Relationen

Äquivalenzrelationen, modulares Rechnen

- Definition

  Eine Relation $R \subseteq M^2$ heißt ***Äquivalenzrelation***, wenn sie reflexiv, symmetrisch und transitiv ist.

- Anmerkung: Bei Äquivalenzrelationen verwendet man statt $a\ R\ b$ üblicherweise die Schreibweise $a \sim b$.

- Beispiele

- Definition

  Es sei R eine Äquivalenzrelation auf der Menge M. Zu jedem $a \in M$ bezeichne $[a]$ die Menge aller Elemente von M, zu denen a in Relation steht, also

  $$[a] = \{x \in M \mid a \sim x\}.$$

  Die Menge $[a]$ heißt ***Äquivalenzklasse*** von a bezüglich R. Das Element a heißt ein Repräsentant von $[a]$.

- Beispiele

- Definition

  Es sei M eine Menge. Die Teilmengen $M_1, \ldots, M_k$ bilden eine ***Zerlegung*** (***Partition***) von M, wenn gilt:

  1. $M_i \cap M_j = \emptyset$ für $i \neq j$ (paarweise disjunkte Mengen),
  2. $\bigcup_{i=1}^{k} M_i = M$ (Vereinigung ist gleich M).

- Anmerkung: Entsprechend bei unendlich vielen Teilmengen. Die Vereinigung muß dann über alle unendlich vielen Mengen gebildet werden.

- Skizze und Beispiele.

- Satz

  Die Äquivalenzklassen einer Äquivalenzrelation auf der Menge M bilden eine Zerlegung von M. D.h. die Vereinigung der Äquivalenzklassen ist gleich M, und für alle $a, b \in M$ gilt entweder $[a] = [b]$ oder $[a] \cap [b] = \emptyset$.

- Beweis
- Beispiele
- Satz

  Gegeben sei eine Menge M sowie eine Zerlegung von M durch die Teilmengen $M_1, \ldots, M_k$. Dann wird durch die Relation $\sim$ mit

  $$a \sim b \qquad \Leftrightarrow \qquad a \text{ und } b \text{ liegen in derselben Teilmenge } M_i$$

  eine Äquivalenzrelation auf M definiert.
- Anmerkung: Entsprechend bei unendlich vielen Teilmengen.
- Einleitendes Beispiel zum modularen Rechnen.
- Sei a eine ganze Zahl, $a \in \mathbb{Z}$, und m eine positive ganze Zahl, $m \in \mathbb{N}$; dann gibt es eindeutig bestimmte ganze Zahlen q und r mit $0 \leq r < m$, so daß

  $$a = qm + r.$$
- Schreibweise für den Rest r: $\quad r = a \bmod m$.
- Definition

  Wir schreiben

  $$a \equiv b \mod m \qquad (\text{gelesen: „}a \text{ kongruent } b \text{ modulo } m\text{“}),$$

  wenn $a \bmod m = b \bmod m$, d.h. wenn a und b bei Division durch m den selben Rest lassen.
- Anmerkung: Die Schreibweise mit Klammern $a \equiv b \pmod{m}$ wird gleichwertig verwendet.
- Satz

  Es gilt

  $$a \equiv b \mod m \qquad \Leftrightarrow \qquad m \mid (a - b)$$

  sowie

  $$a \equiv b \mod m \qquad \Leftrightarrow \qquad a = b + qm \quad \text{mit } q \in \mathbb{Z}.$$
- Satz

  Die Relation $\sim$ auf $\mathbb{Z}$ mit

  $$a \sim b \qquad \text{wenn} \qquad a \equiv b \mod m$$

  ist eine Äquivalenzrelation.
- Beweis und Beispiel.