Diskrete VO 4.12.

$ggT(a,b) = \max\{t \in \mathbb{N} : t|a \text{ und } t|b\}$ $(a \neq 0 \vee b \neq 0)$

$kgV(a,b) = \min\{t \in \mathbb{N} : a|t \text{ und } b|t\}$ $(a \neq 0 \wedge b \neq 0)$

Algorithmus: ggT durch den erweiterten Euklidschen Algorithmus; liefert außerdem $u, v \in \mathbb{Z}$ mit $ggT(a,b) = ua + vb$

kgV: über den ggT & folg. Zsm.hang.

Satz) Seien $a, b \in \mathbb{N}$. Dann gilt: $ggT(a,b) \cdot kgV(a,b) = a \cdot b$

Beweis] Wir zeigen als erstes $ab \mid ggT(a,b) \cdot kgV(a,b)$

Aus dem Euklidschen Algorithmus erhalten wir $u, v \in \mathbb{Z}$, sodass $ggT(a,b) = ua + vb$

Also $ggT(a,b) \cdot kgV(a,b) = ua\, kgV(a,b) + vb\, kgV(a,b)$

($b \cdot s_1$, $a \cdot s_2$; $b \mid$ und $a \mid$ weil wir a bzw. b an dieser Stelle brauchen; beide $\Rightarrow ab \mid$)

Also gilt $ab \mid ggT(a,b) \cdot kgV(a,b)$.

Wir zeigen nun $ggT(a,b) \cdot kgV(a,b) \mid ab$

Sei $x := \frac{ab}{ggT(a,b)}$. Es gilt $x = \underbrace{\frac{a}{ggT(a,b)}}_{\in \mathbb{N}} \cdot b = a \cdot \underbrace{\frac{b}{ggT(a,b)}}_{\in \mathbb{N}}$ (*)

(*) Es gilt $ggT(a,b) \mid a$. Also (Def. Teilbarkeit) gibt es $z \in \mathbb{N}$, sodass $z \cdot ggT(a,b) = a$. Folglich $z = \frac{a}{ggT(a,b)}$, & somit ist $\frac{a}{ggT(a,b)}$ ganzzahlig (& natürlich).

Also ist x ein gemeinsames Vielfaches von a und b.
Nach Satz 4.19 gilt daher $kgV(a,b) \mid x$.
Es gibt also $u \in \mathbb{Z}$ mit $x = kgV(a,b) \cdot u$

Also: $\frac{ab}{ggT(a,b)} = kgV(a,b) \cdot u$, folglich

$ab = kgV(a,b) \cdot ggT(a,b) \cdot u$, und somit
$kgV(a,b) \cdot ggT(a,b) \mid ab$.

Wenn für $s,t \in \mathbb{N}$ gilt $s \mid t$ und $t \mid s$, so gilt $s = t$:
Da $s \mid t$, gibt es u mit $su = t$. Da $t \mid s$, gibt es v mit $tv = s$.
weil s wurde herausgehoben ↘ ↙ $0 = suv - s$
$s = tv = suv$, folglich $s(uv-1) = 0$
Also: $uv - 1 = 0$ und somit $uv = 1$.
Da $s,t \in \mathbb{N}$ gilt $u = v = 1$, und somit $s = t$.

(Andere Begründung: Wegen $s \mid t$ gilt $s \leq t$; genauso gilt auch $t \leq s$, also $s = t$).

Primfaktorzerlegung

Def) Eine Zahl $p \in \mathbb{N}$ ist eine Primzahl $:\Leftrightarrow$
1) $p > 1$
2) $\forall a,b \in \mathbb{N} : p = a \cdot b \Rightarrow (a = 1 \vee b = 1)$

Satz] Es gibt unendl. viele Primzahlen.

Bew:) $F_m := 2^{2^m} + 1$ (m-te Fermatzahl)

$F_0 = 2^{2^0} + 1 = 2^1 + 1 = 3$
$F_1 = 2^{2^1} + 1 = 4 + 1 = 5$
$F_2 = 2^4 + 1 = 17$
$F_3 = 2^8 + 1 = 257$
$F_4 = 2^{16} + 1 = 65537$

Es gilt $\prod_{i=0}^{m-1} F_i = F_m - 2$ für alle $m \in \mathbb{N}$

~~Also gilt ggT (~~

Seien nun $i,j \in \mathbb{N}$ mit $i < j$. Dann gilt:

$ggT(F_i, F_j) \mid ggT(F_j - 2, F_j)$ $\quad F_i \mid F_j - 2$

(Hier verwenden wir:

$\forall a,b,c \in \mathbb{N}: a \mid b \Rightarrow ggT(a,c) \mid ggT(b,c)$

Bew.) Seien $a,b,c \in \mathbb{N}$. Es gilt $ggT(a,c) \mid a$ und $a \mid b$, also: $ggT(a,c) \mid b$

Ebenso gilt: $ggT(a,c) \mid c$.

$ggT(a,c)$ ist also ein gemeinsamer Teiler von b & c, und somit gilt $ggT(a,c) \mid ggT(b,c)$.)

$ggT(F_j - 2, F_j) = ggT(F_j - 2, 2) \mid 2$.

Also $ggT(F_i, F_j) = 1$ oder $ggT(F_i, F_j) = 2$

Da $2 \nmid F_j$, gilt $ggT(F_i, F_j) = 1$

Sei nun für jedes $i \in \mathbb{N}_0$ die Zahl q_i der kleinste Teiler von F_i, der $q_i \geq 2$ erfüllt.

q_i ist eine Primzahl: Seien $a, b \in \mathbb{N}$ so, dass $ab = q_i$. Da $a \mid q_i$, gilt wegen der Minimalität von q_i entweder $a = q_i$ (dann gilt $b = 1$) oder $a = 1$. Also ist q_i eine Primzahl.

Für $i \neq j$ gilt $q_i \neq q_j$: Denn wäre $q_i = q_j$, so gilt $q_i \mid F_i$ und $q_i \mid F_j$, also $q_i \mid ggT(F_i, F_j) = 1$ (aber 1 ist keine Primzahl)

Folgerung:
- $\{q_i \mid i \in \mathbb{N}_0\}$ ist eine unendl. Menge von Primzahlen
- In $\{1, \dots, 2^{2^m} + 1\}$ gibt es mind. m Primzahlen

Somit gilt für die m-te Primzahl p_m die Ungl. $p_m \leq 2^{2^m} + 1$

Satz (Fundamentallemma) Sei p eine Primzahl, und seien $a, b \in \mathbb{Z}$. Falls p ein Produkt $a \cdot b$ teilt, so teilt p einen der Faktoren a oder b.

$$(\forall p \in \mathbb{P} \ \forall a, b \in \mathbb{Z} : p \mid a \cdot b \Rightarrow (p \mid a \vee p \mid b))$$

Bew) Wir nehmen an, dass $p \mid a \cdot b$ und $p \nmid a$.
z.z.: $p \mid b$ $\quad (p \mid ab \wedge p \nmid a) \Rightarrow p \mid b$

Da $p \nmid a$ gilt $ggT(p, a) = 1$. Also gibt es $u, v \in \mathbb{Z}$, sodass $1 = up + va$ $\quad / \cdot b$

Folglich $b = \underbrace{upb}_{p|.} + \underbrace{vab}_{p|.}$

Da $p \mid ub$ und $p \mid vab$, gilt also auch $p \mid b$.

Die ggT-Berechnung über Primfaktorzerlegung beruht auf folgendem Korollar: (= Folgerung)

Sei p_n die n-te Primzahl, also $p_1 = 2, p_2 = 3, \ldots$
Für jedes $i \in \mathbb{N}$ seien $\alpha_i \in \mathbb{N}_0$ und $\beta_i \in \mathbb{N}_0$.

Wir nehmen an, dass nur endl. viele α_i und nur endl. viele $\beta_i \neq 0$ sind.

Sei $a := p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots = \prod_{\substack{i \in \mathbb{N}_0 \\ \alpha_i \neq 0}} p_i^{\alpha_i}$

$$b := \prod_{\substack{i \in \mathbb{N}_0 \\ \beta_i \neq 0}} p_i^{\beta_i}$$

$\alpha = (\alpha_1, \alpha_2, \ldots) = (1, 7, 3, 0, 5, 2, 0, \ldots)$
$\beta = (\beta_1, \beta_2, \ldots) = (0, 8, 2, 1, 7, 0, 0, \ldots)$

$a = 2^1 \cdot 3^7 \cdot 5^3 \cdot 7^0 \cdot 11^5 \cdot 13^2 = \ldots$
$b = 3^8 \cdot 5^2 \cdot 7^1 \cdot 11^7$

Dann sind äquivalent:

1) $a \mid b$.
2) $\forall i \in \mathbb{N}: \alpha_i \leq \beta_i$

Diskrete VO

5.12.

$(p_1, p_2, p_3, \ldots) := (2, 3, 5, 7, 11, \ldots)$ Folge aller Primzahlen

$$a = \prod_{\substack{i \in \mathbb{N} \\ \alpha_i \neq 0}} p_i^{\alpha_i} \quad * \qquad b = \prod_{\substack{i \in \mathbb{N} \\ \beta_i \neq 0}} p_i^{\beta_i} \quad *$$

$a = 2^5 \cdot 3^7 \cdot 19^{11}$

$b = 2^6 \cdot 3^7 \cdot 19^{12}$

Satz) Äquivalent sind

(1) $a \mid b$

(2) $\forall i \in \mathbb{N} : \alpha_i \leq \beta_i$

* α_i & β_i sind hier HOCHZAHLEN!

(2) $\Rightarrow$ (1)

Sei $N \in \mathbb{N}$ definiert als $N := \max \{ i \in \mathbb{N} \mid \alpha_i \neq 0 \vee \beta_i \neq 0 \}$

Dann gilt $a = \prod_{i=1}^{N} p_i^{\alpha_i}$ * und $b = \prod_{i=1}^{N} p_i^{\beta_i}$ *

Wir nehmen an, dass $\forall i \in \{1, \ldots, N\} : \alpha_i \leq \beta_i$ z.z. $a \mid b$

Sei $q := \prod_{i=1}^{N} p_i^{\beta_i - \alpha_i}$ *

Dann gilt $q \cdot a = b$, also gilt $a \mid b$.

(1) $\Rightarrow$ (2)

Wir nehmen an, dass $\prod_{i=1}^{N} p_i^{\alpha_i} \mid \prod_{i=1}^{N} p_i^{\beta_i}$

z.z. $\forall i \in \mathbb{N} : \alpha_i \leq \beta_i$

Sei $i \in \mathbb{N}$. Wir nehmen an, dass $\alpha_i > \beta_i$

$$\left(\prod_{\substack{j=1 \\ j \neq i}}^{N} p_j^{\alpha_j} \right) \cdot p_i^{\alpha_i - \beta_i} \mid \prod_{\substack{j=1 \\ j \neq i}}^{N} p_j^{\beta_j}$$

teilt

⊗ Erklärung siehe Bemerkung

Bem.: Es gilt $\prod_{j=1}^{N} p_j^{\alpha_j} \mid \prod_{j=1}^{N} p_j^{\beta_j}$

Wir dividieren bd. Seiten durch $p_i^{\beta_i}$

Wegen der Annahme gibt es q, sodass

$$\left(\prod_{j=1}^{N} p_j^{\alpha_j}\right) \cdot q = \prod_{j=1}^{N} p_j^{\beta_j} \quad (*)$$

Sei $i \in \mathbb{N}$. Wir wollen zeigen, dass $\alpha_i \leq \beta_i$. Wir nehmen dazu an, dass $\alpha_i > \beta_i$. Wir dividieren beide Seiten der Gleichung $(*)$ durch p_i.

$$p_i^{\alpha_i - \beta_i} \cdot \left(\prod_{\substack{j=1 \\ j \neq i}}^{N} p_j^{\alpha_j}\right) \cdot q = \prod_{\substack{j=1 \\ j \neq i}}^{N} p_j^{\beta_j}$$

Also $$p_i^{\alpha_i - \beta_i} \mid \prod_{\substack{j=1 \\ j \neq i}}^{N} p_j^{\beta_j}$$

Bsp $2^3 \cdot 5^1 \cdot 7^4 \mid 2^4 \cdot 5^3 \cdot 7^5$

hier gilt es

$p_1 = 2$, $p_3 = 5$, $p_4 = 7$

$\alpha_1 = 3$, $\alpha_3 = 1$, $\alpha_4 = 4$ $\quad \beta_1 = 4$, $\beta_3 = 3$, $\beta_4 = 5$

neues Bsp hier nicht

Wir nehmen nun an, dass alle und ein α_i ist größer als β_i

$$2^3 \cdot 5^6 \cdot 7^9 \mid 2^4 \cdot 5^3 \cdot 7^{11} \qquad / : 5^3$$

$$2^3 \cdot 5^3 \cdot 7^9 \mid 2^4 \cdot 7^{11}$$

Satz) $2^3 \cdot 5^6 \cdot 7^9 \nmid 2^4 \cdot 5^3 \cdot 7^{11}$

Beweis: Ann: es gibt $q \in \mathbb{Z}$, sodass

$$2^3 \cdot 5^6 \cdot 7^9 \cdot q = 2^4 \cdot 5^3 \cdot 7^{11}$$

Dann gilt $2^3 \cdot 5^3 \cdot 7^9 \cdot q = 2^4 \cdot 7^{11}$

Also: $5 \mid 2^4 \cdot 7^{11}$

oder
$5^3 \cdot q = 2 \cdot 7^2$
$5 \mid 2 \cdot 7^2$
bringt aber nix

Folglich $5 \mid 2$ oder $5 \mid 7$ Wid. ↯

Wir nehmen an, dass $\prod_{j=1}^{N} p_j^{\alpha_j} \mid \prod_{j=1}^{N} p_j^{\beta_j}$ und $\alpha_i > \beta_i$

Da $\prod_{j=1}^{N} p_j^{\alpha_j} \mid \prod_{j=1}^{N} p_j^{\beta_j}$, gibt es $q \in \mathbb{N}$, sodass

$$q \cdot \prod_{j=1}^{N} p_j^{\alpha_j} = \prod_{j=1}^{N} p_j^{\beta_j}$$

Wir dividieren durch $p_i^{\beta_i}$ & erhalten

$$q \cdot \left(\prod_{\substack{j=1 \\ j \neq i}}^{N} p_j^{\alpha_j} \right) \cdot p_i^{\alpha_i - \beta_i} = \prod_{\substack{j=1 \\ j \neq i}}^{N} p_j^{\beta_j}$$

Da p_i die linke Seite teilt (wegen $\alpha_i - \beta_i \geq 1$), teilt p_i auch die rechte Seite, es gilt also

$$p_i \mid \prod_{\substack{j=1 \\ j \neq i}}^{N} p_i^{\beta_i}$$

Eine Primzahl, die ein Produkt teilt, teilt einen der Faktoren. Dann gibt es $j \neq i$ mit $p_i \mid p_j$. Dann gilt $p_i = 1$ oder $p_i = p_j$. (kann aber beides nicht gelten weil Primzahl $\neq 1$ & das 2. ist der Annahme)

Somit führt die Annahme, dass $\alpha_i > \beta_i$ ist, zu einem Widerspruch. Es gilt also $\alpha_i \leq \beta_i$.

