# § 1: Elementare Gruppentheorie

Erinnerung: eine Verknüpfung auf einer nichtleeren Menge $X$ ist eine Abbildung

$$X \times X \xrightarrow{m} X, \quad (x,y) \longmapsto m(x,y).$$

Häufig schreibt man $m(x,y) = x \cdot y$ oder $m(x,y) = x * y$ oder $m(x,y) = xy$ oder $m(x,y) = x+y$, je nach dem Kontext. Die Schreibweise $m(x,y) = x+y$ wird eigentlich nur für kommutative Verknüpfungen benutzt, d.h. wenn für alle $x,y \in X$ gilt $m(x,y) = m(y,x)$.

1. Def Eine Gruppe $(G, \cdot)$ besteht aus einer Verknüpfung $\cdot$ auf einer nicht leeren Menge $G$, mit folgenden Eigenschaften

(G1) Die Verknüpfung ist assoziativ, d.h. $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ gilt für alle $x,y,z \in G$.
(Folglich darf man Klammern weglassen)

(G2) Es gibt ein Neutralelement $e \in G$, d.h. es gilt $e \cdot x = x \cdot e = x$ für alle $x \in G$

(G3) Zu jedem $x \in G$ gibt es ein Inverses $y \in G$, d.h. $x \cdot y = e = y \cdot x$.
Man schibt dann $y = x^{-1}$ für das Inverse zu $x$.

(Wenn man die Verknüpfg mit + statt mit . schibt, so schibt man für das Neutralelemt 0 ($x+0 = 0+x = x$) und für das Inverse $-x$ ($x + (-x) = 0 = (-x)+x$).)

Fordert man von der Verküpfg nur (G1) und (G2), so spricht man von einer Halbgrpe mit Eins oder einem Monoid. Fordert man nur (G1), so spricht man von einer Halbgruppe.

2. Bsp $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$ sind kommutative Gruppen

$(\mathbb{Z}, \cdot)$
$(\mathbb{N}, \cdot)$, $(\mathbb{N}, +)$ } Monoide

3. Beobachtungen a) Das Neutralelement (einer Verknüpfung) ist eindeutig bestimmt: sind $e, e'$ beides Neutralelemte, so folgt

$$e = e \cdot e' = e'$$
$$\uparrow \qquad \uparrow$$
$e'$ NE $\qquad$ $e$ NE

b) Das Inverse zu $x$ ist eindeutig bestimmt:

$$x \cdot y = e = x \cdot y' \Rightarrow y' = y' \cdot e = y' x y = e y = y$$
$$= y' \cdot x$$

4. Lemma (Sparsame Definition von Gruppen)

Sei $G \times G \to G$ eine assoziative Verknüpfg. Dann ist $G$ schon eine Gruppe, wenn gilt

(i) es gibt $e \in G$ so, dass $ex = x$ für alle $x \in G$ gilt

(ii) zu jedem $x \in G$ gibt es ein $y \in G$ mit $yx = e$.

Beweis Sei $yx = e$, es folgt $yxy = y$. Wähle $z$ mit $zy = e$, es folgt $\underbrace{zyxy}_{=e} = zy = e \Rightarrow xy = e$

Weiter gilt $x \cdot e = xyx = ex = x$ □

5. Beispiel Sei $X$ eine nicht leere Menge, sei $X^X = \{ f : X \to X \}$ die Menge aller Abbildungen von $X$ nach $X$. Als Verknüpfung auf $X$ nehmen wir die Komposition von Abbildungen. Dann gilt wegen $f = id_X \circ f = f \circ id_X$, dass $id_X$ ein Neutralelement ist.

Damit haben wir ein Monoid $(X^X, \circ)$.
Sei $Sym(X) = \{ f : X \to X \mid f \text{ bijektiv} \}$
Zu jeder $f \in Sym(X)$ gibt es also eine Umkehrabbildung $g : X \to X$ mit $f \circ g = g \circ f = id_X$.
Folglich ist $(Sym(X), \circ)$ eine Gruppe, die Symmetrische Gruppe. Wenn $X$ endlich ist mit $n$ Elementen, so gibt es genau

$n! = n(n-1)(n-2) \cdots 2 \cdot 1$ Permutationen
(= bijektive Abbildungen von $X$ in sich), also hat $Sym(X)$ dann genau $n!$ Elemente.
Für $X = \{1, 2, 3, \ldots, n\}$ schreibt man auch
$Sym(X) = Sym(n) \; (= S_n)$

6. Def Sei $G \times G \to G$ eine Verknüpfung.
Wir sagen, $x, y \in G$ vertauschen oder kommutieren oder $x$ zentralisiert $y$, wenn gilt $xy = yx$.
Eine Gruppe, in der alle Elemente vertauschen heißt kommutativ oder abelsch.
Das Pluszeichen "+" wird nur für kommutative Verknüpfungen benutzt.

7. Bsp (a) $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{Q}^*,\cdot)$ sind abelsche Gruppen $\mathbb{Q}^* = \mathbb{Q} - \{0\}$

(b) $K$ Körper, $G = GL_2(K) = \{X \in K^{2\times 2} \mid \det(X) \neq 0\}$ Gruppe der invertierbaren $2\times 2$ Matrizen

$\begin{pmatrix}1&1\\0&1\end{pmatrix}\begin{pmatrix}0&1\\1&0\end{pmatrix} = \begin{pmatrix}1&1\\1&0\end{pmatrix}$

$\begin{pmatrix}0&1\\1&0\end{pmatrix}\begin{pmatrix}1&1\\0&1\end{pmatrix} = \begin{pmatrix}0&1\\1&1\end{pmatrix}$

$\Rightarrow$ nicht abelsch

genauso $GL_n(K)$ für $n \geq 2$.

