Anmerkungen und Lösungen zu

Einführung in die Algebra

Blatt 6

Jendrik Stelzner

Letzte Änderung: 16. Dezember 2017

Aufgabe 4

(a)

Wir bemerken zunächst einige (intuitive) Aussagen über Primfaktorzerlegungen in faktoriellen Ringen:

Lemma 1. *Es seien $x, y \in R$ mit $x, y \neq 0$, so dass x ein Teiler von y ist. Dann lässt sich jede Primfaktorzerlegung $x = \varepsilon p_1 \cdots p_n$ von x zu einer Primfaktorzerlegung $y = \varepsilon' p_1 \cdots p_n p_{n+1} \cdots p_m$ von y ergänzen.*

Beweis. Es gibt $z \in R$ mit $xz = y$, und es gilt $z \neq 0$, da $y \neq 0$ gilt. Also besitzt z eine Primfaktorzerlegung $z = \delta p_{n+1} \cdots p_m$. Dann gilt

$$y = xz = \varepsilon\delta p_1 \cdots p_n p_{n+1} \cdots p_m \,,$$

und die Aussage ergibt sich mit $\varepsilon' \coloneqq \varepsilon\delta$. □

Für $x \in R$, $x \neq 0$ mit Primfaktorzerlegung $x = \varepsilon p_1 \cdots p_n$ bezeichnen wir mit $\nu(x) \coloneqq n$ die Anzahl der vorkommenden Primfaktoren (inklusive Vielfachheit). Die Zahl $\nu(x)$ ist wohldefiniert, da die Primfaktorzerlegung bis Einheiten und Permutation der Faktoren eindeutig ist.

Lemma 2. *Es seien $x, y \in R$ mit $x, y \neq 0$.*

1. *Es gilt genau dann $\nu(x) = 0$, wenn x eine Einheit ist.*
2. *Es gilt $\nu(xy) = \nu(x) + \nu(y)$.*
3. *Ist x ein Teiler von y, so gilt $\nu(x) \leq \nu(y)$.*
4. *Ist x ein echter Teiler von y, also $(y) \subsetneq (x)$, so gilt $\nu(x) < \nu(y)$.*

Beweis.

1. In der Primfaktorzerlegung $x = \varepsilon p_1 \cdots p_n$ gilt $n = 0$ und somit $x = \varepsilon \in R^\times$.
2. Da R ein Integritätsbereich ist, gilt auch $xy \neq 0$. Es seien $x = \varepsilon p_1 \cdots p_n$ und $y = \delta q_1 \cdots q_m$ Primfaktorzerlegungen. Dann
$$xy = (\varepsilon\delta) p_1 \cdots p_n q_1 \cdots q_m$$
eine Primfaktorzerlegung von xy und somit
$$\nu(xy) = n + m = \nu(x) + \nu(y)\,.$$
3. Es gibt $z \in R$ mit $y = xz$. Es gilt $z \neq 0$, da $y \neq 0$ gilt, weshalb $\nu(z)$ definiert ist. Somit gilt
$$\nu(y) = \nu(xz) = \nu(x) + \nu(z) \leq \nu(x)\,.$$
4. Ansonsten gilt in der obigen Situation $\nu(z) = 0$, weshalb z dann eine Einheit ist. Deshalb gilt dann
$$(y) = (xz) = (x)\,.$$

□

(i)

Es sei $p \in R$ irreduzibel, und es seien $x, y \in R$ mit $p \mid xy$. Gilt $x = 0$ oder $y = 0$, so gilt $p \mid x$ oder $p \mid y$.

Ansonsten gibt es Primfaktorzerlegungen $x = \delta q_1 \cdots q_n$ und $y = \delta' q'_1 \cdots q'_m$ Primfaktorzerlegungen. Dann ist
$$xy = (\delta\delta') q_1 \cdots q_n q'_1 \cdots q'_m \tag{1}$$
eine Primfaktorzerlegung von xy. Da p irreduzibel ist und $p \mid xy$ gilt, lässt sich p nach Lemma 1 zu einer Primfaktorzerlegung
$$xy = \varepsilon p p_2 \cdots p_r \tag{2}$$
ergänzen. Da R faktoriell ist, sind die beiden Primfaktorzerlegungen (1) und (2) eindeutig bis auf Einheiten und Permutation. Es gilt deshalb $p \mid q_i$ oder $p \mid q'_i$ für passendes i, und somit $p \mid x$ oder $p \mid y$.

(ii)

Wir nehmen an, dass nicht jede aufsteigende Kette von Hauptidealen stabilisieren würde. Dann gibt es eine unendliche echt aufsteigende Kette von Hauptidealen
$$(a_0) \subsetneq (a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq (a_4) \subsetneq \cdots$$
Dann gilt $a_i \neq 0$ für alle $i \geq 1$ (denn sonst wäre $(a_i) = 0$ für ein solches i, und damit bereits $(a_i) = \cdots = (a_0) = 0$), und für jedes $i \geq 1$ ist a_{i+1} ein echter Teiler von a_i. Nach Lemma 2 erhalten wir eine unendliche absteigende Kette
$$\nu(a_1) > \nu(a_2) > \nu(a_3) > \nu(a_4) > \cdots$$
Dies ist aber nicht möglich.

