Semidirekte Produkte

Def.: Seien U und N Gruppen und $\phi : U \to \mathrm{Aut}(N)$ ein Homomorphismus. Dann nennt man $N \times U$ mit der Verknüpfung $*$ geg. durch

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

das äußere semidirekte Produkt von N und U bzgl. ϕ (Notation: $N \rtimes_\phi U$)

Eigenschaften

- Ist der Hom ϕ nicht trivial (d.h. es gilt nicht $\phi(u) = id_N \ \forall u \in U$), dann ist die Gruppe $N \rtimes_\phi U$ nicht abelsch). Grund:

Sei $u \in U$ mit $\phi(u) \neq id_N$ und $n \in N$ mit $\phi(u)(n) \neq n$, dann gilt

$$(e_N, u) * (n, e_U) = (e_N \phi(u)(n), u \cdot e_U) = (\phi(u)(n), u)$$

$$(n, e_U) * (e_N, u) = (n \underbrace{\phi(e_U)}_{= id_N}(e_N), e_U \cdot u) = (n, u)$$

also $(e_N, u) * (n, e_U) \neq (n, e_U) * (e_N, u)$.

$(gh)^2 = e = (\bar{0}, \bar{0})$.

$gh = (\bar{1}, \bar{0}) * (\bar{0}, \bar{1}) = (\bar{1} + \phi(\bar{0})(\bar{0}), \bar{0} + \bar{1}) =$

- Ist G ein inneres semidirektes Produkt von $N \trianglelefteq G$ und $U \leq G$, dann gilt $G \cong N \rtimes_\phi U$, wobei $\phi : U \to \mathrm{Aut}(N)$ jedes $u \in U$ auf die Konjugationsabb. $c_u : N \to N$, $n \mapsto unu^{-1}$ abbildet.

Standardbeispiel: Sei $n \in \mathbb{N}$, $n \geq 3$.
Setze $N = (\mathbb{Z}/n\mathbb{Z}, +)$, $U = (\mathbb{Z}/2\mathbb{Z}, +)$. Dann ist $\iota : N \to N$, $\bar{a} \mapsto -\bar{a}$ ein Element von $\mathrm{Aut}(N)$, und durch $\bar{0} \mapsto \mathrm{id}_N$, $\bar{1} \mapsto \iota$ ist ein Hom. $\phi : U \to \mathrm{Aut}(N)$ definiert.

Beh: $N \rtimes_\phi U \cong D_n$

2.2g: Es gibt $g, h \in N \rtimes_\phi U$ mit $\operatorname{ord}(g) = n$, $\operatorname{ord}(h) = 2$, $(gh)^2 = e$ und $N \rtimes_\phi U = \langle g, h \rangle$.

Setze $g = (\bar{1}, \bar{0})$, $h = (\bar{0}, \bar{1})$. Überprüfe nur $(gh)^2 = e = (\bar{0}, \bar{0})$.

$$g \cdot h = (\bar{1}, \bar{0}) * (\bar{0}, \bar{1}) = (\bar{1} + \phi(\bar{0})(\bar{0}), \bar{0} + \bar{1}) =$$

$$(\bar{1} + \mathrm{id}_N(\bar{0}), \bar{1}) = (\bar{1}, \bar{1})$$

$$(gh)^2 = gh\, gh = (\bar{1}, \bar{1}) * (\bar{1}, \bar{1}) = (\bar{1} + \phi(\bar{1})(\bar{1}), \bar{1} + \bar{1})$$

$$= (\bar{1} + \iota(\bar{1}), \bar{0}) = (\bar{1} + (-\bar{1}), \bar{0}) = (\bar{0}, \bar{0})$$

<u>Erinnerung</u>: Für jedes $n \in \mathbb{N}$ gilt $(\mathbb{Z}/n\mathbb{Z})^\times \cong \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}, +)$, wobei ein Isom. durch $a + n\mathbb{Z} \mapsto \sigma_a$ definiert ist, mit σ_a geg. durch $\sigma_a(\bar{1} + n\mathbb{Z}) = a + n\mathbb{Z}$.

