M. Künzer, J. Marhenke

Lineare Algebra für Informatiker, WS 03/04

Lösung 8

Aufgabe 32.

(1) Die definierten Produkte sind $ABC = \begin{pmatrix} 7 & 5 \\ -8 & -7 \end{pmatrix}$; $BCA = \begin{pmatrix} 3 & 0 \\ 9 & -3 \end{pmatrix}$; $CAB = \begin{pmatrix} 4 & 1 & 2 \\ -11 & -5 & -1 \\ -1 & -1 & 1 \end{pmatrix}$.

(2) Die definierten Produkte sind $ABC = \begin{pmatrix} 0 & 1 & \alpha \\ 1+\alpha & 1 & 1 \\ 1+\alpha & 1 & 1 \end{pmatrix}$; $BCA = \begin{pmatrix} \alpha & 1 & 1+\alpha \\ 0 & 0 & \alpha \\ 1+\alpha & \alpha & \alpha \end{pmatrix}$; $CAB = \begin{pmatrix} 1+\alpha & 0 \\ 1+\alpha & 1+\alpha \end{pmatrix}$.

Aufgabe 33.

(1) Es gilt $\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \longmapsto \begin{pmatrix} 1+i \\ -i \\ -1 \end{pmatrix}$, $\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \longmapsto \begin{pmatrix} 1+i \\ -i \\ -1 \end{pmatrix}$ und $\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \longmapsto \begin{pmatrix} i \\ 1-i \\ -1 \end{pmatrix}$. Daher ist $A(\varphi)_{\underline{y},\underline{y}} = \begin{pmatrix} 1+i & 1+i & i \\ -i & -i & 1-i \\ -1 & -1 & -1 \end{pmatrix}$ und $A(\varphi^3)_{\underline{y},\underline{y}} = (A(\varphi)_{\underline{y},\underline{y}})^3 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$.

(2) Es gilt $\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \longmapsto \begin{pmatrix} 2 \\ 2 \\ 2 \end{pmatrix} = 2 \cdot \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} + 0 \cdot \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} + 0 \cdot \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$, $\begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \longmapsto \begin{pmatrix} -1 \\ -1 \\ -2 \end{pmatrix} = 0 \cdot \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} + (-1) \cdot \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} + (-1) \cdot \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$ und $\begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \longmapsto \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} = 0 \cdot \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} + 1 \cdot \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} + 0 \cdot \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$. Daher ist $A(\varphi)_{\underline{y},\underline{y}} = \begin{pmatrix} 2 & 0 & 0 \\ 0 & -1 & 1 \\ 0 & -1 & 0 \end{pmatrix}$ und $A(\varphi^3)_{\underline{y},\underline{y}} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

(3) Es gilt $1 \longmapsto 0 = 0 \cdot 1 + 0 \cdot (1+X) + 0 \cdot (1+X)^2$, $(1+X) \longmapsto 2 = 2 \cdot 1 + 0 \cdot (1+X) + 0 \cdot (1+X)^2$ und $(1+X)^2 \longmapsto 12X^2 + 4 = 16 \cdot 1 + (-24) \cdot (1+X) + 12 \cdot (1+X)^2$. Daher ist $A(\varphi)_{\underline{y},\underline{y}} = \begin{pmatrix} 0 & 2 & 16 \\ 0 & 0 & -24 \\ 0 & 0 & 12 \end{pmatrix}$ und $A(\varphi^3)_{\underline{y},\underline{y}} = \begin{pmatrix} 0 & 0 & 1728 \\ 0 & 0 & -3456 \\ 0 & 0 & 1728 \end{pmatrix}$.

