Aufgabe H12T1A4 (2+3 Punkte)

Sei $R = \mathbb{Z}[\frac{1}{2}(1+\sqrt{-7})]$. Sie dürfen ohne Beweis verwenden, dass R bezüglich der Normfunktion $N : R \to \mathbb{N}_0$, $z \mapsto z\bar{z}$ ein euklidischer Ring ist.

(a) Bestimmen Sie alle Einheiten von R.

(b) Zerlegen Sie 3, 5 und 7 in Primfaktoren in R.

Lösung:

Aus der Vorlesung ist bekannt, dass der Ring R auch in der Form

$$R \quad = \quad \{\tfrac{1}{2}a + \tfrac{1}{2}b\sqrt{-7} \mid a, b \in \mathbb{Z}, a \equiv b \bmod 2\}$$

dargestellt werden kann.

zu (a) Die Normfunktion N ist multiplikativ, denn für alle $\alpha, \beta \in R$ gilt $N(\alpha\beta) = (\alpha\beta)(\bar{\alpha}\bar{\beta}) = \alpha\bar{\alpha}\beta\bar{\beta} = N(\alpha)N(\beta)$. Mit Hilfe dieser Eigenschaft kann gezeigt werden, dass die Einheiten in R genau die Elemente $\alpha \in R$ mit $N(\alpha) = 1$ sind. Ist nämlich $\alpha \in R^\times$, dann gibt es ein $\beta \in R$ mit $\alpha\beta = 1$. Es folgt $N(\alpha)N(\beta) = N(\alpha\beta) = N(1) = 1$. Wegen $N(\alpha), N(\beta) \in \mathbb{N}$ bedeutet dies wiederum, dass $N(\alpha) = N(\beta) = 1$ ist. Setzen wir umgekehrt $N(\alpha) = 1$ voraus, dann gilt $\alpha\bar{\alpha} = 1$, und da mit α auch $\bar{\alpha}$ in R liegt, folgt aus dieser Gleichung, dass α in R eine Einheit ist.

Sei nun $\alpha \in R$, $\alpha = \frac{1}{2}a + \frac{1}{2}b\sqrt{-7}$ mit $a, b \in \mathbb{Z}$ und $a \equiv b \bmod 2$. Dann gilt die Äquivalenz

$$\alpha \in R^\times \quad \Leftrightarrow \quad N(\alpha) = 1 \quad \Leftrightarrow \quad N(\tfrac{1}{2}a + \tfrac{1}{2}b\sqrt{-7}) = 1 \quad \Leftrightarrow \quad \tfrac{1}{4}a^2 + \tfrac{7}{4}b^2 = 1 \quad \Leftrightarrow \quad a^2 + 7b^2 = 4.$$

Die einzigen Lösungen der Gleichung $a^2+7b^2 = 4$ in $\mathbb{Z}^2$ sind $(2,0)$ und $(-2,0)$. Wegen $\frac{1}{2}\cdot 2 + \frac{1}{2}\cdot 0 \cdot \sqrt{-7} = 1$ und $\frac{1}{2}\cdot(-2) + \frac{1}{2}\cdot 0 \cdot \sqrt{-7} = -1$ sind ± 1 die einzigen beiden Einheiten in R.

zu (b) Wir zeigen, dass 3 und 5 in R irreduzibel sind. Da es sich bei R um einen euklidischen Ring handelt, folgt daraus, dass 3 und 5 in R auch prim sind. Die Primfaktorzerlegung besteht also für beide Elemente nur aus jeweils einem Faktor.

