Karlsruher Institut für Technologie

Karlsruher Institut für Technologie
Institut für Algebra und Geometrie

PD Dr. Stefan Kühnlein   Dipl.-Math. Jochen Schröder

Einführung in Algebra und Zahlentheorie – Übungsblatt 9 – Musterlösung

Aufgabe 1 (4 Punkte)
Die Begriffe „linear (un-)abhängig" und „Erzeugendensystem" sind in der Modulwelt definiert wie bei Vektorräumen. Eine Basis ist ein linear unabhängiges Erzeugendensystem.

a) Finde einen kommutativen Ring R und einen R-Modul $M \neq \{0\}$, so dass jede nichtleere Teilmenge linear abhängig ist. Begründe, warum M keine Basis besitzt.

b) Gegeben sei $\mathbb{Q}$ als $\mathbb{Z}$-Modul. Zeige, dass $\mathbb{Q}$ keine Basis besitzt.

Lösung

a) Betrachte $R = \mathbb{Z}$ und $M = \mathbb{Z}/42\mathbb{Z}$. M ist – nach der Vorlesung – ein $\mathbb{Z}$-Modul vermöge $z \cdot \overline{a} := \overline{za}$ für alle $z, a \in \mathbb{Z}$.
Ist $L \subseteq M$ eine nichtleere Menge, so gibt es $y \in L$ und wegen $42 \cdot y = \overline{0}$ finden wir eine nichttriviale Linearkombination von $\overline{0}$, also ist L linear abhängig.
Eine mögliche Basis B von M muss also leer sein, denn B ist linear unabhängig. Aber natürlich gilt $\langle \emptyset \rangle = \{\overline{0}\} \neq M$.

b) Seien $\frac{a}{b} \neq 0, \frac{c}{d} \neq 0 \in \mathbb{Q}$. Dann ist $(bc) \cdot \frac{a}{b} - (ad) \cdot \frac{c}{d} = 0$ eine nichttriviale Linearkombination der Null. Wir folgern, dass jede Menge $L \subseteq \mathbb{Q}$ mit $\#L \geq 2$ linear abhängig ist.
Gäbe es in $\mathbb{Q}$ eine Basis, so hätte diese höchstens ein Element.
Annahme: $\mathbb{Q} = \langle \frac{a}{b} \rangle$ mit $a \in \mathbb{Z}, b \in \mathbb{N}$. Sicher ist $a \neq 0$ und ohne Einschränkung ist $a \in \mathbb{N}$ – denn $\langle \frac{a}{b} \rangle = \langle \frac{-a}{b} \rangle$.
Aber wegen $0 \cdot \frac{a}{b} < \frac{1}{b+1} < 1 \cdot \frac{a}{b}$ ist $\frac{1}{b+1} \notin \langle \frac{a}{b} \rangle = \{z \cdot \frac{a}{b} : z \in \mathbb{Z}\}$ (WIDERSPRUCH).

Aufgabe 2 (4 Punkte)
Gegeben sei der Monoidring $\mathbb{Z}[M]$ mit $M = (\mathbb{Z}/2\mathbb{Z}, \cdot)$.

a) Einen halben Punkt erhältst du, wenn du ein allgemeines Element aus $\mathbb{Z}[M]$, das Ergebnis des Produktes zweier solcher Elemente sowie das Null- und das Einselement explizit angibst.

b) Bestimme nun die Einheitengruppe $\mathbb{Z}[M]^\times$.

c) Bestimme alle Nullteiler. Bestimme weiterhin für jeden Nullteiler $x \in \mathbb{Z}[M]$ die Menge

$$N_x = \{y \in \mathbb{Z}[M] : xy = 0\}.$$

Lösung

a) Ein allgemeines Element hat die Form $a \cdot \overline{0} + b \cdot \overline{1}$ mit $a, b \in \mathbb{Z}$. Länger kann man auch $\delta_{\overline{0}}$ anstatt $\overline{0}$ und $\delta_{\overline{1}}$ anstatt $\overline{1}$ schreiben.
Für allgemeine Elemente $a \cdot \overline{0} + b \cdot \overline{1}$, $c \cdot \overline{0} + d \cdot \overline{1}$ (mit $a, b, c, d \in \mathbb{Z}$) gilt

$$(a \cdot \overline{0} + b \cdot \overline{1}) \cdot (c \cdot \overline{0} + d \cdot \overline{1}) = (ac + ad + bc) \cdot \overline{0} + bd \cdot \overline{1}.$$

