Elementare Zahlentheorie

WS 2013/2014

(Dr. Antonella Perucca)

Julian Palme

(Stand: 4. Dezember 2013)

Dies ist eine Mitschrift der Vorlesung 'Elementare Zahlentheorie', gelesen von Frau Dr. Antonella Perucca im Wintersemester 2013/2014 an der Universität Regensburg. Dieses Dokument ist KEIN offizielles Skript und wurde gesetzt in LaTeX von Julian Palme.

Vorlesung 1 vom 16/10/2013

Die Sprache der Mathematik

Einleitung

- KEINE Mehrdeutigkeit, KEINE Interpretationsfreiheit
- Wenn es keine Einschrnkung gibt, dann gibt es totale Freiheit
  „nehmen wir zwei Punkte“ – Dürfen wir zweimal denselben Punkt nehmen? Ja!
  „nehmen wir zwei *verschiedene* Punkte“ ist besser
  NICHT verboten, dann erlaubt!
- NICHT immer wahr, ist falsch
- „es gibt ein . . . “, d. h. mindestens ein, sonst schreiben wir: genau ein

Aussagenlogik

Aussage: ein sprachliches Gebilde, von dem es sinnvoll ist zu fragen, ob es wahr oder falsch ist
„$1 + 1 = 2$“ wahre Aussage
„$1 + 1 = 4$“ falsche Aussage
„$x > 0$“ Was ist mit x? Mit $x = 2$ wahr, mit $x = -2$ falsch

Wahrheitswerte: wahr 1, falsch 0

Konstruktionen mit Aussagen

Negation

Die Negation einer Aussage p ist die Aussage 'nicht p' ($\neg p$)
0 $1 + 1 \neq 2$ 1 $1 + 1 \neq 4$

p	$\neg p$
1	0
0	1

Konstruktion (und)

Seien p, q Aussagen. Dann 'p und q' ($p \wedge q$) ist eine Aussage.

p	$\neg p$	$p \wedge q$
1	1	1
1	0	0
0	1	0
0	0	0

$p \wedge (\neg p)$ 'p und (nicht p)' 0 Widerspruch, Kontradiktion

$p_1 \wedge p_2 \wedge p_3 \wedge \ldots \wedge p_n$
1 genau dann, wenn alle p_i wahr sind, für alle $i = 1, 2, \ldots, n$
0 wenn mindestens eine der Aussagen falsch ist; es gibt eine Aussage, die falsch ist

Adjunktion (oder)

'p oder q' $(p \vee q)$
1 $\underbrace{3+3=6}_{1}$ oder $3+3=7$
In der Mathematik, *oder* ist KEIN 'entweder oder'

p	q	$p \vee q$
1	1	1
1	0	1
0	1	1
0	0	0

$p_1 \vee p_2 \vee p_3 \vee \ldots \vee p_n$
0 nur, wenn alle falsch sind
1 wenn mindestens eine der Aussagen wahr ist

Implikationen

$p \Longrightarrow q$ p impliziert q

p	q	$p \Longrightarrow q$
1	1	1
1	0	0
0	1	1
0	0	1

Hier ist Vorsicht geboten!! Die Prämisse ist wahr, jedoch NICHT die Folgerung. Somit ist die Implikation falsch.
A: Wir sind in Europa
B: Wir sind in Deutschland
$B \Longrightarrow A$ 1, sagt nichts, falls wir NICHT in Deutschland sind
Bemerkung:

- $p \Longrightarrow q$ ist äquivalent zu $(\neg q) \Longrightarrow (\neg p)$!
  Deutschland $\Longrightarrow$ Europa NICHT Europa $\Longrightarrow$ NICHT Deutschland
- $\neg(p \Longrightarrow q)$, die Negation, ist $p \wedge (\neg q)$

Umkehrung von $p \Longrightarrow q$ ist $q \Longrightarrow p$
Doppelte Implikation (Äquivalenz) $p \Longleftrightarrow q$, d. h. $p \Longrightarrow q$ und $q \Longrightarrow p$

Für Dreiecke:

gleichseitig $\Longrightarrow$ gleichschenklig (mindestens 2 Seiten gleich) 1
gleichseitig $\Longleftarrow$ gleichschenklig 0
gleichschenklig $\Longleftrightarrow$ gleichseitig 0
gleichseitig $\Longleftrightarrow$ gleichwinklig 1
gleichseitig $\Longrightarrow$ gleichwinklig 1
gleichseitig $\Longleftarrow$ gleichwinklig 1

Vorlesung 2 vom 17/10/2013

Prädikate

Prädikat

Ein Prädikat ist eine Formel, die von endlich vielen Variablen abhängt und die EIgenschaft besitzt, für jeden eingesetzten Wert der Variablen, eine Aussage zu sein.

Beispiel

- „$x > 0$“ für $x = 2$ wahre Aussage $(2 > 0)$ Beispiel
  „$x > 0$“ für $x = -1$ falsche Aussage $(-1 > 0)$ Gegenbeispiel

  'Beispiel': Werte für die Variablen, sodass das Prädikat eine wahre Aussage wird.
  'Gegenbeispiel': Werte für die Variablen, sodass das Prädikat eine falsche Aussage wird.

- „$x > y$“ $x = 2, y = 0$ Beispiel; $x = 2, y = 2$ Gegenbeispiel

Quantoren

$\exists$ 'es gibt ein' (Existenz)
$\exists!$ 'es gibt genau ein' (Existenz und Eindeutigkeit)
$\forall$ 'für alle'

Beispiele

„$\exists x \underbrace{:}_{\text{sodass}} x > 0$“ wahre Aussage, z. B. $x = 1$ „$\exists! x : x > 0$“ falsche Aussage, z. B. $x = 1, x = 2$
“$\forall x, x > 0$“ falsche Aussage, z. B. $x = -1$

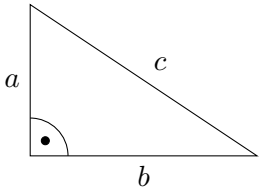
Zweiwertige Prädikate

Sei $p(x, y)$ Prädikat, d. h. x, y sind die Variablen. Dann haben wir die folgenden Aussagen:
„$\forall x \forall y \quad \underbrace{p(x, y)}_{\text{Eigenschaft}}$ “
„$\exists x \exists y : p(x, y)$“
„$\forall x \exists y : p(x, y)$“
„$\exists x : \forall y \; p(x, y)$“

Sätze usw.

Satz

Ein Satz ist eine wahre Aussage. Oft sind Sätze Implikationen:
„Annahme $\Longrightarrow$ Folgerungen“

Pythagoras: 

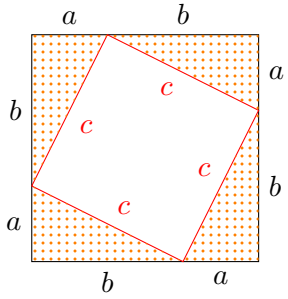
$\Longrightarrow\ a^2 + b^2 = c^2$

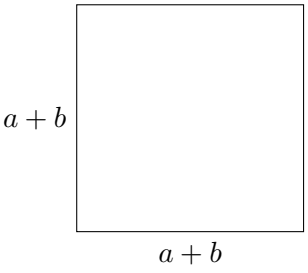
Beweis

Vollständige Begründung, dass der Satz wahr ist.

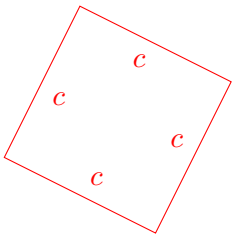
Jeder Satz besitzt mindestens einen Beweis.
Zusammenfassung eines Beweises; Beweisidee

Beweisidee Pythagoras

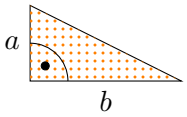




$= (a+b)^2 = a^2 + b^2 + 2ab$



$= c^2$



$= \frac{1}{2}ab$

$$\underbrace{(a+b)^2}_{=a^2+b^2+2ab} = \underbrace{c^2 + 4\left(\frac{1}{2}ab\right)}_{=c^2+2ab} \implies a^2 + b^2 = c^2$$

Details fehlen, z. B. warum das innere Viereck mit Kantenlänge c ein Quadrat ist.

Typische Beweisstrukturen

(1) Direkter Beweis, eine Kette von Deduktionen:
Annahmen $\implies$ Eigenschaften $\implies$ ... $\implies$ Folgerungen (wie oben)

(2) Kontraposition
NICHT Folgerungen $\implies$ ... $\implies$ NICHT Annahmen
Sei $a^2 + b^2 \neq c^2$ (was wir NICHT wollen). Dann, ..., Annahmen NICHT erfüllt (z. B. ist das Dreieck NICHT rechtwinklig).
„$A \implies F$“ äquivalent zu „$(\neg F) \implies (\neg A)$“

(3) Widerspruch
Falls A gilt und NICHT F gilt, dann können wir einen Widerspruch finden.
($\mathbb{R}$ Aussage)
A und NICHT $F \implies R$
A und NICHT $F \implies$ NICHT R
z. B. Falls aus A und NICHT F wir schließen können, dass $1 = 2$, haben wir einen Widerspruch (da $1 \neq 2$ ist bekannt).
was wir NICHT wollen

Kompliziertere Sätze

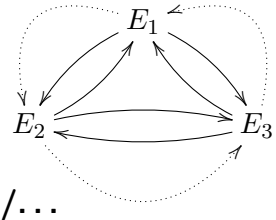
Satz

Die folgenden Eigenschaften sind äquivalent (für ein Dreieck D):
(E1) D ist gleichseitig
(E2) D ist gleichschenklig
(E3) Zwei Winkel in D sind 60°.

Zu beweisen:
E1 $\implies$ E2 , E2 $\implies$ E1
E1 $\implies$ E3 , E3 $\implies$ E1
E2 $\implies$ E3 , E3 $\implies$ E2

Trick: Es reicht

E1 $\Longrightarrow$ E2 , E2 $\Longrightarrow$ E3 , E3 $\Longrightarrow$ E1
nach der Transitivität der Implikation



Beispiele/Lemmata/Vermutung/...

Lemma: Satz, aber NICHT wichtig und benutzt, um wichtige Sätze zu beweisen
Proposition: Satz, aber nicht so wichtig oder nicht schön formuliert.

Im Prinzip muss man die Sätze auswenig lernen (insbesondere die mit einem Namen).

Korollar: Satz, folgt einfach aus einem Satz.
Vermutung: KEIN Satz, könnte falsch sein, hat KEINEN Beweis
Wenn ein Beweis gefunden wird, dann wird die Vermutung ein Satz.

Naive Mengenlehre

„Definition“ (intuitive, naive)

Eine Menge ist eine Sammlung von Elementen, die alle verschieden sind.
(Problem, z. B. die Menge aller Mengen ist KEINE Menge)
Diese Definition ist gut im Alltag und auch für die Arithmatik (reelle Zahlen).

Schreibweise

$\{1, 7, 9\} = \{1, 9, 7\} = \{1, 1, 7, 9\}$ drei Elemente

Möglichkeit

Anzahl der Elemente

- endlich, z. B. $\{1, 7, 9\}$
- unendlich, z. B. $\mathbb{Z}$ =ganze Zahlen

Beispiel

$$\left\{ x \in \mathbb{Z} \;\middle|\; x^3 + x^5 = x^7 \right\} \subseteq \mathbb{Z}$$

Gleichheit

$(A = B)$ A und B haben genau dieselben Elemente

Teilmenge

$(A \subseteq B)$ Alle Elemente von A sind auch in B enthalten

Echte Teilmenge

$(A \subset B)$ $A \subseteq B$ und $A \neq B$

Viele Eigenschaften

z. B. „Transitivität der Inklusion von Mengen“
Seien A, B, C Mengen. Aus $A \subseteq B$ und $B \subseteq C$ folgt $A \subseteq C$.

Beweis

Sei $x \in A$. Da $\underbrace{A \subseteq B}_{\text{Annahme}}$, ist x in B. Da $x \in B$ und $\underbrace{B \subseteq C}_{\text{Annahme}}$, ist $x \in C$. D. h. $\forall\, x \in A$ ist $x \in C$ $(A \subseteq C)$.

□

Durchschnitt

$$A \cap B = \left\{ x \;\middle|\; x \in A \text{ und } x \in B \right\}$$

Vereinigung

$$A \cap B = \left\{ x \;\middle|\; x \in A \text{ und } x \in B \right\}$$

Paarweise disjunkt

$A_1, \ldots, A_n$ Mengen
$\forall\, i, j = 1, \ldots, n$ mit $i \neq n$, dann ist $A_i \cap A_j = \emptyset$ (leere Menge)

Für $n = 3$: $\underbrace{A_1 \cap A_2 = \emptyset}_{A_2 \cap A_1 = \emptyset}$ $\underbrace{A_1 \cap A_3 = \emptyset}_{A_3 \cap A_1 = \emptyset}$ $\underbrace{A_2 \cap A_3 = \emptyset}_{A_3 \cap A_2 = \emptyset}$

j \ i	1	2	3
1		X	X
2	X		X
3	X	X	

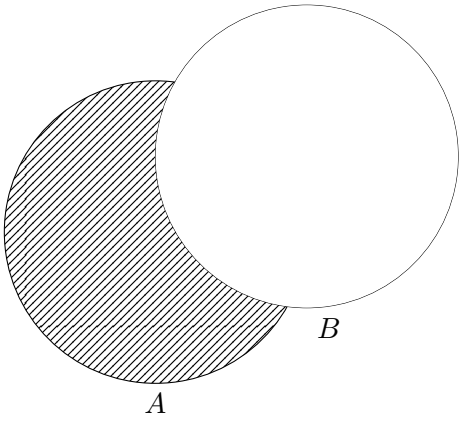
$A_1 \cap \ldots \cap A_n = \emptyset$ notwendig aber NICHT hinreichend!!
$A_1, \ldots, A_n$ paarweise disjunkt $\underset{\not\Leftarrow}{\Rightarrow}$ $A_1 \cap \ldots \cap A_n = \emptyset$

Beispiel

$A_1 = \{1, 2\}$
$A_2 = \{2, 3\}$
$A_3 = \{3, 1\}$
$A_1 \cap A_2 = \{2\} \neq \emptyset$, NICHT paarweise disjunkt
$A_1 \cap A_2 \cap A_3 = \emptyset$, $1 \notin A_2$, $2 \notin A_3$, $3 \notin A_1$

Differenz

$$A \underbrace{\setminus}_{\text{ohne}} B = \left\{ x \in A \;\middle|\; x \notin B \right\} = A \setminus (A \cap B)$$



Vorlesung 3 vom 23/10/2013

Karthesisches Produkt

Definition

Seien A, B Mengen. Das **Karthesische Produkt** von A und B (Notation: $A \times B$) ist die Menge

$$A \times B := \left\{ (a, b) \;\middle|\; a \in A, b \in B \right\}$$

(a, b) ist ein geordnetes Paar: $(a, b) = (b, a)$ nur falls $a = b$

Zusatz

Ein ungeordnetes Paar ist $\{a, b\}$.

