Lösungsvorschlag zu Aufgabe 1 auf Blatt 5

Voraussetzung: A ist ein kommutativer Ring mit $0 \neq 1$.

Behauptung:

(a) Für alle $\ell, m \in \mathbb{N}$ gilt $A[X^\ell] \subseteq A[X^m]$ genau dann, wenn $\ell \in \langle m \rangle_{\mathbb{Z}}$ gilt.

(b) Für alle $\ell, m \in \mathbb{N}$ gilt $A[X^\ell] \cong A[X^m]$.

Bemerkung: Hier ist $A[X^\ell] \subseteq A[X]$ als Unterring zu verstehen, der aus dem Unterring $A \subseteq A[X]$ durch Hinzuadjungieren des Elements $X \in A[X]$ entsteht. Dann gilt gemäß der Definition 3.2.4:

$$A[X^\ell] = \left\{ \sum_{k=0}^{n} a_k (X^\ell)^k \,\middle|\, n \in \mathbb{N}_0, a_0, \ldots, a_n \in A \right\} = \left\{ \sum_{k=0}^{n} a_k X^{\ell k} \,\middle|\, n \in \mathbb{N}_0, a_0, \ldots, a_n \in A \right\}.$$

Beweis:

(a) Seien $\ell, m \in \mathbb{N}$ gegeben.

Beweis von $\ell \in \langle m \rangle_{\mathbb{Z}} \Longrightarrow A[X^\ell] \subseteq A[X^m]$:

Es gelte $\ell \in \langle m \rangle_{\mathbb{Z}}$. Es gilt

$$\langle m \rangle_{\mathbb{Z}} \overset{\text{Satz 2.2.7}}{=} \{km \mid k \in \mathbb{Z}\},$$

also können wir $k \in \mathbb{Z}$ wählen mit $\ell = km$. Sei nun $p \in A[X^\ell]$ geben und seien weiter $n \in \mathbb{N}_0$ und $a_0, \ldots, a_n \in A$ mit $p = \sum_{j=0}^{n} a_j (X^\ell)^j$ gegeben. Wegen $\ell = km$ folgt:

$$p = \sum_{j=0}^{n} a_j (X^\ell)^j = \sum_{j=0}^{n} a_j (X^{km})^j = \sum_{j=0}^{n} a_j (X^m)^{kj} =: \sum_{i=0}^{nj} \widetilde{a}_i (X^m)^i \in A[X^m],$$

wobei $\widetilde{a}_i$ für $i \in \{0, \ldots, nj\}$ im letzten Schritt definiert ist durch

$$\widetilde{a}_i = \begin{cases} a_j & \exists j \in \{0, \ldots, n\} : i = kj, \\ 0 & \text{sonst}. \end{cases}$$

Da $p \in A[X^\ell]$ beliebig war, ist damit $A[X^\ell] \subseteq A[X^m]$ gezeigt. *Der letzte Schritt mit den $\widetilde{a}_i$ ist vielleicht etwas „pedantisch“...*

Beweis von $A[X^\ell] \subseteq A[X^m] \Longrightarrow \ell \in \langle m \rangle_{\mathbb{Z}}$:

Wir nehmen an, dass $A[X^\ell] \subseteq A[X^m]$ gilt. Um zu zeigen, dass $\ell \in \langle m \rangle_{\mathbb{Z}}$ gilt, führen wir einen Widerspruchsbeweis. Dazu nehmen wir an, dass $\ell \notin \langle m \rangle_{\mathbb{Z}}$ gilt. Es gilt

$$\langle m \rangle_{\mathbb{Z}} \overset{\text{Satz 2.2.7}}{=} \{km \mid k \in \mathbb{Z}\},$$

also bedeutet $\ell \notin \langle m \rangle_{\mathbb{Z}}$ gerade, dass $\ell \neq km$ für alle $k \in \mathbb{Z}$ gilt.

