

# Geometrie

Eric Kunze

17. November 2018

# Kapitel 1

## Endliche Gruppen

# 1 Erinnerung und Beispiele

## 1.1 Erinnerung

Eine Gruppe ist ein Paar  $(G, \star)$  bestehend aus einer Menge  $G$  und einer Abbildung  $\star : G \times G \rightarrow G$ , das die Axiome Assoziativität, Existenz eines neutralen Elements und Existenz eines inversen Elements erfüllt. Wir schreiben auch  $G$  für  $(G, \star)$ . Die Gruppe ist abelsch, wenn  $g \star h = h \star g$  für alle  $g, h \in G$  gilt. Eine allgemeine Gruppe schreiben wir multiplikativ mit neutralem Element 1, abelsche Gruppen auch additiv mit neutralem Element 0.

Eine Teilmenge  $H \subseteq G$  ist eine Untergruppe von  $G$ , in Zeichen  $H \leq G$ , wenn  $H \neq \emptyset$  und  $H$  abgeschlossen ist unter der Verknüpfung und dem Bilden von Inversen.

Wir schreiben 1 (bzw. 0) für die triviale Untergruppe  $\{1\}$  (bzw.  $\{0\}$ ) von  $G$ .

Eine Abbildung  $\varphi : G \rightarrow G'$  zwischen Gruppen ist ein Gruppenhomomorphismus, wenn

$$\varphi(g_1 \cdot g_2) = \varphi(g_1) \cdot \varphi(g_2)$$

für alle  $g_1, g_2 \in G$  und in diesem Fall ist

$$\text{Ker}(\varphi) := \varphi^{-1}(\{1\})$$

der Kern von  $\varphi$ .

Wir schreiben  $\text{Hom}(G, G')$  für die Menge der Gruppenhomomorphismen  $\varphi : G \rightarrow G'$ .

## 1.2 Beispiel

Sei  $n \in \mathbb{N}$ ,  $K$  ein Körper und  $X$  eine Menge.

a)  $\text{Sym}(X)$ , die symmetrische Gruppe aller Permutationen der Menge  $X$  mit  $f \cdot g = g \circ f$ , insbesondere  $S_n := \text{Sym}(\{1, \dots, n\})$ . Für  $n \in \{1, 2\}$  ist  $S_n$  abelsch.

b)  $\mathbb{Z}$  und  $\mathbb{Z}/n\mathbb{Z} := \{a + n\mathbb{Z} : a \in \mathbb{Z}\}$  mit der Addition.

c)  $\text{GL}_n(K)$  mit der Matrizenmultiplikation. Spezialfall:

$$\text{GL}_1(K) = K^\times = K \setminus \{0\}$$

d) Für jeden Ring  $R$  bilden die Einheiten  $R^\times$  eine Gruppe unter Multiplikation, z.B.  $\text{Mat}_n(K)^\times = \text{GL}_n(K)$  oder  $\mathbb{Z}^\times = \mu_2 = \{1, -1\}$

## 1.3 Beispiel

Ist  $(G, \cdot)$  eine Gruppe, so ist auch  $(G^{op}, \cdot^{op})$  mit  $G^{op} = G$  und  $g \cdot^{op} h = h \cdot g$  eine Gruppe.

## 1.4 Bemerkung

Ist  $G$  eine Gruppe und  $h \in G$ , so ist die Abbildung

$$\tau_h : \begin{cases} G \rightarrow G \\ g \mapsto g \cdot h \end{cases}$$

eine Bijektion (also  $\tau_h \in \text{Sym}(G)$ ) mit Umkehrabbildung  $\tau_{h^{-1}}$ .

## 1.5 Satz (vgl. LAAG I.3.8)

Sei  $G$  eine Gruppe. Zu jeder Teilmenge  $X \subseteq G$  gibt es eine kleinste Untergruppe  $\langle X \rangle$  von  $G$ , die  $X$  enthält, nämlich

$$\langle X \rangle = \bigcap_{X \subseteq H \leq G} H$$

## 1.6 Bemerkung

Man nennt  $\langle X \rangle$  die von  $X$  erzeugte Untergruppe  $G$ . Die Gruppe  $G$  heißt endlich erzeugt, wenn  $G = \langle X \rangle$  für eine endliche Menge  $X \subseteq G$ .

Bsp.:  $\mathbb{Z} = \langle \{1\} \rangle$

**1.7 Satz (vgl. LAAG II.2.8)**

Ein Gruppenhomomorphismus  $\varphi : G \rightarrow G'$  ist genau dann ein Isomorphismus, wenn es einen Gruppenhomomorphismus  $\varphi' : G' \rightarrow G$  mit  $\varphi' \circ \varphi = \text{id}_G$  und  $\varphi \circ \varphi' = \text{id}_{G'}$  gibt.

**1.8 Beispiel**

Ist  $G$  eine Gruppe, so bilden die Automorphismen  $\text{Aut}(G) \subseteq \text{Hom}(G, G)$  eine Gruppe unter  $\varphi \cdot \varphi' = \varphi' \circ \varphi$ . Ist  $\varphi \in \text{Aut}(G)$  und  $g \in G$  schreiben wir auch  $g^\varphi := \varphi(g)$ .

**1.9 Satz (vgl. LAAG III.2.14)**

Ein Gruppenhomomorphismus  $\varphi : G \rightarrow G'$  ist genau dann injektiv, wenn  $\text{Ker}(\varphi) = 1$ .

**1.10 Beispiel**

Seien  $n \in \mathbb{N}$  und  $K$  ein Körper.

- a)  $\text{sgn} : S_n \rightarrow \mu_2$  ist ein Gruppenhomomorphismus mit Kern die alternierende Gruppe  $A_n$
- b)  $\det : \text{GL}_n(K) \rightarrow K^\times$  ist ein Gruppenhomomorphismus (vgl. Determinantenmultiplikationssatz) mit Kern  $\text{SL}_n(K)$
- c)  $\pi_{n\mathbb{Z}} : \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}, a \mapsto a + n\mathbb{Z}$  ist ein Gruppenhomomorphismus mit Kern  $n\mathbb{Z}$
- d) Ist  $A$  eine abelsche Gruppe, so ist

$$[n] : \begin{cases} A \rightarrow A \\ x \mapsto n \cdot x \end{cases}$$

ein Gruppenhomomorphismus mit Kern  $A[n]$ , die  $n$ -Torsion von  $A$ , und Bild  $nA$

- e) Ist  $G$  eine Gruppe, so ist

$$\begin{cases} G \rightarrow G^{op} \\ g \mapsto g^{-1} \end{cases}$$

ein Isomorphismus (vgl. Übung)

**1.11 Definition**

Seien  $n, k \in \mathbb{N}$ . Für paarweise verschiedene Elemente  $i_1, \dots, i_k \in \{1, \dots, n\}$  bezeichnen wir mit  $(i_1 \dots i_k)$  das  $\sigma \in S_n$  gegeben durch

$$\begin{aligned} \sigma(i_j) &= i_{j+1} \quad \text{für } j = 1, \dots, k-1 \\ \sigma(i_k) &= i_1 \\ \sigma(i) &= i \quad \text{für } i \in \{1, \dots, n\} \setminus \{i_1, \dots, i_k\} \end{aligned}$$

Wir nennen  $(i_1 \dots i_k)$  einen  $(k)$ -Zykel.

