

(folgt aus dem Satz von Lagrange).

H25T2A2 Seien $A, B \in GL_2(\mathbb{F}_3)$ geg.

$$\text{durch } A = \begin{pmatrix} \bar{2} & \bar{2} \\ \bar{2} & \bar{1} \end{pmatrix}, B = \begin{pmatrix} \bar{0} & \bar{2} \\ \bar{1} & \bar{0} \end{pmatrix}$$

und $G = \langle A, B \rangle \leq GL_2(\mathbb{F}_3)$.

zu (a) überprüft: $A^4 = E$, $B^2 = A^2$, $BA B^{-1} = A^3$
($\Leftrightarrow BA = A^3 B$)

zu (b) Sei $U = \{A^j B^l \mid 0 \leq j \leq 3, l \in \{0, 1\}\}$

Beh.: $U = G = \langle A, B \rangle$ dafür zu überprüfen

(0) U ist Untergruppe von $GL_2(\mathbb{F}_3)$ (1) $\{A, B\} \subseteq U$

(2) $V \leq GL_2(\mathbb{F}_3)$, $V \supseteq \{A, B\} \rightarrow V \supseteq U$

$\forall g \in G$

Alternative (geht schneller): $A^j B^l$ für $0 \leq j \leq 3$ und $l \in \{0, 17\}$ explizit ausrechnen.

schon gezeigt: Für jedes $k \in \mathbb{Z}$ existiert ein $j \in \{0, 1, 2, 3\}$ mit $A^k = A^j$ (folgt aus $A^4 = E$) (*)

überprüfe: (i) $E \in U$ (ii) $\forall C, D \in U: CD, C^{-1} \in U$

zu (i) Es gilt $E = A^0 B^0 \rightarrow E \in U$

zu (ii) Seien $C, D \in U \rightarrow \exists j, j' \in \{0, 1, 2, 3\}, l, l' \in \{0, 17\}$ mit $C = A^j B^l$ und $D = A^{j'} B^{l'}$

1. Fall: $l = l' = 0 \Rightarrow CD = A^j A^{j'} = A^{j+j'} (*) \Rightarrow \exists j'' \in \{0, \dots, 3\}$ mit $A^{j+j'} = A^{j''} \Rightarrow CD = A^{j''} B^0 \in U$

2. Fall: $l = 1, l' = 0 \Rightarrow CD = A^j B A^{j'}$

Für alle $m \in \mathbb{N}_0$ gilt $BA^m = A^{3m} B$, denn: Für $m=0$ ist die Gleichung offensichtlich, und setzen wir sie für ein $m \in \mathbb{N}_0$ voraus, dann folgt

(*)

$$\begin{aligned}
 BA^{m+1} &= BA^m A = A^{3m} BA \stackrel{\text{siehe (a)}}{=} A^{3m} A^3 B \\
 &= A^{3(m+1)} B \quad \text{also: } CD = A^j A^{3j'} B \\
 &= A^{j+3j'} B \quad (*) \Rightarrow \exists j'' \in \{0, 1, 2, 3\} \text{ mit} \\
 A^{j+3j'} &= A^{j''} \Rightarrow CD = A^{j''} B^1 \in U
 \end{aligned}$$

$l' \in \{0, 1\}$

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

$$\begin{aligned}
 \text{4. Fall: } l = l' = 1 &\Rightarrow CD = A^j B A^{j'} B \\
 &\stackrel{a)}{=} A^{j+3j'} B^2 \stackrel{(a)}{=} A^{j+3j'} A^2 = A^{j+3j'+2} \quad (*) \Rightarrow
 \end{aligned}$$

$$\exists j'' \in \{0, 1, 2, 3\} \text{ mit } A^{j+3j'+2} = A^{j''} \Rightarrow$$

$$CD = A^{j''} B^0 \in U$$

die Gleichung
glt

Für d

1. Fall

$$A^{-j} =$$

2. Fall

$$B^{-}$$

$$B^3$$

mit

mit

zu (1) A

$\{1, 2, \dots, 37\}$

mit $\phi(f, l) = \phi(f', l')$. z.zg.: $f = f', l = l' \quad (*) \rightarrow A^f B^l = A^{f'} B^{l'}$

Für den Nachweis, dass $C^{-1} \in U$ gilt, unterscheiden wir zwei Fälle.

1. Fall: $l = 0 \Rightarrow C = A^f \Rightarrow C^{-1} = A^{-f} \quad (*) \Rightarrow \exists f'' \in \{0, 1, 2, 37\}$ mit
 $A^{-f} = A^{f''} \Rightarrow C^{-1} = A^{f''} B^0 \in U$

