Lösung zu Zettel 5, Aufgaben 3 und 4

Jendrik Stelzner

29. November 2016

Aufgabe 3

Sofern nicht anders angegeben, handelt es sich bei R und S im folgenden jeweils um den kommutativen Ring R und die multiplikative Teilmenge $S \subseteq R$ aus der Aufgabenstellung. Wir betrachten im Folgenden nur den Fall, dass $0 \notin S$, denn sonst ist ohnehin $R_S = 0$.

Bevor wir mit der Aufgabe beginnen, merken wir an, dass

$$\frac{r_1}{s_1} = \frac{r_2}{s_2} \iff r_1 s_2 = r_2 s_1 \qquad \text{für alle } \frac{r_1}{s_1}, \frac{r_2}{s_2} \in R_S,$$

da R ein Integritätsbereich ist. Diese einfache Form des Vergleichs zweier Brüche wird uns im Folgenden das Leben erleichtern, und wir werden sie verwenden, ohne explizit auf sie hinzuweisen.

Unter anderen erhalten wir damit das folgende (hoffentlich bekannte) Resultat, an das wir hier erinnern möchten:

Lemma 1. Es sei R ein Integritätsbereich und $S \subseteq R$ eine multiplikative Teilmenge mit $0 \notin S$.

1. Die Lokalisierung R_S ist ebenfalls ein Integritätsbereich.
2. Der kanonische Ringhomomorphismus $i \colon R \to R_S, r \mapsto r/1$ ist injektiv.

Beweis. 1. Da $0 \notin S$ gilt $R_S \neq 0$. Für $r_1/s_1, r_2/s_2 \in R_S$ mit

$$\frac{0}{1} = \frac{r_1}{s_1}\frac{r_2}{s_2} = \frac{r_1 r_2}{s_1 s_2}$$

gilt $r_1 r_2 = 0$. Da R ein Integritätsbereich ist, gilt damit bereits $r_1 = 0$ oder $r_2 = 0$, und somit bereits $r_1/s_1 = 0$ oder $r_2/s_2 = 0$.

2. Für $r \in \ker \iota$ gilt $r/1 = 0/1$ und somit $r = 0$.

□

Bemerkung 2. Ist R ein Integritätsbereich und $S \subseteq R$ eine multiplikative Teilmenge mit $0 \notin S$, so können wir die Lokalisierung R_S mit dem Unterring

$$\left\{ \frac{r}{s} \,\middle|\, r \in R, s \in S \right\} \subseteq Q(R)$$

des Quotientenkörpers $Q(R)$ identifzieren.

Wir erinnern auch an die folgende grundlegende Aussage über Einheiten in einem beliebigen kommutativen Ring:

Lemma 3. Es sei R ein kommutativer Ring, $r \in R$ und $\varepsilon \in R^\times$ eine Einheit. Gilt $r \mid \varepsilon$, so ist auch r eine Einheit.

Beweis. Da $r \mid \varepsilon$ gibt es $s \in S$ mit $rs = \varepsilon$. Dann ist $1 = \varepsilon\varepsilon^{-1} = rs\varepsilon^{-1}$ und somit r eine Einheit mit $r^{-1} = s\varepsilon^{-1}$. □

Hieraus ergibt sich ein für diese Aufgabe wichtiges Resultat:

Behauptung 4. Es sei R ein kommutativer Ring und $S \subseteq R$ eine multiplikative Teilmenge. Ein Element $r/s \in R_S$ ist genau dann eine Einheit, wenn $r \mid s'$ für ein $s' \in S$ gilt.

Beweis. Da $(1/s) \in R_S^\times$ (mit $(1/s)^{-1} = (s/1)$) ist genau dann $r/s \in R_S^\times$ wenn $r/1 \in R_S^\times$. Wir können also o.B.d.A. davon ausgehen, dass $s = 1$.

Gilt $r \mid s'$ für ein $s' \in S$, so gilt auch $(r/1) \mid (s'/1)$, und da $s'/1 \in R_S^\times$ gilt dann nach Lemma 3 auch $r/1 \in R_S^\times$.

