

Musterlösung zur Serie 9

Algebra und Zahlentheorie und ihre Didaktik

Dr. Daniel Skodlerack

28. Juni 2017

Aufgabe 1. (10 Punkte)(Matrizenringe und Endomorphismen) Es seien R ein kommutativer unitärer Ring und n eine natürliche Zahl. Zeigen Sie, dass der Matrizenring $M_n(R)$ isomorph zum Ring $\text{End}_R(R^n)$ der R -linearen Endomorphismen von R^n ist.

Lösung: Es sei $e_1, \dots, e_n$ die R -Standardbasis von R^n , d.h. $e_i = (0, \dots, 0, 1, 0, \dots, 0)^T$, wobei der Eintrag 1 in der i -ten Zeile steht. Aufgrund der Linearität ist ein R -linearer Endomorphismus von R^n eindeutig durch seine Werte in den Basisvektoren bestimmt. Also ist die durch

$$\Phi(f) := A := (a_{i,j})_{i,j}, \text{ wobei } f(e_j) = \sum_{i=1}^n a_{i,j} e_i,$$

definierte Abbildung $\Phi : \text{End}_R(R^n) \rightarrow M_n(R)$ wohldefiniert (Basiseigenschaft von $(e_i)_i$) und injektiv, und aus der Definition folgt sofort die Additivität. Es sei A ein Element von $M_n(R)$, dann ist die Abbildung

$$f_A : R^n \rightarrow R^n, f(x) := Ax,$$

R -linear (Hier verwenden wir die Kommutativität von $\cdot_R$) und es gilt $\Phi(f_A) = A$, und somit ist Φ surjektiv. Wir müssen nur noch die Multiplikativität zeigen: Dazu betrachten wir die zu Φ inverse Abbildung Ψ , $\Psi(A) := f_A$.

$$\Psi(AB)(x) = (AB)x = A(Bx) = A(\Psi(B)(x)) = \Psi(A)(\Psi(B)(x)) = (\Psi(A) \circ \Psi(B))(x).$$

Dann ist aber auch Φ multiplikativ, da

$$\Phi(f \circ g) = \Phi(\Psi(\Phi(f)) \circ \Psi(\Phi(g))) = \Phi(\Psi(\Phi(f) \circ \Phi(g))) = \Phi(f) \circ \Phi(g).$$

Anmerkung: Wenn R nicht kommutativ ist, dann gilt die Aussage in abgeänderter Form: Man muss spezifizieren, welche skalare Multiplikation man auf R^n betrachten will: Von links, $r \cdot_{\text{links}} x := (rx_1, \dots, rx_n)$, oder von rechts, $x \cdot_{\text{rechts}} r := (x_1 r, \dots, x_n r)$. Betrachtet man die skalare Multiplikation von rechts, dann ist obiges Φ ein Ringisomorphismus von $\text{End}_{R, \text{rechts}}(R^n)$ nach $M_n(R^n)$. Betrachtet man die skalare Multiplikation von links, so ist Φ ein Ringisomorphismus von $\text{End}_{R, \text{links}}(R^n)$ nach $M_n(R^{op})$, wobei R^{op} der zu R oppositionelle Ring ist, d.h. $r_1 \cdot_{op} r_2 := r_2 r_1$.

Ab jetzt lassen wir in den Übungsserien bei Ringen das Attribut „kommutativ“ weg, da alle von jetzt an betrachteten Ringe kommutativ sind.

Aufgabe 2. (5+5+5* Punkte)(Ideale von $\mathfrak{P}(M)$) Es seien M eine Menge und N eine Teilmenge von M .

