# §1 Gruppen, Untergruppen, Homomorphismen

**1. Def** Eine Verknüpfung auf einer Menge $X$ ist eine Abbildung $m : X \times X \to X$, die zwei Elementen $u, v$ ein Element $m(u,v) \in X$ zuordnet. Häufig schreibt man $m(x,y) = x \cdot y$ oder $m(x,y) = xy$.

Beispiele $\mathbb{N} = \{0, 1, 2, 3, \dots\}$ natürliche Zahlen

$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \dots\}$ ganze Zahlen

(a) Verknüpfung "+" auf $\mathbb{N}$ (oder $\mathbb{Z}$)
$(u,v) \longmapsto u+v$

(b) Verknüpfung "−" auf $\mathbb{Z}$; $(u,v) \longmapsto u-v$

(c) Verknüpfung max auf $\mathbb{N}$, $(u,v) \longmapsto \max(u,v)$

(d) Verknüpfung "·" auf $\mathbb{N}$ (oder $\mathbb{Z}$)
$(u,v) \longmapsto u \cdot v$ (Multiplikation)

Eine Verknüpfung $m$ heißt assoziativ, wenn für alle $u, v, w \in X$ gilt $m(u, m(v,w)) = m(m(u,v), w)$ oder kurz, wenn $u(vw) = (uv)w$ stets gilt.

Eine Menge $(X, \cdot)$ mit einer assoziativen Verknüpfung $\cdot$ heißt Halbgruppe.

Welche der Beispiele (a) – (d) sind assoziativ?

2. Def Eine Gruppe $(G, \cdot)$ besteht aus einer Menge $G$ und einer Verknüpfung $\cdot$ auf $G$ so, dass folgendes gilt:

(G1) Die Verknüpfung ist assoziativ, d.h. für alle $u, v, w \in G$ gilt $u \cdot (v \cdot w) = (u \cdot v) \cdot w$

(G2) Es gibt ein Neutralelement $e \in G$, d.h. ein Element $e$ mit $u \cdot e = u = e \cdot u$ für alle $u \in G$

(G3) Jedes Element $u \in G$ hat ein Inverses $v \in G$, d.h. $u \cdot v = v \cdot u = e$.

Bem • (G1) sagt, dass man Klammern weglassen darf $u \cdot v \cdot w = (u \cdot v) \cdot w = u \cdot (v \cdot w)$

• Das Neutralelement ist eindeutig bestimmt, denn: angenommen, $e, \tilde{e} \in G$ sind beides Neutralelement. Dann gilt $e = e \cdot \tilde{e} = \tilde{e}$.

- Jedes $u \in G$ hat genau ein Inverses $v$,
  denn: wenn $v, \tilde{v}$ beides Inverse zu $u$ sind,
  so folgt $u \cdot v = e = \tilde{v} \cdot u \Rightarrow \tilde{v} = \tilde{v} \cdot e = \tilde{v} \cdot u \cdot v = e \cdot v = v$

Welche der Verknüpfungen aus Bsp (a)–(d) ergeben Gruppen? Wo gibt es Neutralelemente, wo gibt es Inverse? [Nur $(\mathbb{Z}, +)$ ist eine Grp.]

3. Lemma (Sparsamere Definition von Gruppen)
   Sei $(G, \cdot)$ eine Menge mit einer assoziativen Verknüpfung "$\cdot$". Dann ist $(G, \cdot)$ eine Gruppe genau dann, wenn gilt
   (G2') Es gibt ein $e \in G$ so, dass $ue = u$ für alle $u \in G$ gilt.
   (G3') Zu jedem $u \in G$ gibt es ein $v \in G$ mit $u \cdot v = e$.

   Beweis: In jeder Gruppe gelten (G2) und (G3), also auch (G2') und (G3').

   Annahme, es gilt (G1), (G2') und (G3').
   Wir müssen zeigen, dass (G2) und (G3) auch gelten.

Sei $u \in G$ und $v \in G$ mit $u \cdot v = e$, sei $w \in G$ mit $v \cdot w = e$, es folgt

$$v \cdot u = v \cdot u \cdot \underbrace{v \cdot w}_{=e} = v \cdot w = e \quad , \text{also (G3)}$$

sowie $e \cdot u = u \cdot v \cdot u = u \cdot e = u$, also (G2). □

Das eindeutige Inverse von $u \in G$ in einer Gruppe $G$ bezeichnen wir ab jetzt mit $u^{-1}$, also

$$u \cdot u^{-1} = u^{-1} \cdot u = e.$$

4. Ein (wichtiges) Beispiel, die symmetrische Gruppe.

Sei $X \neq \emptyset$ eine Menge. Wir betrachten die Menge $M(X) = \{ f : X \to X \mid f \text{ Abbildung} \}$ aller Abbildungen von $X$ nach $X$.

Auf der Menge $M(X)$ ist die Hintereinanderausführung (Komposition) von Abbildungen eine assoziative Verknüpfung "$\circ$":

$$(f \circ g)(x) = f(g(x)) \quad \text{für } x \in X, \; f, g \in M(X)$$

$$((f \circ g) \circ h)(x) = f(g(h(x))) = (f \circ (g \circ h))(x)$$

Es sei $id_X$ die identische Abbildung,

also $id_X(x) = x$ für alle $x \in X$. Dann gilt für

alle $f \in M(X)$, dass $(id_X \circ f)(x) = f(x)$

$= (f \circ id_X)(x)$

also ist $id_X \in M(X)$ ein Neutralelement und damit

gelten (G1) und (G2). Was ist mit (G3)?

$f \circ g = id_X \Rightarrow$ $f$ surjektiv und $g$ injektiv

$g(x) = g(y) \Rightarrow f(g(x)) = x = f(g(y)) = y \Rightarrow x = y$

$z \in X \Rightarrow z = f(g(z)) \Rightarrow z = f(x)$ für $x = g(z)$

d.h. $f$ hat ein Inverses genau dann, wenn

$f$ bijektiv ist (bijektiv = injektiv und surjektiv)

Wir setzen $Sym(X) = \{ f \in M(X) \mid f \text{ ist bijektiv} \}$

Dann ist $(Sym(X), \circ)$ eine Gruppe, die

symmetrische Gruppe auf der Menge $X$.

