Formelsammlung Mathematik

Marc Landolt

4. Februar 2012

Inhaltsverzeichnis

Vorwort

Dies ist meine Formelsammlung aus dem Unterricht an der ABB Technikerschule und verschiedenen Fachhochschulen. Ich Danke Claudine Blum für ein schönes Jahr in meinem Leben. Die Formelsammlung wurde erstellt mit LaTeX

1 Zahlen

1.1 Arabische Ziffern

$1, 2, 3, 4, 5, 6, 7, 8, 9, 0$

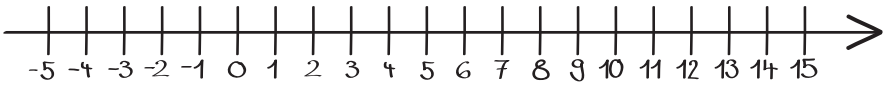
1.2 Kardnalzahlen

Kardinalzahlen sind die natürlichen Zahlen eine mögliche Menge von Grundzahlen

1.3 Ordinalzahlen

Ordinalzahlen sind die natürlichen Zahlen als geordnete Menge mit einem möglichen Abbruch Sie werden für das Konzept der Indexierung verwendet

1.4 Zahlenstrahl



2 Variablen

2.1 Variablen

x, y, z

Platzhalter statische oder variable Rechengrösse

2.2 Formvariablen (Parameter)

a, b, c

Variabel die gemeinsam mit anderen Variablen auftritt. Die Formvariablen müssen beim Addieren gleich sein. werden ungleiche Formvariablen addiert geht die Rechnung nicht auf.

2.3 Winkel

Für Winkel werden die Griechischen Buchstaben verwendet

2.3.1 Griechisches Alphabet

Gross	**klein**	**Name**	**Gross**	**klein**	**Name**
A	α	Alpha	N	ν	Ny
B	β	Beta	Ξ	ξ	Xi
Γ	γ	Gamma	O	o	Omikron
Δ	δ	Delta	Π	π	Pi
E	ϵ	Epsilon	P	ρ	Rho
Z	ζ	Zeta	Σ	σ	Sigma
H	η	Eta	T	τ	Tau
Θ	θ	Theta	Y	υ	Ypsilon
I	ι	Iota	Φ	ϕ	Phi
K	κ	Kappa	X	χ	Chi
Λ	λ	Lambda	Ψ	ψ	Psi
M	μ	My	Ω	ω	Omega

(1)

3 Aussagenlogik

3.1 Axiom

3.2 Streng deduktiv

Aussagen können nur gemacht werden mit Hilfe von vorher bewiesenen Sätzen. Dennoch müssen zu beginn einige Sätze angenommen werden die nicht mit einer Beweiskette bewiesen sind. Diese Sätze nennt man Axiom oder Postulat-

$$a = b \wedge a = c \Rightarrow b = c \tag{2}$$
$$a + x = c \wedge b + x = c \Rightarrow a = b \tag{3}$$
$$a = b \wedge a - x = c \wedge b - x = d \Rightarrow a = b \tag{4}$$

3.3 Aussage

Eine Aussage ist ein Satz der entweder richtig oder falsch ist.

3.4 Negation

$$Negation einer Aussage = \neg(Aussage) = \overline{Aussage} \tag{5}$$

3.5 Aussageform

Subjekt und auch Prädikat kann durch eine Variabel ersetzt werden. Sie enthält mindestens eine Variabel

3.6 Subjekt

3.7 Prädikat

4 Oder, Oder-Aussage, Einschliessende Oder

Oder: $\vee$

A (MSB)	**B**	**A $\vee$ B**
0	0	0
0	1	1
1	0	1
1	1	1

(6)

4.1 Programmiersprachen

die Meisten Programmiersprachen nutzen ||

4.2 Äquivalenz

Äquivalenzsymbol $\leftrightarrow$
Dies beweist man im Normalfall in dem man zuerst die Implikation $A \rightarrow B$ beweist und danach die Implikation $A \leftarrow B$

4.2.1 Kommutativgesetz der Oder Verknüpfung

$$A \vee B \leftrightarrow B \vee A \tag{7}$$

4.2.2 Assoziativgesetz der Oder Verknüpfung

$$(A \vee B) \vee C \leftrightarrow A \vee (B \vee C) \tag{8}$$

5 Und-Aussage

Und: $\wedge$

A (MSB)	**B**	**A $\wedge$ B**
0	0	0
0	1	0
1	0	0
1	1	1

(9)

5.1 Sheffer-Operator

5.2 Peirce-Operator

5.3 Es Falso quodlibet

5.4 Äquivalenz

Äquivalenzsymbol $\leftrightarrow$

5.4.1 Kommutativgesetz der Und Verknüpfung

$$A \wedge B \leftrightarrow B \wedge A \tag{10}$$

5.4.2 Assoziativgesetz der Oder Verknüpfung

$$(A \wedge B) \wedge C \leftrightarrow A \wedge (B \wedge C) \tag{11}$$

5.5 Programmiersprachen

die Meisten Programmiersprachen nutzen $$

5.6 Gesetz von De Morgan

$$\boxed{\neg(A \vee B) = (\neg A) \wedge (\neg B)} \tag{12}$$

$$\boxed{\neg(A \wedge B) = (\neg A) \vee (\neg B)} \tag{13}$$

dieses scheint auch für 3 Variablen zu gelten

6 Operatoren Priorität

¬
∧
∨

7 Implikation

Definition: Die Implikation $A \rightarrow B$ ist falsch wenn A wahr ist und B falsch. Das heisst aus A folgt zwangsläufig B aber B kann auch durch andere Umstände wahr sein. //

$$\boxed{A \rightarrow B \leftrightarrow \neg A \vee B} \tag{14}$$

A	**B**	**A → B**	**¬A**	**¬A ∨ B**
0	0	1	1	1
0	1	1	1	1
1	0	0	0	0
1	1	1	0	1

(15)

Also wenn z.B. der Vater Mafiosi ist ist es eher unwahrscheinlich, dass es der Sohn nicht ist, es kann aber gut sein, dass der Sohn zur Mafia kommt ohne dass sein Vater dabei ist. :%s/Mafia/Militär/g
(folglich "Platon – Protagoras"mit der Zentralen Frage: ïst das 'Gut-Sein' lernbar"bzw. Zitat: "daß die Athener derselben Meinung sind, und daß es endlich gar nicht wundersam ist, wenn Söhne guter Väter schlecht und Söhne schlechter Väter gut geraten")

7.1 Verneinung der Implikation

$$\boxed{\neg(A \to B) \leftrightarrow \neg(\neg A \vee B) \leftrightarrow (A \wedge \neg B)}$$

$$\boxed{(A \to B) \leftrightarrow ((\neg B) \to (\neg A))} \tag{16}$$

Beweis:

$$((\neg B) \to (\neg A)) \leftrightarrow (\neg(\neg B) \vee (\neg A)) \tag{17}$$
$$(\neg(\neg B) \vee (\neg A)) \leftrightarrow ((\neg A) \vee (B)) \tag{18}$$
$$((\neg A) \vee (B)) \leftrightarrow A \to B \tag{19}$$
$$A \to B \tag{20}$$

Beispiel:

$$x > 10 \to x^2 > 100 (A \to B) \tag{21}$$
$$x^2 \leqslant 100 \to x \leqslant 10 (\neg B \to \neg A) \tag{22}$$

Die Implikation $(\neg B) \to (\neg A)$ nennt man **Kontraposition zu** $A \to B$ (23)

7.2 Der Indirekte Beweis (durch Kontraposition)

Im Normalfall beweist man einen mathematischen Satz in dem man die Aussage B aus der Aussage ableitet. Man kann aber auch aus der Verneinung von B die Verneinung von A ableiten. Dies ist Mathematisch äquivalent.

