

2.1.7. Zusammenfassung der Gruppen-eigenschaften

Zusammenfassend: In einer Gruppe (G, \cdot) gilt Folgendes:

- (i) Für alle $a, b, c \in G$ gilt: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
- (ii) Es gibt ein eindeutiges Element $e \in G$ mit $a \cdot e = e \cdot a = a$ für alle $a \in G$.
- (iii) Zu jedem $a \in G$ gibt es ein eindeutiges $b \in G$ mit $a \cdot b = b \cdot a = e$.

(i) - Assoziativgesetz

e aus (ii) - das eindeutige neutrale Element
b aus (iii) ist das inverse Element zu a, das
wir als a^{-1} bezeichnen.

Wenn man eine Gruppe multipaktiv schreibt,
so bezeichnet man oft das neutrale Element
als 1.

Bei Abelschen Gruppen wird die Verknüpfung
oft als + bezeichnet. Man sagt in diesem Fall,
dass die Gruppe additiv erweiterbar wird.
Man nutzt in diesem Fall entsprechende
Bezeichnungen:

0 das neutrale Element von $(G, +)$

-a das inverse Element von $a \in G$
in der Gruppe $(G, +)$.

In einer Abel'schen Gruppe $(G, +)$ gilt:

- Für alle $a, b, c \in G$: $a + (b + c) = (a + b) + c$
- Es existiert ein eindeutiges Element $0 \in G$ mit $0 + a = a + 0 = a$ für alle $a \in G$
- Für alle $a, b \in G$: $a + b = b + a$
- Zu jedem $a \in G$ gibt es ein eindeutiges $b \in G$ mit $a + b = 0$
(Bezeichnung: $b = -a$).

Beispiele

$(\mathbb{Z}, +)$ abelsche Gruppe

$(\mathbb{Q} \setminus \{0\}, \cdot)$ abelsche Gruppe

$(\mathbb{Q}, +)$
 $(\mathbb{R}, +)$
 $(\mathbb{R} \setminus \{0\}, \cdot)$

Permutationen auf n Elementen
(nur abelsch ab $n \geq 3$)

Nicht-Beispiele

$(\mathbb{N}_0, +)$ nur die 0 Bsg. + direkt

(\mathbb{Q}, \cdot) 0 Bsg.
nicht invertierbar

2.1.8. Das inverse des Produkts und der Potenz

Prop. Sei (G, \cdot) Gruppe und seien $a, b \in G$.

Dann gilt

$$(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$$

Darüber hinaus gilt für die Potenz

$$a^n := \underbrace{a \cdot \dots \cdot a}_{n \text{ mal}} \quad (n \in \mathbb{N})$$

$$\text{die Gleichung } (a^n)^{-1} = (a^{-1})^n.$$

Beweis: Übungsaufgabe.

Mit dieser Proposition als Hintergrundwissen definieren wir die Potenzen von a wie folgt:

$$a^n := \underbrace{a \cdot \dots \cdot a}_{n \text{ mal}}$$

$$a^{-n} := (a^{-1})^n = (a^n)^{-1}$$

$$a^0 := e$$

für $n \in \mathbb{N}$ und $a \in G$.

2.1.9. Zyklotische Gruppen

Eine Gruppe (G, \cdot) heißt zyklisch, wenn ein $a \in G$ existiert derart, dass jedes $x \in G$ als $x = a^n$ mit $n \in \mathbb{Z}$ darstellbar ist.

Wenn wir die Gruppe additiv schreiben, d.h. $(G, +)$, so ist zyklisch der Eigenschaft,

dass ein $a \in G$ existiert derart, dass jedes $x \in G$ als $x = n \cdot a$ darstellbar ist, mit $n \in \mathbb{Z}$.

Berechnung:

$$n \cdot a = a + \dots + a \quad \text{bei } n > 0$$

$\underbrace{}_{n \text{ mal}}$

$$n \cdot a = 0 \quad \text{bei } n = 0$$

$$n \cdot a = (-a) + \dots + (-a) \quad \text{bei } n < 0$$

$\underbrace{}_{|n| \text{ mal}}$

Bsp.

$$(\mathbb{Z}, +)$$
 zyklisch

$$\left. \begin{array}{l} a=1 \\ a=-1 \end{array} \right\}$$

die beiden möglichen Wahlen von a

Nicht-Beispiele

$(\mathbb{Q}, +)$ keine zyklische Gruppe

(S_n, \cdot) mit $n \geq 3$ nicht zyklisch, weil sie nicht abelsch ist.

Def.

Die Menge der Äquivalenzklassen auf \mathbb{Z} bzgl. der Äquivalenz modulo $m \in \mathbb{N}$ bezeichnet man als \mathbb{Z}_m . Eine andere Bezeichnung: $\mathbb{Z}/m\mathbb{Z}$.

D.L.

