# Lineare Algebra II

## Lösungen zu ausgewählten Aufgaben

### Blatt 2, Aufgabe 3

a) Wir zeigen, daß das Ideal $(2, X)$ kein Hauptideal in $\mathbb{Z}[X]$ ist. (Dieses Ideal besteht aus allen Elementen in $\mathbb{Z}[X]$, die von der Form $2 \cdot t + X \cdot u$ mit $t, u \in \mathbb{Z}[X]$ sind.) Angenommen nämlich, $(2, X)$ wäre ein Hauptideal, d.h. es gäbe $d \in \mathbb{Z}[X]$ mit $(d) = (2, X)$. Dann gäbe es $a, b \in \mathbb{Z}[X]$ mit $a \cdot d = 2$ und $b \cdot d = X$. Offenbar sind $a, b$ und $d$ Polynome ungleich 0. Da $d \cdot a = 2$ den Grad 0 hat, folgt, daß auch $d$ den Grad 0 hat, also in $\mathbb{Z}$ liegt. Die einzigen ganzen Zahlen, die in $\mathbb{Z}[X]$ Teiler von $X$ sind, sind offenbar 1 und $-1$, also gilt $d = 1$ oder $d = -1$. Wir dürfen also $d = 1$ annehmen. Es genügt also zu zeigen, daß $1 \notin (2, X)$. Nehmen wir also an, es gelte $1 \in (2, X)$, d.h. $r \cdot 2 + s \cdot X = 1$ für geeignete $r, s \in \mathbb{Z}[X]$. Wir schreiben $r = r_0 + r_1 X + r_2 X^2 + ...$, für geeignete $r_i \in \mathbb{Z}$, die bis auf endlich viele alle 0 sind. Dann folgt $r_0 \cdot 2 = 1$. Da 1 aber nicht durch 2 teilbar ist, ist dies nicht möglich. Also ist $1 \notin (2, X)$. Damit existiert kein $d \in \mathbb{Z}[X]$ mit $(d) = (2, X)$, also ist $(2, X)$ kein Hauptideal, also ist $\mathbb{Z}[X]$ kein Hauptidealring.

b) $\mathbb{Z}/4$ ist kein Integritätsbereich, da in diesem Ring $2 \cdot 2 = 0$ gilt, aber $2 \neq 0$. (Analog ist jedes $\mathbb{Z}/n$, wobei $n$ keine Primzahl ist, kein Integritätsbereich.)

### Blatt 3, Aufgabe 1

Wir suchen die kleinste positive ganze Zahl $n$ mit $n \equiv 1 \mod 2, 3, 4, 5, 6$ und $n \equiv 0 \mod 7$. Dies ist äquivalent zu $n \equiv 1 \mod 60$ und $n \equiv 0 \mod 7$. Wir suchen $x$ mit $7x \equiv 1 \mod 60$. Der euklidische Algorithmus liefert: $60 = 8 \cdot 7 + 4,\ 7 = 1 \cdot 4 + 3,\ 4 = 1 \cdot 3 + 1$. Also gilt $1 = 4 - 3 = 4 - (7 - 4) = 2 \cdot 4 - 7 = 2 \cdot (60 - 8 \cdot 7) - 7 = 2 \cdot 60 - 17 \cdot 7$. Also $-17 \cdot 7 \equiv 1 \mod 60$. Also $(60 - 17) \cdot 7 = 301 \equiv 1 \mod 60$ und $301 \equiv 0 \mod 7$. Wegen $301 < 7 \cdot 60$ ist nach dem Chinesischen Restsatz $n = 301$ die kleinste positive ganze Zahl mit dieser Eigenschaft.

