Übersicht:

1.) Körper

2.) Bsp für vollst. Induktion

3.) Binomischer Lehrsatz

Umstrukturierung von Summen

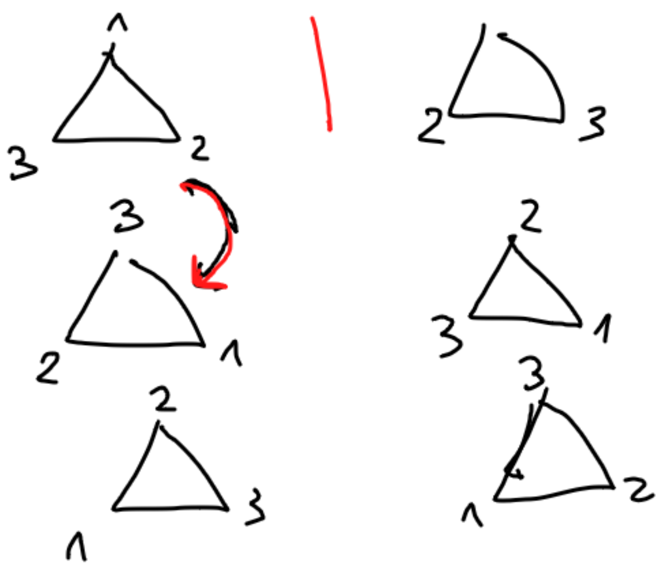
4.) obere/untere Schranken,
Supremum/Infimum

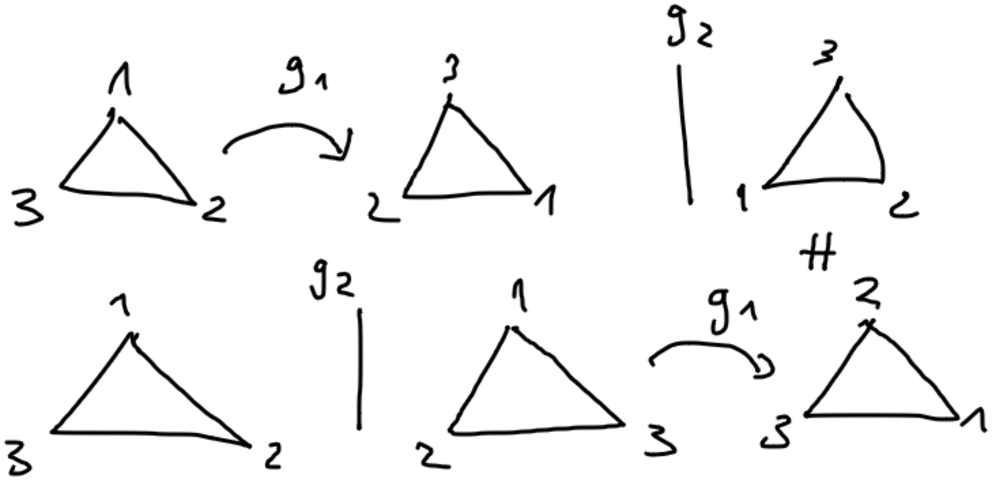
1.) Nachtrag

Diedergruppe $\cong$ Isomorpiegruppe des regelmäßigen n-Ecks

(Drehungen / Spiegelungen + Kombinationen)

$n = 3$





$\circ$: Komposition / Hinterausführung

endliche Körper:

1.) $\mathbb{F}_2 = \{0,1\}$

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

$1+1=0$, $1\cdot 1 = 1$, d.h. 1 war additiv / mult. Selbstinverse

2.) $\mathbb{F}_3 = \{0,1,2\}$

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

alle Körperaxiome erfüllt

$\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$ $\quad$ 0 add. Neutrale, $\quad$ 1 mult. Neutrale

$2 + 3 = 0$ $\quad$ $1 \cdot 1 = 1$

$1 + 4 = 0$ $\quad$ $3 \cdot 2 = 1$

$\vdots$ $\quad$ $4 \cdot 4 = 1$

<u>Restklassenkörper</u> $\quad$ $\mathbb{F}_p$ $\quad$ für ein $\quad$ $p \geq 2$

