F2ST1A2 (Übung: H22T2A2, F12T1A3)

Sei $b \in \mathbb{Z} \setminus \{0\}$ und $R_b = \left\{ \frac{a}{b^k} \mid a \in \mathbb{Z}, k \in \mathbb{N}_0 \right\}$.

(a) Zeigen Sie, dass R_b ein Teilring von $\mathbb{Q}$ und somit ein kommutativer Ring mit 1 ist.

Offenbar gilt $R_b \subseteq \mathbb{Q}$ (da $\frac{a}{b^k} \in \mathbb{Q}$ für alle $a \in \mathbb{Z}$ und $k \in \mathbb{N}_0$). Für die Teilring-Eigenschaft müssen wir überprüfen

(1) $1 \in R_b$ (2) $\forall \alpha, \beta \in R_b : \alpha - \beta, \alpha\beta \in R_b$

genschaft müssen wir überprüfen

zu (1) Es gilt $1 = \frac{1}{b^0}$, und $1 \in \mathbb{Z}$, $0 \in \mathbb{N}_0$.

zu (2) Seien $\alpha, \beta \in R_b \Rightarrow \exists\, a, c \in \mathbb{Z}$ und $k, l \in \mathbb{N}_0$ mit $\alpha = \frac{a}{b^k}$, $\beta = \frac{c}{b^l}$.

$\alpha \cdot \beta = \frac{ac}{b^{k+l}}$, und $ac \in \mathbb{Z}$, $k+l \in \mathbb{N}_0 \Rightarrow \alpha\beta \in R_b$

$\alpha - \beta = \frac{a \cdot b^l - c \cdot b^k}{b^{k+l}}$, und $a b^l - c \cdot b^k \in \mathbb{Z}$, $k+l \in \mathbb{N}_0$

$\Rightarrow \alpha - \beta \in R_b$

Jeder Teilring eines kommutativen Rings mit 1 ist ein kommutativer Ring mit 1. Weil $\mathbb{Q}$ ein kommutativer Ring mit 1 ist, gilt dasselbe für R_b.

(6) Zeigen Sie, dass die Einheitengruppe R_6^* von R_6 gegeben ist durch $R_6^* = \{\frac{a}{6^k} \in R_6 \mid a \in \mathbb{Z} \text{ und } \exists\, c \in \mathbb{Z}\setminus\{0\} \text{ und } l \in \mathbb{N}_0 \text{ mit } ac = 6^l\}$.

Sei U die Menge auf der rechten Seite der Gleichung.

z.zg.: $R_6^* = U$ „$\supseteq$" Sei $\alpha \in U$. z.zg.: Es existiert ein $\beta \in R_6$ mit $\alpha \cdot \beta = 1_{R_6} = 1$. $\alpha \in U \Rightarrow \exists\, a \in \mathbb{Z}$, $c \in \mathbb{Z}\setminus\{0\}$, $k, l \in \mathbb{N}_0$ mit $\alpha = \frac{a}{6^k}$ und $ac = 6^l$

$\Rightarrow \alpha \cdot 6^k \cdot c = 6^l \Rightarrow \alpha \cdot 6^{k-l} \cdot c = 1$

1. Fall: $k - l \geq 0$ (d.h. $k - l \in \mathbb{N}_0$)

Sei $\beta = \frac{6^{k-l} c}{6^0}$. Dieses Element ist in R_6 enthalten.

$\Rightarrow \alpha \cdot b^k \cdot c = b^l \Rightarrow \alpha \cdot b^{k-l} \cdot c = 1$

1. Fall: $k-l \geq 0$ (d.h. $k-l \in \mathbb{N}_0$)

da $b^{k-l} \cdot c \in \mathbb{Z}$ (wg. $k-l \geq 0$) und $0 \in \mathbb{N}_0$. Außerdem gilt $\alpha \cdot \beta = 1$.

2. Fall: $k-l < 0$ Dann liegt $m = l-k$ in $\mathbb{N}$, insb. in $\mathbb{N}_0$. Das Element $\beta = b^{k-l} \cdot c = b^{-m} \cdot c = \frac{c}{b^m}$ liegt in R_b wg. $c \in \mathbb{Z}$, $m \in \mathbb{N}_0$, und wiederum gilt $\alpha \cdot \beta = 1$.