### Blatt 4, Aufgabe 1

Sei $f$ nilpotent und $f^m = 0$. Das charakteristische Polynom von $f$ zerfällt (wie jedes Polynom über $\mathbb{C}$) in Linearfaktoren. Damit ist $f$ trigonalisierbar. Sei $\lambda$ ein Eigenwert von $f$. Dann folgt $\lambda^m = 0$, also $\lambda = 0$. Damit ist $f$ trigonalisierbar, und auf der Diagonalen einer entsprechenden oberen Dreiecksmatrix, die die Matrix von $f$ bzgl. einer geeigneten Basis ist, stehen nur Nullen. Damit folgt $\text{charpol}_f = X^n$, und es gibt es eine Basis $b_1, ..., b_n$ von $V$ mit $f(b_1) = 0$ und $f(b_i) \in < b_1, ..., b_{i-1} >$, für $i \geq 2$. Damit folgt $f^n = 0$. Ist $(ii)$ erfüllt, also $f^n = 0$, so ist $f$ nilpotent. Also gilt $(i) \Leftrightarrow (ii)$ und $(i) \Rightarrow (iii)$. Sei nun $(iii)$ erfüllt. Dann folgt, daß $f$ nur den Eigenwert 0 hat und trigonalisierbar ist. Damit folgt wieder, daß es eine Basis $b_1, ..., b_n$ von $V$ gibt mit $f(b_1) = 0$ und $f(b_i) \in < b_1, ..., b_{i-1} >$ für $i \geq 2$. Damit ist $f^n = 0$.

### Blatt 4, Aufgabe 3

Wir zeigen zunächst, daß $f$ und $g$ einen gemeinsamen Eigenvektor haben. Sei dazu $\lambda$ ein Eigenwert von $f$ (dieser existiert, da $f$ trigonalisierbar ist). Wir behaupten, daß $g$ den Eigenraum von $f$ zu $\lambda$ in sich abbildet, d.h. $g(\ker(f - \lambda \cdot \text{id})) \subseteq \ker(f - \lambda \cdot \text{id})$. Sei dazu $v \in \ker(f - \lambda \cdot \text{id})$. Dann gilt $f(g(v)) = g(f(v)) = g(\lambda \cdot v) = \lambda \cdot g(v)$. Also gilt $g(v) \in \ker(f - \lambda \cdot \text{id})$. Damit ist die Behauptung gezeigt, wir wissen also, daß $g$ einen Endomorphismus von $\ker(f - \lambda \cdot \text{id})$ induziert.

Da das charakteristische Polynom von $g$ in Linearfaktoren zerfällt, gilt dies auch für die Einschränkung von $g$ auf $\ker(f - \lambda \cdot \mathrm{id})$. Es gibt also einen Eigenvektor $b_1$ von $g$ in $\ker(f - \lambda \cdot \mathrm{id})$ zu einem Eigenwert $\mu$ von $g$. Wegen $b_1 \in \ker(f - \lambda \cdot \mathrm{id})$ gilt $f(b_1) = \lambda b_1$, also ist $b_1$ auch Eigenvektor zu $f$. Also haben $f$ und $g$ in der Tat einen gemeinsamen Eigenvektor.

Jetzt verwenden wir Induktion nach $n := \dim V$, um die Behauptung zu zeigen. Für $n = 1$ ist nichts zu tun, jede Basis von $V$ leistet das Gewünschte.

Wir ergänzen nun $b_1$ zu einer Basis $b_1, v_2, ..., v_n$ von $V$. Bezüglich dieser Basis $\mathcal{B}$ haben die Matrizen von $f$ und $g$ die Gestalt

$$M_{\mathcal{B}}^{\mathcal{B}}(f) = \begin{pmatrix} \lambda & * \\ 0 & A \end{pmatrix} \text{ und } M_{\mathcal{B}}^{\mathcal{B}}(g) = \begin{pmatrix} \mu & * \\ 0 & B \end{pmatrix}.$$

Dabei sind $A, B$ Matrizen der Größe $(n-1) \times (n-1)$, und die beiden $*$ stehen jeweils für eine $1 \times (n-1)$ Matrix (die jedoch nicht dieselben zu sein brauchen), weiter seht 0 für die $(n-1) \times 1$ Matrix mit nur 0-Einträgen. Wegen $fg = gf$ gilt auch $M_{\mathcal{B}}^{\mathcal{B}}(f)M_{\mathcal{B}}^{\mathcal{B}}(g) = M_{\mathcal{B}}^{\mathcal{B}}(g)M_{\mathcal{B}}^{\mathcal{B}}(f)$, und daraus folgt $AB = BA$. Wir betrachten den $(n-1)$-dimensionalen Unterraum $U$ von $V$, der von $v_2, ..., v_n$ aufgespannt wird und die Endomorphismen $f'$ und $g'$ von $U$, die bezüglich der Basis $v_2, ..., v_n$ durch die Matrizen $A$ und $B$ gegeben sind. Die charakteristischen Polynome von $f'$ bzw. $g'$ sind Teiler der charakteristischen Polynome von $f$ bzw. $g$, sie zerfallen also auch in Linearfaktoren, also sind $f'$ und $g'$ trigonalisierbar. Wegen $AB = BA$ folgt auch $f'g' = g'f'$. Also können wir die Induktionsvoraussetzung anwenden, finden also ein Matrix $S' \in GL_{n-1}(K)$, so daß $S'AS'^{-1}$ und $S'BS'^{-1}$ obere Dreiecksmatrizen sind. Daraus folgt für die Matrix $S := \begin{pmatrix} 1 & 0 \\ 0 & S' \end{pmatrix} \in GL_n(K)$, daß $SM_{\mathcal{B}}^{\mathcal{B}}(f)S^{-1}$ und $SM_{\mathcal{B}}^{\mathcal{B}}(g)S^{-1}$ obere Dreiecksmatrizen sind. Also sind in der Tat $f$ und $g$ simultan trigonalisierbar.

