R. Herzog, G. Müller
Universität Heidelberg

Hausaufgabe II - 6 (Lösung)

Ausgabedatum: 18. Mai 2026
Abgabedatum: 25. Mai 2026

Hausaufgabe II-6.1 (Basis zu Polynomringen und -homomorphismen) 2 + 2 + 2 + 1 = 7 Punkte

(a) Bestimmen Sie alle Koeffizienten (und damit die Darstellung als Monomsumme) des Polynomprodukts

$$\left(\mathop{\triangle}_{i=1}^{2} [\![1, i]\!] t^{2i}\right) \cap \left(\mathop{\triangle}_{i=0}^{2} \{2^i\} t^i\right)$$

im Polynomring $\mathcal{P}(\mathbb{Z})[t]$ über dem Ring $(\mathcal{P}(\mathbb{Z}), \triangle, \cap)$.

(b) Es sei $(R, +, \cdot)$ ein Integritätsring. Bestimmen Sie die bzgl. der Polynommultiplikation invertierbaren Elemente des Polynomrings $(R[t], +, \cdot)$.

(c) Es seien $(R_1, +_1, \cdot_1)$ und $(R_2, +_2, \cdot_2)$ zwei kommutative Ringe mit Eins und $f\colon R_1 \to R_2$ ein Ringhomomorphismus. Zeigen Sie, dass durch

$$\begin{aligned} \tilde{f}\colon R_1[t] &\to R_2[t] \\ \tilde{f}\Big(\sum_{i=0}^{n} a_i \cdot_1 t^i\Big) &\coloneqq \sum_{i=0}^{n} f(a_i) \cdot_2 t^i \end{aligned}$$

ein Ringhomomorphismus zwischen den entsprechenden Polynomringen $(R_1[t], +_1, \cdot_1)$ und $(R_2[t], +_2, \cdot_2)$ definiert ist.

(d) Es sei $(R, +, \cdot)$ ein kommutativer Ring mit Eins. Beweisen oder widerlegen Sie, dass

$$\begin{aligned} f\colon R[t] &\to R[t] \\ f\Big(\sum_{i=0}^{k} a_i \cdot t^i\Big) &\coloneqq \sum_{i=1}^{k} i\, a_i \cdot t^{i-1}, \end{aligned}$$

genannt die Ableitungsabbildung auf $R[t]$, ein Ringendomorphismus von $(R[t], +, \cdot)$ in sich selbst ist.

Lösung.

(a) Die Koeffizientendarstellung der beiden Polynome ist

$$\begin{aligned}&(\emptyset, \emptyset, \{1\}, \emptyset, [\![1,2]\!], \emptyset, \dots)\\&(\{1\}, \{2\}, \{4\}, \emptyset, \dots)\end{aligned}$$

und damit ergibt sich aus der Definition der Polynommultiplikation die Koeffizientendarstellung

$$\begin{aligned}&(\emptyset \cap \{1\},\\&\ \{1\} \cap \emptyset \triangle \{2\} \cap \emptyset,\\&\ \{1\} \cap \{1\} \triangle \{2\} \cap \emptyset \triangle \{4\} \cap \emptyset,\\&\ \{1\} \cap \emptyset \triangle \{2\} \cap \{1\} \triangle \{4\} \cap \emptyset,\\&\ \{1\} \cap [\![1,2]\!] \triangle \{2\} \cap \emptyset \triangle \{4\} \cap \{1\},\\&\ \{1\} \cap \emptyset \triangle \{2\} \cap [\![1,2]\!] \triangle \{4\} \cap \emptyset,\\&\ \{1\} \cap [\![1,3]\!] \triangle \{2\} \cap \emptyset \triangle \{4\} \cap [\![1,2]\!],\\&\ \{2\} \cap [\![1,3]\!] \triangle \{4\} \cap \emptyset,\\&\ \{4\} \cap [\![1,3]\!])\\ =\ &(\emptyset, \emptyset, \{1\}, \emptyset, \{1\}, \{2\}, \{1\}, \{2\}, \emptyset, \dots)\end{aligned}$$

und damit die Darstellung

$$\{1\}t^2 \triangle \{1\}t^4 \triangle \{2\}t^5 \triangle \{1\}t^6 \triangle \{2\}t^7.$$

(2 Punkte)

