Lösungsvorschläge zu den Aufgaben auf Übungsblatt 07

Aufgabe 1. *Es seien R ein kommutativer Ring mit 1 und $D \in R$. Wir schreiben*

$$Q(R,D) = \left\{ \begin{pmatrix} x & Dy \\ y & x \end{pmatrix} \,\middle|\, x, y \in R \right\}.$$

Dann ist $Q(R,D)$ abgeschlossen bezüglich der Addition und Multiplikation von Matrizen und bildet einen kommutativen Ring mit Einselement $E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Setzen wir $W := \begin{pmatrix} 0 & D \\ 1 & 0 \end{pmatrix} \in Q(R,D)$, so lässt sich jedes $X \in Q(R,D)$ in der Form $X = xE + yW$ mit $x, y \in R$ schreiben. Da wir R vermöge $x \mapsto xE$ als Unterring von $Q(R,D)$ auffasssen können, schreiben wir dann auch $X = x + yW$. Wir definieren die Konjugation *auf $S := Q(R,D)$ durch*

$$\sigma : S \longrightarrow S,\ x + yW \longmapsto x - yW,$$

die Spur *durch*

$$\mathrm{Tr} : S \longrightarrow R,\ X \longmapsto X + \sigma(X),$$

und die Norm *durch*

$$\mathrm{N} : S \longrightarrow R,\ X \longmapsto X\sigma(X).$$

Zeigen Sie:

(i) $X \in Q(R,D)$ ist genau dann invertierbar, wenn $\mathrm{N}(X)$ in R invertierbar ist. In diesem Fall gilt $X^{-1} = \mathrm{N}(X)^{-1}\sigma(X)$.

(ii) Ist K ein Körper und $D \in K$ ein Element, das keine Quadratwurzel in K besitzt, so ist $K[\sqrt{D}] := Q(K,D)$ ein Körper.

(iii) Es sei p eine ungerade Primzahl und $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ der endliche Körper mit p Elementen. Sei p so, dass -1 keine Quadratwurzel in $\mathbb{F}_p$ besitzt. Dann ist die Norm

$$\mathrm{N} : \mathbb{F}_p[\sqrt{-1}] \longrightarrow \mathbb{F}_p$$

surjektiv.

Beweis. Es seien $A, B \in S$ zwei beliebige Elemente. Dann gibt es $a, a', b, b' \in R$ mit $A = a + a'W$ und $B = b + b'W$. Insbesondere gilt $AB = (a + a'W)(b + b'W) = ab + ab'W + a'Wb + a'Wb'W = (ab + a'b'D) + (ab' + a'b)W$, da $W^2 = DE = D$ vermöge der Einbettung $R \hookrightarrow S$ gilt. Daraus folgt

$$\begin{aligned} \mathrm{N}(AB) &= \mathrm{N}((ab + a'b'D) + (ab' + a'b)W) \\ &= ((ab + a'b'D) + (ab' + a'b)W)((ab + a'b'D) - (ab' + a'b)W) \\ &= (ab + a'b'D)^2 - (ab' + a'b)^2W^2 = (ab)^2 + (a'b')^2D^2 - (ab')^2D - (a'b)^2D \\ &= \mathrm{N}(A)\,\mathrm{N}(B). \end{aligned}$$

