Aufgabe 12

(a) Behauptung: Für $m, n \in \mathbb{Z}$ sind äquivalent:

(i) $\overline{m}$ ist eine Einheit in $\mathbb{Z}/n\mathbb{Z}$

(ii) ggT(m, n)= 1

Beweis.
- (i) $\implies$ (ii): Sei $\overline{m} \in \mathbb{Z}/n\mathbb{Z}$. Da $\overline{m}$ eine Einheit ist, existiert ein $k \in \mathbb{Z}$, sodass $\overline{m} \cdot \overline{k} = \overline{1}$. Somit ist $mk - 1 \in \mathbb{Z}$. Weiter existiert ein $l \in \mathbb{Z}$, sodass $mk - 1 = ln \Leftrightarrow 1 = mk - ln$. Sei $d \in \mathbb{Z}$ derart, dass $d|m$ und $d|n$. Dann gilt aber auch $d|(mk - ln) = 1$: Weil $d \in \mathbb{Z}$, folgt $d \in \{-1, 1\}$, also ggT(m, n)= 1.
- (ii) $\implies$ (i): Gelte ggT(m, n)= 1. Es existieren mit dem erweiterten euklidischen Algorithmus $u, v \in \mathbb{Z}$ mit $um + vn = 1$. Daraus folgt $\overline{um} + \overline{vn} = \overline{um} = \overline{1} \implies \overline{u} \cdot \overline{m} = 1$. Somit ist $\overline{m}$ eine Einheit in $\mathbb{Z}/n\mathbb{Z}$.

□

(b) Es gilt mit dem euklidischen Algorithmus:

$$\begin{aligned} 51 &= 1 \cdot 42 + 9 \\ 42 &= 4 \cdot 9 + 6 \\ 9 &= 1 \cdot 6 * 3 \\ 6 &= 2 \cdot 3 \end{aligned}$$

Somit ist der ggT$(51, 42)$= 3, d.h. $\overline{42} \notin (\mathbb{Z}/51\mathbb{Z})^\times$.

$$\begin{aligned} 55 &= 1 \cdot 42 + 13 \\ 42 &= 3 \cdot 13 + 3 \\ 13 &= 4 \cdot 3 + 1 \\ 3 &= 3 \cdot 1 \end{aligned}$$

Somit ist der ggT$(55, 42)$= 1, d.h. $\overline{42} \in (\mathbb{Z}/55\mathbb{Z})^\times$. Außerdem gilt:

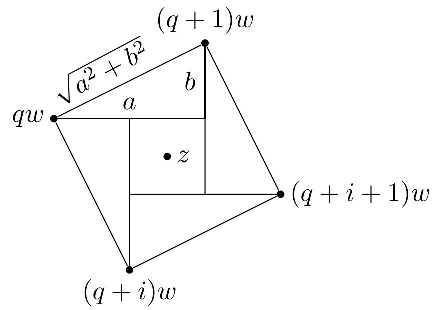
$$\begin{aligned} 1 &= 13 - 4 \cdot 3 \\ &= 13 - 4(42 - 3 \cdot 13) \\ &= 13 \cdot 13 - 4 \cdot 42 \\ &= 13(55 - 42) - 4 \cdot 42 \\ &= 13 \cdot 55 + (-17) \cdot 42 \end{aligned}$$

$55 - 17 = 38$, also gilt $\overline{42} \cdot \overline{38} = \overline{1}$ in $\mathbb{Z}/55\mathbb{Z}$.

Aufgabe 13

(a) Sei $z = c + di$. Dann gilt $|z - (a + bi)| \leq \frac{1}{\sqrt{2}} \iff (c - a)^2 + (d - b)^2 \leq \frac{1}{2}$. Zu jeder reellen Zahl x gibt es eine ganze Zahl $n(x)$, sodass $|n(x) - x| \leq \frac{1}{2}$. Wähle also $a = n(c)$ und $b = n(d)$. Dann ist $(c - a)^2 + (d - b)^2 \leq \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 = \frac{1}{2}$.

(b) Zu jeder Zahl z gibt es ein q, sodass z in einem von qw, $(q + 1)w$, $(q + i)w$ und $(q + 1 + i)w$, wie in der Skizze abgebildet, begrenzten Quadrat liegt. Der maximale Abstand von z zu einem Vielfachen von w ist genau dann erreicht, wenn z in der Mitte dieses Quadrats liegt. Dann ist der Abstand von z zu jedem der 4 Endpunkte durch die Hälfte der Länge der Diagonalen gegeben, also nach dem Satz des Pythagoras $|z - qw| = \frac{1}{2}\sqrt{(a^2 + b^2) + (a^2 + b^2)} = \sqrt{\frac{1}{2}}\sqrt{a^2 + b^2}$. Im Allgemeinen ist $|z - qw|$ aber kleiner als dieser Abstand (für geeignetes q natürlich), also $\delta(z - qw) = |z - qw|^2 \leq \frac{1}{2}(a^2 + b^2) = \frac{1}{2}\delta(w)$. Natürlich könnte man das jetzt noch formalisieren, aber das macht nicht so viel Spaß und die Idee ist klar.



(c) Laut Aufgabentext ist $\mathbb{Z}[i]$ nullteilerfrei. Es genügt also zu zeigen, dass $\forall z, w \in \mathbb{Z}[i]$ mit $w \neq 0 \exists q, r \in \mathbb{Z}[i]$ mit $z = qw + r$, $\delta(r) < \delta(w)$. Wähle $r = z - qw$. Nach Aufgabenteil (b) gilt dann $\deg(r) \leq \frac{1}{2}\deg(w) < \deg(w)$. Daraus folgt sofort die Aussage.