(b) Da $(R, +, \cdot)$ ein Integritätsring ist, ist er insbesondere nullteilerfrei. Für $p, q \in R[t]$ mit den Darstellungen

$$\begin{aligned}p &= a_m \cdot t^m + \dots + a_1 \cdot t + a_0\\ q &= b_n \cdot t^n \ \ + \dots + b_1 \cdot t + b_0\end{aligned}$$

mit $m, n \in \mathbb{N}_0$ ist

$$p \cdot q \coloneqq c_{m+n} \cdot t^{m+n} + \dots + c_1 \cdot t + c_0,$$

mit den Koeffizienten

$$c_k \coloneqq \sum_{i=0}^{k} a_i \cdot b_{k-i} = \sum_{\substack{i,j=0 \\ i+j=k}}^{k} a_i \cdot b_j$$

für $k \in \mathbb{N}_0$. Es ist also $p \cdot q$ das Einspolynom genau dann, wenn $c_0 = a_0 \cdot b_0 = 1_R$ und $c_k = 0$ für $0 < k \leqslant m + n$. Die Koeffizienten a_0 und b_0 müssen also zueinander multiplikativ invers sein (und damit insbesondere ungleich 0_R). (1 Punkt)

Aus $c_k = 0_R$ für $1 \leqslant k \leqslant m + n$ folgern wir nun, dass $a_i = b_j = 0_R$ für $1 \leqslant i \leqslant n$ und $1 \leqslant j \leqslant m$, also dass p und q konstant sein müssen. Entsprechend sind dann die invertierbaren Polynome gerade die konstanten Polynome, deren Koeffizient in $(R, \cdot)$ invertierbar ist. Wir führen den Beweis induktiv über $d \colon n + m$, den Höchstwert der Potenzen von t in $p \cdot q$.

Für $d = 0$ ist nichts zu zeigen, denn p und q sind dann schon konstant. (0.5 Punkte)

Gilt die Aussage für alle Höchstpotenzen kleiner als $d \geqslant 1$, dann ist

$$0_R = c_d = c_{n+m} = a_n \cdot b_m. \tag{0.3}$$

Daraus folgt mit der Nullteilerfreiheit, dass $a_n = 0_R$ oder $b_m = 0_R$. In jedem Fall lässt sich eines der beiden Polynome p, q mit einer Darstellung schreiben, deren höchste Potenz in t um eins niedriger ist und nach Induktionsvoraussetzung sind dann also p und q konstant. (0.5 Punkte)

(c) Für $p, q \in R_1[t]$ mit den Darstellungen

$$\begin{aligned} p &= a_m \cdot_1 t^m +_1 \cdots +_1 a_1 \cdot_1 t +_1 a_0 \\ q &= b_n \cdot_1 t^n \ \ +_1 \cdots +_1 b_1 \cdot_1 t +_1 b_0 \end{aligned}$$

mit $n, m \in \mathbb{N}_0$ und $N = \max(n, m)$ (und den notwendigen Koeffizienten in den jeweiligen Polynomen mit 0_{R_1} aufgefüllt) ist

$$\begin{aligned} \tilde{f}(p +_1 q) &= \tilde{f}\left(\sum_{i=0}^{n} a_i \cdot_1 t^i + \sum_{j=0}^{m} b_j \cdot_1 t^j\right) \\ &= \tilde{f}\left(\sum_{i=0}^{N} a_i \cdot_1 t^i + \sum_{i=0}^{N} b_i \cdot_1 t^i\right) \\ &= \tilde{f}\left(\sum_{i=0}^{N} (a_i +_1 b_i) \cdot_1 t^i\right) \\ &= \sum_{i=0}^{N} f(a_i +_1 b_i) \cdot_2 t^i \end{aligned}$$

$$
\begin{aligned}
&= \sum_{i=0}^{N} (f(a_i) +_2 f(b_i)) \cdot_2 t^i \\
&= \sum_{i=0}^{N} f(a_i) \cdot_2 t^i +_2 \sum_{i=0}^{N} f(b_i) \cdot_2 t^i \\
&= \sum_{i=0}^{n} f(a_i) \cdot_2 t^i +_2 \sum_{j=0}^{m} f(b_j) \cdot_2 t^j \\
&= \tilde{f}(p) +_2 \tilde{f}(q),
\end{aligned}
$$

denn da f ein Ringhomomorphismus ist, ist $f(0_{R_1}) = 0_{R_2}$. (1 Punkt)

