Aufgabe	A1	A2	A3	A4	A5	$\sum$
Punkte						

Aufgabe 1. (a) Sei $d \in \mathbb{Z}$. Beh.: $\mathbb{Z}[\sqrt{d}]$ ist der kleinste Unterring von $\mathbb{C}$, der $\sqrt{d}$ enthält.

Beweis. Durch Nachrechnen ist sofort offensichtlich, dass $\mathbb{Z}[\sqrt{d}]$ ein Unterring ist, der $\sqrt{d}$ enthält. Sei nun $R \subseteq \mathbb{C}$ ein Unterring mit $\sqrt{d} \in R$. Dann ist $\mathbb{Z} \ni 1 \in R$, da R Unterring, d.h. durch Addition der 1 folgt $\mathbb{Z} \subseteq R$. Sei nun $x \in \mathbb{Z}[\sqrt{d}]$. Dann ex. $a, b \in \mathbb{Z}$ mit $x = a + b\sqrt{d}$. Da $a, b, \sqrt{d} \in R$ folgt, da R Unterring, dass auch $x \in R$, also $\mathbb{Z}[\sqrt{d}] \subseteq R$. □

(b) Sei $d = -5$. Beh.: N ist multiplikativ.

Beweis. Seien $x, y \in \mathbb{Z}[\sqrt{-5}]$. Dann ex. $a, b, e, f \in \mathbb{Z}$, s.d. $x = a + b\sqrt{-5}$ und $y = e + f\sqrt{-5}$. Damit folgt direkt

$$\begin{aligned} N(xy) &= N(ae - 5bf + (af + be)\sqrt{-5}) \\ &= (ae - 5bf)^2 + 5(af + be)^2 \\ &= a^2e^2 + 25b^2f^2 + 5a^2f^2 + 5b^2e^2 \\ &= (a^2 + 5b^2)(e^2 + 5f^2) \\ &= N(x)N(y). \end{aligned}$$

□

Beh.: Für $u \in \mathbb{Z}[\sqrt{-5}]$ gilt $u \in \mathbb{Z}[\sqrt{-5}]^x \iff N(u) = 1$.

Beweis. Sei $u \in \mathbb{Z}[\sqrt{-5}]$. „ $\Longrightarrow$ ": Sei $u \in \mathbb{Z}[\sqrt{-5}]^\times$. Dann ex. $v \in \mathbb{Z}[\sqrt{-5}]$, s.d. $uv = 1$. Damit folgt wegen N multiplikativ

$$1 = N(1) = N(uv) = \underbrace{N(u)}_{\in \mathbb{Z}_{\geq 0}} \underbrace{N(v)}_{\in \mathbb{Z}_{\geq 0}}.$$

Es folgt also $N(u) = 1$.

„ $\Longleftarrow$ ": Sei $N(u) = 1$. Es ex. $a, b \in \mathbb{Z}$, s.d. $u = a + b\sqrt{-5}$. Wegen

$$1 = N(u) = N(a + b\sqrt{-5}) = a^2 + 5b^2$$

folgt $b = 0$ und damit $a^2 = 1$, also $u = a$ mit $u^2 = 1$, also $u \in \mathbb{Z}[\sqrt{-5}]^\times$. □

Beh.: $\mathbb{Z}[\sqrt{-5}]^\times = \{\pm 1\}$.

Beweis. Sei $u \in \mathbb{Z}[\sqrt{-5}]$ mit $u = a + b\sqrt{-5}$ für $a, b \in \mathbb{Z}$. Dann ist

$$\begin{aligned} N(u) = 1 &\iff a^2 + 5b^2 = 1 \\ &\iff a^2 = 1 \wedge b = 0 \\ &\iff a \in \{\pm 1\} \wedge b = 0 \\ &\iff u \in \{\pm 1\}. \end{aligned}$$

Damit folgt die Behauptung mit der Vorüberlegung. □

(c) Beh.: $2 \in \mathbb{Z}[\sqrt{-5}]$ ist irreduzibel.

Beweis. Ang.: $\exists x, y \in \mathbb{Z}[\sqrt{-5}]$, s.d. $2 = xy$ mit $x, y \notin \mathbb{Z}[\sqrt{-5}]^\times$. Dann folgt

$$4 = N(2) = N(xy) = N(x)N(y).$$

Da $4 \neq 0 \implies N(x), N(y) \in \mathbb{N}$ und wegen $x, y \notin \mathbb{Z}[\sqrt{-5}]^\times$, ist $N(x), N(y) \neq 1$, also $N(x) = N(y) = 2$. Das heißt es ex. $a, b \in \mathbb{Z}$, s.d $N(a + b\sqrt{-5}) = 2$. Dann folgt $a^2 + 5b^2 = 2$, also $b = 0$ (sonst $a^2 + 5b^2 \geq 5 > 2$). Damit ist $a^2 = 2 \implies \sqrt{2} \in \mathbb{Z}$ ↯. □

Beh.: $\mathbb{Z}[\sqrt{-5}]$ nicht faktoriell.

