

§ 1. Definition der Gruppen, Beispiele

Definition (1.1)

Eine **Gruppe** ist ein Paar $(G, *)$ bestehend aus einer nichtleeren Menge G und einer Verknüpfung $*$ auf G (also einer Abbildung $G \times G \rightarrow G$), so dass die folgenden Bedingungen erfüllt sind.

- (i) Die Verknüpfung ist assoziativ, d.h. es gilt $(a * b) * c = a * (b * c)$ für alle $a, b, c \in G$.
- (ii) Es gibt ein ausgezeichnetes Element $e \in G$, genannt das **Neutralelement** der Gruppe, mit der Eigenschaft, dass $e * a = a * e = a$ für alle $a \in G$ gilt.
- (iii) Für jedes Element $a \in G$ gibt es ein Element $a^{-1} \in G$, genannt das zu a **inverse Element**, mit $a * a^{-1} = a^{-1} * a = e$.

Gilt darüber hinaus $a * b = b * a$ für alle $a, b \in G$, dann spricht man von einer **abelschen** oder auch einer **kommutativen** Gruppe.

YSM 8250 EBJQ

(Moodle-Einschreibschlüssel)

Erste Beispiele für Gruppen

- (1) Ist $(R, +, \cdot)$ ein Ring, dann ist $(R, +)$ eine abelsche Gruppe (Bsp. $(\mathbb{Z}, +)$)
hierbei ist 0_R (Nullelement des Rings),
und für jedes $a \in R$ ist das Negative $-a$ das
in $(R, +)$ zu a inverse Element.

(2) Für jedes $n \in \mathbb{N}$ ist $(\mathbb{Z}/n\mathbb{Z}, +)$ eine abelsche Gruppe bestehend aus n Elementen.

$$\mathbb{Z}/n\mathbb{Z} = \{a+n\mathbb{Z} \mid a \in \mathbb{Z}\} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$$

$$\text{wobei } \bar{a} = a+n\mathbb{Z} = \{a+nk \mid k \in \mathbb{Z}\}$$

$$\text{Bsp: } \mathbb{Z}/3\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}\}, \text{ wobei } \bar{0} = \{\dots, -6, -3, 0, 3, \dots\}$$

$$\bar{1} = \{\dots, -5, -2, 1, 4, 7, \dots\}, \bar{2} = \{\dots, -4, -1, 2, 5, 8, \dots\}$$

$$(\text{beachte: } \bar{2} = \bar{5} = \bar{-1})$$

Verknüpfungstafel von $(\mathbb{Z}/3\mathbb{Z}, +)$

+	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

Regel:

Addiere je zwei Elemente
zunächst in $\mathbb{Z}$ und
bilde dann den Rest

nach Division durch 3

Bsp.: $\overline{2} + \overline{2} = \overline{4} = \overline{1}$

(3) Ist $(K, +, \cdot)$ ein Körper, dann
ist $(K^\times, \cdot)$ eine Gruppe, wobei
 $K^\times = K \setminus \{0_K\}$ genauer: eine abelsche

Gruppe (Bsp. $(\mathbb{C}^*, \cdot)$, $(\mathbb{F}_p^*, \cdot)$)
 sind abelsche Gruppen (wobei p eine Prim-
 zahl bezeichnet)

Erinnerung: $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$

Verknüpfungstafel von $(\mathbb{F}_5^*, \cdot)$

	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Bsp:

$$\overline{3} \cdot \overline{4} = \overline{12} = \overline{2}$$

(4) Ist $(V, +, \cdot)$ ein K -Vektorraum

(wobei K ein Körper ist), dann ist $(V, +)$
eine abelsche Gruppe. Neutralelement ist
der Nullvektor 0_V . Das Inverse von $v \in V$
ist jeweils $-v = (-1_K) \cdot v$. Bsp.: $(\mathbb{R}^3, +)$
ist eine abelsche Gruppe.

ann
ei
abelsche

Definition der Permutationsgruppen

Definition (1.2)

Sei X eine Menge. Dann ist das Paar $(\text{Per}(X), \circ)$ bestehend aus der Teilmenge $\text{Per}(X) \subseteq \text{Abb}(X)$ der **bijektiven** Abbildungen $X \rightarrow X$ und der Komposition $\circ$ von Abbildungen eine Gruppe, die man als **Permutationsgruppe** der Menge X bezeichnet. Die Elemente von $\text{Per}(X)$ nennt man auch **Permutationen** von X .

Definition (1.3)

Ist $r \in \mathbb{N}$ und sind $k_1, \dots, k_r \in \mathbb{N}$ mit $k_1 \geq \dots \geq k_r \geq 2$, dann bezeichnet man das Tupel $(k_1, \dots, k_r)$ als **Zerlegungstyp** eines Elements $\sigma \in S_n$, wenn σ als Produkt disjunkter Zyklen der Längen $(k_1, \dots, k_r)$ dargestellt werden kann.

