H25T3A2 (Forts.)

geg: $G = \left\{ \begin{pmatrix} \overline{1} & a & b \\ \overline{0} & \overline{1} & c \\ \overline{0} & \overline{0} & \overline{1} \end{pmatrix} \;\middle|\; a, b, c \in \mathbb{F}_3 \right\}$

zu (a) bereits gezeigt: G ist Gruppe, $|G| = 27$

noch z.zg: G ist nicht abelsch

Sei $A = \begin{pmatrix} \overline{1} & \overline{1} & \overline{0} \\ \overline{0} & \overline{1} & \overline{0} \\ \overline{0} & \overline{0} & \overline{1} \end{pmatrix}$, $B = \begin{pmatrix} \overline{1} & \overline{0} & \overline{0} \\ \overline{0} & \overline{1} & \overline{1} \\ \overline{0} & \overline{0} & \overline{1} \end{pmatrix}$. Dann ist

$$AB = \begin{pmatrix} \overline{1} & \overline{1} & \overline{0} \\ \overline{0} & \overline{1} & \overline{0} \\ \overline{0} & \overline{0} & \overline{1} \end{pmatrix} \begin{pmatrix} \overline{1} & \overline{0} & \overline{0} \\ \overline{0} & \overline{1} & \overline{1} \\ \overline{0} & \overline{0} & \overline{1} \end{pmatrix} = \begin{pmatrix} \overline{1} & \overline{1} & \overline{0} \\ \overline{0} & \overline{1} & \overline{1} \\ \overline{0} & \overline{0} & \overline{1} \end{pmatrix} \text{ und}$$

$$BA = \begin{pmatrix} \bar{1} & \bar{0} & \bar{0} \\ \bar{0} & \bar{1} & \bar{1} \\ \bar{0} & \bar{0} & \bar{1} \end{pmatrix} \begin{pmatrix} \bar{1} & \bar{1} & \bar{0} \\ \bar{0} & \bar{1} & \bar{0} \\ \bar{0} & \bar{0} & \bar{1} \end{pmatrix} = \begin{pmatrix} \bar{1} & \bar{0} & \bar{0} \\ \bar{0} & \bar{1} & \bar{1} \\ \bar{0} & \bar{0} & \bar{1} \end{pmatrix}$$ Es gilt also

$AB \neq BA$, somit ist G nicht abelsch.

(Man kann leicht zeigen, dass alle Elemente außer dem Neutralelement die Ordnung 3 haben. Die Gruppe $H = (\mathbb{Z}/3\mathbb{Z})^3$ hat dieselbe Eigenschaft. Aber G und H sind nicht isomorph, da G nicht-abelsch und H abelsch ist.)

zu (b) ges. 12 paarweise nicht-isomorphe Gruppen der Ordnung $2025 = 3^4 \cdot 5^2$ $(2 = 1+1$, $4 = 3+1 = 2+2 = 2+1+1 = 1+1+1+1)$

Der Hauptsatz über abelsche Gruppen liefert die folgenden abelschen Gruppen der Ordnung 2025:

$G_1 = \mathbb{Z}/3^4\mathbb{Z} \times \mathbb{Z}/5^2\mathbb{Z}$ (zyklisch), $G_2 = \mathbb{Z}/3^3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5^2\mathbb{Z}$,

$G_3 = (\mathbb{Z}/3^2\mathbb{Z})^2 \times \mathbb{Z}/5^2\mathbb{Z}$, $G_4 = \mathbb{Z}/3^2\mathbb{Z} \times (\mathbb{Z}/3\mathbb{Z})^2 \times \mathbb{Z}/5^2\mathbb{Z}$,

$G_5 = (\mathbb{Z}/3\mathbb{Z})^4 \times \mathbb{Z}/5^2\mathbb{Z}$, $G_6 = \mathbb{Z}/3^4\mathbb{Z} \times (\mathbb{Z}/5\mathbb{Z})^2$,

$G_7 = \mathbb{Z}/3^3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times (\mathbb{Z}/5\mathbb{Z})^2$, $G_8 = (\mathbb{Z}/3^2\mathbb{Z})^2 \times (\mathbb{Z}/5\mathbb{Z})^2$,

$G_9 = \mathbb{Z}/3^2\mathbb{Z} \times (\mathbb{Z}/3\mathbb{Z})^2 \times (\mathbb{Z}/5\mathbb{Z})^2$, $G_{10} = (\mathbb{Z}/3\mathbb{Z})^4 \times (\mathbb{Z}/5\mathbb{Z})^2$

Außerdem gibt es noch $G_{11} = G \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}$ und $G_{12} = G \times \mathbb{Z}/3\mathbb{Z} \times (\mathbb{Z}/5\mathbb{Z})^2$ mit der Gruppe G aus Teil (a). Die Gruppen G_{11}, G_{12} sind nicht abelsch, weil G nicht abelsch ist.

z.zg: Die Gruppen $G_1, \dots, G_{12}$ sind paarweise nicht isomorph.