7.3 Prädikatenlogik

7.3.1 Quantoren

7.3.2 Existenzaussagen

Exiszenzquantor: $\exists$ oder $\bigvee$ (gesprochen Ës existiert ein..."")
Beispiele:
$\exists_x x > 0$ Es existiert ein x dass grösser Null ist.
$\exists_z z^2 = 9$ Es Existiert ein z dessen Quadrat Neun ist.
$\exists_y y^2 < 0$ Es Existiert ein z dessen Quadrat Neun ist.
Zumindest im Körper der Komplexen Zahlen ($\mathbb{C}$)

7.3.3 Allaussage

Allquantor: $\forall$ oder $\bigwedge$ (gesprochen "Für alle ... gilt ...") Beispiele:
$\forall_x x^4 > 0$ Für alle x gilt $x^4 > 0$. Was für $x = 0$ nicht stimmt.
$\forall_z x^2 > 0$ Für alle z gilt $x^2 = 9$. Was mutmasslich nicht stimmt.
$\forall_y y^2 > -1$ Für alle x gilt $x^4 > 0$

7.4 Verneinung von Existenz und Allaussagen

$$\boxed{\neg(\exists_x A(x)) \leftrightarrow \forall \neg(A(x))} \tag{24}$$

Beispiel:

$$\neg(\exists_x x > 0) \leftrightarrow \forall_x \neg(x > 0) \leftrightarrow \forall_x x \geqslant 0) \tag{25}$$

$$\boxed{\neg(\forall_x A(x)) \leftrightarrow \exists_x \neg(A(x))} \tag{26}$$

Beispiel:

$$\neg(\forall_x x > 0) \leftrightarrow \exists_x \neg(x > 0) \leftrightarrow \exists_x x \leqslant 0) \tag{27}$$

$$\neg(\forall_z z^2 = 9) \leftrightarrow \exists_z \neg(z^2 = 9) \leftrightarrow \exists_z z^2 \neq 9) \tag{28}$$

7.5 Distributivgesetze

$$\boxed{A \wedge B \vee C \leftrightarrow (A \wedge B) \vee C \nleftrightarrow A \wedge (B \vee C)} \tag{29}$$

$$\boxed{A \vee (B \wedge C) \leftrightarrow (A \vee B) \wedge (A \vee C)} \tag{30}$$

$$\boxed{A \wedge (B \vee C) \leftrightarrow (A \wedge B) \vee (A \wedge C)} \tag{31}$$

$$A \wedge (B \vee C)$$
$$\neg(\neg A) \wedge (\neg(\neg B) \vee \neg(\neg C))$$
$$\neg(\neg A) \wedge \neg((\neg B) \wedge (\neg C))$$
$$\neg((\neg A) \vee ((\neg B) \wedge (\neg C)))$$
$$\neg((\neg A \vee \neg B) \wedge (\neg A \vee \neg C))$$
$$\neg\neg(\neg(\neg A \vee \neg B) \vee \neg(A \vee \neg C)))$$
$$(\neg(\neg A) \wedge \neg(\neg B)) \vee (\neg(\neg A) \wedge \neg(\neg C))$$
$$(A \wedge B) \vee (A \wedge C)$$

8 Mengenlehre

Mengen gibt es seit ca. 1880, ihr Erfinder ist Georg Cantor. Eine Menge ist eine Ansammlung von Objekten welche wiederum als ein Objekt betrachtet werden kann
$x \in M$ (man Spricht: x ist Element der Menge M

$$\{ x | x \text{ ist eine Natürliche Zahl, die keine Primzahl ist } \}$$
x für die gilt x ist eine Natürliche Zahl

8.1 Leere Menge

die leere Menge $\{\}$ ist eine Teilmenge jeder Menge.

8.2 Beweis der Äquivalenz

um zu beweisen dass eine Aussage äquivalent ist beweist man zuerst die eine Richtung $\leftarrow$ und dann die andere Richtung $\rightarrow$

$$M_1 \subseteq M_2 \wedge M_2 \subseteq M_1 \leftrightarrow M_1 = M_2 \tag{32}$$

8.3 A ist eine Teilmenge von B

Ist x Element von A führt dies dazu dass es automatisch auch Element von B $A \subseteq B \rightarrow A \cap B \subseteq A$ ist und wiederum eine Teilmenge von A bzw. B

$$A \subseteq B \leftrightarrow \bigvee_x x \in A \rightarrow x \in B \tag{33}$$

$$A \subset B \leftrightarrow A \neq B \wedge \bigvee_x x \in A \rightarrow x \in B \tag{34}$$

8.4 Schnittmenge (oder Durchschnittsmenge)

Die Vereinigungsmenge der beiden Mengen A und B ($x \in Aundx \in B$) schreibt man Formal:

$$x \in A \cap B \leftrightarrow x \in A \wedge x \in B \tag{35}$$

$$A \subseteq B \leftrightarrow A \cap B = A \tag{36}$$

Kommutativgesetz der Schnittmenge: $M_1 \cap M_2 = M_2 \cap M_1$
Assoziativgesetz der Schnittmenge $(M_1 \cap M_2) \cap M_3 = M_1 \cap (M_2 \cap M_3)$

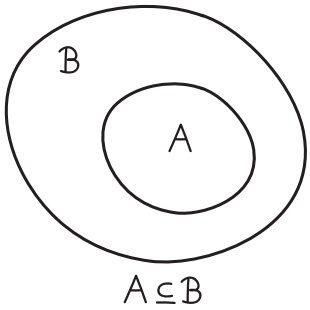


Abbildung 1: Euler-Venn-Diagram der Teilmenge

Erstes Distributivgesetz: $M_1 \cap (M_2 \cup M_3) = (M_1 \cap M_2) \cup (M_1 \cap M_3)$
Zweites Distributivgesetz: $M_1 \cup (M_2 \cap M_3) = (M_1 \cup M_2) \cap (M_1 \cup M_3)$
Stärkere Bindung für $\cap$: $A \cap B \cup C = (A \cap B) \cup C$ würde man das zweite mit der Addition und Multiplikation vergleichen käme das hier falsch raus.

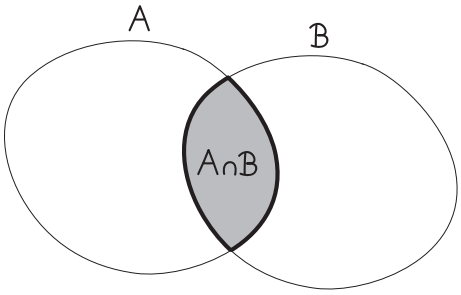


Abbildung 2: Euler-Venn-Diagram der Schnittmenge

Den Beweis erbringt man in dem zeigt dass:
$M_1 \subseteq M_2$
$M_2 \subseteq M_1$
Daraus folgt $M_1 = M_2$

Beweis: $A \subseteq B \leftrightarrow A \cap B = A$

$$A \subseteq B \rightarrow A \cap B \subseteq A \tag{37}$$
$$A \subseteq B \rightarrow A \subseteq A \cap B \tag{38}$$
$$A \cap B = A \leftrightarrow A \subseteq B \tag{39}$$

8.5 Vereinigungsmenge

Vereinigungsmenge zweier Mengen A und B sei die Menge aller x für die gilt $(x \in A) \vee (x \in B)$

$$x \in A \cup B \leftrightarrow x \in A \vee x \in B \tag{40}$$

$$A \subseteq B \leftrightarrow A \cup B = B \tag{41}$$

Kommutativgesetz der Schnittmenge: $M_1 \cup M_2 = M_2 \cup M_1$
Assoziativgesetz der Schnittmenge $(M_1 \cup M_2) \cup M_3 = M_1 \cup (M_2 \cup M_3)$
Erstes Distributivgesetz: $M_1 \cap (M_2 \cup M_3) = (M_1 \cap M_2) \cup (M_1 \cap M_3)$
Zweites Distributivgesetz: $M_1 \cup (M_2 \cap M_3) = (M_1 \cup M_2) \cap (M_1 \cup M_3)$
Stärkere Bindung für $\cap$: $A \cap B \cup C = (A \cap B) \cup C$

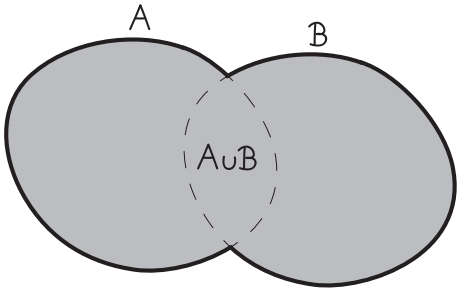


Abbildung 3: Euler-Venn-Diagram der Vereinigungsmenge

8.6 Differenzmenge

Differenzmenge zweier Mengen A und B sei die Menge aller x für die gilt $x \in A \wedge x \notin B$

$$x \in A \setminus B \leftrightarrow x \in A \wedge x \notin B \tag{42}$$

$$A \setminus B \leftrightarrow A \cap \bar{B} \tag{43}$$

8.7 Potenzmenge

Die Potzenzmenge der Menge A $\mathfrak{P}(A)$ ist die Menge aller möglichen Teilmengen die man aus der Grundmenge A konstruieren kann und da die Leere Menge Teilmenge jeder Menge ist gehört diese auch dazu. Somit ist:

$$B \in \mathfrak{P}(A) \leftrightarrow B \subseteq A \tag{44}$$

Beispiel:
Sei $A = \{4, 6, 9\}$
$\mathfrak{P}(A) = \{\{\}, \{4\}, \{6\}, \{9\}, \{4, 6\}, \{4, 9\}, \{6, 9\}, \{4, 6, 9\}\}$

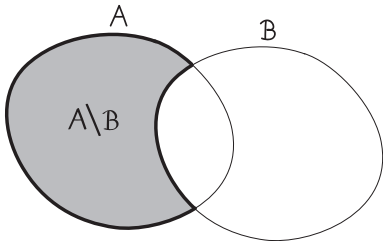


Abbildung 4: Euler-Venn-Diagram der Differenzmenge

8.8 Russell Paradoxon

Die Menge aller Mengen die sich nicht selber beinhalten.
$S = \{M | M \text{ ist Menge und } M \notin M\}$
$R = \{x \mid x \notin x\}$, then $R \in R \iff R \notin R$