Es gilt also $2^{\alpha_1} 3^{\alpha_2} 5^{\alpha_3} 7^{\alpha_4} 11^{\alpha_5} \dots \mid 2^{\beta_1} 3^{\beta_2} 5^{\beta_3} 7^{\beta_4} \dots$ genau dann, wenn für alle $i \in \mathbb{N}$: $\alpha_i \leq \beta_i$

Beispiel zum Euklidschen Algorithmus

		180	153
I	180	1	0
II	153	0	1
III = I − 1·II	27	1	−1
IV = II − 5·III	18	−5	6
	9	6	−7
	0		

$180 = 1 \cdot 180 + 0 \cdot 153$

$153 = 0 \cdot 180 + 1 \cdot 153$

$27 = 1 \cdot 180 + (-1) \cdot 153$

$18 = (-5) \cdot 180 + 6 \cdot 153$

$\boxed{9 = 6 \cdot 180 + (-7) \cdot 153}$

		444	130
	444	1	0
	130	0	1
* 1	54	1 *2	−3
* 2	22	−2	7 (1 − 2·(−3))
	10	5 (−2 − 2·5)	−17 (7 − 2·(−17))
	2	−12	41
	0		

$440 : 130 = 3$ * 054 R.

* 1 $1 \cdot 1 - 3 \cdot 0$

* 3 $130 : 54$

$1 - 2 \cdot (-2)$

$ggT(444, 130) = 2$

$= \underbrace{(-12)}_{u} \cdot 444 + \underbrace{41}_{v} \cdot 130$

Diskrete VO

11. 12.

Satz) Seien $n, i \in \mathbb{N}_0$ mit $i \leq n$. Dann hat $\{1, \dots, n\}$ genau $\binom{n}{i}$ i-elementige Teilmengen.

Bew) $A(n) :\Leftrightarrow \forall i \in \{0, 1, \dots, n\}$: Die Menge $\{1, \dots n\}$ hat genau $\binom{n}{i}$ i-elementige Teilmengen.

Wir zeigen $\forall n \in \mathbb{N}_0 : A(n)$ durch Induktion

Ind. anfang: wir zeigen $A(0)$.

Sei $n := 0$, dann ist $\{1, 2, \dots, n\} = \emptyset$ Sei $i := 0$

Wieviele 0-elementige Teilmengen hat $\emptyset$?

$\mathcal{P}(\emptyset) = \{\emptyset\}$. $\emptyset$ hat genau eine 0-elem. Teilmenge, nämlich $\emptyset$. $\binom{0}{0} = 1$

Also gilt $A(0)$

Ind. schritt: $\forall n \in \mathbb{N}_0 : A(n) \Rightarrow A(n+1)$

Sei $n \in \mathbb{N}_0$.

Ind. annahme [Wir nehmen an, dass $A(n)$ gilt, also dass $\{1, \dots, n\}$ für jedes $i \in \{0, \dots, n\}$ genau $\binom{n}{i}$ i-element. Teilmengen hat.

Z.z. $A(n+1)$. Z.z $\forall i \in \{0, \dots, n+1\} : \{1, \dots, n+1\}$ hat genau $\binom{n+1}{i}$ i-elem. Teilm.

Sei $i \in \{0, \dots, n+1\}$

1. Fall] $i = 0$

Ich habe den Fall isoliert da er nicht analog zu F2 funktioniert

Wieviele 0-elem. Teilmengen hat $\{1, \dots, n+1\}$?

Genau eine, nämlich $\emptyset$.

$\binom{n+1}{0} = \frac{(n+1)!}{(n+1)!\,0!} = 1.$

"#" = Anzahl der Elemente von

2. Fall) $i \geq 1$:

Sei $B = \{T \mid T \subseteq \{1,\dots,n+1\} \text{ und } \#T = i\}$

Wir wollen zeigen, dass $\#B = \binom{n+1}{i}$

disjunkte Vereinigung

$B = \{T \mid T \subseteq \{1,\dots,n+1\},\ \#T = i,\ n+1 \in T\}$
$\cup \{T \mid T \subseteq \{1,\dots,n+1\},\ \#T = i,\ n+1 \notin T\}$

$C := \{T \mid T \subseteq \{1,\dots,n+1\},\ \#T = i,\ n+1 \in T\}.$

$D := \{T \mid T \subseteq \{1,\dots,n+1\},\ \#T = i,\ n+1 \notin T\}$

Wir berechnen nun $\#C$ und $\#D$:

$D = \{T \mid T \subseteq \{1,\dots,n\},\ \#T = i\}$. Nach Ind. annahme gilt $\#D = \binom{n}{i}$

$C = \{S \cup \{n+1\} \mid S \subseteq \{1,\dots n\},\ \#S = i-1\}$

Nach Ind. ann. gilt $\#C = \binom{n}{i-1}$

Also gilt:

$\#B = \#C + \#D = \binom{n}{i} + \binom{n}{i-1} = \binom{n+1}{i}.$

↑ Eigenschaft d. Binominalkoeffizienten

$C' = \{S \mid S \subseteq \{1,\dots,n\},\ \#S = i-1\}$ hat nach Ind. ann. $\binom{n}{i-1}$ Elemente. C' & C haben gleich viele Elemente.

Also $\#C = \#C' = \binom{n}{i-1}$.

Wir zählen die 3-elem. Teilmengen von $\{1,2,3,4,5\}$, die 5 enthalten

$C = \{\{1,2,5\}, \{1,3,5\}, \{1,4,5\}, \{2,3,5\}, \{2,4,5\}, \{3,4,5\}\}$

Nun zählen wir die 2-elem. Teilmengen von $\{1,2,3,4\}$

$C' = \{\{1,2\}, \{1,3\}, \{1,4\}, \{2,3\}, \{2,4\}, \{3,4\}\}$

(Bsp: $n=4$, $i=3$) ← weil 3-elem. Teilmenge

weil $n+1=5$ $\quad i-1=2$

$\#C' = \binom{4}{2}$ $\qquad \#B = \binom{4}{3} + \binom{4}{2} = 4 + 6 = \binom{5}{3}$ $\quad \binom{4}{2} = \frac{4\cdot 3}{1\cdot 2}$

Ich weiß nicht, wie viele Teilmengen C hat, deswegen zählen wir die Teilm. von C'.

Binominalkoeff.

$$\binom{80}{4} = \frac{80\cdot 79\cdot 78\cdot 77}{1\cdot 2\cdot 3\cdot 4}$$

$\frac{80!}{4!\,76!}$

Pascalsches Δ

$\binom{n}{i}$

$$\begin{array}{ccccccccc} & & & & 1 & & & & \\ & & & 1 & & 1 & & & \\ & & 1 & & 2 & & 1 & & \\ & 1 & & 3 & & 3 & & 1 & \\ 1 & & 4 & & 6 & & 4 & & 1 \end{array}$$

$\binom{0}{0}$ $\binom{1}{0}$ $\binom{1}{1}$ $\binom{2}{0}$ $\binom{2}{1}$ $\binom{2}{2}$ $\binom{3}{0}$ $\binom{3}{1}$ $\binom{3}{2}$ $\binom{3}{3}$

$$\binom{n+1}{i} = \binom{n}{i} + \binom{n}{i-1} \quad \text{für } n \in \mathbb{N}_0,\ i \in \{1,\dots,n\}$$

Bsp: $(a+b)^5 = (a+b)\cdot(a+b)\cdot(a+b)\cdot(a+b)\cdot(a+b)$

$= aaaaa + baaaa + abaaa + aabaa +$
$aaaba + aaaab + [bbaaa + babaa +$
$baaba + baaab + abbaa + ababa +$
$abaab + aabba + aabab + aaabb]$ = $\{\{1,2\},\{1,3\},\{1,4\},\dots\{4,5\}\}$
$+ bbbaa + \dots + aabbb$
$+ bbbba + \dots + abbbb$
$+ bbbbb$

$= 1 \cdot a^5 + 5 \cdot a^4 b + 10 \cdot a^3 b^2 + 10\ a^2 b^3 + 5\ ab^4 + 1 b^5$

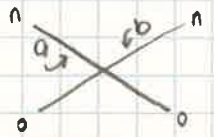
Es gibt also genauso viele Summanden $a^2 b^3$, wie es 2-elem. Teilmengen von $\{1, \dots, 5\}$ gibt.

Satz (Binomischer Lehrsatz)

Für alle $n \in \mathbb{N}$ und für alle $a, b \in \mathbb{R}$ gilt:

$$(a+b)^n = \binom{n}{0} a^n b^0 + \binom{n}{1} a^{n-1} b^1 + \binom{n}{2} a^{n-2} b^2 + \dots + \binom{n}{n-1} a^1 b^{n-1} + \binom{n}{n} a^0 b^n, \text{ also}$$

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i$$



Beweis: Induktion

$$A(n) :\Leftrightarrow \forall a, b \in \mathbb{R} : (a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i$$

Ind. anf.: $A(1)$; $n = 1$. Seien $a, b \in \mathbb{R}$

linke S. $= (a+b)^1 = a+b$ r.S. $\binom{1}{0} \cdot a^1 \cdot b^0 + \binom{1}{1} a^0 b^1 = 1a + 1b$. ✓

Ind. schritt z.z. $\forall n \in \mathbb{N} : A(n) \Rightarrow A(n+1)$:

Sei $n \in \mathbb{N}$. Wir nehmen an, dass $\forall a, b \in \mathbb{R}$:

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i.$$

z.z. $\forall a, b \in \mathbb{R} : (a+b)^{n+1} = \sum_{i=0}^{n+1} \binom{n+1}{i} a^{n+1} b^i$

Seien $a, b \in \mathbb{R}$.

$$(a+b)^{n+1} = (a+b)^n \cdot (a+b) \overset{\text{ind. ann.}}{=} \sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i \,(a+b)$$

(Ausmultiplizieren)

$$= \sum_{i=0}^{n} \binom{n}{i} a^{n-i+1} b^i + \sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^{i+1}$$

$j = i+1$

i	j
0	1
n	n+1

$j - 1 = i$

$$= \sum_{i=0}^{n} \binom{n}{i} a^{n-i+1} b^i + \sum_{j=1}^{n+1} \binom{n}{j-1} a^{n-(j-1)} b^{(j-1)+1}$$

$$= \sum_{i=0}^{n} \binom{n}{i} a^{n-i+1} b^i + \sum_{j=1}^{n+1} \binom{n}{j-1} a^{n+1-j} b^j$$

$$= \binom{n}{0} \cdot a^{n+1} b^0 + \sum_{i=1}^{n} \binom{n}{i} a^{n-i+1} b^i + \sum_{i=1}^{n} \binom{n}{i-1} a^{n+1-i} b^i + \binom{n}{n} a^0 b^{n+1}$$

(ich benenne mein j auf i um)

$$= 1 \cdot a^{n+1} + \left(\sum_{i=1}^{n} \left(\binom{n}{i} a^{n-i+1} b^i + \binom{n}{i-1} a^{n+1-i} b^i \right) \right) + 1 \cdot b^{n+1} =$$

$$= a^{n+1} + \sum_{i=1}^{n} \left(\binom{n}{i} + \binom{n}{i-1} \right) a^{n+1-i} b^i \Big) + b^{n+1}$$

$$\overset{\text{Rekursion für Binom. koeff.}}{=} a^{n+1} + \sum_{i=1}^{n} \binom{n+1}{i} a^{n+1-i} b^i \Big) + b^{n+1}$$

Summand von 0 ergibt a^{n+1} & Summand v. $n+1$ ergibt b^{n+1}

$$= \sum_{i=0}^{n+1} \binom{n+1}{i} \underbrace{a^{n+1-i} \cdot b^i}$$

gehört zum Summenzeichen davor

Somit gilt $A(n+1)$.

Diskrete VO

12.12.

$(p_1, p_2, p_3, \dots) := (2, 3, 5, 7, 11, 13, 17, \dots)$

$a = 2^{\alpha_1} \cdot 3^{\alpha_2} \dots = \prod_{i \in \mathbb{N}} p_i^{\alpha_i}$

$b = 2^{\beta_1} \cdot 3^{\beta_2} \dots = \prod_{i \in \mathbb{N}} p_i^{\beta_i}$

$a \mid b \iff \forall i \in \mathbb{N} : \alpha_i \leq \beta_i$

Bsp: $2^7 \cdot 5^3 \cdot 11 \nmid 2^8 \cdot 5^2 \cdot 13$

Satz) (Existenz und Eindeutigkeit d. Primfaktorzerlegung)
Sei $(p_i)_{i \in \mathbb{N}} = (2, 3, 5, 7, \dots)$ die Folge aller Primzahlen.
Sei $n \in \mathbb{N}$
Dann gibt es genau eine Fkt $\alpha : \mathbb{N} \to \mathbb{N}_0$, sodass
(1) $\{i \in \mathbb{N} \mid \alpha(i) > 0\}$ ist endlich
(2) $n = p_1^{\alpha(1)} \cdot p_2^{\alpha(2)} \dots = \prod_{\substack{j \in \mathbb{N} \\ \alpha(j) \neq 0}} p_j^{\alpha(j)}$

Bsp: $n = 666$

666	2
333	3
111	3
37	37
↗ 1	
Primzahl	

$\alpha(1) = 1$ (Die 1. Primzahl kommt 1× vor)
$\alpha(2) = 2$
$\alpha(3) = \dots = \alpha(11) = 0$
$\alpha(12) = 1$
$\alpha(13) = \dots = 0$

2 3 5 7 11 13 17 19 23 29 31 37
1 2 3 4 5 6 7 8 9 10 11 12

$n = 427$

427	7
61	61
1	

$\alpha(1), \alpha(2), \alpha(3) = 0$
$\alpha(4) = 1$
$\alpha(k) = 1$ wobei 61 die k-te Primzahl ist

$\alpha(\ell) = 0$ für $\ell \notin \{4, 14\}$

504	2
252	2
126	2
63	3
21	3
7	7
1	

$\alpha(1) = 3$ $\quad \alpha(3) = 0$

$\alpha(2) = 2$ $\quad \alpha(7) = 1$

$\alpha(14) = 0$ für $14 \notin \{1, 2, 4\}$

504	7
72	3
24	2
12	3
4	2
2	2
1	

egal mit welcher Primzahl ich anfange, $\alpha(i)$ bleibt gleich!

Primfaktorenzerlegung also immer gleich

Beweis) Existenz:

Für alle $n \in \mathbb{N}$ gibt es $\alpha: \mathbb{N} \to \mathbb{N}_0$, das (1) und (2) erfüllt.