(4) Es gilt $1 \longmapsto 1 = 1 \cdot 1 + 0 \cdot \gamma + 0 \cdot \gamma^2$, $\gamma \longmapsto \gamma^5 = 1 \cdot 1 + 1 \cdot \gamma + (-1) \cdot \gamma^2$ und $\gamma^2 \longmapsto \gamma^{10} = (-2) \cdot 1 + (-2) \cdot \gamma + (-2) \cdot \gamma^2$. Daher ist $A(\varphi)_{\underline{y},\underline{y}} = \begin{pmatrix} 1 & 1 & -2 \\ 0 & 1 & -2 \\ 0 & -1 & -2 \end{pmatrix}$ und $A(\varphi^3)_{\underline{y},\underline{y}} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.
Dies ist nicht weiter verwunderlich, da $\varphi^3 : \xi \longmapsto \xi^{125} = \xi$.

Aufgabe 34.

(1) Die Ordnung von $A := \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}$ ist 13, da $A^{13} = E$, und $A^k \neq E$ für $k \in [1, 12]$, wie man durch direkte Rechnung verifiziert.

(2) Gesucht ist eine Matrix $A \in \mathrm{GL}_2(\mathbf{F}_9)$, für die $A^5 - E = 0$ gilt. Wir zerlegen $X^5 - 1 \in \mathbf{F}_9[X]$ in

$$X^5 - 1 = (X-1)(X - (1-\iota)X + 1)(X - (1+\iota)X + 1) \, .$$

Für eine Matrix $A \in \mathrm{GL}_2(\mathbf{F}_9)$ ist daher entsprechend

$$A^5 - E = (A - E)(A^2 - (1-\iota)A + E)(A^2 - (1+\iota)A + E) \, ,$$

so daß es etwa genügt, A so zu finden, daß $A^2 - (1-\iota)A + E = 0$.

Setzen wir einfachstmöglich mit $A = \begin{pmatrix} 0 & 1 \\ a & b \end{pmatrix}$ an, $a, b \in \mathbf{F}_9$, so sehen wir wegen $A^2 = \begin{pmatrix} a & b \\ ab & a+b^2 \end{pmatrix}$, daß $A^2 - bA - aE = 0$. Wir wählen also $b = 1 - \iota$ und $a = -1$ und erhalten $A = \begin{pmatrix} 0 & 1 \\ -1 & 1-\iota \end{pmatrix}$.

Folglich ist die Ordnung von A eine Teiler von 5. Da $A \neq E$ ist, folgt, dass die Ordnung von A gleich 5 ist. Wegen der linearen Unabhängigkeit der Spalten von A ist $A \in \mathrm{GL}_2(\mathbf{F}_9)$.

Hier ist es eher mühsam, durch Probieren zum Ergebnis zu kommen, da unter den $(9^2-1)(9^2-9)$ Elementen von $\mathrm{GL}_2(\mathbf{F}_9)$ nur 144 Ordnung 5 haben. In einer kleineren Gruppe wäre das aber durchaus möglich.

Aufgabe 35.

(1) Die Aussage ist richtig. $X^2 - a$ ist irreduzibel genau dann, wenn $b^2 \neq a$ für alle $b \in \mathbf{F}_p$ gilt. Es bleibt zu zeigen, dass immer ein solches a existiert, das kein Quadrat eines Elements $b \in \mathbf{F}_p$ ist, d.h., daß die Abbildung $\mathbf{F}_p \longrightarrow \mathbf{F}_p$, $\xi \longmapsto \xi^2$ nicht surjektiv ist. Dazu genügt es, zu zeigen, daß sie nicht injektiv ist. In der Tat ist $-1 \neq +1$ wegen $p \geq 3$, wohingegen $(-1)^2 = (+1)^2$.

(2) Die Aussage ist falsch. Sei $q := \#K$. Es ist $\#(\mathrm{GL}_n(K)) = \prod_{j\in[0,n-1]}(q^n - q^j)$ nach Aufgabe 26 (3). Ferner ist $\#(K^{n\times n}) = q^{n^2}$. Für $n \geq 1$ wird

$$\begin{array}{rcl} \dfrac{\#(\mathrm{GL}_n(K))}{\#(K^{n\times n})} & = & \dfrac{\prod_{j\in[0,n-1]}(q^n - q^j)}{q^{n^2}} \\ & = & \prod_{j\in[0,n-1]}(1 - q^{j-n}) \\ & < & 1 - 1/q\,. \end{array}$$

Damit kann der fragliche Ausdruck nicht gegen 1 konvergieren. (In der Tat konvergiert er gegen einen Wert echt zwischen 0 und 1.)