8.9 Kreuzprodukt

Als Kreuzprodukt bezeichnet man die Menge aller **Elementpaare** (x_1, x_2) für die gilt $x_1 \in M_1$ und $x_2 \in M_2$

$$M_1 \times M_2 ... \times M_n := \{(x_1, x_2 ... x_n) | x_1 \in M_1, x_2 \in M_2 ... x_n \in M_n\} \tag{45}$$

8.10 Tupel

8.10.1 Zweitupel

$$M_1 \times M_2 := \{(x_1, x_2) | x_1 \in M_1 \text{ und } x_2 \in M_2\} \tag{46}$$

Hier beginnt der Mensch allenfalls zu Denken, man könne Systeme (Luhmann Theorie) von Elementen (Menschen, Firmen, Mechanische Systeme) Mathematisch darstellen. Beispiel:
Alle Elemente der ersten Menge mal alle Elemente der zweiten Menge:
$M_1 = \{1, 3, 4\}$
$M_2 = \{2, 4\}$
$M_1 \times M_2 = \{(1, 2), (1, 4), (3, 2), (3, 4), (4, 2), (4, 4)\}$

8.10.2 Dreitupel

$$M_1 \times M_2 \times M_3 := \{(x_1, x_2, x_3) | x_1 \in M_1 \text{ und } x_2 \in M_2 \text{ und } x_3 \in M_3\} \tag{47}$$
$$\tag{48}$$

8.10.3 n-Tupel

$$M_1 \times M_2 \times M_3 ... \times M_n := \tag{49}$$
$$\{(x_1, x_2, x_3 ... x_n) | x_1 \in M_1 \text{ und } x_2 \in M_2 \text{ und } x_3 \in M_3 ... x_n \in M_n\} \tag{50}$$

8.11 Mächtigkeit einer Menge

Die Mächtigkeit einer Menge bedeutet die Anzahl ihrer Mengen, man schreibt:

$$|M| \tag{51}$$

Sei die Menge der Natürlichen Zahlen gegeben $\mathbb{N}$ somit wäre ihre Mächtigkeit unendlich:

$$|\mathbb{N}| = \infty \tag{52}$$

8.11.1 Mächtigkeit eines Kreuzproduktes aus zwei Mengen

Sie entspricht dem Produkt der Mächtigkeiten der einzelnen Mengen. Sind zwei Mengen unendlich so sind diese gleich mächtig wenn es für die beiden Mengen eine Bijektion φ gibt.

$$|M_1 \times M_2| = |M_1| \cdot |M_2| \tag{53}$$
$$\varphi : M \to N \tag{54}$$

8.12 Relation

Eine Relation ist eine **Teilmenge eines Kreuzproduktes** aus den Mengen $M_1, M_2, M_3 ... M_n$, also $R \subseteq M_1 \times M_2 \times M_3 ... M_n$

Beispiel:
$R_7 \subseteq \mathbb{N} \times \mathbb{N}$
$R_7 = \{(a,b) \in \mathbb{N} \times \mathbb{N} | \exists_{d \in \mathbb{Z}} a - b = d \cdot 7\}$

Falls für $(a,b) \subseteq \mathbb{N} \times \mathbb{N}$ gilt $(a,b) \in R_7$ man schreibt auch $a \equiv b (\text{mod } 7)$
z.B. gilt für 17:
$17 \equiv 3 (\text{mod } 7)$, $17 \equiv 10 (\text{mod } 7)$, $17 \equiv 17 (\text{mod } 7)$, $17 \equiv 24 (\text{mod } 7)$
für $[17]_7 = \{b \in \mathbb{N} | b \equiv 17 (\text{mod } 7)$ gilt $[17]_7 = \{17 + d \cdot 7 | d > -3\}$

$$\text{falls für } (a,b) \in \mathbb{N} \times \mathbb{N} \text{ gilt } (a,b) \in R_q \text{ schreibt man auch } a \equiv b \text{ (mod q)} \tag{55}$$

$$R_q \subseteq \mathbb{N} \times \mathbb{N} \tag{56}$$

$$R_q = \{(a,b) \in \mathbb{N} \times \mathbb{N} | \exists_{d \in \mathbb{Z}} a - b = d \cdot q\} \tag{57}$$

$$\text{Sei } 0 \leq x < q \text{ und sei } [x]_q = \{b \in \mathbb{N} | b \equiv x \text{ (mod q) }\}, \text{ dann gilt:} \tag{58}$$
$$[x]_q = \{x + d \cdot q | d \geq 0\} \tag{59}$$

Somit ist $[x]_q$ eine Teilmenge von R_q

9 Abbildungen

Abbildungen sind eine Spezielle Art einer Relation:
Es seinen A und B zwei nicht-leere Mengen. Eine Zuordnungsvorschrift f: $A \to B$ mit $x \to f(x)$ (ausgesprochen: f von A nach B mit x wird abgebildet auf $f(x)$), die jedem Element $x \in A$ genau ein Element aus B zuordnet, heisst *Abbildung* oder *Funktion*. $f(x)$ heisst *Funktionswert* oder das *Bild* von x. X heisst ein Urbild von $f(x)$. Die **Menge** A heisst *Definitionsbereich* von f, B heisst *Bildbereich* von f.

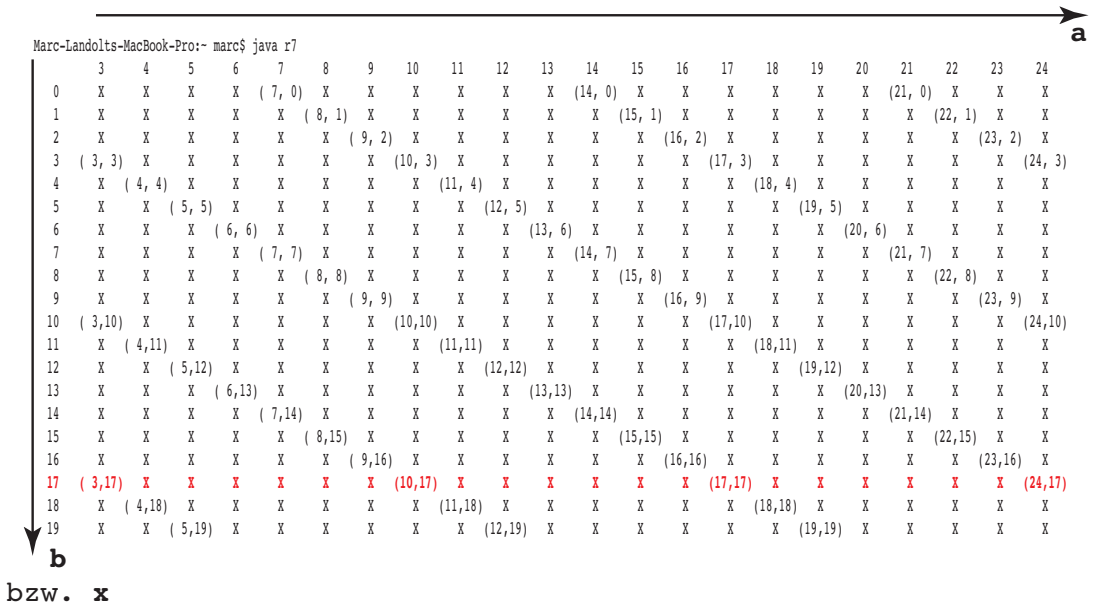


Abbildung 5: $[17]_7$

Beispiele:
$f : \mathbb{Z} \to \mathbb{Z}$ mit $f(x) = 2x + 3$
$f : \mathbb{Q} \to \mathbb{Q}$ mit $f(x) = 2x + 3$
$f : \mathbb{Z} \to \mathbb{N}$ mit $f(x) = x^2$
$f : \mathbb{Z} \to \mathbb{Z}$ mit $f(x) = x^3$

$$F = \{(x, f(x))|x \in A\} \tag{60}$$
$$F \subseteq A \times B \tag{61}$$

Die erste Komponente bezeichnet die Zweite eindeutig

9.1 Injektiv

Unterschiedliche Elemente des Definitionsbereichs (A) müssen auch unterschiedliche Bilder des Bildbereichs haben)

$$\forall_{x_1,x_2 \in A}\ x_1 \neq x_2 \rightarrow f(x_1) \neq f(x_2) \tag{62}$$

$$\forall_{x_1,x_2 \in A} f(x_1) = f(x_2) \rightarrow x_1 = x_2 \tag{63}$$

Beispiel:
$f : \mathbb{R} \rightarrow \mathbb{R}, x \rightarrow x^2$ nicht injektiv, denn $f(1) = f(-1)$ aber $1 \neq -1$
$f : \mathbb{R} \rightarrow \mathbb{R}, x \rightarrow x^3$ ist injektiv