<u>Bsp.</u> $\mathrm{Aut}(\mathbb{Z}/4\mathbb{Z}, +) = \{\sigma_1, \sigma_3\}$

mit $\sigma_1(1 + 4\mathbb{Z}) = \bar{1} + 4\mathbb{Z}$ $(\Rightarrow \sigma_1 = \mathrm{id}_{\mathbb{Z}/4\mathbb{Z}})$

und $\sigma_3(\bar{1} + 4\mathbb{Z}) = 3 + 4\mathbb{Z}$)

$\bar{a}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\sigma_3(\bar{a})$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

$\sigma_3(\bar{2}) = \sigma_3(\bar{1} + \bar{1}) =$
$\sigma_3(\bar{1}) + \sigma_3(\bar{1}) = \bar{3} + \bar{3}$
$= \bar{6} = \bar{2}$

außerdem:

- $(\mathbb{Z}/mn\mathbb{Z})^\times \cong (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$ falls $\operatorname{ggT}(m,n) = 1$
- $(\mathbb{Z}/p^e\mathbb{Z})^\times \cong \mathbb{Z}/p^{e-1}(p-1)\mathbb{Z}$ falls $e \in \mathbb{N}$ und p ungerade Primzahl
- $(\mathbb{Z}/2\mathbb{Z})^\times = \{\bar{1}\}$, $(\mathbb{Z}/4\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z}$ und $(\mathbb{Z}/2^e\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{e-2}\mathbb{Z}$ falls $e \geq 3$

Kriterium für die Existenz von Hom.:

Ist $G = \langle g \rangle$ eine zykl. Gruppe der Ordnung $n \in \mathbb{N}$, H eine weitere Gruppe und $h \in H$ mit $\operatorname{ord}(h) \mid n$, dann existiert ein eind. best. Hom. $\Phi : G \to H$

mit $\phi(g) = h$

F20T1A3 (a), (b) Übung

(c) Geben Sie zwei nicht isomorphe abelsche und zwei nicht-isom. nicht abelsche Gruppen der Ordnung 2020 an. ($2020 = 4 \cdot 5 \cdot 101$, und 101 ist Primzahl)

Sei $G_1 = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/505\mathbb{Z}$ und $G_2 = (\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/505\mathbb{Z}$

Diese Gruppen sind abelsch von Ordnung 2020 (da $4 \cdot 505 = 2^2 \cdot 505 = 2020$). Ang. G_1, G_2 sind isomorph. Es ist $g_1 = (\bar{1}, \bar{0}) \in G_1$ ein Element der Ordnung 4 wegen $2 \cdot g_1 = (\bar{2}, \bar{0}) \neq (\bar{0}, \bar{0})$ und $4 \cdot g_1 = (\bar{4}, \bar{0}) = (\bar{0}, \bar{0})$. Wegen $G_1 \cong G_2$ muss es

...un

...et (d,

$a + n\mathbb{Z}$.

$\mathbb{Z}/4\mathbb{Z})$

$(\bar 1 + \bar 1) =$

$\bar 1) = \bar 3 + \bar 3$

auch in G_2 ein Element der Ordn. 4 geben.

aber: $1010 \cdot (\bar a, \bar b, \bar c) = (\overline{1010\, a}, \overline{1010\, b}, \overline{1010\, c}) =$
$(\bar 0, \bar 0, \bar 0) \ \forall (\bar a, \bar b, \bar c) \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/505\mathbb{Z}$

$\Rightarrow$ Alle Elementordn. in G_2 sind Teiler von 1010.

↯ da $4 \nmid 1010$.

Sei $G_3 = D_{1010}$ (Diedergr. der Ordnung 2020) und

$G_4 = \mathbb{Z}/4\mathbb{Z} \times (N \rtimes_\phi U)$, wobei

$N = \mathbb{Z}/101\mathbb{Z}$, $U = \mathbb{Z}/5\mathbb{Z}$ und

$\phi : \mathbb{Z}/5\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/101\mathbb{Z})$ dadurch zu-
Stande kommt, dass wir den eind. best.
Hom. $\psi : \mathbb{Z}/5\mathbb{Z} \to \mathbb{Z}/100\mathbb{Z}$ mit $\psi(\bar 1) =$
$\overline{20}$ mit einem Isom. $\iota : \mathbb{Z}/100\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/101\mathbb{Z})$

