

## Inhaltsverzeichnis

<b>1 Vorlesung 1 (06.10.2020)</b>	<b>5</b>
1.1 Definition: Menge, Mengenelemente, leere Menge . . . . .	5
1.2 Venn-Diagramme . . . . .	5
1.3 Definition: Aussage . . . . .	5
1.4 Definition: Aussageverknüpfung . . . . .	5
1.5 Beispiele: Verneinung, Konjunktion, Disjunktion, Implikation, Äquivalenz . . . . .	5
<b>2 Vorlesung 2 (07.10.2020)</b>	<b>10</b>
2.1 Aussagenlogik: Tautologie, XOR, Allquantor, Existenzquantor . . . . .	10
2.2 Rechenregeln für Aussageverknüpfung . . . . .	10
2.3 Axiomatische Mengenlehre (Zermelo-Fraenkel) . . . . .	10
2.4 Definition: Potenzmenge . . . . .	10
2.5 Definition: Rechnen mit Mengen - Vereinigung, Durchschnitt, Differenz, Komplement . . . . .	10
<b>3 Vorlesung 3 (12.10.2020)</b>	<b>17</b>
3.1 Zahlenmengen . . . . .	17
3.2 Definition: Aussageform . . . . .	17
3.3 Definition: Kartesisches Produkt von Mengen, Tupel . . . . .	17
3.4 Zahlenstrahl, Anordnung von Zahlen . . . . .	17
<b>4 Vorlesung 4 (13.10.2020)</b>	<b>24</b>
4.1 Beispiele Relationen + Kartesisches Produkt . . . . .	24
4.2 Definition: reflexiv, transitiv, symmetrisch, antisymmetrisch: Äquivalenzrelation, Ordnungsrelation . . . . .	24
4.3 Definition: Äquivalenzklasse . . . . .	24
<b>5 Vorlesung 5 (14.10.2020)</b>	<b>31</b>
5.1 Beispiele Äquivalenzklasse . . . . .	31
5.2 Definition: vollständige Mengenpartition . . . . .	31
5.3 Satz: Äquivalenzklassen bilden vollständige Mengenpartition . . . . .	31
5.4 Definition: Verknüpfung . . . . .	31
5.5 Definition: Abbildung, Funktion, Bild, Graph, Urbild . . . . .	31
5.6 grafische Veranschaulichung der reellen Zahlen . . . . .	31
<b>6 Vorlesung 6 (19.10.2020)</b>	<b>38</b>
6.1 Beispiele Abbildung, Funktion . . . . .	38
6.2 Zahlensysteme . . . . .	38
6.3 Peano-Axiome (natürliche Zahlen definieren) . . . . .	38

6.4 Rechenregeln in den natürlichen Zahlen . . . . .	38
6.5 Definition: Endliche Summe . . . . .	38
6.6 5. Peano-Axiom / Induktionsaxiom / vollständige Induktion . . . . .	38
<b>7 Vorlesung 7 (20.10.2020)</b>	<b>45</b>
7.1 Beispiele Vollständige Induktion . . . . .	45
7.2 Definition durch Rekursion + Beispiele . . . . .	45
7.3 Binomialkoeffizient . . . . .	45
<b>8 Vorlesung 8 (21.10.2020)</b>	<b>52</b>
8.1 Binomialkoeffizienten und Fakultät . . . . .	52
8.2 Eigenschaften Binomialkoeffizient . . . . .	52
8.3 Pascalsches Dreieck . . . . .	52
8.4 1. Binomische Formel (+ 1. allgemeine Binomische Formel) . . . . .	52
8.5 2. Binomische Formel (+ 2. allgemeine Binomische Formel) . . . . .	52
8.6 Wiederholung: Ordnungsrelation, Vollständige Induktion . . . . .	52
<b>9 Vorlesung 9 (26.10.2020)</b>	<b>60</b>
9.1 Rechenregeln für Potenzen . . . . .	60
9.2 3. Binomische Formel (+ 3. allgemeine Binomische Formel) . . . . .	60
9.3 Elementares Multiplikationsprinzip . . . . .	60
9.4 Elementare Kombinatorik (Anordnung, Auswahl) . . . . .	60
<b>10 Vorlesung 10 (27.10.2020)</b>	<b>67</b>
10.1 Zusammenfassung Elementare Kombinatorik . . . . .	67
10.2 Dezimaldarstellung rationaler Zahlen . . . . .	67
10.3 Rechenregeln in den reellen Zahlen . . . . .	67
10.4 Bemerkung: Was ist ein Körper, Anordnungsaxiom . . . . .	67
<b>11 Vorlesung 11 (28.10.2020)</b>	<b>74</b>
11.1 Rechenregeln der Anordnung . . . . .	74
11.2 Intervalle als Mengen . . . . .	74
11.3 unendlich-Symbol . . . . .	74
11.4 Definition: Term . . . . .	74
11.5 Definition: Betrag einer reellen Zahl . . . . .	74
11.6 erste Rechenregeln für den Betrag . . . . .	74
11.7 Betrag, Ungleichung und Intervalle . . . . .	74
<b>12 Vorlesung 12 (02.11.2020)</b>	<b>81</b>
12.1 Anordnung, Ungleichung und Intervalle . . . . .	81

12.2 Potenzen und Wurzeln in den reellen Zahlen . . . . .	81
12.3 Rechenregeln für Wurzeln . . . . .	81
12.4 Quadratische Gleichungen und Ungleichungen in den reellen Zahlen . . . . .	81
12.5 pq-Formel . . . . .	81
<b>13 Vorlesung 13 (03.11.2020)</b>	<b>88</b>
13.1 Linearfaktoren des quadratischen Polynoms . . . . .	88
13.2 Mitternachtsformel . . . . .	88
13.3 Quadratische Ungleichungen . . . . .	88
13.4 Definition: Logarithmus . . . . .	88
13.5 Rechenregeln für Logarithmen . . . . .	88
13.6 Zahldarstellungen (umrechnung) . . . . .	88
<b>14 Vorlesung 14 (04.11.2020)</b>	<b>95</b>
14.1 Beispiel: Zahldarstellungen (umrechnung) . . . . .	95
14.2 Brüche in anderen Zahldarstellungen . . . . .	95
14.3 Zweiter Blick auf Ungleichungen und Betrag . . . . .	95
14.4 Rechenregeln für den Betrag . . . . .	95
14.5 Beweisidee Dreiecksungleichung . . . . .	95
14.6 Definition: Verknüfungen auf Mengen . . . . .	95
14.7 Definition: Gruppe, Halbgruppe, abelsche Gruppe . . . . .	95
14.8 Definition: Ring, Ring mit Eins, Kommutativer Ring mit Eins . . . . .	95
14.9 Definition: Körper . . . . .	95
<b>15 Vorlesung 15 (16.11.2020)</b>	<b>103</b>
15.1 5 Körperaxiome + Beispiele . . . . .	103
15.2 Definition: Ganzzahlige Teiler . . . . .	103
15.3 Definition: Primzahl . . . . .	103
15.4 Definition: Gemeinsame Teiler / Größter gemeinsamer Teiler . . . . .	103
15.5 Division mit Rest . . . . .	103
<b>16 Vorlesung 16 (17.11.2020)</b>	<b>109</b>
16.1 Wiederholung Teilermengen, Primzahl, gemeinsame Teiler . . . . .	109
16.2 Definition: ggT, Division mit Rest, Teilerfremd . . . . .	109
16.3 Beweis: Division mit Rest . . . . .	109
16.4 Euklidischer Algorithmus . . . . .	109
16.5 Lemma von Bézout . . . . .	109
<b>17 Vorlesung 17 (18.11.2020)</b>	<b>115</b>

17.1 Teilen mit Rest . . . . .	115
17.2 Teilen und Äquivalenzrelationen, Restmengen . . . . .	115
17.3 Rechenoperationen in $Z_m$ , Körper?, kommutativer Ring mit Eins? . . . . .	115
<b>18 Vorlesung 18 (23.11.2020)</b>	<b>122</b>
18.1 Restklassen mit Primzahlen sind Körper + Beispiel . . . . .	122
18.2 simultane Kongruenzen . . . . .	122
18.3 chinesischer Restsatz . . . . .	122

# 1 Vorlesung 1 (06.10.2020)

- 1.1 Definition: Menge, Mengenelemente, leere Menge
- 1.2 Venn-Diagramme
- 1.3 Definition: Aussage
- 1.4 Definition: Aussageverknüpfung
- 1.5 Beispiele: Verneinung, Konjunktion, Disjunktion, Implikation, Äquivalenz

- Hinweis auf Portfolio-Prüfung (Kleingruppe / edX-Test / Klausur)
 

5%	15%	80%
----	-----	-----
- Hinweis Zugang edX / OSCA-Plattform
- OSCA-Plattform: Medium für alle Infos zur Vorlesung, Übungsaufgaben, Vorlesungsmitschrift, Skript usw.
- Anmeldung zur Kleingruppenübung (eigenständig anmelden im OSCA-Portal)
 

Gruppe 1	Kampmann montags 8:00	}	14-tägiger Wechsel
Gruppe 2	Meyer donnerstags 12:15		
Gruppe 3			
- Hinweis auf das Skript → Inhaltverzeichnis (Vorlesungsinhalte)  
→ Literaturhinweise

## 1. Mengen und Aussagen

Definitionen regeln, worüber man in der Mathematik spricht!

### Definition:

Eine Menge ist die Zusammenfassung bestimmter, wohlunterschiedener Objekte zu einem Ganzen. Mengen werden mit Großbuchstaben bezeichnet, die Objekte, die zu einer Menge gehören, heißen Elemente der Menge.

### Bemerkung:

- 1) Mengen werden durch Aufzählung ihrer Elemente zwischen Mengenklammern angegeben, z.B.

$$A = \{ 2, 7, a, \text{Katze} \}$$

Name / Bezeichnung  
der Menge ↑      ↑      ↑      Mengenklammern

↓ „ist Element von...“

- 2) Wenn ein Element a zur Menge A gehört, schreibt  $a \in A$

$b \notin A$

„ist nicht Element von...“

Beispiel:  $A = \{2, 7, a, \text{Katze}\}$

$7 \in A, b \notin A, \text{Katze} \in A, z \notin A$

Definition:

① Es gibt genau eine Menge, die kein Element hat.

Diese Menge heißt leere Menge; das Symbol dafür ist  $\emptyset$ .

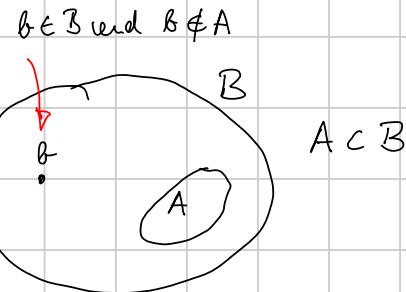
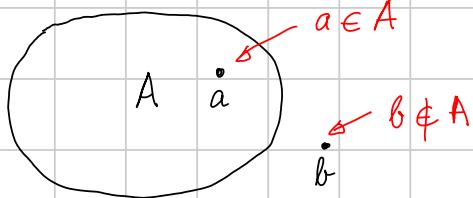
②  $A$  ist Teilmenge von  $B$  (man schreibt  $A \subseteq B$ ), falls jedes Element von  $A$  auch Element von  $B$  ist.

$A$  ist echte Teilmenge von  $B$  (man schreibt  $A \subset B$ ), falls gilt:

$A \subseteq B$  und es gibt mindestens ein  $b \in B$  mit  $b \notin A$ .

③ Es ist  $A = B$  ( Mengengleichheit), falls gilt:  $A \subseteq B$  und  $B \subseteq A$ , d.h. jedes Element von  $A$  gehört auch zu  $B$  und jedes Element von  $B$  gehört auch zu  $A$ .

Venn-Diagramme für Mengen:



Definition:

1) Eine  Aussage ist ein sprachlicher Satz, dem eindeutig und unmissverständlich genau einer der beiden Wahrheitswerte „wahr“ (w, 1) bzw. „falsch“ (f, 0) zugeordnet werden kann.

Aussagen werden (auch) mit Großbuchstaben bezeichnet.

2) Eine Aussage ist eindeutig bestimmt, wenn ihre Wahrheitswerte

festgelegt sind; die Wahrheitswerte „bestimmen“ die Ausage.

Beispiele: Frage: Handelt es sich um Aussagen, wenn ja: Welchen Wahrheitswert haben Sie?

- Merkur ist ein Planet unseres Sonnensystems **Aussage, w**
- Für das Produkt  $2 \cdot 3$  gilt:  $2 \cdot 3 = 7$  **Aussage, f**
- Der beste Fußballverein der Welt ist BVB OSG **Keine Aussage, persönliche Meinung**
- Sonntags finden an der Hochschule keine Vorlesungen in Prof. Kampmann statt **Aussage, w**

Definition:

- Eine Aussageverknüpfung erzeugt aus einer, zwei oder mehreren Aussagen (Input-Aussagen) eine neue Aussage (Output-Aussage).
- Die Aussageverknüpfung ist definiert, wenn die Wahrheitswerte der neuen Aussage (Output-Aussage) in Abhängigkeit von den Wahrheitswerten der beteiligten Aussagen (Input-Aussagen) feststehen; dies geschieht mittels Wahrheitstafeln / Wahrheitstabellen.
- Folgende Aussageverknüpfungen bilden unsere Standardverknüpfungen

a) Verneinung  $\neg$  einfellige Verknüpfung: 1 Input - Aussage

A	$\bar{A} (\neg A)$
w	f
f	w

Input      ↗      Output

b) Konjunktion / und-Verknüpfung  $\wedge$  zweifellige Verknüpfung: 2 Input - Aussagen

A	B	$A \wedge B$
w	w	w
w	f	f
f	w	f
f	f	f

c) Disjunktion / oder - Verknüpfung ← zweistellige Verknüpfung

A	B	$A \vee B$
w	w	w
w	f	w
f	w	w
f	f	f

←  $A \vee B$ : A oder B; v steht für oder

d) Implikation / Folgerung / wenn-dann-Verknüpfung ← zweistellige Verknüpfung

A	B	$A \Rightarrow B$
w	w	w
w	f	f
f	w	w
f	f	w

←  $A \Rightarrow B$ : Wenn A dann B; ⇒ steht für wenn...dann...

↑ Folgerung/Schluss  
↓ Prämisse

→ Aus einer falschen Prämisse darf man alles folgern, die Folgerung ist wahr:

beide Implikationen sind wahr { Wenn der Mond fünfeckig ist dann ist 2 eine gerade Zahl  
Wenn der Mond fünfeckig ist dann ist 2 eine ungerade Zahl

e) Äquivalent / genau dann-wenn-Verknüpfung → zweistellige Verknüpfung

A	B	$A \Leftrightarrow B$
w	w	w
w	f	f
f	w	f
f	f	w

←  $A \Leftrightarrow B$ : A ist äquivalent zu B

Äquivalent ist { A und B haben denselben

„wahr“ Wahrheitswert

Aufgabe:  $A \Leftrightarrow B$  Kann man über  $\wedge$  und  $\Rightarrow$  gewinnen! Wie?

## 2 Vorlesung 2 (07.10.2020)

- 2.1 Aussagenlogik: Tautologie, XOR, Allquantor, Existenzquantor
- 2.2 Rechenregeln für Aussageverknüpfung
- 2.3 Axiomatische Mengenlehre (Zermelo-Fraenkel)
- 2.4 Definition: Potenzmenge
- 2.5 Definition: Rechnen mit Mengen - Vereinigung, Durchschnitt, Differenz, Komplement

Aussagenlogik2-stellige Verknüpfungen:  $\wedge, \vee, \Rightarrow, \Leftrightarrow$ 1-stellige Verknüpfung:  $\neg, \top$ 

A	B	$\Leftrightarrow$	A	B
w	w	w		
w	f	f		
f	w	f		
f	f	w		

genau-dann-wenn  
logische Äquivalenz

A	B	$A \Rightarrow B$
w	w	w
w	f	f
f	w	w
f	f	w

wenn-dann  
logische  
Folgerung

Behauptung: Es gilt  $(A \Leftrightarrow B) \Leftrightarrow (A \Rightarrow B \wedge B \Rightarrow A)$

Beweis: Aufstellen einer Wahrheitstafel/Wahrheitstabelle

des gilt,

A	B	$A \Rightarrow B$	$B \Rightarrow A$	$(A \Rightarrow B) \wedge (B \Rightarrow A)$	$A \Leftrightarrow B$
w	w	w	w	w	w
w	f	f	w	f	f
f	w	w	f	f	f
f	f	w	w	w	w

wenn in den  
beiden Spalten  
dieselbe Verteilung  
von Wahrheitswerten  
steht

Bemerkungen:

1) Für die doppelte Verneinung gilt  $(\overline{\overline{A}}) = \neg(\neg A) \Leftrightarrow A$ .

A	$\overline{A}$	$(\overline{\overline{A}})$	$A \Leftrightarrow (\overline{\overline{A}})$
w	f	w	w
f	w	f	w

2) Aussagen, die immer den Wahrheitswert „w“ haben, heißen Tautologie

3) Eine Aussageverknüpfung mit  $n$  Input-Aussagen heißt  $n$ -stellige (Aussage)verknüpfung

Wieviele voneinander verschiedene 2-stellige Verknüpfungen

gibt es?

A	B	*
w	w	w/f
w	t	w/t
t	w	w/t
t	t	w/w

\* ist eindeutig bestimmt, wenn in jeder der 4 Zeilen ein Wahrheitswert steht  
2 Möglichkeiten pro Zeile, damit insgesamt  
 $2 \cdot 2 \cdot 2 \cdot 2 = 2^4 = 16$  Möglichkeiten

2 dieser Möglichkeiten sind

A	B	$\perp$	XOR	$\top$
w	w	w	f	f
w	f	w	w	f
f	w	w	w	f
f	f	w	f	f

$\top$  ist die immer wahre Aussage

$\perp$  ist die immer falsche Aussage  
 $\wedge$  ist der logische und  
 $\vee$  ist der logische oder  
 $\neg$  ist der logische nicht

$\perp$  ist die immer wahre Aussage

#### 4) Die Aussagen

a) „Für alle  $x \in M$  gilt ...“ wird abgekürzt durch:  $\forall x \in M: \dots$

$\forall$  heißt Allquantor.

b) „Für (mindestens) ein  $x \in M$  gilt ...“ wird abgekürzt durch:  $\exists x \in M: \dots$

$\exists$  heißt Existenzquantor.

c) „Für genau ein  $x \in M$  gilt ...“ wird abgekürzt durch:  $\exists! x \in M: \dots$

„Rechnen“ mit Aussagen

Eine Aussageverknüpfung erzeugt aus  $1, 2, \dots, n$  Input-Aussagen

eine neue Aussage; diese Aussage ist festgelegt (wohldefiniert), wenn

ihre Wahrheitswerte in Abhängigkeit von den Wahrheitswerten der

Input-Aussagen feststellt; dies geschieht z.B. über eine Wahrheitstabelle!

#### Rechengesetze für Aussageverknüpfungen

Die folgende tabellarische Übersicht zeigt die Rechengesetze der Aussagenlogik

Name	und ( $\wedge$ )	oder ( $\vee$ )
Kommutativgesetz	$A \wedge B \Leftrightarrow B \wedge A$	$A \vee B \Leftrightarrow B \vee A$
Assoziativgesetz	$A \wedge (B \wedge C) \Leftrightarrow (A \wedge B) \wedge C$	$A \vee (B \vee C) \Leftrightarrow (A \vee B) \vee C$
<b>b)</b> Existenz neutraler Elemente	$A \wedge 1 \Leftrightarrow A$	$A \vee 0 \Leftrightarrow A$
Existenz komplementärer Elemente	$A \wedge A \Leftrightarrow 0$	$A \vee A \Leftrightarrow 1$
<b>a)</b> Distributivgesetze	$A \wedge (B \vee C) \Leftrightarrow (A \wedge B) \vee (A \wedge C)$	$A \vee (B \wedge C) \Leftrightarrow (A \vee B) \wedge (A \vee C)$
<b>c)</b> DeMorgansche Regeln	$\overline{A \wedge B} \Leftrightarrow \overline{A} \vee \overline{B}$	$\overline{A \vee B} \Leftrightarrow \overline{A} \wedge \overline{B}$

Remerkung:

1) Es reichen die 2-stelligen Verknüpfungen  $\wedge$ ,  $\vee$  und die

1-stellige Verknüpfung  $\neg$  aus, um  $\Rightarrow$ ,  $\Leftarrow$  und weitere

der 16 2-stelligen Verknüpfungen darzustellen (disjunktive/Konjunktive

Normformen  $\rightarrow$  Digitaltechnik)  $\Rightarrow$  Rechengesetze für  $A, V, \neg$  regeln  
also alle Ausgangsknäpfungen!

2) Exemplarische Beweise der Rechengesetze mittels Wahrheitstafeln

a) 1. Distributivgesetz  $A \wedge (B \vee C) \Leftrightarrow (A \wedge B) \vee (A \wedge C)$

$A$	$B$	$C$	$B \vee C$	$A \wedge (B \vee C)$	$A \wedge B$	$A \wedge C$	$(A \wedge B) \vee (A \wedge C)$
8 Zeilen $\Leftrightarrow$ 8 möglichen Kombinationen an Wahrheits- werten bei 3 Inputs	w	w	w	w	w	w	w
	w	w	t	w	w	f	w
	w	f	w	w	t	w	w
	w	f	t	t	t	t	w
	f	w	w	w	f	f	f
	f	w	t	w	f	f	f
	t	f	w	w	t	t	t
	t	f	t	t	t	t	t

b) Existenz neutraler Elemente

$1 \leftarrow$  immer wahre Ausgabe;  $0 \leftarrow$  immer falsche Ausgabe

$A$	$1$	$0$	$A \wedge 1$	$A \vee 0$
w	w	f	w	w
w	w	f	w	w
f	w	f	f	f
f	w	f	f	f

$(A \wedge 1) \Leftrightarrow A$

$(A \vee 0) \Leftrightarrow A$

c) DeMorgan'sche Regeln  $\leftarrow$  wie verträgt sich Verneinung mit und bzw. odr

$$\overline{A \wedge B} \Leftrightarrow \overline{A} \vee \overline{B}; \quad \overline{A \vee B} \Leftrightarrow \overline{A} \wedge \overline{B}$$

$A$	$B$	$A \wedge B$	$A \vee B$	$\overline{A}$	$\overline{B}$	$\overline{A \wedge B}$	$\overline{A \vee B}$	$\overline{\overline{A \wedge B}}$	$\overline{\overline{A \vee B}}$
w	w	w	w	f	f	f	f	f	f
w	t	f	w	f	t	f	w	w	t
f	w	f	w	w	f	w	w	w	w
t	t	f	w	w	w	w	w	w	w

3) zwei weitere Beispiele

$$(A \Rightarrow B) \Leftrightarrow (\bar{A} \vee B) ; \quad (A \Rightarrow B) \Leftrightarrow (\bar{B} \Rightarrow \bar{A})$$

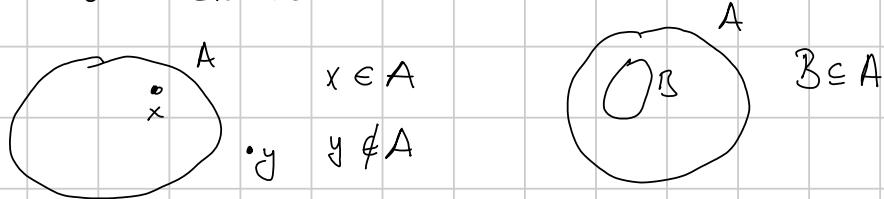
Kontraposition

A	$\bar{B}$	$\bar{A}$	$\bar{B}$	$A \Rightarrow B$	$\bar{A} \vee B$	$\bar{B} \Rightarrow \bar{A}$
w	w	f	f	w	w	w
w	+	f	w	f	f	+
f	w	w	f	w	w	w
f	f	w	w	w	w	w

Mengenlehre  $A, B$  Mengen:  $A \subseteq B, A \subset B, A = B, x \in A, x \notin A$   
 $\emptyset$  leere Menge (einzige Menge ohne Element)

Zusammenfassung bestimmter, wohlunterschiedener Objekte zu einem Ganzen

Venn-Diagramm:



Bemerkung: „Naive“ Mengendefinition (Cantor) kann zu Widersprüchen führen (Russeln), z.B.:

Auf einer kleinen Insel gilt für die männlichen Bewohner: Der Dorffriseur rasiert jeden Mann, der sich nicht selbst rasiert, und nur diese.

Insbesondere rasiert der Dorffriseur keinen Mann, der sich selbst rasiert; der Dorffriseur ist männlich.

$A = \{x \mid x \text{ ist männlicher Einwohner der Insel und wird vom Dorffriseur rasiert}\}$

f bezeichnet den Dorffriseur!

Gilt  $f \in A$  oder  $f \notin A$  ↯ unentscheidbarer Widerspruch

Lösung: Axiomatische Mengenlehre (Zermelo-Fraenkel)

Unsere pragmatische Lösung:

Alle betrachteten Mengen stammen aus einer (aus dem Zusammenhang erreichlichen) Allmengen  $\mathcal{U}$ . Jede in diesem Zusammenhang betrachtete Menge A

ist also Teilmenge von  $\Omega$ .

Definition:  $\Omega$  ist die betrachtete Allmenge

1) Gegeben ist eine Menge  $A$ , dann ist die Menge aller Teilmengen von  $A$  die Potenzmenge von  $A$ , man schreibt



$$\mathcal{P}(A) = \{ B \mid B \subseteq A \}$$

2)  $\emptyset \subseteq A \quad \forall A \subseteq \Omega ; \quad A \subseteq A \quad \forall A \subseteq \Omega$

3) Wenn  $A$  endlich viele Elemente hat, ist  $|A|$  die Anzahl der Elemente von  $A$

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

$$\mathcal{P}(A) = \{ \emptyset, A, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\} \}$$

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

$$\rightarrow |A|=3, \quad |\mathcal{P}(A)|=8=2^3$$

Später wird gezeigt:  $A \subseteq \Omega$  endliche Menge, dann gilt:  $n=|A| \Rightarrow |\mathcal{P}(A)|=2^n$

Verknüpfungen von Mengen (Rechnen mit Mengen)

Definition: Gegeben sind die Mengen  $A$  und  $B$  ( $A \subseteq \Omega, B \subseteq \Omega$ ).

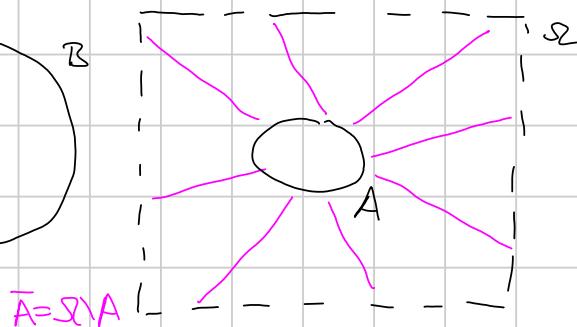
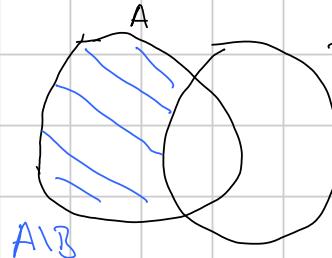
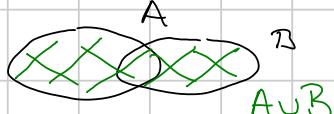
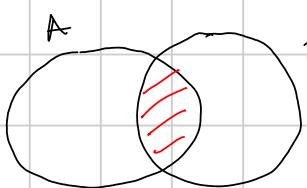
Dann ist definiert

1) die Vereinigung  $A \cup B$  durch:  $(x \in A \cup B) \Leftrightarrow (x \in A \vee x \in B)$

2) die Durchschnitt  $A \cap B$  durch:  $(x \in A \cap B) \Leftrightarrow (x \in A \wedge x \in B)$

3) die Differenz  $A \setminus B$  durch:  $(x \in A \setminus B) \Leftrightarrow (x \in A \wedge x \notin B)$

4) das Komplement  $\bar{A}$  durch:  $\bar{A} = \Omega \setminus A = \{x \in \Omega \mid x \notin A\}$



Bemerkung: Statt  $A \setminus B$  schreibt man auch  $A - B$ .

### **3 Vorlesung 3 (12.10.2020)**

**3.1 Zahlenmengen**

**3.2 Definition: Aussageform**

**3.3 Definition: Kartesisches Produkt von Mengen, Tupel**

**3.4 Zahlenstrahl, Anordnung von Zahlen**

## Verknüpfungen von Mengen (Rechnen mit Mengen)

Definition: Gegeben sind die Mengen A und B ( $A \subseteq \mathcal{S}, B \subseteq \mathcal{S}$ ).

Dann ist definiert

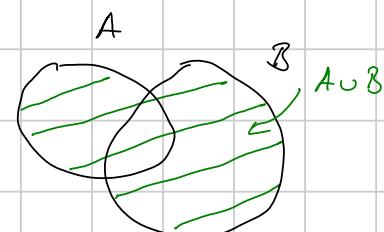
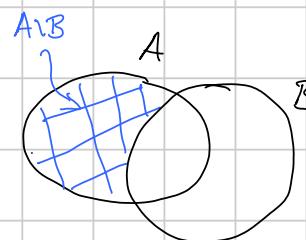
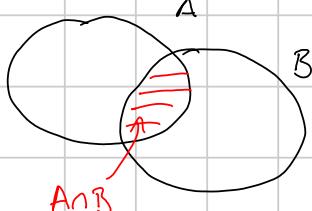
↑  
"Menge aus  
dem Kontext des behandelten  
Themas"

1) die  Vereinigung  $A \cup B$  durch:  $(x \in A \cup B) \Leftrightarrow (x \in A \vee x \in B)$

2) der  Durchschnitt  $A \cap B$  durch:  $(x \in A \cap B) \Leftrightarrow (x \in A \wedge x \in B)$

3) die  Differenz  $A \setminus B$  durch:  $(x \in A \setminus B) \Leftrightarrow (x \in A \wedge x \notin B)$

4) das  Komplement  $\bar{A}$  durch:  $\bar{A} = \mathcal{S} \setminus A = \{x \in \mathcal{S} \mid x \notin A\}$



## Beispiele und Bemerkungen

### 1) Zahlenmengen

$\mathbb{N} = \{1, 2, 3, 4, 5, \dots\} \leftarrow$  Menge der natürlichen Zahlen

$\mathbb{N}_0 = \mathbb{N} \cup \{0\} = \{0, 1, 2, 3, 4, 5, \dots\} \leftarrow$  Menge der natürlichen Zahlen mit Null

$\mathbb{Z} = \{\dots, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, \dots\} \leftarrow$  Menge der ganzen Zahlen

$\mathbb{Q} = \left\{ \frac{z}{n} \mid z \in \mathbb{Z} \wedge n \in \mathbb{N} \right\} \leftarrow$  Menge der rationalen Zahlen (Menge der Brüche)

$\frac{z}{n} \in \mathbb{Q} \Rightarrow z$  heißt Zähler,  $z \in \mathbb{Z}$

$n$  heißt Nenner,  $n \in \mathbb{N}$   $\leftarrow n \neq 0$  denn  $0 \notin \mathbb{N}$

"man darf nicht durch Null teilen"

$$-\frac{3}{4} = -\frac{3}{4} \in \mathbb{Q} \text{ mit } z = -3, n = 4$$

$$\frac{128}{31} \in \mathbb{Q} \text{ mit } z = 128, n = 31$$

$$\left. \begin{array}{l} 5 = \frac{5}{1} \text{ mit } z = 5, n = 1 \\ -8 = \frac{-8}{1} \text{ mit } z = -8, n = 1 \end{array} \right\}$$

Es gilt:  $\mathbb{N} \subset \mathbb{N}_0 \subset \mathbb{Z} \subset \mathbb{Q}$

$(\frac{1}{2}) = \frac{2}{4} = \frac{8}{16} \dots \leftarrow \text{die Darstellung } q = \frac{z}{n} \text{ für } q \in \mathbb{Q} \text{ ist nicht eindeutig}$

vollständig gekürzte Form: Zähler und Nenner haben keinen gemeinsamen Faktor mehr

$$\frac{15}{35} = \frac{3 \cdot 5}{7 \cdot 5} = \frac{3}{7} \leftarrow \text{vollständig gekürzte Form}$$

↑  
„Kürzen“ des gemeinsamen  
Faktors

$$\left. \begin{array}{l} A = \{-2, -1, 0, 3, 5, 7\} \\ B = \{-3, -1, 3, 6\} \\ C = \{\frac{1}{2}, \frac{3}{4}, -5, -2, 0\} \end{array} \right\} \text{ dann gilt}$$

$$A \cup B = \{-3, -2, -1, 0, 3, 5, 6, 7\}$$

$$A \cap B = \{-1, 3\}$$

$$\left. \begin{array}{l} A \setminus B = \{-2, 0, 5, 7\} \\ B \setminus A = \{-3, 6\} \end{array} \right\} \text{ in der Regel (d.h. außer in wenigen Ausnahmefällen)} \quad \text{gilt} \quad A \setminus B \neq B \setminus A$$

$$C \setminus B = C \text{ hier und } B \setminus C = B$$

$$A \cap C = \{0, 2\}, B \cap C = \emptyset$$

↓ A enthält nur ganze Zahlen, also aus dem Kontext:  $\mathbb{S} = \mathbb{Z}$

$$\bar{A} = \mathbb{Z} \setminus A = \{\dots, -4, -3, 1, 2, 4, 6, 8, 9, 10, \dots\}$$

### „Rechenregeln“ für Mengenoperationen

Mengenoperationen sind über aussagenlogische Verknüpfungen definiert, z.B.

$$x \in A \cup B \Leftrightarrow (x \in A) \vee (x \in B)$$

daher folgt: Die „Rechenregeln“ für Mengenoperationen folgen aus den „Rechenregeln“ der Aussagenlogik

Die folgende tabellarische Übersicht zeigt die **Rechengesetze der Mengenlehre**

Name	Durchschnitt ( $\cap$ )	Vereinigung ( $\cup$ )
Kommutativgesetz	$A \cap B \Leftrightarrow B \cap A$	$A \cup B \Leftrightarrow B \cup A$
Assoziativgesetz	$A \cap (B \cap C) \Leftrightarrow (A \cap B) \cap C$	$A \cup (B \cup C) \Leftrightarrow (A \cup B) \cup C$
Existenz neutraler Elemente	$A \cap \Omega \Leftrightarrow A$	$A \cup \emptyset \Leftrightarrow A$
Existenz komplementärer Elemente	$A \cap \bar{A} \Leftrightarrow \emptyset$	$A \cup \bar{A} \Leftrightarrow \Omega$
Distributivgesetze	$A \cap (B \cup C) \Leftrightarrow (A \cap B) \cup (A \cap C)$	$A \cup (B \cap C) \Leftrightarrow (A \cup B) \cap (A \cup C)$
DeMorgansche Regeln	$A \cap \bar{B} \Leftrightarrow A \cup \bar{B}$	$A \cup \bar{B} \Leftrightarrow A \cap \bar{B}$

Beweisidee: Vereinigung  $\cup$  Durchschnitt  $\cap$  Mengenoperationen Verknüpfungen der oder und Ausagenlogik

a)  $x \in A \cup (B \cap C) \Leftrightarrow (x \in A) \vee (x \in B \cap C)$

$$\Leftrightarrow (x \in A) \vee ((x \in B) \wedge (x \in C))$$

Distributivgesetz der Ausagenlogik  $\Leftrightarrow ((x \in A) \vee (x \in B)) \wedge ((x \in A) \vee (x \in C))$

$$\Leftrightarrow (x \in A \cup B) \wedge (x \in A \cup C)$$

$$\Leftrightarrow x \in (A \cup B) \cap (A \cup C)$$

Merke: Mengengleichheit  $A = \emptyset \Leftrightarrow A \subseteq B \wedge B \subseteq A$

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

b)  $x \in \overline{A \cap B} \Leftrightarrow x \notin (A \cap B) \leftarrow x \in (A \cap B) \Leftrightarrow (x \in A) \wedge (x \in B)$

$$\Leftrightarrow (x \in A) \wedge (x \in B)$$

DeMorgansche Regel

der Ausagenlogik

$$\Leftrightarrow (\overline{x \in A}) \vee (\overline{x \in B})$$

$$\Leftrightarrow (x \notin A) \vee (x \notin B)$$

$$\Leftrightarrow (x \in \bar{A}) \vee (x \in \bar{B})$$

$$\Leftrightarrow x \in (\bar{A} \cup \bar{B})$$

Angabe von Mengen durch Aufzählung ihrer Elemente ist bei großen endlichen Mengen insbesondere aber bei Mengen mit unendlich vielen Elementen unpraktisch bzw. unmöglich, daher braucht es eine

Definition:

Eine Ausageform ist ein sprachlicher Satz, der einen oder mehrere

Platzhalter (eine oder mehrere Variablen) enthält, wird zu Aussage wird, sobald man die Platzhalter (Variablen) durch konkrete Elemente der Definitionsmenge D (Grundmenge) der Aussageform ersetzt.

Beispiele:

1)  $A(n) \hat{=} „n \text{ ist ohne Rest durch } 3 \text{ teilbar}"$ ,  $D = \mathbb{N}$   
 ↑  
 Variable

$A(5) \hat{=} „5 \text{ ist ohne Rest durch } 3 \text{ teilbar}" \leftarrow \text{Aussage, Wahrheitswert: f}$

2)  $B(n_1, n_2) \hat{=} „\text{das Produkt } n_1 \cdot n_2 \text{ ist eine ungerade Zahl}"$ ,  
 ↑↑  
 2 Variable

$$D = \{(n_1, n_2) \mid n_1 \in \mathbb{N} \wedge n_2 \in \mathbb{N}\}$$

Was ist das? → Siehe unten: Kartesisches Produkt

$B(3, 6) \hat{=} „\text{das Produkt } 3 \cdot 6 \text{ ist eine ungerade Zahl}" \leftarrow \text{Aussage, Wahrheitswert: f}$

$B(5, 7) \hat{=} „\text{das Produkt } 5 \cdot 7 \text{ ist eine ungerade Zahl}" \leftarrow \text{Aussage, Wahrheitswert: w}$

3)  $G \subseteq \mathbb{Z}$  mit  $G = \{z \in \mathbb{Z} \mid \exists k \in \mathbb{Z}: z = 2 \cdot k\}$  Menge der geraden Zahlen  
 ↓ damit ist die Bedeutung von ... eindeutig geklärt  
 $= \{-6, -4, -2, 0, 2, 4, 6, 8, \dots\}$

3)  $S = \{\lambda \mid \lambda \text{ ist im WS 2021 an der HS Osnabrück als Studierender(r) eingeschrieben}\}, D = \text{Menge aller Menschen}$

Die Aussageform, die eine Menge beschreibt, nennt man auch charakterisierende Eigenschaft der Menge.

Mengen kann man also durch Anfählung aller Elemente oder durch ihre charakterisierende Eigenschaft beschreiben.

## Definition (Kartesisches Produkt von Mengen)

1) Gegeben sind zwei Mengen  $A, B$  (mit  $A \neq \emptyset$  und  $B \neq \emptyset$ ).