„$\subseteq$" Sei $\alpha \in R_b^\times$, z.zg.: $\alpha \in U$ $\alpha \in R_b^\times \Rightarrow \alpha \in R_b$ und $\exists \beta \in R_b$ mit $\alpha \cdot \beta = 1 \Rightarrow \exists a, d \in \mathbb{Z}$ und $k, m \in \mathbb{N}_0$ mit $\alpha = \frac{a}{b^k}$, $\beta = \frac{d}{b^m}$ $\alpha \cdot \beta = 1 \Rightarrow \frac{ad}{b^k b^m} = 1 \Rightarrow$ $ad = b^{k+m}$ Setzen wir $c = d$ und $l = k+m$, dann gilt $ac = b^l$. Wäre $c = 0$, dann würde $ac = 0$ folgen, im Wider-

spruch zu $f' \neq 0$. So aber gilt $c \in \mathbb{Z}/4\mathbb{Z}$, und insgesamt $x \in U$.

Def. Sei R ein Ring. Ideal von R = Teilmenge $I \subseteq R$, die folgende Bedingungen erfüllt (1) $0_R \in I$

(2) $\forall r \in R \; \forall a, b \in I : a+b \in I, \; ra \in I$

Gibt es ein $c \in R$ mit $I = (c) = \{rc \mid r \in R\}$ dann bezeichnet man I als Hauptideal.

Ein Integritätsbereich, in dem jedes Ideal ein Hauptideal ist, heißt Hauptidealring oder Hauptidealbereich.

F25T1A2 (c) Zeigen Sie, dass R_6 ein Hauptidealbereich ist, und das jedes Ideal $I \subset R_6$ die Form $I = R_6 w$ für ein $w \in \mathbb{Z}$ besitzt. (Hinweis: Betrachten Sie die Schnittmenge $I \cap \mathbb{Z}$.)

Es genügt zu zeigen, dass jedes Ideal die angegebene Form hat, denn daraus folgt, dass I mit dem Hauptideal (w) übereinstimmt (Wegen $w = \frac{w}{60}$ ist w ein Element von R_6.), und als Teilring des Körpers $\mathbb{Q}$ ist R_6 ein Integritätsbereich.

Sei also I ein bel. Ideal in R_6. Allgemein gilt: Ist R ein Ring, $S \subseteq R$ ein Teilring von R und I ein Ideal in R, dann ist $I \cap S$ ein Ideal in S. (Grund: $I \cap S$ ist das Urbild von I unter dem Inklusionshom. $\iota: S \to R$, $s \mapsto s$, d.h. $\iota^{-1}(I) = I \cap S$, und Urbilder von Idealen unter Ringhom. sind Ideale.) Da $\mathbb{Z}$ offenbar ein Teilring von R_6 ist ($1 \in \mathbb{Z}$, $\forall a, b \in \mathbb{Z}: a-b, ab \in \mathbb{Z}$), ist $I \cap \mathbb{Z}$ ein Ideal in $\mathbb{Z}$. Da $\mathbb{Z}$ ein Hauptidealring ist, existiert ein $w \in \mathbb{Z}$ mit $I \cap \mathbb{Z} = w\mathbb{Z}$

Beh. $I = R_6 w$ „$\supseteq$" Jedes Element in

$R_G w$ hat die Form αw mit $\alpha \in R_G$. Es gilt $w \in I$, und weil I ein Ideal ist, folgt $\alpha w \in I$.

„$\subseteq$" Sei $\gamma \in I$, z.zg. $\gamma \in R_G w$

$\gamma \in R_G \Rightarrow \exists a \in \mathbb{Z}, k \in \mathbb{N}_0$ mit $\gamma = \frac{a}{b^k}$

$\Rightarrow b^k \gamma = a \in \mathbb{Z}$, und wegen $b^k \in R_G$ und $\gamma \in I$ liegt $b^k \gamma$ auch in I.

$\Rightarrow b^k \gamma \in I \cap \mathbb{Z} \Rightarrow b^k \gamma \in \mathbb{Z} w \Rightarrow$

$\exists c \in \mathbb{Z}$ mit $b^k \gamma = cw \Rightarrow \gamma = \frac{cw}{b^k}$

$= \frac{c}{b^k} \cdot w$, und wegen $\frac{c}{b^k} \in R_G$ folgt

$\gamma \in R_G w$.

□

Def: Sei R ein Ring und I ein Ideal in R.