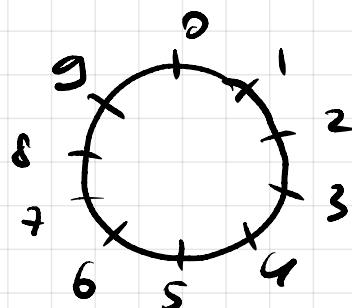
$$\mathbb{Z}_m := \mathbb{Z}/m\mathbb{Z} := \{[z]_m : z \in \mathbb{Z}\}$$

wobei wir als $[z]_m$ die Äquivalenzklasse von $z \in \mathbb{Z}$ bezeichnen:

$$[z]_m := \{u \in \mathbb{Z} : u \equiv z \pmod{m}\}$$
$$= \{u \in \mathbb{Z} : u - z \text{ ist durch } m \text{ teilbar}\}$$

Die Elemente von \mathbb{Z}_m

nennt man
die Restklassen
von \mathbb{Z} modulo m .



$$m=10$$

Bem. Es gibt genau m Restklassen
modulo m :

$$\mathbb{Z}_m = \{[0]_m, [1]_m, \dots, [m-1]_m\}$$

Def Auf \mathbb{Z}_m (mit $m \in \mathbb{N}$) definieren
wir die Plus-Verknüpfung
 $+ : \mathbb{Z}_m \times \mathbb{Z}_m \rightarrow \mathbb{Z}_m$:

$$A + B := [a + b]_m$$

für eine beliebige Wahl von $a \in A$ und
 $b \in B$.

Diese Operation ist wohldefiniert, da
 $[a + b]_m$ nicht der Wert der
Vertreter $a \in A, b \in B$ der
Restklassen A und B abhängig ist.

Prop Sei $m \in \mathbb{N}$ und seien $A, B \subseteq \mathbb{Z}_m$.

Dann gibt es eine endliche Restklasse $C \subseteq \mathbb{Z}_m$ mit $a+b \in C$ für alle $a \in A$ und $b \in B$ gilt.

Beweis: Übungsaufgabe.

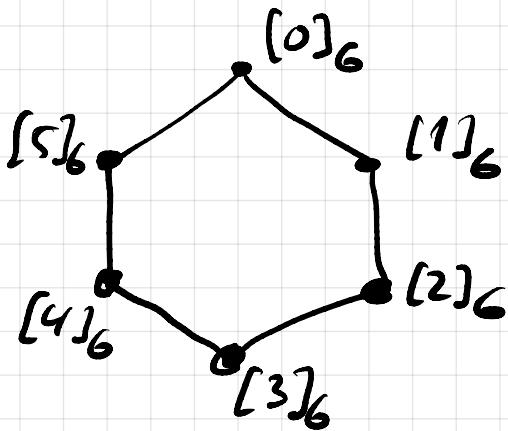
Prop. Für $m \in \mathbb{N}$ ist \mathbb{Z}_m eine zyklische Gruppe.

Beweis: $[1]_m$ ist der Erzeuger von \mathbb{Z}_m , d.h.

$$[2]_m = 2 \cdot [1]_m$$

□

Bsp



$[1]_6$ erzeugt \mathbb{Z}_6 .

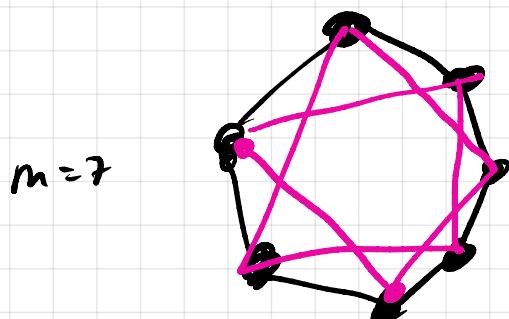
$[2]_6$ kein Erzeuger.

$[3]_6$ kein Erzeuger

$[4]_6$ kein Erzeuger.

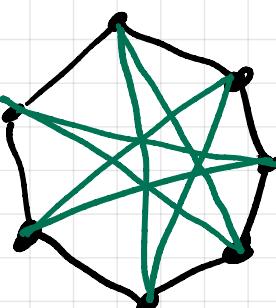
$[5]_6$ ein Erzeuger.

Probieren Sie eine ähnliche Analyse für $m=7$, $m=8$ und $m=12$ zu machen.



$m=7$

$[2]_7$ Erzeuger von \mathbb{Z}_7 .



$[3]_7$ Erzeuger von \mathbb{Z}_7 .

2.1.10. Untergruppen

Für eine Gruppe (G, \cdot) heißt

eine Teilmenge $H \subseteq G$ mit $H \neq \emptyset$

Untergruppe von G , wenn Folgendes gilt:

(i) $a \cdot b \in H$ für alle $a, b \in H$

(ii) $\bar{a}^{-1} \in H$ für alle $a \in H$

Bem. Ist H Untergruppe von G , so liegt das neutrale Element e von G notwendig gewiss in H . Da H nicht leer ist, können wir ein $a \in H$ fixieren.

