Die natürlichen Zahlen

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

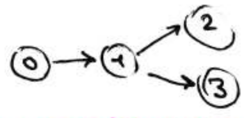
Nach der ÖNORM ist 0 auch eine natürliche Zahl in der Menge der natürlichen Zahlen

Jede natürliche Zahl „n" hat einen Nachfolger „n'", zum weiterzählen

$n' = n+1 \quad S(n) = n+1$

Die Peano-Axiome:

1. 0 ist eine natürliche Zahl
2. Jede natürliche Zahl n hat genau einen Nachfolger



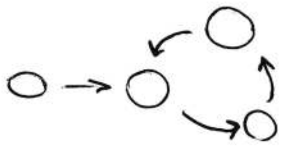
Verzweigungen ausgeschlossen

3. 0 ist nicht Nachfolger einer natürlichen Zahl

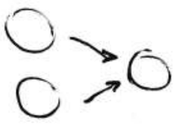
Null als Anfang festgesetzt

4. Verschiedene Zahlen besitzen verschiedene Nachfolger

Wenn $n_1 \neq n_2 \rightarrow$ dann $n_1' \neq n_2'$



Ringe ausgeschlossen.



Verzweigungen und Zwei Pfeile die zur selben Zahl zeigen ausgeschlossen.

⑤ Induktionsaxiom: Fundament der vollständigen Induktion

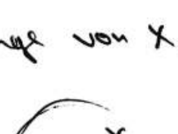
„Wenn 0 teil einer Menge X ist, (X stellt eine Eigenschaft dar) und jede natürliche Zahl n und die Nachfolger n' ebenso teil der Menge sind ...

Dann sind alle natürlichen Zahlen eine Teilmenge von X."

Alternative Beschreibung:

- Eigenschaft kommt 0 zu.
- Überträgt sich von jeder natürlichen Zahl auf den Nachfolger.

⇒ Eigenschaft kommt allen natürlichen Zahlen zu.



Vollständige Induktion:

$$P(n): \forall n \in \mathbb{N}: \sum_{k=1}^{n} k = \frac{n(n+1)}{2}$$

Induktions Anfang I.A.

$P(n_0) = \text{wahr}$

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

Induktions Schritt I.S.

$$P(n) \Rightarrow P(n+1)$$

↓

Induktions Voraussetzung I.V.

zu beweisen:

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

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

Vollständige Induktion

Beispielsweise möchten wir beweisen, dass folgender Satz gilt:

$$1 + 2 + 3 + ... + n = \frac{n \cdot (n + 1)}{2}$$

Zunächst kommt die so genannte Induktionsverankerung: der Beweis, dass der Satz für eine bestimmte kleine Zahl gilt. In diesem Fall wählen wir $n = 1$.

Die Rechnung ist

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

Wir sehen leicht, dass diese Rechnung stimmt.

Als Nächstes kommt der so genannte Schluss von n auf $n + 1$. Dabei nehmen wir an, dass wir den Satz für die Zahl $n - 1$ bereits bewiesen hätten und versuchen, ihn ebenfalls für die Zahl n zu beweisen.

Als Formel ausgedrückt nehmen wir als gegeben an

$(n-1) \rightarrow n$
oder auch
$n \rightarrow (n+1)$

$$1 + 2 + 3 + ... + (n - 1) = \frac{(n - 1) \cdot n}{2}$$

Zu beweisen ist

$$1 + 2 + 3 + ... + n = \frac{n \cdot (n + 1)}{2}$$

Formen wir das etwas um, steht dort

$$1 + 2 + 3 + ... + (n - 1) + n = \frac{n \cdot (n + 1)}{2}$$

Den ersten Teil der linken Seite kennen wir bereits aus unserer Annahme. Wir setzen hierfür die Formel ein, die wir bereits als bewiesen angenommen hatten:

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

Eine kleine Umformung der rechten Seite führt zu

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

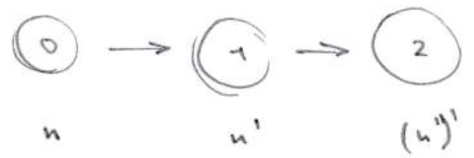
Nun kann man leicht sehen, dass die Gleichung gilt, wir haben bewiesen, dass der Satz für n gilt unter der Voraussetzung, dass er auch für $n-1$ gilt.

Problem

Eines der großen Probleme bei der vorgestellten Lösung des Rucksackproblems lässt sich aber an der Beziehung zwischen dynamischer Programmierung und vollständiger Induktion auch ablesen: Die Lösung funktioniert nur für „ganzzahlige" Problemgrößen.

Alle Kisten bestanden aus einer ganzzahligen Anzahl von Quadraten, ebenso die Schätze. Hier konnte man leicht von einer kleineren Kiste auf eine entsprechend größere schließen. Reale Probleme arbeiten selbstverständlich mit dreidimensionalen Kisten. Jeder „Schatz" hat unterschiedliche Ausmaße in Länge, Breite und Höhe (oder ist sogar völlig unregelmäßig, wie eine lose Krone). Außerdem lassen sich reale Schätze nicht in ganzzahlige Kästchen (Zum Beispiel glatte Zentimeter-Werte) einteilen.
Darüber hinaus berücksichtigt es nicht die begrenzte Anzahl der Gegenstände.

Die „natürliche Ordnung" der natürlichen Zahlen



Als Basis für Vergleiche:

$m \leq n$ $m < n$
$m \geq n$ $m > n$
$m = n$

Die vollständige Induktion

$P(n)$ ... Eigenschaft bzw Prädikat von natürlichen Zahlen

Um zu überprüfen ob $P(n)$ eine Eigenschaft von allen natürlichen Zahlen ist:

1. $P(0)$ überprüfen
   gilt $P(n)$ für Null?
   Hat 0 diese Eigenschaft?

2. Überprüfen ob aus $P(n') = P(n+1)$ gefolgert werden kann unter der Annahme, dass $P(n)$ bereits gültig ist

Nach der Schreibweise der Logik:

$$\underbrace{P(0)}_{1.} \wedge (\forall n \in \mathbb{N}: \underbrace{P(n) \Rightarrow P(n+1)}_{2.}) \Longrightarrow \underbrace{\forall n \in \mathbb{N}: P(n)}_{\text{Gültigkeit}}$$

Gilt für die erste Zahl	Gilt für alle die folgen	gilt allgemein für alle Zahlen $\mathbb{N}$
Induktionsanfang, Induktionsverankerung Induktionsvoraussetzung	Induktionsschritt, Induktionsbehauptung	— Beweis —
— Anker —	— Annahme —	

Beispiel 1.1)

$P(n)$ ist die Aussage:

$$\sum_{k=0}^{n} k = 0+1+2+3 \dots + n = \frac{n(n+1)}{2}$$

$\boxed{P(0)}$ ist wahr weil:

$$\sum_{k=0}^{0} k = 0 = 0 \qquad \frac{0 \cdot (0+1)}{2} = 0$$

→ Also: Induktionsschritt

$$\sum_{k=0}^{\boxed{n+1}} k = 0+1+2 \dots n + (n+1) =$$

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

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

□

Verschiebung des Induktionsanfanges:

+ Es muss nicht immer $P(0)$ bewiesen werden!

Solange $n \geq n_0$ ist → $P(n_0)$ statt $P(0)$ möglich

→ $P(n_0)$
↑
beliebiger Anfang

$P(n)$ ist die Aussage:

$P(n)$: $\underbrace{2^n > n+2}_{\text{erst gültig ab } n \geq 3}$

$P(3)$ ist gültig
$2^3 = 8 > 5 = 2+3$

$P(n) \Rightarrow P(\underline{n+1})$
für $n \geq 3$

$$2^n > n+2 \quad |\cdot 2$$

$$\underbrace{2\cdot 2^n}_{2^{n+1}} > \underbrace{2n+4}_{2(n+2)}$$

$$2n+4 \geq n+4 \geq \underline{(n+1)}+2$$

Ursprünglich
$2^n > \underline{n}+2$

Es gibt viele Beweis-Möglichkeiten:

$P(n-1) \rightarrow P(n)$
$P(n) \rightarrow P(n+1)$
...

Beispiel 1.3)

$P(n)$: n = Primzahl oder mit Primfaktoren darstellbar.

Primzahl: unzerlegbar
- $n > 1$
- nicht Produkt zweier natürlicher Zahlen r, s: $r \cdot s \neq n$
  wobei $r < n$ und $s < n$
- Mit Primzahl-Multiplikation kann man zu jeder beliebigen Zahl gelangen die keine Primzahl ist

Induktionsanfang:
Primzahl $2 = n$
$P(2)$
(gültig)

Induktionsschritt:
$P(k)$ für alle $k \leq n$ ist richtig (Annahme)

Wenn $P(n+1)$ nicht richtig ist
dann muss es mit r und s herstellbar sein

$$\underbrace{r \leq n \quad s \leq n}_{n+1 = r \cdot s} \quad r > 1 \quad s > 1$$

↓ ↓
dadurch trifft aber $P(r)$ und $P(s)$ zu

Also:
$(n+1)$ kann als Produkt von endlich vielen Primfaktoren dargestellt werden

$P(n+1)$ ist wahr
Jede natürliche Zahl kann in Primfaktoren zerlegt werden

Definition von ganzen Zahlen $\mathbb{Z}$

$$\mathbb{Z} = \{\dots -2, \overrightarrow{-1, 0, 1, 2}, \dots\}$$

Die natürliche Ordnung bleibt erhalten

Definition von rationalen Zahlen

$$\mathbb{Q} = \left\{ \frac{m}{n} \mid m \in \mathbb{Z}, n \in \mathbb{Z} \setminus \{0\} \right\}$$

Definition von irrationalen Zahlen

$x^2 = 2 \Rightarrow x = \pm\sqrt{2}$ → nicht als Bruch darstellbar

indirekter Beweis

Angenommen x wäre als Bruch $x = \frac{m}{n}$ darstellbar

1. $\left(\frac{m}{n}\right)^2 = x^2$ also $\left(\frac{m}{n}\right)^2 = 2$

$m^2 \cdot n^{-2} = 2$ oder $m^2 = 2n^2$

↑ siehe 3.

2. Angenommen
m und n sind beide nicht durch Zwei teilbar
weil man sonst $\frac{m/2}{n/2}$ schreiben könnte statt $\frac{m}{n}$
und es irrelevant wäre weil sich die Zweier wegkürzen könnten und
man so zu ungeraden Zahlen gelangen könnte

3. $m^2 \cdot n^{-2} = 2$

m muss gerade sein weil $2n^2$ gerade ist

also:

$m = 2k$

$(2k)^2 = 2(n^2)$

$2\cancel{4}k^2 = 2n^2$

$2k^2 = n^2$ ⟶ n muss auch gerade sein

Widerspruch!

Euklidischer Algorithmus → Erweiterung zur Ermittlung von Linearkombinationen der beiden Zahlen ↳ (Zahlenpaare, Vektoren in linearer Algebra)

$a = 114$

$b = 25$

$ggT(114, 25)$

$114 \mod 25 = 14$	$114 = 4 \cdot 25 + 14$	I $14 = 114 - 4 \cdot 25$
$25 \mod 14 = 11$	$25 = 1 \cdot 14 + 11$	II $11 = 25 - 1 \cdot 14$
$14 \mod 11 = 3$	$14 = 1 \cdot 11 + 3$	III $3 = 14 - 1 \cdot 11$
$11 \mod 3 = 2$	$11 = 3 \cdot 3 + 2$	IV $2 = 11 - 3 \cdot 3$
$3 \mod 2 = 1$	$3 = 1 \cdot 2 + 1$	V $1 = 3 - 1 \cdot 2$
$2 \mod \boxed{1} = 0$	$2 = 2 \cdot 1$	VI –

V: $1 = 3 - 1 \cdot 2$

in 2 einsetzen IV: $1 = 3 - 1 \cdot (11 - 3 \cdot 3) =$ ~~[illegible]~~ 3 $\quad -1 \cdot 11 + 4 \cdot 3$

in 3 einsetzen III: $1 = -1 \cdot 11 + 4 \cdot (14 - 1 \cdot 11) = 4 \cdot 14 - 5 \cdot 11$

in 11 einsetzen II: $1 = 4 \cdot 14 - 5 \cdot (25 - 1 \cdot 14) = -5 \cdot 25 + 9 \cdot 14$

in 14 einsetzen I: $1 = -5 \cdot 25 + 9 \cdot (114 - 4 \cdot 25) =$

$= \underline{-5 \cdot 25} + 9 \cdot 114 \underline{- 36 \cdot 25} =$

$$\boxed{= +\underset{\underset{e}{\downarrow}}{9} \cdot \underset{\underset{a}{\downarrow}}{\boxed{114}} - \underset{\underset{f}{\downarrow}}{41} \cdot \underset{\underset{b}{\downarrow}}{\boxed{25}} = \underset{\underset{\underline{gg}(T)}{\downarrow}}{1}}$$

oder ein Vielfaches vom ggT

bei $ggT(a, b) = d$

$e \cdot a + f \cdot b = d$

$\boxed{9} \cdot a \boxed{-41} \cdot b = 1$

Nützlich in der Informatik für „Integer Programming" bei der zB. nur ganze Zahlen einer Funktion relevant sind

Lösungsalgorithmus für Kongruenzenbeispiele

$8x \equiv 4 \mod 15$

Division durch die einzelnen Elemente nicht erlaubt !

$4 < 15$

$8x \mod 15 = 4$

$$\frac{8x}{15} = \underbrace{y}_{\text{div}} + \underbrace{\frac{4}{15}}_{\text{rest}}$$

gesucht: x
rest ist irrelevant.

$8x = 15y + 4$

$8x - 15y = 4$ → die Gleichung ist nur lösbar wenn ggT(8,15) die Zahl 4 ist oder die Zahl 4 teilt (damit man einfach nach dem erweiterten euklidischen Algorithmus multiplizieren um auf 4 zu kommen)

$ggT(15,8) = 1$

$15 = 8 \cdot 1 + 7 \qquad 7 = 15 - 8 \cdot 1$

$8 = 7 \cdot 1 + 1 \qquad 1 = 8 - 7 \cdot 1$

$7 = ① \cdot 7$

$\overset{ggT}{①} = 8 - 7 \cdot 1$

$1 = 8 - 1 \cdot (15 - 8 \cdot 1)$

$1 = 8 - 15 + 8$

$1 = 8 \cdot \underbrace{2}_{x} + 15 \cdot \underbrace{(-1)}_{y}$

$\cdot 4$

$4 = 8 \cdot \underbrace{8}_{x} + 15 \cdot \underbrace{-8}_{y}$ → irrelevant

$8x \equiv 4 \mod 15$

$8 \cdot 8 \equiv 4 \mod 15$

dadurch gilt:

$64 \mod 15 = 4$

aber nicht nur 8 sondern auch alle Elemente von $\bar{8}$

$\{8 + j \cdot 15,\ j \in \mathbb{Z}\}$

Rechenregeln mit Kongruenzen

wenn: $a \equiv a' \mod m$

$b \equiv b' \mod m$

$\Big\}$ a in Restklasse von a' $\quad \overline{a} = \overline{a'}$

a' in Restklasse von a

b in Restklasse von b' $\quad \overline{b} = \overline{b'}$

b' in Restklasse von b

$\downarrow$

$\overline{a} + \overline{a'} = \overline{a+a'}$

$\overline{b} + \overline{b'} = \overline{b+b'}$

Definition „Restklasse"

$a \equiv a' \mod m$

$a \mod m = a' \mod m$

$\overline{a} = \{a + k \cdot m\}$

$\overline{a'} = \{a' + k \cdot m\}$

$ca \equiv ca' \mod m$ $\longrightarrow$ kürzen: $a \equiv b \mod \left(\frac{m}{ggT(c,m)}\right)$

$a \pm b \equiv a' \pm b' \mod m$

$a \cdot b \equiv a' \cdot b' \mod m$

Erweitern:

$a \equiv b \mod m \rightarrow ca \equiv cb \mod n$

$\nleftarrow$
nur über
Kürzung
möglich

Diophantische Gleichungen $\approx$ Kongruenzen

Teilbarkeit durch 9

Behauptung:

Wenn Quersumme von n, Q(n) durch 9 teilbar ist : $9 \mid Q(n)$

Dann teilt 9 auch 9

$$\downarrow$$

$$9 \mid n$$

Definition:

$$Q(n) = \sum_{k=0}^{j} a_j$$

$$n = \sum_{k=0}^{j} 10^j \cdot a_j$$

Beweis:

$$9 \mid 10^x - 1$$

$$10^x - 1 \mod 9 = 0 \mod 9$$

$$10^x - 1 \equiv 0 \mod 9$$

$$\downarrow$$

Also:

$$\left(\sum_{k=0}^{j} 10^j \right) - 1 \equiv 0 \mod 9 \qquad \mid +1$$

$$\sum_{k=0}^{j} 10^j \equiv 1 \mod 9 \qquad \mid \cdot a^j$$

$$\cancel{\sum_{k=0}^{j} 10^j \cdot a_j}$$

$$\boxed{\sum_{k=0}^{j} 10^j \cdot a_j \equiv \sum a_j \mod 9}$$

Teilbarkeitsregel von 9:

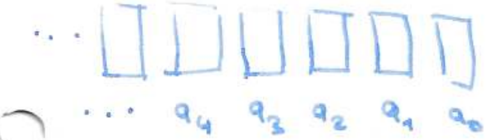
Eine Zahl ist genau dann durch 9 teilbar, wenn die Quersumme / dekadische Ziffernsumme $Q(n)$ durch 9 teilbar ist.

~~Dann~~

$Q(n) \equiv n \bmod 9$

Beweis:

angenommen $n = a_0 + 10 a_1 + 100 a_2 + 1000 a_3 \dots + 10^k a_k$



$\rightarrow \sum_{j=0}^{k} 10^j a_j$

dann ist $Q(n)$:

$\sum_{j=0}^{k} a_j$

$10^j - 1$ besteht nur aus 9

wenn $9 \mid 10^j - 1$ dann gilt $10^j \equiv 1 \bmod 9 \quad | \cdot a_j$

$10^j a_j \equiv a_j \bmod 9$

Alternative Erklärung:

$9 \mid 10 - 1 \rightarrow 10 - 1 : 9 = 1$

OR

$\rightarrow (10 - 1) \bmod 9 = 0$

$\downarrow$

$(10 - 1) \equiv 0 \bmod 9 \quad | +1$

$10 \equiv 1 \bmod 9$

Kleiner Satz von Fermat:

wenn $ggT(a, m) = 1$ (also wenn a sich in anderen Restklassen nicht schon bereits vorkommt)

dann gilt:

$$a^{\varphi(m)} \equiv 1 \mod m$$

\# aller invertierbaren Restklassen von m

$$\overline{1} = \{k \cdot m\} \quad \text{also} \quad a^{\varphi(m)} = k \cdot m$$

Sonderfall bei Primzahlen:

$m \in \mathbb{P}$ dann gilt

$$p \nmid a \rightarrow a^{p-1} \equiv 1 \mod p \quad \text{bzw} \quad p \mid (a^{p-1} - 1)$$

$$\overline{1} = \{k \cdot m\} \quad \text{also} \quad a^{p-1} = k \cdot m \quad \text{also} \quad a^{p-1} = a^{\varphi(m)}$$

ISBN $\boxed{a_1} - \boxed{a_2}\,\boxed{a_3}\,\boxed{a_4} - \boxed{a_5}\,\boxed{a_6}\,\boxed{a_7}\,\boxed{a_8}\,\boxed{a_9} - \boxed{p} \rightarrow p = [0;10]$

Nummer: Wert $10 \cdot a_1 + 9 \cdot a_2 + 8 \cdot a_3 + 7 \cdot a_4 + \dots + 2 \cdot a_9 + p \equiv 0 \mod 11$

Quersumme: $\sum_{k=1}^{9} a_k$

Umformung:

$$10 \cdot a_1 + 9 \cdot a_2 + 8 \cdot a_3 + 7 \cdot a_4 + \dots + 2 \cdot a_9 + p \equiv 0 \mod 11 \quad | -p$$

$$10 \cdot a_1 + 9 \cdot a_2 + 8 \cdot a_3 + \dots + 2 \cdot a_9 \equiv -p \mod 11 \quad | \cdot(-1)$$

$$\underbrace{-10a_1 - 9a_2 - 8a_3 - \dots - 2a_9}_{+11} \equiv p \mod 11$$

$$a_1 + 2a_2 + 3a_3 + 4a_4 + \dots + 9a_9 \equiv p \mod 11$$

Beispiel:

ISBN: 3 - 211 - 82084 - 1

Prüfziffer

$3 + 2 \cdot 2 + 1 \cdot 3 + 1 \cdot 4 + 8 \cdot 5 + 2 \cdot 6 + 0 \cdot 7 + 8 \cdot 8 + 4 \cdot 9 \equiv 1 \mod 11$

$166 \equiv 1 \mod 11$

Probe:

$166 \mod 11 = 1$

$1 \mod 11 = 1$ ✓

Beweis der Effektivität:

Veränderung mit n

$ISBN_1 = S + a \cdot n$

$ISBN_2 = \underbrace{S}_{\text{unveränderter Teil}} + \underbrace{b \cdot n}_{\text{veränderter Teil}}$

dann gilt:

$S + an \equiv S + bn \mod 11$

$a \equiv b \mod 11$

...

?

Invertierbarkeit bei Primzahl-Moduln

(später für Mengen relevant)

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	3	$\bar{2}$	$\bar{1}$

$m = 5$

$5 \in \mathbb{P}$

$\bar{1}^{-1} = \bar{1}$

$\bar{2}^{-1} = \bar{3}$

$\bar{3}^{-1} = \bar{2}$

$\bar{4}^{-1} = \bar{4}$

$\Big\}$ Alle Restklassen $\setminus \bar{0}$ sind invertierbar!

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
2	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

$m = 4$

$4 \in \mathbb{N}$

$\bar{1}^{-1} = \bar{1}$

$\bar{2}^{-1} = /$ → nicht alle Restklassen invertierbar

$\bar{3}^{-1} = \bar{3}$

Die Eulersche φ-Funktion

$$\varphi(m) = |\{a \in \mathbb{Z} \mid 1 \leq a \leq m, \ \text{ggT}(a,m) = 1\}|$$

Anzahl aller invertierbaren Elemente / Restklassen bei modulo m

Beispiel:

$\varphi(3) = 2$ $\quad \varphi(6) = 2 \quad \varphi(5) = 4$

$\text{ggT}(1;3) = 1$

$\text{ggT}(2,3) = 1$

Einfachere Formel zur Berechnung:

$$\text{Es sei } m = \underbrace{p_1^{e1} \cdot p_2^{e2} \cdot \ldots \cdot p_s^{es}}_{\text{Primfaktorzerlegung}}$$

$m = 32$

$32 \mid 2$

$16 \mid 2$

$8 \mid 2$

$4 \mid 2$

$2 \mid 2$

$\rightarrow 32 = 2^5$

$$\varphi(m) = m\left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_n}\right)$$

$$\varphi(32) = 32\left(1 - \frac{1}{2}\right) = 32 \cdot \frac{1}{2} = 16$$

$$\varphi(32) = 16$$

Beispiel

$\varphi(7) = 7 \cdot \left(1 - \frac{1}{7}\right)$

$\varphi(7) = \cancel{7} \cdot \frac{6}{\cancel{7}} = 6$ ✓

~~$\varphi = 16$~~

$\varphi(16) = 16\left(1 - \frac{1}{2}\right)$

$\varphi(16) = 8$ ✓

$$\begin{array}{r|l} 7 & 7 \\ 1 & \end{array} \to \text{Primzahl}$$

$7 = 7^1$

$$\begin{array}{r|l} 16 & 2 \\ 8 & 2 \\ 4 & 2 \\ 2 & 2 \end{array} \qquad 16 = 2^4$$

Seite 21

Beispiel 1.31)

Gesucht: $\overline{15}^{-1}$ bei $\mathbb{Z}_{17}$
↑
„inverse Restklasse"

Meine Erklärung:

Linearfaktor

$(15 \cdot b) - (17 \cdot k) = 1$

weil wenn mehrmals 17 vorkommt es entfernt wird

$\overline{15} \cdot \overline{b} = \overline{1}$ bzw $\overline{15} \cdot \overline{b} \equiv \overline{1}$ mod 17

↳ Das heißt $\overline{15} \cdot \overline{b}$ ist in der Restklasse $\overline{1}$ enthalten und umgekehrt

also: ggT(m, b) = 1

ggT(17, 15) = 1

$17x + 15y = 1$

$17 = 15 \cdot 1 + 2$ | $\textcircled{2} = 17 - 15 \cdot 1$

$15 = 2 \cdot 7 + 1$ | $1 = 15 - 2 \cdot 7$

$2 = \textcircled{1} \cdot 2$

$$1 = 15 - 2 \cdot 7$$

$$1 = 15 - 7 \cdot \textcircled{2}$$

$$1 = 15 - 7 \cdot (17 - 15)$$

$$1 = 15 - 7 \cdot 17 + 7 \cdot 15$$

$$1 = \boxed{8} \cdot 15 - \boxed{7} \cdot 17$$

$x = 8$ $y = -7$

$\overline{15}^{-1} = \overline{8}$ ✓

Wenn $\boxed{\overline{a}}$ eine inverse Klasse $\overline{b}$ besitzt dann gilt

$\boxed{a}b = 1 + q\boxed{m}$ und damit $1 = \boxed{a}b - q\boxed{m}$ ∴ Jeder Teiler von a, m teilt 1.
↑ also ggT(a, m) = 1
beliebiger Faktor

~~Zähne putzen~~

~~Schlafen,~~
~~früh aufstehen~~
~~früh ins~~

Rechenoperationen mit Restklassen:

für mod m:

$\overline{a} + \overline{b} = \overline{a+b}$

$\overline{a} \cdot \overline{b} = \overline{a \cdot b}$

Beispiel:
mod = 9

$\overline{1} + \overline{10} = \overline{11}$

$\{1+9k\} \quad \{10+9k\} \quad \{11+9k\}$

↳ 10 → kann herausgezogen werden
9 + 1 = 10

$\{1+9k\} \quad \{2+9k\}$

Für jede positive ~~[illegible]~~ natürliche Zahl m gibt es auch m Restklassen bezeichnet als $\mathbb{Z}_m$ <

$m = 3 \quad \{\overline{0}, \overline{1}, \overline{2}\}$

ab 3 wiederholt es sich nur selbst!

$\overline{1} \cdot \overline{10} = \overline{10}$

$\{1+9k\} \quad \{10+9k\} \quad \{10+9k\}$ ✓

—"— $+ \{1+9k\} = \{1+9k\}$ ✓

---

mod = 3

+	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

3-3 4-3

·	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

4-3

Satz 1.26

„Für jede positive Zahl $\in \mathbb{N}$ gibt es genau m Restklassen"

$$\mathbb{Z}_m = \{\bar{0}, \bar{1}, \bar{2}, \bar{3} \ldots\ldots \overline{m-1}\}$$

Meine Erklärung:

weil jede Restklasse größer als $\overline{m-1}$ schon mit kleineren ausgedrückt werden kann / in ihnen enthalten ist.

Beispiel:

$\mathbb{Z}_{③}$: $\bar{4} \equiv \bar{1}$ mod 3

$\{1 + 3k\}$ beinhaltet $1 + 3 \cdot 1 = 4$

$\mathbb{Z}_{14}$: $\bar{5} \cdot \bar{3} \equiv \overline{15} \equiv 1$ mod 14

$15 - 14 = 1$

Beweis aus Buch:

Man dividiert $n \in \mathbb{N}$ durch m

$n : m = q$
r Rest

$n = mq + r$

n mod $m = r$

$0 \leqq r < m$

$n \equiv r$ mod m

also

n mod $m = r$ mod m

Beispiel

6 mod 4 = 2

2 mod 4 = 2 weil es kleiner als 4 ist und so überhaupt Rest sein kann!

Es seien unter $\mathbb{Z}_m$
die Restklassen $\bar{a}, \bar{b}$ mit $0 \leqq a < b < m$

ANGENOMMEN

$n \in \bar{a}$
$n \in \bar{b}$

$\bar{a} \equiv \bar{b}$ mod m

bzw

$m \mid (a - n)$

$m \mid (b - n)$

$m \mid \cancel{a}(b - a)$

↯ dann dürfte es keine unterschiedlichen Klassen von anfang an gegeben haben.

Definition:

neutrales Element aka „Nullelement" , „Einselement"
addition multiplikation

$\boxed{\bar{e}} \cdot \bar{a} = \bar{a} \cdot \bar{e} = \bar{a}$

Für alle Elemente „a"
die mit e multipliziert werden muss gelten:
dass sie am Ende selbst herauskommen

multiplikativ inverses Element / inverse Restklasse

a^{-1} → invers von $a \in \mathbb{Z}_n$

$\bar{a}^{-1} \cdot \bar{a} = \bar{a} \cdot \bar{a}^{-1} = \boxed{\bar{1}}$
→ neutrales Element

Beispiel: im mod = 14 bzw $\mathbb{Z}_{14}$
$\bar{5} \cdot \bar{3} \equiv \bar{15} \equiv 1 \bmod 14$
also $\bar{5} \cdot \bar{3} = \bar{1}$

Bsp:
bei $\mathbb{Z}_3$

neutrales Element

+	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

neutrales Element

•	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{1}$

inverse Restklassen

Rechenalgorithmus:

lässt sich mit ggT berechnen:
bzw erweiterten Satz von Euler

$ggT(a,b) = u \cdot a + v \cdot b$
Konstanten

wenn $\mathbb{Z}_{n}$

$ggt(a,n) = 1$ muss sein

$1 = u \cdot a + v \cdot \cancel{b} n$

„~~Satz~~"
„Lemma von Bézout" →

$1 \equiv u \cdot a + v \cdot n \equiv u \cdot a \,(\bmod n$

$a^{-1} \equiv u \,(\bmod n)$

u ist also das inverse Element
von a

Relationen

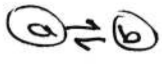
reflexiv

$(a,a) \in R$ für alle $a \in A$

Symmetrisch

$a,b \in A$

immer gleichzeitig



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

antisymmetrisch

$a,b \in A$

entweder ⓐ→ⓑ

oder ⓑ→ⓐ

$(a,b) \in R \wedge (b,a) \in R$ bedeutet $\Rightarrow a=b$

aber nicht gleichzeitig

Also wenn $a \neq b$ ist kann das nur heißen $(a,b) \notin R \vee (b,a) \notin R$

← „höchstens ein Pfeil, Schlingen zugelassen"

asymmetrisch = (antisymmetrisch und ¬ reflexiv)

$a,b \in A$

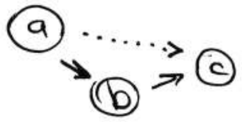
$(a,b) \in R \Rightarrow (b,a) \notin R$

← „höchstens ein Pfeil, Schlingen nicht zugelassen"

transitiv

$a,b,c \in A$

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



bedeutet ⓐ→ⓒ

Objekte mit bestimmten Eigenschaften werden oft zusammengefasst: Äquivalenzrelation

Äquivalenzrelation:

- reflexiv
- symmetrisch
- transitiv

Für $(a,b) \in R$ sagt man: „a ist äquivalent zu b"

Beispiel:

- Identitätsrelation

  $\mathbb{I}_A \subseteq A \times A$

  $\mathbb{I}_A = (a,a)$

Bildet Mengen / Partitionen

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

Wenn R eine Äquivalenzrelation ist.

$$\text{zB} \quad \underset{\text{Partition}}{\underset{\uparrow}{[a]}} = \{ 6, 7, \underset{\text{Vertreter}}{\underset{\uparrow}{9}}, 12 \, .. \}$$

Ordnungsrelation

- reflexiv
- antisymmetrisch
- transitiv

Beispiel: Ordnung der natürlichen Zahlen mit $\leq$

Strikte Ordnungsrelation

- ~~refl~~
- asymmetrisch
- transitiv

→ wie Ordnungsrelation nur ohne $\mathbb{I}_A$

Beispiel: natürliche Ordnung mit $<$

Eine Relation in der Menge der Menschen

$R = \{$ alle Relationen $\}$

Menschen $= \{$ alle Menschen $\}$

$$R \subseteq \underbrace{\text{Menschen} \times \text{Menschen}}_{\text{Ein Mensch kann auch mit sich selbst in Beziehung stehen}}$$

a) R: ist gleich alt wie, ~~oder R: ist ve~~

reflexiv: man ist gleich alt wie man selbst

$I_{\text{Menschen}} = \{$ alle Relationen die Menschen zu sich selbst haben $\}$

Symmetrisch: wenn aRb dann auch bRa

bzw wenn $(a,b) \in R$ dann auch $(b,a) \in R$

↳ dadurch nicht antisymmetrisch oder asymmetrisch

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

b) R: ist verwandt mit

reflexiv: $I_A \subseteq R$

Symmetrisch: wenn aRb, dann auch bRa

transitiv

c) R: ist Mutter von

nicht Reflexiv: $I_A \nsubseteq R$

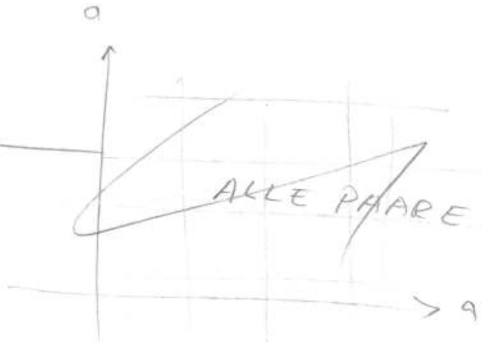
nicht symmetrisch: $aRb \Rightarrow (b,a) \notin R$

nicht transitiv: Großmutter ≠ Mutter

asymmetrisch

~~reflexive Relation:~~

alle ~~Paare (a,a) ∈ A×A~~



Identitätsrelation:

$\mathbb{I}_A = \{ (a,a) \mid a \in A \}$

reflexive Relation:

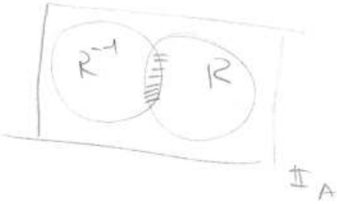
alle Paare $(a,a) \in A \times A$

$\mathbb{I}_A \subseteq R \subseteq A \times A$

} das heißt: $R^{-1} = R$ weil alle bereits inkludiert sind

antisymmetrische Relation:

$R^{-1} \cap R \subseteq \mathbb{I}_A$



asymmetrische Relation:

$R^{-1} \cap R = \{\}$

nsitive Relation:

$R \circ R \subseteq R$

Transitivität:

$\forall a,bc \in A : (aRb \wedge bRc) \Rightarrow aRc$

$\forall n,k,c \in A : (kRc \wedge kRn) \Rightarrow kRn$

Probe: $\downarrow$

① $k \mid c \wedge c \mid n \quad = \quad k \mid n$

② $ggT\left(\frac{c}{k}, k\right) \wedge ggT\left(\frac{n}{c}, c\right) \quad = \quad ggT\left(\frac{n}{k}, k\right)$

① $c = k \cdot f_1$
$n = c \cdot f_2 \longrightarrow n = k \cdot f_1 \cdot f_2$
$k \mid n$

② $ggT\left(\frac{n}{c}, c\right) = 1$

$ggT\left(\frac{\cancel{c} \cdot f_2}{\cancel{c}}, k \cdot f_1\right) = ggT\left(f_2, k \cdot f_1\right) = 1$

$ggT\left(\frac{n}{k}, k\right) =$

$ggT\left(\frac{c \cdot f_2}{\frac{c}{f_1}}, k\right) = ggT\left(\frac{\cancel{c} \cdot f_2}{1} \cdot \frac{f_1}{\cancel{c}}, k\right) = ggT\left(f_1 \cdot f_2, k\right) = 1$

$c \cdot f_2 = n$

$c = k \cdot f_1 \longrightarrow \frac{c}{f_1} = k$

Halbordnung / partielle Ordnung

Weil im Gegensatz zur Totalordnung manche Elemente in keiner Relation zu einander stehen (weil es nicht definiert ist):

$ggT(x,y) \rightarrow$ nur für $\mathbb{N}$ oder $\mathbb{Z}$!

