Prof. Immanuel Halupczok
Dr. Blaise Boissonneau

HHU Düsseldorf
Sommersemester 2026

**Algebra**
**Übungsblatt 7**
**Lösungsvorschlag**

**Aufgabe 1.**

a) Sei $a \in R$. Dann gilt $\underbrace{a + \cdots + a}_{n \text{ mal}} = \underbrace{1 \cdot a + \cdots + 1 \cdot a}_{n \text{ mal}} = (\underbrace{1 + \cdots + 1}_{n \text{ mal}}) \cdot a = 0 \cdot a = 0$.

b) Sei $n \in \mathbb{Z}$. Dann $\underbrace{(\overline{1}, \overline{1}) + \cdots + (\overline{1}, \overline{1})}_{n \text{ mal}} = (\overline{n}, \overline{n}) \in \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. Angenommen, dass $\underbrace{(\overline{1}, \overline{1}) + \cdots + (\overline{1}, \overline{1})}_{n \text{ mal}} = (\overline{0}, \overline{0})$; dann gilt $n \equiv 0 \mod 4$ und $n \equiv 0 \mod 6$. Also $n \in 4\mathbb{Z} \cap 6\mathbb{Z} = 12\mathbb{Z}$. Das heißt, die Charakteristik von $R$ ist 12.

**Aufgabe 2.**

a) Sei $f \in \mathbb{Z}[x]$ sodass $(3, x) = (f)$. Dann existiert $g \in \mathbb{Z}[x]$ mit $3 = fg$. Das impliziert $0 = \deg(3) = \deg(f) + \deg(g)$, also $\deg(f) = \deg(g) = 0$, und $f, g \in \mathbb{Z}$ sind. Also $f|3$ gilt in $\mathbb{Z}$, das heißt, $f \in \{-3, -1, 1, 3\}$.

Es existiert auch $h \in \mathbb{Z}[x]$ sodass $x = fh$. Dann gilt $1 = \deg(x) = \deg(f) + \deg(h) = \deg(h)$, also $h = ax + b$. Daraus folgt $x = fh = fax + fb$, also $fb = 0$ und $fa = 1$. Also $b = 0$, $a = \pm 1$, und $f = \pm 1$; das impliziert $(f) = \mathbb{Z}[x] \neq (3, x)$.

b) Sei $I$ ein Ideal mit $(3, x) \subsetneq I$. Also existiert $f \in I \setminus (3, x)$. Sei $n \in \mathbb{N}$ und $(b_i)_{i<n} \in \mathbb{Z}^n$ mit $f = \sum_{i=0}^{n} b_i x^i$. Aus $f \notin (3, x)$ und $(3, x) = \{\sum_{i=0}^{m} a_i x^i \in \mathbb{Z}[x] \mid a_0 \in 3\mathbb{Z}\}$ folgt, dass $b_0 \notin 3\mathbb{Z}$ ist. Es gilt $\sum_{i=1}^{n} b_i x^i \in (x) \subseteq I$, also $b_0 = f - \sum_{i=1}^{n} b_i x^i \in I$ gilt. $b_0 \notin 3\mathbb{Z}$, also existieren $k \in \mathbb{Z}$ und $r \in \{1, -1\}$ mit $b_0 = 3k + r$. Da $3k \in (3)$ ist, folgt dass $r = b_0 - 3k \in I$. Daraus folgt $I = K$ und $(3, x)$ ist maximal.

c) Sei $h_1 := xf - g = x^3 + 3x^2 + 2x - x^3 - 2x^2 + 1 = x^2 + 2x + 1 \in (f, g)$. Sei auch $h_2 := f - h_1 = x^2 + 3x + 2 - x^2 - 2x - 1 = x + 1 \in (f, g)$. Also $(h_2) \subseteq (f, g)$. Da $f = (x+1)(x+2)$ und $g = (x+1)(x^2 + x - 1)$, gilt auch $f \in (h_2)$ und $g \in (h_2)$, also $(f, g) \subseteq (h_2)$.

**Aufgabe 3.**

a) Sei $f = x - a$. Dann $\mathrm{ev}_a(f) = f(a) = a - a = 0$, also $f \in \ker(\mathrm{ev}_a)$.

b) Sei $g \in (x - a)$, dann existiert $q \in R[x]$ mit $g = (x - a)q$. Es gilt $\mathrm{ev}_a(g) = \mathrm{ev}_a(x - a)\,\mathrm{ev}_a(q) = 0\,\mathrm{ev}_a(q) = 0$, also $g \in \ker(\mathrm{ev}_a)$.

