

... les abus de langage, sans lesquels tout texte mathématique risquerait de devenir pédantesque et même illisible, ...

N. Bourbaki, *Théorie des ensembles*
 Mode d'emploi de ce traité, p.III

einige endliche Gruppen finite groups

$$(\{0\}, +), (\{1\}, \cdot), (\{1, -1\}, \cdot)$$

(additive) Restklassengruppe $(\mathbb{Z}_m, +)$ residue classes

prime Restklassengruppe (\mathbb{Z}_m^*, \cdot) reduced residue classes

symmetrische Gruppe (S_m, \circ) Permutationen (m Dinge)

Untergruppe (einer Gruppe (G, \circ)) subgroup

$\emptyset \neq H \subset G$ ist Untergruppe von G ($H < G$)

: $\Leftrightarrow (H, \circ)$ ist Gruppe

genauer: $(H, \circ|_H)$ Einschränkung $\circ|_H$ von \circ auf H

auch $H < G \Leftrightarrow (a, b \in H \Rightarrow a \circ b, a^{-1} \in H)$ ($\Rightarrow e \in H$)

oder $\emptyset \neq H < G \Leftrightarrow H \circ H^{-1} \subset H$

G endlich: $\emptyset \neq H < G \Leftrightarrow H \circ H \subset H$

Komplex-Multiplikation ($g \in G, A, B \subset G$)

$$A \circ B := \{g \mid g = a \circ b, a \in A, b \in B\}$$

$$a \circ B := \{a\} \circ B = \{g \mid g = a \circ b, b \in B\}$$

\Rightarrow Monoid $(\mathcal{P}(G), \circ)$

(Links-)Nebenklasse $C(a) := a \circ H$ (modulo H)

Faktormenge $G/H := \{a \circ H \mid a \in G\}$

Kongruenz $C(a) \circ C(b) = C(ab)$ (verträglich)

$\Leftrightarrow (aH)(bH) = (ab)H \Leftrightarrow aH = Ha \Leftrightarrow aHa^{-1} = H \Leftrightarrow$

H **Normalteiler** in G ($H \triangleleft G$) : \Leftrightarrow normal subgroup

$(\forall g \in G) gH = Hg \Leftrightarrow (\forall g \in G) gHg^{-1} = H$ (d.h.)

Links- und Rechtsnebenklassen gleich $\Leftrightarrow G/H$ **Faktorgruppe**

$\Leftrightarrow H$ invariant (unter Konjugation gHg^{-1})

Beispiel: $(\mathbb{Z}, +)/(m\mathbb{Z}, +) = \mathbb{Z}/m\mathbb{Z} = (\mathbb{Z}_m, +)$