Dann ist das Kartesische Produkt  $A \times B$  definiert durch

$$A \times B = \{ (a, b) \mid a \in A \wedge b \in B \}$$

dabei heißt  $(a, b)$  geordnetes Paar ( $2\text{-Tupel}$ ) mit festgelegten Komponenten  
 $\begin{array}{c} \uparrow \\ 1.\text{ Komponente} \\ \downarrow \\ 2.\text{ Komponente} \end{array}$

Für alle  $2\text{-Tupel}$  / geordneten Paare  $(a, b)$  aus  $A \times B$  gilt:

1. Komponente  $a$  kommt aus der 1. Menge  $A$

2. Komponente  $b$  kommt aus der 2. Menge  $B$

2) Gegeben sind die Mengen  $A_1, A_2, \dots, A_n$  ( $n \in \mathbb{N}$ ); es gilt  $A_i \neq \emptyset$  für  $i \in \{1, 2, \dots, n\}$

Dann ist das ( $n$ -fache) Kartesische Produkt  $A_1 \times A_2 \times \dots \times A_n$  definiert durch

$$A_1 \times A_2 \times \dots \times A_n = \{ (a_1, a_2, \dots, a_n) \mid a_i \in A_i \text{ für } i \in \{1, 2, \dots, n\} \}$$

dabei heißt  $(a_1, a_2, \dots, a_n)$  ein  $n$ -Tupel

$a_i$  steht in der  $i$ -ten Komponente von  $(a_1, a_2, \dots, a_n)$  für  $i \in \{1, 2, \dots, n\}$ ;

$i$ -te Komponente  $a_i$  kommt aus der  $i$ -ten Menge  $A_i$  für  $i \in \{1, 2, \dots, n\}$ .

## Beispiele:

$$\begin{aligned} 1) \quad A &= \{1, 2, 3\} & \Rightarrow A \times B &= \{(1, a), (1, b), (2, a), (2, b), (3, a), (3, b)\} \\ &B = \{a, b\} & B \times A &= \{(a, 1), (a, 2), (a, 3), (b, 1), (b, 2), (b, 3)\} \\ (a, 1) &\neq (1, a) & \Rightarrow A \times B &\neq B \times A \end{aligned}$$

Das Kartesische Produkt von Mengen ist nicht kommutativ, d.h. die Reihenfolge der „Faktoren“ (also der beteiligten Mengen) ist relevant!

2) Für die Mengen aus 1) gilt:

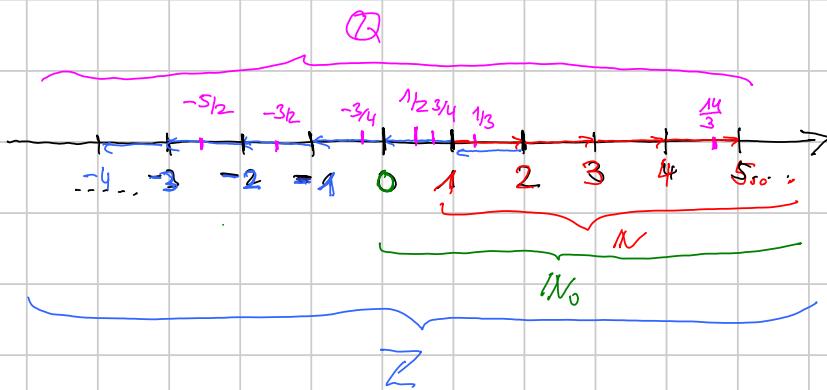
$$\left. \begin{array}{l} |A| = 3 \\ \uparrow \text{Anzahl der Elemente in } A \\ |B| = 2 \end{array} \right\} |A \times B| = |B \times A| = 3 \cdot 2 = 2 \cdot 3 = 6$$

allgemein  $|A \times B| = |A| \cdot |B|$  für endliche Mengen  $A$  und  $B$

$$|A_1 \times A_2 \times \dots \times A_n| = |A_1| \cdot |A_2| \cdot \dots \cdot |A_n| \text{ für endliche Mengen}$$

$$A_i; i \in \{1, 2, \dots, n\}$$

Grafische Veranschaulichung der Zahlenmengen  $\mathbb{N}, \mathbb{N}_0, \mathbb{Z}, \mathbb{Q}$



Zahlenstrahl: Horizontale Gerade mit aufsteigenden äquidistanten Punkten

Zahlenstrahl = gerichtete Gerade  $\Rightarrow$  Anordnung der Zahlen in  $\mathbb{N} \subset \mathbb{N}_0 \subset \mathbb{Z} \subset \mathbb{Q}$ ,

natürlich:  $a < b \Leftrightarrow$  Punkt zu  $a$  auf Zahlenstrahl liegt links vom Punkt zu  $b$  auf dem Zahlenstrahl  
 $a$  kleiner  $b$   $\xrightarrow{\quad}$

$a = b \Leftrightarrow$  Punkt zu  $a$  auf dem Zahlenstrahl ist identisch mit dem Punkt zu  $b$  auf dem Zahlenstrahl  
 $a$  gleich  $b$   $\xrightarrow{\quad}$

$a > b \Leftrightarrow b < a$   
 $a$  größer  $b$   $\xrightarrow{\quad}$

## 4 Vorlesung 4 (13.10.2020)

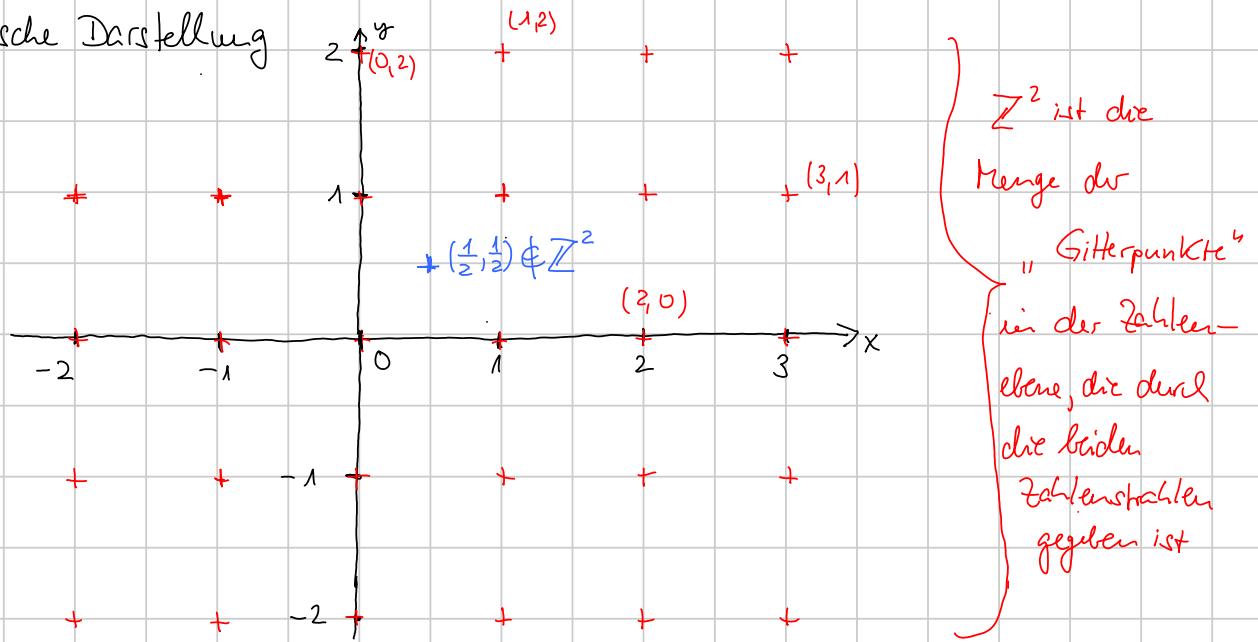
- 4.1 Beispiele Relationen + Kartesisches Produkt
- 4.2 Definition: reflexiv, transitiv, symmetrisch, antisymmetrisch: Äquivalenzrelation, Ordnungsrelation
- 4.3 Definition: Äquivalenzklasse

Beispiel: Kartesisches Produkt von Mengen

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

$$(-1, 4) \in \mathbb{Z}^2, \quad (7, 0) \in \mathbb{Z}^2, \quad \left(\frac{1}{2}, \frac{3}{4}\right) \notin \mathbb{Z}^2$$

grafische Darstellung



Definition:

1) Gegeben sind die Mengen  $A$  und  $B$  ( $A \neq \emptyset, B \neq \emptyset$ ).

Jede Teilmenge  $R \subseteq A \times B$  heißt (2-stellige) Relation über  $A, B$ .

Für  $A = B$ :  $R \subseteq A \times A = A^2$  heißt (2-stellige) Relation über  $A$ .

2) Gegeben sind die Mengen  $A_1, A_2, \dots, A_n$  ( $A_i \neq \emptyset \forall i \in \{1, 2, \dots, n\}$ ).

Jede Teilmenge  $R \subseteq A_1 \times A_2 \times \dots \times A_n$  heißt ( $n$ -stellige) Relation über  $A_1, A_2, \dots, A_n$ .

Für  $A_1 = A_2 = \dots = A_n$ :  $R \subseteq A_1 \times A_1 \times \dots \times A_1 = A_1^n$  heißt ( $n$ -stellige) Relation über  $A_1$ .

Beispiele:

1)  $M = \text{Menge aller Menschen}$

$R$  2-stellige Relation über  $M$  ist gegeben durch

$$R = \{(m_1, m_2) \in M \times M \mid m_1 \text{ ist Vater von } m_2\} \quad \text{„Vater-Relation“}$$

2)  $P$  = Menge aller Profifußballer im deutschen Fußball

$\tilde{R}$  2-stellige Relation über  $P$  ist gegeben durch

$$\tilde{R} = \{(f_1, f_2) \in P \times P \mid f_1 \text{ ist im selben Verein unter Vertrag wie } f_2\}$$

↑ „Fußballer-Relation“

3)  $K \subseteq \mathbb{Z} \times \mathbb{Z} = \mathbb{Z}^2$  ist definiert durch

$$K = \{(x, y) \in \mathbb{Z}^2 \mid x < y\} \leftarrow \text{„Kleiner-Relation“}$$

$K$  ist eine 2-stellige Relation über  $\mathbb{Z}$

↑ Kleiner-gleich

4) Man definiert für  $a, b \in \mathbb{Z}$ :  $a \leq b \Leftrightarrow (a < b) \vee (a = b)$

$$a \geq b \Leftrightarrow (a > b) \vee (a = b)$$

↑ größer-gleich

$KG \subseteq \mathbb{Z} \times \mathbb{Z} = \mathbb{Z}^2$  ist definiert durch

$$KG = \{(x, y) \in \mathbb{Z}^2 \mid x \leq y\} \leftarrow \text{„Kleiner-Gleich-Relation“}$$

$KG$  ist eine 2-stellige Relation über  $\mathbb{Z}$

Definition:

1) Eine 2-stellige Relation  $R$  über  $A$ ,  $A \neq \emptyset$ , heißt Äquivalenzrelation, falls gilt:

a)  $R$  ist reflexiv, d.h.  $(a, a) \in R \quad \forall a \in A$

b)  $R$  ist transitiv, d.h.  $(a, b) \in R \wedge (b, c) \in R \Rightarrow (a, c) \in R$

c)  $R$  ist symmetrisch, d.h.  $(a, b) \in R \Rightarrow (b, a) \in R$

2) Eine 2-stellige Relation über  $A$ ,  $A \neq \emptyset$ , heißt Ordnungsrelation,

falls gilt:  $\downarrow (a, a) \in R \quad \forall a \in A$

a)  $R$  ist reflexiv, b)  $R$  ist transitiv

Ausgangsheraussetzung  
für Prüfung auf Antisymmetrie

c)  $R$  ist antisymmetrisch, d.h.  $(a, b) \in R \wedge (b, a) \in R \Rightarrow a = b$

d.h. für  $a \neq b$  ist niemals  $(a, b) \in R$  und  $(b, a) \in R$

Beispiele:

1)  $G \subseteq \mathbb{Z} \times \mathbb{Z}$  ist definiert durch  $G = \{(x, y) \in \mathbb{Z}^2 \mid x = y\}$  ← „Gleich-Relation“

Es gilt:  $\forall x \in \mathbb{Z}: x = x \Rightarrow (x, x) \in G \quad \forall x \in \mathbb{Z}, G$  ist reflexiv

$(x, y) \in G \wedge (y, z) \in G \Rightarrow (x = y) \wedge (y = z) \Rightarrow x = z$

$\Rightarrow (x, z) \in G, G$  ist transitiv

$(x, y) \in G \Rightarrow x = y \Rightarrow y = x \Rightarrow (y, x) \in G, G$  ist symmetrisch

Zusammen: Die „Gleich-Relation“  $G$  über  $\mathbb{Z}$  ist eine Äquivalenzrelation

2)  $KG \subseteq \mathbb{Z}^2$  mit  $KG = \{(x, y) \in \mathbb{Z}^2 \mid x \leq y\}$  ← „Kleiner-Gleich-Relation“

Es gilt:

$(x, y) \in KG \Rightarrow x \leq y \}$  falls  $(x, y) \in KG$  und  $(y, x) \in KG$  gilt, hat man  
 $(y, x) \in KG \Rightarrow y \leq x \}$   $x \leq y \leq x \Leftrightarrow x = y$   
d.h.  $KG$  ist antisymmetrisch

$\forall x \in \mathbb{Z}: \underbrace{x \leq x}_{(x < x) \vee (x = x)} \Rightarrow (x, x) \in KG, KG$  ist reflexiv

↑  $(x < x) \vee (x = x)$  ← das wahre Ausrufe solange einer der Inputs  $x < x / x = x$  wahr ist

$\forall (x, y) \in KG, (y, z) \in KG:$

$(x, y) \in KG \Rightarrow x \leq y \}$   $\Rightarrow x \leq y \leq z \Rightarrow x \leq z \Rightarrow (x, z) \in KG,$   
 $(y, z) \in KG \Rightarrow y \leq z \}$   $KG$  ist transitiv

Zusammen: Die „Kleiner-Gleich-Relation“  $KG$  über  $\mathbb{Z}$  ist eine Ordnungsrelation

3) Welche der oben definierten Eigenschaften haben die folgenden Relationen

↓ Menge aller Menschen

a)  $R = \{(m_1, m_2) \in M \times M \mid m_1 \text{ ist Vater von } m_2\}$  ← „Vater-Relation“  
↓ Menge aller Profifußballer im DFB

b)  $\tilde{R} = \{(f_1, f_2) \in P \times P \mid f_1 \text{ ist im selben Verein unter Vertrag wie } f_2\}$

c)  $K = \{(x, y) \in \mathbb{Z}^2 \mid x < y\}$  ← „Kleiner-Relation“

zu a)  $R$  ist weder reflexiv, noch transitiv, noch symmetrisch

↑  
niemand ist sein  
eigener Vater       $(a,b) \in R \wedge$   
                         $(b,c) \in R \Rightarrow$   
                        a ist Großvater von c  
                        nicht Vater

↑  
niemand kann  
sein eigenes Kind sein

zu b)  $\tilde{R}$  ist Äquivalenzrelation, denn

$$(f, f) \in \tilde{R} \quad \forall f \in P \Rightarrow \tilde{R} \text{ ist reflexiv}$$

↑ jeder Fußballer gehört  
zu seinem Verein

$$(f_1, f_2) \in \tilde{R} \Rightarrow f_1 \text{ ist im selben Verein wie } f_2 \quad \left. \begin{array}{l} \\ \end{array} \right\} \Rightarrow f_1 \text{ ist im selben Verein} \\ \text{wie } f_2$$

$$(f_2, f_3) \in \tilde{R} \Rightarrow f_2 \text{ ist im selben Verein wie } f_3 \quad \left. \begin{array}{l} \\ \end{array} \right\} \Rightarrow f_2 \text{ ist im selben Verein wie } f_3$$

$\Rightarrow \tilde{R}$  ist transitiv

$$(f_1, f_2) \in \tilde{R} \Rightarrow f_1 \text{ ist im selben Verein wie } f_2$$

$\Rightarrow f_2 \text{ ist im selben Verein wie } f_1$

$$\Rightarrow (f_2, f_1) \in \tilde{R} \Rightarrow \tilde{R} \text{ ist symmetrisch}$$

zu c)  $K = \{ (x, y) \in \mathbb{Z}^2 \mid x < y \}$

$x < x$  ist falsche Aussage  $\forall x \in \mathbb{Z} \Rightarrow (x, x) \notin K \quad \forall x \in \mathbb{Z}$

$\Rightarrow K$  ist nicht reflexiv

ein konkretes Gegenbeispiel reicht aus

↑ für  $(1, 1)$  gilt  $1 < 1$  nicht! Damit ist  $(1, 1) \notin K$

$K$  ist nicht reflexiv

$$\begin{aligned} (x, y) \in K \Rightarrow x < y \\ (y, z) \in K \Rightarrow y < z \end{aligned} \Rightarrow x < y < z \Rightarrow x < z \Rightarrow (x, z) \in K$$

$\Rightarrow K$  ist transitiv

$(x, y) \in K \Rightarrow x < y \Rightarrow y < x$  ist falsche Aussage

$\Rightarrow (y, x) \notin K \Rightarrow K$  ist nicht symmetrisch

Es gibt keine  $(x, y) \in \mathbb{Z}^2$  mit  $(x, y) \in K \wedge (y, x) \in K$ , dann  $x < y$  und  $y < x$

ist immer eine falsche Aussage! Ausgangshypothese für Antisymmetrie ist nie erfüllt!

### Definition:

Gegeben ist eine (2-stellige) Äquivalenzrelation  $R$  über  $A$ . Dann gilt:

1) Falls  $(a, b) \in R$  ist, sagt man  $a$  und  $b$  sind äquivalent.

2) Für  $a \in A$  ist die Menge

$$[a] = \bar{a} = \{b \in A \mid (a, b) \in R\}$$

$$= \{b \in A \mid a \text{ und } b \text{ sind äquivalent}\}$$

die Äquivalenzklasse zu  $a$  (bezügl. der Relation  $R$ )

3) Für  $(a, b) \in R$ , also  $a$  und  $b$  sind äquivalent, wird häufig ein eigenes „Rechenzeichen“ eingeführt, z.B.  $a \equiv b$ .

### Beispiel:

Wir betrachten die Zahl  $m = 5 \in \mathbb{Z}$  und folgende Relation  $R$ :

Für  $a, b \in \mathbb{Z}$  gilt  $a \equiv b \Leftrightarrow 5$  ist echter Teiler von  $b-a$

$\uparrow$   
 $a$  ist äquivalent zu  $b$  /  $a$  ist Kongruent zu  $b$

Bemerkung:  $5$  ist echter Teiler von  $b-a \Leftrightarrow \exists k \in \mathbb{Z}: b-a = k \cdot 5$

a)  $R = \{(a, b) \in \mathbb{Z}^2 \mid a \equiv b\}$  ist eine Äquivalenzrelation

$b-a$  ist ein Vielfaches von  $5$

reflexiv:  $a-a=0=0 \cdot 5 \Rightarrow (a, a) \in R$  oder  $a \equiv a$

symmetrisch:  $a \equiv b \Rightarrow \exists k \in \mathbb{Z}: b-a=k \cdot 5$

$$\Rightarrow a-b = -(b-a) = -k \cdot 5 = (-k) \cdot 5$$

$\Rightarrow$  und  $a-b$  ist ein Vielfaches von  $5$

$$\Rightarrow b \equiv a$$

transitiv:  $a \equiv b \wedge b \equiv c \Rightarrow \exists k, l \in \mathbb{Z}: b-a=k \cdot 5 \wedge c-b=l \cdot 5$

$$\Rightarrow c-a = (\cancel{c-\cancel{b}}^{\stackrel{\equiv}{=}} + \cancel{b-a})$$

$$= l \cdot 5 + k \cdot 5 = (l+k) \cdot 5$$

$\Rightarrow$  und  $c-a$  ist ein Vielfaches von  $5$

$$\Rightarrow c \equiv a$$

b) Äquivalenzklassen dieser Relation  $a \equiv b \Leftrightarrow b-a = k \cdot 5$

$$[0] = \bar{0} = \{ b \in \mathbb{Z} \mid 0 \equiv b \} = \{ b \in \mathbb{Z} \mid b - 0 = b = k \cdot 5 \}$$
$$= \{ b \in \mathbb{Z} \mid b = k \cdot 5 \} = \{ b \in \mathbb{Z} \mid b = k \cdot 5 + 0 \}$$

$$[1] = \bar{1} = \{ b \in \mathbb{Z} \mid 1 \equiv b \} = \{ b \in \mathbb{Z} \mid b - 1 = k \cdot 5 \}$$
$$= \{ b \in \mathbb{Z} \mid b = k \cdot 5 + 1 \}$$

Aufgabe zur 5. Vorlesung: a) Finden Sie die weiteren Äquivalenzklassen

b) Finden Sie die Äquivalenzklassen der Fußballer-Relation (sprachlich beschreiben!)

## 5 Vorlesung 5 (14.10.2020)

**5.1 Beispiele Äquivalenzklasse**

**5.2 Definition: vollständige Mengenpartition**

**5.3 Satz: Äquivalenzklassen bilden vollständige Mengenpartition**

**5.4 Definition: Verknüpfung**

**5.5 Definition: Abbildung, Funktion, Bild, Graph, Urbild**

**5.6 grafische Veranschaulichung der reellen Zahlen**

$$1) R = \{(a, b) \in \mathbb{Z}^2 \mid \exists k \in \mathbb{Z}: b - a = k \cdot 5\}$$

für  $(a, b) \in R$  schreiben wir  $a \equiv b$

4. Vorlesung: Nachweis  $R$  ist Äquivalenzrelation

Äquivalenzklassen:  $[a] = \{b \in \mathbb{Z} \mid a \equiv b\}$  (andere Schreibweise für  $[a]$  ist  $\bar{a}$ )

$$\begin{aligned} [0] &= \bar{0} = \{b \in \mathbb{Z} \mid b - 0 = k \cdot 5\} = \{b \in \mathbb{Z} \mid b = k \cdot 5 + 0\} \\ [1] &= \bar{1} = \{b \in \mathbb{Z} \mid b - 1 = k \cdot 5\} = \{b \in \mathbb{Z} \mid b = k \cdot 5 + 1\} \\ [2] &= \bar{2} = \{b \in \mathbb{Z} \mid b - 2 = k \cdot 5\} = \{b \in \mathbb{Z} \mid b = k \cdot 5 + 2\} \\ [3] &= \bar{3} = \{b \in \mathbb{Z} \mid b - 3 = k \cdot 5\} = \{b \in \mathbb{Z} \mid b = k \cdot 5 + 3\} \\ [4] &= \bar{4} = \{b \in \mathbb{Z} \mid b - 4 = k \cdot 5\} = \{b \in \mathbb{Z} \mid b = k \cdot 5 + 4\} \end{aligned}$$

} es existiert ein  $k \in \mathbb{Z}$ , so dass die Darstellung nur  $b$  gegeben ist

$$\begin{aligned} [5] &= \bar{5} = \{b \in \mathbb{Z} \mid b - 5 = k \cdot 5\} = \{b \in \mathbb{Z} \mid b = k \cdot 5 + 5 = \underbrace{(k+1)}_{\text{= } \tilde{k}} \cdot 5\} \\ &= \{b \in \mathbb{Z} \mid b = \tilde{k} \cdot 5 + 0\} = [0] \end{aligned}$$

Für  $i \in \{0, 1, 2, 3, 4\}$  gilt also

� ganzzahlige Teiler

$[i] = \bar{i}$  ist die Menge aller ganzen Zahlen, die beim Teilen durch 5 den Rest  $i$  lassen.

$$\begin{aligned} [0] &= \{\dots, -10, -5, 0, 5, 10, 15, 20, 25, \dots\} \\ [1] &= \{\dots, -9, -4, 1, 6, 11, 16, \dots\} \quad -9 = \underbrace{(-2)}_k \cdot 5 + 1 \\ [2] &= \{\dots, -13, -8, -3, 2, 7, 12, 17, \dots\} \\ [3] &= \{\dots, -12, -7, -2, 3, 8, 13, 18, \dots\} \\ [4] &= \{\dots, -11, -6, -1, 4, 9, 14, 19, \dots\} \end{aligned}$$

$$\mathbb{Z} = [0] \cup [1] \cup [2] \cup [3] \cup [4], \quad [i] \cap [j] = \emptyset \text{ für } i \neq j$$

2) Fußballer-Relation (aus der 4. Vorlesung)

Eine Äquivalenzklasse dieser Relation ist ein Verein im deutschen Profifußball



� jeder Verein (als Menge seiner Spieler) ist eine Äquivalenzklasse

$P = \text{Menge aller Profifußballer im deutschen Fußball}$   
 $\tilde{R} \text{ 2-stellige Relation über } P \text{ ist gegeben durch}$   
 $\tilde{R} = \{(f_1, f_2) \in P \times P \mid f_1 \text{ ist im selben Verein unter Vertrag wie } f_2\}$   
 ↑ „Fußballer-Relation“

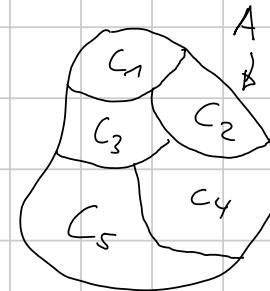
Definition: Gegeben ist eine Menge  $A (A \neq \emptyset)$ .  $P(A)$  ist dann die Potenzmenge von  $A$  (Menge aller Teilmengen von  $A$ ).

Ein Mengensystem  $B \subseteq P(A)$  (also eine Menge von Teilmengen von  $A$ ) heißt vollständige Mengenpartition von  $A$ , wenn gilt:

$$1) C_1 \cap C_2 = \emptyset \quad \forall C_1, C_2 \in B \text{ mit } C_1 \neq C_2$$

$$2) \bigcup_{C_i \in B} C_i = C_1 \cup C_2 \cup C_3 \cup \dots \cup C_N = A$$

$$B = \{C_1, C_2, \dots, C_N\}$$



Bemerkung: Wenn  $B = \{C_1, C_2, \dots, C_N\} \subseteq P(A)$  eine vollständige Mengenpartition von  $A$  ist, gilt: Jedes Element von  $A$  gehört zu genau einer Menge  $C_i$  aus  $B$ .

Satz: Gegeben ist eine Menge  $A, A \neq \emptyset$ .  $R \subseteq A \times A$  ist eine Äquivalenzrelation über  $A$ . Dann gilt:

Die Äquivalenzklassen dieser Relation bilden eine vollständige Mengenpartition von  $A$ , d.h.  $\bigcup_{a \in A} [a] = A$ .

Beweis:

1) Für jedes  $a \in A$  gilt  $a \in [a]$ , denn  $R$  ist reflexiv  $(a, a) \in R$ , damit ist  $\bigcup_{a \in A} [a] = A$

2) Angenommen  $[a] \cap [b] \neq \emptyset \Rightarrow \exists x \in [a] \cap [b] \text{ d.h.}$

$$\underbrace{x \in [a]}_{(a, x) \in R} \wedge \underbrace{x \in [b]}_{(b, x) \in R} \Rightarrow \underbrace{(a, x) \in R \wedge (b, x) \in R}_{R \text{ ist symmetrisch}}$$

$$\Rightarrow \underbrace{(a, x) \in R \wedge (x, b) \in R}_{R \text{ ist transitiv}}$$

$$\Rightarrow (a, b) \in R$$

$$\Rightarrow a \in [b], b \in [a]$$

$$\Rightarrow [a] = [b]$$

### Verknüpfung von Relationen

Definition: A, B, C sind nichtleere Mengen.

Gegaben sind die 2-stelligen Relationen  $R_1 \subseteq A \times B$  und  $R_2 \subseteq B \times C$

Dann ist die Verknüpfung  $R_1 \circ R_2 \subseteq A \times C$  definiert durch:

$$(a, c) \in R_1 \circ R_2 \Leftrightarrow \exists x \in B : (a, x) \in R_1 \wedge (x, c) \in R_2$$

A = Menge der Namen der Studierenden der HS OS

B = Menge der zulässigen Matrikelnummern der HS OS

C = Menge der Studiengänge der HS OS

$R_1 \subseteq A \times B \leftarrow$  Zuordnung des Namens eines Studierenden zur Matrikelnr.

Name	Matr.-Nr.
---	---
Schmidt	12345
Meier	36111
Schulze	21224
:	:

$R_2 \subseteq B \times C \leftarrow$  Zuordnung von Matrikelnr. zu Studiengang

Matrikel-Nr.	Studiengang
---	---
12345	Elektrot.
36111	Medieninf.
21224	Gartenbau
---	---

$$R_1 \circ R_2 \subseteq A \times C$$

$$\left. \begin{array}{l} (\text{Schmidt}, 12345) \in R_1 \\ (12345, \text{Elektrot.}) \in R_2 \end{array} \right\} (\text{Schmidt, Elektrot.}) \in R_1 \circ R_2$$

Name	Studiengang
---	---
Schmidt	Elektrot.
Moser	Medizinteinf.
Schulze	Gartenbau
---	----

## Abbildungen und Funktionen (als Relationen mit bestimmten Zusatzeigenschaften)

### Definition:

Gegeben sind die Mengen  $D$  und  $W$  ( $D \neq \emptyset, W \neq \emptyset$ ).

a) Eine Abbildung  $f: D \rightarrow W$  ist eine 2-stellige Relation  $f \subseteq D \times W$  über  $D$  und  $W$  mit folgender Eigenschaft:

$\forall x \in D \exists ! y \in W : (x, y) \in f$ , man schreibt dafür  $y = f(x)$   
 zu jedem  $x \in D$  gibt es genau ein  
 $y \in W$  mit  $(x, y) \in f$  oder  $y = f(x)$ ;  
 dem  $x \in D$  wird mittels  $f$  genau ein  
 $y \in W$  zugeordnet

Die Menge  $D$  heißt Definitionsbereich / Definitionsmenge der Abbildung;

die Menge  $W$  heißt Wertebereich / Wertemenge der Abbildung

b) Wenn gilt:  $D \subseteq \mathbb{R}$  und  $W \subseteq \mathbb{R}$  nennt man die Abbildung  $f: D \rightarrow W$  eine (reellwertige) Funktion einer (reellen) Veränderlichen

c) Für eine Abbildung  $f: D \rightarrow W$  ist definiert

$$\underline{\text{Bild}(f)} = \{ y \in W \mid \exists x \in D \text{ mit } y = f(x) \text{ (d.h. } (x, y) \in f \subseteq D \times W \text{)} \}$$

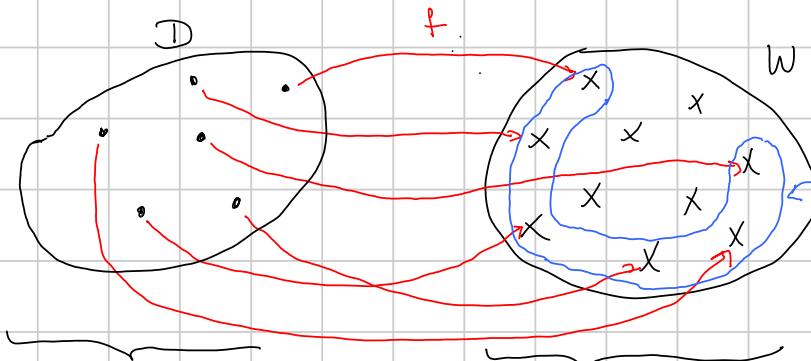
$$\underline{\text{Graph}(f)} = \{ (x, y) \in D \times W \mid y = f(x) \text{ (d.h. } (x, y) \in f \text{)} \}$$

ist der Graph von  $f$  ( $D \subseteq \mathbb{R}, W \subseteq \mathbb{R} : \text{Graph} \hat{=} \text{Funktionskurve}$ )

$$\text{Für } y \in W \text{ ist } \underline{U}_f(y) = \{ x \in D \mid y = f(x) \text{ (d.h. } (x, y) \in f \text{)} \}$$

das Urbild von  $y$  unter  $f$

$f: D \rightarrow W$



Bild( $f$ )

Elemente von  $W$ , bei denen ein Pfeil endet, die also vorkommen

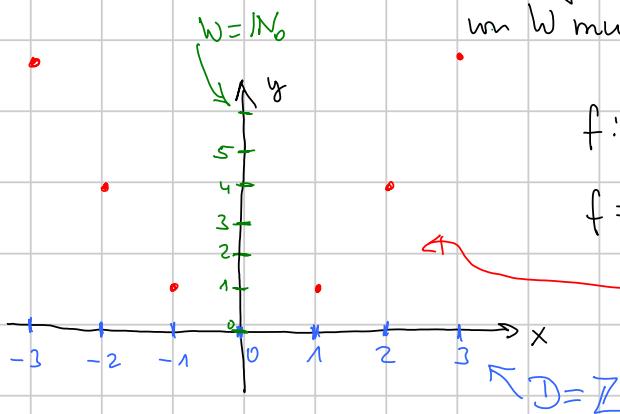
$\forall x \in D$  heißt:

von jedem Element in  $D$  geht ein Pfeil aus

$\exists ! y \in W : (x, y) \in f$

Jeder Pfeil endet bei genau einem Element aus  $W$

Achtung: Nur bei jedem Element von  $W$  muss ein Pfeil enden



$f: \mathbb{Z} \rightarrow \mathbb{N}_0$

$f = \{(z, z^2) \in \mathbb{Z} \times \mathbb{N}_0\}$  also  $f(z) = z^2$

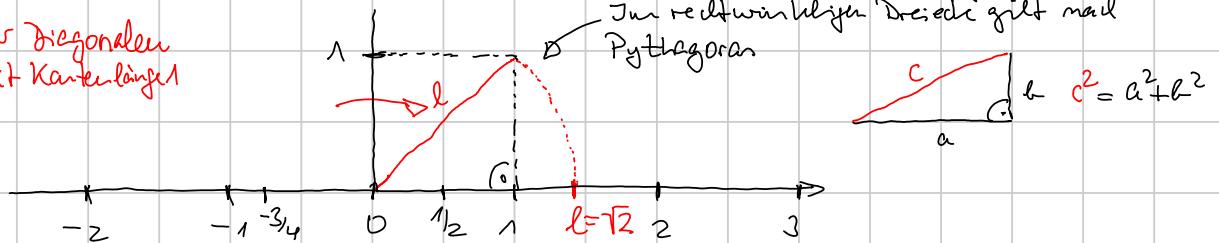
Graph( $f$ ) =  $\{(z, z^2) \mid z \in \mathbb{Z}\}$

Was ist  $\mathbb{R}$ ?

$\mathbb{N} \subset \mathbb{N}_0 \subset \mathbb{Z} \subset \mathbb{Q} \rightarrow$  grafische Veranschaulichung: Zahlenstrahl

$l \triangleq$  Länge der Diagonalen im Quadrat mit Kantenlängel

Im rechtwinkligen Dreieck gilt nach Pythagoras



Zu  $l$  gibt es einen Punkt auf dem Zahlensstrahl, d.h.  $l$  ist eine auf dem Zahlensstrahl repräsentierte Zahl, mit Pythagoras folgt  $l^2 = 1^2 + 1^2 = 2$ .

Wir nennen die Zahl  $l$  Wurzel aus 2, geschrieben  $l = \sqrt{2}$

Es gilt  $\sqrt{2} \notin \mathbb{Q}$ , d.h.  $\sqrt{2}$  gehört zu einer Zahlenmenge (repräsentiert auf dem Zahlensstrahl), die neu ist; das ist  $\mathbb{R}$ , die Menge der reellen Zahlen; es gilt  $\mathbb{N} \subset \mathbb{N}_0 \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$ .

Beweis zu  $\sqrt{2} \notin \mathbb{Q}$ : Widerspruchsbeweis (man nimmt das Gegenteil der Behauptung als wahr an und leitet daraus einen offensichtlichen Widerspruch ab, d.h. das

Gegentil des Behauptung muss falsch sein, die ursprüngliche Behauptung ist also wahr)

Angenommen  $\sqrt{2} \in \mathbb{Q}$   $\Rightarrow$  es gibt  $z \in \mathbb{Z}, n \in \mathbb{N}$  mit  $\sqrt{2} = \frac{z}{n}$  in vollständig gekürzter Form, d.h.  $z$  und  $n$  haben keine gemeinsamen Faktoren mehr:

$$\sqrt{2} = \frac{z}{n} \Rightarrow 2 = \frac{z^2}{n^2} \Rightarrow z^2 = 2 \cdot n^2 \Rightarrow 2 \text{ ist Teiler von } z^2 = z \cdot z \\ \Rightarrow 2 \text{ ist Teiler von } z, \text{ d.h.}$$

es gibt  $k \in \mathbb{Z}$  mit  $z = k \cdot 2$

$$\text{dann gilt } 2 = \frac{z^2}{n^2} \Rightarrow 2 \cdot n^2 = z^2 = (k \cdot 2)^2 = 4k^2$$

$$\Rightarrow n^2 = 2k^2 \Rightarrow 2 \text{ ist Teiler von } n^2 = n \cdot n$$

2 ist ein Teiler von n

Widereindruck darin, dass  $z$  und  $n$  keine gemeinsamen Faktoren haben!

## 6 Vorlesung 6 (19.10.2020)

**6.1 Beispiele Abbildung, Funktion**

**6.2 Zahlensysteme**

**6.3 Peano-Axiome (natürliche Zahlen definieren)**

**6.4 Rechenregeln in den natürlichen Zahlen**

**6.5 Definition: Endliche Summe**

**6.6 5. Peano-Axiom / Induktionsaxiom / vollständige Induktion**

Abbildung / Funktion

Gegaben sind Mengen  $D, W$  ( $D \neq \emptyset, W \neq \emptyset$ ).

Die 2-stellige Relation  $f \subseteq D \times W$  heißt Abbildung, falls gilt:

$\forall x \in D \exists ! y \in W : (x, y) \in f$ , man schreibt dann  $y = f(x)$ .

Wenn gilt  $D \subseteq \mathbb{R}$  und  $W \subseteq \mathbb{R}$ , nennt man  $f$  eine (reellwertige) Funktion einer (reellen) Veränderlichen (Variablen).

$D$  heißt Definitionsbereich / Definitionsmenge

$W$  heißt Wertebereich / Wertemenge

Graph ( $f$ ) =  $\{(x, y) \in D \times W \mid (x, y) \in f\} = \{(x, y) \in D \times W \mid y = f(x)\}$

ist der Graph von  $f$  (bei Funktionen heißt der Graph auch Funktionskurve)

Bild ( $f$ ) =  $\{y \in W \mid \exists x \in D : (x, y) \in f\} = \{(x, y) \in D \times W \mid \exists x \in D : y = f(x)\}$

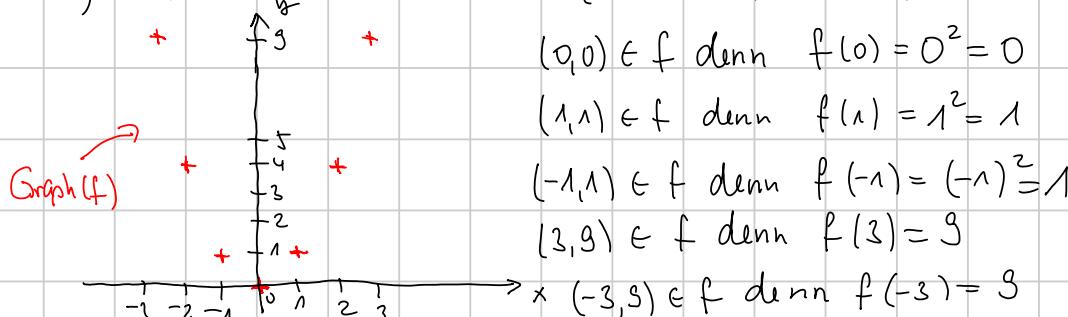
heißt Bild von  $f$ .

