Abgabe Algebra 1, Blatt 04

Studierende(r): Weerts, Steffen, steffen.weerts@uni-oldenburg.de

Aufgabe 4.1

(a) Sei R euklidischer Ring.
Zu zeigen: R Hauptidealring.
Sei $I \trianglelefteq R$ beliebig. Sei $b \in I \setminus 0$, sodass $\mathrm{d}(b)$ das kleinste Element der Menge $M = \{\mathrm{d}(x) \mid x \in I \setminus \{0\}\} \subseteq \mathbb{N}_0$ ist.
Beh.: $I = \langle b \rangle$.

"$\supseteq$": Es gilt:

$$b \in I \implies \langle b \rangle \subseteq I.$$

"$\subseteq$": Sei $a \in I$ beliebig.
Da $b \neq 0$ und R euklidischer Ring, gilt:

$$\begin{aligned} &\exists q, r \in R : a = qb + r \text{ und } (r = 0 \text{ oder } \mathrm{d}(r) < \mathrm{d}(b)) \\ \implies &r = a - qb \in I, \text{ da } I \text{ Ideal, } a \in I, b \in I \text{ und } q \in R. \end{aligned}$$

Da $\mathrm{d}(b)$ das kleinste Element in M ist, gilt:

$$r = 0 \implies a = qb \implies I = \langle b \rangle.$$

Daraus folgt, dass jedes Ideal in R Hauptideal ist, also ist R Hauptidealring.

$\square$

(b) Sei R ein euklidischer Ring und seien $a, b \in R$ mit $b \neq 0$. Sei $d \in R$ ein größter gemeinsamer Teiler von a und b.
Zu zeigen: $\langle a, b \rangle = \langle d \rangle$.

Sei r_{n+1} aus dem euklidischen Algorithmus der Rest, der gleich 0 ist.
Aufgrund der induktiven Vorgehensweise des euklidischen Algorithmus lässt sich jedes $r_i, i \in \{1, \cdots, n\}$ als Linearkombination von a und b schreiben, denn es gilt:

$$\begin{aligned} r_{-1} = q_0 r_0 + r_1 &\iff r_1 = r_{-1} - q_0 r_0 \\ r_0 = q_1 r_1 + r_2 &\iff r_2 = r_0 - q_1 r_1 \\ r_1 = q_2 r_2 + r_3 &\iff r_3 = r_1 - q_2 r_2 \\ &\cdots \\ r_{n-2} = q_{n-1} r_{n-1} + r_n &\iff r_n = r_{n-2} - q_{n-1} r_{n-1} \end{aligned}$$

Durch Einsetzen der Gleichungen $r_i = r_{i-2} - q_{i-1}r_{i-1} \forall i \in \{1, \cdots, n-1\}$ erhält man eine Lösung für r_n, die eine Linearkombination von $r_{-1} = a$ und $r_0 = b$ ist.
Da $r_n =: d$ der größte gemeinsame Teiler von a und b ist, sind alle Linearkombinationen von a und b Vielfache von d. Daraus folgt $\langle a, b\rangle = \langle d\rangle$.

$\square$

Aufgabe 4.2

(a) Fehlt.

(b) Sei $R = \mathbb{Z}$, $a, b \in \mathbb{Z}, b \neq 0$.
Zu zeigen: $\operatorname{ggT}(a,b) \cdot \operatorname{kgV}(a,b) = |ab|$.
Es gilt:

$$\begin{aligned}
&\operatorname{kgV}(a,b) \mid ab \\
\Longrightarrow\ &\exists c \in \mathbb{Z} : \operatorname{kgV}(a,b) \cdot c = ab \\
\Longrightarrow\ &c = \frac{ab}{\operatorname{kgV}(a,b)}
\end{aligned} \tag{1}$$

Außerdem gilt:

$$\begin{aligned}
&c \cdot \frac{\operatorname{kgV}(a,b)}{b} = a \text{ und } c \cdot \frac{\operatorname{kgV}(a,b)}{a} = b \\
\Longrightarrow\ &c \mid a \text{ und } c \mid b \\
\Longrightarrow\ &c \text{ ist gemeinsamer Teiler von } a \text{ und } b.
\end{aligned}$$

Sei d eine weiterer gemeinsamer Teiler von a und b.
Zu zeigen: $d \mid c$.
Es gilt:

$$\begin{aligned}
&\frac{ab}{d} = a \cdot \frac{b}{d} = \frac{a}{d} \cdot b \\
\Longrightarrow\ &a \mid \frac{ab}{d} \text{ und } b \mid \frac{ab}{d} \\
\Longrightarrow\ &\operatorname{kgV}(a,b) \mid \frac{ab}{d} \\
\Longrightarrow\ &\exists z \in \mathbb{Z} : \operatorname{kgV}(a,b) \cdot z = \frac{ab}{d} \\
&\quad \Longleftrightarrow\ d \cdot \operatorname{kgV}(a,b) \cdot z = ab \\
&\quad \overset{(1)}{\Longleftrightarrow}\ d \cdot \operatorname{kgV}(a,b) \cdot z = c \cdot \operatorname{kgV}(a,b) \\
&\quad \Longleftrightarrow\ d \cdot z = c \\
&\quad \Longleftrightarrow\ d \mid c \\
\Longrightarrow\ &c = \operatorname{ggT}(a,b).
\end{aligned}$$

