Aufgabe F13T2A2 (6 Punkte)

Sei $q > 1$ Potenz einer Primzahl p, und sei $\mathbb{F}_q$ ein Körper mit q Elementen. Sei n eine natürliche Zahl, und sei $G = \mathrm{GL}_n(\mathbb{F}_q)$ die Gruppe der invertierbaren $n \times n$-Matrizen über $\mathbb{F}_q$.

(a) Zeigen Sie, dass die Gruppe G von Ordnung $q^{\binom{n}{2}}(q^n - 1)(q^{n-1} - 1) \cdots (q - 1)$ ist.

(b) Zeigen Sie, dass die oberen Dreiecksmatrizen mit charakteristischem Polynom $(x - 1)^n$ eine Sylowsche p-Untergruppe von $\mathrm{GL}_n(\mathbb{F}_q)$ bilden.

Lösung:

zu (a) Eine $n \times n$-Matrix A über $\mathbb{F}_q$ liegt genau dann in $G = \mathrm{GL}_n(\mathbb{F}_q)$, wenn die Spaltenvektoren $v_1, ..., v_n \in \mathbb{F}_q^n$ von A eine geordnete Basis von $\mathbb{F}_q^n$ bilden oder, was wegen $\dim \mathbb{F}_q^n$ dazu äquivalent ist, linear unabhängig sind. Aus der Linearen Algebra ist bekannt, dass jede Basis von $\mathbb{F}_q^n$ dadurch zu Stande kommt, dass man nacheinander Vektoren

$$v_1 \neq 0_{\mathbb{F}_q^n} \quad , \quad v_2 \in \mathbb{F}_q^n \setminus \mathrm{lin}(v_1) \quad , \quad v_3 \in \mathbb{F}_q^n \setminus \mathrm{lin}(v_1, v_2) \quad , \quad ... \quad , \quad v_n \in \mathbb{F}_q^n \setminus \mathrm{lin}(v_1, ..., v_{n-1})$$

wählt. Wir rechnen nach, wieviele Möglichkeiten es für jede einzelne Wahl jeweils gibt. Für den Vektor v_1 gibt es $|\mathbb{F}_q^n \setminus \{0_{\mathbb{F}_q^n}\}| = q^n - 1$ Möglichkeiten. Ist v_1 bereits gewählt, dann gibt es für den Vektor v_2 genau $|\mathbb{F}_q^n \setminus \mathrm{lin}(v_1)| = q^n - q$ Möglichkeiten, denn $\mathrm{lin}(v_1)$ hat als 1-dimensionaler $\mathbb{F}_q$-Vektorraum genau q Elemente. Sei nun allgemein $k \in \{1, ..., n-1\}$, und nehmen wir an, dass $v_1, ..., v_k$ bereits gewählt sind. Dann gibt es für v_{k+1} noch $|\mathbb{F}_q^n \setminus \mathrm{lin}(v_1, ..., v_k)| = q^n - q^k$ Möglichkeiten, denn $\mathrm{lin}(v_1, ..., v_k)$ ist ein k-dimensionaler $\mathbb{F}_q$-Vektorraum mit q^k Elementen. Für das Tupel $(v_1, ..., v_n)$ kommen wir damit auf insgesamt

$$\prod_{k=0}^{n-1} (q^n - q^k) \quad = \quad \prod_{k=0}^{n-1} q^k \cdot \prod_{k=0}^{n-1} (q^{n-k} - 1) \quad = \quad q^{\sum_{k=0}^{n-1} k} \cdot \prod_{k=1}^{n} (q^k - 1) \quad =$$

$$q^{\frac{1}{2}(n-1)n} \prod_{k=1}^{n} (q^k - 1) \quad = \quad q^{\binom{n}{2}} \prod_{k=1}^{n} (q^k - 1)$$

Wahlmöglichkeiten, und somit ist diese Anzahl die Ordnung der Gruppe G.