Zwei Zyklen  $(i_1 \dots i_k)$  und  $(j_1 \dots j_l) \in S_n$  heißen disjunkt, wenn

$$\{i_1, \dots, i_k\} \cap \{j_1, \dots, j_l\} = \emptyset$$

**1.12 Satz (LAAG IV.1.3)**

Jedes  $\sigma \in S_n$  ist Produkt von Transpositionen (d.h. 2-Zyklen).

**1.13 Lemma**

Disjunkte Zyklen kommutieren, d.h. sind  $\tau_1, \tau_2 \in S_n$  disjunkte Zyklen, so ist

$$\tau_1 \tau_2 = \tau_2 \tau_1$$

*Beweis.* Sind  $\tau_1 = (i_1 \dots i_k)$  und  $\tau_2 = (j_1 \dots j_l)$ , so ist

$$\tau_1 \tau_2(i) = \tau_2 \tau_1(i) = \begin{cases} \tau_1(i) & i \in \{i_1, \dots, i_k\} \\ \tau_2(i) & i \in \{j_1, \dots, j_l\} \\ i & \text{sonst} \end{cases}$$

### 1.14 Satz (Zykelzerlegung)

Jedes  $\sigma \in S_n$  ist ein Produkt von paarweise disjunkten  $k$ -Zyklen mit  $k \geq 2$ , eindeutig bis auf Reihenfolge (sogenannte Zykelzerlegung von  $\sigma$ )

*Beweis.* Induktion nach  $N := |\{i : \sigma(i) = i\}|$  (sogenannter Stabilisator von  $\sigma$ )

(IA)  $N = 0$ :  $\sigma = \text{id}$

(IS)  $N > 0$ : Wähle  $i_1$  mit  $\sigma(i_1) \neq i_1$ , betrachte  $i_1, \sigma(i_1), \sigma^2(i_1), \dots$ . Da  $\{i_1, \dots, n\}$  endlich ist und  $\sigma$  bijektiv ist, existiert ein minimales  $k \geq 2$  mit  $\sigma^k(i_1) = i_1$ . Setze  $\tau_1 = (i_1 \sigma(i_1) \dots \sigma^{k-1}(i_1))$ . Dann ist  $\sigma = \tau_1 \cdot \tau_1^{-1} \sigma$  und nach Induktionshypothese ist

$$\tau_1^{-1} \sigma = \tau_2 \cdots \tau_m$$

Eindeutigkeit ist klar, denn jedes  $i$  kann nur in dem Zykel  $(i \sigma(i) \dots \sigma^{k-1}(i))$  vorkommen.  $\square$

### 1.15 Beispiel

Offensichtlich ist  $(1\ 2\ 3\ 4\ 5) \cdot (2\ 4)$  eine nicht-disjunkte Zerlegung in Zykel. Wir suchen daher eine solche Zykelzerlegung.

$$\begin{aligned} (1\ 2\ 3\ 4\ 5) \cdot (2\ 4) &= (1\ 4\ 5) \cdot (2\ 3) \\ &= (1\ 4\ 5) \cdot (3\ 2) \\ &= (4\ 5\ 1) \cdot (3\ 2) \\ &\neq (1\ 5\ 4) \cdot (3\ 2) \end{aligned}$$

## 2 Ordnung und Index

Sei  $G$  eine Gruppe und  $g \in G$ .

### 2.1 Definition

- a)  $\#G = |G| \in \mathbb{N} \cup \{\infty\}$ , die Ordnung von  $G$ .
- b)  $\text{ord}(g) = \#\langle g \rangle$ , die Ordnung von  $g$ .

### 2.2 Beispiel

$$\begin{aligned} \#S_n &= n! \quad , \quad \#A_n = \frac{1}{2} \cdot n! \quad (n \geq 2) \\ \#\mathbb{Z}/n\mathbb{Z} &= n \end{aligned}$$

### 2.3 Lemma

Für  $X \subseteq G$  ist

$$\langle X \rangle = \{g_1^{\varepsilon_1} \cdots g_r^{\varepsilon_r} : r \in \mathbb{N}_0, g_1, \dots, g_r \in X, \varepsilon_1, \dots, \varepsilon_r \in \{1, -1\}\}$$

*Beweis.* klar, da rechte Seite Untergruppe ist, die  $X$  enthält, und jede solche enthält alle Ausdrücke der Form  $g_1^{\varepsilon_1} \cdots g_r^{\varepsilon_r}$ .  $\square$

### 2.4 Satz

- a) Ist  $\text{ord}(g) = \infty$ , so ist  $\langle g \rangle = \{\dots, g^{-2}, g^{-1}, 1, g, g^2, \dots\}$ .
- b) Ist  $\text{ord}(g) = n < \infty$ , so ist  $\langle g \rangle = \{1, g, g^2, \dots, g^{n-1}\}$ .
- c) Es ist  $\text{ord}(g) = \inf\{k \in \mathbb{N} : g^k = 1\}$ .

*Beweis.* Nach 2.3 ist  $\langle g \rangle = \{g^k : k \in \mathbb{Z}\}$ . Sei  $m = \inf\{k \in \mathbb{N} : g^k = 1\}$ .

- $\triangleright |\{g^k : 0 \leq k < m\}| = m$ : Sind  $g^a = g^b$  mit  $0 \leq a < b < m$ , so ist  $g^{b-a} = 1$ , aber  $0 < b-a < m$  im Widerspruch zur Minimalität von  $m$ .
- $\triangleright m = \infty$ :  $\Rightarrow \text{ord}(g) = \infty$   $\checkmark$
- $\triangleright m < \infty$ :  $\Rightarrow \langle g \rangle = \{g^k : 0 \leq k < m\}$ : Die Inklusion  $\{g^k : 0 \leq k < m\} \subseteq \langle g \rangle$  ist klar. Für die andere Inklusion schreibe  $k \in \mathbb{Z}$  als  $k = g \cdot m + r$  mit  $q, r \in \mathbb{Z}, 0 \leq r < m$ .  
 $\Rightarrow g^k = g^{q \cdot m + r} = (g^m)^q \cdot g^r = 1^q \cdot g^r = g^r \in \{1, g, \dots, g^{m-1}\}$   
 $\Rightarrow \langle g \rangle \subseteq \{g^k : 0 \leq k < m\}$   $\square$

### 2.5 Beispiel

Sei  $\sigma \in S_n$  ein  $k$ -Zykel, so ist  $\text{ord}(\sigma) = k$ .

