# Übungen zur Vorlesung "Lineare Algebra II"

**Musterlösung, Blatt 12 (Bonus)**

## Aufgabe 1

Wir unterscheiden in dieser Lösung zur besseren Nachvollziehbarkeit mit $0_R, 0_S$ und $1_R, 1_S$ die Null bzw. Eins in $R$ und $S$.

(a) Zu $\Rightarrow$: Wie im Beweis von Lemma 9.4(a) gesehen, gilt $\varphi(0_R) = 0_S$. Insbesondere gilt also $0_R \in \text{Kern}(\varphi)$. Da $\varphi$ injektiv ist, ist dies das einzige Element, das auf $0_S$ abgebildet wird, d.h. $\text{Kern}(\varphi) = \{0_R\}$.
Zu $\Leftarrow$: Es seien $r_1, r_2 \in R$ mit $\varphi(r_1) = \varphi(r_2)$. Nach Lemma 2.20(ii) gilt $-r = (-1_R) \cdot r$ für jedes $r \in R$. Da $\varphi$ ein Ringhomomorphismus ist, gilt $\varphi(1_R) = 1_S$ und wir erhalten daraus, dass $\varphi(-1_R) = -1_S$, denn

$$\varphi(-1_R) + 1_S = \varphi(-1_R) + \varphi(1_R) = \varphi(-1_R + 1_R) = \varphi(0_R) = 0_S.$$

Damit folgt

$$\begin{aligned} 0_S = \varphi(r_1) + (-\varphi(r_2)) &= \varphi(r_1) + ((-1_S) \cdot \varphi(r_2)) = \varphi(r_1) + (\varphi(-1_R) \cdot \varphi(r_2)) \\ &= \varphi(r_1) + \varphi((-1_R) \cdot r_2) = \varphi(r_1) + \varphi(-r_2) = \varphi(r_1 + (-r_2)). \end{aligned}$$

Da $\text{Kern}(\varphi) = \{0_R\}$, folgt $r_1 + (-r_2) = 0$. Damit ist $-r_2$ das additive Inverse zu $r_1$, d.h. $-r_2 = -r_1$ bzw. $(-1_R) \cdot r_2 = (-1_R) \cdot r_1$ und mit der Kürzungsregel 2.10 folgt $r_1 = r_2$. Damit ist $\varphi$ injektiv.

(b) Da $I \subset R$ ein Ideal ist, gilt $0_R \in I$. Wie im Beweis von Lemma 9.4(a) gilt $\varphi(0_R) = 0_S$ und somit $0_S \in \varphi(I)$. Sind weiter $s_1, s_2 \in \varphi(I)$, so gibt es $r_1, r_2 \in I$ mit $\varphi(r_i) = s_i$ für $i = 1, 2$. Da $I$ ein Ideal ist, gilt $r_1 + r_2 \in I$, d.h.

$$s_1 + s_2 = \varphi(r_1) + \varphi(r_2) = \varphi(r_1 + r_2) \in \varphi(I).$$

Sei zuletzt $s \in S$ beliebig und weiterhin $\varphi(r_1) = s_1 \in \varphi(I)$. Da $\varphi$ surjektiv ist, gibt es ein $r \in R$ mit $\varphi(r) = s$. Da $I$ ein Ideal, erhalten wir

$$s \cdot s_1 = \varphi(r) \cdot \varphi(r_1) = \varphi(r \cdot r_1) \in \varphi(I).$$

