1.5.9 Def: Sei A Menge

1) A heißt endlich, falls jede injektive Abb. $f: A \to A$ auch surjektiv ist.
2) A heißt unendlich, falls A nicht endlich ist, d.h. es exist. eine Abb. $f: A \to A$, die injektiv und nicht surjektiv ist.
A heißt abzählbar (unendlich), falls es eine bijektive Abb. $f: A \to \mathbb{N}$ gibt.
4) A heißt überabzählbar, falls A unendlich und nicht abzählbar ist.

Bsp: $\mathbb{N}$ unendlich: $f: n \mapsto 2n$
$\mathbb{Q}$ ist abzählbar (1. vorher)
$\mathbb{R}$ ist überabzählbar (später)

2. Zahlenkörper

2.1 Mengen und Verknüpfungen

2.1 Def Sei G eine Menge. Eine Abb. $\circ: G \times G \to G: (x,y) \mapsto x \circ y$ heißt Verknüpfung auf G.

1) Eine Verknüpfung heißt assoziativ, falls $\forall g,h,j \in G: g \circ (h \circ j) = (g \circ h) \circ j$
2) $\circ$ heißt kommutativ, falls $\forall g,h \in G: g \circ h = h \circ g$.
3) Ein El. $e \in G$ heißt neutrales Element, falls $\forall g \in G: e \circ g = g = g \circ e$.
4) Sei $g \in G$. Ein El. $h \in G$ heißt inverses

Element zu g, falls $h \circ g = e = g \circ h$.
Schreibe $g^{-1} := h$.

Beisp: $(\mathbb{N}, +)$ assoz., komm., kein neutral. El.
$(\mathbb{N}, \cdot)$ " " , $e=1$, kein inv. El
$(\mathbb{Z}, +)$ " " , $e=0$, $x^{-1} = -x$
$(\mathbb{Q}, \cdot)$ " " , $e=1$, $x^{-1} = \frac{1}{x}$
$x=0$ hat kein inverses El.

2.2 Def: Sei $\circ$ eine Verknüpfung auf G.
1) $(G, \circ)$ heißt Monoid, falls $\circ$ assoziativ und ein neutrales El. existt.

2) $(G, \circ)$ heißt Gruppe, falls $\circ$ assoz., ein neutrales El existt und jedes El ein inverses besitzt.
3) $(G, \circ)$ heißt abelsche Gruppe, falls $(G, \circ)$ Gruppe und $\circ$ kommutativ.

Bsp 1) Monoid: $(\mathbb{N}_0, +)$, $(\mathbb{N}, \cdot)$, M Menge: $(\mathcal{P}(M), \cap)$. Neutrales El $e = M$: $\forall A \subseteq M: A \cap M = A$
2) Abelsche Gruppe: $(\mathbb{Z}, +)$, $(\mathbb{Q} \setminus \{0\}, \cdot)$

3) Wichtig: Permutationsgruppe.
Sei M endl. Menge
$S(M) := \{f : M \to M \mid f \text{ bijektiv}\}$
$\circ : (\pi_1, \pi_2) \mapsto \pi_1 \circ \pi_2$ Hintereinanderausführung

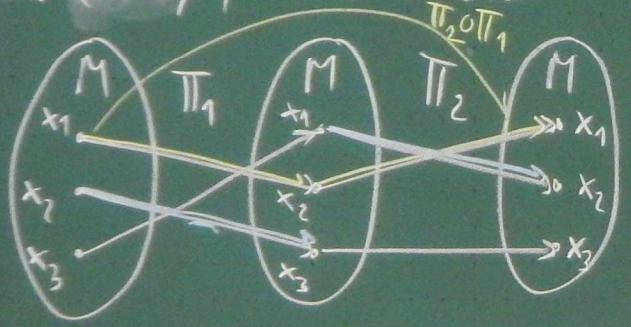
assoziativ:
$\pi_1 \circ (\pi_2 \circ \pi_3)(x) = \pi_1((\pi_2 \circ \pi_3)(x))$
$= \pi_1(\pi_2(\pi_3(x)))$ ←
$((\pi_1 \circ \pi_2) \circ \pi_3)(x) = (\pi_1 \circ \pi_2)(\pi_3(x))$ =
$= \pi_1(\pi_2(\pi_3(x)))$ ←