Gilt andererseits $r/1 \in R_S^\times$, so gibt es $r'/s' \in R_S$ mit

$$\frac{1}{1} = \frac{r}{1}\frac{r'}{s'} = \frac{rr'}{s'}.$$

Dann gibt es $t \in S$ mit $trr' = ts'$ und somit inbesondere $r \mid ts' \in S$. □

Bemerkung 5. Ist R eine kommutativer Ring und $S \subseteq R$ eine multiplikative Teilmenge, so heißt S *saturiert*, falls

$$xy \in S \implies x, y \in S \qquad \text{für alle } x, y \in R.$$

Jede multiplikative Teilmenge $S \subseteq R$ ist in einer saturierten multiplikativen Teilmenge $\overline{S} \subseteq R$ enthalten, die minimial mit dieser Eigenschaft ist. Man bezeichnet diese als die *Saturierung* von S. Abstrakt lässt sie sich als

$$\overline{S} = \bigcap \{T \subseteq R \mid T \text{ ist eine saturierte multiplikative Menge mit } S \subseteq T\}$$

konstruieren; man beachte dabei, dass R selbst eine saturierte multiplikative Menge ist, die S enthält, und somit die obige Menge nicht leer. Etwas konkreter (und für uns interessanter) lässt sich $\overline{S}$ auch als

$$\overline{S} = \{r \in R \mid \text{es gibt } s \in S \text{ mit } r \mid s\}$$

konstruieren.

Die Saturierung $\overline{S}$ hat die angenehme Eigenschaft, dass die Identitäts $\mathrm{id}_R\colon R \to R$ einen Isomorphismus

$$R_S \to R_{\overline{S}}, \quad \frac{r}{s} \mapsto \frac{r}{s}$$

induziert; die Lokalisierung R_S hängt also gar nicht von S selbst ab, sondern nur von der Saturierung $\overline{S}$.

Inbesondere wird jedes Element $r \in R$ mit $r \in \overline{S}$ zu einer Einheit in $R_{\overline{S}}$, und wegen des obigen Isomorphismus' auch zu einer Einheit in R_S. Behauptung 4 ist eine Verschärfung dieser Beobachtung, und zeigt, dass ein Element $r/s \in R_S$ genau dann eine Einheit in R_S ist, wenn $r \in \overline{S}$; die Einheiten in R_S sind also genau die Brüche, deren Zähler in der Saturierung von S enthalten sind.

Wenn wir, wie in dieser Aufgabe, nicht nur mit Elementen aus S hantieren, sondern auch noch mit Teilbarkeitsbedingungen der Form $r \mid s$ mit $r \in R$ und $s \in S$, so können wir uns dies als ein verstecktes Auftreten der Saturierung $\overline{S}$ verstehen.

i)

Wir müssen zunächst zeigen, dass die Elemente $p/1 \in R_S$ mit $p \in P_S$ keine Einheiten sind. Dies ergibt sich aus der folgenden Behauptung.

Behauptung 6. Ist $p \in R$ ein Primelement, so ist $p/1 \in R_S$ genau dann eine Einheit, wenn $p \notin P_S$. Es ist also P_S die Menge aller Primelement aus R, die in R_S nicht zu einer Einheit werden.

Beweis. Man schränke Behauptung 4 auf die Primelemente von R ein. □

Es seien nun $r_1/s_2, r_2/s_2 \in R_S$ mit

$$\frac{p}{1} \,\Big|\, \frac{r_1}{s_1}\frac{r_2}{s_2}\,.$$

Dann gibt es ein $r_3/s_3 \in R_S$ mit

$$\frac{p}{1}\frac{r_3}{s_3} = \frac{r_1}{s_1}\frac{r_2}{s_2},$$

also $pr_3s_1s_2 = r_1r_2s_3$. Dann ist $p \mid (r_1r_2s_3)$ und somit $p \mid r_1$, $p \mid r_2$ oder $p \mid s_3$. Da $p \in P_S$ gilt inbesondere $p \nmid s_3$, weshalb $p \mid r_1$ oder $p \mid r_2$. Damit ist auch $(p/1) \mid (r_1/1)$ oder $(p/1) \mid (r_2/1)$, und somit $(p/1) \mid (r_1/s_1)$ oder $(p/1) \mid (r_2/s_2)$.