zu (b) Da q eine Potenz von p mit $q > 1$ ist, gibt es ein $r \in \mathbb{N}$ mit $q = p^r$. Nach Definition sind die p-Sylowgruppen von G genau die Untergruppen der Ordnung p^s von G, wobei $s \in \mathbb{N}_0$ die maximale Zahl mit $p^s \mid |G|$ bezeichnet. Wegen $p \mid q^k$ gilt jeweils $p \nmid (q^k - 1)$ für $1 \leq k \leq n$. $|G| = q^{\binom{n}{2}} \prod_{k=1}^{n} (q^k - 1)$ und $q^{\binom{n}{2}} = (p^r)^{\binom{n}{2}} = p^{r\binom{n}{2}}$ ist somit $s = r\binom{n}{2}$ der maximale Exponent mit $p^s \mid |G|$.

Die oberen Dreiecksmatrizen mit charakteristischem Polynom $(x - 1)^n$ sind genau die Matrizen $A = (a_{ij}) \in G$ mit $a_{ii} = \bar{1}$ für $1 \leq i \leq n$, $a_{ij} \in \mathbb{F}_q$ für $i < j$ und $a_{ij} = \bar{0}$ für $i > j$. Weil es genau $\binom{n}{2}$ Paare (i, j) mit $1 \leq i < j \leq n$ gibt, ist $q^{\binom{n}{2}} = p^{r\binom{n}{2}} = p^s$ die Anzahl dieser Dreiecksmatrizen. Wenn wir also zeigen können, dass die oberen Dreickecksmatrizen mit ausschließlich $\bar{1}$-en auf der Hauptdiagonale eine Untergruppe von G bilden, dann handelt es sich um eine p-Sylowgruppe von G.

Sei $U \subseteq G$ die Teilmenge dieser Matrizen. Offenbar ist die Einheitsmatrix in U enthalten. Seien nun $A, B \in U$ vorgegeben, mit $A = (a_{ij})$ und $B = (b_{ij})$. Wir müssen überprüfen, dass $C = (c_{ij}) = AB$ in U liegt. Für $i \in \{1, ..., n\}$. Für $k < i$ gilt $a_{ik} = \bar{0}$, und für $k > i$ gilt $b_{ki} = \bar{0}$. Daraus folgt

$$\begin{aligned} c_{ii} \quad &= \quad \sum_{k=1}^{n} a_{ik} b_{ki} \quad = \quad \sum_{k=1}^{i-1} a_{ik} b_{ki} + a_{ii} b_{ii} + \sum_{k=i+1}^{n} a_{ik} b_{ki} \quad = \\ & \sum_{k=1}^{i-1} \bar{0} \cdot b_{ki} + \bar{1} \cdot \bar{1} + \sum_{k=i+1}^{n} a_{ik} \cdot \bar{0} \quad = \quad \bar{1}. \end{aligned}$$

Seien nun $i, j \in \{1, ..., n\}$ mit $i > j$. Dann gilt $a_{ik} = \bar{0}$ für $k < i$ und $b_{kj} = \bar{0}$ für $k \geq i > j$, und somit

$$c_{ij} \quad = \quad \sum_{k=1}^{n} a_{ik} b_{kj} \quad = \quad \sum_{k=1}^{i-1} a_{ik} b_{kj} + \sum_{k=i}^{n} a_{ik} b_{kj} \quad = \quad \sum_{k=1}^{i-1} \bar{0} \cdot b_{kj} + \sum_{k=i}^{n} a_{ik} \cdot \bar{0} \quad = \quad \bar{0}.$$

Damit ist insgesamt $C \in U$ nachgewiesen. Mit A liegt auch A^{-1} in U. Weil nämlich G eine endliche Gruppe ist, gilt $A^{|G|} = I_n$, wobei I_n die Einheitsmatrix bezeichnet. Daraus folgt $A^{-1} = I_n A^{-1} = A^{|G|} A^{-1} = A^{|G|-1}$, und da wir bereits gezeigt haben, dass U unter Multiplikation abgeschlossen ist, ist $A^{|G|-1}$ ein Element aus U. Insgesamt ist damit die Untergruppen-Eigenschaft von U nachgewiesen.