UNIVERSITÄT HEIDELBERG
ZUKUNFT SEIT 1386

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

11. Präsenzblatt – Lösungen

Aufgabe P41 (Anwendung des Spektralsatzes auf unitären Räumen).

Zusammen mit dem von der Matrix $A := \begin{pmatrix} 1 & i & 0 \\ -i & 3 & i \\ 0 & -i & 1 \end{pmatrix}$ induzierten Skalarprodukt ist $V = \mathbb{C}^3$ ein unitärer Raum. Es bezeichne $E = (e_1, e_2, e_3)$ die Standardbasis. Gegeben sei nun $\tilde{B} \in \mathrm{End}_{\mathbb{C}}(V)$ mit

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

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

(b) Zeigen Sie, dass $\tilde{B}$ normal für den Raum $(V, \langle \cdot, \cdot \rangle_A)$ ist, aber nicht im unitären Standardraum $(V, \langle \cdot, \cdot \rangle)$. Ist $\tilde{B}$ unitär oder selbstadjungiert für $(V, \langle \cdot, \cdot \rangle_A)$?

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

Lösung:

(a) Wir bestimmen ausgehend von E eine ONB von V bezüglich $\langle \cdot, \cdot \rangle_A$.

- $\tilde{w}_1 = e_1, \|\tilde{w}_1\|_A^2 = 1 \implies w_1 := \tilde{w}_1 = e_1 = (1, 0, 0)^t$
- $\tilde{w}_2 = e_2 - \langle e_2, w_1 \rangle_A w_1 = e_2 + i w_1 = (i, 1, 0)^t$.
  $\|\tilde{w}_2\|_A^2 = 2 \implies w_2 := \frac{1}{\sqrt{2}}(i, 1, 0)^t$
- $\tilde{w}_1 = e_3 - \langle e_3, w_1 \rangle_A w_1 - \langle e_3, w_2 \rangle_A w_2 = e_3 - 0 \cdot w_1 + \frac{1}{2} i (i, 1, 0)^t = (-1/2, 1/2, 1)^t$
  $\|\tilde{w}_3\|_A^2 = \frac{1}{2} \implies w_3 := \sqrt{2}(-1/2, i/2, 1)^t$

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

(b) Es gilt

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

und $\overline{M_{\mathcal{B}}^{\mathcal{B}}(\tilde{B})}^t M_{\mathcal{B}}^{\mathcal{B}}(\tilde{B}) = M_{\mathcal{B}}^{\mathcal{B}}(\tilde{B}) \overline{M_{\mathcal{B}}^{\mathcal{B}}(\tilde{B})}^t$, also $\tilde{B}$ normal bezüglich $\langle \cdot, \cdot \rangle_A$.
Für die Standardbasis gilt

$$\overline{M_E^E(\tilde{B})}^t M_E^E(\tilde{B}) = \begin{pmatrix} 4 & -4i & -2i \\ 4i & 4 & 2 \\ 2i & 2 & 6 \end{pmatrix} \neq \begin{pmatrix} 9 & i & -2 \\ -i & 1 & 2i \\ -2 & -2i & 4 \end{pmatrix} = M_E^E(\tilde{B}) \overline{M_E^E(\tilde{B})}^t$$

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

Nun ist $M_{\mathcal{B}}^{\mathcal{B}}(\tilde{B})$ offensichtlich nicht unitär und nicht hermitesch (Diagonale besitzt komplexen Eintrag).
$\mathcal{B}$ ONB $\implies \tilde{B}$ ist nicht unitär und nicht selbstadjungiert.

(c) Die Darstellung von $M_{\mathcal{B}}^{\mathcal{B}}(\tilde{B})$ ist bereits diagonal.
Die Eigenvektoren sind gegeben durch die Spalten von $T_E^{\mathcal{B}}$ und sind in $(V, \langle\cdot,\cdot\rangle_A)$ bereits normiert.
Spektralsatz $\implies$ (w_1, w_2, w_3) ist ONB von $(V, \langle\cdot,\cdot\rangle_A)$.