(Man muss genau  $k$ -mal tauschen bis alle Elemente wieder an ihrem Platz sind)

Für  $\bar{1} \in \mathbb{Z}/n\mathbb{Z}$  ist  $\text{ord}(\bar{1}) = n$ .

$$(n \cdot \bar{1} = \bar{n} = \bar{0} \in \mathbb{Z}/n\mathbb{Z})$$

### 2.6 Definition

Seien  $A, B \subseteq G, H \leq G$ .

- $\triangleright AB := A \cdot B := \{a \cdot b : a \in A, b \in B\}$ , das Komplexprodukt von  $A$  und  $B$
- $\triangleright gH := \{g\} \cdot H = \{g \cdot h : h \in H\}$ , die Linksnebenklasse von  $H$  bezüglich  $g$   
 $Hg := H \cdot \{g\} = \{h \cdot g : h \in H\}$ , die Rechtsnebenklasse von  $H$  bezüglich  $g$
- $\triangleright G/H := \{gH : g \in G\}$  (Menge der Linksnebenklassen)  
 $H \backslash G := \{Hg : g \in G\}$  (Menge der Rechtsnebenklassen)

## 2.7 Beispiel

Für  $h \in H$  ist  $hH = H = Hh$  (vgl. 1.4).

## 2.8 Lemma

Seien  $H \leq G$ ,  $g, g' \in G$ .

- a)  $gH = g'H \Leftrightarrow g' = gh \in G$  für ein  $h \in H$ .  
 $Hg = Hg' \Leftrightarrow g' = hg \in G$  für eine  $h \in H$
- b) Es ist  $gH = g'H$  oder  $gH \cup g'H = \emptyset$  und  $Hg = Hg'$  oder  $Hg \cup Hg' = \emptyset$ .
- c) Durch  $gH \mapsto Hg^{-1}$  wird eine wohldefinierte Bijektion  $G/H \rightarrow H \backslash G$  gegeben.

*Beweis.* Seien  $H \leq G$ ,  $g, g' \in G$ .

- a)  $(\Rightarrow) : gH = g'H \Rightarrow g' = g' \cdot 1 \in g'H = gH \Rightarrow \exists h \in H : g' = gh$ .  
 $(\Leftarrow) : g' = gh \Rightarrow g'H = ghH \stackrel{2.7}{=} gH$
- b) Ist  $gH \cap g'H \neq \emptyset$ , so existieren  $h, h' \in H$  mit  $gh = g'h'$ .  $\Rightarrow gH = ghH = g'h'H = g'H$
- c) Wohldefiniertheit:  $gH = g'H \stackrel{a)}{\Rightarrow} g'h = gh$  mit  $h \in H \Rightarrow H(g')^{-1} = Hh^{-1}g^{-1} = Hg^{-1}$   
 Bijektivität: klar, da Umkehrabbildung  $Hg \mapsto g^{-1}H$  □

**Beispiel.** Betrachte  $S_3$  als kleinste nicht-abelsche Gruppe.

## 2.9 Definition

Für  $H \leq G$  ist

$$(G : H) := \#G/H \stackrel{2.8c}{=} \#h \backslash G \in \mathbb{N} \cup \infty$$

der Index von  $H$  in  $G$ .

## 2.10 Beispiel

$$(S_n : A_n) = 2 \quad (n \geq 2)$$

$$(\mathbb{Z} : n\mathbb{Z}) = n$$

## 2.11 Satz

Der Index ist multiplikativ: Sind  $K \leq H \leq G$ , so ist

$$(G : K) = (G : H) \cdot (H : K)$$

*Beweis.* Nach 2.8b bilden die Nebenklassen von  $H$  eine Partition von  $G$ , d.h. es gibt eine Familie  $(g_i)_{i \in I}$  in  $G$  mit  $G = \bigcup_{i \in I} g_i H$  ( $G = \bigcup_{i \in I} g_i H$  und  $g_i H, i \in I$  sind paarweise disjunkt).

Analog ist  $H = \bigcup_{j \in J} h_j K$  mit  $h_j \in H$ . Dann gilt:

$$\begin{aligned} H = \bigcup_{j \in J} h_j K &\stackrel{1.4}{\Rightarrow} gH = \bigcup_{j \in J} g h_j K \quad \text{für jedes } g \in G \\ &\Rightarrow G = \bigcup_{i \in I} g_i H = \bigcup_{i \in I} \bigcup_{j \in J} g_i h_j K = \bigcup_{(i,j) \in I \times J} g_i h_j K \end{aligned}$$

Somit ist  $(G : K) = |I \times J| = |I| \cdot |J| = (G : H) \cdot (H : K)$ . □

## 2.12 Korollar (Satz von Lagrange (wichtigster Satz der Vorlesung))

Ist  $G$  endlich und  $H \leq G$ , so ist

$$\#G = \#H \cdot (G : H)$$

Insbesondere gilt  $\#H \mid \#G$  und  $(G : H) \mid \#G$ .

*Beweis.*  $\#G = (G : 1) \stackrel{2.11}{=} (G : H) \cdot (H : 1) = (G : H) \cdot \#H$

□

### 2.13 Korollar (Kleiner Satz von Fermat)

Ist  $G$  endlich und  $n = \#G$ , so ist  $g^n = 1$  für jedes  $g \in G$ .

*Beweis.* Nach 2.12 gilt  $\text{ord}(g) = \#\langle g \rangle \mid \#G = n$ . Nach 2.4 ist  $g^{\text{ord}(g)} = 1$ , somit auch

$$g^n = \underbrace{(g^{\text{ord}(g)})}_{=1}^{\frac{n}{\text{ord}(g)}} = 1$$

### 2.14 Bemerkung

Nach 2.12 ist die Ordnung jeder Untergruppe von  $G$  ein Teiler der Gruppenordnung  $\#G$ . Umgekehrt gibt es im Allgemeinen aber nicht zu jedem Teiler  $d$  von  $\#G$  eine Untergruppe  $H$  von  $G$  mit  $\#H = d$ .



### 3 Normalteiler und Quotientengruppe

Sei  $G$  eine Gruppe.

