Lineare Algebra 2
Prof. Dr. R. Dahlhaus
Dr. S. Richter, N. Phandoidaen
Sommersemester 2019

11. Abgabeblatt – Lösungen

Aufgabe 41	Aufgabe 42	Aufgabe 43	Aufgabe 44	Aufgabe 45	Aufgabe 46	Summe:

Übungsgruppe: Tutor(in):

Namen:

Aufgabe 41 (Anwendung des Spektralsatzes auf unitären Räumen, 4 = 1 + 1.5 + 1.5 Punkte).

Zusammen mit dem von der Matrix $A := \begin{pmatrix} 1 & 0 & -i \\ 0 & 2 & -1 \\ i & -1 & 2 \end{pmatrix}$ induzierten Skalarprodukt ist $V = \mathbb{C}^3$ ein unitärer Vektorraum. Sei $\mathcal{C} = ((1,0,0)^t, (0,i,0)^t, (0,0,1)^t)$ eine Basis von V und $\tilde{B} \in \mathrm{End}_{\mathbb{C}}(V)$ gegeben über

$$B = \begin{pmatrix} i & 2 & i-2 \\ 0 & i-1 & 0 \\ 0 & 2i & -1-i \end{pmatrix} \in M(3 \times 3, \mathbb{C}).$$

(a) Berechnen Sie ausgehend von $\mathcal{C}$ mit dem Gram-Schmidt-Verfahren eine ONB $\mathcal{B}$ für $(V, \langle \cdot, \cdot \rangle_A)$.

(b) Zeigen Sie, dass $\tilde{B}$ in $(V, \langle \cdot, \cdot \rangle_A)$ eine normale Abbildung ist, aber nicht im unitären Standardraum $(V, \langle \cdot, \cdot \rangle)$. Ist $\tilde{B}$ unitär oder selbstadjungiert in $(V, \langle \cdot, \cdot \rangle_A)$?

(c) Bestimmen Sie eine Basis aus normierten Eigenvektoren von $\tilde{B}$. Ist diese Basis eine ONB in $(V, \langle \cdot, \cdot \rangle_A)$?

Lösung:

(a) Wir bestimmen ausgehend von $\mathcal{C} := (v_1, v_2, v_3)$ eine ONB von V bezüglich $\langle \cdot, \cdot \rangle_A$.

- $\tilde{w}_1 = v_1, \|\tilde{w}_1\|_A^2 = 1 \implies w_1 := \tilde{w}_1 = e_1 = (1,0,0)^t$
- $\tilde{w}_2 = v_2 - \langle v_2, w_1 \rangle_A w_1 = v_2 = (0,i,0)^t$.
  $\|\tilde{w}_2\|_A^2 = 2 \implies w_2 := \frac{1}{\sqrt{2}}(0,i,0)^t$
- $\tilde{w}_1 = v_3 - \langle v_3, w_1 \rangle_A w_1 - \langle v_3, w_2 \rangle_A w_2 = v_3 - i \cdot w_1 - \frac{1}{2} i (0,i,0)^t = (-i, 1/2, 1)^t$
  $\|\tilde{w}_3\|_A^2 = \frac{1}{2} \implies w_3 := \sqrt{2}(-i, 1/2, 1)^t$

Damit ist $\mathcal{B} := (w_1, w_2, w_3)$ eine ONB für $(V, \langle \cdot, \cdot \rangle_A)$.

(b) Es gilt

$$M_{\mathcal{B}}^{\mathcal{B}}(\tilde{B}) = T_{\mathcal{B}}^E \cdot M_E^E(\tilde{B}) \cdot T_E^{\mathcal{B}} = \begin{pmatrix} 1 & 0 & i \\ 0 & -i\sqrt{2} & i/\sqrt{2} \\ 0 & 0 & 1/\sqrt{2} \end{pmatrix} \cdot \begin{pmatrix} i & 2 & i-2 \\ 0 & i-1 & 0 \\ 0 & 2i & -1-i \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & -i\sqrt{2} \\ 0 & i/\sqrt{2} & 1/\sqrt{2} \\ 0 & 0 & \sqrt{2} \end{pmatrix} = \begin{pmatrix} i & 0 & 0 \\ 0 & -1 & 1 \\ 0 & -1 & -1 \end{pmatrix}.$$

und $\overline{M^{\mathcal{B}}_{\mathcal{B}}(\tilde{B})}^t M^{\mathcal{B}}_{\mathcal{B}}(\tilde{B}) = \begin{pmatrix} 1&0&0\\0&2&0\\0&0&2 \end{pmatrix} = M^{\mathcal{B}}_{\mathcal{B}}(\tilde{B})\overline{M^{\mathcal{B}}_{\mathcal{B}}(\tilde{B})}^t$ (*), also $\tilde{B}$ normal bezüglich $\langle\cdot,\cdot\rangle_A$.
Für die Standardbasis gilt

$$\overline{M^E_E(\tilde{B})}^t M^E_E(\tilde{B}) = \begin{pmatrix} 1 & -2i & 1+2i \\ 2i & 10 & -6+4i \\ 1-2i & -6-4i & 7 \end{pmatrix} \neq \begin{pmatrix} 10 & -2-2i & 1-7i \\ -2+2i & 2 & 2+2i \\ 1+7i & 2-2i & 6 \end{pmatrix} = M^E_E(\tilde{B})\overline{M^E_E(\tilde{B})}^t,$$

$\Longrightarrow$ $\tilde{B}$ nicht normal bezüglich $\langle\cdot,\cdot\rangle_E$.