Satz (1.4)

Die Gruppe S_n ist für $n \leq 2$ abelsch und für $n \geq 3$ **nicht abelsch**.

Bem. Ist $X = M_n = \{1, 2, \dots, n\}$ (mit $n \in \mathbb{N}$),
dann ist $(\text{Per}(M_n), \circ)$ die aus der Linearen Algebra
bekannte symmetrische Gruppe S_n .

Nachweis, dass $\text{Per}(X)$ für eine bel. Menge X
jeweils eine Gruppe ist:

- Sind $\sigma, \tau \in \text{Per}(X)$, d.h. $\sigma, \tau: X \rightarrow X$ Bijektor,
dann ist auch $\sigma \circ \tau: X \rightarrow X$ Bijektor.
 $\Rightarrow$ Durch $\circ$ ist eine Verknüpfung auf $\text{Per}(X)$
gegeben.

- Assoziativität: Für alle ρ, σ, τ gilt
 $(\rho \circ \sigma) \circ \tau = \rho \circ (\sigma \circ \tau)$ (Grund: Für alle $x \in X$ gilt $((\rho \circ \sigma) \circ \tau)(x) = \rho(\sigma(\tau(x))) = (\rho \circ (\sigma \circ \tau))(x)$)
- Neutralelement: $\forall \sigma \in \text{Per}(X): \sigma \circ \text{id}_X = \sigma$ und $\text{id}_X \circ \sigma = \sigma$ (Grund: Für alle $x \in X$ gilt $(\sigma \circ \text{id}_X)(x) = \sigma(\text{id}_X(x)) = \sigma(x)$ und $(\text{id}_X \circ \sigma)(x) = \text{id}_X(\sigma(x)) = \sigma(x)$)
- Inverse: Für jedes $\sigma \in \text{Per}(X)$ gilt $\sigma^{-1} \circ \sigma = \text{id}_X$ und $\sigma \circ \sigma^{-1} = \text{id}_X$ (nach Def. der Umkehrabbildung σ^{-1} von σ).

bekannt aus der Linearen Algebra:

- Es gilt $|S_n| = n!$ für alle $n \in \mathbb{N}$.
- Elemente von S_n können in Tabellen-
schriftweise dargestellt werden.

$\begin{pmatrix} 1 & 2 & \dots & n \\ a_1 & a_2 & \dots & a_n \end{pmatrix}$ steht für die Abbil-
dung $M_n \rightarrow M_n$,
 $k \mapsto a_k$.

Achtung: Damit die Tabelle eine bijektive
Abb. von $M_n \rightarrow M_n$ darstellt, muss
 $\{a_1, \dots, a_n\} = M_n$ gelten.

- Sei $n \in \mathbb{N}$ und $k \in \mathbb{N}$ mit $2 \leq k \leq n$.
Ein k -Zykel ist ein Element $\sigma \in S_n$ und der
Eigenschaft, dass eine k -elementige Teil-
menge $\{m_1, \dots, m_k\} \subseteq M_n$ existiert, so dass
 $\rightarrow$ die folgende Form hat:

$$\sigma(x) = \begin{cases} m_{r+1} & \text{falls } x = m_r, r < k \\ m_1 & \text{falls } x = m_k \\ x & \text{falls } x \notin \{m_1, \dots, m_k\} \end{cases}$$

Notation für dieses Element: $(m_1 m_2 \dots m_k)$

Bsp in S_5 : $(1354) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 1 & 4 \end{pmatrix}$

- Jedes Element aus S_n kann als Produkt von endlichen reihen, paarweise disjunkten Zyklen dargestellt werden.
(paarweise disjunkt bedeutet: Je zwei Zyklen im Produkt haben keine gemeinsame Zahl.)

ative

Beispiel:

- Das Element $(135) \circ (24) \in S_5$ ist vom Zerlegungstyp $(3, 2)$.
- Das Element $(13) \circ (25) \circ (46) \in S_6$ ist vom Zerlegungstyp $(2, 2, 2)$.
- Die Identität hat den Zerlegungstyp (1) .

$$(135) \circ (24) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix}$$

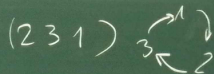
$$1 \mapsto 3 \quad 1 \mapsto 1$$

$$4 \mapsto 4 \quad 2 \mapsto 4$$

$$3 \mapsto 5 \quad 3 \mapsto 3$$

$\left. \begin{matrix} 5 \\ 4 \end{matrix} \right\}$

Anwendung:



- Elemente der Gruppe S_3 :

$\text{id}, (12), (13), (23), (123), (132)$

$$|S_3| = 3! = 6$$

- Elemente der Gruppe S_4 :

$\text{id}, (12), (13), (14), (23), (24), (34),$

$(123), (132), (124), (142), (134), (143),$

$(234), (243), (1234), (1324), (1432),$

$(1243), (1342), (1423), (12)(34), (13)(24),$

$(14)(23)$

$$|S_4| = 4! = 24$$