Das additive Neutralelement ist $N = 0 \cdot \overline{0} + 0 \cdot \overline{1}$, das multiplikative Neutralelement $E = 0 \cdot \overline{0} + 1 \cdot \overline{1}$.

b) Ein Element $a \cdot \overline{0} + b \cdot \overline{1}$ ist dann invertierbar, wenn es $c \cdot \overline{0} + d \cdot \overline{1}$ gibt, so dass

$$(a \cdot \overline{0} + b \cdot \overline{1})(c \cdot \overline{0} + d \cdot \overline{1}) \stackrel{!}{=} 0 \cdot \overline{0} + 1 \cdot \overline{1}.$$

Mit der Multiplikationsformel aus Aufgabenteil a) gibt dies folgende Bedingung:
Es gibt $c, d \in \mathbb{Z}$, so dass $ac + ad + bc = 0$ und $bd = 1$. Letztere ist äquivalent zu $b = d \in \{\pm 1\}$.
Fall 1: $b = d = 1$. Dann ist die zweite Bedingung erfüllt, die erste wird zu $ac + a + c = 0$, was wir umformen zu $0 = ac+a+c = (c+1)a+c = (c+1)a+c+1-1 = (c+1)(a+1)-1 \Rightarrow (a+1)(c+1) = 1$. Ein solches c existiert offensichtlich genau dann, wenn $a+1 \in \{\pm 1\}$ liegt, was zwei Einheiten gibt: $(-2) \cdot \overline{0} + 1 \cdot \overline{1}$ und $0 \cdot \overline{0} + 1 \cdot \overline{1} = E$.
Fall 2: $b = d = -1$. Multiplikation mit $-1 = -E$ bringt uns in den Fall 1 und wir erhalten die Einheiten $2 \cdot \overline{0} - 1 \cdot \overline{1}$ und $0 \cdot \overline{0} - 1 \cdot \overline{1} = -E$.
Insgesamt erhalten wir die Einheitengruppe

$$\mathbb{Z}[M]^\times = \{E, -E, (-2) \cdot \overline{0} + 1 \cdot \overline{1}, 2 \cdot \overline{0} - 1 \cdot \overline{1}\}.$$

c) $a \cdot \overline{0} + b \cdot \overline{1}$ ist ein Nullteiler, wenn es c, d gibt, die nicht beide 0 sind, so dass

$$(a \cdot \overline{0} + b \cdot \overline{1})(c \cdot \overline{0} + d \cdot \overline{1}) \stackrel{!}{=} 0 \cdot \overline{0} + 0 \cdot \overline{1}.$$

Dies gibt die Bedingungen $bd = 0$ und $ac + ad + bc = 0$.
Fall 1: Sei zunächst $b \neq 0$. Dann muss $d = 0$ sein, genau dann ist die erste Bedingung erfüllt. Damit wird die zweite Bedingung zu $0 = ac + bc = (a + b)c$. Da es $(c, d) \neq (0, 0)$ geben soll, muss hier $a = -b$ ($\neq 0$) sein. Für diese Belegung existieren passende c, d, nämlich $d = 0$ (siehe oben), c beliebig.
Für $b \neq 0$ finden wir Nullteiler der Form $(-b) \cdot \overline{0} + b \cdot \overline{1}$ mit $N_{(-b)\cdot\overline{0}+b\cdot\overline{1}} = \{c \cdot \overline{0} + 0 \cdot \overline{1} : c \in \mathbb{Z}\}$.
Fall 2: $b = 0$, die erste Bedingung ist dann automatisch erfüllt.
Die zweite Bedingung wird zu $0 = ac + ad = a(c + d)$ und stets finden wir passende c, d, etwa $c = 1, d = -1$. Also sind alle Elemente der Form $a \cdot \overline{0} + 0 \cdot \overline{1}$ Nullteiler.
Ist dabei $a \neq 0$, so ist $a(c + d) = 0$ genau dann erfüllt, wenn $c = -d$, also ist dann $N_{a\cdot\overline{0}+0\cdot\overline{1}} = \{c \cdot \overline{0} - c \cdot \overline{1} : c \in \mathbb{Z}\}$.
Für $a = 0$ ist natürlich $a \cdot \overline{0} + b \cdot \overline{1} = N$ und $N_N = \mathbb{Z}[M]$.