Denn: $f, g \in Sym(X) \Rightarrow f \circ g \in Sym(X)$

$\Rightarrow$ (G1) gilt

$id_X \in Sym(X)$ $\Rightarrow$ (G2) gilt

$f \in Sym(X) \Rightarrow f$ hat Umkehrabbildung $f^{-1}$

(weil bijektiv: zu jedem $z \in X$ gibt es genau

ein $x \in X$ mit $f(x) = z$. Definiere $g(z) = x$

$\Rightarrow$ $g(f(x)) = g(z) = x$ und $f(g(z)) = f(x) = z$

$\Rightarrow$ $g \circ f = id_X = f \circ g$.

Die Elemente von $Sym(X)$ heißen Permutationen. □

Beispiel • $X = \{1\}$, es gibt genau eine (bijektive) Abbildung $f: X \to X$ $\Rightarrow$ $Sym(X) = M(X) = \{id_X\}$.

• $X = \{1,2\}$, es gibt genau vier Abbildungen $f: X \to X$, davon sind genau zwei bijektiv, nämlich $id_X$ und $t: \begin{cases} 1 \mapsto 2 \\ 2 \mapsto 1 \end{cases}$

$\Rightarrow$ $M(X) \supsetneq Sym(X) = \{id_X, t\}$ mit $t \circ t = id_X$ $\Rightarrow$ $t = t^{-1}$.

• $X = \{1,2,3\}$, es gibt genau $3^3 = 27$ Abbildungen $f: X \to X$, von denen genau 6 bijektiv sind, nämlich $id_X$,

$\alpha: \begin{cases} 1 \mapsto 2 \\ 2 \mapsto 1 \\ 3 \mapsto 3 \end{cases}$, $\beta: \begin{cases} 1 \mapsto 3 \\ 2 \mapsto 2 \\ 3 \mapsto 1 \end{cases}$ $\gamma: \begin{cases} 1 \mapsto 1 \\ 2 \mapsto 3 \\ 3 \mapsto 2 \end{cases}$

$\delta: \begin{cases} 1 \mapsto 2 \\ 2 \mapsto 3 \\ 3 \mapsto 1 \end{cases}$ $\varepsilon = \begin{cases} 1 \mapsto 3 \\ 2 \mapsto 1 \\ 3 \mapsto 2 \end{cases}$

#

Beweis: $\alpha \circ \alpha = \beta \circ \beta = \gamma \circ \gamma = id_X$

$\delta \circ \delta \circ \delta = id_X = \varepsilon \circ \varepsilon \circ \varepsilon$

Weiter $\beta \circ \alpha = \begin{Bmatrix} 1 \mapsto 2 \\ 2 \mapsto 3 \\ 3 \mapsto 1 \end{Bmatrix} = \delta$

$\alpha \circ \beta = \begin{Bmatrix} 1 \mapsto 3 \\ 2 \mapsto 1 \\ 3 \mapsto 2 \end{Bmatrix} = \varepsilon$

insbesondere ist $\alpha \circ \beta \neq \beta \circ \alpha$.

5. Def Ein Gruppe $(G, \cdot)$ heißt kommutativ oder abelsch (→ N. Abel, norw. Mathematiker, 1802 - 1829), wenn für alle $u, v \in G$ gilt $u \cdot v = v \cdot u$

Bsp
- $(\mathbb{Z}, +)$ ist abelsch (Addition ist kommutativ)
- $Sym(\{1\})$, $Sym(\{1,2\})$ sind abelsch
- $Sym(\{1,2,3\})$ ist nicht abelsch.

6. Bsp Die allgemeine lineare Gruppe (vgl. LA I)

Sei $K$ ein Körper, z.B. $K = \mathbb{R}, \mathbb{C}, \mathbb{Q}$, sei $n \geq 1$, $K^{n \times n}$ die Menge der $n \times n$-Matrizen mit Einträgen aus $K$, sei $GL_n(K) = \{ a \in K^{n \times n} \mid \det(a) \neq 0 \}$

In LA I wurde bewiesen:

(1) $\det(ab) = \det(a) \cdot \det(b)$ für $a, b \in K^{n \times n}$
↑ Matrizenmultiplikation

(2) $a \in K^{n \times n}$ ist invertierbar $\Leftrightarrow$ $\det(a) \neq 0$

Damit ist $GL_n(K)$ eine Gruppe (denn Matrizenmultiplikation ist assoziativ), mit Neutralelement $\mathbb{1}_n = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$.

Bsp $\underbrace{\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}}_{\det = 1} \underbrace{\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}}_{\det = -1} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$

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

$\Rightarrow$ $GL_2(K)$ ist nicht abelsch.

6. Def Sei $(G, \cdot)$ eine Gruppe. Eine Teilmenge $H \subseteq G$ heißt Untergruppe von $G$, falls gilt:

(UG1) $e \in H$

(UG2) für alle $u, v \in H$ gilt $u \cdot v \in H$

(UG3) für alle $u \in H$ gilt $u^{-1} \in H$

Beispiel. $(G, \cdot)$ beliebige Gruppe, dann sind sowohl $G$ als auch $\{e\} \subseteq G$ Untergruppen.

- $(G,\cdot) = (\mathbb{Z},+)$ Gruppe der ganzen Zahlen.

Sei $m \in \mathbb{N}$. Dann ist $m\mathbb{Z} = \{m \cdot k \mid k \in \mathbb{Z}\}$ eine Untergruppe, die Gruppe der Vielfachen von $m$.

Denn $0 = m \cdot 0 \in m\mathbb{Z}$ $\rightsquigarrow$ (UG1)

$m \cdot k, m \cdot l \in m\mathbb{Z}$ $\rightsquigarrow$ $m \cdot k + m \cdot l = m(k+l) \in m\mathbb{Z}$

$\rightsquigarrow$ (UG2)

$-(m \cdot k) = (-m) k$ $\rightsquigarrow$ (UG3) □

- $\mathbb{N} \subseteq \mathbb{Z}$ ist keine Untergruppe. Es gelten (UG1) und (UG2), aber nicht (UG3), zum Beispiel ist $-1 \notin \mathbb{N}$ aber $1 \in \mathbb{N}$. □

ÜA (Sparsame Definition von Untergruppen)

Eine Teilmenge $H \subseteq G$ einer Gruppe $(G,\cdot)$ ist genau dann eine Untergruppe, wenn gilt:

(UG1') $H \neq \emptyset$

(UG2') $u, v \in H \Rightarrow u \cdot v^{-1} \in H$. □

Vereinigung von Untergruppen sind im allgemeinen keine Untergruppen.

