D-MATH
Prof. Richard Pink

Algebra I

HS 2022

# Musterlösung Serie 9

## Quotientenkörper, Faktorringe, Primideale, Unterkörper

1. Entscheide, welche der folgenden Faktorringe isomorph sind:

$$\begin{aligned} R_1 &:= \mathbb{Q}[X,Y]/(X^2) & R_4 &:= \mathbb{Q}[X,Y]/(XY+3X+2Y+6) \\ R_2 &:= \mathbb{Q}[X,Y]/(XY) & R_5 &:= \mathbb{Q}[X,Y,Z]/(X^2,Y-Z) \\ R_3 &:= \mathbb{Q}[X,Y]/(X,Y) & R_6 &:= \mathbb{Q}[X,Y,Z]/(XZ-5,Y^2,Z) \end{aligned}$$

*Lösung*: Wir untersuchen alle Ringe separat und vergleichen ihre Eigenschaften am Schluss. Für jedes $1 \leqslant i \leqslant 6$ bezeichnen wir die Restklasse eines Polynoms $f$ in $R_i$ mit $[f]_i$.

Wegen $X \notin (X^2)$ gilt $[X]_1 \neq 0$. Andererseits ist $X^2 \in (X^2)$ und damit $[X]_1^2 = 0$. Also ist $R_1 \neq 0$ und enthält ein von Null verschiedenes nilpotentes Element.

Sodann ist $1 \notin (XY)$ und damit $R_2 \neq 0$. Wegen $X, Y \notin (XY)$ und $XY \in (XY)$ gilt weiter $[X]_2 \cdot [Y]_2 = [XY]_2 = 0$ in $R_2$ mit $[X]_2, [Y]_2 \neq 0$. Also besitzt $R_2$ Nullteiler. Ausserdem betrachte ein $f \in \mathbb{Q}[X,Y]$ mit $[f]_2$ nilpotent. Dann existiert ein $n \geqslant 1$ mit $[f^n]_2 = [f]_2^n = 0$ und damit $f^n \in (XY)$. Darum ist $f^n$ durch $XY$ teilbar. Dann muss aber auch schon $f$ durch $XY$ teilbar und damit $[f]_2 = 0$ sein. Dies zeigt, dass $R_2$ keine nichttrivialen nilpotenten Elemente besitzt.

Weiter betrachte den Auswertungshomomorphismus $\mathbb{Q}[X,Y] \to \mathbb{Q}$, $f \mapsto f(0,0)$. Dieser ist surjektiv. Sein Kern besteht aus allen Polynomen mit konstantem Term Null und ist daher gleich $(X,Y)$. Der Homomorphiesatz liefert also einen Isomorphismus $R_3 \xrightarrow{\sim} \mathbb{Q}$.

Sodann ist $\mathbb{Q}[X,Y] \to \mathbb{Q}[X,Y]$, $f(X,Y) \mapsto f(X+2,Y+3)$ ein Homomorphismus mit dem beidseitigen Inversen $\mathbb{Q}[X,Y] \to \mathbb{Q}[X,Y]$, $f(X,Y) \mapsto f(X-2,Y-3)$ und daher ein Isomorphismus. Das Bild des Ideals $(X,Y)$ unter diesem Isomorphismus ist das Ideal $((X+2)(Y+3)) = (XY+3X+2Y+6)$. Also erhalten wir einen Isomorphismus der Faktorringe $R_2 \xrightarrow{\sim} R_4$.