Aufgabe 3 (3 Punkte)
Seien R ein kommutativer Ring und A eine R-Algebra. Weiterhin sei $s \in A^\times$. Zeige, dass die Konjugation mit s, also die Abbildung $x \mapsto sxs^{-1}$, ein R-Algebren-Automorphismus von A ist.

Lösung Mit K_s sei die Konjugation mit s bezeichnet. Sicher ist K_s eine Abbildung von A nach A. Desweiteren ist $K_{s^{-1}}$ invers zu K_s, also K_s bijektiv.

Nun zeigen wir, dass K_s ein Ringhomomorphismus ist:
Es ist $K_s(1_A) = s1_As^{-1} = ss^{-1} = 1_A$. Außerdem gilt für alle $x, y \in A$:
$K_s(xy) = sxys^{-1} = sxs^{-1}sys^{-1} = K_s(x)K_s(y)$ und
$K_s(x + y) = s(x + y)s^{-1} = (sx + sy)s^{-1} = sxs^{-1} + sys^{-1} = K_s(x) + K_s(y)$.

Es bleibt zu zeigen, dass K_s R-linear ist, das ist äquivalent dazu, dass $K_s \circ \sigma \overset{(!)}{=} \sigma$ für den Strukturhomomorphismus $\sigma\colon R \to A$ ist.
Lösungsweg 1: Für $r \in R$ ist $\sigma(r)$ im Zentrum $Z(A)$ enthalten.
Also ist $K_s(\sigma(r)) = s\sigma(r)s^{-1} \overset{\sigma(r)\in Z(A)}{=} \sigma(r)ss^{-1} = \sigma(r)$.
Lösungsweg 2: Sei $r \in R, x \in A$. Zur Erinnerung: Der Strukturhomomorphismus σ gibt die skalare Multiplikation durch $r \cdot x = \sigma(r) \cdot x$, analog natürlich auch $r \cdot K_s(x) = \sigma(r) \cdot K_s(x)$.
Dann ist $K_s(rx) = K_s(\sigma(r) \cdot x) = s\sigma(r)xs^{-1} \overset{\sigma(r)\in Z(A)}{=} \sigma(r)sxs^{-1} = \sigma(r) \cdot K_s(x) = r \cdot K_s(x)$.

Nachsatz: Besonders einsichtig ist es, wenn $R \subseteq A$ und der Strukturhomomorphismus σ die Einbettung ist. Die skalare Multiplikation ist dann einfach die Multiplikation in A, eingeschränkt auf $R \times A$. Dann ist ein Ringhomomorphismus $\varphi\colon A \to A$ (oder $A \to B$, wenn B....) R-linear, wenn $\varphi(ra) = r\varphi(a)$ für alle $r \in R, a \in A$, so wie wir das kennen!
müssen wir Skalare nach vorne ziehen können. Wegen der Ringhomomorphie gilt aber stets $\varphi(ra) = \varphi(r)\varphi(a)$ für alle $r \in R, a \in A$ und die R-Linearität wird zur Bedingung $\varphi(r) = r$ für alle $r \in R$ (setze $a = 1$ für eine Richtung). Aber das ist doch genau $\varphi \circ \sigma = \sigma$.
Vielleicht hilft dieser Spezialfall, den Zusammenhang zwischen R-Linearität und dem Strukturhomomorphismus etwas genauer zu verstehen.