(b)

Wir müssen zeigen, dass es für jedes Element $x \in R$ mit $x \neq 0$ eine Zerlegung

$$x = \varepsilon p_1 \cdots p_n$$

in eine Einheit $\varepsilon \in R^\times$ und irreduzible Elemente $p_1, \ldots, p_n \in R$ gibt, und dass eine solche Zerlegung eindeutig bis auf Einheiten und Permutation ist.

Existenz

Lemma 3. *Es sei $x \in R$, und es sei $x = yz$ ein Zerlegung mit $z \notin R^\times$. Dann gilt $(x) \subsetneq (y)$.*

Beweis. Es gilt $y \mid x$ und somit $(x) \subseteq (y)$. Wäre $(x) = (y)$, so gebe es ein $z' \in R$ mit $y = xz'$. Dann wäre $x = yz = xzz'$ und somit $1 = zz'$, da R ein Integritätsbereich ist. Dann wäre z eine Einheit mit $z^{-1} = z'$, im Widerspruch zu $z \notin R^\times$. □

Wir nehmen an, dass es ein Element $x \in R$ mit $x \neq 0$ gibt, dass keine entsprechende Zerlegung besitzt. Dann ist x inbesondere keine Einheit und auch nicht irreduzibel. Es gibt deshalb nicht-Einheiten $y_1, y_2 \in R$ mit $x = y_1 y_2$; dabei gelten $y, z \neq 0$ da $x \neq 0$. Würden x und z entsprechende Zerlegungen besitzten, so würden sich diese zu einer Zerlegung von x kombinieren lassen. Also hat x oder y keine entsprechende Zerlegung; wir können o.B.d.A. davon ausgehen, dass y keine Zerlegung hat. Da z keine Einheit ist, gilt $(x) \subsetneq (y)$ nach Lemma 3.

Wir setzen $a_0 \coloneqq x$ und $a_1 \coloneqq y$. Durch Induktion erhalten wir eine unendliche aufsteigende Kette von Hauptidealen

$$(a_0) \subsetneq (a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq \cdots$$

Im Widerspruch zur Annahme (ii).

Bemerkung 4. Ein kommutativer Ring R heißt *noethersch*, wenn jede aufsteigende Kette

$$I_0 \trianglelefteq I_1 \trianglelefteq I_2 \trianglelefteq I_3 \trianglelefteq \cdots$$

von Idealen $I_j \trianglelefteq R$ stabilisiert. Wir haben soeben insbesondere gezeigt, dass in einem notherschen Ring R jedes Element $x \in R$ eine Zerlegung $x = \varepsilon p_1 \cdots p_n$ in eine Einheit $\varepsilon \in R^\times$ und irreduzible Elemente $p_1, \ldots, p_n \in R$ besitzt.

Eindeutigkeit

Es seien

$$x = \varepsilon p_1 \cdots p_n = \delta q_1 \cdots q_m$$

Zerlegungen in Einheiten $\varepsilon, \delta \in R^\times$ und irreduzible Elemente $p_i, q_j \in R$. Wir zeigen die gewünschte Eindeutigkeit per Induktion über n:

Gilt $n = 0$, so ist $x = \varepsilon \in R^\times$ eine Einheit. Dann gilt $q_j \mid x \mid 1$ für alle j, weshalb jedes q_j eine Einheit ist. Irreduzible Elemente sind aber per Definition keine Einheiten,

weshalb $m = 0$ gelten muss. Dann ist also $x = \varepsilon = \delta$, und die beiden Zerlegungen stimmen überein.

Es sei nun $n > 0$. Nach Annahme (i) ist p_1 prim. Aus $p_1 \mid x = \delta q_1 \cdots q_m$ folgt damit, dass $p_1 \mid \delta$, oder dass $p_1 \mid q_j$ für ein j. Wäre $p_1 \mid \delta$, so wäre p_1 eine Einheit, im Widerspruch zur Irreduziblität von p_1. Also gilt $p_1 \mid q_j$ für ein j; wir können o.B.d.A. davon ausgehen, dass $p_1 \mid q_1$. Es gibt also $\delta' \in R$ mit $q_1 = p_1\delta'$. Da q_1 irreduzibel ist folgt dabei, dass bereits p_1 oder δ' eine Einheit ist; p_1 ist wegen Irreduziblität keine Einheit, so dass δ' eine Einheit ist. Also sind p_1 und q_1 gleich bis auf die Einheit δ'.

Es gilt nun

$$x = \varepsilon p_1 \cdots p_n = \delta q_1 \cdots q_m = \delta\delta' p_1 q_2 \cdots q_m. \tag{3}$$

Da R ein Integritätsbereich ist, können wir die obige Gleichung durch $p_1 \neq 0$ teilen, und erhalten, dass bereits

$$\varepsilon p_2 \cdots p_n = (\delta\delta') q_2 \cdots m \tag{4}$$

Nach Induktionsvoraussetzung sind beide Seiten von (4) gleich bis auf Permutation und Einheiten. Da p_1 und q_1 auch gleich bis auf Einheit sind, sind in (3) bereits beide Zerlegungen bis auf Permutation und Einheiten gleich.