Analog ist $\mathbb{Q}[X,Y,W] \to \mathbb{Q}[X,Y,Z]$, $f(X,Y,W) \mapsto f(X,Y,Y-Z)$ ein Isomorphismus mit dem Inversen $\mathbb{Q}[X,Y,Z] \to \mathbb{Q}[X,Y,W]$, $g(X,Y,Z) \mapsto g(X,Y,Y-W)$. Das Bild des Ideals $(X^2,W)$ unter diesem Isomorphismus ist das Ideal $(X^2,Y-Z)$. Somit erhalten wir einen Isomorphismus $\mathbb{Q}[X,Y,W]/(X^2,W) \xrightarrow{\sim} R_5$. Nun besteht das Ideal $(X^2,W)$ aus genau denjenigen Polynomen, die nur Monome der Form $X^iY^jW^k$ enthalten mit $i \geqslant 2$ und $k \geqslant 1$. Die Polynome, die nur Monome der Form $X^iY^j$ mit $i \leqslant 1$ enthalten, bilden darum ein Komplement dieses Ideals als $\mathbb{Q}$-Vektorraum. Aus den gleichen Gründen bilden diese Polynome aber auch ein

Komplement des Ideals $(X^2) \subset \mathbb{Q}[X, Y]$. Die Inklusion $\mathbb{Q}[X, Y] \hookrightarrow \mathbb{Q}[X, Y, W]$ ist die Identität auf diesem Komplement und bildet das Ideal $(X^2)$ in das Ideal $(X^2, W)$ ab. Somit induziert sie einen Isomorphismus $R_1 = \mathbb{Q}[X, Y]/(X^2) \xrightarrow{\sim} \mathbb{Q}[X, Y, W]/(X^2, W) \xrightarrow{\sim} R_5$

Schliesslich beachten wir, dass $1 = \frac{1}{5} \cdot (X \cdot Z - (XZ - 5))$ in dem Ideal $(XZ - 5, Y^2, Z)$ liegt. Also ist das Ideal das Einsideal und $R_6$ der Nullring.

Die gesammelten Eigenschaften zeigen, dass nur $R_6$ der Nullring ist, dass nur $R_3 \cong \mathbb{Q}$ ein Integritätsbereich ist, dass nur $R_1 \cong R_5$ von Null verschiedene nilpotente Elemente besitzen, und dass $R_2 \cong R_4$ ist. Somit gibt es keine weiteren Isomorphien.

2. Zeige, dass ein echtes Ideal $\mathfrak{p} \subsetneq R$ dann und nur dann ein Primideal ist, wenn für beliebige Ideale $\mathfrak{a}, \mathfrak{b} \subset R$ gilt

$$\mathfrak{a}\mathfrak{b} \subset \mathfrak{p} \implies (\mathfrak{a} \subset \mathfrak{p} \text{ oder } \mathfrak{b} \subset \mathfrak{p}).$$

*Lösung*: „nur dann“: Sei $\mathfrak{p}$ ein solches Ideal. Für alle $a, b \in R$ mit $ab \in \mathfrak{p}$ gilt dann $(a)(b) = (ab) \subset \mathfrak{p}$ und folglich $(a) \subset \mathfrak{p}$ oder $(b) \subset \mathfrak{p}$, also $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$. Somit ist $\mathfrak{p}$ ein Primideal.

„dann“: Sei $\mathfrak{p}$ ein Primideal. Betrachte Ideale $\mathfrak{a}, \mathfrak{b} \subset R$ mit $\mathfrak{a}\mathfrak{b} \subset \mathfrak{p}$ und $\mathfrak{a} \not\subset \mathfrak{p}$ und $\mathfrak{b} \not\subset \mathfrak{p}$. Wähle $a \in \mathfrak{a} \setminus \mathfrak{p}$ und $b \in \mathfrak{b} \setminus \mathfrak{p}$. Dann ist $ab \in \mathfrak{a}\mathfrak{b} \subset \mathfrak{p}$ mit $a, b \notin \mathfrak{p}$, was der Definition von Primideal widerspricht.

3. (a) Zeige, dass jeder endliche Integritätsbereich ein Körper ist.

   (b) Sei $R$ ein Ring und $I$ ein Primideal von $R$ mit endlichem Faktorring $R/I$. Folgere aus (a), dass $I$ ein maximales Ideal von $R$ ist.