(c) $Sym(2)$ ist abelsch, aber $Sym(3)$ nicht: $\pi, \lambda \in Sym(3)$

| $\pi$ | $\lambda$ | $\pi\circ\lambda$ | $\lambda\circ\pi$ |
|---|---|---|---|
| $1 \to 1$ | $1 \to 2$ | $1 \to 3$ | $1 \to 2$ |
| $2 \to 3$ | $2 \to 1$ | $2 \to 1$ | $2 \to 3$ |
| $3 \to 2$ | $3 \to 3$ | $3 \to 2$ | $3 \to 1$ |

nicht abelsch, allgemein ist $Sym(X)$ nicht abelsch, falls $\#X \geq 3$ gilt. #

8. Def Sei $G$ eine Gruppe, sei $H \subseteq G$. Wir nennen $H$ Untergruppe von $G$, wenn gilt

(UG1) $e \in H$

(UG2) $x, y \in H \Rightarrow xy \in H$

(UG3) $x \in H \Rightarrow x^{-1} \in H$

Offenbar ist eine Untergruppe dann wieder eine Gruppe, mit der von $G$ vererbten Verknüpfg.

Bsp (a) $(\mathbb{R}, +)$ $\mathcal{U}$ ist Untergruppe, denn

$0 \in \mathcal{U}$, $m, n \in \mathcal{U} \Rightarrow m+n \in \mathcal{U}$ und

$u \in \mathcal{U} \Rightarrow -u \in \mathcal{U}$

(b) $(\mathbb{R}^*, \cdot)$ $\mathcal{U} = \{0\}$ ist keine Untergruppe,

denn: ($1 \in \mathcal{U}$ ok, $m, u \in \mathcal{U} \Rightarrow m \cdot u \in \mathcal{U}$ ok)

$2 \in \mathcal{U}$, aber $2^{-1} = \frac{1}{2} \notin \mathcal{U}$

9. Lemma Sei $G$ eine Gruppe und sei $\mathcal{U}$ eine nicht leere Menge von Untergruppen von $G$. Dann ist auch

$\bigcap \mathcal{U} = \{ g \in G \mid \text{für alle } H \in \mathcal{U} \text{ gilt } g \in H \}$

eine Untergruppe von $G$.

Beweis: Für alle $H \in \mathcal{U}$ gilt $e \in H$, also $e \in \bigcap \mathcal{U}$.

Angenommen, $x, y \in \bigcap \mathcal{U}$. Dann gilt für alle $H \in \mathcal{U}$, dass $x \cdot y \in H$ sowie $x^{-1} \in H$.

Es folgt $x \cdot y \in \bigcap \mathcal{U}$ sowie $x^{-1} \in \bigcap \mathcal{U}$.

□

10. Def Sei $G$ eine Gruppe und $X \subseteq G$ ein Teilmenge. Wir setzen

$$\langle X \rangle = \bigcap \{ H \subseteq G \mid H \text{ Untergruppe und } X \subseteq H \}$$

[nicht leer, enthält mindestens $G$

- Es gilt z.B. $\langle \emptyset \rangle = \{e\}$, denn $\{e\}$ ist Untergruppe.
- Ist $H \subseteq G$ Untergruppe mit $X \subseteq H$, so folgt $X \subseteq \langle X \rangle \subseteq H$, insbesondere also $\langle H \rangle = H$.

Satz Sei $X \subseteq G$ und sei

$$W = \{ x_1 \cdot x_2 \cdots \cdot x_s \mid s \geq 1,\ x_i \in X \text{ oder } x_i^{-1} \in X \text{ für alle } i = 1, \ldots, s \}$$

Dann ist $\langle X \rangle = \{e\} \cup W$.

Beweis Wegen $X \subseteq \langle X \rangle$ und $e \in \langle X \rangle$ folgt $\{e\} \cup W \subseteq \langle X \rangle$. Ist $f, g \in W$, so folgt $f \cdot g \in W$ sowie $f^{-1} \in W$, also ist $H = \{e\} \cup W$ eine Untergruppe von $G$, mit $X \subseteq H$. Es folgt $\langle X \rangle \subseteq H = \{e\} \cup W$. □

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

Für $n \geq 1$ sei $g^n = \underbrace{g \cdot g \cdot \ldots \cdot g}_{n \text{ mal}}$

sowie $g^{-n} = \underbrace{g^{-1} \cdot g^{-1} \ldots \cdot g^{-1}}_{n \text{ mal}}$ und $g^0 = e$.

Dann gilt für alle $k, l \in \mathbb{Z}$, dass

$$g^k \cdot g^l = g^{k+l}.$$

Sei $\langle g \rangle = \langle \{g\} \rangle \underset{\S 1.10}{=} \{ g^n \mid n \in \mathbb{Z} \}$

Man nennt $\langle g \rangle$ die von $g$ erzeugte zyklische Gruppe. Wenn für ein $n \geq 1$ gilt $g^n = e$, so heißt $n$ ein Exponent von $g$.

Die Ordnung von $g$ ist der kleinste Exponent von $g$,

$$o(g) = \min\left( \{ n \geq 1 \mid g^n = 1 \} \cup \{\infty\} \right)$$

$o(g) = \infty$ bedeutet: $g^n \neq e$ für alle $n \geq 1$.