Beweis mit Induktion

um 1 zu zerlegen, nehmen wir jede Primzahl 0 x.

Ind. anfang: $n = 1$: Wir setzen $\alpha(k) = 0$ für alle $k \in \mathbb{N}$.

Dann gelten (1) und (2).

Ind. schritt

neue Variante, ich stelle mir vor, dass ich es vorher schon für alle gezeigt habe

$\forall n \in \mathbb{N}: (\forall k \in \{1, \dots, n-1\}: A(k)) \Rightarrow A(n)$ (S)

$A(n) :\Leftrightarrow$ es gibt $\alpha: \mathbb{N} \to \mathbb{N}_0$, das (1) und (2) erfüllt

in (2) kommt das n vor

Wir zeigen nun (S).

Für $(n = 1)$ gilt (S), da $A(1)$ gilt.

Sei nun $n \geq 2$:

Wir nehmen an, dass alle $k \in \{1, \dots, n-1\}$ eine Zerlegung haben

Z.z. Auch n hat eine Zerlegung

Bsp: 240 Hälfte:

240	2
120	2
60	2
30	2
15	3
5	5
1	

$240 = 2^4 \cdot 3^1 \cdot 5$

$480 = 2^5 \cdot 3^1 \cdot 5$

Bsp: 867 Ein Drittel: 289 (geht durch 17)

$289 = 17^2$

$867 = 3 \cdot 17^2$

jetzt legen wir die Bsp in den Beweis um

Sei $q := \min\{t \in \mathbb{N} : t > 1 \text{ und } t \mid n\}$ Zahl ist mind durch n teilbar

Dann gilt $q \in \mathbb{P}$

Denn sei $q = a \cdot b$ mit $a, b \in \mathbb{N}$. Dann gilt $a \mid q$ und $q \mid n$, also $a \mid n$. Wegen der Minimalität von q gilt $a = 1$ oder $a = q$.

Wenn $a = q$, so gilt $b = 1$, also ist q eine Primzahl.

Da $q > 1$, gilt $\frac{n}{q} < n$. Also gibt es nach Induktionsvoraussetzung $\beta : \mathbb{N} \Rightarrow \mathbb{N}_0$, sodass $\frac{n}{q} = \prod_{i \in \mathbb{N}} p_i^{\beta(i)}$

und $\{i \in \mathbb{N} \mid \beta(i) \neq 0\}$ ist endlich.

Da q prim ist, gibt es $k \in \mathbb{N}$, sodass $q = p_k$.

α wird def. als:

$$\alpha(i) := \begin{cases} \beta(i), & \text{wenn } i \in \mathbb{N} \setminus \{k\} \\ \beta(k) + 1, & \text{wenn } i = k \end{cases}$$

$$\frac{n}{q} = p_1^{\beta(1)} \cdots p_{k-1}^{\beta(k-1)} \cdot p_k^{\beta(k)} \cdot p_{k+1}^{\beta(k+1)} \cdots \cdot |q = p_k$$

$n = p_1^{\beta(1)} \cdots p_{k-1}^{\beta(k-1)} \cdot p_k^{\beta(k)+1} \cdot p_{k+1}^{\beta(k+1)} \cdots$

Somit existiert auch eine Zerlegung für n.

Existenz ✓

Eindeutigkeit:

Seien $\gamma, \delta : \mathbb{N} \to \mathbb{N}_0$ so, dass $n = \prod_{\substack{i \in \mathbb{N} \\ \gamma(i) \neq 0}} p_i^{\gamma(i)} = \prod_{\substack{i \in \mathbb{N} \\ \delta(i) \neq 0}} p_i^{\delta(i)}$

Da $n \mid n$, gilt $\prod_{i \in \mathbb{N}} p_i^{\gamma(i)} \mid \prod_{i \in \mathbb{N}} p_i^{\delta(i)}$

also gilt $\forall i \in \mathbb{N} : \gamma(i) \leq \delta(i)$.

Da $\prod_{i \in \mathbb{N}} p_i^{\delta(i)} \mid \prod_{i \in \mathbb{N}} p_i^{\gamma(i)}$, gilt $\delta(i) \leq \gamma(i)$.

D.h. $\delta(i) = \gamma(i)$

Der Satz: „$a \mid b \iff \forall i \; \alpha(i) \leq \beta(i)$"
rechtfertigt auch die ggT-Berechnung durch

$$ggT(a,b) = \prod_{i \in \mathbb{N}} p_i^{\min(\alpha(i), \beta(i))}$$

und die Berechnung des kgVs durch

$$kgV(a,b) = \prod_{i \in \mathbb{N}} p_i^{\max(\alpha(i), \beta(i))}$$

$$a = \prod_{i \in \mathbb{N}} p_i^{\alpha(i)}$$

$$b = \prod_{i \in \mathbb{N}} p_i^{\beta(i)}$$

Er ist außerdem der wichtigste Schritt zum Beweis der <u>Eindeutigkeit</u> der Primfaktorzerlegung.

Kongruenz

3-stelliges Prädikat

$17 \equiv 7 \pmod 5$ „17 ist kongruent zu 7 modulo 5"

$a \equiv b \pmod c :\Leftrightarrow c \mid (a-b)$

$\Leftrightarrow$ a & b haben gleichen Rest bei d. Division durch c.

Anwendung: RSA - Verschlüsselungssystem beruht auf großen Primzahlen.

FUNKTIONEN

5.1. Relationen

Def.: Seien A, B Mengen. Jede Teilmenge von $A \times B$ heißt auch Relation von A nach B.

Bsp: $A = \{W, N, O, S, T, V, B, St, K\}$ ← (Bundesländer Ö.)

$B = \{\text{Donau}, \text{Inn}, \text{Traun}\}$

$R = \{(a,b) \in A \times B \mid \text{In } a \text{ liegt ein Teil des Ufers von } b\}$

$R = \{(O, \text{Donau}), (N, \text{Donau}), (W, \text{Donau}), (T, \text{Inn}), (O, \text{Inn}), (O, \text{Traun}), (St, \text{Traun})\}$

Oft schreibt man für eine Relation $\rho \subseteq A \times B$ auch $a \rho b$ für $(a,b) \in \rho$ ← Rho

$A := \mathbb{R}$, $B := \mathbb{Z}$

$a \rho b :\Leftrightarrow a \in [b, b+1)$.

$\rho = \{(r,z) \in \mathbb{R} \times \mathbb{Z} \mid r \in [z, z+1)\}$.

$(\pi, 3) \in \rho$ weil π im Intervall 3,4 liegt

$(\frac{7}{4}, 1) \in \rho$ $\frac{7}{4}$ liegt im Intervall 1,2

$(\sqrt{2}, 1) \in \rho$

$(-\sqrt{2}, -2) \in \rho$ man nimmt die nächst kleinere ganze Zahl weil $B := \mathbb{Z}$ — 2. Zahl

$(5,5) \in \rho$

$(7{,}2; 7) \in \rho$

ρ = Rho
↳ Relationen

Bsp: $A = \mathbb{N}$ und $B = \mathbb{N}$

Wir definieren eine Relation K durch:

$(a,b) \in K :\Leftrightarrow \exists c \in \mathbb{N}_0 : a + c = b$

$K = \{(a,b) \in \mathbb{N} \times \mathbb{N} \mid \exists c \in \mathbb{N}_0 : a + c = b\} = \{(a,b) \in \mathbb{N} \times \mathbb{N} \mid a \leq b\}$

K ist die „kleiner gleich" Relation

Bsp: $\equiv_5$ (Kongruenz modulo 5) von $\mathbb{Z}$ nach $\mathbb{Z}$

$a \equiv_5 b :\Leftrightarrow \exists c \in \mathbb{Z} : (5 \cdot c = b - a)$

$\equiv_5 = \{(a,b) \in \mathbb{Z} \times \mathbb{Z} : 5 \mid (b-a)\}$ (5 teilt $(b-a)$)

Relation von A nach A $\hat{=}$ (entspricht) Relation auf A

Def: Eine <u>Relation auf A</u> ist eine Teilmenge von $A \times A$.

2 Funktionen

Def.: Seien A, B Mengen, und sei R eine Relation von A nach B. R ist eine funktionale Relation von A nach B, wenn es für alle $a \in A$ genau ein $b \in B$ gibt, sodass $(a,b) \in R$.

Bsp: $A = \{1,2,3\}$ $B = \{a,b,c\}$

$R := \{(1,a), (3,c), (2,c)\}$

Dann ist R eine funktionale Relation von A nach B.

$R(1) = a$
$R(2) = c$
$R(3) = c$

Bsp $A = \mathbb{R}$, $B = \mathbb{R}$

$f := \{(r, \sin(r)) \mid r \in \mathbb{R}\}$

Dann ist f eine funktionale Relation von $\mathbb{R}$ nach $\mathbb{R}$

Bsp: $A = \mathbb{R}$ $B = \mathbb{R}$

$g := \{(\sin(r), r) \mid r \in \mathbb{R}\}$

Für $a = 2$ gibt es kein $b \in \mathbb{R}$ mit $(2, b) \in g$.
Also keine fkt. Relation.

Für $a = 0$ gilt $(0,0), (0,\pi), (0, 2\pi), \ldots \in g$

Def: Seien A, B Mengen, und sei f funktionale Relation von A nach B.
Für $a \in A$ bezeichnen wir mit $f(a)$ dann jenes $b \in B$, das $(a,b) \in f$ erfüllt.

Funktionale Relationen bezeichnen wir auch als Funktionen.

Angeben einer Fkt

(1) Als Menge

$q := \{(x,y) \in \mathbb{Z} \times \mathbb{Z} \mid x \cdot x = y\}$ Quadratfkt

$q = \{(-1,1), (-2,4), (0,0), (1,1), (5,25) \ldots\}$

(2) Durch Zuordnungsvorschrift

$q: \mathbb{Z} \to \mathbb{Z}$

$x \mapsto x^2$

„q ist eine Fkt von $\mathbb{Z}$ nach $\mathbb{Z}$ die jedes x auf x^2 abbildet"

(3) Durch Angabe eines Fkt werten

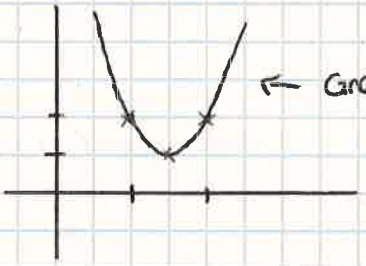
$q : \mathbb{Z} \to \mathbb{Z}, \; q(z) = z^2$ für $z \in \mathbb{Z}$!

(4)... z.B. signaturfkt $sgn : \mathbb{R} \to \mathbb{R}$

$$x \mapsto \begin{cases} -1 & \text{wenn } x < 0 \\ 0 & \text{wenn } x = 0 \\ 1 & \text{wenn } x > 0 \end{cases}$$

$$sgn = \{(x,-1) \mid x \in \mathbb{R}, x<0\} \cup \{(0,0)\} \cup \{(x,1) \mid x \in \mathbb{R}, x>0\}$$

Sei $f : \mathbb{R} \to \mathbb{R}$ mit $f(x) = (x-2)(x-4)+2$ für $x \in \mathbb{R}$



← Graph von $f = \{(x, f(x)) \mid x \in \mathbb{R}\} = f$

eine Fkt ist gleich ihrem Graphen

$f : \mathbb{R} \to \mathbb{R}$ (Zielmenge)

$x \mapsto x^2 + x^3$

$g : \mathbb{N} \to \mathbb{N}$

$x \mapsto x^2 + x^3$

$g = f|_{\mathbb{N}}$ (g ist die Einschränkung von f auf $\mathbb{N}$)

$f|_T = \{(x,y) \in f \mid x \in T\}$ (eingeschränkt auf)

Seien A, B Mengen

$B^A = \{f \mid f \text{ ist Fkt von } A \text{ nach } B\} =$

$\{f \in \mathcal{P}(A \times B) \mid f \text{ ist Fkt von } A \text{ nach } B\}$

Satz) Seien $m, n \in \mathbb{N}$, sei $A = \{1, \dots, m\}$, $B = \{1, \dots, n\}$.
Dann hat B^A genau n^m Elemente.

A	a	1	2	3	4	.....	m
	f(a)	n (Mögl.)	n M.	...			

$\underbrace{n \cdot n \cdot n \cdots n}_{m} = n^m$ Mögl.

$\emptyset^A = \{ f \subseteq A \times \emptyset \mid f \text{ ist Fkt von } A \text{ in } \emptyset \}$

$\emptyset^A = \emptyset$ für $A \neq \emptyset$

$\emptyset$ ist eine Fkt von $\emptyset$ in $\emptyset$

$\emptyset \subseteq \emptyset \times \emptyset$, also ist $\emptyset$ eine Relation von $\emptyset$ nach $\emptyset$.

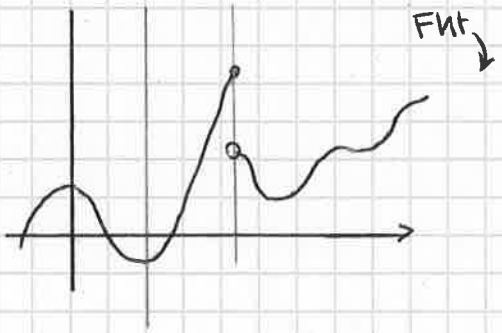
jedes Element $x \in \emptyset$ steht mit genau einem Element aus $\emptyset$ in Relation $\emptyset$.

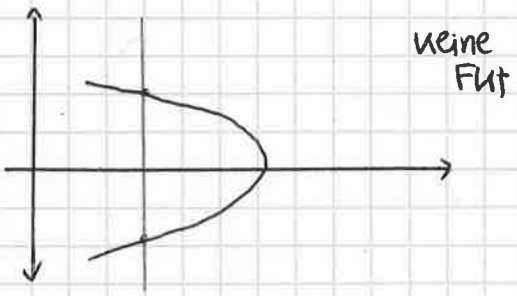
$0^0 = 1$

$0^n = 0 \qquad n \in \mathbb{N}$

$B^\emptyset = \{\emptyset\}$

Funktion von $\mathbb{R}$ nach $\mathbb{R}$





Fkt von $\mathbb{R}$ nach $\mathbb{R}$ sind genau diejenigen Teilmengen des $\mathbb{R} \times \mathbb{R}$, die mit jeder vertikalen Geraden genau einen Schnittpunkt haben.

3. Definitions- und Wertebereich

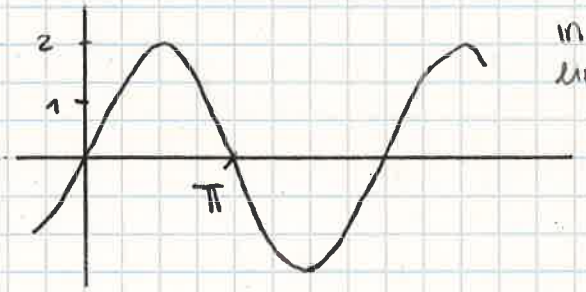
Def: Seien A, B Mengen, und sei f eine Fkt von A nach B. Dann heißt A auch der Definitionsbereich von f.