Hassediagramm

(2,2)
(2,4)
(2,6)
(2,10)

(3,3)
(3,6)
(3,9)

(4,4)

(5,5)
(5,10)

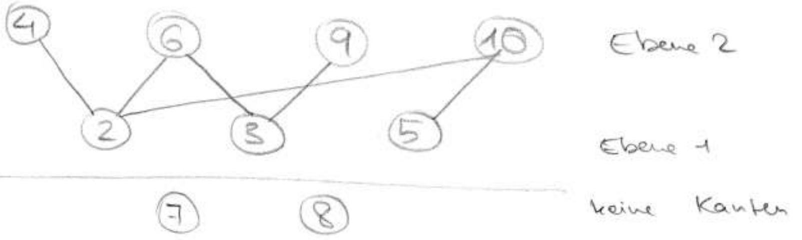
(6,6)

(7,7)

(8,8)

(9,9)

(10,10)



Die Regeln der Kombinatorik

Beispiel: Die Potenzmenge von A, $P(A)$ → Alle möglichen Kombinationen der Elemente aus A:

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

$P(A) = \{\emptyset, c, b, bc, a, ac, ab, abc\}$

a	b	c	
0	0	0	∅
0	0	1	c
0	1	0	b
0	1	1	bc
1	0	0	a
1	0	1	ac
1	1	0	ab
1	1	1	abc

Anzahl der Potenzmengen-Elemente:

2^n bzw $2^{|A|} = |P(A)|$ mit $|A| = n$

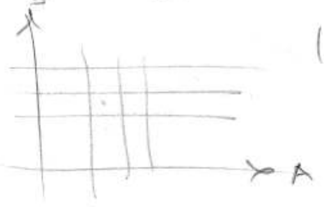
hier:

→ $2^3 = 8$

1) Summenregel

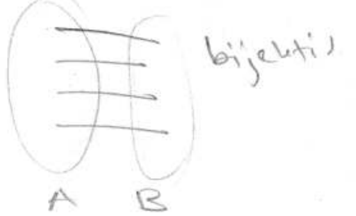
$A \cap B = \emptyset \rightarrow |A \cup B| = |A| + |B|$

2) Produktregel



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

3) Gleichheitsregel

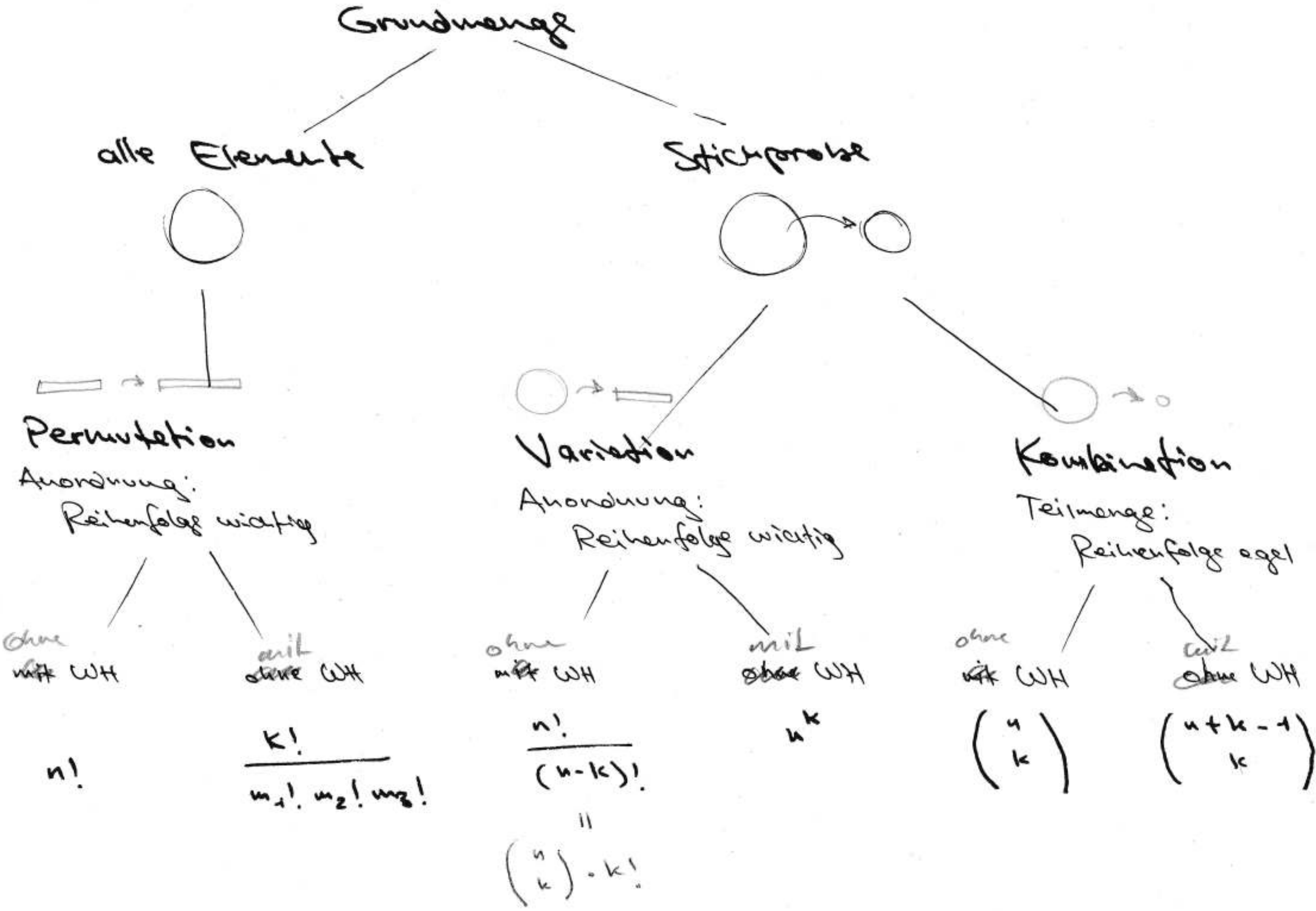


$\exists\, f: \underbrace{A \rightarrow B}_{\text{bijektiv}}$ $\quad |A| = |B|$

Es gibt 2 Problemarten:

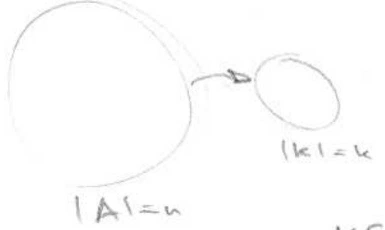
1) Auswahlprobleme → Mengen

2) Anordnungsprobleme → n-Tupel


Grundmenge
alle Elemente
Stichprobe
Permutation
Anordnung:
Reihenfolge wichtig
Variation
Anordnung:
Reihenfolge wichtig
Kombination
Teilmenge:
Reihenfolge egal
ohne ~~mit~~ WH
mit ~~ohne~~ WH
ohne ~~mit~~ WH
mit ~~ohne~~ WH
ohne ~~mit~~ WH
mit ~~ohne~~ WH
$n!$
$\frac{k!}{m_1! \cdot m_2! \cdot m_3!}$
$\frac{n!}{(n-k)!} = \binom{n}{k} \cdot k!$
n^k
$\binom{n}{k}$
$\binom{n+k-1}{k}$

Auswahlen einer Teilmenge

Kombination ohne Wiederholung



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

$K \subseteq A$

Analogie: Multimengen Permutationen

$A := \{a_1, a_2, a_3, a_4, \dots, a_n\}$

$T := \{1, 0, 0, 1, \dots, 0\}$

↳ # der Einser als Teilmenge

x Einser
y Nuller ⟶ $\frac{n!}{x!\,y!}$

Beispiel

Lotto 6 aus 45

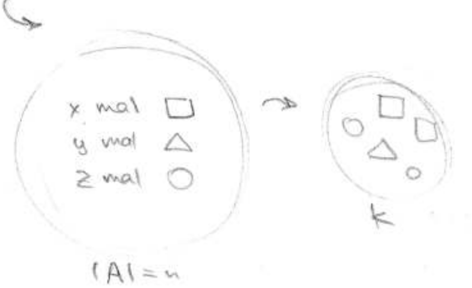
Kugeln auf einmal gezogen & nicht einzeln

$$\frac{45!}{6!\,(45-6)!}$$

Auswahlen einer Teilmultimenge

Kombination mit Wiederholung

Elemente können mehrfach auftreten, wir kennen nur Typen



$A := \{a_1, a_2, a_3, \dots, a_n\}$

$T := \{1, 0, 0, 2, 3, 0, 6\}$

↳ k ist Σ alle dieser Zahlen

Vorsicht: ~~|T|~~
|T| ist die Anzahl der unterschiedl. Elementarten!

Angenommen
k = 7 ⟶ mögliche „Kompositionen" (Zahlentheorie)

3 + 3 + 1 oder 1 + 1 + 1 + 3 + 1

Summe bleibt gleich!

Beispiel: Urne

$A := \{a_1, a_2, a_3, a_4\}$

$|A| = n = 4$

$k = 7$

⟶ beliebige Teilmenge

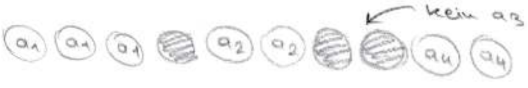
$a_1\ a_1\ a_1\ a_2\ a_2\ a_4\ a_4 \quad k = 7$

$n-1 = 3$ Teiler

$k = 7$ Kugeln

$n = 4$ Typen

$n-1 = 3$ nicht unterscheidbare Kugeln als Teiler



Wenn wir die weißen nicht sehen würden;

$\Sigma = k + n - 1$

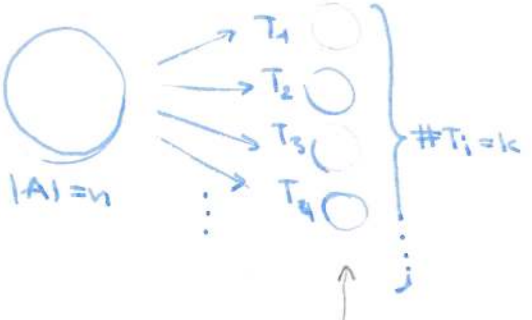
↳ Permutationen einer Multimenge

$n = k + (n-1)$

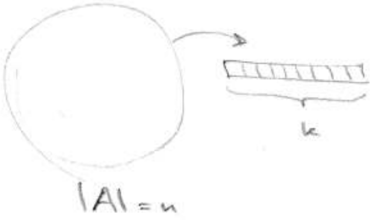
$k = (n-1)$

$$\frac{n+k-1}{[(n+k-1)-(k-1)]!\,(n-1)!} = \binom{n+k-1}{k}$$

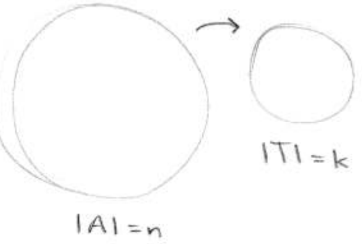
Aufteilungsprobleme



Anordnungsprobleme



Auswahlprobleme



Definition:

Partition: Darf ~~leer sein nicht~~ nicht leer sein

Teilmenge: Darf ~~nicht~~ leer sein

Stirlingzahlen 2. Art

Anzahl der möglichen Partitionen wenn 

$$S_{n,k} = \frac{1}{k!} \sum_{j=0}^{k} (-1)^{k-j} \binom{k}{j} j^n \quad (0 \leq k \leq n)$$ → Es können nicht mehr Partitionen sein als es Elemente in A gibt!

Bellzahlen

Anzahl der möglichen Partitionen bei allen k $[0;n]$

$$B_n = \sum_{k=0}^{n} S_{n,k} \iff |P(A)| = B_{|A|}$$

(BONUS: Auch # von allen möglichen Äquivalenzrelationen bei $|A|=n$)

Potenzmenge

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

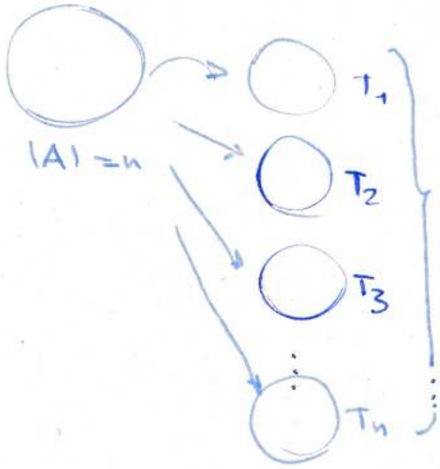
$P(A) = \{\emptyset, \{1\}, \{2\}, \underbrace{\{1,2\}}\}$ → $\{1,2\}$ und $\{2,1\}$ sind gleich

Zahlpartitionen

$\underset{n=4}{P(4)} = 5$ „Partitionsfunktion“ = Quasi Bellzahlen für Zahlen

$$\left.\begin{array}{l} 1+1+1+1 \\ 2+1+1 \\ 2+2 \\ 3+1 \\ 4 \end{array}\right\}$$ 5 mögliche $\boxed{\text{Kompositionen}}$ = Zahlenpartitionen

Schubfachprinzip



$\#T = k$

Wenn $n > k$

dann gibt es min. 1 T wo mehr als 1 Element enthalten ist

Wenn $n < k$

dann gibt es min. 1 T wo kein Element enthalten ist. (Kann keine Partition sein sondern Teilmengen)

$n = 10$

$k < n$, $k = 6$

$\lceil \frac{10}{6} \rceil = 2$

$k > n$, $k = 16$

$\lceil \frac{10}{16} \rceil = 1$

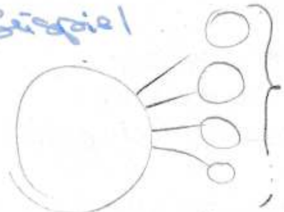
0,625

Es muss min 1 Teilmenge $\lceil n/k \rceil$ Elemente enthalten

→ Es können nicht alle Teilmengen gleich voll sein

→ Es können nicht alle Teilmengen leer sein

Beispiel



|Monate| = 12

|Anzahl von Personen| ≥ 13

$k < n$

$n = 13$

$k = 12$

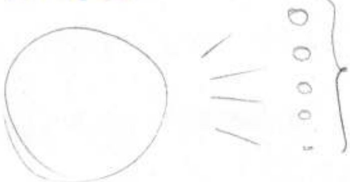
$\frac{n}{k} = 1,083 \ldots$

$\lceil \frac{n}{k} \rceil = 2$

Statistisch gesehen 2 Personen dann im selben Monat Geburtstag

---

Beispiel



Restklassen von 5

|Auswahl an $n \in \mathbb{N}$| = 6

⑥ natürliche Zahlen = n

⑤ Restklassen von 5 = k

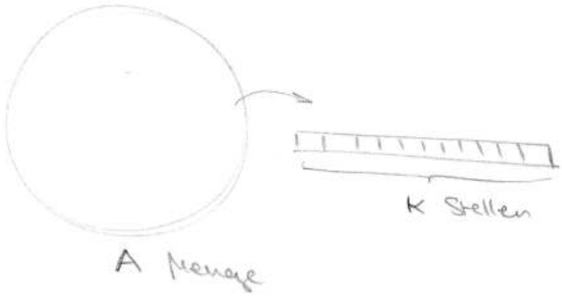
Es muss immer 2 Zahlen geben deren Differenz durch 5 teilbar ist,

$$n \bmod 5 = \left.\begin{matrix} \bar{0} \\ \bar{1} \\ \bar{2} \\ \bar{3} \\ \bar{4} \end{matrix}\right\} k$$

! 2 Zahlen in derselben Restklasse haben die Eigenschaft, dass ihre Differenz durch 5 teilbar ist

Also 2 in $\bar{0}$

Anordnung ohne Einschränkung
geordnete Stichprobe
Auswahl mit Zurücklegen
Variation mit Wiederholung



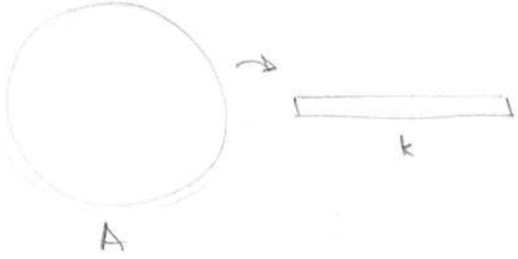
Mögliche Anordnungen von A:
A^k

Beispiel

3^{12} Tototipps

$A = \{1, 2, X\}$ $n = |A| = 3$
$k = 12$

Anordnungen verschiedener Elemente
Variation ohne Wiederholung
geordnete Auswahl ohne Zurücklegen



$k \leq |A|$

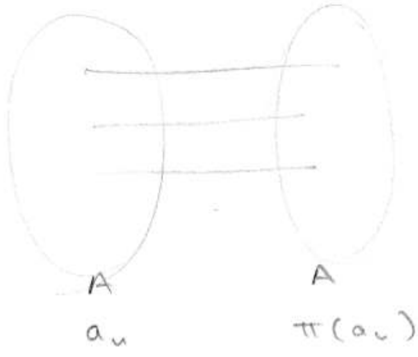
$n \cdot (n-1) \cdot (n-2) \cdot \dots (n-k+1) = \frac{n!}{(n-k)!}$

Beispiel

3 Buchstaben aus 26 Buchstaben (Alphabet)

$26 \cdot (26-1) \cdot \underset{\substack{\uparrow \\ k+1}}{(26-2)}$ $n = 26$, $k = 3$ $\frac{26!}{(26-3)!} = \frac{26!}{23!} = 26 \cdot 25 \cdot 24$

Permutationen einer Menge



Permutation π

$\pi : A \longmapsto A$ (bijektiv)

$n = |A|$

$k = |A|$

$n!$

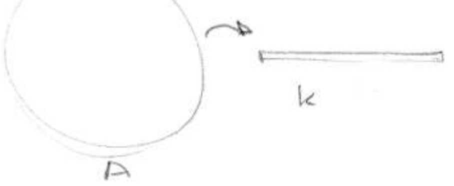
Beispiel:

Menge „Getränke" := { B(ier), S(chnaps), W(ein) }

3 Gläser

$3!$ BSW SBW WSB
BWS SWB WBS

Permutationen einer Multimenge → Elemente dürfen mehrfach vorkommen



Beispiel

Menge „Getränke" := $\{ \underbrace{B, B}, S, W \}$

4 Gläser

nicht unterscheidbar → $B_1 B_2 = B_2 B_1$

\# der nicht unterscheidbaren Anordnungen:

$\frac{4!}{2!}$ ← dividiert! nicht subtrahiert.

Wichtig!

2 Bier werden nicht wie Block behandelt!

$\boxed{BB}\ \boxed{S}\ \boxed{W} \rightarrow 3!$

denn:

BBSW

⋮

Ⓑ S W Ⓑ

S Ⓑ W Ⓑ

Beispiel

Menge := { W, W, S, B, B, B }

6 Gläser

$$\frac{6!}{2!\,1!\,3!}$$

Eigenschaften von Binomialkoeffizienten $\binom{n}{k}$

$$\binom{n}{0} = \binom{n}{n} \rightarrow \text{weil} \quad \frac{n!}{(n-0)!\;0!} = \frac{n!}{n!\;(n-n)!}$$

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

$$\underbrace{\binom{n+1}{k+1}}_{A} = \underbrace{\binom{n}{k} + \binom{n}{k+1}}_{B} \quad \text{wenn } k \neq 0 \qquad A \Rightarrow \frac{(n+1)!}{(k+1)!\;\underbrace{(n+\cancel{1}-k-\cancel{1})!}_{(n-k)!}}$$

Beweis: B → A

$$\binom{n}{k} + \binom{n}{k+1} = \frac{n!}{(n-k)!\;k!} + \frac{n!}{(k+1)!\;(n-k-1)!} =$$

$$\frac{n!}{(n-k)\;(n-k-1)!\;k!} + \frac{n!}{(k+1)\;k!\;(n-k-1)!} =$$

$$\frac{n!}{(n-k-1)!\;k!}\left(\frac{1}{n-k} + \frac{1}{k+1}\right) =$$

herausheben

$$\frac{n!}{(n-k-1)!\;k!}\left(\frac{(k+1)+(n-k)}{(n-k)\,(k+1)}\right) =$$

$$\frac{n!}{(n-k-1)!\;k!}\left(\frac{(n+1)}{(n-k)\,(k+1)}\right) =$$

$$\frac{(n+1)\;n!}{(n-k)\;(n-k-1)!\;\;(k+1)\;k!} = \frac{(n+1)!}{(n-k)!\;(k+1)!} \;\checkmark$$

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n$$

Indexverschiebung / Indexshifting

Um eine Summe / eine Reihe mit unterschiedlichen Werten zu starten als vorgegeben

Erklärung:

$$\sum_{k=1}^{n} a_k = \sum_{k=1+2}^{n+2} a_{k-2}$$

$$\sum_{k=1}^{3} k = \underline{1 + 2 + 3}$$

$$\sum_{k=1+1}^{3+1} k-1 = \sum_{k=2}^{4} k-1 = \underline{1 + 2 + 3}$$

Beispiel:

$$\sum_{\underset{\sim}{k=3}}^{5} \frac{4k+2}{2} \qquad \sum_{k=3-2 \;\rightarrow\; (k+2)=3}^{k=5-2 \;\rightarrow\; (k+2)=5}$$

wir wollen bei 1 anfangen

$$\sum_{(k+2)=3}^{(k+2)=5} \frac{4(k+2)+2}{2} \Rightarrow \sum_{k=1}^{k=3} \frac{4k+8+2}{2} = \sum_{k=1}^{k=3} \frac{4k+10}{2}$$

$$\sum_{k=1}^{k=3} \underbrace{2k+5}_{\text{kürzer als zuvor!}}$$

Beweis:

$$\sum_{k=3}^{5} \frac{4k+2}{2} = \frac{14}{2} + \frac{18}{2} + \frac{22}{2} = 27$$

$$\sum_{k=1}^{3} \frac{4k+10}{2} = \frac{14}{2} + \frac{18}{2} + \frac{22}{2} = 27$$

Allgemein gilt:

$$\sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^{k} = (x+y)^{n}$$

$$\binom{n}{-1} = \binom{n}{n+1} = 0$$

Beweis durch vollständige Induktion

$n \to n+1$

$$(x+y)^{n+1} = (x+y)^{n} (x+y) =$$

$$\sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^{k} (x+y) =$$

$$\sum_{k=0}^{n} \binom{n}{k} x^{n-k+1} y^{k} + \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^{k+1} =$$

---

was wäre wenn $\sum_{k=0}^{n+1}$? keine Auswirkung.

$$k=n+1: \binom{n}{n+1} x^{\cancel{n}-\cancel{n}-\cancel{1}+\cancel{1}} y^{n+1} = 0$$

siehe „Indexshifting"

$n \to n+1$

$k \to k-1$

$$\sum_{k=0}^{n+1} \binom{n}{k} x^{n-k+1} y^{k} + \sum_{k=0}^{n+1} \binom{n}{k-1} x^{n-(k-1)} y^{(k-1)+1} =$$

$$\sum_{k=0}^{n+1} \binom{n}{k} x^{n-k+1} y^{k} + \sum_{k=0}^{n+1} \binom{n}{k-1} x^{n-k+1} y^{k} =$$

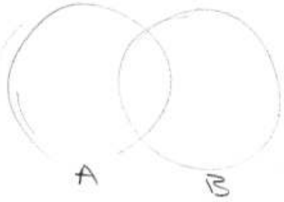
$$\sum_{k=0}^{n+1} \left[\binom{n}{k} + \binom{n}{k-1} \right] x^{n-k+1} y^{k} =$$

$$\sum_{k=0}^{n+1} \binom{n+1}{k} x^{n+1-k} y^{k}$$

□

Inklusions - Exklusions - Prinzip

Siebformel: $n = 2$

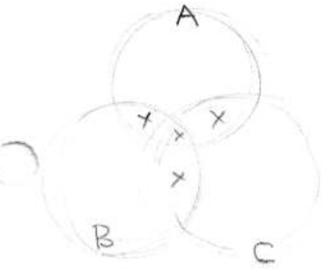


$$|A \cup B| = \underbrace{|A| + |B|}_{\text{Inklusion}} - \underbrace{|A \cap B|}_{\text{Exklusion}}$$

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

$$= \underbrace{|A \setminus B| + |A \cap B|}_{|A|} + \underbrace{|B \setminus A| + \underbrace{|A \cap B| - |A \cap B|}_{0}}_{|B|}$$

$$= |A| + |B| - |A \cap B|$$



$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap C|$$
$$- |A \cap B|$$
$$- |B \cap C|$$
$$+ |A \cap B \cap C|$$

Siebformel: $n = 3$

Prinzip → „Siebformel"

$$\left| \bigcup_{i=1}^{n} A_i \right| = |A_1 \cup A_2 \cup A_3 \dots \cup A_n| =$$

$$= \sum_{i=1}^{n} |A_i| - \sum_{\underbrace{1 \le i < j}_{\substack{\text{alle i und j} \\ \text{zwischen 1 und n}}} \le n} |A_i \cap A_j| + \sum_{1 \le i < j < k \le n} |A_i \cap A_j \cap A_k|$$

$$+ \underbrace{(-1)^{n-1}} |A_1 \cap A_2 \cap A_3 \cap \dots \cap A_n|$$

$(-1)^{2-1} = -1$ bei geraden Mengenanzahl = negativ

$(-1)^{3-1} = 1$ bei ungerader Mengenanzahl = positiv

$n = 4$

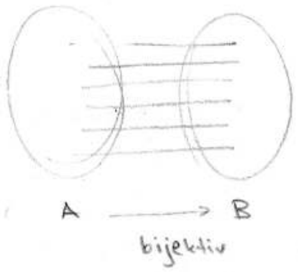
$$- |A_1 \cap A_2| \quad - |A_2 \cap A_3| \quad - |A_3 \cap A_4|$$
$$- |A_1 \cap A_3| \quad - |A_2 \cap A_4|$$
$$\left| \bigcup_{i=1}^{4} A_i \right| = |A_1| + |A_2| + |A_3| + |A_4| - |A_1 \cap A_4|$$
$$|A_1 \cap A_2 \cap A_3| + |A_2 \cap A_3 \cap A_4| +$$
$$\underbrace{(-1)^{4-1}}_{(-1)} \cdot |A_1 \cap A_2 \cap A_3 \cap A_4|$$

Beispiel 2.8), Seite 66

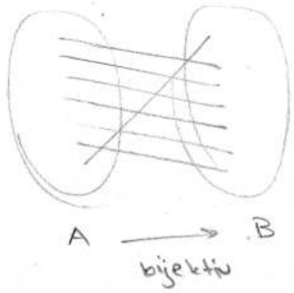
Fixpunktfreie Permutationen

Gruppe an n Personen besitzt k Schirme und besucht Konzert.
Nachdem sie von Konzert zurückkommen bekommen sie alle den falschen Schirm.

Wie hoch ist die Wahrscheinlichkeit, dass alle Personen einen Schirm bekommen den sie vorher nicht hatten



nach Konzert



alle andere Schirme

Wie viele Permutationen von n Elementen gibt es, so dass kein Element an seiner ursprünglichen Stelle steht?

Das Gegenteil von dem was wir suchen

P, Menge aller Permutationen von n Elementen

P_j , $1 \leq j \leq n$
Teilmenge in der ein beliebiges Element
(wenn wir a,b,c haben dann ist zB a=1, b=2, ...)
die Stelle nicht ändert

$|P| = n!$

$|P_j| = (n-1)!$

Beispiel: $n=3$

$|P| = 3! = 6$

$|P_j| = (3-1)! = 2$

$|P_1| = 2$ $\boxed{a=1}$ → a ändert Stelle nicht

a b c
a c b

b c a
b a c

c a b
c b a

a b c
a c b

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

$2! = 1 \cdot 2 \cdot 1$
↑
weil a bleibt

Graphentheorie

$G = (V, E)$

Kanten Edges $E(G)$ $|E(G)| = E$

Knoten Vertices $V(G)$ $|V(G)| = V$

(Graphen sind binäre Relationen auf Menge V.)

„Schlichter und einfacher Graph"

keine Mehrfachkanten und Schlingen

$v_1, v_2 \in V(G)$

gerichtet $\longrightarrow$ $e = (v_1, v_2)$

ungerichtet $e = \{v_1, v_2\} = v_1 v_2$

Schlinge

$(v_1, v_1) = e$

„adjazent"

Knoten durch Kante verbunden, Knoten „indizieren" mit der Kante die sie verbindet.

„Nachbarn"

$\Gamma(v) = \{w \in V(G) \mid vw \in E(G)\}$

$|\Gamma(v)| = d(v)$ Knotengrad → Schlingen wenn da doppelt zählen

„Nachfolger und Vorgänger" - gerichtet, nicht schlicht

$\Gamma^+(v) = \{w \in V(G) \mid (v, w) \in E(G)\}$ Nachfolger

$\Gamma^-(v) = \{w \in V(G) \mid (w, v) \in E(G)\}$ Vorgänger

$\Gamma(v) = \Gamma^+(v) \cup \Gamma^-(v)$ Nachbarn

$|\Gamma^+(v)| = d^+(v)$ Weggrad

$|\Gamma^-(v)| = d^-(v)$ Hingrad

$$\sum_{v \in V} d(v) = 2|E(G)|$$

Handschlaglemma

wenn gerichtet:

$$\sum_{v \in V} d^+(v) = \sum_{v \in V} d^-(v) = |E(G)|$$

Adjazenzmatrix

(sinnvoll für Mehrfachkanten)

$V(G) = \{v_1, v_2, \ldots, v_n\}$

$A(G) = (a_{ij})$

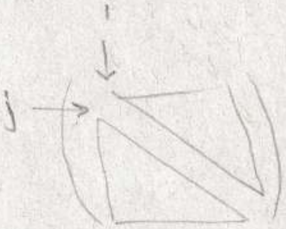
$A^{n \times n}$ Matrix mit $a_{ij} = \begin{cases} 1 & \text{für } (v_i, v_j) \in E(G) \\ 0 & \text{sonst} \end{cases}$

ungerichtet : symmetrische Matrix

Schlingen : Diagonale = 1

Knotengrad, schlicht, ungerichtet

$$d(v_i) = \sum_{j=1}^{n} a_{ij} = \sum_{j=1}^{n} a_{ji}$$



Knotengrad, gerichtet

$$d^+(v_i) = \sum_{j=1}^{n} a_{ij}$$

$$d^-(v_i) = \sum_{j=1}^{n} a_{ji}$$

Erreichbarkeit

$$A(G)^k = \left(a_{ij}^{[k]}\right)_{1 \leq i, j \leq n}$$

der Kantenfolgen der Länge k von v_i nach v_j

wenn $a_{ij} > 0$ dann $\exists$ Kantenfolge von v_i nach v_j mit max Länge $k \leq |E(G)|$ oder $k \leq |V(G)| - 1$

↳ es kann nicht mehr Kanten geben

Die Potenzen bis Maximallänge zu summieren um zu berechnen welche c_{ij} positiv sind

$$C = c_{ij} = \sum_{k=0}^{max} A(G)^k$$

$$max := \min\{|E(G)|, |V(G)| - 1\}$$

Graphen als binäre Relation $V(G) \times V(G)$

$R := \{(v_1, v_2) \mid v_1 \in V(G), v_2 \in V(G)\}$

$v_1 R v_2$ bedeutet sie sind adjazent

Erreichbarkeit berechnen mit Adjazenzmatrix-Potenzen

$a_{ij}^{[k]} = A(G)^k$ Anzahl der Kantenfolgen der Länge k von v_j nach v_j

Wenn das $a_{ij}^{[k]}$-te Element der k-ten Potenz von A(G) positiv ist gibt es eine Kantenfolge.

Die Länge kann nicht länger als |E| bzw |V|-1 sein

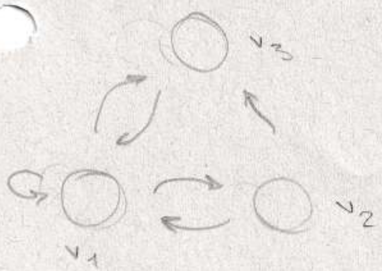
Man berechnet also:

$$\mathbb{C} = (c_{ij}) = \sum_{k=0}^{m} A(G)^k \rightarrow m = \min\{|E|, |V|-1\}$$

$\downarrow$

wenn $c_{ij} > 0$ dann erreichbar!

Beispiel



$$m = \min\{\underbrace{|E(G)|}_{3}, \underbrace{|V(G)|-1}_{6-1}\} = 3$$

$$C = \sum_{k=0}^{3} A(G)^k =$$

$$A(G) = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}^0 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}^1 = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}^2 = \begin{pmatrix} 3 & 1 & 2 \\ 2 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}^3 = \begin{pmatrix} 6 & 3 & 4 \\ 4 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

Summe: Wenn positiv dann ∃ Kantenfolgen der Länge k

← [Wert = Anzahl der möglichen Wege]

(Kanten dürfen mehrfach verwendet werden!)

$$\text{Summe} = \begin{pmatrix} 11 & 5 & 7 \\ 7 & 4 & 5 \\ 5 & 2 & 4 \end{pmatrix}$$

Teilgraphen

$G = (V, E)$

$G' = (V', E')$

$V' \subseteq V$

$E' \subseteq E$

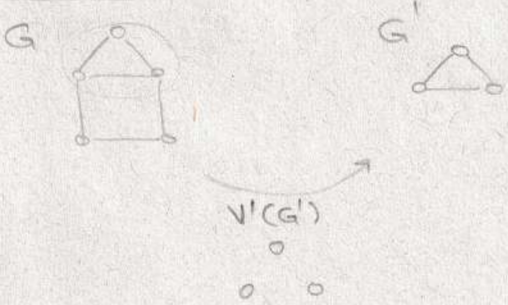
„induzierter Teilgraph"

Angabe nicht vollständig: Man induziert die Kanten durch Knoten

Beinhaltet alle verbindenden Kanten von vorgegebenen Knoten.

$V'(G') \longmapsto E'(G)$

Beispiel



Kantenfolgen

Folge von Kanten die durch Knoten verbunden sind.

Länge Anzahl der Kanten in Kantenfolge um Knoten zu verbinden

Kantenzug alle Kanten in Folge voneinander verschieden

gerichtet: Bahn
ungerichtet: Weg

Geschlossener Kantenzug

gerichtet: Zyklus
ungerichtet: Kreis

Leere Kantenfolge (Länge = 0)

· verbindet Knoten mit sich selbst.

Zusammenhangskomponente

Satz
Bei Zusammenhangskompon.:
n Knoten ⟺ n-1 Kanten

ungerichtet

∃ Kantenfolge für alle Knotenpaare die sie verbindet

gerichtet

Stark zusammenhängend
—— " —— wenn man Kantenrichtung berücksichtigt

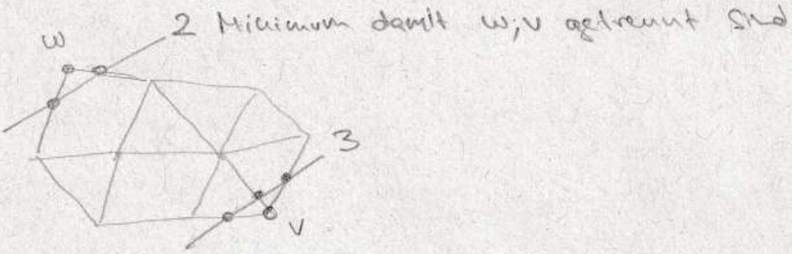
Schwach zusammenhängend
—— " —— wenn man Kantenrichtung nicht berücksichtigt

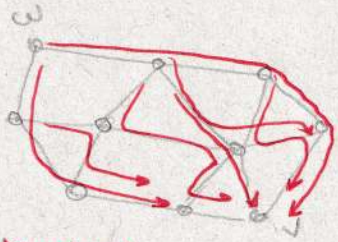
Satz von Menger

zur Bestimmung von der Anzahl der Knotendisjunkten $\underbrace{\text{Wege}}_{\text{ungerichtet}}$

Sei G ein Graph mit $v, w \in V(G)$
Dann ist die Mindestanzahl an Kanten die man entfernen muss damit kein Weg mehr von v nach w führt die Höchstanzahl an kantendisjunkten Wegen zwischen diesen Knoten

Beispiel 1





**Maximal
2 Knotendisjunkte Wege
zugleich.**

2 Wege sind Knotendisjunkt, wenn sie außer Anfangs und Endknoten keine Gemeinsamkeiten haben.

Bsp.: $v_1 \rightarrow v_6$

$P_1 = v_1]\ v_3\ v_5\ \enclose{circle}{v_7}\ \boxed{v_6}$

$P_2 = v_1]\ v_2\ v_8\ \boxed{v_6}$

$P_3 = v_1]\ v_4\ \enclose{circle}{v_7}\ \boxed{v_6}$

Gemeinsam!
Nicht erlaubt.

Bsp.: $v_1 \rightarrow v_2$

$P_1 = v_1]\ v_4\ v_{10}\ \boxed{v_2}$

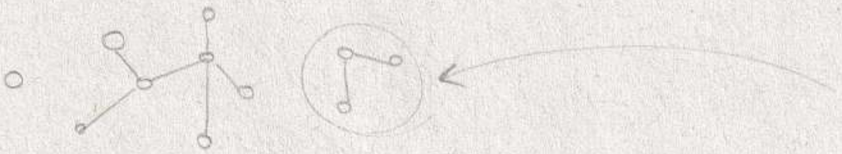
$P_2 = v_1]\ v_6\ v_8\ v_9\ v_5\ \boxed{v_2}$

$P_3 = v_1]\ v_3\ v_7\ \boxed{v_2}$

✓ Kantendisjunkt

Wald W

Schlicht, ungerichtet, keine Kreise



Baum T

Komponent von
Wald, zusammen-
hängend

Nur 1 Weg
zwischen 2 Knoten:
Abstand = $d_T(v,w)$

Es gilt:

$\underbrace{a_0(T)}_{|V(T)|} = \underbrace{a_1(T)}_{|E(T)|} + 1$ für Bäume

$a_0(W) = a_1(T) + k$ für Wald mit k Bäumen

Wurzel

Beliebiger Knoten als tiefster Punkt $d(v) = 1 \quad v \in T$

(● nur Wurzel: $d(v) = 0$)

Blätter, Endknoten, Externe Knoten

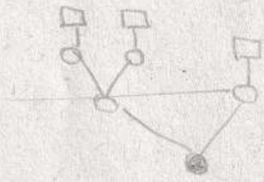
Wie Wurzel, Oben $d(v) = 1 \quad v \in T$

Interne Knoten

Zwischen Wurzel und Blatt $d(v) = 2+ \quad v \in T$

Beispiel

Binärbäume



Blatt
Interner Knoten
Wurzel

↑ Nachfolger
↓ Vorgänger

(d(v) bei internen Knoten ist entweder 2 oder 3.)

Azyklischer Graph

Im Gegensatz zu Baum, Wald sind sie gerichtet

Keine Zyklen = Kantenfolgenlänge beschränkt

Hingrad
$d^-(v) = 0$

Weggrad
$d^+(v) = 0$

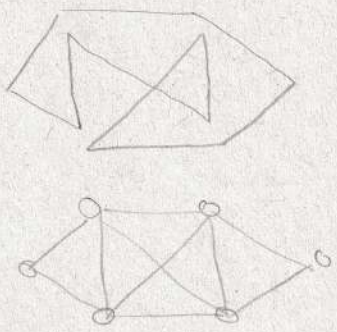
Markierungsalgorithmus

Graph muss zyklisch bleiben wenn man der vordersten Knoten mit $d^+(v)=0$ entfernt

(und diesen Schritt wiederholt)

Eulersche Linie

(im eulerschen Graph)



Kantenzug wobei:

- geschlossen   Anfangsknoten = Endknoten
- offen   Anfangsknoten ≠ Endknoten

Bedingungen

- zusammenhängend
- bei ungerichtetten Graphen

  geschlossene eulersche Linie : $\forall\, d(v)$ gerade

  offene eulersche Linie : $\forall\, d(v)$ ausgenommen von 2 Knoten gerade

- bei gerichteten Graphen

  geschlossene eulersche Linie : $\forall\, d^+(v) = d^-(v)$

  offenere eulersche Linie : $\forall\, d^+(v) = d^-(v)$ ausgenommen von 2 Knoten (w_1 und w_2) für die gilt:

  $d^+(w_1) = d^-(w_1) + 1$

  $d^+(w_2) = d^-(w_2) - 1$

Hamiltonsche Linie

(im hamilton'schen Graph)

Beinhaltet jeden Knoten genau 1x

Kann offen oder geschlossen sein

Bedingung

- wenn schlicht und ungerichtet gilt für alle nicht mit einer einzigen Kante verbundenen Paare

  $d(x) + d(y) \geq |V(G)| \quad x,y \notin E(G)$

Planare Graphen

planar, eben

Kreuzungsfrei in $\mathbb{R}^2$ Ebene darstellbar

Euler'sche Polyederformel

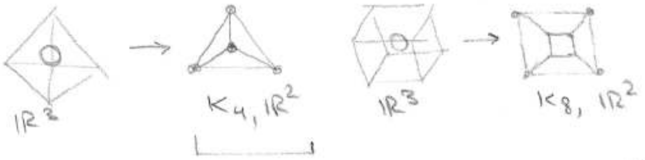
$\alpha_0(G)$ = Knoten $|V(G)|$

$\alpha_1(G)$ = Kanten $|E(G)|$

$\alpha_2(G)$ = Gebiete

$$\alpha_0(G) - \alpha_1(G) + \alpha_2(G) = 2$$

Projektion von Polyeder auf Kugeloberflächen im inneren dieser!



