Aufgabe 1

gegeben: Polynome $f, g \in \mathbb{Q}[x]$:

$$f = x^3 + 2x^2 - 2x - 1,$$

$$g = x^2 + x - 2$$

Untersuchung der Polynome:

Nullstellen von g in $\mathbb{Q}$: 1,-2
Faktorisierung: $g = (x-1)(x+2)$

Nullstellen von f in $\mathbb{Q}$: 1
Faktorisierung: $f = (x-1)(x^2+3x+1)$
(Sonst nur noch zusätzliche 2 Nullstellen in $\mathbb{C}$)

- größter gemeinsamer Teiler d:

  Nach der Faktorisierung ist ein größter gemeinsame Teiler $\boxed{d = x - 1}$. Größte gemeinsame Teiler sind natürlich auch die zu d assoziierten, also skalare Vielfache von d.

  Zur Kontrolle:

$$\begin{aligned} x^3 + 2x^2 - 2x - 1 &= \big(x^2 + x - 2\big) \cdot \big(x + 1\big) + \big(-x + 1\big) \\ x^2 + x - 2 &= \big(-x + 1\big) \cdot \big(-x - 2\big) + 0 \end{aligned}$$

  Division mit Rest $\frac{x^3+2x^2-2x-1}{x^2+x-2}$:

$$\begin{array}{r|l} & \phantom{-x^3 - x^2 + {}} x + 1 \\ \hline x^2 + x - 2 & x^3 + 2x^2 - 2x - 1 \\ & -x^3 - x^2 + 2x \\ \hline & \phantom{-x^3 - {}} x^2 \phantom{{}- 2x} - 1 \\ & - x^2 - x + 2 \\ \hline & - x + 1 \end{array}$$

  Division mit Rest $\frac{x^2+x-2}{x-1}$:

$$
\begin{array}{r|l}
 & x + 2 \\
\hline
x - 1 & x^2 + x - 2 \\
 & -x^2 + x \\
\hline
 & 2x - 2 \\
 & -2x + 2 \\
\hline
 & 0
\end{array}
$$

Das von f, g erzeugte Ideal ist also $(f, g) = (d) = (x - 1)$.

- $(f, g) = (x - 1)$ ist ein Hauptideal,

  denn das von f und g erzeugte Ideal wird von einem Element $d = x - 1$ erzeugt. Weiterhin ist ja bekanntlich ein Polynomring über einem Körper ein Hauptidealring, also muß (f, g) ein Hauptideal sein.

- $(f, g) = (x - 1)$ ist ein Primideal,

  denn $d = x - 1$ ist irreduzibel in $\mathbb{Q}[x], \deg(d) = 1$. In $\mathbb{Q}[x]$ sind die Primideale die Ideale (0) und (p) mit $p \in \mathbb{Q}[x]$ irreduzibel, $\deg(p) > 0$.

- $(f, g) = (x - 1)$ ist ein maximales Ideal,

  denn $d = x - 1$ ist irreduzibel in $\mathbb{Q}[x], \deg(d) = 1$. In $\mathbb{Q}[x]$ sind die maximalen Ideale die Ideale (p) mit $p \in \mathbb{Q}[x]$ irreduzibel, $\deg(p) > 0$.

Aufgabe 3

1. zu zeigen: $\mathbb{Z}[\sqrt{n}]$ ist ein kommutativer und assoziativer Ring mit 1.

   Nach Definition ist $\mathbb{Z}[\sqrt{n}] = \{f(\sqrt{n}) \mid f \in \mathbb{Z}[x]\}$.

   Ich zeige, daß $R := \{a + b\sqrt{n} \mid a, b \in \mathbb{Z}\}$ ein Unterring von $\mathbb{C}$ ist.

   Offenbar sind $0 = 0 + 0\sqrt{n}, 1 = 1 + 0\sqrt{n}, \sqrt{n} = 0 + 1\sqrt{n} \in R$.

   Die Differenz zweier Elemente von R ist auch wieder in R:

   $$(a_1 + b_1\sqrt{n}) - (a_2 + b_2\sqrt{n}) = (a_1 - a_2) + (b_1 - b_2)\sqrt{n} \in R.$$

   Das Produkt zweier Elemente von R ist auch wieder in R:

   $$(a_1 + b_1\sqrt{n}) \cdot (a_2 + b_2\sqrt{n}) = (a_1a_2 + nb_1b_2) + (a_1b_2 + b_1a_2)\sqrt{n} \in R.$$

   Folglich ist R ein Unterring von $\mathbb{C}$ mit $\sqrt{n} \in R$ und $\mathbb{Z} \subset R$.

   $\mathbb{Z}[\sqrt{n}]$ ist der kleinste Unterring von $\mathbb{C}$ mit letztgenannten Eigenschaften, also gilt $\mathbb{Z}[\sqrt{n}] \subset R$. Wegen $R \subset \mathbb{Z}[\sqrt{n}]$ folgt die Gleichheit $R = \mathbb{Z}[\sqrt{n}]$.

   $\mathbb{Z}[\sqrt{n}]$ ist also ein Unterring von $\mathbb{C}$, aus $\mathbb{C}$ übertragen sich die Eigenschaften der Assoziativität und Kommutativität, weiterhin das Einselement. Damit ist die Behauptung gezeigt.

2. gegeben: P sei das von 2 und $1 + \sqrt{-5}$ in $\mathbb{Z}[\sqrt{-5}]$ erzeugte Ideal.

   zu zeigen: P ist ein Primideal. Es ist das einzige Primideal, welches 2 enthält.