Das Urbild von  $y$  unter  $f$  ist  $U_f(y) = \{x \in D \mid (x, y) \in f\}$   
 $= \{x \in D \mid y = f(x)\}$

Beispiele:

$f: \mathbb{Z} \rightarrow \mathbb{Z}$  es ist  $D = \mathbb{Z}$  und  $W = \mathbb{Z}$

1)  $f \subseteq \mathbb{Z} \times \mathbb{Z}$  mit  $f = \{(x, x^2) \in \mathbb{Z} \times \mathbb{Z} \mid x \in \mathbb{Z}\} = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid y = x^2\}$



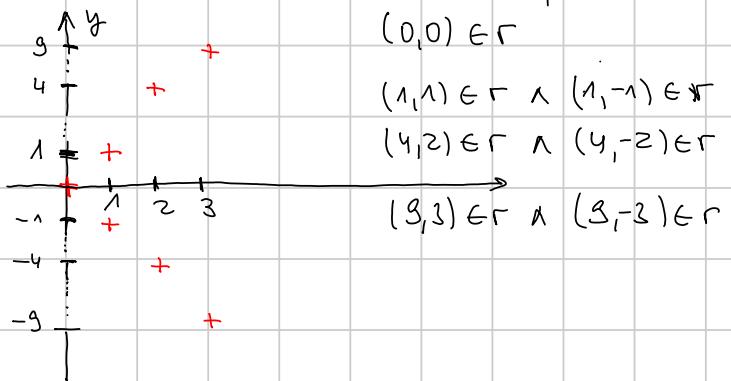
$$\text{Bild}(f) = \{y \in \mathbb{Z} \mid y \geq 0\}$$

$$U_f(16) = \{-4, 4\} \text{ denn } f(-4) = (-4)^2 = 16 \text{ und } f(4) = 4^2 = 16$$

$$U_f(2) = \emptyset \text{ denn es gilt } (\sqrt{2})^2 = 2 \text{ d.h. } f(\sqrt{2}) = 2 \text{ aber } \sqrt{2} \notin \mathbb{Z}$$

$$U_f(-5) = \emptyset \text{ denn für kein } x \in \mathbb{Z} \text{ gilt } x^2 = -5, U_f(0) = \{0\} \text{ denn nur } 0^2 = 0$$

2) Die 2-stellige Relation  $r \subseteq \mathbb{Z} \times \mathbb{Z}$  ist gegeben durch

$$r = \{(x^2, x) \mid x \in \mathbb{Z}\}$$


$r$  ist 2-stellige Relation  
aber Keine Abbildung/Funktion  
denn z.B. zu 1 gibt es  
 $y_1 = -1$  und  $y_2 = 1$  mit  $(1, -1) \in r$   
und  $(1, 1) \in r$

3)  $f \subseteq \mathbb{R} \times \mathbb{R}$  mit  $(x, y) \in f \Leftrightarrow y = x^2$

das definiert die Funktion  $f: \mathbb{R} \rightarrow \mathbb{R}$  mit  $y = f(x) = x^2$

D  $\uparrow$  L W



$$\text{Bild}(f) = \{y \in \mathbb{R} \mid y \geq 0\}$$

$$U_f(0) = \{0\}, U_f(2) = \{-\sqrt{2}, \sqrt{2}\}$$

$$U_f(-4) = \emptyset \text{ denn } x^2 = -4 \text{ hat keine Lösung}$$

$$x \in \mathbb{R}$$

Zahlensystem: Das System der reellen Zahlen

$$\mathbb{N} \subset \mathbb{N}_0 \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$$

Start mit  $\mathbb{N} \subset \mathbb{N}_0$ : natürliche Zahlen und natürliche Zahlen mit 0

$$\mathbb{N} = \{1, 2, 3, 4, \dots\}; \mathbb{N}_0 = \{0, 1, 2, 3, 4, \dots\}$$

Axiomatische Einführung von  $\mathbb{N}_0$  (Peano-Axiome)

$\models$  für Peano  $0 \in \mathbb{N}$

↑ gültige (als richtig gesetzte)  
mathematische Aussagen

1. 0 ist eine natürliche Zahl (alternativ: 1 ist eine natürliche Zahl)

4 von

2. Jede natürliche Zahl  $n$  hat einen Nachfolger, der  $n'$  genannt wird, 0 ist nicht Nachfolger einer natürlichen Zahl, der Nachfolger der 0 heißt 1, also  $0' = 1$ ,

5

$0$  ist neutrales Element der Addition

Peano-

3.  $n + 0 = n$  und  $n + m' = (n + m)'$  und damit:  $n' = (n + 0)' = n + 0' = n + 1$  und  $n + m$  ist der  $m$ -fache Nachfolger von  $n$ , also:  $n + m = ((\dots(n+1)+1)+1)+\dots+1$ ,

Axiomen

4.  $n \cdot 0 = 0$  und  $n \cdot m' = n \cdot m + n$ .

Das Axiomensystem von Peano liefert die natürlichen Zahlen mit 0,

also meine Menge  $\mathbb{N}_0$ , und die Addition und die Multiplikation in der Menge  $\mathbb{N}_0$ . Addition und Multiplikation sind Rechenoperationen, d.h. besondere Abbildungen (Funktionen), nämlich

$$+ : \mathbb{N}_0 \times \mathbb{N}_0 \rightarrow \mathbb{N}_0 \text{ mit } (x, y) \mapsto x + y$$

$$\cdot : \mathbb{N}_0 \times \mathbb{N}_0 \rightarrow \mathbb{N}_0 \text{ mit } (x, y) \mapsto x \cdot y$$

Es gelten folgende Rechenregeln in  $\mathbb{N}_0$

Name	Addition (+)	Multiplikation (·)
Kommutativgesetz	$a + b = b + a$	$a \cdot b = b \cdot a$
Assoziativgesetz	$a + (b + c) = (a + b) + c$	$a \cdot (b \cdot c) = (a \cdot b) \cdot c$
Existenz neutraler Elemente	$a + 0 = a$	$a \cdot 1 = a$
Distributivgesetze	$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$	$(a + b) \cdot c = (a \cdot c) + (b \cdot c)$

neutrales Element der Addition:  $\emptyset$  Null

neutrales Element der Multiplikation: 1 Eins

Distributivgesetz regelt den „Zusammenspiel“ von Addition und Multiplikation.

Bemerkung:

- 1) Die Peano-Axiome führen die Addition (inklusive 0 als neutralem Element) in  $\mathbb{N}_0$  ein!  
 $0 \notin \mathbb{N}$  heißt: In  $\mathbb{N}$  gibt es kein neutrales Element der Addition!
- 2) Multiplikation ist eine wiederholte Addition des selben Elements z.B.

$$3 \cdot 5 = \underbrace{5 + 5 + 5}_{\text{3-fache Addition des Elements } 5 \in \mathbb{N}_0}$$

$$n \cdot m = \underbrace{m + m + \dots + m}_{n-\text{mal}}$$

- 3) Potenzen: Für  $\underbrace{a \in \mathbb{N}}_{a \neq 0}$  und  $n \in \mathbb{N}_0$  ist definiert:

$$a^0 = 1 \leftarrow 0\text{-te Potenz von } a \neq 0 \text{ ist immer 1}$$

$$a^1 = a \leftarrow 1\text{-te Potenz von } a \neq 0 \text{ ist immer } a$$

$$a^2 = a \cdot a$$

$$\vdots$$

$$a^n = \underbrace{a \cdot a \cdot a \cdot \dots \cdot a}_{n-\text{mal Faktor } a}$$

} 2-te, n-te Potenz ist das 2-fache/n-fache Produkt von  $a$  mit sich selbst

Definition:

Gegaben sind  $n \in \mathbb{N}_0$ ,  $\sigma \in \mathbb{N}_0$  mit  $\sigma \leq n$  und Zahlen  $a_i \in \mathbb{R}$ ,  $i \leq \sigma$ ,

$i \in \mathbb{N}_0$ . Dann ist die zugehörige endliche Summe mit unterer Grenze  $u$  und oberer Grenze  $\theta$  definiert durch

$$\sum_{i=u}^{\theta} a_i = a_u + a_{u+1} + a_{u+2} + \dots + a_{\theta}$$

$\sum$  heißt Summenzeichen,  $i$  heißt Laufindex,  $a_i$  sind die Summanden der Summe; für  $u=0$  gilt  $\sum_{i=0}^{\theta} a_i = a_{\theta}$

Beispiele:

1)  $u=3, \theta=9, a_i = 2i+1$  für  $3 \leq i \leq 9, i \in \mathbb{N}_0$

$$\sum_{i=u}^{\theta} a_i = \sum_{i=3}^9 (2i+1) = 7 + 9 + 11 + 13 + 15 + 17 + 19$$

$\downarrow$

$$= a_3 + a_4 + a_5 + \dots + a_9$$

2)  $u=0, \theta=10, a_i = i$  für  $0 \leq i \leq 10, i \in \mathbb{N}_0$

$$\sum_{i=0}^{10} i = 1 + 2 + 3 + 4 + 5 + 6 + 7 + 8 + 9 + 10$$

3)  $\sum_{i=s}^{\theta} (\underbrace{i^2 - i + 2}_{= a_i}) = a_s = 22$

S.Peano-Axiom: Induktionsaxiom  $\Leftrightarrow$  Axiom der vollständigen Induktion

Gegaben ist eine Aussageform  $A(n)$  für  $n \in \mathbb{N}_0$  (bzw.  $n \in \mathbb{N}$ ).

Dann gilt:  $A(n)$  ist wahr für alle  $n \in \mathbb{N}_0$  (bzw.  $n \in \mathbb{N}$ )

falls die folgenden beiden Bedingungen erfüllt sind

① Induktionsanfang

$A(0)$  ist wahr (bzw.  $A(1)$  ist wahr)

d.h. die Aussageform  $A(n)$  liefert eine wahre Aussage für die erste behandelte nat. Zahl 0 bzw. 1

② Induktionsabschluß: Für  $n=k$

$A(k)$  wahr

$\Rightarrow$   $A(k+1)$  wahr

Induktionsannahme

Induktionsbehauptung

das ist die „Beweisarbeit“: Zeigt, dass  $A(k+1)$  wahr ist, wenn  $A(k)$  wahr ist

d.h. wenn die Aussageform  $A(n)$  für  $n=k$  eine wahre Aussage liefert, dann liefert  $A(n)$  auch für die nachfolgende Zahl  $n=k+1$  eine wahre Aussage.

Beispiele:

1) Summenformel vom „Kleinen Gauß“:

$$\text{Für alle } n \in \mathbb{N} \text{ gilt: } \sum_{i=1}^n i = 1 + 2 + 3 + \dots + n = \frac{n \cdot (n+1)}{2},$$

$$A(n): \text{Für } n \in \mathbb{N} \text{ ist } \sum_{i=1}^n i = \frac{n \cdot (n+1)}{2}$$

Induktionsanfang: Man muss nachrechnen, dass  $A(1)$  wahr ist ( $n=1$ )

$$\sum_{i=1}^1 i = 1 \quad (\text{nach Def. einer endlichen Summe mit oberer Grenze} = \text{niedrige Grenze})$$

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

$$\underline{\text{insgesamt}} \quad \sum_{i=1}^1 i = 1 = \frac{1 \cdot (1+1)}{2} \quad \text{d.h. } A(1) \text{ ist wahr}$$

Induktionsschritt:

Induktionsvoraussetzung: Für  $n=k$  ist  $A(k)$  wahr, also

$$\sum_{i=1}^k i = \frac{k \cdot (k+1)}{2} \quad \leftarrow \text{das darf im weiteren Beweis als } \underline{\text{wahr}} \text{ benutzt werden}$$

Induktionsbehauptung: Für  $n=k+1$  ist  $A(k+1)$  ebenfalls wahr, also

$$\begin{aligned} \sum_{i=1}^{k+1} i &= \frac{(k+1) \cdot ((k+1)+1)}{2} \quad \checkmark \quad \leftarrow \text{es muss gezeigt/bewiesen/nachgerechnet werden, dass dieses } = \text{ und wahr ist} \\ &\uparrow n=k+1 \\ \rightarrow \left( \sum_{i=1}^n i = \frac{n \cdot (n+1)}{2} \right) \end{aligned}$$

$$\text{Beweis: } \sum_{i=1}^{k+1} i = \left( \sum_{i=1}^k i \right) + (k+1)$$

$$\begin{aligned} \text{Induktionsvoraus-} \\ \text{setzung} \end{aligned} \quad \rightarrow \quad = \frac{k \cdot (k+1)}{2} + (k+1) = \frac{k \cdot (k+1) + 2(k+1)}{2}$$

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

✓ das rot genau das,  
was getzt werden sollte

## Bemerkung:

$$a) \sum_{i=1}^{50} i = \frac{50 \cdot 51}{2} = \frac{50 \cdot (50+1)}{2} = \frac{50^2 + 50}{2} = \frac{2500 + 50}{2} = 1275$$

$$b) \sum_{i=1}^{100} i = \frac{100 \cdot 101}{2} = 50 \cdot 101 = 5050$$

Gauß:

$$\begin{aligned}
 & 1 + 2 + 3 + 4 + \dots + 99 + 100 = S \\
 & + + + + + + + + + + + + + + + \\
 & 100 + 99 + 98 + 97 + \dots + 2 + 1 = S \\
 \hline
 & \underbrace{101 + 101 + 101 + 101 + \dots + 101 + 101}_{= 100 \cdot 101} = 2S
 \end{aligned}$$

$$\Rightarrow 2S = 100 \cdot 101 \Rightarrow S = \frac{100 \cdot 101}{2}$$

## **7 Vorlesung 7 (20.10.2020)**

**7.1 Beispiele Vollständige Induktion**

**7.2 Definition durch Rekursion + Beispiele**

**7.3 Binomialkoeffizient**

Vollständige Induktion

Eine Aussageform  $A(n)$  mit  $n \in \mathbb{N}$  bzw.  $n \in \mathbb{N}_0$  ist wahr für alle  $n \in \mathbb{N}$  bzw.  $n \in \mathbb{N}_0$ ,

falls gilt: ① Induktionsanfang  $A(1)$  bzw.  $A(0)$  ist wahr, d.h. die Aussage gilt für  $n=1$  bzw.  $n=0$

② Induktionsabschluß  $A(k)$  ist wahr  $\Rightarrow A(k+1)$  ist wahr, d.h.

man zeigt: Wenn die Aussage für  $n=k$  wahr ist, dann ist sie auch für  $n=k+1$  wahr

Beispiele: Gestern (18.10.)  $\sum_{i=1}^n i = 1+2+3+\dots+n = \frac{n \cdot (n+1)}{2}$

$$\textcircled{1} \quad \sum_{i=1}^n i^2 = 1^2 + 2^2 + 3^2 + \dots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

a) Induktionsanfang  $n=1$

$$\sum_{i=1}^1 i^2 = 1^2 = 1$$

$$\left. \begin{aligned} \frac{n \cdot (n+1) \cdot (2n+1)}{6} &= \frac{1 \cdot (1+1) \cdot (2 \cdot 1+1)}{6} = \frac{1 \cdot 2 \cdot 3}{6} = 1 \\ \sum_{i=1}^1 i^2 &= \frac{1 \cdot (1+1) \cdot (2 \cdot 1+1)}{6} \end{aligned} \right\} \checkmark$$

b) Induktionsabschluß

Induktionsvor.  $A(k)$  ist wahr, d.h.  $\sum_{i=1}^k i^2 = \frac{k \cdot (k+1) \cdot (2k+1)}{6}$

das darf beim Beweis als wahr benutzt werden

Induktionsabschluß:  $A(k+1)$  ist wahr, d.h.

$$\begin{aligned} \sum_{i=1}^{k+1} i^2 &= \frac{(k+1) \cdot ((k+1)+1) \cdot (2(k+1)+1)}{6} \\ &= \frac{(k+1) \cdot (k+2) \cdot (2k+3)}{6} \end{aligned}$$

das muss im Beweis gezeigt (nachgerechnet) werden!

$$\text{Beweis: } \sum_{i=1}^{k+1} i^2 = \left( \sum_{i=1}^k i^2 \right) + (k+1)^2$$

$$= \frac{k \cdot (k+1) \cdot (2k+1)}{6} + (k+1)^2$$

$$= \frac{k \cdot (k+1) \cdot (2k+1) + 6(k+1)^2}{6}$$

$$= \frac{(k+1)[k \cdot (2k+1) + 6(k+1)]}{6}$$

$$= \frac{(k+1)[2k^2 + 7k + 6]}{6}$$

$$= \frac{(k+1) \cdot (k+2) \cdot (2k+3)}{6} \quad \checkmark$$

$$(k+2) \cdot (2k+3) = \\ 2k^2 + 3k + 4k + 6 = \\ 2k^2 + 7k + 6$$

$$(2) \quad q \in \mathbb{R}, \quad q \neq 1; \quad \text{dann gilt: } \sum_{i=0}^n q^i = 1 + q + q^2 + q^3 + \dots + q^n = \frac{1-q^{n+1}}{1-q}$$

a) Induktionsanfang:  $n=0$ ;  $A(0)$  ist wahr muss gezeigt werden

$$\sum_{i=0}^0 q^i = q^0 = 1 \quad \left. \begin{array}{l} \sum_{i=0}^0 q^i = \frac{1-q^{0+1}}{1-q} \quad \checkmark \\ \frac{1-q^{0+1}}{1-q} = \frac{1-q}{1-q} = 1 \end{array} \right\} A(0) \text{ ist wahr!}$$

b) Induktionsgesch.

$$\text{Induktionsvor.: } A(k) \text{ ist wahr, d.h. } \sum_{i=0}^k q^i = \frac{1-q^{k+1}}{1-q}$$

das darf beim Beweis als wahr benutzt werden

Induktionssch.:  $A(k+1)$  ist wahr, d.h.

$$\sum_{i=0}^{k+1} q^i = \frac{1-q^{(k+1)+1}}{1-q} = \frac{1-q^{k+2}}{1-q} \quad \checkmark$$

das muss im Beweis gezeigt (nahegeordnet) werden

Beweis:

$$\sum_{i=0}^{k+1} q^i = \left( \sum_{i=0}^k q^i \right) + q^{k+1}$$

Induktionsvor.

$$\begin{aligned}
 &= \frac{1-q^{k+1}}{1-q} + q^{k+1} \\
 &= \frac{1-q^{k+1} + (1-q)q^{k+1}}{1-q} \\
 &= \frac{1-q^{k+1} + q^{k+1} - q^{k+2}}{1-q} = \frac{1-q^{k+2}}{1-q} \quad \checkmark
 \end{aligned}$$

"Anwendungen": a)  $\sum_{i=1}^n q^i = \left( \sum_{i=0}^n q^i \right) - q^0 = \frac{1-q^{n+1}}{1-q} - 1$

$$= \frac{1-q^{n+1} - (1-q) \cdot 1}{1-q}$$

$$= \frac{1-q^{n+1} - 1 + q}{1-q} = \frac{q - q^{n+1}}{1-q} = q \cdot \frac{1-q^n}{1-q}$$

b)  $1 + 2 + 4 + 8 + 16 + \dots + 2^{63} = \sum_{i=0}^{63} 2^i = \frac{1-2^{64}}{1-2} = 2^{64} - 1$

c)  $\sum_{i=5}^{10} \left(\frac{1}{2}\right)^i = \underbrace{\sum_{i=0}^{10} \left(\frac{1}{2}\right)^i}_{\frac{1-(\frac{1}{2})^{11}}{1-\frac{1}{2}}} - \sum_{i=0}^4 \left(\frac{1}{2}\right)^i$   
 $= \frac{1-(\frac{1}{2})^{11}}{1-\frac{1}{2}} - \frac{1-(\frac{1}{2})^5}{1-\frac{1}{2}}$   
 $= 2 \cdot \left(1 - \frac{1}{2^{10}}\right) - 2 \cdot \left(1 - \frac{1}{2^5}\right)$

$$= 2 - \frac{1}{2^{10}} - 2 + \frac{1}{2^4} = \frac{1}{2^4} - \frac{1}{2^{10}} = \frac{1}{16} - \frac{1}{1024}$$

③ A endliche Menge mit  $|A|=n$  Elementen  $\Rightarrow P(A)$  hat  $2^n$  Elemente  
also  $|P(A)| = 2^n$  ( $P(A) = \{B \mid B \subseteq A\}$  Menge aller Teilmengen von A)  
↑ Potenzmenge

Beweis mit vollständiger Induktion:

Induktionsanfang: A hat  $n=1$  Element, also  $A = \{a\}$

$\Rightarrow P(A) = \{\emptyset, \{a\}\} = \{\emptyset, A\}$  mit  $|P(A)| = 2 = 2^1$ ,

die Aussage ist für  $n=1$  wahr!

## Induktionsabschluß:

Induktionsvoraussetzung: Für  $n=k$  ist die Aussage wahr, d.h.

$$|A|=k \text{ Elemente} \Rightarrow |\mathcal{P}(A)| = 2^k \text{ Elemente}$$

das darf beim Beweis als wahr  
verwendet werden

Induktionsbehauptung: Für  $n=k+1$  ist die Aussage ebenfalls wahr, d.h.

$$|A|=k+1 \text{ Elemente} \Rightarrow |\mathcal{P}(A)| = 2^{k+1} \text{ Elemente} \quad \checkmark$$

das muss im Beweis nachgezeichnet/beweisen werden

### Beweis:

$$A = \{a_1, a_2, \dots, a_{k+1}\} \quad A \text{ hat } k+1 \text{ Elemente}$$

$$\mathcal{P}(A) = \{B \mid B \subseteq A\} = \left\{ \tilde{B} \mid \tilde{B} \subseteq A \wedge (a_{k+1} \notin \tilde{B}) \right\} \cup \left\{ \tilde{B} \cup \{a_{k+1}\} \mid \tilde{B} \in M_1 \right\}$$

alle Teilmengen von  
A, die das Element  
 $a_{k+1}$  nicht enthalten

$$\longrightarrow M_1$$

$M_2$   
Teilmengen von A,  
die  $a_{k+1}$  enthalten

$$|\mathcal{P}(A)| = |M_1| + |M_2| = 2 \cdot |M_1| \quad \text{denn } M_2 \text{ enthält alle } \tilde{B} \text{ aus } M_1,$$

vereinigt mit  $\{a_{k+1}\}$  und keine  
weiteren Teilmengen von A

In  $M_1$  sind alle Teilmengen von  $A \setminus \{a_{k+1}\}$ , es gilt  $|A \setminus \{a_{k+1}\}| = k$

$$\Rightarrow |M_1| = |\mathcal{P}(A \setminus \{a_{k+1}\})| = 2^k$$

$$\text{insgesamt: } |\mathcal{P}(A)| = 2 \cdot 2^k = 2^{k+1} \quad \checkmark$$

↓ "Rückgriff" auf vorherige Gegebenheit

## Definition durch Rekursion

Die Zahlen  $a_n \in \mathbb{R}$  sind für alle  $n \in \mathbb{N}$  bzw. für alle  $n \in \mathbb{N}_0$  definiert,  
wenn man angibt, dass

- Definition durch Rekursion
- 1. Anker/Anfang:  $a_1$  bzw.  $a_0$  ist gegeben
  - 2. Bildungsgesetz:  $a_{n+1} = f(a_n)$ ,  $a_{n+1} = f(a_n, a_{n-1}, \dots, a_0)$   
mit Funktionsvorschrift  $f$  für  $n \geq 1$  bzw.  $n \geq 0$

## Beispiele für Definition durch Rekursion

↓ lies: n Fakultät

① Fakultät von n für  $n \in \mathbb{N}_0$  (geschrieben als  $n!$ )

$$\text{Anker: } 0! = 1$$

$$\text{Bildungsgesetz: } (n+1)! = (n+1) \cdot n!$$

$$a_{n+1} = f(a_n) = (n+1) \cdot a_n$$

Konkret:

$$0! = 1$$

$$1! = 1 \cdot 0! = 1 \cdot 1 = 1$$

$$2! = 2 \cdot 1! = 2 \cdot 1$$

$$3! = 3 \cdot 2! = 3 \cdot 2 \cdot 1$$

$$4! = 4 \cdot 3! = 4 \cdot 3 \cdot 2 \cdot 1$$

insgesamt

$n!$  ist das Produkt der ersten n natürlichen Zahlen:

$$n! = 1 \cdot 2 \cdot 3 \cdot 4 \cdots n$$

② Die Folge  $x_0, x_1, x_2, \dots = (x_n)_{n \in \mathbb{N}}$  von Zahlen ist definiert durch

$$\text{Anker: } x_0 = 1, 5 = \frac{3}{2}$$

$$\text{Bildungsgesetz: } x_{n+1} = \frac{1}{2} \left( x_n + \frac{2}{x_n} \right)$$

$$a_{n+1} = f(a_n)$$

$$x_0 = \frac{3}{2}$$

$$x_1 = \frac{1}{2} \left( x_0 + \frac{2}{x_0} \right) = \frac{1}{2} \left( \frac{3}{2} + \frac{2}{\frac{3}{2}} \right) = \frac{1}{2} \left( \frac{3}{2} + \frac{4}{3} \right) = \frac{1}{2} \cdot \frac{9+8}{6} = \frac{17}{12}$$

$$x_2 = \frac{1}{2} \left( x_1 + \frac{2}{x_1} \right) = \frac{1}{2} \left( \frac{17}{12} + \frac{2}{\frac{17}{12}} \right)$$

Es gilt: Je größer  $n$  wird um so besser nähert sich  $x_n$  an  $\sqrt{2}$  an!

	A	B	C	D
$n=0 \rightarrow$	1	1,5	1,41666667	
$n=1 \rightarrow$	2	1,41666667	1,41421569	
$n=2 \rightarrow$	3	1,41421569	1,41421356	
	4	1,41421356	1,41421356	
	5	1,41421356	1,41421356	
	6	1,41421356	1,41421356	
	7	1,41421356	1,41421356	
	8	1,41421356	1,41421356	
	9	1,41421356	1,41421356	
	10	1,41421356	1,41421356	
	11	1,41421356	1,41421356	
	12	1,41421356	1,41421356	
	13	1,41421356	1,41421356	

Berechnung mit EXCEL

Hinweis: Mit  $x_{n+1} = \frac{1}{2} \left( x_n + \frac{a}{x_n} \right)$  für  $a > 0$  bekommt man Näherungen für  $\sqrt{a}$

③ Binomialkoeffizienten für  $k, n \in \mathbb{N}_0$  mit  $k \leq n$

↳ Berechnung  $\binom{n}{k}$  ↪ lies:  $n$  über  $k$   
 Binomialkoeffizient  $n$  über  $k$

Es ist definiert: Anker  $\binom{0}{0} = 1, \binom{n}{0} = 1 \forall n \in \mathbb{N}$

Bildungsgesetz  $\binom{n}{k} = \frac{n}{k} \cdot \binom{n-1}{k-1}$  für  $k, n \in \mathbb{N}$

$$\binom{0}{0} = 1, \binom{n}{0} = 1$$

$$\binom{1}{0} = 1, \binom{1}{1} = \frac{1}{1} \cdot \binom{1-1}{1-1} = 1 \cdot \binom{0}{0} = 1 \cdot 1 = 1$$

$$\binom{2}{0} = 1, \binom{2}{1} = \frac{2}{1} \cdot \binom{2-1}{1-1} = 2 \cdot \binom{1}{0} = 2 \cdot 1 = 2$$

$$\binom{2}{2} = \frac{2}{2} \cdot \binom{2-1}{2-1} = 1 \cdot \binom{1}{1} = 1 \cdot 1 = 1$$

Bildungsgesetz

} diese Rekurrenz liefert alle Binomialkoeffizienten

direkte Definition der Binomialkoeffizienten:

$$\left\{ \begin{array}{l} \binom{0}{0} = 1, \binom{n}{0} = 1 \forall n \in \mathbb{N} \end{array} \right.$$

$$\left\{ \begin{array}{l} \binom{n}{k} = \frac{n!}{k! \cdot (n-k)!} \text{ für } n, k \in \mathbb{N}; k \leq n \end{array} \right.$$

↳ Es folgt sofort:  $\binom{0}{0} = 1, \binom{n}{0} = 1$

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

$$\binom{n}{1} = \frac{n!}{1! \cdot (n-1)!} = \frac{n!}{1 \cdot (n-1)!} = \frac{n \cdot (n-1) \cdot (n-2) \cdot \dots \cdot 3 \cdot 2 \cdot 1}{(n-1) \cdot (n-2) \cdot \dots \cdot 3 \cdot 2 \cdot 1} = n$$

## 8 Vorlesung 8 (21.10.2020)

- 8.1 Binomialkoeffizienten und Fakultät
- 8.2 Eigenschaften Binomialkoeffizient
- 8.3 Pascalsches Dreieck
- 8.4 1. Binomische Formel (+ 1. allgemeine Binomische Formel)
- 8.5 2. Binomische Formel (+ 2. allgemeine Binomische Formel)
- 8.6 Wiederholung: Ordnungsrelation, Vollständige Induktion

Binomialkoeffizienten und Fakultät

Fakultät für Zahlen  $n \in \mathbb{N}_0$ :  $0! = 1$ ,  $\underbrace{n! = n \cdot (n-1)! \text{ für } n \geq 1}$

$$n! = n \cdot (n-1) \cdot (n-2) \cdots 3 \cdot 2 \cdot 1$$

Produkt der natürlichen Zahlen von 1 bis  $n$

Binomialkoeffizient  $\binom{n}{k}$  :  $\binom{0}{0} = 1$ ,  $\binom{n}{0} = 1 \quad \forall n \in \mathbb{N}$

$\binom{n}{k} = \frac{n!}{k! \cdot (n-k)!}$  für  $n \geq 1, k \leq n$

↑  
n über k  
 $k \leq n$

Beispiele:

$$\textcircled{1} \quad \binom{0}{0} = 1, \quad \binom{n}{0} = 1, \quad \binom{n}{n} = \frac{n!}{n! \cdot (n-n)!} = \frac{n!}{n! \cdot 0!} = \frac{n!}{n!} = 1$$

$$\textcircled{2} \quad \binom{6}{2} = \frac{6!}{2! \cdot (6-2)!} = \frac{6!}{2! \cdot 4!} = \frac{\cancel{1 \cdot 2} \cdot \cancel{3 \cdot 4} \cdot \cancel{5} \cdot \cancel{6} \cdot 4!}{\cancel{2!} \cdot \cancel{4!}} = \frac{6 \cdot 5}{1 \cdot 2} = 15$$

$$\binom{11}{3} = \frac{11!}{3! \cdot (11-3)!} = \frac{11!}{3! \cdot 8!} = \frac{\cancel{1 \cdot 2 \cdot 3} \cdot \cancel{4 \cdot 5 \cdot 6 \cdot 7 \cdot 8!}}{\cancel{3!}} = \frac{11 \cdot 10 \cdot 9 \cdot \cancel{8!}}{1 \cdot 2 \cdot \cancel{8!}} = 165$$

(3) allgemein:

$$\binom{n}{k} = \frac{n!}{k! \cdot (n-k)!} = \frac{n \cdot (n-1) \cdot (n-2) \cdots (n-(k-1))}{1 \cdot 2 \cdot 3 \cdots k} = \frac{n \cdot (n-1) \cdot (n-2) \cdots (n-k+1)}{1 \cdot 2 \cdot 3 \cdots k}$$

Weitere Eigenschaften der Binomialkoeffizienten

① Symmetrie: Es gilt  $\binom{n}{k} = \binom{n}{n-k}$

② Additivität:  $\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k}$  ✓

Beweis (durch Nachrechnen)

$$\textcircled{1} \quad \binom{n}{n-k} = \frac{n!}{(n-k)! \cdot (n-(n-k))!} = \frac{n!}{(n-k)! \cdot (\cancel{n-n+k})!} = \frac{n!}{(n-k)! \cdot k!} = \binom{n}{k}$$

$$\textcircled{2} \quad \binom{n}{k-1} + \binom{n}{k} = \frac{n!}{(k-1)! \cdot (n-(k-1))!} + \frac{n!}{k! \cdot (n-k)!}$$

Brüche zur Addition gleichnamig machen,  
d.h. auf den gleichen Nenner bringen (Hauptnenner)

$$\begin{aligned}
 &= \frac{n!}{(k-1)! \cdot (n-k+1)!} + \frac{n!}{k! \cdot (n-k)!} \\
 &= \frac{k \cdot n!}{k \cdot (k-1)! \cdot (n-k+1)!} + \frac{n! \cdot (n-k+1)}{k! \cdot (n-k)! \cdot (n-k+1)!} \\
 &= \frac{k \cdot n! + n! \cdot (n-k+1)}{k! \cdot (n-k+1)!} \\
 &= \frac{n! \cdot [k + (n-k+1)]}{k! \cdot (n+1 - k)!} \\
 &= \frac{n! \cdot (n+1)!}{k! \cdot ((n+1) - k)!} = \frac{(n+1)!}{k! \cdot ((n+1) - k)!} = \binom{n+1}{k} \checkmark
 \end{aligned}$$

Was leisten Binomialkoeffizienten?

Rechenregeln in  $\mathbb{N}_0$

Name	Addition (+)	Multiplikation (·)
Kommutativgesetz	$a + b = b + a$	$a \cdot b = b \cdot a$
Assoziativgesetz	$a + (b + c) = (a + b) + c$	$a \cdot (b \cdot c) = (a \cdot b) \cdot c$
Existenz neutraler Elemente	$a + 0 = a$	$a \cdot 1 = a$
Distributivgesetze	$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$	$(a + b) \cdot c = (a \cdot c) + (b \cdot c)$

$$\mathbb{Z} = \mathbb{N}_0 \cup \{ \dots -5, -4, -3, -2, -1 \} = \{ \dots -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, \dots \}$$

Rechenregeln in  $\mathbb{Z}$

Name	Addition (+)	Multiplikation (·)
Kommutativgesetz	$a + b = b + a$	$a \cdot b = b \cdot a$
Assoziativgesetz	$a + (b + c) = (a + b) + c$	$a \cdot (b \cdot c) = (a \cdot b) \cdot c$
Existenz neutraler Elemente	$a + 0 = a$	$a \cdot 1 = a$
Distributivgesetze	$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$	$(a + b) \cdot c = (a \cdot c) + (b \cdot c)$
<u>neu</u> $\rightarrow$ Existenz additiv inv. Elemente	$a + (-a) = 0$	$\leftarrow$ neu

$$\mathbb{Q} = \left\{ \frac{z}{n} \mid z \in \mathbb{Z} \wedge n \in \mathbb{N} \right\}, z \text{ heißt Zähler, } n \text{ heißt Nenner}$$

$n \in \mathbb{N} \Rightarrow 0$  ist als Nenner verboten: Durch 0 kann man nicht teilen!

Rechenregeln in  $\mathbb{Q}$

Name	Addition (+)	Multiplikation (·)
Kommutativgesetz	$a + b = b + a$	$a \cdot b = b \cdot a$
Assoziativgesetz	$a + (b + c) = (a + b) + c$	$a \cdot (b \cdot c) = (a \cdot b) \cdot c$
Existenz neutraler Elemente	$a + 0 = a$	$a \cdot 1 = a$
Distributivgesetze	$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$	$(a + b) \cdot c = (a \cdot c) + (b \cdot c)$
<u>neu</u> $\rightarrow$ Existenz inverser Elemente	$a + (-a) = 0$	$a \cdot \frac{1}{a} = a \cdot a^{-1} = 1, a \neq 0$ $\leftarrow$ neu

Wir berechnen für  $a, b \in \mathbb{Q}$

$$(a+b)^2 = (a+b) \cdot (a+b)$$

Distributivgesetz  $\rightarrow (a+b) \cdot a + (a+b) \cdot b$

$$\underline{\quad} \Rightarrow a^2 + b \cdot a + a \cdot b + b^2$$

Kommutativgesetz  $\rightarrow a^2 + \underline{a \cdot b + a \cdot b} + b^2 = a^2 + 2a \cdot b + b^2$

Distributivgesetz  $a \cdot b \cdot \frac{(1+1)}{2}$

Die oben angegebenen Rechenregeln liefern die

1. Binomische Formel  $(a+b)^2 = a^2 + 2ab + b^2$

Damit erhält man auch die „Binomische Formel“ für  $(a+b)^3$ , nämlich

$$(a+b)^3 = (a+b) \cdot (a+b)^2$$

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

Anwendung  
der Rechenregeln  $\rightarrow a^3 + \underline{2a^2b} + \underline{ab^2} + \underline{b \cdot a^2} + \underline{2ab^2} + b^3$

$$= a^3 + 3a^2b + 3ab^2 + b^3 \checkmark$$

Binomialkoeffizienten  
sind Faktoren in  
den Binomischen  
Formeln!

$$(a+b)^2 = a^2 + 2ab + b^2 = 1 \cdot a^2 + 2 \cdot a \cdot b + 1 \cdot b^2$$



$$= \binom{2}{0} \cdot a^2 + \binom{2}{1} \cdot a \cdot b + \binom{2}{2} b^2$$

$$= \binom{2}{0} \cdot a^{2-0} \cdot b^0 + \binom{2}{1} a^{2-1} \cdot b^1 + \binom{2}{2} a^{2-2} \cdot b^2$$

$$= a^2$$

$$= \sum_{k=0}^2 \binom{2}{k} a^{2-k} \cdot b^k$$

Behauptung:  $(a+b)^3 = \sum_{k=0}^3 \binom{3}{k} a^{3-k} \cdot b^k$

Wir rechnen aus

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

$$\binom{3}{1} = 3$$

$$\binom{3}{2} \stackrel{\text{Symmetrie}}{=} \binom{3}{3-2} = \binom{3}{1} = 3$$

$$\Rightarrow \binom{3}{0} a^3 \cdot b^0 + \binom{3}{1} a^2 \cdot b^1 + \binom{3}{2} a \cdot b^2 + \binom{3}{3} a^0 \cdot b^3$$

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

$$= a^3 + 3a^2b + 3ab^2 + b^3 \checkmark$$

Allgemein gilt:

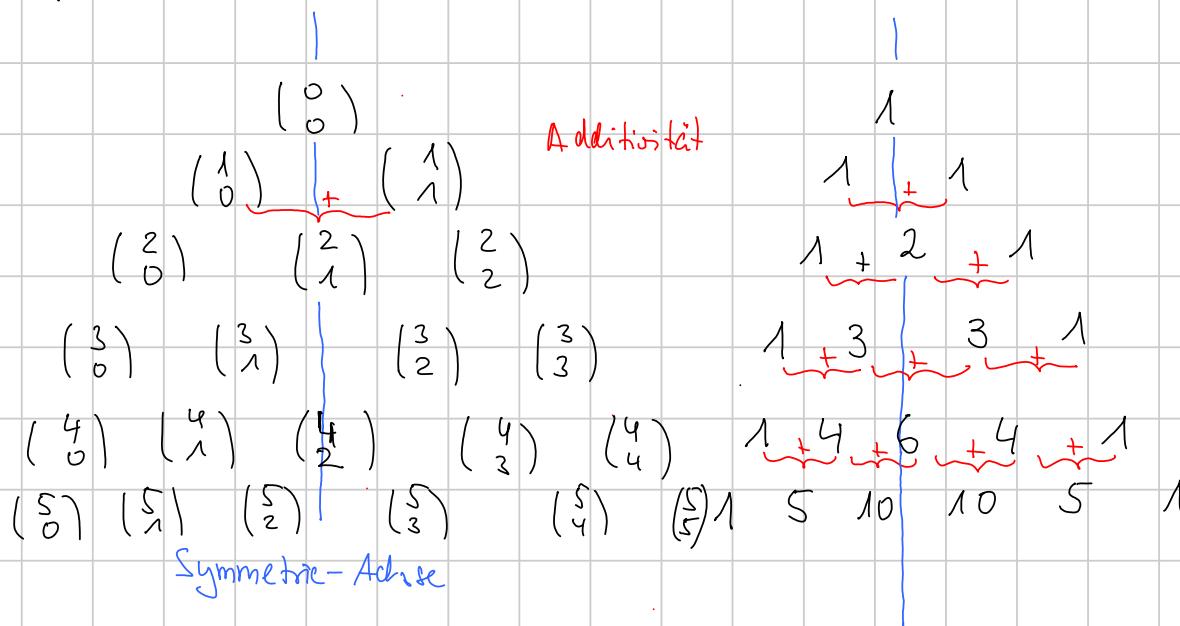
Satz (allgemeine binomische Formel):  $(a+b)^n = \sum_{k=0}^n \binom{n}{k} a^{n-k} \cdot b^k$

$$(a+b)^n = \sum_{k=0}^n \binom{n}{k} a^{n-k} \cdot b^k \quad \text{für } n \geq 2$$

Potenzen von  $a$  „runterzählen“ ↑ Potenzen von  $b$  „raufzählen“ ↑

Ausnutzen der Symmetrie und Additivität der Binomialkoeffizienten

↳ liefert das **Pascalsche Dreieck**



$$(a+b)^5 = a^5 + 5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4 + b^5$$

2. binomische Formel aus der Schule:  $(a-b)^2 = a^2 - 2ab + b^2$

Wie bekommt man allgemein  $(a-b)^n$  für  $n \geq 2$ ?