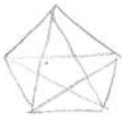
Vollständiger Graph : direkte Verbindung zw. allen Knoten

K_n $n = |V(G)|$

Satz von Kuratowski

Graph nicht planar wenn es K_5 oder $K_{3,3}$ als Teilgraph hat

K_5



$K_{3,3}$

Graphentheorie: Färbungseigenschaften

Farbe eines Knotens / einer Kante = Eigenschaft

Bsp.: Alle Knoten je untersch. Farbe

chromatische Zahl $\chi^{(G)}$ = min. # von Farben die benötigt werden um ∀ Knoten zu markieren

$$\chi^{(K_n)} = n$$

„Vierfarbensatz"

Für planare Graphen gilt:

$\chi(G) \leq 4$ wenn G planar ist

Netzwerke & Algorithmen → als Teil der Graphentheorie

können gerichtet / ungerichtet sein $G=(V,E)$

Netzwerke

1. jede Kante $e \in$ ~~E(G)~~ E hat einen Wert $w(e) \in \mathbb{R}$

   ↳ Funktion: $w: E \to \mathbb{R}$

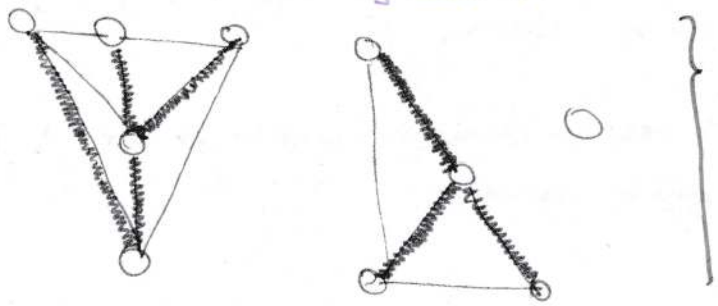
2. Neben Adjazenzmatrix $A(G)$ gibt es auch bewertete Adjazenzmatr.

$$A_w(G) = (\underbrace{w(v_i,v_j)}_{\text{Wert der Kanten}}) \quad 1 \le i,j \le n$$

3. Es muss $w(v_i, v_j) = 0$ definiert werden

Algorithmus: Kruskal-Algorithmus

zur Bestimmung eines minimalen Gerüsts



Gerüst eines Graphen mit 3 Zusammenhangskomponenten

Spannender Baum T ∈

- Teil eines schlichten, unger. Graphen
- beinhaltet alle Knoten aber nicht alle Kanten
- Ist ein Baum

$$V(T) = V(G)$$
$$E(T) \subseteq E(G)$$

Gerüst / spannender Wald W

- Ist ein Wald

$$V(W) = V(G)$$
$$E(W) \subseteq E(G)$$

- Dieselben Komponenten wie G

Ist G ein bewerteter Graph:

Minimales Gerüst wenn Summe aller Kantengewichte des Gerüstes kleinstmöglich ist.

$$w(W) = \sum_{e \in E(W)} w(e)$$

Mit anderen Worten:

minimales Gerüst = Teilgraph als Baum der alle Knoten~~t~~ beinhaltet und den geringsten Wert von den Kanten hat.

Der vollständ. Graph K_n aus n Knoten und $\frac{n(n-1)}{2}$ Kanten hat n^{n-2} mögliche spannende Bäume.

~~Deshalb~~ Das minimale Gerüst des vollständigen Graphen ist nur 1 ~~Ba~~ Gerüst aus den n^{n-2} möglichen Varianten.

~~Algorithmus um das minimale Gerüst zu finden: Kruskal Algorithmus~~

~~1. Sortiere alle $e \in E$ nach steigendem Gewicht und nehme e_1 mit dem kleinstmöglichen Gewicht~~

~~2. Vermeide Kreise und~~

Algorithmus um minimale Spannbäume zu finden:

Kruskal - Algorithmus

Ein greedy-Algorithmus aus der Graphentheorie (in jedem Schritt versucht man hungriger Weise jene Kante mit dem geringsten Gewicht einzusetzen) - so, dass kein Kreis entsteht.

Es ist auch möglich damit maximale Spannbäume zu finden

Der Graph muss zusammenhängend & kantengewichtet sein.

INPUT:

$G = (V, E, w)$

V ... vertices, Ecken/Knoten
E .... edges, Kanten
w ... Gewichtsfunktion $w: E \to \mathbb{R}$

ALGORITHMUS:

1. Man nummeriert die Kanten $E = \{e_1, e_2, \dots, e_m\}$ basierend auf ihrem Gewicht

$$w(e_1) \leq w(e_2) \leq \dots \leq w(e_m)$$

2. Setze

[illegible] $E' \leftarrow \emptyset$
[illegible] $L \leftarrow E$

3. <u>Solange</u> $L \neq \emptyset$

- wähle eine Kante $e \in L$ mit kleinstem Kantengewicht
- entferne e aus L

  <u>wenn</u> der Graph $(V, E' \cup \{e\})$ keinen Kreis enthält
  <u>dann</u> $E' \leftarrow E' \cup \{e\}$

4. $M = (V, E')$ ist minimaler Spannbaum von G

Nach Buch:

1. Man nummeriert die Kanten $E = \{e_1, e_2, e_3, \dots, e_m\}$ nach ihrem steigenden Gewicht:

$$\omega(e_1) \leq \omega(e_2) \leq \dots \leq \omega(e_m)$$

2. $E' := \emptyset$

   $j := 1$

3. Wenn $(V, E' \cup \{e_j\}) = G'$ kreisfrei ist dann setze $E' := E' \cup \{e_j\}$

4. Ist $|E'| = |V| - 1$ oder $j = m$ dann beende Algorithmus $W = (V, E')$ ist das output.

   Andernfalls setze $j := j+1$ und wiederhole Schritt 3

Jedes Gerüst von G hat genau $|V| - k$ Kanten wobei k # der Komponenten ist!

Nach Joseph Kruskal selbst:

Führe den folgenden Schritt so oft wie möglich aus:

~~[illegible]~~

Wähle unter den noch nicht ausgewählten Kanten von G die kürzeste Kante die mit den bereits gewählten keinen Kreis bildet.

Algorithmus um kürzeste Wege und Bahnen zwischen 2 Knoten zu bestimmen: (Teil der Greedy-Algorithmen)

Dijkstra-Algorithmus

Definition:

$G=(V,E)$ Gewichtung: $w: E \to \mathbb{R}_0^+$ = Distanz [illegible]

Länge einer Kantenfolge:

$$w(\{e_1, e_2, e_3, \ldots, e_k\}) = \sum_{j=1}^{k} w(e_j)$$

Distanz:

$d(v,w)$ zwischen 2 Knoten v und $w \in V$ ist ~~die shortest ph~~ der kürzeste Weg.

Wenn es keinen Weg gibt:
dann $d(v,w) = \infty$

Anfangsknoten

$v_0 \in V$
Berechnung von kürzester Distanz $d(v_0, v)$

Algorithmus: (nach Buch)

1. $l(v_0) = 0$
   $l(v) := \infty$ für alle $v \in V \setminus \{v_0\}$
   $U = \{v_0\}$
   $u = v_0$

2. Für alle $v \in V \setminus U$ mit $(u,v) \in E$ die $l(v) > l(u) + w(u,v)$ erfüllen:
   $p(v) := u$
   $l(v) :=$ [illegible] $l(u) + w(u,v)$

3. Man bestimme
   $m = \min_{v \in V \setminus U} l(v)$ → Falls $m = \infty$ terminiere
   → Sonst wähle anderen Knoten $z \in V \setminus U$ mit $l(z) = m$ und setze $U := U \cup \{z\}$ und $u := z$

4. Wenn $U = V$ terminiere
   Sonst

Input:

$G = (\underset{\text{Knoten}}{\underset{\uparrow}{V}}, \underset{\text{Kanten}}{\underset{\nwarrow}{E}})$

Algorithmus:

1. $d(v_0, v_0) = 0$

   $d(v_0, v) = \infty$ für alle anderen Knoten außer v_0 $(v \in V \setminus \{v_0\})$

   $U \subseteq V = \{v_0\}$ Menge an Knoten für die der kürzeste Weg schon bekannt ist.

   $\underset{\sim\sim}{x} = v_0$ Beobachteter Punkt / ausgewählter Punkt → immer das letzte Element aus U

2. Für alle $v \in V \setminus U$ mit $(x, v) \in E$

   mit $\underbrace{d(v_0, v)}_{\text{andere Wege}} > \underbrace{d(v_0, x) + d(x, v)}_{\text{Weg von } v_0 \text{ nach } v \text{ über } x}$ gilt:

   $d(v_0, v) := d(v_0, x) + d(x, v)$

   $P(v) := x$ (Vorgänger von v muss x sein)

3. Berechne

   $$m = \min_{v \in V \setminus U} d(v_0, v)$$

   Falls $m = \infty$ terminiere

   Sonst wähle $z \in V \setminus U$ mit $d(v_0, z) = m$

   und setze

   $U := U \cup \{z\}$

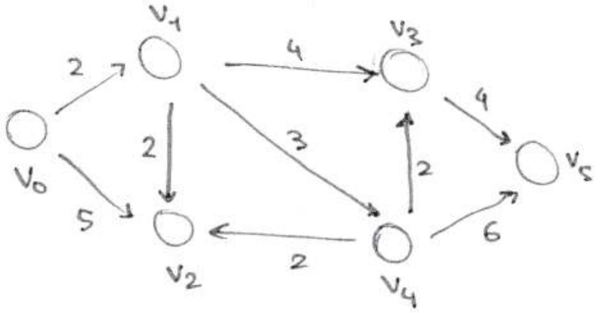
   und setze

   $x := z$

---

4. Wenn $U = V$ terminiere,
   sonst gehe zu Schritt 2

Seite 77
Beispiel 2.39



1. $d(v_0,v_0)=0$

   $d(v_0,v)=\infty$ (also $d(v_0,v_n)=\infty$ für alle $n=[1;5]$)

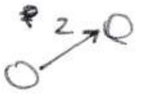
   $x = v_0$

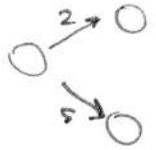
2. $d(v_0,v_1)=\min\{\infty, \cancel{0}\ 0+2\} = \boxed{2}$

   $P(v_1) = v_0$

   $d(v_0,v_2) = \min\{\infty, 0+5\} = 5$

   $P(v_2) = v_0$





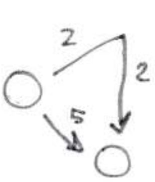
3. $m = 2$ → der kürzeste bisherige Weg

   $z = v_1$

   $U = \{v_0, v_1\}$ aber nicht $\boxed{v_2}$!

   $x = v_1$

4. Beginnt wieder bei Schritt 2



2. $d(v_0,\boxed{v_2}) = \min\{5, 2+2\} = \boxed{4}$

   $P(v_2) = v_1$

   $d(v_0,v_3) = \min\{\infty, 2+4\} = \boxed{6}$

   $P(v_3) = v_1$

   $d(v_0,v_4) = \min\{\infty, 2+3\} = \boxed{5}$

   $P(v_4) = v_1$

3. $m = 4$

   $z = v_2$

   $U = \{v_0, v_1, v_2\}$

   $x = v_2$ ...

Überblick

Algebraische Strukturen:

(a) (A, ∘) heißt **Gruppoid**, falls ∘ eine binäre Operation auf A ist.

z.B. (ℕ, ∘) mit $a \circ b = a^b$

(b) Ein Gruppoid (A, ∘) mit einer assoziativen Operation ∘ heißt **Halbgruppe**.

z.B. (ℕ\{0}, +)

(c) Eine Halbgruppe (A, ∘) mit neutralem Element heißt **Monoid**.

z.B. (Σ*, ∘)

(d) Eine Halbgruppe (G, ∘) heißt **Gruppe**, falls ein neutrales Element und zu jedem Element ein Inverses existiert. Ist ∘ außerdem kommutativ, spricht man von einer **kommutativen (abelschen) Gruppe**.

z.B. (S_n, ∘)

(e) Eine Algebra (R, +, ·) mit zwei binären Operationen + und · heißt **Ring**, falls (R,+) eine kommutative Gruppe, (R, ·) eine Halbgruppe und · distributiv gegenüber + ist. Ist · auch kommutativ (bzw. existiert ein Einselement), dann heißt R **kommutativer Ring** (bzw. **Ring mit Einselement**).

z.B. ($\mathbb{Z}_n$, +, ·)

(f) Ein Ring (R, +, ·) heißt **Integritätsring** (Integritätsbereich), falls R kommutativer Ring mit Einselement 1 (≠ 0) ist und keine Nullteiler besitzt, d.h., falls keine Elemente a, b existieren mit $a \neq 0$, $b \neq 0$ und $a \cdot b = 0$.

z.B. (ℤ, +, ·)

(g) Ein kommutativer Ring (K, +, ·) heißt **Körper**, falls (K\{0}, ·) Gruppe ist.

z.B. (ℂ, +, ·)

(h) Ein **Verband** ist eine Algebra (V, ∧,∨), sodass (V, ∧) und (V, ∨) kommutative Halbgruppen sind und darüber hinaus die beiden Verschmelzungsgesetze $a \wedge (a \vee b) = a$ und $a \vee (a \wedge b) = a$ für alle a,b ∈ V gelten. Ist ∧ gegenüber ∨ und ∨ gegenüber ∧ distributiv, so spricht man von einem **distributiven Verband**.

z.B. (P(M), ∩,∪)

(i) Eine **Boolesche Algebra** ist eine Algebra (B, ∧,∨,',0,1), sodass (B, ∧,∨) distributiver Verband, 0 neutrales Element bzgl. ∨, 1 neutrales Element bzgl. ∧ und' eine einstellige Operation (Komplementbildung) in B ist mit der Eigenschaft $a \wedge a' = 0$ und $a \vee a' = 1$ für alle a ∈ B.

z.B. (𝔹 = {0,1}, ∧,∨,¬,0,1)

Algebraische Strukturen

0) Abgeschlossenheit

$a \circ b \in G$

Gruppoid

1) Assoziativ

$(a \circ b) \circ c = a \circ (b \circ c)$

Halbgruppe

2) Neutrales Element

$e \circ a = a$

Monoid

3) Inverses Element

$a \circ a^{-1} = e$

Gruppe

4) kommutativ

$a \circ b = b \circ a$

abel'sche Gruppe

Ringe $(R, +, \cdot)$

- $(R, +)$ komm. Gruppe
- $(R, \cdot)$ Halbgruppe
- Distributivgesetze

$a(b+c) = ab + ac$

$(a+b)c = ac + bc$

Zusätzlich wenn...

- $(R, \cdot)$ komm → komm Ring
- ∃ Einselement → Ring mit Einselement

Integritätsring

- komm Ring mit Einselement
- ohne Nullteiler a, b

$a \neq 0 \quad b \neq 0 \quad a \cdot b = 0$

Körper

- komm Ring in der $(K \setminus \{0\}, \cdot)$ Gruppe ist

Algebraische Strukturen

Gruppoid: Binäre algebraische Struktur

„binäre Operation o" auf Menge A

$A \times A \mapsto A$

$a, b \in A \mapsto a \circ b \in A$ ..... (Abgeschlossenheit = Voraussetzung)

Das Paar $(A, \circ)$ heißt Gruppoid

Beispiel: Jede beliebige Zahlenmenge mit Addition oder Multiplikation

Gruppen

0) Abgeschlossenheit (immer vorausgesetzt)

1) Assoziativgesetz $a, b, c \in A$ $\quad (a \circ b) \circ c = a \circ (b \circ c)$

2) neutrales Element $e, a \in A$ $\quad a \circ e = e \circ a = a$ [max. 1]

3) inverses Element $a' \in A$ $\quad a \circ a' = e$ [max. 1]

4) Kommutativgesetz $a, b \in A$ $\quad a \circ b = b \circ a$

Halbgruppe 0, 1
Monoid 0, 1, 2
Gruppe 0, 1, 2, 3
kommutative Gruppe ... 0, 1, 2, 3, 4

Untergruppen

Teilmenge $U \subseteq G$ ist Untergruppe.

$$(U, \circ) \leq (G, \circ)$$

Es gibt 2 triviale Untergruppen: $\{e\} \leq G$ und $G \leq G$

Kriterien:

- Abgeschlossenheit
- Existenz von Inversen (impliziert $\exists$ neutrales Element)

(- Assoziativität muss nicht bewiesen werden da es in ganz G gilt!)

Beispiel:

$m \in \mathbb{N}$ $\quad m\mathbb{Z} = \{0, \pm m, \pm 2m, \pm 3m, \dots\} \rightarrow$ Restklasse $\bar{0}$ modulo m
(kein Rest bei Division durch m)

$\bar{a} = a + m\mathbb{Z} \rightarrow$ „Verschobene Untergruppe"

Verschobene Untergruppen:

Nebenklasse einer Untergruppe

$$\left.\begin{array}{ll}(G, \circ) & \text{Gruppe} \\ (U, \circ) & \text{Unterg.} \\ a \in G & \end{array}\right\} \begin{array}{l}\underline{\text{Linksnebenklasse}} \text{ von } U \text{ in } G: a \circ U = \{a \circ u \mid u \in U\} \\ \underline{\text{Rechtsnebenklasse}} \text{ von } U \text{ in } G: U \circ a = \{u \circ a \mid u \in U\}\end{array}$$

Beispiel:

$$\left.\begin{array}{ll}(\mathbb{Z}_m, +) & \text{Gruppe} \\ (m\mathbb{Z}, +) & \text{Untergruppe}\end{array}\right\} \begin{array}{ll}\text{Links} & a + m\mathbb{Z} = \{a, a \pm m, a \pm 2m, a \pm 3m \ldots\} \\ \text{Rechts} & m\mathbb{Z} + a = \{a, \pm m + a, \pm 2m + a, \pm 3m + a \ldots\}\end{array}$$

↳ Restklasse $\bar{0}$

↳ Verschiebung der Restklasse = „Zerlegung von G"

Da $\mathbb{Z}_m$ eine endliche Gruppe ist, ist die Anzahl der möglichen Verschiebungen beschränkt.

Warum?

weil sie nach einer bestimmten Verschiebungsanzahl äquivalent sind.

Links : $a \sim b \iff a + m\mathbb{Z}$ (bezw. $a \circ U$) $= b + m\mathbb{Z}$

Rechts : $a \sim b \iff m\mathbb{Z} + a$ (bzw $U \circ a$) $= m\mathbb{Z} + b$

zwar sind a und b verschiedene Zahlen, aber Kongruent modulo m

Satz von Lagrange

Beispiel:

endliche Gruppe ——— $(\mathbb{Z}_7, +)$ ← kann nicht $(\mathbb{Z}, +)$ sein weil $|\mathbb{Z}| = \infty$

Untergruppe ——— $(m\mathbb{Z}, +)$ ← $\bar{0}$

1. $|U|$ teilt $|G|$

$|U| = 1$
$|G| = 7 \rightarrow 1 | 7$

2. $\underbrace{|G:U|}_{\text{Alle Nebenklassen}} = |G| / |U| = \frac{7}{1} = 7$

Beweis

$m\mathbb{Z} \longmapsto a + m\mathbb{Z}$ ist bijektiv $\rightarrow |\{a + m\mathbb{Z} \mid m = 7\}| = |m\mathbb{Z}|$
$|a + U| = |U|$

daraus folgt:
Linksnebenklasse zerlegt G in $m \cdot |G:U| = 7$ gleich großen Teilmengen

$|G| = 7 \cdot |U|$
$= 7 \cdot 1$

Satz von Lagrange

$(G,\circ)$ endliche Gruppe

$(U,\circ)$ Untergruppe $U \leq G$

$|G:U|$ Index — Anzahl der Nebenklassen (#Rechts = #Links)

$|G|$ Ordnung — Anzahl der Elemente in G

1. $|U|$ teilt $|G|$
2. $|G:U| = |G|/|U|$

Beweis: (Analog für Rechtsnebenklassen)

Abbildung wegen
Gruppeneigenschaft
bijektiv

$$\left.\begin{array}{l} U \longmapsto a\circ U \\ x \longmapsto a\circ x \end{array}\right\} \text{es gilt immer in endlicher Gruppe } |a\circ U| = |U|$$

Linksnebenklasse zerlegt G in
$m = |G:U|$ gleich große Mengen

Restklassen

Daraus folgt: $|G| = m\cdot|U|$

Kleiner Fermat'scher Satz (der Grupp.theorie)

$|\langle a\rangle| = \text{ord}_G(a)$

$\text{ord}_G(a) \underset{\text{teilt}}{|} |G|$

Daraus folgt:

Für jedes $a \in G$
$G := (G,\circ)$ gilt: $\boxed{a^{|G|} = e}$

Beweis:

$G := (G,\circ) \rightarrow$ endliche Gruppe

$U := \langle a\rangle = \{a^n \mid 0 \leq n < \text{ord}_G(a)\}$

$$\left[\begin{array}{l} \text{zB.: } \langle 3\rangle = \{3^0, 3^1, 3^2, 3^3\} \\ \text{bei } (\mathbb{Z}_4, +) \end{array}\right]$$

$k = |\langle a\rangle| = \text{ord}_G(a)$

$m = |G:U|$

$km = |G|$

Beispiel fortführung

$G := (\mathbb{Z}_4, +) \quad |G| = 4$

$\langle 0 \rangle = \{0\} \qquad |\langle 0 \rangle| = 1$

$\langle 1 \rangle = \{0, 1, 2, 3\} \qquad |\langle 1 \rangle| = 4$

$\langle 2 \rangle = \{0, 2\} \qquad |\langle 2 \rangle| = 2$

$\boxed{\langle 3 \rangle = \{0, 3, 6, 9\} \qquad |\langle 3 \rangle| = 4}$

$U := \langle 3 \rangle \quad |\langle 3 \rangle| = 4$

$1 = 4 / 4$

$|G:U| = |G| / |U|$

$k = |\langle a \rangle| \qquad 4 = |\langle 3 \rangle|$

$m = |G:U| \qquad 1 = |G:U|$

$k \cdot m = |G| \qquad 4 \cdot 1 = 4$

$0 \bmod 4 = 0$
$3 \bmod 4 = 3$
$6 \bmod 4 = 2$
$9 \bmod 4 = 1$

Zyklische Gruppe
Die Untergruppe
bildet wieder die Gruppe persönlich

Beweis

Aus $a^k = e$ erhält man

$a^{|G|} = (a^k)^m = e^m = e \rightarrow a^{|G|} = e$

$\left(a^{|\langle a \rangle|}\right)^{|G:U|} = e$

Angenommen

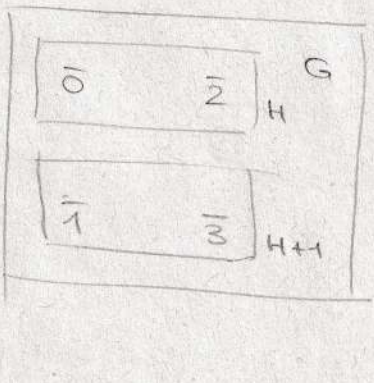
$a = 2$

$k = |\langle 2 \rangle| = 2$

$m = 4 / 2 = 2$

$k\,m = 2 \cdot 2 = 4$

Zyklische Gruppe
weil sich 2 Nebenklassen bilden lassen würden:



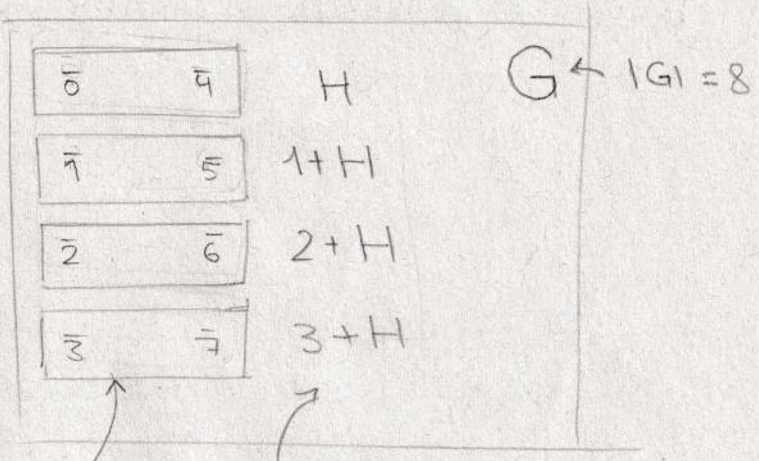
Satz von Lagrange

Beispiel 1:

$G := (\mathbb{Z}/8\mathbb{Z}, +)$

$H := \{\bar{0}, \bar{4}\}$

↑ e muss in H enthalten sein



$|G| = |G:H| \cdot |H|$

$8 = 4 \cdot 2$

$|G:H| = \frac{|G|}{|H}$

$4 = 8/2$

$|G:H| = 4$

Partitionieren G in 4 gleich große Teile

Notation nach Linksnebenklassen, für Rechtsnebenklassen:

$H+1, H+2, \dots$

Beispiel 2:

$G := (\mathbb{Z}_{10}, +) = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \dots, \bar{9}\}$

$|\mathbb{Z}_{10}| = 10$

Wie groß können die Untergruppen sein?

$g \in G$ → Restklassen

g	|g|
0	1
5	2
2, 4, 6, 8	5
1, 3, 7, 9	10

wenn $g \in G$ dann

$|g| \,\big|\, |G|$ also:

→ $H \leq G$ unbekannt aber

$|H| = 1, 2, 5, 10$

Mögliche Kandidaten:

$H = \{\bar{0}, \bar{5}\} \Rightarrow |H| = 2$ ✓

$H = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}\} \Rightarrow |H| = 5$ ✓

Beispiel 3:

$G := (\mathbb{Z}_p, +)$

$|\mathbb{Z}_p| = p$ → Die einzigen möglichen $|H|$ sind p und 1

Beispiel 4:

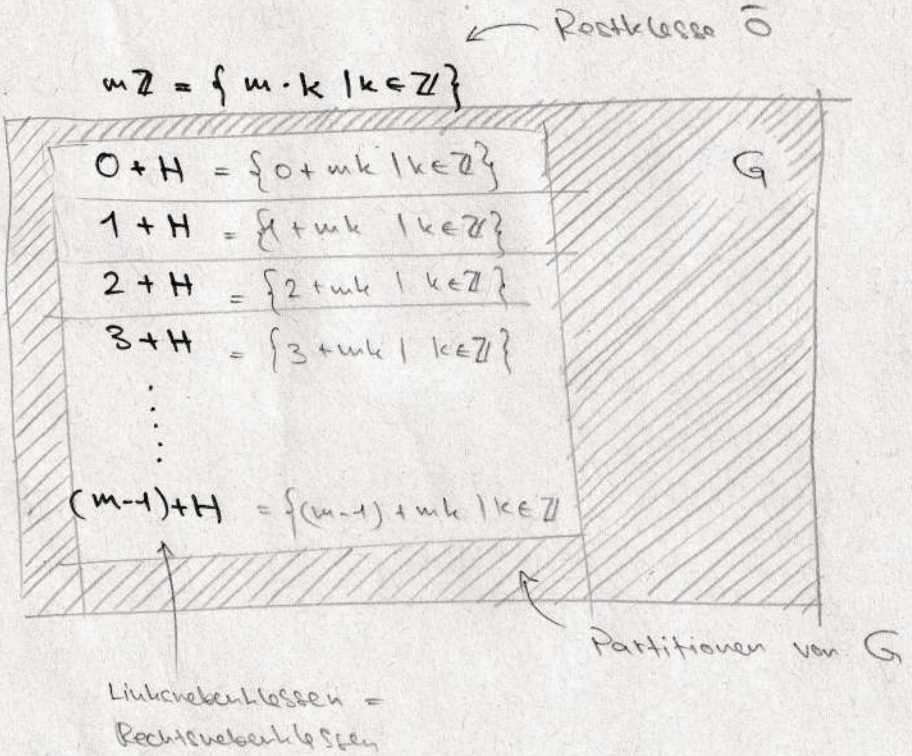
$H \leqslant G$ H partitioniert G in $|G:H|$ gleichgroße Teile

anhand einer Äquivalenzrelation werden alle Zahlen in $|G:H|$ gleiche „Schubladen" gesteckt

-> kongruenz modulo $|G:H|$

$G := (\mathbb{Z},+)$

$H := (m\mathbb{Z},+)$ $m\mathbb{Z} = \{m \cdot k \mid k \in \mathbb{Z}\}$



G sollte eigentlich eine endliche Gruppe sein...

In diesem Fall:

$|\mathbb{Z}_m| = m$

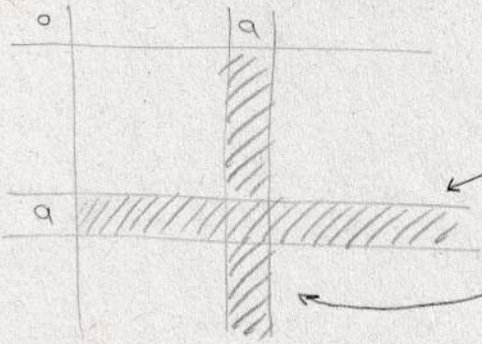
$|m\mathbb{Z}| = 1$

1. $|H|$ teilt $|G|$ -> 1 teilt m ✓
2. Anzahl der Nebenklassen

$$|G:H| = |G| : |H|$$
$$m = m : 1$$ -> wahr ✓

„cosets and Lagranges theorem"

Operationstafel $(G, \circ)$



$a \in G$

$aG = \{a \circ g \mid g \in G\}$ Zeile a ∘ [alle Spalten]

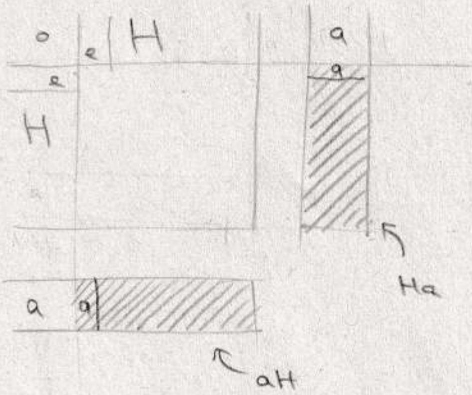
$Ga = \{g \circ a \mid g \in G\}$ [alle Zeilen] ∘ Spalte a

Zeile ∘ Spalte = Eintrag

Wenn man alle a nimmt = G

$\forall a \in G, \ aG = Ga = G$

Untergruppe $(H, \circ)$ $H < G$



$a \in G$

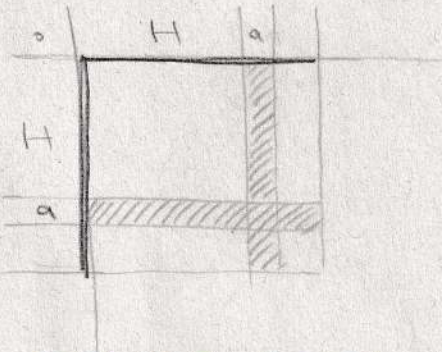
aH = Linksnebenkl. $= \{a \circ h \mid h \in H\}$

Ha = rechtsnebenkl. $= \{h \circ a \mid h \in H\}$

$$\left.\begin{array}{l} a \in aH \\ a \in Ha \end{array}\right] \leftarrow a \circ e = a \quad e \in H$$

Normalteiler: wenn G kommutativ ist

Fall 1: $a \in H \longrightarrow U \trianglelefteq G$



Jede Untergruppe:

$\forall a \in H, \ aH = Ha = H$

wie Beispiel oben

$\forall a \notin H$
aH und Ha haben keine
Elemente von H

$aH = \{a \circ h \mid h \in H\}$
$Ha = \{h \circ a \mid h \in H\}$

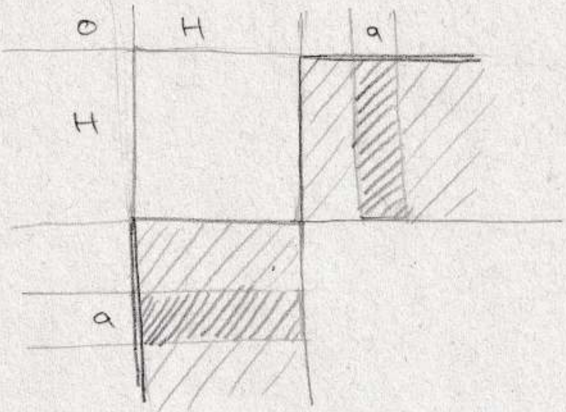
<u>Beweis</u>

Angenommen $a \circ h \in aH$

$a \circ h = h' \quad h' \in H$

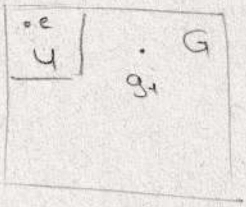
$a = h' \circ h^{-1}$ ↯ $a \notin H$

Fall 2: $a \notin H \qquad U \leq G$



(Soenstea)

Untergruppen und Nebenklassen



$e \in G, U$

$g_1 \in G$

$g_1 \circ U = \{g_1 \circ u \mid u \in U\}$

hat kein Element mit U gemeinsam

bildet eine neue Partition

Normalteiler

$G := (\mathbb{Z}, +)$

$U := (m\mathbb{Z}, +)$ m kann alles mögliche sein

$\overbrace{\mathbb{Z}, 2\mathbb{Z}, 3\mathbb{Z}, 4\mathbb{Z}, \dots}$

Beispiel: $m = 5$

$5\mathbb{Z} = \{\dots, -5, 0, 5, 10, 15 \dots\}$ $5\mathbb{Z} \bmod 5 = \bar{0}$ ← Normalteiler da die Nebenklassen $\mathbb{Z}$ vollständig partitionieren

$1 + 5\mathbb{Z} = \{\dots, -9, -4, 1, 6, 11 \dots\}$

$2 + 5\mathbb{Z} = \{\dots\}$

$3 + 5\mathbb{Z} = \{\dots\}$

$4 + 5\mathbb{Z} = \{\dots\}$

Nebenklassen (Faktorgruppen) $= \mathbb{Z} / 5\mathbb{Z}$

teilt $\mathbb{Z}$ in Partitionen von $5\mathbb{Z}$

$(1 + 5\mathbb{Z}) + (3 + 5\mathbb{Z}) = 4 + 5\mathbb{Z}$

Die Besonderheit von Faktorgruppen ist, dass man mit ihnen (wie Restklassen rechnen kann.

$G := (\mathbb{Z}, +)$

$N := (5\mathbb{Z}, +)$ $N \trianglelefteq G$

Faktorgruppe $\mathbb{Z}_5$ beziehungsweise $G \backslash N$: $\mathbb{Z} \backslash 5\mathbb{Z}$ ← keine Untergruppe von $\mathbb{Z}$ sondern eine völlig neue Gruppe

$\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$

Behauptung

$y^{-1} N y = N$ für $\forall\, y \in G$ $\Rightarrow$ $N \trianglelefteq G$ und Nebenklassen bilden eine Gruppe

(mit Rechengesetzen und neutralem Element)

Beweis

Nebenklassen: xN, yN

$$\underset{\substack{\uparrow \\ n_1 \in xN}}{(x \cdot n_1)}\ \underset{\substack{\uparrow \\ n_2 \in yN}}{(y \cdot n_2)} = x\,(y \cdot y^{-1}) \cdot n_1 \cdot y \cdot n_2 \qquad \boxed{\text{Trick: } y \cdot y^{-1} = e}$$

$= x\,y\,(y^{-1} \cdot n_1 \cdot y) \cdot n_2 =$ ← $\boxed{y^{-1} \cdot n_1 \cdot y \in N}$

$y^{-1} \cdot n_1 \cdot y = n_3$

$= x\,y\,n_3\,n_2 =$ ← $\boxed{n_3 \cdot n_2 \in N}$

$= x\,y\,n_4 \in x\,y\,N$

$n_3 \cdot n_2 = n_4$

$\Downarrow$

$(xN)(yN) = xyN$. ✓

Die Nebenklassen bilden eine Gruppe

↓

Zusammengefasst:

Wenn $N \trianglelefteq G$ und $y^{-1} N y = N$ für alle $y \in G$
dann bilden die Nebenklassen von N alle Gruppen

Diese Gruppen heißen G/N wobei

Identität $= N$

Inverses von $xN \Rightarrow x^{-1}N$

Einfaches Beispiel

Jede Gruppe hat min. 2 Untergruppen: $\underbrace{\{e\} \text{ und } G}_{\text{keine Faktorgruppen}}$

→ technisch gesehen sind das Normalgruppen

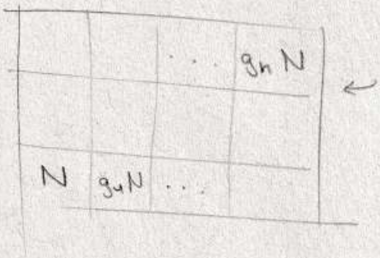
Normalteiler

$G := (G, \circ)$ Man kann mit N Nebenklassen bilden die G partitionieren

$N \trianglelefteq G$ (Faktorgruppen)

Wenn Nebenklassen von N keine Gruppen bilden ist N kein Normalteiler.

Beweis: Ist N ein Normalteiler?