Sei nun $g = \sum_{i=0}^{n} a_i x^i \in \ker(\mathrm{ev}_a)$, also $g(a) = 0$. Daraus folgt, dass $q \in R[x]$ existiert mit $g = (x-a)q$. (Dieses Satz kann man benutzen ohne Beweis.) Wenn $R$ ein Körper

ist, können wir das zeigen mit Polynomdivision (Lem. 2.2.13). Wenn $R$ eine beliebige Ring ist, können wir das zeigen wie folgt:

Wir setzen $b_i = \sum_{k=0}^{n-i} a^k a_{i+k}$ für $0 < i \leqslant n$. Dann gilt $b_i = a_i + ab_{i+1}$ für $0 < i < n$ und $b_n = a_n$. Wir setzen $q = \sum_{i=1}^{n} b_i x^{i-1}$. Dann gilt

$$\begin{aligned}(x-a)q &= \sum_{i=1}^{n} b_i x^i - \sum_{i=1}^{n} ab_i x^{i-1} \\ &= \sum_{i=1}^{n} b_i x^i - \sum_{i=0}^{n-1} ab_{i+1} x^i \\ &= b_n x^n + \sum_{i=1}^{n-1} (b_i - ab_{i+1}) x^i - ab_1 \\ &= a_n x^n + \sum_{i=1}^{n-1} a_i x^i - ab_1 \\ &= g - a_0 - ab_1\end{aligned}$$

Das heißt, $g = (x-a)q + r$, mit $r = (a_0 + ab_1) \in R$.

Da $g \in \ker(\mathrm{ev}_a)$ liegt, gilt $0 = \mathrm{ev}_a(g) = \mathrm{ev}_a(x-a)\,\mathrm{ev}_a(q) + \mathrm{ev}_a(r) = 0\,\mathrm{ev}_a(q) + \mathrm{ev}_a(r) = \mathrm{ev}_a(r)$. Aber $r \in R$ liegt; daraus folgt $\mathrm{ev}_a(r) = r$, also $r = 0$. Schließlich gilt $g = (x-a)q$, also $g \in (x-a)$.

c) Der Homomorphiesatz sagt, dass $R[x]/\ker(\mathrm{ev}_a) \cong \mathrm{im}(\mathrm{ev}_a)$ gilt. Es gilt $\ker(\mathrm{ev}_a) = (x-a)$, und $\mathrm{im}(\mathrm{ev}_a) = R$ (da z.B. $\mathrm{ev}_a(r) = r$ für alle $r \in R$). Daraus folgt, dass $R[x]/(x-a) \cong R$.

**Aufgabe 4.**

a) Siehe Blatt 6 Aufgabe 6.

b) Sei $\iota\colon \mathbb{Z}[x] \to \mathbb{Q}[x]$ die Inklusion und $\mathrm{ev}_{\frac{1}{2}}\colon \mathbb{Q}[x] \to \mathbb{Q}$. Wir betrachten der Ringhomomorphismus $\varphi = \mathrm{ev}_{\frac{1}{2}} \circ \iota\colon \mathbb{Z}[x] \to \mathbb{Q}$.

Sei $c \in \mathrm{im}(\varphi)$. Dann existieren $n \in \mathbb{N}$ und $a_i \in \mathbb{Z}$ für $0 \leqslant i \leqslant n$ sodass

$$c = \sum_{i=0}^{n} a_i \frac{1}{2^i} = \frac{\sum_{i=0}^{n} a_i 2^{n-1}}{2^n}$$

gilt. Das heißt, $c \in S$.

Sei nun $c \in S$. Dann existieren $a \in \mathbb{Z}$ und $n \in \mathbb{N}$ mit $c = \frac{a}{2^n}$. Also $c = \varphi(ax^n) \in \mathrm{im}(\varphi)$; das heißt, $\mathrm{im}(\varphi) = S$.

Wir betrachten nun $\ker(\varphi)$. Es gilt $f \in \ker(\varphi)$ gdw. $\iota(f) \in \ker(\mathrm{ev}_{\frac{1}{2}})$. Aus Aufgabe 3 folgt, dass $\ker(\mathrm{ev}_{\frac{1}{2}}) = (x - \frac{1}{2}) = \left\{ f \in \mathbb{Q}[x] \;\middle|\; \exists q \in \mathbb{Q}[x] \text{ mit } f = (x-\tfrac{1}{2})q \right\}$. Da 2 invertierbar in $\mathbb{Q}$ ist, gilt auch

$$\ker(\mathrm{ev}_{\frac{1}{2}}) = (2x-1) = \{ f \in \mathbb{Q}[x] \mid \exists q \in \mathbb{Q}[x] \text{ mit } f = (2x-1)q \}$$

Sei $f \in \mathbb{Z}[x]$ teilbar durch $2x-1$, also existiert $q \in \mathbb{Z}[x]$ sodass $f = (2x-1)q$. Dann gilt $\iota(f) = (2x-1)\iota(q) \in \ker(\mathrm{ev}_{\frac{1}{2}})$, also $f \in \ker(\varphi)$.