Wir wissen

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

$$\Rightarrow (a-b)^n = (a+(-b))^n = \sum_{k=0}^n \binom{n}{k} a^{n-k} \cdot \underbrace{(-b)^k}_{=(-1)^k \cdot b^k}$$

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

„Vorzeichen“ ist abwechselnd + und -  
alternierendes Vorzeichen

alternierende Summe

## Satz (allgemeine 2. binomische Formel)

$$(a-b)^n = \sum_{k=0}^n (-1)^k \binom{n}{k} a^{n-k} \cdot b^k, \quad n \geq 2$$

Vorschau auf die nächste Vorlesung: Was ist mit der sog. 3. binomischen Formel  $(a-b)(a+b) = a^2 - b^2$ ?

"Wiederholung": Ordnungsrelation, Beispiel zur vollständigen Induktion

① A Menge,  $A \neq \emptyset$ ; die zweistellige Relation  $R \subseteq A \times A$  heißt  
Ordnungsrelation, falls gilt:

a) R ist reflexiv, also  $(a,a) \in R \quad \forall a \in A$

b) R ist transitiv, also  $(a,b) \in R \wedge (b,c) \in R \Rightarrow (a,c) \in R$

c) R ist antisymmetrisch, also  $(a,b) \in R \wedge (b,a) \in R \Rightarrow a = b$

② Die Relation  $R \subseteq \mathbb{N} \times \mathbb{N}$  ist gegeben durch

$$(a,b) \in R \Leftrightarrow \underbrace{\exists k \in \mathbb{N}: b = k \cdot a}$$

d.h. a ist ein (echter) Teiler von b

oder b ist ein Vielfaches von a

Man schreibt statt  $(a,b) \in R$  auch  $a | b$

↑ liest: teilt

$R \subseteq \mathbb{N} \times \mathbb{N}$  ist eine Ordnungsrelation

a) reflexiv:  $a = 1 \cdot a \quad \forall a \in \mathbb{N} \Rightarrow a | a$  also  $(a,a) \in R$

b) transitiv:  $(a,b) \in R \wedge (b,c) \in R \Rightarrow a | b \wedge b | c$

$$\Rightarrow \exists k \in \mathbb{N}: \underbrace{b = k \cdot a}_{\in \mathbb{N}} \wedge \exists l \in \mathbb{N}: c = l \cdot b$$

$$\Rightarrow c = l \cdot b = l \cdot (k \cdot a) = \underbrace{(l \cdot k)}_{\in \mathbb{N}} \cdot a$$

$$\Rightarrow c = m \cdot a \text{ für } m = l \cdot k \in \mathbb{N} \Rightarrow a | c \Rightarrow (a,c) \in R$$

c) antisymmetrisch:  $(a,b) \in R \wedge (b,a) \in R$

$$\Rightarrow \exists k \in \mathbb{N}: b = k \cdot a \wedge \exists l \in \mathbb{N}: a = l \cdot b$$

$$\Rightarrow b = k \cdot a = k \cdot (l \cdot b) = (k \cdot l) \cdot b$$

$$\Rightarrow b = (k \cdot l) \cdot b \text{ mit } k, l \in \mathbb{N}$$

$$\Rightarrow k \cdot l = 1 \text{ mit } k, l \in \mathbb{N}$$

$$\Rightarrow k=1 \wedge l=1 \Rightarrow b = 1 \cdot a = a \wedge a = 1 \cdot b = b \Rightarrow a = b$$

③ Beweisen Sie mit vollständiger Induktion, dass gilt:

$$7 \mid 2^{3n} - 1 \quad \forall n \in \mathbb{N}$$

Induktionsanfang:  $n=1$

$$2^{3 \cdot 1} - 1 = 2^3 - 1 = 8 - 1 = 7 = 1 \cdot 7 \Rightarrow 7 \mid 7 = 2^3 - 1$$

für  $n=1$  ist die Behauptung wahr!

Induktionsschluß:

Induktionsvor: Die Behauptung ist wahr für  $n=k$ , also

$$7 \mid 2^{3k} - 1 \Rightarrow \exists l \in \mathbb{N}: 2^{3k} - 1 = 7 \cdot l$$

das darf beim Beweis als wahre Aussage benutzt werden!

Induktionsbehauptung: Die Behauptung ist wahr für  $n=k+1$ , also

$$7 \mid 2^{3(k+1)} - 1 \Rightarrow \exists m \in \mathbb{N}: 2^{3(k+1)} - 1 = 7 \cdot m \quad \checkmark$$

das muss gezeigt werden!

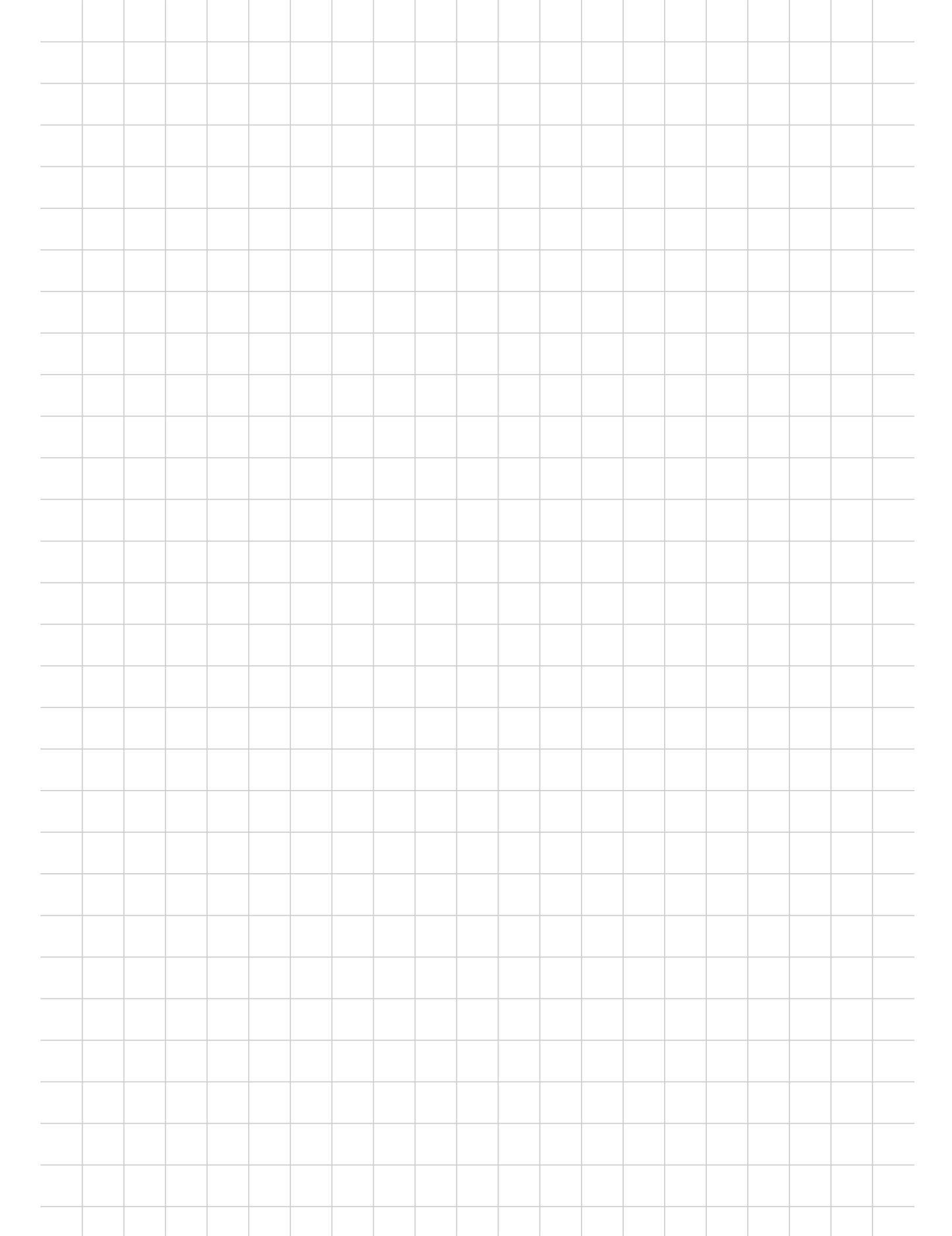
Beweis:

$$\begin{aligned} 2^{3(k+1)} - 1 &= 2^{3k+3} - 1 \\ &= \underbrace{2^{3k} \cdot 2^3 - 1}_{(2^{3k} - 1 + 1) \cdot 2^3 - 1} \\ &= (2^{3k} - 1) \cdot 2^3 + 1 \cdot 2^3 - 1 \\ &= \underbrace{(2^{3k} - 1)}_{(2^{3k} - 1) \cdot 2^k + 7} \cdot 2^k + 7 \end{aligned}$$

Induktionsvor:

$$2^{3k} - 1 = 7 \cdot l \quad \checkmark \quad = 7 \cdot l \cdot 2^k + 7 = 7 \cdot \underbrace{(2^k \cdot l + 1)}_{m} = 7 \cdot m$$

$$\Rightarrow 2^{3(k+1)} - 1 = 7 \cdot m \text{ für ein } m \in \mathbb{N} \Rightarrow 7 \mid 2^{3(k+1)} - 1 \quad \checkmark$$



## 9 Vorlesung 9 (26.10.2020)

**9.1 Rechenregeln für Potenzen**

**9.2 3. Binomische Formel (+ 3. allgemeine Binomische Formel)**

**9.3 Elementares Multiplikationsprinzip**

**9.4 Elementare Kombinatorik (Anordnung, Auswahl)**

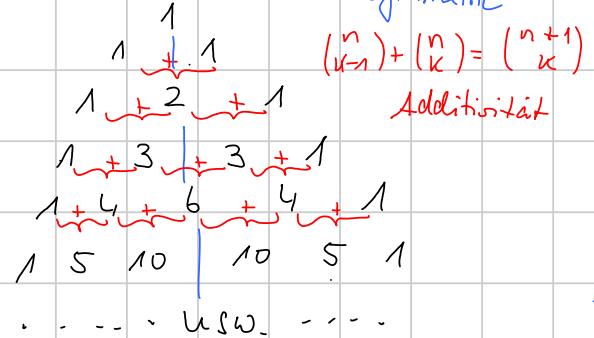
## Verallgemeinerte binomische Formeln

$$(a+b)^2 = a^2 + 2ab + b^2 \rightarrow (a+b)^n = \sum_{k=0}^n \binom{n}{k} a^{n-k} \cdot b^k$$

$$(a-b)^2 = a^2 - 2ab + b^2 \rightarrow (a-b)^n = \sum_{k=0}^n (-1)^k \cdot \binom{n}{k} a^{n-k} \cdot b^k$$

$\left| \begin{matrix} \binom{n}{k} = \binom{n}{n-k} \\ \text{Symmetrie} \end{matrix} \right.$

Binomialkoeffizienten → Pascal'sches Dreieck

"3. binomische Formel"

$$(a-b) \cdot (a+b) = a^2 - b^2 \rightarrow a \neq b: \frac{a^2 - b^2}{a-b} = a+b$$

Gibt es eine Formel für  $\frac{a^n - b^n}{a-b} = ?$ Für  $a \neq b$  gilt:

$$\begin{aligned} \frac{a^n - b^n}{a-b} &= \frac{a^n \cdot \left(1 - \frac{b^n}{a^n}\right)}{a \cdot \left(1 - \frac{b}{a}\right)} \\ &= a^{n-1} \cdot \frac{1 - \left(\frac{b}{a}\right)^n}{1 - \frac{b}{a}} \end{aligned}$$

7. Vorlesung

$$\frac{b}{a} = q$$

$$a+b \Rightarrow q \neq 1$$

$$= a^{n-1} \cdot \left( \sum_{i=0}^{n-1} q^i \right)$$

$$= a^{n-1} \cdot \left( \sum_{i=0}^{n-1} \left(\frac{b}{a}\right)^i \right)$$

$$= \sum_{i=0}^{n-1} a^{n-1} \cdot \left(\frac{1}{a}\right)^i \cdot b^i$$

$$\sum_{i=0}^{n-1} q^i = 1 + q + q^2 + q^3 + \dots + q^{n-1} = \frac{1-q^n}{1-q}$$

Rechenregeln für Potenzen:  $a, b \in \mathbb{R}, n \in \mathbb{N}$ 

$$a^n \cdot a^k = a^{n+k}$$

$$\frac{1}{a} = a^{-1} \quad \text{für } a \neq 0, \quad \frac{1}{a^n} = a^{-n}$$

$$\left(\frac{a}{b}\right)^n = \frac{a^n}{b^n} = a^n \cdot b^{-n}$$

$$\frac{a^n}{a^k} = a^n \cdot a^{-k} = a^{n-k}$$

$$(a \cdot b)^n = a^n \cdot b^n$$

$$(a^n)^k = a^{n \cdot k}$$

$$a^0 = 1 \quad \forall a \in \mathbb{R}, a \neq 0$$

( $0^0$  ist nicht definiert)

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

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

Insgesamt bekommt man die „verallgemeinerte 3. binomische Formel“

$$\frac{a^n - b^n}{a - b} = \sum_{i=0}^{n-1} a^{n-1-i} \cdot b^i ; \quad a \neq b$$

$$a^n - b^n = (a - b) \cdot \left( \sum_{i=0}^{n-1} a^{n-1-i} \cdot b^i \right) \quad \forall a, b \in \mathbb{R}$$

Beispiel:

$$\frac{x^6 - 64}{x - 2} = \frac{x^6 - 2^6}{x - 2} \stackrel{\text{Formel mit } a=x, b=2, n=6}{=} \sum_{i=0}^5 x^{5-i} \cdot 2^i$$

$$= x^5 + 2x^4 + 4x^3 + 8x^2 + 16x + 32$$

Weitere „Anwendungen“ von Fakultät und Binomialkoeffizienten:

### Elementare Kombinatorik

→ Lehre von der Anzahl der Möglichkeiten

endliche Mengen anzordnen oder Auswählen  
von Elementen zu treffen

### Elementares Multiplikationsprinzip

1) Gegeben sind die Menge  $A_1$  mit  $n_1 = |A_1|$  Elementen und

die Menge  $A_2$  mit  $n_2 = |A_2|$  Elementen  $\Rightarrow$

$A_1 \times A_2 = \{(a_1, a_2) \mid a_1 \in A_1 \wedge a_2 \in A_2\}$  hat  $n_1 \cdot n_2$  Elemente, also

$$|A_1 \times A_2| = |A_1| \cdot |A_2|$$

2) Gegeben sind die Mengen  $A_i$  mit  $n_i = |A_i|$  Elementen,  $1 \leq i \leq N \Rightarrow$

$A_1 \times A_2 \times \dots \times A_N = \{(a_1, a_2, \dots, a_N) \mid a_i \in A_i, 1 \leq i \leq N\}$  hat  $n_1 \cdot n_2 \cdots n_N$

Elemente, also

$$|A_1 \times A_2 \times \dots \times A_N| = |A_1| \cdot |A_2| \cdot |A_3| \cdots |A_N|$$

Beispiel:  $H = \{h_1, h_2, h_3\}$  Menge mit drei verschiedenen Hosen

$T = \{t_1, t_2, t_3, t_4\}$  Menge mit vier verschiedenen T-Shirts

$S = \{s_1, s_2\}$  Menge mit zwei verschiedenen Paaren Schuhe

$$\Rightarrow H \times T \times S = \{(h, t, s) \mid h \in H \wedge t \in T, s \in S\}$$

Menge der möglichen „Kombinationen“ von Hose, T-Shirt, Schuh

$$\Rightarrow |H \times T \times S| = |H| \cdot |T| \cdot |S| = 3 \cdot 4 \cdot 2 = 24$$

① Anordnung: a)  $k$  von  $n$  Elementen ( $k \leq n$ ) werden mit Beachtung der Reihenfolge angeordnet; (Anordnung  $\rightarrow$  ohne Wiederholung!)

Anzahl möglicher Anordnungen ist  $n \cdot (n-1) \cdot (n-2) \cdots (n-k+1)$

$$= \frac{n!}{(n-k)!}$$

Anzahl möglicher Besetzung  $\rightarrow$   $n \quad n-1 \quad n-2 \quad \dots \quad n-k+1$

Plätze  $\rightarrow P_1 \quad P_2 \quad P_3 \quad \dots \quad P_k$   $\leftarrow$  numerische Reihenfolge

$\underbrace{\quad}_{(n-k+1)} \quad \underbrace{\quad}_{(n-k+1)} \quad \underbrace{\quad}_{(n-k+1)} \quad \dots$

$$\frac{n!}{(n-k)!} = \frac{n \cdot (n-1) \cdot (n-2) \cdots (n-k+1) \cdot \cancel{(n-k) \cdot (n-k-1) \cdots 3 \cdot 2 \cdot 1}}{\cancel{(n-k) \cdot (n-k-1) \cdots 3 \cdot 2 \cdot 1}} = n \cdot (n-1) \cdot (n-2) \cdots (n-k+1)$$

b) Wenn man  $n$  von  $n$  Elementen mit Reihenfolge ordnet, nennt man dies Permutation von  $n$  Elementen; die Anzahl der Permutationen ist  $n!$  (Formel von oben mit  $k=n$  liefert)

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

c) Anordnung von  $n$  aus  $n$  Elementen, wobei es Gruppen gleicher

Elemente gibt:  $n_1$  Elemente vom Typ 1 ( $T_1$ )

$n_2$  Elemente vom Typ 2 ( $T_2$ )

$\vdots$  Elemente vom Typ  $k$  ( $T_k$ )

$n_1 + n_2 + \dots + n_k \leq n$

Es gibt

$n!$

Die Elemente in den Mengen  $T_i$  sind ununterscheidbar

$\frac{n!}{n_1! \cdot n_2! \cdots n_k!}$  mögliche Anordnungen

Bsp. KAMPMANN  $\rightarrow$

$n=8$	$T_1 = \{K\}, n_1=1$	}
	$T_2 = \{A, A\}, n_2=2$	
	$T_3 = \{M, M\}, n_3=2$	
	$T_4 = \{P\}, n_4=1$	
	$T_5 = \{N, N\}, n_5=2$	

$$n_1 + n_2 + n_3 + n_4 + n_5 = P$$

Diese 8 Buchstaben des Namens KAMPMANN, kann man auf

$$\frac{8!}{2 \cdot 2 \cdot 2} = \frac{8 \cdot 7!}{8} = 7! = 5040$$

alle Buchstaben unterscheidbar  
 bei unterschiedlichen A's  
 bei unterschiedlichen N's  
 bei unterschiedlichen M's

KAMPMANN  
 KAMP M ANN  
 KAM PM ANN  
 KAMPM ANN

2 Möglichkeiten  
 2 Möglichkeiten  
 1 Möglichkeit

② Auswahl von  $K$  aus  $n$  Elementen (Reihenfolge spielt keine Rolle)

mit Reihenfolge  $\rightarrow \frac{n!}{(n-k)!}$  Mögliche Anordnungen von  $K$  Elementen aus  $n$   
 diese  $K$  Elemente können auf  $K!$  Arten  
 umsortiert werden; Reihenfolge spielt keine  
 Rolle, d.h. alle diese  $K!$  Umsortierungen  
 ergeben nur  $1$  Möglichkeit

$$\frac{n!}{(n-k)! k!} = \binom{n}{k} \leftarrow \text{ohne Reihenfolge}$$

Aus  $n$  Elementen kann man ohne Beachtung der Reihenfolge auf  $\binom{n}{k}$   
 verschiedene Arten  $K$  Elemente auswählen ( $k \leq n$ ).

D.h. und:

Eine Menge  $M$  mit  $n$  Elementen hat  $\binom{n}{k}$  Teilmengen mit  $K$  Elementen,  
 denn die Teilmenge mit  $K$  Elementen geschieht durch Auswahl von  $K$  aus  
 $n$  Elementen ohne Beachtung der Reihenfolge!

M mit  $|M|=n \Rightarrow |P(M)| = 2^n$ , d.h. M hat  $2^n$  Teilmengen  
 M hat Teilmengen mit 0 Elementen  $\rightarrow \emptyset$  genau  $1 = \binom{n}{0}$

$\left\{ \begin{array}{l} M \text{ hat Teilmenge mit 1 Element} \rightarrow \binom{n}{1} = n; \{m_1\}, \{m_2\}, \dots, \{m_n\} \\ M \text{ hat Teilmenge mit } k \text{ Elementen} \rightarrow \binom{n}{k} \end{array} \right.$

→ zusammen  $2^n = \sum_{k=0}^n \binom{n}{k} = \binom{n}{0} + \binom{n}{1} + \dots + \binom{n}{n-1} + \binom{n}{n}$

Anzahl aller  $\uparrow$   $\uparrow$  Anzahl der  $k$ -Elementigen Teilmengen  
 Teilmengen  $k=0, 1, 2, \dots, n$

Bemerkung:  $2^n = \sum_{k=0}^n \binom{n}{k}$  — Herleitung über Kombinatorik

$$2^n = (1+1)^n = \sum_{k=0}^n \binom{n}{k} \underbrace{1^{n-k}}_{=1} \cdot \underbrace{1^k}_{=1} = \sum_{k=0}^n \binom{n}{k} \cdot 1 \cdot 1 = \sum_{k=0}^n \binom{n}{k}$$

$(a+b)^n$  mit  $a=1$   
 $b=1$

Rechenregeln für endliche Summen  $a_k, b_k \in \mathbb{R}, u \leq k \leq o, s, t \in \mathbb{R}$

$$\sum_{k=u}^o (s \cdot a_k + t \cdot b_k) = s \cdot \left( \sum_{k=u}^o a_k \right) + t \cdot \left( \sum_{k=u}^o b_k \right) \quad \text{← Linearitätsregel}$$

Beispiel: Aus der 6. Voraussetzung  $\sum_{i=0}^n i = \frac{n \cdot (n+1)}{2}$

Aus der 7. Voraussetzung  $\sum_{i=0}^n i^2 = \frac{n(n+1)(2n+1)}{6}$

Mit Hilfe der **Linearität** bekommt man

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

Beweis ohne vollständige Induktion:

$$\begin{aligned} \sum_{i=1}^n (2i-1) &= 2 \cdot \left( \sum_{i=1}^n i \right) - \left( \sum_{i=1}^n 1 \right) \quad \overbrace{\sum_{i=1}^n 1 = \underbrace{1+1+\dots+1}_{n-\text{mal}} = n} \\ &= 2 \cdot \left( \underbrace{\sum_{i=0}^n i}_{\text{ }} \right) - n \end{aligned}$$

6. Voraussetzung  $\Rightarrow 2 \cdot \frac{n(n+1)}{2} - n = n(n+1) - n = n^2 + n - n = n^2 \checkmark$

$$\sum_{i=0}^n (2i^2 - i - 1) = -1 + 0 + 5 + 14 + \dots + (2n^2 - n - 1)$$

$i=0$   $\downarrow$   
 $i=1$   $\downarrow$   
 $i=2$   $\downarrow$   
 $i=3$   $\downarrow$   
 $i=n$   $\downarrow$

Mit Linearität folgt:

$$\begin{aligned}
 \sum_{i=0}^n (2i^2 - i - 1) &= 2 \cdot \underbrace{\left( \sum_{i=0}^n i^2 \right)}_1 - \underbrace{\left( \sum_{i=0}^n i \right)}_1 - \sum_{i=0}^n 1 \\
 \text{6. 17. Volesung} \quad \Downarrow &= 2 \cdot \frac{n(n+1)(2n+1)}{6} - \frac{n(n+1)}{2} - (n+1) \\
 &= \frac{n(n+1)(2n+1)}{3} - \frac{n(n+1)}{2} - (n+1) \\
 &= \frac{2n(n+1)(2n+1) - 3n(n+1) - 6(n+1)}{6} \\
 &= \frac{(n+1) \cdot [2n(2n+1) - 3n - 6]}{6} \\
 &= \frac{(n+1) \cdot [4n^2 - n - 6]}{6}
 \end{aligned}$$

## 10 Vorlesung 10 (27.10.2020)

**10.1 Zusammenfassung Elementare Kombinatorik**

**10.2 Dezimaldarstellung rationaler Zahlen**

**10.3 Rechenregeln in den reellen Zahlen**

**10.4 Bemerkung: Was ist ein Körper, Anordnungsaxiom**

Zusammenfassung der Formeln der elementaren Kombinatorik ( $K \leq n$ )Anordnungen von  $K$  aus  $n$  Elementen  $\leftarrow$  mit ReihenfolgeAuswahl von  $K$  aus  $n$  Elementen  $\leftarrow$  ohne Reihenfolge

	ohne Wiederh.	mit Wiederh.	
Anordnungen	$\frac{n!}{(n-k)!}$	$n^k$	in der Tabelle steht jeweils die Anzahl der Möglichkeiten
Auswahl	$\binom{n}{k}$	$\binom{n+k-1}{k}$	

6 Elemente auf 4 Plätze anordnen mit Wiederholung:

$$6 \cdot 6 \cdot 6 \cdot 6 = 6^4$$

↓ ↓ ↓ ↓



Auswahl von  $6$  aus  $n$  mit Wiederholungen

$n-1$  Striche kennzeichnen  
 $n$  Elemente  $\hat{=}$   $n$  Plätze

bei Auswahl von Element  $i$   
wird am Platz des Elements  $i$   
ein Kreuz eingezeichnet

Bei der Auswahl von  $K$  aus  $n$  Elementen mit Wiederholungen

entsteht ein Muster mit  $n-1$  Strichen und  $K$  Kreuzen, d.h.

es gibt  $n-1+K = n+K-1$  Symbole in dem Muster, von denen  $K$  Kreuze sind, d.h. aus den  $n-1+K$  Symbolen müssen  $K$  für Kreuze ausgewählt werden, das ist Auswahl von  $K$  aus  $n-1+K$  ohne Wiederholungen, also hat man  $\binom{n-1+K}{K} = \binom{n+K-1}{K}$  Möglichkeiten

\* Spzialfälle bei Anordnungen

a) Permutationen  $\hat{=}$  Anordnung von  $n$  aus  $n$  Elementen ( $K=n$ );

es gibt  $n!$  Möglichkeiten

b) Anordnung von  $n$  aus  $n$  Elementen, wobei die  $n$  Elemente in  $k$  Gruppen identischer Elemente (jeweils Anzahl  $n_i$  pro Gruppe,  $1 \leq i \leq k$ ) aufgeteilt sind; es gibt  $\frac{n!}{n_1! \cdot n_2! \cdots n_k!}$  Möglichkeiten

Zahlen im  $\mathbb{Q}$   $\leftarrow$  Menge der rationalen Zahlen

$$\mathbb{Q} = \left\{ \frac{z}{n} \mid z \in \mathbb{Z} \wedge n \in \mathbb{N} \right\}$$

① Darstellung  $\frac{z}{n}$  ist nicht eindeutig;  $z$  und  $n$  können gemeinsame Faktoren enthalten; Eindeutigkeit bekommt man durch vollständiges Kürzen dieser Faktoren

$$z = z_1 \cdot k, \quad n = n_1 \cdot k \Rightarrow \frac{z}{n} = \frac{z_1 \cdot k}{n_1 \cdot k} = \frac{z_1}{n_1}$$

②  $\mathbb{Q}$  ist die Menge aller Brüche  $\frac{z}{n}$ ; Bruchrechnen:  $q_1 = \frac{a}{b}, q_2 = \frac{c}{d}$

$$q_1 \cdot q_2 = \frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d}$$

$$\frac{q_1}{q_2} = \frac{\left(\frac{a}{b}\right)}{\left(\frac{c}{d}\right)} = \frac{a}{b} \cdot \frac{d}{c} = \frac{ad}{bc}$$

$$q_1 + q_2 = \frac{a}{b} + \frac{c}{d} = \frac{ad}{b \cdot d} + \frac{c \cdot b}{d \cdot b} \\ = \frac{ad + c \cdot b}{d \cdot b}$$

| Bemerkung zur Addition

$$\frac{z_1}{n} + \frac{z_2}{n} = \frac{z_1 + z_2}{n}$$

| Addition gleichnamiger Brüche (Nenner gleich)

"Erweitern" der Brüche

③ Dezimaldarstellung rationaler Zahlen

Zahlendarstellung in einem „Stellenwertsystem“ zur Basis 10, z.B.

$$3246 = 3 \cdot 1000 + 2 \cdot 100 + 4 \cdot 10 + 6$$

$$= 3 \cdot 10^3 + 2 \cdot 10^2 + 4 \cdot 10^1 + 6 \cdot 10^0$$

$$= \sum_{i=0}^3 z_i \cdot 10^i \quad \text{mit } z_0 = 6, z_1 = 4, z_2 = 2, z_3 = 3$$

Allgemein:  $(a_n a_{n-1} a_{n-2} \dots a_2 a_1 a_0)_{10} = \sum_{i=0}^n a_i \cdot 10^i$

$$a_i \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}, a_n \neq 0$$

$$23,\overbrace{75}^{\frac{75}{100}} = 2 \cdot 10 + 3 + \underbrace{\frac{7}{10} + \frac{5}{100}}_{\frac{75}{100}} = 2 \cdot 10^0 + 3 \cdot 10^0 + 7 \cdot 10^{-1} + 5 \cdot 10^{-2}$$

allgemein:  $(a_n a_{n-1} a_{n-2} \dots a_2 a_1 a_0, b_1 b_2 \dots b_k)_{10} =$

$$\sum_{i=0}^n a_i \cdot 10^i + \sum_{j=1}^k b_j \cdot 10^{-j}$$

Wie bekommt man aus der Darstellung  $\frac{z}{n} \in \mathbb{Q}$  (also Darstellung als Bruch) die Dezimaldarstellung?  $\rightarrow$  schriftliche Division ganzer Zahlen

$\downarrow$  gesuchte Dezimaldarstellung von  $\frac{3406}{26}$

$$\begin{array}{r} 3406 : 26 = \underline{1}\underline{3}\underline{1} \\ - 26 \\ \hline 806 \\ - 78 \\ \hline 26 \\ - 26 \\ \hline 0 \end{array}$$

$$\left. \begin{array}{l} \leftarrow 3406 = \underline{100} \cdot 26 + \underline{806} \\ \leftarrow 806 = \underline{30} \cdot 26 + 26 \\ \leftarrow 26 = \underline{1} \cdot 26 + 0 \end{array} \right\} \text{Division mit Rest}$$

$$\begin{array}{r} 33 : 6 = 5,5 \\ - 30 \\ \hline 30 \\ - 30 \\ \hline 0 \end{array} \quad \left. \begin{array}{l} \frac{33}{6} = 5,5 \end{array} \right\}$$

unendlich viele Nachkommastellen alle identisch = 3

$$121 : 12 = 10, \overbrace{08333\dots}^{= 10,08\bar{3}} \leftarrow \text{Periodenstiel}$$

$$\begin{array}{r} - 12 \\ \hline 1 \\ - 0 \\ \hline 10 \\ - 0 \\ \hline 100 \\ - 96 \\ \hline 40 \\ - 36 \\ \hline 40 \\ - 36 \\ \hline 40 \\ \vdots \end{array}$$

Lies: 10,083 Periode

Zahlen unter dem Periodenstiel werden

unendlich oft in identischer Anordnung wiederholt

$$\frac{121}{12} = 10,08\bar{3} \leftarrow \text{periodische Dezimalzahl}$$

$\boxed{\mathbb{Q} = \left\{ \frac{z}{n} \mid z \in \mathbb{Z} \wedge n \in \mathbb{N} \right\}}$   $\stackrel{1}{=} \text{Menge aller Dezimalzahlen mit endlichen Nachkommastellen oder periodisch wiederkehrende Nachkommastellen}$

Beispiel:

$$0, \overline{3} = 0,3333\ldots \in \mathbb{Q}$$

$$12,45 \overline{12} = 12,4512121212\ldots \notin \mathbb{Q}$$

} wie bekommt man die Darstellung  $\frac{2}{n}$  ?

$$\begin{aligned} 10x &= 3, \overline{3} = 3,3333\ldots \\ x &= 0, \overline{3} = 0,3333\ldots \end{aligned} \quad \left. \begin{array}{l} \\ \hline \end{array} \right.$$

$$\underline{9x = 3} \Rightarrow x = \frac{3}{9} = \frac{1}{3}$$

$$\begin{aligned} 100x &= 1245, \overline{1212121212} \\ x &= 12,45 \overline{1212121212} \end{aligned} \quad \left. \begin{array}{l} \\ \hline \end{array} \right.$$

$$\underline{99x = 1245,12 - 12,45} \quad \begin{array}{l} \text{Korrekte Variante} \\ \text{Falsche Variante} \end{array}$$

$$\begin{aligned} 10000x &= 124512, \overline{12121212} \\ 100x &= 1245, \overline{121212} \end{aligned} \quad \left. \begin{array}{l} \\ \hline \end{array} \right.$$

$$\begin{aligned} 9900x &= 124512 - 1245 \\ \Rightarrow x &= \frac{124512 - 1245}{9900} \\ &= \frac{123267}{9900} \end{aligned}$$

Zu jedem  $q \in \mathbb{Q}$  gehört ein Punkt auf dem Zahlenstrahl; wir haben aber schon einen weiteren Punkt auf dem Zahlenstrahl gefunden, der zu  $\sqrt{2}$  gehört und  $\sqrt{2} \notin \mathbb{Q} \Rightarrow$  reellen Zahlen  $\mathbb{R}$  mit  $\mathbb{Q} \subset \mathbb{R}$

$\mathbb{R} \triangleq$  Menge aller Decimalzahlen mit endlich vielen Nachkommastellen  
oder mit unendlich vielen aber periodisch wiederkehrenden Nachkommastellen  
oder mit unendlich vielen aber nicht periodisch wiederkehrenden Nachkommastellen

Die "Rechenregeln" in  $\mathbb{R}$  entsprechen den Regeln in  $\mathbb{Q}$ , d.h. es gelten  
die 5 Körperaxiome

Name	Addition (+)	Multiplikation (·)
1) Kommutativgesetz	$a + b = b + a$	$a \cdot b = b \cdot a$
2) Assoziativgesetz	$a + (b + c) = (a + b) + c$	$a \cdot (b \cdot c) = (a \cdot b) \cdot c$
3) Existenz neutraler Elemente	$a + 0 = a$	$a \cdot 1 = a$
4) Distributivgesetze	$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$	$(a + b) \cdot c = (a \cdot c) + (b \cdot c)$
5) Existenz inverser Elemente	$\forall a \exists (-a) : a + (-a) = 0$	$\forall a \neq 0 \exists \frac{1}{a} = a^{-1} : a \cdot \frac{1}{a} = a \cdot a^{-1} = 1$

↑ Symmetriebereich bei  
den Regeln zwischen Addition  
und Multiplikation

### Bemerkung:

- 1) Wenn man auf einer Menge  $M$  eine Rechenoperation  $+$  und eine Rechengaktion  $\cdot$  erklären kann, die diesen 5 Axiomen genügen, nennt man  $(M, +, \cdot)$  einen Körper.
- 2)  $(\mathbb{Q}, +, \cdot)$  und  $(\mathbb{R}, +, \cdot)$  sind Körper!

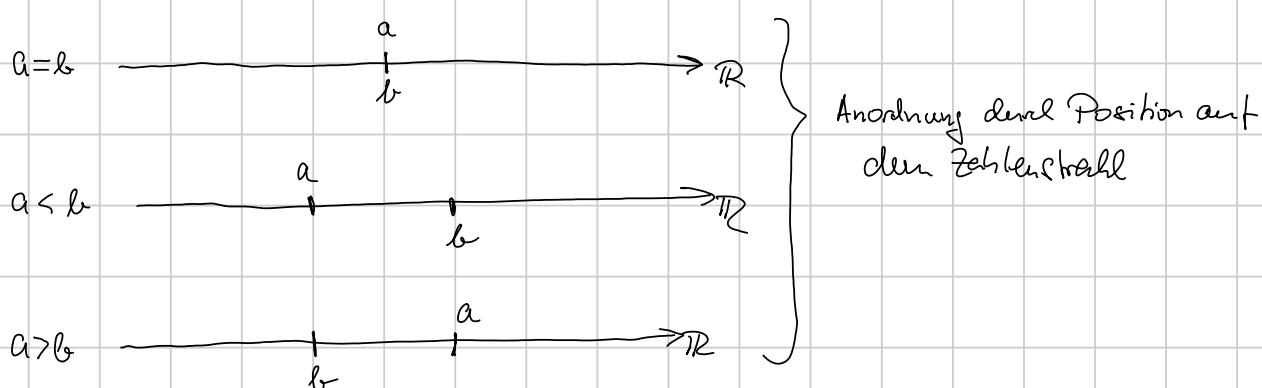
Zu den **5 Körperaxiomen** für  $\mathbb{R}$  (damit auch für  $\mathbb{Q} \subset \mathbb{R}$ ) kommt zusätzlich das **Anordnungsaxiom**, nämlich

Anordnungsaxiom: Für zwei reelle Zahlen  $a, b \in \mathbb{R}$  gilt immer genau eine der folgenden drei Alternativen:

- (1)  $a < b$
- (2)  $a = b$
- (3)  $a > b$

Das Anordnungsaxiom garantiert, dass man zwei reelle Zahlen immer eindeutig in Relation zueinander setzen kann (immer miteinander vergleichen kann mit eindeutigen Ergebnis!)

