# Grundbegriffe und Schreibweisen

# Yoan Tchorenev

# 25. September 2022

# Inhaltsverzeichnis

1	Log	ik 1
	1.1	Begriffe
	1.2	Terme
	1.3	Beweise
<b>2</b>	Mer	ngenlehre
	2.1	Begriffe
	2.2	Operationen auf Mengen
3	Fun	ktionen
	3.1	Begriffe
	3.2	Umkehrfunktion
4	Zah	len 8
	4.1	Sprachunterschiede
	4.2	natürliche Zahlen
	4.3	Ganze Zahlen
	4.4	Primzahlen
	4.5	Teilbarkeit
	4.6	Additionssysteme
	4.7	Positionssysteme
		471 Umrechning

# 1 Logik

# 1.1 Begriffe

Aussage: Eine Aussage ist eine Formel oder ein sprachliches Gebilde dem genau ein Wahrheitswert zugeordnet werden kann.

Warheitswerte Genau der Eine oder der Andere

Falsch	Wahr
0	1
$\perp$	T
$\mathbf{L}$ ow	$\mathbf{H}$ igh

Aussagevariable A,B,C etc. stehen für eine Aussage

Junktoren (Verknüpfer)

Negation 
$$\neg A$$
 "nicht", "NOT", auch:  $\sim A$ ,  $\bar{A}$ ,  $A'$ 

$$\begin{array}{c|c}
A & \neg A \\
\hline
0 & 1 \\
1 & 0
\end{array}$$
 Mathematisch:  $\neg A = (A+1) \bmod 2$ 

**Konjunktion**  $A \wedge B$  "A und B", "AND", auch  $A \cdot B$ , AB

Α	В	$A \wedge B$	Mathematisch:	$A \wedge B = A \cdot B$
0	0	0	Kommutativ:	$A \wedge B \equiv B \wedge A$
0	1	0	Assoziativ:	$A \wedge (B \wedge C) \equiv (A \wedge B) \wedge C$
1	0	0	Idempotent:	$A \wedge A \equiv A$
1	1	1	$A \wedge \bot \equiv \bot$	$A \wedge \top \equiv A$
	A 0 0 1 1	A B 0 0 0 1 1 0 1 1	A     B     A∧B       0     0     0       0     1     0       1     0     0       1     1     1	0         0         0           0         1         0           1         0         0   Kommutativ: Assoziativ: Idempotent:

**Disjunktion** A∨B "A oder B" (inklusiv), "OR"

A	$\mid B \mid$	$A \lor B$	Mathematisch:	$A \vee B = \min(A + B; 1)$
0	0	0	Kommutativ:	$A \vee B \equiv B \vee A$
0	1	1	Assoziativ:	$A \lor (B \lor C) \equiv (A \lor B) \lor C$
1	0	1	Idempotent:	$A \lor A \equiv A$
1	1	1	$A \lor \bot \equiv A$	$A \lor \top \equiv \top$

Kontravalenz A∨B "entweder A, oder B" (exclusiv), "XOR", auch: A⊕B

A	B	A∨̇́B	Mathematisch:	$A\dot{\vee}B = (A+B) \bmod 2$
0	0	0	Kommutativ:	$A\dot{\vee}B \equiv B\dot{\vee}A$
0	1	1	Assoziativ:	$A\dot{\vee}(B\dot{\vee}C) \equiv (A\dot{\vee}B)\dot{\vee}C$
1	0	1	¬Idempotent:	$A\dot{\lor}A\equiv\bot$
1	1	0	$A\dot{\lor}\bot \equiv A$	$A\dot{\lor}\top \equiv \neg A$

**Konditional** A $\Rightarrow$ B "wenn A dann B" auch "Subjunktion", "Implikation", "IMPLY" A  $\mid B \mid \mid A \rightarrow B \mid A$ 

Α	B	А⇒В	A	В	$A \Rightarrow B \equiv \neg A \lor B$
0	0	1	Prämisse	Konklusion	Mathematisch: $A \Rightarrow B =$
0	1	1	Voraussetzung	Konsequenz	$\min((A+1) \bmod 2 + B; 1)$
1	0	0	hinreichende	notwendige	
1	1	1			