## Blatt 5, Aufgabe 1

Wir wissen, daß $\mathrm{charpol}_A = f(X)$, und $f(A) = 0$ nach dem Satz von Cayley-Hamilton. Wir müssen nur noch zeigen, daß es kein Polynom $g(X) \neq 0$ vom Grad $< n$ gibt mit $g(A) = 0$. Angenommen es gibt ein solches Polynom $g(X)$, sei $m$ der Grad von $g(X)$. Wir schreiben $g(X) = \sum_{i=0}^{m} b_i X^i$. Dann folgt $(\sum_{i=0}^{m} b_i A^i)(e_1) = 0$. Es gilt aber $A^i(e_1) = e_{i+1}$ für $i < n$. Also folgt $\sum_{i=0}^{m} b_i e_{i+1} = 0$. Aber die Standardbasisvektoren $e_1, ..., e_{m+1}$ sind linear unabhängig (es gilt $m + 1 \leq n$). Also $b_i = 0$ für alle $i$. Dies widerspricht der Annahme $g(X) \neq 0$.

## Blatt 5, Aufgabe 2

Sei $g(X) = a_0 + a_1 X + ... + a_{m-1}X^{m-1} + X^m$ das Minimalpolynom von $A$. Wir behaupten, daß $a_0 \neq 0$ gilt. Angenommen nämlich, es wäre $a_0 = 0$. Dann wäre $a_1 A + ... + a_{m-1}A^{m-1} + A^m = 0$. Da die Matrix $A$ ist invertierbar ist, folgt $0 = A^{-1}(a_1 A + ... + a_{m-1}A^{m-1} + A^m) = a_1 E_n + a_2 A + ... + A^{m-1}$ (dabei ist $E_n$ die Einheitsmatrix der Größe $n \times n$) . Damit wäre $g(X)$ nicht das Minimalpolynom von $A$ (sondern nur ein Vielfaches des Minimalpolynoms). Also ist $a_0 \neq 0$. Wegen $a_0 E_n + a_1 A + ... + A^m = 0$ und wegen $a_0 \neq 0$ ist $E_n = (-a_1/a_0)A + (-a_2/a_0)A^2 + ... + (-1/a_0)A^m = A \cdot ((-a_1/a_0)E_n + (-a_2/a_0)A + ... + (-1/a_0)A^{m-1})$. Also $A^{-1} = (-a_1/a_0)E_n + (-a_2/a_0)A + ... + (-1/a_0)A^{m-1}$. Das Polynom $f(X) = (-a_1/a_0) + (-a_2/a_0)X + ... + (-1/a_0)X^{m-1}$ leistet also das Gewünschte.

## Blatt 6, Aufgabe 2

Man rechnet nach, daß $\mathrm{charpol}_A = (X-2)(X-4)(X-6)^2$. Das charakteristische Polynom zerfällt also in Linearfaktoren, also kann man die Matrix $A$ in Jordansche

Normalform bringen. Jetzt bestimmt man die Dimension des Eigenraums zum Eigenwert 6. Diese ist 1. Damit lautet die Jordansche Normalform:

$$\begin{pmatrix} 2 & & & \\ & 4 & & \\ & & 6 & 1 \\ & & & 6 \end{pmatrix}.$$

## Blatt 6, Aufgabe 3

a) Siehe Vorlesung.

b) Sei $v = f(w)$. Sei $m \geq 1$ die natürlich Zahl, für die $f^m(v) = 0$, aber $f^{m-1}(v) \neq 0$. Es folgt dann $f^m(t) = 0$ für alle $t \in U$. Angenommen, es gibt einen Unterraum $U' \subseteq V$ mit $V = U \oplus U'$ und $f(U') \subseteq U'$. Wir schreiben $w = u + u'$ mit $u \in U$ und $u' \in U'$. Wir betrachten $f^m(w) = f^{m-1}(v)$. Dies ist ein von 0 verschiedenes Element von $U$. Andererseits $f^m(w) = f^m(u) + f^m(u') = 0 + f^m(u') \in U'$. Damit ist $f^m(w) \in U \cap U'$ und $f^m(w) \neq 0$. Dies widerspricht unserer Annahme $V = U \oplus U'$.

