Sätze von Lagrange und Euler

Satz von Lagrange:

G sei eine endliche Gruppe, $U \leq G$

Dann:

$$|U| \Big| |G|$$

Satz von Euler:

$$a^{|G|} = e \quad \forall a \in G$$

Die Restklassen modulo n:

Gegeben: $n \in \mathbb{N}$

Betrachte: wähle $a \in \mathbb{Z}$

$$\overline{a} = \{a + nz \,|\, z \in \mathbb{Z}\}$$

Wir schließen $a, b \in \mathbb{Z}$:

$a \equiv b(mod \;\; n)$, falls a, b den gleichen Rest bei Div durch n haben:

Es gilt:

$$\left.\begin{array}{l} a = qn + r \\ b = \tilde{q}n + r \end{array}\right\} \Leftrightarrow \left\{\begin{array}{ll} a - b & = (q - \tilde{q})n \\ & \Leftrightarrow n|(a-b) \\ & \Leftrightarrow a + n\mathbb{Z} = b + n\mathbb{Z} \\ & \Leftrightarrow \overline{a} = \overline{b} \end{array}\right.$$

Menge der Restklassen $\rightarrow \mathbb{Z}\Big|n\mathbb{Z} = \mathbb{Z}\Big|n = \mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$

$|\mathbb{Z}_n| = n$

Addition:

$\overline{k}, \overline{l} \in \mathbb{Z}$

$\rightarrow \overline{k} = \overline{l} = \overline{k+l}$

Ringe

Eine Menge R mit zwei Verknüpfungen $+$ und $\cdot$ heißt ein Ring falls gilt:

- $(R, +)$ ist abelsche Gruppe
- $\cdot$ ist assoziativ
- Distributivgesätze $a(b + c) = ab + ac$ und $(a + b)c = ac + bc \forall a, b, c \in R$
- $\exists$ Einselement: $1 \in R$: $1 \cdot a = a = a \cdot 1 \quad \forall a \in R$

Einheitengruppe (= Gruppe der invertierbaren Elemente)

Gegeben: Ring $(R, +, \cdot)$

$R^{\times} = \{a \in R \,|\, a \text{ ist invertierbar}\} = \{a \in R \,|\, \exists b \in R : ab = 1 = ba\}$

$R^{\times}$ ist die Einheitengruppe von R