Aufgabe 1

Ein Polynom $f \in R[x]$ vom Grad 2 ist von der Form

$$ax^2 + bx + c$$

mit $a \neq 0$. Ist nun also $R = \mathbb{F}_2$, so muss bereits $a = \bar{1}$ sein und wir haben für b und c jeweils zwei Möglichkeiten.

Das liefert die Polynome

- $x^2 = x \cdot x$
- $x^2 + \bar{1} = (x + \bar{1}) \cdot (x + \bar{1})$
- $x^2 + x = x(x + \bar{1})$

nicht irreduzibel, da $x, x+\bar{1}$ keine Einheiten sind und

- $\underbrace{x^2 + x + 1}_{}$ $=: f$

hat keine Nullstellen in $\mathbb{F}_2$:

$f(\bar{0}) = \bar{1}$ und $f(\bar{1}) = \underbrace{\bar{1} + \bar{1}}_{= \bar{0}} + \bar{1} = \bar{1}$

Somit kann es hier keine Zerlegung in zwei Polynome kleineren Grades geben, sodass f irreduzibel sein muss.

Aufgabe 2

(i) Beh.: $(4,6) = (2)$:

Haben

- $2 = \underbrace{6-4}_{\in (4,6)} \in (4,6)$ und somit $(2) \subset (4,6)$
- $\underbrace{2}_{\in \mathbb{Z}} \cdot \underbrace{2}_{\in (2)} = 4$ und $\underbrace{3}_{\in \mathbb{Z}} \cdot \underbrace{2}_{\in (2)} = 6$ und somit $(4,6) \subset (2)$.

(ii) Beh.: $(3,29) = (1) = \mathbb{Z}[x]$

Da $1 = \underbrace{10}_{\in \mathbb{Z}[x]} \cdot \underbrace{3}_{\in (3,29)} - \underbrace{29}_{}$, ist $1 \in (3,29)$ und somit

$(3,29) = (1)$.

(iii) Beh.: Ist kein Hauptideal:

Ang., $(\bar{x}, \bar{y}) = (\bar{f})$ für ein $\bar{f} \in \underbrace{\mathbb{R}[x,y]/(xy)}$.

jedes Element hat eindeutigen Repräsentanten aus

$x\mathbb{R}[x] + y\mathbb{R}[y] + \mathbb{R}$

$\rightsquigarrow$ schreibe

$$\bar{g} = \underset{x\mathbb{R}[x]}{\underset{\cap}{g_x}} + \underset{y\mathbb{R}[y]}{\underset{\cap}{g_y}} + \underset{\mathbb{R}}{\underset{\cap}{g_c}}$$

für Elemente $\bar{g} \in \mathbb{R}[x,y]/(xy)$

Zunächst einmal muss $f_c = 0$ sein, da $(\bar{x}, \bar{y})$ sonst Repräsentanten mit konstantem Term hätte.

Da $(\bar{x}, \bar{y}) = (\bar{f})$, ex. also $\bar{g}, \bar{h} \in \mathbb{R}[x,y]/(xy)$ mit

$$\underbrace{(g_x + g_y + g_c)(f_x + f_y)}_{g_c f_x \, + \, (g_y + g_c) f_y} = \bar{g}\bar{f} = \bar{x}$$

Repräsentant nur aus $x\mathbb{R}[x]$

$$= g_x f_x + \underbrace{\qquad}_{\overset{!}{=} 0}$$

und

Repräsentant nur aus $y\mathbb{R}[y]$

$$\underbrace{(h_x + h_y + h_c)(f_x + f_y)} = \bar{h}\bar{f} = \bar{y}$$

$$= \underbrace{h_x f_x}_{\overset{!}{=} 0} + h_y f_y + \underbrace{h_c (f_x + f_y)}_{\overset{!}{=} 0}$$

$$= h_y f_y + h_c f_y + \underbrace{(h_x + h_c) f_x}_{\overset{!}{=} 0}$$

Wäre $f_y = 0$, so $\bar{h}\bar{f} = \bar{0}$ ↯ Also $f_y \neq 0$ und somit $g_y + g_c = 0$ (in $\mathbb{R}[y]$). Da $g_y \neq -g_c$ haben wir also $g_y = g_c = 0$.

Analog $f_x \neq 0$ und $h_x = h_c = 0$.

Somit $\underbrace{\tilde{g}_x \bar{f}_x}_{\in x\mathbb{R}[x]} = \bar{x}$ ↯

(Grad von Produkt also zu hoch)

Also ist $(\bar{x}, \bar{y}) \subset \mathbb{R}[x,y]/(xy)$ kein Hauptideal.

(iv) Beh.: $\left(\frac{xy^2+1}{x}, ix\right) = (1) = \mathbb{C}(x)[y]$

Da $ix \in \mathbb{C}(x)^\times$, ist $1 \in \left(\frac{xy+1}{x}, ix\right)$ und wir sind fertig.