Insgesamt ergibt sich also:

$$\operatorname{ggT}(a,b)\cdot\operatorname{kgV}(a,b)=ab.$$

$\square$

Aufgabe 4.3

(a) (i) Sei $\mathbb{Z}[i\sqrt{n}]=[a+ib\sqrt{n}\mid a,b\in\mathbb{Z}]$ Unterring von $\mathbb{C}$.
Sei

$$N:\mathbb{Z}[i\sqrt{n}]\to\mathbb{N}_0,\quad \alpha:=a+ib\sqrt{n}\mapsto \mathrm{N}(\alpha)=\alpha\bar{\alpha}=a^2+nb^2.$$

Zu zeigen: $\forall\alpha,\beta\in\mathbb{Z}[i\sqrt{n}]:\mathrm{N}(\alpha\cdot\beta)=\mathrm{N}(\alpha)\,\mathrm{N}(\beta)$.
Seien $\alpha,\beta\in\mathbb{Z}[i\sqrt{n}]$ beliebig. Es gilt:

$$\begin{aligned}
\mathrm{N}(\alpha\beta)=&(a_\alpha+ib_\alpha\sqrt{n})(a_\beta+ib_\beta\sqrt{n})\overline{(a_\alpha+ia_\beta\sqrt{n})(a_\beta+ib_\beta\sqrt{n})}\\
=&(a_\alpha+ib_\alpha\sqrt{n})(a_\beta+ib_\beta\sqrt{n})(a_\alpha-ia_\beta\sqrt{n})(a_\beta-ib_\beta\sqrt{n})\\
=&(a_\alpha+ib_\alpha\sqrt{n})(a_\beta+ib_\beta\sqrt{n})(a_\alpha a_\beta-ib_\alpha\sqrt{n}a_\beta-a_\alpha ib_\beta\sqrt{n}-b_\alpha\sqrt{n}b_\beta\sqrt{n})\\
=&(a_\alpha+ib_\alpha\sqrt{n})(a_\beta a_\alpha a_\beta-a_\beta ib_\alpha\sqrt{n}a_\beta-a_\beta a_\alpha ib_\beta\sqrt{n}-a_\beta b_\alpha\sqrt{n}b_\beta\sqrt{n}\\
&+ib_\beta\sqrt{n}a_\alpha a_\beta-ib_\beta\sqrt{n}ib_\alpha\sqrt{n}a_\beta-ib_\beta\sqrt{n}a_\alpha ib_\beta\sqrt{n}-ib_\beta\sqrt{n}b_\alpha\sqrt{n}b_\beta\sqrt{n})\\
=&a_\alpha a_\beta a_\alpha a_\beta-a_\alpha a_\beta ib_\alpha\sqrt{n}a_\beta-a_\alpha a_\beta a_\alpha ib_\beta\sqrt{n}-a_\alpha a_\beta b_\alpha\sqrt{n}b_\beta\sqrt{n}\\
&+a_\alpha ib_\beta\sqrt{n}a_\alpha a_\beta-a_\alpha ib_\beta\sqrt{n}ib_\alpha\sqrt{n}a_\beta-a_\alpha ib_\beta\sqrt{n}a_\alpha ib_\beta\sqrt{n}-a_\alpha ib_\beta\sqrt{n}b_\alpha\sqrt{n}b_\beta\sqrt{n}\\
&+ib_\alpha\sqrt{n}a_\beta a_\alpha a_\beta-ib_\alpha\sqrt{n}a_\beta ib_\alpha\sqrt{n}a_\beta-ib_\alpha\sqrt{n}a_\beta a_\alpha ib_\beta\sqrt{n}-ib_\alpha\sqrt{n}a_\beta b_\alpha\sqrt{n}b_\beta\sqrt{n}\\
&+ib_\alpha\sqrt{n}ib_\beta\sqrt{n}a_\alpha a_\beta-ib_\alpha\sqrt{n}ib_\beta\sqrt{n}ib_\alpha\sqrt{n}a_\beta-ib_\alpha\sqrt{n}ib_\beta\sqrt{n}a_\alpha ib_\beta\sqrt{n}\\
&-ib_\alpha\sqrt{n}ib_\beta\sqrt{n}b_\alpha\sqrt{n}b_\beta\sqrt{n}\\
=&a_\alpha^2a_\beta^2+a_\alpha^2b_\beta^2n+a_\beta^2b_\alpha^2n+b_\alpha^2b_\beta^2n^2\\
=&(a_\alpha^2+nb_\alpha^2)(a_\beta^2+nb_\beta^2)\\
=&\mathrm{N}(\alpha)\,\mathrm{N}(\beta).
\end{aligned}$$

$\square$

(ii) Sei $\mathbb{Z}[i\sqrt{n}]=[a+ib\sqrt{n}\mid a,b\in\mathbb{Z}]$ Unterring von $\mathbb{C}$.
Sei

$$N:\mathbb{Z}[i\sqrt{n}]\to\mathbb{N}_0,\quad \alpha:=a+ib\sqrt{n}\mapsto \mathrm{N}(\alpha)=\alpha\bar{\alpha}=a^2+nb^2.$$

Zu zeigen: $\mathrm{N}(\alpha)=1\iff\alpha\in\mathbb{Z}[i\sqrt{n}]^*$.