$e = id_M$
Zu $\pi \in S(M)$ ist die inverse Abb. π^{-1} das

inverse El: $\pi^{-1} \circ \pi = id_M = \pi \circ \pi^{-1}$

$\Rightarrow (S(M), \circ)$ ist eine Gruppe

Falls M mind drei El. enthält, ist $(S(M), \circ)$ nicht abelsch:



$(\pi_2 \circ \pi_1)(x_1) = x_1$
$(\pi_1 \circ \pi_2)(x_1) = x_3$
$\Rightarrow \pi_2 \circ \pi_1 \neq \pi_1 \circ \pi_2$

2.3 Satz: In jeder Gruppe $(G, \circ)$ gelten:

1) e ist eindeutig
2) Wenn $g \in G$ gegeben ist, ist g^{-1} eindeutig
3) $\forall g, h \in G \; \exists! x \in G : g \circ x = h$
4) $\forall g \in G : (g^{-1})^{-1} = g$
5) $\forall g, h \in G : (g \circ h)^{-1} = h^{-1} \circ g^{-1}$

Reihenfolge verschieden!

Beweis: 1) e, e' neutrale Elemente

$\Rightarrow e = e' \circ e = e' \quad \Rightarrow e = e'$

(e' neutral, e neutral)

2) Seien g^{-1} und h invers zu g.

$\Rightarrow h = e \circ h = (g^{-1} \circ g) \circ h =$

$= g^{-1} \circ (g \circ h) = g^{-1}$ ($g \circ h = e$)

3) a) Eindeutigkeit:

$g \circ x = h \Rightarrow g^{-1} \circ (g \circ x) = g^{-1} \circ h$

$\Rightarrow e \circ x = (g^{-1} \circ g) \circ x = g^{-1} \circ h$

$\Rightarrow x = g^{-1} \circ h$

b) Existenz: Setze $x = g^{-1} \circ h$ in die Gl. ein:

$g \circ x = g \circ (g^{-1} \circ h) = (g \circ g^{-1}) \circ h = e \circ h = h$

$\Rightarrow x$ ist Lösung

4) $g^{-1} \circ (g^{-1})^{-1} = e$

$g^{-1} \circ g = e$

Aus 3): Die Gl. $g^{-1} \circ x = e$ besitzt genau eine Lös. x

$\Rightarrow x = g = (g^{-1})^{-1}$

5) selber als Üb., analog zu 4).

Schreibweise: (im Gruppen) Für $g \in G$, $n \in \mathbb{Z}$

$$g^n := \begin{cases} \underbrace{g \circ g \circ \dots \circ g}_{n\text{-mal}} & \text{falls } n \in \mathbb{N} \\ e & \text{falls } n = 0 \\ \underbrace{g^{-1} \circ \dots \circ g^{-1}}_{-n \text{ Mal}} & \text{falls } -n \in \mathbb{N} \end{cases}$$

2.2 Zwei Verknüpfungen

2.4 Def: Auf einer Menge R seien zwei Verknüpfungen $+$ und $\cdot$ definiert.

1) $(R, +, \cdot)$ heißt Ring, falls

a) $(R, +)$ abelsche Gruppe und

b) $(R, \cdot)$ Monoid und

c) $0 \neq 1$ wobei 0 = neutral bez. $+$ und 1 = neutral bez. $\cdot$

d) Es gelten die Distributivgesetze

$$\forall g, h, j \in R: \left((g+h) \cdot j = g \cdot j + h \cdot j \wedge g \cdot (h+j) = g \cdot h + g \cdot j \right)$$

2) $(R, +, \cdot)$ heißt kommutativer Ring, falls $(R, +, \cdot)$ Ring und $\cdot$ kommutativ.

3) $(R, +, \cdot)$ heißt Körper, falls $(R, +, \cdot)$ Ring und $(R \setminus \{0\}, \cdot)$ abelsche Gruppe.