Für $q_1, q_2 \in \mathbb{Z}$ definieren wir die Relation R_p / $\sim_p$,

wobei $q_1 \sim_p q_2 :\Longleftrightarrow q_1 = q_2 \mod p$

$:\Longleftrightarrow \exists\, k \in \mathbb{Z} :\ q_1 = k \cdot p + q_2$

$\Longleftrightarrow$ „p teilt q_1 mit Rest q_2"

$\sim_p$: (i) reflexiv: $q \sim_p q \quad \forall\, q \in \mathbb{Z}$

(ii) symmetrisch $q_1 \sim_p q_2 \Rightarrow q_2 \sim_p q_1$

(iii) transitiv: $q_1 \sim_p q_2,\ q_2 \sim_p q_3 \Rightarrow q_1 \sim_p q_3$

$\Bigg\}$ Äquivalenz-relation

Äquivalenzklassen: M Menge, $\sim$ Äquivalenzrelation

Für ein $x \in M$, $[x] := \{ y \in M \mid x \sim y \}$

Bsp: $\sim_5$, $1 \in \mathbb{Z}$, $[1] := \{ g \in \mathbb{Z} \mid 1 \sim g \}$

$$:= \{ 1 + k \cdot 5 \mid k \in \mathbb{Z} \}$$

$$= \{ \ldots, -9, -4, 1, 6, 11, 16, \ldots \}$$

$$\subseteq \mathbb{Z}$$

<u>Beh.</u> (i) $\forall x \in M: \quad [x] \neq \emptyset$

(ii) $\forall x, y \in M: \quad [x] \cap [y] = \begin{cases} [x] = [y] & x \sim y \\ \emptyset & x \not\sim y \end{cases}$

<u>Beweis:</u>

(i) Sei $x \in M$. $x \sim x$ nach (i) $\Rightarrow x \in [x] \neq \emptyset$

(ii) 1. Fall $x \sim y$

$z \in [x] \Rightarrow x \sim z \Rightarrow (x \sim z) \wedge (x \sim y)$

$\overset{(ii)}{\Rightarrow} (y \sim x) \wedge (x \sim z)$

$\overset{(iii)}{\Rightarrow} y \sim z \Rightarrow z \in [y]$

$[x] \subseteq [y]$, „$=$" mit Symmetrieargument (analog)

2.) Fall $x \nsim y$

Angenommen $[x] \cap [y] \neq \emptyset$, (mit Auswahlaxiom) wählen $z \in [x] \cap [y]$.

Da $z \in [x]$, $x \sim z$, und da $z \in [y]$, $y \sim z$

$$\Rightarrow (x \sim z) \wedge (y \sim z)$$

$$\overset{(ii)}{\Rightarrow} (x \sim z) \wedge (z \sim y)$$

$$\overset{(iii)}{\Rightarrow} x \sim y$$

$\lightning$ zur Annahme

Also muss der Schnitt $[x] \cap [y]$ leer sein. $\blacksquare$

$$M/_{\sim} := \{ [x] \mid x \in M \} \subseteq \mathcal{P}(M)$$ ← Potenzmenge, enthält alle Teilmengen von M.

Zurück zur Restklassenkörper

$$\mathbb{F}_p :\cong \mathbb{Z}/_{\sim_p} = \{ [0], [1], \ldots, [p-1] \}$$ Wohldefiniert?

$$\mathbb{F}_p = \{0, 1, \ldots, p-1\}$$

$$[q_1] + [q_2] := [q_1 + q_2]$$ Ja!

$$[q_1] \cdot [q_2] := [q_1 \cdot q_2]$$

z.B. $\mathbb{F}_5$:

$$\text{„}4 + 3\text{“} = [4] + [3] = [4+3] = [7] = [2] \text{ „=“ } 2$$

Aber: $\mathbb{F}_8$ kein Körper:

4 hat kein Mult. Inverses.

