Aufgabe 7

Wir benötigen zwei Vorüberlegungen.

Wenn wir konstruktiv arbeiten wollen, benötigen wir sogar noch eine weitere:

Behauptung. *Ein endlich erzeugtes Ideal $\mathfrak{a} = (x_1, \ldots, x_n) \subseteq R$ eines Integritätsbereichs R ist genau dann nicht das Nullideal, wenn es ein reguläres Element enthält.*

Beweis. Die Rückrichtung ist klar. Zur Hinrichtung können wir, da R ein Integritätsbereich ist, von jedem Erzeuger x_i prüfen, ob er null oder regulär ist. Der Fall, dass alle Erzeuger null sind, kann nach Voraussetzung nicht eintreten, daher gibt es ein Erzeuger, der nicht nicht null und somit regulär ist. □

Behauptung. *Sei R ein prüferscher Bereich und seien $\mathfrak{p}, \mathfrak{q}$ Primideale in R mit $\mathfrak{p} \subseteq \mathfrak{q}$. Ferner enthalte $\mathfrak{p}$ ein reguläres Element. Dann gilt sogar schon $\mathfrak{p} = \mathfrak{q}$.*

Beweis. Da R prüfersch ist, können wir $\mathfrak{p} = (\mathfrak{p} : \mathfrak{q})(\mathfrak{p} + \mathfrak{q}) = (\mathfrak{p} : \mathfrak{q}) \cdot \mathfrak{q}$ schreiben. Wegen der Primalität von $\mathfrak{p}$ gilt $\mathfrak{p} = \mathfrak{p} : \mathfrak{q}$ oder $\mathfrak{p} = \mathfrak{q}$. Im zweiten Fall sind wir fertig. Der erste kann nicht eintreten: Denn dann würde $\mathfrak{p} \cdot (1) = (\mathfrak{p} : \mathfrak{q}) \cdot \mathfrak{q} = \mathfrak{p}\mathfrak{q}$ folgen, also, da $\mathfrak{p}$ nach den Voraussetzungen invertierbar ist, $(1) = \mathfrak{q}$. □

Behauptung. *Sei R ein prüferscher Bereich. Dann sind Zerlegungen von Idealen (welche ein reguläres Element enthalten) in Primideale bis auf Umordnung eindeutig, falls sie existieren.*

Beweis. Sei $\mathfrak{a}$ ein Ideal, welches ein reguläres Element enthält, und seien $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ und $\mathfrak{q}_1, \ldots, \mathfrak{q}_m$ Primideale mit

$$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_n = \mathfrak{q}_1 \cdots \mathfrak{q}_m.$$

Nach der ersten Vorüberlegung enthalten auch alle aufgelisteten Primideale jeweils ein reguläres Element, denn es kann jeweils nicht der Fall sein, dass sie das Nullideal sind.

Insbesondere gilt $\mathfrak{q}_1 \cdots \mathfrak{q}_m \subseteq \mathfrak{p}_1$, also gibt es wegen der Primidealeigenschaft von $\mathfrak{p}_1$ ein $i \in \{1, \ldots, m\}$ mit $\mathfrak{q}_i \subseteq \mathfrak{p}_1$. Nach der Vorüberlegung gilt sogar $\mathfrak{p}_1 = \mathfrak{q}_i$, und da $\mathfrak{p}_1 = \mathfrak{q}_i$ invertierbar ist, folgt

$$\mathfrak{p}_2 \cdots \mathfrak{p}_n = \mathfrak{q}_1 \cdots \widehat{\mathfrak{q}_i} \cdots \mathfrak{q}_m.$$

Induktiv folgt die Behauptung. □

Teilaufgabe (α)

Behauptung. *Sei R ein dedekindscher Bereich, in dem jedes endlich erzeugte Ideal $\mathfrak{a} \subseteq R$ irreduzibel oder in echte Faktoren zerlegbar ist. Dann lässt sich jedes nichtverschwindende endlich erzeugte Ideal eindeutig als Produkt von Primidealen schreiben.*

Beweis. Die Eindeutigkeit haben wir bereits oben bewiesen. Zur Existenz können wir prüfen, ob ein gegebenes nichtverschwindendes Ideal $\mathfrak{a} \subseteq R$ irreduzibel ist. Falls ja, sind wir fertig, falls nicht, können wir es in zwei echte Ideale zerlegen. Diese können wir wieder auf Irreduzibilität prüfen, und so weiter.

