

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

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

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. Ist R ein Integritätsbereich und $S \subseteq R$ eine multiplikative Teilmenge mit $0 \notin S$, so ist auch R_S ein Integritätsbereich.

Beweis. 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 $r_2/s_2 = 0$. \square

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

Lemma 2. 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 $r^{-1} = s\varepsilon^{-1}$. \square

Hieraus ergibt sich ein für diese Aufgabe wichtiges Resultat:

Behauptung 3. 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 2 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 insbesondere $r \mid ts' \in S$. \square

Bemerkung 4. Ist R ein kommutativer Ring und $S \subseteq R$ eine multiplikative Teilmenge, so heißt S *saturiert*, falls

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

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

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

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 \bar{S} auch als

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

konstruieren.

Die Saturierung \bar{S} hat die angenehme Eigenschaft, dass die Identitäts $\text{id}_R: R \rightarrow R$ einen Isomorphismus

$$R_S \rightarrow R_{\bar{S}}, \quad \frac{r}{s} \mapsto \frac{r}{s}$$

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

Inbesondere wird jedes Element $r \in R$ mit $r \in \bar{S}$ zu einer Einheit in $R_{\bar{S}}$, und wegen des obigen Isomorphismus' auch zu einer Einheit in R_S . Behauptung 3 ist eine Verschärfung dieser Beobachtung, und zeigt, dass ein Element $r/s \in R_S$ genau dann eine Einheit in R_S ist, wenn $r \in \bar{S}$; 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 \bar{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 5. 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 Primelemente aus R , die in R_S nicht zu einer Einheit werden.

Beweis. Man schränke Behauptung 3 auf die Primelemente von R ein. □

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

$$\frac{p}{1} \mid \frac{r_1}{s_1} \frac{r_2}{s_2}.$$

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 insbesondere $p \nmid s_3$, 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 $n_1, \dots, n_t \geq 1$ und $p_1, \dots, p_t \in R$ paarweise nicht-assozierte Primelemente sind

Hierbei gibt es ein $1 \leq i \leq t$ mit $p_i \in P_S$: Andernfalls gebe es für jedes $i = 1, \dots, t$ 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 3 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 $q := p_1^{n_1-1} p_2^{n_2} \cdots p_t^{n_t}$ 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 Irreduzibilität 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 insbesondere 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 6. Test.

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 7. 1. Zusammen mit Aufgabenteil ii) erhalten wir, dass die Assoziiertheitsklassen der Primelemente $q \in R_S$ genau den Assoziiertheitsklassen der Primelemente $p \in R$ entsprechen, für die $p \in P_S$; nach Behauptung 5 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 gute Zusammenhang zwischen den Primelementen aus R und R_S beruht 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

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

Man bemerke, dass für ein Primelement $p \in R$ genau dann $(p) \cap S = \emptyset$, wenn S kein Vielfaches von p enthält, 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)

Wir bemerken zunächst, dass nach Behauptung ?? 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.

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 $\text{ggT}(p, q) = 1$. Deshalb gibt es Primfaktorzerlegungen $p = p_1^{n_1} \cdots p_s^{n_s}$ und $q = q_1^{m_1} \cdots q_t^{m_t}$, 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

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

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

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

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

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

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 $p_1, \dots, p_s, q_1, \dots, q_t$ paarweise nicht-assoziiert sind.