$o(g) = 1$ bedeutet: $g^1 = g = e$

# 12. Zyklische Gruppen

Eine Gruppe $G$ heißt **zyklisch**, wenn es ein $g \in G$ gibt mit $G = \langle g \rangle$. Wegen $g^k \cdot g^l = g^{k+l} = g^{l+k} = g^l g^k$ gilt: **zyklische Gruppen sind abelsch.**

**Satz** Sei $G = \langle g \rangle$ zyklisch mit $o(g) = n < \infty$. Dann gilt $\#G = n$ und $G = \{g, g^2, g^3, \dots, g^n\}$.

**Beweis** Jedes $m \in \mathbb{Z}$ läßt sich schreiben als

$m = k \cdot n + l$ mit $0 \le l < n$ (Teilen mit Rest)

also $g^m = \underbrace{g^{k \cdot n}}_{=e} g^l = g^l$. Es folgt $G \subseteq \{g, g^2, \dots, g^n\}$ mit $g^n = g^0$

Ist $g^k = g^l$ für $0 \le k \le l < n$, so gilt

$e = g^0 = g^{l-k}$, also $l - k = 0$ (wegen $l < n$)

also $\#\{g, g^2, g^3, \dots, g^n = g_0\} = n$ □

**Folgerung** Ist $G$ endlich mit $\#G = n$ $o(g) = n < \infty$ und ist $h \in G$ mit $o(h) = n$, so folgt $\langle h \rangle = G$. Insbesondere ist dann $G$ □ eine zyklische Gruppe □

# 13. Nebenklassen

Sei $G$ eine Gruppe und sei $H$ eine Untergruppe. Sei $a \in G$. Wir definieren

$$aH = \{ah \mid h \in H\} \subseteq G$$
$$Ha = \{ha \mid h \in H\} \subseteq G$$

Man nennt $aH$ die Linksnebenklasse von $a$ bezüglich $H$ (und $Ha$ die Rechtsnebenklasse).
In nicht abelschen Gruppen gilt im allgemeinen

$$aH \neq Ha$$ (dazu später mehr)

**Lemma** Sei $H \subseteq G$ Untergruppe (der Gruppe $G$) und $a, b \in G$.

Dann sind äquivalent

(i) $b \in aH$

(ii) $bH = aH$

(iii) $bH \cap aH \neq \emptyset$

**Beweis** (i) $\Rightarrow$ (ii) $\quad b \in aH \Rightarrow b = ah$ für ein $h \in H$

$$\Rightarrow bH = \{ahh' \mid h' \in H\} = \{ah'' \mid h'' \in H\} = aH$$

($\uparrow$ $H$ Untergruppe)

(ii) $\Rightarrow$ (iii) klar

(iii) $\Rightarrow$ (i) Sei $g \in bH \cap aH$, $g = bh = ah'$ $\Rightarrow$

$$b = ah'h^{-1} \in aH$$

($\uparrow$ $H$ Untergruppe)

□

**Folgerung** Jedes $g \in G$ liegt in genau einer Linksnebenklasse bezüglich $H$, nämlich $g \in gH$.

Entsprechendes gilt natürlich für Rechtsnebenklassen. Man setzt

$G/H = \{gH \mid g \in G\}$ Menge der Linksnebenklassen

$H\backslash G = \{Hg \mid g \in G\}$ Menge der Rechtsnebenklassen

**Lemma** Sei $H \leq G$ Untergruppe (der Gruppe $G$), sei $a \in G$.

Dann ist die Abbildung

$$H \longrightarrow gH$$
$$h \longmapsto gh$$

bijektiv.

Beweis "Surjektiv" ist klar nach Definition von $gH$.

Injektiv, $gh = gh' \Rightarrow h = g^{-1}gh' = h'$ □

14. **Satz** (Satz von Lagrange) Sei $G$ eine Gruppe und $H \leq G$ eine Untergruppe. Wenn zwei der drei Mengen $G$, $H$, $G/H$ endlich sind, dann ist die dritte ebenfalls endlich und es gilt

$$\#G = \#H \cdot \#G/H$$

Insbesondere ist dann $\#H$ ein Teiler von $\#G$.

**Satz** Wenn $G$ endlich ist, dann sind auch $H$ und $G/H$ endlich.

Angenommen, $G/H$ und $H$ sind endlich. Dann ist auch $G = \bigcup G/H = \bigcup \{gH \mid gH \in G/H\}$ endlich, da $\#gH = \#H$ nach §1.13.

Jetzt zählen wir genauer: sei $\#G/H = m$, $\#H = n$

etwa $G/H = \{g_1H, g_2H, \dots, g_mH\}$

$\#g_iH = n$ (↑ §1.13) $\quad g_iH \cap g_jH = \emptyset$ für $i \neq j$ nach §1.13

$G = g_1H \cup g_2H \cup \dots \cup g_mH \Rightarrow \#G = m \cdot n$ □

**Bem** (1) Eine entsprechende Aussage gilt für Rechtsnebenklassen

(2) Die Abbildung $G \to G$, $g \mapsto g^{-1}$ bildet die Linksnebenklassen bijektiv auf die Rechtsnebenklassen ab:

$$(gH)^{-1} = \{(gh)^{-1} \mid h \in H\} = \{h^{-1}g^{-1} \mid h \in H\}$$

(↑ Achtung!)

$$= \{hg^{-1} \mid h \in H\} = Hg^{-1} \qquad (\ddot{\text{U}}\text{A})$$

**Korollar A** (zum Satz von Lagrange)
Sei $G$ eine endliche Gruppe und sei $g \in G$.
Dann teilt $o(g)$ die Zahl $\#G$.

*Beweis.* Da $G$ endlich ist, folgt $o(g) < \infty$.
Nach dem Satz von Lagrange ist $\#\langle g \rangle = o(g)$ ein Teiler von $\#G$. □

**Korollar B** Sei $G$ eine endliche Gruppe, sei $p$ eine Primzahl (d.h. die einzigen Teiler von $p$ sind 1 und $p$ und $p > 1$). Wenn gilt $\#G = p$, dann ist $G$ zyklisch. Für jedes $g \in G - \{e\}$ gilt $\langle g \rangle = G$.