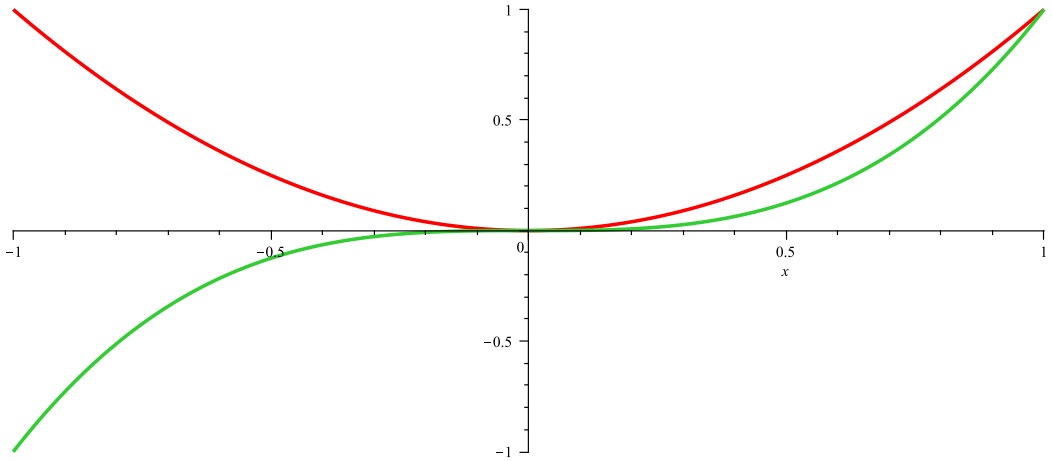


Abbildung 6:

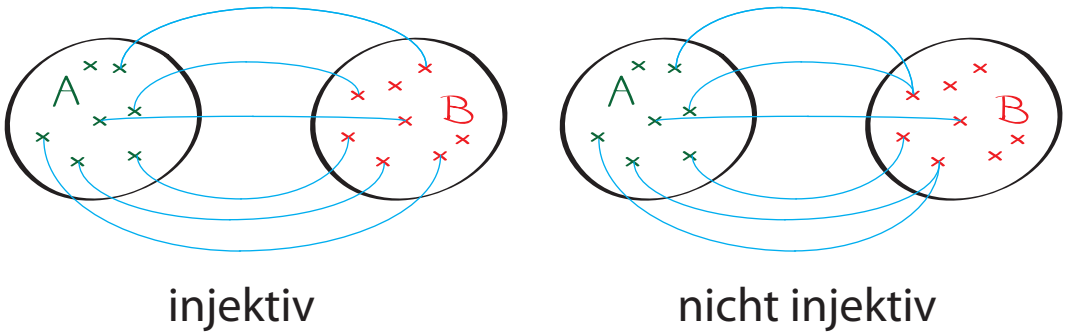


Abbildung 7:

9.2 Surjektiv

Für jedes Element in B wird verwendet und es gibt keine Element in B die nicht durch ein Element des Definitionsbereichs durch die ßpezielle Relationërreicht werden kann.

$$\forall_{y \in B} \exists_{x \in A} \; y = f(x) \tag{64}$$

Beispiel:
$f : \mathbb{R} \to \mathbb{R}, x \to x^2$ nicht surjektiv, für $f(x) = -1$ gibt es keine entsprechendes x
$f : \mathbb{R} \to [0, \infty), x \to x^2$ ist surjektiv, jeder Bildpunkt ist erreichbar
$f : \mathbb{R} \to \mathbb{R}, x \to 40 \cdot sin(x)$ nicht surjektiv, für $f(x) = 50$ gibt es keine entsprechendes x
$f : \mathbb{R} \to [-40, 40], x \to 40 \cdot sin(x)$ ist surjektiv, jeder Bildpunkt ist erreichbar

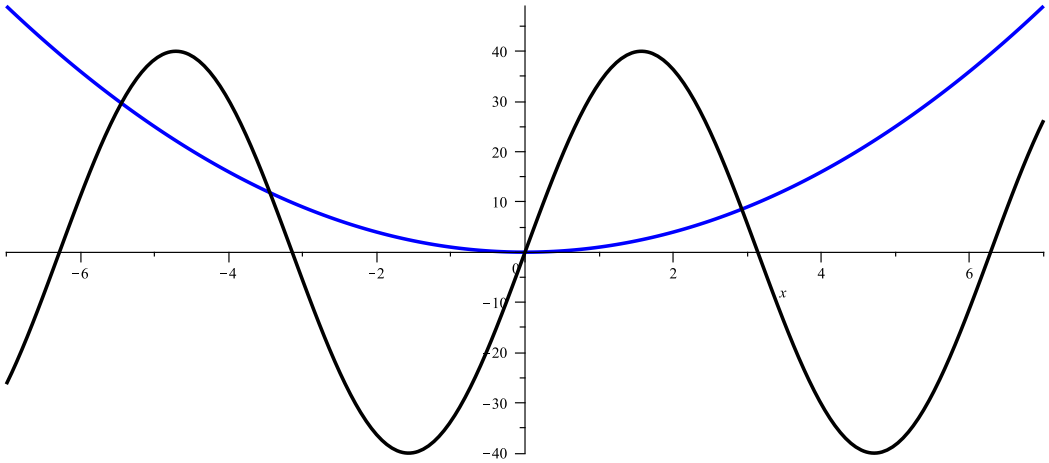


Abbildung 8:

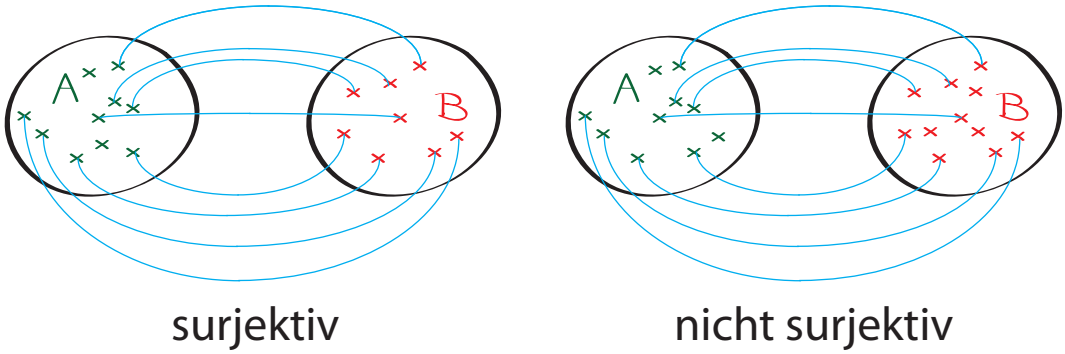


Abbildung 9:

9.3 Bijektiv

Eine Zuordnungsvorschrift welche **Injektiv und Surjektiv** ist nennt man Bijektiv.
$f_1 : \mathbb{R} \to \mathbb{R}, \quad x \mapsto x^2$ nicht injektiv, nicht surjektiv, nicht bijektiv
$f_2 : \mathbb{R}_0^+ \to \mathbb{R}, \quad x \mapsto x^2$ injektiv, nicht surjektiv, nicht bijektiv
$f_3 : \mathbb{R} \to \mathbb{R}_0^+, \; x \mapsto x^2$nicht injektiv, surjektiv, nicht bijektiv
$f_4 : \mathbb{R}_0^+ \to \mathbb{R}_0^+, \; x \mapsto x^2$ injektiv, surjektiv, bijektiv

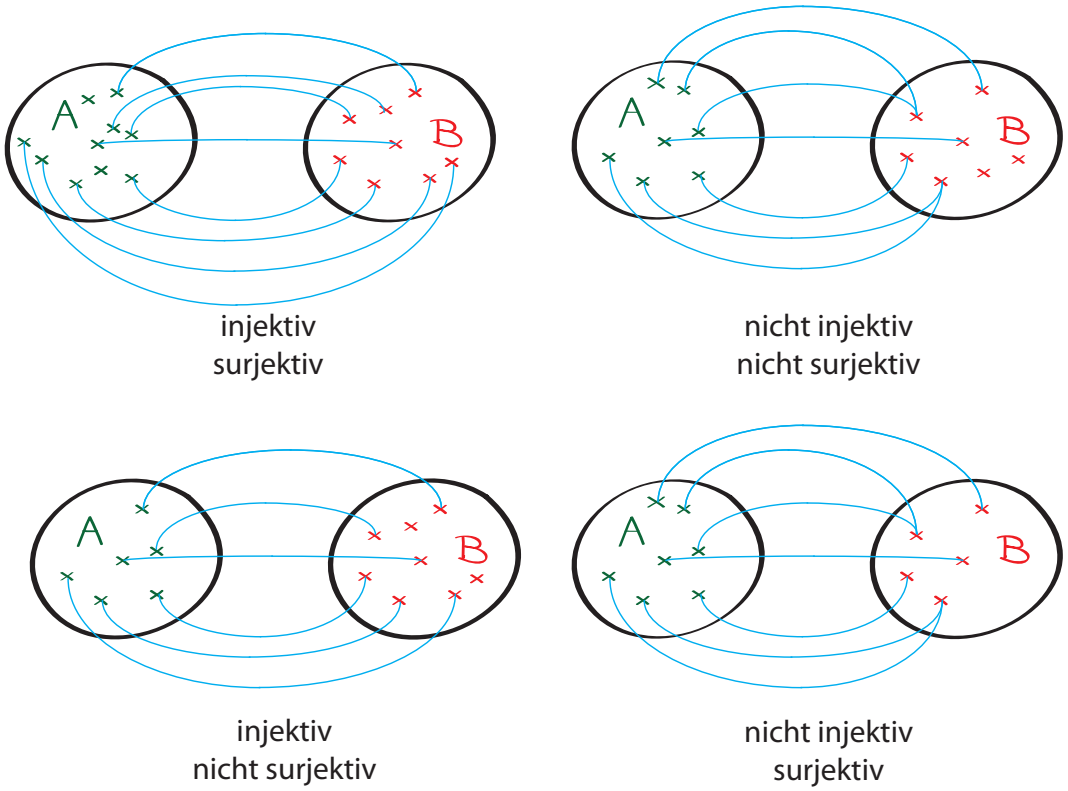


Abbildung 10:

9.4 Zuweisungsoperator $\mapsto$

$f : \mathbb{N} \to \mathbb{N}$
$f : x \mapsto x^2 + 1$
$f(x) = x^2 + 1$

9.5 Die $\mathbb{N}$atürlichen Zahlen

$$\mathbb{N} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, ...\} \tag{65}$$
$$\mathbb{N}_0 = \mathbb{N} \cup \{0\} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, ...\} \tag{66}$$

9.6 Axiomsystem von Giuseppe Peano

Ein Axiomsystem ist ein zusammenhängendes System von Axiomen die z.B. eine Menge eindeutig definiert. Und ein Axiom bezeichnet klassisch ein unmittelbar einleuchtendes Prinzip.

1. $0 \in \mathbb{N}$ (67)

2. $n \in \mathbb{N} \Rightarrow n' \in \mathbb{N}$ (68)

3. $n \in \mathbb{N} \Rightarrow n' \neq 0$ (69)

4. $m, n \in \mathbb{N} \Rightarrow (m' = n' \Rightarrow m = n)$ (wikipedia) (70)

4. $m, n \in \mathbb{N} \Rightarrow (m \neq n \Rightarrow m' \neq n')$ (Mathebuch) (71)

5. $0 \in X \wedge \bigvee n \in \mathbb{N} : (n \in X \Rightarrow n' \in X) \Rightarrow \mathbb{N} \subseteq X$ (72)

Und weil das kein normaler Mensch versteht hier noch auf Deutsch:

1. 0 ist eine natürliche Zahl.
2. Jede natürliche Zahl n hat eine natürliche Zahl n' als Nachfolger.
3. 0 ist kein Nachfolger einer natürlichen Zahl.
4. Sind m und n Natürliche Zahlen folgt daraus, dass zahlen mit gleichem Nachfolger identisch sind (wikipedia)
4. Verschiedene natürliche Zahlen haben verschiedene Nachfolger (Mathebuch)
5. Enthält X die 0 und mit jeder natürlichen Zahl n auch deren Nachfolger n', so bilden die natürlichen Zahlen eine Teilmenge von X. (Induktionsaxiom)
5. Ist die Aussage wahr für die Zahl 0 und ist sie stets, falls sie für eine Natürliche Zahl n wahr ist, dann auch für den Nachfolger von n wahr, dann ist sie für alle Nachfolger wahr.

Dabei wird $1 := 0'$ definiert und alle nachfolgenden $n' = n + 1$

9.6.1 Neumann Modell der natürlichen Zahlen

$$
\begin{aligned}
0 :=& 0 && && (73)\\
1 :=& 0' = \{0\} && = \{0\} && (74)\\
2 :=& 1' = \{0, 1\} && = \{0, \{0\}\} && (75)\\
3 :=& 2' = \{0, 1, 2\} && = \{0, \{0\}, \{0, \{0\}\}\} && (76)\\
& \vdots\!\vdots && \vdots && \\
n' :=& \{0, 1, 2, 3, ..., n\} && = n \cup \{n\} && (77)
\end{aligned}
$$

Die Menge 3 muss die Menge 2 und 1 auch beinhalten, denn ohne zu wissen was die Menge von 2 Objekten sind kann einen Menge von 3 Objekten nicht existieren.

9.6.2 Axiome

$$
\begin{array}{ll}
\text{Assoziativgesetz der Addition:} & (a + b) + c = a + (b + c)\\
\text{Kommutativgesetz der Addition:} & (a + b) = (b + a)\\
\text{Assoziativgesetz der Multiplikation:} & (a \cdot b) \cdot c = a \cdot (b \cdot c)\\
\text{Kommutativgesetz der Multiplikation:} & (a \cdot b) = (b \cdot a)\\
\text{Existenz eines Neutralen Elements:} & \\
\quad 0 \text{ für die Addition:} & a + 0 = 0 + a = a\\
\quad 1 \text{ für die Multiplikation:} & a \cdot 1 = 1 \cdot a = a\\
\text{Distributiv Gesetz:} & a \cdot (b + c) = ab + cb
\end{array}
\tag{78}
$$

Folgende Gleichungen sind in $\mathbb{N}$ nicht immer lösbar:

$$a + x = b \tag{79}$$

$$a \cdot x = b \tag{80}$$

Beispiele:

$$5 + x = 3$$

$$5 \cdot x = 3$$

Mit anderen Worten die inversen Operationen der Addition und Multiplikation sind in $\mathbb{N}$ nicht definiert.

9.7 Multiplikation

Bei der Multiplikation von vier Reihen à fünf Äpfel $4 \cdot 5 = 20$ geht die Information über die Anordnung verloren. Wollen wir das nun mit dem Menschlichen Gehirn wahrnehmen, fällt uns dies nicht ganz leicht da dies wieder die Natur ist. Sehen wir jedoch die vier mal fünf Äpfel vor uns springt es uns geradezu in die Augen, dass man diese ganz einfach unter vier oder fünf Leuten teilen kann. Aber nicht unbedingt, dass man diese auch unter zehn oder Zwanzig Leuten verteilen könnte. (Wahrnehmungspsychologie)

10 Die Ganzen Zahlen $\mathbb{Z}$

$$\mathbb{Z} = \{..., -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, ...\} \tag{81}$$
$$\tag{82}$$

10.0.1 Beweis

Sind die Natürlichen Zahlen $\mathbb{N}$ gegeben lassen sich daraus die Ganzen Zahlen $\mathbb{Z}$ konstruieren in dem man die Menge der Zahlen $\mathbb{N} \times \mathbb{N}$ also aller Paare der Natürlichen Zahlen.

$$0 := 0 \tag{83}$$
$$1 := 0' = \{0\} \qquad = \{0\} \tag{84}$$
$$2 := 1' = \{0, 1\} \qquad = \{0, \{0\}\} \tag{85}$$
$$3 := 2' = \{0, 1, 2\} \qquad = \{0, \{0\}, \{0, \{0\}\}\} \tag{86}$$
$$\vdots \qquad\qquad \vdots$$
$$n' := \{0, 1, 2, 3, ..., n\} \qquad = n \cup \{n\} \tag{87}$$

Die Menge 3 muss die Menge 2 und 1 auch beinhalten, denn ohne zu wissen was die Menge von 2 Objekten sind kann einen Menge von 3 Objekten nicht existieren.

10.0.2 Axiome

Assoziativgesetz der Addition:	$(a + b) + c = a + (b + c)$
Kommutativgesetz der Addition:	$(a + b) = (b + a)$
Assoziativgesetz der Multiplikation:	$(a \cdot b) \cdot c = a \cdot (b \cdot c)$
Kommutativgesetz der Multiplikation:	$(a \cdot b) = (b \cdot a)$
Existenz eines Neutralen Elements:	
0 für die Addition:	$a + 0 = 0 + a = a$
1 für die Multiplikation:	$a \cdot 1 = 1 \cdot a = a$
Distributiv Gesetz:	$a \cdot (b + c) = ab + cb$

Folgende Gleichungen sind in $\mathbb{N}$ nicht immer lösbar

$$a + x = b \tag{88}$$
$$a \cdot x = b \tag{89}$$

Beispiele:

$$5 + x = 3$$
$$5 \cdot x = 3$$

11 Summenzeichen

Das Summenzechen kann verwendet werden um Summen kürzer darzustellen:

$$\sum_{k=m}^{n} = a_m + a_{m+1} + a_{m+2} + ... + a_n \tag{90}$$

$$\sum_{k=m}^{n} (a_k + b_k) = \sum_{k=m}^{n} a_k \sum_{k=m}^{n} b_k \tag{91}$$

$$\sum_{k=m}^{n} \lambda a_k = \lambda \sum_{k=m}^{n} a_k \tag{92}$$

12 Vollständige Induktion

Sie besteht aus zwei Schritten
1. Verankerung (Induktionsanfang): Zuerst wird die Behauptung für die Zahl 0 gezeigt
2. Induktionsschritt): Mit der ersten Zahl probieren
3. Vollständige Induktion: Unter der Voraussetzung der Induktion, dass für eine Zahl $n \in \mathbb{N}$ gilt, wird gezeigt dass die Behauptung auch für n + 1 gilt. Wegen des 5. Peano Axioms gilt dies dann für alle Zahlen von $\mathbb{N}$