*Lösung*:

(a) Sei $R$ ein endlicher Integritätsbereich. Wir beweisen, dass jedes Element $a \in R \setminus \{0\}$ ein multiplikatives Inverses hat. Betrachte dazu die Abbildung

$$r_a : \begin{array}{ccc} R & \longrightarrow & R \\ x & \longmapsto & xa \end{array}.$$

Sie ist injektiv, denn aus $x_1 a = x_2 a$ folgt $x_1 = x_2$, da $R$ ein Integritätsbereich ist. Wegen der Endlichkeit von $R$ ist darum $r_a$ auch surjektiv. Deshalb finden wir ein $b \in R$ mit $ba = ab = 1$. Somit hat jedes $0 \neq a \in R$ ein multiplikatives Inverses. Zudem ist $1 \neq 0$, da dies in Integritätsbereichen vorausgesetzt ist. Daher ist $R$ ein Körper.

(b) Da $I$ ein Primideal von $R$ ist, ist $R/I$ ein Integritätsbereich, der nach Voraussetzung endlich ist. Nach (a) ist darum $R/I$ ein Körper, also ist $I$ ein maximales Ideal von $R$.

4. Sei $R$ der Ring der stetigen Funktionen $f : [0,1] \to \mathbb{R}$.

   (a) Hat $R$ Nullteiler?

   (b) Zeige, dass $R$ überabzählbar viele maximale Ideale hat.

   *(c) Bestimme alle maximalen Ideale von $R$.

   **(d) Sind alle maximalen Ideale von $R$ Hauptideale? Sind sie endlich erzeugt?

   **(e) Gibt es Primideale von $R$, die keine maximalen Ideale sind?

*Lösung*:

(a) Der Ring $R$ enthält Nullteiler; zum Beispiel ist das Produkt der beiden von Null verschiedenen stetigen Funktionen

$$f(x) = \begin{cases} \frac{1}{2} - x\,, & 0 \leqslant x \leqslant \frac{1}{2} \\ 0\,, & \frac{1}{2} \leqslant x \leqslant 1 \end{cases}$$

$$g(x) = \begin{cases} 0\,, & 0 \leqslant x \leqslant \frac{1}{2} \\ \frac{1}{2} - x\,, & \frac{1}{2} \leqslant x \leqslant 1 \end{cases}$$

gleich 0.

(b) Wir zeigen, dass für jedes $a \in [0,1]$ die Teilmenge $\mathfrak{m}_a = \{f \in R \mid f(a) = 0\}$ von $R$ ein maximales Ideal ist. Betrachte dazu die Abbildung

$$\varphi_a : \begin{array}{ccc} R & \longrightarrow & \mathbb{R} \\ f & \longmapsto & f(a) \end{array}.$$

Sie ist ein Ringhomomorphismus und klarerweise surjektiv, da für jedes $y \in \mathbb{R}$ eine stetige Funktion $f : [0,1] \to \mathbb{R}$ mit $f(a) = y$ existiert, nämlich zum Beispiel die konstante Funktion. Weiter gilt $\ker \varphi_a = \mathfrak{m}_a$ nach Definition von $\mathfrak{m}_a$. Nach dem Homomorphiesatz ist darum $\mathfrak{m}_a$ ein Ideal mit $R/\mathfrak{m}_a \cong \mathbb{R}$. Da $\mathbb{R}$ ein Körper ist, folgt daraus, dass $\mathfrak{m}_a$ ein maximales Ideal von $R$ ist.

Für $a \neq b$ in $[0,1]$ ist $\mathfrak{m}_a \neq \mathfrak{m}_b$, da eine stetige Funktion $f : [0,1] \to \mathbb{R}$ mit $f(a) = 0$ und $f(b) \neq 0$ existiert, die also in $\mathfrak{m}_a$ und nicht in $\mathfrak{m}_b$ liegt. Somit bilden die $\mathfrak{m}_a$ für $a \in [0,1]$ überabzählbar viele maximale Ideale von $R$.