Vorsicht: Links und Rechtsnebenklassen können sich unterscheiden wenn G nicht kommutativ ist

Wir arbeiten mit Linksnebenklasse:

$gN = \{ g \circ n \mid n \in N \} \quad g \in G$

↓

1. xN und yN sind Nebenklassen

2. Weil $e \in N$ (weil N eine Gruppe ist)
   $x \circ e = x \in xN$
   $y \circ e = y \in yN$

3. Wenn N eine Normalgruppe ist und sich die Nebenklassen wie eine Faktorgruppe verhalten mit der man rechnen kann:

   $x \cdot y \in (xN) \cdot (yN)$

Beispiel:

$$\underbrace{x + y + N}_{\overline{x+y}} = \underbrace{(x+N)}_{\overline{x}} \cdot \underbrace{(y+N)}_{\overline{y}}$$ „Quasi Restklassen"

Beliebiges Element aus Nebenklasse wählen

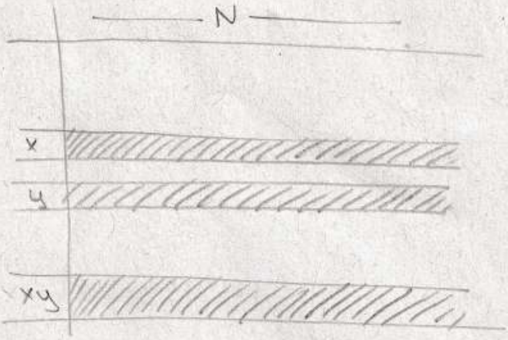
$$\left.\begin{array}{l} xN \mapsto xn_1 \\ yN \mapsto yn_2 \end{array}\right\}$$ konkrete Elemente aus Nebenklasse

$xn_1 \in xN$

$yn_2 \in yN$

$x n_1 \in xN$

$y n_2 \in yN$



$(x \cdot n_1) \cdot (y \cdot n_2) \in xyN$

oder

$(x \cdot n_1) \cdot (y \cdot n_2) = x \cdot y \cdot n_3$

$x y n_3 \in xyN$

$$(x \cdot n_1) \cdot (y \cdot n_2) = x \cdot y \cdot n_3 \quad | \cdot x^{-1}$$
$$x^{-1} \cdot (x \cdot n_1) \cdot (y \cdot n_2) = x^{-1} \cdot (x \cdot y \cdot n_3)$$
$$n_1 \cdot y \cdot n_2 = y \cdot n_3 \quad | y^{-1}$$
$$y^{-1}(n_1 \cdot y \cdot n_2) = y^{-1}(y \cdot n_3)$$
$$y^{-1} \cdot n_1 \cdot y \cdot n_2 = n_3 \quad | \cdot n_2^{-1}$$
$$(y^{-1} \cdot n_1 \cdot y \cdot n_2) \cdot n_2^{-1} = n_3 \cdot n_2^{-1}$$
$$\underbrace{y^{-1} \cdot n_1 \cdot y = n_3 \cdot n_2^{-1} \in N}$$

Daraus folgt:

$$y^{-1} \cdot n_1 \cdot y \in N$$

aus n_2

BEWEIS ↗

DAFÜR DAS NEBENKLASSEN EINE GRUPPE BILDEN

↙ Rechnen mit Faktorgruppen möglich

$\boxed{\text{Wenn: } (xN) \cdot (yN) = xyN \text{, dann } \boxed{y^{-1} \cdot N \cdot y = N}}$ ↙ Gruppe besitzt Inverse Elemente!

Identität:

$$N = eN$$
$$(eN)(gN) = (eg)N = gN$$

Inverses:

$$(gN)^{-1} = g^{-1}N \quad \text{weil} \quad (g^{-1}N)(gN) = (g^{-1} \cdot g)N = eN = N$$

Potenzen

$(G, \circ)$

$a \in G$ $\quad$ a^n = rekursive Ausführung von $\circ$ (n-mal)

$n \in \mathbb{Z}$

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

$3^2 = 3 + 3$

1. $a^{n+m} = a^n \circ a^m$
2. $(a^m)^n = a^{m \cdot n}$

erzeugt
kommutative Untergruppe

$\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$

Unendliche Ordnung

Alle Potenzen voneinander verschieden

$|\langle a \rangle| = \mathrm{ord}_G(a) = \infty$

$\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$

endliche Ordnung

$|\langle a \rangle| = \mathrm{ord}_G(a) = \min\{0 < k \mid a^k = e\}$

(Zyklisch weil $a^{n+|\langle a \rangle|} = a^n$)

$\langle a \rangle = \{a^n \mid 0 \leq n < \mathrm{ord}_G(a)\}$

Zyklische Gruppen

$a \in G$

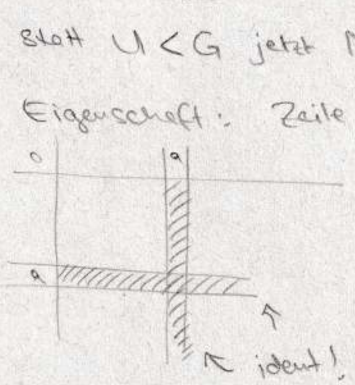
$G := (G, \circ)$

$\langle a \rangle$ bildet Nebenklasse (Untergruppe) oder die Gruppe selbst.

Normalteiler

statt $U < G$ jetzt $N \trianglelefteq G$

Eigenschaft: Zeile von a und Spalte von a sind ident in der Gruppe, deshalb ist jede Untergruppe ein „Normalteiler“:



$a \circ N = N \circ a \quad \forall a \in G$

Linksnebenklasse = Rechtsnebenklasse

Nur [illegible] Normalteilern [illegible] Nebenklassen bilden

- Das ist vor allem der Fall, wenn G kommutativ ist: $a \circ b = b \circ a$
- Oder $|G:U| = 2$

Nebenkl. 1 $\longrightarrow e \circ N = N \circ e = N$

Nebenklasse 2 $\longrightarrow G \setminus N$ (G modulo N)

Die wichtigste Eigenschaft von Normalklassen.
man kann mit ihnen wie Restklassen <u>modulo</u> rechnen!

<u>Beispiel 1)</u>

offensichtlicherweise Normalteiler, da kommutativ

$N := (5\mathbb{Z}, +)$

$G := (\mathbb{Z}, +)$

$$\begin{array}{c|l} & g_1 = 2 \\ g \circ N \Rightarrow & 2 \circ N = \{0, 2\pm 5, 2\pm 10, 2\pm 15, \dots\} \\ = & \quad = \\ N \circ g \Rightarrow & N \circ 2 = \{0, \pm 5 + 2, \pm 10 + 2, \pm 15 + 2, \dots\} \end{array}$$

<u>Beispiel 2)</u>

Nicht kommutativ

$N := Alt(3)$ $\qquad Alt(3) \trianglelefteq Sym(3)$

$G := Sym(3)$ $\qquad Alt(3) = \{Id, (123), (132)\}$

$Sym(3) = \{Id, (12), (13), (23), (123), (132)\}$

$$\begin{array}{c|l} & g_1 = (12)(3) \\ g \circ N & g_1 \circ N = \{\underbrace{(12) \circ Id}_{(12)}, \underbrace{(12) \circ (123)}_{(23)}, \underbrace{(12) \circ (132)}_{(13)}\} \\ = & \\ N \circ g & N \circ g_1 = \{\underbrace{Id \circ (12)}_{(12)}, \underbrace{(123) \circ (12)}_{(13)}, \underbrace{(132) \circ (12)}_{(23)}\} \end{array}$$

$\downarrow$

Inhaltlich gleich:
gleiche Menge aber nicht
gleiche Reihenfolge

G/N bei

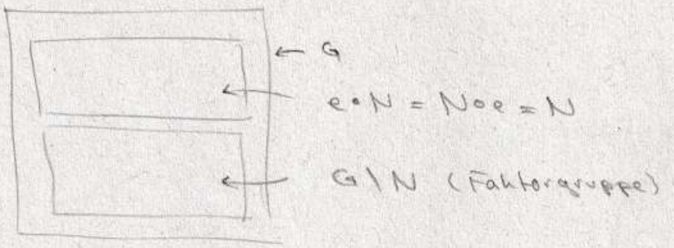
Beispiel 1) $\mathbb{Z}/5\mathbb{Z} = \{0, 1, 2, 3, 4\}$

Beispiel 2) $Sym(3)/Alt(3)$

Normalteiler $N \trianglelefteq G$

Buch

- Links, Rechtsnebenklassen stimmen überein (offensichtlich der Fall wenn kommutativ)
- Jede Untergruppe mit $|G : U| = 2$



(?)

- Man kann mit den Faktorgruppen (Nebenklassen von Normalteilern) wie Restklassen rechnen

Beweis:

$$\left.\begin{array}{l} a \circ N = N \circ a \\ b \circ N = N \circ b \end{array}\right\} \text{Nebenklassen von } N$$

$a_2 \in a \circ N$

$b_2 \in b \circ N$ → daraus folgt $a_2 \circ b_2 \in (a \circ N) \circ (b \circ N)$

Deshalb kann eine Operation für die Nebenklassen definiert werden und sie bilden eine eigene Gruppe:

Faktorgruppe $(G|N, \circ)$

Neutrales Element: $e \circ N = N$

Inverses Element: $\hat{a} \circ N$

Die Menge der Nebenklassen von N

wegen der Normalteilereigenschaft aber:

$$(a \circ N) \circ (b \circ N) =$$
$$(N \circ a) \circ (N \circ b) =$$
$$(N \circ (a \circ b)) \circ N) =$$
$$(a \circ b) \circ (N \circ N) =$$
$$(a \circ b) \circ N$$

Also $a_2 \circ b_2 \in (a \circ b) \circ N$ unabhängig davon welches a_2 und b_2 wir wählen

Faktorgruppen Beispiel

$G := (\mathbb{Z}, +)$

$N := (m\mathbb{Z}, +) \quad m \in \mathbb{N}$

$G/N := \mathbb{Z}/m\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{m-1}\}$

$\hookrightarrow$ ($\mathbb{Z}_m$ ist eine endliche Zyklische Gruppe erzeugt von $\bar{1}$)

Homomorphismen Beispiele

1) $G := (\mathbb{Z}, +)$ → unendliche Gruppe
$H := (\mathbb{Z}/2\mathbb{Z}, +)$ → endliche Gruppe

$\mathbb{Z} = \{\text{gerade Zahlen}\} \cup \{\text{Ungerade Zahlen}\}$

Regeln:

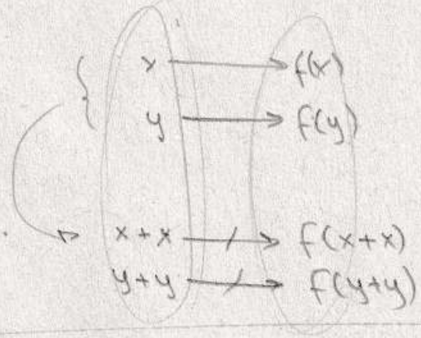
gerade + ungerade = ungerade | $0 + 1 \equiv 1 \mod 2$
ungerade + gerade = ungerade | $1 + 0 \equiv 1 \mod 2$
gerade + gerade = gerade | $0 + 0 \equiv 0 \mod 2$
ungerade + ungerade = gerade | $1 + 1 \equiv 0 \mod 2$

$f: \mathbb{Z} \longmapsto \mathbb{Z}/2\mathbb{Z}$
gerade $\longmapsto 0$
ungerade $\longmapsto 1$ ✓ Homomorphismus

Diese Abbildung ist nicht umkehrbar!

~~$g: \mathbb{Z}/2\mathbb{Z} \longmapsto \mathbb{Z}$~~ ⇒ $0 + 0 \equiv 0 \mod 2 \longrightarrow x + x = x \quad x = 0$
$1 + 1 \equiv 0 \mod 2 \longrightarrow y + y = y \quad y = 0$

$g: 0 \pmod 2 \longmapsto x$
$g: 1 \pmod 2 \longmapsto y$



---

2) $G := (\mathbb{Z}/4\mathbb{Z}, +)$
$H := \{1, -1, i, -i\}$
$(H, \times)$

Isomorphismus

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

×	1	i	-1	-i
1	1	i	-1	-i
i	i	-1	-i	1
-1	-1	-i	1	i
i	-i	1	i	-1

Gruppenhomomorphismus

Homomorphismus:

Abbildung von 2 Gruppen $(G, \circ)$ und $(H, *)$, $a, b \in G$

$$\varphi(a \circ b) = \varphi(a) * \varphi(b) \qquad \varphi: G \mapsto H$$

Isomorphismus:

Bijektive Abbildung $G \cong H$

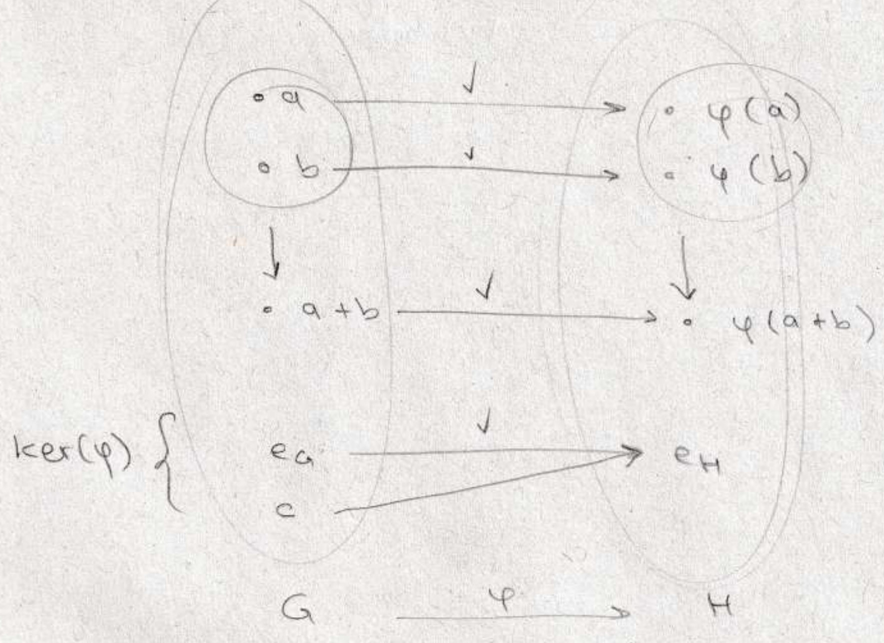
Beispielsweise $\varphi^{-1}: H \mapsto G$ inverse Abbildung

Beispiel

$\varphi: \mathbb{Z} \mapsto \langle a \rangle$, $n \mapsto a^n$ wenn alle Potenzen verschieden sind

mit $a \in G$ Isomorph mit $\mathbb{Z}$: $\langle a \rangle \cong \mathbb{Z}$

Voraussetzungen:



Satz

$\varphi: G \mapsto H \quad a \in G$

neutrales Element von G : e_G

neutrales Element von H : e_H

$\rightarrow$ Es gilt immer

$\varphi(e_G) = e_H$

$\varphi(a^{-1}) = \varphi(a)^{-1}$

Beweis:

$$e_G \circ e_G = e_G$$

$$\varphi(e_G) * \varphi(e_G) = \varphi(e_G \circ e_G)$$

$$\varphi(e_G) * \varphi(e_G) = \varphi(e_G) \quad | \cdot \varphi(e_G)^{-1}$$

$$\varphi(e_G) = e_H$$

$$a \circ a^{-1} = e_G \implies \varphi(a) * \varphi(a^{-1}) = \varphi(a^{-1}) * \varphi(a) = e_H$$

$$\varphi(a^{-1}) = \varphi(a)^{-1}$$

Definition Kern

$\varphi: G \mapsto H$

$\varphi^{-1}(\{e_H\})$ also $\varphi^{-1}(e_H)$

$\ker(\varphi) = \{a \in G \mid \varphi(a) = e_H\}$

Alle Elemente aus G die $\mapsto e_H$

(= Nullstellen in Zielmenge)

(= die x-Werte für die y bzw $\varphi(x) = 0$)

Definition Bild

$\varphi(G) = \{b \in H \mid \exists\, a \in G : \varphi(a) = b\}$

„Bild von G unter φ"

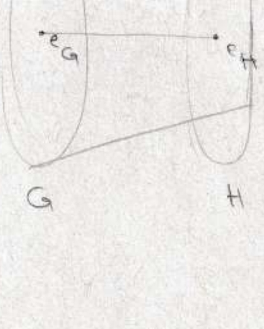
Nach der oberen Regel $\ker(\varphi)$ immer e_G und wenn nicht isomorph auch weitere Elemente

Satz

$\varphi: G \mapsto H$

$\ker(\varphi)$ ist ein Normalteiler von G

$\varphi(G)$ ist eine Untergruppe von G



Satz 2.65

Homomorphismen

$\varphi : G \mapsto H$

1) $\ker(\varphi) = \{a \in G \mid \varphi(a) = e_H\}$ ist ein Normalteiler von G

2) $\varphi(G) = \{\varphi(g) \mid g \in G\}$ ist eine Untergruppe von H

Beweis

$e_G \in \ker(\varphi)$ mit Sicherheit

2) Angenommen $a, b \in \ker(\varphi)$ und $|\ker(\varphi)| = 3$
dann gilt

$$\left.\begin{aligned} \varphi(a \circ b) &= \varphi(a) * \varphi(b) = e_H * e_H = e_H \\ \varphi(a^{-1}) &= \varphi(a)^{-1} = e_H \end{aligned}\right\}$$

→ Abgeschlossenheit
→ beinhaltet Inverses Elem.
→ beinhaltet neutrales El.
= Gruppe,
hier: Untergruppe v. G

$\ker(\varphi) \leq G$

Beweis (kompliziert)

1)
$a \in \ker(\varphi)$
$c \in G$

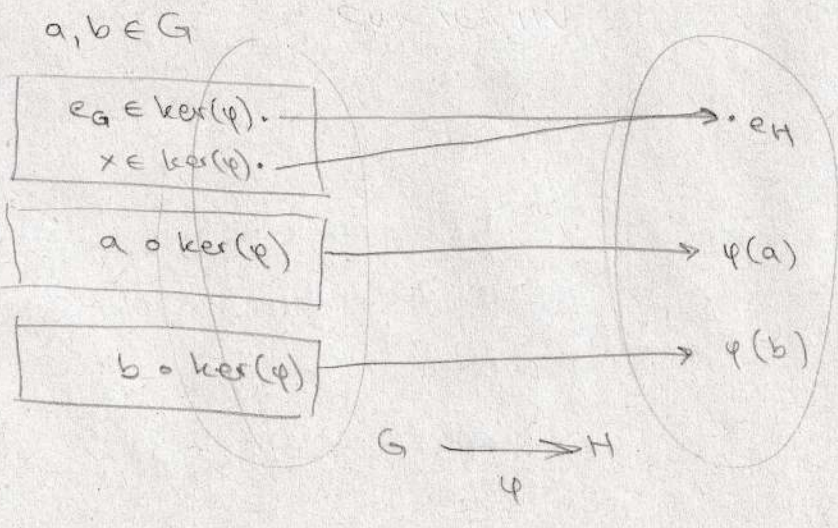
$$\varphi(c^{-1} \circ \ker(\varphi) \circ c) = \varphi(c)^{-1} * \overset{e_H}{\overset{\shortparallel}{\varphi(a)}} * \varphi(c) =$$

$$\varphi(c)^{-1} * e_H * \varphi(c) = e_H$$

$c^{-1} \circ a \circ c \in \ker(\varphi)$ $\quad c^{-1} \circ \ker(\varphi) \circ c \underset{\supseteq}{\subseteq} \ker(\varphi)$

→ ker(φ) ist Normalteiler von G

$a, b \in G$



$\varphi(G) \cong G \backslash \ker(\varphi)$

$\ker(\varphi) \trianglelefteq G$

Untergruppe die G partitioniert mit Nebenklassen (Faktorgruppe $G \backslash \ker(\varphi)$)

$a \circ \ker(\varphi)$
$b \circ \ker(\varphi)$

Homomorphiesatz

$\varphi : G \mapsto H$ Gruppenhomomorphismus

$G / \ker(\varphi)$ Faktorgruppe

$$\boxed{G / \ker(\varphi) \cong \varphi(G)}$$

→ Nebenklasse $\underbrace{a \circ \ker(\varphi)}_{= \{ a \circ k \mid k \in \ker(\varphi)} \in G / \ker(\varphi)$ entspricht $\varphi(a) \in \varphi(G)$

$$\left.\boxed{\begin{array}{l} a \circ \ker(\varphi) \\ b \circ \ker(\varphi) \\ c \circ \ker\varphi \\ \vdots \end{array}}\right\} G / \ker(\varphi)$$

$a \circ \ker(\varphi) \longrightarrow$ entspricht $\varphi(a) \in \varphi(G)$

weil

$\varphi(a \circ \ker(\varphi) =$

$\varphi(a) * \varphi(\ker(\varphi)) =$

$\varphi(a) * e_H$

Beweis

$\Psi : G \setminus \ker(\varphi) \longmapsto \varphi(G)$ —— surjektive Abbildung

$a \circ \ker(\varphi) \longmapsto \varphi(a) \quad a \in G$

wenn: $a \circ \ker(\varphi) = b \circ \ker(\varphi)$ gibt es (2 Nebenklassen gleich sind)

$c, d \in \ker(\varphi)$ mit $a \circ c = b \circ d$ (selbe Äquivalenzklasse)

$$\varphi(a) = \varphi(a) * e_H = \varphi(a \circ c) = \varphi(b \circ d) = \varphi(b) * e_H = \varphi(b)$$

$$\boxed{\begin{array}{l} \varphi(a) = \varphi(b) \Rightarrow \varphi(a \circ b^{-1}) = e_H \\ a \circ b^{-1} \in \ker(\varphi) \\ a \in b \circ \ker(\varphi) \\ a \circ \ker(\varphi) = b \circ \ker(\varphi) \end{array}}$$

$$\boxed{\begin{array}{c} \Psi((a \circ \ker(\varphi)) \circ (b \circ \ker(\varphi))) = \\ \Psi(a \circ \ker(\varphi)) * \Psi(b \circ \ker(\varphi)) \\ \Downarrow \\ \varphi(a \circ b) = \varphi(a) * \varphi(b) \end{array}}$$

Homomorphismen Beispiele

3) $f: \mathbb{Z} \mapsto \mathbb{Z}$

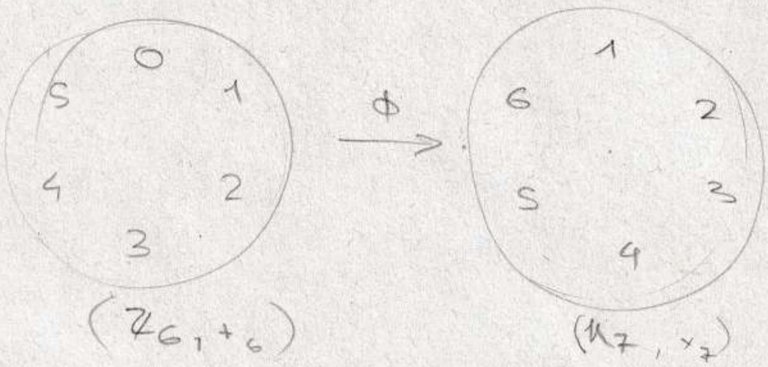
$f(x) = 2x$

$G := \mathbb{Z} \quad (\mathbb{Z}, +)$

$f(x+y) = f(x) + f(y)$

$2(x+y) = 2x + 2y$ ✓

4) $\Phi: \mathbb{Z}_6 \mapsto U_7$



$\Phi(n) = n+1$

$\Phi(1+2) = \Phi(3) = 4$

$\neq$

$\Phi(1) \times_7 \Phi(2) = 2 \times_7 3 = 6$

kein Homomorphismus mit dieser Abbildung aber:

$\Phi: \mathbb{Z}_6 \mapsto U_7$

$\Phi(n) = 3^n \pmod 7$

$\Phi(0) = 1$
$\Phi(1) = 3$
$\Phi(2) = 2$
$\Phi(3) = 6$
$\Phi(4) = 4$
$\Phi(5) = 5$

ISOMORPH ✓

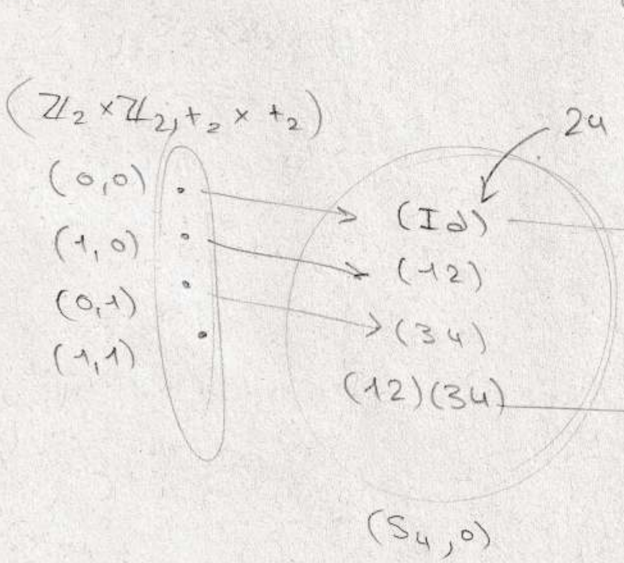
$U_7 \cong \mathbb{Z}_6$

Es gilt:

✓ $\Phi(n+m) = 3^{n+m} =$
$= 3^n \times 3^m = \Phi(n) \times \Phi(m)$

5) $\Phi: \mathbb{Z}_2 \times \mathbb{Z}_2 \mapsto S_4$

$\Phi((1,0)) = (12)(3)(4)$
$\Phi((0,1)) = (34)(1)(2)$ } die einzigen Angaben!



wichtig! $e_G \mapsto e_H$

wichtig! $(1,1) = (1,0) + (0,1)$

also: $(?) = (12) \circ (34)$

$(12)(34)$

Damit = Homomorphismus
aber kein Isomorphismus
weil (13) fehlt.

Beispiel

$G = \mathbb{Z} \quad (\mathbb{Z}, +)$

$H = \{1, \zeta_m, \zeta_m^2, \zeta_m^3, \dots \zeta_m^{m-1}\}$ endliche multiplikative zyklische Gruppe

m-te Einheitswurzeln

$(\zeta_m = e^{2\pi i/m})$

$\varphi : G \mapsto H$

$n \to \zeta_m^n$ surjektiver Homomorphismus mit $\ker(\varphi) = m\mathbb{Z}$ da:

$\varphi(n) - \zeta_m^n = e^{2\pi i n/m} = 1$

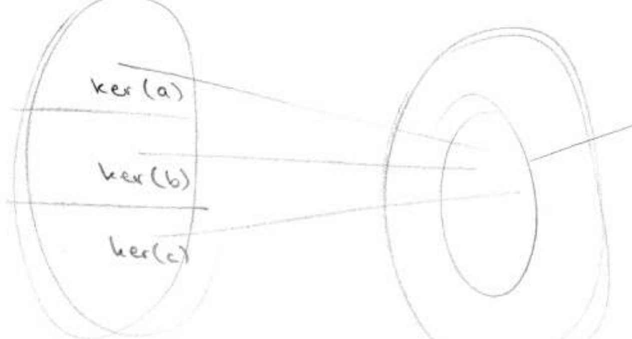
wen n/m

$\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z} \cong H = \langle \zeta_m \rangle$

Homomorphie-Satz: $(G,\circ) \xrightarrow{\text{Homomorphismus } \varphi} (H, *)$

$\varphi(a \circ b) = \varphi(a) + \varphi(b)$

Rechnen, dann abbilden ist gleich mit abbilden, dann rechnen.



φ(G) Bild von G

Kerne sind schöne Untergruppen: Normalteiler

$(a \circ \ker(\varphi)) \circ (c \circ \ker(\varphi)) = (b \circ \ker(\varphi))$

Rechnen mit Nebenklassen:

Faktorgruppe $(G/_{\ker\varphi}, \circ) \underset{\uparrow}{\cong}$ Bild von G $(\varphi(G), *)$

isomorph (bijektiv)

Isomorphismus:

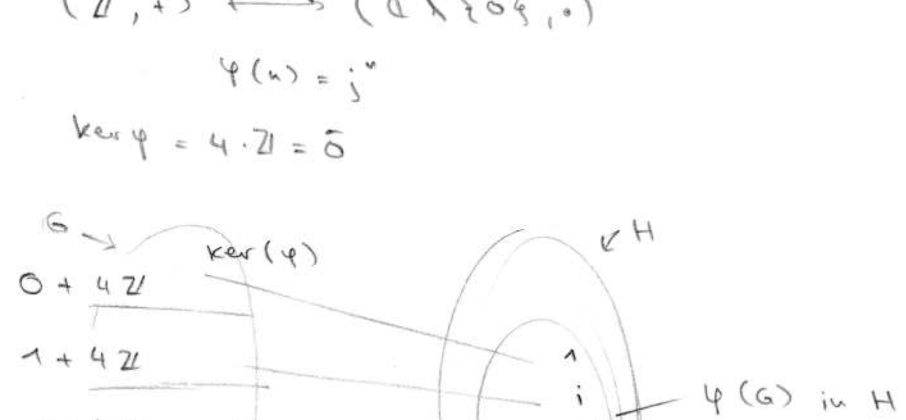
$\psi : G/_{\ker\varphi} \longmapsto \varphi(G)$

Beispiel:

$(\mathbb{Z}, +) \overset{\varphi}{\longmapsto} (\mathbb{C} \setminus \{0\}, \cdot)$

$\varphi(n) = i^n$

$\ker\varphi = 4 \cdot \mathbb{Z} = \bar{0}$



Homomorphiesatz in diesem Fall:

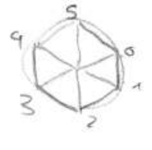
Es ist egal, ob man Berechnungen in Restklassen durchführt oder außerhalb dieser.

Beispiel:

$(\mathbb{Z}/m\mathbb{Z}, +) \longmapsto$ (Einheitswurzeln, +)

wenn $m = 6$

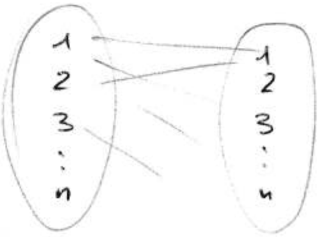
$\bar{0}\ \bar{1}\ \bar{2}\ \bar{3}\ \bar{4}\ \bar{5}$



Symmetrische Gruppen

Symmetrische Gruppe S_n aller $n!$ Permutationen: $|S_n| = n!$

Also S_n = Alle bijektiven Abbildungen von



zB: $\pi = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 3 & 2 & 1 & \dots & n \end{pmatrix}$

$\pi : \{1, 2, 3, \dots, n\} \longrightarrow \{1, 2, 3, \dots, n\}$

Beispiel

$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix}$

$\pi^{-1} \begin{pmatrix} 3 & 5 & 4 & 1 & 2 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} =$

$\pi^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 3 & 2 \end{pmatrix}$

$\pi = (1\,3\,4)(2\,5) = (5\,2)(4\,1\,3)$

$\pi = (5\,2) \circ (4\,1\,3)$ Zerlegung eines Zyklus

$= (5\,2)(1)(3)(4) \circ (4\,1\,3)(2)(5) =$

$= (2\,5)(1\,3\,4)$

Definition: Signum

Vorzeichen von $\pi \in S_{\textcircled{n}}$

a) $\operatorname{sgn}(\pi) := \prod_{1 \le i < j \le \textcircled{n}} \frac{\pi(j) - \pi(i)}{j - i}$ ⓘ?

$\operatorname{Sgn}(\pi)$ / gerade - Signum 1
\ ungerade - Signum -1

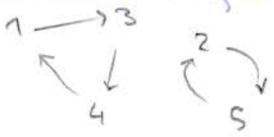
b) Berechnung von Signum anhand der # der Fehlstände von π

$\operatorname{Sgn}(\sigma \circ \pi) = \operatorname{sgn}(\sigma) \circ \operatorname{sgn}(\pi)$

Signum ist ein Gruppenhomomorphismus zwischen der sym Gruppe $(S_n, \circ)$ und der zweielementigen Gruppe $(\{1, 2\}, \circ)$

$\pi = (1\,3\,4)(2\,5)$ ←

Zyklendarstellung der Permut.



Der Graph zerfällt in Zyklen.

①, $\pi(1) = 3$, $\pi(3) = 4$, $\pi(4) = 1$

②, $\pi(2) = 5$, $\pi(5) = 2$

Definition: Fixpunkte

$\mathrm{Id} = (1)(2)(3)(4)(5)$
↑ Fixpunkt

Als Graph mit Schlinge

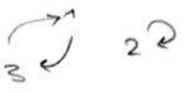
Die Berechnung des Signum

Beispiel:

$\pi : (1\,3)(2) \in S_3$

Liste an Zuordnungen bei Abbildung:

n	$\pi(n)$
1	$\pi(1) = 3$
2	$\pi(2) = 2$
3	$\pi(3) = 1$



Definition Signum:

$$\mathrm{sgn}(\pi) := \prod_{1 \leq i < j \leq n} \frac{\pi(j) - \pi(i)}{j - i}$$

wobei:

$i \longmapsto \pi(i)$

$j \longmapsto \pi(j)$

Berechnung:

$$\mathrm{sgn}(\pi) = \mathrm{sgn}((1\,3)(2)) =$$

$$\frac{\pi(2) - \pi(1)}{2 - 1} \cdot \frac{\pi(3) - \pi(2)}{3 - 2} =$$

$$\frac{2 - 3}{1} \cdot \frac{1 - 2}{1} =$$

$$-1 \cdot -1 = \textcircled{1}$$

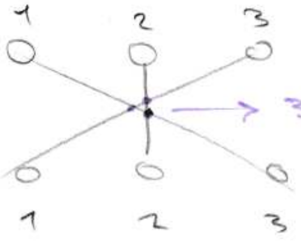
positiv, also # Fehlst muss gerade sein

Die Ermittlung der Fehlstand-Anzahl

Definition Fehlstand:

Paar von π bei der $i < j$ aber $\pi(i) > \pi(j)$

(i, j)



→ 3 Schnittpunkte aber 2 Fehlstände

$$\left.\begin{array}{ll} 1 < 2, & \pi(1) > \pi(2) \\ 1 < 3, & \pi(1) > \pi(3) \end{array}\right\} 2 \checkmark$$

$2 < 3, \quad \pi(2) < \pi(3)$

Alternative Methode zur Berechnung des Signums:

$$\mathrm{sgn}\underbrace{(k_1, k_2, \ldots, k_n)}_{n = \text{Stellen Anzahl}} = (-1)^{n+1}$$

Beispiel:

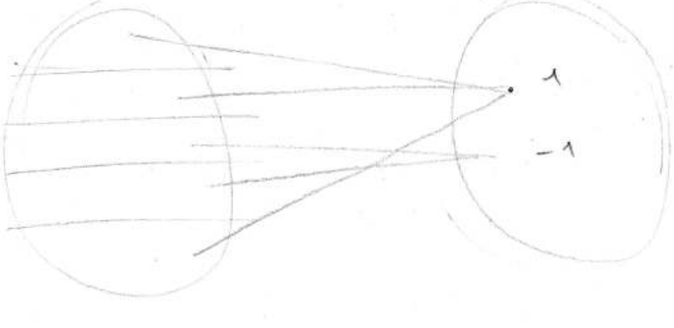
$$(1\,2\,6) \circ \underbrace{(3\,5) \circ (3\,5)}_{\mathrm{Id} = (1)} \Rightarrow \mathrm{sgn}((1\,2\,6) \circ (1)) = \underbrace{\mathrm{sgn}(1\,2\,6)}_{(-1)^{3+1}} \cdot \underbrace{\mathrm{sgn}(1)}_{(-1)^{1+1}} = 1$$

S_n ... Symmetrische Gruppen
A_n ..... Alternierende Gruppe

Gruppenhomomorphismus

Symm. Gruppe — Signum

$$(S_n, \circ) \longmapsto (\{1,-1\}, \cdot)$$



ab $n \geq 2$ auch surjektiv (jedes Element im Abbild min 1 Urbild)

Kern von Signum

$$\ker(sgn) = \{\pi \in S_n \mid sgn(\pi) = 1\} =: A_n$$

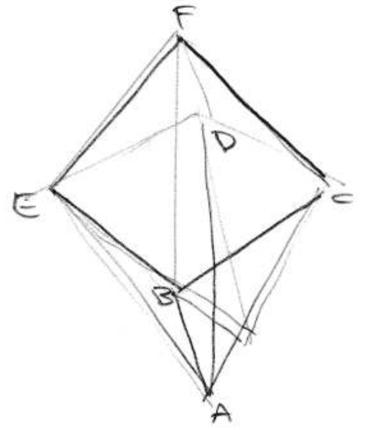
Das Urbild vom Signum welches abgebildet das Einheitselement von Signum zeigt (1)

Alle geraden Permutationen (zeigen auf 1) $\in A_n$
Alle ungerad. Permutationen (zeigen auf -1) $\in S_n \setminus A_n$

A_n ist ein Normalteiler weil $|S_n : A_n| = 2$

$|A_n| = |S_n \setminus A_n| = n!/2 \iff$ es gibt genausoviele gerade wie ungerade Permutationen

Gruppenoperation, Gruppenwirkung ← Homomorphismus + Zyklen



Oktaeder, 6 Ecken

$M := \{A, \dots, F\}$ → statisch

$(G, \circ) := (\mathbb{Z}/4\mathbb{Z}, +)$ → dynamisch

Abbildung: $\bullet$

$G \times M \longrightarrow M$

Kombination von Gruppe und Menge

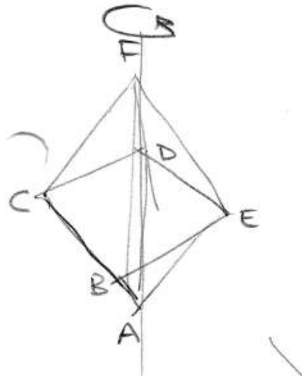
$\bullet$	A	B	C	D	E	F	~~G~~
0	A	B	C	D	E	F	
1	A	E	B	C	D	F	
2	A	D	E	B	C	F	
3	A	C	D	E	B	F	

← A & F werden von Rotation nicht beeinflusst

+90°

+90°

+90°



Rotation um Achse

Wir stellen uns vor:

0 : Rotation um 0°

1 : Rotation um 90°

2 : Rotation um 180°

3 : Rotation um 270°

sehr ähnlich wie:

$(\mathbb{Z}/4\mathbb{Z}, +)$

$3+1 = 4 \equiv 0 \mod 4$

$270+90 = 360 \equiv 0 \mod 360$

↓

Isomorphie

Definition Gruppenwirkung

Abbildungs Operator (erfunden)

$e \bullet m = m$ neutrales Element: 0 oder 0°

für $\forall m \in M$

$$(g_1 \circ g_2) \bullet m = g_1 \bullet (g_2 \bullet m)$$

nach Abbildung rechnen = vor Abbildung rechnen, Assoziativität

Beispiel $\underbrace{(90^\circ + 90^\circ)}_{180^\circ} \bullet m = 90^\circ \bullet (90^\circ \bullet m)$

Stabilisatoren:

Stabilisator von F: alle Elemente $\{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$ → Position bleibt gleich

von B: nur $\bar{0}$

Ziel der Gruppenwirkung:

etwas Statisches dynamisch machen

unsere Abbildung ist eigentlich auch eine Operation! $\bullet$:= Rotieren

Beispiel 2.48)
aus Buch:

Die symmetrische Menge S_n der Permutationen der Zahlen $\{1,2,\dots,n\}$ ist die Menge der bijektiven Abbildungen

$$\pi : \{1,2,3,\dots,n\} \longrightarrow \{1,2,3,\dots,n\}$$

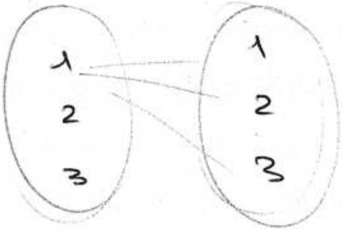
Führt man 2 bijektive Abbildungen hintereinander erhält man wieder eine Bijektive Abbildung

---

$(S_n, \circ)$ bildet die sogenannte Symmetrischen Gruppe
Die identische Abbildung $id(j) = j$ ist das neutrale Element

Erklärung

S_3
$n=3$:



wie viele Möglichkeiten gibt es beide Mengen miteinander bijektiv / Symmetrisch zu verbinden?

$$3 \cdot 2 \cdot 1 = 3! = 6$$

$$P(S_3) = \{ Id(S_3), (1,2)(3), (1\,3)(2),$$

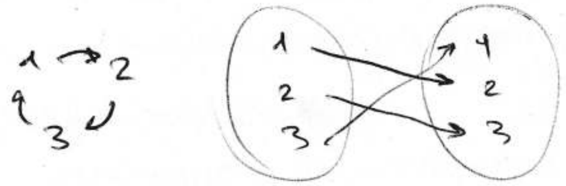
$$\boxed{= (1)(2)(3)}$$

$$(2\,3)(1), (1\,2\,3), (1\,3\,2) \}$$

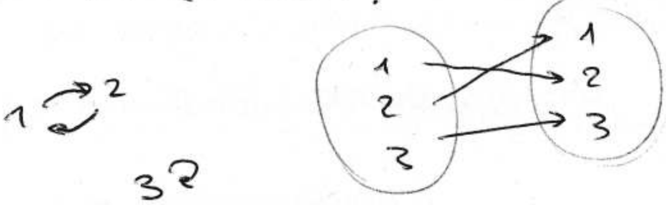
Was ist (1 2 3)?