Auf  $\mathbb{R}$  gibt es zwei Rechenoperationen und die Anordnung.



Wie verhalten sich Anordnung und Rechenoperationen?

$$\text{Es gilt: } a < b \Rightarrow a + c < b + c \quad \forall c \in \mathbb{R}$$

$$a > b \Rightarrow a + c > b + c \quad \forall c \in \mathbb{R}$$

$$a < b \Rightarrow a \cdot c < b \cdot c \quad \forall c \in \mathbb{R} \text{ mit } c > 0$$

$$a > b \Rightarrow a \cdot c > b \cdot c \quad \forall c \in \mathbb{R} \text{ mit } c > 0$$

## 11 Vorlesung 11 (28.10.2020)

**11.1 Rechenregeln der Anordnung**

**11.2 Intervalle als Mengen**

**11.3 unendlich-Symbol**

**11.4 Definition: Term**

**11.5 Definition: Betrag einer reellen Zahl**

**11.6 erste Rechenregeln für den Betrag**

**11.7 Betrag, Ungleichung und Intervalle**

## Anordnung auf $\mathbb{R}$ und Rechenregeln der Anordnung

Anordnung  $\rightarrow$  Position auf dem Zahlenstrahl

Anordnungsaxiom: Für  $a, b \in \mathbb{R}$  gilt immer genau eine der folgenden drei

Alternativen: ①  $a < b$ , ②  $a = b$ , ③  $a > b$

Rechenregeln: Zusammenhang von Rechenoperationen und Anordnung

$$1) \quad a < b \Rightarrow a + c < b + c \quad \forall c \in \mathbb{R}$$

„Addition bewahrt die Anordnung“

$$2) \quad a < b \Rightarrow a \cdot c < b \cdot c \quad \forall c \in \mathbb{R}, c > 0$$

„Multiplikation mit Zahlen  $> 0$  bewahrt Anordnung“

Bemerkung:

$$a) \quad a > b \Leftrightarrow b < a \text{ also und } a > b \Rightarrow a + c > b + c \quad \forall c \in \mathbb{R}$$

$$a > b \Rightarrow a \cdot c > b \cdot c \quad \forall c \in \mathbb{R}, c > 0$$

$$b) \quad a \leq b \Leftrightarrow (a < b) \vee (a = b) \quad \left. \begin{array}{l} \text{die Rechenregeln 1) und 2) gelten} \\ a \geq b \Leftrightarrow (a > b) \vee (a = b) \end{array} \right\} \text{analog für } \leq \text{ und } \geq$$

c)  $\mathbb{R}^+ = \{x \in \mathbb{R} \mid x > 0\}$  ist die Menge der positiven reellen Zahlen

$\mathbb{R}_0^+ = \{x \in \mathbb{R} \mid x \geq 0\}$  ist die Menge der nicht negativen reellen Zahlen

$\mathbb{R}^- = \mathbb{R} \setminus \mathbb{R}_0^+ = \{x \in \mathbb{R} \mid x < 0\}$  ist die Menge der negativen reellen Zahlen

d) Intervalle als Teilmengen von  $\mathbb{R}$ :

Für  $a, b \in \mathbb{R}$  mit  $a < b$  ist definiert

$$\textcircled{1} \quad (a, b) = ]a, b[ = \{x \in \mathbb{R} \mid \underbrace{(a < x) \wedge (x < b)}_{\text{oder}}\} = \{x \in \mathbb{R} \mid \underbrace{a < x < b}_{\text{oder}}\}$$

ist das offene Intervall mit Grenzen  $a$  und  $b$

Es gilt:  $a \notin (a, b)$ ;  $b \notin (a, b)$

②  $[a, b] = \{x \in \mathbb{R} \mid a \leq x \leq b\}$  ist das abgeschlossene Intervall mit Grenzen  $a$  und  $b$ . Es gilt:  $a \in [a, b]$ ;  $b \in [a, b]$

③ Halboffene Intervalle

$$(a, b] = \{x \in \mathbb{R} \mid a < x \leq b\}$$

$$[a, b) = \{x \in \mathbb{R} \mid a \leq x < b\}$$

④ Für  $a=b$  gilt  $(a, b) = (a, a) = \emptyset$ ;  $[a, b] = [a, a] = \{a\}$ ;  
für  $b < a$  ist  $(a, b)$  und  $[a, b]$ ,  $(a, b]$ ,  $[a, b)$  nicht definiert.

c) Abschluss der Anordnung in  $\mathbb{R}$

Zur Vervollständigung der Anordnung definiert man die Symbole  $+\infty$  und  $-\infty$ ; es gilt:

①  $+\infty \notin \mathbb{R}$ ,  $-\infty \notin \mathbb{R} \Rightarrow$  Rechenoperationen für  $+\infty$  und  $-\infty$  sind nicht definiert

②  $\underbrace{\forall x \in \mathbb{R}: (-\infty < x) \wedge (x < +\infty)}$   
in diesem Sinn gilt:  $\mathbb{R} = (-\infty, +\infty)$

Konsequenzen aus den Rechenregeln für die Anordnung

$$a < b \Rightarrow a+c < b+c \quad \forall c \in \mathbb{R}$$

$$a < b \Rightarrow a \cdot c < b \cdot c \quad \forall c \in \mathbb{R}, c > 0$$

1)  $a < 0 \Rightarrow -a > 0$

denn:  $a < 0 \Rightarrow a + (-a) < 0 + (-a) \Rightarrow 0 < -a \Rightarrow -a > 0$

$\uparrow$   
 $c = -a$

analog gilt:  $a > 0 \Rightarrow -a < 0$ ;  $a \leq 0 \Rightarrow -a \geq 0$ ;  $a \geq 0 \Rightarrow -a \leq 0$

2) Für  $a, b$  mit  $a < b$  und  $c < 0$  gilt:  $a < b \Rightarrow a \cdot c > b \cdot c$

Analog gilt:  $a > b$ ,  $c < 0 \Rightarrow a \cdot c < b \cdot c \quad | \quad a \leq b, c < 0 \Rightarrow a \cdot c \geq b \cdot c$   
 $a \geq b$ ,  $c < 0 \Rightarrow a \cdot c \leq b \cdot c \quad | \quad$

denn:  $c < 0 \Rightarrow (-c) > 0$  also  $a < b \Rightarrow a \cdot (-c) < b \cdot (-c)$

$$\Rightarrow -a \cdot c < -b \cdot c \quad | + a \cdot c$$

$$\Rightarrow 0 < a \cdot c - b \cdot c \quad | + b \cdot c$$

$$\Rightarrow b \cdot c < a \cdot c \quad \text{+}$$

Zusammengefasst:  $a < b, c < 0 \Rightarrow a \cdot c > b \cdot c$

### Definition:

- 1) Ein Term besteht aus syntaktisch korrekt gebildeten Wörtern oder Wortgruppen in der formalen Sprache der Mathematik, d.h. ein Term ist ein sinnvoller Ausdruck, der Zahlen, Variablen, Symbole für mathematische Verknüpfungen und Klammern enthalten kann.
- 2) Eine Gleichung ist eine Aussage über die Gleichheit (Äquivalenz) zweier Terme,  $T_1 = T_2$ . Das Symbol  $=$  heißt Gleichheitszeichen.
- 3) Eine Ungleichung ist eine Aussage zum Größenvergleich zweier Terme, z.B.  $T_1 < T_2$ , oder  $T_1 \geq T_2$ . Die Symbole  $<, >, \leq, \geq$  heißen Ungleichheitszeichen.

Definition: (Betrag einer reellen Zahl)

für  $a \in \mathbb{R}$  gilt:

lies: Betrag von  $a$ ,  
oder  $a$  Betrag

$$|a| = \begin{cases} a & \text{falls } a \geq 0 \\ -a & \text{falls } a < 0 \end{cases}$$

aus der Def. des Betrags

folgt:

Wenn man den „Betrag auf-  
löst“ muss man immer zwei  
Fälle betrachten, nämlich

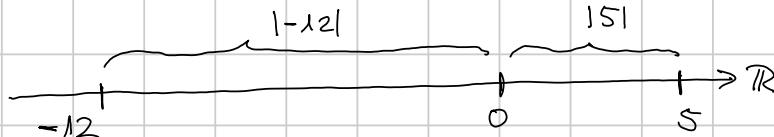
1. Fall: Term im Betrag  $\geq 0$

2. Fall: Term im Betrag  $< 0$

Beispiele:

$$|5| = 5 \text{ denn } 5 \geq 0$$

$$|-12| = 12 \text{ denn } -12 < 0 \text{ und } |-12| = -(-12) = 12$$



Bemerkung:

1)  $|a|$  gibt den Abstand von  $a$  zur 0 auf dem Zahlenstrahl

an;  $|a|$  ist also ein Abstandsmaß, damit:  $|a| \geq 0 \quad \forall a \in \mathbb{R}$ ;

es gilt sogar  $|a| = 0 \Leftrightarrow a = 0$

2) Erste Rechenregeln für den Betrag:

a)  $|a| \geq 0 \forall a \in \mathbb{R}; |a|=0 \Leftrightarrow a=0$

b)  $|a \cdot b| = |a| \cdot |b|$

$$\left| \frac{a}{b} \right| = \frac{|a|}{|b|}$$

c) Für Summen gilt die sog. Dreiecksungleichung:  $|a+b| \leq |a| + |b|$

Bsp.:  $a=7, b=-5 \Rightarrow |a| + |b| = 7 + 5 = 12 \quad \left. \begin{array}{l} 2 \leq 12 \\ |a+b| \leq |a| + |b| \end{array} \right\}$   
 $a+b = 2 \Rightarrow |a+b| = 2$

(Beweis der Dreiecksungleichung später in der Vorlesung)

### 3) Betrag, Ungleichung und Intervalle

a) Gegeben ist die Ungleichung  $|x| < 5$ , gesucht ist die Lösungsmenge  $\mathbb{L}$  dieser Ungleichung, also  $\mathbb{L} = \{x \in \mathbb{R} \mid |x| < 5\}$ .

$$|x| < 5 \Rightarrow \underbrace{\text{1. Fall: } x \geq 0}_{\text{im 1. Fall gilt also}} : |x| < 5 \Leftrightarrow x < 5$$

$$0 \leq x < 5 \Leftrightarrow x \in [0, 5) = \mathbb{L}_1$$

$$\underbrace{\text{2. Fall: } x < 0}_{\text{im 2. Fall gilt also}} : |x| < 5 \Leftrightarrow -x < 5 \quad | \cdot (-1)$$

$$x > -5 \Leftrightarrow -5 < x < 0 \Leftrightarrow x \in (-5, 0) = \mathbb{L}_2$$

insgesamt:  $\mathbb{L} = \mathbb{L}_1 \cup \mathbb{L}_2 = (-5, 5)$



alle  $x \in \mathbb{R}$ , deren Abstand zu 0 auf dem Zahlenstrahl kleiner 5 ist:  $|x| < 5 \Leftrightarrow |x-0| < 5$

b) Gesucht ist die Lösungsmenge der Ungleichung  $|x-2| \leq 3 \Leftrightarrow |x-2| \leq 3$



alle  $x \in \mathbb{R}$  mit Abstand ≤ 3 von 2 ∈ ℝ

Rechnerische Lösung:  $|x-2| \leq 3$

1. Fall:  $x-2 \geq 0 \Leftrightarrow x \in [2, +\infty)$  | 2. Fall:  $x-2 < 0 \Leftrightarrow x \in (-\infty, 2)$

$$\begin{aligned} |x-2| \leq 3 &\Leftrightarrow x-2 \leq 3 \quad |+2 \\ &\Leftrightarrow x \leq 5 \\ &\Leftrightarrow x \in (-\infty, 5] \end{aligned}$$

$$I_L = [2, +\infty) \cap (-\infty, 5] = [2, 5]$$

$$\begin{aligned} |x-2| \leq 3 &\Leftrightarrow -(x-2) \leq 3 \\ &\Leftrightarrow -x+2 \leq 3 \\ &\Leftrightarrow -x \leq 1 \quad | \cdot (-1) \\ &\Leftrightarrow x \geq -1 \\ &\Leftrightarrow x \in [-1, +\infty) \end{aligned}$$
$$I_L = (-\infty, 2) \cap [-1, +\infty) = [-1, 2]$$

insgesamt:  $I_L = I_{L_2} \cup I_{L_1} = [-1, 2) \cup [2, 5] = [-1, 5]$

c)  $|2x+4| < 2$  ← gesucht ist die Lösungsmenge dieser Ungleichung

Variante 1: Fallunterscheiden zum Auflösen des Betrags

1. Fall:  $2x+4 \geq 0 \Leftrightarrow 2x \geq -4 \Leftrightarrow x \geq -2 \Leftrightarrow x \in [-2, +\infty)$

$$\begin{aligned} |2x+4| < 2 &\Leftrightarrow 2x+4 < 2 \quad |-4 \\ &\Leftrightarrow 2x < -2 \quad | \cdot \frac{1}{2} \\ &\Leftrightarrow x < -1 \Leftrightarrow x \in (-\infty, -1) \end{aligned}$$

$$\begin{aligned} I_{L_1} &= [-2, +\infty) \cap (-\infty, -1) \\ &= [-2, -1) \end{aligned}$$

2. Fall:  $2x+4 < 0 \Leftrightarrow 2x < -4 \Leftrightarrow x < -2 \Leftrightarrow x \in (-\infty, -2)$

$$\begin{aligned} |2x+4| < 2 &\Leftrightarrow -(2x+4) < 2 \\ &\Leftrightarrow -2x-4 < 2 \quad |+4 \\ &\Leftrightarrow -2x < 6 \quad | \cdot (-\frac{1}{2}) \\ &\Leftrightarrow x > -3 \\ &\Leftrightarrow x \in (-3, +\infty) \end{aligned}$$

$$\begin{aligned} I_{L_2} &= (-3, +\infty) \cap (-\infty, -2) \\ &= (-3, -2) \end{aligned}$$

ausgesamt:  $I_L = I_{L_2} \cup I_{L_1} = (-3, -2) \cup [-2, -1) = (-3, -1)$

Variante 2: Anwendung von Rechenregeln und „Geometrie“ (Anschauung)

$$|2x+4| < 2 \Leftrightarrow |2 \cdot (x+2)| < 2 \quad |a \cdot b| = |a| \cdot |b|$$

$$\Leftrightarrow |2| \cdot |x+2| < 2$$

$$\Leftrightarrow 2 \cdot |x+2| < 2 \quad | \cdot \frac{1}{2}$$

$$\Leftrightarrow |x+2| < 1$$

$$\Leftrightarrow |x - (-2)| < 1 \quad \leftarrow \text{alle } x, \text{ deren Abstand von } -2 \text{ kleiner } 1 \text{ ist}$$

$$\Leftrightarrow x \in (-3, -1)$$

d) Ungleichungen (ohne Betrag)

Gesucht ist die Lösungsmenge von  $\frac{x+1}{x-1} > 5$

$$D = \mathbb{R} \setminus \{1\} = \{x \in \mathbb{R} \mid x \neq 1\}$$

$$\frac{x+1}{x-1} > 5 \quad | \cdot (x-1)$$

1. Fall  $x > 1 \Rightarrow x-1 > 0$   
 2. Fall  $x < 1 \Rightarrow x-1 < 0$

1. Fall:  $x-1 > 0 \Leftrightarrow x \in (1, +\infty)$

$$\frac{x+1}{x-1} > 5 \Leftrightarrow x+1 > 5 \cdot (x-1)$$

$$\Leftrightarrow x+1 > 5x-5 \quad | -5x+1$$

$$\Leftrightarrow -4x > -6 \quad | \cdot (-\frac{1}{4})$$

$$\Leftrightarrow x < \frac{3}{2} \Leftrightarrow x \in (-\infty, \frac{3}{2}]$$

$$\left. \begin{aligned} L_1 &= (-\infty, \frac{3}{2}] \cap (1, +\infty) \\ &= (1, \frac{3}{2}] \end{aligned} \right\}$$

2. Fall:  $x-1 < 0 \Leftrightarrow x \in (-\infty, 1)$

$$\frac{x+1}{x-1} > 5 \Leftrightarrow x+1 < 5 \cdot (x-1)$$

$$\Leftrightarrow x+1 < 5x-5 \quad | -5x+1$$

$$\Leftrightarrow -4x < -6 \quad | \cdot (-\frac{1}{4})$$

$$\Leftrightarrow x > \frac{3}{2} \Leftrightarrow x \in [\frac{3}{2}, +\infty)$$

$$\left. \begin{aligned} L_2 &= [\frac{3}{2}, +\infty) \cap (-\infty, 1) = \emptyset \end{aligned} \right\}$$

insgesamt:  $L = L_1 \cup L_2 = (1, \frac{3}{2}] \cup \emptyset = (1, \frac{3}{2}]$

## 12 Vorlesung 12 (02.11.2020)

**12.1 Anordnung, Ungleichung und Intervalle**

**12.2 Potenzen und Wurzeln in den reellen Zahlen**

**12.3 Rechenregeln für Wurzeln**

**12.4 Quadratische Gleichungen und Ungleichungen in den reellen Zahlen**

**12.5 pq-Formel**

WICHTIG: Im Rahmen der Portfolio-Prüfung zu Mathematik 1 werden 3 edX-Tests angeboten! Zwei von drei Test muss man mitmachen um Punkte (maximal 15%) für die Gesamtprüfung zu erzielen.

Der 1. Test wird freigeschaltet vom 18.11.2020 12:00 Uhr bis 18.11.2020 18:00 Uhr im edX-Portal. Nach dem Anmelden (Einloggen) zum Test hat man individuell 60 Minuten Bearbeitungszeit.

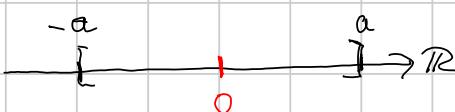
### Anordnung, Ungleichungen, Intervalle in $\mathbb{R}$

① Für  $a \in \mathbb{R}$ ,  $a > 0$  hat die Ungleichung  $|x| \leq a$  die

$$\text{Lösungsmenge } L = \{x \in \mathbb{R} \mid -a \leq x \leq a\} = [-a, a]$$

$[-a, a]$  ist ein symmetrisch um  $0 \in \mathbb{R}$  gelgenes Intervall

$$|x| \leq a \Leftrightarrow \underbrace{|x - 0| \leq a}_{\text{Menge aller } x \in \mathbb{R}, \text{ deren Abstand von } 0 \text{ kleiner oder gleich } a \text{ ist}}$$

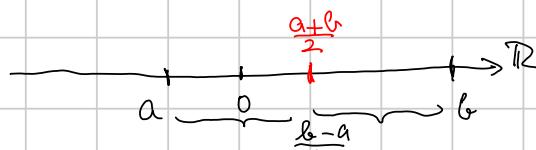


②  $|x - b| \leq a$  hat als Lösungsmenge  $L = [b - a, b + a]$ ,  $b \in \mathbb{R}, a > 0$

Menge aller  $x \in \mathbb{R}$ , deren Abstand von  $b$  kleiner oder gleich  $a$  ist

③ Behauptung: Es gilt  $[a, b] = \left\{ x \in \mathbb{R} \mid |x - \frac{a+b}{2}| \leq \frac{b-a}{2} \right\}$   
für  $a, b \in \mathbb{R}$  mit  $b > a$

"geometrische" Lösung:



$[a, b]$  ist die Menge aller  $x \in \mathbb{R}$ , deren Abstand von  $\frac{a+b}{2}$  kleiner oder gleich  $\frac{b-a}{2}$  ist

"rechnerische" Lösung: Mit Fallunterscheidung;  $a, b \in \mathbb{R}$ ,  $b > a$

$$\left| x - \frac{a+b}{2} \right| \leq \frac{b-a}{2}$$

$x \in [\frac{a+b}{2}, +\infty)$

1. Fall  $x \geq \frac{a+b}{2} \Rightarrow x - \frac{a+b}{2} \geq 0$

$$\left| x - \frac{a+b}{2} \right| \leq \frac{b-a}{2} \Leftrightarrow$$

$$\Leftrightarrow x - \frac{a+b}{2} \leq \frac{b-a}{2} + \frac{a+b}{2}$$

$$\Leftrightarrow x \leq \frac{b-a}{2} + \frac{a+b}{2}$$

$$\Leftrightarrow x \leq \frac{b-a+a+b}{2} = \frac{2b}{2} = b$$

$$\Leftrightarrow x \leq b \Leftrightarrow x \in (-\infty, b]$$

$$I_{L_1} = \left[ \frac{a+b}{2}, +\infty \right) \cap (-\infty, b]$$

$$= \left[ \frac{a+b}{2}, b \right]$$

$x \in (-\infty, \frac{a+b}{2})$

2. Fall  $x < \frac{a+b}{2} \Rightarrow x - \frac{a+b}{2} < 0$

$$\left| x - \frac{a+b}{2} \right| \leq \frac{b-a}{2} \Leftrightarrow$$

$$-(x - \frac{a+b}{2}) \leq \frac{b-a}{2} \Leftrightarrow$$

$$\Rightarrow x + \frac{a+b}{2} \leq \frac{b-a}{2} \quad \left| -\frac{a+b}{2} \right. \Leftrightarrow$$

$$-x \leq \frac{b-a}{2} - \frac{a+b}{2} \Leftrightarrow$$

$$-x \leq \frac{b-a-(a+b)}{2} \Leftrightarrow$$

$$-x \leq \frac{b-a-a-b}{2} = \frac{-2a}{2} = -a \quad | \cdot (-1)$$

$$\Leftrightarrow x \geq a \Leftrightarrow x \in [a, +\infty)$$

$$I_{L_2} = [a, +\infty) \cap (-\infty, \frac{a+b}{2}) = [a, \frac{a+b}{2}]$$

insgesamt:  $I = I_{L_1} \cup I_{L_2} = I_{L_2} \cup I_{L_1} = [a, \frac{a+b}{2}) \cup [\frac{a+b}{2}, b] = [a, b]$

### Potenzen und Wurzeln in $\mathbb{R}$

① Für  $a \in \mathbb{R}$ ,  $a \neq 0$  ist  $\underbrace{a^0 = 1}$  und  $\underbrace{a^n = a \cdot a^{n-1}}_{\text{Rekursive Definition des } n\text{-ten Potenz } a^n \text{ für } a \neq 0} \quad \forall n \in \mathbb{N}$

Rekursive Definition des  $n$ -ten Potenz  $a^n$  für  $a \neq 0$

Es gilt:  $a^n = \underbrace{a \cdot a \cdot a \cdots a}_{n-\text{mal}}$  Produkt von  $a$  mit  $a$   $n$ -mal

②  $0^n = 0 \quad \forall n \in \mathbb{N}$ ,  $0^0$  ist nicht definiert

③  $a^n \cdot a^k = a^{n+k}$ ,  $\frac{a^n}{a^k} = a^{n-k} \Rightarrow \frac{1}{a^k} = a^{-k} \quad \forall n, k \in \mathbb{N}$

$(a^n)^k = a^{n \cdot k}$ ; Bedeutungen  $\begin{array}{l} n \leftarrow \text{Exponent (der Potenz)} \\ a \leftarrow \text{Basis (der Potenz)} \end{array}$

$$(a \cdot b)^n = a^n \cdot b^n, \quad \left(\frac{a}{b}\right)^n = \frac{a^n}{b^n}$$

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

↑ allg. binomische Formel

#### ④ Definition ( $n$ -te Wurzel)

a) Für  $n \in \mathbb{N}$ ,  $n$  gerade (d.h.  $n = 2k$  für ein  $k \in \mathbb{N}_0$ ), ist definiert:

Für  $a \in \mathbb{R}$ ,  $a \geq 0$ , ist  $\sqrt[n]{a}$  die eindeutig bestimmte nicht negative  
↑ Lös:  $n$ -te Wurzel a

Lösung der Gleichung  $x^n = a$ .

↑  $\sqrt[2]{4} = 2$  denn 2 ist die nicht negative Lösung von  $x^2 = 4$

statt  $\sqrt[2]{a}$  schreibt man einfacher  $\sqrt{a}$ .

Bedeutung:  $\sqrt[n]{a}$   
↑ Wurzlexponent  
↑ Radikand

→

b) Für  $n \in \mathbb{N}$ ,  $n$  ungerade (d.h.  $n = 2k+1$  für ein  $k \in \mathbb{N}_0$ ) ist

definiert:

$\forall a \in \mathbb{R}$  ist  $\sqrt[n]{a}$  die eindeutig bestimmte Lösung der Gleichung  
 $x^n = a$ . ↑ Lös:  $n$ -te Wurzel von a

↑  $\sqrt[3]{-8} = -2$  denn  $-2$  ist die eindeutig bestimmte Lösung

von  $x^3 = -8$ :  $(-2) \cdot (-2) \cdot (-2) = (-2)^3 = -8$

$\sqrt[3]{64} = 4$  denn  $4^3 = 64$ , d.h. 4 ist die eindeutig bestimmte  
Lösung von  $x^3 = 64$

→

Bemerkung:

① Wenn  $n$  gerade ist und  $a > 0$  hat  $x^n = a$  die beiden Lösungen

$x_1 = \sqrt[n]{a}$  und  $x_2 = -\sqrt[n]{a}$  denn

$x_1^n = (\sqrt[n]{a})^n = a$  nach Definition [ **MERKE:**  $(\sqrt[n]{a})^n = a$  ]

$$x_2^n = (-\sqrt[n]{a})^n = ((-1) \cdot \sqrt[n]{a})^n = \underbrace{(-1)^n}_{=+1 \text{ für } n \text{ gerade}} \cdot (\sqrt[n]{a})^n = (\sqrt[n]{a})^n = a$$

②  $\sqrt[0]{0} = 0$  für alle  $n \in \mathbb{N}$ ,  $\sqrt[1]{a} = a$  für alle  $a \in \mathbb{R}$

③ Darstellung von  $\sqrt[n]{a}$  als Potenz:

Gesucht  $\alpha$  mit  $\sqrt[n]{a} = a^\alpha \leftarrow$  Darstellung von  $\sqrt[n]{a}$  als Potenz

Falls es ein solches  $\alpha$  gibt, erhält man mit den Rechenregeln für Potenzen

$$\textcircled{1} \quad a = a = (\sqrt[n]{a})^n = (a^\alpha)^n = a^{\alpha \cdot n}$$

$\Rightarrow$  es muss gelten:  $\alpha \cdot n = 1 \Rightarrow \alpha = \frac{1}{n}$ .

$$\boxed{\text{Es gilt also: } \sqrt[n]{a} = a^{\frac{1}{n}}}$$

④ Rechenregeln für Wurzeln (Existenz der Wurzeln wird vorausgesetzt)

$$\sqrt[n]{a \cdot b} = \sqrt[n]{a} \cdot \sqrt[n]{b}$$

Bemerkung: Im Regelfall gilt

$$\sqrt[n]{\frac{a}{b}} = \frac{\sqrt[n]{a}}{\sqrt[n]{b}}$$

$$\sqrt[n]{a+b} \neq \sqrt[n]{a} + \sqrt[n]{b}$$

$$\sqrt[5]{25} = 5, \quad \sqrt[5]{25} = \sqrt[5]{16+9} = \sqrt[5]{16} + \sqrt[5]{9}$$

$$\sqrt[k]{\sqrt[n]{a}} = (a^{\frac{1}{n}})^{\frac{1}{k}} = a^{\frac{1}{n} \cdot \frac{1}{k}} = a^{\frac{1}{n \cdot k}} = \sqrt[n \cdot k]{a}$$

$$\sqrt[n]{a^k} = (a^k)^{\frac{1}{n}} = a^{\frac{k}{n}} = a^{\frac{1}{n} \cdot k} = (a^{\frac{1}{n}})^k = \sqrt[n]{a}^k$$

### Quadratische Gleichungen und Ungleichungen in $\mathbb{R}$

$$\boxed{\begin{aligned} \textcircled{1} \quad x^2 = a &\rightarrow \text{L} = \emptyset \text{ für } a < 0 \\ &\rightarrow \text{L} = \{-\sqrt{a}, \sqrt{a}\} \text{ für } a > 0 \\ &\rightarrow \text{L} = \{0\} \text{ für } a = 0 \end{aligned}}$$

$$\text{denn: } x \in \mathbb{R}, \quad x > 0 \Rightarrow x \cdot x > 0 \cdot x \Rightarrow x^2 > 0 \quad \left. \begin{array}{l} x < 0 \Rightarrow x \cdot x > 0 \cdot x \Rightarrow x^2 > 0 \\ \hline 0^2 = 0 \cdot 0 = 0 \end{array} \right\} x^2 > 0 \quad \forall x \in \mathbb{R}, x \neq 0$$

$$\text{Es gilt: } x^2 \geq 0 \quad \forall x \in \mathbb{R} \quad \text{sogar } x^2 > 0 \quad \forall x \in \mathbb{R}, x \neq 0 \wedge 0^2 = 0$$

d.h.  $x^2 = 0$  hat nur die Lösung  $x = 0$

② Wir hatten definiert  $|x| = \begin{cases} x & \text{für } x \geq 0 \\ -x & \text{für } x < 0 \end{cases}$

es gilt eine andere Darstellung für  $|x|$ , nämlich  $|x| = \sqrt{x^2}$

$$\Gamma 4 = |-4| = \sqrt{(-4)^2} = \sqrt{16}$$

③ Für  $a \geq 0$  gilt:  $x^2 \leq a \iff |x| \leq \sqrt{a}$

$$\iff x \in [-\sqrt{a}, \sqrt{a}]$$

d.h. die Lösungsmenge der Ungleichung  $x^2 \leq a$  für  $a \geq 0$   
ist das Intervall  $[-\sqrt{a}, \sqrt{a}]$

#### ④ Quadratische Gleichungen in $\mathbb{R}$

In ① haben wir gesehen: Für  $a \in \mathbb{R}$  gibt es als Lösungsmenge  
zu  $x^2 = a$  drei Möglichkeiten, nämlich  $\mathcal{L} = \emptyset$  falls  $a < 0$  ist,  
 $\mathcal{L} = \{0\}$  falls  $a = 0$ ,  $\mathcal{L} = [-\sqrt{a}, \sqrt{a}]$  falls  $a > 0$  ist.

allgemeine quadratische Gleichung  $a_2 x^2 + a_1 x + a_0 = 0$  mit  $a_2 \in \mathbb{R}, a_2 \neq 0$   
 $a_0, a_1 \in \mathbb{R}$

Wegen  $a_2 \neq 0$  kann man durch  $a_2$  teilen und erhält

$$x^2 + \frac{a_1}{a_2} x + \frac{a_0}{a_2} = 0$$

setzt man  $\frac{a_1}{a_2} = p \in \mathbb{R}$  und  $\frac{a_0}{a_2} = q \in \mathbb{R}$  hat man die

quadratische Gleichung in Normalform  $x^2 + px + q = 0$

Zur Lösung macht man die sog. quadratische Ergänzung

$$(x+b)^2 = x^2 + 2bx + b^2$$

$$x^2 + px = x^2 + 2bx$$

$$\therefore b = \frac{p}{2}$$

$$x^2 + px + q = 0 \iff$$

$$x^2 + 2 \cdot \frac{p}{2} x + q = 0 \iff$$

$$\underbrace{(x^2 + 2 \cdot \frac{p}{2} x + (\frac{p}{2})^2)}_{=0} - (\frac{p}{2})^2 + q = 0 \iff$$

$$(x + \frac{p}{2})^2 - (\frac{p}{2})^2 + q = 0 \iff$$

damit erhält man

$$\left( x + \frac{P}{2} \right)^2 = \left( \frac{P}{2} \right)^2 - q \quad \leftarrow \begin{array}{l} \tilde{x}^2 = a \text{ mit } a = \left( \frac{P}{2} \right)^2 - q \\ \tilde{x} = \left( x + \frac{P}{2} \right) \end{array}$$

1. Fall:  $\left( \frac{P}{2} \right)^2 - q < 0 \Rightarrow L = \emptyset$

2. Fall:  $\left( \frac{P}{2} \right)^2 - q = 0 \Rightarrow L = \{ \tilde{x} = 0 \} = \{ -\frac{P}{2} \}$

$$\tilde{x} = 0 \Leftrightarrow x + \frac{P}{2} = 0 \Leftrightarrow x = -\frac{P}{2}$$

3. Fall:  $\left( \frac{P}{2} \right)^2 - q > 0 \Rightarrow L = \{ \tilde{x}_1 = -\sqrt{\left( \frac{P}{2} \right)^2 - q}, \tilde{x}_2 = \sqrt{\left( \frac{P}{2} \right)^2 - q} \}$

$$= \left\{ x_1 = -\frac{P}{2} - \sqrt{\left( \frac{P}{2} \right)^2 - q}, \right.$$

$$\left. x_2 = -\frac{P}{2} + \sqrt{\left( \frac{P}{2} \right)^2 - q} \right\}$$

Beispiel:  $x^2 - 5x + 6 = 0$

$$P = -5, q = 6 \Rightarrow \left( \frac{P}{2} \right)^2 - q = \left( -\frac{5}{2} \right)^2 - 6 = \frac{25}{4} - 6 = \frac{25}{4} - \frac{24}{4} = \frac{1}{4} > 0$$

$\Rightarrow$  es gibt 2 Lösungen, nämlich

$$x_1 = -\frac{P}{2} - \sqrt{\left( -\frac{P}{2} \right)^2 - q} = +\frac{5}{2} - \sqrt{\frac{1}{4}} = +\frac{5}{2} - \frac{1}{2} = \frac{4}{2} = 2$$

$$x_2 = -\frac{P}{2} + \sqrt{\left( -\frac{P}{2} \right)^2 - q} = +\frac{5}{2} + \sqrt{\frac{1}{4}} = +\frac{5}{2} + \frac{1}{2} = \frac{6}{2} = 3$$

Es gilt:  $(x - x_1) \cdot (x - x_2) = (x - 2) \cdot (x - 3) = x^2 - 5x + 6$

oder  $x^2 - 5x + 6 = 0 \Leftrightarrow (x - 2) \cdot (x - 3) = 0$

## 13 Vorlesung 13 (03.11.2020)

**13.1 Linearfaktoren des quadratischen Polynoms**

**13.2 Mitternachtsformel**

**13.3 Quadratische Ungleichungen**

**13.4 Definition: Logarithmus**

**13.5 Rechenregeln für Logarithmen**

**13.6 Zahldarstellungen (umrechnung)**

quadr. Gleichung in Normalform  $x^2 + px + q = 0$

$$\text{„formale“ Lösung } x_{1,2} = -\frac{p}{2} \pm \sqrt{\left(\frac{p}{2}\right)^2 - q} = -\frac{p}{2} \pm \sqrt{\left(\frac{p}{2}\right)^2 - q}$$

$$\rightarrow \underline{1. Fall: } \left(\frac{p}{2}\right)^2 - q < 0 \Rightarrow \mathbb{L} = \emptyset$$

$$\rightarrow \underline{2. Fall: } \left(\frac{p}{2}\right)^2 - q = 0 \Rightarrow \mathbb{L} = \left\{-\frac{p}{2}\right\}$$

$$\rightarrow \underline{3. Fall} \quad \left(\frac{p}{2}\right)^2 - q > 0 \Rightarrow \mathbb{L} = \left\{-\frac{p}{2} - \sqrt{\left(\frac{p}{2}\right)^2 - q}, -\frac{p}{2} + \sqrt{\left(\frac{p}{2}\right)^2 - q}\right\}$$

Zur 3. Fall hat man mit  $x_1 = -\frac{p}{2} - \sqrt{\left(\frac{p}{2}\right)^2 - q}$  und  $x_2 = -\frac{p}{2} + \sqrt{\left(\frac{p}{2}\right)^2 - q}$ :

$$(x-x_1) \cdot (x-x_2) = x^2 - x \cdot x_2 - x \cdot x_1 + x_1 \cdot x_2 \\ = x^2 - (x_1 + x_2) \cdot x + x_1 \cdot x_2$$

$$\text{es ist } x_1 + x_2 = \left(-\frac{p}{2} - \sqrt{\left(\frac{p}{2}\right)^2 - q}\right) + \left(-\frac{p}{2} + \sqrt{\left(\frac{p}{2}\right)^2 - q}\right) = -p$$

$$x_1 \cdot x_2 = \left(-\frac{p}{2} - \sqrt{\left(\frac{p}{2}\right)^2 - q}\right) \cdot \left(-\frac{p}{2} + \sqrt{\left(\frac{p}{2}\right)^2 - q}\right) \quad \begin{matrix} \leftarrow (a-b) \cdot (a+b) = a^2 - b^2 \\ \text{mit } a = -\frac{p}{2} \\ b = \sqrt{\left(\frac{p}{2}\right)^2 - q} \end{matrix}$$

$$= \left(-\frac{p}{2}\right)^2 - \left(\sqrt{\left(\frac{p}{2}\right)^2 - q}\right)^2 = \left(\frac{p}{2}\right)^2 - \left(\left(\frac{p}{2}\right)^2 - q\right) = q$$

dann folgt  $(x-x_1) \cdot (x-x_2) = x^2 - \underbrace{(x_1 + x_2)}_{=-p} x + \underbrace{x_1 \cdot x_2}_{=q} = x^2 + px + q$

$\swarrow \uparrow \quad \uparrow \quad \uparrow$   
Linearfaktoren des quadratischen Polynoms

Quadratische Gleichung in allgemeiner Form:  $a_2 x^2 + a_1 x + a_0 = 0$ ,  $a_2 \neq 0, a_1, a_0 \in \mathbb{R}$

$$0 = a_2 x^2 + a_1 x + a_0 = a_2 \cdot \left(x^2 + \frac{a_1}{a_2} x + \frac{a_0}{a_2}\right)$$

$\uparrow \quad \underbrace{\quad}_{\neq 0} \quad \uparrow$

$$x^2 + \frac{a_1}{a_2} x + \frac{a_0}{a_2} = 0 \quad \xrightarrow{\frac{a_1}{a_2} = p; \frac{a_0}{a_2} = q} x^2 + px + q = 0$$

