Algebra I, WiSe 2011\2012 – Lösung Blatt 10

10.1. (i) (α)

- Da $(R,+)$ und $(\mathbb{Z},+)$ abelsche Gruppen sind, ist $(R\times\mathbb{Z},+)$ eine abelsche Gruppe (+ ist in $R\times\mathbb{Z}$ Komponentenweise definiert)

- Neutrales Element der Multiplikation ist $(0,1)$, denn

$$(0,1)\cdot(r,z) = (0\cdot r + z\cdot 0 + 1\cdot r\ ,\ 1\cdot z) = (r,z)$$

$$(r,z)\cdot(0,1) = (r\cdot 0 + 1\cdot r + z\cdot 0\ ,\ z\cdot 1) = (r,z)$$

- Überlegung vorab: $z\in\mathbb{Z}$, $r,s\in R$

$$(z\cdot r)\cdot s = \underset{\text{VZ von } z}{(\pm)}(r+\ldots+r)s = (\pm)(rs+\ldots+rs) = z(rs)$$

$$s(z\cdot r) = (\pm)s(r+\ldots+r) = (\pm)(sr+\ldots+sr) = z(sr).$$

- Distributivgesetze:

$$(r_1,z_1)\big((r_2,z_2)+(r_3,z_3)\big) = (r_1,z_1)(r_2+r_3, z_2+z_3)$$

$$= \big(r_1(r_2+r_3) + (z_2+z_3)r_1 + z_1(r_2+r_3)\ ,\ z_1(z_2+z_3)\big)$$

$$= \big(r_1r_2 + r_1r_3 + z_2r_1 + z_3r_1 + z_1r_2 + z_1r_3\ ,\ z_1z_2 + z_1z_3\big)$$

$$= \big(r_1r_2 + z_2r_1 + z_1r_2\ ,\ z_1z_2\big) + \big(r_1r_3 + z_3r_1 + z_1r_3,\ z_1z_3\big)$$

$$= (r_1,z_1)(r_2,z_2) + (r_1,z_1)(r_3,z_3)$$

$$((r_1,z_1)+(r_2,z_2))(r_3,z_3) = (r_1+r_2, z_1+z_2)(r_3,z_3)$$

$$= ((r_1+r_2)r_3 + z_3(r_1+r_2) + (z_1+z_2)r_3 , (z_1+z_2)z_3)$$

$$= (r_1r_3 + r_2r_3 + z_3r_1 + z_3r_2 + z_1r_3 + z_2r_3 , z_1z_3 + z_2z_3)$$

$$= (r_1r_3 + z_3r_1 + z_1r_3 , z_1z_3) + (r_2r_3 + z_3r_2 + z_2r_3 , z_2z_3)$$

$$= (r_1,z_1)(r_3,z_3) + (r_2,z_2)(r_3,z_3)$$

- Assoziativgesetz (Vorsicht: R muss nicht kommutativ sein)

$$((r_1,z_1)(r_2,z_2))(r_3,z_3) = (r_1r_2 + z_2r_1 + z_1r_2 , z_1z_2)(r_3,z_3)$$

$$= ((r_1r_2+z_2r_1+z_1r_2)r_3 + z_3(r_1r_2+z_2r_1+z_1r_2) + z_1z_2r_3 , z_1z_2z_3)$$

$$= (r_1r_2r_3 + z_2r_1r_3 + z_1r_2r_3 + z_3r_1r_2 + z_3z_2r_1 + z_3z_1r_2 + z_1z_2r_3 , z_1z_2z_3)$$

Andererseits:

$$(r_1,z_1)((r_2,z_2)(r_3,z_3)) = (r_1,z_1)(r_2r_3 + z_3r_2 + z_2r_3 , z_2z_3)$$

$$= (r_1(r_2r_3+z_3r_2+z_2r_3) + z_2z_3r_1 + z_1(r_2r_3+z_3r_2+z_2r_3) , z_1z_2z_3)$$

$$= (r_1r_2r_3 + z_3r_1r_2 + z_2r_1r_3 + z_2z_3r_1 + z_1r_2r_3 + z_1z_3r_2 + z_1z_2r_3 , z_1z_2z_3)$$

$\Rightarrow$ assoziativ.