Wegen (*) ist $M^{\mathcal{B}}_{\mathcal{B}}(\tilde{B})$ nicht unitär und nicht hermitesch (Diagonale von $M^{\mathcal{B}}_{\mathcal{B}}(\tilde{B})$ hat komplexen Eintrag).
$\mathcal{B}$ ONB $\Rightarrow$ $\tilde{B}$ ist nicht unitär und nicht selbstadjungiert.

(c)
- Bestimme Eigenwerte von B:

$$\chi_B = \det(tE_3 - B) = \begin{pmatrix} t-i & 2 & i-2 \\ 0 & t-(i-1) & 0 \\ 0 & 2i & t+(1+i) \end{pmatrix} \overset{\text{Sarrus}}{=} (t-i)(t-(-1+i))(t-(-1-i))$$

$\Longrightarrow$ Eigenwerte sind $i, -1+i, -1-i$.

- Bestimme die Eigenräume zu den Eigenwerten:

$$\begin{aligned}
\mathrm{Eig}(B,i) &= \mathrm{Kern}(B - iE_3) = \mathrm{Kern}\begin{pmatrix} 0 & 2 & i-2 \\ 0 & -1 & 0 \\ 0 & 2i & -1-2i \end{pmatrix} \\
&= \mathrm{Lin}((1,0,0)^t) \\
\mathrm{Eig}(B,-1+i) &= \mathrm{Kern}(B - (-1+i)E_3) = \mathrm{Kern}\begin{pmatrix} 1 & 2 & i-2 \\ 0 & 0 & 0 \\ 0 & 2i & -2i \end{pmatrix} \\
&= \mathrm{Lin}((i,-1,-1)^t) \\
\mathrm{Eig}(B,-1-i) &= \mathrm{Kern}(B - (-1-i)E_3) = \mathrm{Kern}\begin{pmatrix} 2i+1 & 2 & i-2 \\ 0 & 2i & 0 \\ 0 & 2i & 0 \end{pmatrix} \\
&= \mathrm{Lin}((i,0,-1)^t)
\end{aligned}$$

- Normieren der Vektoren in $(V, \langle\cdot,\cdot\rangle_A)$ liefert Basis (v_1, v_2, v_3) aus Eigenvektoren mit

$$\begin{aligned}
v_1 &= \frac{(1,0,0)^t}{\|(1,0,0)^t\|_A} = (1,0,0)^t, \\
v_2 &= \frac{(i,-1,-1)^t}{\|(i,-1,-1)^t\|_A} = (i,-1,-1)^t, \\
v_3 &= \frac{(i,0,-1)^t}{\|(i,0,-1)^t\|_A} = (i,0,-1)^t.
\end{aligned}$$

Spektralsatz $\overset{M^{\mathcal{B}}_{\mathcal{B}}(\tilde{B}) \text{ normal}}{\Longrightarrow}$ (v_1, v_2, v_3) ONB in $(V, \langle\cdot,\cdot\rangle_A)$.

Aufgabe 42 (Eigenschaften normaler Abbildungen, 4 = 2 + 2 Punkte).
Sei $(V, \langle\cdot,\cdot\rangle)$ ein endlichdimensionaler unitärer Vektorraum und $f \in \mathrm{End}_{\mathbb{C}}(V)$.

(a) Sei f normal und $f^3 = f^4$. Zeigen Sie: f ist selbstadjungiert und $f^2 = f$.
Hinweis: Übertragen Sie die gegebene Eigenschaft zunächst auf eine Aussage für $M^{\mathcal{B}}_{\mathcal{B}}(f)$, wobei $\mathcal{B}$ eine ONB aus Eigenvektoren von f ist, und folgern Sie Aussagen für die Eigenwerte von f.

(b) Zeigen Sie:

$$f \text{ ist normal} \quad \Longleftrightarrow \quad \exists p \in \mathbb{C}[t] : f^{\mathrm{ad}} = p(f) \text{ und } \mathrm{grad}(p) \leq \dim_{\mathbb{C}}(V) - 1.$$

Hinweis für „⇒“: Übertragen Sie die geforderte Eigenschaft zunächst auf eine Aussage für $M_{\mathcal{B}}^{\mathcal{B}}(f)$, wobei $\mathcal{B}$ eine ONB aus Eigenvektoren von f ist. Sie erhalten dadurch n Gleichungen, die p erfüllen muss. Konstruieren Sie damit ein geeignetes p.

Lösung:

(a) Spektralsatz $\Longrightarrow$ Es existiert eine ONB $\mathcal{B}$ mit $M_{\mathcal{B}}^{\mathcal{B}}(f) = \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix}$, wobei $\lambda_1, ..., \lambda_n$ die EW von f bezeichnen.
$f^4 - f^3 = 0 \Rightarrow \begin{pmatrix} \lambda_1^4 & & \\ & \ddots & \\ & & \lambda_n^4 \end{pmatrix} = M_{\mathcal{B}}^{\mathcal{B}}(f)^4 = M_{\mathcal{B}}^{\mathcal{B}}(f)^3 = \begin{pmatrix} \lambda_1^3 & & \\ & \ddots & \\ & & \lambda_n^3 \end{pmatrix} \Rightarrow \forall k \in \{1, ..., n\}$:
$\lambda_k^4 = \lambda_k^3$, d.h. $\lambda_k^3(\lambda_k - 1) = 0$
$\Rightarrow \forall k \in \{1, ..., n\}$: $\lambda_k \in \{0, 1\}$.
$\Rightarrow M_{\mathcal{B}}^{\mathcal{B}}(f)^2 = \begin{pmatrix} \lambda_1^2 & & \\ & \ddots & \\ & & \lambda_n^2 \end{pmatrix} = \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix} = M_{\mathcal{B}}^{\mathcal{B}}(f) \Rightarrow f^2 = f$, und

$$M_{\mathcal{B}}^{\mathcal{B}}(f^{\mathrm{ad}}) \overset{\mathcal{B}\text{ ONB}}{=} \overline{M_{\mathcal{B}}^{\mathcal{B}}(f)}^t \overset{\lambda_k \in \mathbb{R}}{=} \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix}^t = \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix} = M_{\mathcal{B}}^{\mathcal{B}}(f),$$