Aufgabe P42 (Eigenschaften normaler Abbildungen).
Sei $(V, \langle\cdot,\cdot\rangle)$ ein endlichdimensionaler unitärer Vektorraum und $f \in \mathrm{End}_{\mathbb{C}}(V)$.

(a) Sei f normal und nilpotent. Zeigen Sie: $f = 0$.

(b) Sei $f^{ad} = -f$. Zeigen Sie, dass f eine ONB aus Eigenvektoren besitzt.

(c) Sei f diagonalisierbar. Zeigen Sie: Es existiert ein Skalarprodukt $\langle\cdot,\cdot\rangle_*$ auf V, so dass f normal bezüglich $\langle\cdot,\cdot\rangle_*$ ist.

Lösung:

(a) f normal $\Rightarrow$ Es gibt 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 Eigenwerte von f bezeichnen.
f nilpotent $\Rightarrow \lambda_i = 0$ $(i = 1, ..., n)$.
$\Rightarrow M_{\mathcal{B}}^{\mathcal{B}}(f) = 0$
$\Rightarrow f = 0$.

(b) $f^{ad} = -f \Rightarrow f^{ad} \circ f = (-f) \circ f = -f \circ f \overset{f \text{ linear}}{=} f \circ (-f) = f \circ f^{ad} \Rightarrow f$ normal.
Spektralsatz $\Rightarrow f$ besitzt ONB aus Eigenvektoren.

(c) f diagonalisierbar $\Rightarrow$ Es gibt Basis $\mathcal{B} = (v_1, ..., v_n)$ aus EV von f.
Definiere $\langle\cdot,\cdot\rangle_* : V \times V \to \mathbb{C}$, so dass $M_{\mathcal{B}}^*(\langle\cdot,\cdot\rangle_*) = E_n$ (bzw. $\langle\cdot,\cdot\rangle_* := \gamma_{E_n}^{\mathcal{B}'}$).
$\Rightarrow \mathcal{B}$ in $(V, \langle\cdot,\cdot\rangle_*)$ ONB aus EV von f.
Spektralsatz für normale Abb. $\Rightarrow f$ normal in $(V, \langle\cdot,\cdot\rangle_*)$.

Aufgabe P43 (Eigenschaften von Idealen).
Sei R ein kommutativer Ring mit 1 und I, J Ideale von R. Zeigen Sie:

(a) $I \cap J$ ist ein Ideal.

(b) Sei $(I_n)_{n\in\mathbb{N}}$ eine aufsteigende Kette von Idealen von R, d.h. $I_m \subset I_n$ für $m \leq n$. Dann ist $M = \cup_{n\in\mathbb{N}} I_n$ ein Ideal von R.

(c) Sei $S \subset R$ eine Teilmenge. $A := \{r \in R \,|\, \forall s \in S : rs = 0\}$ ist ein Ideal in R.

(d) $I : J := \{r \in R \,|\, rJ \subset I\}$ ist ein Ideal in R.

Lösung:

(a) Wir zeigen, dass $I \cap J$ die Eigenschaften eines Ideals in R erfüllt:

- I, J Ideal $\implies 0 \in I, J \implies 0 \in I \cap J$.
- Seien $x, y \in I \cap J$.
  $\implies x \in I$, $y \in I$ und $x \in J$, $y \in J$.
  $\overset{I,J \text{ Ideale}}{\implies} x + y \in I$ und $x + y \in J \implies x + y \in I \cap J$.

- Sei $r \in R$ und $x \in I \cap J$.
  $\implies x \in I$ und $x \in J$
  $\overset{I,J \text{ Ideale}}{\implies} rx \in I$ und $rx \in J \implies rx \in I \cap J$.