*(c) Sei $\mathfrak{m} \subset R$ ein von allen $\mathfrak{m}_a$ verschiedenes maximales Ideal. Für jedes $a \in [0,1]$ gilt dann $\mathfrak{m} \not\subset \mathfrak{m}_a$, denn sonst würde $\mathfrak{m} \subsetneq \mathfrak{m}_a \subsetneq (1)$ der Maximalität von $\mathfrak{m}$ widersprechen. Also existiert eine stetige Funktion $f_a \in \mathfrak{m}$ mit $f_a(a) \neq 0$. Wegen der Stetigkeit existiert eine offene Umgebung $a \in U_a \subset [0,1]$ mit $\forall x \in U_a \colon f_a(x) \neq 0$. Diese $U_a$ für alle $a \in [0,1]$ bilden eine offene Überdeckung von $[0,1]$. Wegen der Kompaktheit existiert eine endliche Teilüberdeckung $[0,1] = \bigcup_{i=1}^n U_{a_i}$. Setze $f := \sum_{i=1}^n f_{a_i}^2$. Diese Funktion ist wieder stetig, also ein Element von $R$. Ausserdem ist $f(x) > 0$ für alle $x \in [0,1]$. Somit ist die Funktion $x \mapsto \frac{1}{f(x)}$ wohldefiniert und stetig; also ist $f \in R^\times$. Nach

Konstruktion ist aber $f \in \mathfrak{m}$, also auch $1 \in \mathfrak{m}$, was der Voraussetzung an $\mathfrak{m}$ widerspricht. Somit sind die Ideale $\mathfrak{m}_a$ für alle $a \in [0,1]$ genau die maximalen Ideale von $R$.

**(d) *Behauptung:* Für jedes $a \in [0,1]$ ist das maximale Ideal $\mathfrak{m}_a$ nicht endlich erzeugt und insbesondere kein Hauptideal.

*Beweis:* Nehmen wir an, es sei $\mathfrak{m}_a = (f_1, \ldots, f_n)$. Die Idee ist, die Funktion $g := \max\{|f_1|, \ldots, |f_n|\}$ zu untersuchen.

Zur Vorbereitung betrachte eine beliebige Funktion $h \in \mathfrak{m}_a$. Nach Annahme existiert dann eine Darstellung $h = h_1 f_1 + \ldots + h_n f_n$ mit $h_1, \ldots, h_n \in R$. Als stetige Funktionen auf einem Kompaktum sind $h_1, \ldots, h_n$ beschränkt; somit folgt $h \leqslant C \cdot g$ für eine gewisse von $h$ abhängige Konstante $C > 0$.

Als erste Anwendung dieses Resultats betrachte einen beliebigen Punkt $b \in [0,1] \setminus \{a\}$. Dann existiert eine Funktion $h \in \mathfrak{m}_a$ mit $h(b) \neq 0$. Für diese impliziert die Ungleichung $h \leqslant C \cdot g$, dass $g(b) \neq 0$ ist. Also ist $g \neq 0$ ausserhalb von $a$.

Andererseits ist $g$ nach Konstruktion stetig und nichtnegativ mit $g(a) = 0$. Dasselbe gilt auch für die Funktion $\sqrt{g}$; somit ist $\sqrt{g} \in \mathfrak{m}_a$. Für $h := \sqrt{g}$ folgt dann auch $\sqrt{g} \leqslant C \cdot g$ für eine Konstante $C > 0$. Für alle $x \in [0,1] \setminus \{a\}$ gilt dann $0 < g(x) \leqslant C^2 \cdot g(x)^2$ und somit $1/C^2 \leqslant g(x)$. Da aber $g$ eine stetige Funktion ist, folgt daraus $0 < 1/C^2 \leqslant g(a) = 0$: ein Widerspruch. *q.e.d.*

**(e) Gibt es Primideale von $R$, die keine maximalen Ideale sind? Ja!

*Konstruktion:* Die natürliche Abbildung $\mathbb{R}[X] \to R$ ist injektiv, da jedes von Null verschiedene Polynom nur endlich viele Nullstellen hat. Wir identifizieren $\mathbb{R}[X]$ mit seinem Bild.