Beispiel 1:
$\sum_{i=1}^{n}(2 \cdot i - 1) = n^2$

$n = 1: \ 1 = 1^2$
$n = 2: \ (2 \cdot 2 - 1) + 1 = 2^2 = 4$
$n = 3: \ (2 \cdot 3 - 1) + (2 \cdot 2 - 1) + 1 = 3^2 = 9$
$n = 4: \ (2 \cdot 4 - 1) + (2 \cdot 3 - 1) + (2 \cdot 2 - 1) + 1 = 4^2 = 16$
$n = 5: \ (2 \cdot 5 - 1) + (2 \cdot 4 - 1) + (2 \cdot 3 - 1) + (2 \cdot 2 - 1) + 1 = 5^2 = 25$

Verankerung: bei $n = 1$
Beweis der Behauptung für $n = 1$:

$\sum_{i=1}^{1}(2 \cdot i - 1) = (2 \cdot 1 - 1) = 1$ (Stimmt also)

Der Satz sei Wahr für $n \in \mathbb{N}$

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

Somit müsste er auch für $n + 1$ wahr sein

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

$$\underbrace{\Big(\sum_{i=1}^{n}(2\cdot i-1)\Big)}_{n^2 \text{ (nach Vorgabe)}}+\big(2\cdot(n+1)-1\big)=$$

$$\overbrace{n^2}+2\cdot(n+1)-1=n^2+2n+2-1=\underbrace{n^2+2n+1}_{\text{Binom}}=(n+1)^2$$

Beispiel 2:
Behauptung:
Für alle $n \in \mathbb{N} \setminus \{0\}$ gilt:

$$\sum_{i=1}^{n} i = 1 + 2 + 3 + ... + n = \frac{n(n+1)}{2}$$

Verankerung bei $n = 1$

$$\sum_{i=1}^{1} i = 1 = \frac{1}{2}1 \cdot (1 + 1) = 1$$

Induktionschritt für $n = 2$

$$\sum_{i=1}^{2} i = 1 + 2 = \frac{1}{2}2 \cdot (2 + 1) = 3$$

Vollständige Induktion für $n' = n + 1$

$$\sum_{i=1}^{n+1} i = 1 + 2...(n + 1) = \big(\sum_{i=1}^{n} i\big) + (n + 1) =$$

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

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

$\frac{1}{2}n^2 + 1.5n + 1 = \frac{1}{2}n^2 + 1.5n + 1 \rightarrow$ Stimmt also.

Beispiel 3:
$\sum_{i=0}^{n} i^3 = 0 + 1 + 8 + 27 + ... + i^3 = \frac{n^2(n+1)^2}{4} = \left(\frac{n(n+1)}{2}\right)^2$

Verankerung bei $n = 0$
$\sum_{i=0}^{n} i^3 = 0 = \frac{0^2(0+1)^2}{4} = \left(\frac{0(n+1)}{2}\right)^2 = 0$ Stimmt also

Induktionschritt für $n = 1$
$\sum_{i=0}^{n} i^3 = 0 + 1 = \frac{1^2(1+1)^2}{4} = \left(\frac{1(1+1)}{2}\right)^2$

Vollständige Induktion für $n' = n + 1$

$$\sum_{i=0}^{n+1} i^3 = \underbrace{\sum_{i=0}^{n} i^3}_{\left(\frac{n(n+1)}{2}\right)^2} + (n+1)^3 = \left(\frac{(n+1)((n+1)+1)}{2}\right)^2$$

$$\left(\frac{n(n+1)}{2}\right)^2 + (n+1)^3 = \left(\frac{(n+1)(n+2)}{2}\right)^2$$

$$\underbrace{\left(\frac{n^2+n}{2}\right)^2}_{\frac{n^4+2n^3+n^2}{4}} + \underbrace{(n+1)(n+1)(n+1)}_{n^3+3n^2+3n+1} = \underbrace{\left(\frac{(n+1)(n+2)}{2}\right)^2}_{\left(\frac{n^2+3n+2}{2}\right)^2}$$

$$\underbrace{\underbrace{\frac{n^4+2n^3+n^2}{4} + \frac{4n^3+12n^2+12n+4}{4}}_{\frac{n^4+6n^3+13n^2+12n+4}{4}} = \underbrace{\frac{(n^2+3n+2)(n^2+3n+2)}{4}}_{\frac{n^4+6n^3+13n^2+12n+4}{4}}}_{\text{somit Identisch}}$$

13 Fakultätsoperator

♡ Die Fakultät $n!$ gibt die Anzahl möglichen Permutationen von n unterscheidbaren Objekten an ♡

Die drei Buchstaben a, b, c können auf $3! = 6$ arten angeordnet werden:
abc, acb, bac, bca, cab, cba

$$n! = \prod_{i=1}^{n} i = 1 \cdot 2 \cdot 3 \cdot ... \cdot n \tag{93}$$

$$n! = (n-1)! \cdot n \text{ für } n \geq 1 \tag{94}$$

$0! = 1$
$1! = 1$
$2! = 2$
$3! = 6$
$4! = 24$
$5! = 120$
$6! = 720$
$7! = 5.040$
$8! = 40.320$
$9! = 362.880$

14 Fibonacci

$f_0 = 0$
$f_1 = 1$
$f_n = f_{n-1} + f_{n-2}$
0 1 1 2 3 5 8 13 21 34 55 89 144 233 377 610 987 1597 2584 4181 6765 10946 17711 28657 46368 75025 ...

15 Binomialkoeffizient

Der Binomialkoeffizient kann verwendet werden um z.B. zu berechnen wie verschiedene dreiergruppen aus 10 verschiedenen Leuten gebildet werden können. $\binom{10}{3}$
Oder wieviele verschiedene Kombinationen es beim Lotto gibt $\binom{45}{6}$

♡ Oder anders ausgedrückt $\binom{n}{k}$ ist die Anzahl der Möglichkeiten, Untermengen von k Objekten aus einer Menge mit n (unterscheidbaren) Objekten zu bilden. ♡

$$\binom{n}{0} = \binom{n}{n} = 1 \tag{95}$$

$$\binom{n}{k} = \frac{n!}{k! \cdot (n-k)!} \tag{96}$$

$$\binom{n}{k} = \frac{n(n-1)(n-2)...(n-k+1)}{1 \cdot 2 \cdot ... \cdot k} \tag{97}$$

$$\binom{n}{k} = \binom{n}{n-k} \tag{98}$$

$$
\begin{array}{ccccccccccccccccccc}
 & & & & & & & & 1 & & & & & & & & & & \\
 & & & & & & & 1 & & 1 & & & & & & & & & \\
 & & & & & & 1 & & 2 & & 1 & & & & & & & & \\
 & & & & & 1 & & 3 & & 3 & & 1 & & & & & & & \\
 & & & & 1 & & 4 & & 6 & & 4 & & 1 & & & & & & \\
 & & & 1 & & 5 & & 10 & & 10 & & 5 & & 1 & & & & & \\
 & & 1 & & 6 & & 15 & & 20 & & 15 & & 6 & & 1 & & & & \\
 & 1 & & 7 & & 21 & & 35 & & 35 & & 21 & & 7 & & 1 & & & \\
1 & & 8 & & 28 & & 56 & & 70 & & 56 & & 28 & & 8 & & 1 & & \\
 & 9 & & 36 & & 84 & & 126 & & 126 & & 84 & & 36 & & 9 & & 1 &
\end{array}
\tag{99}
$$

Der Binomialkoeffizient kann aus den beiden Darüberliegenden werten berechnet werden:

$$
\binom{n}{m-1} + \binom{n}{m} = \binom{n+1}{m} \tag{100}
$$

16 ggT, kgV und Euklid

16.1 ggT

Der grösste gemeinsame Teiler $ggT(a, b)$ sind die Primfaktoren welche in beiden Zahlen a, b vorkommen, kommen sie in beiden Zahlen mehrfach vor so kommen sie im ggT auch mehrfach vor.
Beispiel:

$$\begin{array}{lccccccl} \text{ggT(84,56)} & & & & & & & \\ 84 = & 2 & 2 & & 3 & 7 & & \\ 56 = & 2 & 2 & 2 & & 7 & & \\ \hline & 2 & 2 & & & 7 & = 2 \cdot 2 \cdot 7 = 28 \end{array} \tag{101}$$

$\rightarrow ggT(84, 56) = 28$

Dies kann man einfacher durch den Euklidschen Algorithmus berechnen
Wenn $a, b \in \mathbb{Z} \wedge b \neq 0$ heisst a durch b teilbar wenn eine ganze Zahl $q \in \mathbb{Z}$ existiert für die gilt $a = q \cdot b$

$$\text{Man sagt: } b|\ a \qquad \text{(b ist ein Teiler von a)} \tag{102}$$

Der $g = ggT(a, b)$ wird von jedem anderen Teiler der beiden Zahlen a, b geteilt.

