D-MATH Algebra I HS 2015
Prof. Richard Pink

# Musterlösung 1

## Ringe, Polynome, Potenzreihen

1. Zeige, dass in jedem Ring $R$ die Distributivregel

$$\forall x, y, z \in R : x(y - z) = xy - xz$$

gilt.

*Lösung*: Für alle $x, y, z \in R$ gilt

$$x(y - z) = x(y + (-z)) = xy + x(-z) = xy + (-xz) = xy - xz.$$

2. Zeige, dass ein Ringhomomorphismus $\psi : R \to S$ genau dann ein Isomorphismus ist, wenn er bijektiv ist.

*Lösung*: Sei $\psi : R \to S$ ein bijektiver Ringhomomorphismus. Für alle $s_1, s_2 \in S$ setze $r_1 := \psi^{-1}(s_1)$ und $r_2 := \psi^{-1}(s_2)$. Dann gilt $s_1 = \psi(r_1)$ und $s_2 = \psi(r_2)$. Aus der Homomorphieeigenschaft von $\psi$ folgt

$$\begin{aligned} s_1 + s_2 &= \psi(r_1) + \psi(r_2) = \psi(r_1 + r_2), \\ s_1 \cdot s_2 &= \psi(r_1) \cdot \psi(r_2) = \psi(r_1 \cdot r_2), \end{aligned}$$

also haben wir

$$\begin{aligned} \psi^{-1}(s_1 + s_2) &= r_1 + r_2 = \psi^{-1}(s_1) + \psi^{-1}(s_2), \\ \psi^{-1}(s_1 \cdot s_2) &= r_1 \cdot r_2 = \psi^{-1}(s_1) \cdot \psi^{-1}(s_2). \end{aligned}$$

Zudem gilt $\psi^{-1}(1_S) = 1_R$ wegen $\psi(1_R) = 1_S$. Somit ist $\psi^{-1} : S \to R$ ebenfalls ein Ringhomomorphismus. Deshalb ist $\psi$ ein Isomorphismus.

Umgekehrt ist ein Ringisomorphismus $\psi\colon R \to S$ insbesondere ein Isomorphismus der unterliegenden Mengen, und folglich bijektiv.

3. Sei $K$ ein Körper und sei $\sigma : K[X] \to K[X]$ ein Ringautomorphismus, dessen Einschränkung von $\sigma$ auf $K$ die Identität ist.[1] Zeige, dass es Elemente $a_1 \in K^\times$ und $a_0 \in K$ gibt, so dass $\sigma(X) = a_1X + a_0$ ist.

*Lösung*: Da $\sigma$ eine Bijektion ist, gilt $\sigma(X) \neq 0$. Genauso ist $\sigma^{-1}(X) \neq 0$.

Sei dann

$$P(X) = a_nX^n + ... + a_0$$

[1] Mit anderen Worten ist $\sigma$ ein *Automorphismus von K-Algebren.*

das Bild von $X$ unter $\sigma$ mit $a_i \in K$ und $a_n \neq 0$, und sei

$$Q(X) = b_m X^m + ... + b_0$$

das Bild von $X$ unter $\sigma^{-1}$ mit $b_j \in K$ und $b_m \neq 0$.

Wir berechnen

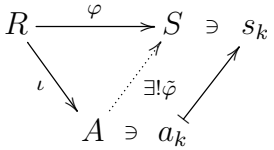
$$X = \sigma(\sigma^{-1}(X)) = \sigma(Q(X)) = b_m \sigma(X)^m + ... + b_0 = b_m(a_n X^n + ... + a_0)^m + ... + b_0$$
$$= b_m a_n^m X^{nm} + \text{niedrigere Terme}$$

Deshalb gilt für den Grad $1 = nm$. Da $n$ und $m$ nicht-negative ganze Zahlen sind, müssen sie gleich 1 sein.

4. Zeige mit der universellen Eigenschaft von Polynomringen, dass $R[X_1, ..., X_n] \cong R[Y_1, ..., Y_m][Y_{m+1}, ..., Y_n]$ für alle $1 \leqslant m \leqslant n$ gilt.