Teil (i): Es sei nun $X \in S$ invertierbar. Dann existiert eine Matrix $X^{-1} \in S$ mit $XX^{-1} = E$. Insbesondere gilt $\mathrm{N}(X)\,\mathrm{N}(X^{-1}) = \mathrm{N}(XX^{-1}) = \mathrm{N}(E) = E\sigma(E) = E = 1$. Also ist $\mathrm{N}(X)$ in R invertierbar.
Wir nehmen jetzt umgekehrt an, dass $X \in S$ eine Matrix ist, deren Norm in R invertierbar ist. Bezeichnen wir wie gewöhnlich das Inverse von $\mathrm{N}(X)$ in R mit $\mathrm{N}(X)^{-1}$. Offensichtlich ist die Matrix $Y := \mathrm{N}(X)^{-1}\sigma(X)$ ebenfalls ein Element von S. Außerdem gilt $XY = \mathrm{N}(X)^{-1}X\sigma(X) = \mathrm{N}(X)^{-1}\,\mathrm{N}(X) = 1$, und die Matrix X ist in S invertierbar. Zusätzlich haben wir auch $X^{-1} = Y = \mathrm{N}(X)^{-1}\sigma(X)$, wie behauptet.
Teil (ii): $K[\sqrt{D}]$ ist offensichtlich ein kommutativer Ring mit 1. Wir müssen also nur zeigen, dass jedes Element aus $K[\sqrt{D}] \setminus \{0\}$ invertierbar ist. Dafür sei $X \in K[\sqrt{D}]$. Es existieren demnach $x, y \in K$ mit

$X = x + yW$. Die Norm von X ist $\mathrm{N}(X) = x^2 - y^2 D$. Da $\mathrm{N}(X)$ ein Element eines Körpers ist, ist $\mathrm{N}(X)$ genau dann invertierbar in K, wenn $\mathrm{N}(X)$ ungleich 0 ist. Nehmen wir also $\mathrm{N}(X) = x^2 - y^2 D = 0$ an. Dann gilt aber auch $y^2 D = x^2$. Ist nun $x = 0$, so ist auch $y = 0$, und umgekehrt. Nehmen wir also $(x, y) \neq (0, 0)$ an. Dann ist aber y in K invertierbar, und es gilt $D = x^2/y^2 = (x/y)^2$, was einen Widerspruch zu der Voraussetzung, dass D kein Quadrat in K ist, darstellt.
Also ist $\mathrm{N}(X) \neq 0$, und X ist nach Teil (i) in $K[\sqrt{D}]$ invertierbar.
Teil (iii): Da -1 nach Voraussetzung keine Quadratwurzel in $\mathbb{F}_p$ besitzt, ist $\mathbb{F}_p[\sqrt{-1}] = Q(\mathbb{F}_p, -1)$ nach Teil (ii) ein Körper. Insbesondere gilt dann $\mathbb{F}_p[\sqrt{-1}]^\times = \mathbb{F}_p[\sqrt{-1}] \setminus \{0\}$.
Ist $x \in \mathbb{F}_p$ ein Quadrat, so existiert ein $y \in \mathbb{F}_p \subseteq \mathbb{F}_p[\sqrt{-1}]$ mit $y^2 = x$. Dann gilt aber auch $\mathrm{N}(y) = \mathrm{N}(yE) = yE\sigma(yE) = y^2 = x$. Also hat jedes Quadrat in $\mathbb{F}_p$ ein Urbild in $\mathbb{F}_p[\sqrt{-1}]$.