(c) Da $\varphi(1_R) = 1_S$ nach Definition des Ringhomomorphismus (für Ringe mit Eins), gilt $1_S \in \text{Bild}(\varphi)$ und per Definition als multiplikatives neutrales Element in $S$ ist $1_S$ auch multiplikativ neutral in $\text{Bild}(\varphi)$. Ebenso übertragen sich alle Rechenregeln für $+$ und $\cdot$ auf $\text{Bild}(\varphi)$, es genügt also zu zeigen, dass diese Menge abgeschlossen bezüglich der Operationen $+$ und $\cdot$ ist. Dazu seien $s_1, s_2 \in \text{Bild}(\varphi)$ und $r_1, r_2 \in R$ mit $\varphi(r_i) = s_i$ für $i = 1, 2$. Dann gilt

$$s_1 + s_2 = \varphi(r_1) + \varphi(r_2) = \varphi(r_1 + r_2) \in \text{Bild}(\varphi),$$

sowie

$$s_1 \cdot s_2 = \varphi(r_1) \cdot \varphi(r_2) = \varphi(r_1 \cdot r_2) \in \text{Bild}(\varphi).$$

**Aufgabe 2**

Es seien $a, b \in R$. Wir zeigen die Äquivalenz der folgenden drei Aussagen

(i) $a \overset{\wedge}{=} b$,

(ii) $a|b$ und $b|a$,

(iii) $(a) = (b)$.

$(i) \Rightarrow (ii)$: Per Definition existiert eine Einheit $u \in R^*$ mit $a = b \cdot u$. Daraus folgt unmittelbar, dass $b|a$. Weiter existiert $u^{-1} \in R$ mit $u \cdot u^{-1} = 1_R$, sodass $b = a \cdot u^{-1}$ und damit $a|b$.

$(ii) \Rightarrow (iii)$: Es gibt $c_1, c_2 \in R$ mit $a = b \cdot c_1$ und $b = a \cdot c_2$. Daraus folgt, dass $a \in (b)$, sowie $b \in (a)$. Ist $c \in (a)$, so gibt es $r \in R$ mit $c = r \cdot a$ und wir folgern, dass $c = (r \cdot c_1) \cdot b$, d.h. $c \in (b)$. Es folgt $(a) \subset (b)$ und analog lässt sich $(b) \subset (a)$ zeigen, wir erhalten also $(a) = (b)$.

$(iii) \Rightarrow (i)$: Offenbar gilt $a \in (b)$ und $b \in (a)$, sodass $r, s \in R$ existieren mit $a = r \cdot b$ und $b = s \cdot a$. Das impliziert $a = (r \cdot s) \cdot a$ und somit $r \cdot s = 1_R$ nach der Kürzungsregel 2.10. Insbesondere sind $r, s$ Einheiten und damit gilt $a \overset{\wedge}{=} b$.

**Aufgabe 3**

(a) Wir notieren $\mathrm{GGT}(a_1, \ldots, a_{n-1}) = \{d_j \mid j \in J\}$ für eine geeignete Indexmenge $J$. Außerdem sei für diese Aufgabe bemerkt, dass man Definition 9.15 auch für beliebige Mengen (statt endlichen) analog formulieren kann, was in der Aufgabenstellung bereits benutzt wurde: Wir sagen dann, dass $d$ ein größter gemeinsamer Teiler von $(a_i)_{i \in I}$ ist, falls

$$\text{(GGT1)} \quad d|a_i \text{ für alle } i \in I \qquad \text{und} \qquad \text{(GGT2)} \quad c|a_i \text{ für alle } i \in I \Longrightarrow c|d.$$

Nun zur eigentlichen Lösung der Aufgabe:

$\subset$: Sei $d \in \mathrm{GGT}(a_1, \ldots, a_n)$. Dann gilt nach (GGT1), dass $d|a_n$ und aus (GGT2) folgt für alle $j \in J$, dass $d|d_j$, denn $d|a_1, \ldots, d|a_{n-1}$ und $d_j$ ist ein ggT für $a_1, \ldots, a_{n-1}$. Damit gilt insgesamt, dass $d$ das Axiom (GGT1) für $\{a_n\} \cup \{d_j \mid j \in J\}$ erfüllt. Es sei nun $c$ so, dass $c|a_n$ und $c|d_j$ für alle $j \in J$. Da $d_j \in \mathrm{GGT}(a_1, \ldots, a_{n-1})$, folgt insbesondere $c|a_1, \ldots, c|a_{n-1}$. Nun folgt nach (GGT2) für $\{a_1, \ldots, a_n\}$, dass $c|d$, da $d \in \mathrm{GGT}(a_1, \ldots, a_n)$ Wir erhalten also $d \in \mathrm{GGT}(\mathrm{GGT}(a_1, \ldots, a_{n-1}), a_n)$.