$$g = ggT(a, b) \leftrightarrow ((t|a \wedge t|b) \leftarrow t|d) \tag{103}$$

16.2 kgV

Das kleinste gemeinsame Vielfache $kgV(a, b)$ ist die kleinste Zahl die sowohl durch a wie auch durch b ohne Rest teilbar sind. Dazu nimmt man alle Primfaktoren der beiden Zahlen von der Zahl bei der sie in der höchsten Potzenz vorkommen.
Beispiel:

$$\begin{array}{lccccccl} \text{kgV(84,56)} & & & & & & & \\ 84 = & 2 & 2 & & 3 & 7 & & \\ 56 = & 2 & 2 & 2 & & 7 & & \\ \hline & 2 & 2 & 2 & 3 & 7 & = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 7 = 168 \end{array} \tag{104}$$

16.3 $kgV \cdot ggT$

$$kgV(a, b) \cdot ggT(a, b) = a \cdot b \tag{105}$$

16.4 Euklid

16.4.1 Pseudocode C64 Style

```
10 a=45, b=20
20 r=a%b
30 a=b
40 b=r
50 if b<>0 goto 20
60 PRINT a
```

16.4.2 Code im Java Style (Rekursiv)

```
public static int euklid(int a, int b)
{
         int r=a%b;
         a=b;
         b=r;
         if(r==0) return a;
         else return euklid(a,b);
}
```

16.4.3 Code im C++ Style

```
#include <iostream>
int euklid( int a, int b);
using namespace std;
int main()
{
        std::cout << "ggT(33,99)" << euklid(33,99) << " ";
        cout << " " << euklid(15,5) << " ";
}
int euklid( int a, int b)
{
        if (a==0) return 0;  //0 signalisiert dass etwas falsch ist
        if (b==0) return 0;
        if (a==b) return a;
        int Qab;             //ziemlich nutzlos, mathematischen korrekt
        int Rab = a%b;       //% ist der Modulo Operator
        while(Rab!=0)
        {       a=b;
                Qab=a/b;     //Integer Division, keine Nachkommastellen
                b=Rab;
                Rab=a%b;
        }
        return b;
}
```

16.5 Euklidscher Alogrithmus

Wenn $a \in \mathbb{Z},\ b \in \mathbb{N} \wedge b \neq 0$ dann gibt es eindeutig bestimmbare zahlen $q \in \mathbb{Z}$ und $r \in \mathbb{N}$ mit $0 \leq r \leq b$ so dass gilt $a = q \cdot b + r$.

$$q = a : b \text{ Ganzzahlige Division} \tag{106}$$
$$a = q \cdot b + r \tag{107}$$
$$a \equiv b(\text{mod q}) \tag{108}$$

Dies wiederholt man solange bis $r = 0$ dann ist $r_a b = a - q * b$ und somit der $ggT(a, b)$

16.5.1 Beweis Euklid

Seien $a, b \in \mathbb{N}$ beliebig, $a \neq b$, $a \neq 0$, $b \neq 0$
Seien a, b, q_{xy} und r_{xy} festgelegt wie in der Definition des Euklidschen Algorithmus: $a = q_{xy} \cdot b + r_{xy}$ mit $0 \leq r_{xy} < y$.
Der Euklidsche Algorithmus benötige m Schleifendurchgänge bis er abbricht.
a_0 = a-Wert bei der Initialisierung
b_0 = b-Wert bei der Initialisierung
q_0 = q_{xy}-Wert bei der Initialisierung
r_0 = r_{xy}-Wert bei der Initialisierung

Für $1 \leq k \leq m$ setze man
a_k = a-Wert nach Schleifendruchgang k
b_k = b-Wert nach Schleifendruchgang k
q_k = q_{xy}-Wert nach Schleifendruchgang k
r_k = r_{xy}-Wert nach Schleifendruchgang k

Es existiert eine Zahl $g = s \cdot a + t \cdot b$ $(s, t \in \mathbb{Z} \setminus \{0\})$

ggT(147,56)

147 =				3	7	7	
56 =	2	2	2		7		
					7		= 7

(109)

```
147=2*56+35
56=1*35+21
35=1*21+14
21=1*14+7
14=1*7+0
```

Bei der Modulooperation zweier zahlen beinhaltet das Resultat immer noch alle gemeinsam vorkommenden Primfaktoren wo hingegen Primfaktoren welche nicht in beiden Zahlen vorhanden sind eliminiert werden. Ausser b ist Teiler von a

S 72 ist noch ein Axiom dass nicht verarbeitet wurde
21 * 7 = 147 8 * 7 = 56

16.6 erweiterter Euklid

Dieser berechnet noch $ggT(a, b) = s \cdot a + t \cdot b$ welchen wir später benötigen werden.

```
/*
Es wird der ggT von a und b berechnet. Zusätzlich werden koeffizienten s und t berechnet,
Falls die Berechnung des ggT nciht möglich ist, wird false zurückgemeldet. Andernfalls tru
*/

#include <iostream>

int euklid( int a, int b);
bool ErwEuklidAlg( int a, int b, int &ggT, int &s, int &t);


using namespace std;


int main(int argc, char** argv)
{
  int a=147;
  int b=56;
  int ggT=0;
  int s=0;
  int t=0;
  ErwEuklidAlg(a,b,ggT,s,t);
  cout <<"ggT(55, 65)"<<a<<" "<<b<<" "<<ggT<<" "<<s<<" "<<t;
}


bool ErwEuklidAlg( int a, int b, int &ggT, int &s, int &t)
{
  if (a==0)return false;
  if (b==0)return false;
  if (a==b)return false;
if (a<b)
  {
    int nTemp=b;
    b=a;
    a=nTemp;
  }
```

```
//nMax ist die maximale Anzahl der möglichen Schleifendruchläufe

  int nMax=b;

  int x, y, r;
  int * q=new int[nMax];

  //Initialisierung
  int m=0;
  x=a;
  y=b;
  q[m]=x/y;
  r=x%y;

  while (r!=0)
  {
    m++;
    x=y; y=r;
    q[m]=x/y;
    r=x%y;
  }

  ggT=y;

  //Spezialfall: b ist bereits Tailer von a
  if (m==0)
  {
    s=1;
    t=-a/b+1;
    return true;
  }

  s=1;
  t=-q[m-1];

  for(int i=(m-2);i>=0;i--)
  {
    int nSalt=s;
    s=t;
    t=nSalt-t*q[i];
  }
```

```
  return true;
}
```

17 Primzahlen

Eine Primzahl sei eine Zahl p $p \in \mathbb{N}, p \neq 0$ und $o \neq 1$ welche nur durch sich selber und durch 1 teilbar ist.

Beispiele:
Im Maple erhält man die ersten 100 Primzahlen mit:
$n \rightarrow ithprime(n)$;
$seq(ithprime), i = 1..100$

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227, 229, 233, 239, 241, 251, 257, 263, 269, 271, 277, 281, 283, 293, 307, 311, 313, 317, 331, 337, 347, 349, 353, 359, 367, 373, 379, 383, 389, 397, 401, 409, 419, 421, 431, 433, 439, 443, 449, 457, 461, 463, 467, 479, 487, 491, 499, 503, 509, 521, 523, 541

Es gibt unendlichviele Primzahlen, denn sind p_i die Primzahlen der Reihe nach von 2 her, so ist $1 + \prod_{i=1}^{n}$ wieder eine Primzahl, aber nicht die nächste.

Eines der schnellsten verfahren Primzahlen zu finden ist das Sieb des Eratosthenes:
1. Generiere eine Liste von Zahlen bis zu der Zahl man Primzahlen finden will
2. für alle Primteiler $\leq \sqrt{g}$ gehe man durch die Liste und streiche alle Vielfachen des Primteilers
3. man gehe zum nächsten Primteiler und streiche wieder alle vielfache durch Was übrig bleibt sind Primzahlen. Auf wikipedia gibt es eine schöne Animation davon

17.1 Implementation in C++

```
#include <iostream>
bool eratosthenes(bool *nListe, int nGrenze);  //Forward Declaration
using namespace std;
int main(int argc, char** argv)
{
  int count=0;
  int grenze=500;
  bool *liste=new bool[grenze];
  eratosthenes(liste, grenze);
  for( int i=0;i<grenze;i++ )
    if(liste[i]==false)
    {
      cout<<" "<<i;
      count++;
    }
  cout<<endl<<count;
 }

bool eratosthenes(bool *nListe, int nGrenze)    //nListe ist true wenn teilbar
{
  if(nGrenze<2) return false;

  int nPrimteiler=2,q=0;
  while(nPrimteiler*nPrimteiler<=nGrenze)
  {
    q=2;
    while(q*nPrimteiler<=nGrenze)
    {
      nListe[q*nPrimteiler]=true;
      q++;
    }

    do
    {
      nPrimteiler++;
    }
    while(nListe[nPrimteiler]==true);
  }
  return true;
}
```