Aus den Berechnungen vor dem Beweis von Teil (i) folgt $\mathrm{N}(AB) = \mathrm{N}(A)\,\mathrm{N}(B)$ für alle $A, B \in \mathbb{F}_p[\sqrt{-1}]$. Bezeichnen wir mit $\mathrm{N}' := N|_{\mathbb{F}_p[\sqrt{-1}]^\times} : \mathbb{F}_p[\sqrt{-1}]^\times \to \mathbb{F}_p^\times$ die Einschränkung von N auf $\mathbb{F}_p[\sqrt{-1}]^\times$, so ist N' ein Gruppenhomomorphismus. Da $0 \in \mathbb{F}_p$ im Bild von N enthalten ist, und da $\mathbb{F}_p^\times = \mathbb{F}_p \setminus \{0\}$ ist, ist N genau dann surjektiv, wenn N' surjektiv ist.
Wir haben bereits gesehen, dass jedes Quadrat von $\mathbb{F}_p^\times$ im Bild von N' liegt, und nach Satz 4.6 gibt es genau $(p-1)/2$ Quadrate modulo p. Somit ist der Index $[\mathbb{F}_p^\times : \mathrm{Im}(\mathrm{N}')]$ von $\mathrm{Im}(\mathrm{N}')$ in $\mathbb{F}_p^\times$ maximal 2. Es gilt also entweder $|\mathrm{Im}(\mathrm{N}')| = (p-1)/2$ oder $|\mathrm{Im}(\mathrm{N}')| = p - 1$. Die Abbildung N' ist genau dann surjektiv, wenn $[\mathbb{F}_p^\times : \mathrm{Im}(\mathrm{N}')] = 1$ ist.
Wir nehmen an, dass der Index $[\mathbb{F}_p^\times : \mathrm{Im}(\mathrm{N}')] = 2$ ist. Das Bild von N' besteht also genau aus den Quadraten in $\mathbb{F}_p^\times$. Insbesondere ist damit $2 \in \mathbb{F}_p^\times$ ein Quadrat, denn es gilt $2 = 1^2 + 1^2 = \mathrm{N}'(1 + 1W)$, wobei hier insbesondere $W = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ ist. Wir definieren uns rekursiv eine Folge (x_n) in $\mathbb{F}_p$ durch $x_0 := 2 \in \mathbb{F}_p$ und $x_{k+1} = x_k + 1$. Dann ist x_n für jedes $n \geq 0$ ein Quadrat. Den Induktionsanfang $x_0 = 2$ haben wir bereits aufgeführt. Wir nehmen also an, dass x_k für ein $k \geq 0$ ein Quadrat ist. Ist $x_k = 0$, so ist $x_{k+1} = 1 = 1^2$. Nehmen wir also $x_k \neq 0$ an. Es sei $y_k \in \mathbb{F}_p^\times$ mit $y_k^2 = x_k$. Damit haben wir aber auch $\mathrm{N}'(y_k + 1W) = y_k^2 + 1^2 = x_k + 1 = x_{k+1}$. Also liegt x_{k+1} im Bild von N' und ist somit ein Quadrat. Damit wären aber alle Elemente von $\mathbb{F}_p$ Quadrate, da die Glieder der Folge (x_n) offensichtlich alle Elemente von $\mathbb{F}_p$ durchlaufen. Dies ist aber ein Widerspruch zu Satz 4.6.
Also ist $[\mathbb{F}_p^\times : \mathrm{Im}(\mathrm{N}')] = 1$, und damit sind N' und N surjektiv. □