(b) Wir zeigen, dass M die Eigenschaften eines Ideals in R erfüllt:

- I_1 Ideal $\implies 0 \in I_1$ und $0 \in M$
- Seien $x, y \in M$.
  $\implies \exists\, m, n : x \in I_m, y \in I_n$
  Sei OBdA $m \leq n$, also $I_m \subset I_n$.
  $\implies x, y \in I_n \overset{I_n \text{ Ideal}}{\implies} x + y \in I_n \implies x + y \in M$.
- Sei $r \in R$ und $x \in I$.
  $\implies \exists\, n : x \in I_n \overset{I_n \text{ Ideal}}{\implies} rx \in I_n \implies rx \in M$.

(c) Wir zeigen, dass A die Eigenschaften eines Ideals in R erfüllt:

- $0 \in R$ und $\forall s \in S : 0 \cdot s = 0 \implies 0 \in A$.
- Seien $x, y \in A$.
  $\implies \forall s \in S : xs = 0$ und $ys = 0$
  $\implies \forall s \in S : (x + y)s = xs + ys = 0 + 0 = 0 \implies x + y \in A$.
- Sei $x \in A$, $r \in R$.
  $\implies \forall s \in S : (rx)s = r(xs) = r \cdot 0 = 0 \implies rx \in A$.

(d) Wir zeigen, dass $I : J$ die Eigenschaften eines Ideals in R erfüllt:

- Es ist $0 \cdot J = \{0 \cdot x : x \in J\} = \{0\} \overset{I \text{ Ideal}}{\subset} I \Rightarrow 0 \in I : J$.
- Seien $x, y \in I : J$.
  $\Rightarrow xJ, yJ \subset I$.
  (im Grunde klar: $(x + y)J = xJ + yJ \subset I + I \overset{I \text{ Ideal}}{=} I$), aber Rechnen mit Mengen wurde in der Vorlesung nicht sauber eingeführt.
  Sei $z \in (x + y)J$. $\Rightarrow$ Es gibt $r \in J$ mit $z = (x + y)r = \underbrace{xr}_{\in xJ \subset I} + \underbrace{yr}_{\in yJ \subset I} \overset{I \text{ Ideal}}{\in} I$.
- Sei $x \in I : J$, $r \in R$.
  $\Rightarrow xJ \subset I$.
  Wir zeigen $(rx)J \subset I$: Sei $z \in (rx)J \Rightarrow$ Es gibt $y \in J$ mit $z = (rx)y = r(\underbrace{xy}_{\in xJ \subset I}) \overset{I \text{ Ideal}}{\in} I$.

Aufgabe P44 (Einheiten, irreduzible Elemente und Primelemente).

(a) (i) Zeigen Sie: Ist R ein kommutativer Ring mit 1 und $r \in R \backslash \{0\}$ ein Nullteiler, so ist $r \notin R^*$.
Hinweis: $r \in R \backslash \{0\}$ heißt Nullteiler, falls es $s \in R \backslash \{0\}$ gibt mit $r \cdot s = 0$.

(ii) Bestimmen Sie die Einheiten und irreduziblen Elemente im Ring $\mathbb{Z}/6\mathbb{Z}$.

(b) Die Menge $\mathbb{Z} \times \mathbb{Z}$ sei ausgestattet mit der komponentenweisen Addition/Multiplikation. Dann ist $R := \mathbb{Z} \times \mathbb{Z}$ ein kommutativer Ring mit 1.

(i) Bestimmen Sie das Null- und das Einselement.

(ii) Bestimmen Sie alle Einheiten. Zeigen Sie, dass $(1,0)$ ein Primelement, aber kein irreduzibles Element ist.

(iii) Warum ist das kein Widerspruch zu den Resultaten der Vorlesung?

(c) (i) Zeigen Sie, dass für einen beliebigen Körper K gilt: $K[t]^* = K^* = K\backslash\{0\}$.

(ii) Wir betrachten den Ring $\mathbb{R}[t]$. Entscheiden Sie, ob $t^2 - t$ und $t^2 + 1$ irreduzibel und/oder Primelemente sind.