Sei $\mathcal{S}$ die Menge aller Ideale $\mathfrak{a} \subset R$ mit $\mathfrak{a} \cap \mathbb{R}[X] = \{0\}$. Diese Menge enthält das Nullideal, ist also nichtleer. Für jede Kette $\mathcal{K} \subset \mathcal{S}$ ist auch $\mathfrak{b} := \bigcup_{\mathfrak{a} \in \mathcal{K}} \mathfrak{a}$ ein Ideal von $R$, und wegen $\mathfrak{a} \cap \mathbb{R}[X] = \{0\}$ für alle $\mathfrak{a} \in \mathcal{K}$ gilt auch $\mathfrak{b} \cap \mathbb{R}[X] = \{0\}$. Somit ist auch $\mathfrak{b}$ ein Element von $\mathcal{S}$. Nach Konstruktion ist $\mathfrak{b}$ also eine obere Schranke von $\mathcal{K}$; somit ist $\mathcal{S}$ induktiv geordnet. Nach dem Zornschen Lemma besitzt $\mathcal{S}$ daher ein maximales Element $\mathfrak{p}$.

Dieses Ideal erfüllt natürlich die Bedingung $\mathfrak{p} \cap \mathbb{R}[X] = \{0\}$. Insbesondere ist daher $\mathfrak{p} \neq R$. Sodann betrachte beliebige Elemente $f_1, f_2 \in R$. Nehmen wir zuerst $f_1, f_2 \notin \mathfrak{p}$ an. Für jedes $i = 1, 2$ ist dann $\mathfrak{p} + (f_i)$ ein echt grösseres Ideal als $\mathfrak{p}$; wegen der Maximalität von $\mathfrak{p}$ ist daher $(\mathfrak{p} + (f_i)) \cap \mathbb{R}[X] \neq \{0\}$. Wähle $g_i \in \mathfrak{p}$ und $h_i \in R$ mit

$$g_i + h_i f_i \;=\; P_i \;\in\; \mathbb{R}[X] \setminus \{0\}.$$

Da $\mathbb{R}[X]$ ein Integritätsbereich ist, ist dann auch

$$(g_1 g_2 + h_1 f_1 g_2 + g_1 h_2 f_2) + h_1 h_2 f_1 f_2 \;=\; P_1 P_2 \;\in\; \mathbb{R}[X] \setminus \{0\}.$$

Die linke Seite dieser Gleichung ist ein Element des Ideals $\mathfrak{p} + (f_1 f_2)$; somit folgt daraus $(\mathfrak{p} + (f_1 f_2)) \cap \mathbb{R}[X] \neq \{0\}$. Wegen $\mathfrak{p} \cap \mathbb{R}[X] = \{0\}$ ist dies nur möglich mit $f_1 f_2 \notin \mathfrak{p}$. Insgesamt haben wir damit die Implikation

$$f_1, f_2 \notin \mathfrak{p} \Longrightarrow f_1 f_2 \notin \mathfrak{p}$$

gezeigt. Diese ist aber äquivalent zu ihrer kontrapositiven Implikation

$$f_1 f_2 \in \mathfrak{p} \Longrightarrow (f_1 \in \mathfrak{p} \vee f_2 \in \mathfrak{p}).$$

Somit ist $\mathfrak{p}$ ein Primideal. Schliesslich ist $\mathfrak{p}$ verschieden von jedem maximalen Ideal $\mathfrak{m}_a$; denn es gilt $X - a \in \mathfrak{m}_a \smallsetminus \mathfrak{p}$.

*5. *Alternative Konstruktion des Quotientenkörpers:* Sei $R$ ein Integritätsbereich. Betrachte den Polynomring $S := R[X_a|_{a \in R \smallsetminus \{0\}}]$ in neuen Variablen $X_a$ und das von den Polynomen $aX_a - 1$ für alle $a \in R \smallsetminus \{0\}$ erzeugte Ideal $\mathfrak{m} \subset S$.