Aufgabe 2. *Es sei p eine ungerade Primzahl. Zeigen Sie: Genau dann lässt sich p darstellen als $p = x^2 + 2y^2$ mit ganzen Zahlen x, y, wenn $p \equiv 1 \mod 8$ oder $p \equiv 3 \mod 8$ ist.*

Beweis. Es seien $x, y \in \mathbb{Z}$ mit $p = x^2 + 2y^2$. Wäre $x = 0$ oder $y = 0$, so wäre p entweder durch zwei teilbar oder ein Quadrat. Also können wir Ohne Beschränkung der Allgemeinheit $x, y > 0$ annehmen. Und daher ist auch $x^2, y^2 < p$, insbesondere haben wir also $p \nmid x, y$.
Aus $p = x^2 + 2y^2$ folgt die Kongruenz $x^2 + 2y^2 \equiv 0 \mod p$. Dies ist aber äquivalent zu $(x/y)^2 \equiv -2 \mod p$, da y modulo p invertierbar ist. Also ist -2 ein Quadrat modulo p. Es gilt demnach $1 = \left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)$. Nach den Ergänzungssätzen 4.16 zum Quadratischen Reziprozitätsgesetz ist das Produkt dieser Legendre-Symbole genau dann 1, wenn entweder $p \equiv 1 \mod 4$, $p \equiv \pm 1 \mod 8$ oder $p \equiv 3 \mod 4$, $p \equiv \pm 3 \mod 8$ gelten. Dabei ist $p \equiv 1 \mod 4$ genau dann, wenn $p \equiv 1 \mod 8$ oder $p \equiv 5 \mod 8$ ist; und $p \equiv 3 \mod 4$ gilt genau dann, wenn $p \equiv 3 \mod 8$ oder $p \equiv 7 \mod 8$ ist. Also gilt $\left(\frac{-2}{p}\right) = 1$ genau dann, wenn $p \equiv 1 \mod 8$ oder $p \equiv 3 \mod 8$ ist.
Die Rückrichtung zeigen wir in mehreren Schritten:
Schritt 1: Ist $a \in \mathbb{Z}$ und $n \in \mathbb{Z}_{>0}$ keine Quadratzahl, so hat die Kongruenz $ax \equiv y \mod n$ eine Lösung $(x, y) \neq (0, 0)$ mit $|x|, |y| < \sqrt{n}$: Wir betrachten alle Zahlen $ax - y$ mit $0 \leq x, y < \sqrt{n}$. Ist m die kleinste ganze Zahl größer oder gleich $\sqrt{n}$, so haben wir für x, y je genau m Möglichkeiten, also insgesamt m^2 Möglichkeiten. Da n keine Quadratzahl ist, ist $m^2 > n$. Aber $\mathbb{Z}/n\mathbb{Z}$ hat nur $n < m^2$ Elemente. Also gibt es Paare $(x_1, y_1) \neq (x_2, y_2)$ mit $ax_1 - y_1 \equiv ax_2 - y_2 \mod n$. Also ist $a(x_1 - x_2) \equiv y_1 - y_2 \mod n$ mit $|x_1 - x_2| < \sqrt{n}$ und $|y_1 - y_2| < \sqrt{n}$.

Schritt 2: Es sei $0 \neq m \in \mathbb{Z}$ und $p \in \mathbb{P}$ mit $\left(\frac{m}{p}\right) = 1$. Dann existieren ganze Zahlen x, y, k mit $(x, y) \neq (0, 0)$ und $|k| \leq |m|$, so dass $x^2 - my^2 = kp$ ist: Da $\left(\frac{m}{p}\right) = 1$ ist, existiert ein $a \in \mathbb{Z}$ mit $a^2 \equiv m \mod p$. Wenden wir Schritt 1 an, so folgt die Existenz eines Paares $(0, 0) \neq (x, y) \in \mathbb{Z} \times \mathbb{Z}$ mit $|x|, |y| < \sqrt{p}$ und $ay \equiv x \mod p$. Quadrieren liefert

$$my^2 \equiv a^2y^2 \equiv x^2 \mod p,$$

also gilt insbesondere $x^2 - my^2 = kp$ für ein $k \in \mathbb{Z}$. Schließlich gilt

$$|k|p = |kp| = |x^2 - my^2| \leq |x^2| + |my^2| = x^2 + |m|y^2 < p + |m|p = (|m| + 1)p.$$

Daraus folgt $|k| < |m| + 1$, was äquivalent zu $|k| \leq |m|$ ist.
Schritt 3: Nehmen wir nun $p \equiv 1 \mod 8$ oder $p \equiv 3 \mod 8$ an. Wir haben im vorigen Abschnitt bereits gesehen, dass in diesen Fällen -2 ein quadratischer Rest modulo p ist. Somit gilt $\left(\frac{-2}{p}\right) = 1$. Und nach Schritt 2 existieren $x, y, k \in \mathbb{Z}$ mit $(x, y) \neq (0, 0)$, $|k| \leq |-2| = 2$ und $x^2 + 2y^2 = kp$. Somit muss $-2 \leq k \leq 2$ gelten. Da aber $x^2 + 2y^2$ nicht negativ ist und $(x, y) \neq (0, 0)$ ist, gilt sogar $k \in \{1, 2\}$. Ist $k = 1$, so haben wir ganze Zahlen x und y mit $x^2 + 2y^2 = p$ gefunden.
Nehmen wir also $k = 2$ an. Somit ist $x^2 + 2y^2 = 2p$, woraus $2|x^2$ und schließlich $2|x$ folgt. Es existiert also ein $u \in \mathbb{Z}$ mit $x = 2u$, und aus $x^2 + 2y^2 = 2p$ wird $4u^2 + 2y^2 = 2p$. Daraus folgt wiederum $y^2 + 2u^2 = p$. Also finden wir auch in diesem Fall eine ganzzahlige Lösung der obigen Gleichung. □

Aufgabe 3.