(iii) Die Menge $R := \mathbb{R} + t^2 \cdot \mathbb{R}[t] \subset \mathbb{R}[t]$ ist ein kommutativer Ring mit 1. Zeigen Sie, dass t^2 irreduzibel, aber nicht prim ist. Ist R ein Hauptidealring?
Hinweis: Nutzen Sie ohne Beweis, dass $R^* = \mathbb{R}\backslash\{0\}$.

(iv) Zeigen Sie: $\text{grad}(f) = 1 \Rightarrow f$ irreduzibel.

(v) Bestimmen Sie (bis auf Assoziiertheit) alle irreduziblen Elemente in $\mathbb{C}[t]$.

(d) Die Menge $\mathbb{Z}[i] := \{a+bi : a, b \in \mathbb{Z}\} \subset \mathbb{C}$ ist als Unterring von $\mathbb{C}$ ein kommutativer Ring mit 1. Es sei $\delta : \mathbb{Z}[i] \to \mathbb{N}_0, \delta(a+bi) := a^2+b^2$. Man kann zeigen (s. Wiederholungsblatt), dass $\mathbb{Z}[i]$ mit Gradfunktion δ ein Euklidischer Ring ist. Zeigen Sie:

(i) Für $f, g \in \mathbb{Z}[i]$ gilt: $\delta(fg) = \delta(f)\delta(g)$, d.h. δ ist *multiplikativ*.

(ii) Für $f \in \mathbb{Z}[i]$ gilt: $\delta(f) = 1 \Rightarrow f \in \mathbb{Z}[i]^*$. Bestimmen Sie damit $\mathbb{Z}[i]^*$.

(iii) Zerlegen Sie $2, 3, 4, 5 \in \mathbb{Z}[i]$ in ein Produkt irreduzibler Elemente.

(iv) Sei $z \in \mathbb{Z}[i]$. Ist $\delta(z) \in \mathbb{N}_0$ eine Primzahl, so ist z ein Primelement in $\mathbb{Z}[i]$.

Lösung:

(a) (i) Sei $r \in \mathbb{R}\backslash\{0\}$ ein Nullteiler $\Rightarrow$ es gibt $s \in R\backslash\{0\}$ mit $r \cdot s = 0$.
Angenommen, $r \in R^* \Rightarrow$ Es gibt $w \in R$ mit $rw = 1$
$\Rightarrow 0 = (sr)w = s(rw) = s$, Widerspruch zu $s \neq 0$.
$\Rightarrow r \notin R^*$.

(ii) In $\mathbb{Z}/6\mathbb{Z}$ gilt:

$$\overline{1} \cdot \overline{1} = \overline{1}, \quad \overline{5} \cdot \overline{5} = \overline{1}.$$

$\overline{2}, \overline{3}, \overline{4}$ sind jedoch keine Einheiten, denn sie sind Nullteiler: $\overline{2} \cdot \overline{3} = \overline{0}$, $\overline{4} \cdot \overline{3} = \overline{0}$.
$\Rightarrow (\mathbb{Z}/6\mathbb{Z})^* = \{\overline{1}, \overline{5}\}$.
Irreduzible Elemente: Es ist $\overline{4} = \overline{2} \cdot \overline{2}$, $\overline{3} = \overline{3} \cdot \overline{3}$, $\overline{2} = \overline{2} \cdot \overline{4}$. Damit ist kein Element in $\mathbb{Z}/6\mathbb{Z}$ irreduzibel.

(b) Nullelement: $(0,0) \in R$, Einselement: $(1,1) \in R$.

Einheiten: Ist $(a,b) \in R$ Einheit, so muss es $(c,d) \in R$ geben mit $(ac, bd) = (a,b)\cdot(c,d) = (1,1)$. $\iff ac = 1, bd = 1 \overset{a,b,c,d\in\mathbb{Z}}{\iff} a, b \in \{-1, 1\}$.
$\Rightarrow R^* = \{(1,1), (1,-1), (-1,1), (-1,-1)\}$.