Der Wertebereich von f ist def durch

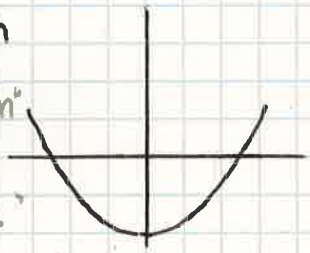
$$f[A] = \{b \in B \mid \exists a \in A : b = f(a)\}$$
$$= \{b \in B \mid \exists a \in A : (a,b) \in f\}$$
$$= \{f(a) \mid a \in A\}$$

$f: \mathbb{R} \to \mathbb{R}, \quad x \mapsto 2\sin(x)$

$f[\mathbb{R}] = \{2\sin(x) \mid x \in \mathbb{R}\} = [-2, 2]$



in $\mathbb{R}$ kann sich ein Wert nicht „durchschwindeln" jeder Wert wird „berührt"



$f: \mathbb{Q} \to \mathbb{Q}$
$x \mapsto x^2 - 2$

Def: Seien A, B Mengen, $\underbrace{f: A \to B}_{f \in B^A}$ „f ist eine Fkt von A nach B"

Sei $T \subseteq A$

Dann ist $f[T] = \{f(t) \mid t \in T\}$

die Bildmenge von T unter f

manchmal nicht eindeutig

Manchmal schreibt man für $f[T]$ auch $f(T)$

Diskrete VO

19.12.

$f: A \to B$, $T \subseteq A$

Bildbereich $f(T) = \{f(t) \mid t \in T\}$

$A = \{1,2,3,4\}$ $B = \{a,b,c\}$

$f = \{(1,a), (2,a), (3,c), (4,a)\}$

$B = \{a,b,c\}$ ist ein Wertevorrat von f

statt „oder" < eine Zielmenge von f

$q_1: \mathbb{Z} \to \mathbb{R}$, $x \mapsto x^2$ $\quad q_2: \mathbb{Z} \to \mathbb{Q}$, $x \mapsto x^2$ $\quad q_3: \mathbb{Z} \to \mathbb{N}_0$, $x \mapsto x^2$

$q_4: \mathbb{Z} \to \{1,2,3\}$, $x \mapsto x^2$ } so ein q_4 gibt es nicht.

$q_1 = \{(x,y) \in \mathbb{Z} \times \mathbb{R} \mid y = x^2\}$

$q_3 = \{(x,y) \in \mathbb{Z} \times \mathbb{N}_0 \mid y = x^2\}$

$q_1 \subseteq q_3$: Sei $(x,y) \in \mathbb{Z} \times \mathbb{R}$ so, dass $y = x^2$.
Da $x \in \mathbb{Z}$, gilt dann $y \in \mathbb{N}_0$. Also gilt $(x,y) \in q_3$.

Bildbereich von $f = f(A) = \{a,c\}$.

$f(\{3,4\}) = \{a,c\}$ $\quad f(\{3\}) = \{c\}$

$f(\{1,2\}) = \{a\}$ $\quad f(\emptyset) = \emptyset$

Satz Seien A,B,C,D Mengen mit $C \subseteq A$, $D \subseteq A$, $f: A \to B$. Dann gilt

(1) $f(C \cup D) = f(C) \cup f(D)$

(2) $f(C \cap D) \subseteq f(C) \cap f(D)$

Bew (1): "⊆": [Wir zeigen $\forall x \in f(C \cup D): x \in f(C) \cup f(D)$]

Sei $x \in f(C \cup D)$. Z.z. $x \in f(C) \cup f(D)$.

Def im Skript: W.w. $x \in \{f(t) \mid t \in C \cup D\}$. Also gibt es $t \in C \cup D$, sodass $x = f(t)$. Da $t \in C \cup D$, gilt $t \in C$ oder $t \in D$.

1. Fall) $t \in C$: Da $t \in C$, gilt $\overbrace{f(t)}^{x} \in f(C)$. Also $x \in f(C) \cup f(D)$

$f(C) = \{f(a) \mid a \in C\}$

$= \{y \mid \exists a \in C: y = f(a)\}$

Also: $t \in C$. Dann gilt $f(t) \in f(C)$

2. Fall) $t \in D$: genau so

"⊇" Sei $x \in f(C) \cup f(D)$. Z.z. $x \in f(C \cup D)$.

Da $x \in f(C) \cup f(D)$, gilt $x \in f(C)$ oder $x \in f(D)$

1. Fall) $x \in f(C)$: Da $x \in f(C)$, gibt es $c \in C$, sodass $x = f(c)$. Da $c \in C$ ist $c \in C \cup D$.

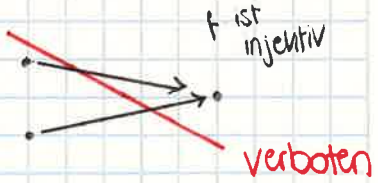
Also gilt $x \in f(C \cup D)$

2. Fall) $x \in f(D)$: genau so

Def: Seien A, B Mengen, sei $f: A \to B$.

(1) f ist <u>injektiv</u>, wenn:

$\forall x, y \in A: f(x) = f(y) \Rightarrow x = y$



Bsp: $f: \mathbb{R} \setminus \{2\} \to \mathbb{R}$

$x \mapsto \frac{x+3}{x-2}$

Behauptung: f ist injektiv

<u>Bew</u>: Seien $x, y \in \mathbb{R} \setminus \{2\}$ so, dass $f(x) = f(y)$ Z.z.: $x = y$

bzw x_1 x_2

W.W. $\frac{x+3}{x-2} = \frac{y+3}{y-2}$

Dann gilt auch $(x+3)(y-2) = (y+3)(x-2)$

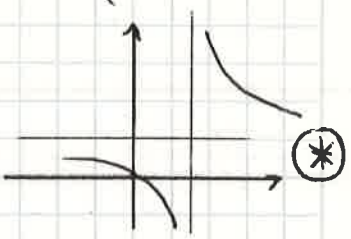
$xy + 3y - 2x - 6 = xy + 3x - 2y - 6$

also $5y = 5x$, also $y = x$

$\frac{x+3}{x-2} = 1$

$0 = 5$ f.

f ist nicht surjektiv auf $\mathbb{R}$



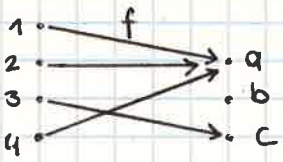
Eine Fkt $f: \mathbb{R} \to \mathbb{R}$ ist genau dann injektiv, wenn ihr Graph mit jeder horizontalen Geraden höchstens einen Schnittpunkt hat.

(2) f ist <u>surjektiv auf B</u>, wenn

$\forall b \in B \; \exists a \in A : b = f(a)$

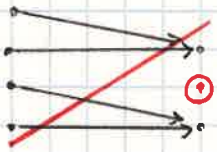
$f = \{(1,a), (2,a), (3,c), (4,a)\}$

$B = \{a, b, c\}$



nicht surjektiv, weil nicht alle Werte erreicht werden (b)

b verdirbt Surjektivität



verboten

„f ist surjektiv auf B"

(*) f ist surjektiv auf $\mathbb{R} \setminus \{1\}$

z.z. $\forall b \in \mathbb{R} \setminus \{1\} \; \exists a \in \mathbb{R} \setminus \{2\} : b = f(a)$

Sei $b \in \mathbb{R} \setminus \{1\}$

Wir suchen nun a mit $f(a) = b$ $\quad \frac{a+3}{a-2} = b$

$$a + 3 = ab - 2b$$

$$a - ab = -3 - 2b$$

$$a \cdot (1 - b) = -3 - 2b$$

$$a = \frac{-3-2b}{1-b}$$ → b darf nicht 1 sein

$$f\left(\frac{-3-2b}{1-b}\right) = \frac{\frac{-3-2b}{1-b} + 3}{\frac{-3-2b}{1-b} - 2} = \dots = b.$$

f ist surjektiv auf $\underbrace{\mathbb{R} \setminus \{1\}}_{!}$.

Diskrete VO

8.1.

Funktionen

z.B.: $f: \mathbb{R} \to \mathbb{R}$

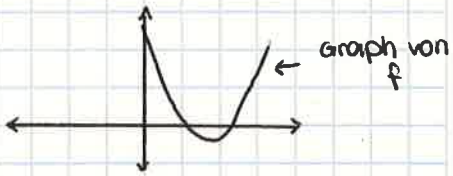
$x \mapsto x^2 - 5x + 6$

$f \subseteq \mathbb{R} \times \mathbb{R}$, d.h., f ist eine Relation von $\mathbb{R}$ nach $\mathbb{R}$

f ist eine Funktion, d.h., $\forall x \in \mathbb{R}\ \exists! y \in \mathbb{R} : (x,y) \in f$

$f = \{(x, x^2-5x+6) \mid x \in \mathbb{R}\}$

= Graph von f



Nicht für jede Relation, sondern nur für Funktionen:

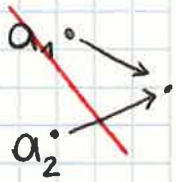
$\underbrace{f(x)}_{\text{f von x}} :=$ jenes $y \in \mathbb{R}$, sodass $(x,y) \in f$.

Funktionen können verschiedene Eigenschaften haben:

$f: A \to B$ ($f \subseteq A \times B$ und f ist Fkt von A nach B)

f ist injektiv:

$\forall a_1, a_2 \in A: f(a_1) = f(a_2) \Rightarrow a_1 = a_2$.



f ist surjektiv: $\Leftrightarrow$ (auf B) $\forall b \in B\ \exists a \in A : b = f(a)$

jede Fkt ist surjektiv auf Wertebereich

Def: $f: A \to B$ ist bijektiv (eine Bijektion von A nach B) $:\Leftrightarrow$ (genau dann wenn) f ist injektiv & surjektiv (auf B).

Bsp] $f: \mathbb{R} \setminus \{3\} \to \mathbb{R} \setminus \{1\}$

$x \longmapsto \frac{x+2}{x-3}$

Behauptung: f ist bijektiv

(1) f ist injektiv:

Seien dazu $x_1, x_2 \in \mathbb{R} \setminus \{3\}$ so, dass $f(x_1) = f(x_2)$

Z.z.: $x_1 = x_2$

W.W. $\frac{x_1+2}{x_1-3} = \frac{x_2+2}{x_2-3}$, also $(x_1+2)(x_2-3) = (x_2+2)\cdot(x_1-3)$

also $x_1x_2 + 2x_2 - 3x_1 - 6 = x_2x_1 + 2x_1 - 3x_2 - 6$

und somit $2x_2 - 3x_1 = 2x_1 - 3x_2$

also $5x_2 = 5x_1$, und folglich $x_1 = x_2$

(2) f ist surjektiv:

Z.z.: $\forall y \in \mathbb{R} \setminus \{1\}\ \exists x \in \mathbb{R} \setminus \{3\}: \quad y = \frac{x+2}{x-3}$

Sei $y \in \mathbb{R} \setminus \{1\}$. Wir versuchen, x zu finden.

$y = \frac{x+2}{x-3} \qquad (x-3)y = x+2 \qquad xy - 3y = x+2$

$xy - x = 3y + 2 \qquad x(y-1) = 3y+2$

$x = \frac{3y+2}{y-1}$

Wir berechnen jetzt für $y \neq 1$:

$f\left(\frac{3y+2}{y-1}\right)$.

$$f\left(\frac{3y+2}{y-1}\right) = \frac{\frac{3y+2}{y-1} + 2}{\frac{3y+2}{y-1} - 3} = \frac{\frac{3y+2+2y-2}{y-1}}{\frac{3y+2-3y+3}{y-1}} = \frac{\frac{5y}{y-1}}{\frac{5}{y-1}}$$

$$= \frac{5y}{y-1} \cdot \frac{y-1}{5} = y$$

Also gibt es ein x mit $f(x) = y$, nämlich

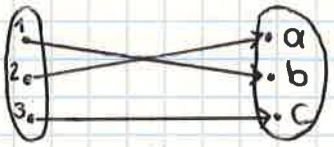
$x = \frac{3y+2}{y-1}$.

$f: \mathbb{R}\setminus\{3\} \to \mathbb{R}\setminus\{1\}$, $x \mapsto \frac{x+2}{x-3}$ $\qquad$ $g: \mathbb{R}\setminus\{1\} \to \mathbb{R}\setminus\{3\}$, $y \to \frac{3y+2}{y-1}$

$A = \{1,2,3\}$ $\qquad$ $B = \{a,b,c\}$

$f = \{(1,b),(2,a),(3,c)\}$

(wenn Fkt bijektiv, kann man sie umdrehen)



bijektiv

$f^{-1} = \{(b,1),(a,2),(c,3)\}$

Satz) Seien A, B Mengen, $f: A \to B$

$g := \{(b,a) \mid (a,b) \in f\}$

Dann sind äquivalent:

(1) g ist eine Fkt von B nach A

(2) f ist bijektiv

Bew: (1) $\Rightarrow$ (2): Wir nehmen an, dass g eine Fkt ist

z.z. f ist bijektiv

Wir zeigen zuerst, dass f surjektiv ist.

z.z.: $\forall b \in B\ \exists a \in A: b = f(a)$, also $\forall b \in B\ \exists a \in A: (a,b) \in f$.

Sei $b \in B$. Da g eine Fkt ist, gilt $(b, g(b)) \in g$.

Also gilt $(g(b), b) \in f$ und somit gilt für $a := g(b)$, dass $f(a) = b$.

Also gibt es $(a',b') \in f$, sodass $(b, g(b)) = (b', a')$.

Dann gilt $b' = b$ und $a' = g(b)$, also wegen $(a',b') \in f$ auch $(g(b), b) \in f$.

Bemerkung: Aus $t(y) \in \{ t(x) \mid x \in B \}$ kann man nicht folgern, dass $y \in B$.

f ist injektiv:

Z.z. $\forall a_1, a_2 \in A : f(a_1) = f(a_2) \Rightarrow a_1 = a_2$

Seien $a_1, a_2 \in A$. Wir nehmen an, dass $f(a_1) = f(a_2)$.

Z.z. $a_1 = a_2$.

W.w. $(a_1, f(a_1)) \in f$ und $(a_2, f(a_2)) \in f$.

Also (nach Def. von g) gilt $(f(a_1), a_1) \in g$ und $(f(a_2), a_2) \in g$. Da g funktional ist, muss also $a_1 = a_2$ gelten weil sonst nicht wie $(x,y) = (x,z)$ wenn $a_1 \neq a_2$ ungleich wären, geht aber g Fkt und $f(a_1) = f(a_2)$

(2) $\Rightarrow$ (1): Ann.: f ist bijektiv.

Z.z. g ist Fkt von B nach A.