$|P(S_3)| = 6$ wie oben gezeigt.

Ein Zykel



Was ist (1 2)(3)? (Schreibt man normalerweise als (1 2) auf)



WIKIPEDIA

Zyklische Gruppe

In der Gruppentheorie ist eine **zyklische Gruppe** eine Gruppe, die von einem einzelnen Element a erzeugt wird. Sie besteht nur aus Potenzen des Erzeugers a:

$$\langle a \rangle := \{a^n \mid n \in \mathbb{Z}\}.$$

Eine Gruppe G ist also zyklisch, wenn sie ein Element a enthält, sodass jedes Element von G eine Potenz von a ist. Gleichbedeutend damit ist, dass es ein Element a gibt, sodass G selbst die einzige Untergruppe von G ist, die a enthält. In diesem Fall wird a ein *erzeugendes Element* oder kurz ein *Erzeuger* von G genannt.

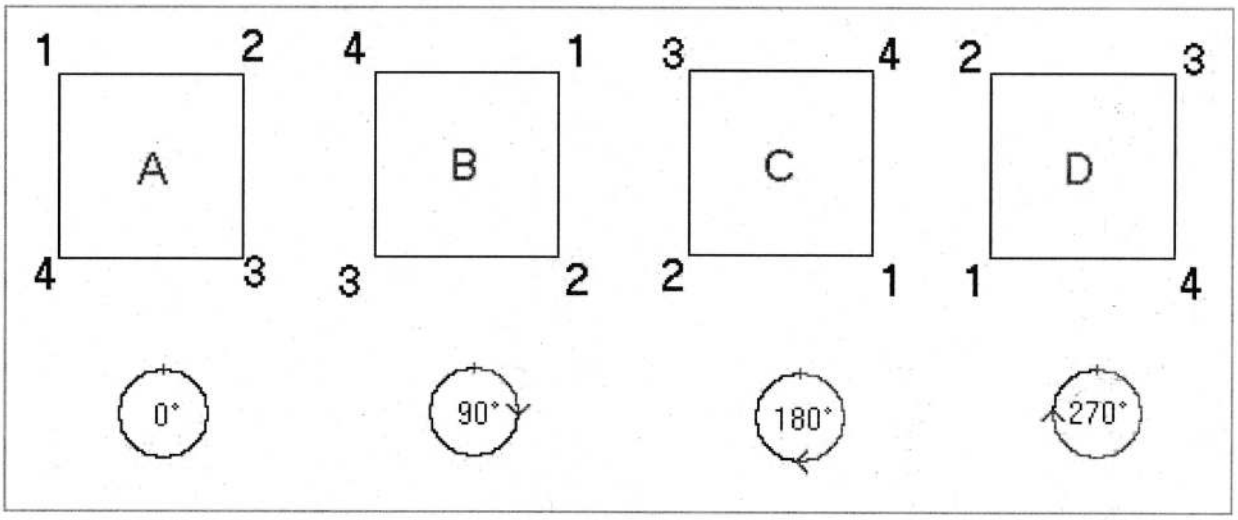
Zyklische Gruppen sind die einfachsten Gruppen und können vollständig klassifiziert werden: Für jede natürliche Zahl n (für diese Aussage betrachten wir 0 nicht als natürliche Zahl) gibt es eine zyklische Gruppe C_n mit genau n Elementen, und es gibt die *unendliche zyklische Gruppe*, die additive Gruppe der ganzen Zahlen $\mathbb{Z}$. Jede andere zyklische Gruppe ist zu einer dieser Gruppen isomorph.

Inhaltsverzeichnis

Veranschaulichung

Drehgruppen

Die endlichen zyklischen Gruppen können veranschaulicht werden als Drehgruppen regulärer Vielecke in der Ebene. Zum Beispiel besteht die Gruppe C_4 aus den möglichen Drehungen der Ebene, die ein vorgegebenes Quadrat in sich überführen.



Die obenstehende Abbildung zeigt ein Quadrat A und die Stellungen B, C und D, in die es durch Drehen überführt werden kann. Darunter ist jeweils die dazu nötige Drehung angegeben. Die Elemente der zyklischen Gruppe sind hier die Bewegungen und nicht die Stellungen des Quadrats. Das heißt, die Gruppe C_4 besteht in dieser Darstellung aus der Menge {0°, 90°, 180°, 270°}. Die Verknüpfung der Elemente ist die Hintereinanderausführung der Drehungen; das entspricht einer Addition der Winkel. Dabei stimmt die Drehung um 360° mit der Drehung um 0° überein, die Winkel werden also genau genommen modulo 360° addiert.

Lässt man nicht nur Drehungen der Ebene zu, sondern auch Spiegelungen, dann erhält man im Fall von Vielecken die so genannten Diedergruppen.

Die Drehgruppe des Kreises, S^1, ist nicht zyklisch.

Restklassengruppen

Eine andere Darstellung einer zyklischen Gruppe liefert die Addition modulo einer Zahl, die so genannte Restklassenarithmetik. In der additiven Gruppe $(\mathbb{Z}/n\mathbb{Z}, +)$ ist die Restklasse der 1 ein Erzeuger, das heißt, man kann jede andere Restklasse erhalten, indem man die 1 wiederholt mit sich selbst addiert. Am Beispiel $\mathbb{Z}/4\mathbb{Z} = \{0, 1, 2, 3\}$ bedeutet dies, dass sich alle 4 Elemente als Summe von 1 darstellen lassen, also 1 = 1, 2 = 1+1, 3 = 1+1+1, 0 = 1+1+1+1. Die Restklassengruppe $\mathbb{Z}/4\mathbb{Z}$ verhält sich genauso wie die oben beschriebene Drehgruppe {0°, 90°, 180°, 270°}: 0 entspricht 0°, 1 entspricht 90° usw: Diese beiden Gruppen sind isomorph.

Notationen

Für die endlichen zyklischen Gruppen sind im Wesentlichen die drei Notationen verbreitet: C_n, $\mathbb{Z}/n\mathbb{Z}$ und $\mathbb{Z}_n$. Für die nichtendliche zyklische Gruppe gibt es die Notationen C_∞ und $\mathbb{Z}$. Als Gruppenoperation wird in $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$ und $\mathbb{Z}_n$ auf die Addition Bezug genommen. In C_n wird die Gruppenoperation oft auch multiplikativ geschrieben.

Die Bezeichnungen $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{Z}_n$ und $\mathbb{Z}$ rühren daher, dass die additiven Gruppen der Restklassenringe $\mathbb{Z}/n\mathbb{Z}$ und von $\mathbb{Z}$ selbst die bekanntesten Vertreter zyklischer Gruppen sind. Alle diese Strukturen sind sogar Ringe, die neben der hier einschlägigen Addition auch eine (hier nicht verwendete) multiplikative Verknüpfung haben.[1]

Die Bezeichnung $\mathbb{Z}_n$ wird außerdem für die n-adischen Zahlen verwendet.

Eigenschaften

Alle zyklischen Gruppen sind abelsche Gruppen.

Eine zyklische Gruppe kann mehrere Erzeuger haben. Die Erzeuger von $\mathbb{Z}$ sind +1 und −1, die Erzeuger von $\mathbb{Z}/n\mathbb{Z}$ sind die Restklassen, die teilerfremd zu n sind; ihre Anzahl $\varphi(n)$ wird von der Eulerschen φ-Funktion angegeben.

Ist allgemein d ein Teiler von n, dann ist $\varphi(d)$ die Anzahl der Elemente von $\mathbb{Z}/n\mathbb{Z}$, die die Ordnung d haben:

$$\Big|\{m \in \mathbb{Z}/n\mathbb{Z} \mid \operatorname{ord}(m) = d\}\Big| = \varphi(d).$$

Das direkte Produkt zweier zyklischer Gruppen C_n und C_m ist genau dann zyklisch, wenn n und m teilerfremd sind; in diesem Fall ist das Produkt isomorph zu C_{mn}.

Jede endlich erzeugte abelsche Gruppe ist direktes Produkt endlich vieler (endlicher und unendlicher) zyklischer Gruppen.

Der Gruppenexponent einer endlichen zyklischen Gruppe ist gleich ihrer Ordnung. Jede endliche zyklische Gruppe ist isomorph zur additiven Gruppe des Restklassenring $\mathbb{Z}/n\mathbb{Z}$, der Isomorphismus ist dabei der diskrete Logarithmus: Ist a ein Erzeuger von C_n, dann ist die Abbildung

$$a^t \mapsto t \bmod n$$

ein Isomorphismus.

Untergruppen und Faktorgruppen

Alle Untergruppen und Faktorgruppen von zyklischen Gruppen sind zyklisch. Insbesondere sind die Untergruppen von $\mathbb{Z}$ von der Form $m\mathbb{Z}$ mit einer natürlichen Zahl $m \in \mathbb{N}_0$. Für verschiedene m sind diese Untergruppen verschieden, und für $m \neq 0$ sind sie isomorph zu $\mathbb{Z}$.

Der Verband der Untergruppen von $\mathbb{Z}$ ist isomorph zum dualen Verband der natürlichen Zahlen mit der Teilbarkeit. Alle Faktorgruppen von $\mathbb{Z}$ sind endlich, mit Ausnahme der trivialen Faktorgruppe $\mathbb{Z}/\{0\}$.

Für jeden positiven Teiler d von n hat die Gruppe $\mathbb{Z}/n\mathbb{Z}$ genau eine Untergruppe der Ordnung d, nämlich die von dem Element n/d erzeugte Untergruppe $\{kn/d \mid k = 0, \ldots, d-1\}$. Andere als diese Untergruppen gibt es nicht. Der Untergruppenverband ist deshalb isomorph zum Teilerverband von n.

Eine zyklische Gruppe ist genau dann einfach, wenn ihre Ordnung eine Primzahl ist.

Endomorphismen und Automorphismen

Der Endomorphismenring (siehe Gruppenhomomorphismus) der Gruppe C_n ist Ring-isomorph zum Restklassenring $\mathbb{Z}/n\mathbb{Z}$. Unter diesem Isomorphismus entspricht die Restklasse r von $\mathbb{Z}/n\mathbb{Z}$ dem Endomorphismus von C_n, der jedes Element auf seine r-te Potenz abbildet. Daraus folgt, dass die Automorphismengruppe von C_n isomorph zur Gruppe $(\mathbb{Z}/n\mathbb{Z})^*$, der Einheitengruppe des Rings $\mathbb{Z}/n\mathbb{Z}$, ist. Diese Gruppe besteht aus den Elementen, die teilerfremd zu n sind, und hat somit genau $\phi(n)$ Elemente.

Der Endomorphismenring der zyklischen Gruppe $\mathbb{Z}$ ist isomorph zum Ring $\mathbb{Z}$, und die Automorphismengruppe ist isomorph zur Einheitengruppe $\{+1, -1\}$ von $\mathbb{Z}$, und diese ist isomorph zur zyklischen Gruppe C_2.

Algebraische Eigenschaften

Ist n eine natürliche Zahl, dann ist $(\mathbb{Z}/n\mathbb{Z})^*$ genau dann zyklisch, wenn n gleich $1, 2, 4, p^k$ oder $2p^k$ ist, für eine Primzahl $p > 2$ und eine natürliche Zahl k. Die Erzeuger dieser zyklischen Gruppe heißen Primitivwurzeln modulo n.

Insbesondere ist für jede Primzahl p die Gruppe $(\mathbb{Z}/p\mathbb{Z})^*$ zyklisch mit $p-1$ Elementen. Allgemeiner ist jede *endliche* Untergruppe der multiplikativen Gruppe eines Körpers zyklisch.

Die Galoisgruppe einer endlichen Körpererweiterung eines endlichen Körpers ist eine endliche zyklische Gruppe. Umgekehrt gibt es für jeden endlichen Körper K und jede endliche zyklische Gruppe G eine endliche Körpererweiterung L/K mit Galoisgruppe G.

Anmerkungen

1. Wegen der Nicht-Invertierbarkeit der Null ist diese multiplikative Verknüpfung *niemals* (außer im trivialen Fall des Nullrings) eine Gruppenverknüpfung für die Grundmenge – und kann dieser auch keine zyklische Gruppenstruktur verleihen. (Etwas Anderes sind die primen Restklassengruppen, die mindestens ein Element weniger haben.)

Siehe auch

- Dizyklische Gruppe
- Polyzyklische Gruppe
- Zyklische Permutation

Modern Algebra

$a, b \in G$ zwei Elemente

$a \circ b \in G$ erhalten eine Zuordnung die ebenfalls $\in G$ ist [Abgeschlossenheit]

in Gruppe $(G, \circ)$ gelten:

1) Assoziativgesetz

$(a \circ b) \circ c = a \circ (b \circ c)$

2) Neutrales Element

$e \circ a = a \circ e = a$

3) inverses Element

$a^{-1} \circ a = e$ bzw $i(a) \circ a = e$ → $i(a \circ b) = i(b) \circ i(a)$ umgekehrt!

4) Kommutativgesetz

$a \circ b = b \circ a$

Eine Untergruppe

$(H, \circ)$ $(G, \circ)$

$\hookrightarrow H \subseteq G \hookleftarrow$ Teilmenge (nicht leer)

1) e von G ist in H enthalten

2) H ist abgeschlossen

3) Alle Elemente haben ein Inverses

Beispiele

Additive Gruppen:

$(\mathbb{Z}, +)$ abel'sche Gruppe

0) – Abgeschlossen

1) – Assoziativ $a + (b+c) = (a+b) + c$

2) – Neutrales Element : 0

3) – Inverses Element : $a \rightarrow i(a) = -a$

4) – Kommutativ Gesetz : $a + b = b + a$

Sowie:

.... $(\mathbb{Z}_m, +)$ $(\mathbb{Q}, +)$ $(\mathbb{R}, +)$ $(\mathbb{C}, +)$

aber:

$(\mathbb{N}_0, +)$ keine Gruppe!

Es können keine Inversen gebildet werden

$(\mathbb{Z}_m, \cdot)$ wenn $m \notin \mathbb{P}$ Primzahlen, keine Gruppe!

Es können keine Inverseen für alle gebildet werden!

Untergruppen

Die geraden Zahlen $H = \{2n \mid n \in \mathbb{Z}\} = 2\mathbb{Z} \rightarrow (H, +)$

$H \subseteq (\mathbb{Z}, +)$

Multiplikative Gruppen

$(\mathbb{Q} \setminus \{0\}, \cdot)$ Rationale Zahlen ohne 0 → kommutative Gruppe

2) Neutrales Element : 1

$(\mathbb{Z}_p \setminus \{0\}, \cdot)$

$(\mathbb{R} \setminus \{0\}, \cdot)$

$(\mathbb{C} \setminus \{0\}, \cdot)$

Aber:

$(\mathbb{N}, \cdot)$ und $(\mathbb{Z}, \cdot)$ können keine Inversen bilden!

Zusammenfassung, Algebraische Strukturen

Körper $(K,+,\cdot)$

1) Addition $(K,+)$ kommutative Gruppe Nullelement $e=0$
2) Multiplikation $(K,\cdot)$ kommutative Gruppe Einselement $e=1$
3) Distributivgesetz $(K,+,\cdot)$ $ab+ac = a(b+c)$

Beispiel:

$(\mathbb{R},+,\cdot)$ bildet $(\mathbb{R},+)$ und $(\mathbb{R}\setminus\{0\},\cdot\}$

genau wie $\mathbb{Q}$, $\mathbb{C}$, $\mathbb{Z}p$

Ring $(R,+,\cdot)$

1) Addition $(R,+)$ kommutative Gruppe Nullelement $e=0$

(!) ~~2) Multiplikation $(R,\cdot)$~~ keine Gruppe!
nicht alle Elemente besitzen ein Inverses

3) Distributivgesetz $ab+ac = a(b+c)$

Man unterscheidet zwischen:

- $ab=ba$ Kommutativgesetz → kommutativer Ring
- $(R,\cdot)$ $e=1$ Einselement → kommutativer Ring mit 1

Körper sind kommutative Ringe mit 1 die alle multiplikative Inverse haben.

Ideale

$I \subseteq R$, Untergruppe von Ring
bezüglich Addition

Jedes Vielfache eines Elementes aus I liegt wieder in I

1) $0 \in I$
$a+b \in I$
$-a \in I$

2) $a \in I$
$\boxed{b \in R}$
$ab \in I$ $ba \in I$

Beispiele:

Körper:

$(\mathbb{Z}_p, +, \cdot)$ mit $p \in \mathbb{P}$

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

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

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

Ringe:

$(\mathbb{Z}, +, \cdot)$ (kein Körper, da es nicht zu jeder Zahl ein multipl. Inv. gibt)

$(\mathbb{Z}_m, +, \cdot)$ mit $m \notin \mathbb{P}$

$\mathbb{R}[x] = \{p_n x^n + \dots + p_1 x + p_0 x^0 \mid p_k \in \mathbb{R}\}$

$(\mathbb{R}[x], +, \cdot)$ – Menge der Polynome: kommutativer Ring mit 1

$p(x) + q(x)$ und $p(x) \cdot q(x)$

- Kommutativgesetz von $\mathbb{R}$ geerbt
- Assoziativgesetz von $\mathbb{R}$ geerbt
- Distributivgesetz von $\mathbb{R}$ geerbt

- Addition, neutrales Element: Nullpolynom $p(x) = 0$
- Multiplikation, neutrales Elem. konstantes Polynom $p(x) = 1$

- Additiv Inverse $p(x) \rightarrow -p(x)$

Aber keine multiplikativ Inversen:

Beispiel:

$p(x) = x^2$

$x^2 \cdot \underbrace{q(x)}_{\text{inv}} = 1$ $\quad q(x) = \frac{1}{x^2}$ → kein Polynom!

Allgemein gilt:

$\mathbb{K}[x]$ Polynomring über $\mathbb{K}$

Ideale

Menge aller geraden Zahlen:

$$\underset{I}{\boxed{\text{gerade}}} + \underset{I}{\boxed{\text{gerade}}} = \underset{I}{\boxed{\text{gerade}}}$$

$$\underset{\text{Ring}}{\boxed{\text{beliebige Zahl}}} \cdot \underset{I}{\boxed{\text{gerade}}} = \underset{I}{\boxed{\text{gerade}}} \rightarrow$$

Jedes Vielfache eines Elementes aus I wieder in I

Beispiel

~~Ale~~ Alle geraden Zahlen

Alle Polynome $p(x)$ für die $p(0) = 0$ ist

Ideal in $\mathbb{R}[x]$

Euklidischer Algorithmus und diophantische Gleichungen

$ggT(e, m) = 1$ gesucht: e^{-1}

$ex + my = 1$

$x \in \mathbb{Z}_m$

- Anwendung: in $\mathbb{Z}_m$ multipl. Inverse finden ↗

Beispiel:

$ggT(217, 63) = 7$

$217 = 3 \cdot 63 + 28$ $ggT(217, 63)$ $217 \bmod 63 = 28$

$63 = 2 \cdot 28 + 7$ $ggT(63, 28)$ $63 \bmod 28 = 7$

$28 = 4 \cdot 7 + 0$ $ggT(28, 7)$ $28 \bmod 7 = 0$

$\underline{ax + by} = ggT(a,b)$

diophantische Gleichung: gesucht sind ganzzahlige Lösungen

Beispiel:

$75x + 38y = \textcircled{1}$ $ggT(75, 38) = 1$ ✓ ~~$x_0 = 1$ $y_0 = 0$ $x_1 = 0$ $y_1 = 1$~~

I $75 = 1 \cdot 38 + 37$ $37 = 75 - 1 \cdot 38$

II $38 = 1 \cdot 37 + 1$ $1 = 38 - 1 \cdot 37$

III $37 = 37 \cdot \textcircled{1} + 0$ $(0 = 37 - 1 \cdot 37)$

muss ein Vielfaches vom ggT sein

II $1 = 38 - 1 \cdot 37$

I $1 = 38 - 1 \cdot (75 - 1 \cdot 38)$

$1 = 38 - 75 + 38$

$$\underbrace{1}_{ggT} = \underbrace{-1}_{x} \cdot 75 + \underbrace{2}_{y} \cdot 38$$

Beispiel

$75x + 38y = 10\,000$

$\ldots$ $x = -10\,000$

$y = 20\,000$

weitere Lösungen →

$$\left.\begin{aligned} \tilde{x} &= -10\,000 + k \cdot 38 \\ \tilde{y} &= 20000 \underset{-}{\cancel{+}} k \cdot 75 \end{aligned}\right\} k \in \mathbb{Z}$$

Beispiel

Das multiplikativ-Inverse von 75 mod 38

$$75 \cdot [inv] \equiv 1 \mod 38$$

$$75 \cdot [inv] = 38 \cdot \mathbb{Z} + 1$$

$$75 \cdot [inv] - 38 \cdot n = 1 \longrightarrow ggT(75,38) = 1$$

$$\begin{array}{l|l} 75 = 1 \cdot 38 + 37 & 37 = 75 - 1 \cdot 38 \\ 38 = 1 \cdot 37 + 1 & 1 = 38 - 1 \cdot 37 \\ 37 = 37 \cdot \textcircled{1} + 0 & \end{array}$$

$$\underset{\substack{\uparrow \\ \textcircled{-1} \\ \downarrow}}{75x} + \underset{\substack{\uparrow \\ 2}}{38y} = 1$$

$$x \equiv -1 \equiv 37 \mod 38$$

Probe ~~37·57~~

$\overline{37 \cdot 75} \equiv 1 \mod 38$ ✓

Polynomring und endliche Körper

Beispiel für unendlich vielen Elementen im Körper: $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$, $(\mathbb{C},+,\cdot)$

endlich vielen Elementen im Körper: $(\mathbb{Z}_p,+,\cdot)$

Polynomring $\mathbb{K}[x]$

Funktion $p: \mathbb{K} \mapsto \mathbb{K}$

Grad $n = \deg(p)$

$$\mathbb{K}[x] = p(x) = \sum_{i=0}^{n} a_i x^i = \boxed{a_n} x^{\boxed{n}} + a_{n-1}x^{n-1} + \ldots + a_1 x^1 + a_0 x^0 \quad \Big] \text{ Polynom über } \mathbb{K}$$

Koeffizient

$a_n \in \mathbb{K}$

Bildet kommutativen Ring mit 1

Wenn $a_n = 1$ „auf 1 normiert“

wenn $p(x) = 0$ $\deg(p) = -\infty$

Beispiele für $\mathbb{K}$

$\mathbb{R}[x], \mathbb{C}[x], \mathbb{Z}_2[x], \mathbb{Z}_3[x] \ldots$

Summe und Produkt eines Polynoms → Polynom

Division zweier Polynome → Rationale Funktion

↳ Man rechnet ~~[illegible] Algorithmus:~~

$$p(x) = s(x)\,q(x) + r(x)$$

→ Restpolynom ~~$\deg(r(x)) < \deg(q(x))$~~

~~$\deg(s(x)) = \deg(p(x)) - \deg(q(x))$~~

$s(x)$ .... Quotientpolynom

$r(x)$ ..... Restpolynom

Normierte Teiler:

Beispiel: $a(x) = (x-5)(x-3)$

Lösung $= \{ (x-5), (x-3), 1, (x^2 - 8x + 15) \}$

Linearfaktor

Wenn x_1 Nullstelle ist, ist $(x - x_1)$ ein Teiler des Polynoms

Rechnen im $\mathbb{Z}_2[x]$

$$p(x) = x^3 + x = 1x^3 + 0x^2 + 1x + 0$$

$$q(x) = x + 1 = 0x^3 + 0x^2 + 1x + 1$$

$$p(x) + q(x) = 1x^3 + 0x^2 + 0x + 1 = x^3 + 1$$

im $\mathbb{Z}_3[x]$ $p(x) = 0x^3 + 1x^2 + 2x + 1$

$$q(x) = 0x^3 + 0x^2 + 1x + 2$$

$p(x) \cdot q(x) =$ [illegible] $2x^3 + x^2 + 2x + 2$

Der Restklassenring $\mathbb{K}[x]_{m(x)}$

(Vergleiche mit: $\mathbb{Z}_n$)

$a(x) \equiv b(x) \bmod m(x)$ .... $a(x)$ und $b(x)$ sind kongruent modulo $m(x)$

..... sie sind inderselben Restklasse

$\hookrightarrow$ Unterschied zu $\mathbb{Z}_m$: es gibt ∞ Restklassen

Alle möglichen Restklassen:

in $\mathbb{Z}_m = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{m-1}\}$

Hier:

deg(Restklasse) < deg(m(x))

Also in $\mathbb{K}[x]_{m(x)} = \{ \underset{\uparrow}{a_{k-1}} x^{k-1}, a_{k-2} x^{k-2} + \ldots + a_1 x^1 + a_0 \} \mid a_i \in \mathbb{K}\}$

alle möglichen/beliebigen Koefizienten

Durch Addition und Multiplikation bildet $\mathbb{K}[x]_{m(x)}$ den Restklassenring

$(\mathbb{K}[x]_{m(x)}, +, \cdot)$

Erfüllt

- Kommutativgesetz
- Assoziativgesetz
- Distributivgesetz
- Rest 0 ist das neutrale Element bez. Addition
- Rest 1 ist das neutrale Element bez. Multiplikation
- Zu jedem Rest gibt es ein additiv (aber nicht multiplikativ) Inverses.

Beispiel:

Additions und Multiplikationstabelle

bei $\mathbb{Z}_{②}[x]_{m(x)}$ mit $m(x) = x^2 + x + 1$

$2 \in \mathbb{P}$ Körper!

Definition: $\mathbb{Z}_2[x]_{x^2+x+1} = \{a_1 x^1 + a_0 x^0 \mid a_i \in \mathbb{Z}_2[x]\} = \{0, 1, x, x+1\}$

Alle haben multipl. Inverse

*	0	1	x	x+1
0	0	0	0	0
1	0	①	x	x+1
x	0	x	x+1	①
x+1	0	x+1	①	x

+	0	1	x	x+1
0	0	1	x	x+1
1	1	0	x+1	x
x	0	x+1	0	1
x+1	x+1	x	1	0

$\hookrightarrow$ Immer mod x^2+x+1 rechnen!

Vorsicht!

$\mathbb{Z}_2[x]_{m(x)}$ muss nicht immer ein Körper sein, auch wenn $2 \in \mathbb{P}$ ist

$ggT(a(x), m(x)) = 1 \rightarrow \exists!$ multipl. Inverses

Endliche Körper

Wie müssen die Eigenschaften von $\mathbb{Z}_p[x]_{m(x)}$ gewählt werden, sodass es ein Körper wird ($\rightarrow$ alle haben a^{-1})?

Irreduzible Polynome

Ein Polynom $p(x)$ mit $\deg(p) > 1$ heißt „irreduzibel über $\mathbb{K}$" wenn es kein $q(x)$ mit $0 < \deg(q) < \deg(p)$ gibt, dass $p(x)$ teilt

sonst $\longmapsto$ Reduzibel

Polynome in Prim-Form zerlegen : „ in irreduzible Faktoren zerlegen"

Faktorisierung:

$$p(x) \in \mathbb{K}[x]$$

$$p(x) = \prod_{i=1}^{n} \underbrace{q_i(x)}$$

irreduzible Polynome mit $q_i = 1$ oder 0

Ein Polynom vom Grad 1 = reduzibel

vom Grad >1 = wenn es keine Nullstellen hat

Beispiel:

Ist $m(x)$ reduzibel oder irreduzibel?

a) $m(x) = x^2+1 \quad \mathbb{K} = \mathbb{R}$

wenn reduzibel: Faktorisierung mit $x^2+1 = (x-a)(x-b)$

x^2+1 hat keine Nullstellen $\longrightarrow$ irreduzibel über $\mathbb{R}$

b) $m(x) = x^2+1 \quad \mathbb{K} = \mathbb{C}$

$x^2+1 = (x-a)(x-b)$

Nullstellen in $\mathbb{C}$! $\pm\sqrt{-1} \rightarrow x^2+1 = (x-i)(x+i) \rightarrow$ reduzibel über $\mathbb{C}$

c) $m(x) = x^2+1 \quad \mathbb{K} = \mathbb{Z}_2$

$1^2+1 = 0 \rightarrow$ Nullstelle $\quad x^2+1 = (x+1)(x+1) \rightarrow$ reduzibel über $\mathbb{Z}_2$

$0^2+1 = 1$

d) $m(x) = x^3+x+1 \quad \mathbb{K} = \mathbb{Z}_2$

$1^3+1+1 = 1 \quad$ keine Nullstellen: irreduzibel!

$0^3+0+1 = 1$

e) $m(x) = x^4 + x^2 + 1 \qquad \mathbb{K} = \mathbb{Z}_2$

$x=1 \quad 1^4 + 1^2 + 1 = 1$
$x=0 \quad 0^4 + 0^2 + 1 = 1$
} keine Nullstelle → keine Teiler vom Grad 1

Teiler Grad 2:

× ~~x^2, x^2+1, [illegible] $+x$ x^2+x~~ → lassen sich ausschließen weil sie reduzibel sind!

✓ $x^2 + x + 1$ einzige Wahl → irreduzibel

↓

$$\cancel{x^4} + \cancel{x^2} + 1 : x^2 + x + 1 = \boxed{x^2 - x + 1} \longrightarrow m(x) \text{ ist irreduzibel}$$

$$-\cancel{x^4} - x^3 - \cancel{x^2}$$

$$-\cancel{x^3} + 1$$

$$\cancel{x^3} + x^2 + x$$

$$x^2 + x + 1$$

$$-x^2 - x - 1$$

$$0R$$

Konkretes Beispiel: ~~Endliche Körper~~

$\mathbb{R}[x]_{x^2+1}$ ist ein Körper, weil x^2+1 irreduzibel ist.
(keine Linearfaktoren weil keine Nullstelle)

Die Menge $\mathbb{R}[x]_{x^2+1} = \{ a_1 x^1 + a_0 x^0 \mid a_i \in \mathbb{R} \}$ Polynome mit grad ≤ 1

→ irreduzibel über $\mathbb{R}$
reduzibel über $\mathbb{C}$

$\mathbb{Z}_p[x]_{m(x)}$ $\deg(m) = k$

$\mathbb{Z}_p[x]_{m(x)}$ ist ein Körper mit p^k Elementen!

bei $\mathbb{Z}_2[x]_{m(x)}$ $\deg(m) = 6 \longrightarrow 2^6$ Elemente!
Möglichkeiten Polynome
zu bilden ...

$\Downarrow$

„Galois-Körper"
engl. Galois-Field, $GF(p^k)$, $\mathbb{F}_{p^k}$

Ring $(R,+,\cdot)$

- $(R,+)$ ist eine kommutative Gruppe mit neutralem Element 0
- $(R,\cdot)$ ist eine Halbgruppe
- Es gelten die Distributivgesetze

$$a(b+c) = ab+ac$$

$$(a+b)c = ac+bc$$

wenn

$(R,\cdot)$ besitzt 1 Element : Ring mit 1 Element
$(R,\cdot)$ kommutativ : kommutativer Ring

Beispiele

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

] komm. Ringe mit 1 Elem.

- Polynome $p(x) \sum_{k=0}^{\infty} a_k x^k \in$ Ring der formalen Potenzreihen mit Koeffizienten $a_k \in R$ mit $+$ und $\cdot$ über R : $R[[x]]$

Nullteiler

wenn $a \cdot b = 0$ $a \neq 0$ $b \neq 0$
dann a & b = Nullteiler

Integritätsring

Ring ohne Nullteiler: man kann kürzen

$a \cdot b = c \cdot b \quad | \cdot b^{-1}$

$a = c$

Beispiele

$(\mathbb{Z},+,\cdot)$
$(\mathbb{Z}_p,+,\cdot)$ integr. Ring (wenn p zusammengesetzt ist nicht)
$R[x]$
$R[[x]]$

Einheiten

Elemente die ein multiplikativ - Inverses besitzen sodass

$$a \cdot a^{-1} \equiv \textcircled{1} \mod m$$

Beispiel $(\mathbb{Z}_{10}, \cdot)$

·	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	①	2	3	4	5	6	7	8	9
2	0	2	4	6	8	⓪	2	4	6	8
3	0	3	6	9	2	5	8	①	4	7
4	0	4	8	2	6	⓪	4	8	2	6
5	0	5	⓪	5	⓪	5	⓪	5	⓪	5
6	0	6	2	8	4	⓪	6	2	8	4
7	0	7	4	①	8	5	2	9	6	3
8	0	8	6	4	2	⓪	8	6	4	2
9	0	9	8	7	6	5	4	3	2	①

Nullteiler von $\mathbb{Z}_{10}$: $ggT(a, m) > 1$
$\{2, 5, 6, 4, 8\}$

Einheiten von $\mathbb{Z}_{10}$: $ggT(a, m) = 1$
$\mathbb{Z}_{10}^{*} = \{1, 3, 7, 9\}$

Wichtig: Klassen tauchen nicht doppelt auf

Einheitengruppe
bildet eigene Gruppe (multiplikativ)

Die Eulersche φ - Funktion
bestimmt $|\mathbb{Z}_{10}^{*}| = \varphi(10)$

Interessant:
Wenn $m \in \mathbb{P}$ $\quad \varphi(m) = m - 1$
(alle Elemente außer 0 sind Einheiten)

Ring $(R,+,\cdot)$

- $(R,+)$ ist eine kommutative Gruppe mit neutralem Element 0
- $(R,\cdot)$ ist eine Halbgruppe
- Es gelten die Distributivgesetze

$$a(b+c) = ab+ac$$

$$(a+b)c = ac+bc$$

wenn

$(R,\cdot)$ besitzt 1 Element: Ring mit 1 Element

$(R,\cdot)$ kommutativ : kommutativer Ring

Beispiele

$\left.\begin{array}{l} -(\mathbb{Z},+,\cdot) \\ -(\mathbb{Z}_m,+,\cdot) \end{array}\right]$ komm. Ringe mit 1 Elem.