ii)

Es sei $p/s \in R_S$ ein Primelement. Da R faktoriell ist gibt es eine Primfaktorzerlegung $p = p_1^{n_1} \cdots p_t^{n_t}$, wobei $n_1, \ldots, n_t \geq 1$ und $p_1, \ldots, p_t \in R$ paarweise nicht-assoziierte Primelemente sind

Hierbei gibt es ein $1 \leq i \leq t$ mit $p_i \in P_S$: Andernfalls gebe es für jedes $i = 1, \ldots, t$ ein $s_i \in S$ mit $p_i \mid s_i$. Für $s' := s_1^{n_1} \cdots s_t^{n_t} \in S$ würde dann $p \mid s'$ gelten, und nach Behauptung 4 wäre dann $p/s \in R_S$ eine Einheit. Dies stünde im Widerspruch dazu, dass p/s prim ist.

Durch passende Nummerierung der p_i kann davon ausgegangen werden, dass $p_1 \in P_S$. Für $q \coloneqq p_1^{n_1-1} p_2^{n_2} \cdots p_t^{n_t}$ gilt dann $p = p_1 q$ und somit

$$\frac{p}{s} = \frac{p_1 q}{s} = \frac{p_1}{1}\frac{q}{s}. \tag{1}$$

Nach Lemma 1 ist R_S ein Integritätsbereich, und das Primelement p/s deshalb irreduzibel. Wegen der Irreduziblität von p/s folgt aus (1), dass p_1/s oder q/s eine Einheit in R_S ist. Wegen $p_1 \in P_S$ wissen wir aus dem vorherigen Aufgabenteil, dass $p_1/1$ prim in R_S ist, und somit inbesondere keine Einheit. Folglich ist q/s eine Einheit in R_S. Nach (1) ist p/s somit assoziiert zu $p_1/1$ mit $p_1 \in P_S$.

Warnung 7. Es gilt für ein Primelement $p/s \in R_S$ nicht notwendigerweise, dass $p \in R$ ebenfalls ein Primelement ist.

Man betrachte etwa den faktoriellen Ring $R = \mathbb{Z}$ sowie die multiplikative Teilmenge $S = \{2^n \mid n \in \mathbb{N}\} \subseteq R$. Da $3 \nmid 2^n$ für alle $n \in \mathbb{N}$ ist $3/1 \in R_S$ nach Aufgabenteil i) ein Primelement. Damit ist auch $6/1 \in R_S$ ein Primelement, denn $3/1$ und $6/1$ sind über die Einheit $2/1 \in R_S^\times$ assoziiert zueinander. Aber 6 ist ein Primelement in $\mathbb{Z}$.

iii)

Es seien $p_1, p_2 \in P_S$.

Gilt $p_1 \sim p_2$, so gibt es ein $\varepsilon \in R^\times$ mit $p_1 = \varepsilon p_2$. Dann gilt auch $(p_1/1) = (\varepsilon/1)(p_2/1)$ mit $\varepsilon/1 \in R_S^\times$ und somit $(p_1/1) \sim (p_2/1)$.

Gilt $(p_1/1) \sim (p_2/1)$, so gibt es ein $r/s \in R_S^\times$ mit

$$\frac{p_1}{1} = \frac{r}{s}\frac{p_2}{1}.$$

Dann gilt $p_1 s = r p_2$ und somit $p_2 \mid (p_1 s)$. Da p_2 prim ist, folgt daraus, dass $p_2 \mid p_1$ oder $p_2 \mid s$. Da $p_2 \in P_S$ gilt $p_2 \nmid s$, also muss $p_2 \mid p_1$. Da p_1 und p_2 prim in R sind, folgt hieraus bereits, dass $p_1 \sim p_2$.