(v) Beh.: Ist kein Hauptideal:

Ang., $\underbrace{\{f \in \mathbb{Z}[x] \mid 2 \text{ teilt } f(0)\}}_{=:\mathfrak{a}} = (g)$ für ein $g \in \mathbb{Z}[x]$. Dann ex. $h \in \mathbb{Z}[x]$ mit

$$2 = hg,$$

sodass die Gradformel $\deg(g) = 0$ liefert. Also $g \in 2\mathbb{Z} \subset \mathbb{Z}[x]$. Somit $x \notin (g)$, aber $\underbrace{x \in \mathfrak{a}}_{\text{da } 2 | 0}$. ↯

Aufgabe 3

(i)

Es ex. $g, g' \in R[x]$ mit $gf = r$ und $g'f = x$, sodass wir

$$0 = \deg(r) = \deg(g) + \deg(f)$$

und

$$1 = \deg(x) = \deg(g') + \deg(f)$$

erhalten. Also ist $\deg(f) = 0$ (und $\deg(g') = 1$).

(ii)

Schreibe $g' = ax + b$ mit $a, b \in R$ (geht aufgrund von $\deg(g') = 1$). Dann haben wir also

$$x = g'f = afx + bf$$

und somit $af = 1$. Das Element $f \in R[x]$ ist also eine Einheit und somit aus $R^\times$.

(iii)

Da $f \in R^\times$, ist $(r, x) = (f) = R[x]$. Es ex. also $h, h' \in R[x]$ mit

$$1 = hr + h'x.$$

Schreiben wir $h = \sum_{i=0}^{n} a_i x^i$, so gilt

$$1 = ev_0(1) = ev_0(hr + h'x) = a_0 r,$$

wobei $ev_0 : R[x] \to R$ die Evaluation an $0 \in R$ ist. Also ist r eine Einheit von R und R somit ein Körper.

(iv)

Sei $R[x_i \mid i \in I]$ ein Polynomring mit $|I| \geq 2$. Wäre dies ein Hauptidealring, so müsste man nach (i) – (iii) der Ring $R[x_i \mid i \in I \setminus \{i_0\}]$ für ein festes $i_0 \in I$ ein Körper sein. Da $|I| \geq 2$, müssten dann also insbesondere die übrigen Unbestimmten invertierbar sein $\lightning$

zB via Grad...

Aufgabe 4

(i)

Als Unterring des integren Ringes $\mathbb{R}$ ist R selbst wieder integer.

(ii)

Sei $u \in R^\times$. Dann erhalten wir

$$1 = N(1) = N(uu^{-1}) = N(u)\,N(u^{-1})$$

vermöge des Hinweises und somit $N(u) = 1$ (da [redacted] $N(u), N(u^{-1}) \in \mathbb{N}$). Nun [redacted] ist

$$N(a+b\sqrt{5}) = a^2 + \underbrace{5b^2}_{=0 \text{ oder } \geq 5} = 1$$

genau dann, wenn $a^2 = 1$ und $b^2 = 0$ sind. Somit können nur $\pm 1 \in R^*$ Einheiten sein. Da sie offenbar auch Einheiten sind, ist also $R^\times = \{\pm 1\}$.

(iii)

In R haben wir

$$6 = 2 \cdot 3$$

und

$$6 = (1+\sqrt{-5})(1-\sqrt{-5}).$$

[redacted] Sind $2, 3, 1 \pm \sqrt{-5} \in R$ irreduzibel, so wären dies also zwei verschiedene Primfaktorzerlegungen nach (ii).

Angenommen, es ex. $r, r' \in R \setminus R^\times = R \setminus \{\pm 1\}$ mit $2 = r \cdot r'$. Dann erhalten wir

$$4 = N(2) = N(\cancel{r}\cdot r') = \underbrace{N(r)}_{\neq 1} \cdot \underbrace{N(r')}_{\neq 1}$$

$\neq 1$, da $r, r' \notin$ [redacted] $\{\pm 1\}$

und somit $N(r) = 2 = N(r')$. Schreiben wir $r = a + b\sqrt{-5}$ mit $a, b \in \mathbb{Z}$, so muss also

$$\underbrace{a^2}_{\in\{0,1,4,\dots\}} + \underbrace{5b^2}_{=0 \text{ oder } \geq 5} = 2$$

sein. Das kann nicht sein. Somit ist $2 \in R$ irreduzibel. Analog [redacted] kann man auch für $3 \in R$ argumentieren.

Angenommen, $1 \pm \sqrt{-5} = r \cdot r'$ mit $r, r' \in R \setminus \{\pm 1\}$.

Dann erhalten wir

$$6 = N(1 \pm \sqrt{-5}) = N(r \cdot r') = \underbrace{N(r) \cdot N(r')}_{\neq 1, \text{ da } r, r' \notin \{\pm 1\}}$$

und somit erneut $N(r) = 2$ oder $N(r) = 3$ ↯

wie eben

Also sind all diese vier Elemente irreduzibel.