1. Aus der Vorlesung wissen Sie, dass $\mathfrak{P}(N)$ ein Ideal von $(\mathfrak{P}(M), \Delta, \cap)$ ist. Zeigen Sie, dass der Faktorring $\mathfrak{P}(M)/\mathfrak{P}(N)$ isomorph zum Ring $(\mathfrak{P}(M \setminus N), \Delta, \cap)$ ist.
2. Es sei M endlich. Zeigen Sie, dass alle Ideale von $\mathfrak{P}(M)$ von der Form $\mathfrak{P}(S)$, $S \subseteq M$, sind.
3. Es sei M unendlich. Zeigen Sie, dass in $\mathfrak{P}(M)$ ein Ideal existiert, welches nicht die Potenzmenge einer Teilmenge von M ist.

Lösung:

- Wir betrachten die Abbildung $\Phi : \mathfrak{P}(M) \rightarrow \mathfrak{P}(M \setminus N)$, $\Phi(A) := A \cap (M \setminus N)$. Wir setzen $T := M \setminus N$.
 - Φ ist multiplikativ: $\Phi(A \cap B) = (A \cap B) \cap T = (A \cap B) \cap (T \cap T) = (A \cap T) \cap (B \cap T)$
 - Φ ist additiv: $\Phi(A \Delta B) = (A \Delta B) \cap T = (A \cap T) \Delta (B \cap T) = \Phi(A) \Delta \Phi(B)$, wobei hier das zweite Distributivgesetz Verwendung fand.
 - Der Kern von Φ ist die Menge der Teilmengen von M , deren Schnitt mit T leer ist, also genau die Menge der Teilmengen von N .
 - Φ ist surjektiv, da die Einschränkung von Φ auf $\mathfrak{P}(T)$ mit der Identität übereinstimmt.

Aus dem 1. Isomorphiesatz folgt nun die Behauptung.

- Aus der Vorlesung wissen wir, dass für jede Teilmenge S von M die Potenzmenge von S ein Ideal von $\mathfrak{P}(M)$ ist. Es sei nun umgekehrt J ein Ideal von $\mathfrak{P}(M)$, und wir setzen voraus, dass M endlich ist. Es sei S die Vereinigung aller Elemente von J (Die Elemente von J sind Teilmengen von M . Deshalb macht die Vereinigung Sinn.). Dann ist J eine Teilmenge von $\mathfrak{P}(S)$. Behauptung: Es ist $\mathfrak{P}(S)$ eine Teilmenge von J .

Beweis: Es sei x ein Element von S . Dann folgt aus der Definition von S , dass ein Element A von J existiert, das x enthält, und aus der Idealeigenschaft von J folgt:

$$\{x\} = \{x\} \cap A \in J.$$

Zu zwei disjunkten Elementen A, B von J ist auch die Vereinigung $A \cup B (= A \Delta B)$ ein Element von J . Also sind alle endlichen Teilmengen von S Elemente von J . S ist endlich, da M endlich ist, und deshalb ist die Potenzmenge von S eine Teilmenge von J . q.e.d.

- Die Menge J der endlichen Teilmengen von M ist ein Ideal von $\mathfrak{P}(M)$, da alle Elemente von M bezüglich Δ zu sich selbst invers sind und die leere Menge, die symmetrische Differenz zweier endlicher Mengen und der Schnitt einer Teilmenge von M mit einer endlichen Menge wieder endlich sind. Angenommen J ist von der Form $\mathfrak{P}(S)$, $S \subseteq M$. J enthält unendlich viele Elemente, da M unendlich viele einelementige Teilmengen besitzt. Aus der Unendlichkeit von $\mathfrak{P}(S)$ folgt die Unendlichkeit von S . Als Element von J muss S aber endlich sein. Ein Widerspruch.

Aufgabe 3. (5+5+5* Punkte)(Primideale)

- Zeigen Sie, dass das Ideal $I := (X+2)_{\mathbb{Z}[X]}$ ein Primideal von $\mathbb{Z}[X]$ ist, und beweisen bzw. widerlegen Sie die Aussage, dass I ein Maximalideal von $\mathbb{Z}[X]$ ist.
- Ist $(X+2)_{\mathbb{Q}[X]}$ ein Maximalideal von $\mathbb{Q}[X]$? Beweisen Sie Ihre Antwort.
- Zeigen Sie, dass jeder unitäre Ring, der $0_R \neq 1_R$ erfüllt, ein Maximalideal enthält.