Beispiele

$$\mathbb{R}^2 = \mathbb{R} \times \mathbb{R} = \left\{ (x, y) \;\middle|\; x \in \mathbb{R}, y \in \mathbb{R} \right\}$$

Schachbrett: $A \times B$ mit $A = \{a, b, c, \ldots, h\}$ und $B = \{1, 2, \ldots, 8\}$

Definition

Das karthesische Produkt von $A_1, \ldots, A_n$ ist die Menge

$$A_1 \times A_2 \times \ldots \times A_n = \left\{ (a_1, \ldots, a_n \;\middle|\; a_i \in A_i \quad \forall\, I = 1, \ldots, n \right\}$$

$(a_1, \ldots, a_n)$ ist hierbei ein geordnetes n-Tupel.

$$\mathbb{R}^3 = \mathbb{R} \times \mathbb{R} \times \mathbb{R} = \left\{ (x, y, z) \;\middle|\; x \in \mathbb{R}, y \in \mathbb{R}, z \in \mathbb{R} \right\}$$

Bemerkung: $A \times B \neq B \times A$ (außer A oder B sind $\emptyset$[1] oder $A = B$[2])
Bemerkung: $(A \times B) \times C \neq A \times (B \times C) \neq A \times B \times C$ außer triviale Fälle
$((a, b), c) \neq (a, (b, c)) \neq (a, b, c)$
$\mathbb{R}^3 \neq \mathbb{R}^2 \times \mathbb{R}$ als Mengen
Oft macht man eine Identifizierung: $(x, y, z) \rightsquigarrow ((x, y), z)$

Mächtigkeit

Seien $A_1, \ldots, A_n$ endliche Mengen.

$$\#(A_1 \times A_2 \times \ldots \times A_n) = \prod_{i=1}^{n} \#A_i = \#A_1 \cdot \#A_2 \cdot \ldots \cdot \#A_n$$

Potenzmenge

Definition

Sei M eine Menge. Die **Potenzmenge** von M (Notation: $\mathcal{P}(M)$) ist die Menge

$$\mathcal{P}(M) = \{\text{Teilmengen von } M\}$$

Mächtigkeit

Sei M eine endliche Menge. Dann

$$\#\mathcal{P}(M) = 2^{\#M}$$

Partition

Definition

Sei M eine Menge. Eine **Partition** von M ist eine Menge P von nicht-leeren Teilmengen von M, sodass

$$M = \bigcup_{A \in P}^{A} \quad \text{(die Vereinigung ist } M\text{)}$$
$$A \cap A' = \emptyset \quad \forall\, A, A' \in P \text{ mit } A \neq A' \quad \text{(paarweise disjunkt)}$$

Beispiel

M Menge, $A \subseteq M$, $A \neq \emptyset$, $A \neq M$ (Partition mit zwei Elementen)

$$P = \{A, M \setminus A\}$$

A ist eine echte nicht-leere Teilmenge, $M \setminus A$ ist das Komplement.
$A \neq \emptyset$; $M \setminus A \neq \emptyset$ (da $A \neq M$)

[1] $A \times \emptyset = \emptyset$ bzw. $\emptyset \times B = \emptyset$
[2] $A \times B = A \times A = B \times B$

$A \cup (M \setminus A) = M$ ✓
$A \cap (M \setminus A) = \emptyset$ ✓

Beispiel

M Menge von Studenten

- Geschlecht (Partition mit 2 Teilmengen)
- Geburtstag (∇ vielleicht erscheinen NICHT alle Geburtstage; Partition mit höchstens 366 Elementen)
- Blutgruppentyp: A, B, AB, 0
- Blutgruppentyp mit RH: A+, A-, B+, B-, AB+, AB-, 0+, 0-

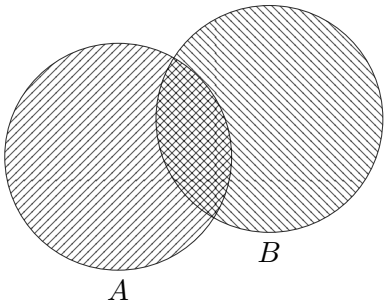
Bemerkung: Jedes Element von M ist in genau einem Element der Partition enthalten.
$\exists!$ $\longrightarrow$ die Vereinigung ist M
$\exists$ Sei $x \in M$. Es gibt mindestens ein $A \in P$, sodass $x \in A$. Grund: $M = \bigcup_{A \in P} A$
! Sei $x \in M$. Es gibt höchstens ein $A \in P$, sodass $x \in A$. Grund: die Elemente von P sind paarweise disjunkt.
„mindestens ein“ und „höchstens ein“ = „genau ein“
P ist eine Menge. Die Elemente sind einige Teilmengen von M. ($P \subseteq \mathcal{P}(M)$)

Beispiel mit 5 Elementen

$M = \{a, b, c, d, e\}$
$P = \{\{a\}, \{b\}, \{c\}, \{d\}, \{e\}\}$ $1+1+1+1+1=5$
$P = \{\{a, b\}, \{c\}, \{d\}, \{e\}\}$ $2+1+1+1=5$
$P = \{\{a, b, c\}, \{d\}, \{e\}\}$ $3+1+1=5$
$P = \{\{a, b\}, \{c, d\}, \{e\}\}$ $2+2+1=5$
$P = \{\{a, b, c, d\}, \{e\}\}$ $4+1=5$
$P = \{\{a, b, c\}, \{d, e\}\}$ $3+2=5$
$P = \{\{a, b, c, d, e\}\}$ $5=5$
Man kann auch die Elemente umbenennen.

Prinzip von Inklusion und Exklusion

„Für je zwei endliche Mengen A und B gilt: $\#(A \cup B) = \#A + \#B - \#(A \cap B)$“
Spezialfall $A \cap B = \emptyset \implies \#(A \cap B) = \#\emptyset = 0$. Dann $\#(A \cup B) = \#A + \#B$
Das ist ein Satz. Der Beweis ist mit „Induktion“.
Intuitive Erklärung:



Für drei endliche Mengen A, B, C gilt:

$$\#(A \cup B \cup C) = \#A + \#B + \#C - \#(A \cap B) - \#(B \cap c) - \#(A \cap C) + \#(A \cap B \cap C)$$

Sei $x \in (A \cap B \cap C)$: $1 = \underbrace{1 + 1 + 1 - 1 - 1 - 1 + 1}_{1}$

Für endliche Mengen $A_1, \ldots, A_n$ gilt:

$$\#\bigcup_{i=1}^{n} A_i = \sum_{i=1}^{n} \#A_i - \sum_{(*)\ 1 \le i < j \le n} \#(A_i \cap A_j) + \sum_{1 \le i < j < k \le n} \#(A_i \cap A_j \cap A_k) - \ldots + (-1)^{n+1} \#(A_1 \cap A_2 \cap \ldots \cap A_n)$$

$(*)\ i \in \{1, \ldots, n\}\ ,\ j \in \{1, \ldots, n\}\ ,\ i \neq j\ ,\ i < j$

Korollar

Für $A_1, \ldots A_n$ endlich, paarweise disjunkt gilt

$$\#\bigcup_{i=1}^{n} A_i = \sum_{i=1}^{n} \#A_i$$

Insbesondere P Partition von M: $P = \{A_1, \ldots, A_n\}$

$$\#M \overset{M = \bigcup_{A \in P} A}{=} \#\left(\bigcup_{i=1}^{n} A_i\right) \overset{\text{pw.disj.}}{=} \sum_{i=1}^{n} \#A_i$$

Proposition

Für $A_1, \ldots, A_n$ endliche Mengen gilt

$$\#\bigcup_{i=1}^{n} A_i \le \sum_{i=1}^{n} \#A_i$$

Beweis

1) TRICK um paarweise disjunkte Teilmengen zu haben

$B_1 = A_1$

$B_2 = A_2 \setminus A_1$

$B_3 = A_3 \setminus (A_1 \cup A_2)$

$\vdots$

$B_i = A_i \setminus \left(\bigcup_{j=1}^{i-1} A_j\right)$

$$\#\bigcup_{i=1}^{n} B_i = \sum_{i=1}^{n} \#B_i$$

2)

$\#B_i \leq \#A_i$ (da $B_i \subseteq A_i$)

3)

$$\bigcup_{i=1}^{n} B_i = \bigcup_{i=1}^{n} A_i$$

($\subseteq$)

Sei $x \in \bigcup B_i$. Dann $x \in B_{i_0}$ mit $i_0 \in \{1, \ldots, n\}$. Dann $x \in A_{i_0}$. Dann $x \in \bigcup A_i$.

($\supseteq$)

Sei $x \in \bigcup A_i$. Sei $x \in A_{i_0}$. Nehmen wir i_0 minimal. Dann $x \in A_{i_0}$ und $x \notin A_j \quad \forall\, j < i_0$.

Dann $x \in B_{i_0}$. Dann $x \in \bigcup_{i=1}^{n} B_i$.

4)

$\#\bigcup A_i = \#\bigcup B_i = \sum \#B_i \leq \sum \#A_i$

□

Schubfachprinzip

Verteilt man n Objekte auf k Mengen ($n, k > 0$, $n, k \in \mathbb{N}$), so gibt es mindestens eine Menge, in der sich zumindest $\lceil \frac{n}{k} \rceil$ Objekte befinden.

Aufrundungsfunktion

$x \in \mathbb{R}$.

$\lceil x \rceil = \min \mathbb{Z} \cap \left\{ \pi \in \mathbb{R} \;\middle|\; \pi \geq x \right\}$

$\lceil 4 \rceil = 4 \quad , \quad \lceil \underbrace{\pi}_{\approx 3{,}14} \rceil = 4 \quad , \quad \lceil \underbrace{-\pi}_{\approx -3{,}14} \rceil = -3$

100 Leute: $n = 100$

7 Farben: $k = 7$

Es gibt mindestens $\lceil \frac{100}{7} \rceil = 15$ Leute mit derselben Lieblingsfarbe.

Vorlesung 4 vom 24/10/2013

Binäre Relationen

Definition

Seien M und N nichtleere Mengen. Eine **binäre Relation** zwischen M und N ist eine Teilmenge $R \subseteq M \times N$.

Falls $M = N$, 'eine Relation auf M'

Beispiel

Anordnung von reellen Zahlen $\mathbb{R} = M = N$
$<$ 'kleiner'
$2 < 3$ ✓ $\longrightarrow$ $(2,3) \in R$ $3 < 2$ X $\longrightarrow$ $(3,2) \notin R$ $2 < 2$ X $\longrightarrow$ $(2,2) \notin R$
$R = \left\{ (a,b) \;\middle|\; a \in \mathbb{R}, b \in \mathbb{R} \text{ und } a < b \right\}$

Eigenschaften

Sei M eine nichtleere Menge und R eine Relation auf M (d. h. $R \subseteq M \times M$).

- reflexiv: $\forall\, x \in M$ gilt $(x,x) \in R$ (< nicht reflexiv)
- irreflexiv: $\forall\, x \in M$ gilt $(x,x) \notin R$ (< irreflexiv)

reflexiv und irreflexiv können NICHT gleichzeitig gelten
Es gibt Relationen, die weder reflexiv noch irreflexiv sind.

reflexiv $\underset{\not\Longleftarrow}{\Longrightarrow}$ NICHT irreflexiv
irreflexiv $\underset{\not\Longleftarrow}{\Longrightarrow}$ NICHT reflexiv

Falls $(x,x) \in R$ für einige x und $(x,x) \notin R$ für einige x.

- symmetrisch: $\forall\, x,y \in M$ gilt $(x,y) \in R \implies (y,x) \in R$ (< NICHT symmetrisch)
- asymmetrisch: $\forall\, x,y \in M$ gilt $(x,y) \in R \implies (y,x) \notin R$ (< asymmetrisch)
- antisymmetrisch: $\forall\, x,y \in M$ gilt $(x,y) \in R$ und $(y,x) \in R \implies x = y$ (< antisymmetrisch)
- transitiv: $\forall\, x,y,z \in M$ gilt $(x,y) \in R$ und $(y,z) \in R \implies (x,z) \in R$ (< transitiv)
- total: $\forall\, x,y \in M$ gilt $(x,y) \in R$ oder $(y,x) \in R$ (> NICHT total)
- konvex: $\forall\, x,y \in M$ gilt, dass genau eine zwischen $(x,y) \in R$, $(y,x) \in R$ oder $x = y$ gilt. (> konvex)

Beispiel

$\leq$ 'kleiner gleich' auf $\mathbb{R}$
$R = \left\{ (a,b) \;\middle|\; a \in \mathbb{R}, b \in \mathbb{R} \text{ mit } a \leq b \right\}$
$(2,3) \in R$, $(3,2) \in R$, $(2,2) \in R$
reflexiv? Ja, da $\forall\, x \in \mathbb{R}$: $x \leq x$ wahr, d. h. $(x,x) \in R$
irreflexiv? Nein, da reflexiv.
symmetrisch? $x \leq y \implies y \leq x$ $\forall\, x,y \in \mathbb{R}$? Nein, Gegenbeispiel: $2 \leq 3$ aber $3 \not\leq 2$, d. h. $(2,3) \in R$ aber $(3,2) \notin R$
asymmetrisch? $x \leq y \implies y \not\leq x$ $\forall\, x,y \in \mathbb{R}$? Nein, Gegenbeispiel: $2 \leq 2$, d. h. $(2,2) \in R$
antisymmetrisch? $x \leq y$ und $y \leq x \implies x = y$ $(\forall\, x,y \in \mathbb{R})$? Ja
transitiv? $x \leq y$ und $y \leq z \implies x \leq z$ $(\forall\, x,y,z \in \mathbb{R})$? Ja
total? $x \leq y$ oder $y \leq x$ $(\forall\, x,y \in \mathbb{R})$? Ja

konvex? genau eine $x \leq y$ oder $y \leq x$ oder $x = y \quad (\forall\, x, y \in \mathbb{R})$? Nein, $(2,2)$, $2 \leq 2$, $(2,2) \in R$, $2 = 2$

$<$ ist konvex $\leq$ ist total

Auswendig muss man wissen

- reflexiv
- symmetrisch
- transitiv

Sind alle drei Eigenschaften erfüllt, so spricht man von einer **Äquivalenzrelation**.

- reflexiv
- antisymmetrisch
- transitiv

Sind alle drei Eigenschaften erfüllt, so spricht man von einer **Halbordnung** oder **Ordnung**. Bsp. $\leq$

- asymmetrisch
- transitiv

Sind alle zwei Eigenschaften erfüllt, so spricht man von einer **Striktordnung**. Bsp. $<$

Äquivalenzrelationen

Sei M eine nichtleere Menge und R eine Relation auf M (d. h. $R \subseteq M \times M$).
Sei R reflexiv, symmetrisch und transitiv (d. h. Äquivalenzrelation).

Definition (Äquivalenzklasse)

Sei $x \in M$. Die **Äquivalenzklasse** von x ist die folgende Teilmenge von M

$$[x] := \left\{ y \in M \;\middle|\; (x,y) \in R \right\} \overset{\text{symmetrisch}}{=} \left\{ y \in M \;\middle|\; (y,x) \in R \right\}$$

alle Elemente von M in Relation mit x

Jedes Element einer Äquivalenzklasse heißt **Repräsentant** für diese Klasse.
Die Menge der Äquivalenzklassen heißt **Quotientenmenge**.