Außerdem ist

$$
\begin{aligned}
\tilde{f}(p \cdot_1 q) &= \tilde{f}\left(\sum_{i=0}^{n} a_i \cdot_1 t^i \cdot_1 \sum_{j=0}^{m} b_j \cdot_1 t^j\right) \\
&= \tilde{f}\left(\sum_{k=0}^{n+m} c_k \cdot_1 t^k\right) \\
&= \sum_{k=0}^{n+m} f(c_k) \cdot_2 t^k \\
&= \sum_{k=0}^{n+m} f\left(\sum_{i=0}^{k} a_i \cdot_1 b_{k-i}\right) \cdot_2 t^k \\
&= \sum_{k=0}^{n+m} \left(\sum_{i=0}^{k} f(a_i) \cdot_2 f(b_{k-i})\right) \cdot_2 t^k \\
&= \sum_{i=0}^{n} f(a_i) \cdot_2 t^i \cdot_2 \sum_{j=0}^{m} f(b_j) \cdot_2 t^j \\
&= \tilde{f}\left(\sum_{i=0}^{n} a_i \cdot_1 t^i\right) \cdot_2 \tilde{f}\left(\sum_{j=0}^{m} b_j \cdot_1 t^j\right) \\
&= \tilde{f}(p) \cdot_2 \tilde{f}(q)
\end{aligned}
$$

(1 Punkt)

(d) Die vorliegende Abbildung stellt das Verhalten der Ableitungen auf den zugehörigen Polynomfunktionen in t dar. Dass die Ableitungen mit Summen verträglich ist, ist ein Standardresultat aus der Analysis, das dürfte uns also keine Probleme machen. Mit Produkten hingegen ist die Ableitung im Allgemeinen nicht verträglich in dem benötigten

Sinn, hier gibt es nämlich die Produktregeln für Ableitungen. Ein Beispiel, an dem man diese Unverträglichkeit auch für Polynome sieht, sind die Polynome 1_R und $1_R \cdot t$, denn hier ist

$$f(1_R \cdot 1_R \cdot t) = 1_R \neq 0_R = 0_R \cdot 1_R = f(1_R) \cdot f(t).$$

Hier sieht man, dass die Abbildung also nicht einmal im Kontext von Polynomringen ohne Eins ein Ringhomomorphismus ist. Im Kontext von Ringen mit Eins erkennt man natürlich schneller, dass $f(1_R) = 0_R$ nur genau dann gleich 1_R ist, wenn R der Nullring war. (1 Punkt)

Hausaufgabe II-6.2 (Polynomgrad) 3 Punkte

Es sei $(R, +, \cdot)$ ein kommutativer Ring mit Eins und $p, q \in R[t]$ zwei Polynome. Zeigen Sie Lemma 28.10 des Skripts, also die folgenden Aussagen:

(a) $\deg(p + q) \leqslant \max\{\deg(p),\ \deg(q)\}$.
(b) $\deg(p \cdot q) \leqslant \deg(p) + \deg(q)$.
(c) Ist R nullteilerfrei, dann gilt sogar $\deg(p \cdot q) = \deg(p) + \deg(q)$.

Dabei sollen formal für $n \in \mathbb{N}_0$ die Beziehungen $\max\{n,\ (-\infty)\} = \max\{(-\infty), n\} = n$ gelten sowie $\max\{(-\infty),\ (-\infty)\} = -\infty$ und $n + (-\infty) = (-\infty) + n = (-\infty) + (-\infty) = -\infty$.

Lösung.

Wenn p oder q das Nullpolynom ist, dann sind Aussagen (a) bis (c) klar, denn deren Produkt ist wieder das Nullpolynom mit Grad $-\infty$.

Wir nehmen also für den Rest des Beweises an, dass p und q beide nicht das Nullpolynom sind und Darstellungen

$$\begin{aligned} p &= a_m \cdot t^m + \cdots + a_1 \cdot t + a_0 \\ q &= b_n \cdot t^n \;\; + \cdots + b_1 \cdot t + b_0 \end{aligned}$$

besitzen. Dabei seien die führenden Koeffizienten a_m und b_n ungleich 0_R, also ist $\deg(p) = m \in \mathbb{N}_0$ und $\deg(q) = n \in \mathbb{N}_0$.

(a) Alle Koeffizienten $a_k + b_k$ von $p + q$ mit $k > N \coloneqq \max\{m, n\}$ sind gleich 0_R. Also gilt $\deg(p + q) \leqslant \max\{m, n\} = \max\{\deg(p),\ \deg(q)\}$. (1 Punkt)
(b) Nach Definition der Polynommultiplikation sind alle Koeffizienten c_k von $p \cdot q$ mit $k > m+n$ gleich 0_R. Also ist $\deg(p \cdot q) \leqslant m + n = \deg(p) + \deg(q)$. (1 Punkt)

(c) Der führende Koeffizient von $p \cdot q$ ist $a_m \cdot b_n$. Da $a_m \neq 0_R$ und $b_n \neq 0_R$ waren und R nullteilerfrei ist, ist auch $a_m \cdot b_n \neq 0_R$. Daraus folgt mit $\deg(p \cdot q) = \deg(p) + \deg(q)$. (1 Punkt)

Hausaufgabe II-6.3 (Basics zu Moduln) 1 + 1 + 2 + 1 = 5 Punkte

(a) Erklären Sie, wann ein R-Modul ein R-Vektorraum ist.

