Def.: Sei $\sigma \in S_n$. Der <u>Zerlegungstyp</u> von σ ist ein Tupel der Form $(k_1, \dots, k_r)$ mit $r \in \mathbb{N}$, $k_1, \dots, k_r \in \mathbb{N}$, $k_1 \geq k_2 \geq \dots \geq k_r \geq 2$ und der Eigenschaft, dass σ als Produkt von r disjunkten Zyklen der Längen $k_1, \dots, k_r$ darstellbar ist.

Erinnerung: Ist $\sigma \in S_n$ vom Zerlegungstyp $(k_1, \dots, k_r)$, dann gilt $\operatorname{ord}(\sigma) = \operatorname{kgV}(k_1, \dots, k_r)$.

$\mathbb{Z}/$

Beisp

ist

$\mathbb{Z}/$

Er

Bs

Bsp. Elemente der Gruppe S_6

Beispielelement	id	(12)	(123)	(1234)	(12345)
Zerlegungstyp	()	(2)	(3)	(4)	(5)
Ordnung	1	2	3	4	5

(123456)	(12)(34)	(123)(45)	(1234)(56)	(123)(456)
(6)	(2,2)	(3,2)	(4,2)	(3,3)
6	2	6	4	3

(12)(34)(56)
(2,2,2)
2

Übung: H13T3A3

Satz

gibt e

Dabei

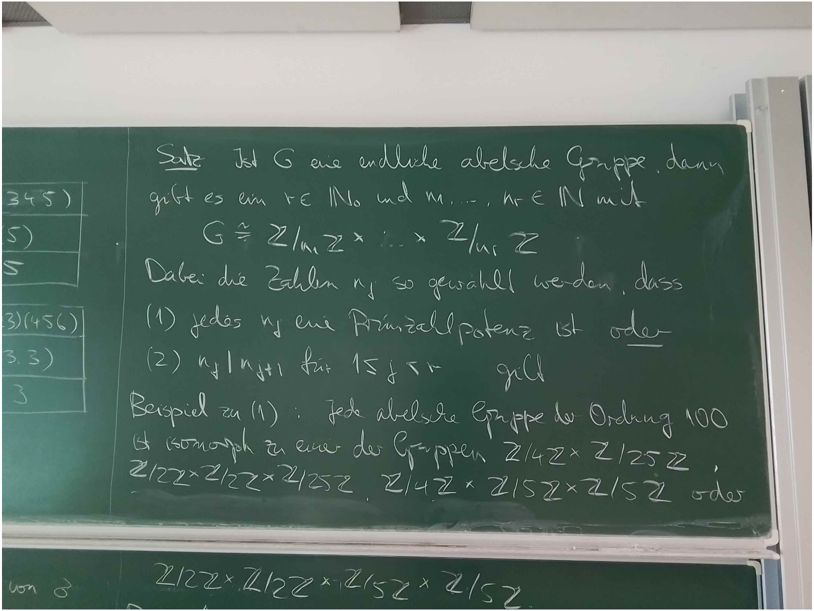
(1)

(2)

Beispi

Ist iso

$\mathbb{Z}/2\mathbb{Z}$



Korrektur: Dabei **können** die Zahlen n_j so gewählt werden, dass ...

$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$.

Beispiel zu (2): Jede abelsche Gruppe der Ordnung 100 ist isomorph zu einer der Gruppen $\mathbb{Z}/100\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/50\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z}$ oder $\mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$.

<u>Erinnerung:</u> Der Chinesische Restsatz für Gruppen besagt, dass für <u>teilerfremde</u> $m, n \in \mathbb{N}$ jeweils

$$\mathbb{Z}/(mn\mathbb{Z})\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

gilt.

Bsp.: $\operatorname{ggT}(4,25) = 1 \Rightarrow \mathbb{Z}/100\mathbb{Z} \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}$

<u>falsch</u>: $\mathbb{Z}/4\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. $(\operatorname{ggT}(2,2) \neq 1)$

<u>Erinnerung</u> Sei G eine Gruppe. Eine Untergruppe $U \leq G$ heißt <u>Normalteiler</u> von G, wenn eine der folgenden (äquivalenten) Bedingungen erfüllt ist.

(i) $\forall g \in G: \; gU = Ug$

(ii) $\forall g \in G: \; gUg^{-1} \subseteq U$

(iii) $\forall g \in G: \; gUg^{-1} = U$

<u>Satz</u>:

(i) Für jede Gruppe G sind $\{e\}$ und G Normalteiler. Eine Gruppe mit genau zwei Normalteilern wird als <u>einfache</u> Gruppe bezeichnet.