Bsp $3\cdot\mathbb{Z}$, $5\cdot\mathbb{Z}$ sind Untergruppen von $\mathbb{Z}$, aber

$8 = 3+5 \notin 3\cdot\mathbb{Z} \cup 5\cdot\mathbb{Z} = \{0, \pm 3, \pm 5, \pm 6, \pm 10, \dots\}$

Anders ist es mit Durchschnitten.

7. Satz Sei $G$ eine Gruppe, sei $\mathcal{U}$ eine (nicht leere) Menge von Untergruppen von $G$.
Dann ist auch der Durchschnitt

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

eine Untergruppe von $G$.
Insbesondere $\Rightarrow$ $H, K \subseteq G$ Untergruppen $\Rightarrow$ $H \cap K$ ist eine Untergruppe (setze $\mathcal{U} = \{H, K\}$).

Beweis Für jedes $H \in \mathcal{U}$ gilt $e \in H \Rightarrow e \in \bigcap \mathcal{U}$.

Ist $x, y \in \bigcap \mathcal{U}$, so gilt für alle $H \in \mathcal{U}$, dass
$x, y \in H \Rightarrow x \cdot y \in H$ und $x^{-1} \in H$ für alle $H \in \mathcal{U}$
$\Rightarrow x \cdot y, x^{-1} \in \bigcap \mathcal{U}$. □

8. Def Sei $G$ eine Gruppe, sei $X \subseteq G$ eine Teilmenge. Wir definieren

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

und nennen das das Erzeugnis von $X$ (in $G$).

Nach §1.7 ist $\langle X \rangle \subseteq G$ eine Untergruppe. Ist $K \subseteq G$ irgend eine Untergruppe mit $X \subseteq K$, so folgt $\langle X \rangle \subseteq K$, also ist $\langle X \rangle$ die (bezüglich Inklusion "$\subseteq$") kleinste Untergruppe, die $X$ enthält.

Falls $X = \emptyset$, so ist $\langle X \rangle = \{e\}$.

Wenn $X$ aus genau einem Element besteht, $X = \{a\}$, so schreibt man $\langle X \rangle = \langle a \rangle \subseteq G$.

9. Satz Sei $G$ eine Gruppe, sei $X \subseteq G$ eine Teilmenge. Wir setzen $W = \{ x_1 \cdot x_2 \cdot \ldots \cdot x_m \mid m \geq 1, x_i \in X \text{ oder } x_i^{-1} \in X \text{ für alle } i = 1, \ldots, m \}$. Die Elemente von $W$ heißen Wörter in $X$.

Dann ist $\langle X \rangle = \{e\} \cup W$ (sogar $\langle X \rangle = W$, falls $X \neq \emptyset$).

Bem: Für jedes Wort $w \in W$ und jede Untergruppe $H \subseteq G$ mit $X \subseteq H$ gilt $w \in H \Rightarrow W \subseteq H$, damit $W \subseteq \langle X \rangle$. Ist $u, v \in W$, so ist $u \cdot w \in W$ und $u^{-1} \in W \Rightarrow W \cup \{e\}$ ist Untergruppe, die $X$ enthält $\Rightarrow \langle X \rangle \subseteq W \cup \{e\}$. Ist $X \neq \emptyset$, so ist $e = x \cdot x^{-1} \in W$ (für $x \in X$ beliebig). □

Ist $X = \{a\}$, so folgt $\langle a \rangle = \{ a^k \mid k \in \mathbb{Z} \}$, wobei

$$a^k = \begin{cases} e & \text{für } k = 0 \\ \underbrace{a \cdots a}_{k\text{-mal}} & \text{für } k > 0 \\ \underbrace{a^{-1} \cdots a^{-1}}_{k\text{-mal}} & \text{für } k < 0 \end{cases}$$ definiert ist.

10. Def Eine Gruppe $G$, die von einem Element $a \in G$ erzeugt wird, heißt zyklische Gruppe.

Bsp (a) $(\mathbb{Z}, +)$ wird von $1 \in \mathbb{Z}$ erzeugt, jede ganze Zahl $k \in \mathbb{Z}$ ist von der Form

$$k = \varepsilon(1 + 1 + \ldots + 1), \quad \varepsilon = \pm 1 \Rightarrow \mathbb{Z} \text{ ist zyklisch}$$

(b) $G = \{\pm 1\}$ mit Multiplikation als Verknüpfung, $G = \langle -1 \rangle$, denn $(-1) \cdot (-1) = 1$.
$\Rightarrow G$ ist zyklisch.

11. Lemma Zyklische Gruppen sind abelsch.

Bew. Sei $G$ zyklisch, also $G = \langle a \rangle$ für ein Element $a \in G$. Jedes $g \in G$ ist von der Form $a^k$ für ein $k \in \mathbb{Z}$. Es gilt $a^k \cdot a^l = a^{k+l} = a^{l+k} = a^l \cdot a^k$, also $G$ abelsch. □ #

12. Def Sei $G$ eine Gruppe, sei $g \in G$. Die Ordnung von $g$ ist

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

also $o(g) = m < \infty \iff g^m = e$ und $g^k \neq e$ für alle $1 \leq k < m$

$o(g) = \infty \iff g^k \neq e$ für alle $k \geq 1$

13. Lemma Wenn $G$ zyklisch ist, $G = \langle a \rangle$, so gilt: $|G| = o(a)$

↑ Anzahl der Elemente von $G$.

Ist $m = |G| < \infty$, so gilt $G = \{a, a^2, a^3, \ldots, a^m\}$.

Man nennt die Anzahl der Elemente $|G|$ die Ordnung der Gruppe $G$.

Beweis: Ist $a^k = a^l$ für $1 \le k < l$, so gilt

$$a^0 = e = a^{l-k}.$$

1. Fall: $o(a) = \infty$. Aus der Rechnung oben folgt, dass $a^k \neq a^l$ für alle $1 \le k < l \Rightarrow |G| = \infty$.

