Sylowsätze

Def. Sei G eine endliche Gruppe, p eine Primzahl, $|G| = p^r m$ mit $r \in \mathbb{N}_0$, $m \in \mathbb{N}$ und $p \nmid m$. Eine Untergruppe $U \leq G$ heißt

(i) <u>p-Untergruppe</u> von G, falls $|U| = p^s$ mit $s \in \{0, 1, \dots, r\}$

(ii) <u>p-Sylowgruppe</u>, falls $|U| = p^r$ gilt.

Nullter Sylowsatz Sei G eine endliche Gruppe wie oben. Dann existiert für jedes $s \in \{0, 1, \dots, r\}$ mindestens eine Untergruppe U mit $|U| = p^s$.

(Hinweis: Ist $d \in \mathbb{N}$ ein beliebiger Teiler von $|G| = p^r m$, dann existiert im Allg. keine Untergruppe U mit $|U| = d$. Zum Beispiel hat A_4 keine Untergruppe der Ordnung 6, obwohl 6 ein Teiler von $|A_4| = 12$ ist.)

Erster Sylowsatz Jede p-Untergruppe von G (wobei G wie oben) ist in einer p-Sylowgruppe von G enthalten.

… Prim-
… N und
… ßt
… p^r gilt

Zweiter Sylowsatz Je zwei p-Sylowgruppen von G sind zueinander konjugiert. (M.a.W., die Operation von G auf der Menge der p-Sylowgruppen (durch Konjugation) ist transitiv.)

Wichtige Folgerung: Sei ν_p die Anzahl der p-Sylowgruppen von G und $P \leq G$ eine beliebige p-Sylowgr.
Dann gilt: $P \trianglelefteq G \iff \nu_p = 1$

Dritter Sylowsatz: Es gilt $\nu_p \mid m$ und $\nu_p \equiv 1 \mod p$.

bekannte Anwendungen aus der Vorlesung:

(i) Jede Gruppe der Ordnung 15 ist zyklisch.
(allgemeiner: Ist p eine Primzahl mit $p > 2$ und $p \equiv 2 \mod 3$, dann ist jede Gruppe der Ordnung $3p$ zyklisch. Also ist auch jede Gruppe der Ordnung 33, 51, 69, 87 ... zyklisch. Beweis als Übung)

(ii) Ist p eine ungerade Primzahl, dann ist jede Gruppe der Ordnung $2p$ zyklisch oder isomorph zur Diedergruppe D_p. (Bsp.: $|G| = 14 \Rightarrow G \cong \mathbb{Z}/14\mathbb{Z}$ oder $G \cong D_7$)

F23T3A3 Bestimmen Sie bis auf Isomorphie alle Gruppen der Ordnung 2023 ($2023 = 7 \cdot 17^2$)

Sei G eine Gruppe mit $|G| = 2023$. Für jede Primzahl p sei ν_p die Anzahl der p-Sylowgruppen von G. Nach dem 3. Sylowsatz gilt $\nu_{17} \mid 7$, also $\nu_{17} \in \{1, 7\}$. außerdem $\nu_{17} \equiv 1 \mod 17$, $7 \not\equiv 1 \mod 17 \Rightarrow \nu_{17} = 1$

ebenso: $\nu_7 \mid 17^2 \Rightarrow \nu_7 \in \{1, 17, 17^2\}$

G

Da

$= Z$

$|P$

($\Rightarrow$ Be

$G \cong$

$|P| = 7$

$\Rightarrow P \cong$

außerdem $\nu_7 \equiv 1 \mod 7$, $17 \equiv 3 \not\equiv 1 \mod 7$,

$17^2 \equiv 3^2 \equiv 9 \equiv 2 \not\equiv 1 \mod 7 \Rightarrow \nu_7 = 1$

Sei P die einzige 7- und Q die einzige 17-Sylowgruppe von G

<u>Beh</u>: G ist inneres direktes Produkt von P und Q. Überprüfe dafür:

(i) $P \trianglelefteq G$, $Q \trianglelefteq G$ (ii) $P \cap Q = \{e\}$

(iii) $G = PQ$

<u>zu (i)</u> $\nu_7 = 1$, 2. Sylowsatz $\Rightarrow P \trianglelefteq G$

$\nu_{17} = 1$, 2. Sylowsatz $\Rightarrow Q \trianglelefteq G$

<u>zu (ii)</u> folgt aus der Teilerfremdheit von $|P| = 7$ und $|Q| = 17^2$

f

ung

023.

die An-

von G.

