Prof. Immanuel Halupczok
Dr. Blaise Boissonneau

HHU Düsseldorf
Sommersemester 2026

Algebra
Übungsblatt 9
Lösungsvorschlag

Aufgabe 1.

a) Seien $g, h \in K[x]$ sodass $f = gh$. Wenn $\deg(g) = 0$ gilt, ist $g \in K^\times$, also ist g ein Einheit. Wenn $\deg(g) = 2$ gilt, gilt $\deg(h) = 0$ und h ist ein Einheit. Wenn $\deg(g) = \deg(h) = 1$ gilt, existieren $a, b \in K$ mit $g = ax + b$ und $a \neq 0$. Dann ist $-\frac{b}{a} \in K$ ein Nullstelle von g und danach auch von f. Also wenn f keine Nullstelle hat, muss f irreduzibel sein.

b) Es gilt $f(0) = 1$, $f(1) = 2$ und $f(2) = f(-1) = 2$, also hat f keine Nullstelle und ist danach irreduzibel.

c) Da f irreduzibel ist, ist (f) Maximal, und daraus folgt, dass $\mathbb{F}_3[x]/(f)$ ein Körper ist.

d) Nein, da $\mathbb{Z}/9\mathbb{Z}$ kein Körper ist: $3 \cdot 3 = 0 \in \mathbb{Z}/9\mathbb{Z}$.

e) Aus Bsp. 2.2.14 folgt, dass $\mathbb{F}_9$ ein $\mathbb{F}_3$-Vektorraum ist, mit Basis $\{1, \overline{x}\}$. Also gilt $\mathbb{F}_9 = \{a + b\overline{x} \mid a, b \in \mathbb{F}_3\}$.

f) Es gilt $\overline{f} = 0$ in $\mathbb{F}_9$, also $\overline{x^2 + 1} = 0$ und $\overline{x}^2 = -1$. Daraus folgt $(a + b\overline{x}) \cdot (c + d\overline{x}) = ac + bc\overline{x} + ad\overline{x} + bd\overline{x}^2 = (ac - bd) + (bc + ad)\overline{x}$.

g) $f = x^2+1$ hat auch kein Nullstelle in $\mathbb{R}$ und ist danach irreduzibel, also ist $(f) \subseteq \mathbb{R}[x]$ maximal und $\mathbb{R}[x]/(f)$ ist ein Körper. Es gilt $\mathbb{R}[x]/(f) = \{a + b\overline{x} \mid a, b \in \mathbb{R}\}$ mit $\overline{x}^2 = -1$, also $\mathbb{R}[x]/(f) \cong \mathbb{C}$.

Aufgabe 2.

a) Alle Elemente der Form $\pm 2^i$ für $i \in \mathbb{Z}$ sind Einheiten in $\mathbb{Z}[\frac{1}{2}]$, da $(\pm 2^i)(\pm 2^{-i}) = 1$ gilt, und $\pm 2^i \in \mathbb{Z}[\frac{1}{2}]$ für alle $i \in \mathbb{Z}$.

Sei nun $x = \frac{a}{2^n} \in \mathbb{Z}[\frac{1}{2}]^\times$, also $a \in \mathbb{Z}$ und $n \in \mathbb{N}$. Da x invertierbar ist, existiert $y = \frac{c}{2^m} \in \mathbb{Z}[\frac{1}{2}]$ mit $xy = 1$, also $c \in \mathbb{Z}$ und $m \in \mathbb{N}$. Es gilt $xy = \frac{ac}{2^{n+m}} = 1$ also $ac = 2^{n+m}$. Daraus folgt $a | 2^{n+m}$ (in $\mathbb{Z}$), also $a = \pm 2^k$ mit $k \leqslant n + m$; also $x = \frac{a}{2^n} = \pm 2^{k-n}$, das heißt, die Einheiten in $\mathbb{Z}[\frac{1}{2}]$ sind genau die Elemente der Form $\pm 2^i$ mit $i \in \mathbb{Z}$.

