Abgabe Algebra 1, Blatt 05

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

Aufgabe 5.1

(a) Sei R faktorieller Ring und sei $P \subset R$ ein Vertretersystem der Assoziiertenklassen aller Primelemente von R.
Zu zeigen: $\forall a, b \in R \setminus \{0\} : b \mid a \iff \upsilon_p(b) \leq \upsilon_p(a)$ für alle $p \in P$.

"$\Longrightarrow$" Seien $a, b \in R \setminus \{0\}$ mit $b \mid a$. Es gilt:

$$
\begin{aligned}
& b \mid a \\
\Longrightarrow\ & \text{Es existieren Primfakorzerlegungen für } a \text{ und } b, \\
& \text{sodass } a = \varepsilon(a) \cdot \prod_{p \in P} p^{\upsilon_p(a)}, b = \varepsilon(b) \cdot \prod_{p \in P} p^{\upsilon_p(b)} \\
\Longrightarrow\ & \varepsilon(b) \cdot \prod_{p \in P} p^{\upsilon_p(b)} \mid \varepsilon(a) \cdot \prod_{p \in P} p^{\upsilon_p(a)} \\
\Longrightarrow\ & \prod_{p \in P} p^{\upsilon_p(b)} \mid \prod_{p \in P} p^{\upsilon_p(a)} \\
\Longrightarrow\ & \prod_{p \in P} p^{0} \mid \prod_{p \in P} p^{\upsilon_p(a) - \upsilon_p(b)}
\end{aligned}
$$

Warum funktioniert diese Umformung? Teilen ist in Ringen nicht erlaubt. Genauer argumentieren. −1 P

$$
\begin{aligned}
\Longrightarrow\ & \forall p \in P : \upsilon_p(a) - \upsilon_p(b) \geq 0 \\
\Longrightarrow\ & \forall p \in P : \upsilon_p(a) \geq \upsilon_p(b).
\end{aligned}
$$

"$\Longleftarrow$" Sei $\upsilon_p(a) \geq \upsilon_p(b)$ für alle $p \in P$.
Es gilt:

$$
\begin{aligned}
& \forall p \in P : \upsilon_p(a) \geq \upsilon_p(b) \\
\Longrightarrow\ & b = \varepsilon(b) \cdot \prod_{p \in P} p^{\upsilon_p(b)} = \varepsilon(b) \cdot \prod_{p \in P} p^{\min\{\upsilon_p(b), \upsilon_p(a)\}} = g,
\end{aligned}
$$

wobei g ein größter gemeinsamer Teiler von a und b ist.
Das gilt nach Aufgabenteil b). Für b) hast Du allerdings Aufgabenteil a) angewendet. −1 P
Also gilt:

$$g \mid a \implies b \mid a.$$

□

Punkte Teil a): 1/3

(b) Sei R faktorieller Ring, $P \subset R$ Repräsentantensystem der Assoziiertenklassen aller Primelemente von R.
Seien

$$d := \prod_{p \in P} p^{\min\{v_p(a), v_p(b)\}} \quad \text{und} \quad k := \prod_{p \in P} p^{\max\{v_p(a), v_p(b)\}}.$$

(1) Zu zeigen: d ist ein größter gemeinsamer Teiler von a und b.
Seien $a, b \in R \setminus \{0\}$. Es gilt:

$$d = \prod_{p \in P} p^{\min\{v_p(a), v_p(b)\}} \quad \Big| \quad \prod_{p \in P} p^{v_p(a)} = a$$

Außerdem gilt:

$$d = \prod_{p \in P} p^{\min\{v_p(a), v_p(b)\}} \quad \Big| \quad \prod_{p \in P} p^{v_p(b)} = b$$

Sei $c \in R \setminus \{0\}$ mit $c \mid a$ und $c \mid b$.
Zu zeigen: $c \mid d$. Es gilt:

$$c = \varepsilon(c) \cdot \prod_{p \in P} p^{v_p(c)} \text{ mit } v_p(c) \leq v_p(a) \text{ und } v_p(c) \leq v_p(b)$$

$$\Longrightarrow v_p(c) \leq \min\{v_p(a), v_p(b)\} \quad \forall p \in P$$

$$\Longrightarrow c \mid d.$$

(2) Zu zeigen: k ist ein kleinstes gemeinsames Vielfaches von a und b.
Seien $a, b \in R \setminus \{0\}$. Es gilt:

$$a = \prod_{p \in P} p^{v_p(a)} \quad \Big| \quad \prod_{p \in P} p^{\max\{v_p(a), v_p(b)\}} = k.$$

Außerdem gilt:

$$b = \prod_{p \in P} p^{v_p(b)} \quad \Big| \quad \prod_{p \in P} p^{\max\{v_p(a), v_p(b)\}} = k.$$