   *Lösung*: First, we restate the universal property satisfied by $R[X_1, ..., X_n]$ in the following way:

   Let $A$ be a ring endowed with a ring homomorphism $\iota : R \to A$ and with a specified $n$-tuple $\bar{a} := (a_1, .., a_n) \in A$. We say the tuple $(A, \iota, \bar{a})$ *satisfies the universal property of* $R[X_1, ..., X_n]$ if for each ring $S$, each ring homomorphism $\varphi : R \to S$ and every $n$-tuple $\bar{s} = (s_1, ..., s_n) \in S^n$, there exists a unique ring homomorphism $\tilde{\varphi} : A \to S$ sending $a_k$ to $s_k$ for $1 \leqslant k \leqslant n$ such that $\tilde{\varphi} \circ \iota = \varphi$. In other words, the following diagram commutes:




(1)

We begin with the following lemma:

**Lemma 0.1.** *Suppose* $(B, \iota, \bar{b})$ *and* $(B', \iota', \bar{b}')$ *satisfy the universal property of* $R[X_1, ..., X_n]$. *Then there is a unique isomorphism* $\tilde{\iota} : B' \to B$ *sending* $b'_i$ *to* $b_i$ *for* $i = 1, .., n$ *and such that* $\tilde{\iota} \circ \iota' = \iota$.

*Beweis.* The universal property with $(A, \iota, \bar{a}) = (B, \iota, \bar{b})$ and $(S, \varphi, \bar{s}) = (B', \iota', \bar{b}')$ yields a ring homomorphism $\tilde{\iota'} : B \to B'$.

Similarly, with $(A, \iota, \bar{a}) = (B', \iota', \bar{b}')$ and $(S, \varphi, \bar{s}) = (B, \iota, \bar{b})$, one attains $\tilde{\iota} : B' \to B$.

Finally, applying the universal property with $(A, \iota, \bar{a}) = (B, \iota, \bar{b})$ and $(S, \varphi, \bar{s}) = (B, \iota, \bar{b})$. Clearly $id_B : B \to B$ satisfies the diagram in (1). One checks that $\tilde{\iota'} \circ \tilde{\iota}$ does as well. By uniqueness, this implies that $\tilde{\iota'} \circ \tilde{\iota} = id_B$.

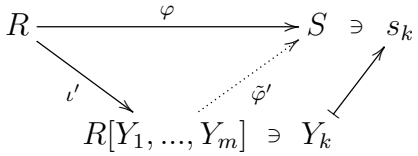
In the same fashion one finds $\tilde{\iota} \circ \tilde{\iota'} = id_{B'}$. Therefore $\tilde{\iota}$ is an isomorphism with inverse $\tilde{\iota'}$.

□

Now let $\iota : R \to R[Y_1, ..., Y_m][Y_{m+1}, ..., Y_n]$ be the canonical injection and $\bar{Y} := (Y_1, ..., Y_n)$. We want to show that $(R[Y_1, ..., Y_m][Y_{m+1}, ...Y_n], \iota, \bar{Y})$ satisfies the universal property of $R[X_1, ..., X_n]$.

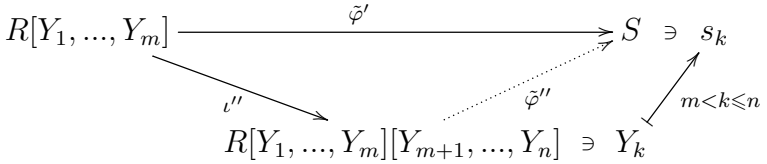
Let $\iota' : R \to R[Y_1, ..., Y_m]$ and $\iota'' : R[Y_1, ..., Y_m] \to R[Y_1, ..., Y_m][Y_{m+1}, ..., Y_n]$ be the canonical inclusions.

The universal property of $R[Y_1, ..., Y_m]$ as a polynomial ring over $R$ implies the existence of a unique $\tilde{\varphi'}$ making the following diagram commute:




(2)

Now we can apply the universal property for $R[Y_1, ..., Y_m][Y_{m+1}, ..., Y_n]$ as a polynomial ring over $R[Y_1, ..., Y_m]$, yielding:




(3)