## Blatt 7, Aufgabe 1

a) Wie in Aufgabe 3 von Blatt 4 zeigt man, daß $g$ jeden Eigenraum von $f$ in sich abbildet. Ist $\lambda$ ein Eigenwert von $f$, so sei $V_\lambda(f)$ der zugehörige Eigenraum. Da $f$ diagonalisierbar ist, ist $V = \oplus_\lambda V_\lambda(f)$, wobei $\lambda$ die Eigenwerte von $f$ durchläuft. Sei nun $\lambda$ ein Eigenwert von $f$. Wir behaupten, daß die Einschränkung $g_{|_{V_\lambda(f)}}$ von $g$ auf $V_\lambda(f)$ diagonalisierbar ist. Ein Endomorphismus eines endlichdimensionalen Vektorraums ist genau dann diagonalisierbar, wenn sein Minimalpolynom erstens in Linearfaktoren zerfällt und zweitens jeder solche Linearfaktor nur mit der Vielfachheit 1 im Minimalpolynom auftritt. Da das Minimalpolynom von $g_{|_{V_\lambda(f)}}$ jedoch offenbar ein Teiler des Minimalpolynoms von $g$ ist, übertragen sich die beiden obigen Eigenschaften des Minimalpolynoms von $g$ auf das Minimalpolynom von $g_{|_{V_\lambda(f)}}$, so daß $g_{|_{V_\lambda(f)}}$ also diagonalisierbar ist. Wir wählen nun eine Basis aus Eigenvektoren zu $g$ von $V_\lambda(f)$. Dies sind auch Eigenvektoren zu $f$, da die Einschränkung von $f$ auf $V_\lambda(f)$ gerade $\lambda \cdot \mathrm{id}$ ist. Indem wir so für jedes $V_\lambda(f)$ verfahren, bildet die Vereinigung der so erhaltenen Basen der $V_\lambda(f)$ eine Basis von $V$ bestehend aus simultanen Eigenvektoren von $f$ und $g$, d.h. die Matrizen von $f$ und $g$ bzgl. dieser Basis sind beide Diagonalmatrizen.

b) Wir wählen eine Basis von $V$, bzgl. der die Matrizen von $f$ und $g$ beide Diagonalgestalt haben (dies ist nach Teil a) möglich). Die Matrix von $f + g$ bzgl. dieser Basis ist dann die Summe dieser beiden Diagonalmatrizen, also selbst eine Diagonalmatrix.

c) Wir wissen aus Aufgabe 3 von Blatt 4, daß $f$ und $g$ simultan trigonalisierbar sind. Sei $B$ eine Basis von $V$ bzgl. der die Matrizen von $f$ und $g$ beide obere Dreiecksmatrizen sind. Wie in Aufgabe 1 von Blatt 4 sehen wir, daß alle Diagoaleinträge von $M_B^B(f)$ und $M_B^B(f)$ gleich 0 sind. Also ist auch $M_B^B(f + g) = \mathrm{M}_B^B(f) + M_B^B(g)$ eine obere Dreiecksmatrix mit nur Nullen auf der Diagonalen. Wie in Aufgabe 1 von Blatt 4 sehen wir, daß diese Matrix nilpotent ist, also ist $f + g$ nilpotent.

d) Wir betrachten die Endomorphismen $f$ und $g$ des $\mathbb{C}^2$, die bzgl. der Standardbasis durch die Matrizen $A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ und $B = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$ gegeben sind. Sie sind nicht simultan diagonalisierbar, jeder für sich ist jedoch diagonalisierbar ist. (Der Endomorphismus $g$ bildet den Eigenraum von $f$ zum Eigenwert 0, also $< e_2 >$ nicht in sich ab.) Offenbar ist $fg \neq gf$. Ebenso ist die Summe von $f$ und $g$ offenbar nicht diagonalisierbar ($A + B$ hat nur den Eigenwert 1, der Eigenraum ist jedoch nur eindimensional). Für ein

Gegenbeispiel zu Teil c) betrachte die Endomorphisen $f$ und $g$ des $\mathbb{C}^2$, die bzgl. der Standardbasis durch die Matrizen $A = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ und $B = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ gegeben sind. Offenbar sind $f$ und $g$ nilpotent, aber $f + g$ ist es nicht. (Und es ist $fg \neq gf$.)

