Musterlösung Serie 7

Polynomringe, Matrizen, Integritätsbereiche

*1. Zeige mit der universellen Eigenschaft von Polynomringen für jedes $1 \leqslant m \leqslant n$ die Isomorphie

$$R[X_1, ..., X_n] \;\cong\; R[X_1, ..., X_m][X_{m+1}, ..., X_n].$$

Lösung: Betrachte einen Ring S, einen Ringhomomorphismus $\varphi\colon R \to S$ und Elemente $y_1, \ldots, y_n \in S$. Nach der universellen Eigenschaft von $R' := R[X_1, ..., X_m]$ existiert dann ein Ringhomomorphismus $\varphi'\colon R' \to S$ mit $\varphi'|R = \varphi$ und $\varphi'(X_i) = y_i$ für alle $1 \leqslant i \leqslant m$. Nach der universellen Eigenschaft von $R'' := R'[X_{m+1}, ..., X_n]$ existiert dann weiter ein Ringhomomorphismus $\varphi''\colon R'' \to S$ mit $\varphi''|R' = \varphi'$ und $\varphi''(X_i) = y_i$ für alle $m+1 \leqslant i \leqslant n$. Für alle $x \in R$ gilt nun $\varphi''(x) = \varphi'(x) = \varphi(x)$, und für alle $1 \leqslant i \leqslant m$ gilt $\varphi''(X_i) = \varphi'(X_i) = y_i$. Somit erfüllt φ'' die Bedingungen $\varphi''|R = \varphi$ und $\varphi''(X_i) = y_i$ für alle $1 \leqslant i \leqslant n$.

Sei $\psi''\colon R'' \to S$ ein weiterer Ringhomomorphismus mit $\psi''|R = \varphi$ und $\psi''(X_i) = y_i$ für alle $1 \leqslant i \leqslant n$. Dann ist $\psi' := \psi''|R'$ ein Ringhomomorphismus $R' \to S$ mit $\psi'|R = \varphi$ und $\psi'(X_i) = y_i$ für alle $1 \leqslant i \leqslant m$. Aufgrund der Eindeutigkeit in der universellen Eigenschaft von R' folgt dann $\psi' = \varphi'$. Weiter ist $\psi''\colon R'' \to S$ ein Ringhomomorphismus mit $\psi''|R' = \psi' = \varphi'$ und $\psi''(X_i) = y_i$ für alle $m+1 \leqslant i \leqslant n$. Aufgrund der Eindeutigkeit in der universellen Eigenschaft von R'' folgt $\psi'' = \varphi''$.

Damit haben wir gezeigt, dass genau ein Ringhomomorphismus $\varphi''\colon R'' \to S$ existiert mit $\varphi''|R = \varphi$ und $\varphi''(X_i) = y_i$ für alle $1 \leqslant i \leqslant n$. Dies ist gerade die universelle Eigenschaft von $R''' := R[X_1, ..., X_n]$.

Daraus erhalten wir nun die gesuchte Isomorphie wie folgt. Aufgrund der gerade bewiesenen universellen Eigenschaft mit $S := R'''$ existiert ein Ringhomomorphismus $\kappa\colon R'' \to R'''$ mit $\kappa|R = \mathrm{id}_R$ und $\kappa(X_i) = X_i$ für alle $1 \leqslant i \leqslant n$. Aufgrund der universellen Eigenschaft von R''' existiert ein Ringhomomorphismus $\lambda\colon R''' \to R''$ mit $\lambda|R = \mathrm{id}_R$ und $\lambda(X_i) = X_i$ für alle $1 \leqslant i \leqslant n$. Für den zusammengesetzten Ringhomomorphismus $\lambda \circ \kappa\colon R'' \to R''$ gilt dann $(\lambda \circ \kappa)|R = \mathrm{id}_R$ und $(\lambda \circ \kappa)(X_i) = X_i$ für alle $1 \leqslant i \leqslant n$. Da die Identität auf R'' dieselben Bedingungen erfüllt, folgt aus der Eindeutigkeit in der universellen Eigenschaft von R'' die Gleichung $\lambda \circ \kappa = \mathrm{id}_R$. Umgekehrt gilt für den zusammengesetzten Ringhomomorphismus $\kappa \circ \lambda\colon R''' \to R'''$ dann $(\kappa \circ \lambda)|R = \mathrm{id}_R$ und $(\kappa \circ \lambda)(X_i) = X_i$ für alle $1 \leqslant i \leqslant n$. Da die Identität auf R''' dieselben Bedingungen erfüllt, folgt aus der Eindeutigkeit in der universellen Eigenschaft von R''' dann die Gleichung $\kappa \circ \lambda = \mathrm{id}_R$. Zusammen zeigt dies, dass κ und λ zueinander inverse Ringisomorphismen sind.