$\Rightarrow f^{ad} = f \Rightarrow f$ selbstadjungiert.

(b)

- „⇒“: Sei f normal.
  Spektralsatz $\Rightarrow$ Es gibt ONB $\mathcal{B}$ von (V, γ) mit $M_{\mathcal{B}}^{\mathcal{B}} = \begin{pmatrix} \lambda_1 & & \\ & \cdots & \\ & & \lambda_n \end{pmatrix}$ und $\lambda_1, ..., \lambda_n \in \mathbb{C}$.
  $\Rightarrow M_{\mathcal{B}}^{\mathcal{B}}(f^{ad}) = \overline{M_{\mathcal{B}}^{\mathcal{B}}(f)}^t = \begin{pmatrix} \overline{\lambda_1} & & \\ & \cdots & \\ & & \overline{\lambda_n} \end{pmatrix}$.

  Es gilt: $f^{ad} = p(f)$ mit einem Polynom $p \in \mathbb{C}[t]$ genau dann, wenn

  $$\begin{pmatrix} \overline{\lambda_1} & & \\ & \cdots & \\ & & \overline{\lambda_n} \end{pmatrix} = M_{\mathcal{B}}^{\mathcal{B}}(f^{ad}) = p\Big(M_{\mathcal{B}}^{\mathcal{B}}(f)\Big) = p\left(\begin{pmatrix} \lambda_1 & & \\ & \cdots & \\ & & \lambda_n \end{pmatrix}\right) = \begin{pmatrix} p(\lambda_1) & & \\ & \cdots & \\ & & p(\lambda_n) \end{pmatrix}.$$

  D.h.: Wir suchen ein Polynom $p \in \mathbb{C}[t]$ mit der Eigenschaft $p(\lambda_i) = \overline{\lambda_i}$, $i = 1, ..., n$.
  Sei $q_j := \prod_{i \in \{1,...,n\} \setminus \{j\}} (t - \lambda_i)$. Setze $p := \sum_{j=1}^n \frac{\overline{\lambda_j}}{q_j(\lambda_j)} \cdot q_j$.
  $\Rightarrow p(\lambda_k) = \sum_{j=1}^n \frac{\overline{\lambda_j}}{q_j(\lambda_j)} \cdot \underbrace{q_j(\lambda_k)}_{= q_j(\lambda_j)\delta_{jk}} = \overline{\lambda_k}$. Damit erfüllt p die gewünschte Eigenschaft.

- „⇐“: Es sei $p \in \mathbb{C}[t]$ mit $f^{ad} = p(f)$.
  $\Rightarrow p = \sum_{k=0}^n a_k t^k$.
  $\Rightarrow f \circ f^{ad} = f \circ p(f) = f \circ \sum_{k=0}^n a_k f^k = \sum_{k=0}^n a_k f^{k+1} = (\sum_{k=0}^n a_k f^k) \circ f = p(f) \circ f = f^{ad} \circ f$.

Aufgabe 43 (Eigenschaften von Idealen, 8 = 1.5 + 1 + 1 + 1.5 + 1 + 2 Punkte).
Sei R ein kommutativer Ring mit 1 und $I, J \subset R$ Ideale. Zeigen Sie:

(a) $I + J := \{x + y | x \in I, y \in J\}$ ist ein Ideal.

(b) $M := \{x \cdot y : x \in I, y \in J\}$ und $I \cup J$ sind im Allgemeinen keine Ideale.
Hinweis: Für ein Gegenbeispiel für M wählen Sie $R = \mathbb{Z}[t]$ und $I = (2, t)$, $J = (3, t)$.

(c) Falls R ein Hauptidealring ist, so ist M ein Ideal.

(d) $I \cdot J := \{\sum_{i=1}^{n} x_i \cdot y_i | n \in \mathbb{N}, x_i \in I, y_i \in J \text{ für } i = 1, ..., n\}$ ist ein Ideal.

(e) Es gilt $I \cdot J \subset I \cap J \subset I \subset I + J$.

(f) Die Inklusionen in Teil (c) können für $R = \mathbb{Z}$ alle echt sein.
Hinweis: Sie müssen nicht für alle Inklusionen dasselbe Beispiel nutzen!