Eigenschaften  $A \Rightarrow \bot \equiv \neg A$ ;  $A \Rightarrow \top \equiv \top$ ;  $\bot \Rightarrow A \equiv \top$ ;  $\top \Rightarrow A \equiv A$ 

Kontraposition  $A \Rightarrow B \equiv \neg B \Rightarrow \neg A$ Abtrennungsregel  $(A \land (A \Rightarrow B)) \Rightarrow B$ 

Kettenschluss  $((A \Rightarrow B) \land (B \Rightarrow C)) \Rightarrow (A \Rightarrow C)$ 

**Bikonditional** A⇔B "A genau dann, wenn B", "XNOR", auch "Aquivalenz" ≡

A	В	A⇔B	Mathematisch:	$A \Leftrightarrow B = (A + B + 1) \mod 2$
0	0	1		$A \Leftrightarrow B \equiv B \Leftrightarrow A$
0	1	0	Assoziativ:	$A \Leftrightarrow (B \Leftrightarrow C) \equiv (A \Leftrightarrow B) \Leftrightarrow C$
1	0	0	¬Idempotent:	
1	1	1	$A \Leftrightarrow \bot \equiv \neg A$	$A \Leftrightarrow \bot \equiv A$

### 1.2 Terme

Tautologie Ein Term W heißt heißt Tautologie, wenn er nur den Wahrheitswert 1 hat.

Äquivalenz Zwei aussagenlogische Terme W und V heißen logisch äquivalent

$$W \equiv V$$

wenn sie gleichen Wahrheitswert haben. Zwei Terme W und V sind genau dann logisch äquivalent, wenn der Term  $W \Leftrightarrow V$  Tautologie ist.

## Klammern Regeln:

- Außenklammern können weggelassen werden
- Die stärke der Zeichen ist konventionell:  $\neg > \land > \lor$ . D.h.:

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

•  $\land$  und  $\lor$  sind distributiv zueinander:

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

$$A \lor (A \land B) \equiv (A \lor B) \land (A \lor C)$$

•  $\wedge$  ist distributiv über  $\dot{\vee}$ :

$$A \wedge (B\dot{\vee}C) \equiv (A \wedge B)\dot{\vee}(A \wedge C)$$

De-Morganische Gesetze

$$\overline{A \wedge B} \equiv \overline{A} \vee \overline{B}$$

$$\overline{A \vee B} \equiv \overline{A} \wedge \overline{B}$$

#### 1.3 Beweise

Aussageform Haben die Form einer Aussage, enthalte aber Variablen.

$$3 + x = 5$$
;  $A(x)$ ;  $B(x; y)$ 

- werden zu Aussagen, wenn die Variablen belegt werden. Für die Variablen ist ein eingrenzender Grundbereich vorzugeben. Z.B.:  $x \in \mathbb{N}$
- Wie Aussagen kann man Aussageformen miteinander Verknüpfen (mit Junktoren) und man erhält neue Aussageformen

Quantoren Außer der Belegung der Variablen mit Werten gibt es noch andere Möglichkeiten aus einer Aussageform eine Aussage zu machen. Ein Grundbereich M muss vorgegeben sein.

"Für alle x aus M gilt A(x)"

Für alle  $x \in \mathbb{N}$  gilt 3 + x = 5 (falsche Aussage) kurz mit Allquantor  $\forall$ :

$$(\forall x \in \mathbb{N}) \ 3 + x = 5$$

"Es existiert ein x aus M mit A(x)"

Es existiert (mindestens) ein  $x \in \mathbb{N}$  mit 3 + x = 5 (wahre Aussage) kurz mit Existenzquantor  $\exists$ :

$$(\exists x \in M) \ 3 + x = 5$$

"Es existiert höchsten ein x aus M mit A(x)"

$$(\forall x)(\forall y) (A(x) \land A(y) \Rightarrow x = y)$$

"Es existiert genau ein x aus M mit A(x)"

$$(\exists!x)A(x) \equiv ((\exists x)A(x)) \land ((\forall x)(\forall y) \ (A(x) \land A(y) \Rightarrow x = y))$$

# 2 Mengenlehre

# 2.1 Begriffe

Georg Cantor (1845-1918)

Cantors naive Mengendefinition Unter einer Menge verstehen wir eine Zusammenfassung von wohldefinierten Objekten m unserer Anschauung oder unseres Denkens welche die Elemente von M genannt werden, zu einem einheitlichen Ganzen.

