

H24 T1A-1 (Fortsetzung)

Bereits gezeigt: $H = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in M_{2, \mathbb{R}} \mid a^2 + b^2 \neq 0 \right\}$ ist Untergr. von $GL_2(\mathbb{R})$

zu (b) geg. $A, B, C \in H$

z.zg. Die Gleichung $A \cdot Y \cdot B = C$ ist in H eindeutig lösbar.

Beh. i) $Y_1 = A^{-1} C B^{-1}$ ist eine Lösung der Gleichung in H .

(ii) Ist $Y_2 \in H$ eine weitere Lsg.,
dann folgt $Y_1 = Y_2$.

zu (i) Da H eine Untergr. von $GL_2(\mathbb{R})$ ist
sind mit A, B auch A^{-1}, B^{-1} in H ent-
halten. Wegen $C \in H$ folgt weiter $CB^{-1} \in H$
und schließlich $Y_1 = A^{-1}CB^{-1} \in H$.

Das Element ist eine Lösung der
Gleichung, denn: $AY_1B = A(A^{-1}CB^{-1})B$
 $= (AA^{-1})C(B^{-1}B) = E_2CE_2 = C.$

zu ii) Y_2 ist Lsg. der Gleichung $\Rightarrow$

$$A Y_2 B = C \Rightarrow A^{-1}(A Y_2 B) B^{-1} = A^{-1} C B^{-1} \\ \Rightarrow Y_2 = A^{-1} C B^{-1} = Y_1.$$

ist
ent-
 $\in M$
zu (c) gesucht: Lsg von $\begin{pmatrix} 4 & 3 \\ -3 & 4 \end{pmatrix} Y \begin{pmatrix} 6 & 2 \\ -2 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 3 \\ -3 & 1 \end{pmatrix}$ in M

Wende die Lösungsformel aus Teil (b) an auf

$$A = \begin{pmatrix} 4 & 3 \\ -3 & 4 \end{pmatrix}, B = \begin{pmatrix} 6 & 2 \\ -2 & 6 \end{pmatrix}, C = \begin{pmatrix} 1 & 3 \\ -3 & 1 \end{pmatrix}$$

$$A^{-1} = \frac{1}{25} \begin{pmatrix} 4 & -3 \\ 3 & 4 \end{pmatrix}, B^{-1} = \frac{1}{40} \begin{pmatrix} 6 & -2 \\ 2 & 6 \end{pmatrix}$$

$$A^{-1} \subset B^{-1} = \frac{1}{1000} \begin{pmatrix} 4 & -3 \\ 3 & 4 \end{pmatrix} \begin{pmatrix} 1 & 3 \\ -3 & 1 \end{pmatrix} \begin{pmatrix} 6 & -2 \\ 2 & 6 \end{pmatrix} =$$

$$\frac{1}{1000} \begin{pmatrix} 13 & 9 \\ -9 & 13 \end{pmatrix} \begin{pmatrix} 6 & -2 \\ 2 & 6 \end{pmatrix} = \frac{1}{1000} \begin{pmatrix} 96 & 28 \\ -28 & 96 \end{pmatrix} = \frac{1}{250} \begin{pmatrix} 24 & 7 \\ -7 & 24 \end{pmatrix}$$

Erinnerung: Ist G eine Gruppe, dann ist ein Normalteiler ^(*) von G eine Untergruppe N mit der zusätzlichen Eigenschaft $\forall g \in G: gN = Ng$
 äquivalente Bedingung: ^(*) Notation:

$$\forall g \in G: gNg^{-1} \subseteq N \quad N \trianglelefteq G$$

zu (ii) γ_2 ist Lsg. der Gleichung $\Rightarrow$

Bem. (i) G abelsch $\Rightarrow$ jede Untergruppe
ist Normalteiler.

(Die Umkehrung ist falsch. Ein Gegenbeispiel ist
die achtelementige Quaternionengruppe Q_8)

(ii) $U \leq G, (G:U) = 2 \Rightarrow U \trianglelefteq G$

Jede Gruppe G hat die trivialen
Normalteiler $\{e\}$ und G . Eine
Gruppe $G \neq \{e\}$, bei der das die
einzigen Normalteiler sind, heißt einfach.

(iii) Ist $\phi: G \rightarrow H$ ein Gruppenhom.,
dann gilt $\ker(\phi) \trianglelefteq G$.

H22T1A1 (b) geg.: die Gruppe

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in M_{2, \mathbb{Q}} \mid ac \neq 0 \right\}$$

und die Teilmenge $U = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in G \mid b=0 \right\}$
 $= \left\{ \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} \mid ac \neq 0 \right\}$ Zeige:

- (i) U ist Untergruppe von G
- (ii) U ist kein Normalteiler von G

zu (i) Übung

zu (ii) ges.: ein $A \in G$ mit $AUA^{-1} \notin U$

Es reicht, dafür Elemente $A \in G$
und $B \in U$ zu finden mit $ABA^{-1} \notin U$.