Lösung:

(a) Wir zeigen die Idealeigenschaften für $I + J$:

- I,J Ideal $\Rightarrow 0 \in I, J \Rightarrow 0 = 0 + 0 \in I + J$.
- Seien $z_1, z_2 \in I + J$.
$\Rightarrow$ Es gibt $x_1, x_2 \in I$, $y_1, y_2 \in J$ mit $z_1 = x_1 + y_1$, $z_2 = x_2 + y_2$.
$\Rightarrow z_1 + z_2 = \underbrace{(x_1 + x_2)}_{\overset{I \text{ Ideal}}{\in} I} + \underbrace{(y_1 + y_2)}_{\overset{J \text{ Ideal}}{\in} J} \in I + J$.
- Sei $z \in I + J$, $r \in R$.
$\Rightarrow$ Es gibt $x \in I$, $y \in J$ mit $z = x + y$.
$\Rightarrow r \cdot z = \underbrace{r \cdot x}_{\overset{I \text{ Ideal}}{\in} I} + \underbrace{r \cdot y}_{\overset{J \text{ Ideal}}{\in} J} \in I + J$.

(b)
- (Es muss ein Ring gewählt werden, der kein Hauptidealring ist). Wähle $R = \mathbb{Z}[t]$ und $I = (2, t)$, $J = (3, t)$. Dann sind $2, t \in I$, $t, 3 \in J$ und damit $2t, 3t \in M$.
Aber $5t = 2t + 3t \notin M$, denn ansonsten müsste es $x \in I, y \in J$ geben mit $xy = 5t$.
$\mathbb{Z}[t]$ nullteilerfrei $\Rightarrow \text{grad}(x) + \text{grad}(y) = 1$
OBdA sei $\text{grad}(x) = 0$, $\text{grad}(y) = 1$.
$\overset{x \in I}{\Rightarrow} x = 2q \ (q \in \mathbb{Z})$
$\Rightarrow xy = 2qy$ ist ein Polynom mit geraden Koeffizienten und daher nicht $5t$.
- Wähle zum Beispiel $R = \mathbb{Z}$. Wähle $I = 2\mathbb{Z}$, $J = 3\mathbb{Z}$. Dann ist $2 \in I \cup J$, $3 \in I \cup J$, aber $5 = 2 + 3 \notin I, J$, d.h. $5 \notin I \cup J$.

(c) I, J Ideale in $R \Rightarrow I = (a), J = (b)$ mit $a, b \in R$. Es gilt

$$(a \cdot b) = M,$$

(und damit ist die rechte Seite ein Ideal) denn:
„$\subset$“: $r \in (a, b) \Rightarrow$ Es gibt $q \in R$ mit $r = \underbrace{a}_{\in I} \underbrace{bq}_{\in J} \in M$.
„$\supset$“: $r \in M \Rightarrow$ Es gibt $x \in I$, $y \in J$ mit $r = xy$.
$\Rightarrow$ Es gibt $q_1, q_2 \in R$ mit $x = q_1 a$, $y = q_2 b$
$\Rightarrow r = (q_1 q_2) ab \in (ab)$.

(d) Wir zeigen die Idealeigenschaften für $I \cdot J$:

- I,J Ideal $\Rightarrow 0 \in I, J \Rightarrow 0 = 0 \cdot 0 \in I \cdot J$.
- Seien $z_1, z_2 \in I \cdot J$.
$\Rightarrow$ Es gibt $n_1, n_2 \in \mathbb{N}$, $x_i, x'_i \in I$, $y_i, y'_i \in J$ mit $z_1 = \sum_{i=1}^{n_1} x_i \cdot y_i$, $z_2 = \sum_{i=1}^{n_2} x'_i \cdot y'_i$.
Definiere $x_{n_1+i} := x'_i$, $y_{n_1+i} := y'_i$ $(i = 1, ..., n_2)$.
$\Rightarrow z_1 + z_2 = \sum_{i=1}^{n_1+n_2} x_i \cdot y_i \in I \cdot J$.

- Sei $z \in I \cdot J$, $r \in R$.
  $\Rightarrow$ Es gibt $n \in \mathbb{N}$, $x_i \in I$, $y_i \in J$ mit $z = \sum_{i=1}^n x_i \cdot y_i$.
  $\Rightarrow r \cdot z = \sum_{i=1}^n \underbrace{(r \cdot x_i)}_{\overset{I \text{ Ideal}}{\in} I} \cdot y_i \in I \cdot J$.

(e)
- „$I \cdot J \subset I \cap J$": Sei $z \in I \cdot J$.
  $\Rightarrow$ Es gibt $n \in \mathbb{N}$, $x_i \in I$, $y_i \in J$ mit

$$z = \sum_{i=1}^n \underbrace{x_i \cdot \underbrace{y_i}_{\in I \subset R}}_{\overset{I \text{ Ideal}}{\in} I} \overset{I \text{ Ideal } (a,b \in I \Rightarrow a+b \in I}{\in} I.$$

  Analog: $z \in J$.
  $\Rightarrow z \in I \cap J$.
- „$I \cap J \subset I$": trivial.
- „$I \subset I + J$": Sei $x \in I$.
  $\Rightarrow x = x + \underbrace{0}_{\overset{J \text{ Ideal}}{\in} J} \in I + J$.

(f) Sei $I := 2\mathbb{Z} = \{2q : q \in \mathbb{Z}\}$ und $J = 4\mathbb{Z} = \{4q : q \in \mathbb{Z}\}$.
Dann gilt:

$$I \cap J = J \neq I.$$

Außerdem:

$$I \cdot J = 8\mathbb{Z} \neq J,$$

denn: „$\subset$": $z \in I \cdot J \Rightarrow$ Es gibt $n \in \mathbb{N}$, $x_i \in I$, $y_i \in J$ mit $z = \sum_{i=1}^n x_i y_i$.
$x_i \in I \Rightarrow$ Es gibt $q_i \in \mathbb{Z}$ mit $x_i = 2q_i$,
$y_i \in J \Rightarrow$ Es gibt $p_i \in \mathbb{Z}$ mit $y_i = 4p_i$,
$\Rightarrow z = \sum_{i=1}^n x_i y_i = 8 \cdot \sum_{i=1}^n p_i q_i \in 8\mathbb{Z}$.
„$\supset$": $x \in 8\mathbb{Z} \Rightarrow$ Es gibt $q \in \mathbb{Z}$ mit $x = 8q = \underbrace{2q}_{\in 2\mathbb{Z}} \cdot \underbrace{4}_{\in 4\mathbb{Z}} \in I \cdot J$.