Beispiel

$M = \{\text{Geraden in } \mathbb{R}^2\}$ „parallel“
$R = \left\{(G, G') \;\middle|\; G, G' \text{ Geraden in } \mathbb{R}^2 \text{ und } G \parallel G'\right\}$
reflexiv: eine Gerade ist zu sich selbst parallel
symmetrisch: $G \parallel G' \implies G' \parallel G$
transitiv: $G \parallel G'$ und $G' \parallel G'' \implies G \parallel G''$

$$[G] = \{\text{die zu } G \text{ parallelen Geraden}\}$$

$\rightsquigarrow$ „Richtung von G“ Quotientenmenge:

$$\left\{[G] \;\middle|\; G \text{ Gerade}\right\}$$

(nicht-orientierte) Richtungen

Eigenschaften von Äquivalenzrelationen

(1) $\forall\, x \in M\colon x \in [x]$ (da $(x, x) \in R$, dank der Reflexivität)
Konsequenz: $[x] \neq \emptyset \quad \forall\, x \in M$
Konsequenz: $\bigcup\limits_{x \in M} [x] = M$
$\Big([x] \subseteq M \quad \forall x \implies \bigcup [x] \subseteq M\Big)$
$\Big(x \in [x] \implies M \subseteq \bigcup [x]\Big)$

(2) $(x, y) \in R \iff [x] = [y] \quad \forall\, x, y \in M$

Beweis

($\Rightarrow$)

Sei $(x, y) \in R$.
Sei $z \in [y]$. Dann $(z, y) \in R$. Wir wissen $(y, x) \in R$. Nach der Transitivität $(z, x) \in R$, d. h. $z \in [x]$.
Dann $[y] \subseteq [x]$.

Sei $(x, y) \in R$. Dann $(y, x) \in R$. Symmetrie. Analog folgt $[x] \subseteq [y]$

Insgesamt: $(x, y) \in R \implies [x] = [y]$.

($\Leftarrow$)

Sei $[x] = [y]$. Dann $y \in [y] = [x]$, d. h. $y \in [x]$. Also $(x, y) \in R$.

□

(3) Je zwei Äquivalenzklassen sind entweder gleich oder disjunkt.
$\forall\, x, y \in M\colon$ entweder $\underbrace{[x] = [y]}_{(x,y) \in R}$ oder $\underbrace{[x] \cap [y] = \emptyset}_{(x,y) \notin R}$

Beweis

siehe Skript.

□

Die Äquivalenzklassen ergeben eine Partition.

- nichtleere Teilmengen von M (siehe (1))
- die Vereinigung ist M (Konsequenz von (1))
- paarweise disjunkt (siehe (3))

„Die Quotientenmenge ist eine Partition von M."

Satz

Sei M eine nichtleere Menge.

(1) Die Quotientenmenge einer Äquivalenzrelation auf M ist eine Partition von M.

(2) Für jede Partition von M gibt es genau eine Äquivalenzrelation auf M, sodass die Partition und die Quotientenmenge übereinstimmen.

Beispiel

$M = \{1, 2, 3, 4\}$, $P\Big\{T_1 = \{1, 2\}, T_2 = \{3, 4\}\Big\}$ Partition

Relation:

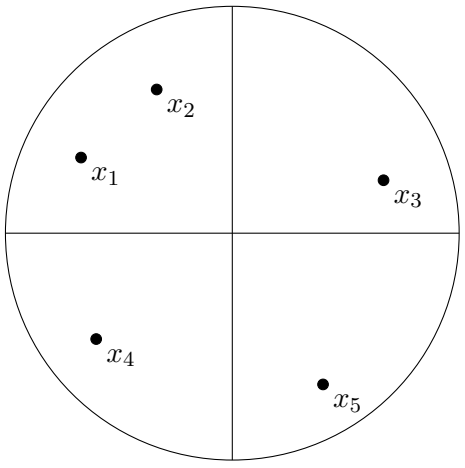
Symmetrie:	Reflexivität:	Transitivität sieht man.
$(1, 2) \in R$	$(1, 1) \in R$	$[1] = \{1, 2\} = T_1$
$(2, 1) \in R$	$(2, 2) \in R$	$[2] = \{1, 2\} = T_1$
$(3, 4) \in R$	$(3, 3) \in R$	$[3] = T_2$
$(4, 3) \in R$	$(4, 4) \in R$	$[4] = T_2$

Quotientenmenge $\{T_1, T_2\}$

Im Allgemeinen: Sei P eine Partition von M. Die gesuchte Äquivalenzrelation ist:

$\forall\, x, y \in M$: $(x, y) \in R$ genau dann, wenn es eine Teilmenge $T \subset P$ mit $\{x, y\} \in T$.

D. h. „x, y gehören zu derselben Teilmenge von M (der Partition)".



$(x_1, x_2) \in R$
$(x_1, x_3) \notin R$

Vorlesung 5 vom 30/10/2013

Beispiele von abzählbaren Mengen

(1) $\mathbb{N} \setminus \{0\}$

$\mathbb{N}$	0	1	2	3	4	...
$\mathbb{N} \setminus \{0\}$	1	2	3	4	5	...

$\mathbb{N} \longrightarrow \mathbb{N} \setminus \{0\} \quad , \quad n \longmapsto n+1$

Analog: $\mathbb{N} \setminus \{0, \ldots, 100\} \quad , \quad n \longmapsto n + 101$

(2) $2\mathbb{N}$ „die geraden natürlichen Zahlen“$= \left\{ 2t \;\middle|\; t \in \mathbb{N} \right\} = \{0, 2, 4, 6 \ldots\}$

$\mathbb{N}$	0	1	2	3	...
$2\mathbb{N}$	0	2	4	6	...

$\mathbb{N} \longrightarrow 2\mathbb{N} \quad , \quad n \longmapsto 2n \quad , \quad \#2\mathbb{N} = \#\mathbb{N}$

$\mathbb{N} \setminus 2\mathbb{N}$ „ungerade natürliche Zahlen“

$\mathbb{N}$	0	1	2	3	...
$\mathbb{N} \setminus 2\mathbb{N}$	1	3	5	7	...

$n \longmapsto 2n+1 \quad , \quad \#(\mathbb{N} \setminus 2\mathbb{N}) = \#\mathbb{N}$

(3) $\mathbb{Z}$

$\mathbb{N}$	0	1	2	3	4	5	6	...
$\mathbb{Z}$	0	1	-1	2	-2	3	-3	...

$$n \longmapsto \begin{cases} -\dfrac{n}{2} & \text{falls } n \text{ gerade} \\ \dfrac{n+1}{2} & \text{falls } n \text{ ungerade} \end{cases}$$

injektiv: $n \longmapsto -\frac{n}{2}$ und $n \longmapsto \frac{n+1}{2}$ beide injektiv; die Bildmengen sind disjunkt (negative bzw. streng positive Zahlen)

surjektiv: Sei $x \leq 0$. Ein Urbild von x ist $-2x$ (natürliche und gerade Zahl).
Sei $x \geq 1$. Ein Urbild von x ist $2x - 1$ (natürliche und gerade Zahl).
(bijektiv)

Anmerkung: Für unendliche Menge $A \subset B \implies \#A < \#B$ falsch. Gegenbeispiel: $A = \mathbb{N}$, $B = \mathbb{Z}$.
Aber $A \subseteq B \implies \#A \leq \#B$ wahr (die Inklusion ergibt eine Injektion).

(4) $\mathcal{P}$ Menge der Primzahlen

$\mathbb{N}$	0	1	2	3	5	...
$\mathcal{P}$	2	3	5	7	11	...

Wir bentuzen einen **Satz von Euklid**:

$$\mathcal{P} \subseteq \mathbb{N} \implies \#\mathcal{P} \leq \#\mathbb{N} \begin{cases} \#\mathcal{P} = \#\mathbb{N} \\ \#\mathcal{P} < \#\mathbb{N} \; \lightning \end{cases}$$ (die kleinste Mächtigkeit für unendliche Menge ist $\#\mathbb{N}$)

$\implies \mathcal{P}$ endlich: unmöglich

Abzählbare Vereinigung

$\rightsquigarrow$ die Indexmenge ist abzählbar
$\bigcup\limits_{i\in I} A_i$ mit $\#I \leq \#\mathbb{N}$ und A_i Mengen.

Proposition

Sei I eine abzählbare Menge. Für alle $i \in I$ sei A_i eine abzählbare Menge. Dann ist $\bigcup\limits_{i\in I} A_i$ abzählbar.

(5) $\mathbb{N}\times\mathbb{N} = \left\{(a,b) \;\middle|\; a,b\in\mathbb{N}\right\} = \underbrace{\bigcup\limits_{a\in\mathbb{N}}}_{\substack{\text{abzählbare}\\ \text{Vereinigung}}} \underbrace{\left\{(a,x) \;\middle|\; x\in\mathbb{N}\right\}}_{\text{abzählbare Menge}}$

(6) $\{\underline{\text{endliche}}\text{ Teilmenge von }\mathbb{N}\} \subsetneq \mathcal{P}(\mathbb{N}) = \underbrace{\bigcup\limits_{n\in\mathbb{N}}}_{\substack{\text{abzählbare}\\ \text{Vereinigung}}} \underbrace{\{\text{Teilmengen von } \mathbb{N} \text{ mit Mächstigkeit } n\}}_{\text{abzählbare Menge}}$

Beispiel

$\left\{A\subseteq\mathbb{N} \;\middle|\; \#A = 5\right\}$
$\xrightarrow[\text{injektiv}]{} \mathbb{N}^5$
$A = \{a_1,a_2,a_3,a_4,a_5\} \longmapsto (a_1,\ldots,a_5)$
$\#\mathbb{N}^5 = \#(\mathbb{N}\times\mathbb{N}\times\mathbb{N}\times\mathbb{N}\times\mathbb{N}) = \#\mathbb{N}$

Vorlesung 6 vom 31/10/2013

Aufgaben zur Induktion

(1) $\sum\limits_{k=0}^{n} k = \sum\limits_{k=1}^{n} k = \frac{n(n+1)}{2} \quad \forall\, n\in\mathbb{N}$ ($n\geq 0$ bzw. $n\geq 1$)

(2) n^2+n ist gerade $\forall\, n\in\mathbb{N}$

(3) Binomischer Lehrsatz: $\forall\, a,b\in\mathbb{R}$ gilt $(a+b)^n = \sum\limits_{k=0}^{n} \binom{n}{k} a^k b^{n-k} \quad \forall\, n\in\mathbb{N}$

(4) $\prod\limits_{k=2}^{n}\left(1-\frac{k-1}{k}\right) = \frac{1}{n!} \quad \forall\, n\in\mathbb{N},\ n\geq 2$

(5) $2^n > n+1 \quad \forall\, n\in\mathbb{N},\ n\geq 2$

(6) Ungleichung von Bernoulli: $(1+x)^n \geq 1+n\cdot x \quad \forall\, x\in\mathbb{R},\ x>-1,\ x\neq 0,\ \forall\, n\in\mathbb{N},\ n\geq 1$

(7) Rekursive FOlge $\left(a_1 = 2,\ a_{n+1} = 2-\frac{1}{a_n}\right)$. Dann ist $a_n = \frac{n+1}{n} \quad \forall\, n\in\mathbb{N},\ n\geq 1$

(8) Ableitungen: $f(x) = e^{ax+b} \quad , \quad f\colon \mathbb{R}\longrightarrow\mathbb{R},\ f^{(n)}(x) = a^n\cdot e^{ax+b} \quad \forall\, n\in\mathbb{N}$

Induktion

sehr wichtig und sehr klausurrelevant

- Beweise durch Induktion sind überall in der Mathematik.
- Oft ist der Beweis durch Induktion der einfachste Beweis.

Das Induktionsprinzip

Sei $M \subseteq \mathbb{N}$ und sei $0 \in M$. Sei auch wahr für alle $n \in \mathbb{N}$: $(n \in M \implies n+1 \in M)$. Dann $M = \mathbb{N}$.

Variante (Verallgemeinerung) des Induktionsprinzip

Sei $M \subseteq \mathbb{N}$ und sei $m_0 \in M$. Sei auch wahr für alle $n \in \mathbb{N}$: $(n \in M \implies n+1 \in M)$. Dann $\left\{ n \in \mathbb{N} \;\middle|\; n \geq m_0 \right\} \subseteq M$.
Bemerkung: Vorher war $m_0 = 0$.

Das Prinzip vom kleinsten Element

„Jede nichtleere Teilmenge von $\mathbb{N}$ besitzt ein Minimum." (bzgl. der Anordnung $\geq$)
Vorsicht: gilt NICHT für $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{Q}_{\geq 0}, \mathbb{R}_{\geq 0}$.

Sei $M \subseteq \mathbb{N}$. Ein **Minimum** für M ist eine Zahl $m_0 \in M$, sodass $\forall\, m \in M \; m_0 \leq m$ gilt.

Beispiele

- $\min(\mathbb{N}) = 0$
- $\min(\mathbb{N} \setminus 2\mathbb{N}) = 1$
- $\min(\mathcal{P}) = 2$

Das Prinzip des kleinesten Elementes $\implies$ Induktionsprinzip

Beweis

Wir haben $M \subseteq \mathbb{N}$, $0 \in M$, $(n \in M \implies n+1 \in M \quad \forall\, n \in \mathbb{N})$.
Zu zeigen: $M = \mathbb{N}$
Sei $M \neq \mathbb{N}$. Dann ist $\tilde{M} = \mathbb{N} \setminus M \neq \emptyset$. Wir benutzen das Prinzip vom kleinsten Element auf $\tilde{M}$: Sei $\tilde{m} \in \tilde{M}$ das Minimum von $\tilde{M}$.
Es gilt $\tilde{m_0} \neq 0$ (da $0 \in M$), d. h. $\tilde{m_0} \geq 1$, $\tilde{m_0} - 1 \in \mathbb{N}$. Da $\tilde{m_0}$ das Minimum von $\tilde{M}$ ist und $\tilde{m_0} \not\leq \tilde{m_0} - 1$ folgt $\tilde{m_0} - 1 \notin \tilde{M}$. Dann $\underbrace{\tilde{m_0} - 1}_{n} \in M$. Es folgt $\underbrace{\tilde{m_0} - 1}_{n} + 1 \in M$, d. h. $\tilde{m_0} \in M$. $\lightning$ Widerspruch: $\tilde{m_0} \in M$ und $\tilde{m_0} \in \mathbb{N} \setminus M = \tilde{M}$.

□

Die Beweismethode Induktion

Sei $P(n)$ eine Aussage für alle $n \in \mathbb{N}$. Wir wollen zeigen, dass $\forall\, n \in \mathbb{N}\ P(n)$ wahr ist.
Beweisschema

- Induktionsanfang: Wir zeigen, dass $P(0)$ wahr ist. ($n = 0$, die erste Aussage)
- Induktionsschritt: Wir beweisen, dass $\forall\, n \in \mathbb{N}$ die Implikation

$$\underbrace{P(n) \text{ wahr}}_{\text{Induktionsvoraussetzung}} \implies \underbrace{P(n+1) \text{ wahr}}_{\text{Induktionsbehauptung}}$$

gilt. Dann ist $P(n)$ für alle n wahr.