   Offensichtlich ist $P \neq (2)$, denn $1 + \sqrt{-5} \notin (2)$. Ich untersuche das Ideal P^2:

   Das Quadrat eines Ideals (a, b) ist gleich (a^2, ab, ba, b^2), wegen der Kommutativität hier also gleich (a^2, ab, b^2). In unserer Aufgabe also

   $$P^2 = (2, 1 + \sqrt{-5})^2 = (4, 2 + 2\sqrt{-5}, -4 + 2\sqrt{-5})$$
   $$= 2(2, 1 + \sqrt{-5}, -2 + \sqrt{-5}),$$
   $$-1 + \sqrt{-5} = (1 + \sqrt{-5}) - 2 \in P^2,$$
   $$P^2 = 2(2, 1 + \sqrt{-5}) = 2P.$$

   Ich betrachte den Quotientenring $\mathbb{Z}[\sqrt{-5}]/P$. P ist echtes Ideal, sonst wäre P=(1), was schon im Widerspruch zu $P^2 = 2P$ steht, denn das bedeutete $(1) = (2)$, 2 ist keine Einheit in $\mathbb{Z}[\sqrt{-5}]$. In $\mathbb{Z}[\sqrt{-5}]/P$ haben wir $2 \equiv 0 \bmod P$, $\mathbb{Z}[\sqrt{-5}]/P$ ist ein Ring mit Charakteristik 2 ($P \neq 1$). Weiterhin ist $1 + \sqrt{-5} \equiv 0 \bmod P$, $\sqrt{-5} \equiv -1 \equiv 1 \bmod P$.

Ich folgere für beliebige $a, b \in \mathbb{Z}$:

$$a + b\sqrt{-5} \equiv a + b \bmod P,$$

$\mathbb{Z}[\sqrt{-5}]/P$ hat Charakterisitik 2 und ist isomorph zu $\mathbb{Z}/2\mathbb{Z}$. Da dies ein Körper ist, ist P nach Satz 6.6. Vorlesung maximal, und insbesondere prim.

Sei I ein Primideal, welches 2 enthält, also $(2) \subset I$. Wegen $P^2 = 2P$, und $2P \subset (2) \subset I$ folgt $P \subset I$, und da P maximal ist, folgt $P = I$. Deshalb ist P das einzige Primideal, welches 2 enthält.

Aufgabe 4

1. zu zeigen: Die Abbildung

$$\begin{aligned} N : \mathbb{Z}[\sqrt{2}] &\to \mathbb{Z} \\ a + b\sqrt{2} &\mapsto a^2 - 2b^2 \end{aligned}$$

   ist multiplikativ.

   Ich bezeichne das „Konjugierte“ zu $x = a + b\sqrt{2}$ mit $\overline{x} = a - b\sqrt{2}$.

   Sei $y := c + d\sqrt{2}$. Wir haben

$$\begin{aligned} \overline{xy} &= \overline{(a + b\sqrt{2})(c + d\sqrt{2})} \\ &= \overline{ac + 2bd + (ad + bc)\sqrt{2}} \\ &= ac + 2bd - (ad + bc)\sqrt{2} \\ &= (a - b\sqrt{2})(c - d\sqrt{2}) \\ &= \overline{(a + b\sqrt{2})}\ \overline{(c + d\sqrt{2})} \\ &= \overline{x}\ \overline{y}. \end{aligned}$$

Weiterhin ist

$$N(x) = N(a + b\sqrt{2}) = a^2 - 2b^2 = (a + b\sqrt{2})(a - b\sqrt{2}) = x\overline{x},$$

somit

$$\begin{aligned} N(xy) &= (xy)(\overline{xy}) = (xy)(\overline{x}\ \overline{y}) \\ &= (x\overline{x})(y\overline{y}) \\ &= N(x)N(y), \end{aligned}$$

die Abbildung ist multiplikativ.

Oder direkter:

$$\begin{aligned} N(x)N(y) &= (a^2 - 2b^2)(c^2 - 2d^2) \\ &= a^2c^2 - 2b^2c^2 - 2a^2d^2 + 4b^2d^2, \\ N(xy) = N((a + b\sqrt{2})(c + d\sqrt{2})) &= N(ac + 2bd + ad\sqrt{2} + bc\sqrt{2}) \\ &= (ac + 2bd)^2 - 2(ad + bc)^2 \\ &= a^2c^2 + 4b^2d^2 + 4abcd - 2a^2d^2 - 2b^2c^2 - 4abcd \\ &= a^2c^2 + 4b^2d^2 - 2a^2d^2 - 2b^2c^2, \end{aligned}$$

die Terme stimmen überein, die Abbildung ist multiplikativ.

2. zu zeigen: $a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]^* \quad \Leftrightarrow \quad N(a + b\sqrt{2}) = \pm 1$

„ $\Rightarrow$ “ : Sei $x \in \mathbb{Z}[\sqrt{2}]^* \;\; \Rightarrow$ es existiert ein $y \in \mathbb{Z}[\sqrt{2}]$ mit $xy = 1 \;\; \Rightarrow$ $N(xy) = N(1) = 1 \;\; \Rightarrow N(x)N(y) = N(xy) = 1$ wegen 1. $\Rightarrow$ $N(x) \in \mathbb{Z}^* \;\; \Rightarrow N(x) = \pm 1$.

„ $\Leftarrow$ “ : wenn $N(x) = 1 \;\; \Rightarrow \;\; x\overline{x} = 1 \;\; \Rightarrow x^{-1} = \overline{x} \;\; \Rightarrow x \in \mathbb{Z}[\sqrt{2}]^*$
wenn $N(x) = -1 \;\; \Rightarrow \;\; x\overline{x} = -1 \;\; \Rightarrow x^{-1} = -\overline{x} \;\; \Rightarrow x \in \mathbb{Z}[\sqrt{2}]^*$