F24-T3-A3

Für eine Primzahl p sei $\mathbb{F}_p$ der endliche Körper mit $|\mathbb{F}_p| = p$; weiter sei $R := \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \mid a, b \in \mathbb{F}_p \right\}$.

a) Zeigen Sie, dass R ein Teilring des Ringes der 2×2- Matrizen über $\mathbb{F}_p$ ist.

b) Zeigen Sie, dass die Einheitengruppe $R^\times$ im Fall $p \neq 2$ nicht einfach ist.

c) Nun sei $p = 257$. Entscheiden Sie begründet, ob die Einheitengruppe $R^\times$ in diesem Fall auflösbar ist.

Lösung

a) Man sieht schnell, dass die 0- und die Einheitsmatrix in R sind. Seien nun $A = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$ und $B = \begin{pmatrix} c & d \\ 0 & c \end{pmatrix} \in R$, dann ist $A + B = \begin{pmatrix} a+c & b+d \\ 0 & a+c \end{pmatrix} \in R$ und $AB = \begin{pmatrix} ac & ad+bc \\ 0 & ac \end{pmatrix} \in R$. Somit ist R ein Teilreing.

b) Wir betrachten $S = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid a \in \mathbb{F}_p^\times \right\}$. Man sieht leicht ein, dass $S \subset R^\times$, denn $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \cdot \begin{pmatrix} a^{-1} & 0 \\ 0 & a^{-1} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Es gilt zudem $\{0\} \subsetneq S \subsetneq R^\times$ für $p \neq 2$, da $R^\times = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \mid a, b \in \mathbb{F}_p, a^2 \neq 0 \right\}$ und somit $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in R^\times \setminus S$. Da $p \neq 2$ ist $S \neq \{0\}$. Wir wollen nun zeigen, dass $S \lhd R^\times$ (Normalteiler) gilt. Sei dazu $A \in R^\times, B \in S$ beliebig, es folgt aus $A \in R^\times$ mit $A = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$ dass $A^{-1} = \frac{1}{a^2} \begin{pmatrix} a & -b \\ 0 & a \end{pmatrix}$. Sei nun $C = \begin{pmatrix} c & 0 \\ 0 & c \end{pmatrix}$, dann gilt

$$ACA^{-1} = \frac{1}{a^2} \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \begin{pmatrix} c & 0 \\ 0 & c \end{pmatrix} \begin{pmatrix} a & -b \\ 0 & a \end{pmatrix} = \begin{pmatrix} c & 0 \\ 0 & c \end{pmatrix} \in S.$$

Demnach gilt $S \lhd R$. Und somit ist R nicht einfach.

c) Zunächst bemerkt man $257 \neq 2$. Wir können also S aus Teilaufgabe b) benutzen. Wir haben also einen Normalteiler gefunden von $R^\times$. Dieser ist auflösbar, da S eine abelsche Gruppe bezüglich der Multiplikation ist (einfach ausprobieren). Wir betrachten jetzt die Gruppe $R^\times/S$. Man sieht leicht, dass S 256 Elemente hat. Wie viele Elemente hat $R^\times$? a darf nicht 0 sein, sonst haben wir für a, b freie Wahl, also $\#R^\times = 257 \cdot 256 = 65792$. Jetzt hat $R^\times/S$ genau $\frac{65792}{256} = 257$ Elemente. Damit ist das eine Gruppe von Primzahlordnung und somit auch abelsch und damit auch auflösbar. Also sind $R^\times/S$ und S auflösbar und demnach auch $R^\times$ (Satz, siehe Skript).

Alternative Lösung zu b) und c) Man kann sich das Leben sehr viel einfacher machen, indem man feststellt, dass $R^\times$ abelsch ist. Es gilt nämlich $AB = \begin{pmatrix} ac & ad+bc \\ 0 & ac \end{pmatrix} = BA$ (kurz nachrechnen). $R^\times$ ist deshalb eine abelsche Gruppe mit $p(p-1)$ Elementen (für b kann man jedes Element in $\mathbb{F}_p$ wählen, für a alle außer 0, da $\mathbb{F}_p$ ein Körper ist). Demnach kann $R^\times$ nicht einfach sein für $p \neq 2$, da es stets eine nichttriviale Untergruppe (z.B. mit Hauptsatz über endliche abelsche Gruppen) und damit einen Normalteiler (da abelsch) gibt. Auch die c) ist jetzt gleich erledigt, da abelsche Gruppen immer auflösbar sind.