$M = \left\{ n \in \mathbb{N} \;\middle|\; P(n) \text{ ist wahr} \right\} \subseteq \mathbb{N}$, $P(0)$ ist wahr (I.A.) $\rightsquigarrow$ $0 \in M$; (I.S.) zeigt $(n \in M \implies n+1 \in M)$ $\forall\, n \in \mathbb{N}$; Nach dem Induktionsprinzip $M = \mathbb{N}$, d. h. $P(n)$ ist für alle $n \in \mathbb{N}$ wahr.

Variante der Beweismethode Induktion

Seien $P(n)$ $\forall\, n \in \mathbb{N}\ ,\ n \geq n_0$ Aussagen.
Beweisschema:

- Induktionsanfang: $P(n_0)$ ist wahr
- Induktionsschritt: $P(n)$ wahr $\implies$ $P(n+1)$ wahr $\forall\, n \in \mathbb{N}\ ,\ n \geq n_0$

Dann ist $P(n)$ $\forall\, n \in \mathbb{N}\ ,\ n \geq n_0$ wahr.

Bearbeitung der obigen Aufgaben

Aufgabe 1

$\sum_{k=0}^{n} k = \frac{n(n+1)}{2}$ $\longleftarrow$ $P(n)$ ist diese Formel für n.
Beispiel: $P(7)$: $\sum_{k=0}^{7} k = \frac{7 \cdot 8}{2} = 28$

I.A.: $n = 0$
$P(0)$: $\sum_{k=0}^{0} k = \frac{0(0+1)}{2}$ wahr, da $\sum_{k=0}^{0} k = 0$ und $\frac{0(0+1)}{2} = 0$

$P(n)$: $\sum_{k=0}^{n} k = \frac{n(n+1)}{2}$
$P(n)$: $\sum_{k=0}^{n+1} k = \frac{(n+1)\big((n+1)+1\big)}{2} = \frac{(n+1)(n+2)}{2}$

Zu zeigen: $P(n)$ wahr $\Longrightarrow$ $P(n+1)$ wahr $\forall\ n \in \mathbb{N}$

$$\sum_{k=0}^{n+1} k = \sum_{k=0}^{n} k + \sum_{k=n+1}^{n+1} k = \underbrace{\sum_{k=0}^{n}}_{\overset{\text{I.V.}}{=} \frac{n(n+1)}{2}} + (n+1)$$

$$= \frac{n(n+1)}{2} + (n+1) = \frac{(n+1)(n+2)}{2}$$

Wäre $\sum\limits_{k=1}^{n} k$, dann ist $n = 1$ der erste Fall.

I.A.: $(n=1)$: $\underbrace{\sum\limits_{k=1}^{1} k}_{=1} = \underbrace{\frac{1(1+1)}{2}}_{=1}$

Aufgabe 2

$P(n)$: $n^2 + n$ ist gerade $\forall\ n \in \mathbb{N}$

I.A.: $(n=0)$: $\underbrace{0^2+0}_{=0}$ ist gerade (0 ist gerade)

I.S.: $P(n)$: n^2+n ist gerade , $P(n+1)$: $\underbrace{(n+1)^2+(n+1)}_{= \underbrace{(n^2+n)}_{\text{gerade nach I.V.}} + \underbrace{2(n+1)}_{\text{gerade}}}$ ist gerade

(Eine Summe von geraden Zahlen ist gerade.)

Dann $\forall\ n \in \mathbb{N}$: $P(n)$ wahr $\Longrightarrow$ $P(n+1)$ wahr.

Dann ist $p(n)$ $\forall\ n \in \mathbb{N}$ wahr.

Aufgabe 3

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

I.A.: $(n=0)$: $(a+b)^0 = \underbrace{\sum\limits_{k=0}^{0} \binom{0}{k} a^k b^{0-k}}_{\binom{0}{0}a^0b^0=1}$

$a \neq 0$, $a \neq -b$, $b \neq 0$, 0^0 (?)

$(a+b)^0 = 1$

I.S.:

$$(a+b)^{n+1} = \underbrace{(a+b)^n}_{\overset{\text{I.V.}}{=} \sum\limits_{k=0}^{n} \binom{n}{k} a^k b^{n-k}} \cdot (a+b)$$

$$= \left(\sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}\right) \cdot (a+b) = \sum_{k=0}^{n} \binom{n}{k} a^{k+1} b^{n-k} + \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$

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

Hilfsformel: $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1} \quad \forall\, n, k \geq 1$ (Aufgabe)
Zu zeigen: $\frac{n!}{k!(n-k)!} = \frac{(n-1)!}{k!(n-1-k)!} + \frac{(n-1)!}{(k-1)!\big((n-1)-(k-1)\big)!}$

Aufgabe 4

I.A.: $(n=2)$: $\underbrace{\prod_{k=2}^{2}\left(1-\frac{k-1}{k}\right)}_{=\frac{1}{2}} = \underbrace{\frac{1}{2!}}_{=\frac{1}{2}}$

I.S.:

$$\prod_{k=2}^{n+1}\left(1-\frac{k-1}{k}\right) = \underbrace{\left(\prod_{k=2}^{n}\left(1-\frac{k-1}{k}\right)\right)}\cdot\underbrace{\left(1-\frac{(n+1)-1}{(n+1)}\right)}_{\frac{1}{n+1}}$$
$$= \frac{1}{n!}\cdot\frac{1}{(n+1)} = \frac{1}{(n+1)!}$$

Aufgabe 5

I.A.: $(n=2)$: $2^2 > 2+1$ wahr
I.S.: $2^{n+1} = \underbrace{2^n\cdot 2 > (n+1)\cdot 2}_{\text{I.V.}} = 2n+2 > n+2 = (n+1)+1$

Aufgabe 6

Sei x fixiert.
I.A.: $(n=1)$: $(1+x)^1 \geq 1+x$ wahr
I.S.:

$$(1+x)^{n+1} = (1+x)^n\cdot\underbrace{(1+x)}_{\geq 0} \geq (1+nx)(1+x)$$
$$= 1+nx+x+nx^2 = 1+(n+1)x+\underbrace{nx^2}_{\geq 0} \geq 1+(n+1)x$$

Aufgabe 7

I.A.: $(n=1)$: $a_1 = \frac{1+1}{1} = 2$ wahr, da $a_1 = 2$.
I.S.:

$$a_{n+1} \overset{\text{Def.}}{=} 2-\frac{1}{a_n} \overset{\text{I.V.}}{=} 2-\frac{1}{\frac{n+1}{n}} = 2-\frac{n}{n+1}$$
$$= \frac{2n+2-n}{n+1} = \frac{n+2}{n+1} = \frac{(n+1)+1}{n+1}$$

Aufgabe 8

I.A.: $(n = 0)$: $f^{(0)}(x) = f(x)$, also zu zeigen: $\underbrace{f^{(0)}(x)}_{f(x)} = \underbrace{a^0 \cdot e^{ax+b}}_{e^{ax+b}}$

I.S.:

$$f^{(n+1)}(x) = \left(f^{(n)}(x)\right)' = (a^n \cdot e^{ax+b})' = a^n (e^{ax+b})'$$
$$= a^n \cdot e^{ax+b} \cdot a = a^{n+1} \cdot e^{ax+b}$$

Vorlesung 7 vom 06/11/2013

Ein falscher Beweis – finde den Fehler

Aussage: Alle Pferde haben dieselbe Farbe.

Beweis (Induktion)

Wir betrachten eine Menge von n Pferden, $(n \geq 1)$.

I.A. $n = 1$ nur ein Pferd, dann nur eine Farbe

I.S. $(n \geq 1)$ I.V.: jede beliebige n Pferde haben dieselbe Farbe

I.B.: jede beliebige $n + 1$ Pferde haben dieselbe Farbe.

Sei $M = \{P_1, \ldots, P_{n+1}$.

$M = M_1 \cup M_2 \quad , \quad M_1 = M \setminus \{P_{n+1}\} \quad , \quad M_2 = M \setminus \{P_1\}$

Alle Pferde in M_1 haben dieselbe Farbe F_1 (da $\#M_1 = n$; nach I.V.)

Alle Pferde in M_2 haben dieselbe Farbe F_2 (da $\#M_2 = n$; nach I.V.)

P_n hat die Farbe F_1, da $P_n \in M_1$

P_n hat die Farbe F_2, da $P_n \in M_2$

↯ hier liegt das Problem bei $n = 1$: $P_1 \notin M_2$

Ansonsten folgte $F_1 = F_2$

Alle Pferde in M haben dieselbe Farbe.

□

Wahr Aussage: Falls je zwei Pferde dieselbe Farbe haben, dann haben alle Pferde dieselbe Farbe.

Aufgabe 1

Seien N, M nicht-leere Mengen. Sei $\#N = n, \#M = m$. Sei $A = \{f \colon N \longrightarrow M\}$ die Menge der Funktionen von N nach M.

Zu zeigen: $\#A = m^n$ **Beweis** (Induktion)

Wir nehzmen M fest und zeigen die Eigenschaft $\forall\ N$.

Induktion auf $n = \#N$ $(n \geq 1)$

I.A. $n = 1$

Sei $\#N = 1$, $N = \{a_1\}$

$f \colon N \longrightarrow M \iff f(a_1)$ zu wählen, $\#M$ Möglichkeiten; $m = m^1 = m^n$

I.S. I.V.: Die Aussage gilt für Mengen mit n Elementen.

I.B.: Die Aussage gilt für $n+1$ Elemente.

Bemerkung: jeweils gilt $n \geq 1$

$N = \{a_1, \ldots, a_{n+1}\}$

$N' = \{a_1, \ldots, a_n\} \quad , \quad A' = \{f \colon N' \longrightarrow M\} \quad , \quad \#A' = m^n$ nach I.V.

Zu zeigen: $A = \{f \colon N \longrightarrow M\} \quad , \quad \#A = m^{n+1}$

Jede Funktion in A ist die Fortsetzung einer Funktion A' (die Einschränkung zu N' ist in A')

Jede Funktion A' können wir fortsetzen. Genau m Fortsetzungen (nur das Bild $f(a_{n+1})$ ist zu wählen).

$\underbrace{m^n}_{\#A'} \cdot \underbrace{m}_{\#A} = m^{n+1}$

□

Aufgabe 2

Sei M eine Menge mit $n \geq 1$ Elementen. Es gibt genau $n!$ Bijektionen von M auf M.

$n! = n(n-1)(n-2) \cdot \ldots \cdot 2 \cdot 1 \quad , \quad n! \ll n^n$

$n!$: bijektive Funktionen $M \longrightarrow M \quad , \quad n^n$ Alle Funktionen $M \longrightarrow M$.

Beweis (Induktion)

Wir beweisen:

M_1, M_2 Mengen mit $\#M_1 = \#M_2 = n$, dann $B = \{f \colon M_1 \longrightarrow M_2$, bijektiv$\}$ gilt $\#B = n!$.

Induktion auf $n \quad (n = \#M_1 = \#M_2) \ , \ n \geq 1$

I.A. $n = 1$

$M_1 = \{a_1\} \quad , \quad M_2 = \{b_1\} \quad , \quad f \colon M_1 \longrightarrow M_2 \ , \ a_1 \longmapsto b_1$ genau eine Funktion und die ist bijektiv $\rightsquigarrow \ 1 = 1!$

I.S. I.V.: die Formel gilt für Mengen mit n Elementen

I.A.: die Formel gilt für Mengen mit $n+1$ Elementen

Sei $\#M_1 = \#M_2 = n+1$

Zu zeigen: $\#\{f \colon M_1 \longrightarrow M_2$, bijektiv$\} = (n+1)!$

$M_1 = \{a_1, \ldots, a_{n+1}\} \quad , \quad M_2 = \{b_1, \ldots, b_{n+1}\}$

$M_1' = \{a_1, \ldots, a_n\} = M \setminus \{a_{n+1}\}$

Sei $f \colon M_1 \longrightarrow M_2$ eine bijektive Funktion.

Dann ist die Funktion

$$f\Big|_{M_1'} \colon M_1' \longrightarrow M_2 \setminus \{f(a_{n+1})\}$$

noch bijektiv.

(1) Wähle b in M_2 als Bild von a_{n+1}
$f(a_{n+1}) = b$

(2) Dann haben wir eine bijektive Funktion $M_1' \longrightarrow M_2 \setminus \{b\}$ ($n!$ Funktionen)
Wir haben $n+1$ Wahlen für b.

Mit jedem b haben wir $n!$ Funktionen.
Insgesamt: $(n+1) \cdot n! = (n+1)!$ ✓

□

Reduktion auf $n = 2$

Satz

Seien A_1, A_n Mengen. Dann $\#(A_1 \times A_2 \times \ldots \times A_n) = \prod_{i=1}^{n} \#A_i$
$(A_1 \times A_2 \times \ldots \times A_n)$ sind geordnete n-Tupel $(a_1, \ldots, a_n)$ mit a_i in A_i.

Beweis

„Der wichtigeste Fall ist $n = 2$."
$n = 1$: $\#(A_1) = \#A_1$ klar
$n = 2$: $A \times B \quad , \quad \#A = \alpha \quad , \quad \#B = \beta$
Zu zeigen: $\#(A \times B) = \alpha \cdot \beta$
Induktion: A fest, Induktion auf $\beta \geq 0$
$\beta = 0$ einfach
$\beta = m + 1 \;\; , \;\; B = B' \cup \{c\} \;\; , \;\; (a, b) \longrightarrow \begin{cases} b \in B' \\ b = c \end{cases}$ $\rightsquigarrow$ Übungsaufgabe
Allgemein: Induktion, mit Hilfe auch von dem Fall $n = 2$
$A_1 \times \ldots \times A_n \times A_{n+1} \overset{\text{bijektion}}{\longleftrightarrow} \underbrace{(A_2 \times \ldots \times A_n)}_{=:A'} \times A_{n+1}$
$(a_1, \ldots, a_{n+1}) \longmapsto \big((a_1, \ldots, a_n), a_{n+1}\big)$

$$\#(A_1 \times \ldots \times A_{n+1}) = \#(A' \times A_{n+1}) \overset{\text{Fall 2 Mengen}}{=} \#A' \cdot \#A_{n+1}$$
$$\overset{\text{I.V.}}{=} \left(\prod_{i=1}^{n} \#A_i\right) \cdot \#A_{n+1} = \prod_{i=1}^{n+1} \#A_i$$

□

Beispiel

Warum ist die Summe von n ganzen Zahlen kommutativ?
Bekannt: $\forall\, a, b \in \mathbb{Z}$: $a + b = b + a$ (Kommutativität der Summe)
Aus dem Fall $n = 2$ folgt der allgemeine Fall.

Erweiterte Induktionsvoraussetzung

der normale I.S.: $\underbrace{P(n)}_{\text{I.V.}} \implies \underbrace{P(n+1)}_{\text{I.B.}}$

mit erweiterte Induktionsvoraussetzung: $\underbrace{\Big(P(0) \text{ und } P(1) \text{ und } \ldots \text{ und } P(n)\Big)}_{\text{die neue I.V.}} \implies P(n+1)$

der I.S. ist einfacher zu beweisen!!