#### 3.1 Definition

Eine Untergruppe  $H \leq G$  ist *normal* (in Zeichen  $H \trianglelefteq G$ ), wenn  $g^{-1}hg \in H$  für alle  $h \in H$  und  $g \in G$ . Ein *Normalteiler* von  $G$  ist eine normale Untergruppe von  $G$ .

#### 3.2 Beispiel

a) Ist  $G$  abelsch, so ist jede Untergruppe von  $G$  ein Normalteiler von  $G$ .

b) Ist  $\varphi: G \rightarrow H$  ein Gruppenhomomorphismus, so ist  $\text{Ker}(\varphi) \trianglelefteq G$ .

$$\varphi(n) = 1 \Rightarrow \varphi(g^{-1}hg) = \varphi(g)^{-1} \cdot \varphi(h) \cdot \varphi(g) = \varphi(g)^{-1} \cdot \varphi(g) = 1 \quad \forall g \in G$$

c) Jede Gruppe hat die trivialen Normalteiler  $1 \trianglelefteq G$  und  $G \trianglelefteq G$ .

#### 3.3 Lemma

Seien  $H \leq G$  und  $N \trianglelefteq G$ .

a)  $H \trianglelefteq G \Leftrightarrow gH = Hg$  für alle  $g \in G$

b)  $HN = NH$  ,  $HN \leq G$  ,  $N \trianglelefteq HN$  ,  $H \cap N \leq N$  ,  $H \cap N \trianglelefteq H$

c) Sind  $N, H \trianglelefteq G$ , so auch  $H \cap N \trianglelefteq G$  und  $HN \trianglelefteq G$ .

d) Für  $g, g' \in G$  ist  $gN \cdot g'N = gg'N$ .

*Beweis.* Wir beweisen die Eigenschaften unter Nutzung der Definition der Normalteiler.

a)  $(\Rightarrow) \forall g \in G \forall h \in H : g^{-1}hg \in H$   
 $\Rightarrow \forall g \in G : g^{-1}Hg \subseteq H$   
 $\Rightarrow \forall g \in G : Hg \subseteq gH$  ,  $g^{-1}H \subseteq Hg^{-1}$   
 $\Rightarrow \forall g \in G : gH = Hg$ .

$(\Leftarrow) \forall g \in G : gH = Hg$ .  
 $\Rightarrow \forall g \in G \forall h \in H \exists h' \in H : gh' = hg$   
 $\Rightarrow \forall g \in G \forall h \in H : g^{-1}hg = h' \in H$

b)  $\triangleright HN = \bigcup_{h \in H} hN \stackrel{(a)}{=} \bigcup_{h \in H} Nh = NH$

$\triangleright HN \cdot HN = H \cdot NH \cdot N = H \cdot HN \cdot N = HN$   
 $(HN)^{-1} = N^{-1}H^{-1} = NH = HN$   
 $\Rightarrow HN \leq G$

$\triangleright N \trianglelefteq HN$ : ✓

$\triangleright H \cap N \leq N$ : ✓

$\triangleright H \cap N \trianglelefteq H$ :  $n \in H \cap N, h \in H \Rightarrow h^{-1}nh \in H \cap N$  (da  $n$  normal in  $G$ )

c)  $\triangleright H \cap N \trianglelefteq G$ :  $h \in H \cap N, g \in G \Rightarrow g^{-1}hg \in H \cap N$

$\triangleright HN \trianglelefteq G$ :  $g \in G \Rightarrow g \cdot HN \stackrel{(a)}{=} Hg \cdot N = H \cdot gN \stackrel{(a)}{=} H \cdot Ng = HNg$

d)  $gN \cdot g'N = g \cdot Ng' \cdot N = g \cdot g'N \cdot N = gg'N$  □

#### 3.4 Satz

Sei  $N \trianglelefteq G$ . Dann ist  $G/N$  mit dem Komplexprodukt als Verknüpfung eine Gruppe und  $\pi_N: G \rightarrow$

$G/N, g \mapsto gN$  ein Gruppenhomomorphismus mit  $\text{Ker}(\pi_N) = N$ .

*Beweis.*  $\triangleright$  Komplexprodukt ist Verknüpfung auf  $G/N$ : vgl. 3.3(d)

$\triangleright$  Gruppenaxiome übertragen sich von  $G$  auf  $G/N$  mit neutralem Element  $1N$  und inverselem Element  $g^{-1}N$ .

$\triangleright \pi_N$  ist Gruppenhomomorphismus: 3.3(d)

$\triangleright \text{Ker}(\pi_N) = N$ : 2.8(a) □

### 3.5 Korollar

Die Normalteiler sind genau die Kerne von Gruppenhomomorphismen.

### 3.6 Definition

Für  $N \trianglelefteq G$  heißt  $G/N$  zusammen mit dem Komplexprodukt als Verknüpfung die *Quotientengruppe* (oder auch Faktorgruppe) von  $G$  nach  $N$  (oder auch  $G$  modulo  $N$ ).

### 3.7 Lemma

Sei  $N \trianglelefteq G$ . Für  $H \leq G$  ist  $\pi_N(H) = HN/H \leq G/N$  und  $H \mapsto \pi_N(H)$  liefert eine Bijektion zwischen

a) den  $H \leq G$  mit  $N \leq H$ , und

b)  $H \leq G/N$

*Beweis.* Wir zeigen die Untergruppeneigenschaft und die Bijektivität der Abbildung separat, letzteres durch Angabe der Umkehrabbildung.

$\triangleright \pi_N(H) = \{hN : h \in H\} = \{hnN : h \in H, n \in N\} = HN/H$

$\triangleright$  Umkehrabbildung:  $H \mapsto \pi_N^{-1}(H)$

$H \leq G/N$ :  $\pi_N(\pi_N^{-1}(H)) = H$ , da  $\pi_N$  surjektiv ist

$N \leq H \leq G$ :  $\pi_N^{-1}(\pi_N(H)) = \pi_N^{-1}(HN/N) = HN \subseteq HH = H$  □

### 3.8 Satz (Homomorphiesatz)

Sei  $\varphi: G \rightarrow H$  ein Gruppenhomomorphismus und  $N \trianglelefteq G$  mit  $N \subseteq \text{Ker}(\varphi)$ . Dann existiert genau ein Gruppenhomomorphismus  $\bar{\varphi}: G/N \rightarrow H$  mit  $\bar{\varphi} \circ \pi_N = \varphi$ .

*Beweis.* Existiert so ein  $\bar{\varphi}$ , so ist  $\bar{\varphi}(gN) = (\bar{\varphi} \circ \pi_N)(g) = \varphi(g)$ . Definiere  $\bar{\varphi}$  nun so.

