

# 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. Dabei betrachten wir 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 jeweils 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  $i: R \rightarrow R_S, r \mapsto r/1$  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 deshalb bereits  $r_1 = 0$  oder  $r_2 = 0$ , und somit bereits  $r_1/s_1 = 0$  oder  $r_2/s_2 = 0$ .

2. Für  $r \in \ker i$  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

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

des Quotientenkörpers  $Q(R)$  identifizieren.

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

**Lemma 3.** Es sei  $R$  ein kommutativer Ring und  $r \in R$ . Gilt  $r \mid \varepsilon$  für eine Einheit  $\varepsilon \in R^\times$ , so ist auch  $r$  eine Einheit in  $R$ . Teiler von Einheiten sind also selber schon Einheit.

*Beweis.* Da  $r \mid \varepsilon$  gibt es  $r' \in R$  mit  $rr' = \varepsilon$ . Dann ist  $1 = \varepsilon\varepsilon^{-1} = rr'\varepsilon^{-1}$  und somit  $r$  eine Einheit mit  $r^{-1} = r'\varepsilon^{-1}$ .  $\square$

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 insbesondere  $r \mid ts' \in S$ .  $\square$

**Bemerkung 5.** 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 ist. Etwas konkreter (und für uns interessanter) lässt sich  $\bar{S}$  auch als

$$\bar{S} = \{r \in R \mid \text{es gibt } s \in S, \text{ das von } r \text{ geteilt wird}\}$$

konstruieren.

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

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

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, mit Teilbarkeitsbedingungen der Form  $r \mid s$  mit  $r \in R$  und  $s \in S$  arbeiten, 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 Primelemente 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  $r_1/s_1, r_2/s_2 \in R_S$  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  $p \nmid s_3$  und somit  $p \mid r_1$  oder  $p \mid r_2$ . Deshalb gilt 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-assoziierte Primelemente sind

Hierbei gibt es ein  $1 \leq i \leq t$  mit  $p_i \in P_S$ : Andernfalls gebe es für jedes  $i = 1, \dots, t$  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 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  $q := p_1^{n_1-1} p_2^{n_2} \cdots p_t^{n_t}$  gilt dann  $p = p_1 q$  und somit

$$\frac{p}{s} = \frac{p_1 q}{s} = \frac{p_1}{1} \frac{q}{s}. \quad (1)$$

Nach Lemma 1 ist  $R_S$  ein Integritätsbereich, und das Primelement  $p/s$  deshalb irreduzibel. Wegen der Irreduzibilität von  $p/s$  folgt aus Gleichung (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 Gleichung (1) ist  $p/s$  somit assoziiert zu  $p_1/1$  mit  $p_1 \in P_S$ .

**Warnung 7.** Ist  $p/s \in R_S$  prim, so gilt nicht notwendigerweise, dass bereits  $p \in R$  prim 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 kein 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 jenen Assoziiertheitsklassen von Primelementen  $p \in R$  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 Zusammenhang zwischen den Primelementen von  $R$  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  $R$  und  $R_S$  die Primideale in diesen Ringen. Zwischen diesen gibt es dann immer noch einen Zusammenhang, nämlich 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  $\mathfrak{p} \cap S = \emptyset$  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  $\mathcal{P} \subset R$  ein Repräsentantensystem der Assoziiertheitsklassen von Primelementen aus  $R$ .

Wir bemerken zunächst, dass nach Behauptung 6 für jedes Primelement  $p \in \mathcal{P}$  mit  $p \notin P_S$  das Element  $p/1$  eine Einheit in  $R_S$  ist. In dieser Situation ergibt deshalb der Ausdruck  $(p/1)^n$  für alle  $n \in \mathbb{Z}$  Sinn.