Die Gruppen G_{11}, G_{12} sind zu keiner der Gruppen $G_1, \dots, G_{10}$ isomorph, da Erstere nicht abelsch, Letztere abelsch sind.

<u>Beh</u>: $G_{11} \ncong G_{12}$ In G_{11} gibt es mit $g = (E, \bar{0}, \bar{1})$ ein Element der Ordnung 25 (wobei E = Einheitsmatrix in $M_3, \mathbb{F}_3$), denn es gilt $g^k = (E^k, \bar{0}, \bar{k}) \neq (E, \bar{0}, \bar{0}) = e_{G_{11}}$ für $1 \leq k \leq 25$ und $g^{25} = (E^{25}, \bar{0}, \overline{25}) = (E, \bar{0}, \bar{0}) = e_{G_{11}}$. In G_{12} existiert

aber kein solches Element. Denn wegen
$|G| = 27$ gilt $A^{27} = E \ \forall A \in G$, und
daraus folgt $h^{135} = (\bar{A}, \bar{k}, \bar{a}, \bar{b})^{135}$

$$((A^{27})^5, \overline{135k}, \overline{135a}, \overline{135b}) = (E^5, \bar{0}, \bar{0}, \bar{0}) = e_{G_{12}}$$

$3 \mid 135$
$5 \mid 135$

für jedes Element $h \in G_{12}$ der Form
$h = (\bar{A}, \bar{k}, \bar{a}, \bar{b})$ mit $A \in G$ und
$\bar{k} \in \mathbb{Z}/3\mathbb{Z}$, $a, b \in \mathbb{Z}/5\mathbb{Z}$ ($\Rightarrow$ Beh.)

Genauso zeigt man, dass keine der Gruppen $G_1, \dots, G_5$ zu einer der Gruppen $G_6, \dots, G_{10}$ isomorph ist.

noch zu zeigen:

(b

Zu

C(

Es

Elem

keite

die a

$\cong \mathbb{Z}/$

Für a

$$\begin{pmatrix} \bar{1} & \bar{0} & a \\ \bar{0} & \bar{1} & b \\ \bar{0} & \bar{0} & \bar{1} \end{pmatrix}$$

$$\begin{pmatrix} \bar{1} & \bar{0} & a \\ \bar{0} & \bar{1} & b \\ \bar{0} & \bar{0} & \bar{1} \end{pmatrix}$$

Die Gruppen $G_1, \dots, G_5$ sind paarweise nicht isomorph, ebenso die Gruppen $G_6, \dots, G_{10}$.

Überprüfe dazu: Die Gruppen G_1, G_6 besitzen Element der Ordnung 81, aber keine der Gruppen $G_2, \dots, G_5, G_7, \dots, G_{10}$.

ebenso: G_2, G_7 sind zu keiner der Gruppen $G_3, G_4, G_5, G_8, G_9, G_{10}$ (wg. Elementen der Ordnung 27) und G_3, G_4, G_8, G_9 sind zu keiner der Gruppen G_5, G_{10} isomorph.

Es bleibt zu zeigen: $G_3 \not\cong G_4$ und $G_8 \cong G_9$

Bestimme dazu in den Gruppen G_3, G_4 die Anzahl der Elemente der Ordnung 3

Sei $g = (\bar{a}, \bar{b}, \bar{c}) \in G_3$ (mit $a, b \in \mathbb{Z}/9\mathbb{Z}$, $c \in \mathbb{Z}/3^2\mathbb{Z}$)

...ße

$G_6, \dots, G_{10}$.

besitzen

Gruppen

ruppen

...menten der

g sind zu

ph.

