Anmerkungen und Lösungen zu

Einführung in die Algebra

Blatt 4

Jendrik Stelzner

Letzte Änderung: 20. November 2017

Aufgabe 3

(b)

Wir haben im Tutorium gesehen, dass für $A \in \mathrm{M}_n(K)$ die Implikationen

$$A \text{ ist nicht injektiv} \implies A \text{ ist ein Linksnullteiler}$$

und

$$A \text{ ist nicht surjektiv} \implies A \text{ ist ein Rechtsnullteiler}$$

gelten. Dabei handelt es sich tatsächlich schon um Äquivalenzen. Aus der linearen Algebra wissen wir dabei, dass wegen der Endlichdimensionalität von K^n die Injektivität und Surjektivität von A äquivalent sind. Deshalb kann der Matrizenring $\mathrm{M}_n(K)$ keine Beispiele liefern.

Im Tutorium haben wir dieses Problem dadurch gelöst, dass wir den endlichdimensionalen K-Vektorraums K^n durch einen unendlichdimensionalen K-Vektorraum V ersetzt haben, also anstelle von $\mathrm{M}_n(K) \cong \mathrm{End}(K^n)$ den Endomorphismenring $\mathrm{End}(V)$ betrachtet haben.

Ein anderer Ansatz besteht darin, die Einträge der Matrizen nicht aus einem Körper K zu wählen:

- Ein erster Ansatz besteht darin, anstelle eines Körpers K einen passenden kommutativen Ring R zu betrachten, und dann im Matrizenring $\mathrm{M}_n(R)$ nach Beispielen zu suchen. Aufgrund der folgenden Resultate aus der kommutativen Algebra wird dies allerdings nicht zum Erfolg führen:
  Lemma 1. *Ist R ein kommutativer Ring, so gilt für $A \in \mathrm{M}_n(R)$ genau dann $\ker A \neq 0$, wenn $\det A \in R$ ein Nullteiler ist.*
  Korollar 2. *Ist R ein kommutativer Ring, so sind für $A \in \mathrm{M}_n(R)$ die folgenden Bedingungen äquivalent:*

i) Die Matrix A ist ein Linksnullteiler in $\mathrm{M}_n(R)$.

ii) Der Skalar $\det A$ *ist ein Nullteiler in* R.

iii) Die Matrix A ist ein Rechtsnullteiler in $\mathrm{M}_n(R)$.

- Der obige Ansatz lässt sich dadurch reparieren, dass man die Matrixeinträge aus verschiedenen kommutativen Ringen wählt. So kann man etwa

$$R = \begin{pmatrix} \mathbb{Z} & \mathbb{Z}/2 \\ 0 & \mathbb{Z} \end{pmatrix} = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \,\middle|\, a, c \in \mathbb{Z}, b \in \mathbb{Z}/2 \right\}$$

mit der Addition

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} + \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix} = \begin{pmatrix} a + a' & b + b' \\ 0 & c + c' \end{pmatrix}$$

und der Multiplikation

$$\begin{pmatrix} a & \overline{b} \\ 0 & c \end{pmatrix} \cdot \begin{pmatrix} a' & \overline{b'} \\ 0 & c' \end{pmatrix} = \begin{pmatrix} aa' & \overline{ab' + bc'} \\ 0 & cc' \end{pmatrix}$$

betrachten. Dass R mit den oberen Operationen tatsächlich einen Ring bildet, erkennt man durch direktes Nachrechnen. In diesem Ring lässt sich dann die Matrix

$$A := \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \in R$$

betrachten. Es gilt

$$\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & \overline{1} \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & \overline{2} \\ 0 & 0 \end{pmatrix} = 0,$$

weshalb A ein Linknullteiler ist. Andererseits gilt

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2a & b \\ & c \end{pmatrix};$$

wobei genau dann $2a = 0$, wenn $a = 0$. Deshalb ist A kein Rechtsnullteiler.

Im Tutorium kam die Frage auf, ob es auch Beispiele in endlichen Ringen gibt. Wie sich (entgegen meiner spontanen Vermutung) herausstellt[1], ist dies nicht möglich:

Lemma 3. *Ist R ein endlicher (nicht notwendigerweise kommutativer) Ring und $r \in R$ kein Links-, bzw. Rechtsnullteiler, so ist r eine Einheit.*

Beweis. Wir betrachten den Fall, dass r kein Linksnullteiler ist; der Fall, dass r kein Rechtsnullteiler ist, verläuft analog. Nach Annahme ist dann die Abbildung

$$\pi_r \colon R \to R, \quad a \mapsto ra$$

[1] Siehe https://math.stackexchange.com/a/45220/300783.