"formale" Lösung  $x_{1,2} = -\frac{p}{2} \pm \sqrt{\left(\frac{p}{2}\right)^2 - q}$

$$\text{mit } \frac{p}{2} = \frac{a_1}{2a_2}, \quad q = \frac{a_0}{a_2} : \quad \left(\frac{p}{2}\right)^2 - q = \frac{a_1^2}{4a_2^2} - \frac{a_0}{a_2} = \frac{a_1^2 - 4a_0a_2}{4a_2^2}$$

$$\sqrt{\left(\frac{p}{2}\right)^2 - q} = \sqrt{\frac{a_1^2 - 4a_0a_2}{4a_2^2}} = \frac{\sqrt{a_1^2 - 4a_0a_2}}{2|a_2|}$$

$$\text{insgesamt } x_{1,2} = -\frac{a_1}{2a_2} \pm \frac{\sqrt{a_1^2 - 4a_0a_2}}{2|a_2|} = \frac{-a_1 \pm \sqrt{a_1^2 - 4a_0a_2}}{2a_2}$$

$$\rightarrow \underline{1. Fall}: \quad a_1^2 - 4a_0a_2 < 0 \Rightarrow \mathbb{L} = \emptyset$$

$$\rightarrow \underline{2. Fall}: \quad a_1^2 - 4a_0a_2 = 0 \Rightarrow \mathbb{L} = \left\{ -\frac{a_1}{2a_2} \right\}$$

$$\rightarrow \underline{3. Fall}: \quad a_1^2 - 4a_0a_2 > 0 \Rightarrow \mathbb{L} = \left\{ \frac{-a_1 + \sqrt{a_1^2 - 4a_0a_2}}{2a_2}, \frac{-a_1 - \sqrt{a_1^2 - 4a_0a_2}}{2a_2} \right\}$$

$$\left. \frac{-a_1 - \sqrt{a_1^2 - 4a_0a_2}}{2a_2} \right\}$$

Quadratische Ungleichungen: (12. Vorlesung):  $x^2 \leq a$  für  $a \in \mathbb{R}, a > 0$   
 $\Rightarrow |x| \leq \sqrt{a} \Rightarrow$   
 $x \in [-\sqrt{a}, \sqrt{a}]$

$$x^2 + px + q \leq a$$

$$\Leftrightarrow \left(x + \frac{p}{2}\right)^2 + q - \left(\frac{p}{2}\right)^2 \leq a$$

$y^2 \leq b$        $b < 0 \quad \mathbb{L} = \emptyset$   
 $b \geq 0 \quad \mathbb{L} = [-\sqrt{b}, \sqrt{b}]$   
 $(x + \frac{p}{2}) = y \in [-\sqrt{b}, \sqrt{b}] \Rightarrow$   
 $x \in [-\frac{p}{2} - \sqrt{b}, -\frac{p}{2} + \sqrt{b}]$

$$\Leftrightarrow \underbrace{\left(x + \frac{p}{2}\right)^2}_y \leq a + \underbrace{\left(\frac{p}{2}\right)^2 - q}_b \quad \begin{cases} \mathbb{L} \neq \emptyset \text{ für } a + \left(\frac{p}{2}\right)^2 - q \geq 0 \\ \mathbb{L} = \emptyset \text{ für } a + \left(\frac{p}{2}\right)^2 - q < 0 \end{cases}$$

insbesondere gilt:  $\mathbb{L} = \left\{ -\frac{p}{2} \right\}$  falls  $a + \left(\frac{p}{2}\right)^2 - q = 0$  ist und

$$\mathbb{L} = \left[ -\frac{p}{2} - \sqrt{a + \left(\frac{p}{2}\right)^2 - q}, -\frac{p}{2} + \sqrt{a + \left(\frac{p}{2}\right)^2 - q} \right] \text{ falls } a + \left(\frac{p}{2}\right)^2 - q > 0.$$

Bemerkung:  $x^2 \leq a$ ,  $a > 0$  hat Lösungsmenge  $\mathbb{L} = [-\sqrt{a}, \sqrt{a}]$

$x^2 < a$ ,  $a > 0$  hat Lösungsmenge  $\mathbb{L} = (-\sqrt{a}, \sqrt{a})$

$x^2 \geq a$ ,  $a > 0$  hat Lösungsmenge  $\mathbb{L} = \mathbb{R} \setminus (-\sqrt{a}, \sqrt{a})$

$$= (-\infty, -\sqrt{a}] \cup [\sqrt{a}, +\infty)$$

$$x^2 > a, \quad a > 0 \text{ hat Lösungsmenge } \mathbb{L} = \mathbb{R} \setminus [-\sqrt{a}, \sqrt{a}] \\ = (-\infty, -\sqrt{a}) \cup (\sqrt{a}, +\infty)$$

## Logarithmen

Definition: Für  $a, b \in \mathbb{R}$  mit  $a > 0$  und  $b > 0$  ist der Logarithmus von  $a$  zur Basis  $b$  definiert als

$$x = \log_b(a) \Leftrightarrow b^x = a$$

( $\log_b(a)$  ist die Zahl  $x$ , die als Exponent  $b^x = a$  ergibt)

Beispiele: a)  $\log_{10}(1000) = 3$  denn  $10^3 = 1000$

$$\log_{10}\left(\frac{1}{100}\right) = -2 \text{ denn } 10^{-2} = \frac{1}{10^2} = \frac{1}{100}$$

$$\log_5(125) = 3 \text{ denn } 5^3 = 5 \cdot 5 = 25 \cdot 5 = 125$$

b) Die Lösung der Gleichung  $2^x = 8$  ist  $x = \underbrace{\log_2(8)}_{2^3 = 8} = 3$

MERKE:  $x = \log_b(a)$  ist die Lösung der Gleichung  $b^x = a$

## Bemerkung:

1) Logarithmus zur Basis 10  $\rightarrow$  10er Logarithmus:  $\log_{10}(a) = \lg(a) = \log(a)$

Logarithmus zur Basis 2  $\rightarrow$  2er Logarithmus:  $\log_2(a) = \text{ld}(a)$

↑  
logarithmus dualis

Logarithmus zur Basis e  $\rightarrow$  Logarithmus zur Basis e  $\hat{=}$  natürlicher

$e \in \mathbb{R}$

↔

Logarithmus:  $\log_e(a) = \ln(a)$

↑  
logarithmus naturalis

$e = 2,7182818\dots$

unendlich viele nicht  
periodische Nachkommastellen.

$e \in \mathbb{R} \setminus \mathbb{Q}$

## 2) Rechenregeln für Logarithmen (folgen aus den Regeln für Potenzen)

Da die Regeln für jede zulässige Basis  $b \in \mathbb{R}$ ,  $b > 0$  gleich sind, schreiben wir jetzt einfach  $\log$  statt  $\log_b$ .

$$a) \log(a_1 \cdot a_2) = \log(a_1) + \log(a_2) \quad \xrightarrow{\text{Beweis}}$$

$$b) \log\left(\frac{a_1}{a_2}\right) = \log(a_1) - \log(a_2)$$

$$c) \log(a_1^\alpha) = \alpha \cdot \log(a_1)$$

linke Seite

$$x = \log_b(a_1 \cdot a_2) \Leftrightarrow b^x = a_1 \cdot a_2$$

rechte Seite

$$x = \log_b(a_1) + \log_b(a_2) \Rightarrow$$

$$b^x = b^{\log_b(a_1) + \log_b(a_2)}$$

$$= \underbrace{b^{\log_b(a_1)}}_{a_1} \cdot \underbrace{b^{\log_b(a_2)}}_{a_2} = a_1 \cdot a_2$$

## 3) Umrechnung von Logarithmen

gesucht  $x = \log_b(a)$  bekannt ist  $\log_{\tilde{b}}(a)$  Logarithmus zur Basis  $\tilde{b}$

d.h.  $\log_{\tilde{b}}(a)$  und  $\log_{\tilde{b}}(b)$  sind bekannt

$$x = \log_b(a) \Leftrightarrow b^x = a \quad | \log_{\tilde{b}}(\dots)$$

$$\Leftrightarrow \log_{\tilde{b}}(b^x) = \log_{\tilde{b}}(a)$$

$$\stackrel{c)}{\Leftrightarrow} x \cdot \log_{\tilde{b}}(b) = \log_{\tilde{b}}(a)$$

$$\Leftrightarrow x = \frac{\log_{\tilde{b}}(a)}{\log_{\tilde{b}}(b)}$$

insgesamt: 
$$\log_b(a) = \frac{\log_{\tilde{b}}(a)}{\log_{\tilde{b}}(b)}$$

Beispiel:  $\log_{10}(35) = \frac{\ln(35)}{\ln(10)}, \ln(35) = \frac{\log_{10}(35)}{\log_{10}(e)}$

## Rückblick auf Zahldarstellungen

Dezimalsystem  $\rightarrow$  Basis 10 :  $273,12 = 2 \cdot 10^2 + 7 \cdot 10^1 + 3 \cdot 10^0 + 1 \cdot 10^{-1} + 2 \cdot 10^{-2}$

$$\underbrace{a_n a_{n-1} \dots a_1 a_0}_{\text{Basis } 10}, \underbrace{b_1 b_2 \dots b_K}_{\text{Basis } c} = \sum_{i=0}^n a_i \cdot 10^i + \sum_{j=1}^K b_j \cdot 10^{-j}$$

c-adisches System  $\rightarrow$  Basis  $c > 0$ :

$$\underbrace{a_n a_{n-1} \dots a_1 a_0}_{\text{Basis } c}, \underbrace{b_1 b_2 \dots b_K}_{\text{Basis } c} = \sum_{i=0}^n a_i \cdot c^i + \sum_{j=1}^K b_j \cdot c^{-j}$$

$c = 2 \rightarrow$  Dualsystem,  $c = 16 \rightarrow$  Hexadezimalsystem

$$\begin{aligned} 1357 &= 135 \cdot 10 + 7 \uparrow \\ 135 &= 13 \cdot 10 + 5 \uparrow \\ 13 &= 1 \cdot 10 + 3 \uparrow \\ 1 &= 0 \cdot 10 + 1 \uparrow \end{aligned} \quad \left. \begin{array}{l} \text{Teilen mit Rest durch 10} \\ \text{1357} \end{array} \right\}$$

für die Zahlendarstellung c-adischer Systeme gilt: Teilen mit Rest durch  $c$ ;

z.B. Dualsystem  $c = 2$ : Gegeben 135 im Dezimalsystem  $(135)_{10}$ ;  
gesucht 135 im Dualsystem  $(135)_2$

$$\begin{aligned} 135 : 2 &= \overbrace{67 \cdot 2}^{134} + 1 \uparrow \\ 67 : 2 &= 33 \cdot 2 + 1 \uparrow \\ 33 : 2 &= 16 \cdot 2 + 1 \uparrow \\ 16 : 2 &= 8 \cdot 2 + 0 \uparrow \\ 8 : 2 &= 4 \cdot 2 + 0 \uparrow \\ 4 : 2 &= 2 \cdot 2 + 0 \uparrow \\ 2 : 2 &= 1 \cdot 2 + 0 \uparrow \\ 1 : 2 &= 0 \cdot 2 + 1 \uparrow \end{aligned} \quad \left. \begin{array}{l} \text{Teilen mit Rest durch 2} \\ (10000111)_2 \\ \text{Probe: } (10000111)_2 = \\ 1 \cdot 2^0 + 1 \cdot 2^1 + 1 \cdot 2^2 + 0 \cdot 2^3 + 0 \cdot 2^4 + 0 \cdot 2^5 + 0 \cdot 2^6 + 1 \cdot 2^7 = \\ 1 + 2 + 4 + 0 + 0 + 0 + 0 + 128 = 135 \end{array} \right\}$$

$c = 5$  : Gegeben  $(232)_{10}$ , gesucht 232 zur Basis 5

Teilen mit Rest durch 5 liefert

$$\begin{array}{l}
 232 : 5 = 46 \cdot 5 + 2 \\
 46 : 5 = 9 \cdot 5 + 1 \\
 9 : 5 = 1 \cdot 5 + 4 \\
 1 : 5 = 0 \cdot 5 + 1
 \end{array}
 \quad
 \left. \begin{array}{l}
 2 \\
 1 \\
 4 \\
 1
 \end{array} \right\} \quad
 \left. \begin{array}{l}
 (232)_{10} = (1412)_5 \\
 \text{Probe: } (1412)_5 = \\
 2 \cdot 5^0 + 1 \cdot 5^1 + 4 \cdot 5^2 + 1 \cdot 5^3 = 2 + 5 + 100 + 125 = 232
 \end{array} \right\}$$

Frage: Was ist  $(0,25)_{10}$  im System zur Basis 2?

$$\hookrightarrow 0,25 = \frac{25}{100} = \frac{1}{4} = \frac{1}{2^2} = 2^{-2}$$

$$(0,25)_{10} = (0,01)_2$$

Wie geht das generell bei Zahlen mit Nachkommastellen?

## 14 Vorlesung 14 (04.11.2020)

- 14.1 Beispiel: Zahldarstellungen (umrechnung)
- 14.2 Brüche in anderen Zahldarstellungen
- 14.3 Zweiter Blick auf Ungleichungen und Betrag
- 14.4 Rechenregeln für den Betrag
- 14.5 Beweisidee Dreiecksungleichung
- 14.6 Definition: Verknüfungen auf Mengen
- 14.7 Definition: Gruppe, Halbgruppe, abelsche Gruppe
- 14.8 Definition: Ring, Ring mit Eins, Kommutativer Ring mit Eins
- 14.9 Definition: Körper

Zahldarstellung: Basis b ( $b=10$ ,  $b=2$ ,  $b=16$ )

$$\left( a_n a_{n-1} \dots a_1 a_0, c_1 c_2 \dots c_K \right)_b = \sum_{i=0}^n a_i \cdot b^i + \sum_{j=1}^K c_j \cdot b^{-j}$$

Umrechnung ganzer Zahlen aus Dezimalsystem in ein anderes System  
durch „Division mit Rest“

Beispiel: (327)<sub>10</sub> gesucht Darstellung im Dualsystem

$$\begin{array}{rcl}
 327 & = & 163 \cdot 2 + 1 \\
 163 & = & 81 \cdot 2 + 1 \\
 81 & = & 40 \cdot 2 + 1 \\
 40 & = & 20 \cdot 2 + 0 \\
 20 & = & 10 \cdot 2 + 0 \\
 10 & = & 5 \cdot 2 + 0 \\
 5 & = & 2 \cdot 2 + 1 \\
 2 & = & 1 \cdot 2 + 0 \\
 1 & = & 0 \cdot 2 + 1
 \end{array}$$

$$(101000111)_2 = (327)_{10}$$

Prob:

$$1 + 2 + 2^2 + 2^4 + 2^8 = 1 + 2 + 4 + 64 + 256 \\ = 327 \checkmark$$

Wie kann man Brüche umschreiben?

Beispiel:  $\frac{1}{p}$  Darstellung im Dezimalsystem also  $0, c_1 c_2 \dots c_n$

$$1 : \vartheta = 0,125$$

10 ·       $\begin{array}{r} 0 \\ 10 \\ \hline 10 \\ \hline 8 \\ \hline 20 \\ \hline 16 \\ \hline 40 \\ \hline 0 \end{array}$

$\left\{ \frac{1}{\vartheta} = (0,125)_{10}$

Zer-System  
 $\frac{1}{p}$  Darstellung im Dualsystem als  $0, c_1 c_2 \dots c_n$

| Es ist:

$$\left| \frac{1}{\mathcal{P}} = \frac{1}{2^3} = 2^{-3} = (0,001)_2 \right.$$

$$1 : \varphi = 0,001$$

2.  $\frac{1}{\varphi}$   
 $\frac{1}{2}$   
 $\frac{0}{4}$   
 $\frac{0}{8}$   
 $\frac{0}{8}$   
 $0$

$\left. \begin{array}{l} \\ \\ \\ \end{array} \right\} \quad \frac{1}{\varphi} = (0,125)_{10} = (0,001)_2$

## Ein zweiter Blick auf Ungleichungen und Betrag

1) Beispiel für eine quadratische Ungleichung:

Gesucht ist die Lösungsmenge der Ungleichung  $x \cdot (x+1) \leq 0$

$$x \cdot (x+1) \leq 0 \Leftrightarrow x^2 + x \leq 0$$

Quadratische Erg.  $\rightarrow x^2 + 2 \cdot \frac{1}{2} \cdot x + \underbrace{\left(\frac{1}{2}\right)^2 - \left(\frac{1}{2}\right)^2}_{=0} \leq 0$

$$\Leftrightarrow \left(x + \frac{1}{2}\right)^2 - \left(\frac{1}{2}\right)^2 \leq 0$$

$$\Leftrightarrow \left(x + \frac{1}{2}\right)^2 \leq \left(\frac{1}{2}\right)^2$$

$\sqrt{\dots}$   $\rightarrow \sqrt{(x+\frac{1}{2})^2} \leq \sqrt{\frac{1}{4}}$

$\sqrt{x^2} = |x| \rightarrow |x + \frac{1}{2}| \leq \frac{1}{2}$

$|x| \leq a \Leftrightarrow x \in [-a, a]$

$$\Leftrightarrow x + \frac{1}{2} \in \left[-\frac{1}{2}, \frac{1}{2}\right]$$

$$\Leftrightarrow -\frac{1}{2} \leq x + \frac{1}{2} \leq \frac{1}{2}$$

$-\frac{1}{2}$   $\rightarrow -1 \leq x \leq 0$

$$\Leftrightarrow x \in [-1, 0] \Rightarrow L = [-1, 0]$$

2) Rechenregeln für  $|x|$  also für den Betrag:

Aus der M. Vorlesung haben wir

## Erste „Rechenregeln“ für den Betrag

a)  $|a| \geq 0 \quad \forall a \in \mathbb{R}; \quad |a|=0 \Leftrightarrow a=0$

b)  $|a \cdot b| = |a| \cdot |b|$

$$\left| \frac{a}{b} \right| = \frac{|a|}{|b|}$$

c) Für Summen gilt die sog. Dreiecksungleichung:  $|a+b| \leq |a| + |b|$

Bsp.:  $a=7, b=-5 \Rightarrow |a| + |b| = 7 + 5 = 12 \quad \left. \begin{array}{l} 2 \leq 12 \\ |a+b| \leq |a| + |b| \end{array} \right\}$

(Beweis der Dreiecksungleichung später in der Vorlesung)

↳ jetzt: 14. Vorlesung

### Beweisidee zur Dreiecksungleichung

1) Es gilt  $|x| = \sqrt{x^2}$  also  $|a+b| = \sqrt{(a+b)^2}$

$$(a+b)^2 = a^2 + 2a \cdot b + b^2 \stackrel{?}{=} |a|^2 + |b|^2$$

2) Es gilt:  $|a| = \sqrt{a^2} \Rightarrow |a|^2 = a^2$   
 $|b| = \sqrt{b^2} \Rightarrow |b|^2 = b^2$ .

3) Es gilt auch:  $a \leq |a| \quad \forall a \in \mathbb{R}$ , denn

dann ist  $a \cdot b \leq |a| \cdot |b|$  und

$$2 \cdot a \cdot b \leq 2 \cdot |a| \cdot |b|$$

$\left. \begin{array}{l} 1. \text{ Fall: } a \geq 0 \Rightarrow  a  = a \\ a \leq a \Leftrightarrow a \leq  a  \end{array} \right\}$
$\left. \begin{array}{l} 2. \text{ Fall: } a < 0 \Rightarrow  a  = -a \\ a < 0 \Rightarrow -a > 0 \text{ also} \\ a < 0 < -a \Rightarrow a < -a \\ \Rightarrow a <  a  \end{array} \right\}$

4) Zusammen:  $(a+b)^2 \leq |a|^2 + 2 \cdot a \cdot b + |b|^2$

$$\leq |a|^2 + 2|a| \cdot |b| + |b|^2 = (|a| + |b|)^2$$

$\uparrow$  1. bin. Formel

also:  $(a+b)^2 \leq (|a| + |b|)^2$

$$\Rightarrow |a+b| = \sqrt{(a+b)^2} \leq \sqrt{(|a| + |b|)^2} = |a| + |b|$$

Welche allgemeinen Strukturen stecken hinter unseren Zahlensystemen?

→ algebraische Strukturen

Es geht um „Rechnen“ in einer Menge von Objekten!

Definition:

Gegeben ist eine Menge  $M$ ,  $M \neq \emptyset$ , eine Verknüpfung auf  $M$  (Rechenoperation auf  $M$ ) ist eine Abbildung  $\otimes: M \times M \rightarrow M$ , d.h. jeder Typel  $(a, b) \in M$  wird genau ein Element  $a \otimes b \in M$  zugeordnet.

Beispiele:  $M = \mathbb{Z}$ ,  $+ : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z} : (a, b) \in \mathbb{Z} \times \mathbb{Z} \rightarrow a + b \in \mathbb{Z}$   
 $\cdot : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z} : (a, b) \in \mathbb{Z} \times \mathbb{Z} \rightarrow a \cdot b \in \mathbb{Z}$

Definition:

Gegeben ist eine Menge  $M$ ,  $M \neq \emptyset$  und eine Verknüpfung (Rechenoperation)  $\otimes: M \times M \rightarrow M$ .

1)  $(M, \otimes)$  ist eine Halbgruppe, wenn gilt

Assoziativgesetz:  $a \otimes (b \otimes c) = (a \otimes b) \otimes c, \forall a, b, c \in M$

2)  $(M, \otimes)$  ist eine Gruppe, wenn gilt

Assoziativgesetz:  $a \otimes (b \otimes c) = (a \otimes b) \otimes c, \forall a, b, c \in M$

Existenz eines neutralen Elements:  $\exists n \in M : a \otimes n = a, \forall a \in M$

Existenz inverser Elemente:  $\forall a \in M \exists a^{-1} \in M : a \otimes a^{-1} = n$ ,

gilt zusätzlich das

Kommutativgesetz:  $a \otimes b = b \otimes a, \forall a, b \in M$

heißt  $(M, \otimes)$  abelsche Gruppe.

Beispiele: 1)  $(\mathbb{N}, +)$  ist eine Halbgruppe, denn

$$\forall a, b, c \in \mathbb{N} : a + (b + c) = (a + b) + c$$

$(\mathbb{N}, \cdot)$  ist auch eine Halbgruppe, denn

$$\forall a, b, c \in \mathbb{N} : a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

2)  $(\mathbb{N}, +)$  ist keine Gruppe, denn es gibt kein neutrales Element der Addition ( $0 \notin \mathbb{N}$ )

3)  $(\mathbb{N}, \cdot)$  besitzt mit  $1 \in \mathbb{N}$  das neutrale Element der Multiplikation;  $(\mathbb{N}, \cdot)$  ist aber keine Gruppe, denn es gibt z.B. zur  $2 \in \mathbb{N}$  kein

inverses Element bezüglich der Multiplikation

$$\left(\frac{1}{2} \notin \mathbb{N}\right)$$

4)  $(\mathbb{Z}, +)$  ist eine abelsche Gruppe, denn

$$a + (b + c) = (a + b) + c \quad \forall a, b, c \in \mathbb{Z}$$

$\text{OE } \mathbb{Z}: a + 0 = a \quad \forall a \in \mathbb{Z}, 0 \text{ ist neutrales Element}$

$a \in \mathbb{Z} \Rightarrow -a \in \mathbb{Z} \text{ mit } a + (-a) = 0 \quad \forall a \in \mathbb{Z},$

$-a$  ist das inverse Element zu  $a$

$$a + b = b + a \quad \forall a, b \in \mathbb{Z}$$

5)  $(\mathbb{Z}, \cdot)$  ist Venne Gruppe, denn (wie bei  $(\mathbb{N}, \cdot)$ ) z.B.

$2 \in \mathbb{Z}$  hat bezüglich der Multiplikation in  $\mathbb{Z}$  kein

inverses Element:  $\frac{1}{2} \notin \mathbb{Z}$

### Definition:

Gegeben sind eine Menge  $M, M \neq \emptyset$  und zwei Verknüpfungen (Rechenoperationen)

$$\oplus : M \times M \rightarrow M \text{ und } \otimes : M \times M \rightarrow M.$$

$(M, \oplus, \otimes)$  ist ein Ring, falls gilt:

1)  $(M, \oplus)$  ist eine abelsche Gruppe  $\leftarrow$  bezüglich  $\oplus$

2)  $(M, \otimes)$  ist eine Halbgruppe  $\leftarrow$  bezüglich  $\otimes$

3) Es gilt das Distributivgesetz:  $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c) \quad \forall a, b, c \in M. \leftarrow$  "Verträglichkeit" der beiden Verknüpfungen

$\downarrow$  bezogen auf  $\otimes$

Hat  $(M, \otimes)$  zusätzlich ein neutrales Element, nennt man  $(M, \oplus, \otimes)$  einen Ring mit Eins. Gilt in einem Ring mit Eins zusätzlich in  $(M, \otimes)$  das Kommutativgesetz, nennt man  $(M, \oplus, \otimes)$  einen kommutativen Ring mit Eins.

Beispiel:

1)  $(\mathbb{Z}, +, \cdot)$  ist ein Ring, denn  $(\mathbb{Z}, +)$  ist eine abelsche

Gruppe und  $(\mathbb{Z}, \cdot)$  ist eine Halbgruppe ( $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

$\forall a, b, c \in \mathbb{Z}$ ) und wir haben das Distributivgesetz

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$

2)  $(\mathbb{Z}, +, \cdot)$  ist ein kommutativer Ring mit Eins, denn

wegen  $a = a \cdot 1 \quad \forall a \in \mathbb{Z}$ , ist  $1 \in \mathbb{Z}$  das neutrale Element (Eins)

element) der Multiplikation und  $a \cdot b = b \cdot a \quad \forall a, b \in \mathbb{Z}$

3)  $(\mathbb{Q}, +, \cdot)$  ist ein Kommutativer Ring mit Eins,

außerdem gilt:  $\forall q \in \mathbb{Q}, q \neq 0 \exists \frac{1}{q} \in \mathbb{Q}$  mit  $q \cdot \frac{1}{q} = 1$

also zu  $q \in \mathbb{Q}, q \neq 0$  gibt es  $\frac{1}{q}$  als inverses Element bezügl.  
der Multiplikation:

$\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$ , dann gilt  $(\mathbb{Q}^*, \cdot)$  ist eine abelsche Gruppe

Definition: Eine Menge  $M, M \neq \emptyset$ , mit zwei Verknüpfungen

$\oplus: M \times M \rightarrow M$  und  $\otimes: M \times M \rightarrow M$  heißt Körper, falls gilt

1)  $(M, \oplus, \otimes)$  ist ein Kommutativer Ring mit Eins

2)  $e \in M$  ist das neutrale Element in  $(M, \oplus)$  also

$a \oplus e = e \oplus a = a \quad \forall a \in M$ , denn ist  $M^* = M \setminus \{e\}$

und  $(M^*, \otimes)$  ist eine Kommutative (abelsche) Gruppe.

Beispiele:  $(\mathbb{Q}, +, \cdot)$ ;  $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$

$(\mathbb{R}, +, \cdot)$ ;  $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$

Weitere Beispiele:  $M = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$  Menge mit 4 Elementen

$\oplus: M \times M \rightarrow M$  ist durch folgende Tabelle definiert

$\oplus$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

Hauptdiagonale.

$\bar{0}$  ist das neutrale Element bezügl.

$\oplus$  in  $M$ :  $\bar{a} + \bar{0} = \bar{a} \quad \forall \bar{a} \in M$

Verknüpfungstabelle ist spiegel-symmetrisch zur Hauptdiagonale  $\Rightarrow$

$\bar{a} + \bar{b} = \bar{b} + \bar{a} \quad \forall \bar{a}, \bar{b} \in M$ ,

$\oplus$  ist Kommutativ  
(Assoziativgesetz gilt auch)

$\bar{0} + \bar{0} = \bar{0} \Rightarrow \bar{0}$  ist bezgl.  $\oplus$  invers zu  $\bar{0}$

}

$$\begin{aligned} \bar{1} + \bar{3} = \bar{0} &\Rightarrow \bar{3} \text{ ist bezgl. } \oplus \text{ invers zu } \bar{1} \text{ und} \\ &\quad \bar{1} + \bar{3} = \bar{3} + \bar{1} \text{ also ist } \bar{1} \text{ invers zu } \bar{3} \text{ bezgl. } \oplus \\ \bar{2} + \bar{2} = \bar{0} &\Rightarrow \bar{2} \text{ ist bezgl. } \oplus \text{ invers zu } \bar{2} \end{aligned} \quad \left. \begin{array}{l} \\ \\ \end{array} \right\} (\mathbb{M}, \oplus) \text{ ist eine} \\ \text{abelsche Gruppe}$$

## 15 Vorlesung 15 (16.11.2020)

**15.1 5 Körperaxiome + Beispiele**

**15.2 Definition: Ganzzahlige Teiler**

**15.3 Definition: Primzahl**

**15.4 Definition: Gemeinsame Teiler / Größter gemeinsamer Teiler**

**15.5 Division mit Rest**

Aus der 14. Vorlesung:

Definition: Eine Menge  $M, M \neq \emptyset$ , mit zwei Verknüpfungen

$\oplus: M \times M \rightarrow M$  und  $\otimes: M \times M \rightarrow M$  heißt Körper, falls gilt

1)  $(M, \oplus, \otimes)$  ist ein kommutativer Ring mit Eins

2)  $e \in M$  ist das neutrale Element in  $(M, \oplus)$  also

$a \oplus e = e \oplus a = a \forall a \in M$ , denn ist  $M^* = M \setminus \{e\}$

und  $(M^*, \otimes)$  ist eine kommutative (abelsche) Gruppe.

Merke: Ein Körper  $(M, \oplus, \otimes)$  ist gekennzeichnet durch die

5 Körperaxiome, nämlich

Name	$\oplus$	$\otimes$
Assoziativgesetz	$a \oplus (b \oplus c) = (a \oplus b) \oplus c$	$a \otimes (b \otimes c) = (a \otimes b) \otimes c$
Kommutativgesetz	$a \oplus b = b \oplus a$	$a \otimes b = b \otimes a$
Distributivgesetz		$a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$
Existenz neutraler Elemente	$\exists ! 0 \in M: a \oplus 0 = a \quad \forall a \in M$	$\exists ! 1 \in M: a \cdot 1 = a \quad \forall a \in M$
Existenz inverser Elemente	$\forall a \in M \exists (-a) \in M: a + (-a) = 0$	$\forall a \in M \setminus \{0\} \exists a^{-1} \in M: a \cdot a^{-1} = 1$

Beispiele:

①  $K = \{0, 1\}$  mit  $\oplus: K \times K \rightarrow K$

Verknüpfungstabelle

$\oplus$	0	1
0	0	1
1	1	0

Kommutativ  $\hat{=}$  Spiegel an der Diagonale lässt die Tabelle gleich!

$\otimes: K \times K \rightarrow K$

$\otimes$	0	1
0	0	0
1	0	1

$K = \{0, 1\}$  mit  $\oplus, \otimes$  laut Verknüpfungstabelle ist der kleinste

mögliche Körper (Hinweis: 4. Übung  $\rightarrow 0 \neq 1$  in einem Körper)

②  $(\mathbb{Q}, +, \cdot)$  und  $(\mathbb{R}, +, \cdot)$  sind Körper.

③  $K = \{0, 1, a, b\}$  mit folgenden Verknüpfungen

$$\oplus: K \times K \rightarrow K$$

$\oplus$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

Spiegelsymmetrisch zur Diagonale,  
also Kommutativ, 0 neutrales Element  
für  $\oplus$ , in jeder Zeile steht genau  
einmal die 0, d.h. zu jedem Element  
gibt es genau ein inverses Element  
bezüglich  $\oplus$

$$\odot: K \times K \rightarrow K$$

$\odot$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	a	b	0	1
b	b	a	1	0

$K^* = K \setminus \{0\}$  mit  $\odot$   
in jeder Zeile steht  
genau einmal die 1, d.h.  
zu jedem Element  $\neq 0$

Spiegelsymmetrisch zur Diagonale  
gibt es genau ein inverses  
Element bezüglich  $\odot$ .  
Kommutativ, 1 neutrales  
Element für  $\odot$

Exemplarische (an einem Beispiel) der Distributivgesetze

$$a \odot (b \oplus 1) = a \odot a = b$$

$$(a \odot b) \oplus (a \odot 1) = 1 \oplus a = b$$

$$a \odot (b \oplus 1) = b = (a \odot b) \oplus (a \odot 1)$$

den Distributivgesetz ist  
erfüllt!

### Elementare Zahlentheorie

Zahlentheorie beschäftigt sich mit  $\mathbb{N}, \mathbb{N}_0, \mathbb{Z}$   
und Rechenoperationen für diese Mengen

### Definition:

Gegeben sind  $a, b \in \mathbb{Z}$ ,  $a \neq 0$ . Dann gilt:

①  $a$  teilt  $b$  (geschrieben  $a | b$ ), falls gilt:  $\exists k \in \mathbb{Z}: b = k \cdot a$ .

Man sagt dann auch:  $b$  ist ein (ganzzahliges) Vielfaches von  $a$

②  $\tilde{T}(b) = \{a \in \mathbb{Z} \mid a | b\}$  Teilermenge von  $b$  (Menge aller  
(ganzzahligen) Teiler von  $b$ )

### Beispiele:

$$\textcircled{1} \quad 5 | 15 \text{ dann } 15 = 3 \cdot 5$$

$$5 | -50 \text{ dann } -50 = (-10) \cdot 5$$

$$5 \nmid 7 \text{ dann } 7 \neq k \cdot 5 \forall k \in \mathbb{Z}$$

$\hookrightarrow \times$  steht für „teilt nicht (ganzahlig)“  
 ↗ „Spiegelsymmetrie“

$$\textcircled{2} \quad \tilde{T}(12) = \{-12, -6, \textcolor{blue}{(-4)}, -3, -1, 1, 2, 3, 4, 6, 12\} \subseteq [-12, 12]$$

$$\hookrightarrow \text{dann } 12 = (-3) \cdot (-4) = k \cdot (-4) \text{ mit } k = -3$$

Es gilt folgende Symmetrie:  $a \in \tilde{T}(12) \Leftrightarrow (-a) \in \tilde{T}(12)$

$$\textcircled{3} \quad \tilde{T}(7) = \{-7, -1, 1, 7\}$$

Es gilt folgender Satz:  $\forall a, b \in \mathbb{Z}, a \neq 0$  } es ist ausreichend alle Überlegungen zur (ganzahligen) Teilbarkeit für  $a, b \in \mathbb{N}$  durchzuführen

### Beweisidee:

$$\hookrightarrow 1) \quad a \in T(b) \Leftrightarrow \exists k \in \mathbb{Z} : b = k \cdot a \quad | \cdot (-1) \uparrow \\ \Leftrightarrow \exists -k \in \mathbb{Z} : -b = (-k) \cdot a \quad \downarrow \\ \Leftrightarrow a \in T(-b)$$

$$2) \quad a \in T(b) \Leftrightarrow \exists k \in \mathbb{Z} : b = k \cdot a \quad | \cdot 1 = (-1) \cdot (-1) \uparrow \\ \Leftrightarrow b = (-k) \cdot (-a) \\ \Leftrightarrow (-a) \in T(b)$$

Ab jetzt:  $T(b) = \tilde{T}(b) \cap \mathbb{N} \leftarrow$  wir betrachten nur mit negativen Teileren

$$\hookrightarrow T(b) = \{ a \in \mathbb{N} \mid b = k \cdot a \text{ für ein } k \in \mathbb{Z} \}$$

$$\hookrightarrow T(7) = \tilde{T}(7) \cap \mathbb{N} = \{1, 7\}$$

Definition:  $p \in \mathbb{N}$  heißt Primzahl, falls gilt  $T(p) = \{1, p\}$ , d.h.

$p$  hat (außer 1 und  $p$ ) keine ganzzahligen Teiler!

Bemerkung: 2 ist die einige gerade Primzahl

Es gilt:  $\forall b \in \mathbb{Z}$  ist  $\tilde{T}(b) \subseteq [-|b|, |b|]$  und  $\overline{\tilde{T}(b)} \cap \mathbb{N} \subseteq [1, |b|]$

Jur Intervall  $[-|b|, |b|]$  liegen nur endlich viele ganze Zahlen, d.h.  
 $\tilde{T}(b)$  ist eine endliche Menge!

$T(a, b) = T(a) \cap T(b)$ ; es gilt  $T(a) \cap T(b) \subseteq T(b)$  und  $T(a) \cap T(b) \subseteq T(a)$

Menge der gemeinsamen Teiler von  $a$  und  $b$   $\Rightarrow T(a, b)$  ist als Teilmenge endlicher Mengen ebenfalls eine endliche Menge

$\Rightarrow$  jede endliche Menge (Menge mit endlich vielen Zahlen als Element) kann nach Größe der Zahlen sortiert werden und es gibt ein größtes Element in  $T(a, b)$ .

Definition:

Das größte Element in  $T(a, b) = T(a) \cap T(b)$  heißt  
größter gemeinsamer Teiler von  $a$  und  $b$ , man schreibt dafür ggT(a, b).

Beispiel:  $\tilde{T}(12) = \{-12, -6, -4, -3, -2, -1, 1, 2, 3, 4, 6, 12\}$

$$\tilde{T}(8) = \{-8, -4, -2, -1, 1, 2, 4, 8\}$$

$$\hookrightarrow \tilde{T}(12) \cap \mathbb{N} = \{1, 2, 3, 4, 6, 12\} = \underline{\underline{T(12)}}$$

$$\hookrightarrow \tilde{T}(8) \cap \mathbb{N} = \{1, 2, 4, 8\} = \underline{\underline{T(8)}}$$

$$\Rightarrow T(12, 8) = T(12) \cap T(8) = \{1, 2, 4\} \Rightarrow ggT(8, 12) = 4$$

Gibt es einen Algorithmus zur Berechnung im ggT(a, b) ohne  $T(a)$  und  $T(b)$  einzeln zu ermitteln,  $T(a, b) = T(a) \cap T(b)$  zu bilden, die Zahlen in  $T(a, b)$  der Größe nach anzuordnen und dann das größte

Element anzugeben? Antwort: Ja  $\rightarrow$  euklidischer Algorithmus

Vorbereitung: Division mit Rest

Gegaben sind  $a, b \in \mathbb{Z}$ ,  $a \neq 0$  dann existieren  $k \in \mathbb{Z}$  und  $m \in \mathbb{Z} \cap \mathbb{N}_0$  mit  $b = k \cdot a + m$ ;  $0 \leq m < |b|$   
Reste sind immer nicht negativ  
 $\hookrightarrow$  (ganzheitliches) Teilen von  $b$  durch  $a$  mit Rest  $m$

Beispiel:  $a = 8, b = 21 \Rightarrow 21 = 2 \cdot 8 + 5$

$$a = 8, b = -27 \Rightarrow -27 = (-4) \cdot 8 + 5$$

$\uparrow \quad \uparrow$   
 $k = -4 \quad m = 5$

Behauptung:  $\text{ggT}(a, b) = \text{ggT}(a, m)$  falls gilt  $b = k \cdot a + m, 0 \leq m < |b|$

Beweisidee:  $\text{ggT}(a, b)$  ist das größte Element in  $T(a, b) = T(a) \cap T(b)$

$\text{ggT}(a, m)$  ist das größte Element in  $T(a, m) = T(a) \cap T(m)$

Wir zeigen (mögliche)  $\boxed{T(a, b) = T(a, m)}$

da die Mengen gleich sind,

sind die größten Elemente in beiden Mengen gleich!

