Erinnerung: Für jede Gruppe G und jede Teilmenge $S \subseteq G$ gibt es eine eindeutig bestimmte kleinste Untergruppe $\langle S \rangle \leq G$ mit $\langle S \rangle \supseteq S$ (d.h. für jede Untergr. $U \leq G$ mit $U \supseteq S$ gilt $U \supseteq \langle S \rangle$).

H25T2A2 Sei $G = \langle A, B \rangle \leq GL_2(\mathbb{F}_3)$ gegeben durch die Matrizen $A = \begin{pmatrix} \bar{2} & \bar{2} \\ \bar{2} & \bar{1} \end{pmatrix}$ und $B = \begin{pmatrix} \bar{0} & \bar{2} \\ \bar{1} & \bar{0} \end{pmatrix}$.

(a) Überprüfen Sie: $A^4 = E$, $B^2 = A^2$, $BAB^{-1} = A^3$

mit $U \supseteq S$ gilt $U \supseteq \langle S \rangle$).

$$A^2 = \begin{pmatrix} \bar{2} & \bar{2} \\ \bar{2} & \bar{1} \end{pmatrix}\begin{pmatrix} \bar{2} & \bar{2} \\ \bar{2} & \bar{1} \end{pmatrix} = \begin{pmatrix} \bar{2} & \bar{0} \\ \bar{0} & \bar{2} \end{pmatrix}, \quad A^4 = (A^2)^2 = \begin{pmatrix} \bar{2}^2 & \bar{0} \\ \bar{0} & \bar{2}^2 \end{pmatrix}$$

$$= \begin{pmatrix} \bar{4} & \bar{0} \\ \bar{0} & \bar{4} \end{pmatrix} = \begin{pmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{pmatrix} = E, \quad B^2 = \begin{pmatrix} \bar{0} & \bar{2} \\ \bar{1} & \bar{0} \end{pmatrix}\begin{pmatrix} \bar{0} & \bar{2} \\ \bar{1} & \bar{0} \end{pmatrix} = \begin{pmatrix} \bar{2} & \bar{0} \\ \bar{0} & \bar{2} \end{pmatrix}$$

$= A^2$ $\det(\bar{B}) = -\bar{2} = \bar{1} \neq \bar{0} \Rightarrow \bar{B}$ ist invertierbar

Überprüfe: $BA = A^3B$ (daraus folgt $BAB^{-1} = A^3$)

$$BA = \begin{pmatrix} \bar{0} & \bar{2} \\ \bar{1} & \bar{0} \end{pmatrix}\begin{pmatrix} \bar{2} & \bar{2} \\ \bar{2} & \bar{1} \end{pmatrix} = \begin{pmatrix} \bar{1} & \bar{2} \\ \bar{2} & \bar{2} \end{pmatrix}, \quad A^3B = A^2AB$$

$$= \begin{pmatrix} \bar{2} & \bar{0} \\ \bar{0} & \bar{2} \end{pmatrix}\begin{pmatrix} \bar{2} & \bar{2} \\ \bar{2} & \bar{1} \end{pmatrix}\begin{pmatrix} \bar{0} & \bar{2} \\ \bar{1} & \bar{0} \end{pmatrix} = \begin{pmatrix} \bar{2} & \bar{0} \\ \bar{0} & \bar{2} \end{pmatrix}\begin{pmatrix} \bar{2} & \bar{1} \\ \bar{1} & \bar{1} \end{pmatrix} = \begin{pmatrix} \bar{1} & \bar{2} \\ \bar{2} & \bar{2} \end{pmatrix}$$

$\in G$ $D = A_1 \cdots A_r$ mit $r \in \mathbb{N}_0$, $A_j \in \{A, B\}$ $1 \leq j \leq r$,
d.h. man erhält $CD \in U$ durch r-fache Anwendung von $(*)$.

(b) Zeigen Sie, dass jedes Element in G auf eindeutige Weise in der Form $A^k B^l$ mit $0 \leq k \leq 3$ und $l \in \{0, 1\}$ dargestellt werden kann, und bestimmen Sie die Ordnung von G.

