

$$\begin{aligned}
 a &\equiv b \pmod{m} \Leftrightarrow m \mid b - a \\
 [a]_m &:= \{b \in \mathbb{Z} : b \equiv a \pmod{m}\} = \{qm + a : q \in \mathbb{Z}\} = \{\dots, a - m, a, a + m, a + 2m, \dots\} \\
 [1]_3 &= \{\dots, -5, -2, 1, 4, 7, \dots\} \\
 \mathbb{Z}_m &:= \{[a]_m : a \in \mathbb{Z}\} = \{[0]_m, [1]_m, \dots, [m-1]_m\}
 \end{aligned}$$

Satz

Wenn $m \in \mathbb{P}$, dann ist \mathbb{Z}_m mit $+$ und \cdot ein Körper.

11. Algebraische Strukturen

Gruppen

Definition

Sei G eine Menge und $(a, b) \in G \times G \mapsto a \cdot b \in G$ eine Abb. mit

1. $\forall a, b, c \in G : (a \cdot b) \cdot c = a \cdot (b \cdot c)$
2. $\exists e \in G \forall a \in G : e \cdot a = a \cdot e = a$
3. $\forall a \in G \exists a^{-1} \in G : a \cdot a^{-1} = a^{-1} \cdot a = e$ Die Gruppe (G, \cdot) heißt kommutativ (oder Abel'sch), wenn gilt:
4. $\forall a, b \in G : a \cdot b = b \cdot a$

Bemerkungen

1. e ist eindeutig bestimmt: $e_1 \cdot e_2 = e_2 = e_1$
2. a^{-1} ist eindeutig bestimmt: $(a^{-1})_1 = \underbrace{e = a(a^{-1})_2}_{(a^{-1})_1 \cdot e = (a^{-1})_1 = \underbrace{(a^{-1})_1}_{e} a(a^{-1})_2 = (a^{-1})_2}$

Beispiele

1. $G := \mathbb{R} \ a \cdot b := a + b$ additive Gruppe der reellen Zahlen
 $G := \mathbb{Z} \ a \cdot b := a + b$ additive Gruppe der ganzen Zahlen
2. $G := \mathbb{R} \setminus \{0\}, a \cdot b := a \cdot b \ G := (0, \infty), a \cdot b := a \cdot b$
3. $G := \{z \in \mathbb{C} : |z| = 1\}, z_1 \cdot z_2 := z_1 \cdot z_2 \ G$ heißt S^1
4. Matrizengruppen:
 $\{A \in \mathbb{M}(n \times n, \mathbb{R}) : \det A \neq 0\}, A \cdot B := A \cdot B \ GL(n; \mathbb{R})$ lineare Gruppe
 $\{A \in \mathbb{M}(n \times n, \mathbb{R}) : A^T = A^{-1}\}, A \cdot B := A \cdot B \ O(n; \mathbb{R})$ orthogon. Gruppe
 $\{A \in O(n) : \det A = 1\}, A \cdot B := A \cdot B \ SO(n; \mathbb{R})$ spezielle orthogon. Gruppe

$A \in SO(2) \Leftrightarrow A = \begin{bmatrix} \cos \varphi & -\sin \varphi \\ \sin \varphi & \cos \varphi \end{bmatrix}$ mit einem $\varphi \in \mathbb{R} \Leftrightarrow A$ ist eine Drehung von \mathbb{R}^2 um den Nullpunkt gegen den Uhrzeigersinn

5. Transformationsgruppen: sei M Menge
 $G :=$ Menge aller bijektiven Abb. $f : M \mapsto M$
 $f \cdot g := f \circ g$ (G ist im allg. nicht kommutativ)
 $M = \{1, 2, \dots, n\} \Rightarrow G =$ Gruppe der Permutationen der Ordnung n ,
 $\text{card } G = n!$

Definition

Zwei Gruppen (G, \cdot) und (H, \cdot) heißen isomorph, wenn eine bijektive Abb. $\Phi : G \mapsto H$ ex. mit $\Phi(a \cdot b) = \Phi(a) \cdot \Phi(b) \forall a, b \in G$

Beispiel

$G = S^1, H = SO(2), \Phi : G \mapsto H : \underbrace{\Phi(e^{i\varphi})}_{\varphi \in [0, 2\pi]} = \begin{bmatrix} \cos \varphi & -\sin \varphi \\ \sin \varphi & \cos \varphi \end{bmatrix}$ Φ ist offenbar bijektiv.

Definition

$H \subseteq G$ Untergruppe, wenn H mit der Multiplikation von G eine Gruppe ist, d.h.:
 $a, b \in H \Rightarrow a \cdot b \in H, a^{-1} \in H, e \in H$

- $(G, \cdot) = (\mathbb{R}, +), H = \mathbb{Z}$
- $GL(n; \mathbb{R}) \supseteq (n; \mathbb{R}) \supseteq SO(n; \mathbb{R})$
- $S^1 \supseteq \{e^{i \frac{2\pi}{n} k} \mid k \in \mathbb{Z}\}$

Satz

$H \subseteq G$ ist Untergruppe genau dann, wenn: $\forall a, b \in H : a \cdot b^{-1} \in H$