Lösung:

- Aus dem ersten Isomorphiesatz, angewandt auf den Ringhomomorphismus: $\Phi : \mathbb{Z}[X] \rightarrow \mathbb{Z}$, $\Phi(P) := P(-2)$, folgt direkt dass $\mathbb{Z}[X]/\ker(\Phi)$ ringisomorph zu $\text{im}(\Phi)$ ist. Die Surjektivität von Φ folgt sofort, da Φ die konstanten Polynome auf sich selbst abbildet, und wir müssen nur noch den Kern von Φ berechnen. Es sei P ein Element von $\mathbb{Z}[X]$. Mittels Polynomdivision erhalten wir Polynome $S \in \mathbb{Z}[X]$ und $R \in \mathbb{Z}$, so dass $P = (X+2)S + R$ gilt. Daraus folgt, dass P genau dann im Kern von Φ liegt, wenn R gleich Null ist, also ist der Kern von Φ eine Teilmenge von I . Die andere Inklusion $I \subseteq \ker(\Phi)$ folgt daraus, dass -2 eine Nullstelle von $X+2$ ist. Also ist der Faktorring von $\mathbb{Z}[X]$ modulo I isomorph zu $\mathbb{Z}$ und somit nullteilerfrei, nicht der Nullring und kein Körper. Nach Satz 78 ist I ein Primideal, aber kein Maximalideal.
- Komplett analog zum ersten Teil der Aufgabe zeigt man, dass $\mathbb{Q}[X]/(x+2)_{\mathbb{Q}[X]}$ ringisomorph zu $\mathbb{Q}$ ist. Also ist $(x+2)_{\mathbb{Q}[X]}$ nach Satz 78 ein Maximalideal von $\mathbb{Q}[X]$.
- Es sei M die Menge aller echten Ideale von R . Diese Menge ist nicht leer, da sie das Nullideal enthält, da $1 \neq 0$ gilt. Wir zeigen, dass M bezüglich der Inklusionsrelation induktiv geordnet ist. Es sei $N \subseteq M$ eine Kette von M . Dann ist $I := \bigcup_{J \in N} J$ wieder ein echtes Ideal von R wie folgende Punkte zeigen:

- $1_R \notin I$, da $1_R \notin J$ für jedes Element J von N .
- I ist nicht leer, da N nicht leer ist und $J \in N$ das Nullelement von R enthält.
- Für Elemente x und x' von I gibt es nach der Definition von I Elemente J und J' von N , so dass x ein Element von J und x' ein Element von J' ist. Nun ist aber N eine Kette, woraus $J \subseteq J'$ oder $J' \subseteq J$ folgt. Ohne Einschränkung liegen also x, x' in J . Da J ein Ideal ist, liegen $x - x'$ und für jedes $r \in R$ auch rx in J , also auch in I .

Wir haben somit mit I ein Element von M gefunden, das eine obere Schranke von N ist. Damit ist gezeigt, dass $(M, \subseteq)$ induktiv geordnet ist. Nach dem Zornschen Lemma, angewandt auf $(M, \subseteq)$, besitzt R ein Maximalideal.

Aufgabe 4. ((5+5)+5* Punkte)(Chinesischer Restsatz)

1. Es sei R ein Ring, und es seien zwei Ideale I und J von R gegeben.

(a) Zeigen Sie, dass die *Idealsumme*

$$I + J := \{x + y \mid x \in I \wedge y \in J\}$$

und das *Idealprodukt*

$$I \cdot_{Id} J := \{x_1 y_1 + x_2 y_2 + \dots + x_l y_l \mid l \in \mathbb{N} \wedge (\forall_{i \in \mathbb{N} \leq l} : x_i \in I \wedge y_i \in J)\}$$

Ideale von R sind.