Betrachte in $GL_2(\mathbb{F}_3)$ die Teilmenge

$$U = \{A^k B^l \mid 0 \leq k \leq 3,\ l \in \{0, 1\}\}$$

Beh.: (1) $U \leq GL_2(\mathbb{F}_3)$ (d.h. U ist Untergr.)
(2) $U = \langle A, B \rangle$ (3) $|G| = 8$

zu (1) zu überprüfen: (1.1) $E \in U$
(1.2) $\forall C, D \in U: CD \in U$ (1.3) $\forall C \in U: C^{-1} \in U$

zu (1.1) $E = A^0 \cdot B^0 \in U$

zu (1.2) Es genügt zu überprüfen:

$$\forall C \in U : CA \in U,\ CB \in U \quad (*)$$

denn: Sind $C, D \in U$, dann hat D die Form

$D = A_1 \cdots A_r$ mit $r \in \mathbb{N}_0$, $A_j \in \{A, B\}$ $1 \leq j \leq r$,

d.h. man erhält $CD \in U$ durch r-fache Anwendung von $(*)$.

Zeige durch vollst. Ind. über $r \in \mathbb{N}_0$:

$C \in U,\ A_1, \ldots, A_r \in \{A, B\} \Rightarrow CA_1 \cdots A_r \in U$

Ind.-Anf.: $r = 0$ $CA_1 \cdots A_r = C \in U$

Ind.-Schritt: $r \mapsto r+1$ geg: $C \in U,\ A_1, \ldots, A_{r+1} \in U$

Ind.-V. $\Rightarrow C' = C \cdot A_1 \cdots A_r \in U \Rightarrow C(A_1 \cdots A_{r+1})$

$= C^1 \cdot A_{r+1} \overset{(*)}{\in} U$

$C^1 \in U,\ A_{r+1} \in \{A, B\}$

Überprüfe nun (*): Sei $C \in U$, d.h.

$C = A^k B^l$ mit $0 \leq k \leq 3$, $l \in \{0, 1\}$

1. Fall: $l = 0$ $\quad C \cdot A = A^{k+1}$

Ist $k \in \{0, 1, 2\}$, dann folgt direkt $k+1 \in \{1, 2, 3\}$

und $A^{k+1} = A^{k+1} \cdot B^0 \in U$. Im Fall $k = 3$ gilt

$C \cdot A = A^3 \cdot A = A^4 = E = A^0 \cdot B^0 \in U$.

außerdem: $C \cdot B = A^k \cdot B^1 \in U$

2. Fall: $l = 1$ Dann ist $C \cdot A = A^k \cdot B \cdot A$

$= A^k \cdot (A^3 \cdot B) = A^{k+3} \cdot B$ Im Fall $k = 0$ ist

$C \cdot A = A^3 B^1 \in U$. Im Fall $k \in \{1, 2, 3\}$ gilt

$k+3-4 = k-1 \in \{0,1,2\}$ und

$C \cdot A = A^{k+3} \cdot B = A^{k+3} E^{-1} \cdot B = A^{k+3} (A^4)^{-1} \cdot B$

$= A^{k+3-4} \cdot B^1 \in U$

außerdem: $C \cdot B = A^k \cdot B \cdot B = A^k \cdot B^2$

$= A^k A^2 = A^{k+2}$ Ist $k \in \{0,1\}$, dann

erhalten wir $C \cdot B = A^{k+2} \cdot B^0 \in U$, für

$k \in \{2,3\}$ entsprechend $C \cdot B = A^{k+2} A^{-4} =$

$A^{k-2} B^0 \in U$ wg. $k-2 \in \{0,1\}$

zu (1.3) geg. $C \in U$, $C = A^k B^l$ mit $k \in \{0,1,2,3\}$,

$l \in \{0,1\}$ Wir gehen alle acht Möglichkeiten ein-

zeln durch. $(A^0 B^0)^{-1} = E^{-1} = E = A^0 B^0 \in U$

$(A^k \cdot B^0)^{-1} = A^{-k} = A^4 \cdot A^{-k} = A^{4-k} \cdot B^0 \in U$ für $k \in \{1,2,3\}$