Beispiele für einfache Gruppen:

$(\mathbb{Z}/p\mathbb{Z},+)$, p Primzahl, A_n für $n \geq 5$

(ii) Jede Untergruppe U einer Gruppe G mit $(G:U)=2$ ist Normalteiler von G.
(Erinnerung: Index $(G:U)$ = Anzahl der Linksnebenklassen von U)

(iii) Kerne von Gruppenhomomorphismen sind Normalteiler

(iv) Zweiter Sylowsatz: Sei G eine endliche Gruppe, p eine Primzahl, P eine p-Sylowgruppe, und ν_p die Anzahl der p-Sylowgruppen von G.
Dann ist jede p-Sylowgp. von G zu P konjugiert

G.

G.

Links-

und

endliche

-Sylowgruppe,

gruppen von G

P konjugiert.

Unmittelbare Folge: $P \trianglelefteq G \iff \nu_p = 1$

(Zwei Untergr. $U, V \leq G$ heißen <u>konjugiert</u>, wenn $V = gUg^{-1}$ für ein $g \in G$ gilt.)

<u>Def.</u> Sei G eine Gruppe und $N \trianglelefteq G$ (d.h. N ist Normalteiler von G. Dann existiert auf der Menge G/N der Linksnebenklassen von N eine eindeutig best. Verknüpfung $\circ$ mit

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

Man nennt $(G/N, \circ)$ die <u>Faktorgruppe</u> von G modulo N.

wichtige Regel: $\forall g, h \in G : gN = hN \iff h \in gN$

a

G

genau

che

<u>H25T2A2</u> $G = \langle A, B \rangle \subseteq GL_2(\mathbb{F}_3)$,

$A^4 = E$, $B^2 = A^2$, $BA = A^3 B$

bekannt: $|G| = 8$, $N = \langle A^2 \rangle = \{E, A^2\}$ ist die <u>einzige</u> Untergruppe der Ordnung 2

<u>zu (d)</u> Zeigen Sie, dass N ein Normalteiler von G ist, und bestimmen Sie den Isomorphietyp der Faktorgruppe G/N.

bekannt: Die Ordnung einer Untergruppe ändert sich durch Konjugation mit Gruppenelementen nicht. $\Rightarrow$ Für alle $C \in G$ ist CNC^{-1} eine Untergruppe von G der Ordnung 2. N einzige Untergruppe der Ordn. 2 $\Rightarrow CNC^{-1} = N \ \forall C \in G$
$\Rightarrow N \trianglelefteq G$

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

4 Primzahlquadrat $\Rightarrow$ G/N ist abelsch

Satz über endl. abelsche Gruppen $\Rightarrow$

$G \cong \mathbb{Z}/4\mathbb{Z}$ oder $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

bekannt: $\mathbb{Z}/4\mathbb{Z}$ hat nur ein Element der Ordnung 2 (nämlich $\bar{2}$) Gibt es in G mehr als ein Element der Ordnung 2, dann muss also $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ gelten

Sei $\bar{g} = AN$. $A \notin N$, da $N = \{E, A^2\}$

$\Rightarrow \bar{g} \neq e_{G/N}$ $\quad \bar{g}^2 = A^2 N \overset{A^2 \in N}{=} N = e_{G/N}$

Nach Def

somit ist

$\phi: GL_2(\mathbb{F}$

Homomorph

$\Rightarrow \frac{|GL_2}{|SL}$

$\det \begin{pmatrix} a & \bar{0} \\ \bar{0} & \end{pmatrix}$

$\phi\left(\begin{pmatrix} a & \bar{0} \\ \bar{0} & \end{pmatrix}\right)$

$= q-1$

$\bar g \neq e_{G/N}$. $\bar g^2 = e_{G/N} \Rightarrow \operatorname{ord}(\bar g) = 2$

Sei $\bar h = BN$. $B \notin N \Rightarrow \bar h \neq e_{G/N}$

$\bar h^2 = B^2 N = A^2 N \overset{s.o.}{=} e_{G/N}$

also: $\operatorname{ord}(\bar h) = 2$

Ang $\bar g = \bar h \Rightarrow AN = BN \Rightarrow B \in AN$

$\Rightarrow B = A$ oder $B = A^3$ ↯ Also sind $\bar g, \bar h$

zwei verschiedene Elemente der Ordnung 2 in G/N.

$\Rightarrow G/N \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ $\square$

Übung: S

Bestimmen

Homomorph

morphismus

morphismus

für alle $g \in$

H25T1A

bekannt a

(b) Zeige

$= 2$

N $\square$

Übung: Sei $G = ((\mathbb{Z}/4\mathbb{Z})^2, +)$ und $N = \{(a,a) \mid a \in \mathbb{Z}/4\mathbb{Z}\}$.
Bestimmen Sie den Isomorphietyp von G/N.

Homomorphiesatz Sei $\phi : G \to H$ ein Gruppenhomomorphismus und $N = \ker(\phi)$. Dann gibt es einen Isomorphismus $\bar{\Phi} : G/N \to \operatorname{im}(\phi)$ definiert durch $\bar{\Phi}(gN) = \phi(g)$ für alle $g \in G$.

