1.2 Gruppen

a) Definition

<u>Def.:</u> Sei G eine Menge. Eine Verknüpfung auf G ist eine Abbildung $*: G \times G \to G$, $(a,b) \mapsto a*b$.

<u>Bsp.:</u>

(1) Auf $G = \mathbb{N}, \mathbb{Z}, \mathbb{Q}$ oder $\mathbb{R}$ kennen wir Addition und Multiplikation, also für $a,b \in G$:

$$a*b := a+b \quad \text{oder} \quad a*b := a \cdot b$$

(2) $G = \mathrm{Abb}(X,X) = \{f: X \to X\}$. Für $f,g \in G$ gilt auch $f \circ g \in G$. Also ist die Komposition $\circ$ eine Verknüpfung auf G. Vorsicht: $f \circ g \neq g \circ f$

<u>Def.:</u> Eine Gruppe ist ein Paar $(G,*)$ aus einer nichtleeren Menge G und einer Verknüpfung $*$ auf G mit den Eigenschaften

(G1) Assoziativgesetz:

$$(a*b)*c = a*(b*c) \text{ für alle } a,b,c \in G$$

(G2) Es gibt ein (links-)neutrales Element $e \in G$ mit:

(i) $e*a = a$ für alle $a \in G$

(ii) zu jedem $a \in G$ gibt es ein (Links-)Inverses $a' \in G$, so daß $a' * a = e$.

Die Gruppe heißt abelsch (oder kommutativ) falls außerdem $a*b = b*a$ für alle $a,b \in G$.

Schreibweisen:

abelsche Gruppe: $a+b$ statt $a*b$, $e=0$, $a' = -a$

allgemein: ab statt $a*b$, $e=1$, $a' = a^{-1}$

Wegen (G1): $abc = (ab)c = a(bc)$

Bsp.: (i) $(\mathbb{Z},+)$, dann ist $e=0$, $a'=-a$

Konkret: $2+(-3) = -1 \in \mathbb{Z}$, $(1+2)+3 = 1+(2+3)$

$0+2 = 2 = 2+0$, $(-2)+2 = 0$

(ii) $(\mathbb{R}\setminus\{0\},\cdot)$, dann ist $e=1$, $a' = \frac{1}{a}$

(iii) Ist $(\mathrm{Abb}(X,X),\circ)$ eine Gruppe?

$\circ$ ist assoziativ, und $e = id_X$ $\qquad id_X \circ f = f$

aber aus der Existenz von g mit $g \circ f = id_X$ folgt, daß f injektiv ist $\Rightarrow$ kein Inverses

Reparatur:

$S(X) = \{ f: X \to X \text{ bijektiv} \} \subset \mathrm{Abb}(X,X)$

Dann ist $\circ$ eine Verknüpfung auf $S(X)$ und $(S(X),\circ)$ bildet die symmetrische Gruppe auf X.

Für $X = \{1,\dots,n\}$ heißt $S_n = S(X)$ Permutationsgruppe, jedes $\sigma \in S_n$ beschreibt eine Permutation von $\{1,\dots,n\}$.

nützliche Aussage

Proposition: Ist G eine Gruppe, so gilt:

(i) das linksneutrale Element $e \in G$ ist eindeutig und zugleich Rechtsneutrales, d.h. $ae = a \quad \forall a \in G$.

(ii) das Linksinverse $a' \in G$ ist eindeutig und zugleich Rechtsinverses, d.h. $aa' = e \quad \forall a \in G$.

Bew: Sei $a \in G$. Zu a' gibt es a'' mit $a''a' = e$. Folglich:

$$aa' = e(aa') = (a''a')(aa') = a''\underbrace{(a'a)}_{e}a' = a''a' = e.$$

$\Rightarrow$ a' ist Rechtsinverses. Außerdem gilt:

$$ae = a(a'a) = (aa')a = ea = a \Rightarrow e \text{ ist Rechtneutrales.}$$

Sei $\tilde{e} \in G$ ein zweites neutrales Element, dann ist

$$e\tilde{e} = e \text{ und } e\tilde{e} = \tilde{e}, \text{ also } e = \tilde{e}.$$

Sei $\tilde{a}' \in G$ ein zweites Inverses zu a, so folgt

$$\tilde{a}' = \tilde{a}'\underbrace{(aa')}_{e} = \underbrace{(\tilde{a}'a)}_{e}a' = a'. \qquad \square$$

Bem.:

Im Beispiel (iii) oben reicht es nicht, sich auf injektive Abbildungen zu beschränken, damit $Abb(X,X)$ eine Gruppe ist. Zu jedem $f: X \to X$ muß ein $g: X \to X$ existieren, so daß $g \circ f = id_X$, aber auch $f \circ g = id_X$ gilt.

