F25-T2-A5

Sei p eine Primzahl und sei $\mathbb{F}_p$ der endliche Körper mit p Elementen. Sei weiter

$$G = \left\{ \begin{pmatrix} a & 0 \\ b & a \end{pmatrix} \mid a \in \mathbb{F}_p^\times, b \in \mathbb{F}_p \right\}.$$

Zeigen Sie:

a) Die Menge G ist eine Untergruppe von $\mathrm{GL}_2(\mathbb{F}_p)$.

b) Die Gruppe G enthält eine zyklische Untergruppe H_{p-1} der Ordnung $p-1$ und eine zyklische Untergruppe der Ordnung p.

c) Die Gruppe G ist zyklisch.

Lösung

a) Wir zeigen, dass G eine Untergruppe von $\mathrm{GL}_2(\mathbb{F}_p)$ ist.

- $\mathrm{id} \in G$ ist klar mir $a = 1, b = 0$;
- Seien $M = \begin{pmatrix} a & 0 \\ b & a \end{pmatrix}$ und $M' = \begin{pmatrix} a' & 0 \\ b' & a' \end{pmatrix}$ Elemente von G. Es gilt $MM' = \begin{pmatrix} aa' & 0 \\ a'b + ab' & aa' \end{pmatrix}$. MM' ist in G, da $aa' \in \mathbb{F}_p^\times$ und $a'b + ab' \in \mathbb{F}_p$;
- Für M wie oben ist $M^{-1} = \frac{1}{a^2} \begin{pmatrix} a & 0 \\ -b & a \end{pmatrix} = \begin{pmatrix} \frac{1}{a} & 0 \\ \frac{-b}{a^2} & \frac{1}{a} \end{pmatrix} \in G$.

b) Wir betrachten $H_{p-1} = \left\{ a \cdot \mathrm{id} \mid a \in \mathbb{F}_p^\times \right\}$ sowie $H_p = \left\{ \begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix} \mid b \in \mathbb{F}_p \right\}$. Man zeigt nun, dass H_{p-1} und H_p die gewünschten Eigenschaften erfüllen. Das beide Mengen Untergruppen von G sind, überlasse dem Leser. Wir zeigen, dass H_{p-1} und H_p zyklisch sind. H_{p-1} ist zyklisch, da $\mathbb{F}_p^\times$ zyklisch ist. Sei dazu a ein Erzeuger von $\mathbb{F}_p^\times$, und $b \in \mathbb{F}_p^\times$ beliebig. Dann gibt es ein $k \in \mathbb{Z}$ sodas $b = a^k$. Demnach ist auch $b \cdot \mathrm{id} = (a \cdot \mathrm{id})^k$.
Für die Untergruppe H_p bemerkt man, dass $\begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ b+c & 1 \end{pmatrix}$. Da $\mathbb{F}_p$ additiv durch 1 erzeugt wird, folgt $H_p = \langle \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \rangle$. Das die beiden zyklischen Gruppen jetzt jeweils die besagte Ordnung haben folgt leicht mit obigem.

c) $H_{p-1} \cap H_p = \{\mathrm{id}\}$. Wir betrachten $H_{p-1} \cdot H_p$. Sei $a\mathrm{id} \in H_{p-1}$ und $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^k \in H_p$. Dann gilt $a \cdot \mathrm{id} \cdot \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^k = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^k \cdot a \cdot \mathrm{id}$. Daraus folgern wir, dass $H_{p-1} \cdot H_p$ eine Untergruppe von G ist. Betrachtet man die Abbildung

$$\phi : H_{p-1} \cdot H_p \to H_{p-1} \times H_p, \quad a \cdot \mathrm{id} \cdot \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^k \mapsto \left(a \cdot \mathrm{id}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^k \right)$$

und verwendet, dass $H_{p-1} \cap H_p = \{\mathrm{id}\}$, so zeigt man leicht (siehe Skript und selber nachrechnen), dass ϕ ein Ismorphismus ist. Da $H_{p-1} \times H_p$ genauso viele Elemente wie G hat, und $H_{p-1} \cdot H_p$ eine Untergruppe von G ist, folgt

$$G = H_{p-1} \cdot H_p \cong H_{p-1} \times H_p \cong \mathbb{Z}/p-1\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}/p \cdot (p-1)\mathbb{Z}.$$

Der letzte Isomorphismus ist der chinesische Restsatz, den man hier anwenden kann, denn es gilt $\mathrm{ggT}(p, p-1) = 1$.