2. Fall: $o(a) = m < \infty$. Jedes $k \in \mathbb{Z}$ lässt sich schreiben als $k = l \cdot m + r$ mit $0 \le r < m$ (Teilen mit Rest). Also $a^k = a^{lm+r} = a^r$, es folgt $G = \{a, a^2, \dots, a^m\}$ und $|G| = m$. □

14. Korollar: Ist $G$ endlich, $|G| = m < \infty$ und gibt es ein Element $a \in G$ mit $o(a) = m$, so ist $G = \langle a \rangle$. Insbesondere ist $G$ dann abelsch.

Beweis: Ist $o(a) = m = |G|$, so ist $|\langle a \rangle| = m$ nach dem Lemma oben, damit $G = \langle a \rangle$. □

Wir werden bald sehen: für jedes $m \in \mathbb{N}$ gibt es eine zyklische Gruppe $G = \langle a \rangle$ mit $|G| = m$.

15 Def (Nebenklassen)

Sei $G$ eine Gruppe und sei $H \subseteq G$ eine Untergruppe. Für $a \in G$ definieren wir Teilmengen von $G$

$aH = \{ah \mid h \in H\}$ Linksnebenklasse von $a$

$Ha = \{ha \mid h \in H\}$ Rechtsnebenklasse von $a$

bzgl. $H$.

Im allgemein ist $aH \neq Ha$

Lemma A Sei $G$ eine Gruppe, $H \subseteq G$ eine Untergruppe, sei $a, b \in G$. Dann sind äquivalent

(i) $b \in aH$

(ii) $bH = aH$

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

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

$\rightsquigarrow bH = ahH = \{a\underbrace{hh'}_{\in H} \mid h' \in H\} = aH$

(ii) $\Rightarrow$ (iii) klar.

(iii) $\Rightarrow$ (i) Sei $g \in bH \cap aH \rightsquigarrow$

$g = ah = bh' \rightsquigarrow b = \underbrace{ah}_{\in H}h'^{-1} \in aH$ □

"Nebenklassen sind entweder gleich oder disjunkt!"

Entsprechend gilt für Rechtsnebenklassen.

Man schreibt $G/H = \{aH \mid a \in G\}$ Menge aller Linksnebenklassen

$H\backslash G = \{Ha \mid a \in G\}$ Menge aller Rechtsnebenklassen

Lemma 15 Sei $H \subseteq G$ Untergruppe von $G$, sei $a, b \in H$. Dann ist die Abbildung

$$aH \longrightarrow bH, \quad ah \longmapsto (ba^{-1})ah = bh$$

bijektiv. Insbesondere hat $aH$ und $bH$ gleich viele Elemente.

Beweis: Die Umkehrabbildung ist $bH \longrightarrow aH$
$bh \longmapsto (ab^{-1})bh$ □

16. Theorem (Satz von Lagrange) Sei $G$ eine Gruppe, sei $H$ eine Untergruppe. Wenn zwei der drei Mengen $G$, $H$, $G/H$ endlich sind, so ist es auch die dritte.

Dann gilt

$$|G| = |H| \cdot |G/H|$$

↑ Anzahl der Elemente

J.-L. Lagrange, 1736–1813, italienisch/französischer Mathematiker

Insbesondere ist $|H|$ dann ein Teiler von $|G|$.

Beis: Klar: $G$ endlich $\Rightarrow H, G/H$ auch endlich

Wenn $H, G/H$ endlich sind, so auch

$$G = \bigcup G/H = \bigcup \{ gH \mid g \in G \}$$

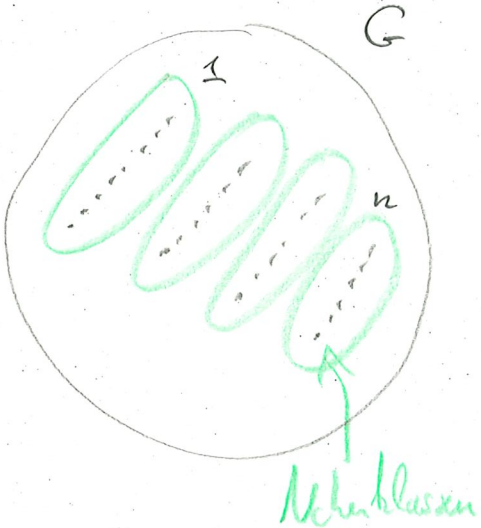
denn: $|gH| = |H|$, $G/H = \{ g_1 H, g_2 H, \dots, g_n H \}$

Jetzt zählen wir zusammen: $|G/H| = n$, $|H| = m$

Für $i \neq j$ ist $g_i H \cap g_j H = \emptyset$ nach §1.15 Lemma A.

$|g_i H| = |H|$ nach §1.15 Lemma B

$\Rightarrow |G| = |H| \cdot |G/H|$




□

Bemerkung: Eine ähnliche Aussage gilt für Rechtsnebenklassen

- Die Abbildung $gH \longmapsto Hg^{-1} = \{ (gh)^{-1} \mid h \in H \}$ ist eine Bijektion $G/H \longrightarrow H\backslash G$

es gibt "gleich viele" Links- und Rechtsnebenklassen von $H$.

**Def** Sei $G$ eine Gruppe, $H \leq G$ eine Untergruppe. Wir definieren $[G:H] = |G/H| = |H\backslash G|$, den **Index von $H$ in $G$**.

Ist $G$ endlich, so gilt also $|G| = |H| \cdot [G:H]$.

**Korollar A** Sei $G$ eine endliche Gruppe, sei $a \in G$. Dann ist $o(a)$ ein Teiler von $|G|$.

**Denn:** $|\langle a \rangle| = o(a)$ und $\langle a \rangle \leq G$ ist eine Untergruppe.

**Korollar B** Ist $G$ eine endliche Gruppe und ist $|G| = p$ eine **Primzahl**, so ist $G$ zyklisch (also insbesondere abelsch).

Für jedes $a \in G$ mit $a \neq e$ gilt dann $\langle a \rangle = G$.

Beweis Sei $a \in G$, $a \neq e$ ( $|G| \geq 2$ ).

Dann ist $o(a)$ ein Teiler von $p$ und $o(a) \neq 1$ weil $a \neq e$. Also ist $o(a) = p$, damit $G = \langle a \rangle$. □

Beispiel Für $G = \mathrm{Sym}(\{1,2,3\})$ ist $|G| = 6 = 2 \cdot 3$, vgl §1,4. Für jedes $a \in G$ gilt also $o(a) = 1, 2, 3$ ( $o(a) = 6$ kommt nicht vor - Warum? ) ≠1

17. Def Sei $(G, \cdot)$ eine Gruppe, sei $N \subseteq G$ eine Untergruppe. Wir nennen $N$ einen Normalteiler in $G$, wenn $N$ eine der folgenden äquivalenten Bedingungen erfüllt. Dann schreibt man $N \trianglelefteq G$.