$4 \cdot 0 = 0$

$4 \cdot 1 = 4$ $\qquad$ $4 \cdot 5 = 4$

$4 \cdot 2 = 0$ $\qquad$ $4 \cdot 6 = 0$

$4 \cdot 3 = 4$ $\qquad$ $4 \cdot 7 = 4$

$4 \cdot 4 = 0$

Fazit: $\mathbb{F}_p$ Körper $\Leftrightarrow$ p Primzahl

2.) Vollständige Induktion

Beh: $\sum_{k=1}^{n} (2k-1) = n^2$ und $\sum_{k=1}^{n} 2k = n^2+n = n\cdot(n+1)$

$\forall n \geq 1$

nur das zuerst.

Erinnere: $\sum_{k=1}^{n} k = \frac{n\cdot(n+1)}{2}$

Beweis: mit vollständige Induktion

Induktionsanfang: $n=1$,

$$\sum_{k=1}^{1} (2k-1) = (2\cdot 1 - 1) = 1 = 1^2 \quad \checkmark$$

Induktionsvoraussetzung: Es gelte $\sum_{k=1}^{n}(2k-1) = n^2$

Induktionsschritt: $n \to n+1$

$$\sum_{k=1}^{n+1}(2k-1) = (2\cdot(n+1)-1) + \sum_{k=1}^{n}(2k-1)$$

$$\overset{IV}{=} (2n+1) + n^2$$

$$= n^2 + 2n + 1$$

$$= (n+1)^2 \quad \checkmark$$

$$\underbrace{\sum_{k=1}^{n}(2k-1)}_{n^2} + \sum_{k=1}^{n} 2k = \sum_{k=1}^{2n} k = \frac{2n\cdot(2n+1)}{2}$$

$$= n\cdot(2n+1)$$

$$= n^2 + n\cdot(n+1)$$

$$\Rightarrow \boxed{\sum_{k=1}^{n} 2k = n\cdot(n+1)}$$

$$\blacksquare$$

$$n^2 = \sum_{k=1}^{n} 2k-1 = \sum_{k=1}^{n} 2k - \sum_{k=1}^{n} 1$$

$$= \cancel{n^2}\ \sum 2k - n \iff \sum 2k = n^2+n$$

Beh: $\sum_{k=1}^{n} 2k = n\cdot(n+1) = n^2+n \qquad n \geq 1$

Beweis: mit vollständiger Induktion

Induktionsanfang: $n = 1$

$$\sum_{k=1}^{1} 2k = 2\cdot 1 = 2 = 1\cdot(1+1) \quad \checkmark$$

Induktionsvoraussetzung: Es gelte $\sum_{k=1}^{n} 2k = n\cdot(n+1)$

Induktionsschritt: $n \longrightarrow n+1$

$$\sum_{k=1}^{n+1} 2k = 2(n+1) + \sum_{k=1}^{n} 2k$$

$$\overset{IV.}{=} 2n+2 + n\cdot(n+1)$$

$$= 2n+2 + n^2 + n$$

$$= n^2 + 3n + 2$$

$$= (n+1)(n+2)$$

NR:

$$(n+1)(n+2)$$

$$= n^2 + 2n + n + 1\cdot 2$$

$$= n^2 + 3n + 2$$

$$\blacksquare$$

3.) <u>Binomischer Lehrsatz</u>

Vorlesung / Übung: $\forall x,y \in \mathbb{R}: \quad (x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$

$\binom{n}{k}$ Binomialkoeffizient „n über k"

$$\binom{n}{k} := \frac{n!}{k!\,(n-k)!} \qquad (k \leq n) \qquad n! = n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot 2 \cdot 1$$

$$\binom{n}{k} := 0 \qquad \text{für } k > n$$

$$(x+y)^n = \underbrace{(x+y)\cdot(x+y)\cdot(x+y)\cdot \quad \cdot \quad (x+y)}_{}^{n\text{-mal}}$$

$$= \underline{1}\cdot x^n + \underline{n}\, x\cdot y^{n-1} + \ldots\ldots \quad + \ldots$$

$$+ \underline{n}\, x^{n-1} y^1 + \underline{1}\, y^n$$

Faktor vor $x^k y^{n-k}$: $\binom{n}{k}$ $\quad \binom{n}{n-1} = \binom{n}{1} = \frac{n!}{1!(n-1)!} = \frac{n!}{(n-1)!}$

$$\binom{n}{0} = \binom{n}{n} = 1 \qquad = \frac{n\cdot(n-1)!}{(n-1)!}$$

$$= n$$

$\binom{n}{k}$: Wie viele Möglichkeiten gibt es ~~eine~~ k-Elemente aus einer n elementigen Menge herauszunehmen (ohne Zurücklegen, ohne Reihenfolge)