Bemerkung 8. 1. Zusammen mit Aufgabenteil ii) erhalten wir, dass die Assoziiertheitsklassen der Primelemente $q \in R_S$ genau dan Assoziiertheitsklassen der Primelemente $p \in R$ entsprechen, für die $p \in P_S$; nach Behauptung 6 sind dies genau die Primelemente von R, die in R_S keine Einheit werden.

   Anschaulich sind die Primelemente aus R_S also (bis auf Assoziiertheit) die Primelemente aus R, die beim Übergang zu R_S nicht invertierbar werden.

2. Dieser guter Zusammenhang zwischen den Primelementen aus R und R_S beruhrt darauf, dass R faktoriell ist. Ist R ein beliebiger kommutativer Ring und $S \subseteq R$ eine multiplikative Teilmenge, so betrachtet man anstelle der Primelemente von R, bzw. R_S, die Primideale dieser Ringe. Zwischen diesen gibt es dann immer noch einen wichtigen Zusammenhang:

Es gibt eine Bijektion

$$\begin{aligned}\{\text{Primideale } \mathfrak{p} \subseteq R \text{ mit } \mathfrak{p} \cap S = \emptyset\} &\longleftrightarrow \{\text{Primideale } \mathfrak{q} \subseteq R_S\},\\ \mathfrak{p} &\longmapsto \left\{ \frac{r}{s} \,\middle|\, r \in \mathfrak{p}, s \in S \right\},\\ \left\{ r \in R \,\middle|\, \frac{r}{1} \in \mathfrak{q} \right\} &\longmapsto \mathfrak{q}.\end{aligned}$$

Man bemerke, dass für ein Primelement $p \in R$ genau dann $(p) \cap S = \emptyset$, wenn S kein Vielfaches von p enhtält, d.h. wenn p kein Element aus S teilt. Sieht man Primideale $\mathfrak{p} \subseteq R$ als Verallgemeinerung von Primelementen $p \in R$, so ist daher die Bedingung, dass $\mathfrak{p} \cap S = \emptyset$ gilt, eine Verallgemeinerung der in dieser Aufgaben genutzten Bedingung, dass p kein Element aus S teilt.

Umgekehrt lässt sich Aufgabenteil i) auch aus diesem allgemeineren Zusammenhang herleiten.

iv)

Es sei $P \subset R$ ein Repräsentantensystem der Assoziiertheitsklassen von Primelementen aus R.

Wir bemerken zunächst, dass nach Behauptung 6 die Elemente $p/1$ für $p \in R$ prim mit $p \notin P_S$ Einheiten sind. Daher ergibt der Ausdruck $(p/1)^n$ mit $p \in R$ prim und $p \notin P_S$ für alle $n \in \mathbb{Z}$ Sinn.

Ist nun $r/s \in R_S$ mit $r/s \neq 0$, so gibt es in R Primfaktorzerlegungen $r = u_1 \prod_{p \in P} p^{n_p}$ und $s = u_2 \prod_{p \in P} p^{m_p}$ mit $u_1, u_2 \in R^\times$. Für jedes Primelement $p \in P$ mit $p \in P_S$ gilt $p \nmid s$ und somit $m_p = 0$; deshalb ist $(1/p)^{-m_p}$ nicht nur für $p \notin P \cap P_S$ definiert, sondern für alle $p \in P$.

Da nach Lemma 1 der kanonische Ringhomomorphismus $\iota \colon R \to R_S, x \mapsto x/1$ injektiv ist, können wir im Folgendem außerdem R mit dem Unterring $\operatorname{im} \iota \subseteq R$ identifizieren. Wir unterscheiden also nicht zwischen $r \in R$ und $r/1 \in R_S$.

Bemerkung 9. Wir hätten diese Identifikation bereits früher machen können, haben dies aber bewusst nicht getan. Die Leser, denen diese Identifikation mitfällt, mögen sich an Bemerkung 2 erinnern: Wir können R_S also Unterring des Quotientenkörpers $Q(R)$ auffassen, und auch R fasst man für gewöhnlich als Unterring von $Q(R)$ auffasst, siehe etwa $\mathbb{Z}$ als Unterring von $\mathbb{Q}$. Unter diesen Identifikationen ergibt sich in $Q(R)$ dann die Inklusion $R \subseteq R_S$.