$\nu_{17} \mid 7$.

n. $\nu_{17} \equiv$

$\nu_{17} = 1$

$\{1, 17, 17^2\}$

zu (iii) Wegen $P \trianglelefteq G$ und $Q \trianglelefteq G$ ist das Komplexprodukt PQ eine Untergruppe von G

$P \leq PQ \xRightarrow{\text{Lagrange}} |P| = 7$ teilt $|PQ|$

$Q \leq PQ \xRightarrow{\text{Lagrange}} |Q| = 17^2$ teilt $|PQ|$

Damit ist auch $\mathrm{kgV}(7, 17^2) = 7 \cdot 17^2 = 2023$ Teiler von $|PQ|$. $\Longrightarrow$

$|PQ| \geq 2023 = |G| \xRightarrow{PQ \subseteq G} G = PQ$

($\Rightarrow$ Beh.) Auf Grund der Beh. gilt

$G \cong P \times Q$.

$|P| = 7$ ist Primzahl $\Rightarrow$ P ist zyklisch

$\Rightarrow P \cong \mathbb{Z}/7\mathbb{Z}$

mod 7,

$= 1$

2 98

von

$= \{e\}$

G

$\trianglelefteq G$

eit von

$|Q| = 17^2$ ist Primzahlquadrat $\Rightarrow$ Q ist abelsch. Nach dem Hauptsatz für endliche abelsche Gruppen ist Q isomorph zu einem direkten Produkt von zyklischen Gruppen von Primzahlpotenzordnung > 1. Wegen $|Q| = 17^2$ sind dabei 17 und 17^2 die einzigen möglichen Primzahlpotenzen $\Rightarrow Q \cong \mathbb{Z}/17^2\mathbb{Z}$ oder $Q \cong (\mathbb{Z}/17\mathbb{Z})^2$.

insgesamt:

$$G \cong P \times Q \cong \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/17^2\mathbb{Z} \cong \mathbb{Z}/2023\mathbb{Z}$$

└ Chin. Restsatz anwend. wg. $\mathrm{ggT}(7, 17^2) = 1$

oder $G \cong \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/17\mathbb{Z} \times \mathbb{Z}/17\mathbb{Z}$

$\cong \mathbb{Z}/119\mathbb{Z} \times \mathbb{Z}/17\mathbb{Z}$

└ Chin. Restsatz anwendbar wg. $\mathrm{ggT}(7, 17) = 1$

bisher gezeigt: Es gibt höchstens zwei Isomorphietypen von Gruppen der Ordnung 2023, repräsentiert durch $G_1 = \mathbb{Z}/2023\mathbb{Z}$ und $G_2 = \mathbb{Z}/119\mathbb{Z} \times \mathbb{Z}/17\mathbb{Z}$. Um zu zeigen, dass es genau zwei Isom.-typen gibt, überprüfen wir, dass G_1 und G_2 nicht isomorph sind. In G_1 existiert mit $\bar{1}$ ein Element der Ordnung 2023. In G_2 gilt

$$119 \cdot (a, b) = (119a, 119b) = (\bar{0}, \bar{0}) = 0_{G_2}$$

für alle $a \in \mathbb{Z}/119\mathbb{Z}$, $b \in \mathbb{Z}/17\mathbb{Z}$ (wg. $17 | 119$)

Somit ist jede Elementordnung in G_2 ein Teiler von 119, und es gibt kein Element der Ordn. 2023.

Daraus folgt $G_1 \not\cong G_2$ $\square$

Übung: H15T1A3

<u>H22T3A3</u> (Übung: F15T3A3, F15T1A3)

Seien p, q, r Primzahlen mit $p < q < r$ und G eine Gruppe der Ordnung pqr. Für $i \in \{p, q, r\}$ sei ν_i jeweils die Anzahl der i-Sylowgruppen von G.

ng
2322
gen,
ver-
so-
n
ilt
$) = O_{G_2}$

(a) Zeigen Sie: Besitzt G keine normale Sylowgruppe, dann gilt $\nu_p \geq q$, $\nu_q \geq r$ und $\nu_r = pq$.

(b) Zeigen Sie, dass G eine normale Sylowgruppe besitzt.

(c) Beweisen Sie, dass keine einfache Gruppe der Ordnung 2022 existiert. (Es gilt $2022 = 2 \cdot 3 \cdot 337$, und 337 ist eine Primzahl.)

<u>zu (a)</u> 3. Sylowsatz $\Rightarrow \nu_p \mid (qr) \Rightarrow \nu_p \in \{1, q, r, qr\}$

Im Fall $\nu_p = 1$ wäre die einzige p-Sylowgruppe nach dem 2. Sylowsatz ein Normalteiler von G, im Widerspruch zur Voraussetzung $\Rightarrow \nu_p \in \{q, r, qr\}$. Wegen $qr > r > q$

g)
eiler
23.
$\square$
1A3)
r
Für
ahl den

folgt daraus $\nu_p \geq q$.