(a) Konstruiere einen natürlichen surjektiven Homomorphismus $S/\mathfrak{m} \to \mathrm{Quot}(R)$.

(b) Zeige: Für jedes $f \in S$ existieren $r \geqslant 0$ und $a_1, \ldots, a_r \in R \smallsetminus \{0\}$ sowie $\nu_1, \ldots, \nu_r \in \mathbb{Z}_{\geqslant 0}$ und $b \in R$ mit $f \equiv b X_{a_1}^{\nu_1} \cdots X_{a_r}^{\nu_r} \mod \mathfrak{m}$.

(c) Zeige, dass $\mathfrak{m}$ ein maximales Ideal ist.

(d) Folgere, dass der Homomorphismus in (a) ein Isomorphismus ist.

**(e) Beweise $\mathfrak{m} \neq (1)$ ohne den Quotientenkörper $\mathrm{Quot}(R)$ zu benutzen.

**(f) Zeige unabhängig von (a) und (d), dass $S/\mathfrak{m}$ dieselbe universelle Eigenschaft wie $\mathrm{Quot}(R)$ hat.

*Lösung*:

(a) Sei $\varphi\colon S \to \mathrm{Quot}(R)$ der Auswertungshomomorphismus, bei dem jede Variable $X_a$ auf $\frac{1}{a}$ abgebildet wird. Dieser ist surjektiv, da jedes $\frac{a}{b} \in \mathrm{Quot}(R)$ das Bild von $aX_b \in S$ ist. Für jedes $a \in R \smallsetminus \{0\}$ gilt weiter $\varphi(aX_a - 1) = \frac{a}{a} - 1 = 0$. Somit liegen die Erzeugenden von $\mathfrak{m}$ in $\mathrm{Kern}(\varphi)$ und es folgt $\mathfrak{m} \subset \mathrm{Kern}(\varphi)$. Daher faktorisiert $\varphi$ durch einen eindeutigen surjektiven Homomorphismus $\bar{\varphi}\colon S/\mathfrak{m} \to \mathrm{Quot}(R)$.

(b) Jedes $f \in S$ ist schon ein Polynom in endlich vielen der Variablen, also existieren $r, n, \nu_{ij} \geqslant 0$ und $a_j, b_i \in R$ mit

$$f \;=\; \sum_{i=1}^{n} b_i \cdot X_{a_1}^{\nu_{i1}} \cdots X_{a_r}^{\nu_{ir}}.$$

Nach der Definition von $\mathfrak{m}$ gilt nun $1 \equiv a_j X_{a_j}$ modulo $\mathfrak{m}$ für jedes $1 \leqslant j \leqslant r$. Mit $\nu_j := \max\{\nu_{1j}, \ldots, \nu_{nj}\}$ folgt daraus

$$1 \;\equiv\; \prod_{j=1}^{r} (a_j X_{a_j})^{\nu_j - \nu_{ij}} \mod \mathfrak{m}$$

für alle $1 \leqslant i \leqslant n$. In die Formel für $f$ eingesetzt erhalten wir damit

$$f \;\equiv\; \left[\sum_{i=1}^n \left(b_i \prod_{j=1}^r a_j^{\nu_j - \nu_{ij}}\right)\right] X_{a_1}^{\nu_1} \cdots X_{a_r}^{\nu_r} \quad \bmod \mathfrak{m}.$$

(c) Betrachte ein grösseres Ideal $\mathfrak{m} \subsetneqq \mathfrak{a} \subset S$. Wähle $f \in \mathfrak{a} \smallsetminus \mathfrak{m}$ und schreibe $f \;\equiv\; bX_{a_1}^{\nu_1} \cdots X_{a_r}^{\nu_r} \bmod \mathfrak{m}$ wie in (b). Wegen $f \notin \mathfrak{m}$ ist dann $b \neq 0$. Sodann ist

$$a_1^{\nu_1} \cdots a_r^{\nu_r} X_b f \;\equiv\; (bX_b) \prod_{\rho=1}^r (a_\rho X_{a_\rho})^{\nu_\rho} \;\equiv\; 1 \quad \bmod \mathfrak{m}.$$

Also gilt $1 \in \mathfrak{a}$ und darum $\mathfrak{a} = (1)$. Wegen $\mathfrak{m} \neq (1)$ ist $\mathfrak{m}$ daher ein maximales Ideal.