Aus $A[X^\ell] \subseteq A[X^m]$ folgt insbesondere $X^\ell \in A[X^m]$. Also gibt es ein $n \in \mathbb{N}_0$ und $a_0, \ldots, a_n \in A$ mit $X^\ell = \sum_{k=0}^{n} a_k (X^m)^k = \sum_{k=0}^{n} a_k X^{mk}$. Es folgt

$$0 = \sum_{k=0}^{n} a_k X^{mk} - X^\ell =: p \in A[X].$$

Wir haben hier em Ende die rechte Seite p genannt und als Element von $A[X]$ aufgefasst. Aus der definierenden Eigenschaft von Polynomringen folgt, dass alle Koeffizienten von p gleich 0 sein müssen. Wegen $\ell \neq km$ für alle $k \in \mathbb{Z}$ ist der ℓ-te Koeffizient von p gerade -1 (beachte hier, wie die Addition in $A[X]$ definiert ist). Also folgt $-1 = 0$ und Multiplikation mit -1 ergibt, dass auch $1 = 0$ gilt. Dies ist aber ein Widerspruch zur Voraussetzung $0 \neq 1$. Damit kann $\ell \notin \langle m \rangle_{\mathbb{Z}}$ nicht gelten, es muss also $\ell \in \langle m \rangle_{\mathbb{Z}}$ gelten.

(b) Wir zeigen zunächst, dass $A[X^N]$ für jedes $N \in \mathbb{N}$ zu $A[X]$ isomorph ist. Die Behauptung ergibt sich dann mit der Transitivität der Isomorphie (die genaue Begründung folgt am Ende). Sei also $N \in \mathbb{N}$ gegeben. Um zu zeigen, dass $A[X^N]$ isomorph zu $A[X]$ ist, geben wir konkret einen Isomorphismus von $A[X]$ nach $A[X^N]$ an.

Zwischenbemerkung: Wir definieren diesen Isomorphismus unter Verwendung von Satz 3.2.14. Nach diesem ist ein Ringhomomorphismus $f : A[X] \to B$ schon eindeutig bestimmt, wenn gesagt ist, worauf jedes Elemente $a \in A$ und worauf X abgebildet werden. Sie sollten sich klar machen, warum das so ist, dann haben Sie viel darüber verstanden wie Ringhomomorphismen und auch Polynomringe funktionieren.

Sei dazu zunächst $\varphi : A \to A[X^N]$ definiert durch $\varphi(a) := a$. Diese Abbildung ist ein Ringhomomorphismus, denn es gilt (beachte wie die Addition und Multiplikation von Polynomen definiert sind):

$$\begin{aligned} \varphi(a+b) &= a+b = \varphi(a)+\varphi(b)\,, \\ \varphi(1_A) &= 1_A = 1_{A[X]}\,, \\ \varphi(ab) &= ab = \varphi(a)\varphi(b)\,. \end{aligned}$$

Wir setzen φ nun mittels Satz 3.2.14 zu einem Ringhomomorphismus $\psi : A[X] \to A[X^N]$ fort, indem wir $\psi(X) := X^N$ „fordern“. Genauer besagt Satz 3.2.14, dass ein (eindeutiger) Ringhomomorphismus $\psi : A[X] \to A[X^N]$ mit $\psi|_A = \varphi$ und $\psi(X) = X^N$ *(X^N entspricht dem x in Satz 3.2.14)* exisiert, der konkret gegeben ist durch

$$\psi\left(\sum_{k=0}^{n} a_k X^k\right) = \sum_{k=0}^{n} a_k (X^N)^k = \sum_{k=0}^{n} a_k X^{Nk}\,.$$

Wir zeigen, dass ψ bijektiv und somit ein Ringisomorphismus ist.