zusammensetzen. (Es gilt $\mathrm{Aut}(\mathbb{Z}/101\mathbb{Z})$
$\cong (\mathbb{Z}/101\mathbb{Z})^\times \cong \mathbb{Z}/100\mathbb{Z}$, weil 101 eine
Primzahl ist.) Der Hom. ϕ ist nicht-
trivial, weil ψ wegen $\psi(\bar{1}) = \overline{20} \neq \bar{0}$
nichttriv. und ι ein Isomorphismus ist
$\Rightarrow N \rtimes_\phi U$ ist nicht-abelsche Gruppe der
Ordnung 505
$\Rightarrow G_4 = \mathbb{Z}/4\mathbb{Z} \times (N \rtimes_\phi U)$ ist nicht-
abelsche Gruppe der Ordnung 2020.

Be
w
Di
Ri

<u>Beh</u>: $G_3 \not\cong G_4$

Das Element $g_4 = (\bar{1}, e_{N \rtimes_\phi U})$ in G_4 ist von Ordnung 4 wegen $g_4^2 = (2 \cdot \bar{1}, e_{N \rtimes_\phi U}^2)$
$= (\bar{2}, e_{N \rtimes_\phi U}) \neq (\bar{0}, e_{N \rtimes_\phi U}) = e_{G_4}$ und
$g_4^4 = (4 \cdot \bar{1}, e_{N \rtimes_\phi U}^4) = (\bar{0}, e_{N \rtimes_\phi U}) = e_{G_4}$.

Wäre $G_3 \cong G_4$, dann müsste es auch in $G_3 = D_{1010}$ ein Element der Ordn. 4 geben.

Allgemein existieren in D_n mit $n \geq 3$ nur Elemente der Ordnung 2 und solche, deren

Ordnung ein Teiler von n ist. Aber 4 ist kein Teiler von 1010, deshalb existiert in G_3 kein Element der Ordnung 4. $\square$

Übungen zum semidir. Produkt:

F13T3A1 (Zahlenbsp)

H21T1A4 (Theorie)

<u>Hinweis</u>: Häufig lassen sich verschiedene semidirekte Produkte dadurch unterscheiden, dass man die Anzahl der Elemente der Ordnung 2 bestimmt.

Ringtheorie

Def: Ring = Menge R mit zwei Verknüpfungen $+$ und $\cdot$, so dass gilt (1) $(R,+)$ ist abelsche Gruppe

(2) $(R,\cdot)$ ist abelsches Monoid

(3) Es gilt das Distributivgesetz $a\cdot(b+c) = a\cdot b + a\cdot c$ für alle $a, b, c \in R$.

Bem: Einige Autoren fordern unter (2) nur „Halbgruppe", und unter (3) noch das Gesetz $(a+b)\cdot c = a\cdot c + b\cdot c \ \forall a, b, c \in R$.
Die Definition von oben entspricht dann einem „kommutativen Ring mit 1".

Def. Sei $(R,+,\cdot)$ ein Ring.

(i) $a \in R$ ist <u>Einheit</u> $\Leftrightarrow \exists c \in R: ac = 1_R$

$R^\times$ = Einheitengruppe von R = Menge der Einheiten mit der Multiplikation als Verknüpfung.

(ii) $a \in R$ ist <u>Nullteiler</u> $\Leftrightarrow \exists c \in R \setminus \{0_R\}$ mit $a \cdot c = 0_R$ (Bsp: $\overline{2}$ in $\mathbb{Z}/4\mathbb{Z}$, $(1,0), (0,1)$ in $\mathbb{Z} \times \mathbb{Z}$)

(iii) <u>Integritätsbereich</u> = Ring R, in dem $\{0_R\}$ die Menge der Nullteiler ist

(iv) <u>Körper</u> = Ring R mit der Eigenschaft $R^\times = R \setminus \{0_R\}$

(Jeder Körper ist ein Integritätsbereich.)

Def Sei $(R, +, \cdot)$ ein Ring.

Teilring von R = Teilmenge S mit den Eigenschaften $1_R \in S$ und $\forall a, b \in S$:

$a - b,\ ab \in S$