Lineare Algebra 1
6. Tutoriumsblatt

TECHNISCHE UNIVERSITÄT DARMSTADT

Fachbereich Mathematik
Prof. Dr. Kollross
Dipl.-Math. Schwieger, Dipl.-Math. Schröder

WS 2011/2012
20.01.2012

Aufgabe T1 (Die allgemeine lineare Gruppe $\mathrm{GL}_2\,\mathbb{F}_p$)
Wir betrachten in dieser Aufgabe die Gruppe $\mathrm{GL}_2\,\mathbb{F}_p$, dass heißt die Gruppe aller invertierbaren 2×2-Matrizen mit Elementen aus $\mathbb{F}_p$, wobei p eine beliebige Primzahl ist.

(a) Bestimmen Sie die Ordnung, dass heißt die Anzahl der Elemente, von $\mathrm{GL}_2\,\mathbb{F}_p$. Gehen Sie hierzu folgendermaßen vor:

  i. Untersuchen Sie, wie viele Vektoren (a, b) mit $(a, b) \in \mathbb{F}_p$ es gibt, die nicht der Nullvektor sind.

  ii. Bestimmen Sie die Anzahl der Vektoren (c, d) mit $c, d \in \mathbb{F}_p$, sodass die Matrix
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$
  invertierbar ist.

(b) Zeigen Sie, dass $\mathrm{GL}_2\,\mathbb{F}_2$ isomorph zur symmetrischen Gruppe S_3 ist.

Aufgabe T2
Beweisen Sie:

(a) Für $A \in \mathbb{K}^{n\times n}$ und $m \in \mathbb{N}$ gilt:
$$E_n - A^m = (E_n - A)(\sum_{i=0}^{m-1} A^i) = (\sum_{i=0}^{m-1} A^i)(E_n - A).$$

(b) Ist $A \in \mathbb{K}^{n\times n}$ eine Matrix, für die ein $m \in \mathbb{N}$ existiert mit $A^m = 0$, so ist $E_n - A$ invertierbar. Wie sieht die inverse Matrix aus?

Aufgabe T3 (Schnitt- und Summenbasen)
Der Algorithmus von Zassenhaus ist ein Verfahren zur Bestimmung von Schnitt- und Summenbasen von zwei Untervektorräumen. Der Algorithmus stellt eine Verallgemeinerung des Verfahrens zur Bestimmung einer Basis des von den Zeilen einer Matrix aufgespannten Unterraums dar.
Algorithmus Seien zwei Untervektorräume von $\mathbb{K}^n$ durch
$$U = \mathrm{span}(u_1, \dots, u_t)$$
$$W = \mathrm{span}(w_1, \dots, w_r)$$
gegeben. Konstruiere dann die folgende Matrix
$$A = \begin{pmatrix} u_1 & u_1 \\ \vdots & \vdots \\ u_t & u_t \\ w_1 & 0 \\ \vdots & \vdots \\ w_r & 0 \end{pmatrix} \in \mathbb{K}^{(t+r)\times 2n}.$$

Bringe A durch elementare Zeilenumformungen auf die Form

$$A' = \begin{pmatrix} v_1 & \star \\ \vdots & \vdots \\ v_l & \star \\ 0 & y_1 \\ \vdots & \vdots \\ 0 & y_{m-l} \end{pmatrix}$$

wobei $m = r + t$, $v_1, \dots, v_l$ linear unabhängig sind und $\star$ für beliebige Einträge steht.
Dann ist $v_1, \dots, v_l$ eine Basis von $U + W$ und $y_1, \dots, u_{m-l}$ ein Erzeugendensystem von $U \cap W$.
Beispiel Für $U = \operatorname{span}((1,1,0),(1,1,1))$ und $W = \operatorname{span}((1,0,1),(0,-1,0))$ (mit Zeilenvektoren als Elementen) kann

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

durch elementare Zeilenumformungen auf die Form

$$A' = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & -1 & 1 & -1 & -1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}$$

gebracht werden. Dann ist $U \cap W = \operatorname{span}((1,1,1))$ und $U + W = \operatorname{span}((1,1,0),(0,0,1),(0,-1,1))$.

(a) Zeigen Sie, dass $v_1, \dots, v_l$ und $y_1, \dots, y_{m-l}$ tatsächlich eine Basis von $U + W$ und ein Erzeugendensystem von $U \cap W$ bilden.

Hinweis: Betrachten Sie hierzu das Bild und den Kern der linearen Abbildung

$$\phi : T \to \mathbb{K}^n,\ (x, y) \mapsto x,$$

mit $T := \{(u,u) | u \in U\} + \{(w,0) | w \in W\}$, also ist T der von den Zeilen der Matrix A aufgespannte Raum.

