Abgabe Algebra 1, Blatt 01

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

Aufgabe 1.1

(a) Seien $a, b, c, d \in \mathbb{Z}$. Sei $d = ggT(a, b)$. Es gilt:

$$\begin{aligned} & d = ggT(a,b) \\ \Longrightarrow\ & ggT\left(\frac{a}{ggT(a,b)}, \frac{b}{ggT(a,b)}\right) = 1 \\ \Longrightarrow\ & ggT\left(\frac{a}{d}, \frac{b}{d}\right) = 1. \end{aligned}$$

$\square$

(b) Seien $a, b, c, d \in \mathbb{Z}$. Sei $ggT(a, b) = 1, c \mid a$ und $d \mid b$.
Sei $a = \prod_{i=1}^{n} p_i$ die Primfaktorzerlegung von a. Sei $b = \prod_{i=1}^{m} q_i$ die Primfaktorzerlegung von b. Es gilt:

$$c \mid a \implies N := \{p \in \mathbb{P} : p \mid c\} \subseteq \{p_1, \cdots, p_n\}.$$

Außerdem gilt:

$$d \mid b \implies M := \{p \in \mathbb{P} : p \mid d\} \subseteq \{q_1, \cdots, q_m\}.$$

Da $ggT(a, b) = 1$, haben a und b keine gemeinsamen Teiler, insbesondere keine gemeinsamen Primteiler, d.h.

$$\begin{aligned} & \{p_1, \cdots, p_n\} \cap \{q_1, \cdots, q_m\} = \emptyset \\ \Longrightarrow\ & N \cap M = \emptyset \\ \Longrightarrow\ & ggT(c, d) = 1. \end{aligned}$$

$\square$

(c) Seien $a, b, c \in \mathbb{Z}$. Sei $ggT(a, b) = ggT(a, c) = 1$. Es gilt:

$$\begin{aligned} & ggT(a,b) = 1 \\ \Longrightarrow\ & \forall p \in \mathbb{P} : p \mid a \Rightarrow p \nmid b. \end{aligned}$$

Außerdem gilt:

$$\begin{aligned} & ggT(a,c) = 1 \\ \Longrightarrow\ & \forall p \in \mathbb{P} : p \mid a \Rightarrow p \nmid c. \end{aligned}$$

$$\begin{aligned}
&\Longrightarrow \forall p \in \mathbb{P} : p \mid a \Rightarrow p \nmid b \text{ und } p \nmid c\\
&\Longrightarrow \forall p \in \mathbb{P} : p \mid a \Rightarrow p \nmid bc\\
&\Longrightarrow ggT(a, bc) = 1.
\end{aligned}$$

$\square$

Aufgabe 1.2

Sei $n \in \mathbb{N}$ und seien $a_1, \cdots, a_n \in \mathbb{Z}$ nicht alle gleich 0.

$\boxed{\textbf{IA}}$ $\underline{n = 1}$

$$\begin{aligned}
&\langle a_1 \rangle\\
=\ &\{x_1 a_1 : x_1 \in \mathbb{Z}\}\\
=\ &\{x_1 a_1 + x_2 \cdot 0 : x_1, x_2 \in \mathbb{Z}\}\\
=\ &\{x \cdot ggT(a_1, 0) : x \in \mathbb{Z}\}\\
=\ &\langle ggT(a_1, 0) \rangle.
\end{aligned}$$

$\boxed{\textbf{IV}}$ Gelte die Behauptung für ein beliebiges, aber festes $n \in \mathbb{N}$.

$\boxed{\textbf{IS}}$ $\underline{n \to n + 1}$

$$\begin{aligned}
&\langle a_1, \cdots, a_{n+1} \rangle\\
=\ &\{\sum_{i=1}^{n+1} x_i a_i \mid x_1, \cdots x_{n+1} \in \mathbb{Z}\}\\
=\ &\{\sum_{i=1}^{n} x_i a_i + x_{n+1} a_{n+1} \mid x_1, \cdots x_{n+1} \in \mathbb{Z}\}\\
\overset{IV}{=}\ &\{x \cdot ggT(a_1, \cdots, a_n) + x_{n+1} a_{n+1} \mid x, x_{n+1} \in \mathbb{Z}\}\\
=\ &\{x \cdot ggT(ggT(a_1, \cdots, a_n), a_{n+1}) \mid x \in \mathbb{Z}\}\\
=\ &\{x \cdot ggT(a_1, \cdots, a_{n+1}) \mid x \in \mathbb{Z}\}\\
=\ &\langle ggT(a_1, \cdots, a_{n+1}) \rangle.
\end{aligned}$$

Somit gilt die Behauptung $\langle a_1, \cdots, a_n \rangle = \langle ggT(a_1, \cdots a_n) \rangle$ für alle $n \in \mathbb{N}$.