Betrachte $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$.

Dann gilt $A \in G$, $B \in U$.

$$A^{-1} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}, \quad ABA^{-1} =$$

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \\ = \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix} \notin U. \quad \square$$

M24T3A1

(a) Sei K ein Körper und

$$G(K) = \left\{ \begin{pmatrix} 1 & 0 & a \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \mid a, b \in K \right\}$$

Zeigen Sie, dass $G(K)$ eine
abelsche Untergruppe von $GL_3(K)$ ist.

Für beliebige $a, b, c, d \in K$
gilt

$$\begin{pmatrix} 1 & 0 & a \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & c \\ 0 & 1 & d \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & a+c \\ 0 & 1 & b+d \\ 0 & 0 & 1 \end{pmatrix}$$

Rest als Übung

(b) Stellen Sie $G(\mathbb{F}_p)$ als
direktes Produkt von Gruppen
der Form $\mathbb{Z}/m\mathbb{Z}$ mit $m \in \mathbb{N}$
dar, wobei p eine Primzahl bezeichnet.

$$\text{Ind.-Auf: } \begin{pmatrix} 1 & 0 & a \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & a \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 \cdot a \\ 0 & 1 & 1 \cdot b \\ 0 & 0 & 1 \end{pmatrix}$$

Hauptsatz über endliche abelsche Gruppen $\Rightarrow$ Es gibt ein $r \in \mathbb{N}_0$ und Primzahlpotenzen $q_1, \dots, q_r > 1$ mit $G(\mathbb{F}_p) \cong \mathbb{Z}/q_1\mathbb{Z} \times \dots \times \mathbb{Z}/q_r\mathbb{Z}$, wobei $q_1 \cdot \dots \cdot q_r = |G(\mathbb{F}_p)|$.

Die Abb. $\mathbb{F}_p^2 \rightarrow G(\mathbb{F}_p), (a, b) \mapsto \begin{pmatrix} 1 & 0 & a \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}$ ist offenbar bijektiv. $\Rightarrow |G(\mathbb{F}_p)| = |\mathbb{F}_p^2| = p^2$

$\Rightarrow$ einzige Möglichkeiten: (i) $r=1, q_1 = p^2$
 (ii) $r=2, q_1 = q_2 = p$

also: $G(\mathbb{F}_p) \cong \mathbb{Z}/p^2\mathbb{Z}$ oder $G(\mathbb{F}_p) \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$

Erinnerung: Die Ordnung eines Gruppenelements $g \in G$ ist definiert durch $\text{ord}(g) = |\langle g \rangle|$.

Ist $\text{ord}(g)$ endlich, dann ist dies die kleinste Zahl $n \in \mathbb{N}$ mit $g^n = e_G$.

Beh.: Für alle $a, b \in \mathbb{F}_p$ und alle $n \in \mathbb{N}$ gilt

$$\begin{pmatrix} \overline{1} & \overline{0} & a \\ \overline{0} & \overline{1} & b \\ \overline{0} & \overline{0} & \overline{1} \end{pmatrix}^n = \begin{pmatrix} \overline{1} & \overline{0} & na \\ \overline{0} & \overline{1} & nb \\ \overline{0} & \overline{0} & \overline{1} \end{pmatrix}$$

Seien $a, b \in \mathbb{F}_p$. Beweise die Gleichung durch vollständ.

Ind. über n . Ind.-Auf: $\begin{pmatrix} \overline{1} & \overline{0} & a \\ \overline{0} & \overline{1} & b \\ \overline{0} & \overline{0} & \overline{1} \end{pmatrix}^1 = \begin{pmatrix} \overline{1} & \overline{0} & a \\ \overline{0} & \overline{1} & b \\ \overline{0} & \overline{0} & \overline{1} \end{pmatrix} = \begin{pmatrix} \overline{1} & \overline{0} & 1 \cdot a \\ \overline{0} & \overline{1} & 1 \cdot b \\ \overline{0} & \overline{0} & \overline{1} \end{pmatrix}$

