Übungsblatt 5

Aufgabe 1. 1. Für $x = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ sei $\bar{x} := a - b\sqrt{d}$. Zeigen Sie, dass $N(x) = x\bar{x}$ für jedes $x \in \mathbb{Q}(\sqrt{d})$ gilt, und folgern Sie, dass N multiplikativ ist.

2. Zeigen Sie, dass für $d \in \{-2, -1, 2, 3\}$ die Abbildung

$$n : \mathcal{O}_d \setminus \{0\} \to \mathbb{N}_0,\ a + b\sqrt{d} \mapsto |a^2 - b^2 d|$$

eine euklidische Normabbildung ist, bezüglich derer der Ring $\mathcal{O}_d$ euklisch ist.

3. Zeigen Sie die gleiche Aussage wie in (2) für

$$d \in \{-11, -7, -3, 5\}.$$

Beweis. 1. Für $x = a + b\sqrt{d}$ gilt $N(x) = N(a + b\sqrt{d}) = a^2 - db^2 = (a + b\sqrt{d})(a - b\sqrt{d}) = x\bar{x}$. Sei zusätzlich $y = e + f\sqrt{d}$, so erhalten wir

$$\overline{xy} = \overline{(ae + bfd) + (af + be)\sqrt{d}} = (ae + bfd) - (af + be)\sqrt{d} = (a - b\sqrt{d})(e - f\sqrt{d}) = \bar{x}\bar{y}.$$

Aus letzterem folgt nun schließlich

$$N(xy) = xy\overline{xy} = xy\bar{x}\bar{y} = x\bar{x}y\bar{y} = N(x)N(y).$$

2. Für $d \in \{-2, -1, 2, 3\}$ gilt $d \not\equiv 1 \bmod 4$ und somit ist $\mathcal{O}_d = \mathbb{Z} \oplus \mathbb{Z}\sqrt{d}$. Stelle zunächst fest, dass für alle $q \in \mathbb{Q}$ Zahlen $q_1 \in \mathbb{Z}$ und $q_2 \in \mathbb{Q}$ existieren, sodass $q = q_1 + q_2$ und $|q_2| \le \frac{1}{2}$. Ist $q - \lfloor q \rfloor \le \frac{1}{2}$, so setze $q_1 := \lfloor q \rfloor$, ansonsten setze $q_1 := \lfloor q \rfloor + 1$. Seien nun $a, b \in \mathcal{O}_d$ mit $b \neq 0$, so existieren $x_1', x_2' \in \mathbb{Q}$ mit $\frac{a}{b} = x_1' + x_2'\sqrt{d} \in \mathbb{Q}(\sqrt{d})$. Nach der anfänglichen Feststellung existieren $x_1, x_2 \in \mathbb{Z}$, sodass für $s_1 := x_1' - x_1$ und $s_2 := x_2' - x_2$ gilt $|s_1|, |s_2| \le \frac{1}{2}$. Mit $r := b(s_1 + s_2\sqrt{d})$ und $x := x_1 + x_2\sqrt{d} \in \mathcal{O}_d$ gilt nun

$$bx + r = bx + b(s_1 + s_2\sqrt{d}) = b\left((x_1 + s_1) + (x_2 + s_2)\sqrt{d}\right) = b\frac{a}{b} = a \in \mathcal{O}_d$$

und damit auch $r = a - bx \in \mathcal{O}_d$. Außerdem gilt mit $-3 < d < 4$

$$-1 = -\frac{1}{4} \cdot 4 < -s_2^2 d \le s_1^2 - s_2^2 d < \frac{1}{4} + 3 \cdot \frac{1}{4} = 1$$

und somit die Abschätzung

$$\begin{aligned} n(r) &= \left|N\left(b(s_1 + s_2\sqrt{d})\right)\right| \\ &= |N(b)| \cdot \left|N(s_1 + s_2\sqrt{d})\right| \\ &= |N(b)| \cdot \underbrace{|s_1^2 - s_2^2 d|}_{<1} \\ &< n(b). \end{aligned}$$