~~Z.z.: $\forall b \in B \; \exists! \, a \in A : g(a) = b$~~

~~Sei $b \in B$.~~

~~Wir suchen $a \in A$ mit~~

Diskrete VO

9. Jänner

Fortsetzung 8.1.20

Satz) Seien A, B Mengen, $f: A \to B$.
$g := \{(b,a) \mid (a,b) \in f\}$. Dann sind
äquivalent:

(1) g ist Fkt von B nach A

(2) f ist bij. von A nach B

(2) $\Rightarrow$ (1): Ann.: $f: A \to B$ ist bijektiv

z.z. g ist Fkt von B nach A

z.z. $\forall b \in B \; \exists! \, a \in A : (b,a) \in g$. und $g \subseteq B \times A$

(Def. Fkt / Relation: $h \subseteq X \times Y$; h ist Fkt v. X nach $Y \Leftrightarrow \forall x \in X \; \exists! y \in Y : (x,y) \in h$)

Sei $b \in B$. (b wurde hier fixiert, also kein Quantor nötig)

z.z. bei $\exists!$

Existenz: z.z. $\exists \, a \in A : (b,a) \in g$

Dazu suchen wir ein $a \in A$, sodass $(a,b) \in f$, also $f(a) = b$.
Da f surjektiv ist, gibt es $a \in A$ mit $f(a) = b$, also
$(a,b) \in f$. Dann gilt $(b,a) \in g$.

Eindeutigkeit: z.z. $\forall a_1, a_2 \in A : (b,a_1) \in g$ und $(b,a_2) \in g$
$\Rightarrow a_1 = a_2$

wir zeigen: $\exists! \, a : P(a)$
z.z. $\exists a : P(a)$ Existenz
$\forall a_1, a_2 : P(a_1) \wedge P(a_2) \Rightarrow a_1 = a_2$ Eindeutigkeit

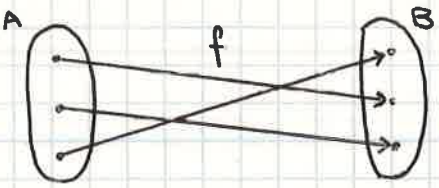
Da $(b,a_1) \in g$, gilt $(a_1,b) \in f$, also $f(a_1) = b$.

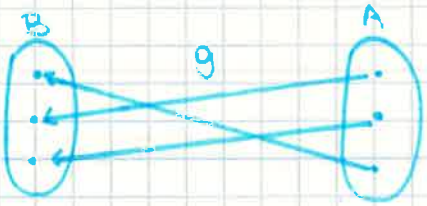
Da $(b,a_1) \in g$, gibt es $(a',b') \in f$, sodass $(b,a_1) = (b',a')$

Also $b = b'$, $a_1 = a'$. Da $(a',b') \in f$, gilt $(a_1,b) \in f$.

Da $(b, a_2) \in g$, gilt $(a_2, b) \in f$, also $f(a_2) = b$
Also gilt $f(a_1) = b = f(a_2)$. Wegen der Injektivität von f gilt $a_1 = a_2$.

graf isch





W.W. f ist bijektiv
Z.Z. g ist Fkt

Def (Umkehrfkt)
Seien A, B Mengen, und sei $f: A \to B$ bijektiv.
Die Fkt $g := \{(b, a) \mid (a, b) \in f\}$ heißt zu f inverse Fkt oder Umkehrfkt von f.
Man bezeichnet diese Fkt g auch mit f^{-1}.

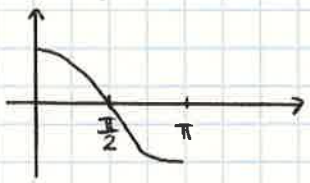
$f(x) = \exp(x) = e^x$
$f = \{(x, e^x) \mid x \in \mathbb{R}\}$

f ist bij von $\mathbb{R}$ nach $\mathbb{R}^+ = \{r \in \mathbb{R} \mid r > 0\} =]0; \infty[$.

$f^{-1} = \{(e^x, x) \mid x \in \mathbb{R}\} = \{(z, \log(z)) \mid z \in \mathbb{R}^+\}$
(gl. Elemente / gl. Mengen; $\mathbb{R}^+$ ∈ Bildbereich)

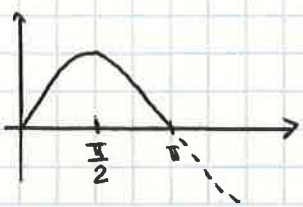
Wir berechnen nun $f^{-1}(z)$ für $z \in \mathbb{R}^+$
$u = \log(z)$
$u = f^{-1}(z) \iff (z, u) \in f^{-1} \iff (u, z) \in f \iff z = e^u$
$u = \log(z)$

cos:



$\cos: [0; \pi] \to [-1; 1]$ bij

sin:



$\sin: [0; \pi] \to [-1; 1]$
weder surj. noch inj

weil log in $\mathbb{R}^+$ def?!

Beh: $\{(e^x, x) \mid x \in \mathbb{R}\} = \{(z, \log(z)) \mid z \in \mathbb{R}^+\}$

Bew: Sei $p \in \{(e^x, x) \mid x \in \mathbb{R}\}$

$a \in \{t(x) \mid x \in X\}$ Dann gibt es $x \in X$ mit $a = t(x)$

"$\subseteq$" Also gibt es $x \in \mathbb{R}$, sodass $p = (e^x, x)$. Sei $z := e^x$.

Dann gilt $\log(z) = \log(e^x) = x$

Es gilt $z \in \mathbb{R}^+$ und $p = (e^x, x) = (z, \log(z))$.

Also gilt $p \in \{(z, \log(z)) \mid z \in \mathbb{R}^+\}$

"$\supseteq$" Sei $p \in \{(z, \log(z)) \mid z \in \mathbb{R}^+\}$ (wobei)

Also gibt es $z \in \mathbb{R}^+$ mit $p = (z, \log(z))$

Sei $x := \log(z)$

Dann gilt $e^x = e^{\log(z)} = z$.

Da $p = (z, \log(z))$, gilt $p = (e^x, x)$.

Somit liegt p in der linken Seite.

$\{t(x) \mid x \in A\}$ wobei

$\{x \mid P(x)\}$ für die gilt

Eig: Sei $a \in [1,3] = A$

Es gilt: $(-2)^2 \in A$

Also $(-2) \in [1,3]$ ↯

Blödsinn!

Richtig: Also gibt es $a \in [1,3]$ sodass $(-2)^2 = a^2$

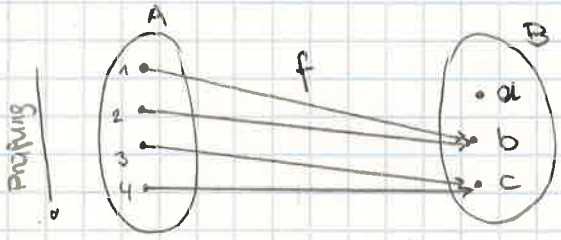
Buch: Halmos Naive Mengenlehre

Def (Urbild)

Sei $f: A \to B$, $D \subseteq B$ $f^{-1}(D)$

$f^{-1}[D] := \{x \in A \mid f(x) \in D\}$

hat nichts mit Umkehrfkt zu tun



Prüfung

- Was ist das Bild v $\{1,3\}$?
- $f(\{1,3\}) = \{b, c\}$

$f^{-1}(\{a,b\}) = \{x \in A \mid f(x) \in \{a,b\}\}$

$= \{1,2\}$

$f^{-1}(\{a\}) = \emptyset$

$f^{-1}(\emptyset) = \emptyset$

Familien & Folgen

$h = \left(\frac{1}{n}\right)_{n \in \mathbb{N}}$ $\quad h = (1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \frac{1}{5}, \ldots)$

Was ist h?

Antw: h ist eine Fkt von $\mathbb{N}$ nach $\mathbb{R}$.
Es gilt $h(n) = \frac{1}{n}$ für alle $n \in \mathbb{N}$.

Def: Seien I, X Mengen, sei x eine Fkt von I nach X. Wir schreiben oft x_i für $x(i)$.

Wir definieren

$\langle x_i \mid i \in I \rangle := \{(i, x_i) \mid i \in I\}$
$= \{(i, x(i)) \mid i \in I\}$

$\langle x_i \mid i \in I \rangle$: die Folge aller x_i ...

"Folge der x_i, wobei $i \in I$"

Es gilt $x = \langle x_i \mid i \in I \rangle$

Wir können h auch so angeben:

$h: \mathbb{N} \to \mathbb{R}$
$x \mapsto \frac{1}{x}$

Für Folgen bevorzugen wir $h = \underbrace{\langle \frac{1}{n} \mid n \in \mathbb{N} \rangle}_{\left(\frac{1}{n}\right)_{n \in \mathbb{N}}}$ schreibweise um Indizes zu vermeiden; gleichbedeutend

Diskrete VO

15.1.

Folgen

$a = ((1+\frac{1}{n})^n)_{n \in \mathbb{N}}$

$a(1) = 2 \quad a(2) = 2{,}25 \ldots$

$\lim_{n \to \infty} a(n) =: e$

$f(x) = e^x$

$f'(x) = e^x$

Die FKt $f(x) = e^x$ ist die Lösung der Differentialgleichung $f'(x) = f(x)$ für alle $x \in \mathbb{R}$, $f(0) = 1$.

$$a = ((1+\tfrac{1}{n})^n)_{n \in \mathbb{N}}$$
$$= \langle (1+\tfrac{1}{n})^n \mid n \in \mathbb{N} \rangle$$
$$= \{(n, (1+\tfrac{1}{n})^n) \mid n \in \mathbb{N}\}$$

Eine andere Art, a anzugeben, ist $a: \mathbb{N} \to \mathbb{R}$, $n \mapsto (1+\frac{1}{n})^n$.

Wir schreiben auch a_n für $a(n)$.

a_1 / $a(1)$ \ die Var a_1 (neues Symbol)

(a mit dem Index 1 kann also verschiedenes bedeuten bzw eine andere FKt haben.)

Tupel werden ähnlich erklärt:

Def: Sei A Menge, $n \in \mathbb{N}$. Mit dem n-Tupel $\langle a_1, \ldots, a_n \rangle$ meinen wir die Familie $\langle a_i \mid i \in \{1, \ldots, n\} \rangle$

Daher gilt

$$\langle a_1, \ldots, a_n \rangle = \langle a_i \mid i \in \{1, \ldots, n\} \rangle$$
$$= \{(i, a_i) \mid i \in \{1, \ldots, n\}\}$$

$\langle -5, 2, 3 \rangle = v$ $\quad v: \{1,2,3\} \to \mathbb{R}$

$v(1) = -5$

$v(2) = 2$

$v(3) = 3$

Vektoren in der Mengenlehre

$$\mathbb{R}^3 = \{\langle x,y,z\rangle \mid x,y,z \in \mathbb{R}\} = \{f \mid f: \{1,2,3\} \to \mathbb{R}\} = \mathbb{R}^{\{1,2,3\}}$$

Wir schreiben für $\langle 1,-5,9\rangle$ auch $(1,-5,9)$ oder $\begin{pmatrix}1\\-5\\9\end{pmatrix}$.

$(-7,3)$ hat jetzt zwei Bedeutungen:

- $(-7,3)$ kann das Paar aus -7 und 3 sein, also
  $(-7,3) = \{\{-7\},\{-7,3\}\} \in \mathbb{R}\times\mathbb{R}$
- $(-7,3)$ kann der Vektor $\langle -7,3\rangle$ sein, also die Fkt
  $\{(1,-7),(2,3)\} = \{\{\{1\},\{1,-7\}\},\{\{2\},\{2,3\}\}\} \in \mathbb{R}^2$.

Def. Für eine Menge A und $n \in \mathbb{N}$ ist

$$A^n := \{\langle a_1,\dots,a_n\rangle \mid a_1,\dots,a_n \in A\} = \{a \mid a: \{1,\dots,n\} \to A\} = A^{\{1,\dots,n\}}$$

Bsp.: $\mathbb{R}^3 = \{\begin{pmatrix}x\\y\\z\end{pmatrix} \mid x,y,z \in \mathbb{R}\}$

$$\mathbb{R}^2 = \{\langle a,b\rangle \mid a,b \in \mathbb{R}\} = \mathbb{R}^{\{1,2\}} \quad \| \quad \mathbb{R}\times\mathbb{R} = \{(a,b) \mid a,b \in \mathbb{R}\}$$

Frage: Was ist $\mathbb{R}\times\mathbb{R}\times\mathbb{R}$? — $(\mathbb{R}\times\mathbb{R})\times\mathbb{R}$, $\mathbb{R}\times(\mathbb{R}\times\mathbb{R})$, $\mathbb{R}^3$ — also nicht eindeutig weil nicht dasselbe •

$$\langle 5,4\rangle = \{(1,5),(2,4)\} = \{\{1\},\{1,5\}\},\{\{2\},\{2,4\}\}\}$$
$$(5,4) = \{\{5\},\{5,4\}\}$$
Paare

~~Folge~~ Familie = Funktion

$$(a_n)_{n\in\mathbb{N}} := \left((1+\tfrac{1}{n})^n\right)_{n\in\mathbb{N}} = \langle (1+\tfrac{1}{n})^n \mid n \in \mathbb{N}\rangle = a,$$

wobei $a: \mathbb{N} \to \mathbb{R},\ x \mapsto (1+\tfrac{1}{x})^x$

Familie = Folgen mit einer anderen Indexmenge

Folgen = Familien mit Indexmenge $\mathbb{N}$
= Fkt mit Definitionsbereich $\mathbb{N}$.

(S.58)!

