Semidirekte Produkte

Ziel: Konstruktion nicht-abelscher Gruppen

gegeben: N, U Gruppen, $\phi: U \to \mathrm{Aut}(N)$ Gruppenhomomorphismus

Def. (äußeres) semidirektes Produkt von N und U bzgl. ϕ = Gruppe $N \rtimes_\phi U$ bestehend aus der Menge $N \times U$ und der Verknüpfung geg. durch

$$(n_1, u_1) * (n_2, u_2) = (n_1 \underbrace{\phi(u_1)}_{\in \mathrm{Aut}(N)}(n_2), u_1 u_2)$$

$$(n_1, u_1) * (u_2, u_2) = (n_1 \phi(u_1)(n_2), u_1 u_2)$$

Die Gruppe $N \rtimes_\phi U$ ist genau dann nicht-abelsch, wenn N nicht-abelsch ist <u>oder</u> U nicht-abelsch ist <u>oder</u> der Hom ϕ nichttrivial ist, d.h. es gilt <u>nicht</u> $\phi(u) = \mathrm{id}_N \; \forall u \in U$.

<u>Frage</u>: Wenn N und U zyklische Gruppen sind, $N = \mathbb{Z}/n\mathbb{Z}$ $U = \mathbb{Z}/u\mathbb{Z}$ mit $n, u \in \mathbb{N}$, wie findet man einen nichttrivialen Hom.

$$\phi : U \to \mathrm{Aut}(N) \quad ?$$

bekannt aus der Vorlesung:

- Es gilt $\mathrm{Aut}(N) = \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^*$.

Bsp

(dan

Gru

Es genügt somit, einen nichttrivialen Hom. $\mathbb{Z}/u\mathbb{Z} \to (\mathbb{Z}/n\mathbb{Z})^\times$ anzugeben.

- Über die Struktur von $(\mathbb{Z}/n\mathbb{Z})^\times$ ist bekannt:

  Ist $n = \prod_{j=1}^{r} p_j^{e_j}$ die Primfaktorzerlegung von n, dann gilt $(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{e_1}\mathbb{Z})^\times \times \ldots \times (\mathbb{Z}/p_r^{e_r}\mathbb{Z})^\times$ auf Grund des Chinesischen Restsatzes. außerdem:

  p ungerade Primzahl, $e \geq 1 \Rightarrow (\mathbb{Z}/p^e\mathbb{Z})^\times \cong \mathbb{Z}/p^{e-1}(p-1)\mathbb{Z}$

  $(\mathbb{Z}/2\mathbb{Z})^\times = \{\bar{1}\}$, $(\mathbb{Z}/4\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z}$ und

  $(\mathbb{Z}/2^e\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{e-2}\mathbb{Z} \quad \forall e \geq 3$.

$(\mathbb{Z}/2\mathbb{Z})^\times = \{\bar{1}\}$. $(\mathbb{Z}/4\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z}$ und

- Existenz von Hom auf zyklischen Gruppen:

Ist G eine bel. Gruppe und $g \in G$ mit $\mathrm{ord}(g) \mid u$, dann existiert ein eind. bestimmter Hom. $\phi : \mathbb{Z}/u\mathbb{Z} \to G$ mit $\phi(\bar{1}) = g$. Ein nichttrivialer Hom. $\phi : \mathbb{Z}/u\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ existiert also genau dann, wenn in $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ (oder $(\mathbb{Z}/n\mathbb{Z})^\times$) ein Element σ mit $\mathrm{ord}(\sigma) \mid u$ und $\mathrm{ord}(\sigma) > 1$ existiert.

__Bsp.__: Es gibt einen nichttriv. Hom. $\phi : \mathbb{Z}/3\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/56\mathbb{Z})$. (dann ist $\mathbb{Z}/56\mathbb{Z} \rtimes_\phi \mathbb{Z}/3\mathbb{Z}$ eine nicht-abelsche Gruppe der Ordnung 168).

Es gilt $\mathrm{Aut}(\mathbb{Z}/56\mathbb{Z}) \cong (\mathbb{Z}/56\mathbb{Z})^\times \cong$
$(\mathbb{Z}/8\mathbb{Z})^\times \times (\mathbb{Z}/7\mathbb{Z})^\times \cong (\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/6\mathbb{Z}$.

$\Rightarrow$ genügt z.zg.: Es gibt einen nichttriv. Hom. $\mathbb{Z}/3\mathbb{Z} \to (\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/6\mathbb{Z}$.

Benötige dafür in $(\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/6\mathbb{Z}$ ein Element der Ordnung 3, z.B. $(\bar{0},\bar{0},\bar{2})$.