Aufgabe

Fibonacci Zahlen: 0,1,1,2,3,5,8,13,21,...

rekursive Folge

$a_0 = 0$

$a_1 = 1$

$a_n = a_{n-2} + a_{n-1} \quad \forall\ n \geq 2$

Beweis (Induktion)

$a_n = \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right]$

$a_0 = \frac{1}{\sqrt{5}}[1-1] = 0$ wahr

$a_1 = \frac{1}{\sqrt{5}} \cdot \frac{1+\sqrt{5}-1+\sqrt{5}}{2} = 1$ wahr

$\varphi := \frac{1+\sqrt{5}}{2}$

$\psi := \frac{1-\sqrt{5}}{2}$

Zu zeigen: $a_n = \frac{1}{\sqrt{5}}(\varphi^n - \psi^n)$

Benutze die Formel $a_n = a_{n-2} + a_{n-1}$

Falls $a_{n_2} = \frac{1}{\sqrt{5}}(\varphi^{n-2} - \psi n - 2)$

und $a_{n-1} = \frac{1}{\sqrt{5}}(\varphi^{n-1} - \psi^{n-1})$

dann ist $a_{n-2} + a_{n-1} = \frac{1}{\sqrt{5}}(\varphi^n - \psi^n)$

□

Vorlesung 8 vom 07/11/2013

Gruppen

Gruppen, abelsche Gruppen „abelsch=kommutativ“

Verknüpfung

Sei A eine nicht-leere Menge.

Eine **Verknüpfung** auf A ist eine Funktion

$$*\colon A \times A \longrightarrow A \quad , \quad (a,b) \longmapsto *(a,b) \quad , \quad a,b \in A$$

$a * b \quad , \quad a, b \longmapsto a * b$

Beispiel

$\mathbb{Z}, *$
$a * b = 7 \quad \forall\, a, b \in \mathbb{Z}$
$(a, b) \longmapsto 7$

Eigenschaften

- **kommutativ**: $\forall\, a, b \in A$: $a * b = b * a$
- **assoziativ**: $\forall\, a, b, c \in A$: $\underbrace{(a * b)}_{\in A} * c = a * \underbrace{(b * c)}_{\in A}$
- **neutrales Element**: ein Element $e \in A$, sodass $\forall\, a \in A$ gilt: $e * a = a * e = a$
  $\exists\, e \in A \colon \forall\, a \in A \quad e * a = a * e = a$
  e ist NICHT von a abhängig!
- **inverses Element**: Sei $a \in A$. Ein Element $a' \in A$ heißt Inverses zu a, falls $a * a' = a' * a = e$
  a' ist von a abhängig.
  $\forall\, a \in A\ \exists\, a' \in A \colon a * a' = a' * a = e$

Wenn eine Verknüpfung KEIN neutrales Element hat, dürfen wir NICHT von Inversen sprechen (e in der Definition ist das neutrale Element).

Proposition

Das neutrale Element ist eindeutig (falls es existiert, dann gibt es genau eins).

Beweis

Seien e, e' neutrale Elemente. Zu zeigen: $e = e'$!
Für alle $a \in A$ gilt: $a * e = e * a = a$
Für alle $b \in A$ gilt: $b * e = e * b = b$
$e = e * e' = e'$. Dann ist $e = e'$

□

Proposition

Sei $*$ assoziativ und mit neutralem Element. Dann sind die Inversen eindeutig.

Beweis

Sei $a \in A$. Seien b und c Inverse zu a. Zu zeigen: $b = c$
Wir haben $a * b = b * a = e$ und $a * c = c * a = e$
$b = b * e = b * (a * c) = (b * a) * c = e * c = c$

□

Definition

Eine nicht-leere Menge A mit einer Verknüpfung $*$ ($*\colon A \times A \longrightarrow A$) heißt **Gruppe**, falls $*$ assoziativ ist, ein neutrales Element besitzt und jedes Element von A ein Inverses hat.
Falls $*$ auch kommutativ ist: **abelsche Gruppe**

Beispiel

- $(\mathbb{Z}, +)$: abelsche Gruppe mit neutralem Element 0, Inverses zu a ist $-a$
- $(\mathbb{Z}, \cdot)$: KEINE Gruppe, neutrales Element 1, aber $a \cdot x = 1$ hat KEINE Lösung $x \in \mathbb{Z}$, außer für $a = \pm 1$ ($x = \pm 1$).
- $(\mathbb{R}, +)$: abelsche Gruppe
- $(\mathbb{Q}, +)$: abelsche Gruppe
- $(\mathbb{N}, +)$: 0 neutrales Element, $a + x = 0$ hat KEINE Lösung $x \in \mathbb{N}$ (außer für $a = 0$, $x = 0$)
- $(\mathbb{Q}, \cdot)$: assoziativ (kommutativ) neutrales Element 1, Inverses zu 0 gibt es NICHT
  $\Longrightarrow$ KEINE Gruppe

Beispiele

$A = \{f\colon \mathbb{R} \longrightarrow \mathbb{R}\}$ $(A, +)$ abelsche Gruppe: $(f+g)(x) := f(x) + g(x) \quad \forall\, x \in \mathbb{R}$
neutrales Element $f \equiv 0$ konstant
Inverses $-f$

$(A, \cdot)$: KEINE Gruppe (Inverse?)

$(B, \cdot)$: $B \subseteq A \quad B = \{f\colon \mathbb{R} \longrightarrow \mathbb{R}_{\neq 0}\}$ KEINE Nullstellen
$(f \cdot g)(x) := f(x) \cdot g(x) \quad \forall\, x \in \mathbb{R}$
neutrales Element $f \equiv 1$
Inverses $\frac{1}{f}(x) = \frac{1}{f(x)} \in \mathbb{R}_{\neq 0}$

Proposition

Sei $(A, *)$ eine Gruppe. Es gilt: $(a * b)^{-1} = b^{-1} * a^{-1}$.
Das Inverse zu $a * b$ ist das Inverse von b verknüpft mit dem Inversen zu a ($\forall\, a, b \in A$).

Beweis

$(a * b) * (b^{-1} * a^{-1}) = a * (b * b^{-1}) * a^{-1} = a * e * a^{-1} = a * a^{-1} = e$
Analog: $(b^{-1} * a^{-1}) * (a * b) = e$. Dann ist $b^{-1} * a^{-1}$ das Inverse zu $a * b$.

□

Proposition

Kürzungsregeln in Gruppe: Sei $(A, *)$ eine Gruppe.
$\forall\ a, b, c \in A$: $a * c = b * c \implies a = b$
Analog: $c * a = c * b \implies a = b$

Beweis

$$a = a * e = a * (c * c^{-1}) = (a * c) * c^{-1} = (b * c) * c^{-1} = b * (c * c^{-1}) = b * e = b$$

□

Proposition

Sei $(A, *)$ eine Gruppe. ine Gleichung der Form $a * x = b$ hat als Lösungsmenge $\{a^{-1} * b\}$.
Analog, für $x * a = b$, $b * a^{-1}$

Bemerkung: $\{f : \mathbb{R} \longrightarrow \mathbb{R}\}$, $\circ$Verkettung
$f(x) = x^3$, $g(x) = e^x$
$(g \circ f)(x) = e^{x^3}$
$(f \circ g)(x) = (e^x)^3 = e^{3x}$

Eine nicht-abelsche Gruppe: $\{f : \mathbb{R} \longrightarrow \mathbb{R}$ bijektiv, $\circ$ Verkettung

- **assiziativ**: $h \circ (g \circ f) = (h \circ g) \circ f \quad \forall\ f, g, h$
- **neutrales Element**: $x \longmapsto h\Big(g(f(x))\Big)$
  die Identität $x \longmapsto x$
- **Inverse**: die Umkehrfunktion (Ok, da bijektive Funktionen)
- **NICHT kommutativ**

Vorlesung 9 vom 13/11/2013

Ringe und Körper

Erinnerung

$(A, *)$ ist eine Gruppe, falls die Verknüpfung

(1) assoziativ ist.

(2) ein neutrales Element besitzt.

(3) jedes Element von A ein Inverses besitzt.

Verknüpfung auf einer Menge A ist eine Funktion $*: A \times A \longrightarrow A$.

Sei $(A, *)$ eine Gruppe. Die **Ordnung** der Gruppe ist die Mächtigkeit von A.

Beispiel

$A = \{g, u\}$, $g * g = u * u = g$, $u * g = g * u = u$ abelsche Gruppe der Ordnung 2

Untergruppen

Sei $(A, *)$ eine Gruppe. Dann ist eine Untergruppe von A eine Teilmenge U von A, sodass U eine Gruppe ist, mit der Einschränkung von $*$:

$$*\colon A \times A \longrightarrow A$$

$$\tilde{*} = *\Big|_{U \times U} \colon U \times U \longrightarrow A \quad , \quad U \times U \subseteq A \times A$$

Frage: Ist $\tilde{*}$ eine Verknüpfung auf U? Ist $(U, \tilde{*})$ eine Gruppe?

(1) abgeschlossen: $\tilde{*}\colon U \times U \longrightarrow A$. Ist die Bildmenge in U enthalten?

Beispiel

$(2\mathbb{Z}, +)$ gerade Zahlen
$g_1, g_2 \in \mathbb{Z}$ die gerade sind. Dann ist $g_1 + g_2 \in \mathbb{Z}$ $(\mathbb{Z}, +)$ ist eine Gruppe
Ist $g_1 + g_2$ gerade?
$U \subseteq \mathbb{Z}$ $U = 2\mathbb{Z}$, U ist abegschlossen für die Summe.

$U = \mathbb{Z} \setminus 2\mathbb{Z}$ ungerade Zahlen
Ist $u_1 + u_2 \in U$, falls $u_1, u_2 \in U$? NEIN. Gegenbeispiel: $1 + 1 = 2$ $u_1 + u_2 = g$

$(\mathbb{Z}, \cdot)$
$U = 2\mathbb{Z}$ abgeschlossen
$(2\mathbb{Z}, \cdot)$

$U = \mathbb{Z} \setminus 2\mathbb{Z}$ abgeschlossen
$(\mathbb{Z} \setminus 2\mathbb{Z}, \cdot)$ wohldefinierte Verknüpfung

(2) Ist $\tilde{*}$ assoziativ? Ja, automatisch (da $(A, *)$ assoziativ war)
$\forall\ a, b, c \in U\colon \ (a \tilde{*} b) \tilde{*} c = a \tilde{*} (b \tilde{*} c)$
Betrachte $a, b, c \in A\colon \ (a * b) * c = a * (b * c)$ folgt aus der Assoziativität von $*$

Beispiel

$a, b, c \in 2\mathbb{Z}$
$a + (b + c) = (a + b) + c$ weil a, b, c auch ganze Zalen sind.

(3) Besitzt $\tilde{*}$ ein neutrales Element?
Sei e das neutrale Element für $(A, *)$. Falls $e \in U$, dann ist e ein neutrales Element für $(U, \tilde{*})$.

Beispiel

$(\mathbb{Z} \setminus 2\mathbb{Z}, \cdot)$ neutrales Element $(\mathbb{Z}, \cdot)$ neutrales Element 1
1 funktioniert
$(2\mathbb{Z}, +)$ neutrales Element $(\mathbb{Z}, +)$ neutrales Element 0
$0 \in 2\mathbb{Z}$ ✓ funktioniert
$(0 + g = g + 0 = g \quad \forall\, g \in 2\mathbb{Z})$
$(2\mathbb{Z}, \cdot)$ neutrales Element? $(\mathbb{Z}, \cdot)$ neutrales Element 1
$1 \notin 2\mathbb{Z}$ suche $g \in 2\mathbb{Z}$, sodass $g \cdot a = a \cdot g = a \quad \forall\, a \in 2\mathbb{Z}$. KEINE Lösung.
$(g \cdot a = a \implies g = 1$, aber $1 \notin 2\mathbb{Z})$

(4) Gibt es Inverses? Sei $a \in U$. Falls a^{-1} (Inverses bzgl. $\tilde{*}$ auf A) in U ist, dann a^{-1} ist auch das Inverse bzgl. $\tilde{*}$.
„$a \in U \implies a^{-1} \in U$“ ?

Beispiel

$(2\mathbb{Z}, +)$, $-g$ ist gerade $\forall\, g$ gerade
Dann ist $(2\mathbb{Z}, +)$ eine Gruppe und eine Untergruppe von $(\mathbb{Z}, +)$.

Triviale Untergruppen:

- $(A, *)$, $A \subseteq A$
- $(\{e\}, \tilde{*})$, $\{e\} \subseteq A$, $e\tilde{*}e = e$
  $(e$ ist das neutrale Element von $(A, *)$; insbesondere $e * e = e)$

$(\mathbb{Z}, +)$, $(\{0\}, +)$, $0 + 0 = 0$
$(\mathbb{Z}, \cdot)$, $(\{1\}, \cdot)$, $1 \cdot 1 = 1$

Bemerkung

- $(A, *)$ kommutativ $\implies$ $(U, \tilde{*})$ kommutativ
- Falls $(A, *)$ abelsche Gruppe und $(U, \tilde{+})$ eine Gruppe
  $\implies$ $(U, \tilde{*})$ abelsche Gruppe
  Erklärung: $\forall\, a, b \in A\colon \; a * b = b * a$
  $\implies \forall\, a, b \in U\colon \; a\tilde{*}b = b\tilde{*}a$

Beispiel

$(2\mathbb{Z}, +)$ abelsche Gruppe
$(\mathbb{Z} \setminus 2\mathbb{Z}, \cdot)$ kommutativ, aber KEINE Gruppe (Inverse fehlen)
$\rightsquigarrow$ kommutativ, da $(\mathbb{Z}, \cdot)$ kommutativ.

Definition RING

Eine Menge R mit 1. Verknüpfung $+$ und 2. Verknüpfung $\cdot$ heißt **Ring**, falls:

(1) $(R, +)$ abelsche Gruppe

(2) $(R, \cdot)$ assoziativ

(3) Distributivgesetze: $\forall\ a, b, c \in R$ gilt:

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c) \quad \text{und} \quad (a + b) \cdot c = a \cdot c + b \cdot c$$

Notation: $(R, +, \cdot)$

Beispiel

$(\mathbb{Z}, +, \cdot)$ ist ein Ring
ein kommutativer Ring: $\cdot$ ist kommutativ
ein Ring mit Eins: $\cdot$ hat ein neutrales Element $(1 \in \mathbb{Z})$
Problem mit Inversen: Welche $a \in \mathbb{Z}$ haben ein multiplikatives Inverses?
1 hat Inverses -1
-1 hat Inverses -1
$a \in \mathbb{Z} \setminus \{-1, 1\}$ hat KEIN multiplikatives Inverses in $\mathbb{Z}$.