(b) Bestimmen Sie alle Untermoduln eines kommutativen Rings R über sich selbst. Was ist besonders, wenn R sogar ein Körper ist?

(c) Bestimmen Sie alle $n, m \in \mathbb{N}$, für die $n\mathbb{Z}$ mit den Ringverknüpfungen aus $\mathbb{Z}$ ein Modul über dem Unterring $m\mathbb{Z}$ von $\mathbb{Z}$ ist und entscheiden Sie, wann es sich um unitäre Moduln handelt.

(d) Erklären Sie, welche Moduln über dem Nullring existieren.

Lösung.

(a) Ein R-Modul ist genau dann ein R-Vektorraum, wenn R ein Körper ist. Das ist offensichtlich eine notwendige Bedingung, weil wir Vektorräume ausschließlich über Körpern definiert haben. Hinreichend ist die Bedingung, denn die Definitionen sind für Körper (welche per Definition ein Einselement besitzen) exakt gleich. (1 Punkt)

(b) Entsprechend des Untermodulkriteriums sind alle Untermoduln gerade nichtleer und sind additiv und multiplikativ abgeschlossen, sie sind also Untergruppen der additiven abelschen Gruppe, die $R \cdot U = U \cdot R \subseteq U$ erfüllen, und sind damit genau die Ideale. (1 Punkt)

(c) Der Unterring $m\mathbb{Z}$ von $\mathbb{Z}$ ist kommutativ, es macht also schonmal zumindest Sinn sich diese Frage zu stellen. Weiterhin gibt es in $m\mathbb{Z}$ genau dann ein Einselement, wenn $m = 1$ ist, und bezüglich der aus $\mathbb{Z}$ geerbten Multiplikation ist dieses Element auch neutral, das haben wir also schonmal aus dem Weg.

Nun ist $n\mathbb{Z}$ mit der geerbten Addition offensichtlich eine Untergruppe von $\mathbb{Z}$ und damit abelsch, es gilt also die Verträglichkeit der beiden Verknüpfungen zu prüfen. Da es sich hier um die Ringverknüpfungen aus $\mathbb{Z}$ handelt gelten alle Distributivitäts- und Assoziativitätsgesetze weiter und somit sind alle $n\mathbb{Z}$ auch $m\mathbb{Z}$-Moduln für beliebige $n, m \in \mathbb{N}$. (2 Punkte)

(d) Wird der Nullring als Ring mit Eins interpretiert, indem die Eins mit der Null übereinstimmt, dann bildet nur die triviale Nullgruppe ein unitäres Modul über dem Nullring, denn aus den Distributivitätsgesetzen folgt exakt wie schon im Fall von Vektorräumen

(Lemma 11.5), dass $0_R \cdot v = 0_M$ für alle $v \in M$. Damit folgt aus der Neutralität von 1_R bezüglich der S-Multiplikation, dass für jedes $v \in M$ gilt:

$$v = 1_R \cdot v = 0_R \cdot v = 0_M.$$

(0.5 Punkte)

Wird der Nullring nicht als Ring mit Eins interpretiert, dann bildet die S-Multiplikation notwendigerweise konstant auf 0_M ab (Argumentation wie oben) und alle zusätzlichen Bedingungen aus der Definition eines Modul sind trivialerweise von jeder abelschen Gruppe erfüllt. (0.5 Punkte)

Hausaufgabe II-6.4 (Basen, Synthese und Analyse in Moduln) 3 + 4 = 7 Punkte

(a) Zeigen Sie, dass

$$\left(\begin{pmatrix}2\\0\end{pmatrix}, \begin{pmatrix}1\\1\end{pmatrix}, \begin{pmatrix}0\\3\end{pmatrix}\right)$$

ein linear abhängiges Erzeugendensystem von $\mathbb{Z}^2$ über $\mathbb{Z}$ ist, welches keine Basis als Teilfamilie enthält.