Wir zeigen: $(1,0)$ ist Primelement. Beweis: Seien $x = (x_1, x_2), y = (y_1, y_2) \in \mathbb{R}$ mit $(1,0)|xy \Rightarrow$ Es gibt $q = (q_1, q_2) \in R$ mit $(x_1y_1, x_2y_2) = xy = q(1,0) = (q_1, 0) \Rightarrow x_2 = 0$ oder $y_2 = 0$.
OBdA. sei $x_2 = 0$. $\Rightarrow x = (x_1, 0) = x_1 \cdot (1,0) \Rightarrow (1,0)|x$.

$(1,0)$ ist nicht irreduzibel, denn $(1,0) = (1,0) \cdot (1,0)$, aber $(1,0) \notin R^*$.

Es entsteht kein Widerspruch zur Vorlesung, da R nicht nullteilerfrei ist (z.B. $(1,0)\cdot(0,1)=(0,0)$).

(c) (i) Es ist $K^* = K\backslash\{0\}$ („$\subset$“ klar, „$\supset$“: Ist $r \in K\backslash\{0\}$, so ist $r^{-1}\cdot r = 1 \Rightarrow r \in K^*$).

- „$\subset$“: Sei $p \in K[t]^*$ (insbes. $p \neq 0$) $\Rightarrow$ es gibt $q \in K[t]\backslash\{0\}$ mit $pq = 1 \Rightarrow 0 = \mathrm{grad}(pq) = \mathrm{grad}(p) + \mathrm{grad}(q)$ $\overset{\mathrm{grad}(p),\mathrm{grad}(q)\in\mathbb{N}_0}{\Rightarrow}$ $\mathrm{grad}(p) = \mathrm{grad}(q) = 0 \Rightarrow p \in K\backslash\{0\}$.
- „$\supset$“: Sei $p \in K\backslash\{0\} \Rightarrow p^{-1} \in K\backslash\{0\} \subset K[t]$ existiert $\Rightarrow p^{-1}\cdot p = 1 \Rightarrow p \in K[t]^*$.

(ii) $\mathbb{R}[t]$ ist nach Vorlesung Hauptidealring $\Rightarrow$ irreduzible Elemente sind genau die Primelemente.
Es ist $t^2 - t = t(t-1)$ und $t, t-1 \notin \mathbb{R}[t]^* \Rightarrow t^2 - t$ nicht irreduzibel, nicht prim.
$f := t^2+1$ ist irreduzibel (und damit prim), denn: Gäbe es $p, q \in \mathbb{R}[t]\backslash(\mathbb{R}[t]^* \cup \{0\})$ mit $t^2+1 = pq \Rightarrow 2 = \mathrm{grad}(t^2+1) = \mathrm{pq} = \mathrm{grad}(p) + \mathrm{grad}(q)$ $\overset{\mathrm{grad}(p),\mathrm{grad}(q)\in\mathbb{N}}{\Rightarrow}$ $\mathrm{grad}(p) = \mathrm{grad}(q) = 1 \Rightarrow p = at + b$ mit $a, b \in \mathbb{R}$, $a \neq 0 \Rightarrow f(-b/a) = p(-b/a)q(-b/a) = 0$, Widerspruch (denn f hat keine Nullstellen in $\mathbb{R}$).