Sei $f \in R \setminus \{0\}$ mit $a \mid f$ und $b \mid f$.
Zu zeigen: $k \mid f$. Es gilt:

$$a \mid f \text{ und } b \mid f$$

$$\Longrightarrow v_p(f) \geq v_p(a) \text{ und } v_p(f) \geq v_p(b)$$

$$\Longrightarrow v_p(f) \geq \max\{v_p(a), v_p(b)\}$$

$$\Longrightarrow k = \varepsilon(k) \cdot \prod_{p \in P} p^{\max\{v_p(a), v_p(b)\}} \quad | \quad \varepsilon(f) \cdot \prod_{p \in P} p^{v_p(f)} = f$$

$$\Longrightarrow k \text{ ist ein kleinstes gemeinsames Vielfaches von } a \text{ und } b.$$

Ferner ist zu zeigen: $kd \sim db$, d. h. $\exists x \in R^* : kdc = db$. Es gilt:

$$\begin{aligned} kd =& \left(\varepsilon(k) \cdot \prod_{p \in P} p^{\max\{v_p(a), v_p(b)\}}\right) \cdot \left(\varepsilon(d) \cdot \prod_{p \in P} p^{\min\{v_p(a), v_p(b)\}}\right) \\ =& \varepsilon(k)\varepsilon(d) \cdot \prod_{p \in P} p^{\max\{v_p(a), v_p(b)\} + \min\{v_p(a), v_p(b)\}} \\ =& \varepsilon(k) \cdot \varepsilon(d) \cdot \prod_{p \in P} p^{v_p(a) + v_p(b)} \\ =& \varepsilon(k) \cdot \varepsilon(d) \cdot \prod_{p \in P} p^{v_p(a)} \cdot \prod_{p \in P} p^{v_p(b)} \\ =& \varepsilon(k) \cdot \varepsilon(d) \cdot ab \end{aligned}$$

$\prod_{p \in P} p^{v_p(a)} \neq a$ im Allgemeinen. Es gibt nur ein $\varepsilon(a) \in R^* : a = \varepsilon \cdot \prod_{p \in P} p^{v_p(a)}$. Dasselbe für b. $-0,5$ P.

$$\implies \frac{kd}{\varepsilon(k)\varepsilon(d)} = kd \cdot c = ab.$$

□

Punkte Teil b): $2,5/3$

$3,5/6$ P

Aufgabe 5.2

(a) Sei $n \in \mathbb{N}, n \geq 2$ und sei $R := \mathbb{Z}/n\mathbb{Z}$.
Seien $f, g \in R[t], f := t^2 + [2]_n t + [1]_n, g := [3]_n t^3 + [6]_n t^2 + [33]_n t + [15]_n$.
Zu zeigen: $f \mid g$ für $n \in \{3, 5, 15\}$. Es gilt:

$$f \mid g \iff \exists h \in R[t] : f \cdot h = g.$$

Da $\deg(g) - \deg(f) = 1$ für $n \neq 3$ gilt, gilt $f \mid g$ nur dann, wenn $[15]_n = [0]_n$, da ansonsten kein $h \in R[t]$ existiert, sodass $f \cdot h = g$.
Es wurde nicht gezeigt, dass ein solches h dann nicht existieren kann. -1 P
Es gilt:

$$\begin{aligned} & [15]_n = [0]_n \iff n \mid 15 \\ \implies & n \in \{3, 5, 15\}. \end{aligned}$$

Für $n \notin \{3, 5, 15\}$ gilt: $f \nmid g$. Betrachte nun die einzelnen Fälle:

$\underline{n=3}$ Es gilt:

$$f = t^2 + [2]_3 t + [1]_3 \mid [0]_3 = [3]_3 t^3 + [6]_3 t^2 + [33]_3 t + [15]_3 = g$$

$\underline{n=5}$ Es gilt:

$$f = t^2 + [2]_5 t + [1]_5 \mid [3]_5 t^3 + [1]_5 t^2 + [3]_5 t = [3]_5 t^3 + [6]_5 t^2 + [33]_5 t + [15]_5 = g$$

$\underline{n=15}$ Es gilt:

$$f = t^2 + [2]_{15} t + [1]_{15} \mid [3]_{15} t^3 + [6]_{15} t^2 + [3]_{15} t = [3]_{15} t^3 + [6]_{15} t^2 + [33]_{15} t + [15]_{15} = g$$

Insgesamt ergibt sich, dass $f \mid g$ genau dann gilt, wenn $n \in \{3, 5, 15\}$ gilt.

□

Punkte Teil a): 2/3

(b) Sei $x := 2154878968 \in \mathbb{Z}$. Zu zeigen: x ist keine Quadratzahl. Es gilt:

$$\begin{aligned} 2154878968 &= 2^3 \cdot 269359871 \\ &= 2^3 \cdot 11 \cdot 24487261 \\ &= 2^3 \cdot 11 \cdot 71 \cdot 344891 \\ &= 2^3 \cdot 11 \cdot 71 \cdot 193. \end{aligned}$$

Da nicht alle Primfaktoren einen geraden Exponenten haben, kann man sie nicht so auseinanderziehen, dass jeweils die Hälfte der gleichen Primfaktoren zu einem Faktor gehört, d. h. es gibt keine Zerlegung, sodass:

$$x = \prod_{p \in P} p^{v_p(x)} = \left(\prod_{p \in P} p^{\frac{v_p(x)}{2}} \right) \cdot \left(\prod_{p \in P} p^{\frac{v_p(x)}{2}} \right) = \left(\prod_{p \in P} p^{\frac{v_p(x)}{2}} \right)^2$$

Daraus folgt, dass x keine Quadratzahl ist.
Es wurde nicht gezeigt, dass es so eine Zerlegung geben muss, wenn x eine Quadratzahl ist. -1 P.