*Beweis.* Sei $g \in G - \{e\}$. Dann ist $o(g) > 1$ und $o(g)$ teilt $p$. Es folgt $o(g) = p$, also $G = \langle g \rangle$ vgl. §1.12. □

Für endliche Gruppen sind Teilbarkeitseigenschaften wichtig, wie wir sehen werden.

Die Zahl $\#G/H = [G : H]$ nennt man auch den **Index von $H$ in $G$**

# Wichtige Rechenregeln in Gruppen

(a) Man darf kürzen $\quad ax = ay \Rightarrow x = y$
$\qquad\qquad\qquad\quad xa = ya \Rightarrow x = y$

(multipliziere linke Seite von links / rechts mit $a^{-1}$)

(b) Es gilt $(x^{-1})^{-1} = x$

($x^{-1} \cdot x = e = x \cdot x^{-1} \Rightarrow (x^{-1})^{-1} = x$)

(c) beim Invertieren die Reihenfolge umdrehen

$$(ab)^{-1} = b^{-1} a^{-1}$$

($ab(b^{-1}a^{-1}) = e = (b^{-1}a^{-1})ab \Rightarrow (ab)^{-1} = b^{-1}a^{-1}$)

(in abelsch Gruppen gilt natürlich damit $(ab)^{-1} = a^{-1}b^{-1}$)

15. Def: **Homomorphismen** Seien $G, K$ Gruppen. Ein Abbildung $\varphi: G \to K$ heißt **(Gruppen-)Homomorphismus**, wenn für alle $x, y \in G$ gilt

$$\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$$

($x \cdot y$: Verknüpfung in $G$; $\varphi(x) \cdot \varphi(y)$: Verknüpfung in $K$.)

Bsp (a) $id_G : G \to G$ ist Homomorphismus.

(b) $H \leq G$ Untergruppe $i : H \hookrightarrow G$, $h \mapsto h$ Inklusion ist Homomorphismus

(c) $(G, \cdot) = (\mathbb{Z}, +)$ $m \in \mathbb{Z}$ $\varphi : \mathbb{Z} \to \mathbb{Z}$, $x \mapsto m \cdot x$ ist Homomorphismus, denn $\varphi(x+y) = m(x+y)$
$= mx + my = \varphi(x) + \varphi(y)$

(d) $G$ Gruppe, $a \in G$ beliebig

$C_a : G \to G$, $x \mapsto axa^{-1}$ ist Homomorphismus, denn

$C_a(x \cdot y) = axya^{-1}$

$C_a(x) \cdot C_a(y) = axa^{-1}aya^{-1} = axya^{-1}$

(e) $G$ Gruppe, $a \in G$, $a \neq e$

$\lambda_a(x) = ax$ $\lambda_a : G \to G$ ist kein Homomorphismus, denn $\lambda_a(e) = a$

$\lambda_a(e \cdot e)$, aber $\lambda_a(e)\lambda_a(a) = a \cdot a \neq a$ (kürzen!)

**Lemma** Sei $\varphi: G \to K$ ein Homomorphismus von Gruppen. Dann gilt $\varphi(e_G) = e_K$ und $\varphi(x^{-1}) = \varphi(x)^{-1}$ für alle $x \in G$. ($e_G$ Neutralelement in $G$ und $e_K$ Neutralelement in $K$)

**Beweis** $\varphi(e_G) = \varphi(e_G \cdot e_G) = \varphi(e_G) \cdot \varphi(e_G)$

Kürzen

$\Rightarrow \quad e_K = \varphi(e_G)$

$\varphi(x^{-1}x) = \varphi(x^{-1})\varphi(x) \quad \Rightarrow \quad \varphi(x)^{-1} = \varphi(x^{-1})$

$\varphi(e_G) = e_K$

□

Achtung: $\varphi(x)^{-1}$ ist das Inverse in $K$ von $\varphi(x)$ **nicht** die "Umkehrabbildung"!

Das **Bild** eines Homomorphismus $\varphi: G \to K$ ist $\varphi(G) \subseteq K$, der **Kern** ist

$$\ker(\varphi) = \{ x \in G \mid \varphi(x) = e_K \} \subseteq G$$

16. **Satz** Bilder und Kerne von Gruppenhomomorphismen sind Untergruppen.

**Beweis** Sei $H = \varphi(G) \subseteq K$. Es folgt $e_K \in H$. Für $\varphi(x), \varphi(y) \in H$ ist $\varphi(x)\varphi(y) = \varphi(xy) \in H$ sowie $\varphi(x)^{-1} = \varphi(x^{-1}) \in H$, also ist $H$ Untergruppe.

Betrachte jetzt $\ker(\varphi) \subseteq G$. Es gilt $\varphi(e_G) = e_K$, also $e_G \in \ker(\varphi)$. Ist $x, y \in \ker(\varphi)$, so folgt

$\varphi(xy) = \varphi(x) \cdot \varphi(y) = e_K \cdot e_K = e_K$, also $xy \in \ker(\varphi)$

$\varphi(x^{-1}) = \varphi(x)^{-1} = e_K^{-1} = e_K$, also $x^{-1} \in \ker(\varphi)$ □

Bem Jede Untergruppe $H \subseteq G$ ist Bild eines geeigneten Homomorphismus (nämlich der Inklusion $H \hookrightarrow G$). Wir werden sehen, dass* nicht jede Untergruppe $H \subseteq G$ Kern eines Homomorphismus ist.