Damit ergibt sich nun insgesamt, dass

$$\frac{r}{s} = \frac{u_1 \prod_{p \in P} p^{n_p}}{u_2 \prod_{p \in P} p^{m_p}} = u_1 \prod_{p \in P} p^{n_p} u_2^{-1} \prod_{p \in P} p^{-m_p} = u_1 u_2^{-1} \prod_{p \in P} p^{n_p - m_p}.$$

Da $u_1 u_2^{-1} \in R^\times$ und $n_p - m_p \geq n_p \geq 0$ für alle $p \in P \cap P_S$ gelten, zeigt dies die Existenz.

Zum Beweis der Eindeutigkeit seien $u_1, u_2 \in R^\times$ und $n_p, m_p \in \mathbb{Z}$ für $p \in P$ mit $n_p = 0$ und $m_p = 0$ für fast alle $p \in P$, sowie $n_p, m_p \geq 0$ für alle $p \in P_S \cap P$, so dass

$$u_1 \prod_{p \in P} p^{n_p} = u_2 \prod_{p \in P} p^{m_p}.$$

Um zu zeigen, dass $u_1 = u_2$ und $n_p = m_p$ für alle $p \in P$ dürfen wir diese Gleichung zunächst beliebig mit Elementen $p \in P$ multiplizieren; hierbei ändern sich auf beiden Seiten die Exponenten n_p und m_p um gleiche Weise. Durch Multiplikation mit $\prod_{p\in P} p^{|n_p|+|m_p|}$ können wir deshalb davon ausgehenn, dass bereits $n_p, m_p \geq 0$ für alle $p \in P$. Da die Elemente $p \in P$ paarweise nicht assoziierte Primelemente sind, folgt die Eindeutigkeit nun daraus, dass R faktoriell ist.

Bemerkung 10. In der Aufgabenstellung wird nicht mit einem Repräsentantensystem $P \subseteq R$ der Assozziertheitsklassen der Primelemente von R gearbeitet, sondern wird direkt ein Produkt $\prod_{[p]}$ über alle Assoziiertheitsklassen von Primelementen von R genutzt.

Dieses Vorgehen führt allerdings zu einem Problem: Die Assozziertheitsklasse $[p]$ definiert ein Primelement $p \in R$ nur bis auf Assozziertheit. Dies führt dazu, dass auch der Ausdruck $\prod_{[p]} p^{n_p}$ nur bis auf Assoziiertheit mit einer Einheit aus R Sinn ergibt. In der auf dem Aufgabenzettel angegeben Darstellung $u \prod_{[p]} p^{n_p}$ sind dann zwar die Potenten $n_p \in \mathbb{Z}$ wohldefiniert, nicht aber die Einheit $u \in R^\times$.

Als ein konkretes Beispiel betrachte man den Ring $R = \mathbb{Z}$ und die multiplikatve Menge $S = \mathbb{Z}\backslash\{0\}$. Dann gilt $R_S = Q(R) = Q(\mathbb{Z}) = \mathbb{Q}$. Betrachtet man das Element $x = 1/8 \in \mathbb{Q}$, so lässt sich dieses als $1/8 = 1 \cdot 2^{-3}$ schreiben, aber auch als $(-1)\cdot(-2)^{-3}$. Die Potenz -3 ist zwar gleich, die Vorfaktoren $1, -1 \in \mathbb{Z}^\times$ unterscheiden sich jedoch. Da 2 und -2 die gleiche Assoziiertheitsklasse darstellen, müssen wir, um dieses Problem zu lösen, angeben, welchen dieser beiden Repräsentanten wir nutzen.