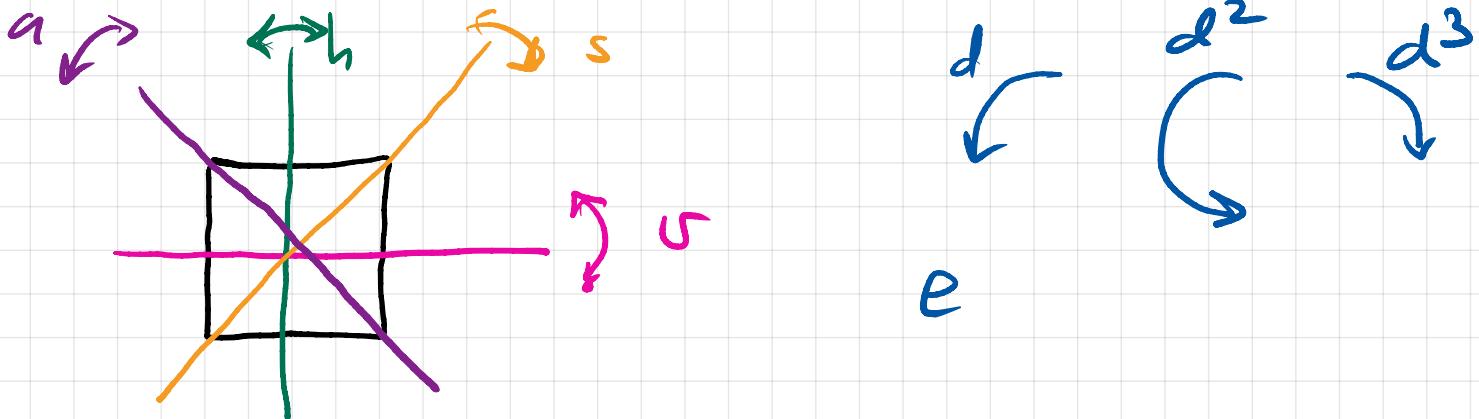
Dann ist $\bar{a}^{-1} \in H$, wegen (ii). Damit erhält man (i)

$$a \cdot \bar{a}^{-1} = e \text{ ebenfalls in } H.$$

Somit hat die Gruppenstruktur bez. der \cdot -Verknüpfung. Das ist eine äquivalente Beschreibung von Untergruppen.

Bsp

Symmetrien des Quadrats.



Untergruppen von $\{e, a, h, s, \cup, d, d^2, d^3\}$

Die gesuchte Gruppe \rightarrow

$$\begin{array}{lll} \{e, d, d^2, d^3\} & \{e, \cup, h, d^2\} & \{e, a, s, d^2\} \\ \{e, \cup\} & \{e, h\} & \{e, a\} \quad \{e, s\} \quad \{e, d^2\} \end{array}$$

{e}

findet alle Untergruppen?

2.2. Ringe

2.2.1. Ring

Eine nichtleere Menge R mit zwei binären Verknüpfungen $+ : R \times R \rightarrow R$ und

$\cdot : R \times R \rightarrow R$ heißt Ring, wenn

Folgendes erfüllt ist:

(R1) $(R, +)$ ist Abel'sche Gruppe

(R2) \cdot ist assoziativ, d.h.

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c \text{ für alle } a, b, c \in R$$

(R3) Es gelten die Distributivgesetze

$$a \cdot (b+c) = a \cdot b + a \cdot c,$$

$$(b+c) \cdot a = b \cdot a + c \cdot a$$

für alle $a, b, c \in R$.

Ist \circ kommutativ auf R

(d.h. $a \cdot b = b \cdot a$ für alle $a, b \in R$),

so nennt man den Ring $(R, +, \circ)$ kommutativ. Einen Ring nennt man unital, wenn \circ ein neutrales Element besitzt, d.h. es existiert ein Element $1 \in R$ mit

$$1 \cdot a = a \cdot 1 = a \text{ für alle } a \in R.$$

Bsp.

$(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ sind kommutative Ringe mit 1

$(\mathbb{Z}, +, \cdot)$ kommutativer Ring mit 1.

Bem

Ist $(R, +, \cdot)$ ein Ring so gilt:

$$0 \cdot a = a \cdot 0 = 0$$

für alle $a \in R$.

Defn:

(R3)

$$0 \cdot a = \underbrace{(0+0) \cdot a}_{\text{denn } 0 \text{ ist das}} = 0 \cdot a + 0 \cdot a$$

denn 0 ist das

Element, mit $0+r=r$

für alle $r \in R$.

$(R,+)$ ist Abelsche Gruppe. Also findet man für jedes $r \in R$ ein eindeutiges Element $-r$ mit $r+(-r)=0$. Also gilt

$$0 \cdot a + (-0 \cdot a) = (0 \cdot a + 0 \cdot a) + (-0 \cdot a)$$



$$0 = (0 \cdot a + 0 \cdot a) + (-0 \cdot a)$$



$$0 = 0 \cdot a + (0 \cdot a + (-0 \cdot a))$$

↑
Nach dem Assoziativgesetz
für t , das in (R1)
enthalten ist.



$$0 = 0 \cdot a + 0$$



$$0 = 0 \cdot a.$$