(a) Es sei $\rho = \frac{-1+i\sqrt{3}}{2}$. Zeigen Sie: Jedes Element $\zeta \in \mathbb{Z}[\rho]$ ist assoziiert zu einem Element $\zeta_1 \in \mathbb{Z}[\sqrt{-3}]$.

(b) Zeigen Sie: Eine Primzahl p lässt sich genau dann in der Form $p = x^2 + 3y^2$ mit ganzen Zahlen x, y darstellen, wenn $p = 3$ oder $p \equiv 1 \mod 6$ ist.

Beweis. Teil (a): Es gilt offensichtlich $\rho^2 = \frac{-1-i\sqrt{3}}{2}$, und dadurch ist auch $\sqrt{-3} = \rho - \rho^2$ und $\rho + \rho^2 = -1$. Es gilt also $\mathbb{Z}[\sqrt{-3}] \subseteq \mathbb{Z}[\rho]$.
Es seien nun $a, b \in \mathbb{Z}$ und $x = a + b\rho \in \mathbb{Z}[\rho]$. Wir zeigen, dass es dann eine Einheit $y \in \mathbb{Z}[\rho]$ mit $xy \in \mathbb{Z}[\sqrt{-3}]$ gibt.
Wir betrachten zuerst den Fall, dass $a \equiv b \mod 2$ ist. Es sei $y := \rho$. Dann gelten

$$y^3 = \rho^3 = \frac{1}{8}(-1 + 3\sqrt{-3} - 3\sqrt{-3}^2 + \sqrt{-3}^3) = \frac{1}{8}(-1 + 9) = 1,$$

also insbesondere $y \in \mathbb{Z}[\rho]^\times$, und

$$xy = x\rho = a\rho + b\rho^2 = a\rho - a\rho^2 + a\rho^2 + b\rho^2 = a(\rho - \rho^2) + (a + b)\rho^2 = a\sqrt{-3} + (a + b)\rho^2.$$

Da $a \equiv b \mod 2$ ist, ist $a + b$ gerade, somit folgt $(a + b)\rho^2 = \frac{a+b}{2}(-1 - \sqrt{-3}) \in \mathbb{Z}[\sqrt{-3}]$, also gilt $xy \in \mathbb{Z}[\sqrt{-3}]$.
Es sei ab jetzt $a \not\equiv b \mod 2$. Als Erstes untersuchen wir den Fall $a \equiv 0 \mod 2$ und $b \equiv 1 \mod 2$. Wir setzen $y = 1 + \rho$. Dann gilt

$$y(-\rho) = (1 + \rho)(-\rho) = -\rho - \rho^2 = 1,$$

also $y \in \mathbb{Z}[\rho]^\times$. Zudem haben wir

$$\begin{aligned} xy = x + x\rho &= a + b\rho + a\sqrt{-3} + (a + b)\rho^2 = a + a\sqrt{-3} + b(\rho + \rho^2) + a\rho^2 \\ &\overset{\rho+\rho^2=-1}{=} (a - b) + a\sqrt{-3} + \frac{a}{2}(-1 - \sqrt{-3}). \end{aligned}$$

Dabei ist aber offensichtlich $(a-b)+a\sqrt{-3} \in \mathbb{Z}[\sqrt{-3}]$, und da $a \equiv 0 \mod 2$ ist, haben wir auch $\frac{a}{2} \in \mathbb{Z}$. Insgesamt bekommen wir demnach ebenfalls $xy \in \mathbb{Z}[\sqrt{-3}]$.