* im allgemeinen

17. Definition + Satz Sei $G$ eine Gruppe und $N \subseteq G$ eine Untergruppe. Wir nennen $N$ normal in $G$ oder Normalteiler in $G$, wenn eine der folgenden äquivalenten Bedingungen erfüllt ist

(i) Für alle $a \in G$ gilt $aN = Na$
(Rechtsnebenklassen sind Linksnebenklassen)

(ii) Für alle $a \in G$ gilt $aNa^{-1} = N$
$(aNa^{-1} = \{ana^{-1} \mid n \in N\})$

(iii) für alle $a \in G$ gilt $aN \subseteq Na$

(iv) für alle $a \in G$ gilt $aNa^{-1} \subseteq N$

**Beweis** (i) und (ii) sind äquivalent:

multiplizieren von rechts mit $a^{-1}$ bzw $a$

Genauso sind (iii) und (iv) äquivalent.

Klar: (ii) $\Rightarrow$ (iv) ($\checkmark$)

Zeige (iv) $\Rightarrow$ (ii):

Setze $b = a^{-1}$, es folgt aus (iv), dass

$bNb^{-1} \subseteq N \rightsquigarrow N \subseteq b^{-1}Nb = aNa^{-1}$

also gilt für alle $a \in G$, dass $N \subseteq aNa^{-1}$

und $aNa^{-1} \subseteq N$, damit gilt (ii) $\square$

**Lemma** Ist $\varphi: G \to K$ ein Homomorphismus von Gruppen, dann ist $\ker(\varphi)$ ein Normalteiler in $G$.

**Beweis** Sei $N = \ker(\varphi) = \{n \in G \mid \varphi(n) = e\}$,

sei $a \in G$. Dann gilt $\varphi(ana^{-1}) =$

$\varphi(a)\underbrace{\varphi(n)}_{=e}\varphi(a^{-1}) = \varphi(aa^{-1}) = e$, also gilt

$aNa^{-1} \subseteq N$ für alle $a \in G$. $\square$

Achtung: Bilder von Homomorphismen sind nicht immer Normalteiler, nach Beispiel § 1.15 (b) ist jede Untergruppe Bild eines Homomorphismus – aber nicht jede Untergruppe ist normal.

Beispiel $G = \mathrm{Sym}(3)$ · $g = (1,2)$ Transposition, die 1 und 2 vertauscht $g^2 = \mathrm{id}$, $\langle g \rangle = \{g, \mathrm{id}\}$ $\subseteq \mathrm{Sym}(3)$ ist Untergruppe, aber für $h = (2,3)$ gilt $h\langle g \rangle h^{-1} = \{ hgh^{-1}, h\,\mathrm{id}\,h^{-1} \}$

$= \{ \underbrace{(2,3)(1,2)(2,3)}_{=(3,1)}, \mathrm{id} \} \notin \langle g \rangle$, also ist $\langle g \rangle$ kein Normalteiler in $\mathrm{Sym}(3)$.

Schreibweise: Ist $N \subseteq G$ ein Normalteiler, schreibt man kurz

$$N \trianglelefteq G$$

Beachte: Ist $G$ abelsch, dann sind alle Untergruppen $H \subseteq G$ automatisch normal.

18. Def + Satz

Für Teilmengen $X, Y, Z \subseteq G$ in einer Gruppe schreibe kurz

$$XY = \{xy \mid x \in X, y \in Y\} \subseteq G$$

$$X^{-1} = \{x^{-1} \mid x \in X\} \subseteq G$$

Es gilt dann $(XY)Z = X(YZ)$

(weil die Verknüpfung assoziativ ist).

Satz Sei $N \trianglelefteq G$ Normalteiler in der Gruppe $G$. Dann ist $G/N = \{gN \mid g \in G\}$ eine Gruppe mit der Verknüpfung

$$(gN) \cdot (hN) = ghN$$

Das Neutralelement ist $eN = N$, das Inverse zu $gN$ ist $g^{-1}N$.

Beweis. Da $N$ Normalteiler ist, gilt für $g, h \in G$

$$gNhN = g(Nh)N = g(hN)N = ghNN$$

($Nh = hN$ nach §1.17)

$$= ghN$$

($N$ Gruppe)

Die Verknüpfung ist also einfach gegeben durch

$$gN \cdot hN = gNhN = ghN$$

und damit assoziativ nach obiger Bemerkg.

Es gilt $N\,gN = gNN = gN = gNN$

also ist $N$ ein Neutralelement. Weiter gilt

$gN\,g^{-1}N = gg^{-1}N = N = g^{-1}gN = g^{-1}N\,gN$ □

19. Def Ist $G$ eine Grp und $H$ eine Untergrp, so definieren wir $\pi_H : G \to G/H$ durch $\pi_H(g) = gH$.

Satz Ist $N \trianglelefteq G$ ein Normalteiler, dann ist $\pi_N : G \to G/N$ ein surjektiver Homomorphismus mit $\ker N = \ker(\pi_N)$.

Beweis $\pi_N$ ist nach Definition surjektiv und $\pi_N(gh) = ghN = gNhN = \pi_N(g)\pi_N(h)$.