## 16 Vorlesung 16 (17.11.2020)

**16.1 Wiederholung Teilmengen, Primzahl, gemeinsame Teiler**

**16.2 Definition: ggT, Division mit Rest, Teilerfremd**

**16.3 Beweis: Division mit Rest**

**16.4 Euklidischer Algorithmus**

**16.5 Lemma von Bézout**

Aus der 15. Vorlesung

$b \in \mathbb{Z}$ , Teilmenge von  $b$ :  $\tilde{T}(b) = \{a \in \mathbb{Z} \mid b = k \cdot a \text{ für ein } k \in \mathbb{Z}\}$   
 $a \in \tilde{T}(b) \Rightarrow -a \in \tilde{T}(b) \Leftarrow \text{"Symmetrie" der Teilmenge } \tilde{T}(b)$   
 Für alle  $a \in \tilde{T}(b)$  gilt:  $-|b| \leq a \leq |b| \Rightarrow \tilde{T}(b)$  ist eine  
endliche Menge.  
 $\tilde{T}(b) = \tilde{T}(-b)$  denn:  $b = k \cdot a \Rightarrow -b = (-k) \cdot a$

→ es reicht aus bei Fragen zur Teilbarkeit in  $\mathbb{Z}$  die positiven Zahlen zu betrachten also Teilbarkeit in  $\mathbb{N}$  zu diskutieren!

$$T(b) = \{a \in \mathbb{N} \mid b = k \cdot a\} \subseteq \mathbb{N}$$

$\uparrow b \in \mathbb{N}$

$$p \in \mathbb{N} \text{ ist Primzahl} \Leftrightarrow T(p) = \{1, p\}$$

Gegaben  $a, b \in \mathbb{N}$ :  $T(a, b) = T(a) \cap T(b)$

$\uparrow$  Menge der gemeinsamen Teiler von  $a$  und  $b$

$T(a, b)$  ist eine endliche Menge, da  $T(a)$  und  $T(b)$  endliche Mengen sind.

In einer endlichen Menge von Zahlen gibt es immer ein größtes (maximales) Element.

Definition:

Der größte gemeinsame Teiler  $\text{ggT}(a, b)$  ist definiert als

$$\text{ggT}(a, b) = \max \{x \mid x \in T(a, b)\}$$

Zur Berechnung des ggT dient der euklidische Algorithmus basierend auf (ganzzahlige) Division mit Rest.

Gegeben sind  $a, b \in \mathbb{Z}$ ,  $a \neq 0$ , dann existieren  $k \in \mathbb{Z}$  und  $r \in \mathbb{N}_0$  mit

$b = k \cdot a + r$ ;  $0 \leq r < |a|$ .  $r$  ist der Rest beim (ganzzahligen) Dividieren von  $b$  durch  $a$ !

Euklidischer Algorithmus als Anwendung des Satzes über Division mit Rest:

Für  $a, b \in \mathbb{Z}$  mit  $b = k \cdot a + r$  nach Division mit Rest

gilt:  $\underbrace{\text{ggT}(a, b)}_{\text{zum Beweis zeigen wir, dass die Teilermengen}} = \underbrace{\text{ggT}(a, r)}$

zum Beweis zeigen wir, dass die Teilermengen  $T(a, b)$  und  $T(a, r)$  gleich sind, dann sind auch die größten Elemente dieser Mengen gleich!

$$\left\{ \begin{array}{l} t \in T(a, b) \Rightarrow t | a \wedge t | b \Rightarrow a = n \cdot t, b = \tilde{n} \cdot t \text{ für } n, \tilde{n} \in \mathbb{Z} \\ \text{mit } b = k \cdot a + r \text{ folgt } r = b - k \cdot a = \tilde{n} \cdot t - k \cdot n \cdot t = (\tilde{n} - k \cdot n) \cdot t \in \mathbb{Z} \\ \Rightarrow t | r \wedge t | a \Rightarrow t \in T(a, r) \\ \rightarrow \text{dann: } T(a, b) \subseteq T(a, r) \end{array} \right.$$

$$\left\{ \begin{array}{l} t \in T(a, r) \Rightarrow t | a \wedge t | r \Rightarrow a = m \cdot t \wedge r = \tilde{m} \cdot t \text{ für } m, \tilde{m} \in \mathbb{Z} \\ \text{mit } b = k \cdot a + r \text{ folgt } b = k \cdot m \cdot t + \tilde{m} \cdot t = (\underbrace{k \cdot m + \tilde{m}}_{\in \mathbb{Z}}) \cdot t \\ \Rightarrow t | b \wedge t | a \Rightarrow t \in T(a, b) \\ \rightarrow \text{dann: } T(a, r) \subseteq T(a, b) \end{array} \right.$$

Insgesamt:  $T(a, r) = T(a, b)$

Gesucht  $\text{ggT}(a, b)$ , dann: Führe Division mit Rest aus

$a \leq b$   $\xrightarrow{}$

$b = k \cdot a + r$

$\Rightarrow \boxed{\text{ggT}(a, b) = \text{ggT}(a, r)}$

und wiederhole diesen Schritt bis  $r = 0$  ist;  
der letzte von 0 verschiedene Rest in der Schrittfolge ist der gesuchte  $\text{ggT}(a, b)$ !

Beispiel: 1) ggT(426, 54)

$$426 = \overbrace{7 \cdot 54}^{378} + 48$$

$$54 = 1 \cdot 48 + 6$$

$$48 = 8 \cdot 6 + 0$$

$\left. \begin{array}{l} \leftarrow \text{ggT}(426, 54) = \text{ggT}(54, 48) \\ \leftarrow \text{ggT}(54, 48) = \text{ggT}(48, 6) \\ \leftarrow \text{Rest } r=0 \text{ Algorithmus endet} \end{array} \right\}$

(letzter von 0 verschiedener Rest: ) 6 = ggT(426, 54)

2) ggT(1312, 251)

$$1312 = \overbrace{5 \cdot 251}^{1255} + 57$$

$$251 = \overbrace{4 \cdot 57}^{228} + 23$$

$$57 = \overbrace{2 \cdot 23}^{46} + 11$$

$$23 = 2 \cdot 11 + 1$$

$$11 = 11 \cdot 1 + 0$$

$\left. \begin{array}{l} \leftarrow \text{ggT}(1312, 251) = \text{ggT}(251, 57) \\ \leftarrow \text{ggT}(251, 57) = \text{ggT}(57, 23) \\ \leftarrow \text{ggT}(57, 23) = \text{ggT}(23, 11) \\ \leftarrow \text{ggT}(23, 11) = \text{ggT}(11, 1) \\ \leftarrow \text{Rest } r=0 \text{ Algorithmus endet} \end{array} \right\}$

(letzter von 0 verschiedener Rest) 1 = ggT(1312, 251)

Definition: Zwei Zahlen  $a, b \in \mathbb{Z}$  heißen teilerfremd, falls

gilt  $\text{ggT}(a, b) = 1$ , d.h.  $T(a, b) = \{1\}$

Beispiel: 1312 und 251 sind teilerfremd!

Beweis zum Teilen mit Rest

Gegeben sind  $a, b \in \mathbb{Z}$ ,  $a \neq 0$ , dann existieren  $k \in \mathbb{Z}$  und  $r \in \mathbb{N}_0$  mit

$b = k \cdot a + r$ ;  $0 \leq r < |a|$ .  $r$  ist der Rest beim (ganzzahligen) Dividieren von  $b$  durch  $a$ !

1) Wegen  $T(b) = T(-b)$  reicht es aus, den Satz für  $a, b \in \mathbb{N}$  zu beweisen!

2) Es reicht aus  $a < b$  anzunehmen, denn für  $a = b$  hat

$$\text{man } b = 1 \cdot b + 0 = \underbrace{1 \cdot a}_{b=a} + \underbrace{0}_{r=0} = k \cdot a + r \text{ mit } k=1, r=0 < a$$

3) Es reicht aus  $a \geq 2$  zu betrachten, denn

$$\text{für } a=1 \text{ gilt } b = b \cdot 1 + 0 = b \cdot a + 0 = k \cdot a + r \text{ mit } k=b, r=0 < a=1$$

4) Zu beweisen bleibt: Für  $a, b \in \mathbb{N}$  mit  $b \geq a \geq 2$  gilt:

Es existieren  $k, r \in \mathbb{N}$  mit  $b = k \cdot a + r$ ,  $0 \leq r < a$

Beweis durch vollständige Induktion bezogen auf  $b \in \mathbb{N}$

Induktionsanfang  $b=2$ :  $2 = 1 \cdot 2 + 0$   
 $a=2$   $\uparrow$   $\uparrow r=0, 0 \leq r < a$

Induktionsumritt:

Induktionsvoraussetzung Aussage ist wahr für  $b=u$  also

$$u = k \cdot a + r \text{ für ein } k \in \mathbb{N}, 0 \leq r < a$$

Induktionsbehauptung Aussage ist auch wahr für  $u+1$  also

$$u+1 = \tilde{k} \cdot a + \tilde{r} \text{ für ein } \tilde{k} \in \mathbb{N}, 0 \leq \tilde{r} < a$$

Beweis:  $u+1 = (k \cdot a + r) + 1, k \in \mathbb{N}, \underbrace{0 \leq r < a}_{r < a, r \in \mathbb{N}, a \in \mathbb{N} \text{ also } r \leq a-1}$

$\hookrightarrow$  Induktionsvor.

$$= k \cdot a + (r+1)$$

1. Fall:  $r+1 < a \Rightarrow \tilde{k}=k, \tilde{r}=r+1 : u+1 = \tilde{k} \cdot a + \tilde{r} \text{ mit } \tilde{k} \in \mathbb{Z}, 0 \leq \tilde{r} < a$

2. Fall  $r+1=a \Rightarrow u+1 = k \cdot a + \underbrace{(r+1)}_{=a}$

$$= k \cdot a + a$$

$$= (\underbrace{k+1}_{\tilde{k}}) \cdot a = \tilde{k} \cdot a + \tilde{r} \text{ mit } \tilde{k}=k+1 \text{ und } \tilde{r}=0$$

$\uparrow 0 \leq \tilde{r} < a$

Beispiel:  $\text{ggT}(125, 13)=1$  dann 13 ist Primzahl also  $\mathbb{T}(13)=\{1, 13\}$   
 und  $13 \nmid 125$

Der euklidische Algorithmus liefert

$$125 = \overbrace{9 \cdot 13}^{112} + 8$$

$$13 = 1 \cdot 8 + 5$$

$$8 = 1 \cdot 5 + 3$$

$$5 = 1 \cdot 3 + 2$$

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

$\text{ggT}(125, 13)=1$  letzter von 0 verschiedenen Rest

$$2 = 2 \cdot 1 + 0 \quad \text{Punkt 0, Algorithmus endet}$$

„Umkehrung  $\hat{=} \text{ Rückwärtsrechnung}$ “ in diesem Algorithmus

$$\begin{aligned} 1 &= \text{ggT}(125, 13) = 3 - 1 \cdot 2 \\ &= 3 - 1 \cdot (5 - 1 \cdot 3) = (-1) \cdot 5 + 2 \cdot 3 \\ &= (-1) \cdot 5 + 2 \cdot (8 - 1 \cdot 5) = 2 \cdot 8 - 3 \cdot 5 \\ &= 2 \cdot 8 - 3(13 - 1 \cdot 8) = (-3) \cdot 13 + 5 \cdot 8 \\ &= (-3) \cdot 13 + 5(125 - 9 \cdot 13) \\ &= \underbrace{5 \cdot 125}_{s} - \underbrace{48 \cdot 13}_{t} = s \cdot 125 + t \cdot 13 \end{aligned}$$

d.h. es gibt  $s \in \mathbb{Z}$  (hier  $s=5$ ) und  $t \in \mathbb{Z}$  (hier  $t=-48$ ) mit

$$\text{ggT}(125, 13) = s \cdot 125 + t \cdot 13$$

Lemma von Bézout:

Gegaben sind  $a, b \in \mathbb{Z}$ ; dann existieren Zahlen  $s, t \in \mathbb{Z}$  mit

$$\text{ggT}(a, b) = s \cdot a + t \cdot b$$

Beweisidee: euklidischen Algorithmus „Umkehr  $\hat{=} \text{ rückwärts rechnen}$ “  
 math. exakt ist Beweis mit vollständiger Induktion (siehe Skript)

Beispiel:  $\text{ggT}(378, 45)$

$$\left. \begin{array}{l} 378 = \underbrace{8 \cdot 45}_{360} + 18 \\ 45 = \underbrace{2 \cdot 18}_{16} + 9 \\ 18 = 2 \cdot 9 + 0 \end{array} \right\} \Rightarrow \text{ggT}(378, 45) = 9$$

$$\hookrightarrow 9 = 45 - 2 \cdot 18$$

$$= 45 - 2 \cdot (378 - 8 \cdot 45)$$

$$= (-2) \cdot 378 + 17 \cdot 45 = s \cdot 378 + t \cdot 45 \text{ mit } s = -2 \text{ und } t = 17.$$

## 17 Vorlesung 17 (18.11.2020)

**17.1 Teilen mit Rest**

**17.2 Teilen und Äquivalenzrelationen, Restmengen**

**17.3 Rechenoperationen in  $\mathbb{Z}_m$ , Körper?, kommutativer Ring mit Eins?**

Heute (18.11.) 12:00 Uhr bis morgen (19.11.) 18:00 Uhr 1. edX-Test!

$$b, m \in \mathbb{Z} \Rightarrow b = k \cdot m + r \text{ mit } 0 \leq r < |m|$$

Division mit Rest

speziell mit  $m \in \mathbb{N}$  (also  $m \geq 1$ ):  $b = k \cdot m + r$  mit  $0 \leq r < m$

$r$  ist der Rest, der beim ganzzahligen Teilen von  $b$  durch  $m$  entsteht

Bedeutung: Gauß:  $r$  heißt Modul von  $b$  bezüglich  $m$  und

Schreibt dafür  $r = b \bmod m$  → Rest, der beim Teilen von  $b$  durch  $m$  bleibt

auch  $r = b \bmod m \Leftrightarrow b = k \cdot m + r$  mit  $0 \leq r < m$

als Rest  $r$  kommen nur die  $\leftarrow r \in \mathbb{N}_0$  ↑  
Zahlen  $0, 1, 2, \dots, m-1$  in Frage (denn falls  $r = m+l$  für ein  $l \in \mathbb{N}_0$   
gilt:  $b = k \cdot m + r = k \cdot m + (m+l) = (k+1) \cdot m + l \Rightarrow l = b \bmod m$ )

Die möglichen Reste  $0, 1, 2, \dots, m-1$  beim ganzzahligen Teilen durch  $m$

liefern uns folgende Mengen:

$$\bar{0} = \{ b \in \mathbb{Z} \mid b = k \cdot m \} = \{ b \in \mathbb{Z} \mid b = k \cdot m + 0 \}$$

$$\bar{1} = \{ b \in \mathbb{Z} \mid b = k \cdot m + 1 \}$$

:

$$\bar{m-1} = \{ b \in \mathbb{Z} \mid b = k \cdot m + (m-1) \}$$

Beispiel:  $m = 3 \rightarrow \left\{ \begin{array}{l} \bar{0} = \{ b \in \mathbb{Z} \mid b = k \cdot 3 \} \\ = \{ \dots, -9, -6, -3, 0, 3, 6, 9, 12, \dots \} \\ \bar{1} = \{ b \in \mathbb{Z} \mid b = k \cdot 3 + 1 \} \\ = \{ \dots, -8, -5, -2, 1, 4, 7, 10, \dots \} \end{array} \right.$

$$\bar{0} \cup \bar{1} \cup \bar{2} = \mathbb{Z}$$

$$\bar{0} \cap \bar{1} = \emptyset$$

$$\bar{1} \cap \bar{2} = \emptyset$$

$$\bar{2} \cap \bar{0} = \emptyset$$

$$\hookrightarrow -2 = (-1) \cdot 3 + 1$$

$$\bar{2} = \{ b \in \mathbb{Z} \mid b = k \cdot 3 + 2 \}$$

$$= \{ \dots, -7, -4, -1, 2, 5, 8, 11, \dots \}$$

## Teilen durch m ( $m \in \mathbb{N}$ ) und Äquivalenzrelationen

Die zweistellige Relation  $R_m \subseteq \mathbb{Z} \times \mathbb{Z}$  über  $\mathbb{Z}$  ist definiert durch:  
 $(a, b) \in R_m \iff m \mid b - a \iff b - a = k \cdot m \text{ für ein } k \in \mathbb{Z}$

Behauptung:

- 1)  $R_m$  ist eine Äquivalenzrelation
- 2) Für  $m \in \mathbb{N}$  sind die Äquivalenzklassen gerade die Mengen  $\overline{0}, \overline{1}, \dots, \overline{m-1}$

Beweis:

1) reflexiv, symmetrisch, transitiv

$$\hookrightarrow (a, a) \in R_m \quad \hookrightarrow (a, b) \in R_m \Rightarrow (b, a) \in R_m$$

a) reflexiv  $(a, a) \in R_m \quad \forall a \in \mathbb{Z}; \text{ dann } a - a = 0 = 0 \cdot m$   
 $\Rightarrow m \mid a - a$

b) symmetrisch  $(a, b) \in R_m \Rightarrow b - a = k \cdot m$   
 $\Rightarrow a - b = (-k) \cdot m$   
 $\Rightarrow m \mid a - b \Rightarrow (b, a) \in R_m$

c) transitiv  $(a, b) \in R_m \wedge (b, c) \in R_m \Rightarrow$   
 $b - a = k \cdot m \wedge c - b = \tilde{k} \cdot m \Rightarrow$   
 $c - a = (c - b) + (b - a)$   
 $= \tilde{k} \cdot m + k \cdot m = (\tilde{k} + k) \cdot m$   
 $\Rightarrow m \mid c - a \Rightarrow (a, c) \in R_m$

2) zugehörige Äquivalenzklassen

$\bar{a}$  ist Äquivalenzklasse zu  $a$  in  $R_m \Rightarrow$

$$\bar{a} = \{b \in \mathbb{Z} \mid (a, b) \in R_m\}$$

$$= \{b \in \mathbb{Z} \mid b - a = k \cdot m\}$$

$$= \{b \in \mathbb{Z} \mid b = k \cdot m + a\}$$

↑ Menge aller ganzen Zahlen, die beim Teilen durch  $m$  den Rest  $a$  lassen

Beim Teilen durch  $m$  gibt es die Reste  $0, 1, 2, \dots, m-1$

mit den Mengen  $\overline{0}, \overline{1}, \overline{2}, \dots, \overline{m-1} \Rightarrow \bar{a} \in \{\overline{0}, \overline{1}, \overline{2}, \dots, \overline{m-1}\}$

Definition: Für  $m \in \mathbb{N}$ ,  $m \geq 2$  ist definiert

$\mathbb{Z}_m = \{\overline{0}, \overline{1}, \overline{2}, \dots, \overline{m-1}\}$  die Menge der Äquivalenzklassen

der Relation  $R_m$ . Für  $\bar{k} \in \mathbb{Z}_m$  gilt also: Jede Zahl in  $\bar{k}$  lässt beim Teilen durch  $m$  den Rest  $k$  ( $0 \leq k \leq m-1$ ).

Rechenoperationen in  $\mathbb{Z}_m$ :

Beispiel:  $\mathbb{Z}_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$

$$\begin{array}{l} \overline{1} \leftarrow b = k \cdot 5 + 1 \\ \overline{2} \leftarrow \tilde{b} = \tilde{k} \cdot 5 + 2 \end{array} \quad \left. \begin{array}{l} b + \tilde{b} = (k + \tilde{k}) \cdot 5 + 1 + 2 = \underbrace{(k + \tilde{k})}_{l} \cdot 5 + 3 = l \cdot 5 + 3 \\ \Rightarrow b + \tilde{b} \in \overline{3} \end{array} \right\}$$

$\overline{1} + \overline{2} = \overline{3}$

↑ Repräsentanten von  $\overline{1}, \overline{2}$

$$\begin{array}{l} \overline{2} \leftarrow \tilde{b} = \tilde{k} \cdot 5 + 2 \\ \overline{4} \leftarrow b = k \cdot 5 + 4 \end{array} \quad \left. \begin{array}{l} b + \tilde{b} = \underbrace{(k + \tilde{k})}_{l} \cdot 5 + 2 + 4 = l \cdot 5 + 6 = l \cdot 5 + (5+1) \\ = (l+1) \cdot 5 + 1 \end{array} \right\}$$

$\overline{2} + \overline{4} (= \overline{6}) = \overline{1}$

↑ Repräsentanten von  $\overline{2}, \overline{4}$

$\Rightarrow b + \tilde{b} \in \overline{1}$

$\overline{2} + \overline{4} (= \overline{6}) = \overline{1}$

$\hookrightarrow b = 1 \cdot 5 + 1 \Rightarrow \overline{6} = \overline{1}$

Strich über  $l$  heißt: Bestimme den Rest von  $l$  beim Teilen durch  $m$

Addition in  $\mathbb{Z}_m$  ist definiert durch

$$\overline{l}, \overline{k} \in \mathbb{Z}_m \Rightarrow \overline{l} + \overline{k} = \underbrace{(l+k) \bmod m}_{\substack{\text{Rest, der beim Teilen von } l+k \\ \text{durch } m \text{ bleibt}}} = \overline{l+k}$$

$\mathbb{Z}_m = \{\overline{0}, \overline{1}, \overline{2}, \dots, \overline{m-1}\}$  ist eine endliche Menge, die Addition kann man dann in einer Verknüpfungstabelle darstellen

Beispiel:  $\mathbb{Z}_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$

$\bar{+}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$

$\bar{0}$  ist das neutrale Element der Addition  
in  $\mathbb{Z}_5$ , das inverse Element zu  $\bar{1}$  bz.  
der Addition in  $\mathbb{Z}_5$  ist  $\bar{4}$ , denn  $\bar{1} + \bar{4} = \bar{0}$ ,  
ebenso:  $\bar{2} + \bar{3} = \bar{0}$ ,  $\bar{3} + \bar{2} = \bar{0}$ ,  $\bar{4} + \bar{1} = \bar{0}$

Verknüpfungstafel spiegelsymmetrisch }  $\bar{x} + \bar{t} = \bar{t} + \bar{x}$   
zur Diagonale }  
diese Verknüpfung (Addition) ist Kommutativ

$$\bar{3} + (\bar{4} + \bar{2}) = \overline{\bar{3} + (\bar{4} + \bar{2})} = \overline{(\bar{3} + \bar{4}) + \bar{2}} = (\bar{3} + \bar{4}) + \bar{2}$$

$\swarrow$  Assoziativgesetz in  $\mathbb{Z}$

Für die Addition in  $\mathbb{Z}_5$  gilt auch das Assoziativgesetz!

insgesamt:  $(\mathbb{Z}_5, +)$  ist eine abelsche (Kommutative) Gruppe

allgemein:  $(\mathbb{Z}_m, +)$  ist eine abelsche (Kommutative) Gruppe  
für  $m \in \mathbb{N}, m \geq 2$

Assoziativgesetz gilt (s.o. Reduzieren in  $\mathbb{Z}$ )

Multiplikation in  $\mathbb{Z}_m$  ist definiert durch:  $\bar{k} \cdot \bar{l} = \overline{\bar{k} \cdot l}$

Beispiel:  $\mathbb{Z}_5$ ; die Multiplikation regelt folgende Verknüpfungstabelle

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

$\bar{1}$  ist das neutrale Element bezügl. der  
Multiplikation in  $\mathbb{Z}_5$

$\leftarrow \mathbb{Z}_5^* = \mathbb{Z}_5 \setminus \{\bar{0}\} = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\} \leftarrow$  in jeder  
Zeile der Teiltafel steht genau einmal  $\bar{1}$ ,  
d.h. jedes  $\bar{k} \in \mathbb{Z}_5^*$  hat bezügl. der  
Multiplikation ein inverses Element, z.B.  
 $\bar{3} \cdot \bar{2} = \bar{1}$

Spiegelsymmetrie zur Diagonale

die Multiplikation in  $\mathbb{Z}_5$  ist Kommutativ

$$\text{Distributivgesetz: } \bar{k} \cdot (\bar{l} + \bar{m}) = \overline{\bar{k} \cdot (\bar{l} + \bar{m})} = \overline{(\bar{k} \cdot \bar{l}) + (\bar{k} \cdot \bar{m})} = \overline{(\bar{k} \cdot \bar{l})} + \overline{(\bar{k} \cdot \bar{m})}$$

$\swarrow$  Distributivgesetz in  $\mathbb{Z}$

$$= \bar{k} \cdot \bar{l} + \bar{k} \cdot \bar{m}$$

insgesamt:  $(\mathbb{Z}_5, +, \cdot)$  ist ein Körper (endlicher Körper mit 5 Elementen)

Beispiel:  $\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$

.	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Es gibt kein  $\bar{k} \in \mathbb{Z}_4$  mit  $\bar{2} \cdot \bar{k} = \bar{1}$   
d.h. zu  $\bar{2} \in \mathbb{Z}_4$  gibt es bezgl. der Multiplikation  
kein inverses Element  
 $\mathbb{Z}_4^* = \mathbb{Z}_4 \setminus \{\bar{0}\}$  ist keine Gruppe

$\Rightarrow (\mathbb{Z}_4, +, \cdot)$  ist kein Körper sonder (nur) ein kommutativer Ring mit Eins!

Allgemein:  $(\mathbb{Z}_m, +, \cdot)$  ist ein kommutativer Ring mit Eins.

Frage: Wenn hat  $\bar{k} \in \mathbb{Z}_m$  ein inverses Element bezgl. der Multiplikation in  $\mathbb{Z}_m$ ? Wann ist  $(\mathbb{Z}_m, +, \cdot)$  ein Körper?

Satz:

für  $\bar{k} \in \mathbb{Z}_m$  gilt:  $\bar{k}$  hat ein inverses Element bezgl. der Multiplikation in  $\mathbb{Z}_m$ , falls ggT( $k, m$ )=1 ist (d.h.  $k$  und  $m$  sind teilerfremd).

Beweisidee: Angenommen  $\text{ggT}(k, m) = 1$ , dann gibt es nach dem Lemma von Bézout ganze Zahlen  $s, t \in \mathbb{Z}$  mit  $1 = s \cdot k + t \cdot m$ , damit gilt für die Reste beim Teilen durch  $m$

$$\begin{aligned}\bar{1} &= \overline{s \cdot k + t \cdot m} = \bar{s} \cdot \bar{k} + \bar{t} \cdot \bar{m} \quad \leftarrow \bar{m} = \bar{0} \text{ in } \mathbb{Z}_m \\ &= \bar{s} \cdot \bar{k} + \bar{t} \cdot \bar{0} \quad \leftarrow \bar{t} \cdot \bar{0} = \bar{0} \\ &= \bar{s} \cdot \bar{k}\end{aligned}$$

Es gilt also  $\bar{1} = \bar{s} \cdot \bar{k}$  d.h.  $\bar{s}$  ist das Inverse Element zu  $\bar{k}$  bezgl. der Multiplikation in  $\mathbb{Z}_m$ .

Beispiel:  $\mathbb{Z}_{42}$ ; gesucht ist die Inverse bezgl. der Multiplikation  
zu  $\bar{5}$  in  $\mathbb{Z}_{42}$  (falls es sie gibt).

$\hookrightarrow$  Inverse existiert, falls  $\text{ggT}(42, 5) = 1$  ist

$$42 = 8 \cdot 5 + \underline{\underline{2}}$$

$$5 = 2 \cdot 2 + \underline{\underline{1}} \Leftrightarrow \text{ggT}(42, 5) = 1$$

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

Anwendung des Lemmas von Bézout:

Reste beim Teilen durch 42 bilden!

$$\hookrightarrow 1 = 5 - 2 \cdot \underline{\underline{2}}$$

$$\begin{aligned} &= 5 - 2 \cdot (42 - 8 \cdot 5) \\ &= 17 \cdot 5 + (-2) \cdot 42 \end{aligned}$$

$$\left. \begin{aligned} \Rightarrow \bar{1} &= \overline{17 \cdot 5 + (-2) \cdot 42} \\ &= \overline{17} \cdot \overline{5} + \overline{(-2)} \cdot \overline{42} \\ &= \overline{17} \cdot \overline{5} \end{aligned} \right\}$$

$\Rightarrow \bar{17}$  ist die Inverse zu  $\bar{5}$  bezgl. der Multiplikation in  $\mathbb{Z}_{42}$ .

Probe:

$$17 \cdot 5 = 85 = 2 \cdot 42 + \underline{\underline{1}} \Rightarrow \bar{17} \cdot \bar{5} = \bar{1}$$

## **18 Vorlesung 18 (23.11.2020)**

**18.1 Restklassen mit Primzahlen sind Körper + Beispiel**

**18.2 simultane Kongruenzen**

**18.3 chinesischer Restsatz**

Bemerkungen zur 3. Übung

zur 6. Aufgabe Finden Sie Binome bzw. berechnen Sie mit geeigneten Binomen

c)  $99^2$

$$99^2 = (100-1)^2 = 100^2 - 2 \cdot 1 \cdot 100 + 1^2 = 10000 - 200 + 1 = 9801$$

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

zur 1. Aufgabe: c)  $\sum_{i=0}^{10} \binom{10}{i}$  ←  $(a+b)^n = \sum_{i=0}^n \binom{n}{i} a^{n-i} \cdot b^i$  ↗  $a=1, b=1, n=10$

$$\sum_{i=0}^{10} \binom{10}{i} = \sum_{i=0}^{10} \binom{10}{i} \cdot 1 \cdot 1 = \sum_{i=0}^{10} \binom{10}{i} \cdot 1^{10-i} \cdot 1^i$$

$$= (1+1)^{10} = 2^{10} = 1024$$

siehe z.B.  
8. Vorlesung

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

$$\sum_{k=0}^n (-1)^k \cdot \binom{n}{k} 1^{n-k} \cdot 1^k$$

$$= (1-1)^n = 0^n = 0$$

e)  $\sum_{n=4}^7 \binom{n}{n-2}$  ↗ "stwe" Einsetzen  
 $= \binom{4}{2} + \binom{5}{3} + \binom{6}{4} + \binom{7}{5}$  dann ausrechnen

→ 2. Variante Symmetrie von Binomialkoeffizienten:

$$\binom{n}{k} = \binom{n}{n-k} \text{ also } \binom{n}{n-2} = \binom{n}{n-(n-2)} = \binom{n}{2}$$

$$\sum_{n=4}^7 \binom{n}{n-2} = \sum_{n=4}^7 \binom{n}{2} = \binom{4}{2} + \binom{5}{2} + \binom{6}{2} + \binom{7}{2}$$

$$= \frac{4 \cdot 3}{1 \cdot 2} + \frac{5 \cdot 4}{1 \cdot 2} + \frac{6 \cdot 5}{1 \cdot 2} + \frac{7 \cdot 6}{1 \cdot 2}$$

$$= 6 + 10 + 15 + 21 = 52$$

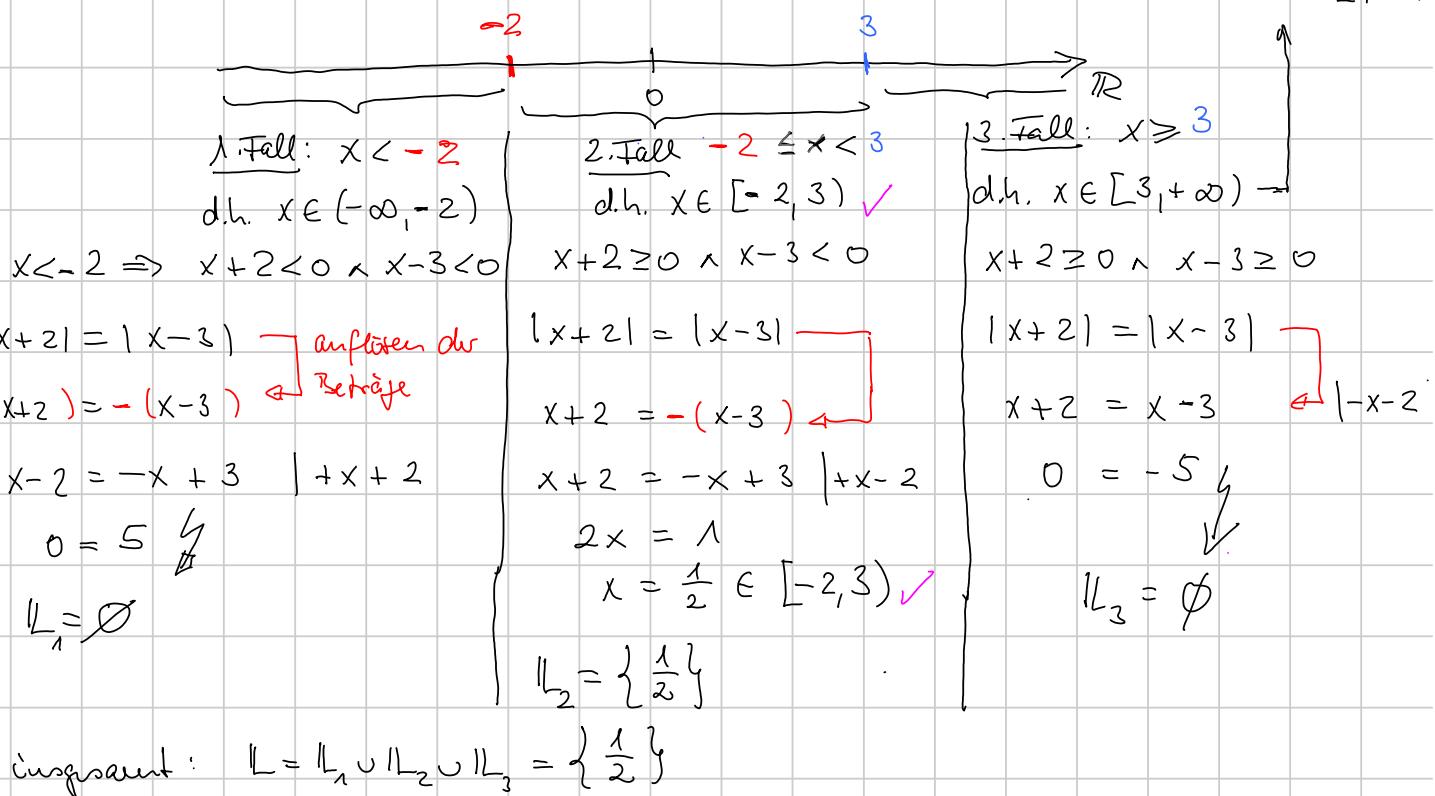
zu Aufgabe 4 d:

$$|x+2| = |x-3|$$

Vorzeichenwechsel bei -2  
Vorzeichenwechsel bei +3

Welche Fälle muss man bei der Fallunterscheidung betrachten!

$$\mathbb{R} = (-\infty, -2) \cup [-2, 3) \cup [3, +\infty)$$



zu Aufgabe 3: Berechnung von Quadratzahlen natürlicher Zahlen, wenn die

letzte Ziffer eine 5 ist!

$$\begin{cases} 125^2 = 15625 \\ \hookrightarrow n=12, n \cdot (n+1) = 12 \cdot 13 \\ \hookrightarrow 12 \cdot 10 + 5 \end{cases}$$

$$\begin{cases} 85^2 = 7225 \\ \hookrightarrow n=8, n \cdot (n+1) = 8 \cdot 9 \\ \hookrightarrow 8 \cdot 10 + 5 \end{cases}$$

Warum geht das?

$$a_n a_{n-1} a_{n-2} \dots a_1 5 = z \quad \text{gesucht } z^2$$

$$z = a_n a_{n-1} a_{n-2} \dots a_1 5 = (\underbrace{a_n a_{n-1} a_{n-2} \dots a_1}_n) \cdot 10 + 5$$

$$\Rightarrow z = n \cdot 10 + 5 \Rightarrow z^2 = (n \cdot 10 + 5)^2$$

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

$$\begin{aligned} &\stackrel{\oplus}{=} (n \cdot 10)^2 + 2 \cdot (n \cdot 10) \cdot 5 + 5^2 \\ &= \underbrace{n^2 \cdot 100}_{(n^2+n)} + n \cdot 100 + 25 \\ &= \underbrace{(n^2+n)}_{n \cdot (n+1)} \cdot 100 + 25 \\ &= n \cdot (n+1) \cdot 100 + 25 \quad \checkmark \end{aligned}$$

Weiter in der Vorlesung: Rechnen in  $\mathbb{Z}_m = \{\bar{k} \mid 0 \leq k \leq m-1\}$

↑ Restklassen beim (ganzzahligen) Teilen durch  $m$

Aus der 17. Vorlesung ist bekannt:

a)  $(\mathbb{Z}_m, +, \cdot)$  ist ein Kommutativer

Ring mit 1

b)  $\bar{k} \in \mathbb{Z}_m$  hat ein inverses Element bezüglich der Multiplikation (also ein  $\bar{l} \in \mathbb{Z}_m$  mit  $\bar{k} \cdot \bar{l} = \bar{l} \cdot \bar{k} = \bar{1}$ ), falls  $k$  und  $m$  teiler-fremd sind, d.h.  $\text{ggT}(k, m) = 1$

$\Rightarrow p \in \mathbb{N}$  Primzahl  $\Rightarrow \text{ggT}(k, p) = 1 \quad \forall k \in \mathbb{Z} \Rightarrow (\mathbb{Z}_p, +, \cdot)$  ist ein Körper, d.h. es gelten die 5 Körperaxiome (wie in  $\mathbb{Q}$  und  $\mathbb{R}$ )

Beispiel:  $(\mathbb{Z}_{13}, +, \cdot)$  13 ist Primzahl  $\Rightarrow (\mathbb{Z}_{13}, +, \cdot)$  ist ein Körper

a) Berechnen Sie das inverse Element bezüglich der Multiplikation von  $\bar{11} \in \mathbb{Z}_{13}$

b)  $(\mathbb{Z}_{13}, +, \cdot)$  ist ein Körper also gelten binomische Formeln!  
Rechnen Sie dies mal für  $(\bar{5} + \bar{7})^2$

Zu a) zunächst euklid. Algorithmus für  $\text{ggT}(11, 13) = 1$

$$13 = 1 \cdot 11 + 2$$

$$11 = 5 \cdot 2 + 1 \leftarrow 1 = \text{ggT}(11, 13)$$

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

Es gibt  $s, t \in \mathbb{Z}$  mit  
 $1 = \text{ggT}(11, 13) = s \cdot 11 + t \cdot 13$

"Rückwärtsrechnen" (Lemma von Bezout)

$$1 = 11 - 5 \cdot 2$$

$$= 11 - 5 \cdot (13 - 1 \cdot 11)$$

$$= (-5) \cdot 13 + 6 \cdot 11$$

} in  $\mathbb{Z}_{13}$  gilt also

$$\bar{1} = \overline{(-5) \cdot 13 + 6 \cdot 11}$$

$$= \overline{(-5) \cdot \underbrace{13}_{\bar{0}} + 6 \cdot \bar{11}} = \bar{6} \cdot \bar{11}$$

$$= \bar{0}$$

$\Rightarrow$  die inverse Zahl zu  $\bar{11}$  in  $\mathbb{Z}_{13}$  bezüglich der Multiplikation ist  $\bar{6}$

Probe:  $\bar{6} \cdot \bar{11} = \bar{66} = \bar{65} + \bar{1} = \underbrace{\bar{5} \cdot \bar{13}}_{\substack{\hookrightarrow 65=5 \cdot 13 \\ =\bar{0}}} + \bar{1} = \bar{1}$

b)  $(\bar{5} + \bar{7})^2 = \bar{12}^2 = \bar{12} \cdot \bar{12} = \overline{12 \cdot 12} = \overline{(12)^2} = \bar{144} = \bar{143} + \bar{1} =$   
 $= \bar{11} \cdot \bar{13} + \bar{1} = \bar{0}$

$$\bar{5}^2 + \bar{2} \cdot \bar{5} \cdot \bar{7} + \bar{7}^2 = \textcircled{\bar{25}} + \bar{5} \cdot \textcircled{\bar{14}} + \textcircled{\bar{49}} = \bar{12} + \bar{5} + \bar{10}$$

$$\bar{14} = \bar{1} \cdot \bar{13} + \bar{1} = \bar{1} \quad \begin{matrix} \bar{12} \\ \parallel \\ \bar{1} \end{matrix} \quad \begin{matrix} \bar{11} \\ \parallel \\ \bar{10} \end{matrix} = \bar{27} = \bar{2} \cdot \bar{13} + \bar{1} = \bar{1} - \bar{0}$$

$$\bar{49} = \overline{39+10} = \bar{3} \cdot \bar{13} + \bar{10} = \bar{10}$$

$$(\bar{5} + \bar{7})^2 = \bar{5}^2 + \bar{2} \cdot \bar{5} \cdot \bar{7} + \bar{7}^2$$

$$\bar{25} = \bar{13} + \bar{12} = \bar{12}$$

Merke: Potenzen ist wiederholtes Multiplizieren mit dem selben Faktor  
also gilt für  $\bar{k} \in \mathbb{Z}_m$ :  $\bar{k}^n = (\bar{k}^n)$

### Einführung in „simultane Kongruenzen“

c) Bemerkung zu Bezeichnungen:

$$\begin{aligned} \bar{k} \in \mathbb{Z}_m \Rightarrow \bar{k} &= \{ b \in \mathbb{Z} \mid b \text{ hat beim Teilen durch } m \text{ den Rest } k \} \\ &= \{ b \in \mathbb{Z} \mid m \mid b - k \text{ d.h. } m \text{ teilt } b - k \} \\ &= \{ b \in \mathbb{Z} \mid (k, b) \in R_m \} \end{aligned}$$

↑ Äquivalenzrelation aus der 17. Vorlesung

statt  $(k, b) \in R_m$  sagt man auch „ $k$  ist Kongruent zu  $b$  modulo  $m$ “  
und schreibt dafür  $k \equiv b \pmod{m}$

↑ ist Kongruent zu

b) Was sind „simultane Kongruenzen“?