Betrachten wir schließlich noch den letzten Fall, also $a \equiv 1 \mod 2$ und $b \equiv 0 \mod 2$. Dann ist aber insbesondere $2|b$, woraus $b\rho = \frac{b}{2}(-1+\sqrt{-3}) \in \mathbb{Z}[\sqrt{-3}]$ folgt. Daher ist $x = a + b\rho \in \mathbb{Z}[\sqrt{-3}]$, und $y = 1$ erfüllt die Behauptung.
Teil (b): Die Primzahl 3 lässt sich offensichtlich in der angegebenen Form darstellen. Nehmen wir also an, dass die Primzahl p größer als 3 ist. Somit ist entweder $p \equiv 1 \mod 6$ oder $p \equiv 5 \mod 6$.
Zuerst nehmen wir an, dass es ganze Zahlen x, y mit $p = x^2 + 3y^2$ gibt. Ist $x \in \mathbb{Z}$, so gilt $x^2 \equiv a \mod 6$ für ein $a \in \{0, 1, 3, 4\}$ und $3x^2 \equiv b \mod 6$ mit $b \in \{0, 3\}$. Wir erhalten also $p = x^2 + 3y^2 \equiv c \mod 6$ mit $c \in \{0, 1, 3, 4\}$. Da p entweder den Rest 1 oder den Rest 5 modulo 6 besitzt, muss $p \equiv 1 \mod 6$ sein.
Wir zeigen nun die Rückrichtung. Dazu sei $p \in \mathbb{P}$ mit $p \equiv 1 \mod 6$ (der Fall $p = 3$ wurde bereits behandelt). Da p ungerade ist, ist die vorige Kongruenz äquivalent zu $p \equiv 1 \mod 3$.
Wir setzen $R = \mathbb{Z}[\rho]$ mit $\rho = \frac{-1+\sqrt{-3}}{2}$. Nach Beispiel 5.10 ist R der Ganzheitsring von $\mathbb{Q}(\sqrt{-3})$, und nach Satz 5.15 ist p genau dann reduzibel in R, falls ein $z \in R$ mit $\mathrm{N}(z) = \pm p$ existiert ($\mathrm{N}(.)$ bezeichnet hier wie oben die Norm definiert auf dem Körper $\mathbb{Q}(\sqrt{-3})$). Nun ist R nach Aufgabe 4 ein Hauptidealring und daher ist p genau dann reduzibel in R, wenn p nicht prim ist. Da $p \neq 3$, ist p nach Satz 5.16 genau dann nicht prim in R, falls $\left(\frac{-3}{p}\right) = 1$ ist.
Berechnen wir also $\left(\frac{-3}{p}\right)$. Es gilt $\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)$. Ist $p \equiv 1 \mod 4$, so gelten $\left(\frac{-1}{p}\right) = 1$ und $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)$. Ist dagegen $p \equiv 3 \mod 4$, so haben wir $\left(\frac{-1}{p}\right) = 1$ und $\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right)$. In beiden Fällen gilt also $\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right) = 1$, da $p \equiv 1 \mod 3$ und damit ein quadratischer Rest modulo 3 ist.
Also ist p reduzibel in R. Somit existieren nach Satz 5.15 ein $z \in R$ mit $\mathrm{N}(z) = \pm p$. Nun ist z nach Teil (a) in R assoziiert zu einem Element $z' \in \mathbb{Z}[\sqrt{-3}]$. Insbesondere existiert eine Einheit $e \in R$ mit $z' = ze$. Da e eine Einheit ist, gilt $\mathrm{N}(e) = \pm 1$, siehe Satz 5.11. Es seien weiterhin $a, b \in \mathbb{Z}$ mit $z' = a + b\sqrt{-3}$.
Wir müssen beachten, dass das Bild jedes Elements aus $\mathbb{Q}(\sqrt{-3})$ unter der Norm die Form $c^2 + 3d^2$ mit $c, d \in \mathbb{Q}$ hat. Insbesondere folgt daraus $\mathrm{N}(w) \geq 0$ für alle $w \in \mathbb{Q}(\sqrt{-3})$. Wenden wir dies an, so erhalten wir $p = \mathrm{N}(z) = \mathrm{N}(z)\,\mathrm{N}(e) = \mathrm{N}(ze) = \mathrm{N}(z') = \mathrm{N}(a + b\sqrt{-3}) = a^2 + 3b^2$ mit $a, b \in \mathbb{Z}$. Es folgt die Behauptung. □