Fixiert man beispielsweise das Repräsentantensystem

$$P = \{2, 3, 5, 7, \dots\} = \{p \in \mathbb{Z} \mid p \text{ ist prim und positiv}\},$$

so ergibt sich bezüglich P die Schreibweise $1/8 = 1 \cdot \prod_{p\in P} p^{n_p}$ $n_2 = -3$, wobei $1 \in \mathbb{Z}^\times$, sowie $n_2 = -3$ und $n_p = 0$ für alle $p \in P$ mit $p \neq 2$. Fixiert man hingegen das Repräsentantensystem

$$P' = \{-2, 3, 5, 7, \dots, \} = \{-2\} \cup \{p \in \mathbb{Z} \mid p \text{ ist prim mit } p \geq 5\}$$

so ergibt bezüglich P' die eindeutige Schreibweise $1/8 = (-1) \cdot \prod_{p\in P} p^{m_p}$ mit $m_{-2} = -3$ und $m_p = 0$ für alle $p \in P$ mit $p \neq -2$.

Der Preis für die Eindeutigkeit des Vorfaktors $u \in R^\times$ liegt also darin, dass wir festlegen müssen, welche Primelement wir verwenden.

Aufgabe 4

Wir nehmen an, es gebe eine Nullstelle $x \in Q(R)$ von f, die nicht schon in R liegt. Für $x = p/q$ ist dann insbesondere $x \neq 0$ und somit $p \neq 0$. Wir können o.B.d.A. davon ausgehen, dass ggT$(p, q) = 1$. Deshalb gibt es Primfaktorzerlegungen $p = p_1^{n_1} \cdots p_s^{n_s}$ und $q = q_1^{m_1} \cdots q_t^{n_t}$, so dass die Primelemente $p_1, \dots, p_s, q_1, \dots, q_t \in P$ paarweise nicht assoziiert sind, und $n_i, m_j \geq 1$ für alle $i = 1, \dots, s$ und $j = 1, \dots, t$. Ist $f(X) = X^d + \sum_{i=0}^{n} a_i X^i$,

so erhalten wir, dass

$$0 = f(x) = x^d + \sum_{i=0}^{d-1} a_i x^i = \left(\frac{p_1^{n_1} \cdots p_s^{n_s}}{q_1^{m_1} \cdots q_t^{m_t}}\right)^d + \sum_{i=0}^{d} a_i \left(\frac{p_1^{n_1} \cdots p_s^{n_s}}{q_1^{m_1} \cdots q_t^{m_t}}\right)^i$$
$$= \frac{(p_1^{n_1} \cdots p_s^{n_s})^d}{(q_1^{m_1} \cdots q_t^{m_t})^d} + \sum_{i=0}^{d-1} a_i \frac{(p_1^{n_1} \cdots p_s^{n_s})^i}{(q_1^{n_1} \cdots q_s^{n_s})^i}.$$

Durch Multiplikation mit $(q_1^{m_1} \cdots q_t^{m_t})^d$ erhalten wir in R die Gleichung

$$0 = (p_1^{n_1} \cdots p_s^{n_s})^d + \sum_{i=0}^{d-1} a_i (p_1^{n_1} \cdots p_s^{n_s})^i (q_1^{m_1} \cdots q_s^{m_t})^{d-i}. \tag{2}$$

Wegen der Annahme $x \notin R$ gilt $t \geq 1$. Damit erhalten wir aus (2), dass

$$0 \equiv (p_1^{n_1} \cdots p_s^{n_s})^d \mod q_1$$

und somit

$$q_1 \mid (p_1^{n_1} \cdots p_s^{n_s})^d = \underbrace{p_1 \cdots p_1}_{n_1 d} \underbrace{p_2 \cdots p_2}_{n_2 d} \cdots \underbrace{p_s \cdots p_s}_{n_s d}.$$

Da q_1 prim ist, folgt hieraus, dass $q_1 \mid p_i$ für ein $1 \leq i \leq n$. Dann ist aber $q_1 \sim p_i$, im Widerspruch dazu, dass $p_1, \ldots, p_s, q_1, \ldots, q_t$ paarweise nicht-assoziiert sind.