Beweis. Es gilt

$$2 \cdot 3 = 6 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

Aber $2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$ irreduzibel, also hat 6 zwei verschiedene Darstellungen als Produkt von irreduziblen Elementen. Damit ist $\mathbb{Z}[\sqrt{-5}]$ nicht faktoriell. □

Aufgabe 2. Sei $(*)$: Für R Ring, ex. ein $n \in \mathbb{N}_{\geq 2}$, s.d. $x^n = x$ für alle $x \in R$.

(a) Beh.: Endliche nullteilerfreie Ringe R sind Körper.

Beweis. Sei R nullteilerfreier, endlicher Ring. Zunächst ist $R \neq 0$, da R nullteilerfrei. Sei nun $x \in R \setminus \{0\}$. Dann betrachte $f_x \colon R \to R, y \mapsto xy$. Es ist f_x injektiv, denn für $y_1, y_2 \in R$ folgt

$$f_x(y_1) = f_x(y_2) \implies xy_1 = xy_2 \overset{R \text{ nullteilerfrei}, x \neq 0}{\implies} x(y_1 - y_2) = 0 \implies y_1 = y_2.$$

Da R endlich ist f_x auch surjektiv, inbes. ex. ein $y \in R$, s.d $f_x(y) = 1 \implies xy = 1$, also $x \in R^x$. Insgesamt also $R^x = R \setminus \{0\}$. □

(b) Beh.: R nullteilerfrei mit $(*) \implies R$ endlicher Körper.

Beweis. Sei $x \in R \setminus \{0\}$. Wegen $n \geq 2$ ist $n - 2 \geq 0$. Es gilt

$$x^n = x \implies x^{n-1}x = x.$$

Da $x \neq 0$ und R nullteilerfrei, folgt $x^{n-1} = 1$. Damit ist

$$x^{n-2}x = 1 \implies x \in R^x.$$

□

(c) Beh.: Jedes Primideal in R mit $(*)$ ist maximal.

Beweis. Sei $I \subsetneq R$ Primideal. Dann sei $\overline{x} \in R/I$. Dann ist $\overline{x}^n = \overline{x^n} = \overline{x}$, wegen $(*)$. Da I Primideal, ist R/I nullteilerfrei mit Eigenschaft $(*)$. Mit (b) ist R/I also Körper, also I Maximalideal. □

Aufgabe 3. Zunächst sind Polynome vom Grad 1 immer irreduzibel über $\mathbb{F}_2[X]$, da $\mathbb{F}_2$ nullteilerfrei und damit auch $\mathbb{F}_2[X]$ nullteilerfrei. Damit folgt für ein $f \in \mathbb{F}_2[X]$ mit $\deg(f) = 1$ und $f = gh$ für $g, h \in \mathbb{F}_2[\mathrm{X}]$, dass

$$1 = \deg(f) = \deg(gh) = \deg(g) + \deg(h).$$

Da $\deg(f) = 1$ ist $g, h \neq 0$, also $\deg(g), \deg(h) \geq 0$ und damit $\deg(g) = 0$ oder $\deg(h) = 0$. Da $\mathbb{F}_2$ Körper ist damit $g \in \mathbb{F}_2[X]^\times$ oder $h \in \mathbb{F}_2[X]^\times$, also f irreduzibel.

Da $\mathbb{F}_2$ Körper sind zudem alle Polynome vom Grad 0 Einheiten also nicht irreduzibel.