$\triangleright \bar{\varphi}$  ist wohldefiniert:

$gN = g'N \xrightarrow{2.8} \text{ex. } g' = gn \text{ für ein } n \in N \Rightarrow \varphi(g') = \varphi(g) \cdot \varphi(n) = \varphi(g)$

$\triangleright \bar{\varphi}$  ist Homomorphismus:

$\bar{\varphi}(gN \cdot g'N) = \bar{\varphi}(gg'N) = \varphi(gg') = \varphi(g)\varphi(g') = \bar{\varphi}(gN) \cdot \bar{\varphi}(g'N)$  □

### 3.9 Korollar

Ein Gruppenhomomorphismus  $\varphi: G \rightarrow H$  liefert einen Isomorphismus

$$\bar{\varphi}: G/\text{Ker}(\varphi) \rightarrow \text{Im}(\varphi) \leq H$$

### 3.10 Korollar (1. Noetherscher Isomorphiesatz)

Seien  $H \leq G$  und  $N \trianglelefteq G$ . Der Homomorphismus

$$\varphi: H \xhookrightarrow{\iota} HN \rightarrow HN/N$$

induziert einen Isomorphismus

$$\bar{\varphi}: H/(H \cap N) \rightarrow HN/N$$

*Beweis.*  $\varphi$  surjektiv, denn für  $h \in H, n \in N$  ist  $hnN = hN = \varphi(n) \in \varphi(H) = \text{Im}(\varphi)$ .  
Außerdem ist  $\text{Ker}(\varphi) = H \cap \text{Ker}(\pi_N) = H \cap N$ .  $\square$

### 3.11 Korollar

Seien  $N \trianglelefteq G$  und  $N \leq H \trianglelefteq G$ . Der Homomorphismus

$$\pi_N: G \rightarrow G/H$$

induziert einen Isomorphismus

$$(G/N)/(H/N) \xrightarrow{\cong} G/H$$

*Beweis.* Da  $N \leq H$  liefert  $\pi_H$  einen Epimorphismus  $\pi_N: G/N \rightarrow G/H$  (vgl. 3.8). Dieser hat  $\text{Ker}(\pi_H) = H/N$  und induziert nach 3.9 einen Isomorphismus

$$(G/N)/\text{Ker}(\pi_H) \xrightarrow{\cong} \text{Im}(\pi_H) = G/H$$

### 3.12 Definition

Seien  $x, x', g \in G$  und  $H, H' \leq G$ .

- a)  $x^g := g^{-1}xg$  ist die *Konjugation* von  $x$  mit  $g$ .
- b)  $x$  und  $x^{-1}$  sind *konjugiert* (in  $G$ )  $:\Leftrightarrow \exists g \in G : x' = x^g$
- c)  $H$  und  $H'$  heißen *konjugiert* (in  $G$ )  $:\Leftrightarrow \exists g \in G : H' = H^g := \{h^g : h \in H\}$

### 3.13 Lemma

Die Abbildung

$$\text{int} : \begin{cases} G \rightarrow \text{Aut}(G) \\ g \mapsto (x \mapsto x^g) \end{cases}$$

ist ein Gruppenhomomorphismus.

*Beweis.*  $\triangleright \text{int}(g) \in \text{Hom}(G, G): \quad (xy)^g = g^{-1}xyg = g^{-1}xgg^{-1}yg = x^g \cdot y^g \quad \forall x, y, g \in G$

$$\triangleright \quad (x^g)^h = h^{-1}x^gh = h^{-1}g^{-1}xgh = (gh)^{-1}x(gh) = x^{gh} \quad (1)$$

$\triangleright \text{int}(g) \in \text{Aut}(G): \quad$  Umkehrabbildung zu  $\text{int}(g)$  ist  $\text{int}(g^{-1})$

$$\triangleright \text{int} \in \text{Hom}(G, \text{Aut}(G)): \quad \text{int}(gh) \stackrel{(1)}{=} \text{int}(h) \circ \text{int}(g) = \text{int}(g) \cdot \text{int}(h) \quad \square$$

### 3.14 Definition

- a)  $\text{Inn}(G) := \text{Im}(\text{int}) \leq \text{Aut}(G)$  Gruppe der *inneren Automorphismen* von  $G$
- b)  $Z(G) := \text{ker}(\text{int}) = \{g \in G : gx = xg \quad \forall x \in G\}$  das *Zentrum* von  $G$
- c)  $H \leq G$  ist charakteristisch  $:\Leftrightarrow \forall \sigma \in \text{Aut}(G) : H = H^\sigma = \{h^\sigma : h \in H\}$

### 3.15 Bemerkung

- $\triangleright$  Konjugiertheit ist eine Äquivalenzrelation (auf  $G$  oder Menge der Untergruppen von  $G$ )
- $\triangleright H \leq G$  ist normal  $\Leftrightarrow H = H^\sigma \quad \forall \sigma \in \text{Inn}(G)$
- $\triangleright$  Deshalb gilt für  $H \leq G$ :  $H$  ist charakteristisch  $\Rightarrow H$  ist normal

### 3.16 Beispiel

$Z(G)$  ist charakteristisch in  $G$ .

## 4 Abelsche Gruppen

Sei  $G$  eine Gruppe.

### 4.1 Definition

$G$  ist *zyklisch*  $\Leftrightarrow G = \langle g \rangle$  für ein  $g \in G$ .

### 4.2 Beispiel

- a)  $\mathbb{Z}$  ist zyklisch.
- b)  $\mathbb{Z}/n\mathbb{Z}$  ist zyklisch der Ordnung  $n$ .
- c)  $C_n = \langle (1\ 2 \cdots n) \rangle \leq S_n$  ist zyklisch der Ordnung  $n$ .
- d) Ist  $\#G = p$  eine Primzahl, so ist  $G$  zyklisch (vgl. Ü6).

### 4.3 Lemma (!)

Die Untergruppen von  $(\mathbb{Z}, +)$  sind genau die  $\langle k \rangle = k\mathbb{Z}$  mit  $k \in \mathbb{N}_0$  und für  $k_1, \dots, k_r \in \mathbb{Z}$  ist  $\langle k_1, \dots, k_r \rangle = \langle k \rangle$  mit  $\text{ggT}(k_1, \dots, k_r) = k$ .