(i) für alle $a \in G$ gilt

$$aNa^{-1} = N$$

$$( aNa^{-1} = \{ ana^{-1} \mid n \in N \} )$$

(ii) Für alle $a \in G$ gilt $aN = Na$

( Linksnebenklassen von $N$ sind auch Rechtsnebenklassen )

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

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

Beweis, dass die vier Bedingungen äquivalent sind.

(i) $\Leftrightarrow$ (ii) $aNa^{-1} = N \Leftrightarrow \underbrace{aNa^{-1}a}_{=aN} = Na$

(iii) $\Leftrightarrow$ (iv) genauso $aN \subseteq Na \Leftrightarrow aNa^{-1} \subseteq \underbrace{Naa^{-1}}_{=N}$

(ii) $\Rightarrow$ (iv) klar.

(iv) $\Rightarrow$ (ii): Ist $aNa^{-1} \subseteq N$ für alle $a \in G$,

so folgt $N \subseteq a^{-1}Na$ für alle $a \in G$,

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

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

Bemerkung: In einer abelschen Gruppe gilt stets

$aN = Na$, also ist jede Untergruppe einer

abelschen Gruppe ein Normalteiler.

Bsp $\mathrm{Sym}(\{1,2,3\})$ $H = \langle \alpha \rangle$, wobei

$$\alpha: \begin{cases} 1 \mapsto 2 \\ 2 \mapsto 1 \\ 3 \mapsto 3 \end{cases} \qquad H = \{id_X, \alpha\} \qquad X = \{1,2,3\}$$

$\alpha \circ \alpha = id_X$ das ist kein Normalteiler,

für $\beta: \begin{cases} 1 \mapsto 3 \\ 2 \mapsto 2 \\ 3 \mapsto 1 \end{cases}$ gilt $\underbrace{\beta \circ \alpha \circ \beta^{-1}}_{=\tau} = \begin{cases} 1 \mapsto 1 \\ 2 \mapsto 3 \\ 3 \mapsto 2 \end{cases}$

$\beta^{-1} = \beta \Rightarrow \beta H \beta^{-1} = \{id_X, \tau\} \neq H.$

$\Rightarrow H \not\trianglelefteq \mathrm{Sym}(\{1,2,3\})$

18. Def Sei $(G,\cdot)$ eine Gruppe und seien $X, Y, Z \subseteq G$ Teilmengen. Wir definieren

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

$$X \cdot Y = \{ x \cdot y \mid x \in X,\ y \in Y \}$$

Es gilt dann $(X \cdot Y) \cdot Z = X \cdot (Y \cdot Z)$.

Satz Ist $G$ eine Gruppe, $N \trianglelefteq G$ ein Normalteiler, so ist die Menge der (Links-)Nebenklassen $G/N$ eine Gruppe mit der Verknüpfung

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

Inverses $(gN)^{-1} = Ng^{-1} = g^{-1}N$

und Neutralelement $N$

Beweis $N$ ist Normalteiler, also gilt $aN = Na$ für alle $a \in G$. Es folgt $gNhN = ghN$,

$gN \cdot N = gN$ (wegen $N \cdot N = N$)

$(gN)^{-1} = Ng^{-1} = g^{-1}N$. □

**Beispiel** Sei $m \in \mathbb{N}$, $m \geq 1$. Dann ist

$m\mathbb{Z} \subseteq \mathbb{Z}$ Untergruppe vom Index $m = [\mathbb{Z} : m\mathbb{Z}]$,

denn $\mathbb{Z} = m\mathbb{Z} \cup (1 + m\mathbb{Z}) \cup (2 + m\mathbb{Z}) \cup \ldots \cup (m-1 + m\mathbb{Z})$

wobei $k + m\mathbb{Z} = \{ k + ml \mid l \in \mathbb{Z} \}$.

Zum Beispiel $m = 2$: $\mathbb{Z} = 2\mathbb{Z} \cup (1 + 2\mathbb{Z})$

($2\mathbb{Z}$: gerade Zahlen; $1 + 2\mathbb{Z}$: ungerade Zahlen.)

Also ist $\mathbb{Z}/m\mathbb{Z}$ eine Gruppe der Ordnung $m$. ⊛

Diese Gruppe ist zyklisch, denn $a = 1 + m\mathbb{Z}$ ist

ein Erzeuger, $\mathbb{Z}/m\mathbb{Z} = (1 + m\mathbb{Z}) \cup (2 + m\mathbb{Z}) \cup \ldots \cup (m-1 + m\mathbb{Z})$

$$k + m\mathbb{Z} = \underbrace{(1 + m\mathbb{Z}) + \ldots + (1 + m\mathbb{Z})}_{k\text{-mal}}.$$

Normalteiler werden durch Homomorphismen bestimmt.

**19. Def** Seien $G, K$ Gruppen. Ein **Homomorphismus** (genauer: Gruppenhomomorphismus) ist eine Abbildung $\varphi : G \to K$ mit der Eigenschaft

$$\varphi(u \cdot v) = \varphi(u) \cdot \varphi(v)$$

($u \cdot v$: Verknüpfung in $G$; $\varphi(u) \cdot \varphi(v)$: Verknüpfung in $K$)

---

⊛ Ist $0 \leq r < s < m$, so ist $r + m\mathbb{Z} \neq s + m\mathbb{Z}$, sonst wäre $s - r$ ein Vielfaches von $m$ ↯

**Lemma** Sei $\varphi: G \to K$ ein Gruppenhomomorphismus. Seien $e_G \in G$ und $e_K \in K$ die Neutralelemente, sei $a \in G$. Dann gilt: (i) $\varphi(e_G) = e_K$

(ii) $\varphi(a^{-1}) = \varphi(a)^{-1}$

↑ Inverses von $\varphi(a)$, nicht Umkehrabbildg!