Außerdem ist zu zeigen, dass $ggT(a_1, \cdots, a_n)$ die kleinste positive Zahl ist, welche als ganzzahlige Linearkombination von $a_1, \cdots, a_n$ dargestellt werden kann.

Die induktive Definition des ggT ermöglicht es, die Bézout-Identität mehrfach zu verwenden, sodass die Behauptung folgt. Es gilt:

$$ggT(a_1, \cdots, a_n) = \; ggT(ggT(\cdots ggT(ggT(a_1, a_2), a_3) \cdots, a_{n-1}), a_n).$$

Da $ggT(a_1, a_2)$ die kleinste natürliche Zahl ist, die als ganzzahlige Linearkombination von a_1 und a_2 dargestellt werden kann, ist $ggT(ggT(a_1, a_2), a_3)$ die kleinste natürliche Zahl, die als Linearkombination von $ggT(a_1, a_2)$ und a_3 dargestellt werden kann.
Da alle Linearkombinationen von a_1 und a_2 Vielfache von $ggT(a_1, a_2)$ sind, ist $ggT(ggT(a_1, a_2), a_3) = ggT(a_1, a_2, a_3)$ die kleinste natürliche Zahl, die als Linearkombination von a_1, a_2 und a_3 dargestellt werden kann.
Dieses Argument wird solange angewendet, bis sich ergibt, dass $ggT(a_1, \cdots, a_n)$ die kleinste natürliche Zahl ist, die als Linearkombination von $a_1, \cdots, a_n$ dargestellt werden kann.

$\square$

Aufgabe 1.3

(a) Sei $(M, *)$ Monoid. Zu zeigen: $(M^*, *)$ Gruppe. Es gilt:

$$\begin{aligned} & (M,*) \text{ Monoid} \\ \overset{M^* \subseteq M}{\Longrightarrow} \; & (AG) \text{ gilt in } M^* \\ \Longrightarrow \; & (M^*, *) \text{ Halbgruppe.} \end{aligned}$$

Es gilt für NE $e \in M$:

$$\begin{aligned} e * e^{-1} = e = e^{-1} * e & \\ & \Longrightarrow e \in M^* \\ & \Longrightarrow \forall a \in M^* : a * e = a = e * a \\ & \Longrightarrow (M^*, *) \text{ Monoid.} \end{aligned}$$

Da M^* die Menge der invertierbaren Elemente aus M ist, gilt:

$$\begin{aligned} & \forall a \in M^* \; \exists b \in M^* : a * b = e = b * a \\ \Longrightarrow \; & (M^*, *) \text{ Gruppe.} \end{aligned}$$

Sei R Ring mit 1. Zu zeigen: R^* Gruppe. Es gilt:

$$\begin{aligned} & (R, +, *) \text{ Ring mit } 1 \\ \Longrightarrow \; & (R, *) \text{ Monoid} \\ \Longrightarrow \; & R^* \text{ Gruppe.} \end{aligned}$$

Wenn $(R, +, *)$ Ring ohne 1 ist, dann ist $(R, *)$ kein Monoid, sondern lediglich eine Halbgruppe. Da ein neutrales Element nicht in einer Halbgruppe gegeben ist, gilt die Aussage nicht für Ringe ohne 1.

$\square$

(b) Sei R kommutativer Ring mit 1. Zu zeigen: Jedes Ideal I von R enthält das Nullelement.
Sei $I = \langle a_1, \cdots, a_n \rangle$ Ideal von R beliebig. Es gilt:

$$\begin{aligned} & \forall a \in I\ \forall r \in \mathbb{Z} : ar \in I \\ \Longrightarrow\ & a \cdot 0 = 0 \in I. \end{aligned}$$

Ferner ist zu zeigen, dass I ein Unterring von R ist, welcher genau dann das Einselement enthält, wenn $I = R$.

Zunächst wird gezeigt, dass I Unterring von R ist.