Wähle nun $J = 3\mathbb{Z} = \{3q : q \in \mathbb{Z}\}$.
Dann gilt:

$$I \neq \mathbb{Z} \overset{!}{=} I + J = 2\mathbb{Z} + 3\mathbb{Z},$$

da: „$\subset$" ist klar, „$\supset$": $1 = 3 - 2 \in I + J$. Ist $r \in \mathbb{Z}$ beliebig, so ist also auch $r = r \cdot 1 \overset{I+J \text{ Ideal}}{\in} I + J$.

Aufgabe 44 (Beispiel für einen nicht-faktoriellen Ring, 7 = 1 + 1 + 1.5 + 1 + 1 + 1.5 Bonuspunkte).

Diese Aufgabe gibt ein Beispiel für einen Ring, der nicht faktoriell ist. Wir werden sehen, dass die Existenz eines größten gemeinsamen Teilers und die eindeutigen Zerlegung in irreduzible Faktoren hier nicht vorliegt.

Wir betrachten den Unterring $\mathbb{Z}[\sqrt{-5}] := \{a + b\sqrt{-5} | a, b \in \mathbb{Z}\} \subset \mathbb{C}$ von $\mathbb{C}$. Es sei $\delta : \mathbb{Z}[\sqrt{-5}] \to \mathbb{N}_0, a + b\sqrt{-5} \mapsto a^2 + 5b^2$. Zeigen Sie:

(a) Für $f, g \in \mathbb{Z}[\sqrt{-5}]$ gilt: $\delta(fg) = \delta(f)\delta(g)$.

(b) $\mathbb{Z}[\sqrt{-5}]^* = \{-1, +1\}$.

(c) Die Elemente $2, 1+\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ sind irreduzibel, aber nicht prim.
Bemerkung: Analoge Aussagen gelten für $3, 1-\sqrt{5}$ *(dies darf im Folgenden ohne Beweis angenommen werden).*

(d) Geben Sie für $6 \in \mathbb{Z}[\sqrt{-5}]$ zwei verschiedene Darstellungen in irreduzible Faktoren an und zeigen Sie, dass diese nicht zueinander assoziiert sind.

(e) Ist $\mathbb{Z}[\sqrt{-5}]$ ein Hauptidealring?

(f) Es gilt $\mathrm{GGT}(6, 2+2\sqrt{-5}) = \emptyset$.

Lösung:

(a) Seien $f = a + b\sqrt{-5}, g = c + d\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$.
$\Rightarrow fg = (a+b\sqrt{-5})(c+d\sqrt{-5}) = (ac-5bd) + (ad+bc)\sqrt{-5}$.
$\Rightarrow$

$$\begin{aligned}\delta(fg) &= (ac-5bd)^2 + 5(ad+bc)^2 \\ &= a^2c^2 - 10abcd + 25b^2d^2 + a^2d^2 + 10abcd + 5b^2c^2 \\ &= a^2(c^2+d^2) + 5b^2(c^2+5d^2) \\ &= (a^2+5b^2)(c^2+5d^2) = \delta(f)\delta(g).\end{aligned}$$

(b) Wir zeigen zunächst: $z \in \mathbb{Z}[\sqrt{-5}]^* \Rightarrow \delta(z) = 1$.
Sei $z \in \mathbb{Z}[\sqrt{-5}]^* \Rightarrow$ Es gibt $w \in \mathbb{Z}[\sqrt{-5}]$ mit $z \cdot w = 1 \Rightarrow 1 = 1^2 + 5 \cdot 0^2 = \delta(1) = \delta(z \cdot w) \overset{(a)}{=} \delta(z) \cdot \delta(w)$.
$\overset{\delta(z),\delta(w)\in\mathbb{N}_0}{\Rightarrow} \delta(z) = \delta(w) = 1$.

Sei $z = a + b\sqrt{-5}$ und $1 = \delta(z) = a^2 + 5b^2$.
$\Rightarrow b = 0$ (bereits $|b| \geq 1$ liefert $\delta(z) \geq 5$).
$\Rightarrow 1 = a^2 \Rightarrow a \in \{-1, +1\}$.
$\Rightarrow z \in \{-1, +1\}$.
Damit ist gezeigt: $\mathbb{Z}[\sqrt{-5}]^* \subset \{-1, +1\}$.
Tatsächlich gilt sogar Gleichheit, denn $1 \cdot 1 = 1$ und $(-1) \cdot (-1) = 1$.