Beis. $\varphi(e_G) = \varphi(e_G \cdot e_G) = \varphi(e_G) \cdot \varphi(e_G) \Rightarrow \varphi(e_G) = e_K$

$\| \quad e_K \cdot \varphi(e_G)$

$\varphi(a a^{-1}) = \varphi(a) \cdot \varphi(a^{-1}) \Rightarrow \varphi(a^{-1}) = \varphi(a)^{-1}$

$\|$

$\varphi(e_G) = e_K$

□

20. **Satz** Sei $\varphi: G \to K$ ein Gruppenhomomorphismus. Dann ist das Bild $\varphi(G) = \{\varphi(g) \mid g \in G\} \subseteq K$ eine Untergruppe von $K$ und der Kern $\ker(\varphi) = \{g \in G \mid \varphi(g) = e_K\} \subseteq G$ ist ein Normalteiler in $G$.

Beis. Sei $u, v \in G$. Dann ist $\varphi(u)^{-1}\varphi(v)$

$= \varphi(u^{-1})\varphi(v) = \varphi(u^{-1}v) \in \varphi(G)$ und $\varphi(G) \neq \emptyset$

(weil $\varphi(e_G) = e_K \in \varphi(G)$), also ist $\varphi(G) \subseteq K$ eine Untergruppe.

Ist $u, v \in \ker(\varphi)$, $a \in G$, so folgt

$\varphi(u^{-1}v) = \underbrace{\varphi(u)^{-1}}_{=e_K} \cdot \underbrace{\varphi(v)}_{=e_K} = e_K$ und $e_G \in \ker(\varphi)$,

also ist $\ker(\varphi) \subseteq G$ eine Untergruppe.

Weiter gilt $\varphi(aua^{-1}) = \varphi(a) \underbrace{\varphi(u)}_{=e_K} \varphi(a)^{-1} = e_K$

$\Rightarrow aua^{-1} \in \ker\varphi$, damit $a \ker(\varphi) a^{-1} \subseteq \ker(\varphi)$

$\Rightarrow \ker(\varphi) \trianglelefteq G$. □ #

21. Konstruktion Sei $G$ eine Gruppe, sei $N \trianglelefteq G$ ein Normalteiler. Wir definieren $p_N : G \to G/N$ durch $p_N(g) = gN$. Das ist ein Homomorphismus mit $\ker(p_N) = N$, denn:

$p_N(gh) = ghN = gN \cdot hN = p_N(g) \cdot p_N(h)$.

$p_N(g) = N \Leftrightarrow gN = N \Leftrightarrow g \in N$,

(denn: $g \in N \Rightarrow gN = N$ und $gN = N \Rightarrow g = g \cdot e \in N$.)

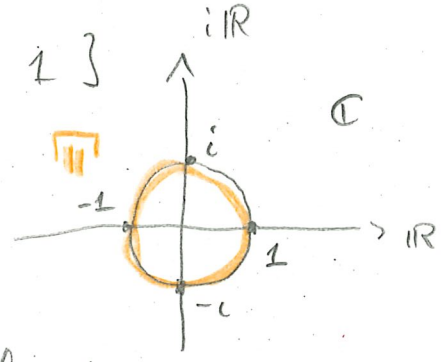
vgl. §1.15 Lemma A

Fazit $N \subseteq G$ ist genau dann ein Normalteiler in $G$, wenn es einen Homomorphismus $\varphi$ gibt mit $N = \ker(\varphi)$.

Denn: Wenn $N \trianglelefteq G$, so ist $N = \ker(\varphi_N)$

Ist $N = \ker(\varphi)$, so ist $N \trianglelefteq G$ nach §1.20. □

22. Beispiel (a) Sei $\Pi = \{ z \in \mathbb{C} \mid |z| = 1 \}$ $\quad i = \sqrt{-1}$




Für $u, v \in \Pi$ gilt $|uv| = |u| \cdot |v| = 1$

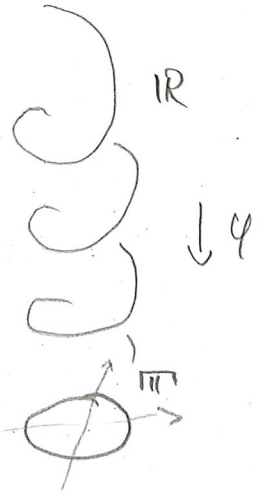
$|u^{-1}| = |\bar{u}| = 1$ und $1 \in \Pi$

$\Rightarrow (\Pi, \cdot)$ ist eine abelsche Gruppe, die Kreisgruppe oder der 1-Torus.

Wir haben einen Homomorphismus $\varphi: \mathbb{R} \to \Pi$

via $t \longmapsto \exp(2\pi i t) = \cos(2\pi t) + i \cdot \sin(2\pi t)$

$\exp(2\pi i t) = 1 \iff t \in \mathbb{Z}$, also $\ker(\varphi) = \mathbb{Z} \subseteq \mathbb{R}$.




(b) Sei jetzt $m \in \mathbb{N}$, $m \geq 1$. Wir setzen

$\xi_m = \exp\left(\frac{2\pi i}{m}\right) \in \Pi$ m-te primitive Einheitswurzel.

$m = 1 \rightsquigarrow \xi_m = 1$

$m = 2 \rightsquigarrow \xi_m = -1$

$m = 4 \rightsquigarrow \xi_m = i = \sqrt{-1}$

Es gilt $(\xi_m)^k = \exp\left(\frac{2\pi i}{m} \cdot k\right)$ $\quad$ (weil $\exp(a)\exp(b) = \exp(a+b)$)

**Lemma** Die zyklische Gruppe $\langle \xi_m \rangle \subseteq \Pi$ hat

Ordnung $m$ und die Abbildung $\varphi_m: \mathbb{Z} \longrightarrow \Pi$

$k \longmapsto (\xi_m)^k$ hat $\ker(\varphi_m) = m\mathbb{Z} \subseteq \mathbb{Z}$

Beweis: Es gilt $\xi_m^k = \xi_m^l \Leftrightarrow (\xi_m)^{k-l} = 1$

$\Leftrightarrow \exp\left(\frac{2\pi i}{m}(k-l)\right) = 1 \Leftrightarrow \frac{k-l}{m}$ ganzzahlig

$\Rightarrow \langle \xi_m \rangle = \underbrace{\{\xi_m, \xi_m^2, \dots, \xi_m^{m-1}, \xi_m^m = 1\}}_{m \text{ Elemente}}$

Weiter ist $\varphi_m : k \mapsto (\xi_m)^k$ ein Homomorphismus, und

$\ker(\varphi_m) = \{k \in \mathbb{Z} \mid \frac{k}{m} \text{ ganzzahlig}\} = m\mathbb{Z}$. □

Wir hatten in §1.18 das Beispiel $\mathbb{Z}/m\mathbb{Z}$ betrachtet.
Was ist der Zusammenhang zu $\langle \xi_m \rangle \subseteq \mathbb{T}$?

