# Algebra

**[Relation]** Sei ~ eine Relation auf $M$ und für alle $x, y, z \in M$ gilt

(reflexiv) $x \sim x$

(symmetrisch) $x \sim y \Rightarrow y \sim x$

(transitiv) $x \sim y \wedge y \sim z \Rightarrow x \sim z$ <u>Äquivalenzrelation</u>

Ist $(M, \cdot)$ ein Gruppoid dann gibt

(kongruenz) $x \sim x' \wedge y \sim y' \Rightarrow x \cdot x' \sim y \cdot y'$ <u>Kongruenzrelation</u>

**[Eulersche $\varphi$ Funktion]** Für $n \in \mathbb{N}$ ist $\varphi(n)$ die Anzahl der mit $n$ teilerfremden Zahlen, die kleiner als $n$ sind.

$$\varphi(n) = \left|\mathbb{Z}_n^\times\right| \qquad p,q \text{ prim} \wedge \mathrm{p} \neq \mathrm{q} \Rightarrow \quad \varphi(p) = p-1 \quad \varphi(p^k) = p^{k-1}(p-1) \quad \varphi(pq) = \varphi(p)\varphi(q)`$$

**[Euler - Fermat]** Für teilerfremde $a, n \in \mathbb{N}$ gilt: $a^{\varphi(n)} \equiv_n 1$ …daraus folgt: $p \text{ prim} \Rightarrow a^p \equiv_p a$

**[Lagrange]** $H$ Untergruppe von $G \Rightarrow |G| = |H| \cdot (G:H)$ $\quad |H|$ teilt $|G|$ $\quad (G:H)$ teilt $|G|$

**[Sylow]** Sei $G$ eine endliche Gruppe und $p$ eine Primzahl dann gilt:

(1) $(\forall n \in \mathbb{N})\, p^n$ teilt $G \Rightarrow (\exists U \text{ Untergruppe von } G)\, |U| = p^n$

(2) Ist $a$ die Anzahl der Untergruppen $U_i$ mit Ordnung $p^n$ so gilt: $a \equiv_p 1$

**[Normal]** Ist $N$ Untergruppe von $G$ dann $\quad N \text{ normal} \Leftrightarrow (\forall g \in G)\, gNg^{-1} \subseteq N$

**[Homomorphiesatz]** Sei G eine Gruppe dann gilt für jeden Homomorphismus $\varphi : G \to \mathrm{im}(\varphi)$

$\bar{\varphi} : G/\ker\varphi \to \mathrm{im}\varphi : \bar{x} \mapsto \varphi(x)$ ist ein Isomorphismus

$|G| = |\ker\varphi| \cdot |\mathrm{im}\varphi| \quad \wedge \quad |\mathrm{im}\varphi| = (G : \ker\varphi)$

**[Permutationsgruppen]** Sei $X$ eine endliche Menge und $G$ eine Gruppe dann ist $\mathcal{S}_X$ die Gruppe aller Perm. auf $X$

$$G \text{ operiert auf } X \quad \Leftrightarrow (\exists \varphi : G \to \mathcal{S}_X : g \mapsto \sigma_g)\, \varphi \text{ homomorphismus} \quad \Leftrightarrow (\forall g, h \in G)\, \sigma_g \circ \sigma_h = \sigma_{gh}$$

**[Standgruppe, Bahn, Bahngleichung]** Sei $G$ eine Gruppe die auf $X$ operiert, dann ist für ein festes $x \in X$

$G_x := \{g \in G : \sigma_g(x) = x\}$ Standgruppe von $x$. Die $g \in G$ deren Perm. $x$ nicht verändern.

$B_x := \{\sigma_g(x) : g \in G\}$ Bahn von $x$. Alle Elemente, die man durch Perm. aus $x$ machen kann.

$|G| = |G_x| \cdot |B_x|$ $\quad |G_x|$ teilt $|G|$ $\quad |B_x|$ teilt $|G|$

**[Burnside Lemma]** $G$ operiere auf $X$. Für jedes $g \in G$ seien $\mathrm{Fix}(g) := \{x \in X : \sigma_g(x) = x\}$ Fixpunkte von $\sigma_g$

$\frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}(g)| = k$ wobei $k$ die Anzahl der verschiedenen Bahnen ist.

**[Integritätsbereich]** $R$ nullteilerfreier kommutativer Ring $\Leftrightarrow$ $R$ Integritätsbereich

**[Teilbarkeit]** Sei $R$ ein Integritätsbereich dann gilt $\forall a, b, c, d \in R$:

(i) $a \mid a$

(ii) $a \mid b \wedge b \mid a \Leftrightarrow \exists x \in R^\times : a = xb$

(iii) $a \mid b \wedge b \mid c \Rightarrow a \mid c$

(iv) $a \mid b \wedge c \mid d \Rightarrow ac \mid bd$

(v) $a \mid b \wedge a \mid c \Rightarrow a \mid b \pm c$

**[Ideal]** $I \subseteq R \text{ Ideal} \quad \Leftrightarrow \quad 0 \in I \quad \wedge \quad a, b \in I \Rightarrow a + b \in I \quad \wedge \quad a \in I, x \in R \Rightarrow ax \in I, xa \in I$

**[Irreduzibel]** $p \neq 0 \text{ irreduzibel} \Leftrightarrow \forall a, b \in R : p = a \cdot b \Rightarrow a \in R^\times \vee b \in R^\times$

**[Hauptideal]** $I \subseteq R \text{ Hauptideal} \quad \Leftrightarrow \quad I \text{ Ideal} \quad \wedge \quad \exists x \in R : I = xR$

es gilt: $a, b \text{ teilerfremd} \wedge a \mid b \cdot c \Rightarrow a \mid c$

$\forall p \text{ irreduzibel} : p \mid a \cdot b \Rightarrow p \mid a \vee p \mid b$

**[ggT]** $ggT(a,b) = d \quad \Leftrightarrow \quad d \mid a \wedge d \mid b \quad \wedge \quad \forall c \in R : c \mid a \wedge c \mid b \Rightarrow c \mid d$