Aufgabe 4. *Zeigen Sie, dass die Ringe der ganzen Zahlen in den Zahlkörpern $\mathbb{Q}(\sqrt{d})$ für $d = -1, -2, -3, -7, -11$ und $d = 2, 3, 5, 6, 7$ Hauptidealringe sind.*

Beweis. Nach Satz 5.18 ist der Ring R der ganzen Zahlen in $\mathbb{Q}(\sqrt{d})$ euklidisch, wenn es zu jedem $z \in \mathbb{Q}(\sqrt{d})$ ein $w \in R$ mit $|\,\mathrm{N}(z - w)| < 1$ gibt. Da ein euklidischer Ring immer ein Hauptidealring ist, wollen wir das soeben zitierte Kriterium anwenden.
Außerdem gilt für $d \neq 0, 1$ quadratfrei, dass der Ring R der ganzen Zahlen in $\mathbb{Q}(\sqrt{d})$ folgende Form hat:

$$R = \begin{cases} \mathbb{Z}[\sqrt{d}], & d \equiv 2 \mod 4 \text{ oder } d \equiv 3 \mod 4, \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}], & d \equiv 1 \mod 4. \end{cases}$$

Fall $d \in \{2, -1, -2\}$: Es sei $z = r + s\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ mit $r, s \in \mathbb{Q}$. Dann existieren $x, y \in \mathbb{Z}$ mit $|r - x| \leq \frac{1}{2}$ und $|s - y| \leq \frac{1}{2}$. Wir setzen $w := x + y\sqrt{d}$. Dann gelten $w \in R = \mathbb{Z}[\sqrt{d}]$ und

$$|\,\mathrm{N}(z - w)| = |(r - x)^2 - d(s - y)^2| \leq |r - x|^2 + |d||s - y|^2 \leq \frac{1}{4} + \frac{|d|}{4} \leq \frac{1}{4} + \frac{2}{4} = \frac{3}{4} < 1.$$

Fall $d \in \{5, -3, -7, -11\}$: In diesem Fall gilt $d \equiv 1 \mod 4$, der Ring der ganzen Zahlen in $\mathbb{Q}(\sqrt{d})$ ist also $R = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$. Es sei wieder $z = r + s\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ mit $r, s \in \mathbb{Q}$. Wir wählen ein $y \in \mathbb{Z}$ mit $|2s - y| \leq \frac{1}{2}$, und es sei $x \in \mathbb{Z}$ mit $|r - x - \frac{1}{2}y| \leq \frac{1}{2}$. Nun setzen wir $w := x + \frac{1}{2}(1 + \sqrt{d})y$. Offensichtlich

ist $w \in \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$, und es gilt

$$|\,\mathrm{N}(z-w)| = \left|\mathrm{N}\left(\left(r-x-\frac{1}{2}y\right)+\sqrt{d}\left(s-\frac{1}{2}y\right)\right)\right| = \left|\left(r-x-\frac{1}{2}y\right)^2 - d\left(s-\frac{1}{2}y\right)^2\right|$$
$$\leq \left|r-x-\frac{1}{2}y\right|^2 + |d|\left|s-\frac{1}{2}y\right|^2 \leq \frac{1}{4}+\frac{|d|}{16} \leq \frac{1}{4}+\frac{11}{16} = \frac{15}{16} < 1.$$