Weiter gilt $\pi_N(g) = N \Leftrightarrow gN = N$

$\Leftrightarrow g \in N$

↑ §1.13 □

Folgerung: Jeder Normalteiler ist auch ein Kern eines Homomorphismus.

## 20. Theorem (Der Homomorphisatz)

Sei $G \xrightarrow{\varphi} K$ ein Homomorphismus von Gruppen, sei $N \trianglelefteq G$ ein Normalteiler. Wenn gilt $N \subseteq \ker(\varphi)$, dann gibt es genau einen Homomorphismus $\bar{\varphi}: G/N \to K$ mit $\bar{\varphi} \circ \pi_N = \varphi$

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & K \\ & {\scriptstyle \pi_N} \searrow \quad \nearrow {\scriptstyle \bar{\varphi}} & \\ & G/N & \end{array}$$

#

Beweis Existenz von $\bar{\varphi}$: Für $g \in G$ sei $\bar{\varphi}(gN) = \varphi(g)$. Das ist eine wohldefinierte Abbildung, denn angenommen, $gN = g'N$

$\Rightarrow g^{-1}g' \in N \subseteq \ker(\varphi) \Rightarrow \varphi(g^{-1}g') = e$

$\Rightarrow \varphi(g) = \varphi(g')$. Es gilt damit

$\bar{\varphi}(gNhN) = \bar{\varphi}(ghN) = \varphi(gh) = \varphi(g)\varphi(h)$

$= \bar{\varphi}(gN)\bar{\varphi}(hN)$, also ist $\bar{\varphi}$ ein Homomorphismus.

Eindeutigkeit von $\bar{\varphi}$: Sei $\psi: G/N \to K$ ein Homomorphismus mit $\psi \circ \pi_N = \varphi$.

Es folgt $\varphi(gN) = \varphi(\pi_N(g)) = \varphi(g) = \bar{\varphi}(gN)$
für alle $g \in G$. □

Bem In der Situation von Homomorphiesatz gilt:

(i) $\ker(\varphi) = \pi_N^{-1}\ker(\bar{\varphi})$

(ii) $\ker(\bar{\varphi}) = \pi_N \ker(\varphi)$

(iii) $\varphi(G) = \bar{\varphi}(G/N)$

Beweis (iii) ist klar nach Konstruktion, $\bar{\varphi}(gN) = \varphi(g)$

(ii) $\bar{\varphi}(gN) = e = \varphi(g) \Leftrightarrow g \in \ker(\varphi) \Leftrightarrow$

also $\ker(\bar{\varphi}) = \pi_N(\ker(\varphi))$

(i) $\varphi(g) = e \Rightarrow g \in \ker(\varphi) \Rightarrow \pi_N(g) \in \ker(\bar{\varphi})$

$\Rightarrow \varphi(g) = e$ □

21. Def Ein Gruppenhomomorphismus

$\varphi: G \to K$ heißt Mono/Epi/Isomorphismus, wenn $\varphi$ injektiv/surjektiv/bijektiv ist.

(Klar: $\varphi$ Epimorphismus $\Leftrightarrow \varphi(G) = K$)

Für ein Mono/Epi/Isomorphismus schreibt man

$\xrightarrow{\varphi}$ $\quad\xrightarrow{\varphi}\!\!\!\rightarrow$ und $\xrightarrow{\cong}$

**Lemma** Ein Gruppenhomomorphismus $G \xrightarrow{\varphi} K$ ist genau dann injektiv, wenn gilt $\ker(\varphi) = \{e_G\}$.

**Beweis:** Wenn $\varphi$ injektiv ist, dann ist $\ker(\varphi) = \{e_G\}$ (klar). Angenommen, $\ker(\varphi) = \{e\}$ und $a, b \in G$ mit $\varphi(a) = \varphi(b)$ $\Rightarrow$ $\varphi(a)\varphi(b)^{-1} = \varphi(ab^{-1}) = e_K$

$\Rightarrow ab^{-1} = e_G \Rightarrow a = b$ □

22. **Satz** Sei $G \xrightarrow{\varphi} K$ ein Gruppenhomomorphismus. Dann gilt folgendes:

(i) Ist $H \leq G$ Untergruppe, so ist $\varphi(H) \leq K$ Untergruppe. Wenn $H \trianglelefteq G$, so gilt $\varphi(H) \trianglelefteq \varphi(G)$

(ii) Ist $L \leq K$ Untergruppe, so ist $\varphi^{-1}(L) \leq G$ Untergruppe. Ist $L \trianglelefteq K$, so gilt $\varphi^{-1}(L) \trianglelefteq G$.

**Beweis:** (i) Sei $a, b \in H$ und $g \in G$. Es gilt

$\varphi(a)\varphi(b) = \varphi(ab) \in \varphi(H)$, $\varphi(a)^{-1} = \varphi(a^{-1}) \in \varphi(H)$

$\varphi(e_G) = e_K \in \varphi(H) \Rightarrow \varphi(H)$ Untergruppe.