(d)

$$\begin{aligned} 9 &= (1-i)(3+4i) + 2 - i & \delta(2-i) = 5 < 25 = \delta(3+4i) \\ 3+4i &= (2i)(2-i) + 1 & \delta(1) = 1 < 5 = \delta(2-i) \\ 2-i &= (2-i)(1) + 0 \\ \implies & 1 \in \mathrm{ggT}(9, 3+4i) \end{aligned}$$

Aufgabe 14

Behauptung: Für einen Ring $\neq 0$ sind folgende Aussagen äquivalent:

(i) R ist ein Körper

(ii) $R[t]$ ist ein euklidischer Ring

(iii) $R[t]$ ist ein Hauptidealring

Beweis. (i) $\implies$ (ii): Jeder Polynomring über Körpern ist nach VL euklidisch

(ii) $\implies$ (iii): Jeder Euklidische Ring ist nach VL ein Hauptidealring

(iii) $\implies$ (i): Sei R ein Körper. Ist R nicht nullteilerfrei, folgt direkt die Behauptung. Sei nun also R nullteilerfrei, weshalb $\exists x \in R \setminus \{0\}$ sodass $xy \neq 1 \forall y \in R$.

Behauptung: (x, t) ist kein Hauptideal.

Beweis. Angenommen $\exists f \in R[t]$, sodass $(f) = (x, t)$, dann $\exists h \in R[t]$, sodass $x = fh$. R ist nullteilerfrei, also gilt

$$0 = \deg(x) = \deg(f) + \deg(h) \implies \deg(f) = \deg(h) = 0.$$

Es existiert also ein $a \in R$ sodass $f = a$ und ein $g \in R[t]$ sodass $t = fg = ag$. Somit gilt $\deg(g) = 1$ und wegen $e(t) = 1$

$$1 = e(t) = e(a) \cdot e(g) = a \cdot e(h) \in R.$$

Folglich ist a eine Einheit auf R. Wegen $aa^{-1} = 1$ gilt zudem $1 \in (a) = (x, t)$ und es existieren $u, v \in R[t]$ sodass

$$1 = xu + tv \overset{t=0}{\implies} 1 = x \cdot u(0) \in R.$$

Damit ist aber $x \in R^\times$, was ein Widerspruch ist. $\square$

$\square$

Aufgabe 15

(a)

$$
\begin{pmatrix} 0 & 20 & 0 \\ 10 & 12 & 6 \\ 20 & 12 & 10 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 0 & 20 & 0 \\ 10 & 2 & 6 \\ 20 & -8 & 10 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 20 & 0 & 0 \\ 2 & 10 & 6 \\ -8 & 20 & 10 \end{pmatrix}
$$

$$
\rightsquigarrow \begin{pmatrix} 2 & 10 & 6 \\ 20 & 0 & 0 \\ -8 & 20 & 10 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 2 & 0 & 0 \\ 20 & -100 & -60 \\ -8 & 60 & 34 \end{pmatrix}
$$

$$
\rightsquigarrow \begin{pmatrix} 2 & 0 & 0 \\ 0 & -100 & -60 \\ 0 & 60 & 34 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 2 & 0 & 0 \\ 0 & 20 & 8 \\ 0 & 60 & 34 \end{pmatrix}
$$

$$
\rightsquigarrow \begin{pmatrix} 2 & 0 & 0 \\ 0 & 20 & 8 \\ 0 & -20 & 2 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & -20 \\ 0 & 8 & 20 \end{pmatrix}
$$

$$
\rightsquigarrow \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & -20 \\ 0 & 0 & 100 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 100 \end{pmatrix}
$$

Die Elementarteiler sind also $2, 2$ und 100. Die Fittingideale dieser Matrix sind nach Fittings Lemma gleich den Fittingidealen von A. Es gilt daher $\mathrm{Fit}_1(A) = (2, 2, 100) = (2)$, $\mathrm{Fit}_2(A) = (4, 200, 200) = (4)$ und $\mathrm{Fit}_3(A) = (400)$.

(b)

$$
\begin{pmatrix} 1-t & -1 & 2 \\ -1 & -1 & 3 \\ 0 & -1 & 3-t \end{pmatrix} \rightsquigarrow \begin{pmatrix} -1 & -1 & 3 \\ 1-t & -1 & 2 \\ 0 & -1 & 3-t \end{pmatrix} \rightsquigarrow \begin{pmatrix} -1 & 0 & 0 \\ 1-t & -2+t & 5-3t \\ 0 & -1 & 3-t \end{pmatrix}
$$

$$
\rightsquigarrow \begin{pmatrix} -1 & 0 & 0 \\ 0 & -2+t & 5-3t \\ 0 & -1 & 3-t \end{pmatrix} \rightsquigarrow \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 3-t \\ 0 & -2+t & 5-3t \end{pmatrix}
$$

$$
\rightsquigarrow \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 3-t \\ 0 & 0 & -1+2t-t^2 \end{pmatrix} \rightsquigarrow \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -(t-1)^2 \end{pmatrix}
$$

Daraus folgt $F_1(B) = (1, 1, (t-1)^2) = \mathbb{R}[t], F_2(B) = (1, (t-1)^2, (t-1)^2) = \mathbb{R}[t], F_3(B) = ((t-1)^2)$.