und $G_8 \cong G_9$

en G_3, G_4

Ordnung 3

$\in \mathbb{Z}/9\mathbb{Z}, c \in \mathbb{Z}/3^2\mathbb{Z}$

Dann gilt die Äquivalenz $3g = 0_{G_3} \Leftrightarrow$ $(\overline{3a}, \overline{3b}, \overline{3c}) = (\bar{0}, \bar{0}, \bar{0}) \Leftrightarrow a, b \in \{\bar{0}, \bar{3}, \bar{6}\}$, $c = \bar{0}$. Es gibt also $3 \cdot 3 \cdot 1 = 9$ Elemente der Ordnung 1 oder 3, somit genau 8 Elemente der Ordnung 3. Dieselbe Rechnung für G_4 zeigt, dass es dort 26 Elemente der Ordnung 3 gibt. $26 \neq 8 \Rightarrow G_3 \not\cong G_4$. Der Nachweis von $G_8 \not\cong G_9$ läuft analog. $\square$

H24T3A1 Für jeden Körper K sei

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

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

wegen
und
135
)
=
$= 3 \mid 135$
$5 \mid 135$
m
und
($\Rightarrow$ Beh.)
der
Gruppen
ch zu zeigen.

(b) Sei nun p eine Primzahl und $K = \mathbb{F}_p$. Zu welchem Produkt zyklischer Gruppen ist $G(\mathbb{F}_p)$ isomorph?

Es ist $|G(\mathbb{F}_p)| = p \cdot p = p^2$, da es für die Elemente $a, b \in \mathbb{F}_p$ jeweils p Wahlmöglichkeiten gibt. Aus dem Hauptsatz über endliche abelsche Gruppen folgt somit $G(\mathbb{F}_p) \cong \mathbb{Z}/p^2\mathbb{Z}$ oder $G(\mathbb{F}_p) \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Für alle $a, b \in \mathbb{F}_p$ gilt

$$\begin{pmatrix} \overline{1} & \overline{0} & a \\ \overline{0} & \overline{1} & b \\ \overline{0} & \overline{0} & \overline{1} \end{pmatrix} \begin{pmatrix} \overline{1} & \overline{0} & a \\ \overline{0} & \overline{1} & b \\ \overline{0} & \overline{0} & \overline{1} \end{pmatrix} = \begin{pmatrix} \overline{1} & \overline{0} & \overline{2}a \\ \overline{0} & \overline{1} & \overline{2}b \\ \overline{0} & \overline{0} & \overline{1} \end{pmatrix}.$$

<u>Beh.</u>:

$$\begin{pmatrix} \overline{1} & \overline{0} & a \\ \overline{0} & \overline{1} & b \\ \overline{0} & \overline{0} & \overline{1} \end{pmatrix}^k = \begin{pmatrix} \overline{1} & \overline{0} & \overline{k}a \\ \overline{0} & \overline{1} & \overline{k}b \\ \overline{0} & \overline{0} & \overline{1} \end{pmatrix} \quad \forall k \in \mathbb{N}_0$$

...ppe
...-1 der
...fen:
Gruppe
...lord-
...$)\,|\,a\in\mathbb{F}_p^\times\}$

Beweis durch vollständige Induktion (aus Zeitgründen weggelassen) Insb. gilt also $\begin{pmatrix}\bar{1}&\bar{0}&\bar{a}\\ \bar{0}&\bar{1}&\bar{b}\\ \bar{0}&\bar{0}&\bar{1}\end{pmatrix}^p = \begin{pmatrix}\bar{1}&\bar{0}&\overline{pa}\\ \bar{0}&\bar{1}&\overline{pb}\\ \bar{0}&\bar{0}&\bar{1}\end{pmatrix}$

$= \begin{pmatrix}\bar{1}&\bar{0}&\bar{0}\\ \bar{0}&\bar{1}&\bar{0}\\ \bar{0}&\bar{0}&\bar{1}\end{pmatrix} = e_{G(\mathbb{F}_p)}$, es gibt in $G(\mathbb{F}_p)$ also nur Elemente der Ordnung p, während es in $\mathbb{Z}/p^2\mathbb{Z}$ mit $\bar{1}$ ein Element der Ordnung p^2 gibt. Also gilt $G(\mathbb{F}_p) \not\cong \mathbb{Z}/p^2\mathbb{Z}$ und es folgt $G \cong (\mathbb{Z}/p\mathbb{Z})^2$.

(c) Zu welchem Produkt zyklischer Gruppen ist $G(\mathbb{F}_{p^2})$ isomorph?

Es gilt $|G(\mathbb{F}_{p^2})| = p^2 \cdot p^2 = p^4$, weil es für jedes der Elemente $a, b \in \mathbb{F}_{p^2}$ in der Matrix jeweils p^2 Wahlmögund es folgt $G \cong (\mathbb{Z}/p\mathbb{Z})^2$.