- Polynome $p(x) \sum_{k=0}^{\infty} a_k x^k \in$ Ring der formalen Potenzreihen mit Koeffizienten $a_k \in R$ mit + und · über R : $R[[x]]$

Nullteiler

wenn $a \cdot b = 0 \quad a \neq 0 \quad b \neq 0$

dann a & b = Nullteiler

Integritätsring

Ring ohne Nullteiler: man kann kürzen

$a \cdot b = c \cdot b \quad | \cdot b^{-1}$

$a = c$

Beispiele

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

$(\mathbb{Z}_p,+,\cdot)$ integr. Ring (wenn p zusammengesetzt ist nicht)

$R[x]$

$R[[x]]$

Einheiten

Elemente die ein multiplikativ - Inverses besitzen sodass

$$a \cdot a^{-1} \equiv \boxed{1} \mod m$$

Beispiel $(\mathbb{Z}_{10}, \cdot)$

·	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	1	8	5	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	1

Nullteiler von $\mathbb{Z}_{10}$: $ggT(a,m) > 1$

$\{2, 5, 6, 4, 8\}$

Einheiten von $\mathbb{Z}_{10}$: $ggT(a,m) = 1$

$\mathbb{Z}_{10}^{*} = \{1, 3, 7, 9\}$

Wichtig: Klassen tauchen nicht doppelt auf

Die Eulersche φ - Funktion bestimmt $|\mathbb{Z}_{10}^{*}| = \varphi(10)$

Einheitengruppe

bildet eigene Gruppe (multiplikativ)

Interessant:

Wenn $m \in \mathbb{P}$ $\quad \varphi(m) = m - 1$

(alle Elemente außer 0 sind Einheiten)

Körper $(K,+,\cdot)$

- kommutativer Ring mit Einselement
- Alle Elemente sind Einheiten (besitzen multiplikativ Inverse)
- $(K,+)$ und $(K \setminus \{0\},\cdot)$ kommutative Gruppen
- Es gelten Distributivgesetze

Beispiele

$(\mathbb{Q},+,\cdot)$
$(\mathbb{R},+,\cdot)$
$(\mathbb{C},+,\cdot)$
$(\mathbb{Z}_p,+,\circ)$ $p \in \mathbb{P}$

Integritätsring: kommut. Ring mit 1
ohne Nullteiler

+ Endlich

Körper: kommut. Ring mit 1
alle Elemente Einheiten

Jeder Körper ist ein Integritätsring aber
Nur endliche Integritätsringe sind Körper

Beweis

angenommen $a, b \in K \setminus \{0\}$

$a \cdot b = 0 \quad | \cdot a^{-1}$

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

$1 \cdot b = 0$

$b = 0$ ↯ → daher: Körper = Integritätsrings, keine 0

Beispiel

Polynome Grad ≤ 1 über Körper $\mathbb{Z}_2$

$M = \{\bar{0}, \bar{1}, x, \bar{1}+x\} \longrightarrow$ Körper

Satz: $|\text{Körper}| = p^m$ $\quad m \geq 1$
$\quad p \in \mathbb{P}$

$2^2 = 4$ ✓

Polynom $\in K[x]$ Satz 2.77)

Alle Polynome $\in K[x]$

$$a(x) = \underset{\neq 0}{b(x)}\ \underbrace{q(x)} + \underbrace{r(x)}, \quad \text{grad}(r(x)) < \text{grad}(b(x)$$

Durch euklidischen Algorithmus:

$$\text{ggT}(a(x), b(x)) = \boxed{d(x)}$$ ← jeder Teiler von $a(x)$ und $b(x)$ teilt $d(x)$

Durch erweiterten eukl. Algorithm.
kann man die diophantische Gleichung lösen

$$a(x)\boxed{e(x)} + b(x)\boxed{f(x)} = \text{ggT}(a(x), b(x))$$

$n(x) \in K[x]$

Vielfache von $n(x)$: $\underbrace{n(x) \cdot k}$ mit $k \in K[x]$ (vgl. $m\mathbb{Z}$)

additiver Normalteiler von $K[x]$ (vgl. $\mathbb{Z}$)

Bildet additive Faktorgruppe:

$F := K[x] / n(x) \cdot K[x]$

worauf multiplikationen definiert werden können wodurch es von der Faktorgruppe zum Faktorring wird

$$a(x) \cdot b(x) = a(x) b(x)$$

Faktorring

$(K[x] / n(x) K[x], +, \cdot)$

auch Körper wenn Polynom n irreduzibel über K ist:

wenn es nicht als

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

geschrieben werden kann

↓

grad (a)
grad (b) < grad(n)

→ Restklassen $K[x]$ modulo $q(x)$

$$\overline{p(x)} = p(x) + n(x) K[x]$$

Körper: $\mathbb{Z}_p$ → Beispiel:

$n(x) = x^2 + 1$ irreduzibel über $\mathbb{R}$

Nebenklasse $I = x + \boxed{x^2 + 1} \cdot \mathbb{R}[x] \cong \mathbb{C}$

Verband

Algebraische Struktur $(M, \wedge, \vee)$

- kommutative Halbgruppe (assoziativ, kommutativ) bezüglich $\wedge$ und $\vee$
- Verschmelzungsgesetze

$$a = a \wedge (a \vee b)$$
$$a = a \vee (a \wedge b)$$

Beispiele

+ $(P(A), \cap, \cup)$
+ $(\mathbb{N}, \min(a,b), \max(a,b))$ $\longrightarrow$ Elemente die höher / niedriger sind (vgl. $\inf(a,b)$ und $\sup(a|b)$)
+ $(\mathbb{N} \setminus \{0\}, ggT(a,b), kgV(a,b))$
+ $(B, \wedge, \vee)$
  mit $B = \{0,1\}$

$\wedge$	0	1
0	0	0
1	0	1

$\vee$	0	1
0	0	1
1	1	1

auch mit $B^n = \{(x_1, x_2, x_3, \ldots x_n) \mid x_j \in B, (1 \leq j \leq n)\}$

$\inf(a,b)$ und $\sup(a,b)$
in Halbordnungen

$\inf(a,b) = c \Leftrightarrow c \leq a \wedge c \leq b$
wobei wenn
$d \leq a \wedge d \leq b$
dann
$d \leq c$ ist.

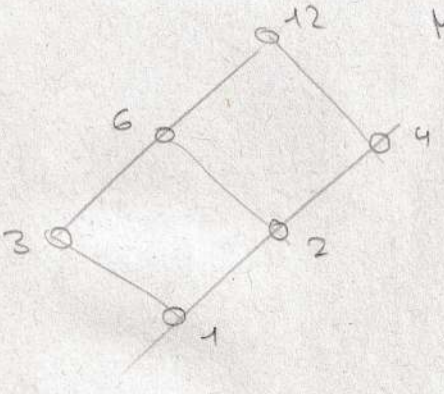
$\sup(a,b) = c$ umgekehrt.

Satz

Sei $(M, \wedge, \vee)$ ein Verband
$a \leq b \Leftrightarrow a = a \wedge b$
definiert Halbordnung

$\exists \inf(a,b)$ und $\sup(a,b)$
$$\inf(a,b) = a \wedge b \qquad \sup(a,b) = a \vee b$$

Hassediagramm



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

$a \wedge b = ggT(a,b)$
$a \vee b = kgV(a,b)$

Satz

Halbordnungen $\neq$ Verband wenn $\nexists$ inf und sup für alle Paare?
mehrere Kanten von einem Knoten

Distributiver Verband

$$\left.\begin{aligned} a \wedge (b \vee c) &= (a \wedge b) \vee (a \wedge c) \\ a \vee (b \wedge c) &= (a \vee b) \wedge (a \vee c) \end{aligned}\right\} \text{(Distributivgesetze)}$$

Bool'sche Algebra

Es gibt ein neutrales Element $1 \in M$ bezüglich $\wedge$

Es gibt ein neutrales Element $0 \in M$ bezüglich $\vee$

Zu jedem $a \in M$ gibt es ein Komplement $a' \in M$

$$a \vee a' = 1$$

$$a \wedge a' = 0$$

De Morgan'sche Regeln

$$(a \wedge b)' = a' \vee b'$$

$$(a \vee b)' = a' \wedge b'$$

Beweis $a \vee 1 = (a \wedge 1) \vee 1 = 1$

$a \wedge 0 = (a \vee 0) \wedge 0 = 0$

„Integritätsbereiche", „Integritätsringe" $(R,+,\circ)$

- mit Einselement
- Nullteilerfrei

Beispiele:

$(\mathbb{Z},+,\cdot)$, $(\mathbb{Z}_{\underset{\text{Primzahl}}{p}},+,\cdot)$, $(\mathbb{Q},+,\circ)$

$(\mathbb{Z}[x],+,\circ)$, $(\mathbb{Q}[x],+,\circ)$

Exkurs:

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Endliche Körper (Fields)

kommutative Ringe $(R,+,\circ)$

- mit Einselement → impliziert $\exists$ Nullelement

betrachte Elemente in R welche ein multiplikatives Inverses besitzen

$a \cdot a' = 1$ (ausgenommen 0)

↳ Elemente mit multiplikativen Inversen = „Einheiten"

$(R^*,\circ)$ ... Einheitengruppe

Körper Definition:

komm. Ring $(K,+,\circ)$ mit Einselement, $1 \neq 0$
wo jedes Element ein multiplikatives Inverses besitzt

- $(K,+)$ ... kommutative Gruppe
- $(K \setminus \{0\},\cdot)$ ... kommutative Gruppe
- Distributivgesetz ... $a(b+c) = ab + ac$

↳ jeder Körper ist automatisch ein Integritätsring!

weil es Nullteilerfrei ist

↓

Körper sind schöne Ringe

sei $a \neq 0$, $a \cdot b = 0 \mid a^{-1}$

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

$b = 0$ $\Rightarrow$ kein Nullteiler im Integritätsring!

Umkehrung ist falsch!

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

Es gibt Integritätsringe die keine Körper sind (unendliche)

aber alle Körper sind Integritätsringe

Satz: jeder endliche Integritätsring ist ein Körper

$(R, +, \cdot)$

R ist endlich, abzählbar

$\to \{r_1, r_2, r_3, \dots, r_n\}$

$a \in R \neq 0$

$a \circ \{r_1, r_2, r_3, \dots, r_n\} = a \cdot R =$

alle Elemente müssen verschieden sein $\leftarrow$ $a \cdot r_1, a \cdot r_2, a \cdot r_3, a \cdot r_4, \dots, a \cdot r_n$

angenommen

$a \cdot r_k = a \cdot r_{i \neq}$ kürzen:

$r_k = r_i$

$\exists_j\ a \cdot \overset{a^{-1}}{r_j} = 1 \Rightarrow$ a ist Einheit

bei nicht Inversen

Körper $(K, +, \cdot)$

kommutativer Ring mit 1-Element $(1 \neq 0)$

wo jedes Element $\neq 0$ ein multipl. Inverses besitzt

(also ohne eine "Einheit" ist)

„informell" wir können mit den 4 Grundrechnungsarten uneingeschränkt

(außer division durch 0 rechnen)

Beispiel: $(\mathbb{Z}_p, +, \cdot)$

$p \in \mathbb{P}$ $\qquad \mathbb{Z}_p = \{\bar{0}, \bar{1}, \dots, \overline{p-1}\}$

$ggT(a, p) = 1$ ⟶ Bedingung dafür, dass alle Elemente $\bar{a}^{-1}$ haben.

so lange $a \neq 0$

Beispiel: $(\mathbb{Z}_3, +, \cdot)$

$a x + b = c \;, \; a \neq 0$

$\bar{2} x + \bar{1} = \bar{2}$

$x = \frac{\bar{2} - \bar{1}}{\bar{2}} = \frac{\bar{1}}{\bar{2}} = \bar{2}^{-1} = \boxed{\bar{2}}$

Es gilt: $q = p^k \Leftrightarrow$ es gibt endliche Körper mit q Elementen

$p \in \mathbb{P}, \; k \in \mathbb{N} \setminus \{0\}$

Lösungsalgorithmus:

wir betrachten Polynome über Körper K $\quad K[x]$

$$K = \mathbb{R}: \quad x^3 + x^2 = (x^2 + 1) \underbrace{(x + 1)}_{q(x)} \underbrace{- x - 1}_{r(x)}$$

Polynom Division

$$\begin{array}{l} -x^3 - x \\ \hline \quad\; x^2 - x \\ \quad -x^2 + 1 \\ \hline \quad\; 0 - y - 1 \end{array}$$

Satz: Polynomdivision „mit Rest"

gegeben: $a(x), b(x) \in K(x) \qquad b(x) \neq 0$

Dann gibt es Polynome $q(x), r(x) \in K[x]$

sodass $a(x) = b(x) \cdot q(x) + r(x)$

wobei $r(x) = 0$ oder $grad(r(x)) < grad(b(x))$

Beispiel

$\mathbb{Z}_2[x]$ ist unser Rahmen

$q(x) := \bar{1} \cdot x^2 + \bar{1} \cdot x + \bar{1}$

$a(x) \in \mathbb{Z}_2[x]$: best. Rest bei Polynomdivision durch $q(x)$

Alle möglichen Reste: $\bar{0}$, $\bar{1}$, x, $x+\bar{1}$

$\swarrow$

Rechnen mit Resten

$\cdot$	$\bar{0}$	$\bar{1}$	x	$x+\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	x	$x+\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$	$x+\bar{1}$	x
x	x	$x+\bar{1}$	$\bar{0}$	$\bar{1}$
$x+\bar{1}$	$x+\bar{1}$	x	$\bar{1}$	$\bar{0}$

$+$	$\bar{0}$	$\bar{1}$	x	$x+\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	x	$x+\bar{1}$
x	$\bar{0}$	x	$x+\bar{1}$	$\bar{1}$
$x+\bar{1}$	$\bar{0}$	$x+\bar{1}$	$\bar{1}$	$\bar{x}$

$x^2+1 =$

$(x^2+x+\bar{1}) \cdot \ldots$

Rest

modulo $q(x)$ rechnen wenn Werte Rahmen sprengen

$(x+\bar{1}) \cdot (x+\bar{1}) =$

$x^2 + \cancel{x} + \cancel{x} + \bar{1} =$

$x^2 + \bar{1}$

$x^2 = (x^2 + x + \bar{1}) \cdot \bar{1} \; \underbrace{\boxed{-x - \bar{1}}}_{}$

eigentlich auch

$x + \bar{1}$

Irreduzibles Polynom

$q(x) = x^2 + x$ geeignet $\longrightarrow$ ungeeignet:

$q(x) = x^2 + x$

$(x+\bar{1})^2 = x^2 + 1$

Polynom $q(x) \in K[x]$

heißt irreduzibel über K falls es keine Polynome

$(a(x), b(x) \in K[x])$ mit $\text{grad}\, a(x) < \text{grad}\, q(x)$

$\text{grad}\, b(x) < \text{grad}\, q(x)$

. lässt sich nicht in kleinere Faktoren zerlegen: ähnlich wie Primzahlen

sodass $a(x) \cdot b(x) = q(x)$

Wie kann man Körper mit $q = p^k$ Elementen konstruieren?

Polynome $\mathbb{Z}p[x]$: rechne modulo $q(x) \in \mathbb{Z}p[x]$,

wobei
- grad $q(x) = k$
- $q(x)$ irreduzibel über $\mathbb{Z}p$

Daher:

→ Elemente & Restklassen mod $q(x)$ sind in Körper

Beispiel

$8 = 2^3$ Elemente

grad $(q(x)) = 3$ $q(x) \in \mathbb{Z}_2[x]$

irreduzibel in $\mathbb{Z}_2$: $q(x) = x^3 + x + 1$

$\boxed{a_2 x^2 + a_1 x + a_0}$ Reste

wobei $a \in \mathbb{Z}_2$ → also $\{0, 1\}$

→ insgesamt 8 mögliche Reste

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

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

Normalklasse:

$N \trianglelefteq \mathbb{Z}$

$\parallel$

$m \cdot \mathbb{Z} = \{ \dots, -m, 0, m, 2m, \dots \}$

$\bar{a} := a + m \cdot \mathbb{Z}$

$\bar{a} + \bar{b} := \overline{a+b}$

$\bar{a} \cdot \bar{b} := \overline{a \cdot b}$

$(a + m\mathbb{Z}) + (b + m\mathbb{Z}) := (a+b) + m \cdot \mathbb{Z}$

$(a + m\mathbb{Z}) \cdot (b + m\mathbb{Z}) := (ab) + m\mathbb{Z}$

$$a \cdot b + \underbrace{b \cdot m\mathbb{Z}}_{\subseteq m\mathbb{Z}} + \underbrace{a \cdot m\mathbb{Z}}_{\subseteq m\mathbb{Z}} + \underbrace{m^2 \cdot \mathbb{Z} \cdot \mathbb{Z}}_{\subseteq m\mathbb{Z}}$$ „Ideal"

Man zeige, dass die von $\bar{3}$ erzeugte Untergruppe U von $\langle \mathbb{Z}_9 , + \rangle$ ist und bestimme die Gruppentafel der Faktorgruppe $\mathbb{Z}_9 / U$. 372)

Def Normalteiler:

Untergruppe $N \trianglelefteq G$ heißt Normaltei~~ge~~ler
wenn $LNK = RNK$ also $a \circ N = N \circ a$ gilt

Def Faktorgruppe:

Die Menge der Nebenklassen bei Normalteilern bildet die Faktorgruppe
G / N

$\{ a \circ N \mid a \in G \}$

$\langle \mathbb{Z}_9 , + \rangle$ kommutative Gruppe

$\mathbb{Z}_9 = \bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}$

Untergruppe durch 3 erzeugt:

$U = \langle 3 \rangle = \bar{0}, \bar{3}, \bar{6}$

$\text{ord}_G(3) = 3$ weil $3+3+3 = 9 \equiv 0 \mod 9$

U ist Normalteiler, da + kommutativ ist

3 Neben-klassen von 3

~~$U = 0 + U = U + 0$~~ $0 + U = U = 3 + U = 6 + U$

~~$U = 3 + U = U + 3$~~ $1 + U = \{\bar{1}, \bar{4}, \bar{7}\} = 4 + U = 7 + U$

~~$U = 6 + U = U + 6$~~ $2 + U = \{\bar{2}, \bar{5}, \bar{8}\} = 5 + U = 8 + U$

$\mathbb{Z}_9 / U = \{ U , 1+U , 2+U \}$

+	U	1+U	2+U
U	U	1+U	2+U
1+U	1+U	2+U	U
2+U	2+U	U	1+U

390)

Sei $(G, *)$ eine Gruppe.

Hätte $(G \times G, \circ)$ mit $\circ: (a,b) \circ (c,d) = (a * c, b * d)$ dieselben Eigenschaften wie eine Gruppe?

Gruppenaxiome die für $(G, *)$ gültig sind:

0) Abgeschlossenheit : $\forall a,b \in G \quad (a * b) \in G$

1) Assoziativität : $\forall a,b,c \in G \quad (a * b) * c = a * (b * c)$

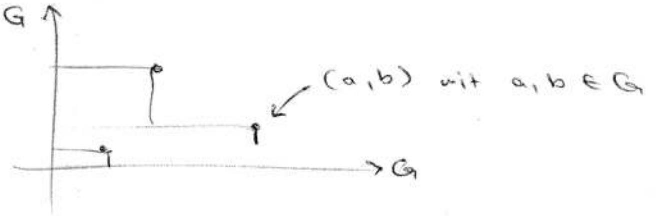
2) Neutrales Element : $\forall a \in G \quad e * a = a * e = a$

3) Inverses Element : $\forall a \in G \quad \exists a^{-1} \in G: a * a^{-1} = a^{-1} * a = e$

Vergleichen mit Vektoren:

$$\begin{pmatrix} a \\ b \end{pmatrix} \circ \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} a * b \\ c * d \end{pmatrix}$$

$G \times G$ bildet Tupeln



---

0) Abgeschlossenheit:

wenn $\forall a, b \in G$ gilt $\overset{\text{denn}}{\rightsquigarrow} (\underbrace{a * c}_{\in G}, \underbrace{b * d}_{\in G}) \in G \times G$

1) Assoziativität

$$\left(\begin{pmatrix} a \\ b \end{pmatrix} \circ \begin{pmatrix} c \\ d \end{pmatrix} \right) \circ \begin{pmatrix} e \\ f \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix} \circ \left(\begin{pmatrix} c \\ d \end{pmatrix} \circ \begin{pmatrix} e \\ f \end{pmatrix} \right)$$

$$\begin{pmatrix} a * c \\ b * d \end{pmatrix} \circ \begin{pmatrix} e \\ f \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix} \circ \begin{pmatrix} c * e \\ d * f \end{pmatrix}$$

$$\begin{pmatrix} a * c * e \\ b * d * f \end{pmatrix} = \begin{pmatrix} a * c * e \\ b * d * f \end{pmatrix}$$

2) Neutrales Element

je G hat ~~[illegible]~~ 1 neutrales Element, also $(e,e) \in G \times G$

3) Inverses Element

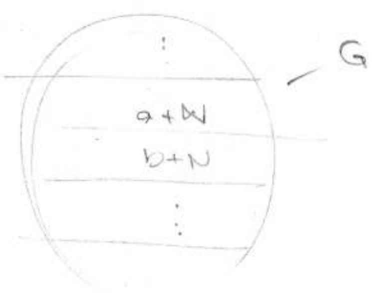
$\forall a, b \in G \; \exists a^{-1}, b^{-1} \in G$

$\forall (a,b) \in (G \times G) \; \exists (a^{-1}, b^{-1}) \in G \times G \rightarrow$ sodass:

$(a,b) \circ (a^{-1}, b^{-1}) = (a^{-1}, b^{-1}) \circ (a,b) = (e,e)$

Gruppe $(G, +)$

Normalteiler $(N, +)$ $N \trianglelefteq G$



Wir können mit Nebenklassen addieren

$$(a+N)+(b+N) = (a+b)+N$$

für Reste

$$\bar{a} + \bar{b} = \overline{a+b}$$

Ideale: Besondere Normalteiler

$$\left.\begin{array}{l} -(I,+) \trianglelefteq (R,+) \\ a \cdot I \subseteq I \end{array}\right\} \forall\ a \in R$$

Wir können mit Nebenklassen auch multiplizieren (neben der Addition) wenn wir Ideale haben.

$$(a+I) \circ (b+I) := a \cdot b + I$$

da ja $ab + \underbrace{\underset{\subseteq I}{aI} + \underset{\subseteq I}{Ib} + \underset{\subseteq I}{II}}_{\subseteq I}$

$$\overline{ab} = \bar{a} \cdot \bar{b}$$

$(R/I, +, \cdot)$ ist selbst ein Ring

$\{a + I \mid a \in R\}$ Faktorring / Quotientenring

Beispiel

$(\mathbb{Z}, +, \cdot)$ Modul m; $I = m \cdot \mathbb{Z} = \{-m, 0, m, 2m, \dots\}$

$m = 4$, $3 \cdot I = \{\dots, -3 \cdot 4, 0, 3 \cdot 4, 6 \cdot 4, \dots\} \subseteq I$

Ist Ideal

$I = q(x) \cdot K[x] = \{q(x) \cdot p(x) \mid p(x) \in K[x]\} = \{0, q(x), x q(x), x+1 \cdot q(x)\}$

Alle Polynome, welche durch $q(x)$ (ohne Rest) teilbar sind

Wir können auch mit Nebenklassen + & ·

$\left(K[x] / q(x), K[x], +, \cdot \right)$ Faktorring

$\mathbb{Z}_p[x]$
$q(x) \in \mathbb{Z}_p[x]$

$\overline{g(x)}$ $\underbrace{a(x) + g(x)\,K[x]}$

alle Polynome, welche Rest $a(x)$ bestimmen bei Division durch $g(x)$

WIKIPEDIA

Verband (Mathematik)

Ein **Verband** ist in der Mathematik eine Struktur, die sowohl als Ordnungsstruktur als auch als algebraische Struktur vollständig beschrieben werden kann. Als Ordnungsstruktur ist ein Verband dadurch gekennzeichnet, dass es zu je zwei Elementen a, b ein Supremum $a \vee b$ gibt, d. h. ein eindeutig bestimmtes kleinstes Element, das größer oder gleich a und b ist, und umgekehrt ein Infimum $a \wedge b$, ein größtes Element, das kleiner oder gleich a und b ist. Als algebraische Struktur ist ein Verband dadurch gekennzeichnet, dass es zwei assoziative und kommutative Operationen gibt, für die die *Absorptionsgesetze* kennzeichnend sind: Für beliebige Elemente gilt

$$u \vee (u \wedge v) = u \quad \text{und} \quad u \wedge (u \vee v) = u.$$

Für jede in der Verbandstheorie vorkommende algebraische Aussage gibt es eine direkte Übersetzung in eine Ordnungsaussage und umgekehrt. Diese Übersetzung ist in den meisten Fällen auch anschaulich nachzuvollziehen. Die Möglichkeit, Ergebnisse doppelt zu interpretieren und dadurch besser zu verstehen, macht die Untersuchung und die Verwendung von Aussagen aus der Verbandstheorie so interessant. Der Begriff Verband wurde im hier beschriebenen Sinne von Fritz Klein-Barmen geprägt.[1]

Obwohl diese doppelte Charakterisierung auf den ersten Blick sehr speziell aussieht, treten Verbände häufig auf:

- die z. B. in der Mengenlehre, der Logik und als Schaltalgebren auftretenden Booleschen Algebren sind Verbände.
- totale Ordnungen, die z. B. in den verschiedenen Zahlbereichen wie $\mathbb{N}$ (natürliche Zahlen), $\mathbb{Z}$ (ganze Zahlen), $\mathbb{Q}$ (rationale Zahlen) oder $\mathbb{R}$ (reelle Zahlen) auftreten, sind Verbände.
- für jede beliebige natürliche Zahl ist die Menge der Teiler (durch die Teilbarkeit geordnet) ein Verband.
- die Unterstrukturen einer beliebigen algebraischen oder sonstigen Struktur bilden einen Verband mit der Teilmengenrelation als Ordnung.

der Literatur sind auch die Symbole $\sqcup$ und $\sqcap$ anstelle von $\vee$ und $\wedge$ verbreitet. Diese Notation wird hier aufgrund von technischen Einschränkungen allerdings nicht verwendet.

In einer früher üblichen Terminologie wurde ein Verband (nach Richard Dedekind) auch als *Dualgruppe* bezeichnet.

Inhaltsverzeichnis

Präzisierung

Verbände als algebraische Strukturen

Ein Verband $(V, \vee, \wedge)$ ist eine Menge V mit zwei inneren binären Verknüpfungen $\vee$ (Vereinigung, engl. *join*) und $\wedge$ (Durchschnitt, engl. *meet*), die folgenden Bedingungen für alle u, v, w aus V genügen:

Assoziativgesetze:

- $u \vee (v \vee w) = (u \vee v) \vee w,$
- $u \wedge (v \wedge w) = (u \wedge v) \wedge w.$

Kommutativgesetze:

- $u \vee v = v \vee u,$
- $u \wedge v = v \wedge u.$

Absorptionsgesetze:

- $u \vee (u \wedge v) = u,$
- $u \wedge (u \vee v) = u.$

Aus diesen Bedingungen folgt die Idempotenz beider Verknüpfungen:

- $u \vee u = u,$
- $u \wedge u = u.$

V ist also bezüglich jeder einzelnen Verknüpfung ein **Halbverband**, d. h. eine kommutative Halbgruppe, in der jedes Element idempotent ist. Die Verknüpfungen treten bei den Absorptionsgesetzen in Wechselwirkung.

Verbände als Ordnungsstrukturen

Man kann nach einer Idee von Leibniz auf V eine Halbordnung definieren durch:

- $v \leq w \quad \iff \quad v \wedge w = v.$

Mit dem Absorptionsgesetz erkennt man die Gültigkeit der Äquivalenzen

- $v \leq w \quad \iff \quad v \wedge w = v \quad \iff \quad v \vee w = w.$

Bezüglich dieser Halbordnung hat jede zweielementige Teilmenge $\{v, w\}$ ein Supremum (obere Grenze) $s = v \vee w$ und ein Infimum (untere Grenze) $i = v \wedge w$. Dabei ist ein Element s ein Supremum von $\{v, w\}$, wenn gilt:

- $v \leq s$ und $w \leq s$ (d. h. s ist obere Schranke).
- Aus $v \leq t$ und $w \leq t$ folgt $s \leq t$ (d. h. s ist die kleinste obere Schranke).

Analoges gilt für das Infimum i. Man kann per Induktion zeigen, dass jede nichtleere endliche Teilmenge ein Supremum und ein Infimum hat. Man schreibt allgemein das Supremum einer Menge M als $\bigvee M$, und das Infimum von M als $\bigwedge M$, falls diese existieren.

Umgekehrt kann man für eine halbgeordnete Menge, bei der jede zweielementige Teilmenge ein Infimum und ein Supremum hat, definieren:

- $v \wedge w = \inf\{v, w\}$ und $v \vee w = \sup\{v, w\}.$

Die beiden Verknüpfungen erfüllen dann die Verbandsaxiome, wie man leicht nachrechnet.

Hasse-Diagramme für einige Beispiele

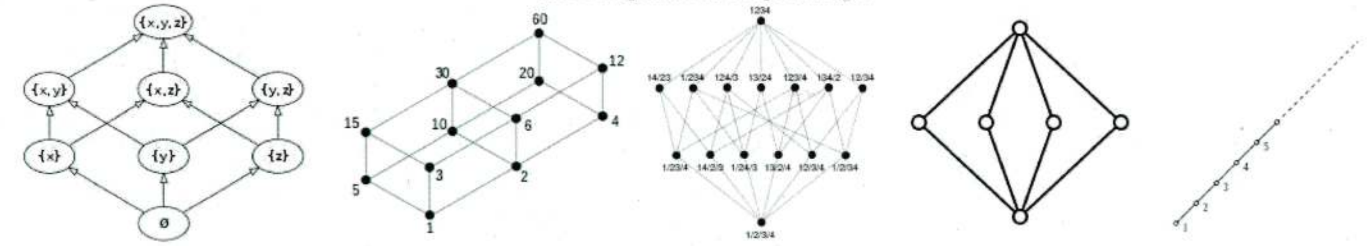
→ Hauptartikel: Hasse-Diagramm

Eine endliche halbgeordnete Menge $(M, \leq)$ kann man durch einen gerichteten Graphen darstellen, den man *Hasse-Diagramm* nennt.

Wenn man den Graph so anordnet, dass alle Kanten von unten nach oben gerichtet sind, dann kann man die Ordnung leicht sehen:

> $a < b$ ist dann gleichwertig mit: a ist durch einen (nach oben führenden) Kantenzug mit b verbunden.

Hasse-Diagramme für einige Verbände



Verband der Teilmengen von {x,y,z} (eine Boolesche Algebra)

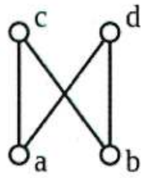
Verband der Teiler von 60

Partitionen der Menge {1,2,3,4}, durch gröber = geordnet

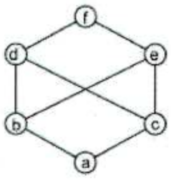
Verband, der nicht distributiv, aber orthokomplementierbar ist

Die Menge der natürlichen Zahlen: Total geordnete Mengen sind Verbände

Diagramme, die keine Verbände darstellen



kein Verband, da c⊔d nicht existiert



kein Verband, da b⊔c nicht existiert (d und e sind zwar beide minimal größer, aber keins von beiden ist kleinstes der größeren Elemente)

Spezielle Elemente in Verbänden

Neutrale Elemente

Falls die Verknüpfung $\vee$ ein neutrales Element 0 hat,

$$0 \vee a = a,$$

dann ist es eindeutig bestimmt und man nennt es das *Nullelement* des Verbandes. Bzgl. $\wedge$ ist 0 absorbierend und bzgl. der Ordnung das kleinste Element:

$$0 \wedge a = 0 \text{ und } 0 = \bigwedge V.$$

Man nennt den Verband dann *nach unten beschränkt*.

Falls die Verknüpfung $\wedge$ ein neutrales Element 1 hat,

$$1 \wedge a = a,$$

dann ist es eindeutig bestimmt und man nennt es das *Einselement* des Verbandes. Bzgl. $\vee$ ist 1 absorbierend und bzgl. der Ordnung das größte Element:

$$1 \vee a = 1 \text{ und } 1 = \bigvee V.$$

Man nennt den Verband dann *nach oben beschränkt*.

Ein Verband heißt *beschränkt*, wenn er nach unten und nach oben beschränkt ist, also für beide Verknüpfungen ein neutrales Element hat.

Komplementäre Elemente

→ *Hauptartikel: Komplement (Verbandstheorie)*

Für ein gegebenes Element a eines beschränkten Verbandes nennt man ein Element b mit der Eigenschaft

- $a \wedge b = 0$ und $a \vee b = 1$

ein *Komplement* von a.

Ein beschränkter Verband, in dem jedes Element (mindestens) ein Komplement hat, heißt *komplementärer Verband.*

Im Allgemeinen kann es zu einem Element mehrere komplementäre Elemente geben.

Es gilt aber: In einem distributiven beschränkten Verband ist das Komplement eines Elements a im Falle seiner Existenz eindeutig bestimmt. Man schreibt es oft als a^c (vor allem bei Teilmengenverbänden), $\neg a$ (vor allem bei Anwendungen in der Logik) oder $\bar{a}$.

In jedem beschränkten Verband gilt

- $\neg 0 = 1, \neg 1 = 0.$

In einem distributiven beschränkten Verband gilt: Falls a ein Komplement $\neg a$ hat, dann hat auch $\neg a$ ein Komplement, nämlich:

- $\neg(\neg a) = a.$

Spezielle Verbände

Modulare Verbände

→ *Hauptartikel: Modularer Verband und Semimodularer Verband*

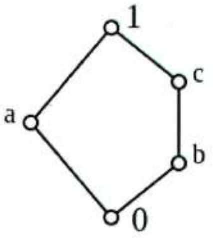
Ein Verband V heißt *modular*, falls gilt:

- $u \leq w \Longrightarrow u \vee (v \wedge w) = (u \vee v) \wedge w$ für alle $u, v, w \in V$.

Für einen Verband V sind wiederum jeweils äquivalent:

- V ist modular.
- $u \geq w \Longrightarrow u \wedge (v \vee w) = (u \wedge v) \vee w$ für alle $u, v, w \in V$.
- $u \vee (v \wedge (u \vee w)) = (u \vee v) \wedge (u \vee w)$ für alle $u, v, w \in V$.
- $u \wedge (v \vee (u \wedge w)) = (u \wedge v) \vee (u \wedge w)$ für alle $u, v, w \in V$.

Ein nicht modularer Verband enthält immer den Verband N_5 als Unterverband.[2]



N_5, der minimale nicht-modulare Verband

Distributive Verbände

→ *Hauptartikel: Distributiver Verband*

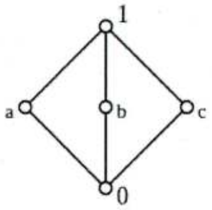
Im Folgenden meinen wir mit dem Verband V stets den Verband $(V, \vee, \wedge)$.

Ein Verband V heißt *distributiv*, wenn die Verknüpfungen in doppelter Hinsicht distributiv sind:

- $u \vee (v \wedge w) = (u \vee v) \wedge (u \vee w)$ für alle $u, v, w \in V$ und
- $u \wedge (v \vee w) = (u \wedge v) \vee (u \wedge w)$ für alle $u, v, w \in V$.

Da diese beiden Aussagen zueinander äquivalent sind, genügt es, die Gültigkeit eines dieser beiden Distributivgesetze zu verlangen.

Jeder distributive Verband ist modular, aber nicht umgekehrt. Ein modularer Verband, der nicht distributiv ist, enthält immer den Verband M_3, den Verband der Untergruppen der Kleinschen Vierergruppe als Unterverband.[3]



M_3, der minimale modulare, nicht-distributive Verband

Dies ergibt den Test: hat ein Verband weder einen Unterverband der Form N_5 noch einen der Form M_3, dann ist er distributiv.

Distributive Verbände sind auch anders zu charakterisieren, denn Birkhoff (1933) und Stone (1936) haben gezeigt:

> Ein Verband ist genau dann distributiv, wenn er isomorph zu einem Mengenverband ist.[4]

Boolesche Algebren

→ *Hauptartikel: Boolesche Algebra und Heyting-Algebra*

Ein distributiver komplementärer Verband heißt *Boolesche Algebra* oder *Boolescher Verband*;

Eine weitere Verallgemeinerung, bei der statt Komplementen nur relative Pseudokomplemente gefordert werden, heißt *Heyting-Algebra*.

Vollständige Verbände

Ein Verband V heißt *vollständig*, wenn jede (auch die leere ebenso wie gegebenenfalls unendliche) Teilmenge ein Supremum und ein Infimum hat.

Es genügt, für jede Teilmenge M die Existenz des Supremums zu verlangen, denn es ist

- $\bigwedge M = \bigvee \{x \in V : (\forall y \in M : x \leq y)\}$.

Jeder vollständige Verband V ist beschränkt mit

- $0 = \bigwedge V = \bigvee \emptyset$ und $1 = \bigvee V = \bigwedge \emptyset$.

Jeder endliche, nichtleere Verband V ist vollständig, also auch beschränkt.

Längenendliche Verbände

Wenn jede bezüglich der Ordnung totalgeordnete Teilmenge (Kette) endlich ist, nennt man den Verband *längenendlich*.[5] Für viele Beweise innerhalb der Verbandstheorie muss ein Verband nicht endlich sein, sondern es reicht, wenn er längenendlich ist.

Kompakte Elemente und algebraische Verbände

Man nennt ein Element a eines vollständigen Verbandes V *kompakt* (nach der verwandten Eigenschaft *kompakter Räume* in der Topologie), wenn jede Teilmenge M von V mit

- $a \leq \bigvee M$

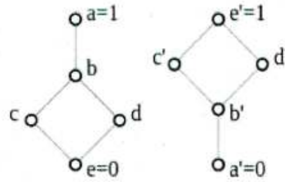
eine endliche Teilmenge E enthält, für die gilt:

- $a \leq \bigvee E$

Ein Verband V heißt *algebraisch*, wenn er vollständig ist und wenn jedes Element von V das Supremum von kompakten Elementen ist.

Dualität in Verbänden

→ *Hauptartikel: Dualität (Verbandstheorie)*



Die beiden Verbände sind dual zueinander (aber offensichtlich nicht isomorph).

Vertauscht man in einem Verband V die beiden Verknüpfungen $\wedge$ und $\vee$, erhält man eine neue Struktur W. Man nennt W die *duale* Struktur.

Ersetzt man in einer beliebigen Formel φ der Sprache der Verbandstheorie und setzt überall die beiden Zeichen $\wedge$ und $\vee$ wechselseitig füreinander ein und ersetzt außerdem überall 0 durch 1 und umgekehrt, dann nennt man die entstandene Formel $\widehat{\varphi}$ die *duale Formel* von φ.

Offensichtlich gelten in dem zu V dualen Verband W die dualen zu den in V gültigen Formeln. Da in der Definition eines Verbands zu jeder Formel auch die duale Formel vorkommt, folgt, dass W ebenfalls ein Verband ist, der als der zu V *duale* Verband bezeichnet wird.

Aus dieser Beobachtung folgt:

- Gilt eine Formel in *allen* Verbänden, dann gilt auch ihre duale Formel in allen Verbänden.

Das Modularitätsgesetz ist selbstdual und die beiden Distributiv-Gesetze sind zueinander dual und die beiden Komplementärgesetze sind zueinander dual. Daher gilt entsprechend:

- Gilt eine Formel in *allen* modularen oder in allen distributiven Verbänden oder in allen Booleschen Algebren, dann gilt auch die duale Formel in den entsprechenden Verbänden.

Unterstrukturen

Unterverbände

Ein **Unterverband** von V ist eine Teilmenge U, die *mit den eingeschränkten Verknüpfungen von* V ein Verband ist, d. h. es liegen

- $a \vee b$ und $a \wedge b$ in U für alle a, b aus U.

Teilverbände

Ein **Teilverband** von V ist eine Teilmenge U, die ein Verband ist, d. h. U ist eine halbgeordnete Menge mit Supremum und Infimum für endliche Teilmengen.

Natürlich ist jeder Unterverband ein Teilverband, aber nicht umgekehrt.

Hier ist eine der wenigen Stellen, wo man den Unterschied in der Betrachtungsweise merkt: Für Verbände als *Ordnungsstrukturen* sind alle Teilverbände Unterstrukturen, für Verbände als *algebraische Strukturen* sind nur die Unterverbände Unterstrukturen.