2. (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

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

- 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. Dann existiert $b_0 + \sum_{i>0} b_i X^i \in R[[X]]$ mit

$$\left(a_0 + \sum_{i>0} a_i X^i\right)\left(b_0 + \sum_{i>0} b_i X^i\right) = a_0 b_0 + \sum_{n>0}\left(\sum_{i=0}^n a_i b_{n-i}\right) X^n = 1.$$

Nach obiger Beschreibung des Einselements folgt daraus

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

Insbesondere ist a_0 eine Einheit von R.

Betrachte umgekehrt $a_0 + \sum_{i>0} a_i X^i \in R[[X]]$ mit einer Einheit $a_0 \in R^\times$. Dann definieren wir induktiv:

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

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

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

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

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

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

3. Sei $K[X]$ der Polynomring in einer Variablen X über einem Körper K. Betrachte einen Ringautomorphismus $\sigma : K[X] \to K[X]$, dessen Einschränkung auf K die Identität ist. (Mit anderen Worten ist σ ein *Automorphismus von K-Algebren.*) Zeige, dass es Elemente $a_1 \in K^\times$ und $a_0 \in K$ gibt, so dass $\sigma(X) = a_1 X + a_0$ ist.

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

   $$\sigma(X) \;=\; a_n X^n + ... + a_0 \qquad \text{und} \qquad \sigma^{-1}(X) \;=\; b_m X^m + ... + b_0$$

   mit $a_i, b_j \in K$ und $a_n, b_m \neq 0$ und berechne

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

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

4. Der Satz von Cayley-Hamilton besagt, dass jede quadratische Matrix über einem Ring Nullstelle ihres charakteristischen Polynoms ist. Beweise dies wie folgt:

   (a) Für obere Dreiecksmatrizen durch Induktion über die Grösse der Matrix.

   (b) Für alle quadratischen Matrizen über $\mathbb{C}$.

   (c) Im allgemeinen Fall analog zu Meta-Proposition 2.6.1 der Vorlesung.

   Lösung:

(a) Betrachte eine obere Dreiecksmatrix A der Grösse $n \times n$. Im Fall $n = 0$ ist $\chi_A(A)$ die Nullmatrix, da je zwei 0×0-Matrizen gleich sind. Im Fall $n > 0$ schreiben wir $A = \left(\begin{smallmatrix} A' & * \\ 0 & a \end{smallmatrix}\right)$ mit einer oberen Dreiecksmatrix A' der Grösse $(n-1) \times (n-1)$. Das charakteristische Polynom von A ist dann

$$\chi_A(X) \;=\; \det(X \cdot I_n - A) \;=\; \det \begin{pmatrix} X \cdot I_{n-1} - A' & * \\ 0 & X - a \end{pmatrix} \;=\; \chi_{A'}(X) \cdot (X - a)$$

mit dem charakteristischen Polynom $\chi_{A'}(X)$ von A'. Nach der Induktionsannahme gilt nun schon $\chi_{A'}(A') = O_{n-1}$. Mit den üblichen Rechenregeln für Blockdreiecksmatrizen folgt daraus $\chi_{A'}(A) = \left(\begin{smallmatrix} O_{n-1} & * \\ 0 & * \end{smallmatrix}\right)$ und daher

$$\chi_{A'}(A) \;=\; \chi_{A'}(A) \cdot (A - a \cdot I_n) \;=\; \begin{pmatrix} O_{n-1} & * \\ 0 & * \end{pmatrix} \begin{pmatrix} * & * \\ 0 & 0 \end{pmatrix} \;=\; O_n.$$

Durch Induktion über n folgt die gewünschte Aussage somit für alle $n \geqslant 0$.

(b) In der Linearen Algebra I haben wir — ohne Verwendung des Satzes von Cayley-Hamilton — gezeigt, dass jeder Endomorphismus eines endlich-dimensionalen Vektorraums über einem algebraisch abgeschlossenen Körper trigonalisierbar ist (siehe §8.4 der Zusammenfassung Lineare Algebra). Für Matrizen bedeutet dies insbesondere, dass für jede komplexe $n \times n$-Matrix A eine invertierbare komplexe $n \times n$-Matrix U existiert, so dass $B := UAU^{-1}$ eine obere Dreiecksmatrix ist. Als ähnliche Matrizen haben A und B nun dasselbe charakteristische Polynom χ_A, und nach (a) gilt demnach $\chi_A(B) = O_n$. Daraus folgt

$$\chi_A(A) \;=\; \chi_A(U^{-1}BU) \;=\; U^{-1}\chi_A(B)U \;=\; U^{-1}O_nU \;=\; O_n.$$