3. Sylowsatz $\Rightarrow \nu_q \mid (pr) \Rightarrow \nu_q \in \{1, p, r, pr\}$

Wieder gilt $\nu_q \neq 1$ (da sonst die einzige q-Sylowgruppe Normalteiler wäre). außerdem: $\nu_q \equiv 1 \mod q$. Ang. $\nu_q = p \Rightarrow$ $p \equiv 1 \mod q \Rightarrow q \mid (p-1) \Rightarrow q \leq p-1$ $\lightning$ zu $q > p$.

also: $\nu_q \in \{r, pr\} \overset{pr > r}{\Longrightarrow} \nu_q \geq r$

3. Sylowsatz $\Rightarrow \nu_r \mid (pq) \Rightarrow \nu_r \in \{1, p, q, pq\}$

Wie oben folgt aus der Vor., dass $\nu_r \neq 1$ ist, und aus $p < r$ und $q < r$ folgt wie oben $\nu_r \neq p$ und $\nu_r \neq q$. Also gilt $\nu_r = pq$.

<u>zu (b)</u> Allgemein gilt: Ist G eine Gruppe, p eine Primzahl, μ_p die Anzahl der Untergruppen der Ordnung p von G und α_p die Anzahl der Elemente der Ordnung p, dann gilt $\alpha_p = (p-1)\mu_p$.

Grund: Ist $g \in G$ mit $\operatorname{ord}(g) = p$, dann ist $\langle g \rangle$ die einzige Untergr. der Ordnung p, die g enthält. Andererseits ist jede Gruppe der Ordnung p zyklisch und enthält somit $\varphi(p) = p-1$ Elemente der Ordnung p.

Angenommen, G hat keine normale Sylow-gruppe. Dann gilt nach Teil (a) $r_p \geq q$, $r_q \geq r$, $r_r = pq$. Wegen $|G| = pqr$ sind die p-Sylowgruppen genau die Untergruppen der Ordnung p, ebenso für q und r. Auf Grund der Vorbem. gibt es mindestens $(p-1)q$ Elemente der Ordn. p, mind. $(q-1)\cdot r$ Elemente der Ordnung q und genau $pq(r-1)$ Elemente der Ordnung r. Zählt man dazu das Neutralelt., kommt man auf mind. $(p-1)\cdot q + (q-1)\cdot r + pq(r-1)+1$ Elemente. Wegen $|G| = pqr$ folgt

…ow-
$\geq q$,
pqr
die Un-
für q
es min-
, mind.
genau
. Zählt
…nd man
$pq(r-1)+1$
folgt

$$(p-1)q + (q-1)r + pq(r-1) + 1 \leq pqr$$

$$\Leftrightarrow \cancel{pq} - q + rq - r + \cancel{pqr} - \cancel{pq} + 1 \leq \cancel{pqr}$$

$$\Leftrightarrow rq \leq q + r - 1$$

$$\Leftrightarrow q(r-1) \leq r - 1 \quad (*)$$

Wegen $q > p \geq 2$ gilt $q \geq 3$, aus $(*)$ folgt also $3(r-1) \leq r-1$ ↯ da $r-1 \geq 1$

__zu (c)__ Ang., G ist eine einfache Gruppe der Ordnung 2022. Anwendung von Teil (b) auf die Primzahlen $p=2$, $q=3$, $r=337$ zeigt, dass G eine normale Sylowgruppe P besitzt. Auf Grund der Primfaktorzerlegung von 2022 e

e An-

g p von

te der

p-1) μ_p.

p. dann

Ordnung

ist jede

sch und ent-

mente der

gilt $|P| \in \{2, 3, 337\}$. $\Rightarrow 1 < |P| < |G|$

$\Rightarrow$ P ist nichttriv. Normalteiler von G $\lightning$ zur Einfachheit von G. $\square$

<u>Erinnerung</u>: Sei G eine Gruppe und X eine Menge.

(i) Ist $\cdot : G \times X \to X$ eine Operation von G auf X, dann ist die Abb. $\tau_g : X \to X$, $x \mapsto g \cdot x$ für jedes $g \in G$ eine Bijektion, und $G \to \mathrm{Per}(X)$, $g \mapsto \tau_g$ ist ein Gruppenhom.

(ii) Ist $\phi : G \to \mathrm{Per}(X)$ ein Hom., dann ist durch $g \cdot x = \phi(g)(x)$ für $g \in G, x \in X$ eine Op. von G auf X definiert.