Übung:

(i) $$\sum_{k=0}^{n} \binom{n}{k} = 2^n \quad \ldots \qquad (n \geq 1)$$

(ii) $$\sum_{k=0}^{n} \binom{n}{k} (-1)^k = \ldots \qquad (n \geq 1)$$

(i) Vorschlag 2^n:
$$\sum_{k=0}^{n} \binom{n}{k} \underset{x}{\underset{\shortparallel}{1}}^k \cdot \underset{y}{\underset{\shortparallel}{1}}^{n-k} = (\cancel{1}+1)^n = 2^n$$

(ii) $$\sum_{k=0}^{n} \binom{n}{k} \underset{x}{\underset{\shortparallel}{(-1)}}^k \cdot 1^{n-k} = ((-1)+1)^n$$
$$= (1-1)^n = 0^n = 0$$

<u>Beobachtung:</u>

Kommutativität

$$\sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k} = (x+y)^n = (y+x)^n$$

$k = 0 \; \dots \; n$ $\qquad$ $k = n \dots 0$

$$= \sum_{k=0}^{n} \binom{n}{k} y^k x^{n-k}$$

Summe endlich

$$\sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k} = \sum_{j=0}^{n} \binom{n}{k(j)} x^{k(j)} y^{\overbrace{n-k(j)}^{j}}$$

$$= \sum_{j=0}^{n} \binom{n}{n-j} x^{n-j} y^{n-(n-j)}$$

$$= \sum_{j=0}^{n} \binom{n}{n-j} y^j x^{n-j}$$

$$= \sum_{j=0}^{n} \binom{n}{j} y^j x^{n-j}$$

$k = n-j$

$k : \{0, 1, \dots, n\} \to \{0, \dots, n\}$

$k(j) = n-j$

$$\binom{n}{n-j} = \frac{n!}{(n-j)!\,(n-(n-j))!} = \frac{n!}{(n-j)!\,j!} = \frac{n!}{j!\,(n-j)!} = \binom{n}{j}$$

$$\forall\, n, j: \quad \binom{n}{n-j} = \binom{n}{j}$$

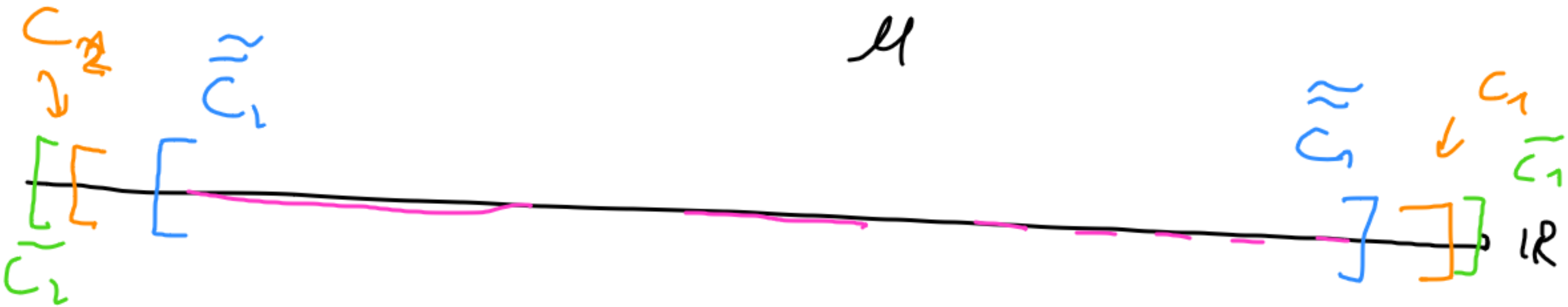
4.) Beschränkte Mengen

$\mathbb{K}$ angeordneter Körper

$M \subseteq \mathbb{K}$, Wir sagen M ist nach oben/ unten beschränkt, falls ein $C \in \mathbb{K}$ ex. mit

$$\forall m \in M: \ m \leq C \quad / \quad \forall m \in M: \ m \geq C$$

Wir sagen M ist beschränkt, falls M nach unten und nach oben beschränkt ist.



