Aufgabe F16T3A1 (12 Punkte)

Sei K ein Körper, $n \in \mathbb{N}$, und $K^{n\times n}$ der K-Vektorraum der $n \times n$-Matrizen. Ferner sei $\mathrm{GL}_n(K)$ die Gruppe der invertierbaren Matrizen aus $K^{n\times n}$.

(a) Sei $A \in K^{n\times n}$, und V der von den Matrizen $A^0, A^1, A^2, ...$ erzeugte Untervektorraum von $K^{n\times n}$. Man zeige, dass $\dim V \leq n$ gilt.
(*Hinweis:* Satz von Cayley-Hamilton)

(b) Sei K ein endlicher Körper. Man zeige, dass jedes Element aus $\mathrm{GL}_n(K)$ höchstens die Ordnung $|K|^n - 1$ hat.
(*Hinweis:* Für $A \in \mathrm{GL}_n(K)$ vergleiche man die von A erzeugte Untergruppe von $\mathrm{GL}_n(K)$ mit V.)

Lösung:

zu (a) Sei $U = \langle\{A^0, ..., A^{n-1}\}\rangle_K$ der von den Matrizen A^k mit $0 \leq k < n$ aufgespannte Untervektorraum U von V. Wenn wir zeigen können, dass $U = V$ gilt, dann besitzt V ein n-elementiges Erzeugendensystem, und es folgt $\dim V \leq n$. Die Inklusion $U \subseteq V$ ist offensichtlich. Wir zeigen, dass umgekehrt auch $V \subseteq U$ gilt, indem wir durch vollständige Induktion über k nachweisen, dass $A^k \in U$ für alle $k \in \mathbb{N}_0$ gilt. Für $0 \leq k \leq n-1$ ist dies nach Definition klar, dies ist unser Induktionsanfang.

Sei nun $k \in \mathbb{N}_0$ mit $k \geq n$, und setzen wir $A^\ell \in U$ für alle ℓ mit $0 \leq \ell < k$ voraus. Sei $\chi_A = x^n + a_{n-1}x^{n-1} + ... + a_0 \in K[x]$ das charakteristische Polynom von A. Nach dem Satz von Cayley-Hamilton gilt $\chi_A(A) = 0$, was zu

$$A^n \quad = \quad -a_{n-1}A^{n-1} - ... - a_1A^1 - a_0A^0$$

umgestellt werden kann. Durch Multiplikation dieser Gleichung mit A^{k-n} von links erhalten wir

$$A^k \quad = \quad -a_{n-1}A^{k-1} - ... - a_1A^{k-n+1} - a_0A^{k-n}.$$

Weil die Matrizen $A^{k-1}, A^{k-2}, ..., A^{k-n+1}, A^{k-n}$ nach Induktionsvoraussetzungen in U liegen, gilt dasselbe auch für A^k. Damit ist der Induktionsbeweis abgeschlossen.

zu (b) Sei $A \in \mathrm{GL}_n(K)$, $G = \langle A\rangle$ die von A erzeugte Untergruppe von $\mathrm{GL}_n(K)$ und V der von den Potenzen von A aufgespannte Untervektorraum wie in Teil (a). Mit K ist auch die Gruppe $\mathrm{GL}_n(K)$ und damit auch $m = |G| = \mathrm{ord}(A)$ endlich. Die Elemente von G haben also die Form A^k mit $0 \leq k < m$ und sind damit in V enthalten. Es folgt $G \subseteq V$, und da mit A auch die Potenzen A^k invertierbar sind, gilt sogar $G \subseteq V \setminus \{0\}$. Als Vektorraum der Dimension $\leq n$ über dem Körper K hat V höchstens $|K|^n$ Elemente. Es folgt $\mathrm{ord}(A) \leq |V \setminus \{0\}| \leq |K|^n - 1$.