23. Lemma: Ein Homomorphismus $\varphi: G \to K$ ist genau dann injektiv, wenn gilt $\ker(\varphi) = \{e_G\}$.

Beweis: $\varphi$ injektiv $\Rightarrow \varphi^{-1}(\varphi(e_G)) = \ker(\varphi) = \{e_G\}$.

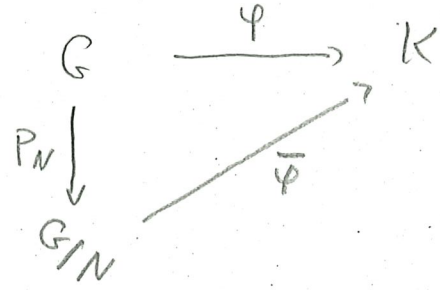
Angenommen, $\ker(\varphi) = \{e_G\}$ und $\varphi(a) = \varphi(b)$. Dann gilt
$\varphi(ab^{-1}) = e_K \rightsquigarrow ab^{-1} = e_G \rightsquigarrow a = b \rightsquigarrow \varphi$ injektiv. □

24. Theorem (Der Homomorphisatz)

Es sei $\varphi: G \to K$ ein Homomorphismus von Gruppen und es sei $N \trianglelefteq G$ ein Normalteiler mit $N \subseteq \ker(\varphi)$ (zum Beispiel $N = \ker(\varphi)$).
Dann gibt es genau einen Homomorphismus

$$\overline{\varphi}: G/N \to K \quad \text{mit} \quad \overline{\varphi} \circ p_N = \varphi$$

d.h. mit einem kommutativen Diagram




Beweis Existenz von $\bar{\varphi}$. Für $g \in G$ setze

$\bar{\varphi}(gN) = \varphi(g)$. Diese Abbildung ist wohldefiniert, d.h. sie hängt nicht von der speziellen Wahl von g ab.

Denn: wenn $gN = \tilde{g}N$ für $g, \tilde{g} \in G$, dann $\tilde{g} = g \cdot n$ für ein $n \in N$ (vgl. §1.15 Lemma A)

$\Rightarrow \varphi(\tilde{g}) = \varphi(g \cdot n) = \varphi(g) \cdot \underbrace{\varphi(n)}_{= e_K}$, weil $n \in \ker(\varphi)$.

Für $a, b \in G$ folgt $\bar{\varphi}(abN) = \varphi(ab) = \varphi(a)\varphi(b)$

$= \bar{\varphi}(aN) \cdot \bar{\varphi}(bN) \Rightarrow \bar{\varphi}$ ist ein Homomorphismus. □

Eindeutigkeit von $\bar{\varphi}$. Angenommen, $\psi: G/N \to K$ ist ein weiterer Homomorphismus mit $\psi \circ P_N = \varphi$.

Es folgt $\psi(gN) = \psi \circ P_N(g) = \varphi(g) \Rightarrow \psi = \bar{\varphi}$. □ #

Bemerkung Nach Konstruktion gilt $\varphi(G) = \bar{\varphi}(G/N)$, d.h. Homomorphismen haben dasselbe Bild in K.

25. Def Ein Gruppenhomomorphismus $\varphi: G \to K$ heißt Isomorphismus, wenn es einen Homomorphismus $\psi: K \to G$ gibt mit $\psi \circ \varphi = id_G$ und $\varphi \circ \psi = id_K$.

Satz Ein Homomorphismus ($\varphi: G \to K$) ist genau dann ein Isomorphismus, wenn $\varphi$ bijektiv ist

Beis: $\varphi$ Isomorphismus $\overset{\text{Def}}{\Rightarrow}$ $\varphi$ injektiv ($\psi \circ \varphi = id_G$) und surjektiv ($\varphi \circ \psi = id_K$) $\Rightarrow$ $\varphi$ bijektiv. □

Angenommen, $\varphi$ ist ein bijektiver Homomorphismus, mit Umkehrabbildung $\psi: K \to G$ (also $\psi \circ \varphi = id_G$ und $\varphi \circ \psi = id_K$). Beh: $\psi$ ist ein Homomorphismus.

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

$$\varphi(\psi(a)\psi(b)) = \varphi(\psi(a)) \cdot \varphi(\psi(b)) = ab$$

D. $\varphi$ injektiv ist, folgt $\psi(ab) = \psi(a)\psi(b)$ □

Folgerung Ein Homomorphismus $\varphi: G \to K$ ist genau dann ein Isomorphismus, wenn $\ker(\varphi) = \{e_G\}$ und $\varphi(G) = K$ gilt.

Dann schreibt man $G \xrightarrow{\cong} K$, $G \cong K$

Isomorphiesymbol "$\cong$"

26. **Korollar** (zum Homomorphiesatz)

Sei $\varphi: G \to K$ ein Homomorphismus mit $N = \ker(\varphi)$.
Dann ist $\bar{\varphi}: G/N \to K$ ein injektiver Homomorphismus.
Falls $\varphi$ surjektiv ist, so ist $\bar{\varphi}: G/N \to K$ sogar ein Isomorphismus.