2. Fall: $l = 1 \Rightarrow C = A^f B \Rightarrow C^{-1} = (A^f B)^{-1} = B^{-1} A^{-f} =$
 $B^{-1} \in A^{-f} \stackrel{(*)}{=} B^{-1} A^f A^{-f} = B^{-1} (A^2)^2 A^{-f} \stackrel{(*)}{=} B^{-1} (B^2)^2 A^{-f} =$
 $B^3 A^{-f} = B B^2 A^{-f} = B A^2 A^{-f} = B A^{2-f} \quad (*) \Rightarrow \exists f''' \in \{0, \dots, 37\}$
 $\rightarrow$ mit $A^{2-f} = A^{f'''} \Rightarrow C^{-1} = B A^{f'''} \stackrel{so}{=} A^{3f'''} B \quad (*) \Rightarrow \exists f'''' \in \{0, \dots, 37\}$
mit $A^{3f'''} = A^{f''''} \Rightarrow C^{-1} = A^{f''''} B^1 \in U$

zu (1) $A = A^1 B^0 \Rightarrow A \in U, B = A^0 B^1 \Rightarrow B \in U$
insgesamt: $\{A, B\} \subseteq U$.

zu (2) Sei $V \leq GL_2(\mathbb{F}_3)$ mit $\{A, B\} \subseteq V$. z.zg: $U \subseteq V$

Sei $C \in U \Rightarrow \exists j \in \{0, 1, 2, 3\}, l \in \{0, 1\}$ mit $C = A^j B^l$

$A, B \in V, V \leq GL_2(\mathbb{F}_3) \Rightarrow A^j, B^l \in V \Rightarrow A^j B^l \in V$
 $\Rightarrow C \in V$ (Damit ist der Beweis von $G = U$ abgeschlossen.)

weitere Aufgabe: Bestimmung der Ordnung $|G|$ von G

Beh. $|G| = |U| = 8$ Es genügt zu zeigen, dass die Abb.

$\phi: \{0, 1, 2, 3\} \times \{0, 1\} \rightarrow U, (j, l) \mapsto A^j B^l$ bijektiv ist. wegen

$|\{0, \dots, 3\} \times \{0, 1\}| = 4 \cdot 2 = 8$ Die Surjektivität folgt direkt aus der

Definition von U . Injektivität: Seien $j, j' \in \{0, 1, 2, 3\}, l, l' \in \{0, 1\}$

mit $\phi(j, l) = \phi(j', l')$. z.zg: $j = j', l = l'$ ($\Leftrightarrow$) $\rightarrow A^j B^l = A^{j'} B^{l'}$

$$\Rightarrow B^l = A^{j'-j} B^{l'} \Rightarrow B^{l-l'} = A^{j'-j}$$

$$\text{1. Fall: } l=l'=0 \rightarrow A^{j'-j} = E$$

$$\text{Beh. } \forall m \in \mathbb{Z}: A^m = E \Rightarrow 4 \mid m$$

Sei $m \in \mathbb{Z}$ mit $A^m = E$. Division mit Rest

$$\Rightarrow \exists q, r \in \mathbb{Z} \text{ mit } m = 4q + r, 0 \leq r \leq 3$$

$$\Rightarrow A^m = A^{4q+r} = (A^4)^q \cdot A^r \stackrel{(\text{a})}{=} E^q \cdot A^r = A^r$$

$$\text{überprüfe: } A, A^2, A^3 \neq E \quad \begin{matrix} A^m = E \\ \Rightarrow \\ A^r = E \end{matrix} \quad r=0$$

$$\Rightarrow m = 4q \Rightarrow 4 \mid m \quad (\Rightarrow \text{Beh.})_{j, j' \in \{0, \dots, 37\}}$$

$$\text{also: } A^{j'-j} = E \Rightarrow 4 \mid (j'-j) \quad \begin{matrix} \Rightarrow \\ j'-j \in \{0, \dots, 37\} \end{matrix}$$

$$\rightarrow j=j' \quad \text{also: } j=j', l=l' \text{ in diesem Fall}$$

2. Fall: $l=1, l'=0 \Rightarrow A^{j'-j} = B$

(*) $\Rightarrow \exists j'' \in \{0, 1, 2, 3\} : A^{j'-j} = A^{j''} \Rightarrow A^{j''} = B$

überprüfe: $A^0, A^1, A^2, A^3 \neq B \Rightarrow \nexists$ (2. Fall unmöglich)

3. Fall: $l=0, l'=1 \Rightarrow B^{-1} = A^{j'-j} \quad B^{-1} = B^{-1} E =$

$B^{-1}(A^2)^2 = B^{-1}(B^2)^2 = B^3 = BB^2 = BA^2 \Rightarrow BA^2 = A^{j'-j}$

$\Rightarrow B = A^{j'-j-2} \quad (*) \Rightarrow \exists j'' \in \{0, \dots, 3\} \text{ mit } A^{j'-j-2} = A^{j''}$

$\Rightarrow B = A^{j''} \quad \nexists$ (siehe 2. Fall)

4. Fall: $l=l'=1 \Rightarrow A^{j'-j} = E \xrightarrow{\text{so:}} 4 \mid (j'-j) \xrightarrow{j'-j \in \{1, 3, \dots, 3\}}$

$\Rightarrow j=j'$ also: $l=l', j=j'$ in diesem Fall

Alternative (geht schneller): $A^l B^l$ für $0 \leq j \leq 3$ und $l \in \{0, 1\}$ explizit ausrechnen.

