Prof. Dr. Benjamin Klopsch
Dr. Philip Möller
Wintersemester 2024–25

Zahlentheorie I – Blatt 9

Vorstellung/Abgabe der Lösungen in der Übungsstunde am 09.12.2024, ab 14.30 Uhr

Bitte reichen Sie Lösungen zu den Aufgaben 9.3 und 9.4 ein; weitere Informationen auf

`http://reh.math.uni-duesseldorf.de/~internet/ZahlenI_WS2425/`.

Aufgabe 9.1

Finden Sie in $\mathfrak{o} = \mathbb{Z}[\sqrt{2}]$ alle Ideale $\mathfrak{a}$, deren Norm $\mathcal{N}(\mathfrak{a}) = |\mathfrak{o} : \mathfrak{a}|$ gleich 18 ist.

Aufgabe 9.2

Sei R ein Integritätsbereich mit Quotientenkörper K. Betrachten Sie, wie in der Vorlesung für Ganzheitsringe, die kommutative Halbgruppe $\mathcal{I}(R)$ aller von $\{0\}$ verschiedenen Ideale von R unter der Idealmultiplikation $\circ$. Für $\mathfrak{a} \in \mathcal{I}(R)$ sei $\mathfrak{a}^* = \{x \in K \mid x\mathfrak{a} \subseteq R\}$, und wir nennen $\mathfrak{a}$ *invertierbar*, falls $\mathfrak{a}^* \circ \mathfrak{a} = \{\sum_{i=1}^m x_i a_i \mid m \in \mathbb{N},\ x_i \in \mathfrak{a}^*,\ a_i \in \mathfrak{a}\}$ gleich R ist.

Sei R noethersch, und jedes Primideal $\mathfrak{p} \in \mathcal{I}(R)$ sei invertierbar: $\mathfrak{p}^* \circ \mathfrak{p} = R$.

(a) Zeigen Sie: Zu jedem $\mathfrak{a} \in \mathcal{I}(R)$ gibt es ein $m \in \mathbb{N}_0$ und Primideale $\mathfrak{p}_1, \dots, \mathfrak{p}_m \in \mathcal{I}(R)$ mit $\mathfrak{a} = \mathfrak{p}_1 \circ \dots \circ \mathfrak{p}_m$.

Hinweis. Führen Sie einen Widerspruchsbeweis. Nutzen Sie, daß R noethersch ist, um ein $\subseteq$-maximales Ideal $\mathfrak{a} \in \mathcal{I}(R)$ zu identifizieren, welches sich nicht als Produkt von Primidealen schreiben lassen. Nach dem Satz von Krull liegt $\mathfrak{a}$ dann seinerseits in einem maximalen Ideal $\mathfrak{p}_0 \trianglelefteq_{\max} R$. Zeigen Sie $\mathfrak{p}_0 \circ \mathfrak{a} \neq \mathfrak{a}$ (wie in der Vorlesung für Ganzheitsringe), und nutzen Sie zudem, daß $\mathfrak{p}_0$ invertierbar ist.

(b) Zeigen Sie: Die Primfaktorzerlegung in (a) ist, bis auf die Reihenfolge der Faktoren, sogar eindeutig, d. h., R ist ein Dedekindscher Ring.

Hinweis. Betrachten Sie für konkurrierende Darstellungen $\mathfrak{p}_1 \circ \dots \circ \mathfrak{p}_m = \mathfrak{q}_1 \circ \dots \circ \mathfrak{q}_n$ jeweils $\subseteq$-minimale Faktoren, um diese anschließend koordiniert zu “kürzen”.

(c) Folgern Sie: Jedes Ideal in $\mathcal{I}(R)$ ist invertierbar, und es gelten die Kürzungsregel und die Teilerregel:

$$\forall \mathfrak{a}, \mathfrak{b}, \mathfrak{c} \in \mathcal{I}(R): \ \mathfrak{a} \circ \mathfrak{b} = \mathfrak{a} \circ \mathfrak{c} \ \rightarrow \ \mathfrak{b} = \mathfrak{c} \qquad \text{und} \qquad \forall \mathfrak{a}, \mathfrak{b} \in \mathcal{I}(R): \ \mathfrak{a} \mid \mathfrak{b} \ \leftrightarrow \mathfrak{a} \supseteq \mathfrak{b}.$$

Aufgabe 9.3 (4 Punkte)

In $\mathfrak{o} = \mathbb{Z}[\sqrt{-17}]$ gilt $2 \cdot 3^2 = 18 = (1 + \sqrt{-17})(1 - \sqrt{-17})$.

(a) Erläutern Sie anhand dieser Gleichung, warum $\mathfrak{o}$ kein gaußscher Ring[1] ist.

Hinweis. Bestimmen Sie hierzu die Einheitengruppe $\mathfrak{o}^\times$ und vergewissern Sie sich dann, daß die Elemente 2, 3, $1 + \sqrt{-17}$, $1 - \sqrt{-17}$ paarweise nicht assoziiert und irreduzibel sind.

(b) Bestimmen Sie die Primfaktorisierung von $18\mathfrak{o}$ in $\mathcal{I}(\mathfrak{o})$ und finden Sie heraus, welche Gruppierung der beteiligten Primideale jeweils die Faktorisierung von $18\mathfrak{o}$ als $2\mathfrak{o} \circ (3\mathfrak{o})^2$ bzw. $(1 + \sqrt{-17})\mathfrak{o} \circ (1 - \sqrt{-17})\mathfrak{o}$ liefert.

Bitte wenden!

[1] auch: faktorieller Ring oder ZPE-Ring

Aufgabe 9.4 (4 Punkte)

Betrachten Sie den Polynomring $R = \mathbb{Z}[X]$. Aus der Algebra-Vorlesung ist bekannt, daß R ein gaußscher Ring ist. Sogar die Primelement in R sind gut beschreibbar.

(a) Geben Sie eine (möglichst genaue) Beschreibung der Primideale von R.

Hinweis. Erinnern Sie sich dazu unter anderem an den Begriff eines primitiven Polynoms über $\mathbb{Z}$ und daran, daß $\mathfrak{p} \trianglelefteq_{\text{prim}} R$ stets $\mathfrak{p} \cap \mathbb{Z} \trianglelefteq_{\text{prim}} \mathbb{Z}$ impliziert.

(b) Weisen Sie nach, daß $R = \mathbb{Z}[X]$ kein Dedekindscher Ring ist, indem Sie ein Ideal $\mathfrak{a} \in \mathcal{I}(R)$ finden, daß sich nicht als Produkt von Primidealen schreiben läßt.

Hinweis. Wenn Sie keine andere zündende Idee haben, versuchen Sie es mit dem Ideal, das von 6 und $X^2 + X + 1$ erzeugt wird.