Aufgabe H12T1A1 (6 Punkte)

Sei p eine Primzahl und $q = p^\ell$ für ein $\ell > 0$ ($\ell \in \mathbb{N}$). Sei $\mathbb{F}_q$ der endliche Körper mit q Elementen.

(a) Zeigen Sie, dass die Gruppe $G = \mathrm{SL}_2(\mathbb{F}_q)$ der 2×2-Matrizen mit Einträgen in $\mathbb{F}_q$ und Determinante 1 die Ordnung $q(q^2-1)$ hat.

Wir betrachten nun in G die Untergruppen

$$B \quad = \quad \left\{ \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \in G \;\middle|\; a \in \mathbb{F}_q^\times \;,\; b \in \mathbb{F}_q \right\}$$

und

$$N^- \quad = \quad \left\{ \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix} \in G \;\middle|\; a \in \mathbb{F}_q \right\}.$$

(b) Sei $\Omega = G/B$ die Menge der Linksnebenklassen von G bzgl. B. Bestimmen Sie die Ordnungen von N^- und B und die Anzahl $|\Omega|$ der Elemente von Ω.

(c) Die Gruppe N^- operiert auf Ω durch Multiplikation von links. Zeigen Sie, dass diese Operation einen Fixpunkt besitzt.

Lösung:

zu (a) Zunächst bestimmen wir die Ordnung der Gruppe $\mathrm{GL}_2(\mathbb{F}_q)$. Eine Matrix $A = (v, w)$ bestehend aus zwei Spaltenvektoren $v, w \in \mathbb{F}_q^2$ ist genau dann in $\mathrm{GL}_2(\mathbb{F}_q)$ enthalten, wenn die Vektoren v, w linear unabhängig sind (oder wegen $\dim \mathbb{F}_q^2 = 2$ gleichbedeutend, eine Basis von $\mathbb{F}_q^2$ als $\mathbb{F}_q$-Vektorraum bilden). Für v kann jeder Vektor außerdem dem Nullvektor $0_{\mathbb{F}_q^2}$ gewählt werden, hierfür gibt es $|\mathbb{F}_q^2 \backslash \{0_{\mathbb{F}_q^2}\}| = q^2-1$ Möglichkeiten. Ist v bereits gewählt, so ist (v, w) genau dann linear unabhängig, wenn w in $\mathbb{F}_q^2 \setminus \mathrm{lin}(v)$ gilt. Wegen $|\mathrm{lin}(v)| = q$ gibt es also $|\mathbb{F}_q^2 \setminus \mathrm{lin}(v)| = q^2 - q$ Möglichkeiten, den Vektor w zu wählen. Insgesamt gibt es also $(q^2-1)(q^2-q) = q(q-1)(q^2-1)$ Möglichkeiten für das Paar (v, w), folglich ist $(q^2-1)(q^2-q) = q(q-1)(q^2-1)$ die Ordnung von $\mathrm{GL}_2(\mathbb{F}_q)$.

Um die Ordnung von $G = \mathrm{SL}_2(\mathbb{F}_q)$ zu bestimmen, wenden wir den Homomorphiesatz auf die Abbildung $\det : \mathrm{GL}_2(\mathbb{F}_q) \to \mathbb{F}_q^\times$ an. Wegen $\det(AB) = \det(A)\det(B)$ ist für alle $A, B \in \mathrm{GL}_2(\mathbb{F}_q)$ ist dies ein Homomorphismus von Gruppen. Dieser ist surjektiv, denn für vorgegebenes $a \in \mathbb{F}_q^\times$ gilt

$$\begin{pmatrix} a & \bar{0} & \bar{0} & \bar{1} \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_q) \qquad \text{und} \qquad \det \begin{pmatrix} a & \bar{0} & \bar{0} & \bar{1} \end{pmatrix} = a.$$

Weil $\bar{1}$ das Neutralelement von $\mathbb{F}_q^\times$ ist, gilt für alle $A \in \mathrm{GL}_2(\mathbb{F}_q)$ die Äquivalenz $A \in \ker(\det) \Leftrightarrow \det(A) = \bar{1} \Leftrightarrow A \in G$. Damit sind alle Voraussetzungen des Homomorphiesatzes überprüft. Wir erhalten einen Isomorphismus $\mathrm{GL}_2(\mathbb{F}_q)/G \cong \mathbb{F}_q^\times$ und somit die Gleichung $|\mathrm{GL}_2(\mathbb{F}_q)|/|G| = |\mathbb{F}_q^\times| = q-1$. Daraus folgt

$$|G| \quad = \quad \frac{|\mathrm{GL}_2(\mathbb{F}_q)|}{|\mathbb{F}_q^\times|} \quad = \quad \frac{q(q-1)(q^2-1)}{q-1} \quad = \quad q(q^2-1).$$

zu (b) Die Anzahl der Elemente von N^- stimmt offenbar mit $|\mathbb{F}_q| = q$ überein, und $|B|$ ist gleich der Anzahl der Paare (a, b) mit $a \in \mathbb{F}_q^\times$ und $b \in \mathbb{F}_q$, also gleich $(q-1)q$. Die Mächtigkeit von $|\Omega|$ erhalten wir mit dem Satz von Lagrange: Es gilt

$$|\Omega| \quad = \quad (G : B) \quad = \quad \frac{|G|}{|B|} \quad = \quad \frac{q(q^2-1)}{(q-1)q} \quad = \quad \frac{q(q-1)(q+1)}{(q-1)q} \quad = \quad q+1.$$

zu (c) Sei $F \subseteq \Omega$ die Fixpunktmenge der Operation, und sei $R \subseteq \Omega$ ein Repräsentantensystem der Bahnen mit mehr als einem Element. Auf Grund der Bahngleichung für Gruppenoperationen gilt

$$|\Omega| \quad = \quad |F| + \sum_{x \in R} (N_- : (N_-)_x).$$

Wegen $|N_-| = q = p^\ell$ und $(N_- : (N_-)_x) = |N_-(x)| > 1$ für $x \in R$ ist jeder Summand $(N_- : (N_-)_x)$ eine p-Potenz größer als 1 und insbesondere durch p teilbar. Auch $\sum_{x \in R}(N_- : (N_-)_x)$ ist somit durch p teilbar. Wäre $F = \varnothing$, so würde die Gleichung auch die Teilbarkeit von $|\Omega|$ durch p liefern. Aber wegen $|\Omega| = q + 1 = p^\ell + 1$ sind p und $|\Omega|$ teilerfremd, denn jeder gemeinsame Teiler $d \in \mathbb{N}$ von $p^\ell + 1$ und p ist auch ein Teiler von $(p^\ell + 1) + (-p^{\ell-1})p = 1$. Also ist die Menge F der Fixpunkte nicht leer.