Bsp: 1) $(\mathbb{Z}, +, \cdot)$ komm. Ring

2) $(\mathbb{Q}, +, \cdot)$ Körper

3) p sei Primzahl, Dann ist $(\mathbb{N}/p\mathbb{N}, +, \cdot)$ ein Körper. (vgl letztes Mal)

4) m keine Primzahl: $(\mathbb{N}/m\mathbb{N}, +, \cdot)$ kein Körper, aber kommut. Ring

5) $R := \{f : \mathbb{Q} \to \mathbb{Q}$ Abbildung$\}$

$f+g : \mathbb{Q} \to \mathbb{Q} : x \mapsto f(x)+g(x)$

$f \cdot g : \mathbb{Q} \to \mathbb{Q} : x \mapsto f(x) \cdot g(x)$

Hier gibt es Nullteiler

$(R, +, \cdot)$ ist kommut. Ring.

2.5 Schreibweisen

$-x$:= inverses El. zu x bezügl. $+$

$y - x := y + (-x)$

$\frac{1}{x} = x^{-1}$:= inverses El. zu x bezügl. $\cdot$

$\frac{y}{x} := y \cdot \frac{1}{x}$

$x^n := \underbrace{x \cdot x \cdot \ldots \cdot x}_{n\text{-mal}}$ für $n \in \mathbb{N}$

$x^{-n} := (x^{-1})^n$ für $-n \in \mathbb{N}$

$x^0 := 1$

$n \cdot x := \underbrace{x + \ldots + x}_{n\text{-Mal}}$ für $n \in \mathbb{N}$

26 Folg: In jedem Körper $(\mathbb{K}, +, \cdot)$ gelten für $a, b, c, d \in \mathbb{K}$:

1) $-(-a) = a$

2) $0 \cdot a = 0 = a \cdot 0$

3) $ab = 0 \Rightarrow a = 0 \vee b = 0$

4) $(-a) \cdot b = -(a \cdot b)$

5) $(-a)(-b) = a \cdot b$

6) $\frac{1}{\frac{1}{a}} = a$ für $a \neq 0$

7) $\frac{a}{b} + \frac{c}{d} = \frac{ad + b \cdot c}{bd}$

8) $\frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d}$

9) $\frac{\frac{a}{b}}{\frac{c}{d}} = \frac{a}{b} \cdot \frac{d}{c}$

Beweis: 1) und 6): Siehe 2.3: $(g^{-1})^{-1} = g$

2) $0 \cdot a = (0+0) \cdot a = 0 \cdot a + 0 \cdot a$

$\Rightarrow 0 \cdot a = 0 \cdot a + 0 \cdot a \quad | + (-0 \cdot a)$

$\Rightarrow \underbrace{0 \cdot a + (-0 \cdot a)}_{=0} = 0 \cdot a + \underbrace{(0 \cdot a + (-0 \cdot a))}_{=0}$

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

3) Sei $a \cdot b = 0$

Fall (i): $a = 0$ ✓

Fall (ii): $a \neq 0 \Rightarrow \frac{1}{a} \in \mathbb{K}$ exist.

$a \cdot b = 0 \quad | \cdot \frac{1}{a}$

$\Rightarrow 1 \cdot b = 0 \cdot \frac{1}{a} \overset{2)}{=} 0$

$\Rightarrow b = 0$

4) Zeige, dass $(-a) \cdot b$ und $-(a \cdot b)$ Lösung derselben Gleichung sind

$a \cdot b + (-a) \cdot b \overset{DG}{=} (a + (-a)) \cdot b = 0 \cdot b \overset{3)}{=} 0$

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

$\Rightarrow (-a) \cdot b$ und $-(a \cdot b)$ sind Lös. der Gleichung $a \cdot b + x = 0$, also gleich nach 2.3, 3)

5) genauso wie 4

7) $\frac{a}{b} + \frac{c}{d} = a \cdot b^{-1} + c \cdot d^{-1} \cdot 1$

$= a \cdot b^{-1} \cdot d \cdot d^{-1} + c \cdot d^{-1} \cdot b^{-1} \cdot b$

$\overset{KG}{=} (a \cdot d)(d^{-1} \cdot b^{-1}) + (c \cdot b) \cdot (d^{-1} \cdot b^{-1})$

$\overset{DG}{=} (a \cdot d + c \cdot b) \cdot \underbrace{(d^{-1} \cdot b^{-1})}_{=(b \cdot d)^{-1} \text{ wieso?}}$

$\overset{\text{Def. Bruch}}{=} \frac{a \cdot d + c \cdot b}{b \cdot d}$

8), 9) entsprechend.