(3) Die Aussage ist falsch. Es bezeichnet $D^k \in \mathrm{End}_{\mathbf{R}}\,\mathbf{R}[X]$ die Abbildung, die ein Polynom k-fach ableitet. Man betrachte für beliebiges n das Tupel $(D^0, \dots, D^n)$. Angenommen, dieses Tupel sei linear abhängig. Dann existieren $(\lambda_0, \dots, \lambda_n) \neq (0, \dots, 0)$ so, daß $\lambda_0 D^0 + \dots + \lambda_n D^n = 0$. Sei l der kleinste Index mit $\lambda_l \neq 0$. Dann ist

$$0 \;=\; \left(\sum_{k=l}^{n} \lambda_k D^k\right)(X^l) \;=\; \lambda_l D^l(X^l) \;=\; \lambda_l \cdot l!\,,$$

und wir haben einen Widerspruch.

Folglich ist das Tupel $(D^0, \dots, D^n)$ für jedes $n \in \mathbf{N}$ linear unabhängig, und somit ist $\mathrm{End}_{\mathbf{R}}\,\mathbf{R}[X]$ nicht endlichdimensional über $\mathbf{R}$.

(4) Die Aussage ist richtig.

$\Longleftarrow$. Gibt es ein $V \xleftarrow{g} W$ mit $f \circ g = 1_W$, so ist f wegen $y = f(g(y))$ für gegebenes $y \in W$ surjektiv.

$\Longrightarrow$. Sei f surjektiv und sei $(x_1, \dots, x_n)$ eine Basis von V. Dann ist $(f(x_1), \dots, f(x_n))$ ein erzeugendes Tupel von W. Daraus wählt man eine Basis $(f(x_{i_1}), \dots, f(x_{i_m}))$ von W aus und definiert die lineare Abbildung $V \xleftarrow{g} W$ dadurch, daß $f(x_{i_j}) \overset{g}{\longmapsto} x_{i_j}$ gesetzt wird für alle $j \in [1, m]$. Dann ist wegen $f \circ g : f(x_{i_j}) \overset{g}{\longmapsto} x_{i_j} \overset{f}{\longmapsto} f(x_{i_j})$ in der Tat $f \circ g = 1_W$. Die Injektivität von g folgt aus der linearen Unabhängigkeit von $(x_{i_1}, \dots, x_{i_m})$, oder aber auch aus $f \circ g = 1_W$.

(5) Die Aussage ist falsch. Wir haben etwa das Gegenbeispiel $A = \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$.

(6) Die Aussage ist richtig. Sei $A = \begin{pmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & & \vdots \\ a_{n,1} & \cdots & a_{n,n} \end{pmatrix}$. Dann ist $A^{\mathrm{t}}A = \left(\sum_{k\in[1,n]} a_{k,i}a_{k,j}\right)_{i,j}$. Ist $A^{\mathrm{t}}A = 0$, so muss also insbesondere $\sum_{k\in[1,n]} a_{k,i}^2 = 0$ für alle $i \in [1, n]$ gelten, woraus $a_{k,i} = 0$ für alle $i,\, k \in [1, n]$ folgt, d.h. $A = 0$.

(7) Die Aussage ist richtig. Es gilt $\xi^2 \in \{0, 1, 2, 4\}$ für alle $\xi \in \mathbf{F}_7$, so daß wir aus $\xi_1^2 + \xi_2^2 = 0$ mit $\xi_1,\, \xi_2 \in \mathbf{F}_7$ folgern können, daß $\xi_1 = \xi_2 = 0$. Folglich kann man wie in (6) argumentieren.

(8) Die Aussage ist falsch. Wir haben etwa das Gegenbeispiel $A = \left(\begin{smallmatrix} 1 & 0 & 0 \\ 2 & 0 & 0 \\ 3 & 0 & 0 \end{smallmatrix}\right)$.