#### Schreibweise

- $m \in M$  (m ist Element von M)
- $m \notin M$  (m ist nicht Element von  $M, \neg m \in M$ )

Mengendarstellung verschiedene Möglichkeiten:

• allgemein mitels Eigenschaft E(m) (Aussageform)  $A = \{m | E(m)\}$  bzw.

$$A = \{m \in M | E(m)\} = \{m | m \in M \land E(m)\}\$$

• explizit für Menge mit wenigen endlich vielen Elementen:

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

**Problem** Man darf nicht alle möglichen Zusammenfassungen bilden. Z.B.: die Menge aller Mengen die sich nicht selbst enthalten:

$$R = \{M | M \notin M\}$$

$$R \in R \Leftrightarrow R \not\in R \equiv \bot$$

#### Lösung Axiomatischer Aufbau der Mengenlehre

**Extensionalitätsaxiom** Zwei Mengen A und B sind genau dann gleich, wenn sie die selben Elemente haben:

$$A = B \Leftrightarrow (\forall x)(x \in A \Leftrightarrow x \in B)$$

Leere Menge  $\emptyset = \{x | x \neq x\} = \{\}$ 

Einermenge  $A = \{a\}, A = \{x | x = a\}, A \neq a$ 

**Zweiermenge**  $A = \{a, b\}, A = \{x | (x = a \lor x = b) \land a \neq b\}$ 

andere Mengen

- $\mathbb{N} = \{0; 1; 2; 3; \dots\}$  natürliche Zahlen
- $\mathbb{Z} = \{...; (-1); 0; 1; ...\}$  ganze Zahlen
- Q rationale Zahlen
- $\mathbb{R}$  reelle Zahlen
- $\mathbb{C}$  komplexe Zahlen

Betrag Anzahl der Elemente in der Menge (bei endlichen Mengen)

**Teilmenge**  $A \subseteq B \Leftrightarrow (\forall x)(x \in A \Rightarrow x \in B)$ 

$$A \subseteq B \land B \subseteq C \Rightarrow A \subseteq C$$

$$A \subseteq B \land B \subseteq A \Rightarrow A = B$$

**Echte Teilmenge**  $A \subset B$  oder  $A \subsetneq B \Leftrightarrow (\forall x)(x \in A \Rightarrow x \in B) \land A \neq B$ 

**disjunkt** Die Mengen A und B heißen disjunkt (elementfremd) wenn:  $A \cap B = \emptyset$ 

Kardinalität Mächtigkeit

**gleichmächtig** Zwei Mengen A; B heißen gleich mächtig, wenn es eine bijektive Funktion  $f: A \longrightarrow B$  gibt.

$$A \sim B \Leftrightarrow (\exists f : A \longrightarrow B)$$

$$A \sim B \wedge B \sim C \Rightarrow A \sim C$$

endlich Menge A heißt endlich, wenn  $|A| \in \mathbb{N}$ 

abzählbar unendlich Eine Menge A heißt abzählbar unendlich, wenn

$$\mathbb{N} \sim A \wedge \exists f : \mathbb{N} \longrightarrow A \text{ (bijektiv)}$$

nicht abzählbar unendlich Meine Menge heißt nicht abzählbar unendlich, wenn sie weder endlich noch abzählbar unendlich ist.