3. Für $d \in \{-11, -7, -3, 5\}$ gilt $d \not\equiv 1 \bmod 4$ und somit ist $\mathcal{O}_d = \mathbb{Z} \oplus \mathbb{Z}\frac{1+\sqrt{d}}{2}$. Stelle zunächst fest, dass für $t \in \left(-\frac{1}{2}, \frac{1}{2}\right] \cap \mathbb{Q}$ und $q \in \mathbb{Q}$ ein $q_1 \in \mathbb{Z}$ und $q_2 \in \left(-\frac{1}{2}(1+t), \frac{1}{2}(1-t)\right]$ existieren, sodass $q = q_1 + q_2$ gilt. Letzteres sieht man, indem man $q' := q + \frac{t}{2} \in \mathbb{Q}$ betrachtet. Nach dem 2. Teil der Aufgabe existieren $q_1' \in \mathbb{Z}$ und $q_2 \in \left(-\frac{1}{2}, \frac{1}{2}\right]$ mit $q' = q_1' + q_2'$. Insbesondere gilt $q = q' - \frac{t}{2} = q_1' + \left(q_2' - \frac{t}{2}\right)$ und setze $q_1 := q_1'$ und $q_2 := q_2' - \frac{t}{2}$. Somit gilt $q_2 \in \left(-\frac{1}{2} - \frac{t}{2}, \frac{1}{2} - \frac{t}{2}\right] = \left(\frac{1}{2}(1+t), \frac{1}{2}(1-t)\right]$.

Seien $a, b \in \mathcal{O}_d$ mit $b \neq 0$ und $\frac{a}{b} = x_1' + x_2'\omega_d$ mit $x_1', x_2' \in \mathbb{Q}$, so wähle, wie zuvor besprochen, $x_1, x_2 \in \mathbb{Z}$ mit $t \coloneqq x_2' - x_2$, $|t| \leq \frac{1}{2}$, $s \in \left(-\frac{1}{2}(1+t), \frac{1}{2}(1-t)\right]$ und $x_1' = x_1 + s$, $x_2' = x_2 + t$. Mit $-12 < d \leq 5 < 16$ gilt

$$-1 = -\frac{16}{4}\left(\frac{1}{2}\right)^2 < \left(s + \frac{t}{2}\right)^2 - \frac{d}{4}t^2 < \frac{1}{4} - \frac{-12}{4}\left(\frac{1}{2}\right)^2 = 1$$

und somit erhalten wir für $r \coloneqq a - xb \in \mathcal{O}_d$

$$\begin{aligned} n(r) &= |N(b(s + t\omega_d))| \\ &= n(b) \cdot \left| N\left((s + \frac{1}{2}t) - \frac{1}{2}t\sqrt{d}\right)\right| \\ &= n(b) \cdot \underbrace{\left|\left(s + \frac{1}{2}t\right)^2 - \frac{d}{4}t^2\right|}_{<1} \\ &< n(b). \end{aligned}$$

□

Aufgabe 2. Finden Sie Erzeuger für die folgenen Ideale in $\mathcal{O}_{-1}$:

1. $(1+3i, 5+10i)$,
2. $(1+3i, 2+4i, 4+5i, \ldots)$.

Zunächst beweisen wir folgendes Hilfslemma.

Lemma 0.1. *Sei R ein Hauptidealring und $(a_1, \ldots, a_n) \lhd R$ mit $a_1, \ldots, a_n \in R$, so gilt $(a_1, \ldots, a_n) = ggT(a_1, \ldots, a_n)$.*

Beweis. Da R faktoriell ist, existieren der ggT und nach Definition $b_1, \ldots, b_n \in R$ mit g_i $\mathrm{ggT}(a_1, \ldots, a_n) = a_i$ für alle $1 \leq i \leq n$.
Sei $x = \sum_{i=1}^{n} r_i a_i \in (a_1, \ldots, a_n)$ mit $r_i \in R$, so gilt mit $y = \sum_{i=1}^{n} r_i b_i$

$$\mathrm{ggT}(a_1, \ldots, a_n)y = \sum_{i=1}^{n} r_i \ \mathrm{ggT}(a_1, \ldots, a_n)b_i = \sum_{i=1}^{n} r_i a_i = x,$$