b) Sei $p \in \mathbb{N}$ eine ungerade Primzahl. Dann ist p irreduzibel in $\mathbb{Z}[\frac{1}{2}]$: Angenommen, dass $x, y \in \mathbb{Z}[\frac{1}{2}]$ existieren, mit $p = xy$. Seien $a, b \in \mathbb{Z}$ und $n, m \in \mathbb{N}$ mit $x = \frac{a}{2^n}$ und $y = \frac{b}{2^m}$. Dann gilt $p = xy = \frac{ab}{2^{n+m}}$, also $2^{n+m}p = ab$. Da $p \neq 2$ eine Primzahl ist, bei der Primfaktorzerlegung in $\mathbb{Z}$, folgt dass $a = \pm 2^r p^{r'}$ und $b = \pm 2^s p^{s'}$, mit $r + s = n + m$ und $r' + s' = 1$. Also, entweder $r' = 0$ oder $s' = 0$, das heißt, entweder x oder y ist ein Einheit.

Daraus folgt, dass alle Elemente der Form $\pm 2^n p$ mit $n \in \mathbb{Z}$ und p eine ungerade Primzahl irreduzibel sind.

Sei nun $x \in \mathbb{Z}[\frac{1}{2}]$ irreduzibel. Dann existiert $a \in \mathbb{Z}$ und $n \in \mathbb{N}$ mit $x = \frac{a}{2^n}$. Sei $m \in \mathbb{N}$ sodass $2^m | a$ und $2^{m+1} \not| a$ in $\mathbb{Z}$. Sei $b \in \mathbb{N}$ mit $a = \pm 2^m b$. Dann ist x assoziiert zu b da $x = \pm 2^{m-n} b$. Wenn b nicht prim ist, kann man $b = cd$ schreiben mit $c, d \in \mathbb{N}$, $c, d > 2$; also ist b reduzibel in $\mathbb{Z}[\frac{1}{2}]$, und daraus x auch. Wenn $b = 1$ ist, dann ist x ein Einheit. Das heißt, b muss ein ungerade Primzahl sein, und x ist der Form $\pm 2^n p$ mit $n \in \mathbb{Z}$ und p ungerade und prim.

c) Die Menge $P = \left\{ p = \frac{p}{1} \in \mathbb{Z}[\frac{1}{2}] \;\middle|\; p \text{ ist eine ungerade Primzahl} \right\}$ ist ein Repräsentantensystem der irreduziblen Elemente von $\mathbb{Z}[12]$. Seien $a \in \mathbb{Z}$ und $n \in \mathbb{N}$. Wir schreiben $a = \pm 2^r \prod_{i=1}^{k} p_i^{r_i}$, mit $k \in \mathbb{N}$, $p_i \in P$ und $r_i \in \mathbb{N}$. Dann gilt $\frac{a}{2^n} = \pm 2^{r-n} \prod_{i=1}^{k} p_i^{r_i}$, mit $\pm 2^{r-n}$ ein Einheit.

Angenommen, dass eine andere Zerlegung von $\frac{a}{2^n}$ exitiert, also $u \in \mathbb{Z}[\frac{1}{2}]$, $m \in \mathbb{N}$, $p_i' \in P$ und $r_i \in \mathbb{N}$ mit $\frac{a}{2^n} = u \prod_{i=1}^{m} p_i'^{r_i'}$. Dann gilt $a = u 2^n \prod_{i=1}^{m} p_i'^{r_i'}$; aber bei der Eindeugtigkeit der Primfaktorzerlegung in $\mathbb{Z}$, ist $\{(p_i, r_i) \mid i \leqslant k\} = \{(p_i', r_i') \mid i \leqslant m\}$, das heißt, die Zerlegung von $\frac{a}{2^n}$ ist eindeutig und $\mathbb{Z}[\frac{1}{2}]$ faktoriel ist.

Aufgabe 3.

a) Sei R ein Hauptidealring, und seien $a, b \in R$ teilerfremd. Dann existiert $c \in R$ mit $(a, b) = (c) = cR$. Da $a \in (a, b)$ gilt $c | a$ in R. Ähnlich gilt $c | b$ in R; also, c ist ein Einheit in R. Daraus folgt $(c) = R$.