(c)
- Seien $f, g \in \mathbb{Z}[\sqrt{-5}]$ mit $2 = fg \Rightarrow 4 = \delta(2) \overset{(a)}{=} \delta(f)\delta(g)$.
$\Rightarrow \delta(f) = 2 = \delta(g)$ oder $\{\delta(f), \delta(g)\} = \{1, 4\}$. $\delta(f) = 2$ ist jedoch nicht möglich (ist $f = a + b\sqrt{-5}$, so ist $\delta(f) = a^2 + 5b^2$. $\delta(f) = 2 \Rightarrow b = 0 \Rightarrow 2 = a^2$; dies besitzt keine Lösung für $a \in \mathbb{Z}$).
- Seien $f, g \in \mathbb{Z}[\sqrt{-5}]$ mit $3 = fg \Rightarrow 9 = \delta(3) \overset{(a)}{=} \delta(f)\delta(g)$.
$\Rightarrow \delta(f) = 3 = \delta(g)$ oder $\{\delta(f), \delta(g)\} = \{1, 9\}$. $\delta(f) = 3$ ist jedoch nicht möglich (ist $f = a + b\sqrt{-5}$, so ist $\delta(f) = a^2 + 5b^2$. $\delta(f) = 3 \Rightarrow b = 0 \Rightarrow 3 = a^2$; dies besitzt keine Lösung für $a \in \mathbb{Z}$).
- Analog für $1+\sqrt{-5}, 1-\sqrt{-5}$ wegen $\delta(1+\sqrt{-5}) = \delta(1-\sqrt{-5}) = 6 = 2 \cdot 3$.

$\Rightarrow 2, 3, 1+\sqrt{-5}, 1-\sqrt{-5}$ irreduzibel.

- 2 ist nicht prim, denn: Seien $a = 1+\sqrt{-5}, b = 1-\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$. Dann gilt $a \cdot b = 1 - (-5) = 6 = 2 \cdot 3$, d.h. $2 | a \cdot b$.
Aber $2 \nmid a$, $2 \nmid b$ (sonst gäbe es $f \in \mathbb{Z}[\sqrt{-5}]$ mit $a = 2 \cdot f \Rightarrow 6 = \delta(a) = \delta(2) \cdot \delta(f) = 4\delta(f)$, Widerspruch).

- Analog (mit den gleichen a, b) zeigt man: 3 ist nicht prim.
- $1+\sqrt{-5}$ ist nicht prim, denn: Seien $a = 2, b = 3 \in \mathbb{Z}[\sqrt{-5}]$. Dann gilt $a \cdot b = 6 = (1+\sqrt{-5})(1-\sqrt{-5})$, d.h. $(1+\sqrt{-5}) | a \cdot b$.
  Aber $(1+\sqrt{-5}) \nmid a$, $(1+\sqrt{-5}) \nmid b$ (sonst gäbe es $f \in \mathbb{Z}[\sqrt{-5}]$ mit $a = (1+\sqrt{-5}) \cdot f$ $\Rightarrow 4 = \delta(a) = \delta(1+\sqrt{-5}) \cdot \delta(f) = 6\delta(f)$, Widerspruch).
- Analog (mit den gleichen a, b) zeigt man: $1-\sqrt{-5}$ ist nicht prim.

(d) Es ist $6 = (1+\sqrt{-5})(1-\sqrt{-5}) = 2 \cdot 3$.
Wäre $2 \hat{=} 1+\sqrt{-5}$, würde gelten: Es gibt $f \in \mathbb{Z}[\sqrt{-5}]^*$ mit $2 = f \cdot (1+\sqrt{-5})$.
$\Rightarrow 4 = \delta(2) = \delta(f)\delta(1+\sqrt{-5}) = 6\delta(f)$, Widerspruch.
(Alternative Argumentation: Es wurde bereits gezeigt, dass $\mathbb{Z}[\sqrt{-5}]^* = \{-1, +1\}$. Offensichtlich ist $2 \neq (-1) \cdot (1+\sqrt{-5})$ und $2 \neq 1 \cdot (1+\sqrt{-5})$).
Analog zeigt man, dass $2 \hat{=} 1-\sqrt{-5}$ nicht gilt.

(e) Angenommen $\mathbb{Z}[\sqrt{-5}]$ wäre ein Hauptidealring. $\Rightarrow$ Jedes irreduzible Element ist prim, Widerspruch zu (c).
Also ist $\mathbb{Z}[\sqrt{-5}]$ kein Hauptidealring.

(f) Angenommen, $d \in GGT(6, 2+2\sqrt{-5})$.
$6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$, $2+2\sqrt{-5} = 2(1+\sqrt{-5}) \overset{\text{Eig. 2 ggT}}{\Rightarrow} 2|d$, $(1+\sqrt{-5})|d$
$\Rightarrow$ Es gibt $f, g \in \mathbb{Z}[\sqrt{-5}]$ mit $d = 2 \cdot f = (1+\sqrt{-5}) \cdot g$
$\Rightarrow \delta(d) = \underbrace{\delta(2)}_{=4} \delta(f) = \underbrace{\delta(1+\sqrt{-5})}_{=6} \delta(g)$.
$\Rightarrow 12|\delta(d)$.
Eig. 1 ggT $\Rightarrow d|6$, $d|(2+2\sqrt{-5}) \Rightarrow$ Es gibt $p, q \in \mathbb{Z}[\sqrt{-5}]$ mit $6 = d \cdot p$, $2+2\sqrt{-5} = d \cdot q$.
$\Rightarrow 36 = \delta(6) = \delta(d)\delta(p)$, $24 = \delta(2+2\sqrt{-5}) = \delta(d)\delta(q)$.
$\Rightarrow \delta(d)|24$, $\delta(d)|36$.
$\Rightarrow 12|\delta(d)|24, 36 \Rightarrow d = 12$.
Sei $d = a + b\sqrt{-5}$ mit $a, b \in \mathbb{Z}$.
$12 = \delta(d) = a^2 + 5b^2$. Dies ist für $a, b \in \mathbb{Z}$ nicht möglich. (für $b^2 = 0$ müsste $a^2 = 12$ sein, für $b^2 = 1$ müsste $a^2 = 7$ sein, für $b^2 \geq 4$ ist $\delta(d) > 12$), d.h. es entsteht ein Widerspruch.