$(A^0 B^1)^{-1} = B^{-1} = A^4 B^{-1} = A^2 \cdot A^2 B^{-1} =$
$A^2 \cdot B^2 \cdot B^{-1} = A^2 \cdot B^1 \in U$

$(A^1 B^1)^{-1} = B^{-1} A^{-1} = A^2 B A^{-1} = A^2 B A^3$
$\in U$, da $A^2 B, A^3 \in U$ und U abg. bzgl.
Mult. $(A^2 B)^{-1} = B^{-1} A^{-2} = (A^2 B) A^4 A^{-2}$
$= (A^2 \cdot B) A^2 \in U$, $(A^3 B)^{-1} = B^{-1} A^{-3}$
$= (A^2 B) \cdot A^4 \cdot A^{-3} = (A^2 \cdot B) \cdot A \in U$, aus
demselben Grund

zu (2) s.o. $\rightarrow U$ ist bzgl. mit $\{A, B\} \subseteq U$
$(A = A^1 B^0 \in U, B = A^0 B^1 \in U) \Rightarrow \langle A, B \rangle \subseteq U$
umgekehrt: Aus $A, B \in \langle A, B \rangle$ folgt $A^k B^l$
$\in \langle A, B \rangle$ für $0 \leq k \leq 3$, $l \in \{0, 1\} \Rightarrow U \subseteq \langle A, B \rangle$

zu (3) Sei $S = \{0,1,2,3\} \times \{0,1\}$. Betrachte die Abbildung $\phi : S \to G, (k,l) \mapsto A^k B^l$

E genügt z.zg., dass die Abb. ϕ bijektiv ist (dann folgt $|G| = |S| = 4 \cdot 2 = 8$ und die Eindeutigkeit und Existenz der Darst. der Elemente von G) Die Surjektivität folgt direkt aus (2)

zur Injektivität: geg. $k, k' \in \{0,1,2,3\}$, $l, l' \in \{0,1\}$ mit $A^k B^l = A^{k'} B^{l'}$, z.zg.: $k = k'$, $l = l'$

1. Fall: $l = l' = 0 \Rightarrow A^k = A^{k'}$ Ang. $k \neq k'$, o.B.d.A. $k < k'$. $\Rightarrow A^{k'-k} = E$, $k'-k \in \{1,2,3\}$

↯ da $A, A^2, A^3 \neq E$ also: $k = k'$; $l = l'$

2. Fall: $l = l' = 1 \Rightarrow A^k B = A^{k'} B \overset{\cdot B^{-1}}{\Longrightarrow}$

$A^k = A^{k'}$ siehe Fall 1 $\Rightarrow$ $k = k'$, $l = l'$

3. Fall: $l = 0, l' = 1 \Rightarrow A^k = A^{k'} B$

Im Fall $k' \leq k$ folgt $B = A^{k-k'}$, $k - k' \in$

$\{0, 1, 2, 3\}$ ↯ da $B \notin \{E, A, A^2, A^3\}$

Im Fall $k' > k$ folgt $B = A^{k-k'} = A^{4+k-k'}$

und $4 + k - k' \in \{1, 2, 3\}$ ↯ da $B \notin \{A, A^2, A^3\}$

4. Fall: $l = 1, l' = 0$ analog zum 3. Fall

zu (c) z.zg. G hat genau eine Untergr. der Ordnung 2

$A^2 \neq E$, $(A^2)^2 = A^4 = E \Rightarrow \operatorname{ord}(A^2) = 2 \Rightarrow$

$N = \langle A^2 \rangle$ ist Untergruppe der Ordnung 2

Sei nun U eine beliebige Untergr. der Ordnung 2

2 Primzahl $\Rightarrow U$ ist zyklisch $\Rightarrow \exists C \in G$ mit $U = \langle C \rangle$,

wobei $\operatorname{ord}(C) = 2$

$A^4 = E$, $A^2 \neq E \Rightarrow \operatorname{ord}(A) = 4$

$\operatorname{ord}(A^3) = \operatorname{ord}(A) = 4$ wegen $\operatorname{ggT}(3,4) = 1$