Man geht weder bei Teilverbänden noch bei Unterverbänden davon aus, dass die *neutralen Elemente* in der Unterstruktur erhalten bleiben. Sonst muss man ausdrücklich von einem Verband mit 0 und 1 reden.

Ideale und Filter

→ *Hauptartikel: Ideal (Mathematik), Primideal und Maximales Ideal*
→ *Hauptartikel: Filter (Mathematik) und Ultrafilter*

Ein **Ideal** I ist ein Unterverband eines Verbandes V, der zusätzlich folgende Bedingung erfüllt: sind $a \in I$ und $x \in V$, dann ist $a \wedge x \in I$. (Die Definition entspricht also formal der Definition, die man in einem Ring erwartet).

Bezüglich der Halbordnung auf V gilt aber $a \wedge x \leq a$. Daher kann man die Definition auch so interpretieren:

> Ein Ideal ist ein Unterverband, der zusammen mit einem Element a auch alle Elemente von V enthält, die kleiner als a sind.

Filter werden dual zu Idealen definiert:

> Ein Filter ist ein Unterverband, der zusammen mit einem Element a auch alle Elemente von V enthält, die größer als a sind.

Homomorphismen

Sind $(V, \vee, \wedge)$ und $(W, \vee, \wedge)$ zwei Verbände und $f \colon V \to W$ eine Funktion, sodass für alle a, b aus V gilt

- $f(a \vee b) = f(a) \vee f(b)$,
- $f(a \wedge b) = f(a) \wedge f(b)$,

dann heißt f *Verbandshomomorphismus*. Ist f zusätzlich bijektiv, dann heißt f *Verbandsisomorphismus* und die Verbände V und W sind *isomorph*.

Falls $(V, \vee, \wedge)$ und $(W, \vee, \wedge)$ vollständig sind und $f \colon V \to W$ sogar

- $f\left(\bigvee T\right) = \bigvee\{f(a) \mid a \in T\}$,
- $f\left(\bigwedge T\right) = \bigwedge\{f(a) \mid a \in T\}$

für alle $T \subseteq V$ erfüllt, nennt man f einen *vollständigen Verbandshomomorphismus*. Jeder vollständige Verbandshomomorphismus ist offensichtlich auch ein Verbandshomomorphismus.

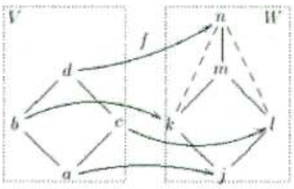
Die Klasse aller Verbände bildet mit diesen Homomorphismen jeweils eine Kategorie.

Ein Verbandshomomorphismus ist gleichzeitig ein Ordnungshomomorphismus, d. h. eine isotone Abbildung:

- aus $a \leq b$ folgt $f(a) \leq f(b)$.

Jedoch ist nicht jede isotone Abbildung zwischen Verbänden ein Verbandshomomorphismus.

In beschränkten Verbänden gilt: Die Menge der Elemente von V, die durch einen Verbandshomomorphismus auf das Nullelement des Bildes abgebildet werden, bilden ein Ideal von V und dual, die Menge der Elemente, die auf das Einselement abgebildet werden, bilden einen Filter.



Die Funktion f ist monoton aber kein Homomorphismus; zum Beispiel ist die hier dargestellte monotone Abbildung f zwischen den Verbänden V und W kein Homomorphismus, da $f(b \vee c) = n$, aber $f(b) \vee f(c) = m$. Außerdem ist aus demselben Grund das Bild $f(V) = \{j, k, l, n\}$ zwar ein Verband (mit $k \vee l = n$), aber kein Unterverband von W.

Weitere Beispiele für Verbände

Total geordnete Mengen

Jede total geordnete Menge M ist ein distributiver Verband mit den Verknüpfungen Maximum und Minimum. Insbesondere gilt für alle a, b, c aus M:

- $\max(a, \min(b, c)) = \min(\max(a, b), \max(a, c))$,
- $\min(a, \max(b, c)) = \max(\min(a, b), \min(a, c))$.

Nur im Fall einer ein- oder zweielementigen Menge M ist der Verband komplementär.

Beispiele für die übrigen Eigenschaften:

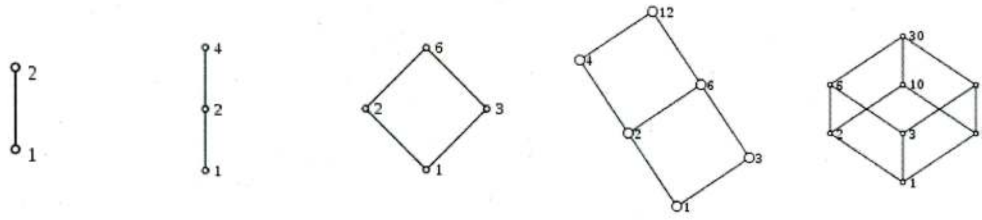
- Das abgeschlossene reelle Intervall $[0, 1]$ und die erweiterte reelle Gerade ($\mathbb{R}$ mit ∞ und $-\infty$) sind jeweils vollständige distributive Verbände (und damit beschränkt).
- Das offene reelle Intervall $(0, 1)$, die Mengen $\mathbb{R}$, $\mathbb{Q}$ und $\mathbb{Z}$ sind jeweils unvollständige unbeschränkte distributive Verbände.
- Das rationale Intervall $[0, 1] \cap \mathbb{Q}$ ist ein unvollständiger beschränkter distributiver Verband.
- Die Menge $\mathbb{N}_0$ ist ein unvollständiger distributiver Verband mit Nullelement 0.

Teilerverbände

Betrachtet man für eine natürliche Zahl n die Menge T aller Teiler von n, dann ist $(T, \operatorname{ggT}, \operatorname{kgV})$ ein vollständiger distributiver Verband mit Einselement n (neutralem Element für ggT) und Nullelement 1 (neutralem Element für kgV). Er heißt Teilerverband von n. Die Absorptionsgesetze und Distributivgesetze für ggT und kgV folgen dabei z. B. mit der Primfaktorzerlegung aus den Eigenschaften von max und min, man kann sie aber auch durch Teilbarkeitsbetrachtungen herleiten. Der Verband ist genau dann komplementär (und damit boolesch), wenn n quadratfrei ist, d. h. wenn n keine Quadratzahl $\neq 1$ als Teiler hat. Die Halbordnung auf T ist die Teiler-Relation:

- $a \leq b$ genau dann, wenn $a|b$ (genau dann, wenn $\operatorname{ggT}(a, b) = a$).

Beispiele für Teilerverbände



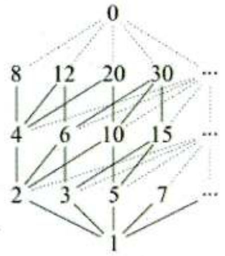
T_2 ist Boolesche Algebra (und lineare Ordnung)

T_4 ist lineare Ordnung

T_6 ist eine Boolesche Algebra

T_{12} ist nicht komplementär

T_{30} ist eine Boolesche Algebra



$(\mathbb{N}_0, \operatorname{kgV}, \operatorname{ggT})$ ist beschränkt und distributiv, aber nicht komplementär. Jeder Teilerverband ist als Unterverband enthalten

Teilmengenverbände

Für eine Menge M bildet die Potenzmenge $\mathcal{P}(M)$ mit den Verknüpfungen Vereinigung $\cup$ und Durchschnitt $\cap$ einen algebraischen booleschen Verband mit Nullelement $\emptyset$ (neutrales Element bezüglich $\cup$) und Einselement M (neutrales Element bezüglich $\cap$) sowie Komplement $A^c = M \setminus A$ für alle $A \in \mathcal{P}(M)$. Er heißt Potenzmengen- oder Teilmengenverband von M. Die Halbordnung auf $(\mathcal{P}(M), \cup, \cap)$ ist die Mengeninklusion:

- $A \leq B$, falls $A \subseteq B$ (oder äquivalent dazu $A \cap B = A$)

(Trägermengen von) Unterverbände(n) von $(\mathcal{P}(M), \cup, \cap)$ heißen Mengenverbände (zwischen den Verbänden und ihren Trägermengen wird oft nicht unterschieden). Diese Verbände sind immer distributiv, müssen jedoch weder vollständig sein, noch neutrale Elemente oder Komplemente haben. (Ein Beispiel dafür ist der Verband der rechts-unendlichen reellen Intervalle $[a, \infty)$ mit a aus $\mathbb{R}$, der isomorph zum Verband der reellen Zahlen ist.)

Unterstrukturenverbände von algebraischen Strukturen, Untergruppenverbände

Für eine Gruppe $(G, *)$ bildet die Menge A aller Untergruppen von G einen algebraischen (im Allgemeinen nicht modularen und damit auch nicht distributiven) Verband mit den Verknüpfungen *Erzeugnis der Vereinigung* und *Durchschnitt*. Er heißt Untergruppenverband von G.

Beispielsweise ist der Untergruppenverband der kleinschen Vierergruppe, der gerade dem Verband M_3 entspricht, nicht-distributiv, aber modular.

Ebenso bilden

- die normalen Untergruppen einer Gruppe,
- die Untergruppen einer abelschen Gruppe,
- die Unterringe eines Ringes,
- die Unterkörper eines Körpers,
- die Untermoduln eines Moduls,
- die Ideale eines Ringes

mit analogen Verknüpfungen einen modularen algebraischen Verband. Die Untergruppen einer beliebigen Gruppe und die Unterverbände eines beliebigen Verbands ergeben zwar immer einen algebraischen Verband, dieser muss aber nicht modular sein.

Ganz allgemein bilden die Unterstrukturen einer algebraischen Struktur stets einen algebraischen Verband (wobei auch die leere Menge als Unterstruktur betrachtet wird, falls der mengentheoretische Durchschnitt – also das Infimum bezüglich der Mengeninklusion – von der Menge aller Unterstrukturen leer ist).

Insbesondere ist ein Verband genau dann algebraisch, wenn er isomorph ist zum Verband der Unterstrukturen einer algebraischen Struktur (daher auch der Name algebraischer Verband).

Schränkt man die Menge der Untergruppen auf Obergruppen einer festen Untergruppe U ein, so bilden alle diese Zwischengruppen $\{V : U \leq V \leq G\}$ auch einen beschränkten Verband. Analog dazu gibt es Verbände von Zwischenringen, Zwischenkörpern, Zwischenmoduln, Zwischenidealen.

Besonderes Interesse hat man am Untergruppenverband der Galoisgruppe einer galoisschen Körpererweiterung L/K, denn er ist isomorph zum dualen Zwischenkörperverband von L/K.

Literatur

- Rudolf Berghammer: *Ordnungen, Verbände und Relationen mit Anwendungen*. 2. Auflage. Springer+Vieweg, Wiesbaden 2012, ISBN 978-3-658-00618-1.
- Garrett Birkhoff: *Lattice Theory*. 3. Auflage. AMS, Providence RI 1973, ISBN 0-8218-1025-1.
- Hilda Draškovičová: *Ordered Sets and Lattices*. AMS, 1992, ISBN 0-8218-3121-6.
- Hans Hermes: *Einführung in die Verbandstheorie*. 2. Auflage. Springer-Verlag, Berlin/Heidelberg 1967.
- Heinz Liermann: *Verbandsstrukturen im Mathematikunterricht*. Diesterweg Salle, Frankfurt a. M. 1971, ISBN 3-425-05317-5.
- Gábor Szász: *Einführung in die Verbandstheorie*. Akademiai Kiado, Budapest 1962.

Weblinks

Commons: Verband (https://commons.wikimedia.org/wiki/Category:Lattice_theory?uselang=de) – Sammlung von Bildern, Videos und Audiodateien

Einzelnachweise und Anmerkungen

1. Leo Corry: *Modern Algebra and the Rise of Mathematical Structures*, Springer, 2004, ISBN 3-7643-7002-5, S. 267
2. H.Gericke, *Theorie der Verbände*. 2. Auflage. Mannheim 1967, S. 76 (Figur dazu auf S. 70)
3. H.Gericke, *Theorie der Verbände*. 2. Auflage. Mannheim 1967, S. 111
4. G.Grätzer, *Lattice Theory*, 1971, S. 75
5. Helmuth Gericke: *Theorie der Verbände*. Bibliographisches Institut, Mannheim 1963, § 6.2

Abgerufen von „https://de.wikipedia.org/w/index.php?title=Verband_(Mathematik)&oldid=183120430“

Diese Seite wurde zuletzt am 27. November 2018 um 11:26 Uhr bearbeitet.

$(A, \wedge, \vee)$

Definition: Verbände

Algebraische Struktur mit 2 binären Operationen

- $(A, \wedge)$ kommutative Halbgruppe
- $(A, \vee)$ kommutative Halbgruppe
- Es gilt <u>Verschmelzungsgesetz</u> / Absorptionsgesetz:

$$a = a \wedge (a \vee b) \qquad \forall\, a, b \in A$$
$$a = a \vee (a \wedge b)$$

Beispiel

Verband $(P(M), \cap, \cup)$

Boolsche Menge:

$B = \{0, 1\} \qquad (B, \wedge, \vee)$

$B = \{w, f\} \qquad (B^n, \wedge, \vee)$

$\qquad\qquad\qquad\quad \| $

$\qquad\qquad\quad \{x_1, x_2, \dots, x_n\}$

Komponentenweise

Auch beweisbar:

$$(T_n, \overset{\wedge}{\widetilde{ggT}}, \overset{\vee}{\widetilde{kgV}})$$

$\downarrow$

$n \in \mathbb{N} \setminus \{0\}$

$\{m | n \mid 1 \leq m \leq n\}$

Halbordnung / Hierarchiebildung:

$(A, \wedge, \vee) \Rightarrow HO(A, \leq)$

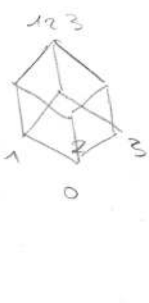
$a \leq b :\Leftrightarrow a = a \wedge b$

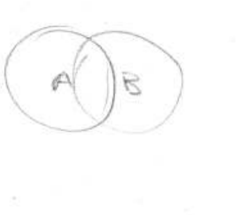
$(P(\{1,2,3\}), \cap, \cup) \;\Big|\; (T_{36}, ggT, kgV)$ $\quad 2^2 \cdot 3^2$

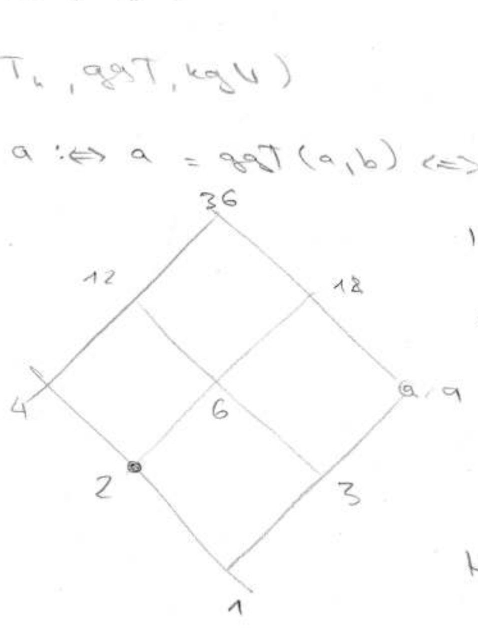
$(P(M), \cap, \cup) \qquad (T_n, ggT, kgV)$

$A = B \Leftrightarrow A = A \cap B \qquad a :\Leftrightarrow a = ggT(a, b) \Leftrightarrow a | b$

$\{1,2,3\} \Leftrightarrow A \subseteq B$







Infimum
untere Schranke

Supremum
obere Schranke

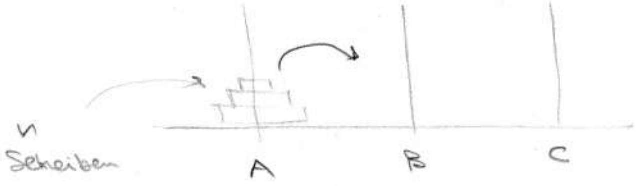
$\downarrow$

Verband $\Rightarrow$ Halbordnung

Halbordnung $\not\Rightarrow$ Verban

Differenzengleichungen / Rekursionen

Türme von Hanoi

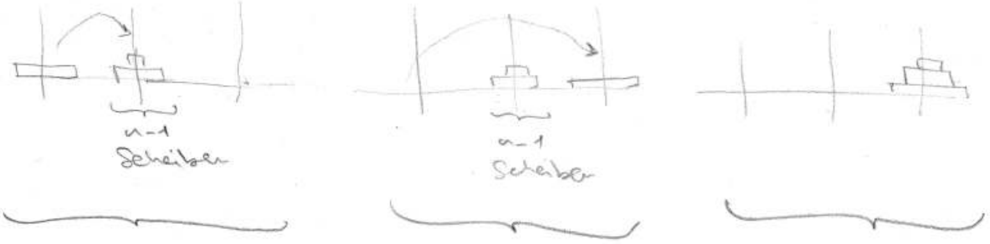


Umlegen der Scheiben von A nach B.
- in jedem „Zug" um eine Scheibe bewegen.
- immer nur kleinere Scheiben auf größere

n	x_n
0	0
1	1
2	$1+1+1 = 3$
3	$3+1+3 = 7$
4	$7+1+7 = 15$
	$15+1+15 = 31$
	… 63
	… 127
	⋮

optimale Strategie:
Bsp 3

2 bereits gelöst　　+1　　erneut 2



$$x_n = x_{n-1} + 1 + x_{n-1}$$

Vermutung:

n	x_n
0	0
1	1 ← Binär-Darstellung
2	11
3	111
4	1111
⋮	⋮

$$\boxed{x_n = 2^n - 1}$$

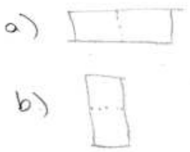
Rekursion: (1. Ordnung)

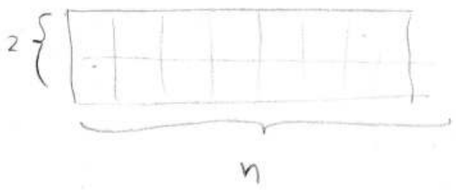
$$x_n = 2 \cdot x_{n-1} + 1 \qquad n \geq 1 \qquad x_0 = 0$$

Beweis: Vollständige Induktion

· Fibonacci - Zahlen:

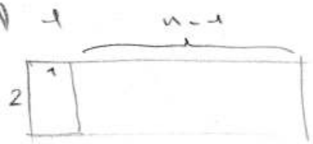
Pflasterbeispiel aus Kombinatorik:





F_n .... Möglichkeiten Band der Größe $2 \times n$ mit Dominos zu pflastern

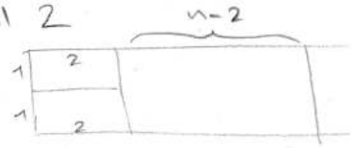
Fall 1

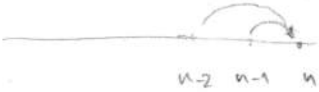


Folge der Fibonacci Z. $F_0 = F_1 = 1$

$F_n = F_{n-1} + F_{n-2}$

Fall 2





Rekursion 2. Ordnung

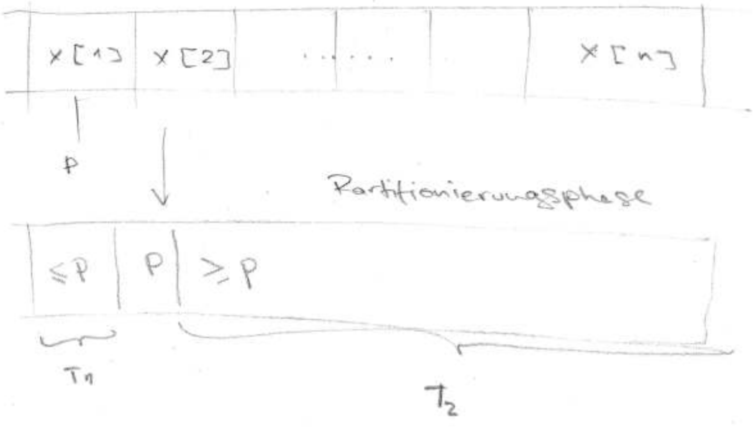
Beweis durch vollst. Induktion mit 2 Induktionsanker

Folge: (1, 1, 2, 3, 5, 8, 13, 21, 34, 55 ...)

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

Beispiel: Quicksort

(Mergesort ist effektiver, ein wenig)



x[1] als Pivot-Element ausgeschlossen

Rekursive Anwendung auf T_1 und T_2.

P(Pivotelement ist k). = $\frac{1}{n}$
Wahrscheinlichkeit, dass an erster Stelle ein k ist

Ø Anzahl an Vergleichen $= X_n$
Wahrscheinlichkeitsmodell:
die Werte (Schlüssel) sind zufällige Werte von Permutationen von $\{1, \dots n\}$

Jede Permutation tritt mit gleicher Wahrscheinlichkeit auf

Rekursion:

Number of Comperisions

$$C_n = n-1 + \sum_{k=1}^{n} P(\text{Pivotelement ist } k) \cdot (\underbrace{C_{k-1}}_{T_1} + \underbrace{C_{n-k}}_{T_2})$$

„Full history recursion" → Zugriff auf <u>ALLE</u> Vorgänger

$$C_n = n-1 + \frac{1}{n} \sum_{k=1}^{n} \left(C_{k-1} + C_{n-k} \right) \qquad n \geq 1 \quad C_0 = 0$$
$$n \geq 2 \quad C_1 = 0.$$

Was ist die <u>allgemeine Lösung</u> einer Rekursion?

Eine die unabhängig von Anfangswerten eingegeben werden kann.

↗ wenn Parameter Vorgegeben: <u>Spezielle lösung</u>

Beispiel: „Lineare homogene Rekursion 1. Ordnung"

$$a_n = c \cdot a_{n-1} \longrightarrow a_n = a_0 \cdot c^n$$

Lineare Rekursionen mit konstanten Koofizienten lassen sich systematisch lösen:

Definition:

$$a_n = \sum_{j=1}^{k} c_j(n)\ a_{n-j} + g_n = c_1(n) \cdot a_{n-1} + C_2(n) \cdot a_{n-2} + \dots + c_k(n)\, a_{n-k} + g_n$$

wenn alle c_j konstant sind: konstante Rek.

inhomogener Anteil (ohne dem: homogen)

<u>nicht</u> $a_{n-1} \cdot a_{n-2}$

<u>nicht</u> $(a_{n-6})^2$

autonome Rekursion: $a_n = f(a_{n-1}, a_{n-2}, \dots, a_{n-k})$ wenn c_j nicht von n abhängt, also $\cancel{c_j(n)}$

ohne n

ZB <u>nicht</u> $n^2 \cdot a_{n-1} = a_n$

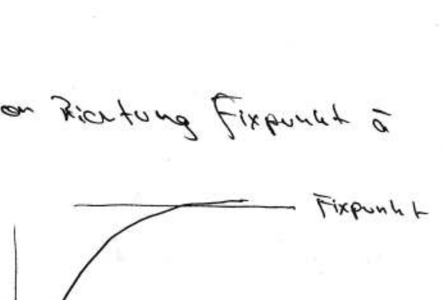
Allgemeine Lösung für inhomogene Rekursionen (linear, konstant) erster Ordnung

$$a_n = c\, a_{n-1} + g$$

$$a_n \begin{cases} c \neq 1 & a_0 \cdot c^n + \frac{1-c^n}{1-c} \cdot g \\ c = 1 & a_0 + n g \end{cases}$$

Wenn $|c| < 1$ dann konvergiert die Rekursion Richtung Fixpunkt $\bar{a}$

$$\left.\begin{array}{l} \bar{a} = c\bar{a} + g \\ a_0 = c \cdot a_0 + g \\ \vdots \end{array}\right\} \text{keine Veränderung}$$



weil $(\text{kleine Zahl})^{\infty} = 0$

$0{,}001^{\infty} = 0$

$$c \cdot 0 + \frac{1-0}{1-c} \cdot g = \frac{g}{1-c} = \bar{a}$$ → Wert ab dem sich nichts mehr verändert!

Eine Rekursion <u>k-ter Ordnung</u> ist eine Gleichung

$$a_n = f(n, a_{n-1}, a_{n-2}, \dots, a_{n-k}) \quad \leftarrow$$

rekursives Bildungsgesetz:
Zugriff auf vorherige Werte

↑
Input der Funktion,
Vorherige Outputs

Durch Lösung der Rekursion
gelangt man zum
nicht-Rekursiven
Bildungsgesetz:

$$a_n = f(n)$$

↑
Input nur n
1, 2, 3, 4, 5 ...

↓

Eine Folge die
idente Glieder hat
zur Rekursion.

Wenn $f(..)$ nicht von n abhängt „autonome Rekursion"

Rekursion = Differenzengleichung

Iteration = Autonome Rekursion erster Ordnung
(Spezialfall)

$a_n = f(a_{n-1})$ Beispiel: Heron'sche Folge

$$\to a_n = \frac{1}{2}\left(a_{n-1} + \frac{2}{a_{n-1}}\right)$$

Parameter
=
Anfangsbedingungen bestimmen
Entwicklung der Rekursion → „spezielle Lösung"
durch Parameter

bei Rekursion k-ter Ordnung:
k-mögliche Anfangswerte
für „allgemeine Lösung"

↓

Beispiel: Rekursion

$a_n = 2a_{n-1} - a_{n-2}$

Parameter $\left.\begin{array}{l} a_1 = 1 \\ a_2 = 1 \end{array}\right\}$ spezielle Lösung: $a_n = 1$

Parameter $\left.\begin{array}{l} a_1 = 1 \\ a_2 = 2 \end{array}\right\}$ spezielle Lösung: $a_n = n$

ohne n in $f(\dots)$

Allgemeine Lösung:

$a_n = k_1 + k_2 \cdot n$

k_1, k_2 := Parameter

$a_n = 1 \to k_1 = 1 \quad k_2 = 2$

$a_n = n \to k_1 = 0 \quad k_2 = 1$

Beweis dafür, dass es diese Lösung gibt:

$\boxed{a_n = n}$ Einsetzen in Differenzeng

$n = 2 \cdot (n-1) - (n-2)$

$n = 2n - 2 - n + 2$

$n = n$ ✓

Die Lösung für lineare Rekursionen 2. Ordnung
homogen, konstante Koeffizienten:

$$a_n = c_1 \cdot a_{n-1} + c_2 a_{n-2}$$

„Superpositionsprinzip"

Vielfache einer Lösung = Lösung

$\sum$ Lösungen = Lösung

Bei Grad 2: 2 Lösungen ausreichend um alle anderen herzuleiten

$a_n = c_1 a_{n-1} + c_2 a_{n-2}$

wenn p_n, q_n spezielle Lösungen sind und nicht Vielfache voneinander:

$k \cdot p_n \neq q_n$

$k \cdot q_n \neq p_n$

Dann lässt sich jede Lösung von $\underline{k_1 p_n + k_2 q_n}$ herleiten!

Die Suche nach 2 speziellen Lösungen: komplexe Zahlen

Ansatz $\boxed{\lambda^n} = a_n$

$$a_n = c_1 a_{n-1} + C_2 a_{n-2}$$

$$\downarrow$$

$$\lambda^n = c_1 \lambda^{n-1} + c_2 \lambda^{n-2} \quad | : (\lambda^{n-2})$$

$$\frac{\lambda^n}{\lambda^{n-2}} = \frac{c_1 \cancel{\lambda^{n-1}}}{\cancel{\lambda^{n-2}}} + \frac{c_2 \cancel{\lambda^{n-2}}}{\cancel{\lambda^{n-2}}}$$

$$\lambda^2 = c_1 \lambda + c_2 \quad \rightarrow \text{Quadratische Gleichung}$$

$$\lambda^2 - c_1\lambda - c_2 = 0$$

$a = 1$

$b = -c_1$

$c = -c_2$

Kleine Lösungsformel:

$$x = -\left(\frac{p}{2}\right) \pm \sqrt{\left(\frac{p}{2}\right)^2 - q}$$

~~$x = 0 = px^2 + qx$~~

$$0 = x^2 + px + q$$

$$\boxed{\begin{array}{l} p = -c_1 \\ q = -c_2 \end{array}}$$

Vektorraum: V ← nur Definition, keine Anwendung für mich

kann reel oder komplex sein

heißt Norm oder normierter Raum wenn

$|\vec{a}| > 0$ wenn $\vec{a} \neq \vec{0}$ (Nullvektor)

$|k \cdot \vec{a}| = |k| \cdot |\vec{a}|$

$|\vec{a}+\vec{b}| \leq |\vec{a}| + |\vec{b}|$ (Gleichheit wenn Dreieck zu Linie ausartet!)

Linearkombination

$$\sum_{j=1}^{m} k_j \vec{a}_j = k_1\vec{a}_1 + k_2\vec{a}_2 + \ldots + k_m\vec{a}_m$$

wobei $a_1, a_2, a_3, \ldots, a_m \in V$

lineare Abhängigkeit

Der Nullvektor $\vec{0}$ per Definition

Wenn es <u>andere Lösungen</u> außer der Triviallösung zu

$$\sum_{j=1}^{m} k_j \vec{a}_j = \vec{0}$$ gibt.

Wenn sich irgendein beliebiger Vektor aus der Linearkombination durch die anderen ausdrücken lässt.

weil

$$\overset{\text{Nicht Null}}{k_1\vec{a}_1} + \overset{\text{Null}}{k_2\vec{a}_2} + \overset{\text{nicht Null}}{k_3\vec{a}_3} = \vec{0}$$

$a - a = 0$

$a - (b+c) = 0$

umstrukturierung:

$$k_2\vec{a}_2 + k_3\vec{a}_3 = -k_1\vec{a}_1$$

weil sie sonst vielfache voneinander wären

$$k_1\vec{a}_1 = k_2\vec{a}_2$$

nicht 0

lineare Unabhängigkeit

Alle Vektoren im Vektorraum lassen sich mit der linear unabhängigen Linearkombination erzeugen.

Wenn $k_1, k_2, k_3, \ldots, k_n = 0$ die <u>einzige</u> Lösung zu

$$\sum_{j=1}^{m} k_j \vec{a}_j = \vec{0}$$ ist.

Maximale Menge

kein weiterer Vektor könnte hinzugefügt werden, ohne die lineare Unabhängigkeit zu zerstören.

Basis von V

$$\vec{a} = \sum_{j=1}^{n} \underbrace{\boxed{k_j}}_{\uparrow}\vec{a}_j = \underbrace{\boxed{k_1\vec{a}_1}}_{\uparrow} + k_2\vec{a}_2 + \dots + k_m\vec{a}_m \quad \Big\}\ \text{Linearkoeffizient}$$

Basisvektoren

eindeutig bestimmte Koeffizienten → Koordinaten von $\vec{a}$ bezüglich der Basis von V

In $\mathbb{R}^3$: Basisvektoren

$$x\underbrace{\begin{pmatrix}1\\0\\0\end{pmatrix}}_{\vec{a}} + y\underbrace{\begin{pmatrix}0\\1\\0\end{pmatrix}}_{\vec{b}} + z\underbrace{\begin{pmatrix}0\\0\\1\end{pmatrix}}_{\vec{c}} = \vec{0} \longrightarrow$$

Interessant:

$$\begin{pmatrix}a_1\\a_2\\a_3\end{pmatrix} = \boxed{a_1}\cdot\vec{a} + \boxed{a_2}\cdot\vec{b} + \boxed{a_3}\cdot\vec{c}$$

Jeder mögliche Vektor!

Die Basis von V wird auch mit $\vec{e}$ angegeben!

Allgemein gilt: Basisvektoren in $\mathbb{R}^n$: bzw $\mathbb{K}^n$

$$\text{~~n-~~ n-Zeilen}\left\{\begin{pmatrix}1\\0\\\vdots\\0\end{pmatrix}\right. = e_1 \quad \begin{pmatrix}0\\1\\\vdots\\0\end{pmatrix} = e_2 \quad \dots \begin{pmatrix}0\\0\\\vdots\\1\end{pmatrix} = e_n$$

„Standardbasis"
„kanonische Basis"

$$\vec{a} = \sum_{j=1}^{n} \boxed{a_j}\boxed{\vec{e}_j}$$

Beispiel:

Vektorraum aller Polynome mit Grad ≤ 2

↪ ~~e~~1, x, x^2

$$e\quad \left.\begin{array}{l} P_0(x) = 1 \\ P_1(x) = x \\ P_2(x) = x^2 \end{array}\right\}$$

Alle anderen Polynome lassen sich mit Linearkombination aus Basis ausdrücken!

„Körper"

Vektorraum über Skalarkörper K

Vektoraddition: $+: \vec{x}, \vec{x} \in V: \vec{x}+\vec{x} \in V$

Skalarmultiplikation: $\lambda \in k, \vec{x} \in V: \lambda \cdot \vec{x} \in V$

Kommutative Gruppe $(V,+)$

Skalarmultiplikation erfüllt Eigenschaften

Linearkombination von Vektoren

$\vec{v}_1, \vec{v}_2, \vec{v}_3, \dots, \vec{v}_n \in V$

$\lambda_1 \cdot \vec{v}_1 + \lambda_2 \cdot \vec{v}_2 + \lambda_3 \vec{v}_3 + \dots + \lambda_n \vec{v}_n \in V$

↖ Koeffizienten

(falls alle $=0$ dann „triviale Linearkombination")

Sonst „nicht triviale Linearkombination"

$M \neq \emptyset$ ← Nullvektor

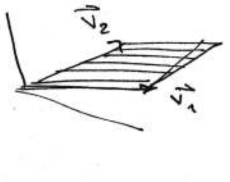
$[M] := \{ \lambda_1 \vec{v}_1 + \lambda_2 \vec{v}_2 \dots \lambda_n \vec{v}_{\cancel{n}} \mid \lambda_j \in k, n \in \mathbb{N} \}$

↳ Lineare Hülle von M → Unterraum der von M erzeugt wird

~~Eben~~ „kleinster, nicht leerer Unterraum, der alle Vektoren aus M enthält"

$[M] := \{\vec{0}\}$

R^3:



$[\vec{v}_1, \vec{v}_2] = \{ \lambda_1 \vec{v}_1 + \lambda_2 \vec{v}_2 + \cancel{\lambda_3 \vec{v}_3} \mid \lambda_1, \lambda_2 \in \mathbb{R} \}$

Lineare Abhängigkeit | ~~[illegible]~~ Unabhängigkeit

Teilräume / Untervektorräume

ähnlich wie Untergruppen:

$U \subseteq V$, Nullvektor $\in U$

Abgeschlossenheit unter Multipli., Addit.

$a, b \in U$ und $k \in \mathbb{K}$

$a, b \in U \Rightarrow a + b \in U$

$a \in U \Rightarrow ka \in U$

Beispiel

$$\begin{array}{c} x \\ y \\ z \end{array} \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \cdot k_1 + \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} k_2 = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$$

bildet die Ebene xy als Teilraum von $\mathbb{R}^3$

$$\begin{pmatrix} k_1 \\ k_2 \\ 0 \end{pmatrix}$$

Lineare Hülle

$$LH\{a_1, a_2, a_3, \dots, a_m\} = \left\{ \sum_{j=1}^{m} k_j a_j \;\middle|\; k_j \in \mathbb{K} \right\} \subseteq V$$

= Alle Vektoren die gebildet werden können aus Linearkombination mit $a_1 \dots a_m$

„Die Lineare Hülle wird von den Vektoren $a_1, \dots a_m$ AUFGESPANNT"

Lineare Abbildungen

Drehung
Spiegelung
Stauchung
Streckung

} Beispiele

Abbildung

$$F: \mathbb{K}^n \rightarrow \mathbb{K}^m$$

$x \in \mathbb{K}^n \quad y = F(x) \in \mathbb{K}^m$

Abbildungen sind linear wenn

$$F(x) = A x = y \qquad A^{m \times n}$$

$$F \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} a_{11} x_1 + a_{12} x_2 + \dots + a_{mn} x_n \\ a_{m1} x_1 + a_{m2} x_2 + \dots + a_{mn} x_n \end{pmatrix}$$

$\rightarrow A = \mathbb{1}$

Warum?

Angenommen: $F(x) = -x$

$$F(x) = \underbrace{-1}_{} \cdot x$$

veränderte Einheitsmatrix!

bei $\mathbb{R}^2$ $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$

Matrizen Multiplikation

$$A^{\textcircled{m} \times n} \cdot B^{n \times \textcircled{r}} = C^{\textcircled{m \times r}}$$

Nur definiert, wenn A Spaltenanzahl = B Zeilenanzahl

Koeffizienten von C:

$$c = \sum_{k=1}^{n} a_{ik} \cdot b_{kj} = a_{i1} \cdot b_{1j} + a_{i2} \cdot b_{2'j} + a_{i3} + b_{3'j} + \dots + a_{in} + b_{nj}$$

Beispiel:

$$A = \begin{pmatrix} 4 & 2 & 0 \\ -1 & 3 & 5 \end{pmatrix} \qquad B = \begin{pmatrix} 2 & 1 \\ 3 & 7 \\ 1 & 0 \end{pmatrix} \qquad C = \begin{pmatrix} 7 & 1 \\ 2 & 5 \end{pmatrix}$$

a) AB =

„Falkschema"

$$\begin{array}{cccc|ccc} & & & & 2 & 1 & \\ & & & & 3 & 7 & \to B \\ & & & & 1 & 0 & \\ \hline A \leftarrow & 4 & 2 & 0 & 14 & 18 & \\ & -1 & 3 & 5 & 12 & 20 & \longrightarrow C \end{array}$$

$$c_{11} = a_{11} \cdot b_{11} + a_{12} b_{21} + a_{13} b_{31} =$$
$$= 4 \cdot 2 + 2 \cdot 3 + 0 \cdot 1 = 14$$

$$c_{12} = 4 \cdot 1 + 2 \cdot 7 + 0 \cdot 0 = 18$$

$$c_{21} = -1 \cdot 2 + 3 \cdot 3 + 5 \cdot 1 = 12$$

$$c_{22} = -1 \cdot 1 + 3 \cdot 7 + 5 \cdot 0 = 20$$

b) BA =

$$\begin{array}{cc|ccc} & & 4 & 2 & 0 \\ & & -1 & 3 & 5 \\ \hline 2 & 1 & 7 & 7 & 5 \\ \hline 3 & 7 & 5 & 27 & 35 \\ \hline 1 & 0 & 4 & 2 & 0 \end{array}$$

c) CB =

$$\begin{array}{cc|cc} & & \boxed{2} & 1 \\ & & \boxed{3} & 7 \\ & & \boxed{1} & 0 \\ \hline \boxed{7} & \boxed{1} & & \\ 2 & 5 & & \end{array}$$

Nicht definiert !

d) BC =

$$\begin{array}{cc|cc} & & \boxed{7} & 1 \\ & & \boxed{2} & 5 \\ \hline \boxed{2} & \boxed{1} & 16 & 7 \\ 3 & 7 & 35 & 38 \\ 1 & 0 & 7 & 1 \end{array}$$

definiert

Division mit Matrizen

$$A \cdot \underbrace{B^{-1}}_{\substack{\text{Kehrwert} \\ \text{von } B \\ \frac{1}{B}}} = \frac{A}{B}$$

$\frac{1}{B} \leftarrow \mathbb{I}$

Quadratische Matrix!

wie ermittelt man Inverse Matrizen?

$$A \cdot A^{-1} = \mathbb{I} \qquad \text{weil} \quad \frac{1}{B} \cdot B = 1$$

↑ Matrix muss „invertierbar" („regulär" sein

A^{-1} = inverse Matrix zu A
hat dieselbe Dimension wie A

Wenn quadratische Matrix nicht invertierbar ist:
„Singulär"

$$A = \begin{pmatrix} 3 & 0 \\ 0 & 0 \end{pmatrix}$$ nicht invertierbar

↑ kann multipliziert nicht $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ ergeben!