Sind $a, b, p \in \ltimes$ und alles Primzahlen, und p das Produkt $a \cdot b$ teilt, so gilt entweder $p|a \vee p|b$

$$p|a \cdot b \rightarrow p|a \vee p|b \text{ für Primzahlen} \tag{110}$$

Allenfalls hier noch Beweis einfügen

17.2 Zahlen als Primfaktoren

Jede Natürliche Zahl $a > 1$ lässt sich als Produkt von Primzahlen darstellen:

$$a = \prod_{i=1}^{n} p_i \tag{111}$$

Da einige Primfaktoren mehrfach vorkommen kann man diese in der Potenzschreibweise darstellen

$$a = \prod_{i=1}^{n} p_i^{m_i} \tag{112}$$

```
public class systemumrechnung
{

        public static void main(String[] args)
        {
                System.out.println("b= "+toSystem(3091, 7));
                System.out.println("b= "+toDecimal("12004",7));
        }

        public static String toSystem(int a, int sysb)
        {
                int stelleB=0;
                String b=" ";
                while(a>0)
                {
                        b+=(a%sysb);
                        stelleB++;
                        a=a-(a%sysb);
                        a=a/sysb;
                        System.out.println(a);
                }
                return new StringBuffer(b).reverse().toString();
        }
```

```
        public static int toDecimal(String a, int sysa)
        {
                int result=0;
                for(int i=a.length(); i>0; i--)
                {
                        result+=(java.lang.Integer.parseInt(a.substring(i-1,i))) * Math.po
                }
                return result;
        }
}
```

18 Allgemeine Zahlentheorie

18.1 Zahlensysteme

Für alle Zahlensysteme, z.B. das Zehnersystem ($b = 10$) gilt

$$\forall_{0 \leq i < m} 0 \leq z_i < b \tag{113}$$

$$z_m \neq 0 \tag{114}$$

$$n = \sum_{i=0}^{m} z_i \cdot b^i \tag{115}$$

$$\tag{116}$$

18.2 Zahlenmengen

= Leere Menge
N = Natürliche Zahlen
Z = Ganze Zahlen
Q = Rationale Zahlen
R = Reelle Zahlen
C = Komplexe Zahlen

18.3 Die Ganzen Zahlen $\mathbb{Z}$

Subtraktion: abgeschlossen Multiplikation: abgeschlossen Division: nicht abgeschlossen, es fehlen Werte

Assoziativgesetz der Addition:	$\bigforall_{a,b,c\in\mathbb{Z}}\ (a+b)+c=a+(b+c)$	
Kommutativgesetz der Addition:	$\bigforall_{a,b\in\mathbb{Z}}\ (a+b)=(b+a)$	
Assoziativgesetz der Multiplikation:	$(a\cdot b)\cdot c=a\cdot(b\cdot c)$	
Kommutativgesetz der Multiplikation:	$(a\cdot b)=(b\cdot a)$	
Distributiv Gesetz:	$a\cdot(b+c)=ab+cb$	
Existenz eines Neutralen Elements:		
0 für die Addition:	$\bigexists_{e\in\mathbb{Z}}\ \bigforall_{a\in\mathbb{Z}}\ a+e=e+a=a$	$a+0=0+a=a$
1 für die Multiplikation:	$\bigexists_{e\in\mathbb{Z}}\ \bigforall_{a\in\mathbb{Z}}\ a\cdot e=e\cdot a=a$	$a\cdot 1=1\cdot a=a$
Inverses Element:	$\bigforall_{z\in\mathbb{Z}}\ \bigexists_{-z\in\mathbb{Z}}\ z+(-z)=(-z)+z=e$	

(117)

18.4 allgemeine Definition einer Gruppe

Das Tupel $(G,\otimes)$ aus der Menge G und der Verknüpfung $\otimes\ G\times G\to G$ heisst Gruppe wenn gilt

Assoziativgesetz: $\bigforall_{a,b,c\in G}\ (a\otimes b)\otimes c=a\otimes(b\bigotimes c)$
Neutrales Element: $\bigexists_{e\in G}\bigforall_{a\in G}\ a\otimes e=e\otimes a=a$
Inverses Element: $\bigforall_{x\in G}\bigexists_{y\in G}\ x\otimes y=y\otimes x=e$

y heisst das Inverse Element zu x bezüglich der Operation $\otimes$ z.B. $(\mathbb{Z},+)$ ist eine Gruppe

$$a\otimes x=b\quad|\otimes\alpha \tag{118}$$
$$\alpha\otimes a\otimes x=\alpha\otimes b \tag{119}$$
$$e\otimes x=\alpha\otimes b \tag{120}$$
$$x=\alpha\otimes b \tag{121}$$
$$a\otimes x=b\to x=\alpha\otimes b \tag{122}$$
$$\alpha\otimes b\to x=a\otimes x=b \tag{123}$$
$$a\otimes x=b\leftrightarrow x=\alpha\otimes b \tag{124}$$
$$ \tag{125}$$

18.5 kommutative Gruppe oder Abelsche Gruppe

$$(G, \otimes) \text{ ist eine Gruppe} \tag{126}$$

$$\forall_{x,y \in G} x \otimes y = y \otimes x \tag{127}$$

$(\mathbb{Z}, +)$ ist eine Kommutative (bzw. Abelsche) Gruppe

18.6 Ganze Zahlen und Ringe

$(\mathbb{Z}, \cdot)$ ist keine Gruppe, denn folgendes ist nicht lösbar:
$0 \cdot x = 0$ nicht eindeutig lösbar
$0 \cdot x = 5$ oder $4 \cdot x = 7$ ist in $\mathbb{Z}$ überhaupt nicht lösbar

18.6.1 Ring $(R, +, \cdot)$

$(R, +)$	ist eine Kommutative Gruppe
$\forall_{x,y,z \in R}\ x \cdot (y \cdot z) = (x \cdot y) \cdot z$	Assoziativität gegenüber Multiplikation
$\forall_{x,y,z \in R}\ x \cdot (y + z) = x \cdot y + x \cdot z$	Distributivität
$\forall_{x,y,z \in R}\ (y + z) \cdot x = y \cdot x + z \cdot x$	Distributivität

18.6.2 Kommutiativer Ring $(R, +, \cdot)$

$(R, +, \cdot)$ ist ein Ring

$\forall_{x,y,z \in R}\ x \cdot y = y \cdot x$	Kommutativgesetz der Multiplikation

18.7 Die Rationalen Zahlen

$\mathbb{Q} = \left\{ x | x = \frac{p}{q} \text{ für } p = \mathbb{Z} \text{ und } q = \mathbb{Z} \setminus \{0\} \right\}$

Assoziativgesetz der Addition:	$\forall_{a,b,c\in\mathbb{Q}}\ (a+b)+c=a+(b+c)$	
Kommutativgesetz der Addition:	$\forall_{a,b\in\mathbb{Q}}\ (a+b)=(b+a)$	
Assoziativgesetz der Multiplikation:	$(a\cdot b)\cdot c=a\cdot(b\cdot c)$	
Kommutativgesetz der Multiplikation:	$(a\cdot b)=(b\cdot a)$	
Distributiv Gesetz:	$a\cdot(b+c)=ab+cb$	
Existenz eines Neutralen Elements:		
0 für die Addition:	$\exists_{e\in\mathbb{Z}}\ \forall_{a\in\mathbb{Z}}\ a+e=e+a=a$	$a+0=0+a=a$
1 für die Multiplikation:	$\exists_{e\in\mathbb{Z}}\ \forall_{a\in\mathbb{Z}}\ a\cdot e=e\cdot a=a$	$a\cdot 1=1\cdot a=a$
Inverses Element:		
für die Addition:	$\forall_{z\in\mathbb{Q}}\ \exists_{-z\in\mathbb{Q}}\ z+(-z)=(-z)+z=e$	manchmal auch $\widetilde{a}$
für die Multiplikation:	$\forall_{q\in\mathbb{Q}\setminus\{0\}}\ \exists_{\frac{1}{q}\in\mathbb{Q}}\ q\cdot\frac{1}{q}=\frac{1}{q}\cdot q=q\cdot q^{-1}=e$	
mit Brüchen:	$\forall_{\frac{p}{q}\in\mathbb{Q}\setminus\{0\}}\ \exists_{\frac{q}{p}\in\mathbb{Q}}\ \frac{p}{q}\cdot\frac{q}{p}=\frac{q}{p}\cdot\frac{p}{q}=e$	

(128)

$(\mathbb{Q}\setminus\{0\},\cdot)$ ist eine Abelsche Gruppe

18.8 Körper

$(K,+)$	ist eine Kommutative Gruppe
$(K\setminus\{0\},\cdot)$	ist eine Gruppe
$\forall_{x,y,z\in K}\ x\cdot(y+z)=x\cdot y+x\cdot z$	Distributivität
$\forall_{x,y,z\in K}\ (y+z)\cdot x=y\cdot x+z\cdot x$	Distributivität

18.8.1 Kommutativer Körper

Ist $(K\setminus\{0\},\cdot)$ eine abelsche Gruppe ist $(K\setminus\{0\},+,\cdot)$ ein Kommutativer Körper

18.9 Dezimalstellen

$$0,a_1a_2a_3a_4...a_n=\frac{a_1a_2a_3a_4...a_n}{10^n} \tag{129}$$

$$0,\overline{a_1a_2a_3a_4...a_n}=\frac{a_1a_2a_3a_4...a_n}{10^n-1} \tag{130}$$

$$0,a_1a_2a_3a_4...a_n\overline{b_1b_2b_3b_4...b_m}=0,a_1a_2a_3a_4...a_n+\frac{1}{(10^n-1)\cdot 10^m} \tag{131}$$