(b) Es sei $V = \mathbb{C}^4$ (mit Zeilenvektoren als Elementen) und

$$\begin{aligned} U &:= \operatorname{span}((\mathrm{i}, 2+\mathrm{i}, -1, 1-\mathrm{i}), (-1, 2\mathrm{i}, 0, 1+3\mathrm{i}), (-\mathrm{i}, -2, -1+\mathrm{i}, -3-\mathrm{i})), \\ W &:= \operatorname{span}((-\mathrm{i}, -3-\mathrm{i}, 1-\mathrm{i}, 0), (-i, -1-i, 1+i, -1+3\mathrm{i}), (1-\mathrm{i}, -4\mathrm{i}, 2+2\mathrm{i}, -1+3\mathrm{i})). \end{aligned}$$

Berechnen Sie Basen von $U + W$ und $U \cap W$.

Lösung:

(a)

(b)

$$A = \begin{pmatrix} i & 2+i & -1 & 1-i & i & 2+i & -1 & 1-i \\ -1 & 2i & 0 & 1+3i & -1 & 2i & 0 & 1+3i \\ -i & -2 & -1+i & -3-i & -i & -2 & -1+i & -3-i \\ -1 & -3-i & 1-i & 0 & 0 & 0 & 0 & 0 \\ -i & -1-i & 1+i & -1+3i & 0 & 0 & 0 & 0 \\ 1-i & -4i & 2+2i & -1+3i & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$\to \begin{pmatrix} i & 2+i & -1 & 1-i & i & 2+i & -1 & 1-i \\ 0 & 1 & i & 2i & 0 & 1 & i & 2i \\ 0 & i & -2+i & -2-2i & 0 & i & -2+i & -2-2i \\ 0 & -1 & -i & 1-i & i & 2+i & -1 & 1-i \\ 0 & 1 & i & 2i & i & 2+i & -1 & 1-i \\ 0 & 1-i & 1+i & 1+3i & -1+i & 1+3i & -1-i & 2 \end{pmatrix}$$

$$\to \begin{pmatrix} i & 2+i & -1 & 1-i & i & 2+i & -1 & 1-i \\ 0 & 1 & i & 2i & 0 & 1 & i & 2i \\ 0 & 0 & -1+i & -2i & 0 & 0 & -1+i & -2i \\ 0 & 0 & 0 & 1+i & i & 3+i & -1+i & 1+i \\ 0 & 0 & 0 & 0 & i & i+1 & -1-i & 1-3i \\ 0 & 0 & 0 & -1+i & -1+i & 4i & -2-2i & -2i \end{pmatrix}$$

$$\to \begin{pmatrix} i & 2+i & -1 & 1-i & i & 2+i & -1 & 1-i \\ 0 & 1 & i & 2i & 0 & 1 & i & 2i \\ 0 & 0 & -1+i & -2i & 0 & 0 & -1+i & -2i \\ 0 & 0 & 0 & 1+i & i & 3+i & -1+i & 1+i \\ 0 & 0 & 0 & 0 & i & i+1 & -1-i & 1-3i \\ 0 & 0 & 0 & 0 & i & i+1 & -1-i & 1-3i \end{pmatrix}$$

Also ist $((i,2+i,-1,1-i),(0,1,i,2i),(0,0,-1+i,-2i),(0,0,0,1+i))$ eine Basis von $U+W$ und $((i,1+i,-1-i,1-3i))$ eine Basis von $U\cap W$.

Aufgabe T4

Seien V, W zwei endlichdimensionale Vektorräume.

(a) Seien $\mathcal{A}$ und $\mathcal{B}$ Basen von V. Seien $\mathcal{A}^\star$ und $\mathcal{B}^\star$ die zugehörigen dualen Basen von $V^\star$. Zeigen Sie, dass dann für die Transformationsmatrizen gilt

$$T^{\mathcal{A}^\star}_{\mathcal{B}^\star} = (T^{\mathcal{A}}_{\mathcal{B}})^{-T}.$$

(b) Sei $F : V \to W$ ein Homomorphismus und $U \subset W$ ein Untervektorraum. Zeigen Sie:

$$F^\star(U^0) = (F^{-1}(U))^0.$$

Hinweis: $U^0 := \{\varphi \in W^\star : \varphi(u) = 0 \text{ für alle } u \in U\} \subset W^\star$ ist der sogenannte Annullator von U.