> Sei $f := (\sin(x))_{x \in \mathbb{R}}$. Bestimme die Abl. von f.
> $f' = \langle \cos(x) \mid x \in \mathbb{R} \rangle$

> Sei $a: \mathbb{N} \to \mathbb{R}$, $a(n) = \frac{n^2}{2n^2+n}$. Bestimmen Sie den Grenzwert von a
> $\lim_{n \to \infty} a(n) = \frac{1}{2}$

. Sei $f: \mathbb{R} \to \mathbb{R}$ gegeben durch $f(x) = \sin(x)$ für $x \in \mathbb{R}$
Bestimmen Sie f'

. Sei $(a_n)_{n \in \mathbb{N}}$ die Folge aus $\mathbb{R}$, die durch $a_n = \frac{n^2}{2n^2+n}$ für $n \in \mathbb{N}$ gegeben ist....

bzw.: Sei $a = \left(\frac{n^2}{2n^2+n}\right)_{n \in \mathbb{N}}$

$a = \{(n, (1+\frac{1}{n})^n) \mid n \in \mathbb{N}\}$

Sichtweise: als Fkt

$\mathbb{N}$... Definitionsbereich $\parallel$ $x \in \mathbb{N}$ ist ein Argument
$\mathbb{R}$... eine Zielmenge
$\{(1+\frac{1}{n})^n \mid n \in \mathbb{N}\}$ ... Wertebereich von a
$a: \mathbb{N} \to \mathbb{R}$, $n \mapsto (1+\frac{1}{n})^n$

} Fkt

als Familie:

$\mathbb{N}$ ... Indexmenge ($x \in \mathbb{N}$ ist ein Index)
a ist eine Familie aus $\mathbb{R}$
$\{(1+\frac{1}{n})^n \mid n \in \mathbb{N}\}$ ist eine durch n indizierte Menge
$a = ((1+\frac{1}{n})^n)_{n \in \mathbb{N}}$

jede Fkt ist eine Familie
Δ umgekehrt nur anders Blickweise

Folgen sind Fkt mit Def.bereich $\mathbb{N}$ (oder $\mathbb{N}_0$).
Familien und Funktionen sind das gleiche
Folgen sind Familien mit Indexmenge $\mathbb{N}$

$a(3)$

als Fkt: $a(3)$ ist der Fkt-wert an der Stelle 3

als Fam.: $a(3) = a_3$ ist der von 3 indizierte Wert d. Folge, das 3 Folgenglied

$(3, (1+\frac{1}{3})^3)$ ist ein Element der Folge

↯↯ falsch: $(1+\frac{1}{3})^3$ ist Element d. Folge ↯

Sei $n \in \mathbb{N}$

n-Tupel sind Funktionen mit Def. bereich $\{1, \dots n\}$

n-Tupel von reellen Zahlen sind Fkt von $\{1, \dots, n\}$ nach $\mathbb{R}$.

n-Tupel sind Familien mit Indexmenge $\{1, \dots n\}$

n-Tupel reeller Zahlen sind Familien aus $\mathbb{R}$ mit Indexmenge $\{1, \dots n\}$

Kartesische Produkte

Def: Sei $(X_i)_{i \in I}$ eine mit I indizierte Familie von Mengen.
(d.h. für jedes $i \in I$ ist X_i eine Menge).

$$\prod_{i\in I} X_i := \{ x : I \to \bigcup \{X_i \mid i \in I\} \mid \forall i \in I : x(i) \in X_i \}$$

$$= \{(x_i)_{i\in I} \mid (x_i)_{i\in I} \text{ ist eine Familie mit Indexmenge } I \text{ und der Eigenschaft } \forall i \in I : x_i \in X_i\}$$

<u>Bsp</u> Für $i \in \mathbb{N}$ sei $A_i := \{i-1, i\}$.

Sei $f: \mathbb{N} \to \mathbb{R}$,

$n \mapsto 2 \cdot \lfloor \frac{n}{2} \rfloor$.

$\prod_{i\in\mathbb{N}} A_i = A_1 \times A_2 \times A_3 \ldots$

Dann gilt $f \in \prod_{i\in\mathbb{N}} A_i$

$(f(i))_{i\in\mathbb{N}} \in \prod_{i\in\mathbb{N}} A_i$

Frage: Gibt es ein weiteres Element von $\prod_{i\in\mathbb{N}} A_i$?

Ja: $f(n) = n$ für alle $n \in \mathbb{N}$. (& auch $n-1$ usw.)

$I = \{1,2\}$ $A_1 = \mathbb{R}$ $A_2 = \mathbb{R}$

Ges.: Ein Element aus $\prod_{i\in\{1,2\}} A_i$

ges.: Fkt von $\{1,2\}$ nach $\mathbb{R}$

Bsp: $\langle 5{,}3 , \frac{\pi}{2} \rangle \in \prod_{i\in\{1,2\}} A_i$

2-Tupel ≠ Paar!

Diskrete VO

16.1.

Geben Sie jeweils ein Element der folgenden Mengen an!

- $\mathbb{R}^{\mathbb{N}} = \{f \mid f: \mathbb{N} \to \mathbb{R}\}$ $\qquad B^A = \{f \mid f: A \to B\}$

Sei $f: \mathbb{N} \to \mathbb{R}$

$x \mapsto \sqrt{x}$

Dann gilt $f \in \mathbb{R}^{\mathbb{N}}$ $\left(f = \{(x, \sqrt{x}) \mid x \in \mathbb{N}\} \in \mathbb{R}^{\mathbb{N}}\right)$

- $\mathbb{N}^{\mathbb{R}}$ $\qquad g: \mathbb{R} \to \mathbb{N}$

$x \mapsto \left\lfloor \frac{|x|}{2} \right\rfloor \cdot 2 + 1$ $\qquad$ (o. $\lfloor |x| \rfloor + 1$)

(o. $n: \mathbb{R} \to \mathbb{N}$, $n(r) = \lceil r^2 + 1 \rceil$)

Dann gilt $g \in \mathbb{N}^{\mathbb{R}}$.

$\lfloor x \rfloor := \max \{n \in \mathbb{Z} \mid n \leq x\} = [x]$ floor nächstkleinere

$\lceil x \rceil := \min \{m \in \mathbb{Z} \mid n \geq x\}$ ceiling nächstgrößere

$rd(x) := \lfloor x + \frac{1}{2} \rfloor$ runden!?

- $\mathbb{R}^3$

$\langle 1, 2, 3 \rangle \in \mathbb{R}^3$ (Vektor)

Für $i \in \mathbb{N}$ sei $A_i := [2i, 2i + \frac{1}{i}]$

$A_1 = [2, 3]$ $\quad A_2 = [4, 4\frac{1}{2}]$ $\quad A_3 = [6, 6\frac{1}{3}]$, ...

- $\prod_{i \in \mathbb{N}} A_i$ enthält als Element Folgen $= \{(a_i)_{i \in \mathbb{N}} \mid \forall i \in \mathbb{N}: a_i \in A_i\}$ Familie

$a_1 = 2$, $a_2 = 4$ $\quad a_n = 2n$

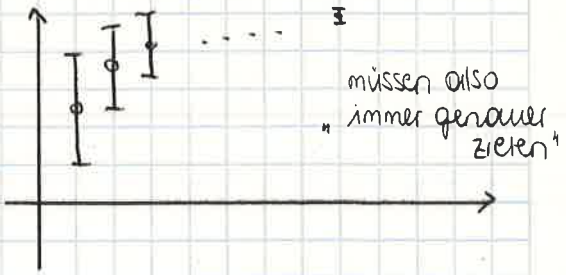
Sei $a: \mathbb{N} \to \mathbb{R}$, $a(x) = 2x$ für $x \in \mathbb{R}$.

Dann gilt $a \in \prod_{i \in \mathbb{N}} A_i$.

$b = (2n + \frac{1}{n})_{n \in \mathbb{N}}$ $\quad b \in \prod_{i \in \mathbb{N}} A_i$

$B_i :=]i, i + \frac{1}{i}[= \{x \in \mathbb{R} \mid i < x < i + \frac{1}{i}\}$

Ges.: $c \in \prod_{i \in \mathbb{N}} B_i$



Sei $c: \mathbb{N} \to \mathbb{R}$ (wählen wir selbst)

$n \mapsto n + \frac{1}{n+1}$

Dann gilt $c \in \prod_{i \in \mathbb{N}} B_i$

Sei $d: \mathbb{N} \to \mathbb{R}$

$m \mapsto m + \frac{1}{2m}$. Dann gilt $d \in \prod_{i \in \mathbb{N}} B_i$

Für $i \in \mathbb{N} \setminus \{3\}$ sei $A_i = \mathbb{R}$. $\quad A_3 := \emptyset$

Gesucht ist ein Element in $\prod_{i \in \mathbb{N}} A_i$

$c: \mathbb{N} \to \mathbb{R}$. Wenn $c \in \prod_{i \in \mathbb{N}} A_i$, so gilt $c(3) \in \emptyset$. (das ist das Problem!)

Das ist falsch, also kann es so ein c nicht geben.

↳ $\mathbb{R} \times \emptyset = \emptyset$

$\mathbb{R} \times \mathbb{R} \times \emptyset \times \mathbb{R} \times \mathbb{R} \times \ldots$

$\prod$

Gibt es eine Folge $(A_i)_{i \in \mathbb{N}}$ von Mengen, sodass (1) $\prod_{i \in \mathbb{N}} A_i$ leer ist, und (2) jedes A_i nicht leer ist.

Durch die Axiome der Mengenlehre nicht festgelegt

Alle A_i nicht leer

$A_1 \times A_2 \times A_3 \times \ldots$

$a: \mathbb{N} \to \bigcup_{i \in \mathbb{N}} A_i$

$a(i) :=$ ein Element von A_i

↳ Definiert das eine Fkt a? Nein

Auswahlaxiom

Axiom Sei $(X_i)_{i \in I}$ eine Familie von nicht leeren Mengen. Dann gibt es ein f mit Def. bereich I, sodass $f \in \prod_{i \in I} X_i$.

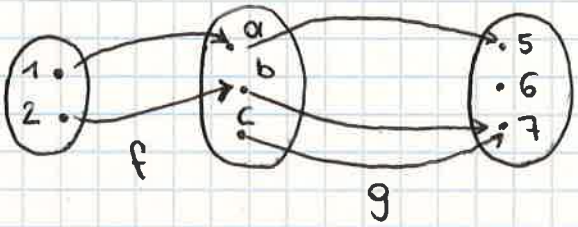
(f: eine Funktion; $f: I \to \bigcup_{i \in I} X_i$)

5.5. Hintereinanderausführung von Funktionen

Def: Seien A, B, C Mengen, sei f eine Fkt von A nach B, sei g eine Fkt von B nach C. Wir definieren $g \circ f$ durch

$$g \circ f : A \to C$$
$$a \mapsto g(f(a))$$

„g nach f"



$g \circ f(1) = g(f(1)) = g(a) = 5$

$g \circ f(2) = g(f(2)) = g(b) = 7$

$f: \mathbb{R} \to \mathbb{R}$, $x \mapsto x+3$ $\qquad$ $g: \mathbb{R} \to \mathbb{R}$, $x \mapsto x^2$

$g \circ f(x) = g(f(x)) = g(x+3) = (x+3)^2$

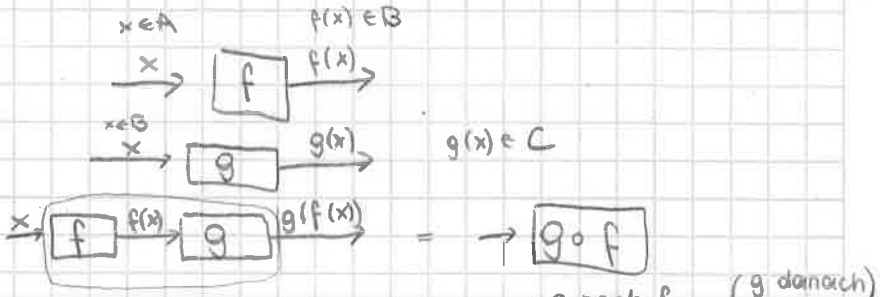
$f \circ g(x) = f(g(x)) = f(x^2) = x^2 + 3$

Satz: Seien A, B, C, D Mengen, $f: A \to B$, $g: B \to C$, $h: C \to D$. Dann gilt

$$h \circ (g \circ f) = (h \circ g) \circ f$$

$h \circ (g \circ f)$

$C \to D$; $B \to C$; $A \to B$; $A \to C$; $A \to D$



g nach f (g danach)

$h \circ (g \circ f)$ und $(h \circ g) \circ f$ sind beides Funktionen von A nach D.

Zwei Fkt von A nach D sind gleich, wenn sie für alle $a \in A$ den gleichen Fkts.wert haben.

$f: \mathbb{R} \to \mathbb{R}$, $x \mapsto (x+2)^2$ $\qquad$ $g: \mathbb{R} \to \mathbb{R}$, $x \mapsto x^2 + 4x + 4$

Es gilt $f = g$.

gl. Def.bereich + werte dann gleich

Sei $a \in A$.

$h \circ (g \circ f)(a) = h(g \circ f(a)) = h(g(f(a)))$.

(an der Stelle a)

$(h \circ g) \circ f(a) = h \circ g(f(a)) = h(g(f(a)))$.

$f: A \to B$

$g: B \to C$

$f \circ g(b) = f(\underbrace{g(b)}_{\in C})$

(zunächst) nicht definiert

Satz Seien A, B Mengen, und sei $f: A \to B$ bijektiv.
Sei $f^{-1} = \{(b,a) \mid (a,b) \in f\}$.
Dann gilt $f \circ f^{-1} = id_B$ und $f^{-1} \circ f = id_A$

id_B = identische Fkt auf B

Beweis: Sei $b \in B$. Z.z. $f \circ f^{-1}(b) = b$.
Da f surjektiv ist, gibt es a mit $(a,b) \in f$.
Dann gilt $(b,a) \in f^{-1}$, also $a = f^{-1}(b)$.
Somit gilt $f(a) = f(f^{-1}(b))$, und wegen $(a,b) \in f$
gilt $f(a) = b$.

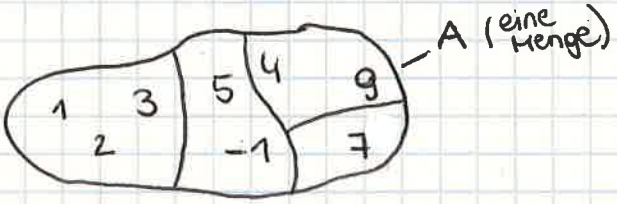
Sei $a \in A$. Z.z. $f^{-1} \circ f(a) = a$

Dokumentenname für Bsp:
UE - DM19 - B08 - Bauer.pdf

Stoff: Skript + Übungen
Theoriefragen kommen, Sätze,...

6. RELATIONEN

6.1. Äquivalenzrelationen



$1 \neq 2$
1 & 2 sind äquivalent
$1 \equiv_\rho 2$. 1 ist äquivalent zu 2 bezüglich ρ.
(ρ ↑ Rho)

$\rho = \{(1,1), (1,2), (1,3), (2,1), (2,2), (2,3), (3,1), (3,2), (3,3),$ 1. Kl. – 9 Elemente
$(5,5), (5,-1), (-1,-1), (-1,5),$ 4 Elemente
$(4,4), (4,9), (9,4), (9,9),$ 4 Elemente
$(7,7)\}$ 1 Element

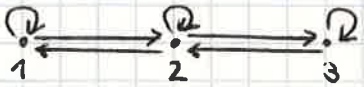
Was ist ρ für ein Objekt?
$\rho \subseteq A \times A$ bzw $\rho \in \mathcal{P}(A \times A)$. ρ ist also eine Relation auf A.

- $\forall a,b \in A : (a,b) \in \rho \Rightarrow (b,a) \in \rho$ ← besser! } ρ ist symmetrisch
  $(\forall (a,b) \in \rho : (b,a) \in \rho)$

- $\forall a \in A : (a,a) \in \rho$ } ρ ist reflexiv.

hat eig. 7 Elemente weil 2× (2,2)

$$\rho = \{(1,2), (2,1), (1,1), (2,2), (2,3), (3,2), (2,2), (3,3)\}$$



⇒ ρ ist nicht transitiv!