Beispiel: Nikolaus verteilt Geschenke. Wenn er in jedem Haushalt 3 Geschenke abgibt, hat er zum Schluss 2 Geschenke übrig.  
Wenn er in jedem Haushalt 5 Geschenke abgibt, hat zum Schluss 4 Geschenke übrig.

Wieviel Geschenke hat der Nikolaus mindestens dabei? Gibt es weitere mögliche Anzahlen von Geschenken?

↓ Geschenkset mit Nikolaus 15 = 3.5

$$\text{③ Geschenke / 2 Rest} : S_1 = \{2, 5, 8, 11, 14, 17, 20, 23, 26, 29, \dots\}$$

$$\textcircled{5} \text{ Geschenke / 4 Rest: } S_2 = \{4, 9, \textcolor{blue}{14}, 13, 24, \textcolor{magenta}{29}, 34, \dots\}$$

$15 = 3 \cdot 5$

Der Nikolaus hat mindestens 14 Geschenke dabei, weitere Möglichkeiten

und  $X_k = 14 + k \cdot 3.5$ ,  $\tilde{x} = 14$  ist kleinste positive Lösung!

$$\bar{x} = \bar{2} \text{ in } \mathbb{Z}_3 \leftarrow x \equiv 2 \pmod{3} \quad \left\{ \begin{array}{l} 2, \text{ simultane Kongruenzen} \end{array} \right.$$

$$\bar{x} = \bar{4} \quad \text{in } \mathbb{Z}_5 \quad \leftarrow \quad x \equiv 4 \pmod{5}$$

Allgemein gilt:

Satz (chinesischer Restsatz für zwei simultane Kongruenzen):

## Die simultanen Kongruenzen

$\bar{x} = \bar{n}$  in  $\mathbb{Z}_{m_1}$  und  $\bar{x} = \bar{k}$  in  $\mathbb{Z}_{m_2}$

sind lösbar, wenn gilt:  $\text{ggT}(m_1, m_2) = 1$ .

Es gilt dann:  $x_0 = n \cdot a \cdot m_2 + k \cdot b \cdot m_1$  ist **eine** Lösung, falls gilt  $\bar{a} \cdot \bar{m}_2 = \bar{1}$  in  $\mathbb{Z}_{m_1}$  und  $\bar{b} \cdot \bar{m}_1 = \bar{1}$  in  $\mathbb{Z}_{m_2}$ .

Weitere (positive) Lösungen sind  $x = x_0 + i \cdot m_1 \cdot m_2$  für  $i \in \mathbb{Z}$  (solange  $x \geq 0$  gilt).

## Bemerkung:

- a)  $\text{ggT}(m_1, m_2) = 1$  heißt  $m_1$  und  $m_2$  sind teilerfremd

b)  $x_0 = n \cdot a \cdot m_2 + k \cdot b \cdot m_1$  mit  $\bar{a} \cdot \bar{m}_2 = \bar{1}$  in  $\mathbb{Z}_{m_1}$  und  $\bar{b} \cdot \bar{m}_1 = \bar{1}$  in  $\mathbb{Z}_{m_2}$   
 ist nicht immer sofort die kleinste pos. Lösung sondern auf jeden Fall  
 1 Lösung von den unendlich vielen Möglichkeiten  $x = x_0 + i \cdot m_1 \cdot m_2, i \in \mathbb{Z}$

c) Wie sieht das in unserem Beispiel aus:

$$n=2, m_1=3 \quad \left. \begin{array}{l} \\ K=4, m_2=5 \end{array} \right\} \text{gesucht in } \mathbb{Z}_3: \bar{a} \text{ mit } \bar{a} \cdot \bar{5} = \bar{1} \text{ in } \mathbb{Z}_3$$

gibt es in  $\mathbb{Z}_5$ :  $\bar{b}$  mit  $\bar{b} \cdot \bar{3} = \bar{1}$  in  $\mathbb{Z}_5$

$\bar{b} \cdot \bar{3} = \bar{1}$  in  $\mathbb{Z}_5 \rightarrow$  Lösung durch "Hingucker"  $\bar{b} = \bar{2}$

$\bar{a} \cdot \bar{5} = \bar{1}$  in  $\mathbb{Z}_3 \Rightarrow \bar{a} \cdot \bar{2} = \bar{1}$  in  $\mathbb{Z}_3 \rightarrow$  Lösung durch "Hingucker"  $\bar{a} = \bar{2}$

also:  $x_0 = 2 \cdot 2 \cdot 5 + 4 \cdot 2 \cdot 3 = 20 + 24 = \underline{\underline{44}}$

## **Vorlesung 19 (24.11.2020)**

**Chinesischer Restsatz: Beweis, Beispiel**

**Allgemeiner chinesischer Restsatz**

**RSA: Anwendung von modularer Arithmetik**

Allgemein gilt:

**Satz (chinesischer Restsatz für zwei simultane Kongruenzen):**

Die simultanen Kongruenzen

$\bar{x} = \bar{n}$  in  $\mathbb{Z}_{m_1}$  und  $\bar{x} = \bar{k}$  in  $\mathbb{Z}_{m_2}$  ✓  
sind lösbar, wenn gilt:  $\text{ggT}(m_1, m_2) = 1$ .

Es gilt dann:  $x_0 = n \cdot a \cdot m_2 + k \cdot b \cdot m_1$  ist eine Lösung, falls gilt  $\bar{a} \cdot \bar{m}_2 = \bar{1}$  in  $\mathbb{Z}_{m_1}$  und  $\bar{b} \cdot \bar{m}_1 = \bar{1}$  in  $\mathbb{Z}_{m_2}$ .

Weitere (positive) Lösungen sind  $x = x_0 + i \cdot m_1 \cdot m_2$  für  $i \in \mathbb{Z}$  (solange  $x \geq 0$  gilt).

Beweis: ①  $\text{ggT}(m_1, m_2) = 1 \Rightarrow$  (euklid. Algor. & Lemma von Bézout)

es existiert  $\bar{a}$  in  $\mathbb{Z}_{m_1}$  mit  $\bar{a} \cdot \bar{m}_2 = \bar{1}$  in  $\mathbb{Z}_{m_1}$ ; a)

es existiert  $\bar{b}$  in  $\mathbb{Z}_{m_2}$  mit  $\bar{b} \cdot \bar{m}_1 = \bar{1}$  in  $\mathbb{Z}_{m_2}$  b)

② Bildet  $x_0 = n \cdot a \cdot m_2 + k \cdot b \cdot m_1$  mit a, b aus ①, dann gilt

$$\begin{aligned} \text{(2.1) in } \mathbb{Z}_{m_1}: \quad \bar{x}_0 &= \overline{n \cdot a \cdot m_2 + k \cdot b \cdot m_1} \\ &= \overline{n} \cdot \overline{a} \cdot \overline{m}_2 + \overline{k} \cdot \overline{b} \cdot \overline{m}_1 = \overline{n} \quad \checkmark \\ &\quad \underbrace{\overline{a}}_{\text{a)}} = \bar{1} \quad \underbrace{\overline{b}}_{\text{b)}} = \bar{1} \end{aligned}$$

$$\begin{aligned} \text{(2.2) in } \mathbb{Z}_{m_2}: \quad \bar{x}_0 &= \overline{n \cdot a \cdot m_2 + k \cdot b \cdot m_1} \\ &= \overline{n} \cdot \overline{a} \cdot \overline{m}_2 + \overline{k} \cdot \overline{b} \cdot \overline{m}_1 = \bar{k} \quad \checkmark \\ &\quad \underbrace{\overline{a}}_{\text{a)}} = \bar{0} \quad \underbrace{\overline{b}}_{\text{b)}} = \bar{1} \end{aligned}$$

Beispiel: Lösen Sie folgende simultane Kongruenzen

$$\bar{x} = \bar{10} \text{ in } \mathbb{Z}_{101} \rightarrow x \equiv 10 \pmod{101} \quad \left. \begin{array}{l} \text{alternative} \\ \text{Schreibweise} \end{array} \right\}$$

$$\bar{x} = \bar{11} \text{ in } \mathbb{Z}_{47} \rightarrow x \equiv 11 \pmod{47} \quad \left. \begin{array}{l} \text{alternative} \\ \text{Schreibweise} \end{array} \right\}$$

Geben Sie und die kleinste pos. Zahl  $x$  an, die die gegebenen simultanen Kongruenzen löst.

①  $\text{ggT}(101, 47)$  bestimmen

$$101 = 2 \cdot 47 + 7$$

$$47 = 6 \cdot 7 + 5$$

$$7 = 1 \cdot 5 + 2$$

$$5 = 2 \cdot 2 + 1 \quad \leftarrow \text{ggT}(101, 47) = 1$$

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

⇒ Problem lösbar

② Lemma von Bezout anwenden und Inverse (begr. Kult.) bestimmen

$$\begin{aligned}
 1 &= 5 - 2 \cdot 2 \\
 &= 5 - 2 \cdot (7 - 1 \cdot 5) \\
 &= (-2) \cdot 7 + 3 \cdot 5 \\
 &= (-2) \cdot 7 + 3 \cdot (47 - 6 \cdot 7) \\
 &= 3 \cdot 47 - 20 \cdot 7 \\
 &= 3 \cdot 47 - 20 \cdot (101 - 2 \cdot 47) \\
 &= (-20) \cdot 101 + 43 \cdot 47
 \end{aligned}$$

②.1 In  $\mathbb{Z}_{47}$  gilt

$$\bar{1} = \overbrace{(-20) \cdot 101 + 43 \cdot 47}^{\text{b}}$$

$$= (\overline{-20}) \cdot \overline{101} + \overline{43} \cdot \overline{47} = \overline{(-20)} \cdot \overline{101}$$

$= \bar{0}$

Inverse zu  $\overline{101}$  in  $\mathbb{Z}_{47}$  ist  $\overline{(-20)} = \overline{(-20+47)} = \overline{27}$

②.2 In  $\mathbb{Z}_{101}$  gilt

$$\bar{1} = \overbrace{(-20) \cdot 101 + 43 \cdot 47}^{\text{b}}$$

$$= (\overline{-20}) \cdot \overline{101} + \overline{43} \cdot \overline{47} = \overline{43} \cdot \overline{47}$$

$= \bar{0}$

Inverse zu  $\overline{47}$  in  $\mathbb{Z}_{101}$  ist  $\overline{43} \leftarrow a$

③ Ergebnis:  $x_0 = a \cdot 47 \cdot 10 + b \cdot 101 \cdot 11$

$$= 43 \cdot 47 \cdot 10 + 27 \cdot 101 \cdot 11 = 150207$$

$x_0 = 150207$  ist eine Lösung des geg. simultanen Kongruenzen

Weitere Lösungen sind  $x = x_0 + k \cdot 47 \cdot 101$  mit  $k \in \mathbb{Z}$ , mit  $k = -10$

erhält man  $x = 150207 - 47470 = 2737$  als kleinste positive Lösung!

Bemerkung:  $\bar{x} = \bar{n}_1$  in  $\mathbb{Z}_{m_1} \rightarrow a_1$  mit  $\bar{a}_1 \cdot \bar{m}_2 = \bar{1}$  in  $\mathbb{Z}_{m_1}$

$\bar{x} = \bar{n}_2$  in  $\mathbb{Z}_{m_2} \rightarrow a_2$  mit  $\bar{a}_2 \cdot \bar{m}_1 = \bar{1}$  in  $\mathbb{Z}_{m_2}$

$\Rightarrow \left\{ \begin{array}{l} x = n_1 \cdot a_1 \cdot m_2 + n_2 \cdot a_2 \cdot m_1 \text{ löst die simultanen Kongruenzen} \\ = n_1 \cdot a_1 \cdot \frac{m_2 \cdot m_1}{m_1} + n_2 \cdot a_2 \cdot \frac{m_2 \cdot m_1}{m_2} \end{array} \right.$

andere Darstellung der  
 chin. Restklassen  
 für 2 Kongruenzen

$$\begin{aligned}
 &= n_1 \cdot a_1 \cdot \frac{M}{m_1} + n_2 \cdot a_2 \cdot \frac{M}{m_2} \quad \leftarrow M = m_1 \cdot m_2 \\
 &\quad \bar{a}_1 \cdot \left( \frac{M}{m_1} \right) = \bar{1} \text{ in } \mathbb{Z}_{m_1} \\
 &\quad \bar{a}_2 \cdot \left( \frac{M}{m_2} \right) = \bar{1} \text{ in } \mathbb{Z}_{m_2} \\
 &= \sum_{i=1}^2 n_i \cdot a_i \cdot \frac{M}{m_i} \quad \text{mit } \bar{a}_i \cdot \left( \frac{M}{m_i} \right) = \bar{1} \text{ in } \mathbb{Z}_{m_i}
 \end{aligned}$$

Diese Darstellung liefert sofort folgende Verallgemeinerung

Satz (Chin. Restsatz für mehrere simultane Kongruenzen)

Die  $K$  simultanen Kongruenzen

$$\bar{x} = \bar{n}_i \text{ in } \mathbb{Z}_{m_i}, 1 \leq i \leq K$$

sind lösbar, falls gilt  $\text{ggT}(m_i, m_j) = 1$  für  $i \neq j$ ,  $1 \leq i, j \leq K$ .

Es gilt dann

$$x_0 = \sum_{i=1}^K n_i \cdot a_i \cdot \frac{M}{m_i} \text{ ist eine Lösung}$$

mit  $M = m_1 \cdot m_2 \cdots m_K$  und  $\bar{a}_i \cdot \left(\frac{M}{m_i}\right) = \bar{1}$  in  $\mathbb{Z}_{m_i}$ ,  $1 \leq i \leq K$ .

Weitere Lösungen sind  $x = x_0 + l \cdot M$  für  $l \in \mathbb{Z}$ .

(Beispiel: Siehe Skript S. 66/67)

Anwendung modularer Arithmetik (= Rechnen mit Restklassen):

Algorithmen zur Verschlüsselung von Daten!

hier: Grundidee des RSA - Algorithmus (asymmetrische Verschlüsselung)

Rivest, Shamir, ↗  
Adelman

Sendu und Empfänger der  
Daten haben verschiedene Schlüssel

Empfänger (E) hat einen „privaten“ Schlüssel und einen  
„öffentlichen“ Schlüssel

Sendu (S) kennt (erhält) den „öffentlichen“ Schlüssel des Empfängers E

S verschlüsselt seine Daten mit dem öffentl. Schlüssel von E und  
sendet diese (verschlüsselten) Daten an E.

Nur E kann mit seinem (geheim gehaltenen) privaten Schlüssel die  
verschlüsselten Daten von S entschlüsseln.

Damit ist der Ablauf des Verfahrens klar aber wie/warum funktioniert das?

Konkaktes Beispiel (Skript S. 68-72)

Sendu (S) ist Student und möchte Empfänger E (Prof. K) verschlüsselt  
mitteln, dass MATHE sein Lieblingsfach ist!

① Kodierung des Wortes MATHE in Zahlen

Text	A	B	C	...	Z	$\Rightarrow$	MATHE	$\rightarrow 13 1 20 8 5$
zahl	1	2	3		26			

Sender (S) will die Zahlenfolge  $13|1|20|8|5$  verschlüsselt senden

② Schlüsselgenerierung (Jetzt vor ① gelaufen)

Der Empfänger E nimmt eine sehr große natürliche Zahl  $N$ , die

das Produkt zweier sehr großer Primzahlen ist:  $N = p \cdot q$

$p, q$  Primzahlen (mit mehreren hundert Dezimalstellen.)

$N$  ist dann (momentan) und mit den leistungsfähigsten Computern  
nicht in (endlicher) angemessener Zeit in das Produkt  $p \cdot q$  faktorisierbar!

Empfänger E hat  $N = p \cdot q$ ; er nimmt  $\tilde{N} = (p-1) \cdot (q-1)$  und rechnet

in  $\mathbb{Z}_{\tilde{N}}$ : Er bestimmt zunächst  $e$  mit  $0 < e < \tilde{N}$  und  $\text{ggT}(e, \tilde{N}) = 1$

$\Rightarrow e$  hat in  $\mathbb{Z}_{\tilde{N}}$  ein inverses Element bezgl. der Multiplikation d;

der Empfänger berechnet d mit  $\bar{d} \cdot \bar{e} = \bar{1}$  in  $\mathbb{Z}_{\tilde{N}}$ .

Der „öffentliche“ Schlüssel des Empfängers ist  $(N, e)$ .

Der „privater“ Schlüssel des Empfängers ist  $(N, d)$ .

Bei hinreichend großen  $N$  kann niemand (kein Supercomputer) in  
(endlicher) angemessener Zeit aus  $(N, e)$  den Schlüssel  $(N, d)$   
berechnen!

Konkretes Beispiel

Empfänger E wählt  $N = 33 = 3 \cdot 11$  also  $p = 3, q = 11$

Empfänger E berechnet  $\tilde{N} = (p-1) \cdot (q-1) = 2 \cdot 10 = 20$

Erechnet also in  $\mathbb{Z}_{20}$ , er wählt  $e = 7$  mit  $\text{ggT}(7, 20) = 1$

und bestimmt d mit  $\bar{d} \cdot \bar{e} = \bar{1}$  in  $\mathbb{Z}_{20}$ : Es ist  $\bar{1} = \bar{7} \cdot \bar{3}$  in  $\mathbb{Z}_{20}$

$\Rightarrow d = 3, \bar{d} = \bar{3}$  in  $\mathbb{Z}_{20}$

„öffentlicher“ Schlüssel ist  $(33, 7)$ , „privater“ Schlüssel ist  $(33, 3)$

③ Sender will  $13|1|20|8|5$  mit dem „öffentlichen“ Schlüssel verschlüsseln.

Für die zu verschlüsselnde Ziffernfolge  $a_1 a_2 \dots a_n$  muss gelten:  $\text{ggT}(a_i, N) = 1$

hier im Beispiel:  $\text{ggT}(33, 13) = 1$ ,  $\text{ggT}(33, 1) = 1$ ,  $\text{ggT}(20, 33) = 1$ ,  $\text{ggT}(8, 33) = 1$

$$\text{ggT}(5, 33) = 1$$

Der Sender S rechnet mit dem „öffentlichen“ Schlüssel  $(N, e) = (33, 7)$

in  $\mathbb{Z}_{33}$  und zwar

$$\overline{13^7} = \overline{62748517} = \overline{7} \text{ denn } 62748517 = 1801470 \cdot 33 + \textcircled{7}$$

$$\overline{1^7} = \overline{1} \text{ denn } 1^7 = 1 = 0 \cdot 33 + \textcircled{1}$$

$$\overline{20^7} = \overline{1280600000} = \overline{26} \text{ denn } 1280000000 = 38787878 \cdot 33 + \textcircled{26}$$

$$\overline{8^7} = \overline{2097152} = \overline{2} \text{ denn } 2097152 = 63550 \cdot 33 + \textcircled{2}$$

$$\overline{5^7} = \overline{78125} = \overline{14} \text{ denn } 78125 = 2367 \cdot 33 + \textcircled{14}$$

$\Rightarrow$  Sender verschlüsselt  $13|1|20|8|5$  in  $\overline{7}|1|26|2|14$

(4) Empfänger E bekommt die Ziffernfolge  $\overline{7}|1|26|2|14$

und entschlüsselt mit seinem „privaten“ Schlüssel  $(N, d) = (33, 3)$

und zwar durch Rechnung in  $\mathbb{Z}_{33}$ :

$$\overline{7^3} = \overline{343} = \overline{13} \text{ denn } 343 = 10 \cdot 33 + \textcircled{13}$$

$$\overline{1^3} = \overline{1} \text{ denn } 1 = 0 \cdot 33 + \textcircled{1}$$

$$\overline{26^3} = \overline{17567} = \overline{20} \text{ denn } 17567 = 532 \cdot 33 + \textcircled{20}$$

$$\overline{2^3} = \overline{8} \text{ denn } 8 = 0 \cdot 33 + \textcircled{8}$$

$$\overline{14^3} = \overline{2744} = \overline{5} = 2744 = 83 \cdot 33 + \textcircled{5}$$

$\Rightarrow$  Empfänger nimmt  $13|1|20|8|5$  als entschlüsselte Nachricht,  
dekodieren mit Buchstabentabelle liefert: M A T H E

Theorie dazu (warum funktioniert dieses Verfahren): Vorsicht margin!

## **Vorlesung 20 (25.11.2020)**

**Prinzip der RSA-Verschlüsselung**

**Eulersche-phi-Funktion**

**Satz von Euler**

**'kleiner' Satz von Fermat**

**Beweis: RSA-Algorithmus**

**Beweis: Satz von Euler**

**Einführung: Lineare Gleichungssysteme**

## Prinzip der RSA-Verschlüsselung

Empfänger:  $N = p \cdot q$  Produkt zweier sehr großer Primzahlen,  
 er rechnet in  $\mathbb{Z}_N$  mit  $\tilde{N} = (p-1) \cdot (q-1)$  folgendes aus:  
 er bestimmt  $e$  mit  $1 < e < \tilde{N}$  und  $\text{ggT}(e, \tilde{N}) = 1 \Rightarrow$   
 $e$  hat in  $\mathbb{Z}_N$  eine Inverse bezüglich der Multiplikation,  
 er berechnet diese Inverse, d.h. er löst  $\bar{e} \cdot \bar{d} = \bar{1}$  in  $\mathbb{Z}_N$   
öffentlicher Schlüssel ist  $(N, e)$   
privater Schlüssel ist  $(N, d)$

Sender: Er kennt den öffentlichen Schlüssel  $(N, c)$ .  
 Er kodiert den zu verschlüsselnden Text in eine  
 Zahlenfolge  $a_1, a_2, \dots, a_k$  mit  $\text{ggT}(a_i, N) = 1, 1 \leq i \leq k$   
 Für jede Zahl  $a_i (1 \leq i \leq k)$  berechnet er in  $\mathbb{Z}_N$   
 die Zahl  $\bar{A}_i = \overline{a_i^c}$   
 die Zahlenfolge  $\bar{A}_1, \bar{A}_2, \dots, \bar{A}_k$  ist dann die verschlüsselte Nachricht!

Empfänger: Er bekommt die Zahlenfolge  $A_1, A_2, \dots, A_k$  und berechnet mit  
 dem privaten Schlüssel  $(N, d)$  in  $\mathbb{Z}_N$  die Zahlen  $\bar{A}_i^d$ ;  
 es gilt  $\bar{A}_i^d = a_i$ , d.h. aus  $A_1, A_2, \dots, A_k$  wird wieder  $a_1, a_2, \dots, a_k$ .

Warum funktioniert das?

Definition: Für  $n \in \mathbb{N}$  wird definiert

a)  $\phi(n) = \{k \in \mathbb{N} \mid 1 \leq k < n \wedge \text{ggT}(k, n) = 1\}$

Das ist die Menge der zu  $n$  teilerfreien nat. Zahlen kleiner als  $n$ .

b) Die Funktion  $\varphi: \mathbb{N} \rightarrow \mathbb{N}$  mit  $\varphi(n) = |\phi(n)| \hat{=} \text{Anzahl der Elemente}$   
 in der Menge  $\phi(n)$ ; diese Funktion heißt Eulersche-phi-Funktion.

Beispiele:

$$n=18 \Rightarrow \phi(18) = \{1, 5, 7, 11, 13, 17\}, \quad \varphi(18) = |\phi(18)| = 6$$

$$\left\{ \begin{array}{l} n=21 \Rightarrow \phi(21) = \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}, \quad \varphi(21) = 12 \\ n=7 \Rightarrow \phi(7) = \{1, 2, 3, 4, 5, 6\}, \quad \varphi(7) = 6 = 7-1 \\ n=3 \Rightarrow \phi(3) = \{1, 2\}, \quad \varphi(3) = 2 = 3-1 \end{array} \right.$$

$\rightarrow 12 = \varphi(21) = \varphi(3 \cdot 7) = \underbrace{\varphi(3)}_{=2} \cdot \underbrace{\varphi(7)}_{=6}$

Bemerkung:

$$1) \ p \in \mathbb{N} \text{ Primzahl} \Rightarrow \varphi(p) = p-1 \text{ denn } \phi(p) = \{1, 2, 3, \dots, p-1\}$$

$$2) \ p, q \in \mathbb{N} \text{ beide Primzahlen} \Rightarrow \varphi(p \cdot q) = \varphi(p) \cdot \varphi(q) = (p-1) \cdot (q-1)$$

Satz von Euler:

Gegeben sind  $a, N \in \mathbb{N}$  mit  $\text{ggT}(a, N) = 1$ , d.h.  $a$  und  $N$  sind teilerfremd.

Dann gilt

$$a^{\varphi(N)} \equiv 1 \pmod{N} \quad \text{anders formuliert: } a^{\varphi(N)} = \bar{1} \text{ in } \mathbb{Z}_N$$

Folgerung daraus ist der „Kleine“ Satz von Fermat, nämlich:

$$\text{Für jede Primzahl } p \in \mathbb{N} \text{ gilt } a^{p-1} \equiv 1 \pmod{p} \Leftrightarrow a^p \equiv a \pmod{p}$$

$$(p \text{ Primzahl} \Rightarrow \varphi(p) = p-1, \text{ dann ist nach dem Satz von Euler } a^{\varphi(p)} = a^{p-1} \equiv 1 \pmod{p})$$

Beweisidee zum RSA - Algorithmus

öffentlicher Schlüssel  $(N, e)$  mit  $N = p \cdot q$   $p$  und  $q$  Primzahlen

$$\varphi(N) = \varphi(p \cdot q) = (p-1) \cdot (q-1) = \tilde{N} \text{ und } \overline{e} \cdot \overline{d} = \bar{1} \text{ in } \mathbb{Z}_{\tilde{N}} = \mathbb{Z}_{\varphi(N)}$$

privater Schlüssel  $(N, d)$  mit diesem  $d$

Klartext als Zahl:  $a$  mit  $\text{ggT}(a, N) = 1$ , verschlüsselt wird  $a$  in

$$\overline{a^e} \in \mathbb{Z}_N \text{ (Rest von } \overline{a} \text{ beim Teilen durch } N): \overline{A} = \overline{a^e}, A \text{ wird gesendet}$$

Zur Entschlüsselung wird berechnet:

$\overline{A^d} \in \mathbb{Z}_N$  berechnet; es ist

$$\overline{A^d} = \overline{(a^e)^d} = \overline{a^{ed}} \text{ in } \mathbb{Z}_N$$

Es gilt  $\overline{e} \cdot \overline{d} = \overline{1}$  in  $\mathbb{Z}_{\varphi(N)} = \mathbb{Z}_{\varphi(N)}$ , d.h.  $e \cdot d$  hat Rest 1 beim Teilen durch  $\varphi(N)$ ; es gibt also ein  $i \in \mathbb{N}$  mit  $e \cdot d = i \cdot \varphi(N) + 1$

$$\Rightarrow \overline{a^{ed}} \text{ in } \mathbb{Z}_N \text{ ist } \overline{a^{i \cdot \varphi(N)+1}} \text{ in } \mathbb{Z}_N \text{ und damit: } \overline{a^{ed}} = \overline{a^{i \cdot \varphi(N)+1}}$$

$$\Rightarrow \underbrace{\overline{a^{e \cdot d}}}_{\overline{A^d}} = \overline{a^{i \cdot \varphi(N)}} \cdot \overline{a} = \overline{a} \cdot (\underbrace{\overline{a^{\varphi(N)}}}_{} )^i = \overline{a} \cdot \overline{1}^i = \overline{a} \cdot \overline{1} = \overline{a}$$

= Satz von Euler

Insgesamt gilt:  $\overline{A^d} = \overline{a}$  in  $\mathbb{Z}_N$ .

Beweisidee zum Satz von Euler  $a, N \in \mathbb{N}$  mit  $\text{ggT}(a, N) = 1$

Behauptung  $a^{\varphi(N)} \equiv 1 \pmod{N}$  ( $\overline{a^{\varphi(N)}} = \overline{1}$  in  $\mathbb{Z}_N$ )

Setze  $l = \varphi(N)$ , dann ist  $\Phi(N) = \{K_1, K_2, \dots, K_e\}$  mit  $\text{ggT}(K_i, N) = 1$  für  $1 \leq i \leq l$ ; d.h.  $\overline{K_1}, \overline{K_2}, \dots, \overline{K_e}$  in  $\mathbb{Z}_N$  haben inverse Elemente bezgl. der Multiplikation in  $\mathbb{Z}_N$ .

Für die Zahlen  $a \cdot K_i$  ( $1 \leq i \leq n$ ) gilt und  $\text{ggT}(a \cdot K_i, N) = 1$ , d.h. und  $\overline{a \cdot K_1}, \overline{a \cdot K_2}, \dots, \overline{a \cdot K_e}$  in  $\mathbb{Z}_N$  haben inverse Elemente bezgl. der Multiplikation in  $\mathbb{Z}_N$ .

Für  $\mathbb{Z}_N^* = \{ \overline{k} \in \mathbb{Z}_N \mid \text{es gibt } \overline{l} \in \mathbb{Z}_N \text{ mit } \overline{k} \cdot \overline{l} = \overline{1} \}$

$$= \{ \overline{k} \in \mathbb{Z}_N \mid \text{ggT}(k, N) = 1 \} = \{ \overline{K_1}, \overline{K_2}, \dots, \overline{K_e} \};$$

es ist aber auch  $\overline{a \cdot K_1}, \overline{a \cdot K_2}, \dots, \overline{a \cdot K_e} \in \mathbb{Z}_N^* = \{ \overline{K_1}, \overline{K_2}, \dots, \overline{K_e} \}$

$\overline{a \cdot K_1}, \overline{a \cdot K_2}, \dots, \overline{a \cdot K_e}$  ist nur eine andere Sortierung (eine Permutation) der Zahlen  $\overline{K_1}, \overline{K_2}, \dots, \overline{K_e}$  und damit in  $\mathbb{Z}_N$ :

$$\overline{K_1 \cdot K_2 \cdot K_3 \cdots K_e} = (\overline{a} \overline{K_1}) \cdot (\overline{a} \overline{K_2}) \cdots (\overline{a} \overline{K_e}) \iff ggt(K_i | N) = 1$$

$$\overline{K_1 \cdot K_2 \cdot K_3 \cdots K_e} = \overline{a^l} \cdot \overline{K_1 \cdot K_2 \cdot K_3 \cdots K_e} = (\overline{a^l}) \cdot (\overline{K_1 \cdot K_2 \cdots K_e})$$

noch Kürzen hat man  $\overline{a} = \overline{a^l}$  in  $\mathbb{Z}_N$  also  $\overline{a} = \overline{a^{φ(N)}}$  in  $\mathbb{Z}_N$

## Lineare Gleichungssysteme und Gauß-Algorithmus

Definition: (Wir betrachten nur die Fälle  $n \leq k$ )

Gegaben sind  $n \cdot k$  reelle Zahlen  $a_{ij}$  ( $1 \leq i \leq n, 1 \leq j \leq k$ ) und  $n$  reelle Zahlen  $b_i$  ( $1 \leq i \leq n$ ).

① Gesucht sind die Werte der  $k$  Unbekannten  $x_j$  ( $1 \leq j \leq k$ ) mit

$$\left. \begin{array}{l} a_{11}x_1 + a_{12}x_2 + \dots + a_{1k}x_k = b_1 \\ a_{21}x_1 + a_{22}x_2 + \dots + a_{2k}x_k = b_2 \\ \vdots \quad \vdots \quad \vdots \quad \vdots \\ a_{n1}x_1 + a_{n2}x_2 + \dots + a_{nk}x_k = b_n \end{array} \right\} \text{in Kurzform}$$

$$\sum_{j=1}^k a_{ij} \cdot x_j = b_i, \quad 1 \leq i \leq n$$

also Lösungen dieses linearen Gleichungssystems mit  $n$  Gleichungen für  $k$  Unbekannte.

② Die Zahlen  $a_{ij}, 1 \leq i \leq n, 1 \leq j \leq k$  heißen Koeffizienten des linearen Gleichungssystems; die Zahlen  $b_i, 1 \leq i \leq n$  heißen rechte Seite des linearen Gleichungssystems und die gesuchten Zahlen  $x_j, 1 \leq j \leq k$  heißen Unbekannte des linearen Gleichungssystems.

## Beispiele:

$$\left. \begin{array}{l} 3x_1 - 5x_2 + x_3 - x_4 = 1 \\ 2x_2 - x_3 = 0 \\ 0 \cdot x_1 + x_2 + x_3 - 5x_4 = -2 \end{array} \right\} \begin{array}{l} \text{lineares Gleichungssystem mit} \\ n=3 \text{ Gleichungen und } k=4 \\ \text{Unbekannten } x_1, x_2, x_3, x_4 \\ \text{rechte Seite: } b_1=1, b_2=0, b_3=-2 \end{array}$$

Koeffizienten  $a_{11} = 3$ ,  $a_{12} = -5$ ,  $a_{13} = 1$ ,  $a_{14} = -1$

$a_{21} = 0$ ,  $a_{22} = 2$ ,  $a_{23} = -1$ ,  $a_{24} = 0$

$a_{31} = 1$ ,  $a_{32} = 1$ ,  $a_{33} = 1$ ,  $a_{34} = -5$

(2)  $\begin{array}{l} 5x - 2y = 0 \\ -2x + 3y = 0 \end{array}$  }  $n=2$  Gleichungen für  $K=2$  Unbekannte nämlich  $x$  und  $y$ , formal  
Unbekannte  $x_1 = x$ ,  $x_2 = y$

Koeffizienten:  $a_{11} = 5$ ,  $a_{12} = -2$ ,  $a_{21} = -2$ ,  $a_{22} = 3$

rechte Seite:  $b_1 = 0$ ,  $b_2 = 0$

Bezeichnung:  $n \leq K$  heißt: Wir betrachten nur lineare Gleichungssysteme mit weniger Gleichungen als Unbekannte ( $n < K$ ) oder genauso viele Gleichungen wie Unbekannte ( $n = K$ ).

Definition:

(1) Die  $n \cdot K$  Koeffizienten  $a_{ij}$ ,  $1 \leq i \leq n$ ,  $1 \leq j \leq K$  eines lin. GLS bilden die Koeffizientenmatrix  $A$  des lin. GLS; das ist ein rechteckiges Zahlenschema mit  $n$  Zeilen und  $K$  Spalten, nämlich

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1K} \\ a_{21} & a_{22} & \dots & a_{2K} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nK} \end{pmatrix} \stackrel{j \text{ heißt Spaltenindex } (1 \leq j \leq K)}{=} (a_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq K}}$$

$\uparrow i$  heißt Zeilenindex ( $1 \leq i \leq n$ )

(2) Die  $K$  Unbekannten  $x_1, x_2, \dots, x_K$  bilden den Vektor der Unbekannten, nämlich

$$\vec{x} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_K \end{pmatrix}$$

(Ein solcher Vektor  $\vec{x}$  kann auch als Matrix mit  $K$  Zeilen und 1 Spalte interpretiert werden)

③ Die  $n$  Zahlen  $b_1, b_2, \dots, b_n$  bilden den Vektor der rechten Seite,  
nämlich

$$\vec{b} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}$$

(Ein solcher Vektor  $\vec{b}$  kann auch als Matrix mit  $n$  Zeilen und 1 Spalte  
interpretiert werden)

Beispiel: 
$$\left. \begin{array}{l} 3x_1 - 5x_2 + x_3 - x_4 = 1 \\ 2x_2 - x_3 = 0 \\ x_1 + x_2 + x_3 - 5x_4 = -2 \end{array} \right\} \Rightarrow$$

$$A = \begin{pmatrix} 3 & -5 & 1 & -1 \\ 0 & 2 & -1 & 0 \\ 1 & 1 & 1 & -5 \end{pmatrix}, \quad \vec{x} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}, \quad \vec{b} = \begin{pmatrix} 1 \\ 0 \\ -2 \end{pmatrix}$$