & -y \\ y & x \end{pmatrix} \quad (x, y \in \mathbb{R})$$

$$\begin{aligned} \forall (x, y), (u, v) \in \mathbb{C} : \varphi((x, y) + (u, v)) & \stackrel{\text{Def. „+“ in } \mathbb{C}}{=} \varphi((x + u) + i(y + v)) \\ & \stackrel{\text{Def. } \varphi}{=} \begin{pmatrix} x + u & -(y + v) \\ y + v & x + u \end{pmatrix} = \begin{pmatrix} x + u & -y - v \\ y + v & x + u \end{pmatrix} \\ & \stackrel{\text{Def. Matrix-Add.}}{=} \begin{pmatrix} x & -y \\ y & x \end{pmatrix} + \begin{pmatrix} u & -v \\ v & u \end{pmatrix} \\ & \stackrel{\text{Def. } \varphi}{=} \varphi(x + iy) + \varphi(u + iv) = \varphi((x, y)) + \varphi((u, v)) \end{aligned}$$

Damit ist (1) aus Teil (a) bewiesen.

Beweis zu (2) :

$$\begin{aligned}
 \forall x, y, u, v \in \mathbb{R} : \varphi((x + iy) \cdot (u + iv)) &\stackrel{\text{Produkt in } \mathbb{C}}{=} \varphi(xu - yv, xv + uy) \\
 &\stackrel{\text{Def. } \varphi}{=} \begin{pmatrix} xu - yv & -(xv + uy) \\ xv + uy & xu - yv \end{pmatrix} \\
 &= \begin{pmatrix} xu + (-y)v & x(-v) + (-y)u \\ yu + xv & y(-v) + xu \end{pmatrix} \\
 &\stackrel{\text{Def. Matrixprodukt}}{=} \begin{pmatrix} x & -y \\ y & x \end{pmatrix} \cdot \begin{pmatrix} u & -v \\ v & u \end{pmatrix} \\
 &\stackrel{\text{Def. } \varphi}{=} \varphi(x + iy) \cdot \varphi(u + iv) \quad \text{q.e.d.}
 \end{aligned}$$

Damit ist  $(L, +, \cdot)$  wie in (a) gezeigt ein Körper und es gilt insbesondere, da  $(L \setminus \{0_L\}, \cdot)$  eine Gruppe ist, daß  $1_L = \varphi(1_{\mathbb{C}}) = \varphi(1 + i \cdot 0) \stackrel{\text{Def. } \varphi}{=} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ .

$$\mathbf{Ad (c)} \quad \forall (x, y) \in \mathbb{C} \setminus \{0\} = \mathbb{R}^2 \setminus \{(0, 0)\} : \begin{pmatrix} x & -y \\ y & x \end{pmatrix}^{-1} = \frac{1}{x^2 + y^2} \cdot \begin{pmatrix} x & y \\ -y & x \end{pmatrix}$$

Beweis:

In (■) hatten wir gesehen, daß  $\varphi$  Inverse auf Inverse abbildet:

$$\forall \mathbb{C} \ni (x + iy) \neq 0 : \varphi((x + iy)^{-1}) = (\varphi(x + iy))^{-1} \quad (\heartsuit)$$

Damit:

$$\forall (x, y) \in \mathbb{C} \setminus \{(0, 0)\} : \begin{pmatrix} x & -y \\ y & x \end{pmatrix} = \varphi(x + iy) \implies$$

$$\begin{aligned}
 \begin{pmatrix} x & -y \\ y & x \end{pmatrix}^{-1} &= \left( \varphi(x + iy) \right)^{-1} \\
 &\stackrel{(\heartsuit)}{=} \varphi((x + iy)^{-1}) \\
 &\stackrel{\text{Aufgabe (19)(a)}}{=} \varphi\left(\frac{x}{x^2 + y^2} + i \frac{-y}{x^2 + y^2}\right) \\
 &\stackrel{\text{Def. } \varphi}{=} \begin{pmatrix} \frac{x}{x^2 + y^2} & -\frac{-y}{x^2 + y^2} \\ \frac{-y}{x^2 + y^2} & \frac{x}{x^2 + y^2} \end{pmatrix} \\
 &= \begin{pmatrix} \frac{x}{x^2 + y^2} & \frac{y}{x^2 + y^2} \\ \frac{-y}{x^2 + y^2} & \frac{x}{x^2 + y^2} \end{pmatrix} \\
 &\stackrel{\text{Def. (2.5)}}{=} \frac{1}{x^2 + y^2} \cdot \begin{pmatrix} x & y \\ -y & x \end{pmatrix}
 \end{aligned}$$