injektiv, und wegen der Endlichkeit von R somit bereits bijektiv. Die Bjiektion π_r ist also ein Element der symmetrischen Gruppe

$$S(R) = \{\pi \colon R \to R \mid \pi \text{ ist eine Bijektion}\}.$$

Die Gruppe $S(R)$ ist endlich, da R endlich ist. Also hat π_r endliche Ordnung, d.h. es gibt $n \geq 1$ mit $\pi_r^n = \mathrm{id}_R$. Dabei ist die Abbildung π_r^n durch Multiplikation mit r^n gegeben. Also ist r^n linksneutral bezüglich der Multiplikation, und somit bereits $r^n = 1$. Folglich ist r eine Einheit mit $r^{-1} = r^{n-1}$. □

Korollar 4. *Ist R ein endlicher (nicht notwendigerweise kommutativer) Ring, so ist jedes Element $r \in R$ entweder eine Einheit oder ein beidseitiger Nullteiler.*

Beweis. Ist r keine Einheit, so ist r nach Lemma 3 ein beidseitiger Nullteiler. Außerdem sind Einheiten niemals Nullteiler. □

Aufgabe 4

(a)

Lemma 5. *Es sei R_i, $i \in I$ eine Familie von Ringen. Dann trägt $\prod_{i \in I} R_i$ eine Ringstruktur durch*

$$(r_i)_{i \in I} + (r'_i)_{i \in I} = (r_i + r'_i)_{i \in I} \quad \textit{und} \quad (r_i)_{i \in I} \cdot (r'_i)_{i \in I} = (r_i r'_i)_{i \in I}.$$

Beweis. Die Ringaxiome ergeben sich durch direktes Nachrechnen wie in Aufgabe 2 (c). Das Nullelement ist durch $0 = (0_{R_i})_{i \in I}$ gegeben, und das Einselement durch $1 = (1_{R_i})_{i \in I}$. □

Der hier beschrieben Ring ist $A = \prod_{i \geq 1} \mathbb{Z}/p_i$.

(b)

Es gilt $0 = (0, 0, 0, \dots) \in B$. Für $x, y \in B$ mit $x = (x_1, x_2, \dots)$ und $y = (y_1, y_2, \dots)$ gibt es $n, m \geq 1$ mit $x_i = 0$ für alle $i \geq n$ und $y_i = 0$ für alle $i \geq m$. Dann ist $x - y = (x_1 - y_1, x_2 - y_2, \dots)$ mit $x_i - y_i = 0$ für alle $i \geq \max(n, m)$, und somit $x - y \in B$.

(c)

Für jedes $x \in \mathbb{Z}/n$ gilt $n \cdot x = 0$. Für $x \in B$ mit $x = (x_1, \dots, x_n, 0, 0, \dots)$ gilt deshalb

$$\begin{aligned} \prod_{i=1}^{n} p_i \cdot x &= \prod_{i=1}^{n} p_i \cdot (x_1, \dots, x_n, 0, \dots) = \left(\prod_{i=1}^{n} p_i \cdot x_1, \dots, \prod_{i=1}^{n} p_i \cdot x_n, 0, \dots \right) \\ &= \left(\prod_{i=2}^{n} p_i \cdot p_1 \cdot x_1, \dots, \prod_{i=1}^{n-1} p_i \cdot p_n \cdot x_n, 0, \dots \right) = (0, \dots, 0, 0, \dots). \end{aligned}$$

Somit hat x endliche Ordnung.

(d)

Gilt $\operatorname{ord}(1_R) = \infty$, so git auch $\exp(G) = \infty$. Es sei also $n \coloneqq \operatorname{ord}(1_R) < \infty$. Für jedes $r \in R$ gilt dann

$$n \cdot r = \underbrace{r + \cdots + r}_{n} = \underbrace{1_R \cdot r + \cdots + 1_R \cdot r}_{n} = \underbrace{(1_R + \cdots + 1_R)}_{n} \cdot r = (n \cdot 1_R) \cdot r = 0 \cdot r = 0,$$

und deshalb $\operatorname{ord}(r) \mid \operatorname{ord}(1_R)$. Somit gilt dann

$$\operatorname{kgV}\{\operatorname{ord}(r) \,|\, r \in R\} = \operatorname{ord}(1_R).$$

(e)

Für jedes $j \geq 1$ gilt für das Element $x^{(j)} \in B$ mit

$$x_i^{(j)} = \delta_{ij} \qquad \text{für alle } i \geq 1,$$

dass $\operatorname{ord}(x^{(j)}) = p_j$. Somit ist $\{\operatorname{ord}(x) \,|\, x \in B\} \supseteq \{\operatorname{ord}(x^{(j)}) \,|\, j \geq 1\} = \{p_j \,|\, j \geq 0\}$ und somit $\exp(B) = \infty$.

(f)

Gebe es eine Ringstruktur auf B, so wäre $\infty = \exp(B) = \operatorname{ord}(()1_B) < \infty$.

(g)

Das Einselement von A ist durch $1_A = (1, 1, 1, \dots) \notin B$ gegeben. Deshalb ist B kein Unterring von A.