(iii) R ist kein Hauptidealring, sonst wäre jedes irreduzible Element auch prim.

t^2 ist irreduzibel, denn: Seien $p, q \in R\backslash(R^* \cup \{0\})$ mit $t^2 = pq$. $\Rightarrow 2 = \mathrm{grad}(t^2) = \mathrm{grad}(pq) = \mathrm{grad}(p) + \mathrm{grad}(q)$ $\overset{\mathrm{grad}(p),\mathrm{grad}(q)\in\mathbb{N}}{\Rightarrow}$ $\mathrm{grad}(p) = \mathrm{grad}(q) = 1$. Aber es gibt keine Elemente mit Grad 1 in R, Widerspruch.

t^2 ist nicht prim, denn: Wähle $p = q = t(t-1)$. Dann gilt $t^2 | pq = t^2(t-1)^2$, aber $t^2 \nmid p$ (und analog $t^2 \nmid q$), denn: Gäbe es $f \in R$ mit $t^2 f = p = t(t-1) \Rightarrow tf = t-1$. Aber (Einsetzen von 0): $(tf)(0) = 0 \neq -1 = (t-1)(0)$, Widerspruch.

(iv) Seien $p, q \in K[t]\backslash\{0\}$ mit $f = pq \Rightarrow 1 = \mathrm{grad}(f) = \mathrm{grad}(p) + \mathrm{grad}(q)$ $\overset{\mathrm{grad}(p),\mathrm{grad}(q)\in\mathbb{N}_0}{\Rightarrow}$ $\mathrm{grad}(p) = 0$ oder $\mathrm{grad}(q) = 0 \Rightarrow p \in K\backslash\{0\} = K[t]^*$ oder $q \in K[t]^*$.
$\Rightarrow f$ ist irreduzibel.

(v) (iv) $\Rightarrow \{at + b : a \in \mathbb{C}\backslash\{0\}, b \in \mathbb{C}\}$ sind irreduzibel (es genügt jedoch die Angabe von $\{t + b : b \in \mathbb{C}\}$, da $at + b = a(t + b/a) \hat{=} t + b/a$).
Wir zeigen, dass es keine weiteren irreduziblen Elemente in $\mathbb{C}[t]$ gibt: Wegen $\mathbb{C}[t]^* = \mathbb{C}\backslash\{0\}$ können konstante Polynome nicht irreduzibel sein (Einheiten sind per Definition nicht irreduzibel).
Sei $f \in \mathbb{C}[t]$, $\mathrm{grad}(f) \geq 2$.
Fundamentalsatz der Algebra $\Rightarrow f$ hat Nullstelle in $\mathbb{C}$ $\overset{A45(a)}{\Rightarrow}$ f nicht irreduzibel.

(d) (i) Seien $f = a + bi, g = c + di \in \mathbb{C}$.
$\Rightarrow fg = (a+bi)(c+di) = (ac - bd) + (ad + bc)i$.
$\Rightarrow$

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

(ii)
- „$\Rightarrow$“: Sei $z \in \mathbb{Z}[i]^*$
  $\Rightarrow$ Es gibt $w \in \mathbb{Z}[i]^*$ mit $w \cdot z = 1$

$\Rightarrow 1 = 1^2 + 0^2 = \delta(1) = \delta(wz) \overset{(a)}{=} \delta(w)\delta(z)$
$\overset{\delta(w),\delta(z)\in\mathbb{N}_0}{\Rightarrow} \delta(w) = \delta(z) = 1.$

- „$\Leftarrow$“: Sei $z = a + bi \in \mathbb{Z}$ mit $\delta(z) = 1$.
  $\Rightarrow 1 = \delta(z) = a^2 + b^2$
  $\overset{a,b\in\mathbb{Z}}{\Rightarrow} a, b \in \{(0,1), (0,-1), (1,0), (-1,0)\}$.
  $\Rightarrow z \in \{1, -1, i, -i\}$.
  Tatsächlich sind dies alles Einheiten, denn: $1\cdot 1 = 1$, $(-1)\cdot(-1) = 1$, $i\cdot(-i) = 1$
  $\Rightarrow z \in \mathbb{Z}[i]^*$.

(iii) Mögliche Werte von $\delta(z)$ für $z \in \mathbb{Z}[i]\backslash\{0\}$:

$$\delta(z) \in \{1, 2, 4, 5, 8, 9, ...\} \quad (*)$$

(für z.B. $z \in \{1, 1+i, 2, 2+i, 2+2i, 3\}$).