$\Leftrightarrow$ f ist bijektiv.

b) Untergruppen

Def.: Sei $(G,*)$ eine Gruppe. Eine nichtleere Teilmenge $G' \subset G$ heißt **Untergruppe**, wenn für alle $a, b \in G'$ auch $a*b \in G'$ und $a^{-1} \in G'$.

Restriktion $*|_{G'} : G' \times G' \to G'$

Bem.:

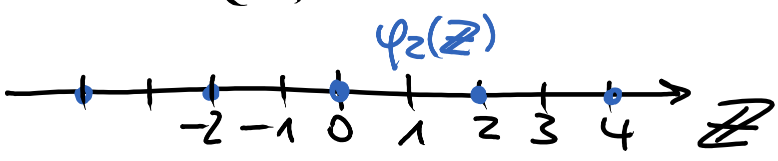
(1) Eine (Unter-)gruppe ist abgeschlossen bzgl. $*$

(2) $(G', *)$ ist wieder eine Gruppe.

Bew.: es gibt ein $a \in G'$, also auch $a^{-1} \in G'$ und $a a^{-1} = e \in G'$. $\square$

(3) Bsp.: Gruppe $(\mathbb{Z}, +)$

- $\mathbb{N} \subset \mathbb{Z}$ ist keine Untergruppe, da z.B. $-1 \notin \mathbb{N}$.
- Die Menge $m\mathbb{Z} := \{ ma \mid a \in \mathbb{Z} \} \subset \mathbb{Z}$ ist eine Untergruppe, weil $ma + mb = m(a+b) \in m\mathbb{Z}$ und $-mb = m(-b) \in m\mathbb{Z}$.



Def.: Sei G eine Gruppe und $A \subset G$. Die von A erzeugte Untergruppe $\mathrm{erz}(A)$ ist definiert durch

$$\mathrm{erz}(A) = \{a_1 \cdot \ldots \cdot a_n \mid n \in \mathbb{N},\ a_i \in A \text{ oder } a_i^{-1} \in A\},$$

also die Menge aller endlichen Produkte von Elementen aus A bzw. deren Inversen.

Bem.:

4) Beispiel: Gruppe $(\mathbb{Z}, +)$, $A = \{2\}$. Dann ist

$$\mathrm{erz}(A) = \{2, 4, 6, \ldots, 0, -2, -4, \ldots\} = 2\mathbb{Z}$$

5) allgemein für $(G, \cdot)$ und ein $a \in G$:

$$\mathrm{erz}(\{a\}) = \{a, a^2, a^3, \ldots, 1, a^{-1}, a^{-2}, \ldots\}$$
$$= \{a^n \mid n \in \mathbb{Z}\} \qquad \text{zyklische Gruppe}$$

Schreibweise für $(G, +)$: $\mathrm{erz}(\{a\}) = \{na \mid n \in \mathbb{Z}\}$

Satz: $\mathrm{erz}(A)$ ist die kleinste Untergruppe von G, die A enthält, d.h.

$$\mathrm{erz}(A) = \bigcap \{U \mid U \subset G \text{ Untergruppe},\ A \subset U\}.$$

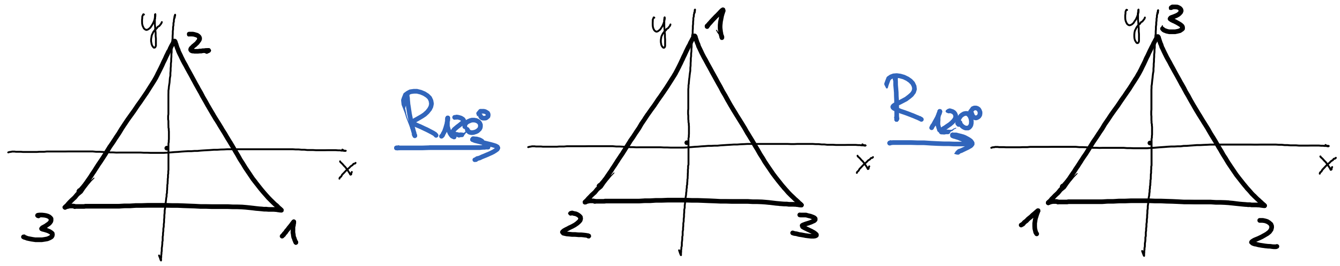
Beweis: es ist zu zeigen: (→ Übung)

i) $\mathrm{erz}(A)$ ist eine Untergruppe

ii) Ist $U \subset G$ eine beliebige Untergruppe mit $A \subset U$, so folgt $\mathrm{erz}(A) \subset U$.