## Blatt 7, Aufgabe 2

a) Das charakteristische Polynom von $A$ ist $\text{charpol}_A = (X + 1)^5$. Also steht auf der Diagonalen der Jordanschen Normalform von $A$ nur der Eintrag $-1$. Ist ein Endomorphismus diagonalisierbar und hat nur einen Eigenwert, so ist seine Matrix offenbar bezüglich jeder Basis die Diagonalmatrix mit diesem Eigenwert als Diagonaleintrag. Also ist für $D = -E_5$ die Matrix $N := A - D$ nilpotent, und es gilt $A = D + N$ und $DN = ND$.

b) Wir bestimmen der Reihe nach die Dimensionen von $\ker(A + E_5)^i$. Die Ergebnisse lauten: $\dim \ker(A+E_5) = 2$. Also gibt es zwei Jordanblöcke. $\dim \ker(A+E_5)^2 = 4$. Also gibt es $4 - 2 = 2$ Jordanblöcke $J_{r,-1}$ mit $r \geq 2$. Da $A$ eine $5 \times 5$-Matrix ist, folgt, daß es einen Jordanblock der Größe 2 und einen Jordanblock der Größe 3 gibt. Also lautet die Jordannormalform von $A$:

$$\begin{pmatrix} -1 & 1 & & & \\ & -1 & & & \\ & & -1 & 1 & \\ & & & -1 & 1 \\ & & & & -1 \end{pmatrix}$$

c) Sei $f$ ein nilpotenter Endomorphismus eines $n$-dimensionalen $K$-Vektorraumes. Sei $V_1 \subset V$ ein $(n-1)$-dimensionaler Untervektorraum mit $f(V) \subset V_1$. Der Beweis von Satz 3.17 zeigt, wie man eine Zerlegung von $V$ in $f$-zyklische Unterräume erhält, wenn man für $f_{|V_1} : V_1 \to V_1$ bereits eine solche Zerlegung gefunden hat. Das ist natürlich noch nicht der Fall, deshalb wählen wir einen $(n-2)$-dimensionalen Unterraum $V_2 \subset V_1$ mit $f(V_1) \subset V_2$. Anschließend wählen wir einen $(n-3)$-dimensionalen Unterraum $V_3 \subset V_2$ mit $f(V_2) \subset V_3$ usw., bis wir schließlich einen 1-dimensionalen Unterraum $V_{n-1} \subset V_{n-2}$ mit $f(V_{n-2}) \subset V_{n-1}$ gewählt haben. $V_{n-1}$ ist dann als 1-dimensionaler Vektorraum trivialerweise $f$-zyklisch und man benutzt nun das Rezept aus dem Beweis von Satz 3.17, um erst eine Zerlegung von $V_{n-2}$ in $f$-zyklische Unterräume zu konstruieren, um dann daraus eine Zerlegung von $V_{n-3}$ in $f$-zyklische Unterräume zu konstruieren usw., bis man schließlich die gewünschte Zerlegung von $V$ in $f$-zyklische Unterräume gefunden hat.

Konkret geht das bei Aufgabe 7.2 so: Sei $B = A + E_5$, d.h.

$$B = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & -1 & 1 & -1 \\ 1 & 0 & -1 & 1 & 0 \\ 2 & 1 & -2 & 1 & -3 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Sei $f$ der Endomorphismus von $V = \mathbb{C}^5$ der bezüglich der Standardbasis durch $B$ beschrieben wird.