Fall $d = 3$: Hier gilt $R = \mathbb{Z}[\sqrt{3}]$ für den Ring R der ganzen Zahlen in $\mathbb{Q}(\sqrt{3})$. Es sei $z = r+s\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ mit $r, s \in \mathbb{Q}$, und es seien $x, y \in \mathbb{Z}$ mit $|r-x| \leq \frac{1}{2}$ und $|s-y| \leq \frac{1}{2}$. Setzen wir $w = x + y\sqrt{3}$, so gilt $w \in R$, und wir haben

$$|\,\mathrm{N}(z-w)| = |(r-x)^2 - d(s-y)^2| = |(r-x)^2 - 3(s-y)^2| \leq \frac{3}{4} < 1,$$

da $0 \leq (r-x)^2 \leq \frac{1}{4}$ und $0 \leq 3(s-y)^2 \leq \frac{3}{4}$ gelten.
Fall $d \in \{6, 7\}$: Auch hier gilt $R = \mathbb{Z}[\sqrt{d}]$. Es seien $z = r + s\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ mit $r, s \in \mathbb{Q}$ und $y \in \mathbb{Z}$ mit $|s-y| \leq \frac{1}{2}$. Dann gilt hier $0 \leq d(s-y)^2 \leq \frac{7}{4}$. Falls $d(s-y)^2 = 0$ ist, so wählen wir uns $x \in \mathbb{Z}$ mit $|r-x| \leq \frac{1}{2}$. Dann gilt für $w = x + y\sqrt{d} \in R$

$$\mathrm{N}(z-w) = |(r-x)^2 - d(s-y)^2| = (r-x)^2 \leq \frac{1}{4}.$$

Wir nehmen nun $0 < d(s-y)^2 < \frac{5}{4}$ an. Dann existiert ein $x \in \mathbb{Z}$ mit $r-x \in [\frac{1}{2}, 1]$ oder $r-x \in [-1, -\frac{1}{2}]$. Somit gilt $\frac{1}{4} \leq (r-x)^2 \leq 1$. Damit haben wir aber auch $(r-x)^2 - d(s-y)^2 < 1-0 = 1$ und $(r-x)^2 - d(s-y)^2 > \frac{1}{4} - \frac{5}{4} = -1$. Also gilt in diesem Fall mit $w = x + y\sqrt{d} \in R$

$$\mathrm{N}(z-w) = |(r-x)^2 - d(s-y)^2| < 1.$$

Betrachten wir jetzt den Fall $\frac{5}{4} < d(s-y)^2 \leq \frac{7}{4}$. Zudem existiert eine ganze Zahl $x \in \mathbb{Z}$ mit $r-x \in [1, \frac{3}{2}]$ oder $r-x \in [-\frac{3}{2}, -1]$. Wir haben also insbesondere $1 \leq (r-x)^2 \leq \frac{9}{4}$. Somit ist aber $(r-x)^2 - d(s-y)^2 < \frac{9}{4} - \frac{5}{4} = 1$ und $(r-x)^2 - d(s-y)^2 > 1 - \frac{7}{4} = -\frac{3}{4}$. Insgesamt erhalten wir mit $w = x + y\sqrt{d} \in R$ auch hier

$$N(z-w) = |(r-x)^2 - d(s-y)^2| < 1.$$

Offen bleibt nur noch der Fall $d(s-y)^2 = \frac{5}{4}$. Da $s \in \mathbb{Q}$ ist, ist auch $s - y \in \mathbb{Q}$, und es existieren teilerfremde ganze Zahlen t_1, t_2 mit $s - y = \frac{t_1}{t_2}$. Dann ist aber auch $4dt_1^2 = 5t_2^2$. Da d nicht durch 5 teilbar ist, gilt $5|t_1$, woraus $5^2|t_1^2$ folgt. Damit muss 5 aber auch ein Teiler von t_2 sein, was der Teilerfremdheit von t_1 und t_2 widerspricht.
Somit folgt aus Satz 5.18 in jedem dieser Fälle, dass R ein euklidischer Ring ist. Also ist R insbesondere auch ein Hauptidealring. □