Insgesamt: $(R \times \mathbb{Z}, +, \cdot)$ ist ein Ring mit Eins.

(β) • Definiere $\varphi: R \to R \times \mathbb{Z}$, $r \mapsto (r,0)$ $\Rightarrow \varphi$ injektiv.

Es gilt:

$$\varphi(r+s) = (r+s,0) = (r,0)+(s,0) = \varphi(r)+\varphi(s)$$

$$\varphi(r\cdot s) = (r\cdot s, 0) = (r\cdot s + 0\cdot r + 0\cdot s, 0\cdot 0)$$
$$= (r,0)\cdot(s,0) = \varphi(r)\cdot\varphi(s)$$

$\Rightarrow \varphi$ ist Homomorphismus

• Ist $1 \in R$ die Eins, dann:

$$\varphi(1) = (1,0) \neq (0,1) = E \quad (\text{Eins in } R\times\mathbb{Z})$$

(ii) Sei R ein Ring mit Eins 1.

Betrachte den Ring $R\times R$ (Komponentenweise Verknüpfungen)

$\Rightarrow R \cong R\times\{0\}$, d.h. $(1,0)$ ist Eins in $R\times\{0\} \subset R\times R$.

Aber: In $R\times R$ ist $(1,1) \neq (1,0)$ die Eins.

∎

<u>10.2.</u> (i) N_E sei die Menge der Nichteinheiten.

- N_E sei Ideal.

  $\Rightarrow \forall a \in R \setminus N_E$ gilt: a ist Einheit.

  $\Rightarrow (N_E, a) \overset{VL}{=} R \quad \forall a \in R \setminus N_E$

  $\Rightarrow N_E$ ist ein maximales Ideal

  Ist $J \subset R$ ein Ideal mit $J \not\subset N_E$, so $\exists\, b \in J$ mit $b \notin N_E$.

  $\Rightarrow b$ ist Einheit $\Rightarrow J = R$ also nicht maximal.

  $\Rightarrow N_E$ ist einziges maximales Ideal in R

  $\Rightarrow R$ ist lokaler Ring.

- R sei lokaler Ring, maximales Ideal sei M.

  Sei $a \in R \setminus M$ beliebig.

  $\nearrow (a) \neq R \overset{VL}{\Rightarrow} \exists$ maximales Ideal $J \subset R$ mit $(a) \subset J$, d.h. $a \in J$. Da M einziges maximales Ideal in R ist, folgt $J = M$, d.h. $a \in M$ $\lightning_{a \in R \setminus M}$

  $\Rightarrow (a) = R \overset{VL}{\Rightarrow} a$ ist Einheit.

  Also: Alle $a \in R \setminus M$ sind Einheiten.

  Andererseits enthält M wegen $M \neq R$ keine Einheiten.

  $\Rightarrow N_E = M$, also ist N_E ein Ideal.

(ii) Aus Vorlesung bekannt:

Ist $\varphi: R_1 \to R_2$ Ringhomomorphismus und $J_2 \subset R_2$ Ideal, so ist auch $\varphi^{-1}(J_2) \subset R_1$ Ideal.

Ist φ surjektiv und $J_1 \subset R_1$ Ideal, dann ist auch $\varphi(J_1) \subset R_2$ Ideal und offenbar gilt:

$$J_1 \subset J_2 \subset R \Rightarrow \varphi(J_1) \subset \varphi(J_2).$$

Damit zur Aufgabe. Betrachte kanonische Projektion

$$\pi: R \to R/\mathfrak{a}$$

Ist $J \subset R/\mathfrak{a}$ Ideal, dann folgt:

$\pi^{-1}(J)$ Ideal in R. Bezeichne M das maximale Ideal in R.

$\overset{VL}{\Longrightarrow}$ $\pi^{-1}(J) \subset M$

$\overset{\pi \text{ surj.}}{\Longrightarrow}$ $J = \pi(\pi^{-1}(J)) \subset \pi(M) =: M/\mathfrak{a}$ und $M/\mathfrak{a} \subset R/\mathfrak{a}$ ist Ideal.