We claim that $\tilde{\varphi} := \tilde{\varphi}''$ satisfies the conditions in (1). Indeed, for $1 \leqslant k \leqslant m$, $\tilde{\varphi}(Y_k) = \tilde{\varphi}(\iota(Y_k)) = \tilde{\varphi}'(Y_k) = s_k$ and thus $\tilde{\varphi}(Y_j) = s_j$ for $j = 1, ..., n$. Furthermore,

for $r \in R$ we have

$$\tilde{\varphi} \circ \iota(r) = \tilde{\varphi} \circ (\iota'' \circ \iota')(r) = (\tilde{\varphi} \circ \iota'') \circ \iota'(r) = \tilde{\varphi}' \circ \iota'(r) = \varphi(r)$$

Lastly, we need to show that $\tilde{\varphi}$ is the unique morphism satisfying (1). Let $\tilde{\psi}$ be such a map. Then $\tilde{\psi} \circ \iota''$ satisfies (2) and is therefore equal to $\tilde{\varphi}'$ by the uniqueness of $\tilde{\varphi}'$. From this it follows that $\tilde{\psi}$ satisfies (3) and therefore $\tilde{\psi} = \tilde{\varphi}$, again by uniqueness.

5. (a) Verifiziere die Ringaxiome für Ring $R[[X]]$ der *formalen Potenzreihen* in einer Variable über einem Ring $R$.

   (b) Zeige, dass ein Element $a_0 + \sum_{i>0} a_i X^i \in R[[X]]$ genau dann invertierbar ist, wenn $a_0 \in R$ eine Einheit ist.

   *Lösung*:

   (a)
   - Aus den Axiomen für $(R, +)$ folgt, dass $(R[[X]], +)$ eine abelsche Gruppe mit der Nullfolge (0) als Neutralelement ist.
   - Die Multiplikation ist assoziativ, denn für $(a_n), (b_n), (c_n) \in R[[X]]$ gilt

$$\begin{aligned} ((a_n)(b_n))(c_n) &= \left(\sum_{i=0}^{n} a_i b_{n-i}\right)(c_n) = \left(\sum_{j=0}^{n} \left(\sum_{i=0}^{j} a_i b_{j-i}\right) c_{n-j}\right) \\ &= \left(\sum_{i=0}^{n} \sum_{j=i}^{n} a_i b_{j-i} c_{n-j}\right) = \left(\sum_{i=0} a_i \left(\sum_{j=0}^{n-i} b_j c_{n-i-j}\right)\right) \\ &= (a_n)\left(\sum_{j=0}^{n} b_j c_{n-j}\right) = (a_n)((b_n)(c_n)). \end{aligned}$$

   - Die Multiplikation ist kommutativ, denn wegen der Kommutativität von $R$ gilt für $(a_n), (b_n) \in R[[X]]$

$$(a_n)(b_n) = \left(\sum_{i=0}^{n} a_i b_{n-i}\right) = \left(\sum_{i=0}^{n} b_{n-i} a_i\right) = \left(\sum_{j=0}^{n} b_j a_{n-j}\right) = (b_n)(a_n).$$

   - Die Folge $(e_n)$ mit $e_0 = 1$ und $e_i = 0$ für $i > 0$ ist Einselement, denn für $(a_n) \in R[[X]]$ beliebig ist

$$(e_n)(a_n) = (a_n)(e_n) = \left(\sum_{i=0}^{n} a_i e_{n-i}\right) = (a_n).$$

   - Die Gültigkeit des Distributivgesetzes folgt aus einer analogen Rechnung und dem Distributivgesetz für $R$.

   Im Folgenden schreiben wir ein Element $(a_n) \in R[[X]]$ als *formale Potenzreihe* $a_0 + \sum_{n>0} a_n X^n$.

   (b) Wir nehmen zunächst an, dass $a_0 + \sum_{i>0} a_i X^i \in R[[X]]$ invertierbar ist. Das heisst, es existiert $b_0 + \sum_{i>0} b_i X^i \in R[[X]]$, so dass $(a_0 + \sum_{i>0} a_i X^i)(b_0 + \sum_{i>0} b_i X^i) = a_0 b_0 + \sum_{n>0} (\sum_{i=0}^{n} a_i b_{n-i}) X^n = 1$ ist. Daraus folgt nach obiger Beschreibung des Einselements

$$a_0 b_0 = 1 \quad \text{und} \quad \sum_{i=0}^{n} a_i b_{n-i} = 0, \ n > 0.$$

Insbesondere ist $a_0$ in $R$ invertierbar.

