Def (2.2.2): Eine **Gruppe** ist eine Menge G zusammen mit einer Verknüpfung

$$* : G \times G \longrightarrow G,$$

die folgende Bedingungen erfüllt:

(Assoziativität) $\forall a, b, c \in G$:

$$(a * b) * c = a * (b * c)$$

$\exists e \in G$: (eindeutig)

(neutrales Element) $\forall a \in G$:

$$e * a = a \qquad a * e = a$$

\+ (Inverse) $\forall \in G$: $\exists a^{-1} \in G$:

$$a^{-1} * a = e. \qquad a * a^{-1} = e$$

Def (2.2.4): $(G, *)$ Gruppe, $a \in G$.

Rechtstranslation τ_a:

$$\begin{aligned} G &\longrightarrow G \\ g &\longmapsto g * a \end{aligned}$$

Linkstranslation ${}_a\tau$:

$$\begin{aligned} G &\longrightarrow G \\ g &\longmapsto a * g \end{aligned}$$

Satz (2.2.4):

1. Für jede Gruppe $(G, *)$ und jedes $a \in G$ sind τ_a und ${}_a\tau$ bijektiv.

② Ist $G \neq \emptyset$ eine Menge mit einer assoziativen Verknüpfung $*$, und sind für jedes $a \in G$ die wie oben definierten $\overbrace{\text{Abbildungen}}^{\tau_a \text{ und } {}_a\tau}$ surjektiv, so ist $(G, *)$ eine Gruppe.

Def (2.2.6): $(G, *)$ Gruppe

Eine **Untergruppe** ist eine nicht-leere Teilmenge $H \subset G$, für die gilt:

$$\forall a, b \in H : \quad a * b \in H$$
$$\text{und} \quad a^{-1} \in H$$

Notiz: In diesem Fall definiert $*$ eine Verknüpfung auf H, die induzierte Verknüpfung und $(H, *)$ ist eine Gruppe.

Def (2.2.6): Ein **Homomorphismus** von Gruppen $f:(G,*) \longrightarrow (H,\circ)$ ist eine Abbildung $f: G \to H$, mit der Eigenschaft:

$$\forall a,b \in G \qquad f(a*b) = f(a)\circ f(b)$$

Ein **Isomorphismus** von Gruppen ist ein bijektiver Homomorphismus.

Notiz: Für eine Homomorphismus $f:(G,*) \longrightarrow (H,\circ)$ gilt

$$f(e_G) = e_H \quad \text{und} \quad f(a^{-1}) = f(a)^{-1} \quad \forall a \in G$$

in G

in H

Notiz: Für jeden Isomorphismus

$$f: (G, *) \longrightarrow (H, \odot)$$

ist auch die Umkehrabb.

$$(G, *) \longleftarrow (H, \odot) : f^{-1}$$

ein Isomorphismus.

Satz (2.2.7): Division mit Rest

$\forall n, m \in \mathbb{Z}$ mit $m \geq 1$

$\exists q, r \in \mathbb{Z}$ mit $\underline{0 \leq r < m}$

derart, dass

$$\underset{\text{Quotient}}{q} \cdot m + \underset{\text{Rest}}{r}$$

$$n = q \cdot m + r$$

Quotient Rest

bei Division von n durch m

Ferner sind q & r eindeutig bestimmt.

Offenbar: $m \mid n \iff r = 0$

Notiz (2.2.8) Für festes $m \in \mathbb{Z}$, $m \geq 1$, definiert

$$x \sim_m y \quad :\iff \quad m \mid (x - y)$$

eine Äquivalenzrelation auf $\mathbb{Z}$.

Für die Äquivalenklassen gilt in obiger Notation

$$[n] = [r] \qquad (0 \leq r < m)$$

<u>Notation</u> $\mathbb{Z}/m\mathbb{Z} := \mathbb{Z}/_{\sim_m}$

<u>Lemma (2.2.8)</u> Für $m \in \mathbb{Z}$, $m \geq 1$ ist

$$\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \xrightarrow{\oplus} \mathbb{Z}/m\mathbb{Z}$$

$$([x], [y]) \longmapsto [x+y]$$

eine wohldefinierte Verknüpfung.

<u>Satz (2.2.8)</u> $(\mathbb{Z}/m\mathbb{Z}, \oplus)$ ist eine abelsche Gruppe und die Quotientenabb.

$$(\mathbb{Z}, +) \longrightarrow (\mathbb{Z}/m\mathbb{Z}, \oplus)$$

ist ein Homomorphismus.