Also: Alle Ideale $J \subset R/\mathfrak{a}$ sind in $M/\mathfrak{a}$ enthalten

$M/\mathfrak{a}$ ist maximales Ideal, denn $M/\mathfrak{a} \subset I$, I maximales Ideal

$$\Rightarrow I \subset M/\mathfrak{a} \Rightarrow M/\mathfrak{a} = I.$$

Also: $M/\mathfrak{a}$ ist das einzige maximale Ideal in $R/\mathfrak{a}$

$\Rightarrow R/\mathfrak{a}$ ist lokaler Ring. ∎

10.3. Vorab: $S = \mathbb{Z} \setminus (p)$ ist multiplikativ abgeschlossen ($S \neq \emptyset$ ist klar). Dazu:

$$a \in (p) \Leftrightarrow a = b \cdot p \text{ für ein } b \in \mathbb{Z}$$
$$\Leftrightarrow p \mid a.$$

Sind $x, y \in S \Rightarrow p \nmid x,\ p \nmid y$

$$\overset{p \text{ Primzahl}}{\Longrightarrow} p \nmid x \cdot y$$
$$\Rightarrow x \cdot y \in S.$$

Also: Können Quotientenring $\mathbb{Z}_{(p)} := \mathbb{Z}_S$ betrachten.
Elemente in $\mathbb{Z}_{(p)}$ sind von der Form

$$\frac{a}{b} \quad \text{mit } a, b \in \mathbb{Z},\ p \nmid b.$$

(wobei wir $\frac{a}{b} := [(a,b)]$ mit $(a,b) \in \mathbb{Z} \times S$ schreiben).

Damit zur Aufgabe:

(i) (α) Einheiten in $\mathbb{Z}$ sind $\{+1, -1\}$. Damit sind die Einheiten in $\mathbb{Z}_{(p)}$ genau die $\frac{a}{b}$ mit $a \in S$, d.h. $p \nmid a$

(beachte: $+1, -1 \in S$ da (p) Primideal also $(p) \neq \mathbb{Z}$)

$\Rightarrow$ Die Nichteinheiten in $\mathbb{Z}_{(p)}$ sind genau die

$$\frac{a}{b} \in \mathbb{Z}_{(p)} \text{ mit } p \mid a \quad (\text{und } p \nmid b).$$

$\Rightarrow p \cdot \mathbb{Z}_{(p)} \subset \mathbb{Z}_{(p)}$ ist die Menge der Nichteinheiten

Wegen $p \cdot \mathbb{Z}_{(p)} = (p)$ (in $\mathbb{Z}_p$ gelesen) bilden diese ein

Ideal

$\overset{\text{Aufgabe 2}}{\Longrightarrow}$ $\mathbb{Z}_{(p)}$ ist lokaler Ring und $p \cdot \mathbb{Z}_{(p)}$ das (einzige) maximale Ideal (vgl. Beweis von 2 (i))

(β) Betrachte $\varphi : \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)}$, $n + p\mathbb{Z} \longmapsto n + p\mathbb{Z}_{(p)}$

(wobei wir $n \in \mathbb{Z}$ mit $\frac{n}{1} \in \mathbb{Z}_{(p)}$ identifizieren

- φ ist wohldefiniert:

$$n + p\mathbb{Z} = m + p\mathbb{Z} \Rightarrow n - m = p \cdot k \text{ für ein } k \in \mathbb{Z}.$$

$$\Rightarrow \frac{n}{1} - \frac{m}{1} = \frac{n-m}{1} = \frac{p \cdot k}{1} = p \cdot \frac{k}{1} \in p \cdot \mathbb{Z}_{(p)} \quad \text{ok.}$$