(c) Betrachte den Polynomring $R := \mathbb{Z}[X_{ij}|_{1 \leqslant i,j \leqslant n}]$ in den Variablen X_{ij} und die $n \times n$-Matrix $A := (X_{ij})_{i,j}$ mit Koeffizienten in R. Ihr charakteristisches Polynom ist dann ein Polynom $\chi_A(X) \in R[X]$, und $\chi_A(A) = (F_{\mu\nu})_{\mu,\nu}$ ist wieder eine Matrix mit Koeffizienten in R. Eine beliebige $n \times n$-Matrix $B = (b_{ij})_{i,j}$ über einem Ring S erhalten wir aus A durch Einsetzen der Werte $X_{ij} := b_{ij}$ für alle i, j. Mit derselben Substitution erhalten wir aus $\chi_A(A)$ die Matrix $\chi_B(B)$.

Im Fall $S = \mathbb{C}$ gilt nun aber nach (b) schon $\chi_B(B) = 0$ für beliebige Werte $b_{ij} \in \mathbb{C}$. Dies bedeutet, dass für jedes μ und ν die Werte von $F_{\mu\nu}$ auf ganz $\mathbb{C}^{n^2}$ verschwinden. Da $\mathbb{C}$ ein unendlicher Körper ist, muss $F_{\mu\nu}$ also das Nullpolynom sein.

Das Einsetzen beliebiger Werte $b_{ij} \in S$ in $F_{\mu\nu}$ liefert dann ebenfalls immer das Nullelement $0_S \in S$. Somit gilt für jede $n \times n$-Matrix B über jedem Ring S die Gleichung $\chi_B(B) = O_n$, wie zu zeigen war.

5. (a) Zeige: Für jeden Integritätsbereich R gilt $(R[X])^\times = R^\times$.

   (b) Finde einen Ring R mit $(R[X])^\times \neq R^\times$.

   Lösung:

   (a) Für jeden Ring R induziert der injektive Ringhomomorphismus $R \hookrightarrow R[X]$ eine Inklusion $R^\times \hookrightarrow (R[X])^\times$.

   Sei nun R ein Integritätsbereich und $f \in (R[X])^\times$. Dann existiert ein $g \in R[X]$ so dass $fg = 1$ ist. Wegen $1 \neq 0$ in R gilt dasselbe auch in $R[X]$, und daraus folgt $f, g \neq 0$. Schreibe $f = \sum_{i=0}^{n} a_i X^i$ und $g = \sum_{j=0}^{m} b_j X^j$ für Koeffizienten $a_0, \ldots, a_n \in R$ und $b_0, \ldots, b_m \in R$ mit $a_n \neq 0 \neq b_m$. Dann ist $fg = \sum_{k=0}^{n+m} \sum_{i+j=k} a_i b_j X^k$, und der Koeffizient von X^{n+m} darin ist gleich $a_n b_m$. Weil $a_n \neq 0 \neq b_m$ gilt und R ein Integritätsbereich ist, folgt $a_n b_m \neq 0$. Also hat fg den Grad $n + m$. Wegen $fg = 1$ muss nun aber $n + m = 0$ sein, was nur mit $n = m = 0$ möglich ist. Somit liegen f, g schon in R und wegen $fg = 1$ also auch schon in $R^\times$. Insgesamt zeigt dies $(R[X])^\times \subset R^\times$ und damit (a).

   (b) Im Ring $\mathbb{Z}/4\mathbb{Z}[X]$ ist das Element $1+2X$ wegen $(1+2X)(1-2X) = 1-4X^2 = 1$ invertierbar, aber $1 + 2X \notin \mathbb{Z}/4\mathbb{Z}$.

   Bemerkung: Allgemeiner kann man zeigen, dass ein Polynom $f = \sum_i' a_i X^i \in R[X]$ über einem beliebigen Ring R genau dann invertierbar ist, wenn $a_0 \in R^\times$ ist und alle höheren Koeffizienten $a_1, a_2, \ldots$ nilpotent sind.

6. (a) Zeige: Jeder Unterring $R \subset \mathbb{C}$, der ein endlich-dimensionaler Vektorraum über $\mathbb{Q}$ ist, ist ein Körper.

   (*Hinweis:* Für jedes $f \in R \setminus \{0\}$ untersuche die Abbildung $R \to R,\ g \mapsto gf$.)

   (b) Zeige: Für jedes $n > 0$ ist

$$\mathbb{Q}[\sqrt[n]{2}] \;=\; \left\{ \sum_{i=0}^{n-1} a_i (\sqrt[n]{2})^i \;\middle|\; \forall i\colon a_i \in \mathbb{Q} \right\}.$$

   Folgere, dass $\mathbb{Q}[\sqrt[n]{2}]$ ein Körper ist.