Wie man sieht, gilt $\text{im}\, f \subset \langle e_1, \ldots, e_4 \rangle$, d.h. wir setzen

$$V_1 = \langle e_1, \ldots, e_4 \rangle .$$

Bezüglich der Basis $\mathcal{B}_1 = (e_1, \dots, e_4)$ von $V_1$ wird $f_{|V_1}$ durch die Matrix

$$B_1 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & -1 & 1 \\ 1 & 0 & -1 & 1 \\ 2 & 1 & -2 & 1 \end{pmatrix}$$

beschrieben. Wie man sieht, gilt $f(V_1) \subset \langle e_2, e_3, e_4 \rangle$, wir setzen deshalb

$$V_2 = \langle e_2, e_3, e_4 \rangle .$$

Bezüglich der Basis $\mathcal{B}_2 = (e_2, e_3, e_4)$ von $V_2$ wird $f_{|V_2}$ durch die Matrix

$$B_2 = \begin{pmatrix} 0 & -1 & 1 \\ 0 & -1 & 1 \\ 1 & -2 & 1 \end{pmatrix}$$

beschrieben. Daran erkennt man $f(V_2) \subset \langle e_4, e_2 + e_3 + e_4 \rangle$: Es bilden nämlich die erste und die dritte Spalte von $B_2$ zusammen eine Basis von $\operatorname{im} B_2$ und diese erste bzw. dritte Spalte ist gerade der Koordinatenvektor von $e_4$ bzw. $e_2 + e_3 + e_4$ bezüglich der Basis $\mathcal{B}_2$.

Wir setzen deshalb

$$V_3 = \langle e_4, e_2 + e_3 + e_4 \rangle .$$

Nun ist $f(e_4) = (0, 1, 1, 1, 0)^t = e_2 + e_3 + e_4$ und $f(e_2 + e_3 + e_4) = 0$. Bezüglich der Basis $\mathcal{B}_3 = (e_4, e_2 + e_3 + e_4)$ von $V_3$ wird deshalb $f_{|V_3}$ durch die Matrix

$$B_3 = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$$

beschrieben. Also gilt $f(V_3) \subset \langle e_2 + e_3 + e_4 \rangle$. Wir setzen deshalb zum Abschluss

$$V_4 = \langle e_2 + e_3 + e_4 \rangle .$$

Dann ist $V_4$ $f$-zyklisch und wir können den Beweis von Satz 3.17 verwenden, um nach und nach Zerlegungen der anderen $V_i$ in $f$-zyklische Unterräume zu bestimmen.

Zu wählen ist ein Vektor in $V_3 \backslash V_4$, es bietet sich $e_4$ an. Dann ist $f(e_4) = e_2 + e_3 + e_4$ und es ist $e_2 + e_3 + e_4 \notin f(V_4)$. Folglich ist

$$V_3 = \langle e_4, f(e_4) \rangle = \langle e_4, e_2 + e_3 + e_4 \rangle$$

bereits die gewünschte „Zerlegung“ in $f$-zyklische Unterräume.

Zu wählen ist nun ein Vektor in $V_2 \backslash V_3$. Es bietet sich $e_2$ an. Dann gilt $f(e_2) = e_4$ und $e_4 \notin f(V_3)$. Wieder ist der Algorithmus direkt beendet und

$$V_2 = \langle e_2, f(e_2), f^2(e_2) \rangle = \langle e_2, e_4, e_2 + e_3 + e_4 \rangle$$

ist die gewünschte „Zerlegung“ in $f$-zyklische Unterräume.

Zu wählen ist ein Vektor in $V_1 \backslash V_2$. Es bietet sich $e_1$ an. Dann ist $f(e_1) = (0, 1, 1, 2, 0)^t$. Hier wird es zum ersten Mal interessant, da nun $f(e_1) \in f(V_2)$ gilt: Es ist nämlich $f(e_1) = -f(e_3)$. Der Algorithmus verlangt deshalb von uns, $e_1$ so durch ein Element von $V_2$ abzuändern, dass wir ein Element von $\ker f$ erhalten. Wir gehen deshalb von $e_1$ über zu $e_1 + e_3$, dann gilt wie gewünscht $f(e_1 + e_3) = 0$. Eine Zerlegung von $V_1$ in $f$-zyklische Unterräume ist deshalb gegeben durch

$$V_1 = \underbrace{\langle e_1 + e_3 \rangle}_{=:U_1} \oplus \underbrace{\langle e_2, f(e_2), f^2(e_2) \rangle}_{=:U_2}.$$

Schließlich ist ein Element von $V \backslash V_1$ zu wählen. Es bietet sich $e_5$ an. Dann ist $f(e_5) = (1, -1, 0, -3, 0)^t$ und es ist folglich

$$f(e_5) = \underbrace{(e_1 + e_3)}_{\in U_1} + \underbrace{(0, -1, -1, -3, 0)^t}_{\in U_2}$$

die entsprechende Zerlegung von $f(e_5)$ bezüglich der Zerlegung $V_1 = U_1 \oplus U_2$.