Ist $H \trianglelefteq G$, so folgt $\varphi(g)\varphi(H)\varphi(g)^{-1}$

$= \varphi(gHg^{-1}) \underset{\uparrow H \trianglelefteq G}{=} \varphi(H)$ □

(ii) Si $a,b \in \varphi^{-1}(L)$, $g \in G$ (also $\varphi(a), \varphi(b) \in L$)

Es folgt $\varphi(ab) \in L$, $\varphi(a^{-1}) = \varphi(a)^{-1} \in L$ usw

$\varphi(e_G) = e_K \Rightarrow ab, a^{-1}, e_G \in \varphi^{-1}(L) \rightsquigarrow$ Untergruppe

Außerdem, $L \trianglelefteq K$. Es folgt

$\varphi(gag^{-1}) = \varphi(g)\varphi(a)\varphi(g)^{-1} \in L$, also

$g\,\varphi^{-1}(L)\,g^{-1} \subseteq \varphi^{-1}(L)$ □

<u>Beispiele</u> Gruppe $G = (\mathbb{Z}, +)$, $\varphi(z) = m \cdot z$

$m \in \mathbb{Z}$ fest $\varphi : \mathbb{Z} \to \mathbb{Z}$ Homomorphismus

$\varphi(\mathbb{Z}) = m\mathbb{Z} = \{mz \mid z \in \mathbb{Z}\} = (-m)\mathbb{Z}$

z.B. $m = 2 \rightsquigarrow 2\mathbb{Z} = \{0, \pm 2, \pm 4, \pm 6, \ldots\}$ gerade Zahlen

$$\ker(\varphi) = \begin{cases} \{0\} & \text{wenn } m \neq 0 \\ \mathbb{Z} & \text{wenn } m = 0 \end{cases}$$

$\varphi$ surjektiv $\Leftrightarrow m = \pm 1$

$\varphi$ injektiv $\Leftrightarrow m \neq 0$

Außerdem, $m > 0$, $a, b \in \mathbb{Z}$

$a + m\mathbb{Z} = b + m\mathbb{Z}$ Nebenklassen

$\Leftrightarrow a \in b + m\mathbb{Z} \Leftrightarrow a - b \in m\mathbb{Z}$

↑ §1.13

Folglich $\mathbb{Z}/m\mathbb{Z} = \{m\mathbb{Z}, 1+m\mathbb{Z}, 2+m\mathbb{Z}, \dots, (m-1)+m\mathbb{Z}\}$

insbesondere $\#\,\mathbb{Z}/m\mathbb{Z} = m$

Schreibe $\overline{k} = k + m\mathbb{Z}$ Kongruenzklasse von $k$ modulo $m$

$\mathbb{Z}/m\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \dots, \overline{m-1}\}$ wird erzeugt

von $\overline{1}$ $\rightsquigarrow$ $\mathbb{Z}/m\mathbb{Z} = \langle \overline{1} \rangle$ zyklische Gruppe der Ordnung $m$. $o(\overline{1}) = m$.

Später mehr dazu.

## 23. Die Isomorphiesätze

**Lemma** Sei $G$ eine Gruppe, seien $H, N \subseteq G$ Untergruppen. Wenn $N \trianglelefteq G$ gilt, dann ist $HN = NH \subseteq G$ eine Untergruppe.

**Beweis.** Es gilt $e = e \cdot e \in N \cdot H$. Weiter gilt für $h_1, h_2 \in H$ $n_1, n_2 \in N$, dass

$$h_1 n_1 h_2 n_2 = \underbrace{h_1 h_2}_{\in H} \underbrace{h_2^{-1} n_1 h_2}_{\in N} n_2 \in HN$$

$$(h_1 n_1)^{-1} = n_1^{-1} h_1^{-1} = h_1^{-1} \underbrace{h_1 n_1^{-1} h_1^{-1}}_{\in N} \in HN$$

$$(HN)^{-1} = N^{-1} H^{-1} = NH \subseteq HN \quad \text{genauso } HN \subseteq NH \qquad \square$$

**Satz** Sei $G \xrightarrow{\varphi} K$ ein Epimorphismus von Gruppen. Sei $N = \ker(\varphi)$. Dann ist die Abbildung $\bar{\varphi} : G/N \to K$ aus dem Homomorphiesatz §1.20 ein Isomorphismus.

**Beweis** $\bar{\varphi}(G/N) = \varphi(G)$ und $\ker(\bar{\varphi}) = \{N\}$ nach dem Beweis §1.20 □

Den Isomorphismus $\bar{\varphi} : G/\ker(\varphi) \xrightarrow{\cong} K$ nennt man ~~#~~ kanonisch / natürlich.

< 26½

**Theorem** (1. Isomorphiesatz) Sei $G$ eine Gruppe, seien $H, N \leq G$ Untergruppen mit $N \trianglelefteq G$. Dann gilt $H \cap N \trianglelefteq H$, $N \trianglelefteq NH$ und die Abbildung

$$H/H\cap N \xrightarrow{\psi} NH/N$$
$$aH\cap N \longmapsto aN$$

ist ein Isomorphismus. ("Kürzungsregel")

**Beweis** Für alle $h \in H$ gilt $h(H\cap N)h^{-1} \subseteq N \cap H$, weil $N \trianglelefteq G$ und $hHh^{-1} = H$. $\Rightarrow N \cap H \trianglelefteq H$

Für alle $g \in NH$ gilt $gNg^{-1} \subseteq N \Rightarrow N \trianglelefteq NH$

**Lemma** Sei $G \xrightarrow{\varphi} K$ ein Gruppenhomomorphismus. Dann sind äquivalent:

(i) $\varphi$ ist bijektiv

(ii) es gibt ein Homomorphismus $\psi: K \to G$ mit $\varphi \circ \psi = id_K$ und $\psi \circ \varphi = id_G$.

**Beweis** (ii) $\Rightarrow$ (i) klar, aus $\varphi \circ \psi = id_K$ folgt, dass $\varphi$ surjektiv ist und aus $\psi \circ \varphi = id_G$ folgt, dass $\varphi$ injektiv ist.

(i) $\Rightarrow$ (ii) Sei $\psi: K \to G$ die eindeutig bestimmte Umkehrabbildung, also $\varphi \circ \psi = id_K$, $\psi \circ \varphi = id_G$.