Potenzmengen  $M \not\sim \mathcal{P}(M)$ 

Beweis: Angenommen es gäbe eine bijektive Funktion  $f: A \longrightarrow \mathcal{P}(M)$  und

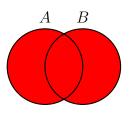
$$A = \{x \in M | x \not\in f(x)\} \subset M$$

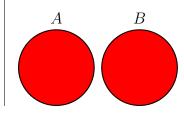
Wir nehmen an dass  $(\exists x \in M) \ f(x) = A$ 

- wenn  $x \in f(x)$  dann  $x \notin A$  wegen  $x \notin f(x)$ . Widerspruch da:  $x \notin A = x \notin f(x)$
- wenn  $x \notin f(x)$  dann  $x \in A$  wegen  $x \in M$ . Widerspruch da:  $x \notin A = x \notin f(x)$

# 2.2 Operationen auf Mengen

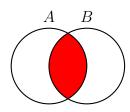
Vereinigung  $A \cup B = \{x | x \in A \lor x \in B\}$ 

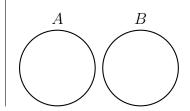




$$|A \cup B| = |A| + |B \setminus A|$$
$$= |B| + |A \setminus B|$$

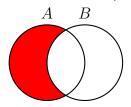
**Durchschnitt**  $A \cap B := \{x | x \in A \land x \in B\}$ 

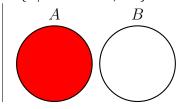




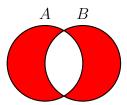
$$\begin{array}{rcl} |A\cap B| &=& |A|-|A\setminus B| \\ &=& |B|-|B\setminus A| \end{array}$$

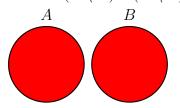
Mengendifferenz  $A \setminus B = \{x | x \in A \land x \notin B\}$ 





symmetrische Differenz  $A\Delta B = (A \setminus B) \cup (B \setminus A)$ 





$$|A\Delta B| = |A \setminus B| + |B \setminus A|$$

Potenzmengen  $\mathcal{P}(A) := \{B | B \subseteq A\}; |\mathcal{P}(A)| = 2^{|A|}$ 

 $\mathbf{ungeordnets} \ \mathbf{Paar} \ \left\{ a,b \right\} = \left\{ c,d \right\} \Rightarrow \left( a = c \land b = d \right) \lor \left( a = d \land b = c \right)$ 

**geordnetes Paar**  $\{a,b\} = \{c,d\} \Rightarrow a = c \land b = d \text{ (Das geht!)}$ 

**Mengenprodukt**  $A \times B = \{(a,b)| a \in A \land b \in B\}$  (nicht Kommutativ, (strenggenommen) nicht assoziativ)

$$(A \times B) \times C \neq A \times (B \times C)$$
$$((a,b),c) \neq (a,(b,c))$$

Gegeben sein

$$A = \{1, 2\}$$

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

dann ist:

$$A\times B=\{(1,a),(2,a)(1,b)(2,b),(1,c)(2,c)\}$$

$$|A \times B| = |A| \cdot |B|$$

# 3 Funktionen

Funktionen sind im wesentlich Zuordnungen.

# 3.1 Begriffe

**Definition** Zur Definition einer Funktion f braucht man drei Dinge

- Menge A, der Definitionsbereich von f,  $A = D_f$
- Menge B, der Wertevorrat von f,  $B = W_f$
- Eine Zuordnung, die jedem  $a \in A$  genau ein Element  $b \in B$  zuordnet Schreibweise: b = f(a) bzw.  $a \longmapsto f(a)$  Mathematisch wird diese Zuordnung gegeben durch eine Menge von geordneten Paaren

$$Graph(f) = \{(a, f(a)) | a \in A\} \subseteq A \times B$$

mit den Eigenschaften:

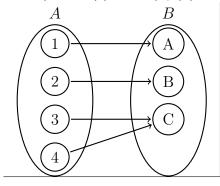
- $(\forall a \in A)(\exists b \in B) (a; b) \in Graph(f) (Vollständigkeit)$
- $(\forall a \in A)(\forall b_1, b_2 \in B) (a; b_1); (a; b_2) \in Graph(f) \Rightarrow b_1 = b_2 (Eindeutigkeit)$

#### Schreibweise

$$f: A \longrightarrow B$$
 ,  $a \longmapsto f(a) = \cdots$   
 $D_f \quad W_v$  Graph