- φ ist Ringhomomorphismus:

$$\varphi((n + p\mathbb{Z}) + (m + p\mathbb{Z})) = \varphi((n+m) + p\mathbb{Z}) = (n+m) + p\mathbb{Z}_{(p)}$$

$$= (n + p\mathbb{Z}_{(p)}) + (m + \mathbb{Z}_{(p)})$$

$$= \varphi(n + p\mathbb{Z}) + \varphi(m + p\mathbb{Z}).$$

$$\varphi((n + p\mathbb{Z}) \cdot (m + p\mathbb{Z})) = \varphi((n \cdot m) + p\mathbb{Z}) = n \cdot m + p\mathbb{Z}_{(p)}$$

$$= (n + p\mathbb{Z}_{(p)})(m + p\mathbb{Z}_{(p)})$$

$$= \varphi(n + p\mathbb{Z}) \cdot \varphi(m + p\mathbb{Z}).$$

• φ ist injektiv:

$$\varphi(n+p\mathbb{Z}) = 0 + p\,\mathbb{Z}_{(p)}$$

$$\Leftrightarrow \quad n + p\,\mathbb{Z}_{(p)} = 0 + p\,\mathbb{Z}_{(p)}$$

$$\Leftrightarrow \quad n \in p\,\mathbb{Z}_{(p)}$$

$$\Leftrightarrow \quad n = p \cdot \underbrace{\frac{k}{l}}_{\in \mathbb{Z},\text{ da } n \in \mathbb{Z} \text{ und } p \nmid l} \qquad k, l \in \mathbb{Z},\ p \nmid l$$

$$\Leftrightarrow \quad n = p \cdot q \qquad \text{für ein } q \in \mathbb{Z}$$

$$\Leftrightarrow \quad n \in p\mathbb{Z}$$

$$\Leftrightarrow \quad n + p\mathbb{Z} = 0 + p\mathbb{Z}.$$

$$\Rightarrow \quad \operatorname{Kern} \varphi = \{0 + p\mathbb{Z}\} \quad \Rightarrow \quad \varphi \text{ injektiv.}$$

• φ ist surjektiv:

Sei $\frac{a}{b} \in \mathbb{Z}_{(p)}$ beliebig, d.h. $a \in \mathbb{Z}$, $b \in \mathbb{Z}$ mit $p \nmid b$.

Zunächst suchen wir ein $c \in \mathbb{Z}$ mit

$$\frac{a}{b} + \frac{c}{b} \cdot p \in \mathbb{Z}$$

$$\Leftrightarrow \quad a + cp \equiv 0 \mod b$$

$$\Leftrightarrow \quad cp \equiv -a \mod b \qquad (*)$$

Da p Primzahl und $p \nmid b$ folgt:

$$ggT(p, b) = 1$$

$\overset{VL}{\Longrightarrow}$ $\exists\, K, l \in \mathbb{Z}$ mit $K \cdot p + l \cdot b = 1$

$\Rightarrow$ $\exists\, K \in \mathbb{Z}$ mit $K \cdot p \equiv 1 \mod b$

Wähle $c := -K \cdot a \in \mathbb{Z}$.

$\Rightarrow$ $c \equiv -K \cdot a \mod b$

$\Rightarrow$ $c \cdot p \equiv -\underbrace{K \cdot p}_{\equiv 1 \bmod b} \cdot a \mod b$

$\Rightarrow$ $c \cdot p \equiv -a \mod b$.

Also: Dieses c erfüllt $(*)$ und damit gilt

$$\frac{a}{b} + \frac{c}{b} \cdot p \in \mathbb{Z} \qquad \text{(siehe oben).} \qquad (**)$$

Setze $z := \frac{a}{b} + \frac{c}{b} \cdot p \in \mathbb{Z}$

$\Rightarrow$ $\frac{a}{b} \equiv z \mod p\,\mathbb{Z}_{(p)}$ (Können Gleichung $(**)$ in $\mathbb{Z}_{(p)}$ lesen)

$\Rightarrow$ $\varphi(z + p\mathbb{Z}) = z + p\,\mathbb{Z}_{(p)} = \frac{a}{b} + p\,\mathbb{Z}_{(p)}$.

$\Rightarrow$ φ surjektiv (da Repräsentant $\frac{a}{b} \in \mathbb{Z}_{(p)}$ beliebig war).

(ii) Suchen $v \in \{0,1,2,3,4\}$ mit $\overline{v} = \frac{1}{3} + \frac{1}{4}$.