Aufgabe 4 (5 Punkte)
Seien K ein Körper und $A = K^{2\times 2}$ die K-Algebra der 2×2-Matrizen über K. In A seien die Matrizen $e_1 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, e_2 = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ gegeben. Zeige die folgenden Aussagen:

a) A besitzt nur zwei Ideale. Folgere, dass jeder Endomorphismus[1] von A ein Isomorphismus ist.

b) Ist $\varphi \in \mathrm{Aut}_{K-\mathrm{Alg}}(A)$ ein Automorphismus von A, dann gibt es eine Matrix $S \in \mathrm{GL}_2(K)$, so dass $\varphi(e_i) = S e_i S^{-1}$ für $i = 1, 2$ gilt.
(Eine mögliche Art, das zu zeigen, ist folgende: Warum ist $\varphi(e_i)$ konjugiert zu e_i und wieso ist sogar – ohne Einschränkung – $\varphi(e_1) = e_1$? Variiere die zweite Gleichung $\varphi(e_2) = T \cdot e_2 \cdot T^{-1}$ (mit $T \in \mathrm{GL}_2(K)$) geeignet durch Konjugation, ohne die Bedingung $\varphi(e_1) = e_1$ zu zerstören.)

c) In der Situation von b) gilt sogar $\varphi(M) = SMS^{-1}$ für alle $M \in A$.

d) Die Gruppen $\mathrm{Aut}_{K-Alg}(A)$ und $\mathrm{GL}_2(K)/\{aI_2 \mid a \in K^\times\}$ sind isomorph.

Lösung

a) $\{0\}$ und A sind die einzigen Ideale, denn:
Sei $J \neq \{0\}$. Dann gibt es eine Matrix $B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \in J$, $B \neq 0$. Ohne Einschränkung sei $b_{11} \neq 0$

[1]als Endomorphismus von K-Algebren

(sonst analog).
Wegen $A \cdot J \cdot A = J$, ist dann auch $\begin{pmatrix} \frac{1}{b_{11}} & 0 \\ 0 & 0 \end{pmatrix} \cdot B \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} =: E_{11} \in J$.
Weiterhin sind $E_{12} := \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = E_{11} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $E_{21} := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot E_{11}$ und $E_{22} := \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot E_1 1 \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in J$.
Schlussendlich ist $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \cdot E_{11} + \begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix} \cdot E_{12} + \begin{pmatrix} c & 0 \\ 0 & c \end{pmatrix} \cdot E_{21} + \begin{pmatrix} d & 0 \\ 0 & d \end{pmatrix} \cdot E_{22} \in J$ für alle $a, b, c, d \in K$ und damit gilt $J = A$.

Sei nun $\psi \in \mathrm{End}(A)$. ψ ist ein Ringhomomorphismus, also ist der Kern ein Ideal. Wegen $\psi(I_2) = I_2 \neq 0$ ist $\mathrm{Kern}(\psi) \neq A$.
Wegen der Vorüberlegung ist $\mathrm{Kern}(\psi) = \{0\}$, also ψ (als Gruppenhomomorphismus) injektiv.
ψ ist zusätzlich ein Vektorraumhomomorphismus zwischen zwei vierdimensionalen Vektorräumen, aus der Injektivität folgt damit die Surjektivität (LA).

b) **Vorüberlegung:** Nach Aufgabe 3 sind alle Konjugationen K_B mit $B \in \mathrm{GL}_2(K)$ K-Automorphismen.
Behauptung: Es gibt genau dann $S_1 \in \mathrm{GL}_2(K)$ mit $\varphi(e_1) = S_1 e_1 S_1^{-1}$ und $\varphi(e_2) = S_1 e_2 S_1^{-1}$, wenn es eine Matrix $S_2 \in \mathrm{GL}_2(K)$ mit $(K_B \circ \varphi)(e_1) = S_2 e_1 S_2^{-1}$ und $(K_B \circ \varphi)(e_2) = S_2 e_2 S_2^{-1}$.
Beweis der Behauptung: „$\Rightarrow$“ Nachrechnen zeigt $S_2 = B \cdot S_1$ beziehungsweise „$\Leftarrow$“ $S_1 = B^{-1} S_2$.