Bsp.:

6) Drehung um $\frac{2\pi}{3}$ ($120°$) in der Ebene:



$R_{120°}: \mathbb{R}^2 \to \mathbb{R}^2$ ist bijektiv und $(R_{120°})^3 = id$

$\Rightarrow$ Drehgruppe $C_3 = \text{erz}(\{R_{120°}\})$

$= \{R_{0°}, R_{120°}, R_{240°}\} \subset S(\mathbb{R}^2)$

7) Nun sei $\cdot : G \to G$ eine Verknüpfung mit

$a^n = 1$ und $a^m \neq 1$ für $1 \leq m < n$, $a \in G$.

Dann ist die zyklische Gruppe $C_n = \text{erz}(\{a\})$ endlich und hat genau n Elemente: $C_n = \{1, a, a^2, \dots, a^n\}$

Inverses von a^2 ist a^{n-2}, da $a^{n-2}a^2 = a^n = 1$, usw.

Satz: (Kleiner Satz von Fermat)

Sei G eine endliche Gruppe aus n Elementen.

Dann gilt für jedes $a \in G$: $a^n = 1$.

Originalversion: Sei p eine Primzahl und $a \in \mathbb{N}$, $a < p$.

Dann gilt: $a^{p-1} = 1 \mod p$. ($\to$ Zahlentheorie)

Beweis: s. Beutelspacher, Abschnitt 9.2.2

c) Homomorphismen

<u>Def.:</u> Seien G und H Gruppen. Eine Abbildung $f: G \to H$ heißt Homomorphismus (von Gruppen), wenn $f(ab) = f(a) f(b)$ für alle $a, b \in G$. Wir nennen f einen Isomorphismus, wenn er bijektiv ist. Zwei Gruppen G und H heißen isomorph $(G \cong H)$, falls ein Isomorphismus von G nach H existiert.

Homomorphismus:
„f und die Gruppenverknüpfungen sind vertauschbar."

<u>Bem.:</u>
Für einen Gruppenhomomorphismus $f: G \to H$ gilt:
(i) $f(e_G) = e_H$,
(ii) $f(a^{-1}) = f(a)^{-1}$ für alle $a \in G$.

Die neutralen Elemente von G und H werden aufeinander abgebildet. Inversion und f vertauschen.

Bew.: $e_H = f(e_G) f(e_G)^{-1} = f(e_G e_G) f(e_G)^{-1}$
$= f(e_G) f(e_G) f(e_G)^{-1} = f(e_G)$

$e_H = f(e_G) = f(a^{-1}a) = f(a^{-1}) f(a) \Rightarrow f(a)^{-1} = f(a^{-1})$

□

Bsp.:

(1) Die Exponentialfunktion $\exp: \mathbb{R} \to \mathbb{R}_{>0}$, $x \mapsto e^x$ ist ein Isomorphismus von $(\mathbb{R},+)$ nach $(\mathbb{R}_{>0},\cdot)$, da $e^{x+y} = e^x e^y$

$\Rightarrow$ $(\mathbb{R},+)$ und $(\mathbb{R}_{>0},\cdot)$ sind isomorph

($\nearrow$ Rechenschieber: $xy = e^{\log(x)+\log(y)}$)

(2) betrachte die abelsche Gruppe $(\mathbb{Z},+)$. Für jedes $m \in \mathbb{Z}$ ist $\varphi_m : \mathbb{Z} \to \mathbb{Z}$, $a \mapsto ma$ ein Homomorphismus, da $m(a+b) = ma + mb$.

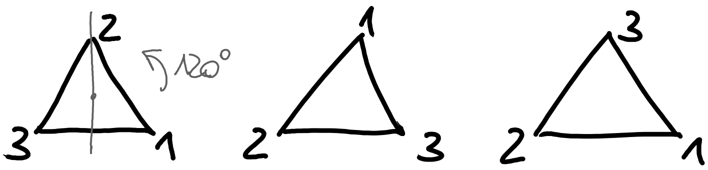
Das Bild $\varphi_m(\mathbb{Z}) = m\mathbb{Z} := \{ma \mid a \in \mathbb{Z}\} \subset \mathbb{Z}$ ist eine Untergruppe.

(3) Betrachte ein gleichseitiges n-Eck mit Mittelpunkt im Koordinatenursprung. Es ist invariant unter:

- Drehung $R_{2\pi/n} : \mathbb{R}^2 \to \mathbb{R}^2$ um den Winkel $2\pi/n$
- Spiegelung $s: \mathbb{R}^2 \to \mathbb{R}^2$ an einer Symmetrieachse

$\Rightarrow$ Die Diedergruppe $D_n = \mathrm{erz}(\{R_{2\pi/n}, s\}) \subset S(\mathbb{R}^2)$ mit der Komposition als Verknüpfung enthält alle Symmetrietransformationen eines gleichseitigen n-Ecks.

Für $n=3$ gilt: $D_3 \cong S_3$ (Permutationsgruppe)



usw.

für $n>3$ ist $2n = |D_n| < |S_n| = n!$, also $D_n \not\cong S_n$.