Sei nun $f \in \ker(\varphi)$. Dann gilt $\iota(f) \in \ker(\mathrm{ev}_{\frac{1}{2}})$, also existiert $q \in \mathbb{Q}[x]$ mit $\iota(f) = (2x-1)q$. Da $f = \iota(f)$, gilt $f = (2x-1)q$; wir zeigen nun, dass $q \in \mathbb{Z}$ liegt.

Seien $n \in \mathbb{N}$ und $a_i \in \mathbb{Z}$ für $0 \leqslant i \leqslant n$ sodass $f = \sum_{i=0}^{n} a_i x^i$. Seien auch $b_i \in \mathbb{Q}$ für $0 \leqslant i < n$ sodass $q = \sum_{i=0}^{n-1} b_i x^i$. Dann gilt $a_0 = b_0$, also $b_0 \in \mathbb{Z}$. Angenommen, dass $b_i \in \mathbb{Z}$ für einige $i < n-1$. Dann gilt $b_{i+1} + 2b_i = a_{i+1}$, also $b_{i+1} = a_{i+1} - 2b_i \in \mathbb{Z}$ liegt; das heißt, $q \in \mathbb{Z}[x]$.

Schließlich gilt $\ker(\varphi) = (2x-1) \cdot \mathbb{Z}[x]$.

Also bei der Homomorphiesatz haben wir $\mathbb{Z}[x]/(2x-1) \cong S$.

**Aufgabe 5.**

a) Sei $x \in (m_1) \cap \cdots \cap (m_k)$. Dann ist $x$ teilbar durch $m_1$, $m_2$,... und $m_k$. Da die $m_i$ sind paarweise teilerfremd, ist $x$ teilbar durch der Produckt $m_1 m_2 \dots m_k$, also $x \in (m_1 m_2 \dots m_k)$.

Sei nun $x \in (m_1 m_2 \dots m_k)$. Dann ist $x$ teilbar durch $m_i$ für $1 \leqslant i \leqslant k$, also $x \in (m_i)$ für jede $i$. Das heißt, $(m_1) \cap \cdots \cap (m_k) = (m_1 m_2 \dots m_k)$

b) Weil die $m_i$ paarweise teilerfremd sind, ist die Projektion $\mathbb{Z} \to \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z}$, $n \mapsto (n \mod m_1, \dots n \mod m_k)$ surjetkiv. Insbesondere existiert $n \in \mathbb{Z}$ mit

$$(n \mod m_1, \dots, n \mod m_k) = (a_1 \mod m_1, \dots, a_k \mod m_k)$$

c) Seien $n, n'$ sodass $n \equiv n' \equiv a_i \mod m_i$ für $1 \leqslant i \leqslant k$. Dann ist $n - n' \equiv 0 \mod m_i$, also $n - n' \in (m_i)$ für jede $i$; das heißt, $n - n' \in (m_1) \cap \cdots \cap (m_k) = (m_1 m_2 \dots m_k)$, also existiert $a \in \mathbb{Z}$ mit $n' = n + a m_1 m_2 \dots m_k$.

Angenommen nun, dass $n' = n + a m_1 m_2 \dots m_k$ für einige $a \in \mathbb{Z}$; dann folgt $n - n' = 0 \mod m_i$ für jede $i$ und $n' \equiv n \equiv a_i \mod m_i$. Also, die Menge von $n' \in \mathbb{Z}$, die (*) erfüllen, ist genau $\{n' \in \mathbb{Z} \mid n' \equiv n \mod m_1 m_2 \dots m_k\}$.

**Aufgabe 6.** Sei $n \in \mathbb{Z}$ nicht teilerfremd mit 12. Sei $a > 1$ mit $a|n$ und $a|12$, also existieren $b < 12$ und $c < n$ mit $12 = ab$ und $n = ac$. Angenommen, dass $m \in \mathbb{Z}$ existiert sodass $nm \equiv 1 \mod 12$. Dann $bnm = bacm = 12cm \equiv 0 \mod 12$, aber $bnm \equiv b \cdot 1 \equiv b \not\equiv 0 \mod 12$. Das heißt, Einheiten des Rings $\mathbb{Z}/12\mathbb{Z}$ sind teilerfremd mit 12, also in der List $\overline{1}, \overline{5}, \overline{7} = -\overline{5}, \overline{11} = -\overline{1} \in \mathbb{Z}/12\mathbb{Z}$.

Es gilt $1 \cdot 1 \equiv 1 \mod 12$, $5 \cdot 5 = 25 \equiv 1 \mod 12$, $(-5) \cdot (-5) = 5 \cdot 5 \equiv 1 \mod 12$, und $(-1) \cdot (-1) = 1 \equiv 1 \mod 12$.

Das heißt, die Einheiten des Rings $\mathbb{Z}/12\mathbb{Z}$ sind genau $\overline{1}$, $\overline{5}$, $-\overline{5}$ und $-\overline{1}$.