*Beweis.* Jede Untergruppe von  $\mathbb{Z}$  ist ein Ideal von  $(\mathbb{Z}, +, \cdot)$  und  $\mathbb{Z}$  ist Hauptidealring. □

*Beweis.* Sei  $H \leq \mathbb{Z}$ . Setze  $k = \min(H \cap \mathbb{N})$ , o.E. sei  $H \neq \{0\}$ . Offensichtlich gilt  $\langle k \rangle \subseteq H$ .

$$\triangleright n \in H \Rightarrow n = q \cdot k + r \text{ mit } q, r \in \mathbb{Z}, 0 \leq r < k \Rightarrow r = n - \underbrace{q \cdot k}_{k + \dots + k}$$

$\Rightarrow r = 0$  wegen der Minimalität von  $k$

$\Rightarrow n = q \cdot k$ , d.h.  $n \in \langle k \rangle$

$\triangleright k = \text{ggT}(k_1, \dots, k_r)$ :

$k_i \in \langle k \rangle \Rightarrow k \mid k_i \ \forall i$

$k \in \langle k_1, \dots, k_r \rangle \Rightarrow k = n_1 k_1 + \dots + n_r k_r$  mit  $n_i \in \mathbb{Z}$

$d \mid k_i \ \forall i \Rightarrow d \mid k$  □

### 4.4 Satz

Sei  $G = \langle g \rangle$  zyklisch. Dann ist  $G$  abelsch und  $G \cong (\mathbb{Z}, +)$  oder  $G \cong (\mathbb{Z}/n\mathbb{Z}, +)$  mit  $n = \#G < \infty$ .

*Beweis.* Betrachte

$$\varphi: \begin{cases} \mathbb{Z} \rightarrow G \\ k \mapsto g^k \end{cases}$$

$\varphi$  ist Homomorphismus und surjektiv, da  $G = \langle g \rangle$ . Nach 3.9. ist  $G = \text{Im}(\varphi) \cong \mathbb{Z} / \text{Ker}(\varphi)$ . Nach 4.3 ist  $\text{Ker}(\varphi) = \langle n \rangle$  für ein  $n \in \mathbb{N}_0$ . Ist  $n = 0$ , so ist  $\text{Ker}(\varphi) = \{0\}$  und  $G \cong \mathbb{Z}$ . Ist  $n > 0$ , so ist  $G \cong \mathbb{Z}/n\mathbb{Z}$  und  $n = \#\mathbb{Z}/n\mathbb{Z} = \#G$ . □

### 4.5 Satz

Sei  $(G, +) = \langle g \rangle$  zyklisch der Ordnung  $n \in \mathbb{N}$ .

- a) Zu jedem  $d \in \mathbb{N}$  mit  $d \mid n$  hat  $G$  genau eine Untergruppe der Ordnung  $d$ , nämlich  $U_d := \langle \frac{n}{d} g \rangle$ . Damit ist jede Untergruppe einer zyklischen Gruppe wieder zyklisch.
- b) Für  $d \mid h$  und  $d' \mid h'$  ist  $U_d \subseteq U_{d'} \Rightarrow d \mid d'$ .
- c) Für  $k_1, \dots, k_r \in \mathbb{Z}$  ist  $\langle k_1 g, \dots, k_r g \rangle = \langle e g \rangle = U_{\frac{n}{e}}$  mit  $e = \text{ggT}(k_1, \dots, k_r, n)$ .
- d) Für  $k \in \mathbb{Z}$  ist  $\text{ord}(kg) = \frac{n}{\text{ggT}(k, n)}$ .

*Beweis.* Betrachte wieder  $\varphi: \mathbb{Z} \rightarrow G, k \mapsto kg$ .

- a) Nach 3.7 und 4.3 liefert  $\varphi$  eine Bijektion  $\{e \in \mathbb{Z} : n\mathbb{Z} \leq e\mathbb{Z}\} \rightarrow \{H \leq G\}$  und  $n\mathbb{Z} \leq e\mathbb{Z} \Leftrightarrow e \mid n$ .

Ist  $H = \varphi(e\mathbb{Z}) = \langle eg \rangle$ , so ist  $H \cong e\mathbb{Z}/n\mathbb{Z}$  ( $n\mathbb{Z} = \ker(\varphi)$ ), also

$$n = (\mathbb{Z} : n\mathbb{Z}) = (\mathbb{Z} : e\mathbb{Z})(e\mathbb{Z} : n\mathbb{Z}) = e \cdot \#H$$

- b)  $U_d \subseteq U_{d'} \Leftrightarrow \langle \frac{n}{d} g \rangle \subseteq \langle \frac{n}{d'} g \rangle \Leftrightarrow \frac{n}{d}\mathbb{Z} \leq \frac{n}{d'}\mathbb{Z} \Rightarrow \frac{n}{d} \mid \frac{n}{d'} \Leftrightarrow d \mid d'$

- c) Mit  $H = \langle k_1, \dots, k_r \rangle \leq \mathbb{Z}$  ist  $n\mathbb{Z} \leq H$ ,  $\varphi(H) = \langle k_1g, \dots, k_rg \rangle$  ( $n \in \ker(\varphi)$ ).

Nach 4.3 ist  $H = \langle e \rangle$  mit  $e = \text{ggT}(k_1, \dots, k_r, n)$  und somit  $\langle k_1g, \dots, k_rg \rangle = \varphi(e\mathbb{Z}) = U_{\frac{n}{e}}$ .

- d)  $\text{ord}(kg) = \# \langle kg \rangle \stackrel{(c)}{=} U_{\frac{n}{e}}$  mit  $e = \text{ggT}(k, n)$ . (Fall (c) mit  $r = 1$ ) □

#### 4.6 Lemma

Seien  $a, b \in G$ . Kommutieren  $a$  und  $b$  und sind  $\text{ord}(a), \text{ord}(b)$  teilerfremd, so ist  $\text{ord}(a \cdot b) = \text{ord}(a) \cdot \text{ord}(b)$ .

*Beweis.* Nach 2.12 ist  $\langle a \rangle \cap \langle b \rangle = \{1\}$ . Ist  $(ab)^k = a^k \cdot b^k$ , so ist  $a^k = b^{-k} \in \langle a \rangle \cap \langle b \rangle = 1$ , also  $a^k = b^k = 1$ . Somit ist  $(ab)^k = 1 \Leftrightarrow a^k = 1$  und  $b^k = 1$ , und damit

$$\text{ord}(ab) = \text{kgV}(\text{ord}(a), \text{ord}(b)) = \text{ord}(a) \cdot \text{ord}(b)$$

#### 4.7 Korollar

Ist  $G$  abelsch und sind  $a, b \in G$  mit  $\text{ord}(a) = < \infty, \text{ord}(b) = n < \infty$ , so existiert ein  $c \in G$  mit  $\text{ord}(c) = \text{kgV}(\text{ord}(a), \text{ord}(b))$ .