Lösung: Sei V ein endlich-dimensionaler Vektorraum. Der Dualraum ist dann

$$V^* := \mathrm{Hom}_{\mathbb{K}}(V, \mathbb{K}).$$

Sei $\mathcal{A} = (v_1, \dots, v_n)$ eine Basis von V. Dann ist

$$v_i^* : V \to \mathbb{K}, \text{ mit } v_i^*(v_j) = \delta_{ij}$$

eine lineare Abbildung und insbesondere ist $\mathcal{A}^* = (v_1^*, \dots, v_n^*)$ eine Basis von V^*, die duale Basis. Schließlich ist für eine lineare Abbildung $F : V \to W$ die duale Abbildung definiert durch

$$F^* : W^* \to V^*, \psi \mapsto F^*(\psi) := \psi \circ F.$$

(a) Für die Transformationsmatrixen gilt

$$T_{\mathcal{A}}^{\mathcal{B}} = M_{\mathcal{A}}^{\mathcal{B}}(id_V) \text{ und } T_{\mathcal{A}^*}^{\mathcal{B}^*} = M_{\mathcal{A}^*}^{\mathcal{B}^*}(id_{V^*}).$$

Wir zeigen, dass $M_{\mathcal{A}^*}^{\mathcal{B}^*}(id_{V^*}) = (M_{\mathcal{B}}^{\mathcal{A}}(id_V))^T$ ist. Sei hierzu $\mathcal{A} = (v_1, \ldots, v_n)$ und $\mathcal{B} = (w_1, \ldots, w_n)$. Dann gilt mit $M_{\mathcal{B}}^{\mathcal{A}}(id_V) = (a_{ij})$:

$$v_j = \sum_{i=1}^{n} a_{ij} w_i, \text{ also } a_{ij} = w_i^*(v_j).$$

Ähnlich gilt für $M_{\mathcal{A}^*}^{\mathcal{B}^*}(id_{V^*}) = (b_{ji})$:

$$w_i^* = \sum_{j=1}^{n} b_{ji} v_j^*, \text{ also } b_{ji} = w_i^*(v_j).$$

Daraus folgt also $a_{ij} = b_{ji}$ und $M_{\mathcal{A}^*}^{\mathcal{B}^*}(id_{V^*}) = (M_{\mathcal{B}}^{\mathcal{A}}(id_V))^T$.
Es folgt

$$T_{\mathcal{A}^*}^{\mathcal{B}^*} = M_{\mathcal{A}^*}^{\mathcal{B}^*}(id_{v^*}) = (M_{\mathcal{B}}^{\mathcal{A}}(id_V))^T = (T_{\mathcal{B}}^{\mathcal{A}})^T = (T_{\mathcal{A}}^{\mathcal{B}})^{-T}.$$

(b) Zuerst zeigen wir die Inklusion $F^*(U^0) \subseteq (F^{-1}(U))^0$. Sei $\psi \in F^*(U^0)$. Dann existiert ein $\varphi \in U^0$ mit $\psi = \varphi \circ F$, da ψ ja im Bild der dualen Abbildung F^* von F liegt. Da φ im Annulator von U liegt, gilt $\varphi|_U = 0$ und daher $\psi|_{F^{-1}}(U) = 0$. Also folgt $\psi \in (F^{-1}(U))^0$.
Es fehlt noch die Inklusion $(F^{-1})^0 \subseteq F^*(U^0)$. Sei $\psi \in (F^{-1}(U))^0$, d.h. $\psi|_{F^{-1}(U)} = 0$. Seien nun die folgenden Zerlegungen von V und W gegeben:

$$V = F^{-1}(U) \oplus \tilde{V} \text{ und } W = U \oplus \tilde{W} \text{ mit } \tilde{W} = F(\tilde{V}) \oplus W', \text{ wobei } W' \subseteq W.$$

Insbesondere ist $F(\tilde{V}) \subseteq \tilde{W}$ und $\dim F(\tilde{V}) = \dim \tilde{W}$. Da $\ker F \subseteq F^{-1}(U)$ ist $F|_{\tilde{V}}$ injektiv.
Sei $(\tilde{v}_1, \ldots, \tilde{v}_k)$ eine Basis von $\tilde{V}$ und $(\tilde{w}_1, \ldots, \tilde{w}_k)$ eine Basis von $F(\tilde{V})$ mit $F(\tilde{v}_i) = \tilde{w}_i$ für $i = 1, \ldots, k$. Wir können diese Basis zu einer Basis $(\tilde{w}_1, \ldots, \tilde{w}_k, w_1, \ldots, w_m)$ von $\tilde{W}$ ergänzen. Es gibt dann nur genau ein $\varphi \in \mathrm{Hom}(W, \mathbb{K})$ mit $\varphi(\tilde{w}_i) = \psi(\tilde{v}_i)$ für $i = 1, \ldots, k$ und $\varphi(w_j) = 0$ für $j = 1, .., m$ sowie $\varphi|_U = 0$. Es ist also $\psi = \varphi \circ F$. Also liegt ψ, da $\varphi \in U^0$, in $F^*(U^0)$.