- $\forall a,b,c \in A : ((a,b) \in \rho \wedge (b,c) \in \rho) \Rightarrow (a,c) \in \rho)$

↳ ρ ist transitiv

Def: sei $\rho \subseteq A \times A$. ρ ist eine <u>Äquivalenzrelation</u> auf A, wenn ρ reflexiv, symmetrisch und transitiv ist.

Bsp: Äquivalenzklasse von 5 bzgl. ρ:

$[5]_\rho = \{5, -1\}$ $\quad [9]_\rho = \{9,4\}$

$[4]_\rho = \{9,4\}$

Def: sei ρ Äquivalenzrelation auf A, sei $a \in A$. Die Äquivalenzklasse von a bzgl. ρ ist def. durch $[a]_\rho := \{b \in A \mid (a,b) \in \rho\}$

$[a]_\rho = a/\rho$.

$C \subseteq A$ ist eine Äquivalenzklasse bzgl. ρ, wenn es ein $a \in A$ gibt, sodass $C = a/\rho$.

in unserem Bsp.: 4 Klassen!

Lemma: Sei ρ eine Äquivalenzrelation auf A, und seien $a, b \in A$. Wenn $(a,b) \in \rho$, so gilt $[a]_\rho = [b]_\rho$

Bew: Wir nehmen an, dass $(a,b) \in \rho$ und zeigen $[a]_\rho = [b]_\rho$.

Wir zeigen zunächst $[a]_\rho \subseteq [b]_\rho$

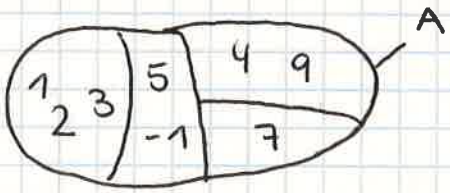
Sei $x \in [a]_\rho$. Z.z. $x \in [b]_\rho$.

Da $x \in [a]_\rho$, gilt $(a,x) \in \rho$ (siehe Def). Da $(a,b) \in \rho$, gilt auch $(b,a) \in \rho$.

Weil ρ transitiv ist, gilt $(b,x) \in \rho$, und somit $x \in [b]_\rho$.

"$\supseteq$" so ähnlich

2. Partitionen



eg geht auch $\{\{1,2,3\},\{5,-1\},\{4,9\},\{7\},\emptyset\}$

* wollen wir aber verbieten

variable
$\mathcal{P} = \{\{1,2,3\},\{5,-1\},\{4,9\},\{7\}\}$.

$\mathcal{P} \subseteq \mathcal{P}(A)$, also $\mathcal{P} \in \mathcal{P}(\mathcal{P}(A))$

Potenzmenge

$Q := \{\{1,2,3\},\{3,5\},\{9\}\}$

Def: Sei A eine Menge. Eine Teilmenge $\mathcal{P}$ von $\mathcal{P}(A)$ ist eine <u>Partition</u> von A :$\Leftrightarrow$

(1) $\forall P \in \mathcal{P} : P \neq \emptyset$.

(2) $\bigcup \{P \mid P \in \mathcal{P}\} = A$ *

(3) $\forall P_1, P_2 \in \mathcal{P} : P_1 \neq P_2 \Rightarrow P_1 \cap P_2 = \emptyset$ *

$\forall a \in A \; \exists P \in \mathcal{P} : a \in P.$ * äquivalent

$\forall a \in A \; \forall P, Q \in \mathcal{P} : (a \in P \wedge a \in Q) \Rightarrow P = Q$ * äquivalent

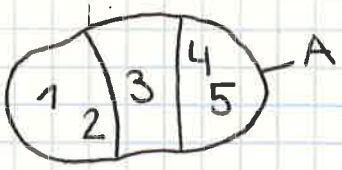
* $\forall P \in \mathcal{P} : P \neq \emptyset$

Bsp: $\bigcup \{\{1,2,3\}, \{5,-1\}, \{4,9\}, \{7\}\}$

$= \{1,2,3,5,-1,4,9,7\}$

Diskrete VO

23.01.



Äquivalenzrelation ÄR

$\alpha = \{(1,1), (1,2), (2,1), (2,2), (3,3), (4,4), (4,5), (5,4), (5,5)\}$

α ist ÄR auf A $\Leftrightarrow$ $\forall a \in A : (a,a) \in \alpha$ (α ist reflexiv)

$\forall a,b \in A : (a,b) \in \alpha \Rightarrow (b,a) \in \alpha$ (α ist symm.)

$\forall a,b,c \in A : ((a,b) \in \alpha \wedge (b,c) \in \alpha) \Rightarrow (a,c) \in \alpha$

Partition

$\mathcal{A} = \{\{1,2\}, \{3\}, \{4,5\}\}$

$\mathcal{A}$ ist Partition von A $\Leftrightarrow$ $\mathcal{A} \subseteq \mathcal{P}(A)$, (oder heißt das Potenzmenge?!)

$\forall P \in \mathcal{A} : P \neq \emptyset$,

$\bigcup \{P \mid P \in \mathcal{A}\} = A$ $(\bigcup \mathcal{A} = A)$

$\forall P_1, P_2 \in \mathcal{A} : P_1 \neq P_2 \Rightarrow P_1 \cap P_2 = \emptyset$.

Menge von der Menge Menge Elemente: schöne Buchstaben! Großbuchst. Kleinbuchst.

Zur besseren Verständlichkeit, benennen wir die Var. um

$\mathcal{B}$ ist Partition von A $:\Leftrightarrow$ $\mathcal{B} \subseteq \mathcal{P}(A)$

$\forall K \in \mathcal{B} : K \neq \emptyset$

$\bigcup \{K \mid K \in \mathcal{B}\} = A$

$\forall K, L \in \mathcal{B} : K \cap L \neq \emptyset \Rightarrow K = L$

Faktormenge:

Die Faktormenge von A bzgl. der Äquivalenzrelation α ist die Menge der Äquivalenzklassen von α.

Def: Sei A Menge, $\alpha \subseteq A \times A$ eine ÄR auf A. Dann ist die Faktormenge A/α def. durch

$$A/\alpha := \{[x]_\alpha \mid x \in A\}.$$

A/α „A nach α"

Bsp: $A/\alpha = \{[1]_\alpha, [2]_\alpha, [3]_\alpha, [4]_\alpha, [5]_\alpha\} =$

$= \{\{1,2\}, \{1,2\}, \{3\}, \{4,5\}, \{4,5\}\} =$

$= \{\{1,2\}, \{3\}, \{4,5\}\} = \{[1]_\alpha, [3]_\alpha, [5]_\alpha\}$

$= \{[2]_\alpha, [3]_\alpha, [5]_\alpha\}$

$|A/\alpha| = \#A/\alpha$

$|A/\alpha| = 3$ (3 Elemente)

Satz) Sei α ÄR auf A. Dann ist A/α eine Partition von A.

$A = \{1,2,3,4,5,6\}$

$\mathcal{A} = \{\{1,6\}, \{2,5\}, \{3,4\}\}$

$\alpha = \{(1,1), (1,6), (6,1), (6,6), (2,5), (2,2), (5,2), (5,5), (3,4), (3,3), (4,3), (4,4)\}$

$\mathcal{B}$ Partition von B

β ÄR auf B, die zu $\mathcal{B}$ gehört:

$(x,y) \in \beta :\Leftrightarrow$ es gibt $P \in \mathcal{B}$, sodass $x \in P$ und $y \in P$

$\beta \subseteq B \times B$

($(x,y) \in \beta :\Leftrightarrow$ x und y sind beide Element des gleichen $P \in \mathcal{B}$.)

sei B eine Menge, und ...

Satz: ...sei $\mathcal{B}$ eine Partition von B. Dann ist

$\beta = \{(x,y) \in B \times B \mid \exists P \in \mathcal{B} : x \in P \text{ und } y \in P\}$

eine Äquivalenzrelation auf B.

Schreibweise: β ÄR $(x,y) \in \beta \Leftrightarrow x \equiv_\beta y$ (passiver Satz) $(\Leftrightarrow x \beta y)$

Außerdem gilt $B/\beta = \mathcal{B}$

Beweis: z.z. β ist ÄR auf B.

(1) $\beta \subseteq B \times B$ ✓ so definiert

(2) z.z. β ist refl., symm., trans.

Reflexivität: $\forall b \in B : (b,b) \in \beta$

Sei $b \in B$. Da $\mathcal{B}$ Partition ist, gilt $\bigcup \{P \mid P \in \mathcal{B}\} = B$

Da $b \in B$, gilt also $b \in \bigcup \{P \mid P \in \mathcal{B}\}$. Also gibt es $P \in \mathcal{B}$ mit $b \in P$. Nach der Def. von β gilt also $(b,b) \in \beta$.

Symmetrie: $\forall a,b \in B : (a,b) \in \beta \Rightarrow (b,a) \in \beta$

Sei $a,b \in B$. Wir nehmen an, dass $(a,b) \in \beta$.

z.z. $(b,a) \in \beta$. Da $(a,b) \in \beta$, existiert $P \in \mathcal{B}$, sodass $a \in P$ und $b \in P$. Also gilt $b \in P$ und $a \in P$, und folglich $(b,a) \in \beta$.

Transitivität: $\forall a,b,c \in B : ((a,b) \in \beta \wedge (b,c) \in \beta) \Rightarrow (a,c) \in \beta$.

Seien $a,b,c \in B$. Wir nehmen an, dass $(a,b) \in \beta$ und $(b,c) \in \beta$.

z.z. $(a,c) \in \beta$.

Da $(a,b) \in \beta$, gibt es $P \in \mathcal{B}$, sodass $a \in P$ und $b \in P$.

Da $(b,c) \in \beta$, gibt es $Q \in \mathcal{B}$, sodass $b \in Q$ und $c \in Q$.

Es gilt $b \in P \cap Q$. Folglich $P \cap Q \neq \emptyset$.

Da $\mathcal{B}$ Partition ist, gilt $P = Q$ (wegen Def Partition)

Also gilt $c \in P$. Also $a \in P$ und $c \in P$. Somit gilt $(a,c) \in \beta$.

Außerdem: $\mathcal{B}/\beta = \mathcal{B}$

"$\subseteq$": Sei $X \in \mathcal{B}/\beta$. z.z. $X \in \mathcal{B}$.

Da $X \in \mathcal{B}/\beta$, gibt es $b \in B$, sodass $X = [b]_\beta$.

$X = \{c \in B \mid (b,c) \in \beta\}$, und folglich

$X = \{c \in B \mid \exists P \in \mathcal{B} : b \in P \text{ und } c \in P\}$

Diskrete VO

29. 1.

Zahlen als Äquivalenzklassen

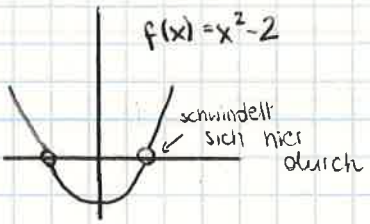
$\mathbb{N} \to \mathbb{N}_0 \to \mathbb{Z} \to \mathbb{Q}$ (Algebra) $\to \mathbb{A}$ (NS v. Polyn.) alg. Zahlen (Analysis) $\to \mathbb{C}$

$\mathbb{Q} \to \mathbb{R}$ (Analysis) $\to \mathbb{C}$ (Algebra)

$\mathbb{N}$: Peano

$\mathbb{N}_0$: von Neumann

d.h. $\mathbb{Q}$ ist nicht vollständig



$\sqrt{7} \notin \mathbb{Q}$ $\sqrt{2} \notin \mathbb{Q}$

$\mathbb{Z}$: $(5,2) \equiv_\rho (4,1) \equiv_\rho (3,0)$

$(a,b) \equiv_\rho (c,d) :\Leftrightarrow a+d = b+c$

Überlegung: $a-b = c-d$

Wir definieren also auf $\mathbb{N}_0 \times \mathbb{N}_0$ eine ÄR ρ durch

$$\rho = \{((a,b),(c,d)) \in (\mathbb{N}_0 \times \mathbb{N}_0) \times (\mathbb{N}_0 \times \mathbb{N}_0) \mid a+d = b+c\}$$

$(5,2) \equiv_\rho (4,1) \equiv_\rho (33,30) \equiv_\rho (3,0)$ wir def. hier 3

$(2,5) \equiv_\rho (1,4) \equiv_\rho (0,3)$ wir def. hier -3

Def: $\mathbb{Z}$ ist die Menge der Äquivalenzklassen bzgl. dieser Relation ρ.

$$[(5,2)]_\rho = [(4,1)]_\rho = [(3,0)]_\rho =: 3$$

$$[(1,8)]_\rho = [(0,7)]_\rho = [(5,12)]_\rho = [(10,17)]_\rho =: -7$$

$\mathbb{Z} := (\mathbb{N}_0 \times \mathbb{N}_0)/\rho$.

Q: Frage: Gilt $\frac{3}{4} = \frac{6}{8}$? Soll gelten

$(3,4) \equiv_6 (6,8)$ soll $\frac{3}{4} = \frac{6}{8}$ ausdrücken

(6 ↖ sigma)

$(a,b) \equiv_6 (c,d) :\Leftrightarrow a \cdot d = b \cdot c$

$P := \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$

Def. Die rationalen Zahlen sind die Faktormenge $(\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})) / 6$. Für die Äquivalenz- (↑ bezüglich)
klasse $[(a,b)]_6$ schreiben wir auch $\frac{a}{b}$.

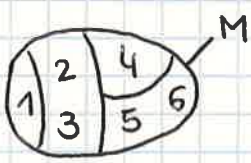
$\frac{3}{4} = [(3,4)]_6 = [(6,8)]_6 = \frac{6}{8}$

$(3,4) \equiv_6 (6,8)$, da $3 \cdot 8 = 4 \cdot 6$

Def.:

Sei M eine Menge und ψ eine ÄR auf M.
Dann ist $R \subseteq M$ <u>ein Repräsentantensystem</u> von M: $\Leftrightarrow$
$\forall m \in M : [m]_\psi \cap R$ hat genau ein Element

Bsp:



$R = \{1,3,4,6\}$ ist ein Rep.system, $R' = \{1,2,4,5\}$ auch.

Für $\mathbb{Q} = (\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})) / 6$ ist
$R = \{(a,b) \mid a \in \mathbb{Z}, b \in \mathbb{N}, ggT(a,b) = 1\}$ ein
Repräsentantensystem.