(Es gilt $\mathrm{ord}((\bar{0},\bar{0},\bar{2})) = 3$ wg. $(\bar{0},\bar{0},\bar{2}) \neq (\bar{0},\bar{0},\bar{0})$ und $3\cdot(\bar{0},\bar{0},\bar{2}) = (\bar{0},\bar{0},\bar{6}) = (\bar{0},\bar{0},\bar{0})$.)

(c)

zu (a)

der O

ist , i

2. Fal

Sei G

Sei ν_3

Sylow

$\Rightarrow \nu_p$

$3 \neq$

Aufgaben zum semidirekten Produkt:

Zahlenbeispiele: F13T3A1, F16T2A2(b), F20T1A3

Theorie: H16T2A2(a), H21T1A4

Aufgabe

(a) Sei p eine Primzahl. Zeigen Sie: Genau dann ist jede Gruppe der Ordnung $3p$ abelsch, wenn $p = 3$ oder zugleich $p > 2$ und $p \equiv 2 \mod 3$ erfüllt ist.

(b) Geben Sie drei paarweise nicht isomorphe nicht abelsche Gruppen der Ordnung 70 als äußere semidirekte Produkte zyklischer Gruppen an.

eb

auße

$p \neq$

Sei

3-Sy

Produ

(i) $P,$

zu (i)

zu (ii)

zu (iii)

$P \leq P$

(c) Zeigen Sie, dass eine der Gruppen aus (b) isomorph zur Diedergruppe D_{35} ist.

<u>zu (a)</u> „$\Longleftarrow$" 1. Fall: $p = 3$ Sei G eine Gruppe der Ordnung 9. Da $9 = 3^2$ ein Primzahlquadrat ist, ist G abelsch.

2. Fall: $p > 2$ und $p \equiv 2 \mod 3$

Sei G eine Gruppe der Ordnung $3p$.

Sei ν_3 bzw. ν_p die Anzahl der 3- bzw. p-Sylowgruppen. 3. Sylowsatz $\Rightarrow \nu_p \mid 3$.

$\Rightarrow \nu_p \in \{1, 3\}$, außerdem $\nu_p \equiv 1 \mod p$.

$3 \not\equiv 1 \mod p$ wegen $p > 2 \Rightarrow \nu_p = 1$

Produkt:
1, F16T2A2(b),
3
T1A4

Sie: Genau
Ordnung 3p
zugleich $p > 2$
t.
se nicht isomorphe
Ordnung 70
Produkte zyklischer

ebenso: $\nu_3 \mid p$, p prim $\Rightarrow$ $\nu_3 \in \{1, p\}$

außerdem $\nu_3 \equiv 1 \mod 3$, $p \equiv 2 \mod 3$ $\Rightarrow$
$p \not\equiv 1 \mod 3$ (da $1 \not\equiv 2 \mod 3$) $\Rightarrow$ $\nu_3 = 1$

Sei P die einzige p- und Q die einzige 3-Sylowgruppe. Beh.: G ist inneres direktes Produkt von P und Q überprüfe:

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

zu (i) folgt wegen $\nu_3 = \nu_p = 1$ aus dem 2. Sylowsatz

zu (ii) folgt aus der Teilerfremdheit von $|P| = p$ und $|Q| = 3$ ($3, p$ verschiedene Primzahlen)

zu (iii) $P \trianglelefteq G$, $Q \leq G$ $\Rightarrow$ PQ ist Untergr. von G
$P \leq PQ$, $Q \leq PQ$, Lagrange $\Rightarrow$ $|P| = p$ und

sym-

$2 \wedge$

lt –

t.

$2 \bmod 3)$

$|Q| = 3$ sind Teiler von $|PQ| \Rightarrow \mathrm{kgV}(3, p) = 3p$ teilt $|PQ| \Rightarrow |PQ| \geq 3p = |G| \overset{PQ \subseteq G}{\Longrightarrow} PQ = G$ ($\Rightarrow$ Beh.)

Aus der Beh. folgt $G \cong P \times Q$. Als Gruppen von Primzahlordnung sind P und Q abelsch, damit auch $P \times Q$ und G.

„$\Rightarrow$" Setze voraus, dass $p \neq 3$ und $p \not\equiv 2 \bmod 3$.

zeige: Dann gibt es eine nicht-abelsche Gruppe der Ordnung $3p$.

Sei $N = \mathbb{Z}/p\mathbb{Z}$ und $U = \mathbb{Z}/3\mathbb{Z}$.