Bemerkung

Inverse bzgl. $+$ existieren: $(R, +)$ ist eine Gruppe
Inverse bzgl. $\cdot$ existieren NICHT UNBEDINGT. Die ELemente mit einem Inversen für die zweite Verknüpfung heißen **Einheiten**.
Für den Ring $\mathbb{Z}$ sind die Einheiten ± 1.

Sei $E \subseteq R$ die Teilmenge der Einheiten. Falls R ein Ring mit 1 ist, dann ist $(E, \cdot)$ eine Gruppe.

Beispiel

$(\mathbb{Z}, \cdot)$, $E = \{\pm 1\}$, $(-1) \cdot (-1) = 1$, $1 \cdot 1 = 1$
assoziative, 1 neutrales Element, Inverse: $1 \longrightarrow 1$, $-1 \longrightarrow -1$

Proposition

Sei $(R, +, \cdot)$ ein Ring. Dann gilt:

(1) $\forall\ a \in R$: $a \cdot 0_R = 0_R \cdot a = 0_R$ wobei 0_R das neutrale Element für $(R, +)$ ist

Beweis

$(a \cdot 0_R = 0_R)$
$a \cdot 0_R = a(0_R \cdot 0_R) = a \cdot 0_R + a \cdot 0_R$ 0_R neutrales Element für die Summe
$a \cdot 0_R + (-a \cdot 0_R) = a \cdot 0_R + a \cdot 0_R + (-a \cdot 0_R)$

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

□

(2) $\forall\, a, b \in R$: $\underbrace{(-a)}_{+\text{-Inv. zu } a} \cdot b = a \cdot \underbrace{(-b)}_{+\text{-Inv. zu } b} = -\underbrace{(ab)}_{+\text{-Inv. zu } ab}$

Vorlesung 10 vom 14/11/2013

$\sigma\colon \{1,2,3,\ldots,n\} \longrightarrow \{1,2,3,\ldots,n\}$ **Partition**

$$\begin{array}{cc} \text{Elemente} & \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 8 & 6 & 7 & 5 & 1 & 3 & 2 & 4 \end{pmatrix} \quad n = 8 \\ \text{Bilder} & \end{array}$$

$1 \longrightarrow 8 \longrightarrow 4 \longrightarrow 5$ $\qquad$ $2 \longrightarrow 6 \longrightarrow 3 \longrightarrow 7$

Zykeln: (1845)(2637)

Partition $\mathcal{P} = \{P_1, P_2\}$, $P_1 = \{1,4,5,8\}$, $P_2 = \{2,3,6,7\}$

Gruppe

$(A, *)$ assoziativ; neutrales Element; Inverse

Ring

$(R, +, \cdot)$, $(R, +)$ abelsche Gruppe; $(R, \cdot)$ assoziativ; Distributivgesetz
& neutrales Element „Ring mit Eins“
& kommutativ „kommutativer Ring“
Inverse? „Selten“ Die Elemente mit Inversen heißen Einheiten.

Proposition

In einem Ring $(R, +, \cdot)$ gilt:

$$\forall\, a, b \in R: \quad \underbrace{(-a)}_{+\text{-Inv. zu } a} \cdot b = a \cdot \underbrace{(-b)}_{+\text{-Inv. zu } b} = -\underbrace{(ab)}_{+\text{-Inv. zu } ab}$$

Beweis

(nur, dass $(-a) \cdot b = -(ab)$)
zu zeigen: $(-a) \cdot b$ ist das Inverse zu ab.
Also zu zeigen: $[(-a) \cdot b] + [ab] = O_R$ und $[ab] + [(-a) \cdot b] = 0_R$
nur 1. Gleichung:

$$(-a) \cdot b + a \cdot b \overset{\text{distr.}}{=} (-a + a) \cdot b \overset{-a \text{ +-Inv. zu } a}{=} 0 \cdot b \overset{\text{VL}}{=} 0$$

□

Beispiel

$(\mathbb{Z}, +, \cdot)$ Ring
Dann $(-3)(-5) = -(3 \cdot (-5)) = 15$
Zweimal die Proposition; Zwei Minuse sind Plus
Das Inverse des Inversen ist das ursprüngliche Element.

Unterring

Eine Teilmenge eines Ringes, die noch ein Ring ist mit den Eigenschaften der zwei Verknüfungen.

Beispiel

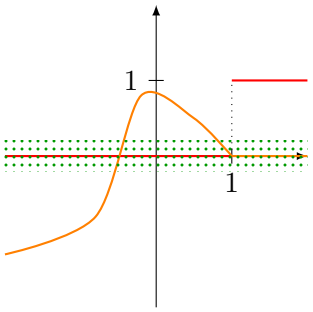
$(\mathbb{Z}, +, \cdot)$ Ring
$(2\mathbb{Z}, +, \cdot)$ Unterring $(0 \in 2\mathbb{Z}\ ,\ -g \in 2\mathbb{Z} \quad \forall\ g \in frm{-}e\mathbb{Z})$
$(0, +, \cdot)$ Nullring $(0 + 0 = 0\ ,\ 0 \cdot 0 = 0)$

Nullteiler in Ringen

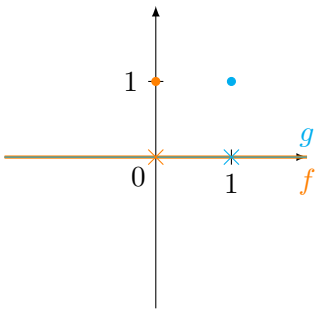
Sei $(R, +, \cdot)$ ein kommutativer Rung. Dann $a \in R$ heißt **Nullteiler**, falls $a \neq 0_R$ und $\exists\ b \in R \setminus \{0_R\}$.

Beispiele

$(\mathbb{Z}, +, \cdot)$ KEINE Nullteiler
$(F, +, \cdot)$, $F = \{\mathbb{R} \longrightarrow \mathbb{R}\}$, $(f + g\ ,\ f \cdot g)$
$f \neq 0$, sodass $\exists\ g \neq 0$ mit $f \cdot g = 0$ ($\forall\ x \in \mathbb{R}$: $f(x) \cdot g(x) = 0$, aber $\forall\ x$: $f(x) = 0$ fasch; $\forall\ x$: $g(x) = 0$ falsch)



$$f(x) = \begin{cases} 1 & x = 0 \\ 0 & x \neq 0 \end{cases} \qquad g(x) = \begin{cases} 1 & x = 1 \\ 0 & x \neq 1 \end{cases}$$



Beispiel

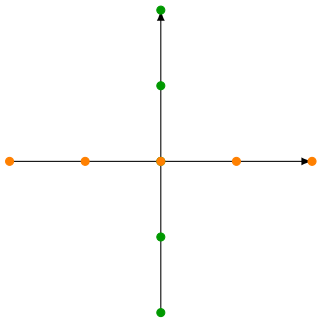
$\mathrm{Mat}_{2\times 2}(\mathbb{R}) \quad +, \cdot$
$M = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \quad a_{ij} \in \mathbb{R}$
Detail: dieser Ring ist NICHT kommutativ
$A = \begin{pmatrix} 0 & 1 & 0 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 0 & 1 & 0 & 0 \end{pmatrix}$, $A \cdot A = \begin{pmatrix} 0 & 0 & 0 & \end{pmatrix}$
$A \cdot B = B \cdot A = 0$ (die Matrix Null)

Nullteiler

$\exists\ a, b \neq 0$, sodass $a \cdot b = b \cdot a = 0$
OHNE Nullteiler: $forall\ a, b$, sodass $\boxed{a \cdot b = b \cdot a = 0}$ gilt $a = 0$ oder $b = 0$

Beispiel

$(\mathbb{Z}, +, \cdot)$ hat KEINE Nullteiler
Dann $(x, y \in \mathbb{Z})\ x \cdot y = 0 \implies x = 0$ oder $y = 0$
Lösungsmenge von $xy = 0$: $L = \left\{(0, t) \;\middle|\; t \in \mathbb{Z}\right\} \cup \left\{(s, 0) \;\middle|\; s \in \mathbb{Z}\right\}$



Definition: Integritätsbereich

Ein nullteilerfreier kommutativer Ring mit Eins.

Beispiel

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

Körper

Definition

Eine Menge K mit zwei Verknüfungen $+$ und $\cdot$ heißt **Körper**, falls:

- $(K, +)$ ist eine abelsche Gruppe
- $(K \setminus \{0\}, \cdot)$ ist eine abelsche Gruppe
- Distributivgesetze

Unterschied zu Ringen

- ist kommutativ, hat ein neutrales Element und alle Elemente in $K \setminus \{0\}$ (d. h. alle Elemente in K außer 0) haben ein multiplikatives Inverses.

Beispiele

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

Der Körper mit zwei Elementen

$K = \{g, u\}$, $g + g = u + u = g$, $g + u = u + g = u$, $g \cdot g = u \cdot g = g \cdot u = g$, $u \cdot u = u$
Danke an $+$ und $\cdot$ von geraden bzw. ungeraden Zahlen.
Alternative Notation: $K = \{0, 1\}$, wobei $g \hat{=} 1$ und $u \hat{=} 1$

Im Alltag

$(K, +)$, Schatten $\begin{cases} 0 & \text{wir machen nichts} \\ 1 & \text{wir drücken} \end{cases}$
Eine Münze drehen: „$1 + 1 = 0$“

$+$	g	u
g	g	u
u	u	g

$(K, +)$ abelsche Gruppe

$\cdot$	g	u
g	g	g
u	g	u

Kommutativ: die Tabelle ist symmetrisch

$\forall\, u \in K \setminus \{g\}\colon\ a \cdot \square = \square \cdot a = a$
$u\colon\ u \cdot u = u \cdot u = u$
u ist das neutrale Element für $(K \setminus \{0\}, \cdot)$
$K \setminus \{0\} = \{u\}$ $(\{u\}, \cdot)$ ist eine abelsche Gruppe
& neutrales Element
das Inverse zu u ist u

Distributivgesetze: Beispiel

$a, b, c \in \{u, g\}$ 8 Möglichkeiten
$(a + b)c = ac + bc$ $(a = g, b = u, c = g)$
$(g + u)g = ug = g = gg + ug = g + g = g$

Das zweite Distributivgesetz

„$a(b + c) = ab + ac$“
folgt aus dem ersten, da die Multiplikation kommutativ ist.

Bemerkung

Sei $(A, *)$ kommutativ.
Neutrales Element: $e \in A$, sodass $\forall\ a \in A$: $e * a[= a * e] = a$
Inverses zu $a \in A$: $a^{-1} \in A$, sodass $a^{-1} * a[= a * a^{-1}] = e$

Sei $(R, +, \cdot)$ mit $+$; kommutativ:
Distributivgesetze
$\forall\ a, b, c \in R$: $(a + b)c = ac + bc$
$\forall\ x, y, z \in R$: $\underbrace{x(y + z)}_{(y+z)x} = \underbrace{xy + xz}_{yx+zx}$
„für alle geordneten Tripel von Elementen in R gilt“: $y = a\ ,\ z = b\ ,\ x = c$

Vorlesung 11 vom 20/11/2013

Beispiel

7 hat Nachfolger 8
7 ist Nachfolger von 6
0 hat Nachfolger 1
0 ist KEIN Nachfolger

Definition der Summe

„$a + b$“ $\forall\ a, b \in \mathbb{N}$

Induktive Definition

Wir nehmen a fest.
I.A.: $b = 0 \quad , \quad a + 0 = a$ in der Definition
I.S.: $b \rightsquigarrow b + 1 = S(b)$
I.V.: Wir haben $a + b$ definiert
I.B.: Wir definieren $a + S(b)$
Aus der Formel ist $a + S(b) = S(\underbrace{a + b}_{\mathbb{N}}) \in \mathbb{N}$

$a + 0 = 0 \quad \forall\ a \in \mathbb{N}$
$a + S(b) = S(a + b) \quad \forall\ a, b \in \mathbb{N}$
Schließlich können wir $a + b$ für alle $a, b \in \mathbb{N}$ definieren.

Warum ist 0^0 NICHT definiert?
Aus der Analysis: (mit $\mathbb{R}$)
Die Funktion 0^x ist für alle $x > 0$ definiert:

$$0^x = 0 \quad \forall\ x > 0$$

$0 = \lim\limits_{x \to 0^+} 0^x = \lim\limits_{x \to 0^+} 0 = 0$
Die Funktion y^0 ist für alle $y > 0$ definiert:

$$y^0 = 1 \quad \forall\, y > 0$$

$0 = \lim\limits_{y \to 0^+} y^0 = \lim\limits_{y \to 0^+} 1 = 1$

Anordnung

Ist $3 < 5$? Ja, da $5 = S(S(3))$, $n = 2$ $S^2(3) = 5$

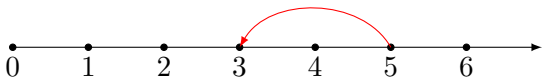
Eine äquivalente Definition der Anordnung

$<$: $a < b$ heißt: die Gleichung $a + x = b$ hat eine Lösung $x \in \mathbb{N}$ und $a \neq b$ (bzw. hat eine Lösung $x \in \mathbb{N} \setminus \{0\}$)
$\leq$: $a \leq b$ heißt: die Gleichung $a + x = b$ hat eine Lösung $x \in \mathbb{N}$
$>$: $a > b$ heißt $b < a$
$\geq$: $a \geq b$ heißt $b \geq a$

Beispiel

$3 < 5$ ist wahr, da $x = 2$ löst $3 + x = 0$ und $2 \in \mathbb{N}$

Mit Hilfe der Zahlengerade:



$a < b$ heißt: a steht links zu b

Addition

$+ : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ Verknüpfung auf $\mathbb{N}$
kommutativ, assoziativ, $0 \in \mathbb{N}$ ist das neutrale Element.
Inverse: Für welche $a \in \mathbb{N}$ gibt es ein $b \in \mathbb{N}$, sodass $a + b = b + a = 0$?
$a + x = 0$ mit $x \in \mathbb{N}$
Nur für $a = 0$ ist die Gleichung lösbar ($x = 0$).
$0 + 0 = 0$
Mit $a = 2$ hat $a + x = 0$ KEINE Lösung $x \in \mathbb{N}$

$$2 + x = 0 \begin{cases} \text{ansonsten wäre } 0 \geq 2 & \text{falsch} \\ \text{In } \mathbb{Z} \text{ ist } -2 \text{ die einzige Lösung und } -2 \notin \mathbb{N}. & \text{wahr} \end{cases}$$

$(\mathbb{Z}, +)$ ist eine Gruppe $\Longrightarrow$ $\forall\, a, b \in \mathbb{Z}$ hat $a + x = b$ genau eine Lösung $x \in \mathbb{Z}$

Kürzungsregel Summe

- Für alle $a, b, c \in \mathbb{N}$ gilt: $a + c = b + c \implies a = b$

Begründung: Siehe $\mathbb{N} \subseteq \mathbb{Z}$ und benutze die Kürzungsregel der Gruppe $(\mathbb{Z}, +)$.
„addiere $-c$“

Eigenschaft Summe

$$\sum_{i=1}^{k} a_i = 0 \quad \text{mit } a_1, \dots a_k \in \mathbb{N} \implies \forall\, i = 1, \dots, k\colon\ a_i = 0$$

Multiplikation

$\cdot\colon \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ Verknüpfung auf $\mathbb{N}$
kommutativ, assoziativ, mit neutralem Element 1
Inverse? $(1)^{-1} = 1$; KEINE weitere natürliche Zahl hat ein multiplikatives Inverses.
$a = 0\colon\ 0 \cdot x = x \cdot 0 = 1$ hat KEINE Lösung, da $0 \cdot x = x \cdot 0 = 0$ und $0 \neq 1$ $(x \in \mathbb{N})$.
$a > 1\colon\ a \cdot x = x \cdot a = 1$ $\mathbb{N} \subseteq \mathbb{Q}$; die einzige Lösung $x \in \mathbb{Q}$ ist $x = \frac{1}{a} \notin \mathbb{N}$.