$\operatorname{ord}(E) = 1 \Rightarrow C \notin \{E, A, A^3\}$

$\Rightarrow$ nur $C \in \{A^2, B, AB, A^2B, A^3B\}$

$B^2 = A^2 + E$, $(AB)^2 = ABAB = A(A^3B)B =$

$A^4B^2 = A^2 + E$, $(A^2B)^2 = (A^2B)(A^2B) = A^2(BA)AB$

$= A^5BAB = A^8B^2 = A^8 \cdot A^2 = A^2 + E$

$(A^3B)^2 = A^3BA^3B = A^3(BA)(A^2B) =$

$A^6BA^2B = A^6A^3BAB = A^9A^3B^2 = A^{12}B^2$

$= A^2 + E \Rightarrow A^2$ ist das einzige Element der Ordnung 2 in G

$\Rightarrow C = A^2$, $U = \langle A^2 \rangle = N$ □

Erinnerung: Sei G eine Gruppe, $N \trianglelefteq G$.
Dann ist die Faktorgruppe G/N die Menge der Linksnebenklassen mit der Verknüpfung $*$ gegeben durch

$(gN) * (hN) = (gh)N \quad \forall g, h \in G$

wichtige Regel:

$\forall g, h \in G: \; gN = hN \Leftrightarrow h \in gN \Leftrightarrow g \in hN$

H2ST2A2 (d)

Zeigen Sie, dass N ein Normalteiler von G ist, und bestimmen Sie den Isomorphietyp der Faktorgruppe G/N.

Sei $C \in G$. Da $G \xrightarrow{\phi} G, D \mapsto CDC^{-1}$ ein Automorphismus von G ist, ist mit N auch $CNC^{-1} = \phi(N)$ eine Untergr. der Ordnung 2 von G. Eindeutigkeit $\Rightarrow CNC^{-1} = N$

Bestimmung des Isomorphietyps von G/N:

Lagrange $\Rightarrow |G/N| = (G:N) = \frac{|G|}{|N|} = \frac{8}{2} = 4$

4 ist Primzahlquadrat $\Rightarrow$ G/N ist abelsch.

Hauptsatz über endl. abelsche Gruppen $\Rightarrow$

$G/N \cong \mathbb{Z}/4\mathbb{Z}$ oder $G/N \cong (\mathbb{Z}/2\mathbb{Z})^2$

Wenn G/N zwei verschiedene Elemente der Ordnung 2 hat, folgt $G/N \cong (\mathbb{Z}/2\mathbb{Z})^2$, da $\bar{2}$ in $\mathbb{Z}/4\mathbb{Z}$ das einzige Element der Ordnung 2 ist.

$A \notin N$, da $N = \langle A^2 \rangle = \{E, A^2\} \Rightarrow A \cdot N \neq e_{G/N}$

$A^2 \in N \Rightarrow (A \cdot N)^2 = A^2 \cdot N = N = e_{G/N}$

$\Rightarrow \operatorname{ord}(A \cdot N) = 2$ in G/N

$= (A \cdot B) \cdot A \in U \cdot (A \cdot B) = B \cdot A^2$

G/N :

$= \frac{8}{2} = 4$

velsch :

en $\Rightarrow$

$ZZ)^2$

ente der

$/2ZZ)^2$, da

Ordnung 2 ist.

$\} \Rightarrow A \cdot N \neq e_{G/N}$

$= e_{G/N}$

$B \notin N \rightarrow B \cdot N \neq e_{G/N}$

$B^2 = A^2 \in N \rightarrow (B \cdot N)^2 = B^2 N = N = e_{G/N}$

$\Rightarrow \operatorname{ord}(B \cdot N) = 2$ in G/N

noch z.zg.: $A \cdot N \neq B \cdot N$

Ang. $A \cdot N = B \cdot N \rightarrow B \in A \cdot N$

$\Rightarrow B \in \{A \cdot E, A \cdot A^2\} \Rightarrow B \in \{A, A^3\}$

↯ da jedes Element in G eine eind. Darst. der Form $A^k B^l$, $k \in \{0, \dots, 3\}$, $l \in \{0, 1\}$ hat

also: $G/N \cong (\mathbb{Z}/2\mathbb{Z})^2$ □