Weiter ist $\#\mathbb{F}_2 = 2$, also existieren genau 2^k paarweise verschiedene Polynome vom Grad k, für $k \geq 0$. Da $\mathbb{F}_2$ Körper, ist $\mathbb{F}_2$ HIR, also faktoriell und nach Satz von Gauß ist auch $\mathbb{F}_2[X]$ faktoriell. Das heißt die irreduziblen Polynome sind diejenigen die nicht als Produkt von irreduziblen Polynomen enstehen. Damit sind also

$$f_1 \coloneqq X$$
$$f_2 \coloneqq X + 1$$

alle Polynome vom Grad 1 und irreduzibel. Daraus entstehen als Produkte die Polynome

$$f_3 \coloneqq X^2 = X \cdot X$$
$$f_4 \coloneqq X^2 + X = X(X + 1)$$
$$f_5 \coloneqq X^2 + 1 = (X + 1)^2$$

Es bleibt als viertes Polynom vom Grad 2 nur

$$f_6 \coloneqq X^2 + X + 1$$

das damit irreduzibel sein muss. Aus den irreduziblen Polynome vom Grad ≤ 2 ergeben sich

$$\begin{aligned} f_7 &\coloneqq X^3 \\ f_8 &\coloneqq X^3 + X^2 = X^2(X+1) \\ f_9 &\coloneqq X^3 + X^2 + X = X(X^2 + X + 1) \\ f_{10} &\coloneqq X^3 + X^2 + X + 1 = (X+1)^3 \\ f_{11} &\coloneqq x^3 + X = X(X+1)^2 \\ f_{12} &\coloneqq X^3 + 1 = (X^2 + X + 1)(X+1) \end{aligned}$$

Damit bleiben als Polynome vom Grad 3 nur noch

$$\begin{aligned} f_{13} &\coloneqq X^3 + X^2 + 1 \\ f_{14} &\coloneqq X^3 + X + 1 \end{aligned}$$

die damit irreduzibel sein müssen. Damit sind alle irreduziblen Polynome vom Grad ≤ 3 in $\mathbb{F}_2[X]$ gegeben als

$$\{f_1, f_2, f_6, f_{13}, f_{14}\}.$$

Es existieren genau $2^4 = 16$ Polynome vom Grad 4 in $\mathbb{F}_2[X]$. Die reduziblen ergeben sich wieder als Produkte der irreduziblen Polynome vom Grad ≤ 3. Da sich die Grade bei Produktbildung addieren, treten folgende Kombinationen auf:

$$\begin{aligned} &\text{(i)} && 4 = 1+1+1+1 \\ &\text{(ii)} && 4 = 1+1+2 \\ &\text{(iii)} && 4 = 1+3 \\ &\text{(iv)} && 4 = 2+2. \end{aligned}$$

Die Anzahl der Kombinationen pro Fall ergibt sich durch Produktbildung der Möglichkeiten Polynome der entsprechenden Grade auszuwählen. Damit ergeben sich nach Ana I für (i) $\binom{2+4-1}{4} = 5$ Kombinationen, für (ii): $1 \cdot \binom{2+3-1}{2} = 3$, für (iii): $2 \cdot 2$ und für (iv): $1 \cdot 1 = 1$ Kombinationen. In Summe also $5 + 3 + 4 + 1 = 13$ reduzible Polynome, also $16 - 13 = 3$ irreduzible Polynome vom Grad 4.

Aufgabe 4. (a) $f = \frac{(X-1)^3}{1} \in Q(\mathbb{R}[X]) \implies v_{X-1}(f) = 3$ und $g = \frac{1}{(X-1)^2} \in Q(\mathbb{R}[X]) \implies v_{X-1}(g) = -2$. Folgt direkt aus der Definition.

(b) $X^2 + 1$ ist irreduzibel über $\mathbb{R}$, da $X^2 + 1$ keine Nullstellen in $\mathbb{R}$ hat.

(c) $(2, X)$ ist kein Hauptideal in $\mathbb{Z}[X]$.

Beweis. Ang. es ex. ein $f \in \mathbb{Z}[X]$ mit $(f) = (2, X)$, dann ex. $g \in \mathbb{Z}[X]$ mit $2 = fg$, da $\mathbb{Z}[X]$ nullteilerfrei, folgt mit Gradformel, dass $\deg(f) = 0$, also $f \in \mathbb{Z}$. Außerdem ex. ein $h \in \mathbb{Z}[X]$ mit $X = fh$. Dann ist $e(X) = 1 = e(f)e(g)$, also $f \in \mathbb{Z}^\times$. Damit ist $(f) = (2, X) = (1) = \mathbb{Z}$. Insbesondere ist $1 \in (2, X)$, d.h. es ex. $h, g \in \mathbb{Z}[X]$ mit

$$1 = 2h + Xg.$$

Es ist offensichtlich $h, g \neq 0$ also $\deg(2h + Xg) \geq 1 > 0 = \deg(1)$. ↯. □

(d) (X) in $\mathbb{Z}[X, Y]$. Es ist offensichtlich $(X) \subsetneq (X, Y) \subsetneq \mathbb{Z}[X, Y]$, denn $Y \notin (X)$ und $1 \notin \mathbb{Z}[X, Y]$. Da X irreduzibel über $\mathbb{Z}[X, Y]$ und $\mathbb{Z}[X, Y]$ faktoriell ist X auch Primelement also (X) Primideal, aber kein Maximalideal.