Sei nun $a, b \in R$ mit $(a, b) = R$, und sei $c \in R$ mit $c | a$ und $c | b$. Dann gilt $a \in (c)$, $b \in (c)$, also $R = (a, b) \subseteq (c)$. Insbesondere, $1 \in (c) = cR$, also existiert $d \in R$ mit $1 = cd$; das heißt, c ist ein Einheit. Daraus folgt, dass a, b teilerfremd sind.

b) Sei R ein faktoriel Ring und $a, b \in R$ teilerfremd. Es gilt $(ab) \subseteq (a)$ und $(ab) \subseteq (b)$, also $(ab) \subseteq (a) \cap (b)$. Sei zuletzt $x \in (a) \cap (b)$. Also gilt $a | x$ und $b | x$. Sei $P \subseteq R$ ein Repräsentantensystem der irreduziblen Elemente von R. Dann existieren $p_1, \ldots, p_k \in P$, $r_1, \ldots, r_k, s_1, \ldots, s_k, t_1, \ldots, t_k \in \mathbb{N}$, und $u, v, w \in \mathbb{R}^\times$ mit $a = u \prod_{i=1}^{k} p_i^{r_i}$, $b = v \prod_{i=1}^{k} p_i^{s_i}$, und $x = w \prod_{i=1}^{k} p_i^{t_i}$. Da a und b teilerfremd sind, folgt $r_i = 0$ oder $s_i = 0$ für jede i. Da $a | x$, folgt $r_i \leqslant t_i$ für jede i. Da $b | x$, folgt $s_i \leqslant t_i$ für jede i. Also gilt für alle i, dass $r_i + s_i = \max(r_i, s_i) \leqslant t_i$. Daraus folgt, dass $ab = uv \prod_{i=1}^{k} p_i^{r_i + s_i}$ ein Teiler von x ist, dass heißt, $x \in (ab)$.

c) Sei R ein Hauptidealring und seien $a, b \in R$ teilerfremd. Aus a) folgt, dass $(a, b) = ((a) \cup (b)) = R$. Aus den Chinesischer Restsatz folgt, dass der Ringhomorphismus $f \colon R \to R/(a) \times R/(b)$ surjektiv ist, mit $\ker(f) = (a) \cap (b)$. Da R ein Hauptidealring ist, ist R auch faktoriel. Aus b) folgt, dass $(a) \cap (b) = (ab)$. Schließlich gilt $R/\ker(f) \cong \mathrm{im}(f)$, also $R/(ab) \cong R/(a) \times R/(b)$.

d) Es gilt $x^2 - 1 = (x - 1)(x + 1)$. Sei $f \in \mathbb{R}[x]$ mit $f | (x + 1)$ und $f | (x - 1)$, also $\deg(f) \leqslant 1$. Angenommen, dass $\deg(f) = 1$. Wir nehmen auch an, dass f normiert ist, also $f = x + a$ mit $a \in \mathbb{R}$. Da $f | (x+1)$, existiert $b \in \mathbb{R}$ mit $bf = bx + ba = (x+1)$; also $b = 1$ und $ba = a = 1$. Dann gilt $f = x + 1$; aber dann $f \not| (x - 1)$. Also muss $\deg(f) < 1$ sein, das heißt, $f \in \mathbb{R}[x]^\times$ und $(x + 1)$, $(x - 1)$ sind teilerfremd. Da $\mathbb{R}[x]$ ein Hauptidealring ist, folgt aus c), dass $R/(x^2 - 1) \cong \mathbb{R}[x]/(x - 1) \times \mathbb{R}[x]/(x + 1)$.

Zuletxt betrachten wir $\mathbb{R}[x]/(f)$ mit $\deg(f) = 1$. Da f irreduzibel ist, ist $\mathbb{R}[x]/(f)$ ein $\mathbb{R}$-Vektorraum mit Basis $\{1\}$; also $\mathbb{R}[x]/(f) \cong \mathbb{R}$; schließlich gilt $R/(x^2 - 1) \cong \mathbb{R} \times \mathbb{R}$.