Falls umgekehrt $a_0 + \sum_{i>0} a_i X^i \in R[[X]]$ mit $a_0$ in $R$ invertierbar gegeben ist, definieren wir induktiv:

$$\begin{array}{rcl} b_0 & := & a_0^{-1} \\ b_n & := & -a_0^{-1}\big(\sum_{i=1}^{n} a_i b_{n-i}\big) \quad \text{für } n > 0 \end{array}$$

Dann ist $b_0 + \sum_{i>0} b_i X^i \in R[[X]]$ und

$$\big(a_0 + \textstyle\sum_{i>0} a_i X^i\big)\big(b_0 + \sum_{i>0} b_i X^i\big) = a_0 b_0 + \sum_{n>0}(\sum_{i=0}^{n} a_i b_{n-i}) X^n = 1,$$

denn für $n = 0$ ist $a_0 b_0 = a_0 a_0^{-1} = 1$ und für $n > 0$ ist

$$\begin{array}{rcl} \sum_{i=0}^{n} a_i b_{n-i} & = & a_0 b_n + \sum_{i=1}^{n} a_i b_{n-i} \\ & = & -\sum_{i=1}^{n} a_i b_{n-i} + \sum_{i=1}^{n} a_i b_{n-i} \\ & = & 0. \end{array}$$

Somit ist $a_0 + \sum_{i>0} a_i X^i$ in $R[[X]]$ invertierbar.

6. Welche der Unterringe

$$\mathbb{Z}[i, \tfrac{1}{5}], \quad \mathbb{Z}[\tfrac{i}{25}], \quad \mathbb{Z}[\tfrac{4i}{5}], \quad \mathbb{Z}[\tfrac{4i}{5}, 4+3i]$$

von $\mathbb{C}$ sind gleich?

*Lösung*: Zuerst bemerken wir, dass sich der Unterring $\mathbb{Z}[i, \frac{1}{5}] \subset \mathbb{C}$ als

$$\mathbb{Z}[i, \tfrac{1}{5}] = \{\tfrac{a+bi}{5^k} \mid a, b \in \mathbb{Z},\, k \in \mathbb{Z}^{\geqslant 0}\}$$

schreiben lässt. In der Tat ist die rechte Seite ein Unterring von $\mathbb{C}$, da sie abgeschlossen unter Addition, Bildung von additiven Inversen und Multiplikation ist. Zudem ist sie wegen $\frac{a+bi}{5^k} = \big(\frac{1}{5}\big)^k \cdot (a+bi)$ als Ring von $i$ und $\frac{1}{5}$ über $\mathbb{Z}$ erzeugt, also ist sie gleich $\mathbb{Z}[i, \frac{1}{5}]$.

Die Elemente $\frac{i}{25}, \frac{4i}{5}, 4+3i$ liegen daher alle in $\mathbb{Z}[i, \frac{1}{5}]$. Somit sind $\mathbb{Z}[\frac{i}{25}]$, $\mathbb{Z}[\frac{4i}{5}]$ und $\mathbb{Z}[\frac{4i}{5}, 4+3i]$ in $\mathbb{Z}[i, \frac{1}{5}]$ enthalten. Wegen

$$\begin{array}{lll} i = 25\,\big(\frac{i}{25}\big) & & \text{und} \quad \frac{1}{5} = -125(\frac{i}{25})^2, \\ i = 5\,\big(\frac{4i}{5}\big) - (4+3i) + 4 & & \text{und} \quad \frac{1}{5} = -5\,\big(\frac{4i}{5}\big)^2 - 3 \end{array}$$

gilt für $\mathbb{Z}[\frac{i}{25}]$ und $\mathbb{Z}[\frac{4i}{5}, 4+3i]$ auch die umgekehrte Inklusion. Es gilt also

$$\mathbb{Z}[i, \tfrac{1}{5}] = \mathbb{Z}[\tfrac{i}{25}] = \mathbb{Z}[\tfrac{4i}{5}, 4+3i].$$

Der Unterring $\mathbb{Z}[\frac{4i}{5}]$ enthält wegen

$$4i = 5\,\big(\tfrac{4i}{5}\big) \quad \text{und} \quad \tfrac{1}{5} = -5\,\big(\tfrac{4i}{5}\big)^2 - 3$$

die Elemente $4i$ und $\frac{1}{5}$. Deshalb gilt die Inklusion

$$\{\tfrac{a+4bi}{5^k} \mid a, b \in \mathbb{Z},\, k \in \mathbb{Z}^{\geqslant 0}\} \subset \mathbb{Z}[\tfrac{4i}{5}].$$