Es ist $e_1 + e_3 \notin f(U_1)$, aber $(0, -1, -1, -3, 0)^t \in f(U_2)$, nämlich $(0, -1, -1, -3, 0)^t = f(e_3 - e_2)$. Der Algorithmus verlangt, dass wir $e_5$ so abändern, dass der Anteil des Bildes von $e_5$ in $U_2$ zu Null wird. Wir gehen deshalb von $e_5$ über zu $e_5 - e_3 + e_2$. Nach dem Algorithmus ist dann

$$\begin{aligned} V &= \langle e_5 - e_3 + e_2, f(e_5 - e_3 + e_2) \rangle \oplus \langle e_2, f(e_2), f^2(e_2) \rangle \\ &= \langle e_5 - e_3 + e_2, e_1 + e_3 \rangle \oplus \langle e_2, e_4, e_2 + e_3 + e_4 \rangle \end{aligned}$$

die gewünschte Zerlegung von $V$ in $f$-zyklische Unterräume.

Die Basis $\mathcal{B} = (f(e_5 - e_3 + e_2), e_5 - e_3 + e_2, f^2(e_2), f(e_2), e_2)$ ist dann eine Jordanbasis für $A$. Die zugehörige Basiswechselmatrix ist gegeben durch

$$S = M^{\mathcal{B}}_{\text{std. B.}} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & -1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

und in der Tat gilt

$$S^{-1}AS = \begin{pmatrix} -1 & 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 1 & 0 \\ 0 & 0 & 0 & -1 & 1 \\ 0 & 0 & 0 & 0 & -1 \end{pmatrix}.$$

## Blatt 7, Aufgabe 3

Wegen $f^m(v) = 0$ ist $U =< v, f(v), ..., f^{m-1}(v) >$. Um $\dim U = m$ zu zeigen, genügt es zu zeigen, daß $v, f(v), ..., f^{m-1}(v)$ linear unabhängig sind. Angenommen also, die Elemente $v, f(v), ..., f^{m-1}(v)$ sind linear abhängig. Dann gibt es $a_0, ..., a_{m-1} \in K$, die nicht alle gleich 0 sind, mit $a_0 v + a_1 f(v) + ... + a_{m-1} f^{m-1}(v) = 0$. Sei $k \in \{0, ..., m-1\}$ minimal mit der Eigenschaft, daß $a_k \neq 0$. Dann gilt $0 = f^{m-1-k}(a_0 v + a_1 f(v) + ... + a_{m-1} f^{m-1}(v)) = a_k f^{m-1}(v)$. Wegen $f^{m-1}(v) \neq 0$ folgt $a_k = 0$, ein Widerspruch.

## Blatt 8, Aufgabe 2

Siehe Vorlesung

## Blatt 8, Aufgabe 3

Siehe Vorlesung

## Blatt 9, Aufgabe 2

Es gilt $\varphi(0) = 0$ und $\varphi(-x) = -\varphi(x)$ für jedes $x \in \mathbb{Z}^n$. Außerdem gilt $\varphi(x + y) = \varphi(x) + \varphi(y)$. Somit liegt das neutrale Element im Bild, das inverse jedes Elements von

$\operatorname{im}\varphi$ liegt in $\operatorname{im}\varphi$ und $\operatorname{im}\varphi$ ist abgeschlossen unter Summenbildung. Folglich ist $\operatorname{im}\varphi$ eine Untergruppe von $\mathbb{Z}^n$.

Sei $e_1, ..., e_n$ die Standardbasis des $\mathbb{Z}^n \subseteq \mathbb{Q}^n$. Wir definieren die Abbildung $\varphi_\mathbb{Q}$, indem wir für $x = x_1e_1 + ... + x_ne_n \in \mathbb{Q}^n$ setzen $\varphi_\mathbb{Q}(x) = x_1\varphi(e_1) + ... + x_n\varphi(e_n)$. Dann ist $\varphi_\mathbb{Q}$ ein Endomorphismus, die Einschränkung von $\varphi_\mathbb{Q}$ auf $\mathbb{Z}^n$ offenbar gleich $\varphi$, und $\varphi_\mathbb{Q}$ ist der einzige Endomorphismus mit dieser Eigenschaft, da ein Endomorphismus durch die Bilder einer Basis bereits eindeutig festgelegt ist.