Aufgabe 45 (Irreduzibilität im Polynomraum, 4 = 1 + 1 + 2 Bonuspunkte).
Sei K ein Körper und $f \in K[t]$.

(a) Zeigen Sie: Ist $\text{grad}(f) \geq 2$, so gilt: f irreduzibel $\Rightarrow f$ hat keine Nullstelle in K.

(b) Zeigen Sie: Ist $\text{grad}(f) \in \{2, 3\}$, so gilt:

$$f \text{ irreduzibel} \iff f \text{ hat keine Nullstelle in } K.$$

(c) Bestimmen Sie alle irreduziblen Elemente $f \in F_2[t]$ mit $\text{grad}(f) \leq 3$.

Lösung:

(a) Sei $\text{grad}(f) \geq 2$. Wir zeigen die Kontraposition. f habe Nullstelle $\lambda \in K \Rightarrow$ Es gibt $q \in K[t]$ mit $f = (t-\lambda)q$.
$\Rightarrow 2 \leq \text{grad}(f) = \text{grad}((t-\lambda)q) = \underbrace{\text{grad}(t-\lambda)}_{=1} + \text{grad}(q) \Rightarrow \text{grad}(q) \geq 1 \overset{(a)}{\Rightarrow} q \notin K[t]^* \Rightarrow$
f nicht irreduzibel.

(b) Sei $\mathrm{grad}(f) \in \{2,3\}$.

- „$\Rightarrow$“: Folgt aus (a).
- „$\Leftarrow$“: Wir zeigen die Kontraposition. Sei f nicht irreduzibel $\Rightarrow$ Es gibt $p, q \in K[t] \setminus \underbrace{(K[t]^* \cup \{0\})}_{=K}$ mit $f = pq$ ($\Rightarrow \mathrm{grad}(p), \mathrm{grad}(q) \in \mathbb{N}$).

  $\Rightarrow \{2,3\} \ni \mathrm{grad}(f) = \mathrm{grad}(pq) = \mathrm{grad}(p) + \mathrm{grad}(q) \overset{\mathrm{grad}(p),\mathrm{grad}(q) \in \mathbb{N}}{\Rightarrow} \mathrm{grad}(p) = 1$ oder $\mathrm{grad}(q) = 1$.
  OBdA. sei $\mathrm{grad}(p) = 1$. $\Rightarrow p = at + b$, $a \in K \setminus \{0\} \Rightarrow p(-ba^{-1}) = 0 \Rightarrow f(-ba^{-1}) = p(-ba^{-1})q(-ba^{-1}) = 0 \Rightarrow f$ besitzt Nullstelle $-ba^{-1} \in K$.

(c) Grad 1: (b) $\Rightarrow t, t+1$ sind irreduzibel.
Grad 2: Die Polynome $t^2, t(t+1) = t^2 + t, (t+1)^2 = t^2 + 1$ sind offensichtlich nicht irreduzibel.
Das noch fehlende Polynom vom Grad 2, $p = t^2 + t + 1$, ist irreduzibel, denn: $p(0) = p(1) = 1$, d.h. p hat keine Nullstellen $\overset{A45(b)}{\Rightarrow}$ p irreduzibel.
Grad 3: Die Polynome $t^3, t^2(t+1) = t^3 + t^2, t(t+1)^2 = t^3 + t, (t+1)^3 = t^3 + t^2 + t + 1, t(t^2 + t + 1) = t^3 + t^2 + t^2 + t, (t+1)(t^2 + t + 1) = t^3 + 1$ sind offensichtlich nicht irreduzibel.
Die beiden fehlenden Polynome $p_1 = t^3 + t^2 + 1$, $p_2 = t^3 + t + 1$ sind irreduzibel, denn: $p_1(0) = p_1(1) = p_2(0) = p_2(1) = 1$, d.h. p_1, p_2 haben keine Nullstellen $\overset{A45(c)}{\Rightarrow}$ p_1, p_2 irreduzibel.

Aufgabe 46 (Anwendungen des Homomorphiesatzes, 5 = 2 + 3 Bonuspunkte).

(a) Es sei $\mathbb{R}^2 := \mathbb{R} \times \mathbb{R}$ der kommutative Ring mit 1, welcher durch komponentenweise Addition/Multiplikation entsteht. Zeigen Sie, dass

$$\varphi : \mathbb{R}[t] \to \mathbb{R}^2, \quad p \mapsto (p(0), p(1))$$

ein Ringhomomorphismus ist und folgern Sie $\mathbb{R}[t]/(t(t-1)) \cong \mathbb{R}^2$. Ist $\mathbb{R}[t]/(t(t-1))$ ein Körper?

(b) Die Menge $\mathbb{Q}[\sqrt{-5}] := \{a + b\sqrt{-5} : a, b \in \mathbb{Q}\} \subset \mathbb{C}$ ist als Unterring von $\mathbb{C}$ ein kommutativer Ring mit 1. Zeigen Sie, dass $\mathbb{Q}[t]/(t^2 - 2t + 6) \cong \mathbb{Q}[\sqrt{-5}]$. Ist $\mathbb{Q}[t]/(t^2 - 2t + 6)$ ein Körper?