   (c) Bestimme das inverse Element $\left(1 + \sqrt[3]{2} - \sqrt[3]{4}\right)^{-1} \in \mathbb{Q}[\sqrt[3]{2}]$ in der Darstellung $a_0 + a_1\sqrt[3]{2} + a_2\sqrt[3]{4}$ für $a_0, a_1, a_2 \in \mathbb{Q}$.

   Lösung:

   (a) Als Unterring eines Körpers ist R bereits ein Integritätsbereich. Wir müssen daher nur noch zeigen, dass jedes Element $f \in R \setminus \{0\}$ in R invertierbar ist. Betrachte dafür die Abbildung $m_f\colon R \to R,\ g \mapsto gf$. Dies ist eine lineare Abbildung von $\mathbb{Q}$-Vektorräumen. Für jedes $g \neq 0$ ist auch $m_f(g) = fg \neq 0$ im Körper $\mathbb{C}$. Also ist $\mathrm{Kern}(m_f) = \{0\}$ und m_f somit injektiv. Weil R ein

endlichdimensionaler $\mathbb{Q}$-Vektorraum ist, ist der Endomorphismus m_f demnach auch surjektiv! Also existiert ein $h \in R$ mit $hf = m_f(h) = 1$. Somit ist f invertierbar, was zu zeigen war.

(b) Wegen $(\sqrt[n]{2})^n = 2 \in \mathbb{Q}$ zeigt man schnell, dass die Menge

$$K \;:=\; \left\{ \sum_{i=0}^{n-1} a_i (\sqrt[n]{2})^i \;\middle|\; \forall i\colon a_i \in \mathbb{Q} \right\}$$

ein Unterring von $\mathbb{C}$ ist. Der kleinste Unterring $\mathbb{Q}[\sqrt[n]{2}]$, der $\mathbb{Q}$ und $\sqrt[n]{2}$ enthält, ist also schon in K enthalten. Umgekehrt folgt aus der expliziten Beschreibung von $\mathbb{Q}[\sqrt[n]{2}]$ in Proposition 2.4.4 der Vorlesung die Inklusion $K \subset \mathbb{Q}[\sqrt[n]{2}]$. Zusammen folgt $K = \mathbb{Q}[\sqrt[n]{2}]$.

Als $\mathbb{Q}$-Vektorraum ist $\mathbb{Q}[\sqrt[n]{2}]$ daher von den endlich vielen Elementen $(\sqrt[n]{2})^i$ für $0 \leqslant i < n$ erzeugt und somit endlichdimensional. Wegen (a) ist er damit ein Unterkörper von $\mathbb{C}$.

(c) Für das gesuchte Element $a_0 + a_1\sqrt[3]{2} + a_2\sqrt[3]{2}$ muss gelten

$$\begin{aligned} 1 &= (a_0 + a_1\sqrt[3]{2} + a_2\sqrt[3]{4})(1 + \sqrt[3]{2} - \sqrt[3]{4}) \\ &= a_0 - 2a_1 + 2a_2 + (a_0 + a_1 - 2a_2)\sqrt[3]{2} + (a_1 - a_0 + a_2)\sqrt[3]{4} \end{aligned}$$

Dies ist sicher dann der Fall, wenn das lineare Gleichungssystem

$$\begin{aligned} a_0 + a_1 - 2a_2 &= 0, \\ a_1 - a_0 + a_2 &= 0, \\ a_0 - 2a_1 + 2a_2 &= 1 \end{aligned}$$

erfüllt ist. (Ob bzw. dass dies tatsächlich auch notwendig ist, muss uns hier nicht kümmern.) Wir suchen also eine Lösung der Matrixgleichung

$$\begin{pmatrix} 1 & 1 & -2 \\ -1 & 1 & 1 \\ 1 & -2 & 2 \end{pmatrix} \cdot \begin{pmatrix} a_0 \\ a_1 \\ a_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}.$$

Der Gauss-Algorithmus

$$\left(\begin{array}{ccc|c} 1 & 1 & -2 & 0 \\ -1 & 1 & 1 & 0 \\ 1 & -2 & 2 & 1 \end{array}\right) \rightsquigarrow \left(\begin{array}{ccc|c} 1 & 0 & 0 & \frac{3}{5} \\ 0 & 1 & 0 & \frac{1}{5} \\ 0 & 0 & 1 & \frac{2}{5} \end{array}\right)$$

liefert die Lösung $a_0 = \frac{3}{5},\ a_1 = \frac{1}{5},\ a_2 = \frac{2}{5}$. Es gilt also

$$\left(1 + \sqrt[3]{2} - \sqrt[3]{4}\right)^{-1} \;=\; \tfrac{3}{5} + \tfrac{1}{5}\sqrt[3]{2} + \tfrac{2}{5}\sqrt[3]{4}.$$