□

Punkte Teil b): 2/3

4/6 P

Aufgabe 5.3

(a) Seien $a, b, c \in \mathbb{Z}$ und es gelte $d := \text{ggT}(a, b) \mid c$. Weiter sei $(x_0, y_0) \in \mathbb{T} \times \mathbb{Z}$ eine partikuläre Lösung der linearen diophantischen Gleichung $aX+bY = c$. Zu zeigen: $\left\{(x_0 + k\frac{b}{d}, y_0 - k\frac{a}{d}) \mid k \in \mathbb{Z}\right\}$ sind alle Lösungen der Gleichung $aX + bY = c$.

(1) Zu zeigen: $(x_0 + k\frac{b}{d}, y_0 - k\frac{a}{d})$ ist Lösung von $aX + bY = c$.
Es gilt:

$$\begin{aligned} & c = a\left(x_0 + k\frac{b}{d}\right) + b\left(y_0 - k\frac{a}{d}\right) \\ \iff & c = ax_0 + k\frac{ab}{d} + by_0 - k\frac{ab}{d} \\ \iff & c = ax_0 + by_0. \end{aligned}$$

Da $c = ax_0 + by_0$ nach Vorraussetzung eine Lösung der Gleichung ist, ist somit auch $(x_0 + k\frac{b}{d}, y_0 - k\frac{a}{d})$ eine Lösung der Gleichung.

(2) Sei (x, y) Lösung von $aX + bY = c$.
Zu zeigen: $(x, y) \in \left\{(x_0 + k\frac{b}{d}, y_0 - k\frac{a}{d}) \mid k \in \mathbb{Z}\right\}$.
Es gilt:

$$\begin{aligned} & (I)\ ax + by = c \quad \text{und} \quad (II)\ ax_0 + by_0 = c \\ \overset{(I)-(II)}{\implies} & ax + by - ax_0 - by_0 = c - c \\ \implies & a(x - x_0) + b(y - y_0) = 0 \\ \implies & a(x - x_0) = -b(y - y_0) \\ \implies & a(x - x_0) = b(y_0 - y) \\ \overset{d|a,b}{\implies} & a(x - x_0) = -b(y - y_0) \\ \implies & \frac{a}{d}(x - x_0) = \frac{b}{d}(y_0 - y) \\ \overset{\frac{a}{d}\frac{b}{d} teilerfremd}{\implies} & \frac{b}{d} \mid (x - x_0) \\ \implies & \exists k \in \mathbb{Z} : k\frac{b}{d} = x - x_0 \\ \implies & \exists k \in \mathbb{Z} : x = x_0 + k\frac{a}{d}. \end{aligned}$$

In (III) einsetzen:

$$\begin{aligned} & \frac{a}{d} \cdot z\frac{b}{d} = \frac{b}{d}(y_0 - y) \\ \Longrightarrow\ & z\frac{a}{d} = y_0 - y \\ \Longrightarrow\ & y = y_0 - z\frac{a}{d}. \end{aligned}$$

$z = k$? Wo finde ich (III)?
Also ist die Lösung (x, y) in der Menge $\left\{(x_0 + k\frac{b}{d}, y_0 - k\frac{a}{d}) \mid k \in \mathbb{Z}\right\}$ enthalten. Daraus folgt, dass die Menge $\left\{(x_0 + k\frac{b}{d}, y_0 - k\frac{a}{d}) \mid k \in \mathbb{Z}\right\}$ alle Lösungen der linearen diophantischen Gleichung $aX + bY = c$ enthält.

□

Punkte Teil a): 4/4

(b) Sei $105X + 429Y = 21$ eine lineare diophantische Gleichung.
Zu zeigen: $\{(86 + 143k, -21 - 35k) \mid k \in \mathbb{Z}\}$ enthält alle ganzzahligen Lösungen der Gleichung $105X + 429Y = 21$.
Es gilt:

$$105 \cdot 86 + 429 \cdot (-21) = 9030 - 9009 = 21.$$

Außerdem gilt:

$$\text{ggT}(105, 429) = \text{ggT}(3 \cdot 5 \cdot 7, 3 \cdot 11 \cdot 13) = 3.$$

Nach Aufgabe 5.3 (a) ist

$$\left\{(86 + k\frac{429}{3}, -21 - k\frac{105}{3}) \mid k \in \mathbb{Z}\right\} = \{(86 + 143k, -21 - 35k) \mid k \in \mathbb{Z}\}$$

die Menge aller Lösungen der linearen diophantischen Gleichung $105X + 429Y = 21$.

□

Punkte Teil b): 4/4

8/8 P

Insgesamt 15, 5/20 Punkten

korrigiert von Tom Engels am 28.05.2020