Schritt 1: Es ist $e_1^2 = 0$, also auch $\varphi(e_1)^2 = \varphi(e_1^2) = 0$. Es folgt, dass 0 Eigenwert von $\varphi(e_1)$ ist (denn der Rang ist nicht voll) und zwar der einzige (denn ist λ Eigenwert von $\varphi(e_1)$, dann ist λ^2 Eigenwert von $\varphi(e_1)^2 = 0$).
Jedes Polynom vom Grad 2, das eine Nullstelle besitzt, zerfällt in Linearfaktoren. Da 0 der einzige Eigenwert des charakteristischen Polynoms $f(X)$ der Matrix $\varphi(e_1)$, gilt $f(X) = X^2$.
Wegen $e_1 \neq 0$ und der Injektivität von φ gilt $\varphi(e_1) \neq 0$. Also besitzt $\varphi(e_1)$ die Jordannormalform e_1 (bzw. e_2, es ist egal, wo die 1 steht) – insbesonders sind $\varphi(e_1)$ und e_1 ähnlich, also gilt $\varphi(e_1) = T' e_1 T'^{-1}$ für ein $T' \in \mathrm{GL}_2(K)$.
Das analoge Argument gilt für e_2: Also ist $\varphi(e_2) = T e_2 T^{-1}$ für ein $T \in \mathrm{GL}_2(K)$.

Schritt 2: Mit der Vorüberlegung können wir $\varphi' = K_{T'^{-1}} \circ \varphi$ anstelle von φ betrachten. Dann ist $\varphi'(e_1) = e_1$. Ohne Einschränkung war bereits $T' = I$.

Situation:
Es ist $\varphi(e_1) = e_1, \varphi(e_2) = T e_2 T^{-1}$ für ein $T \in \mathrm{GL}_2(K)$.
Aufgabe: Finde $U \in \mathrm{GL}_2(K)$, so dass $U e_1 U^{-1} \stackrel{!}{=} e_1$, $U T e_2 T^{-1} U^{-1} \stackrel{!}{=} e_2$. Dann erfüllt $K_U \circ \varphi$ die Bedingung, also mit der Vorüberlegung auch φ.

Schritt 3: Ansatz für U: Sei $U = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(K)$ mit Inverser $U^{-1} = \frac{1}{ad-bc} \cdot \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$.
Dann ist $U \cdot e_1 \cdot U^{-1} = \frac{1}{ad-bc} \cdot \begin{pmatrix} -ca & a^2 \\ -c^2 & ac \end{pmatrix}$.
Die Bedingung $U \cdot e_1 \cdot U^{-1} \stackrel{!}{=} e_1$ ergibt $c = 0$ und dann $\frac{a^2}{ad-bc} = \frac{a^2}{ad} = 1$, also $a = d$.
Damit ist für jedes U von der Gestalt $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$ (mit $a \neq 0$) auch $(K_U \circ \varphi)(e_1) = e_1$ und wegen Konjugation mit $\begin{pmatrix} \frac{1}{a} & 0 \\ 0 & \frac{1}{a} \end{pmatrix}$ können wir uns auf den Fall $a = 1$ beschränken.