**Beweis** $\bar{\varphi}(gN) = \varphi(g) = e_K \Leftrightarrow gN = N \Leftrightarrow g \in N$

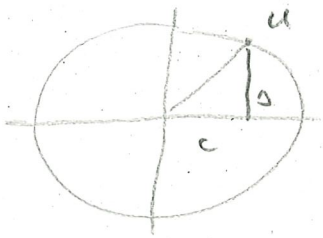
also ist $\ker(\bar{\varphi}) = \{N\}$. Nach §1.23 ist $\bar{\varphi}$ also injektiv. Wenn $\varphi(G) = \bar{\varphi}(G/N) = K$, dann ist $\bar{\varphi}$ surjektiv, also nach §1.25 ein Isomorphismus. □

Damit zurück zu dem Beispiel in §1.22

(a) $\varphi: \mathbb{R} \to \mathbb{T}$, $t \mapsto \exp(2\pi i t)$

$\varphi$ ist surjektiv ( $u \in \mathbb{T} \Rightarrow u = c + i\cdot s$ mit $c, s \in \mathbb{R}$,

$c^2 + s^2 = 1$




Analysis I

$\Rightarrow$ es gibt $t \in \mathbb{R}$ mit $\cos(t) = c$, $\sin(t) = s$ $\Rightarrow \exp(2\pi i t) = u$

$\ker(\varphi) = \mathbb{Z} \subseteq \mathbb{R}$. Also haben wir ein

Isomorphismus $\mathbb{R}/\mathbb{Z} \cong \mathbb{T}$ mit $\bar{\varphi}(t+\mathbb{Z}) = \exp(2\pi i t)$

$t + \mathbb{Z} \in \mathbb{R}/\mathbb{Z}$ Nebenklasse

(b) $\varphi_m : \mathbb{Z} \to \langle \xi_m \rangle$ $\qquad \xi_m = \exp\left(\frac{2\pi i}{m}\right) \in \mathbb{T}$

$k \mapsto (\xi_m)^k$ $\qquad m \in \mathbb{N}, m \geq 1$

$\ker(\varphi_m) = m\mathbb{Z}$, also hat wir ein Isomorphism

$$\mathbb{Z}/m\mathbb{Z} \xrightarrow[\cong]{\overline{\varphi_m}} \langle \xi_m \rangle, \quad k + m\mathbb{Z} \mapsto (\xi_m)^k .$$

Das sehr etwas allgemeiner.

27. Satz Sei $G = \langle a \rangle$ eine zyklische Gruppe der Ordnung $m$. Dann ist $G \cong \mathbb{Z}$ falls $m = \infty$ und $G \cong \mathbb{Z}/m\mathbb{Z}$ falls $1 \leq m < \infty$.

Beweis: Betrachte den Homomorphismus $\varphi : \mathbb{Z} \to G$, $\varphi(k) = a^k$. Das ist ein Homomorphismus, denn $\varphi(k+l) = a^{k+l} = a^k \cdot a^l = \varphi(k) \cdot \varphi(l)$.
Weiter ist $\varphi$ surjektiv, weil $\langle a \rangle = \{ a^k \mid k \in \mathbb{Z} \}$, vgl §1.9. Wenn $\varphi$ injektiv ist, so ist $\varphi$ ein Isomorphismus (nach §1.25) $\Rightarrow \langle a \rangle \cong \mathbb{Z}$, $m = \infty$. □

Wenn $\varphi$ nicht injektiv ist, so gibt es $k \neq 0$ mit $a^k = e \Rightarrow \underbrace{|\langle a \rangle|}_{= m < \infty} = o(a)$ und §1.13

$k = l \cdot m + r \quad 0 \leq r < m$ (Teil mit Rest)

$\Rightarrow a^r = e \Rightarrow r = 0 \Rightarrow k \in m\mathbb{Z}$

$\Rightarrow \ker(\varphi) = m\mathbb{Z}$ und damit $\langle a \rangle \cong \mathbb{Z}/m\mathbb{Z}$. □

**Fazit** Zyklische Gruppen, die die gleiche Ordnung haben, sind isomorph. Daher spricht man von "der" zyklischen Gruppe der Ordnung $n$, wenn man z.B. $\mathbb{Z}/n\mathbb{Z}$ meint.

## 28. Produkt von Gruppen

Seien $G, K$ Gruppen. Auf der Menge $G \times K$ definieren wir eine Verknüpfung durch

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

Dann ist $G \times K$ eine Gruppe, mit Neutralelement $(e_G, e_K) \in G \times K$. Das Inverse von $(g,k) \in G \times K$ ist $(g,k)^{-1} = (g^{-1}, k^{-1})$.

**Denn:** Die Verknüpfung ist assoziativ,

$$((g_1,k_1)(g_2,h_2))(g_3,h_3) = (g_1 g_2 g_3, k_1 k_2 k_3)$$

$$= (g_1,k_1)((g_2,k_2)(g_3,h_3)) \quad \text{usw.}$$

**Bem** Wenn $G$ und $K$ abelsch sind, so auch $G \times K$ (und umgekehrt)

Wir haben Homomorphismen $pr_1 : G \times K \to G$
$(g,k) \mapsto g$

$pr_2 : G \times K \to K$
$(g,k) \mapsto k$

Produkte sind nicht immer offensichtlich!

Bsp $\varphi: \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ Homomorphismus

$k \mapsto (k+2\mathbb{Z}, k+3\mathbb{Z})$

$\ker(\varphi) = 2\mathbb{Z} \cap 3\mathbb{Z} = 6\mathbb{Z}$ $\Rightarrow$ injektiver Homomorphismus

$\bar{\varphi}: \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$

Also ist $\bar{\varphi}$ bijektiv und damit ein Isomorphismus!

Ganz ähnlich zeigt man allgemein: wenn $m, n \geq 1$ teilerfremde ganze Zahlen sind ($ggT(m,n)=1$), so erhält man einen Isomorphismus $\bar{\varphi}: \mathbb{Z}/m\cdot n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. → ÜA #

## 2.9. Allgemeines Produkt von Gruppen

Sei $J$ eine Indexmenge, z.B. $J = \{1, 2, 3, \ldots, n\}$ (oder auch unendliche Menge). Für jedes $j \in J$ sei $G_j$ eine Gruppe. Dann ist das Produkt

$\prod_{j \in J} G_j = G$ eine Gruppe. Erinnerung: die Elemente von $G$ sind Folgen oder Tupel $(g_j)_{j \in J}$ mit $g_j \in G_j$. Wir verknüpfen solche Tupel

koordinatenweise, also $(a_j)_{j\in J} \cdot (b_j)_{j\in J} = (a_j \cdot b_j)_{j\in J}$.

Das Inverse von $(a_j)_{j\in J}$ ist $(a_j^{-1})_{j\in J}$, das Neutralelement ist $(e_j)_{j\in J}$, $e_j \in G_j$ Neutralelement.

Bsp $(\mathbb{R}, +)$ ist Gruppe $\Rightarrow (\mathbb{R}^n, +)$ ist Gruppe (sogar Vektorraum) mit koordinatenweiser Addition,

$(a_1, \dots, a_n) + (b_1, \dots, b_n) = (a_1 + b_1, \dots, a_n + b_n)$.