Ind. - Schritt :

$$\begin{pmatrix} \overline{1} & \overline{0} & a \\ \overline{0} & \overline{1} & b \\ \overline{0} & \overline{0} & \overline{1} \end{pmatrix}^{n+1} = \begin{pmatrix} \overline{1} & \overline{0} & a \\ \overline{0} & \overline{1} & b \\ \overline{0} & \overline{0} & \overline{1} \end{pmatrix}^n \begin{pmatrix} \overline{1} & \overline{0} & a \\ \overline{0} & \overline{1} & b \\ \overline{0} & \overline{0} & \overline{1} \end{pmatrix}$$

$$\begin{aligned} \text{Ind. - V.} \quad & \begin{pmatrix} \overline{1} & \overline{0} & na \\ \overline{0} & \overline{1} & nb \\ \overline{0} & \overline{0} & \overline{1} \end{pmatrix} \begin{pmatrix} \overline{1} & \overline{0} & a \\ \overline{0} & \overline{1} & b \\ \overline{0} & \overline{0} & \overline{1} \end{pmatrix} = \\ & = \begin{pmatrix} \overline{1} & \overline{0} & (n+1)a \\ \overline{0} & \overline{1} & (n+1)b \\ \overline{0} & \overline{0} & \overline{1} \end{pmatrix} \quad (\Rightarrow \text{Beh}) \end{aligned}$$

Auf Grund der soeben bewiesenen
Formel gilt für alle $a, b \in \mathbb{F}_p$

$$\text{jeweils } \begin{pmatrix} \overline{1} & \overline{0} & a \\ \overline{0} & \overline{1} & b \\ \overline{0} & \overline{0} & \overline{1} \end{pmatrix}^p = \begin{pmatrix} \overline{1} & \overline{0} & pa \\ \overline{0} & \overline{1} & pb \\ \overline{0} & \overline{0} & \overline{1} \end{pmatrix} =$$

$$\begin{pmatrix} \overline{1} & \overline{0} & \overline{0} \\ \overline{0} & \overline{1} & \overline{0} \\ \overline{0} & \overline{0} & \overline{1} \end{pmatrix} \Rightarrow \text{Alle Elemente in } G(\mathbb{F}_p)$$

haben eine Ordnung $\leq p$.

In der Gruppe $\mathbb{Z}/p^2\mathbb{Z}$ ist $\overline{1}$ aber ein
Element der Ordnung $p^2 > p$. $\Rightarrow$

$G(\mathbb{F}_p) \cong \mathbb{Z}/p^2\mathbb{Z}$ ausgeschlossen $\Rightarrow$ ein-

zige Möglichkeit: $G(\mathbb{F}_p) \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$

Bem. Anstatt mit dem Hauptsatz über endliche abelsche Gruppen zu arbeiten,

hätte man auch überprüfen können, dass die Abbildung

$$\phi: \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \rightarrow G(\mathbb{F}_p),$$

$$(a, b) \mapsto \begin{pmatrix} 1 & 0 & a \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \text{ ein}$$

Isomorphismus von Gruppen ist.

dafür zu überprüfen:

ii) Homomorphismus-Eigenschaft:

Für alle $a, b, c, d \in \mathbb{Z}/p\mathbb{Z}$ gilt

$$\phi((a, b) + (c, d)) = \phi(a, b) \cdot \phi(c, d)$$

$$\text{iii) } \ker(\phi) = (\bar{0}, \bar{0})$$

iii) Surjektivität von ϕ (Übung)

c) Stellen Sie auch die Gruppe $G(\mathbb{F}_p^2)$ als direktes Produkt von Gruppen der Form $\mathbb{Z}/m\mathbb{Z}$ mit $m \in \mathbb{N}$ dar.

Da $\text{char}(\mathbb{F}_p^2) = p$ ist, zeigt dieselbe Rechnung wie in Teil (b), dass für alle

$\mathbb{Z}/p\mathbb{Z}$

$\Rightarrow$ über
seiten.

nen,

)

x

ist.

$$a, b \in \mathbb{F}_{p^2} \text{ jeweils } \begin{pmatrix} 1 & 0 & a \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}^p = \begin{pmatrix} 1 & 0 & pa \\ 0 & 1 & pb \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ gilt.}$$

Auch in $G(\mathbb{F}_{p^2})$ gibt es nur Elemente der Ordnung $\leq p$. Hauptsatz über abelsche Gruppen, $|G(\mathbb{F}_{p^2})| = |\mathbb{F}_{p^2}^2| = (p^2)^2 = p^4 \Rightarrow \exists r \in \mathbb{N}_0$

und $l_1, \dots, l_r \in \mathbb{N}$ mit

$$G(\mathbb{F}_{p^2}) \cong \mathbb{Z}/p^{l_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p^{l_r}\mathbb{Z}$$

$$\text{und } l_1 + \dots + l_r = 4.$$

Da es für jedes $j \in \{1, \dots, r\}$ in dieser Gruppe ein Element der Ordnung p gibt (nämlich $(\bar{0}, \bar{0}, \dots, \bar{0}, \bar{1}, \bar{0}, \dots, \bar{0})$ mit 1 an der j -ten Stelle), andererseits aber alle Elementordnungen $\leq p$ sind, ist die einzige Mögl. $r=4, l_1=l_2=l_3=l_4=1$ also: $G(\mathbb{F}_{p^2}) \cong (\mathbb{Z}/p\mathbb{Z})^4$. $\square$

dieselbe
für alle