- *Ansatz: Sei* $2 = f \cdot g$ *mit* $f, g \in \mathbb{Z}[i] \overset{(a)}{\Rightarrow} 4 = \delta(z) = \delta(f)\delta(g)$
  Das ist möglich, wenn $\delta(f) = 2 = \delta(g)$.
  Es gilt $(1+i)\cdot(1-i) = 1 - i^2 = 2$.
  $(1+i), (1-i)$ sind irreduzibel und damit obige Zerlegung die Zerlegung in irreduzible Faktoren, da $\delta(1+i) = \delta(1-i) = 2 = \delta(f)\delta(g)$ mit $f, g \in \mathbb{Z}[i]$ nur möglich ist, wenn $\delta(f) = 1$ oder $\delta(g) = 1$ (und damit f oder g Einheit ist).
- Sei $3 = f \cdot g$ mit $f, g \in \mathbb{Z}[i] \overset{(a)}{\Rightarrow} 9 = \delta(z) = \delta(f)\delta(g)$
  Wegen (*) ist dies nur möglich, wenn $\delta(f) = 1$ oder $\delta(g) = 1$ (d.h. wenn f oder g Einheit ist).
  $\Rightarrow 3$ ist bereits irreduzibel.
- Es gilt $4 = 2\cdot 2 \overset{s.o.}{=} (1+i)^2(1-i)^2$, wie oben argumentiert man, dass $1+i, 1-i$ irreduzibel sind.
- *Ansatz: Sei* $5 = f \cdot g$ *mit* $f, g \in \mathbb{Z}[i] \overset{(a)}{\Rightarrow} 25 = \delta(z) = \delta(f)\delta(g)$
  Das ist möglich, wenn $\delta(f) = 5 = \delta(g)$.

  Es gilt $(2+i)\cdot(2-i) = 5$.

  $(2+i), (2-i)$ sind irreduzibel und damit obige Zerlegung die Zerlegung in irreduzible Faktoren, da $\delta(2+i) = \delta(2-i) = 5 = \delta(f)\delta(g)$ mit $f, g \in \mathbb{Z}[i]$ nur möglich ist, wenn $\delta(f) = 1$ oder $\delta(g) = 1$ (und damit f oder g Einheit ist).

(iv) $\mathbb{Z}[i]$ euklidisch $\implies$ $\mathbb{Z}[i]$ ist HIR. $\implies$ Die Primelemente in $\mathbb{Z}[i]$ sind genau die irreduziblen Elemente in $\mathbb{Z}[i]$.
Wir zeigen daher: Ist $z = z_1 z_2$ für $z_1, z_2 \in \mathbb{Z}$, so muss $z_1 \in Z[i]^*$ oder $z_2 \in \mathbb{Z}[i]^*$ sein.
Es gilt $\delta(z) = \delta(z_1)\delta(z_2) \overset{\delta(z) \text{ ist Primzahl}}{\implies} \delta(z_1) = 1$ oder $\delta(z_2) = 1 \overset{(c)}{\implies} z_1 \in \mathbb{Z}[i]^*$ oder $z_2 \in \mathbb{Z}[i]^*$.

Aufgabe P45 (Anwendungen des Homomorphiesatzes).

(a) Zeigen Sie, dass $\mathbb{Q}[t]/(t) \cong \mathbb{Q}$. Ist $\mathbb{Q}[t]/(t)$ ein Körper?

(b) Zeigen Sie, dass $f : \mathbb{R}[t] \to \mathbb{C}, p \mapsto p(i)$ ein Ringhomomorphismus ist. Folgern Sie, dass $\mathbb{R}[t]/(t^2+1) \cong \mathbb{C}$.