Die linke Seite ist selber ein Unterring, da sie 1 enthält und abgeschlossen unter Addition, Bildung von additiven Inversen, und Multiplikation ist. Zudem ist $\frac{4i}{5}$ ein Element dieses Unterrings. Somit gilt sogar

$$\mathbb{Z}[\tfrac{4i}{5}] = \{\tfrac{a+4bi}{5^k} \mid a, b \in \mathbb{Z},\, k \in \mathbb{Z}^{\geqslant 0}\}.$$

Da $\frac{4b}{5^k} \neq 1$ für alle $b \in \mathbb{Z}$ und $k \in \mathbb{Z}^{>0}$ gilt, ist $i$ kein Element von $\mathbb{Z}[\frac{4i}{5}]$. Daher ist $\mathbb{Z}[\frac{4i}{5}]$ echt in $\mathbb{Z}[i, \frac{i}{5}] = \mathbb{Z}[\frac{i}{25}] = \mathbb{Z}[\frac{4i}{5}, 4 + 3i]$ enthalten.

*7. Zeige, dass jeder endlich erzeugte unitäre Unterring von $\mathbb{Q}$ die Form $\mathbb{Z}[\frac{1}{n}]$ für ein $n \in \mathbb{Z}^{>0}$ hat. Folgere daraus, dass $\mathbb{Q}$ als Ring nicht endlich erzeugt ist.

*Lösung*: Sei $R \subset \mathbb{Q}$ ein endlich erzeugter unitärer Unterring mit Erzeugenden $\alpha_1, \ldots, \alpha_k \in \mathbb{Q}$. Wegen $1 \in R$ enthält $R$ den Unterring $\mathbb{Z}$, also ist $R = \mathbb{Z}[\alpha_1, \ldots, \alpha_k]$. Wir können jedes $\alpha_i$ auf eindeutige Weise schreiben als $\alpha_i = \frac{p_i}{q_i}$ für teilerfremde $p_i \in \mathbb{Z}$ und $q_i \in \mathbb{Z}^{>0}$. Sei $n := \mathrm{kgV}(q_1, \ldots, q_k)$.

Dann ist $\alpha_i = \frac{p_i}{q_i} = \frac{p_i d_i}{n}$ für $1 \leqslant i \leqslant k$, wobei $d_i := \frac{n}{q_i}$. Also sind alle Erzeugende ganzzahlige Vielfache von $\frac{1}{n}$, und somit $R = \mathbb{Z}[\alpha_1, \ldots, \alpha_k] \subset \mathbb{Z}[\frac{1}{n}]$.

Da $p_i$ und $q_i$ für $1 \leqslant i \leqslant k$ teilerfremd sind, existieren nach dem chinesischen Restsatz $a_i, b_i \in \mathbb{Z}$ mit $a_i p_i + b_i q_i = 1$. Dann gilt $\frac{1}{q_i} = a_i \alpha_i + b_i$, und somit $\mathbb{Z}[\frac{1}{q_1}, \ldots, \frac{1}{q_k}] \subset \mathbb{Z}[\alpha_1, \ldots, \alpha_k] = R$. Zudem ist $n$ ein Teiler von $q_1 \cdots q_k$, also ist $\frac{1}{n} = l \frac{1}{q_1} \cdots \frac{1}{q_k}$ für ein $\ell \in \mathbb{Z}$, und es gilt $\mathbb{Z}[\frac{1}{n}] \subset \mathbb{Z}[\frac{1}{q_1}, \ldots, \frac{1}{q_k}]$.

Also haben wir gezeigt, dass $R = \mathbb{Z}[\frac{1}{n}]$ gilt.

Ist nun $R = \mathbb{Z}[\frac{1}{n}] \subset \mathbb{Q}$ ein beliebiger endlich erzeugter unitärer Unterring, so existiert eine Primzahl $p$ mit $p \nmid n$; dann ist $\frac{1}{p} \in \mathbb{Q} \setminus R$, also $R \neq \mathbb{Q}$. Dies zeigt, dass $\mathbb{Q}$ als Ring nicht endlich erzeugt ist.