1. Zu zeigen: $(I, +)$ ist abelsche Gruppe.

(U1) Zu zeigen: $I \neq \emptyset$. Es gilt:

$$I \text{ ist Ideal} \Longrightarrow\ I \neq \emptyset.$$

(U2) Seien $a, b \in I$ beliebig. Zu zeigen: $a - b \in I$. Es gilt:

$$\begin{aligned} & \forall x, y \in \mathbb{Z} : xa + yb \in I \\ \Longrightarrow\ & 1 \cdot a + (-1) \cdot b \in I \\ \Longrightarrow\ & a - b \in I. \end{aligned}$$

$\Longrightarrow$ $(I, +)$ ist nach Proposition 2.1.7 Untergruppe von R.

Seien $a = \sum_{i=1}^{n} x_i a_i$, $b = \sum_{i=1}^{n} y_i a_i \in I$ beliebig. Zu zeigen: $a + b = b + a$.
Es gilt:

$$\begin{aligned} & a + b \\ =\ & \sum_{i=1}^{n} x_i a_i + \sum_{i=1}^{n} y_i a_i \\ =\ & \sum_{i=1}^{n} y_i a_i + \sum_{i=1}^{n} x_i a_i \\ =\ & b + a. \end{aligned}$$

$\Longrightarrow$ $(I, +)$ abelsche Gruppe.

2. Zu zeigen: $(I, \cdot)$ Halbgruppe.
   Seien $a = \sum_{i=1}^{n} x_i a_i,\ \ b = \sum_{i=1}^{n} y_i a_i,\ \ c = \sum_{i=1}^{n} z_i a_i \in I$ beliebig. Es gilt:

$$\begin{aligned} & (a \cdot b) \cdot c \\ = \ & ((\sum_{i=1}^{n} x_i a_i) \cdot (\sum_{i=1}^{n} y_i a_i)) \cdot (\sum_{i=1}^{n} z_i a_i) \\ = \ & (\sum_{i=1}^{n} x_i a_i) \cdot ((\sum_{i=1}^{n} y_i a_i) \cdot (\sum_{i=1}^{n} z_i a_i)) \\ = \ & a \cdot (b \cdot c). \end{aligned}$$

   $\Longrightarrow \quad (I, \cdot)$ ist Halbgruppe.

3. Zu zeigen:
   (i) $\forall a, b, c \in I : (a + b) \cdot c = ac + bc$
   (ii) $\forall a, b, c \in I : a \cdot (b + c) = ab + ac$.

   Seien $a = \sum_{i=1}^{n} x_i a_i,\ \ b = \sum_{i=1}^{n} y_i a_i,\ \ c = \sum_{i=1}^{n} z_i a_i \in I$ beliebig. Es gilt:

$$\begin{aligned} & (a + b) \cdot c \\ = \ & (\sum_{i=1}^{n} x_i a_i + \sum_{i=1}^{n} y_i a_i) \cdot \sum_{i=1}^{n} z_i a_i \\ = \ & (\sum_{i=1}^{n} x_i a_i) \cdot (\sum_{i=1}^{n} z_i a_i) + (\sum_{i=1}^{n} y_i a_i) \cdot (\sum_{i=1}^{n} z_i a_i) \\ = \ & ac + bc. \end{aligned}$$

   Seien $a = \sum_{i=1}^{n} x_i a_i,\ \ b = \sum_{i=1}^{n} y_i a_i,\ \ c = \sum_{i=1}^{n} z_i a_i \in I$ beliebig. Es gilt:

$$\begin{aligned} & a \cdot (b + c) \\ = \ & \sum_{i=1}^{n} x_i a_i \cdot (\sum_{i=1}^{n} y_i a_i + \sum_{i=1}^{n} z_i a_i) \\ = \ & (\sum_{i=1}^{n} x_i a_i) \cdot (\sum_{i=1}^{n} y_i a_i) + (\sum_{i=1}^{n} x_i a_i) \cdot (\sum_{i=1}^{n} z_i a_i) \\ = \ & ab + ac. \end{aligned}$$

$\Longrightarrow \quad (I, +, \cdot)$ ist Ring
$\Longrightarrow \quad (I, +, \cdot)$ ist Unterring von R.

Nun soll gezeigt werden, dass $1 \in I \Longleftrightarrow I = R$.

"$\Longrightarrow$": Sei I Ring mit 1. Es gilt:

$$1 \in I \implies \forall a \in \mathbb{Z} : a \cdot 1 \in I \implies I = R.$$

"$\Longleftarrow$": Sei $I = R$. Es gilt:

$$1 \in R \implies 1 \in I.$$

$\implies \forall I \trianglelefteq R : 0 \in I$. Außerdem ist I Unterring von R, für den genau dann $1 \in I$ gilt, wenn $I = R$.

$\square$

korrigiert von am