"$\Rightarrow$" Sei $\mathrm{N}(a) = a^2 + nb^2 = 1$.
Es gilt:

$$\begin{aligned}
&a^2 + nb^2 = 1 \\
\implies &(a = 0, n = 1, b = \pm 1) \text{ oder } (b = 0, a = 1) \\
\implies &\alpha = 1 \text{ oder } (\alpha = \pm i, n = 1) \\
\implies &\mathbb{Z}[i\sqrt{n}] \ni \alpha = 1 = \frac{1}{1} \text{ oder } \left(\mathbb{Z}[i\sqrt{1}] \ni \alpha = \pm i \implies \frac{i}{i} = 1 \in \mathbb{Z}[i\sqrt{1}]\right) \\
\implies &\alpha \in \mathbb{Z}[i\sqrt{n}]^*.
\end{aligned}$$

"$\Leftarrow$" Sei $\alpha \in \mathbb{Z}[i\sqrt{n}]^*$.
Es gilt:

$$\begin{aligned}
&\alpha \in \mathbb{Z}[i\sqrt{n}]^* \\
\implies &\exists \beta \in \mathbb{Z}[i\sqrt{n}]^* : \alpha\beta = 1 \\
\implies &\alpha\beta = (a_\alpha + ib_\alpha\sqrt{n})(a_\beta + ib_\beta\sqrt{n}) \\
&\quad = a_\alpha a_\beta + a_\alpha * ib_\beta\sqrt{n} + a_\beta * ib_\alpha\sqrt{n} + i^2 b_\alpha b_\beta * n \\
&\quad = a_\alpha a_\beta + a_\alpha * ib_\beta\sqrt{n} + a_\beta * ib_\alpha\sqrt{n} - b_\alpha b_\beta * n \\
&\quad = 1 \\
\implies &a_\alpha * ib_\beta\sqrt{n} + a_\beta * ib_\alpha\sqrt{n} = 0 \text{ und } a_\alpha a_\beta - b_\alpha b_\beta * n = 1
\end{aligned}$$

Sei $\beta \neq \bar{\alpha}$. Es gilt:

$$\begin{aligned}
\alpha\beta =&1 \\
\neq&a_\alpha a_\beta + a_\alpha * ib_\beta\sqrt{n} + a_\beta * ib_\alpha\sqrt{n} - b_\alpha b_\beta * n \\
=&a_\alpha^2 + a_\alpha * i(-b_\alpha)\sqrt{n} + a_\alpha * ib_\alpha\sqrt{n} - b_\alpha(-b_\alpha) * n \\
=&a_\alpha^2 + b_\alpha^2 * n \\
=&1. \text{ Widerspruch } \alpha\beta = 1 \neq 1. \\
\implies &\beta = \bar{\alpha} \\
\implies &\mathrm{N}(\alpha) = \alpha\bar{\alpha} = 1.
\end{aligned}$$

Wenn $n \geq 2$, dann ist $\mathbb{Z}[i\sqrt{n}]^* = \{\pm 1\}$, denn es gilt:

$$\begin{aligned}
&\mathrm{N}(\alpha) = 1 \iff \alpha \in \mathbb{Z}[i\sqrt{n}]^* \\
\implies &\mathrm{N}(\alpha) = a^2 + n * b^2 \geq a^2 + 2 * b^2
\end{aligned}$$

Nun gilt für $n = 2$:

$$\begin{aligned}
|b| = 0 &\implies \mathrm{N}(\alpha) = a^2. \\
|b| = 1 &\implies \mathrm{N}(\alpha) = a^2 + 2. \\
|b| \geq 2 &\implies \mathrm{N}(\alpha) \geq a^2 + 4.
\end{aligned}$$

Außerdem gilt für $n > 2$:

$$\begin{aligned} |b| = 0 &\implies \mathrm{N}(\alpha) = a^2. \\ |b| = 1 &\implies \mathrm{N}(\alpha) > a^2 + 2. \\ |b| \geq 2 &\implies \mathrm{N}(\alpha) > a^2 + 4. \end{aligned}$$

Daraus folgt, dass $\mathrm{N}(\alpha) = 1 \iff b = 0$ für $n \geq 2$ gilt.

$\square$

(b) Fehlt.

korrigiert von am