Kürzungsregel Multiplikation

$\forall\, a, b, c \in \mathbb{N}$ mit $c \neq 0$ gilt

$$ac = bc \implies a = b$$

(1) $\mathbb{N} \subseteq \mathbb{Z}\colon\ ac = bc \implies ac - bc = 0 \overset{\text{distr.}}{\implies} (a - b) \cdot c = 0$

$$\overset{\text{KEINE Nullteiler in } \mathbb{Z}}{\Longrightarrow} \begin{cases} c = 0 & \text{unmöglich, da } c \neq 0 \\ (a - b) = 0 \implies a = b \end{cases}$$

(2) $\mathbb{N} \subseteq \mathbb{Q}\colon$ multipliziere mal $\frac{1}{c}$. $c \neq 0$, dann $\frac{1}{c} \in \mathbb{Q}$

$$a \cdot \underbrace{c \cdot \frac{1}{c}}_{=1} = b \cdot \underbrace{c \cdot \frac{1}{c}}_{=1} \implies a = b$$

Distributivgesetze

$$\forall\, a, b, c \in \mathbb{N}\colon\ (a + b)c = ac + bc \quad , \quad a(b + c) = ab + ac$$

Anordnung

Seien $a, b \in \mathbb{N}$. Wir sagen $a \leq b$, falls $a + x = b$ eine Lösung $x \in \mathbb{N}$ hat.
$a < b$ heißt: $a \leq b$ und $a \neq b$
$a \geq b$ heißt: $b \geq a$
$a > b$ heißt $b > a$

Die Anordnung ist eine Relation auf $\mathbb{N}$.

$$R_{\leq} = \left\{ (a, b) \in \mathbb{N} \times \mathbb{N} \;\middle|\; a + x = b \text{ ist lösbar mit } x \in \mathbb{N} \right\}$$

Analog sind $R_<$, $R_\geq$, $R_>$ Realationen auf $\mathbb{N}$.

Eigenschaften Anordnung

Die Relation $\leq$ ist reflexiv $(a \leq a)$, transitiv $(a \leq b$ und $b \leq c \implies a \leq c)$, antisymmetrisch $(a \leq b$ und $b \leq a \implies a = b)$, total $(a \leq b$ oder $b \leq a)$ $(\forall\, a, b, c \in \mathbb{N})$.
Die Realtion $<$ ist irreflexiv $(a \not< a)$, transitiv $(a < b$ und $b < c \implies a < c)$, asymmetrisch $(a < b \implies b \not< a)$, konvex (es gibt genau eine zwischen $a = b$, $a < b$, $b < a)$ $(\forall\, a, b, c \in \mathbb{N})$.

Monotonie

$\forall\, a, b, c \in \mathbb{N}$ gilt:

$$
\begin{aligned}
a \geq b &\implies a + c \geq b + c \\
a > b &\implies a + b > b + c \\
a \geq b &\implies ac \geq bc \quad \text{(hier ist } c \in \mathbb{N} \text{ also } c > 0 \\
a < b &\implies ac \geq bc \quad \text{falls } c \neq 0 \text{ (also } c > 0\text{): } ac > bc
\end{aligned}
$$

Analog: $\leq, <$

Beispiel

$5 \geq 3 \implies 10 \geq 6$ $(c = 2)$
$5 \geq 3 \implies -10 \leq -6$ $(c = -2 \notin \mathbb{N})$

$5 > 3 \implies 10 > 6$ $(c = 2)$
$5 > 3 \implies 5 \cdot 0 \geq 3 \cdot 0$ aber $5 \cdot 0 \not> 3 \cdot 0$

Vorlesung 12 vom 27/11/2013

Rekursive Folgen

Definition

Eine Folge ist eine Abbildung von $\mathbb{N}$ auf eine Menge A

$$f \colon \mathbb{N} \longrightarrow A$$

(dies ist eine Folge von Elementen aus A)

Beispiel

$f(n) = n^2$, $f \colon \mathbb{N} \longrightarrow \mathbb{N}$, $f(0) = 0$, $f(1) = 1$, $f(2) = 4$ $\ldots$
$f(n) = n \cdot \sqrt{2}$, $f \colon \mathbb{N} \longrightarrow \mathbb{R}$, $f(0) = 0$, $f(1) = \sqrt{2}$, $f(2) = 2\sqrt{2}$ $\ldots$

Satz: Rekursionssatz von Dedekind

Sei A eine Menge, $T\colon A \longrightarrow A$ eine Abbildung und sei $\alpha \in A$. Dann gibt es genau eine Funktion

$$f\colon \mathbb{N} \longrightarrow A$$

mit folgenden Eigenschaften:

(1) Anfangsglied: $f(0) = \alpha$

(2) Rekursionsgleichung: $f(n+1) = T\big(f(n)\big) \quad \forall\, n \in \mathbb{N}$

Diese Funktion ist eine Folge und sie heißt die **rekursive Folge** mit Anfangsglied α und Rekursionsgleichung $f(n+1) = T\big(f(n)\big)$.

Definition: rekursive Folge

Eine rekursive Folge von Elementen von A ist eine Funktion

$$f\colon \mathbb{N} \longrightarrow A$$

sodass es eine Abbildung $T\colon A \longrightarrow A$ gibt mit

$$f(n+1) = T\big(f(n)\big) \quad \forall\, n \in \mathbb{N}$$

Beispiel

$f\colon \mathbb{N} \longrightarrow \mathbb{N}$
$f(n) = 2 \cdot n \quad , \quad 0, 2, 4, 6, 8 \ldots$
rekursive Folge: $T\colon \mathbb{N} \longrightarrow \mathbb{N} \;\; , \;\; T(m) = m + 2 \quad \forall\, m \in \mathbb{N}$

$$f(n+1) = T\big(f(n)\big)$$
$$2n + 2 = 2(n+1) = T(2n)$$

$f\colon \mathbb{N} \longrightarrow \mathbb{R}$
$f(n) = (\sqrt{2})^n \quad , \quad 1, \sqrt{2}, 2, 2\sqrt{2}, 4 \ldots$
rekursive Folge: $T\colon \mathbb{R} \longrightarrow \mathbb{R} \;\; , \;\; T(m) = \sqrt{\cdot} m \quad \forall\, m \in \mathbb{R}$
$f(n) = (\sqrt{2})^n$
$f(n+1) = (\sqrt{2})^{n+1}$

$$f(n+1) = T\big(f(n)\big)(\sqrt{2})^{n+1} \qquad = \sqrt{2} \cdot (\sqrt{2})^n$$

Beweis (Satz von Dedekind – Skizze)

Eindeutigkeit: Seien $f, g\colon \mathbb{N} \longrightarrow A$ mit $f(0) = g(0) = \alpha$ und

$$f(n+1) = T\big(f(n)\big) \quad \forall\, n \in \mathbb{N}$$
$$g(n+1) = T\big(g(n)\big) \quad \forall\, n \in \mathbb{N}$$

zu zeigen: $f = g$
Induktion: Sei $M \subseteq \mathbb{N}$ die Menge, wo die Funktionen f und g übereinstimmen.
(z.z.: $M = \mathbb{N}$)
I.A.: $M \ni 0$, da $f(0) = g(0) = \alpha$
I.S.: $f(n) = g(n) \implies f(n+1) = g(n+1)$
$\Big(n \in M \implies n+1 \in M\Big)$
Es gilt

$$f(n+1) \overset{(*)}{=} T\big(f(n)\big) \overset{f(n)=g(n)}{=\!=} T\big(g(n)\big) \overset{(**)}{=} g(n+1) \quad \forall\, n \in \mathbb{N}$$

$(*)$ Rekusionsgleichung für f
$(**)$ Rekursionsgleichung für g
Dann ist $M = \mathbb{N}$.

$\exists$: Bemerkung über Funktionen:
Seien $D_i \subseteq \mathbb{R}$ mit $i \in I$ (I Indexmenge, endlich oder abzählbar unendlich) und sei $f_i\colon D_i \longrightarrow \mathbb{R}$ eine Funktion $\forall\, i \in I$.
Dann gibt es eine Funktion

$$f\colon D \longrightarrow \mathbb{R} \quad \text{wobei } D = \bigcup_{i \in I} D_i$$

genau dann, wenn $\forall\, i, j \in I$ gilt:

$$f_i = f_j \quad \text{auf } D_i \cap D_j$$

Beispiel: $I = \{1, 2\}$
$f_1\colon \mathbb{N} \longrightarrow \mathbb{R}$, $f_1(x) = x$
$f_2\colon \underbrace{-\mathbb{N}}_{\mathbb{Z}_{\leq 0}} \longrightarrow \mathbb{R}$, $f_2(x) = -x$
Kompatibilität: $\mathbb{N} \cap -\mathbb{N} = \{0\}$ und $f_1(0) = f_2(0) = 0$
Es gibt $f\colon \underbrace{\mathbb{Z}}_{\mathbb{N} \cup -\mathbb{N}} \longrightarrow \mathbb{R}$ sodass $f(x) = \begin{cases} x & x \geq 0 \\ -x & x \leq 0 \end{cases}$ ($f(x) = |x| \;\rightsquigarrow$ Betragsfunktion)

Für den Beweis: $I = \mathbb{N}$, $f_i\colon D_i \longrightarrow A$
$D_i = \{0, 1, \ldots, i\}$
$\forall\, i, j\colon$ $f_i = f_j$ auf $D_i \cap D_j$. Hier ist $D_i \subseteq D_j$ f+r $i \leq j$.
$\forall\, i, j$ mit $i \leq j\colon$ $f_j\Big|_{D_i} = f_i$

Es folgt: es gibt eine Funktion $f: \mathbb{N} \longrightarrow A$, sodass $f\Big|_{D_i} = f_i$

Beweisstruktur für $\exists$:

(1) Man zeigt durch Induktion die Existenz von Funktionen f_i wie oben, sodass $f_i(0) = \alpha$ und $f_i(n+1) = T(f_i(n)) \quad \forall\, n = 0, \ldots, i-1$.

(2) Mit der Bemerkung über Funktionen findet man die gewünschte Folge.

Dies sollte eine Beweisskizze darstellen ...

□

Satz: k-Rekursions-Satz

Sei A eine Menge. Sei $k \geq 1$. Sei $T: A^k \longrightarrow A$ eine Funktion. Dann wird durch Vorgabe von $f_0, \ldots, f_{k-1}$ und die Rekursionsvorschrift $f_{n+k} = T(f(n), \ldots, f(n+k-1))$ eine eindeutig bestimmte Folge definiert:

$$f: \mathbb{N} \longrightarrow A$$

Eine Folge wie im Satz heißt eine **k-Rekursive-Folge**.

Beispiel

$k = 2$, die Fibonacci Folge $f: \mathbb{N} \longrightarrow \mathbb{N}$
$f(0) = 0\ ,\ f(1) = 1$
$T: \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}\ ,\ f(n+2) = \underbrace{f(n) + f(n+1)}_{T\left(f(n), f(n+1)\right)}$
$T(a, b) = a + b$
Mit Angangsgliedern $f(0) = 0\ ,\ f(1) = 0$ und derselben Rekursionsgleichung, dann ist $f(n) = 0 \quad \forall\, n \in \mathbb{N}$. (Aufgabe: Induktion)

Vorlesung 13 vom 28/11/2013

Beispiele Schranken

$\mathbb{N} \subseteq \mathbb{R}$
0 Minimum: $0 \in \mathbb{N}\ ,\quad \forall\, n \in \mathbb{N}:\ n \geq 0$
$-7 \notin \mathbb{N}$, untere Schranke $\forall\, n \in \mathbb{N}:\ n \geq -7$
$-90 \ldots$
KEIN Maximum, KEINE obere Schranke

$2\mathbb{Z} \subseteq \mathbb{Z}$

gerade Zahlen
KEIN Maximum, KEIN Minimum, KEINE Schranken

---

13 : 3, Quotient 4, Rest 1
13 : 4, Quotient 3, Rest 1

Satz (Division mit Rest)

Seien $a, b \in \mathbb{Z}$ mit $b \neq 0$. Dann gibt es zu a, b genau ein (Quotient und Rest existieren eindeutig) geordnetes Paar (q, r) von ganzen Zahlen mit

$$a = qb + r$$
$$0 \leq r < |b|$$

wobei q den Quotienten und r den Rest in der Division $a : b$ bezeichne.

TEST

16 : 3, Quotient 5, Rest 1
$-16 : 3$, Quotient -6, Rest2
$16 : -3$, Quotient -5, Rest 1
$-16 : -3$, Quotient 6, Rest 2

Beweis

$\exists$: **1. Fall** $(b > 0)$

Wir definieren die Menge $M = \left\{ a + tb \;\middle|\; t \in \mathbb{Z}\ ,\ a + tb \geq 0 \right\}$

Eigenschaften von M:

- $M \subseteq \mathbb{N}$ (weil $m \in M \implies m = a + tb$ mit $t \in \mathbb{Z}$ und $a + tb \geq 0$, d. h. $m \geq 0$)
- $M \neq \emptyset$. Sei $t' = |a| \in \mathbb{Z}$. Dann

$$a + t'b = a + \underbrace{|a| \cdot b}_{|a|+|a|(b-1)} = \underbrace{(a + |a|)}_{\geq 0} + \underbrace{|a|}_{\geq 0}\ \underbrace{(b-1)}_{\geq 0, b>0}$$

$a + t'b \geq 0\ ,\ t' \in \mathbb{Z} \rightsquigarrow \underbrace{a + t'b}_{a+|a|\cdot b \in M} \in M$

Da M eine nichtleere Teilmenge von $\mathbb{N}$ ist, besitzt M ein Minimum. Sei dann $r := \min(M)$.
$r \in M$ und $r \leq m \quad \forall\ m \in M$
$\rightsquigarrow\ \exists\ t_r \in \mathbb{Z}\colon\ r = a + t_r b$ und $r \geq 0$
$q = -t_r$

Wir überprüfen die Eigenschaften Quotient/Rest:

- $r \in \mathbb{Z}\ ,\ q \in \mathbb{Z}$ wahr $(a, b, t_r \in \mathbb{Z})$

- $qb + r = (-t_r)b + (a + t_r b) = a$
- $0 \leq r$ wahr $(r \in M)$
- $r < |b|$ (?) Wäre $r \geq |b|$, dann ist $r - |b| \geq 0$
  $r - |b| = a + (t_r - 1)b$
  Dann $r - |b| \in M$, aber $r - \underbrace{|b|}_{\geq 1, b>0} < r$
  Ein Element von M kleiner als das Minimum von M. Das kann NICHT sein $\lightning$.