(d) Nach (c) ist der Faktorring $S/\mathfrak{m}$ ein Körper. Also ist der in (a) konstruierte Homomorphismus $\bar{\varphi}$ ein Homomorphismus von Körpern und daher injektiv. Da er bereits surjektiv ist, ist er bijektiv und damit ein Isomorphismus.

**(e) Nehmen wir an, es sei $1 \in \mathfrak{m}$. Dann existieren $n \geqslant 0$ und $a_1, \ldots, a_n \in R \smallsetminus \{0\}$ sowie $f_i \in R[X_{a_1}, \ldots, X_{a_n}]$ mit

$$1 \;=\; \sum_{i=1}^n f_i \cdot (a_i X_{a_i} - 1). \tag{$*$}$$

Sodann schreiben wir

$$f_i \;=\; \sum_{\underline{\nu}} b_{i,\underline{\nu}} \cdot \prod_{j=1}^n X_{a_j}^{\nu_j}$$

mit $\underline{\nu} = (\nu_1, \ldots, \nu_n) \in (\mathbb{Z}^{\geqslant 0})^n$ und fast allen $b_{i,\underline{\nu}} \in R$ gleich Null. Wähle $\underline{\mu} = (\mu_1, \ldots, \mu_n) \in (\mathbb{Z}^{\geqslant 0})^n$, so dass $b_{i,\underline{\nu}}$ nur dann ungleich Null sein kann, wenn $\nu_j \leqslant \mu_j$ gilt für alle $j$. Da $R$ ein Integritätsbereich ist, ist dann $a := a_1^{\mu_1} \cdots a_n^{\mu_n}$ ungleich Null. Nach Multiplizieren der Gleichung $(*)$ mit $a$ erhalten wir

$$a \;=\; \sum_{i=1}^n \sum_{\underline{\nu}} b_{i,\underline{\nu}} \cdot \prod_{j=1}^n a_j^{\mu_j - \nu_j} \cdot \prod_{j=1}^n (a_j X_{a_j})^{\nu_j} \cdot (a_i X_{a_i} - 1). \tag{$**$}$$

Nun betrachte den Ringhomomorphismus

$$\varphi\colon\; R[Y_1, \ldots, Y_n] \longrightarrow S, \quad g \mapsto g(a_1 X_{a_1}, \ldots, a_n X_{a_n}).$$

Dieser bildet ein beliebiges Polynom in $R[Y_1, \ldots, Y_n]$ wie folgt ab:

$$\varphi\Big(\sum_{\underline{\nu}} c_{\underline{\nu}} \cdot \prod_{j=1}^n Y_j^{\nu_j}\Big) \;=\; \sum_{\underline{\nu}} c_{\underline{\nu}} \cdot \prod_{j=1}^n a_j^{\nu_j} \cdot \prod_{j=1}^n X_{a_j}^{\nu_j}.$$

Da $R$ ein Integritätsbereich ist, ist die Abbildung $R \to R$, $c \mapsto c \cdot \prod_{j=1}^n a_j^{\nu_j}$ aber injektiv. Insgesamt folgt daraus, dass auch $\varphi$ injektiv ist. Wähle jetzt das Polynom

$$h \;:=\; \sum_{i=1}^n \sum_{\underline{\nu}} b_{i,\underline{\nu}} \cdot \prod_{j=1}^n a_j^{\mu_j-\nu_j} \cdot \prod_{j=1}^n Y_j^{\nu_j} \cdot (Y_i - 1) \qquad (***)$$

in $R[Y_1, \ldots, Y_n]$. Dann ist die obige Gleichung $(**)$ äquivalent zu $a = \varphi(h)$. Wegen $\varphi(a) = a$ und der Injektivität von $\varphi$ folgt daraus $a = h$. Nach Einsetzen von $Y_i = 1$ für alle $i$ und der Konstruktion $(***)$ von $h$ folgt daraus weiter $a = 0$. Damit haben wir einen Widerspruch, und somit ist $1 \notin \mathfrak{m}$.