Für $a, b \in K$ folgt $\psi(ab) = \psi(\varphi\psi(a)\,\varphi\psi(b))$

$= \psi(\varphi(\psi(a)\psi(b)))$ $= \psi(a)\psi(b)$ □

($\varphi$ Hom; $\psi \circ \varphi = id$)

Betrachte die Abbildung $\varphi: H \to HN/N \subseteq G/N$
$h \longmapsto hN$

das ist ein Homomorphismus, weil $H \xrightarrow{i} G \xrightarrow{\pi_N} G/N$ ein ist. Für $hn \in HN$ gilt $\varphi(h) = hN = hnN$, also ist $\varphi$ ein Epimorphismus. Der Kern ist $\ker(\varphi) = \{h \in H \mid hN = N\} = H \cap N$. Also gilt nach dem vierten Satz $H/N \cap H \xrightarrow[\cong]{\bar{\varphi}} HN/N$ □

Theorem (2. Isomorphiesatz) Sei $G$ Gruppe, seien $M, N \trianglelefteq G$ Normalteiler mit $M \subseteq N \subseteq G$. Dann gilt $N/M \trianglelefteq G/M$ und

$$\frac{G/M}{N/M} \cong G/N$$

"Kürzungsregel"

Beweis: Es gilt $N/M = \{nM \mid n \in N\} = \pi_M(N) \subseteq G/M$

Nach §1.22 (i) gilt $N/M \trianglelefteq G/M$.

Liefert Homomorphiesatz §1.20

$$\begin{array}{ccc} G & \xrightarrow{\pi_N} & G/N \\ & \searrow^{\pi_M} \quad \nearrow_{\bar{\pi}_N} & \\ & G/M & \end{array}$$

$\bar{\pi}_N$ ← surjektiv

Nach d vorn Satz gilt

$$\frac{G/M}{\ker(\overline{\pi}_N)} \xrightarrow{\cong} G/N$$

$$\ker(\overline{\pi}_N) = \pi_M(N) = N/M$$

(↑ §1.20) □

## 24. Produkt von Gruppen

Seien $G, K$ zwei Gruppen. Dann ist das Produkt $G \times K$ wieder eine Gruppe mit Verknüpfung, das direkt Produkt, wird

$$(g_1, k_1) \cdot (g_2, k_2) = (g_1 g_2, k_1 k_2)$$

Neutralelement $e = (e_G, e_K)$

Das Inverse zu $(g, k) \in G \times K$ ist

$$(g, k)^{-1} = (g^{-1}, k^{-1})$$

Den Beweis lassen wir weg, die Gruppenaxiome (G1) – (G3) sind leicht nachzuprüfen.

Wir haben kanonische Homomorphismen

$$i_G : G \to G \times K \qquad i_K : K \to G \times K$$
$$g \mapsto (g, e_K) \qquad k \mapsto (e_G, k)$$

sowie $pr_G : G \times K \to G$, $(g,k) \mapsto g$

$pr_K : G \times K \to K$, $(g,k) \mapsto k$

mit $pr_G \circ i_G = id_G$ $\quad pr_K \circ i_K = id_K$

$\ker(pr_G) = \{e_G\} \times K \cong K$ $\quad \ker(pr_K) = G \times \{e_K\} \cong G$

Das gilt auch mit Familien von (auch unendlich vielen) Gruppen: ist $(G_i)_{i \in I}$ eine Familie von Gruppen, so ist $\prod_{i \in I} G_i$ wieder eine Gruppe, das <u>direkte Produkt</u> der $G_i$. Die Elemente sind Folgen $(g_i)_{i \in I}$ $g_i \in G_i$ mit Verknüpfung $(g_i)_{i \in I} \cdot (g_i')_{i \in I} = (g_i g_i')_{i \in I}$ usw.

<u>Satz</u> Sei $G$ eine Gruppe mit Untergruppen $H, K \leq G$. Angenommen, es gilt folgendes

(i) $G = HK$

(ii) $H \cap K = \{e\}$

(iii) $hk = kh$ für alle $h \in H$ $k \in K$.

Dann ist die Abbildung $H \times K \xrightarrow{\varphi} G$, $(h,k) \mapsto hk$

ein Isomorphismus, d.h. $G$ "ist" das direkte Produkt aus $H$ und $K$.

Beis: Wegen (iii) gilt

$$\varphi((h_1,k_1)(h_2,k_2)) = \varphi((h_1h_2, k_1k_2)) = h_1h_2k_1k_2$$

$$\varphi(h_1,k_1)\varphi(h_2,k_2) = h_1k_1h_2k_2 = h_1h_2k_1k_2$$

also ist $\varphi$ ein Homomorphismus. Wegen (i) ist $\varphi$ surjektiv. $(h,k) \in \ker(\varphi) \Leftrightarrow hk = e \Leftrightarrow$ $h = k^{-1} \Leftrightarrow h = k = e$ wegen (ii)

($h \in H$, $k \in K$) □

Beispiel $G = \mathbb{Z}/6\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$ vgl. § 1.24. Dann sind $H = \{\bar{0}, \bar{3}\}$ sowie $K = \{\bar{0}, \bar{2}, \bar{4}\}$

Untergruppen (nachrechnen!), $H \cong \mathbb{Z}/2\mathbb{Z}$, $K \cong \mathbb{Z}/3\mathbb{Z}$

und (i), (ii) (iii) aus dem vor. Satz sind erfüllt. Es folgt

$$\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \quad (!)$$

#