- (b) Es sei R nun zusätzlich unitär, und wir setzen $I + J = R$ voraus. Zeigen Sie, dass $I \cdot_{Id} J$ und $I \cap J$ übereinstimmen.

2. Zeigen Sie, dass der Ring $\mathbb{Z}[X]/(X^2 + 5X + 6)_{\mathbb{Z}[X]}$ ringisomorph zu $\mathbb{Z} \times \mathbb{Z}$ ist.

Lösung:

1. (a) Wir stellen zunächst fest, dass $I + J$ nicht leer ist, da es das Nullelement enthält. Des Weiteren gilt für $r \in R$, $x_1, x_2 \in I$ und $y_1, y_2 \in J$: $x_1 - x_2, rx_1 \in I$ und $y_1 - y_2, ry_1 \in J$, da I und J Ideale sind. Deshalb erhalten wir $x_1 + y_1 - (x_2 + y_2) \in I + J$ und $r(x_1 + y_1) \in I + J$. Also ist die Idealsumme von I und J ein Ideal von R . Wir zeigen nun, dass $I \cdot_{Id} J$ ein Ideal ist. Es enthält das Nullelement ($0 = 0 \cdot 0$) und für zwei Elemente $\sum_{i=1}^l x_i y_i$ und $\sum_{i=1}^{l'} x'_i y'_i$ von $I \cdot_{Id} J$ und $r \in R$ gelten die Gleichungen

$$\sum_{i=1}^l x_i y_i - \sum_{i=1}^{l'} x'_i y'_i = \sum_{i=1}^l x_i y_i + \sum_{i=1}^{l'} (-x'_i) y'_i$$

und $r \sum_{i=1}^l x_i y_i = \sum_{i=1}^l (rx_i) y_i$. Aus der Abgeschlossenheit von I bezüglich skalarer Multiplikation und der Definition von $I \cdot_{Id} J$ folgt, dass $I \cdot_{Id} J$ ein Ideal von R ist.

- (b) Aus der Abgeschlossenheit bezüglich skalarer Multiplikation folgt, dass für Elemente $x \in I$ und $y \in J$ das Produkt xy sowohl ein Element von I als auch eines von J ist. Des Weiteren ist $I \cap J$ ein Ideal von R und insbesondere abgeschlossen bezüglich der Addition, und deshalb ist das Idealprodukt von I und J eine Teilmenge vom Schnitt von I mit J . Wir zeigen nun die andere Inklusion. Als Vorbereitung stellen wir fest, dass aus $I + J = R$ folgt, dass die Eins eine Zerlegung der Form $1 = x + y$ mit $x \in I$ und $y \in J$ besitzt. Es sei nun z ein Element von $I \cap J$. Dann folgt aus der Gleichung $z = xz + zy$, dass z ein Element des Idealprodukts von I und J ist.
2. Wir haben die Faktorisierung $X^2 + 5X + 6 = (X + 2)(X + 3)$ und aus Rechnungen wie in Aufgabe 3 folgt mittels des 1. Isomorphiesatzes, dass die Faktorringe von $\mathbb{Z}[X]$ modulo $(X + 2)_{\mathbb{Z}[X]}$ und $(X + 3)_{\mathbb{Z}[X]}$ isomorph zu $\mathbb{Z}$ sind. Aus dem chinesischen Restsatz folgt, dass $\mathbb{Z}[X]/((X + 2)_{\mathbb{Z}[X]} \cap (X + 3)_{\mathbb{Z}[X]})$ ringisomorph zu $\mathbb{Z} \times \mathbb{Z}$ ist. Wir müssen also nur noch

$$(X + 2)_{\mathbb{Z}[X]} \cap (X + 3)_{\mathbb{Z}[X]} = (X^2 + 5X + 6)_{\mathbb{Z}[X]}$$

zeigen. Das ist eine Konsequenz aus Aufgabe 4.1(b), da sich die Eins wie folgt darstellen lässt: $1 = X + 3 - (X + 2)$.