$\exists$: **2. Fall** $(b < 0)$

Wir benutzen den 1. Fall für $-b > 0$:
$\exists\ q', r' \in \mathbb{Z}$, sodass $a = q'(-b) + r'$ und $0 \leq r' < |-b|$
Dann gilt: $q = -q'$ und $r = r'$
$a = (-q')(b) + r' = qb + r$
$0 \leq r < |-b| = |b|$
$q, r \in \mathbb{Z}$
Dann sind q, r Quotient und Rest für $a : b$

Eindeutigkeit: Seien $q, r, q'r' \in \mathbb{Z}$, sodass

$$a = qb + r = q'b + r'$$
$$0 \leq r < |b|$$
$$0 \leq r' < |b|$$

z.z.: $q = q'$, $r = r'$
Falls $r \neq r'$, o. B. d. A.: $r' > r$. Dann ist

$$|r' - r| = r' - r \underset{r' < |b|}{<} |b| - r \underset{r \geq 0}{\leq} |b|$$
$$\implies |r' - r| < |b|$$

Wir haben $(q - q') \cdot b = r' - r$ (aus der zweiten Gleichung für a)
Dann

$$|r' - r| = |q - q'| \cdot |b| = \begin{cases} 0 & \text{falls } |q - q'| = 0 \\ \geq |b| & \text{falls } |q - q'| \neq 0 \text{ (unmöglich!)} \end{cases}$$

Also $|q - q'| = 0$.
$|q' - q| = 0 \iff q = q'$. Aus $a = qb + r = q'b + r'$ folgt $r = r'$.

□

Teilbarkeitsrelation auf $\mathbb{Z}$

Definition

Seien $a, b \in \mathbb{Z}$. Wir sagen a iszt durch b teilbar $\left(b \,\middle|\, a\right)$, wenn es ein $t \in \mathbb{Z}$ gibt mit $a = t \cdot b$.

Beispiel

$3 \mid 6 \ \rightsquigarrow \ 6 = 2 \cdot 3 \ , \ 2 \in \mathbb{Z}$

$5 \nmid 6 \ \rightsquigarrow \ 6 = x \cdot 5 \ , \ x \in \mathbb{Z}.$
Falls $x \leq 1$ ist $x \cdot 5 \leq 5 < 6$ ↯;
$x \geq 2$: $x \cdot 5 \geq 10 < 6$ ↯;
NICHT lösbar mit $x \in \mathbb{Z}$.

Teilbarkeitsrelation

$$R \subseteq \mathbb{Z} \times \mathbb{Z} \ , \ R = \left\{ (a,b) \ \middle| \ b \mid a \ , \ a,b \in \mathbb{Z} \right\}$$

Eigenschaften der Teilbarkeitsrelation

- reflexiv
- transitiv
- NICHT symmetrisch
- NICHT antisymmetrisch (die Einschränlung auf $\mathbb{N}$ ist antisymmetrisch)

Proposition

Für ganze Zahlen a, b mit $b \neq 0$ sind die folgenden Aussagen äquivalent:

(i) es gibt ein $t \in \mathbb{Z}$ mit $a = t \cdot b$

(ii) der Rest von $a : b$ ist Null

(iii) die rationale Zahl $\frac{a}{b}$ ist eine ganze Zahl

Beweis

(i) ⇒ (ii)

Sei $a = t \cdot b$ mit $t \in \mathbb{Z}$. Dann $t = q$ und $0 = r$ sind Quotient und Rest, insbesondere ist der Rest Null.

$a : b \ , \ q, r \in \mathbb{Z} \ , \ a = t \cdot b = \underbrace{q}_{t} \cdot b + \underbrace{r}_{0}$

$0 \leq \underbrace{r}_{=0} < \underbrace{|b|}_{\geq 1, b \neq 0}$

(ii) ⇒ (i)

Seien q, r Quotient und Rest für $a : b$ mit $r = 0$. Dann

$$a = q \cdot b + r \overset{r=0}{=} q \cdot b \implies a = t \cdot b \ , \ t = q \in \mathbb{Z}$$

(i) $\Rightarrow$ (iii)

Sei $a = t \cdot b$ mit $t \in \mathbb{Z}$. Dann

$$\frac{a}{b} = \frac{t}{1} = t \in \mathbb{Z}$$

(iii) $\Rightarrow$ (i)

Sei $\frac{a}{b} = s \in \mathbb{Z}$. Dann

$$\frac{a}{b} = \frac{s}{1} \implies a = s \cdot b \ , \ t = s \in \mathbb{Z} \ , \ a = t \cdot b$$

□

Bemerkung: Für $b \neq 0$ sind die Aussagen in der Proposition äquivalente Definitionen für $b \mid a$.

Beispiel

$5 \nmid 6$

(ii) $6 = \frac{1}{q} \cdot 5 + \frac{1}{r} \ , \ r \neq 0$

(iii) $\frac{6}{5} \notin \mathbb{Z}$, da $1 < \frac{6}{5} < 2$

VORSICHT bei $b = 0$!! Benutze in diesem Fall nur die erste Definition.

Vorlesung 14 vom 04/12/2013

Erinnerung

Division mit Rest

$a, b \in \mathbb{Z} \ , \ b \neq 0$ Quadriert und Rest für $a : b$ sind die eizige
q, r sodass

- $q, r \in \mathbb{Z}$
- $a = bq + r$
- $0 \leq r < |b|$

Teilbarkeit

Seien $a, b \in \mathbb{Z}$. Dann $a \mid b$, falls $\exists \ t \in \mathbb{Z}$ mit $b = t \cdot a$.
Falls $a, b \neq 0$ ist dies äquivalent zu

- der Rest in $b : a$ ist Null
- $\frac{b}{a} \in \mathbb{Z}$

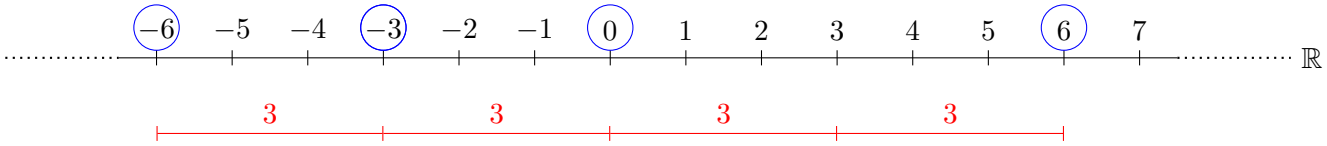
Notation

Seien $a, b \in \mathbb{Z}$. Falls $a \mid b$, dann ist a ein **Teiler** von b und b ist ein **Vielfaches** von a.

Anmerkungen Gerade Zahlen

- $M = \mathbb{Z}$ „genau so viele“ gerade Zahlen als ungerade Zahlen
  $\#(2\mathbb{Z}) = +\infty$, $\#(\mathbb{Z} \setminus 2\mathbb{Z}) = +\infty$, Bijektion $2\mathbb{Z} \xrightarrow{+1} \mathbb{Z} \setminus 2\mathbb{Z}$
- $M = \{1, 2, 3\}$: 1 gerade Zahl, 2 ungerade Zahlen
- Primzahlen: 2 ist die einzige gerade Primzahl
  es gibt unendlich viele ungerade Primzahlen
- $M =$ die Vielfachen von 6: es gibt nur gerade Zahlen

Die Zahlgerade

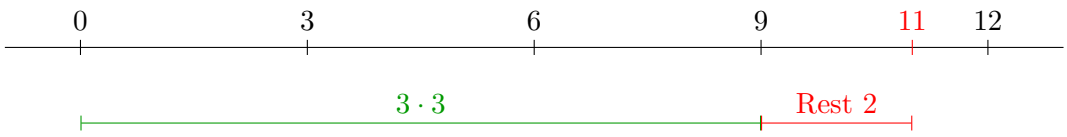


Vielfache von 3: $t \cdot 3$, $t \in \mathbb{Z}$

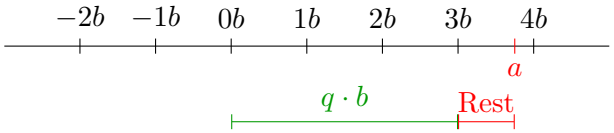
$$0 = 0 \cdot 3$$
$$3 = 1 \cdot 3$$
$$6 = 2 \cdot 3$$
$$-3 = -1 \cdot 3$$
$$-6 = -2 \cdot 3$$

Verallgemeinerung: Sei $a > 0$. Konsekutive Vielfachen von a findet man auf der Zahlgeraden mit Abstand a.

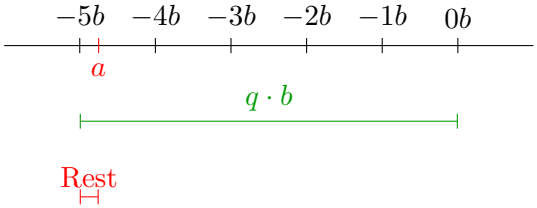
Division mit Rest auf der Zahlgeraden



$11 : 3$, Quotient 3, Rest 2
Allgemein: $a : b$ mit $b > 0$



Von 0 bis q hat man q „Strecken“, falls $a > 0$.



$b > 0$, $a < 0$
Von Null bis a hat man $|a| - 1$ „Strecken“
Der Rest ist eine Strecke links von a, zwischen a und dem nächsten Vielfachen von b.

Eigenschaften der Teilbarkeit

Seien $a, b \in \mathbb{Z} \setminus \{0\}$.

(1) Falls $a \mid b$ und $b \mid a$, dann ist $a = \pm b$.

(2) $a \mid b \iff |a| \mid |b|$

(3) Aus $a \mid b$ folgt $|a| \leq |b|$

Beweis

(3) Sei $a \mid b$, d. h. $\exists\, t \in \mathbb{Z}$ mit $b = t \cdot a$. Es ist $t \neq 0$, da $b \neq 0$.

$b = t \cdot a \overset{(*)}{\Longrightarrow} |b| = |t| \cdot |a|$

$(*)$ zwei Zahlen sind gleich, dann sind ihre Beträge gleich; $|x \cdot y| = |x| \cdot |y|$

Wir haben: $t \in \mathbb{Z} \setminus \{0\}$. Dann ist $|t| \geq 1$.

Dann gilt

$$|b| = |t| \cdot |a| \overset{|t| \geq 1}{\geq} 1 \cdot |a| = |a|$$

D. h. $|b| \geq |a|$.

□

Weitere Eigenschaften

Seien $a, b, c, d \in \mathbb{Z} \setminus \{0\}$.

(4) Aus $a \mid b$ und $c \mid d$ folgt $a \cdot c \mid c \cdot d$.

(5) Aus $a \cdot c \mid b \cdot c$ folgt $a \mid b$.

(6) Aus $a \mid b$ und $a \mid c$ folgt $a \mid (b + c)$ und $a \mid (b - c)$ und allgemeiner $\forall\, x, y \in \mathbb{Z}$: $a \mid (bx + cy)$

Beweis

Zentralübung (Aufgabe).

□

Teilermengen

Notation

Sei $a \in \mathbb{Z}$.
$T(a) = \{\text{Teiler von } a\} = \left\{ b \in \mathbb{Z} \;\middle|\; b \,\middle|\, a \right\}$
$T^+(a) = \{\text{positive Teiler von } a\} = \left\{ b \in \mathbb{Z}_{\geq 0} \;\middle|\; b \,\middle|\, a \right\} = T(a) \cap \mathbb{Z}_{\geq 0} = T(a) \cap \mathbb{N}$
$T^-(a)$ negative Teiler; $T^-(a) = T(a) \cap \mathbb{Z}_{\leq 0}$

Beispiel

$T(6) = \{\pm 1, \pm 2, \pm 3, \pm 6\}$
$T^+(6) = \{1, 2, 3, 6\}$
$T^-(6) = \{-1, -2, -3, -6\}$

Notation

$b \in T(a)$ mit $b = \pm 1$ oder $b = \pm a$ heißt **trivialer Teiler**. Alle anderen Teiler heißen **echte Teiler**.

Bemerkung

$\forall\, a \in \mathbb{Z}\ ,\ a \,\big|\, 0 \quad ; \quad 0 \,\big|\, a \iff a = 0$ (ZÜ, Aufgabe)
Dann $T(0) = \mathbb{Z}\ ,\ T^+(0) = \mathbb{N}\ ,\ T^-(0) = \mathbb{Z}_{\leq 0}$
Es folgt auch:
Sei $a \in \mathbb{Z} \setminus \{0\}$. Dann $0 \notin T(a)$.

Bemerkung

$\forall\, a \in \mathbb{Z}\colon\ 1 \,\big|\, a$ und $(-1) \,\big|\, a$
Dann $\forall\, a \in \mathbb{Z}\colon\ 1 \in T^+(a)\ ,\ -1 \in T^-(a)\ ,\ \{1, -1\} \subseteq T(a)$

Bemerkung

$\forall\, a \in \mathbb{Z}\colon\ a \,\big|\, a\ ,\ -a \,\big|\, a$
$\forall\, a \in \mathbb{Z}\colon\ \{a, -a\} \subseteq T(a)\ ,\ T^+(a) \ni \{|a|\}\ ,\ T^-(a) \ni \{-|a|\}$

Weitere Eigenschaften

(1) $T^+(a)$ und $T^-(a)$ ergeben eine Partition von $T(a)$.

(2) $T^-(a) = -T^+(a)\ ,\ T^+(a) = -T^-(a)$

(3) $T(a) = T(-a) = T(|a|)$

(4) $T^+(a) \subseteq \{1, \ldots, |a|\}$, $T^-(a) \subseteq \{-1, \ldots, -|a|\}$

Beweis

(1)

$T^+(a) \neq \emptyset$, da z. B. $1 \in T^+(a)$
$T^-(a) \neq \emptyset$, da z. B. $-1 \in T^-(a)$
$T^+(a) \subseteq T(a)$
$T^-(a) \subseteq T(a)$

$T^+(a) \cap T^-(a) \subseteq \{0\}$
Da $a \neq 0$ ist $0 \notin T(a)$, also $0 \notin T^+(a)$
Es folgt $T^+(a) \cap T^-(a) = \emptyset$
$T(a) = T^+(a) \cup T^-(a)$, da $\mathbb{Z}_{\geq 0} \cup \mathbb{Z}_{\leq 0} = \mathbb{Z}$
(ein Teiler ist eine ganze Zahl also positiv oder negativ)

(2)

Grund: $t \mid a \iff -t \mid a \quad \forall\, t \in \mathbb{Z}$
„minus ein Teiler ist ein Teiler“

(3)

Grund: $t \mid a \iff t \mid -a \quad \forall\, t \in \mathbb{Z}$

(4)

Äquivalent: $0 \neq t \in T(a) \implies |t| \leq |a| \quad (-|a| \leq t \leq |a|)$
Wir wissen schon: $b \mid a \implies |b| \leq |a|$

□

Konsequenz von (4): Es gibt höchstens $2 \cdot |a|$ Teiler.