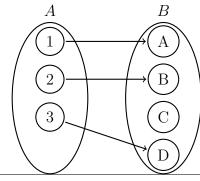
**Bild** Die Menge aller Funktionswerte von f.  $\{f(a)|a\in A\}=\{b\in B|(\exists a\in A)b=f(a)\}\subseteq B$  surjektiv  $(\forall b\in B)(\exists a\in A)\ f(a)=b$ 

6



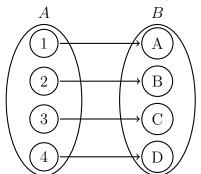
Für jedes Element in B existiert (mindestens) ein Urbild in A. Für jede rein surjektive Abbildung gilt:

**injektiv**  $(\forall a_1, a_2 \in A)(a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_2))$ 



Für jede zwei Elemente in A gilt, dass wenn sie verschieden von einander sind, dann auch ihre Funktionswerte von f verschieden sind. Also hat jedes Element in B höchstens ein Urbild. Für jede rein injektive Abbildung gilt:

**bijektiv** surjektiv  $\land$  injektiv:  $(\forall b \in B)(\exists! a \in A) \ f(a) = b$ 



Für jedes Element in B existiert genau ein Urbild in A. Für jede bijektive Abbildung gilt:

$$|A| = |B|$$

Identitätsfunktion  $id_A: A \longrightarrow A, a \longmapsto a \text{ z.B. } f(x) = x$ 

**Komposition**  $f: A \longrightarrow B; g: B \longrightarrow C$ 

$$(g \circ f) : A \longrightarrow C, a \longmapsto g(f(a))$$

$$f: A \longrightarrow B \Rightarrow f = f \circ id_A = id_A \circ f$$
  
 $f(a) = f(id_A(a)) = id_A(f(a))$ 

### 3.2 Umkehrfunktion

Umkehrbarkeit (im engeren sinne)  $f: A \longrightarrow B$ 

$$\leftrightarrow (\exists g : B \longrightarrow A)g \circ f = id_A \land f \cdot g = id_B$$
$$(\forall a \in A) \ g(f(a)) = a$$
$$(\forall b \in B) \ f(g(b)) = b$$

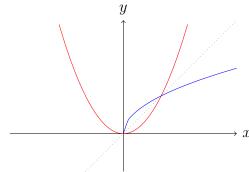
Die Funktion  $g: B \longrightarrow A$  heißt dann Umkehrfunktion von f, geschrieben  $g = f^{-1}$ .

$$f^{-1} \neq (f)^{-1}$$

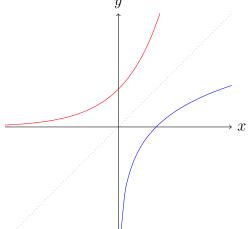
Satz: Eine Funktion  $f:A\longrightarrow B$  ist genau dann umkehrbar (i.e.s), wenn sie bijektiv ist.

**Umkehrbarkeit in der Analysis** Eine Funktion  $f:A\longrightarrow B$  heißt Umkehrbar, wenn die zugehörige Funktion  $f:A\longrightarrow \operatorname{Bild}(f)$  umkehrbar ist. Satz: Eine Funktion  $f:A\longrightarrow B$  ist genau dann umkehrbar (i.w.s), wenn sie injektiv ist.

Quadratische  $f: \mathbb{R} \longrightarrow \mathbb{R}, x \longmapsto x^2$ 



$$f^*: \mathbb{R}_0^+ \longrightarrow \mathbb{R}_0^+ \text{ (bijektiv)}$$
  
 $f^{*-1}: \mathbb{R}_0^+ \longrightarrow \mathbb{R}_0^+, x \longmapsto \sqrt{x}$ 



#### Zahlen 4

#### Sprachunterschiede 4.1

	deutsch	US-Englisch
$10^{6}$	Million	million
$10^{9}$	Milliarde	billion
$10^{12}$	Billion	trillion
$10^{15}$	Billiarde	quadrillion
$10^{18}$	Trillion	quintillion

#### natürliche Zahlen 4.2

$$\mathbb{N} = \{0, 1, 2, 3, \dots\}$$

unendlichkeits Axiom Es gibt unendliche Mengen

Peano-Axiome 5 Stück:

- $0 \in \mathbb{N}$ , null ist eine natürliche Zahl
- es gibt eine Nachfolgerfunktion  $s: \mathbb{N} \longrightarrow \mathbb{N}$
- s ist injektiv
- $0 \notin Bild(s)$ , Null ist nicht Nachfolger einer natürlichen Zahl
- Für jede Menge  $M \subseteq \mathbb{N}$  gilt:

$$(0 \in \mathbb{N} \land (\forall n \in \mathbb{N})(n \in M \Rightarrow s(n) \in M)) \Rightarrow M = \mathbb{N}$$

Modifikation: steht  $M \subseteq \mathbb{N}$  kann man das auch als Eigenschaft  $E_M(n)$  ausdrücken.

$$E_M(n) \Leftrightarrow n \in M$$

Vollständige Induktion am Beispiel für einen Beweis der Gaußschen Summenformel

Induktionsvoraussetzung Die Annahme:  $A(n) \Leftrightarrow 1 + 2 + \cdots + n = \frac{n(n+1)}{2}$ 

**Induktionsanfang** Der Beweis, dass der Anfang gültig ist: A(1) = 1

**Induktionsbehauptung** Das Einsetzen von (n + 1) für n:

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

Induktionsschritt Zeigen, dass aus der Induktionsvoraussetzung

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

die Induktionsbehauptung

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

folgt. In diesem speziellen Fall:

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

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

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

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

**Addition**  $m \in \mathbb{N}$ ; m fest

$$m + 0 := m$$
$$m + s(n) := s(m + n)$$

(rekursive (induktive) Definition für m+n)

$$m \cdot 0 := 0$$

$$m \cdot s(n) \coloneqq m + s(m+n)$$

#### 4.3 Ganze Zahlen

Motivation  $\mathbb{Z} := \{0, 1, -1, 2, -2 \dots\}$  (abzählbar) x + 1 = 0 ist nicht lösbar in  $\mathbb{N}$ 

x+a=0 man nimmt zu jeder Zahl  $a\in\mathbb{N}$  eine Gegenzahl -aLösung für x+a=0 (Ausnahme: a=0, denn -0=0)

Operationen +; -;  $\cdot$ 

spezielle Elemente 0, 1

lineare Ordnung  $\langle ; \leq ; \rangle ; \geq$ 

Gesetze  $(\forall a \in \mathbb{Z})$  gilt:

, ,	Addition	Multiplikation
	a + 0 = a	$a \cdot 1 = a$
Kommutativ	a+b=b+a	$a \cdot b = b \cdot a$
Assoziativ	(a+b) + c = a + (b+c)	$(a \cdot b) \cdot c = a \cdot (b \cdot c)$
	a + (-a) = 0	

Ring-Identitäten:  $a \cdot (b+c) = a \cdot b + a \cdot c$ 

Betrag 
$$|a| = \begin{cases} a & a \ge 0 \\ -a & a < 0 \end{cases}$$

**Division** Es sein  $a; m \in \mathbb{Z} | m \ge 1$  dann gibt es  $q \in \mathbb{Z}$  mit  $a = q \cdot m + r$  und  $0 \le r < m$ . q; r sind eindeutig bestimmt

### 4.4 Primzahlen

**Teiler**  $a; b \in \mathbb{Z}$ 

a ist ein Teiler von b, geschrieben  $a \mid c$ , falls  $(\exists c \in \mathbb{Z})$   $a \cdot c = b$ 

Jede ganze Zahl b ist teilbar durch: 1, -1, b , -b. Diese heißen die trivialen Teiler von b. Eigenschaften:

$$\begin{array}{l} a\mid 0;\ a\mid 0\\ a\mid b\wedge b\mid c\Rightarrow a\mid b\\ a\mid b\Rightarrow a\mid (-b), (-a)\mid b, (-a)\mid (-b)\\ a;b\geq 1\wedge a\mid b\Rightarrow a\leq b \end{array}$$