d.h. $x \in (\mathrm{ggT}(a_1, \ldots, a_n))$ und somit gilt $(a_1, \ldots, a_n) \subseteq (\mathrm{ggT}(a_1, \ldots, a_n))$.
Da R ein Hauptidealring ist, existiert ein $d \in R$ mit $(a_1, \ldots, a_n) = (d)$, also existieren $b_1, \ldots, b_n \in R$ mit $db_i = a_i$. Daraus folgt, dass es ein $r \in R$ gibt, sodass $dr = \mathrm{ggT}(a_1, \ldots, a_n)$. Somit gilt $\mathrm{ggT}(a_1, \ldots, a_n) \in (d) = (a_1, \ldots, a_n)$ und damit auch $(\mathrm{ggT}(a_1, \ldots, a_n)) \subseteq (d) = (a_1, \ldots, a_n)$. □

1. Nach vorherigem Lemma reicht es also aus, den ggT von $1+3i$ und $5+10i$ in $\mathcal{O}_{-1}$ zu berechnen. Führe hierfür den euklidischen Algorithmus durch. Es gilt

   $$\frac{5+10i}{1+3i} = \frac{7}{2} - \frac{1}{2}i.$$

   Wähle nun $\lambda_1, \lambda_2 \in \mathbb{Z}$, sodass $|\lambda_1 - \frac{7}{2}| \leq \frac{1}{2}$ und $|\lambda_2 - \left(-\frac{1}{2}\right)| \leq \frac{1}{2}$ gelten. Seien $\lambda_1 = 3$ und $\lambda_2 = 0$, so gilt

   $$5 + 10i = (\lambda_1 + \lambda_2 i)(1+3i) + (2+i) = 3(1+3i) + (2+i).$$

   Da $2+i$ ein Teiler von $1+3i$ ist, gilt $\mathrm{ggT}(1+3i, 5+10i) = 2+i$ und somit gilt $(1+3i, 5+10i) = (2+i)$.

2. Im Folgenden zeigen wir, dass $(1+3i, 2+4i, 3+5i, \ldots) = (1-i)$. Es gilt für alle $n \in \mathbb{N}$

   $$n + (n+2)i = (-1 + (n+1)i)\,(1-i)\,,$$

   d.h. $(1+3i, 2+4i, 3+5i, \ldots) \subseteq (1-i)$. Andersherum können wir, analog zum ersten Teil, nachrechnen, dass $\mathrm{ggT}(1+3i, 3+5i) = 1-i$ gilt. Somit erhalten wir

   $$(1-i) = (1+3i, 3+5i) \subseteq (1+3i, 3+5i, 4+6i, \ldots).$$

Aufgabe 3. Zeigen Sie, dass der Ring $\mathcal{O}_{-5}$ nicht euklidisch ist.

Beweis. Zunächst beweisen wir das folgende Lemma, dass die Einheiten in $\mathcal{O}_{-5}$ charakterisiert.

Lemma 0.2. *Sei $w \in \mathcal{O}_{-5}$ und es gilt w ist genau dann invertierbar, wenn $N(w) = 1$. Insbesondere gilt $\mathcal{O}_{-5}^* = \{\pm 1\}$.*

Beweis. Wenn w invertierbar ist, so gilt $1 = N(1) = N(ww^{-1}) = N(w)N(w^{-1})$, d.h. $N(w^{-1}) = 1$. Ist $w \in \mathcal{O}_{-5}$ mit $1 = N(w) = w\bar{w}$, so gilt $w^{-1} = \bar{w}$ und somit ist w invertierbar. □