(b) Es sei M ein R-Modul, $n \in \mathbb{N}_0$ und $(v_i)_{i \in [\![1,n]\!]}$ eine Familie von Vektoren aus M. Zeigen Sie, dass die Abbildung

$$R^n \ni \begin{pmatrix}r_1\\ \vdots \\ r_n\end{pmatrix} \mapsto \sum_{i=1}^n r_i v_i \in M$$

ein Modulhomomorphismus ist. Wann handelt es sich um einen Isomorphismus?

Lösung.

(a) Die lineare Abhängigkeit der Familie sieht man direkt ein, denn

$$3 \cdot \begin{pmatrix}2\\0\end{pmatrix} - 6 \cdot \begin{pmatrix}1\\1\end{pmatrix} + 2 \cdot \begin{pmatrix}0\\3\end{pmatrix} = 0.$$

(1 Punkt)

Wir versuchen nun beliebige Vektoren

$$\begin{pmatrix}z_1\\z_2\end{pmatrix} \in \mathbb{Z}^2$$

aus der gegebenen Familie zu erzeugen.

Klar ist, dass

$$\left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right)$$

(die „Standardbasis“) ein Erzeugendensystem ist, denn

$$\begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = z_1 \begin{pmatrix} 1 \\ 0 \end{pmatrix} + z_2 \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

Wir erzeugen also diese Standardbasisvektoren aus unserer Basis und sind dann fertig. Konkret gilt:

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} = 2 \begin{pmatrix} 2 \\ 0 \end{pmatrix} - 3 \begin{pmatrix} 1 \\ 1 \end{pmatrix} + \begin{pmatrix} 0 \\ 3 \end{pmatrix}$$
$$\begin{pmatrix} 0 \\ 1 \end{pmatrix} = 1 \begin{pmatrix} 2 \\ 0 \end{pmatrix} - 2 \begin{pmatrix} 1 \\ 1 \end{pmatrix} + \begin{pmatrix} 0 \\ 3 \end{pmatrix}$$

Entsprechend ist

$$\begin{aligned} \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} &= z_1 \begin{pmatrix} 1 \\ 0 \end{pmatrix} + z_2 \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ &= (2z_1 + z_2) \begin{pmatrix} 2 \\ 0 \end{pmatrix} - (3z_1 + 2z_2) \begin{pmatrix} 1 \\ 1 \end{pmatrix} + (z_1 + z_2) \begin{pmatrix} 0 \\ 3 \end{pmatrix}. \end{aligned}$$

(2 Punkte)

(b) Wir bezeichnen die Abbildung hier als Φ in Anlehnung an die Syntheseabbildung in Vektorräumen. Auf Grund der Struktur im Modul M, konkret den gemischten Distributivitäts- und Assoziativitätsgesetzen) gilt für $\alpha, \beta \in R$:

$$\begin{aligned} \Phi\left(\alpha \begin{pmatrix} r_1 \\ \vdots \\ r_n \end{pmatrix} + \beta \begin{pmatrix} s_1 \\ \vdots \\ \tilde{s}_n \end{pmatrix} \right) &= \sum_{i=1}^{n} (\alpha r_i + \beta s_i) v_i) \\ &= \sum_{i=1}^{n} \alpha r_i v_i + \beta s_i v_i \\ &= \alpha \sum_{i=1}^{n} r_i v_i + \beta \sum_{i=1}^{n} s_i v_i \end{aligned}$$

$$= \alpha\Phi\begin{pmatrix} r_1 \\ \vdots \\ r_n \end{pmatrix} + \beta\Phi\begin{pmatrix} s_1 \\ \vdots \\ \tilde{s}_n \end{pmatrix}.$$

(2 Punkte)

Surjektivität liegt genau dann vor, wenn die Familie der v_i erzeugend ist bezüglich der Darstellungen als Linearkombinationen mit Ringkoeffizienten. Besitzt der Ring R ein Einselement (ist also M ein unitärer Modul), dann stimmt das gerade mit der Erzeugung im Hüllensinn überein, wie wir das aus Vektorräumen gewohnt sind. Falls keine Eins in R existiert ist die Bedingung „erzeugend bezüglich der Darstellungen als Linearkombinationen" i. A. sogar strenger, denn evtl können die v_i selbst nicht in der Summe eingebracht werden. (1 Punkt)

Injektivität liegt genau dann vor, wenn die Familie linear unabhängig ist, denn eindeutige Darstellbarkeit von Vektoren als Linearkombination ist auch in Moduln äquivalent zur linearen Unabhängigkeit, der Beweis folgt ganz analog wie in Vektorräumen. (1 Punkt)