## Primzahl Eigenschaften:

- Eine ganze Zahl  $p \in \mathbb{Z}$  heißt Primzahl, wenn  $p \geq 2$  und p nur triviale Teiler hat.
- Jede ganze Zahl  $b \ge 2$  hat mindesten einen Primitiver.
- Es gibt unendlich viele Primzahlen. Beweis durch Widerspruch

$$|\mathbb{P}| \in \mathbb{N}$$

n sei die Anzahl aller Primzahl, und alle Primzahlen seien in der Menge  $\mathbb{P}=\{p_1;p_2;p_3;\ldots;p_n\}$ . Man bilde  $b=\prod_{p\in\mathbb{P}}+1$ . Dann ist  $b\geq 2$  und laut Hilfssatz hat b einen Primteiler, dieser sei q. Damit hat man eine Primzahl  $q\not\in\mathbb{P}$  gefunden. Daraus folgt, dass die Konstruktion  $\mathbb{P}=\{p_1;\ldots;p_n\}|n\in\mathbb{N}$  nicht alle Primzahlen enthalten kann.

• Der kleinste Teiler einer Zahl  $b \in \mathbb{N} | b \ge 2$  ist eine Primzahl.

Fundamentalsatz der Arithmetik Jede Zahl  $b \ge 2$  lässt sich als Produktion von Primzahlen darstellen (Primfaktorisierung). Vorkommende Primzahlen und ihre Anzahl sind bis auf Reihenfolge eindeutig bestimmt.

#### 4.5 Teilbarkeit

 $a \in \mathbb{Z}, \ a \ge 2, \ a = (z_{n-1}z_{n-2}\dots z_1z_0)$ 

- $2 \Leftrightarrow z_0 \text{ gerade}$
- $3 \Leftrightarrow \text{Quersumme durch 3 teilbar}$
- $4 \Leftrightarrow (z_1 z_0)_{10} \text{ durch } 4 \text{ teilbar}$
- $5 \Leftrightarrow z_0 \in \{0; 1\}$
- $6 \Leftrightarrow \operatorname{durch} 2 \text{ und } 3 \text{ teilbar}$
- $7 \Leftrightarrow ...$
- $8 \Leftrightarrow (z_2 z_1 z_0)_{(10)}$  durch 8 teilbar
- $9 \Leftrightarrow \text{quersumme durch } 9 \text{ teilbar}$
- 10  $\Leftrightarrow$  durch 2 und 5 teilbar bzw.  $z_0 = 0$

# 4.6 Additionssysteme

"Strichliste (mit Abkürzungen)"

Z.B.: 5 = ||||| = |||| oder römische Ziffern:

Großbuchstaben	I	V	X	L	С	D	M
Wert	1	5	10	50	100	500	1000

# 4.7 Positionssysteme

- Basis  $B, B \in \mathbb{N}, B >= 2$
- Ziffern für 0 bis B-1. Jede Ziffer ein Zeichen.
- Zahl = ...  $z_2B^2 + z_1B^1 + z_0B^0 + z_{-1}B^{-1}$  ...

## 4.7.1 Umrechnung

**Polynom**  $(z_{n-1}B^{n-1}z_{n-2}B^{n-2}...z_1B^1z_0B^0)_{(B)}$ 

zu kleinere Basis Fortgesetzte ganzzahlige Division mit Rest $217_{(10)}$ zur Basis 3

217 1

72 0

 $\begin{array}{ccc} 24 & 0 \\ 8 & 2 \end{array} 217_{(10)} = 22001_{(3)}$ 

2 2

0 0

zu größerer Basis mit Horner-Schema zum Dezimalsystem:

Ziffern	2	2	0	0	1	
B=3	0	6	24	72	216	Addition $\downarrow$ dann Multiplikation $\nearrow$ mit $B$
	2	8	24	72	217	

Wenn die Zielbasis eine Potenz der Ursprungsbasis ist, können  $\log_{B_U}(B_Z)$  Stellen direkt zusammengefasst werden:

$$(1000\ 0111\ 0001\ 1111)_{(2)}=(?)_{(16)}$$

Hier können jeweils  $\log_2(16) = 4$  Stellen zusammengefasst werden:

B=2	1000	0111	0001	1111
B = 10	8	7	1	15
B = 16	8	7	1	F