<u>Beh.</u>: ~~Es~~ gibt einen nichttriv. Hom. $\phi: U \to \mathrm{Aut}(N)$.

Ist dies gezeigt, dann folgt daraus, dass $N \rtimes_\phi U$ eine nicht-abelsche Gruppe der Ordnung $3p$ ist.

Laut Vorlesung gilt $\mathrm{Aut}(N) \cong (\mathbb{Z}/p\mathbb{Z})^* \cong \mathbb{Z}/(p-1)\mathbb{Z}$, da p eine ungerade Primzahl ist. Es genügt somit zu zeigen, dass ein nicht triv. Hom. $\mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}/(p-1)\mathbb{Z}$ existiert. Ist $a \in \mathbb{Z}/(p-1)\mathbb{Z}$ ein Element der Ordnung 3, dann existiert lt. Vl. ein Hom. $\phi : \mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}/(p-1)\mathbb{Z}$ mit $\phi(\bar{1}) = a$, und dieser Hom. ist dann nicht trivial.

Da $\mathbb{Z}/(p-1)\mathbb{Z}$ zyklisch ist, existiert ein solches Element, wenn 3 ein Teiler von $p-1$ ist. $p \not\equiv 2 \mod 3 \Rightarrow p \equiv 0 \mod 3$ oder $p \equiv 1 \mod 3$.

<u>1. Fall</u>: $p \equiv 0 \mod 3 \Rightarrow 3 \mid p \xRightarrow{p \text{ Primzahl}} p = 3$ ↯

<u>2. Fall</u>: $p \equiv 1 \mod 3$ Dann gilt $3 \mid (p-1)$.

Ist $p = 2$, dann gibt es ebenfalls eine nicht-abelsche Gruppe der Ordnung $3p$, nämlich die symmetrische Gruppe S_3.

(Logik: Unter der Bed. $\varphi = \neg(p=3 \vee (p>2 \wedge p \equiv 2 \mod 3))$ ist zzg., dass es eine nicht-abelsche Gruppe der Ordnung $3p$ gibt.

Es gilt $\varphi \iff p \neq 3 \wedge \neg(p>2 \wedge p \equiv 2 \mod 3)$

$\iff p \neq 3 \wedge (p=2 \vee p \not\equiv 2 \mod 3)$

$\iff p = 2 \vee (p \neq 3$ und $p \not\equiv 2 \mod 3)$.)

zu (b) $70 = 2 \cdot 5 \cdot 7$ Sei $U = \mathbb{Z}/2\mathbb{Z}$
und $N = \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$ (Nach dem Chin. Restsatz ist $N \cong \mathbb{Z}/35\mathbb{Z}$ wg. $ggT(5,7) = 1$
also ist nicht nur U, sondern auch N zyklisch!)

Für die Konstruktion nicht-abelscher Gruppen benötigen wir nichttriv. Hom. $\mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(N)$
und dafür wiederum benötigen wir Elemente in $\mathrm{Aut}(N)$ von Ordnung 2.
Betrachte die Elemente $\rho, \sigma, \tau \in \mathrm{Aut}(N)$
geg. durch $\rho: \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \to \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}, (a,b) \mapsto (-a,-b)$

$\sigma: \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \to \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}, (a,b) \mapsto (-a, b)$

$\tau: \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \to \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}, (a,b) \mapsto (a, -b)$

Es ist $\mathrm{ord}(\rho) = 2$, denn $\rho \neq \mathrm{id}$ und

$\rho^2(a,b) = \rho(-a,-b) = \rho(-(-a), -(-b)) = (a,b)$

$\forall (a,b) \in \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$, also $\rho^2 = \mathrm{id}$.

Genauso zeigt man $\mathrm{ord}(\sigma) = \mathrm{ord}(\tau) = 2$.

Definiere nun $\phi_1, \phi_2, \phi_3 : U \to \mathrm{Aut}(N)$ durch

$\phi_1(\bar{1}) = \rho$, $\phi_2(\bar{1}) = \sigma$, $\phi_3(\bar{1}) = \tau$ und

$G_1 = N \rtimes_{\phi_1} U$, $G_2 = N \rtimes_{\phi_2} U$, $G_3 = N \rtimes_{\phi_3} U$.

Wg. ρ, σ, τ sind ϕ_1, ϕ_2, ϕ_3 nichttrivial

und somit G_1, G_2, G_3 nicht abelsch, von Ord-

$\Leftarrow$

$\Leftarrow$

Im F

$c =$

$\Rightarrow 1$

1 oder

in de

$\phi_1(\bar 1) = \rho,\ \phi_2(\bar 1) = \sigma,\ \phi_3(\bar 1) = \tau$ und

...ung $|N| \cdot |U| = 35 \cdot 2 = 70$.