Wir müssen noch zeigen, dass dieses Verfahren irgendwann endet. Dazu können wir uns die Situation als (nach unten wachsenden) verzweigten Baum veranschaulichen: Ganz oben an die Wurzel setzen wir das gegebene Ideal $\mathfrak{a}$. Die beiden Faktoren von $\mathfrak{a}$ setzen wir als die beiden Kinder der Wurzel. Deren Faktoren fügen wir wiederum als deren Kinder ein, und so weiter.

Insgesamt erhalten wir einen Baum, der mit endlich erzeugten Idealen beschriftet ist. In klassischer Logik gilt nun: Da der Ring R noethersch ist, stabilisiert sich jeder von der Wurzel ausgehende Pfad, da die Ideale entlang eines jeden Pfads aufsteigende Ketten bilden. Insgesamt kommen daher also nur endlich viele Ideale vor, daher endet das angegebene Faktorisierungsverfahren. (Wer die letzte Schlussfolgerung genauer nachlesen will, kann sich auf Wikipedia das Lemma von König anschauen.) □

Teilaufgabe (β)

Eine Vorüberlegung:

Behauptung. *Sei R ein dedekindscher Bereich, in dem jedes endlich erzeugte Ideal, welches nicht das Einsideal ist, maximal ist oder durch ein Ringelement echt zu einem weiteren Ideal, welches nicht das Einsideal ist, erweitert werden kann. Dann liegt jedes endlich erzeugte Ideal, welches nicht das Einsideal ist, in einem maximalen Ideal.*

Beweis. Wir beschreiben ein Verfahren, welches ausgehend von einem gegebenen endlich erzeugten Ideal $\mathfrak{a}$ ein aufsteigende Kette endlich erzeugter Ideale produziert: Ist das gegebene Ideal $\mathfrak{a}$ maximal, so produziere $\mathfrak{a}$. Sonst gibt es ein $x \in R$ mit $\mathfrak{a} \subsetneq \mathfrak{a} + (x) \subsetneq (1)$, produziere $\mathfrak{a} + (x)$. Fahre immer so fort.

Da R noethersch ist, muss die so produzierte Kette eine Stoppstelle aufweisen. Das jeweils neu produzierte Ideal ist aber genau dann gleich dem Ausgangsideal, wenn das Ausgangsideal maximal war. Damit folgt die Behauptung. □

Behauptung. *Sei R ein dedekindscher Bereich, in dem jedes endlich erzeugte Ideal maximal ist oder durch ein Ringelement echt zu einem weiteren Ideal, welches nicht das Einsideal ist, erweitert werden kann. Dann lässt sich jedes nichtverschwindende endlich erzeugte Ideal, welches nicht das Einsideal ist, eindeutig als Produkt von Primidealen schreiben.*

Beweis. Wie produzieren eine aufsteigende Kette endlich erzeugter Ideale nach folgendem Verfahren: Ein gegebenes endlich erzeugtes Ideal $(0) \subsetneq \mathfrak{a} \subsetneq (1)$ prüfen wir auf Maximalität. Falls es maximal ist, produzieren wir $\mathfrak{a}$ und fahren damit fort. Sonst finden wir ein maximales Ideal $\mathfrak{m}$ mit $\mathfrak{a} \subseteq \mathfrak{m}$. Da R prüfersch ist, gilt $\mathfrak{a} = (\mathfrak{a} : \mathfrak{m})(\mathfrak{a} + \mathfrak{m}) = (\mathfrak{a} : \mathfrak{m}) \cdot \mathfrak{m}$. Wir produzieren das über $\mathfrak{a}$ liegende Ideal $(0) \subsetneq \mathfrak{a} : \mathfrak{m} \subsetneq (1)$ und fahren damit fort. (Es kann nicht der Fall sein, dass $\mathfrak{a} = \mathfrak{a} : \mathfrak{m}$. Denn sonst wäre $\mathfrak{a} = (\mathfrak{a} : \mathfrak{m}) \cdot \mathfrak{m} = \mathfrak{a}\mathfrak{m}$ und damit, da $\mathfrak{a}$ invertierbar, $\mathfrak{m} = (1)$.)

Da R noethersch ist, muss diese Kette eine Stoppstelle aufweisen. Das ist genau dann der Fall, wenn das jeweilige Ausgangsideal maximal war. Somit erhalten wir eine endliche Zerlegung als Produkt maximaler Ideale. Da maximale Ideale insbesondere prim sind, folgt die Behauptung. $\square$