(c) Zu welchem Produkt zyklischer Gruppen ist $G(\mathbb{F}_{p^2})$

lichkeiten gilt. Hauptsatz über endl. abelsche Gruppen $\Rightarrow$ $G(\mathbb{F}_{p^2})$ ist isomorph zu einem Produkt zykl. Gruppen, wobei das Produkt der Ordnungen p^4 ist. $\Rightarrow$ $G(\mathbb{F}_{p^2})$ ist isomorph zu einer der fünf Gruppen $G_1 = \mathbb{Z}/p^4\mathbb{Z}$, $G_2 = \mathbb{Z}/p^3\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$, $G_3 \cong (\mathbb{Z}/p^2\mathbb{Z}) \times (\mathbb{Z}/p^2\mathbb{Z})$, $G_4 \cong \mathbb{Z}/p^2\mathbb{Z} \times (\mathbb{Z}/p\mathbb{Z})^2$, $G_5 = (\mathbb{Z}/p\mathbb{Z})^4$. Wie in Teil (b) zeigt ein Induktionsbeweis, dass für alle $a, b \in \mathbb{F}_{p^2}$ und alle $k \in \mathbb{N}_0$ jeweils

$$\begin{pmatrix} 1 & 0 & a \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}^k = \begin{pmatrix} \bar{1} & \bar{0} & \overline{ka} \\ \bar{0} & \bar{1} & \overline{kb} \\ \bar{0} & \bar{0} & \bar{1} \end{pmatrix}$$

gilt. Wegen $\operatorname{char}(\mathbb{F}_{p^2}) = p$ gilt jeweils $\overline{pa} = \overline{pb} = \bar{0}$ und somit auch hier $\begin{pmatrix} 1 & 0 & a \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}^p = e_{G(\mathbb{F}_{p^2})}$.

Also gibt es auch in $G(\mathbb{F}_{p^2})$ nur Elemente der

$H_p \leq G$ (Übung) Offenbar ist H_p eine Gruppe

Ordnung 1 und p. In G_1, G_2, G_3, G_4 gibt es dagegen jeweils ein Element der Ordnung p^2, denn ... (Übung). Also gilt

$$G(\mathbb{F}_p^2) \cong G_5 = (\mathbb{Z}/p\mathbb{Z})^4. \qquad \square$$

Erinnerung: Eine Gruppe G wird *inneres direktes Produkt* von $U, N \leq G$ genannt, wenn gilt

(1) $U, N \trianglelefteq G$ (2) $N \cap U = \{e\}$ (3) $G = NU$

Unter diesen Voraussetzungen gilt dann

$$\boxed{G \cong N \times U}$$

F25T2A5 Sei p eine Primzahl und

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

(a) Zeigen Sie: $G \leq GL_2(\mathbb{F}_p)$ (Übung)

(b) Zeigen Sie, dass G eine zyklische Untergruppe H_p der Ordnung p und eine zykl. Untergr. H_{p-1} der Ordnung $p-1$ besitzt.

Sei $H_p = \left\{ \begin{pmatrix} 1 & 0 \\ b & \bar{1} \end{pmatrix} \middle| b \in \mathbb{F}_p \right\}$ zu überprüfen: $H_p \leq G$ (Übung) Offenbar ist H_p eine Gruppe der Ordnung p und als Gruppe von Primzahlordnung zyklisch. Sei außerdem $H_{p-1} = \left\{ \begin{pmatrix} a & \bar{0} \\ \bar{0} & a \end{pmatrix} \middle| a \in \mathbb{F}_p^{\times} \right\}$

(c)

Es

der E

überprüfe: $H_{p-1} \leq G$ Offenbar hat H_{p-1} die Ordnung $|\mathbb{F}_p^\times| = p-1$. Als multiplikative Gruppe eines endl Körpers ist $\mathbb{F}_p^\times$ zyklisch. Daraus folgt, dass auch H_{p-1} zyklisch ist. Denn die Abbildung

$$\phi: \mathbb{F}_p^\times \to H_{p-1}, \quad a \mapsto \begin{pmatrix} a & \bar{0} \\ \bar{0} & a \end{pmatrix}$$

ist offenbar bijektiv, wegen $\phi(ab) = \begin{pmatrix} ab & \bar{0} \\ \bar{0} & ab \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \cdot \begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix} = \phi(a)\phi(b)$ insgesamt ein Isomorphismus. Mit $\mathbb{F}_p^\times$ ist also auch H_{p-1} zyklisch.