(c) Es sei $n \in \mathbb{N}$, $n \geq 2$ und $(F_n, +_n, \cdot_n)$ der in der Vorlesung definierte kommutative Ring mit 1. Zeigen Sie, dass $f : \mathbb{Z} \to F_n, z \mapsto r_n(z)$ ein Ringhomomorphismus ist. Folgern Sie, dass $\mathbb{Z}/n\mathbb{Z} \cong F_n$. Für welche $n \in \mathbb{N}$ ist $\mathbb{Z}/n\mathbb{Z}$ ein Körper?

Lösung:

(a) Wir geben einen geeigneten surjektiven Ringhomomorphismus an, so dass die Aussagen aus dem Homomorphiesatz für Ringe folgen.

- Sei $\varphi : \mathbb{Q}[t] \to \mathbb{Q}, p \mapsto p(0)$.
  φ ist ein surjektiver Ringhomomorphismus, denn:
  - $\varphi(1) = 1(0) = 1_{\mathbb{Q}}$
  - für $p, q \in \mathbb{Q}[t]$ gilt:

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

  - φ ist surjektiv, denn: Für $r \in \mathbb{Q}$ wähle $p = t + r \Rightarrow \varphi(p) = 0 + r = r$.

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

(b) Wir rechnen nach, dass f ein surjektiver Ringhomomorphismus ist:

- $f(1) = 1(i) = 1_{\mathbb{C}}$,
- Für $p, q \in \mathbb{R}[t]$ gilt $f(pq) = (pq)(i) = p(i)q(i) = f(p)f(q)$,
- Für $p, q \in \mathbb{R}[t]$ gilt $f(p+q) = (p+q)(i) = p(i) + q(i) = f(p) + f(q)$.
- Sei $z = a + bi \in \mathbb{C}$ beliebig. Wähle $p = bt + a \Rightarrow f(p) = bi + a = z$. $\Rightarrow f$ surjektiv.

Homomorphiesatz $\Rightarrow \mathbb{R}[t]/\text{Kern}(f) \cong \mathbb{C}$.
Hier ist $\text{Kern}(f) = \{p \in \mathbb{R}[t] : p(i) = f(p) = 0\} \overset{!}{=} (t^2+1)$, denn:

- „$\subset$“: Sei $p \in \text{Kern}(f) \Rightarrow p(i) = 0 \overset{\text{P0.4, } p \in \mathbb{R}[t]}{\Rightarrow}$ Es gibt $q \in \mathbb{R}[t]$ mit $p = (t-i)(t+i)q = (t^2+1)q \Rightarrow p \in (t^2+1)$.
- „$\supset$“: $p \in (t^2+1) \Rightarrow$ es gibt $q \in \mathbb{R}[t]$ mit $p = (t^2+1)q \Rightarrow p(i) = \underbrace{(i^2+1)}_{=0} q(i) = 0$.

(c) Wir rechnen nach, dass f ein surjektiver Ringhomomorphismus ist:

- $f(1) = r_n(1) = 1_{F_n}$,
- Für $a, b \in \mathbb{Z}$ gilt $f(ab) = r_n(ab) \overset{\text{Regel } r_n}{=} r_n(r_n(a)r_n(b)) = f(a) \cdot_n f(b)$,
- Für $a, b \in \mathbb{Z}$ gilt $f(a+b) = r_n(a+b) \overset{\text{Regel } r_n}{=} r_n(r_n(a) + r_n(b)) = r_n(a) +_m r_n(b) = f(a) +_m f(b)$.
- Für $z \in \{0, ..., n-1\} = F_n$ gilt $f(z) = r_n(z) = z$, d.h. f ist surjektiv.

Homomorphiesatz $\Rightarrow \mathbb{Z}/\text{Kern}(f) \cong F_n$.
Hier ist $\text{Kern}(f) = \{x \in \mathbb{Z} : r_n(x) = f(x) = 0\} = \{x \in \mathbb{Z} : x = qn, q \in \mathbb{Z}\} = n\mathbb{Z}$.

Dieses Blatt ist **nicht abzugeben** und wird in den Übungsgruppen besprochen.

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