*Beweis.* Schreibe  $m = m_0 \cdot m'$  und  $n = n_0 \cdot n'$  mit  $m_0 \cdot n_0 = \text{kgV}(m, n)$  und  $\text{ggT}(m_0, n_0) = 1$ .

$$\Rightarrow \text{ord}(a^{m'}) = m_0, \text{ord}(b^{n'}) = n_0$$

$$\Rightarrow \text{ord}(a^{m'} b^{n'}) \stackrel{4.6}{=} m_0 \cdot n_0 = \text{kgV}(m, n)$$

Dann ist  $c := a^{m'} b^{n'}$ . □

#### 4.8 Theorem (Struktursatz für endlich erzeugte abelsche Gruppen)

Jede endlich erzeugte abelsche Gruppe  $G$  ist eine direkte Summe zyklischer Gruppen

$$G^r \cong \mathbb{Z}^r \oplus \bigoplus_{i=1}^k \mathbb{Z}/d_i\mathbb{Z}$$

mit eindeutig bestimmten  $d_1, \dots, d_k > 1$ , die  $d_i \mid d_{i+1}$  für alle  $i$  erfüllen.

*Beweis.* Die Existenz folgt aus LAAG VIII.6.14 (Hauptsatz über endlich erzeugte Moduln über Hauptidealringen).

Eindeutigkeit: Für  $d \in \mathbb{N}$  ist  $\#G/dG = \#(\mathbb{Z}/d\mathbb{Z})^r \oplus \bigoplus_{i=1}^k (\mathbb{Z}/d_i\mathbb{Z})/d \cdot \mathbb{Z}/d_i\mathbb{Z} \stackrel{4.5(d)}{=} d^r \cdot \prod_{i=1}^k \frac{d_i}{\text{ggT}(d, d_i)}$ . Daraus kann man nun  $r, k, d_1, \dots, d_k$  erhalten, z.B. für  $p$  prim  $p \mid \text{nicht } d_i \forall i$  ist  $\#G/pG = p^r \cdot \prod_{i=1}^k d_i$ . □

#### 4.9 Lemma

Sei  $G = (G, +) = \langle g \rangle$  zyklisch der Ordnung  $n \in \mathbb{N}$ . Die Endomorphismen von  $G$  sind genau die

$$\varphi_{\bar{k}} : \begin{cases} G \rightarrow G \\ x \mapsto kx \end{cases}$$

für  $\bar{k} = k + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$ . Dabei ist  $\varphi_{\bar{l}} \circ \varphi_{\bar{k}} = \varphi_{\bar{k}\bar{l}}$  für  $\bar{k}, \bar{l} \in \mathbb{Z}/n\mathbb{Z}$ .

*Beweis.* Zu zeigen sind eine Reihe von Aussagen.

$$\triangleright \varphi_{\bar{k}} \text{ wohldefiniert: } \bar{k}_1 = \bar{k}_2 \Rightarrow k_2 = k_1 + an \text{ mit } a \in \mathbb{Z}. \text{ Dann ist auch } k_2x = k_1x + a \cdot nx = k_1x \quad \forall x \in G.$$

- ▷  $\varphi_{\bar{k}} \in \text{Hom}(G, G)$ : klar, da  $G$  abelsch.
- ▷  $\bar{k} = \bar{l} \Leftrightarrow \varphi_{\bar{k}} = \varphi_{\bar{l}}$ : (zeige  $\Leftarrow$ ;  $\Rightarrow$  ist Wohldefiniertheit)  
 $\varphi_{\bar{k}} = \varphi_{\bar{l}} \Rightarrow \varphi_{\bar{k}}(g) = \varphi_{\bar{l}}(g) \Rightarrow (k - l)g = 0 \xrightarrow{\text{ord}(g)=n} n \mid k - l \Rightarrow \bar{k} = \bar{l}$
- ▷  $\varphi \in \text{Hom}(G, G)$ :  $\Rightarrow \varphi = \varphi_{\bar{k}}$  für ein  $k \in \mathbb{Z}$ ;  $\varphi(g) = k \cdot g$  für ein  $k \in \mathbb{Z} \Rightarrow \varphi = \varphi_{\bar{k}}$
- ▷  $\varphi_{\bar{l}} \circ \varphi_{\bar{k}} = \varphi_{\overline{kl}}$ :  $l \cdot (k \cdot x) = (l \cdot k) \cdot x \checkmark$

#### 4.10 Satz

Ist  $G$  zyklisch von Ordnung  $n \in \mathbb{N}$ , so ist  $\text{Aut}(G) \cong (\mathbb{Z}/n\mathbb{Z})^\times$ . (multiplikativ)

*Beweis.*  $\text{Aut}(G) \subseteq \text{Hom}(G, G) = \{\varphi_{\bar{k}} : \bar{k} \in \mathbb{Z}/n\mathbb{Z}\}$ .

$$\begin{aligned} \varphi_{\bar{k}} \in \text{Aut}(G) &\Leftrightarrow \exists \bar{l} \in \mathbb{Z}/n\mathbb{Z} : \varphi_{\bar{l}} \circ \varphi_{\bar{k}} = \varphi_{\bar{1}} \\ &\Leftrightarrow \exists \bar{l} \in \mathbb{Z}/n\mathbb{Z} : \bar{l} \cdot \bar{k} = 1 \\ &\Leftrightarrow \bar{k} \in (\mathbb{Z}/n\mathbb{Z})^\times \end{aligned}$$

und die Abbildung  $(\mathbb{Z}/n\mathbb{Z})^\times \rightarrow \text{Aut}(G)$  mit  $\bar{k} \mapsto \varphi_{\bar{k}}$  ist ein Isomorphismus. Offensichtlich ist diese ein Homomorphismus und die Bijektivität folgt aus der Tatsache, dass jeder Endomorphismus genau diese Gestalt  $\varphi_{\bar{k}}$  hat.  $\square$

#### 4.11 Definition

Die Abbildung  $\Phi: \mathbb{N} \rightarrow \mathbb{N}$  gegeben durch

$$\Phi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times$$

ist die *Euler'sche Phi-Funktion*.

#### 4.12 Beispiel

Ist  $p$  prim, so ist  $\Phi(p) = p - 1$ , da  $\mathbb{Z}/p\mathbb{Z}$  ein Körper ist.

## 5 Direkte und semidirekte Produkte

Sei  $G$  eine Gruppe und  $n \in \mathbb{N}$ .

### 5.1 Definition

Das direkte Produkt von Gruppen  $G_1, \dots, G_n$  ist das kartesische Produkt

$$G = \prod_{i=1}^n G_i = G_1 \times \dots \times G_n$$

mit komponentenweise Multiplikation.