Angenommen $\mathcal{O}_{-5}$ wäre euklidisch, so auch faktoriell und somit ist jedes irreduzibles Element prim. Betrachte das Element $9 = 3^2 = (2+\sqrt{5})(2-\sqrt{5}) \in \mathcal{O}_{-5}$. Im Folgenden zeigen wir, dass 3, $(2+\sqrt{5})$ und $(2-\sqrt{5})$ irreduzibel sind.
Nehmen wir an, dass 3 reduzibel ist, so gibt es $x, y \in \mathcal{O}_{-5}$, die jeweils keine Einheiten sind und $3 = xy$ erfüllen. Es gilt $9 = N(3) = N(x)N(y)$ und damit $N(x) \in \{1, 3, 9\}$. Da x keine Einheit ist, impliziert das vorherige Lemma, dass $N(x) \neq 1$ gilt. Ist $N(x) = 9$, so ist $N(y) = 1$, ein Widerspruch zur Wahl von y. Also gilt $N(x) = 3$. Mit $x = a + b\sqrt{-5}$ gilt $3 = N(x) = a^2 + 5b^2$, woraus $b = 0$ und $a^2 = 3$ folgt, d.h. $a \notin \mathbb{Z}$, ein Widerspruch.
Betrachte nun $2 + \sqrt{-5}$ und argumentiere analog. Angenommen $2 + \sqrt{-5}$ ist reduzibel, so existieren $x, y \in \mathcal{O}_{-5}$, die jeweils keine Einheiten sind und für die $2 + \sqrt{-5} = xy$ gilt. Es gilt $9 = N(2 + \sqrt{-5}) = N(x)N(y)$ und somit ist $N(x) \in \{1, 3, 9\}$. Wie zuvor kann nur $N(x) = 3$ gelten, aber aus letzterem folgt mit $x = a + b\sqrt{-5}$

$$3 = N(x) = a^2 + 5b^2$$

und somit $b = 0$ und $a^2 = 3$, ein Widerspruch. Der Fall $2 - \sqrt{-5}$ lässt sich genauso beweisen.
Man sieht schnell, dass 3 und $2 \pm \sqrt{5}$ nicht assoziiert sind, denn es gilt $\mathcal{O}_{-5}^* = \{-1, 1\}$.
Insgesamt sind also $3, 2 \pm \sqrt{5}$ prim, aber in faktoriellen Ringen gilt die eindeutige Primfaktorzerlegung, ein Widerspruch. □

Aufgabe 4. Sei K ein Körper und $R = K[X][Y]/(X^2 - Y^3)$. Zeigen Sie, dass die Restklassen $\bar{X}$ und $\bar{Y}$ der Elemente X und Y in R, d.h. die Bilder der jeweiligen Elemente unter der natürlichen Reduktion $K[X][Y] \to R$, jeweils irreduzibel in R sind, nicht jedoch prim.

Beweis. Nach Blatt 4 Aufgabe 2 gilt $K[X][Y]/(X^2 - Y^3) \cong \left\{ \sum_{i=0}^{n} a_i X^i \mid n \in \mathbb{N}_0, a_i \in K, a_1 = 0 \right\} =: L$, vermöge der Zuordnung $\overline{X} \mapsto X^3$ und $\overline{Y} \mapsto X^2$. Wir können also statt $\overline{X}, \overline{Y}$ die Polynome X^3 und X^2 in L betrachten. Als erstes zeigen wir, dass X^3 irreduzibel ist. Seien hierfür $f, g \in L$ mit $X^3 = f(X)g(X)$, so gilt mit

$$3 = \deg(X^3) = \deg(fg) = \deg(f) + \deg(g)$$

$(\deg(f), \deg(g)) \in \{(0,3), (1,2), (2,1), (3,0)\}$. Da die Möglichkeiten $(1,2)$ und $(2,1)$ wegen der Definition von L ausscheiden, gilt also $\deg(f) = 0$ oder $\deg(g) = 0$. Letzteres ist äquivalent zu $f \in K^*$ oder $g \in K^*$, woraus die Irreduzibilität von X^3 folgt. Analog zeigt man die Irreduzibilität von X^2.
Nun zeigen wir, dass X^3 nicht prim ist. Betrachte $f(X) = X^4 = g(X) \in L$, so gilt $X^3 \mid f(X)g(X) = X^8$, aber $X^3 \nmid f(X) = X^4 = g(X)$. Folglich ist X^3 nicht prim.
Betrachte nun X^2 und $f(X) = X^3 = g(X)$. Es gilt $X^2 \mid f(X)g(X) = X^6$, aber $X^2 \nmid f(X) = g(X) = X^3$ in L. Folglich ist X^2 nicht prim. □