Wir nennen die kleinste obere Schranke Supremum $\sup M$,
und die größte untere Schranke Infimum. $\inf M$

(Falls sie existieren!)

Formale Definition: $(M \subseteq \mathbb{K})$

Wir sagen $s \in \mathbb{K}$ ist das Supremum von M, falls

(i) s ist obere Schranke, $\forall\, m \in M: s \geq m$

(ii) Für ~~∀~~ obere oberen Schranke $C \in \mathbb{K}$, $s \leq C$.

$$(ii) :\iff (ii') : \forall\, C < s : \exists\, \underbrace{m}_{m(C)} \in M : C < m$$

<u>Beh.</u> (ii) $\Leftrightarrow$ (ii') ($\forall C$ obere Schranke: $s \leq C$ $\Leftrightarrow$ $\forall C < s\ \exists m \in M: C < m$)

„$\Rightarrow$" Es gelte (ii). Sei $C < s$.

Angenommen $\forall m \in M: C \geq m$

$\Rightarrow$ C obere Schranke

$\overset{(ii)}{\Rightarrow}$ $C \geq s$ ↯ Trichotomie

$\Rightarrow$ $\exists m \in M: C < m$.

„$\Leftarrow$" Es gelte (ii'). Sei C obere Schranke, d.h. $\forall m \in M: C \geq m$.

Angenommen $C < s$.

$\overset{(ii')}{\Rightarrow}$ $\exists m \in M: C < m$ ↯ obere Schranke

$\Rightarrow$ $C \geq s$

$\blacksquare$

$\mathbb{K} = \mathbb{Q}$

$x_0 = 2 \in \mathbb{Q}$, $x_{n+1} = \frac{1}{2}\left(x_n + \frac{2}{x_n}\right) \in \mathbb{Q}$ z.B. $x_1 = \frac{3}{2}$, $x_2 = \frac{17}{12}, \dots$

$\forall n \geq 0$: $M_n = (1, x_n)$, $M_0 = (1, 2)$, $M_1 = (1, \frac{3}{2})$, $M_2 = (1, \frac{17}{12})$, ...

Was ist das Sup / Inf von M_n ?

$\sup M_n = x_n$ (Falls $x_n < 1$: $M_n = \emptyset$)

$x_{n+1} = \frac{1}{2}\left(x_n + \frac{2}{x_n}\right) \geq \sqrt{x_n \cdot \frac{2}{x_n}} = \sqrt{2} > 1$

$\inf M_n = 1$

sowohl in $\mathbb{Q}$, als auch in $\mathbb{R}$.

Babylonisch Algorithmus: x_n immer näher an $\sqrt{2}$

$$M := \bigcap_{n\in\mathbb{N}} M_n = \bigcap_{n\in\mathbb{N}} (1, x_n) \overset{\text{„in } \mathbb{R}\text{"}}{=} (1, \sqrt{2}]$$

$\sqrt{2} \notin \mathbb{Q}$ dementsprechend hat M kein Sup über $\mathbb{Q}$.

(ii): $\forall$ oberen Schranke $\underset{\in\mathbb{Q}}{C} > \sqrt{2}$, finden wir $C > \underset{\in\mathbb{Q}}{\tilde{C}} > \sqrt{2}$

(ii) $\underset{\in\mathbb{Q}}{\tilde{\tilde{C}}} < \sqrt{2}$, $\underset{\in\mathbb{Q}}{\tilde{\tilde{C}}} \in M$ $\tilde{\tilde{C}} < \tilde{\tilde{\tilde{C}}} < \sqrt{2}$.