### 5.2 Bemerkung

Wir identifizieren  $G_j$  mit der Untergruppe

$$G_j \times \prod_{i \neq j} 1 = 1 \times \dots \times G_j \times 1 \times \dots \times 1$$

von  $\prod_{i=1}^n G_i$ . Für  $i \neq j, g_i \in G_i$  und  $g_j \in G_j$  gilt dann

$$g_i g_j = g_j g_i \quad (2)$$

### 5.3 Definition

Seien  $H_1, \dots, H_n \leq G$ . Dann ist  $G$  das (interne) direkte Produkt von  $H_1, \dots, H_n$ , in Zeichen

$$G = \prod_{i=1}^n H_i = H_1 \times \dots \times H_n$$

wenn

$$\begin{cases} H_1 \times \dots \times H_n & \rightarrow G \\ (g_1, \dots, g_n) & \mapsto g_1 \cdot \dots \cdot g_n \end{cases}$$

ein Gruppenhomomorphismus ist.

### 5.4 Satz (!)

Seien  $U, V \leq G$ . Dann sind äquivalent

$$(1) \quad G = U \times V$$

$$(2) \quad U \trianglelefteq G, \quad V \trianglelefteq G, \quad U \cap V = 1, \quad UV = G$$

*Beweis.* Wir zeigen beide Richtungen der Äquivalenz.

(1)  $\Rightarrow$  (2): Im (externen) direkten Produkt  $U \times V$  gilt:

$$\triangleright UV = G = U \times V: \text{ Für } u \in U, v \in V \text{ ist } (u, v) = (u, 1) \cdot (1, v) \in UV$$

$$\triangleright U \cap V = 1: \checkmark$$

$$\triangleright U \trianglelefteq G = U \times V: \text{ Für } g = (u, v) \in U \times V \text{ und } u_0 = (u_0, 1) \in U \text{ ist}$$

$$u_0^g = g^{-1} \cdot u_0 \cdot g = (u^{-1}, v^{-1}) \cdot (u_0, 1) \cdot (u, v) = (u_0^u, 1) \in U$$

$$\triangleright V \trianglelefteq U \times V: \text{ analog}$$

(2)  $\Rightarrow$  (1): Betrachte  $\varphi: U \times V \rightarrow G$  mit  $(u, v) \mapsto u \cdot v$ .

$$\triangleright (2) \text{ gilt: Für } u \in U \text{ und } v \in V \text{ gilt in } G:$$

$$u^{-1}v^{-1}uv = \underbrace{(v^{-1})^u}_{\in V} \cdot \underbrace{v}_{\in V} = \underbrace{u^{-1}}_{\in U} \cdot \underbrace{u^v}_{\in U} \in U \cap V = 1 \Rightarrow uv = vu$$

$$\triangleright \varphi \text{ ist Homomorphismus:}$$

$$\varphi((u_1, u_2)(v_1, v_2)) = \varphi(u_1v_1, u_2v_2) = u_1u_2 \cdot v_1v_2 \stackrel{(2)}{=} (u_1v_1)(u_2v_2) = \varphi(u_1, u_2) \cdot \varphi(v_1, v_2)$$

▷  $\varphi$  surjektiv:  $\text{Im}(\varphi) = UV = G$

▷  $\varphi$  injektiv:  $1 = \varphi(u, v) = uv$

$$\Rightarrow u = v^{-1} \in U \cap V = 1 \Rightarrow (u, v) = (1, 1) \Rightarrow \text{Ker}(\varphi) = \{(1, 1)\}$$

□

### 5.5 Korollar

Seien  $H_1, \dots, H_n \leq G$ . Dann sind äquivalent

$$G = H_1 \times \dots \times H_n \quad (3)$$

$$G = H_1 \cdot \dots \cdot H_n \text{ und für alle } i \text{ ist } H_i \trianglelefteq G \text{ und } H_1 \cdots H_{i-1} \cap H_i = 1 \quad (4)$$

*Beweis.* Wir beweisen die Implikation (4)  $\Rightarrow$  (3) durch vollständige Induktion nach  $n$ . Für  $n = 1$  ist die Aussage trivial. Sei also  $n > 1$  und setze  $U := H_1 \cdots H_{n-1}$  und  $V = H_n$ . Dann ist  $U \trianglelefteq G$  nach 3.3(c),  $V \trianglelefteq G$ ,  $UV = H_1 \cdots H_n = G$  und  $U \cap V = 1$ , sodass die Bedingungen aus Gleichung (4) erfüllen. Somit ist  $\varphi: U \times V \rightarrow G$  ein Isomorphismus nach Satz 5.4. Da  $H_i \trianglelefteq U$  für  $i < n$  folgt nach Induktionshypothese, dass

$$\varphi': \begin{cases} H_1 \times \dots \times H_{n-1} & \rightarrow U \\ (h_1, \dots, h_{n-1}) & \mapsto h_1 \cdots h_{n-1} \end{cases}$$

ein Isomorphismus ist. Somit ist auch

$$\varphi \circ (\varphi' \times \text{id}_{H_n}): \begin{cases} H_1 \times \dots \times H_n & \rightarrow G \\ (h_1, \dots, h_n) & \mapsto \varphi(\varphi'(h_1 \cdots h_{n-1}), h_n) = h_1 \cdots h_n \end{cases}$$

ein Isomorphismus. □

### 5.6 Definition

Seien  $H, N \leq G$ . Dann ist  $G$  das *semidirekte Produkt* von  $H$  und  $N$ , in Zeichen

$$G = H \ltimes N = N \rtimes H,$$

wenn  $N \trianglelefteq G$ ,  $H \cap N = 1$ ,  $HN = G$ .

### 5.7 Bemerkung

Ist  $G = H \ltimes N$ , so ist

$$\alpha: \begin{cases} H & \rightarrow \text{Aut}(N) \\ h & \mapsto \text{int}_h|_N \end{cases}$$

Ein Gruppenhomomorphismus. Im Fall  $G = H \times N$  ist  $\alpha_h = \text{id}_N$  für alle  $h \in H$ . Für  $h_1, h_2 \in H$ ,  $n_1, n_2 \in N$  ist

$$h_1 n_1 \cdot h_2 n_2 = h_1 h_2 h_2^{-1} n_1 h_2 n_2 = h_1 h_2 \cdot \underbrace{n_1^{h_2}}_{\in N \trianglelefteq G} \cdot n_2 = h_1 h_2 \cdot n_1^{\alpha_{h_2}} \cdot n_2$$

### 5.8 Definition

Seien  $H, N$  Gruppen und  $\alpha \in \text{Hom}(H, \text{Aut}(N))$ . Das semidirekte Produkt  $H \ltimes_\alpha N$  von  $H$  und  $N$  bezüglich  $\alpha$  ist das kartesische Produkt  $H \times N$  mit der Multiplikation

$$(h_1, n_1)(h_2, n_2) = (h_1 \cdot h_2, n_1^{\alpha_{h_2}} \cdot n_2)$$

für  $h_1, h_2 \in H$  und  $n_1, n_2 \in N$