Lösung:

(a) φ ist ein surjektiver Ringhomomorphismus, denn:

- $\varphi(1) = (1(0), 1(1)) = (1, 1) = 1_{\mathbb{R}^2}$
- für $p, q \in \mathbb{R}[t]$ gilt:

$$\begin{aligned}
\varphi(p+q) &= ((p+q)(0), (p+q)(1)) = (p(0) + q(0), p(1) + q(1)) \\
&= (p(0), p(1)) + (q(0), q(1)) = \varphi(p) + \varphi(q), \\
\varphi(p \cdot q) &= ((p \cdot q)(0), (p \cdot q)(1)) = (p(0) \cdot q(0), p(1) \cdot q(1)) \\
&= (p(0), p(1)) \cdot (q(0), q(1)) = \varphi(p) \cdot \varphi(q).
\end{aligned}$$

- φ ist surjektiv, denn: Sei $(r, s) \in \mathbb{R}^2$ beliebig. Wähle $p = -r(t-1) + st \in \mathbb{R}[t]$, so gilt $\varphi(p) = (-r \cdot (-1) + s \cdot 0, -r \cdot 0 + s \cdot 1) = (r, s)$.

Weiter ist $\mathrm{Kern}(\varphi) = \{p \in \mathbb{R}[t] : (p(0), p(1)) = \varphi(p) = (0,0)\} = (t(t-1))$, denn:
$p \in \mathrm{Kern}(\varphi) \iff p(0) = 0,\ p(1) = 0 \iff$ Es gibt $q \in \mathbb{R}[t]$ mit $p = (t-0)(t-1)q = t(t-1)q \iff p \in (t(t-1))$.
Homomorphiesatz $\Rightarrow \mathbb{R}[t]/(t(t-1)) = \mathbb{R}[t]/\mathrm{Kern}(\varphi) \cong \mathbb{R}^2$.
$\mathbb{R}^2$ kein Körper $\Rightarrow \mathbb{R}[t]/(t(t-1))$ kein Körper.

(b) Es ist $t^2 - 2t + 6 = (t-\lambda_1)(t-\overline{\lambda_1})$ mit $\lambda_1 := 1 + \sqrt{-5} = 1 + i\sqrt{5}$. Definiere die Abbildung

$$\varphi : \mathbb{Q}[t] \to \mathbb{Q}[\sqrt{-5}], \quad \varphi(p) := p(\lambda_1).$$

φ ist ein surjektiver Ringhomomorphismus, denn:

- $\varphi(1) = 1(\lambda_1) = 1 = 1_{\mathbb{Q}[\sqrt{-5}]}$,
- Für $p, q \in \mathbb{Q}[t]$ gilt

$$\varphi(pq) = (pq)(\lambda_1) = p(\lambda_1)q(\lambda_1) = \varphi(p)\varphi(q),$$
$$\varphi(p+q) = (p+q)(\lambda_1) = p(\lambda_1) + q(\lambda_1) = \varphi(p) + \varphi(q).$$

- φ ist surjektiv, denn: Sei $a + b\sqrt{-5} \in \mathbb{Q}[\sqrt{-5}]$ beliebig. Wähle $p = a + b(t-1)$, dann gilt $\varphi(p) = p(\lambda_1) = a + b(\lambda_1 - 1) = a + b\sqrt{-5}$.

Außerdem ist $\mathrm{Kern}(\varphi) = \{p \in \mathbb{Q}[t] : p(\lambda_1) = \varphi(p) = 0\} = (t^2 - 2t + 6)$, denn:
„$\subset$“: Ist $p(\lambda_1) = 0 \overset{P0.4}{\Rightarrow} \Rightarrow$ Es gibt $q \in \mathbb{Q}[t]$ mit $p = (t-\lambda_1)(t-\overline{\lambda_1})q = (t^2 - 2t + 6)q \in (t^2 - 2t + 6)$.
„$\supset$“: Ist $p \in (t^2 - 2t + 6)$, so gibt es $q \in \mathbb{Q}[t]$ mit $p = (t^2 - 2t + 6)q \Rightarrow p(\lambda_1) = \underbrace{(\lambda_1^2 - 2\lambda_1 + 6)}_{=0} q = 0$.

Homomorphiesatz $\Rightarrow \mathbb{Q}[t]/(t^2 - 2t + 6) = \mathbb{Q}[t]/\mathrm{Kern}(\varphi) \cong \mathbb{Q}[\sqrt{-5}]$.
$\mathbb{Q}[\sqrt{-5}]$ ist ein Körper, denn: Für $a + b\sqrt{-5} \in \mathbb{Q}[\sqrt{-5}]$ erfüllt $\frac{1}{a+b\sqrt{-5}} = \frac{a-b\sqrt{-5}}{(a+b\sqrt{-5})(a-b\sqrt{-5})} = \frac{a-b\sqrt{-5}}{a^2+5b^2} \in \mathbb{Q}[\sqrt{-5}]$ offensichtlich $8a + b\sqrt{-5}) \cdot \frac{1}{a+b\sqrt{-5}} = 1$.
$\Rightarrow \mathbb{Q}[t]/(t^2 - 2t + 6)$ Körper.

Abgabe:
In Zweiergruppen, bis spätestens Donnerstag, den **11. Juli 2019, 09:15 Uhr**.
(Die Zettelkästen für das Abgabeblatt sind im 1. OG, INF 205, vor dem Dekanat.)

Homepage der Vorlesung:
`https://ssp.math.uni-heidelberg.de/la2-ss2019/index.html`