Schritt 4: Bestimmen von U in Abhängigkeit von T

Es ist $T = \begin{pmatrix} e & f \\ g & h \end{pmatrix} \in GL_2(K)$ eine feste Matrix.
Analog zu 3 berechnen wir $\varphi(e_2) = T \cdot e_2 \cdot T^{-1} = \frac{1}{eh-fg}\begin{pmatrix} fh & -f^2 \\ h^2 & -fh \end{pmatrix}$.
Insbesondere ist dabei $h \neq 0$, sonst wäre $\varphi(e_2) = \frac{j}{k} \cdot e_1 = \frac{j}{k} \cdot \varphi(e_1) = \varphi(\frac{j}{k} \cdot e_1)$, aber φ ist injektiv.
Nun suchen wir $b \in K$ beziehungsweise $U = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$, so dass $U \cdot \begin{pmatrix} fh & -f^2 \\ h^2 & -fh \end{pmatrix} \cdot U^{-1} = \begin{pmatrix} 0 & 0 \\ * & 0 \end{pmatrix}$.
Ausrechnen ergibt $U \cdot e_2 \cdot U^{-1} = \begin{pmatrix} fh + bh^2 & -2fbh - b^2h^2 - f^2 \\ h^2 & -bh^2 - fh \end{pmatrix} \cdot \frac{1}{eh-fg}$ und Koeffizientenvergleich ergibt $b = \frac{-j}{l}$.

Schritt 5: Es verbleibt nur zu zeigen, dass der letzte Eintrag $*$ (konkret ist das $* = \frac{h^2}{eh-fg}$) in $UTe_2t^{-1}U^{-1}$ tatsächlich 1 ist.
Sei nun also $\varphi' = K_U \circ \varphi$, also $\varphi'(e_1) = e_1, \varphi'(e_2) = * \cdot e_2$.
Es ist $e_1e_2 + e_2e_1 = I_2$, also $I_2 = \varphi(I_2) = \varphi(e_1)\varphi(e_2) + \varphi(e_2)\varphi(e_1) = * \cdot I_2$ und damit ist $* = 1$.

UFF!

c) e_1, e_2 erzeugen A als K-Algebra, denn mit $E_{11} = e_2e_1, E_{12} = e_1, E_{21} = e_2$, $E_{22} = e_1e_2$ sind alle Elementarmatrizen in $\langle e_1, e_2 \rangle$ und diese erzeugen A als K-Vektorraum, also insbesondere als K-Algebra.
Es gilt $\varphi(e_1e_2) = \varphi(e_1)\varphi(e_2) = Se_1S^{-1}Se_2S^{-1} = Se_1e_2S^{-1}$ und analog $\varphi(e_2e_1) = Se_2e_1S^{-1}$, also $\varphi(E_{ij}) = SE_{ij}S^{-1}$ für alle Elementarmatrizen E_{ij}, $i, j \in \{1, 2\}$.
Sei nun $B = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in A$ beliebig, so ist $B = aE_{11} + bE_{12} + cE_{21} + dE_{22}$ und $\varphi(B) = \varphi(aE_{11} + bE_{12} + cE_{21} + dE_{22}) = a\varphi(E_{11}) + b\varphi(E_{12}) + c\varphi(E_{21}) + d\varphi(E_{22}) = aSE_{11}S^{-1} + bSE_{12}S^{-1} + cSE_{21}S^{-1} + dSE_{22}S^{-1} = SBS^{-1}$.

d) Nach Aufgabe 3 sind alle Konjugationen Automorphismen. Dies gibt eine Abbildung $\psi\colon \mathrm{GL}_2(K) \to \mathrm{Aut}_{K-Alg}(A), S \mapsto K_S$.
Das ist ein Gruppenhomomorphismus, denn $\psi(ST) = K_{ST} \overset{(!)}{=} K_S \circ K_T = \psi(S) \circ \psi(T)$ für alle $S, T \in \mathrm{GL}_2(K)$, wie man für $x \in A$ nachrechnet:
$K_{ST}(x) = (ST)x(ST)^{-1} = S(TxT^{-1})S^{-1} = (K_S \circ K_T)(x)$.

In 4c) haben wir gesehen, dass jeder K-Automorphismus eine Konjugation ist, also ist ψ surjektiv.

Der Kern von ψ ist das Zentrum von A, aber das ist gerade $\{aI_2 \mid a \in K^\times\}$, wie man weiß oder leicht nachrechnet.[1]

[1] Oder seinen Tutor fragt?