**(f) Nach (c) und (e) ist $\mathfrak{m}$ ein maximales Ideal und darum $S/\mathfrak{m}$ ein Körper. Ausserdem haben wir einen natürlichen Homomorphismus $\kappa\colon R \to S/\mathfrak{m}$, $b \mapsto b + \mathfrak{m}$. Betrachte nun einen beliebigen injektiven Homomorphismus in einen Körper $\psi\colon R \hookrightarrow K$. Nach der universellen Eigenschaft des Polynomrings können wir diesen fortsetzen zu einem Homomorphismus $\tilde{\psi}\colon S \to K$ mit $\tilde{\psi}(X_a) = \frac{1}{a}$ für alle $a \in R \smallsetminus \{0\}$. Dieser erfüllt $\tilde{\psi}(aX_a - 1) = 0$ und damit $\mathfrak{m} \subset \mathrm{Kern}(\tilde{\psi})$. Somit faktorisiert $\tilde{\psi}$ durch einen Körperhomomorphismus $\bar{\psi}\colon S/\mathfrak{m} \to K$, und für diesen gilt $\bar{\psi} \circ \kappa = \psi$.

Sei $\omega\colon S/\mathfrak{m} \to K$ ein weiterer Körperhomomorphismus mit $\omega \circ \kappa = \psi$. Für jedes $a \in R \smallsetminus \{0\}$ gilt dann

$$\varphi(a) \cdot \omega(X_a + \mathfrak{m}) - 1 \;=\; \omega(aX_a - 1 + \mathfrak{m}) \;=\; \omega(0) \;=\; 0$$

und somit $\omega(X_a + \mathfrak{m}) = \frac{1}{\varphi(a)} = \bar{\psi}(X_a + \mathfrak{m})$. Also stimmt $\omega$ auf allen Erzeugenden von $S/\mathfrak{m}$ über $R$ mit $\bar{\psi}$ überein und ist deshalb gleich $\bar{\psi}$. Damit ist die universelle Eigenschaft bewiesen.

**6. Der Satz von Krull besagt, dass jeder von Null verschiedene Ring ein maximales Ideal besitzt. Im Beweis dieses Satzes haben wir das Zornsche Lemma verwendet. Kann man umgekehrt das Zornsche Lemma oder das Auswahlaxiom aus dem Satz von Krull herleiten?

*Lösung*: Die Antwort lautet: Ja! Ein Beweis finden sich in [Ba94].

[Ba94] B. Banaschewski, A New Proof that “Krull implies Zorn”, *Mathematical Logic Quarterly* **40** (1994), 478–480

7. Gegeben seien ein Körper $K$, eine nichtleere Indexmenge $I$ und für jedes $i \in I$ ein Unterkörper $K_i \subset K$. Zeige: $\bigcap_{i\in I} K_i$ ist ein Unterkörper von $K$.

*Lösung*: Setze $K' := \bigcap_{i\in I} K_i$. Für alle $i \in I$ gilt $1 \in K_i$, also $1 \in K'$. Betrachte beliebige Elemente $a, b, c \in K'$ mit $c \neq 0$. Für jedes $i \in I$ gilt dann $a, b, c \in K_i$, und da $K_i$ ein Unterkörper ist, liegen $a + b$, $ab$, $-a$, $c^{-1}$ alle in $K_i$. Da $i$ beliebig ist, liegen diese Elemente in $K'$. Damit ist $K'$ ein Unterkörper von $K$.