Injektivität:

Da ψ ein Ringhomomorphismus ist, ist Injektivität äquivalent zu $\ker(\psi) = \{0\}$. Zum Nachweis dieser Gleichheit beachten wir zunächst, dass $0 \in \ker(\psi)$ gilt einfach da ψ ein Ringhomomorphismus ist. Für die umgekehrte Mengennklusion sei $p \in \ker(\psi)$ gegeben, d.h. es gilt $p \in A[X]$ und $\psi(p) = 0$. Schreibe $p = \sum_{k=0}^{n} a_k X^k$ für gewisse $n \in \mathbb{N}_0$, $a_0, \ldots, a_n \in A$. Dann gilt

$$0 = \psi(p) = \sum_{k=0}^{n} a_k X^{Nk}\,.$$

Wir lesen diese Gleichung in $A[X] \supseteq A[X^N]$ und folgern aus der definierenden Eigenschaft des Polynomrings, dass $a_k = 0$ für alle $k \in \{0, \ldots, n\}$ gilt. Also gilt $p = 0$. Dies zeigt, dass auch $\ker(\psi) \subseteq \{0\}$ gilt. Damit ist gezeigt, dass ψ injektiv ist.

Surjektivität:

Sei hierzu $p \in A[X^N]$ gegeben. Wir müssen ein $q \in A[X]$ angeben, für das $\psi(q) = p$ gilt. Schreibe $p = \sum_{k=0}^{n} a_k X^{Nk}$ für gewisse $n \in \mathbb{N}_0$ und $a_0, \ldots, a_n \in A$. Definiere $q \in A[X]$ durch $q := \sum_{k=0}^{n} a_k X^k$. Dann gilt offensichtlich $\psi(q) = p$. Damit ist gezeigt, dass ψ surjektiv ist.

Also ist ψ bijektiv und somit ein Ringisomorphismus.

Da in ebigem Beweis $N \in \mathbb{N}$ beliebig war, sind insbesondere $A[X^\ell]$ und $A[X^m]$ beide isomorph zu $A[X]$. Seien $f : A[X] \to A[X^\ell]$ und $g : A[X] \to A[X^m]$ zwei Ringisomorphismen. Da die inverse Abbildung eines Ringisomorphismuses und die Verkettung zweier Ringisomorphismen wieder Ringisomorphismen sind, ist zunächst $f^{-1} : A[X^\ell] \to A[X]$ ein Ringisomorphismus und damit auch $g \circ f^{-1} : A[X^\ell] \to A[X^m]$. Also sind $A[X^\ell]$ und $A[X^m]$ isomorphe kommutative Ringe.

□

Alternative Lösungmöglichkeit für Teil (b)

Man kann auch zeigen, dass $A[X^N]$ für jedes $N \in \mathbb{N}$ selbst ein Polynomring ist, d.h. die Eigenschaften aus der Definition erfüllt. Dann folgt aus Satz 3.2.17 direkt, dass $A[X^\ell]$ und $A[X^m]$ für gegebene $\ell, m \in \mathbb{Z}$ isomorph sind.

Sei also $N \in \mathbb{N}$ gegeben. Wir zeigen nun, dass $A[X^N]$ die Eigenschaften der Definition eines Polynomrings erfüllt. Zunächst ist offensichtlich $A[X^N]$ von der prinzipiell notwendigen Gestalt (d.h. von der Gestalt „A adjungiert ein Element“). Es bleibt zu zeigen, dass gilt:

$$\forall n \in \mathbb{N}_0 : \forall a_0, \ldots, a_n \in A : \quad \left(\sum_{k=0}^{n} a_k (X^N)^k = 0 \implies a_0 = \ldots = a_k = 0 \right).$$

Seien dazu $n \in \mathbb{N}_0$ und $a_0, \ldots, a_n \in A$ gegeben. Wir nehmen an, dass $\sum_{k=0}^{n} a_k (X^N)^k = 0$ gilt. Nun fassen wir (wie schon zuvor) dieses Polynom wieder einfach als Element des größeren Rings $A[X]$, d.h. wir erinnern uns daran, dass $A[X^N] \subseteq A[X]$ gilt. Da $A[X]$ ein Polynomring ist, folgt $a_0 = \ldots = a_n = 0$. □