b) Wir behaupten, daß $\varphi$ genau dann injektiv ist, wenn $\varphi_\mathbb{Q}$ injektiv ist. Es ist klar, daß $\varphi$ injektiv ist, wenn $\varphi_\mathbb{Q}$ injektiv ist. Ist umgekehrt $\varphi$ injektiv, so auch $\varphi_\mathbb{Q}$, denn wenn $\varphi_\mathbb{Q}(x) = 0$ für ein $x \in \mathbb{Q}^n$, so ist $a \cdot x \in \mathbb{Z}^n$ für ein geeignetes $a \in \mathbb{Z} \setminus \{0\}$, und also $0 = a \cdot \varphi_\mathbb{Q}(x) = \varphi_\mathbb{Q}(a \cdot x) = \varphi(a \cdot x)$, also $a \cdot x = 0$ (da $\varphi$ injektiv), also $x = 0$ (da $a \neq 0$), also ist $\varphi_\mathbb{Q}$ injektiv.

Nehmen wir nun an, $\varphi$ sei injektiv. Dann ist auch $\varphi_\mathbb{Q}$ injektiv, also als Endomorphismus eines endlichdimensionalen Vektorraums bijektiv, also liegen die Standardbasisvektoren $e_1, ..., e_n$ im Bild von $\varphi_\mathbb{Q}$. Folglich gibt es positive ganze Zahlen $q_1, ..., q_n$ so daß $q_1e_1, ..., q_ne_n$ im Bild von $\varphi$ liegen. (Sei nämlich etwa $\varphi_\mathbb{Q}(x_i) = e_i$, dann gibt es eine positive ganze Zahl $q_i$ mit $q_ix_i \in \mathbb{Z}^n$, also gilt $q_ie_i = \varphi_\mathbb{Q}(q_ix_i) = \varphi(q_ix_i)$.) Daraus folgt, daß der Quotient $\mathbb{Z}^n / \operatorname{im}\varphi$ aus höchstens $q_1 \cdot ... \cdot q_n$ Elementen besteht, also endlich ist.

Nehmen wir umgekehrt an, der Quotient $\mathbb{Z}^n / \operatorname{im}\varphi$ bestehe aus nur endlich vielen Elementen. Für jedes $x$ in $\mathbb{Z}^n$ bezeichnen wir mit $\overline{x}$ das Bild von $x$ in $\mathbb{Z}^n / \operatorname{im}\varphi$. Sei $i \in \{1, ..., n\}$. Dann gibt es ganze Zahlen $r_i > s_i > 0$ mit $\overline{r_ie_i} = \overline{s_ie_i}$. (Sonst bestünde $\mathbb{Z}^n / \operatorname{im}\varphi$ ja aus unendlich vielen Elementen.) Also ist $q_i := r_i - s_i > 0$, und es gilt $\overline{q_ie_i} = 0$. Daraus folgt $q_ie_i \in \operatorname{im}\varphi$, also gilt $e_i \in \operatorname{im}\varphi_\mathbb{Q}$, also ist $\varphi_\mathbb{Q}$ surjektiv, also auch injektiv. Also ist auch $\varphi$ injektiv.

## Blatt 9, Aufgabe 3

Es ist $901 = 17 \cdot 53$. Sei also $p = 17$ und $q = 53$. Gesucht ist eine Zahl $d$ mit $d \cdot e \equiv 1 \mod (p-1)(q-1)$, also $d \cdot 123 \equiv 1 \mod 832$. Wir verwenden den Euklidischen Algorithmus. Es ist $832 = 6 \cdot 123 + 94$. Weiter ist $123 = 1 \cdot 94 + 29$, weiter ist $94 = 3 \cdot 29 + 7$, weiter ist $29 = 4 \cdot 7 + 1$. Also ist $1 = 29 - 4 \cdot 7 = 29 - 4 \cdot (94 - 3 \cdot 29) = 13 \cdot 29 - 4 \cdot 94 = 13 \cdot (123 - 94) - 4 \cdot 94 = 13 \cdot 123 - 17 \cdot 94 = 13 \cdot 123 - 17 \cdot (832 - 6 \cdot 123) = 115 \cdot 123 - 17 \cdot 832$. Also ist $115 \cdot 123 \equiv 1 \mod 832$. Wir können also $d = 115$ wählen.

## Beliebiges Blatt, Aufgabe 4

Siehe Moodleseite