R/I = Menge der Nebenklassen von I

$= \{a+I \mid a \in R\}$

Faktorring von R modulo I = Menge R/I mit den Verknüpfungen $+$ und $\cdot$ gegeben durch

$(a+I)+(b+I) = (a+b)+I$ und

$(a+I)\cdot(b+I) = a\cdot b + I$ für alle $a, b \in R$

wichtige Regel: Für alle $a, b \in R$ gilt die Äquivalenz $a+I = b+I \iff b \in a+I \iff b-a \in I$

Nach Definition ist die Kongruenzrelation modulo I auf R definiert durch $a \equiv b \bmod I$
$\Leftrightarrow b - a \in I$. Es gilt also auch

$$a + I = b + I \iff a \equiv b \bmod I$$

Def. Seien R, S Ringe, I ein Ideal in R und $\phi : R \to S$ ein Ringhom. mit $\ker(\phi) \supseteq I$. Dann existiert ein eind. bestimmter Hom. $\overline{\phi} : R/I \to S$ mit $\overline{\phi}(a+I) = \phi(a)$ $\forall a \in R$, die sog durch ϕ induzierte Hom. $R/I \to S$.

Homomorphiesatz für Ringe:

Sei $\phi : R \to S$ ein Ringhom. und $I = \ker(\phi)$.
Dann definiert der durch ϕ induzierte Hom. $\bar{\phi}$ einen Isomorphismus zwischen R/I und $\mathrm{im}(\phi)$.

F26T1A3 Sei p eine Primzahl und $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$, $a \mapsto \bar{a} = a + p\mathbb{Z}$ der kanonische Epimorphismus.

(a) Zeigen Sie, dass die Abb. $\varphi : \mathbb{Z}[x] \to \mathbb{Z}/p\mathbb{Z}$, $h \mapsto \overline{h(0)}$ ein surjektiver Ringhom. ist.

Surjektivität: Sei $\bar{a} \in \mathbb{Z}/p\mathbb{Z}$, $\bar{a} = a + p\mathbb{Z}$ mit $a \in \mathbb{Z}$.
Dann gilt $a \in \mathbb{Z}[x]$, $a(0) = a$ und $\varphi(a) = \overline{a(0)} = \bar{a}$.

Hom.-Eig Laut Vorlesung existiert ein eind. bestimmter Ringhom. $\phi: \mathbb{Z}[x] \to \mathbb{Z}$ mit $\phi|_{\mathbb{Z}} = \mathrm{id}_{\mathbb{Z}}$ und $\phi(x) = 0$, der sog. Einsetzungshom. Diese ist geg. durch $\phi(h) = h(0)$ für alle $h \in \mathbb{Z}[x]$. Offenbar ist φ die Komposition von ϕ mit dem kan. Epimorphismus $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$, und die Komposition zweier Hom ist wieder ein Hom.

(6) Beweisen Sie die Gleichung $\ker(\varphi) = (p, x)$.

[Nach Def gilt $(p, x) = \{up + vx \mid u, v \in \mathbb{Z}[x]\}$.]

Für alle $h \in \mathbb{Z}[x]$ gilt die Äquivalenz

$h \in \ker(\varphi) \iff \varphi(h) = \overline{0} \iff \overline{h(0)} = \overline{0} \iff$

$h(0) + pZ = 0 + pZ \iff h(0) \in pZ$

$\iff$ konstanter Term von h ist teilbar durch p

$\overset{(*)}{\iff} \exists\, u, v \in \mathbb{Z}[x]$ mit $u \cdot p + v \cdot x = h$

$\iff h \in (p, x)$

zu $(*)$ „$\Leftarrow$" Der konstante Term von $u \cdot x$ ist gleich 0, und der von $v \cdot p$ durch p teilbar $\Rightarrow$ Der konst. Term von h ist durch p teilbar

„$\Rightarrow$" Ist $h = \sum_{k=0}^{m} a_k x^k$ mit $m \in \mathbb{N}_0, a_0, \dots, a_m \in \mathbb{Z}$, und ist $a_0 = p b_0$ mit $b_0 \in \mathbb{Z}$, dann erfüllen $v = \sum_{k=1}^{m} a_k x^{k-1}$ und $u = b_0$ die angeg. Gleichung

Übung: F19T2A4

Zeigen Sie zunächst

$$\mathbb{Q}[x]/(x^5-2, x^6+x^5-2x-2)$$

$$\cong \mathbb{Q}[x]/(x^5-2) \text{ und } \mathbb{Z}[x]/(5, x^3-2x^2+4)$$

$$\cong \mathbb{F}_5[x]/(x^3-\bar{2}x^2+\bar{4})$$