H25T1A2 geg.: Primzahlpotenz $q > 1$

bekannt aus Teil (a): $|GL_2(\mathbb{F}_q)| = (q-1)^2 q (q+1)$

(b) Zeigen Sie: $|SL_2(\mathbb{F}_q)| = (q-1) q (q+1)$

bekannt aus Teil (a): $|GL_2(\mathbb{F}_q)| = (q-1)q(q+1)$

(b) Zeigen Sie: $|SL_2(\mathbb{F}_q)| = (q-1)q(q+1)$

Nach Def. gilt $SL_2(\mathbb{F}_q) = \{ A \in GL_2(\mathbb{F}_q) \mid \det(A) = \bar{1} \}$

somit ist $SL_2(\mathbb{F}_q)$ gleich dem Kern des Homomorphismus

$\phi : GL_2(\mathbb{F}_q) \to \mathbb{F}_q^\times,\ A \mapsto \det(A)$.

Homomorphiesatz $\Rightarrow GL_2(\mathbb{F}_q) / SL_2(\mathbb{F}_q) \cong \mathrm{im}(\phi)$

$\Rightarrow \dfrac{|GL_2(\mathbb{F}_q)|}{|SL_2(\mathbb{F}_q)|} \overset{(*)}{=} |\mathrm{im}(\phi)|$ Für alle $a \in \mathbb{F}_q^\times$ gilt

$\det\begin{pmatrix} a & \bar{0} \\ \bar{0} & \bar{1} \end{pmatrix} = a \cdot \bar{1} = a$, also $\begin{pmatrix} a & \bar{0} \\ \bar{0} & \bar{1} \end{pmatrix} \in GL_2(\mathbb{F}_q)$ und

$\phi\left(\begin{pmatrix} a & \bar{0} \\ \bar{0} & \bar{1} \end{pmatrix}\right) = a \Rightarrow \mathrm{im}(\phi) = \mathbb{F}_q^\times \Rightarrow |\mathrm{im}(\phi)| = |\mathbb{F}_q^\times|$

$= q-1$ einsetzen in $(*)$ $\Rightarrow \dfrac{(q-1)^2 q (q+1)}{|SL_2(\mathbb{F}_q)|} = q-1 \Rightarrow$

$$|SL_2(\mathbb{F}_q)| = \frac{(q-1)^2 q (q+1)}{q-1} = (q-1)\, q\, (q+1)$$

(c) Begründen Sie, dass jede Untergruppe der Ordnung q von $SL_2(\mathbb{F}_q)$ zur Untergruppe $U = \left\{ \begin{pmatrix} \bar{1} & a \\ \bar{0} & \bar{1} \end{pmatrix} \mid a \in \mathbb{F}_q \right\}$ konjugiert ist, und dass U kein Normalteiler von $SL_2(\mathbb{F}_q)$ ist.

Nach Voraussetzung existiert eine Primzahl p und ein $r \in \mathbb{N}$ mit $q = p^r$.

$p \mid q \Rightarrow p \nmid (q-1)$ und $p \nmid (q+1) \Rightarrow$ $p \nmid (q-1)(q-1)$. Wegen $|SL_2(\mathbb{F}_q)| = q \cdot (p-1) \cdot (q+1)$ sind die p-Sylowgruppen von $SL_2(\mathbb{F}_q)$ genau die Untergruppen der Ordnung q. Da $\mathbb{F}_q \to U$,

$q+1)$

gruppe

gruppe

, und

$\mathbb{F}_q)$ ist.

imzahl p

$\Longrightarrow$

$| = q \cdot (p-1)$.

$SL_2(\mathbb{F}_q)$ genau

$a\ \mathbb{F}_q \to U$.

$a \mapsto \begin{pmatrix} \bar{1} & a \\ 0 & \bar{1} \end{pmatrix}$ offenbar bijektiv ist, gilt $|U| = |\mathbb{F}_q| = q$, d.h. U ist eine p-Sylowgruppe von $SL_2(\mathbb{F}_q)$. Nach dem 2. Sylowsatz ist jede p-Sylowgruppe zu U konjugiert, also jede Untergruppe der Ordnung q. Aus dem 2. Sylowsatz folgt auch, dass U nur dann Normalteiler ist, wenn es sich bei U um die <u>einzige</u> p-Sylowgruppe, also die einzige Untergr. der Ordnung q von $SL_2(\mathbb{F}_q)$ handelt. aber: $V = \left\{ \begin{pmatrix} \bar{1} & \bar{0} \\ a & \bar{1} \end{pmatrix} \,\middle|\, a \in \mathbb{F}_q \right\}$ ist weitere Untergruppe dieser Ordnung (Nachweis: Übung)

$\Longrightarrow$ U ist kein Normalteiler von $SL_2(\mathbb{F}_q)$. $\square$

sehr ähnlich: F13T1A3