Wir zeigen, dass G_1, G_2, G_3 paarweise nicht isomorph sind, in dem wir zeigen, dass die Anzahl der Elemente der Ordnung 2 unterschiedlich ist.

Sei $((a,b),c) \in G_1$ $(a \in \mathbb{Z}/5\mathbb{Z}, b \in \mathbb{Z}/7\mathbb{Z}, c \in \mathbb{Z}/2\mathbb{Z})$

$\operatorname{ord}((a,b),c) \in \{1,2\} \Leftrightarrow$

$((a,b),c) * ((a,b),c) = ((\bar 0,\bar 0),\bar 0) \Leftrightarrow$

$((a,b) + \phi_1(c)(a,b), c+c) = ((\bar 0,\bar 0),\bar 0) \Leftrightarrow$

$\left(c = \bar 0 \text{ und } ((a,b)+(a,b), \bar 0) \overset{(*)}{=} (\bar 0,\bar 0)\right)$

oder $\left(c = \bar 1 \text{ und } ((a,b) + \rho(a,b), \bar 0) = (\bar 0, \bar 0)\right)$

$(*)$ $\phi_1(\bar 0)(a,b) = \mathrm{id}(a,b) = (a,b)$

$\phi_1(\bar 1)(a,b) = \rho(a,b)$

Se...

ord...

$(c = \bar 0$ ...

$(c = \bar 1$ ...

$(c = \bar 0$ ...

$(c = \bar 1$ ...

$(c = \bar 0$ ...

$(c = \bar 1$ ...

$(c = \bar 0$ ...

$(c = \bar 1$ ...

Gilt, ...

$(a,b) \to$ ...

$\Rightarrow 5$ ...

$b)$

$-b)$

$) = (a,b)$

id

$) = 2.$

$)$ durch

und

$N \rtimes_{\phi_3} U.$

ttrivial

, von Ord-

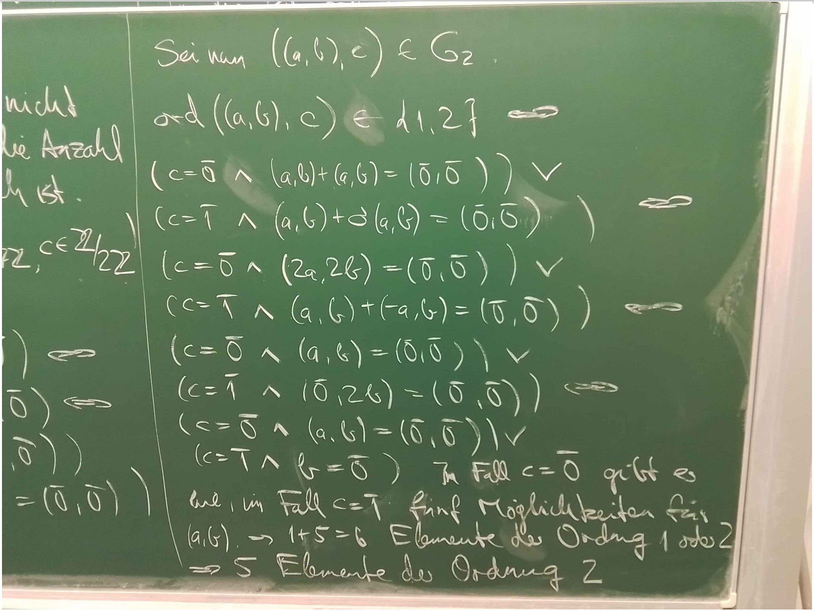
$\iff \big((2a,2b) = (\bar{0},\bar{0})$ und $c = \bar{0} \big)$

$\big((a,b)+(-a,-b) \big) = (\bar{0},\bar{0})$ und $c = \bar{1} \big)$

$\iff \big((a,b) = (\bar{0},\bar{0})$ und $c = \bar{0} \big)$ oder $c = \bar{1}$

Im Fall $c = \bar{0}$ gibt es eine, im Fall $c = \bar{1}$ 35 Mögl. für (a,b)

$\Rightarrow 1+35 = 36$ Elemente der Ordn. 1 oder 2 $\Rightarrow$ 35 Elemente der Ordn. 2 in der Gruppe G.



Genauso kommt man zu dem Ergebnis, dass die Gruppe G_3 genau 7 Elemente der Ordnung 2 enthält.