Es ist

$$\overline{\frac{1}{3}} + \overline{\frac{1}{4}} = \overline{\frac{7}{12}} \qquad \text{(beachte: } 3,4 \notin (5)\text{)}$$

Außerdem:

$$\overline{\frac{7}{12}} + 5 \cdot \overline{\frac{1}{12}} = \overline{1}$$

$$\Rightarrow \overline{\frac{1}{3}} + \overline{\frac{1}{4}} \equiv \overline{1} \mod 5 \cdot \mathbb{Z}_{(5)}$$

Also: Wähle $v = 1$.

$\blacksquare$

10.4. (i) Zeigen zunächst: 2 ist irreduzibel in $\mathbb{Z}[\sqrt{-5}]$.

Gelte $(a+b\sqrt{-5})(c+d\sqrt{-5}) = 2$

für $a, b, c, d \in \mathbb{Z}$

$$\Rightarrow \quad ac + ad\sqrt{-5} + bc\sqrt{-5} - 5bd = 2$$

$$\Rightarrow \quad ac + (ad+bc)\sqrt{-5} - 5bd = 2$$

$\Rightarrow \quad ad + bc = 0.$ und $ac - 5bd = 2$

Betrachte $(a - b\sqrt{-5})(c - d\sqrt{-5})$

$$= ac - ad\sqrt{-5} - bc\sqrt{-5} - 5bd$$

$$= ac - \underbrace{(ad+bc)}_{=0}\sqrt{-5} - 5bd$$

$$= ac - 5bd$$

$$\overset{\text{s.o.}}{=} 2$$

$$\Rightarrow \quad \underbrace{(a+b\sqrt{-5})(a-b\sqrt{-5})}_{= a^2 - (b\sqrt{-5})^2 = a^2 + 5b^2}(c+d\sqrt{-5})(c-d\sqrt{-5}) = 4$$

$\Rightarrow \quad a^2 + 5b^2 \mid 4$ d.h. $a^2 + 5b^2 \in \{1, 2, 4\}$

nicht möglich

$\Rightarrow$ $b = 0$ und $a \in \{1, -1, 2, -2\}$

2 besitzt also in $\mathbb{Z}[\sqrt{-5}]$ nur triviale Teiler

$\Rightarrow$ 2 ist irreduzibel

↯ Y wäre Hauptideal

$$\overset{2 \in Y}{\underset{\text{irreduzibel}}{\Longrightarrow}} \quad Y = (2)$$

Aber: $1+\sqrt{-5} \in Y$ und $2(a+b\sqrt{-5}) = 1+\sqrt{-5}$
nicht mit $a,b \in \mathbb{Z}$ lösbar ↯

(ii) Zeigen: $\mathbb{Z}[\sqrt{-5}]/Y$ ist Körper ($\overset{VL}{\Leftrightarrow}$ Y maximales Ideal)

Wegen $Y = (2, 1+\sqrt{-5})$ werden in $\mathbb{Z}[\sqrt{-5}]/Y$ alle geraden Zahlen mit 0 und alle ungeraden Zahlen mit 1 identifiziert. Da $1+\sqrt{-5} \in Y$ ist, wird $\sqrt{-5}$ mit -1 und damit mit 1 identifiziert.

Also: $a+b\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ wird mit $a+b$, $a,b \in \{0,1\}$ identifiziert.

$$\Longrightarrow \mathbb{Z}[\sqrt{-5}]/Y = \{[0],[1]\}$$

$\left([1]\cdot[1] = [\underset{\text{in } \mathbb{Z}[\sqrt{-5}]}{1\cdot 1}] = [1] \right.$

$\Rightarrow$ Multiplikation:

$\cdot$	$[0]$	$[1]$
$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$

$\left.\right)$

$$\overset{\text{Keine}}{\underset{\text{Wahl}}{\Longrightarrow}} \quad \mathbb{Z}[\sqrt{-5}]/Y \cong \underbrace{\mathbb{Z}/2\mathbb{Z}}_{\text{sogar Körper}} \quad \text{(als Ring.)}$$

$$\Rightarrow \mathbb{Z}[\sqrt{-5}]/Y \text{ ist Körper.}$$

∎