(e) $R = \mathbb{Z}[X, Y]$ und $a = X$, $b = Y$. Es ist $\mathrm{ggT}(X, Y) = 1$, da X, Y prim aber $1 \notin (X) + (Y)$, also $(X) + (Y) \neq (1)$.

(f) $K = Q(\mathbb{Z}/2\mathbb{Z}[X])$ ist Körper mit Charakteristik 2, denn $\frac{\overline{1}}{\overline{1}} = 1 \in Q(\mathbb{Z}/2\mathbb{Z}[X])$ und damit

$$1 + 1 = \frac{\overline{1}}{\overline{1}} + \frac{\overline{1}}{\overline{1}} = \frac{\overline{1} + \overline{1}}{\overline{1}} = \frac{\overline{0}}{\overline{1}} = 0 \in Q(\mathbb{Z}/2\mathbb{Z}[X]),$$

aber $Q(\mathbb{Z}/2\mathbb{Z}[X])$ unendlich, da $\mathbb{Z}/2\mathbb{Z}[X]$ Polynomring und hat damit unendlich viele Elemente, also auch $Q(\mathbb{Z}/2\mathbb{Z}[X])$.

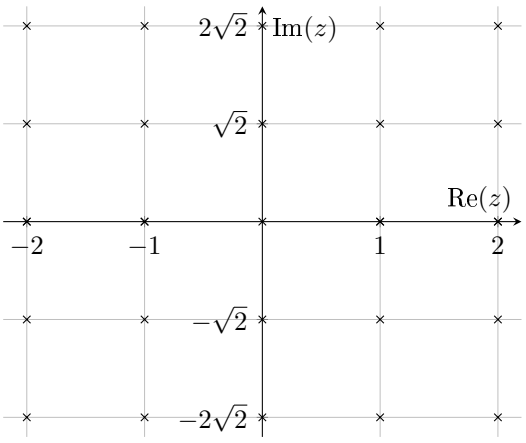

Abbildung 1: Ausschnitt von $\mathbb{Z}[\sqrt{-2}] \subseteq \mathbb{C}$ in der komplexen Ebene

Aufgabe 5. (a) Beh.: $\mathbb{Z}[\sqrt{-2}]$ euklidisch. Sei dazu $\mathrm{rd}\colon \mathbb{R} \to \mathbb{Z}$ die Rundungsfunktion. Bei zwei Möglichkeiten wähle die größere. Dann ist $\forall x \in \mathbb{R}\colon |x - \mathrm{rd}(x)| \leq \frac{1}{2}$.

Schritt 1: Sei zunächst $z \in \mathbb{C}$ mit $z = c + id$ mit $c, d \in \mathbb{R}$. Dann wähle $a = \mathrm{rd}(c)$ und $b = \mathrm{rd}(d)$. Dann ist $a + b\sqrt{-2} \in \mathbb{Z}[\sqrt{-2}]$ und

$$|z - (a + \sqrt{-2}b)| = |(c-a) + i\sqrt{2}(d-b)| = \sqrt{(c-a)^2 + 2(d-b)^2} = \sqrt{\frac{1}{4} + \frac{2}{4}} = \frac{\sqrt{3}}{2} < 1.$$

Schritt 2: $\mathbb{Z}[\sqrt{-2}]$ ist nullteilerfrei.

Schritt 3: Seien nun $z, w \in \mathbb{Z}[\sqrt{-2}]$ mit $w \neq 0$. Dann ist $\frac{z}{w} \in C$ und es ex. nach Schritt 1 ein $q \in \mathbb{Z}[\sqrt{-2}]$ mit $\left|\frac{z}{w} - q\right| \leq \frac{\sqrt{3}}{2}$. Dann setze $r := z - qw$. Dann gilt, da der komplexe Betrag multiplikativ ist:

$$N(r) = N(z - qw) = |z - qw|^2 = |\frac{z}{w} - q|^2 |w|^2 \leq \frac{3}{4} N(w) < N(w).$$

Damit ist $\mathbb{Z}[\sqrt{-2}]$ euklidisch mit der Normfunktion N.

(b) Beh.: $\mathbb{Z}[\sqrt{-2}]^\times = \{\pm 1\}$

Beweis. Es ist schnell nachgerechnet, dass N multiplikativ ist. Wende dann das exakt selbe Argument wie in 1(b) an. □