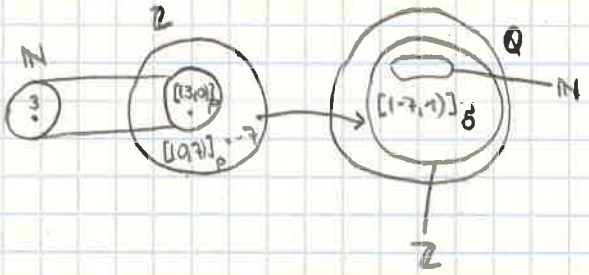
Der Repräsentant von $\overbrace{\frac{11}{-77}}^{\text{Klasse}}$ ist $(-1,7)$ ← das kommt raus wenn ich kürze

$$\frac{3}{7} + \frac{7}{5} = \frac{15}{35} + \frac{49}{35} = \frac{64}{35}$$

ggT (7,5) = 1

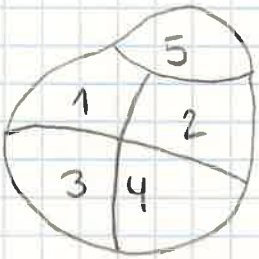
$\mathbb{N} \subsetneq \mathbb{Q}$ $\quad 3 \in \mathbb{N}$ als rationale Zahl: $[(3,1)]_\sim$.

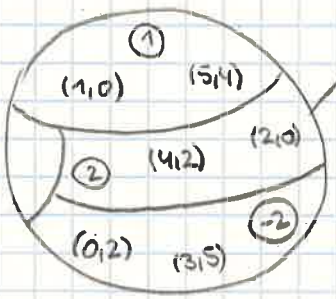
$[(3,1)]_\sim = [([3,0]_\rho, [5,4]_\rho)]_\sim$



Es soll gelten: $3 = \frac{-15}{-5}$

Man ändert die Konstruktion dahingehend, dass $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$



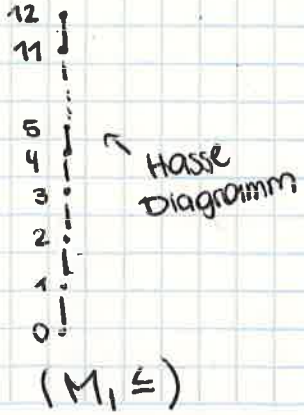


$\mathbb{N}_0 \times \mathbb{N}_0$

$\sim \subseteq (\mathbb{N}_0 \times \mathbb{N}_0) \times (\mathbb{N}_0 \times \mathbb{N}_0)$

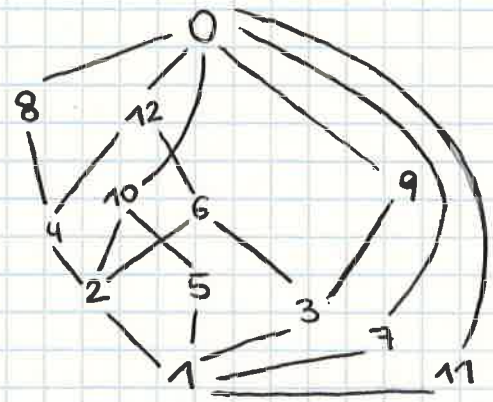
Ordnungsrelationen

$M = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 0\}$



Hasse Diagramm

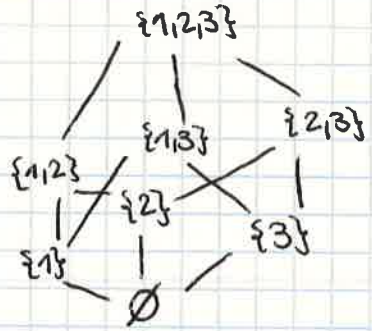
$(M, \leq)$



Ordnung nach Teilbarkeit

$(M, |)$

(M, Teilbarkeit)



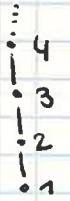
$(P(\{1,2,3\}), \subseteq)$

Def: Sei M eine Menge, und sei ρ eine Relation auf M. Die Relation ρ ist <u>antisymmetrisch</u> $:\Leftrightarrow$
$\forall x,y \in M: ((x,y) \in \rho \wedge (y,x) \in \rho) \Rightarrow x = y.$

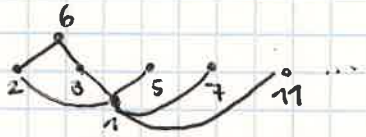
Def: Sei M Menge und ρ Relation auf M. ρ ist eine Ordnungsrelation auf $M :\Leftrightarrow \rho$ ist reflexiv, ρ ist antisymmetrisch, ρ ist transitiv.

Bsp:

$(\mathbb{N}, \rho)$ wobei $(a,b) \in \rho :\Leftrightarrow a \leq b$.



$(\mathbb{N}, \underset{\text{"Teil"}}{|})$ wobei $(a,b) \in | :\Leftrightarrow a|b$



$(P(\{1,2,3\}), \mu)$, wobei $(A,B) \in \mu :\Leftrightarrow A \subseteq B$

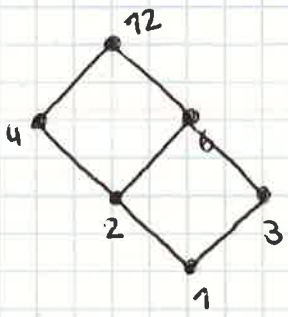
Manchmal verwendet man statt der griech. Buchstaben auch das Zeichen $\leq$.

$ab \leq_{lex} acx \leq_{lex} mayr \leq_{lex} meier \leq_{lex} \cdots$ [lex - Lexograph. Ordnung als Zusatz (nicht wichtig)

Diskrete VO

30.1.

4. Ordnungsrelationen



$M = \{1,2,3,4,6,12\}$

$\rho: (a,b) \in \rho :\Leftrightarrow a \mid b$

(M,ρ) ist eine geordnete Menge

Def: Sei $(M, \leq)$ eine geordnete Menge. Die Relation $\leq$ ist <u>linear</u> (oder <u>total</u>), wenn

$\forall x,y \in M: x \leq y \vee y \leq x$

$(M, \leq)$ ist dann eine total geordnete Menge

Wenn $(M, \leq)$ geordnete Menge ist, so bedeutet

$a < b :\Leftrightarrow a \leq b$ und $a \neq b$.

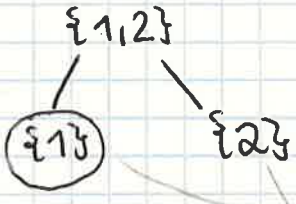
Def: Sei $(M, \leq)$ eine geordnete Menge, und sei $a \in M$.

(1) a ist ein kleinstes Element von $M :\Leftrightarrow \forall b \in M: a \leq b$ (unter allen anderen)

(2) a ist ein minimales Element von $M :\Leftrightarrow \neg \exists b \in M: b < a$ (kann nicht unterboten werden)

$M = \mathcal{P}(\{1,2\}) \setminus \{\emptyset\}$

$(M, \leq)$:



$\{1\}$ ist minimal

$\{1\}$ ist minimales Element

$\{2\}$ ist ebenfalls ein min. Element

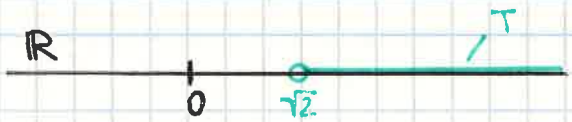
ein kleinstes Element gibt es nicht

diese dürfen nicht verglichen werden
wäre $\emptyset$ dabei, wäre es bei $\{1\}$ das kleinste Element

(3) Sei $T \subseteq M$, sei $m \in M$. m ist eine untere Schranke für $T :\Leftrightarrow \forall t \in T : m \leq t$.

Bsp: $M = (\mathbb{R}, \leq)$

$T := \{x \in \mathbb{R} \mid x > 0 \text{ und } x^2 > 2\}$



1,2 ist eine untere Schranke für T

Bsp zu (1)

$(\mathbb{N}, \leq)$ hat 1 als kleinstes Element

$(\mathbb{Z}, \leq)$ hat kein kleinstes Element

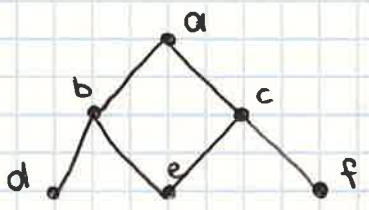
$(\{x \in \mathbb{R} \mid x > 0\}, \leq)$ hat kein kleinstes Element

} haben auch kein minimales Element

(4) a ist ein größtes Element $:\Leftrightarrow \forall b \in M : b \leq a$

(5) a ist maximales Element $\Leftrightarrow \neg \exists b \in M : a < b$

(6) m ist obere Schranke von $T :\Leftrightarrow \forall t \in T : t \leq m$.



kleinste Elemente: -

minimale Elemente: d, e, f

größte Elemente: a

maximale Elemente: a

untere Schranken von {e, f}: -

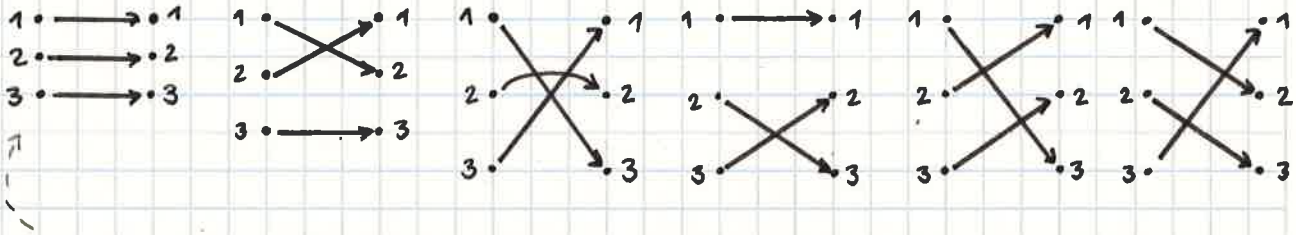
obere Schranken von {e, f}: c, a

5.6. Permutationen

$\underline{n} := \{1, 2, \dots, n\}$

Def: Eine Permutation von $\underline{n}$ ist eine bijektive Abb. von $\underline{n}$ nach $\underline{n}$.

Bsp: $n = 3$, $\underline{n} = \{1, 2, 3\}$



6 Permutationen auf einer 3-elementigen Menge

$$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix} \quad \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} \quad \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} \quad \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} \quad \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} \quad \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$$

$$\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} = \{(1,1), (2,3), (3,2)\}$$

$(1)(2)(3) \quad (12)(3) \quad (13)(2) \quad (1)(23) \quad (132) \quad (123)$

Zyklenschreibweise „$\circ$ geht auf $\bullet$, $\bullet$ auf $\diamond$ & $\diamond$ auf $\circ$"

$$f = \begin{pmatrix}1&2&3&4&5&6&7&8\\5&3&1&2&7&4&6&8\end{pmatrix}$$

$f = (1\,5\,7\,6\,4\,2\,3)(8)$

$$g = \begin{pmatrix}1&2&3&4&5&6&7&8\\3&4&5&8&7&2&1&6\end{pmatrix}$$

$g = (1\,3\,5\,7)(2\,4\,8\,6)$

paarweise verschieden sind

Wenn $i_1, \dots, i_k \in \underline{n} \forall$, dann ist $f = (i_1\ i_2\ \dots\ i_k)$ def. durch

$f(i_j) = i_{j+1}$ für $j \in \{1, \dots, k-1\}$, $f(i_k) = i_1$,
$f(x) = x$ für $x \in \underline{n} \setminus \{i_1, \dots, i_k\}$

$f = (i_1 \dots . i_k)$ heißt k- Zyklus.
2- Zyklen heißen Transpositionen.

Lemma
Sei $n \in \mathbb{N}$ und seien f, g Permutationen von $\underline{n}$.
Dann ist $f \circ g$ wieder eine Permutationen.

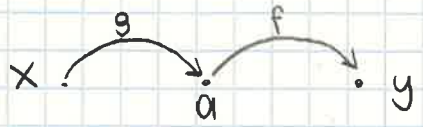
Beweis: Wir müssen zeigen, dass $f \circ g$ bijektiv ist

Injektivität: z.z. $\forall x, y \in \underline{n} : f \circ g\ (x) = f \circ g\ (y) \Rightarrow x = y$
(f nach g auf x)

Sei $x, y \in \underline{n}$. Wir nehmen an, dass $f \circ g\ (x) = f \circ g\ (y)$.
z.z. $x = y$.
Es gilt $f \circ g\ (x) = f \circ g\ (y)$, also $f(g(x)) = f(g(y))$.
Da f injektiv ist, gilt $g(x) = g(y)$. Da g injektiv ist, gilt $x = y$. → weil w.w. dass f eine Permutation

$f \circ g$ ist surjektiv:
z.z. $\forall y \in \underline{n}\ \exists x \in \underline{n} : f \circ g\ (x) = y$

Sei $y \in \underline{n}$. z.z. $\exists x \in \underline{n} : f \circ g\ (x) = y$



Da f surjektiv ist, gibt es $a \in \underline{n}$, sodass $f(a) = y$
Da g surjektiv ist, gibt es $\otimes \in \underline{n}$, sodass $g(\otimes) = a$.
Wir berechnen nun $f \circ g(\otimes)$.

$f \circ g(\otimes) = f(g(\otimes)) = f(a) = y$. Also gilt: $\exists x \in \underline{n} : f \circ g(x) = y$

Kapitel 7 kommt nicht!
Lückentexte werden kommen

Bspfragen:

1. Zeigen Sie, dass für alle Mengen A, B, C gilt:
   $B \cap C \subseteq (B \setminus A) \cup (A \cap C)$
   (Venn Diagramme erlaubt, liefern aber keine Punkte)

2. Def von + auf $\mathbb{N}_0$ ... Zeigen Sie:
   $\forall x, y, z \in \mathbb{N}_0 : (x+y)+z = x+(y+z)$ → Lückentext

   ... $S := \{ z \in \mathbb{N}_0 \mid \forall x, y \in \mathbb{N} : (x+y)+z = x+(y+z) \}$
   Zeigen Sie $\forall z \in \mathbb{N}_0 : z \in S \Rightarrow z^+ \in S^+$ so:
   Sei $z \in \mathbb{N}_0$. Wir nehmen an $\underline{z \in S}$. Das bedeutet,
   dass $\forall \underline{x \in \mathbb{N}_0}$ $\forall \underline{y \in \mathbb{N}_0}$: $\underline{(x+y)+z = x+(y+z)}$

3. Seien $a = 104$ $b = 65$
   a) Bestimmen Sie ggT (a,b) und ganze Zahlen
      u, v mit ggT $(a,b) = va + ub$

   b) Best. Sie kgV (a,b)
   c) Best. Sie Primfaktorzerl. von $a \cdot b$

4. Sei $f: \mathbb{R}\setminus\{1\} \to \mathbb{R}\setminus\{0\}$, $f(x) = \frac{2}{x-1}$

z.z. f surj. auf $\mathbb{R}\setminus\{0\}$ ist.

5. Geben Sie eine vollst. Formulierung der Sätze für <u>einen</u> der Pkt a) und b) an.

a) Peano - Axiome in der Sichtweise d. Mengenlehre

b) Verhalten des ggT und kgV zweier Zahlen zu anderen gem. Teilern und Vielfachen in Bezug auf die Teilbarkeit.

6. Beweisen Sie <u>einen</u> der folgenden Sätze:

1)
2)
3)
} eher schwere Sätze

Klausur: ws. 90 min