$\supset$: Es sei $d \in \mathrm{GGT}(\mathrm{GGT}(a_1, \ldots, a_{n-1}), a_n) = \mathrm{GGT}(\{a_n\} \cup \{d_j \mid j \in J\})$. Da $d|d_j$ für alle $j \in J$ und $d_j|a_1, \ldots, d_j|a_{n-1}$, folgt $d|a_1, \ldots, d|a_{n-1}$. Nach Wahl von $d$ gilt außerdem $d|a_n$, sodass (GGT1) für $d$ und $\{a_1, \ldots, a_n\}$ unmittelbar folgt. Es gelte nun $c|a_1, \ldots, c|a_n$ für ein $c \in R$. Nach (GGT2) ergibt sich hieraus zusammen mit $d_j \in \mathrm{GGT}(a_1, \ldots, a_{n-1})$, dass $c|d_j$ für alle $j \in J$. Nach Voraussetzung galt außerdem $c|a_n$, sodass nach (GGT2) für $\{a_n\} \cup \{d_j \mid j \in J\}$ folgt, dass $c|d$. Insgesamt erhalten wir also auch (GGT2) für $d$ und die Menge $\{a_1, \ldots, a_n\}$, woraus $d \in \mathrm{GGT}(a_1, \ldots, a_n)$ folgt.

(b) Gilt $d_1, d_2 \in \mathrm{GGT}(a_1, \ldots, a_n)$, so gilt $d_i|a_1, \ldots, d_i|a_n$ für $i = 1, 2$. Nach (GGT2) folgt dann direkt, dass $d_1|d_2$ und $d_2|d_1$. Die restlichen Äquivalenzen ergeben sich dann direkt aus Aufgabe 2.

**Aufgabe 4**

Wir zeigen zunächst, dass $2 \in \mathbb{Z}[\sqrt{-5}]$ irreduzibel ist. Wir nehmen also an, dass

$$2 = (a + b\sqrt{-5})(c + d\sqrt{-5}).$$

Betrachten wir auf beiden Seiten den quadrierten komplexen Absolutbetrag erhalten wir

$$4 = (a^2 + 5b^2)(c^2 + 5d^2).$$

Da $a, b, c, d \in \mathbb{Z}$ ist dies nur möglich, falls $b = d = 0$. In diesem Fall erhalten wir $4 = a^2c^2$ bzw. $2 = |ac|$. Das ist nur möglich, falls entweder $|a| = 1$ oder $c = |1|$. Ist oBdA $|a| = 1$, so gilt $a + b\sqrt{-5} = \pm 1$, was eine Einheit in $\mathbb{Z}[\sqrt{-5}]$ ist. Somit ist 2 irreduzibel.

Wir zeigen nun, dass $2 \in \mathbb{Z}[\sqrt{-5}]$ kein Primelement ist. In $\mathbb{Z}[\sqrt{-5}]$ gilt

$$4 = \left(1 + \sqrt{-5}\right) \cdot \left(-1 + \sqrt{-5}\right).$$

Nun teilt 2 die linke Seite und damit das Produkt auf der rechten, jedoch ist 2 kein Teiler von $\pm 1 + \sqrt{-5}$: Angenommen, $2(a + bi) = 2a + 2bi = \pm 1 + \sqrt{-5}$, so wäre $2a = \pm 1$ und $2b = 1$, was für $a, b \in \mathbb{Z}$ nicht möglich ist.