Wegen $N(3) = 9 > 1$ und $N(5) = 25 > 1$ sind 3 und 5 nach Teil (a) jedenfalls keine Einheiten. Nehmen wir nun an, das Element 3 ist reduzibel. Dann gibt es Nicht-Einheiten $\alpha, \beta \in R$ mit $3 = \alpha\beta$. Auf Grund der Multiplikativität der Normfunktion gilt $N(\alpha)N(\beta) = N(\alpha\beta) = N(3) = 9$. Weil α und β keine Einheiten sind, gilt $N(\alpha), N(\beta) > 1$. Aus $N(\alpha), N(\beta) \in \mathbb{N}$, $N(\alpha), N(\beta) > 1$ und $N(\alpha)N(\beta) = 9$ folgt nun $N(\alpha) = N(\beta) = 3$. Schreiben wir nun $\alpha = \frac{1}{2}a + \frac{1}{2}b\sqrt{-7}$ mit $a, b \in \mathbb{Z}$, dann folgt $\frac{1}{4}a^2 + \frac{7}{4}b^2 = N(\alpha) = 3$, und Multiplikation mit 4 liefert $a^2 + 7b^2 = 12$. Für b^2 sind nur die Werte 0 und 1 möglich. Im ersten Fall wäre $a^2 = 12$, im zweiten $a^2 = 5$. Aber weder 12 noch 5 ist eine Quadratzahl in $\mathbb{Z}$. Also ist die Gleichung $a^2 + 7b^2 = 12$ mit $a, b \in \mathbb{Z}$ unlösbar. Dies zeigt, dass in R kein Element der Norm 3 existiert. Die Annahme, dass 3 reduzibel ist, war also falsch, und folglich ist 3 tatsächlich ein Primelement in R.

Beim Element 5 gehen wir nach demselben Schema vor. Nehmen wir an, 5 ist reduzibel, und $\alpha, \beta \in R$ sind Nicht-Einheiten mit $5 = \alpha\beta$. Wegen $\alpha, \beta \notin R^\times$ gilt $N(\alpha), N(\beta) > 1$, und aus $N(\alpha)N(\beta) = N(\alpha\beta) = N(5) = 25$ folgt $N(\alpha) = N(\beta) = 5$. Wieder stellen wir α in der Form $\frac{1}{2}a + \frac{1}{2}\sqrt{-7}b$ dar, mit $a, b \in \mathbb{Z}$. Es gilt dann $\frac{1}{4}a^2 + \frac{7}{4}b^2 = N(\alpha) = 5$, und Multiplikation mit 4 liefert $a^2 + 7b^2 = 20$. Auch hier sind für b^2 nur die Wert 0 und 1 möglich. Weil aber die Gleichungen $a^2 = 20$ und $a^2 = 13$ in $\mathbb{Z}$ keine Lösung haben, ist $a^2 + 7b^2 = 20$ mit $a, b \in \mathbb{Z}$ lösbar. Es gibt also kein Element der Norm 5 in R. Dies zeigt, dass auch 5 ein Primelement in R ist.

Die Zahl 7 besitzt in R die Zerlegung $7 = \sqrt{-7}(-\sqrt{-7})$. Wegen $N(\sqrt{-7}) = N(-\sqrt{-7}) = 7 > 1$ sind $\pm\sqrt{-7}$ keine Einheiten in R. Nehmen wir an, dass $\sqrt{-7}$ in R reduzibel ist. Dann gibt es Nicht-Einheiten $\alpha, \beta \in R$ mit $\sqrt{-7} = \alpha\beta$. Es folgt $N(\alpha)N(\beta) = N(\alpha\beta) = N(\sqrt{-7}) = 7$. Zusammen mit $N(\alpha), N(\beta) > 1$ und $N(\alpha), N(\beta) \in \mathbb{N}$ folgt $N(\alpha) = 1$ oder $N(\beta) = 1$. Nach Teil (a) würde dies bedeuten, dass α oder β eine Einheit in R ist, im Widerspruch zur Annahme. So aber haben wir gezeigt, dass $\sqrt{-7}$ in R irreduzibel und damit ein Primelement ist. Weil $-\sqrt{-7}$ zu $\sqrt{-7}$ assoziiert ist, handelt es sich auch bei $-\sqrt{-7}$ um ein Primelement. Insgesamt haben wir damit gezeigt, dass $7 = \sqrt{-7}(-\sqrt{-7})$ die Primfaktorzerlegung von 7 in R ist.