Wdh. Elementordnungen in Gruppen

Def. Ordnung eines Gruppenelements $g \in G$

$$\text{ord}(g) = |\langle g \rangle| \quad (\text{ord}(g) \in \mathbb{N} \text{ oder } \text{ord}(g) = \infty)$$

Satz Sei G eine Gruppe, $g \in G$.

(i) $n \in \mathbb{N}$ minimal mit $g^n = e \implies n = \text{ord}(g)$

(ii) $g^n \neq e \quad \forall n \in \mathbb{N} \implies \text{ord}(g) = \infty$

(iii) Setze $n = \text{ord}(g) \in \mathbb{N}$ voraus. Dann gilt

$$\forall m \in \mathbb{Z}: g^m = e \implies n \mid m$$

(iv) $g^n = e$ ($n \in \mathbb{N}$), $g^{n/p} \neq e$ für jeden Primteiler p von $n \implies \text{ord}(g) = n$

(v) Ist G endlich, dann gilt $\text{ord}(g) \mid |G| \quad \forall g \in G$
(folgt aus dem Satz von Lagrange).

- (folgt aus dem Satz von Lagrange)
- Erinnerung:
- (i) Jede Gruppe von Primzahlordnung ist zyklisch (folgt aus Satz v. Lagrange)
 - (ii) Jede zyklische Gruppe der Ordnung n enthält genau $\varphi(n)$ Elemente der Ordnung n , wobei φ die Eulersche φ -Funktion bezeichnet.
 - (iii) Jede Gruppe von Primzahlquadratordnung ist abelsch.

H25T2A2 (c) Zeigen Sie, dass G genau eine Untergruppe der Ordnung 2 hat.

Da 2 eine Primzahl ist, ist jede Untergr. der Ordnung 2 zyklisch, und wird von einem Element der Ordnung 2 erzeugt. Wir bestimmen die Ordnungen der Elemente von G .
 $\text{ord}(E) = 1$ (Neutralelement), $2 + 4 \stackrel{?}{=} A^2 + E$

$l \in 10, 17$ explizit ausrechnen.

$\Rightarrow \text{ord}(A) > 2$, $(A^2)^2 = A^4 = E \Rightarrow \text{ord}(A^2) = 2$, $(A^3)^2 = A^6 \neq E$
wegen $4 \nmid 6 \Rightarrow \text{ord}(A^3) > 2$ $B^2 = A^2 \neq E \Rightarrow \text{ord}(B) > 2$

$(AB)^2 = ABAB = A^3AB B = A^4 B^2 = B^2 \neq E \Rightarrow$

$\text{ord}(AB) > 2$ $\stackrel{BA=A^3B}{(A^2B)^2} = A^2BA^2B \stackrel{so}{=} A^2 \cdot A^6 \cdot B \cdot B =$

$(A^4)^2 \cdot B^2 = B^2 \neq E \Rightarrow \text{ord}(A^2B) > 2$

$(A^3B)^2 = A^3BA^3B = A^3A^9BB = A^{12}B^2 = (A^4)^3 \cdot B^2 =$
 $= B^2 \neq E \Rightarrow \text{ord}(A^3B) > 2$

Es gibt nur ein Element der Ordnung 2, nämlich A^2 , und somit ist $\langle A^2 \rangle$ die einzige Untergr. von G der Ordnung 2.

Übung: F14T3A1

Def. Seien G, H Gruppen.

(i) Eine Abb. $\phi: G \rightarrow H$ heißt Gruppenhomomorphismus, wenn $\phi(gh) = \phi(g) \phi(h) \quad \forall g, h \in G$.

(ii) Ein Isomorphismus von Gruppen ist ein bijektiver Gruppenhom.

(iii) Man bezeichnet Gruppen G, H als isomorph (Notation: $G \cong H$), wenn ein Hom. $\phi: G \rightarrow H$ existiert.

wichtig: Zwei isomorphe Gruppen stimmen in allen Struktur-eigenschaften überein (abelsch, auflösbar, Anzahl der Untergruppen, Anz. Elemente der Ordnung 3 usw.),

H25T3A1 (a) Zeigen Sie, dass die Gruppen $(\mathbb{R}^*, \cdot)$
und $(\mathbb{C}^*, \cdot)$ nicht isomorph sind.

Wegen $i^2 = -1 \neq 1$ und $i^4 = 1$ ist i in $(\mathbb{C}^*, \cdot)$ ein Element
der Ordnung 4. Wären die Gruppen isomorph, dann müsste
es auch in $(\mathbb{R}^*, \cdot)$ ein Element a der Ordnung 4 geben.

$$\begin{aligned} \text{ord}(a) = 4 &\Rightarrow a^4 = 1, a^2 \neq 1 & a^4 = 1 &\Rightarrow a^4 - 1 = 0 \Rightarrow \\ (a^2 - 1)(a^2 + 1) &= 0 \Rightarrow a^2 - 1 = 0 \text{ oder } a^2 + 1 = 0 \Rightarrow \\ a^2 &= 1 \text{ oder } a^2 = -1 & \Downarrow \end{aligned}$$