### Zu Aufgabe 24:

Der Körper  $GF(2^3)$  besitzt als additive Gruppe  $(\mathbb{Z}_2^3, +)$ . In dieser Aufgabe wird die multiplikative Gruppe  $(\mathbb{Z}_2^3 \setminus \{0\}, *)$  mit dem Einselement  $e$  durch die folgenden Bedingungen festgelegt:

$$e := (\bar{0}, \bar{0}, \bar{1}) \quad \wedge \quad a := (\bar{0}, \bar{1}, \bar{0}) \quad \wedge \quad a^2 := (\bar{1}, \bar{0}, \bar{0})$$

wobei  $a$  erzeugendes Element der zyklischen multiplikativen Gruppe  $(\mathbb{Z}_2^3 \setminus \{0\}, *)$  ist und der Gleichung

$$a^3 = a + e$$

genügt.

### Ad (a) :

$$\begin{aligned} a^3 &\stackrel{\text{Def.}}{=} a + e \\ a^4 &= a^3 \cdot a \stackrel{\text{Def.}}{=} (a + e) \cdot a \stackrel{\text{Distr.}}{=} a^2 + a \\ a^5 &= a^2 \cdot a^3 \stackrel{\text{Def.}}{=} a^2 \cdot (a + e) \stackrel{\text{Distr.}}{=} a^3 + a^2 \stackrel{\text{Def.}}{=} (a + e) + a^2 = a^2 + a + e \\ a^6 &= a^3 \cdot a^3 \stackrel{\text{Def.}}{=} (a + e) \cdot (a + e) \stackrel{\text{Distr.}}{=} a^2 + a \cdot e + e \cdot a + e \cdot e \stackrel{\substack{e \\ \text{neutral}}}{=} a^2 + e \cdot a + e \cdot a + e \\ &= a^2 + \underbrace{(e + e)}_{\substack{=0 \text{ in} \\ GF(2^3)}} \cdot a + e = a^2 + e \\ a^7 &= a \cdot a^6 \stackrel{\text{s.o.}}{=} (a^2 + e) \cdot a \stackrel{\text{Distrib.}}{=} a^3 + a \stackrel{\text{Def.}}{=} (a + e) + a = \underbrace{a + a}_{\substack{=0 \\ \text{s.o.}}} + e = 0 + e = e \end{aligned}$$

Damit folgt:

$$\begin{array}{llll} a^0 &= e & &= (\bar{0}, \bar{0}, \bar{1}) \\ a^1 &= a & &= (\bar{0}, \bar{1}, \bar{0}) \\ a^2 &= & &= (\bar{1}, \bar{0}, \bar{0}) \\ a^3 &= a + e &= (\bar{0}, \bar{1}, \bar{0}) + (\bar{0}, \bar{0}, \bar{1}) &= (\bar{0}, \bar{1}, \bar{1}) \\ a^4 &= a^2 + a &= (\bar{1}, \bar{0}, \bar{0}) + (\bar{0}, \bar{1}, \bar{0}) &= (\bar{1}, \bar{1}, \bar{0}) \\ a^5 &= a^2 + a + e &= (\bar{1}, \bar{0}, \bar{0}) + (\bar{0}, \bar{1}, \bar{0}) + (\bar{0}, \bar{0}, \bar{1}) &= (\bar{1}, \bar{1}, \bar{1}) \\ a^6 &= a^2 + e &= (\bar{1}, \bar{0}, \bar{0}) + (\bar{0}, \bar{0}, \bar{1}) &= (\bar{1}, \bar{0}, \bar{1}) \\ a^7 &= e & &= (\bar{0}, \bar{0}, \bar{1}) \end{array}$$

### Ad (b) :

Es sind das Produkte  $(\bar{1}, \bar{1}, \bar{0}) * (\bar{0}, \bar{1}, \bar{1})$  und der Quotient  $\frac{(\bar{1}, \bar{0}, \bar{0})}{(\bar{1}, \bar{1}, \bar{1})}$  zu bestimmen:

- $(\bar{1}, \bar{1}, \bar{0}) * (\bar{0}, \bar{1}, \bar{1}) \stackrel{\text{s.o.}}{=} a^4 * a^3 = a^7 = e = (\bar{0}, \bar{0}, \bar{1})$
- $\frac{(\bar{1}, \bar{0}, \bar{0})}{(\bar{1}, \bar{1}, \bar{1})} \stackrel{\text{s.o.}}{=} \frac{a^2}{a^5} \stackrel{a^7=e}{=} \frac{a^2 \cdot a^7}{a^5} = \frac{a^9}{a^5} = a^{9-5} = a^4 = (\bar{1}, \bar{1}, \bar{0})$