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

Da nach Lemma 1 der kanonische Ringhomomorphismus  $\iota: R \rightarrow R_S, x \mapsto x/1$  injektiv ist, können wir im Folgenden außerdem  $R$  mit dem Unterring  $\text{im } \iota = \{r/1 \mid r \in R\} \subseteq R_S$  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  $Q(R)$  auf, 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

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

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

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

$$u_1 \prod_{p \in \mathcal{P}} p^{n_p} = u_2 \prod_{p \in \mathcal{P}} p^{m_p}. \quad (2)$$

Es gilt zu zeigen, dass  $u_1 = u_2$  und  $n_p = m_p$  für alle  $p \in \mathcal{P}$ .

Hierfür dürfen wir Gleichung (2) zunächst beliebig mit Elementen  $p \in \mathcal{P}$  multiplizieren; hierbei ändern sich auf beiden Seiten die Exponenten  $n_p$  und  $m_p$  auf gleiche Weise, nämlich

durch Addition mit 1. Durch Multiplikation mit  $\prod_{p \in \mathcal{P}} p^{|n_p|+|m_p|}$  können wir deshalb davon ausgehen, dass bereits  $n_p, m_p \geq 0$  für alle  $p \in \mathcal{P}$ . Da die Elemente  $p \in \mathcal{P}$  paarweise nicht assoziierte Primelemente sind, folgt die gewünschte Gleichheit nun daraus, dass  $R$  faktoriell ist.

**Bemerkung 10.** In der Aufgabenstellung wird nicht mit einem Repräsentantensystem  $\mathcal{P} \subseteq R$  der Assoziiertheitsklassen 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 Assoziiertheitsklasse  $[p]$  definiert ein Primelement  $p \in R$  nur bis auf Assoziiertheit. 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 angegebenen Darstellung  $u \prod_{[p]} p^{n_p}$  sind dann zwar die Potenzen  $n_p \in \mathbb{Z}$  wohldefiniert, nicht aber die Einheit  $u \in R^\times$ .

Als ein konkretes Beispiel betrachte man den Ring  $R = \mathbb{Z}$  und die multiplikative Menge  $S = \mathbb{Z} \setminus \{0\}$ . Dann gilt  $R_S = Q(R) = Q(\mathbb{Z}) = \mathbb{Q}$ . Das Element  $x = 1/8 \in \mathbb{Q}$  lässt sich als  $1/8 = 1 \cdot 2^{-3}$  schreiben, aber auch als  $(-1) \cdot (-2)^{-3}$ . Die Potenz  $-3$  ist zwar für beide Darstellungen 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

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

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

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

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

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

## Aufgabe 4

Wir nehmen an, es gebe eine Nullstelle  $x \in Q(R)$  von  $f$ , die nicht schon in  $R$  liegt. Für  $x = p/q$  gilt dann insbesondere  $x \neq 0$  und somit  $p \neq 0$ , und es gilt  $d := \deg f \geq 2$ . 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  $p_1, \dots, p_s, q_1, \dots, q_t \in R$  paarweise nicht assoziierte Primelemente sind, und  $n_i, m_j \geq 1$  für alle  $i = 1, \dots, s$  und  $j = 1, \dots, t$ . Da  $x \notin R$  gilt  $t \geq 1$ .

Ist  $f(X) = X^d + \sum_{i=0}^{d-1} a_i X^i$ , 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 der obigen Gleichung mit  $(q_1^{m_1} \cdots q_t^{m_t})^d$  erhalten wir in  $R$  die Gleichung

$$0 = (p_1^{n_1} \cdots p_s^{n_s})^d + \sum_{i=0}^{d-1} a_i (p_1^{n_1} \cdots p_s^{n_s})^i (q_1^{m_1} \cdots q_t^{m_t})^{d-i}. \quad (3)$$

Da  $t \geq 1$  erhalten wir aus Gleichung (3), 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 gilt bereits  $q_1 \sim p_i$  da  $q_1$  und  $p_i$  prim in  $R$  sind. Dies steht im Widerspruch dazu, dass  $p_1, \dots, p_s, q_1, \dots, q_t$  paarweise nicht-assoziert sind.