Es ist ein B gesucht für das gilt

$$A \cdot B = \mathbb{I} \quad \underline{\text{oder}} \quad B \cdot A = \mathbb{I}$$

Dadurch $B = A^{-1}$

Beispiel:

$$A = \begin{pmatrix} 2 & 4 \\ -1 & 3 \end{pmatrix} \quad B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$$

$$\begin{array}{cc|cc} & & b_{11} & b_{12} \\ & & b_{21} & b_{22} \\ \hline 2 & 4 & 2b_{11} + 4b_{21} & 2b_{12} + 4b_{22} \\ -1 & 3 & -1b_{11} + 3b_{21} & -1b_{12} + 3b_{22} \end{array}$$

$$AB = \begin{pmatrix} 2 & 4 \\ -1 & 3 \end{pmatrix} \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 2b_{11} + 4b_{21} & 2b_{12} + 4b_{22} \\ -b_{11} + 3b_{21} & -b_{12} + 3b_{22} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Lineares Gleichungssystem:

$$\left.\begin{array}{l} 2b_{11} + 4b_{21} = 1 \\ 2b_{12} + 4b_{22} = 0 \\ -b_{11} + 3b_{21} = 0 \\ -b_{12} + 3b_{22} = 1 \end{array}\right\} \quad \begin{array}{ll} b_{11} = \frac{3}{10} & b_{12} = -\frac{2}{5} = -\frac{4}{10} \\ b_{21} = \frac{1}{10} & b_{22} = \frac{1}{5} = \frac{2}{10} \end{array}$$

$$B = \frac{1}{10} \begin{pmatrix} 3 & -4 \\ 1 & 2 \end{pmatrix}$$

$$AB = \mathbb{I}_2 \xrightarrow[\text{daraus folgt}]{} BA = \mathbb{I}_2$$

Matrizenmultiplikation mit $\mathbb{I}$

$$\begin{pmatrix} 1 & 0 & 0 & & 0 \\ 0 & 1 & 0 & & 0 \\ 0 & 0 & 1 & & 0 \\ \vdots & & & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}$$

$$\begin{array}{cc|cc} & & 1 & 0 \\ & & 0 & 1 \\ \hline a & b & a & b \\ c & d & c & d \end{array}$$

Satz:

$$A^{m \times n} \cdot \mathbb{I}_n = \mathbb{I}_m \cdot A^{m \times n} = A$$

Einheitsmatrix vergleichbar mit 1 bei reelen Zahlen.

$n \times n$ Matrizen bilden mit $\mathbb{I}_n$ einen Ring

für quadratische $n \times n$ Matrizen sind auch Potenzen definiert

$$A^0 = \mathbb{I}$$
$$A^1 = A$$
$$A^2 = AA$$

Lineare Gleichungssysteme lösen

$$\downarrow_{m} \overset{\longrightarrow n}{A}$$

m Gleichungen
n Unbekannte

kann in der Form $Ax = b$ geschrieben werden.

Die Matrix $A^{m \times n}$ enthält koeffizienten des Gleichungssystems:
„koeffizientenmatrix"

Beispiel:
Das lineare Gleichungssystem in Form von $Ax = b$

$$4x_1 - x_2 = 7$$
$$2x_1 + 5x_2 = 9$$

$$\begin{pmatrix} 4 & -1 \\ 2 & 5 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 7 \\ 9 \end{pmatrix}$$

Beispiel:

$$A = \begin{pmatrix} 5 & 3 \\ 2 & -1 \end{pmatrix} \quad x = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \quad b = \begin{pmatrix} 2 \\ 3 \end{pmatrix}$$

$Ax = b$ in Form von 2 Gleichungen

$$\begin{pmatrix} 5x_1 + 3x_2 \\ 2x_1 - x_2 \end{pmatrix} = \begin{pmatrix} 2 \\ 3 \end{pmatrix}$$

Entspricht:

$$5x_1 + 3x_2 = 2$$
$$2x_1 - x_2 = 3$$

$$Ax = b$$
$$x = b \cdot \bigcirc\!\!\!\!A^{-1} \text{ invertierte Matrix}$$

Vorsicht: nicht alle Gleichungssysteme lassen sich so lösen
weil nicht alle Matrizen invertierbar sind.

Anwendung der Linearen Algebra in der Informatik:

LINEARE CODES

Block mit k Bit wird übermittelt

$$\hat{=} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \end{pmatrix} \in \mathbb{Z}_2^k$$
$x_k.$

Es werden $\boxed{n-k}$ Kontrollbits angehängt und es entsteht ein

Vektor $\underbrace{c \in \mathbb{Z}_2^n}_{\text{„Codewort"}} \leftarrow$ (Warum nicht $\mathbb{Z}_2^{n-k}$?)
weil sie ein Teilraum von $\mathbb{Z}_2^n$ sind!

Codewörter bilden Vektorraum
$= \text{Teilraum von } \mathbb{Z}_2^n$

„Lineare Codes"
Weil sich die Codewörter als Linearkombination darstellen lassen können.

$$x = \sum_{j=1}^{k} x_1 e_1 = x_1 \begin{pmatrix}1\\0\\0\\0\\\vdots\\0\end{pmatrix} + x_2 \begin{pmatrix}0\\1\\0\\\vdots\\0\end{pmatrix} + \dots + x_k \begin{pmatrix}0\\0\\0\\0\\\vdots\\1\end{pmatrix}$$

} Jeder mögliche Code kann damit ausgedrückt werden.

Erweiterung mit Kontrollbits

$$c = \begin{pmatrix}1\\0\\\vdots\\0\end{pmatrix} x_1 + \begin{pmatrix}0\\1\\0\\\vdots\\0\end{pmatrix} x_2 + \dots + \begin{pmatrix}0\\\vdots\\1\end{pmatrix} x_k$$

$$\text{Kontroll-Bits} \left\{ \begin{array}{ccc} a_{1,1} & a_{2,1} & a_{k,1} \\ a_{1,2} & a_{2,2} & a_{k,2} \\ \vdots & \vdots & a_{k,3} \\ a_{1,n-k} & a_{2,n-k} & \vdots \\ \uparrow & & a_{k,n-k} \end{array} \right.$$

n ist die Gesamtlänge!

Generatormatrix

Alle Additionskomponente von c werden waagrecht als Zeilen einer Generatormatrix geschrieben $\longrightarrow (k, n)$ matrix
↓ ↓
Zeilen Spalten

Transponierte Matrix

$$c = G^T x$$

Alle codes lassen sich mit Generatormatrix bilden

Transponiert bedeutet:

$$(a_{ij})^T = a_{ji} \qquad \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}^T = \begin{pmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{pmatrix}$$

$$\boxed{\begin{array}{ll} a_{11} = a_{11} & a_{21} = a_{12} \\ a_{12} = a_{21} & a_{22} = a_{22} \\ a_{13} = a_{31} & a_{23} = a_{32} \end{array}}$$

Deshalb:

$c = G^T x$ weil $G = (\mathbb{I}_k \; A)$ beziehungsweise

$$G = \begin{pmatrix} \underbrace{\begin{matrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & & \vdots \\ 0 & 0 & \ddots & \vdots \\ \vdots & & \ddots & 0 \\ 0 & 0 & \cdots 0 & 1 \end{matrix}}_{(k \times k \text{ Matrix})} & \begin{matrix} a_{11} & a_{12} & \cdots & a_{1,n-k} \\ a_{21} & & & \vdots \\ \vdots & & & \vdots \\ a_{k,1} & \cdots & \cdots & a_{k,n-k} \end{matrix} \end{pmatrix}$$

Beispiel:

$$A = \left.\begin{pmatrix} 1 \\ 1 \end{pmatrix}\right\} k = 2 \quad \text{also} \quad G = \begin{pmatrix} \underbrace{\begin{matrix} 1 & 0 \\ 0 & 1 \end{matrix}}_{\mathbb{I}_k} & \underbrace{\begin{matrix} 1 \\ 1 \end{matrix}}_{A} \end{pmatrix}$$

Hier:

$H = (1 \; 1 \; 1)$

Die Kontrollmatrix
zur Generatormatrix

$$H = (A^T \; \mathbb{I}_{n-k}) \qquad A^T \text{ wenn } A = \begin{pmatrix} 1 \\ 1 \end{pmatrix} \rightarrow A^T = (1 \;\; 1)$$

$$\mathbb{I}_{\underset{\underset{n=3}{\uparrow}}{n-2}} = (1)$$

Lineare Gleichungssysteme LGS

$A \cdot \vec{x} = \vec{b}$

$\hookrightarrow (A \, \vec{b})$ erweiterte Systemmatrix

$\text{rang}\, A = \text{rang}\, (A \vec{b})$

$(\vec{a}_1 \, \vec{a}_2 \, \vec{a}_3 \, \dots \, \vec{a}_n) \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \vec{b}$

„Satz von Kronecker"
Wenn $\vec{b}$ in A ist: Das Gleichungssystem lösbar ist, dann haben A und $A\vec{b}$ denselben Rang

$[\vec{a}_1 \, \vec{a}_2 \, \dots \, \vec{a}_n] = [\vec{a}_1 \, \vec{a}_2 \dots \vec{a}_n \, \vec{b}]$

↖ Spalten der A-Matrix

Sie spannen beide denselben Untervektorraum auf.

Beispiel:

$$(A \mid \vec{b}) = \left(\begin{array}{ccc|c} 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 \\ 4 & 5 & 6 & 8 \end{array}\right)$$

$A\vec{x} = \vec{b}$ lösbar

↓

$Z2 - Z1, \; (4 \cdot Z1) - (Z3)$

$$\left(\begin{array}{ccc|c} 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 \\ 0 & 1 & 2 & 4 \end{array}\right)$$

Stufenform ~~„Rang sehen"~~ ?

↓

$$\left(\begin{array}{ccc|c} 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 \\ 0 & 0 & 0 & 1 \end{array}\right)$$

Rang $A = 2$
Rang $(A b) = 3$ } unlösbar

Angenommen: lineares Gleichungssystem = lösbar

$A\vec{x} = \vec{b}$

$f(\vec{x}) = A\vec{x}$

lineare Abbildung

$f \; K^n \longrightarrow K^n$

$A\vec{x}_0 = \vec{b}$

$A(x - x_0) = \vec{b} - \vec{b} = \vec{0}$

Wenn: $A(x - x_0) = \vec{0}$ → Homogene LGS mit Y_0 als Lösung

~~At~~ $A\vec{x} = \vec{0} \Rightarrow f(\vec{x}) = \vec{0}$

$\vec{x} - \vec{x}_0 \in Ker(f)$

↑ Spezielle Lösung

↑ Alle Lösungen

} ähnlich wie Differenzengleichungen!

$x = x_0 + Ker(f)$

defekt ⇒ $def(f) = dim(ker(f))$

⇓

Dimension vom Vektorraum - Rang von f bzw. Rang von A

$\dim V = n - rg(f) =$

$= n - rg(A)$

Liefert die # der Vektoren einer Basis von f

Bzw auch # der Parameter

Basisvektoren ~~der~~ Linearhülle

$[b_1, b_2, b_3 \ldots b_n]$

$\vec{x} = \vec{x}_0 + t_1 \cdot \vec{b}_1 + t_2 \cdot \vec{b}_2 + t_3 \cdot \vec{b}_3 \ldots + t_n \vec{b}_n$

Spezialfälle:

$f(x) = A\vec{x} \quad f : K^n \mapsto K^m$

angenommen f ist surjektiv: $rang(f) = rang(A) = m$

LGS für jede beliebige Wahl $\vec{b} \in K^m$ lösbar

angenommen f ist injektiv: $rang(f) = rang(A) = n$

$Ker(f) = \{\vec{0}\}$

LGS für jede Wahl höchstens eine Lösung

Bei quadratische Koeffizientenmatrix:

$A\vec{x} = \vec{b}$ $\qquad \underset{\text{quadratische Matrix}}{A \in K^{n \times m}}$ $\longrightarrow$ und f ist $\underbrace{\text{surjektiv \& injektiv}}_{\text{bijektiv}}$

rang(A) = n = m für jede beliebige Wahl genau 1 Lsg.

→ Matrix ist invertierbar

$\vec{x} = A^{-1} \cdot \vec{b}$

Wenn Matrix:

$$\left(\begin{array}{cccc|c} 1 & & 0 & a_{1\,m+1} \; \cdots \; a_{1n} & b_1 \\ & 1 & & a_{2\,m+1} \; \cdots \; a_{2n} & b_2 \\ 0 & & \ddots\, 1 & \vdots & \vdots \\ & & & a_{m\,m+1} \; \cdots \; a_{mn} & b_n \end{array}\right)$$

$(\mathbb{I}_m \; \tilde{A} \mid \vec{b})$ besitzt folgende Lösungsgesamtheit:

~~$\vec{x} = \begin{pmatrix} \vec{b} \\ \vec{0} \end{pmatrix} + t_1 \underbrace{\begin{pmatrix} a_{1\,m+1} \\ \vdots \\ a_{m\,m+1} \end{pmatrix}}_{\text{1. Spalte } \tilde{A}} + t$~~

$$\vec{x} = \begin{pmatrix} \vec{b} \\ \vec{0} \end{pmatrix} + t_1 \begin{pmatrix} a_{1\,m+1} \\ \vdots \\ a_{m\,m+1} \\ \vec{e}_1 \end{pmatrix} + t_2 \begin{pmatrix} a_{m+2} \\ \vdots \\ \vec{e}_2 \end{pmatrix} + \ldots + t_{n-m} \begin{pmatrix} \vec{a}_n \\ \vec{e}_{n-m} \end{pmatrix}$$

Spezielle Lsg

1. Spalte von $\tilde{A}$

1. kanonischer Basisvektor

Fortsetzung des Beispieles

Vorlesung

$$\left(\begin{array}{cccc|c} \textcircled{1} & 1 & 3 & 2 & 0 \\ 2 & 1 & 4 & 5 & 1 \\ 3 & 1 & 5 & 8 & 2 \end{array}\right) \longmapsto \left(\begin{array}{cccc|c} 1 & 1 & 3 & 2 & 0 \\ 0 & -1 & -2 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

$x_3 = t_1 \leftarrow$ (Parameter)

$x_4 = t_2$

$-x_2 - 2x_3 + x_4 = 1$

$\vdots$

Lösung in Parameterdarstellung:

$$\vec{x} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 1 - t_1 - 3t_2 \\ -1 - 2t_1 + t_2 \\ t_1 \\ t_2 \end{pmatrix}$$

Beispiel:
Spaltenvertauschung

$$\left(\begin{array}{cccc|c} 1 & -1 & 1 & 2 & 3 \\ 1 & -1 & 0 & 5 & 1 \\ 2 & -2 & 3 & 1 & 8 \end{array}\right) \rightarrow \left(\begin{array}{cccc|c} 1 & -1 & 1 & 2 & 3 \\ 0 & 0 & -1 & 3 & -2 \\ 0 & 0 & 1 & -3 & 2 \end{array}\right)$$

Zeilenvertauschung nicht Sinnvoll:
Spaltenvertauschung!

~~Zz~~ Spalte$_2$ $\rightleftarrows$ Spalte$_3$

$$\left(\begin{array}{cccc|c} 1 & 1 & -1 & 2 & 3 \\ 0 & -1 & 0 & 3 & -2 \\ 0 & 1 & 0 & -3 & 2 \\ y_1 & y_3 & y_2 & y_4 & \end{array}\right)$$

$$\downarrow$$

$$\left(\begin{array}{cccc|c} 1 & 1 & -1 & 2 & 3 \\ 0 & -1 & 0 & 3 & -2 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

$$\begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{pmatrix} \rightarrow \begin{pmatrix} x_1 \\ x_3 \\ x_2 \\ x_4 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \\ 0 \\ 0 \end{pmatrix} + t_1 \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} + t_2 \begin{pmatrix} -5 \\ 3 \\ 0 \\ 1 \end{pmatrix}$$

$$\vec{x} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 2 \\ 0 \end{pmatrix} + t_1 \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} + t_2 \begin{pmatrix} -5 \\ 0 \\ 3 \\ 1 \end{pmatrix}$$

Beispiel:

$$\left(\begin{array}{ccc|c} 1 & 2 & 1 & 3 \\ -2 & 1 & 2 & 1 \\ 3 & 0 & -2 & 0 \\ 1 & 1 & 1 & 4 \end{array}\right) \rightarrow \left(\begin{array}{ccc|c} 1 & 2 & 1 & 3 \\ 0 & 5 & 4 & 7 \\ 0 & -6 & -5 & -9 \\ 0 & -1 & 0 & 1 \end{array}\right) \xrightarrow{\text{Zeilen vertauschen}} \left(\begin{array}{ccc|c} 1 & 2 & 1 & 3 \\ 0 & -1 & 0 & 1 \\ 0 & -6 & -5 & 9 \\ 0 & 5 & 4 & 7 \end{array}\right)$$

$$\left(\begin{array}{ccc|c} 1 & 2 & 1 & 3 \\ 0 & -1 & 0 & 1 \\ 0 & 0 & -5 & -15 \\ 0 & 6 & 4 & 12 \end{array}\right) \rightarrow \left(\begin{array}{ccc|c} 1 & 2 & 1 & 3 \\ 0 & -1 & 0 & 1 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 1 & 3 \end{array}\right) \rightarrow \left(\begin{array}{ccc|c} 1 & 2 & 1 & 3 \\ 0 & -1 & 0 & 1 \\ 0 & 0 & 1 & 3 \\ \cancel{0} & \cancel{0} & \cancel{0} & \cancel{0} \end{array}\right)$$

$$\vec{x} = \begin{pmatrix} 3 \\ -1 \\ 3 \end{pmatrix}$$

$x_3 = 3$

$-x_2 = 1 \Rightarrow x_2 = -1$

$x_1 = 3 - 2x_2 - x_3$

$= 3 + 2 - 3 = 2$

Codierungstheorie als Anwendung! } optionaler Inhalt.

Determinanten

Quadratische Matrix

$$A^{m \times m} \in K^{m \times m}$$

$$\det A = \sum_{\pi \in S_n} \operatorname{sgn}(\pi) \cdot a_{\pi(1)1} \cdot a_{\pi(2)2} \cdots a_{\pi(m)m}$$

Die Siebformel dient zur Berechnung der Mächtigkeit von mehreren (nicht disjunkten) Menge und ist wie folgt definiert:

$$\sum_{I\subseteq\{1,\ldots,n\},I\neq 0} (-1)^{|I|-1}\left|\bigcap_{i\in I} A_i\right|$$

Dadurch ergibt sich die Formel für 2 bzw. 3 endliche Teilmengen:

$$|A\cup B| = |A| + |B| - |A\cap B|$$

$$|A\cup B\cup C| = |A| + |B| + |C| - |A\cap B| - |A\cap C| - |B\cap C| + |A\cap B\cap C|$$

Beispiel 3b

Bestimmen Sie mit Hilfe der Siebformel die **Permutationen** ("Anzahl aller Anordnungen") von den Buchstaben $\{a,b,c,d,e,f\}$, in denen weder der Block "bcf" noch "eb" vorkommt!

$A_1 = \{a,b,c,d,e,f\}, n_1 = 6 \qquad A_2 = \text{"}bcf'', n_2 = 3 \qquad A_3 = \text{"}eb'', n_3 = 2$

$$|A_1| - \Big(|A_2| + |A_3|\Big) = n_1! - \Big([(n_1-n_2+1)*(n_1-n_2)!] + [(n_1-n_3+1)*(n_1-n_3)!]\Big)$$

$$= 6! - \Big((4*3!) + (5*4!)\Big) = 720 - \Big(24+120\Big) = \mathbf{576}$$

Beispiel 4a

Bestimmen Sie für das folgende lineare Gleichungssystem alle Werte von a für:

1. keine Lösung.
2. eine eindeutige Lösung.
3. unendlich viele Lösungen und zusätzlich die Dimension des Lösungsraumes und die allgemeine Lösung $\vec{x} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$.

$$\begin{aligned} x_1 + x_2 - x_3 &= 1 \\ 2x_1 + 3x_2 + ax_3 &= 3 \\ x_1 + ax_2 + 3x_3 &= 2 \end{aligned}$$

Die Koeffizienten des LGS lässt sich sehr schön als Matrix darstellen mit der weitergerechnet werden kann:

$$\left(\begin{array}{ccc|c} 1 & 1 & -1 & 1 \\ 2 & 3 & a & 3 \\ 1 & a & 3 & 2 \end{array}\right) = \dots$$

Beispiel 4b

Bestimmen Sie für die Matrix A die inverse Matrix A^{-1} und die Matrix $C = ABA^{-1}$!

$$\mathbf{A} = \begin{pmatrix} 5 & 1 \\ 3 & 1 \end{pmatrix} \quad \mathbf{B} = \begin{pmatrix} 4 & 2 \\ -15 & -7 \end{pmatrix}$$

Die inverse Matrix $A^{-1} = \frac{1}{det(A)} * A^{\#}$, wobei $A^{\#}$ die Komplementärmatrix von A ist (Transposition der vorzeichenbehaftete Minoren). Es kann natürlich auch der Gauß-Jordan-Algorithmus verwendet werden.
Weiters gilt $A * A^{-1} = A^{-1} * A = E$ (E ist die Einheitsmatrix von A) und zeigt, dass A^{-1} das inverse Element bezüglich der Matrizenmultiplikation ist.
Eine Matrix A ist invertierbar (regulär) wenn gilt $det(A) \neq 0$:

$$\mathbf{det(A)} = a_{11}a_{22} - a_{12}a_{21} = 5 * 1 - 1 * 3 = \mathbf{2}$$

Mithilfe der Determinante kann nun weitergerechnet werden:

$$\mathbf{A^{-1}} = \frac{1}{2} * \begin{pmatrix} +|1| & -|3| \\ -|1| & +|5| \end{pmatrix}^T = \frac{1}{2} * \begin{pmatrix} 1 & -1 \\ -3 & 5 \end{pmatrix} = \begin{pmatrix} 0.5 & -0.5 \\ -1.5 & 2.5 \end{pmatrix}$$

Überprüfung durch Matrizenmultiplikation mit Hilfe des Falk Schemas.

$$\mathbf{AA^{-1}} = \begin{pmatrix} 5 & 1 \\ 3 & 1 \end{pmatrix} * \begin{pmatrix} 0.5 & -0.5 \\ -1.5 & 2.5 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = E$$

Um die Matrix C zu berechnen wird das Falk Schema nacheinander angewendet.

$$\mathbf{C} = ABA^{-1} = \begin{pmatrix} 5 & 1 \\ 3 & 1 \end{pmatrix} * \begin{pmatrix} 4 & 2 \\ -15 & -7 \end{pmatrix} * A^{-1}$$

$$= \begin{pmatrix} 5 & 3 \\ -3 & -1 \end{pmatrix} * \begin{pmatrix} 0.5 & -0.5 \\ -1.5 & 2.5 \end{pmatrix} = \begin{pmatrix} -2 & 5 \\ 0 & -2 \end{pmatrix}$$

Lineare Differenzengleichungen

Linear, homogen, 2. Ordnung

$a_n = c_1 a_{n-1} + c_2 a_{n-2}$ (c = konstant) $\longrightarrow$ wir brauchen 2 Lösungen um restliche darzustellen: [q_n und p_n]

Wenn sie keine Vielfachen voneinander sind;

Superpositionsprinzip:

gilt für alle homogene lineare Rekursionen:

1) Vielfache einer Lösung = Lösung

2) Summe von 2 Lösungen = Lösung → $k_1 p_n + k_2 p_n =$

Alle möglichen Lösungen

k_1 und k_2 werden aus Anfangsbedingungen bestimmt

Um 2 geeignete spezielle Lösungen zu finden:

„Ansatz λ^n" $= a_n$

$$\lambda^n = c_1 \lambda^{n-1} + c_2 \lambda^{n-2} \quad | : \lambda^{n-2}$$

$$\frac{\lambda^n}{\lambda^{n-2}} = c_1 \frac{\lambda^{n-1}}{\lambda^{n-2}} + c_2 \frac{\lambda^{n-2}}{\lambda^{n-2}}$$

$\boxed{\lambda^2 = c_1 \lambda + c_2}$ Charakteristische Gleichung (Quadratisch)

	Nullstellen λ_1 und λ_2
$a_n = k_1 \lambda_1^n + k_2 \lambda_2^n$ k_1 und k_2 durch Anfangsbed. herausfinden $a_0 = k_1 + k_2$ $a_1 = k_1 \lambda_1 + k_2 \lambda_2$	verschieden und reel
$a_n = (k_1 + k_2 n) \lambda^n$ $a_0 = k_1$ $a_2 = (k_1 + k_2) \lambda$	identisch und reel
$\lambda_1 = r(\cos(\varphi) + i\sin(\varphi))$ $\lambda_2 = r(\cos(\varphi) - i\sin(\varphi))$	komplex (konjugiert)

$a_n = k_1 r^n \cos(n\varphi) + k_2 r^n \sin(n\varphi)$

(Satz von Moivre)

$a_0 = k_1$

$a_1 = k_1 r \cos(\varphi) + k_2 r \sin(\varphi)$

Linear inhomogen 2. Ordnung

konstante Koeffizienten $c_1, c_2 \in \mathbb{R}$

$a_n = c_1 a_{n-1} + c_2 a_{n-2} + g(n)$

$a_n = h_n + \boxed{i_n}$ ← spezielle Lösung

$\overbrace{h_n = c_1 h_{n-1} + c_2 h_{n-2}}$ ← allgemeine Lösung

Angenommen p(n) und q(n) sind spezielle Lösungen

Lineare Differenzengleichungen

lassen sich mit konst. Koeffizienten systematisen lösen

$$a_n = \sum_{j=1}^{k} c_j(n) \cdot a_{n-j} + g_n$$

inhomogener Anteil

k-ter Ordnung

Autonom:

Inhomogener Anteil = 0 oder konst.

konstante Koeffizienten

Linear, inhomogen, 1. Ordnung

$$a_n = c\, a_{n-1} + g \rightarrow \text{konstant}$$

$$a_n = \begin{cases} a_0 c^n + \frac{1-c^n}{1-c} g & c \neq 1 \\ a_0 + ng & c = 1 \end{cases}$$

Konvergiert gegen <u>Fixpunkt</u> $\bar{a}$

$|c| < 1$: $\bar{a} = \frac{g}{1-c}$ weil ang. $c=0$ $c \cdot 0 + \frac{1-0}{1-c} \cdot g$

$|c| > 1$:
- wenn $a_0 > \bar{a} \rightarrow +\infty$
- wenn $a_0 < \bar{a} \rightarrow -\infty$
- wenn $a_0 = \bar{a} \rightarrow$ alle bleiben gleich $\bar{a}$

Linear, inhomogen, 1. Ordnung

g nicht konstant!

$$a_n = c\, a_{n-1} + g_n$$

$$a_n = k c^n + r_n \leftarrow$$ beliebige spezielle Lösung (raten)

komplizierter wenn
$c \neq$ konstant ... $c(n)$

Beispiel zum Erraten von i_n:

$$\underbrace{a_n = 3a_{n-1} + 2n}_{a_n = c\,a_{n-1} + g_n} \longrightarrow a_n = kc^n + \underbrace{\boxed{i_n}}_{} \qquad k \in \mathbb{R}$$

hat die Form

$i_n = 3i_{n-1} + 2n$

Polynom ersten Grades

$i_n = cn + d \quad c, d \in \mathbb{R}$

$$cn + d = 3\,\underbrace{(c(n-1) + d)}_{} + 2n$$

$$\rightarrow i_n = 3i_{n-1} + 2n$$

$$cn + d = 3(cn - c + d) + 2n$$

$$cn + d = 3cn - 3c + 3d + 2n$$

$$= n(-2c - 2) + (-2d + 3c) = 0$$

nur möglich wenn

$-2c - 2 = 0 \quad c = -1$

$-2d + 3c = 0 \quad d = -\frac{3}{2}$

$\longleftarrow \quad \boxed{i_n = -1n - \frac{3}{2}}$ spezielle Lösung

Allgemeine Form

$a_n = 3a_{n-1} + 2n$

$a_n = k \cdot 3^n - n - \frac{3}{2} \quad k \in \mathbb{R}$

Spezielle Lösung

$a_0 = 3$

$3 = a_0 = \boxed{k} \cdot 3^0 - 3 - \frac{3}{2}$

$\downarrow$

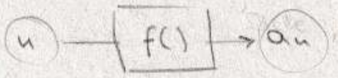
$k = \frac{9}{2}$ für $a_0 = 3$

$a_n = \frac{9}{2} \cdot 3^n - n - \frac{3}{2}$

Differenzengleichungen

explizites/
Durch Lösung der Rekursion: nicht-rekursives Bildungsgesetz $a_n = f(n)$

Rekursion k-ter Ordnung

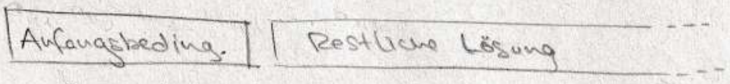


$$a_n = f(n, \underbrace{a_{n-1}, a_{n-2}, \dots, a_{n-k}}_{\text{vorherige Werte}}) \leftarrow \text{k Werte davor}$$

Wenn f(..) n nicht braucht: autonom
Wenn $f(a_{n-1})$ ... 1. Ordnung / Iteration

Lösung

Folge deren Glieder die Rekursion erfüllen:

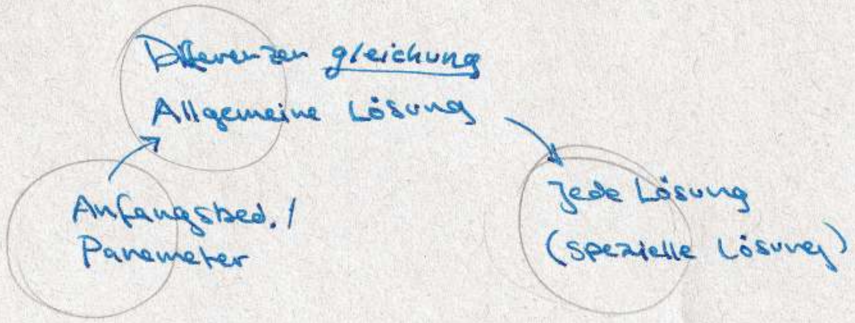


(vorgegeben)

$$\begin{pmatrix} n_0 = a_{n0} \\ n_1 = a_{n1} \end{pmatrix}$$

↑ Index: die Stelle in der Folge

← Wert



Linear, homogen, 1. Ordnung

Beispiel: allgemeine Lösung: $a_n = a_0 (1,06)^n$
spezielle Lösung: $a_n = 1000 (1,06)^n$ ... Anfangsbedingung $a_0 = 1000$

der Rekursion $a_n = a_{n-1} \cdot 1,06$

Es gilt:

$$a_n = c \cdot a_{n-1} \longrightarrow a_n = a_0 \cdot c^n$$

Differenzengleichungen → Beziehung zwischen Elementen einer Folge Tesen1

Autonom: unabhängig von n (nur konstante Werte)

Allgemeine Lösung: $n \longrightarrow f(n) \longrightarrow a_n$

Spezielle Lösung : Abhängig von Anfangsbedingungen

Linear: Ähnlich wie Polynom

Ordnung $\longrightarrow c_4 a_{n-4} + c_3 a_{n-3} + c_2 a_{n-2} + c_1 a_{n-1} + \boxed{g} \longrightarrow$ Inhomogener Teil
Störfunktion

Beispiel nicht linear:

$a_n = a_{n-1} + a^2_{n-3}$

$c_n = (1 - c_{n-1}) c_{n-2}$

Konstant wenn kein Koeffizient und nicht Störfunktion von n abhängen (g_n, c_n)

Lösungen 1. Ordnung

1. Ordnung, homogen

$a_n = c \cdot a_{n-1}$

$a_n = a_0 \cdot c^n$

1. Ordnung, inhomogen

$a_u = c \cdot a_{n-1} + g$

$a_n = a_0 c^n + \frac{1-c^n}{1-c} g$ (wenn c=1, weglassen)

1. Ordnung, inhomogen, nicht konstante Störfunktion

$a_n = c \cdot a_{n-1} + g_{n}$

$a_n = h_n + i_n$

homogene Lösung h_n : $a_0 \cdot c^n$

spezielle Lösung i_n :

* Fixpunkt $\bar{a}$ $|c| < 1$

$\bar{a} = \frac{g}{1-c}$

$c^n \longmapsto 0$

Beispiel:

$a_n = 3a_{n-1} + \underbrace{2n}$

g_n = Polynom Grad 1

$c = 3$

$a_0 = 3$

↓

$a_n = k \cdot 3^n - n - \frac{3}{2}$

$a_0 = k \cdot 3^0 - 0 - \frac{3}{2} = 3$

$k = \frac{9}{2}$

$a_n = k \cdot 3^n + i_n$ Selber Typ:

$i_n = 3 i_{n-1} + 2n$

Lösung: Polynom 1. Grades

$cn + d = 3(c(n-1)+d) + 2n$

⋮

$n(-2c-2) + (-2d+3c) = 0$

nur gültig für alle n wenn:

$c = -1$

$d = -\frac{3}{2}$

$i_n = -1n - \frac{3}{2}$

Spezielle Lsg !

von

$i_n = 3i_{n-1} + 2n$

Lösungen 2. Ordnung

Superpositionsprinzip: wenn $q(n)$, $p(n)$ 2 spezielle Lösungen sind von einer beliebigen homogenen linearen Differenzengleichung und keine Vielfachen voneinander sind

Kann man jede Lösung anhand einer Linearkombination schreiben:

$$\underset{\uparrow}{k_1 \underline{p(n)}} + \underset{\uparrow}{k_2 \underline{q(n)}}$$

Abhängig von Anfangsbedingungen

} Differenz von 2 spez. Lösungen erfüllt homogene Diff. Gleichung

Die Suche nach 2 geeigneten speziellen Lösungen durch Ansatz λ: $a_n = c_1 a_{n-1} + c_2 a_{n-2}$

homogen

$a_n = \lambda^n$

$a_n = c_1 a_{n-1} + c_2 a_{n-2} \quad n \geq 2$

$\lambda^n = c_1 \lambda^{n-1} + c_2 \lambda^{n-2}$ Charakteristische Gleichung

$\lambda^2 = c_1 \lambda + c_2$ Quadratische Gleichung

$\downarrow$

$\lambda_1 \neq \lambda_2 \in \mathbb{R} \quad a_n = k_1 \lambda_1^n + k_2 \lambda_2^n$

$\lambda_1 = \lambda_2 \in \mathbb{R} \quad a_n = (k_1 + k_2 n) \lambda^n$

$\lambda_1 \neq \lambda_2 \in \mathbb{C} \quad a_n = k_1 r^n \cos(n\varphi) + k_2 r^n \sin(n\varphi)$

Inhomogen, 2. Ordnung $a_n = c_1 a_{n-1} + c_2 a_{n-2} + g$ (Konstant)

inhomogen

$g_n = g$

$a_n = h_n + \bar{a}$

Wenn $|\lambda_1|$ und $|\lambda_2|$ beide < 1 dann $\longmapsto \bar{a}$

Fixpunkt $\bar{a} = c_1 \bar{a} + c_2 \bar{a} + g$

$$\bar{a} = \frac{g}{1 - c_1 - c_2}$$

Inhomogen, nicht konst. Störfunktion

nicht konst. Störfunktion

Bei beliebiger Ordnung:

$a_n = h_n + i_n$

Das Charakteristische Polynom von Grad k hat k-Nullstellen

→ k spezielle Lösungen ⟼ als Linearkombination allg. Lösung

Koeffizienten ≠ konst.
Nicht linear
} keine Lösung

Beispiel

Gegeben: $x_{n+2} - 2x_{n+1} + x_n = 5 + n + 4 \cdot 3^n$

$x_n^{(h)}$ homogene Lösung

$x_{n+2} - 2x_{n+1} + x_n = 0$

$\lambda^2 - 2\lambda + 1 = (\lambda - 1)^2 = 0 \longrightarrow x_n^{(h)} = (C_1 + C_2 \cdot n) \cdot 1^n = C_1 + C_2 n$

$\lambda_1 = \lambda_2 = 1$

$x_n^{(p)}$ partikuläre Lösung

Versuchslösung

Superpositionsprinzip:

wir zerlegen $5+n+4\cdot 3^n$ in

$S_n^{(1)} = 5+n \rightarrow$ linear Polynom $x_n^{(1)} = A_0 + A_1 n$

$S_n^{(2)} = 4 \cdot 3^n \rightarrow$ exponent $y_n^{(2)} = A \cdot 3^n$

$A \cdot 3^{n+2} - 2A\, 3^{n+1} + A\, 3^n =$

$4\, A\, 3^n = 4\, 3^n$

$A = 1 \quad x_n^{(2)} = 3^n$

Resonanzfall: mit n multiplizieren weil

$A_0 + A_1 n \cong C_1 + C_2 n$

$\downarrow$

$A_0 n + A_1 n^2$

$\downarrow$

$\boxed{A_0 n^2 + A_1 n^3}$

Einsetzen in

$x_{n+2} - 2x_{n+1} + x_n = 5 + n$

$A_0(n+2)^2 + A_1(n+2)^3 -$

$2\left(A_0(n+1)^2 - A_1(n+1)^3\right) +$

$A_0 n^2 + A_1 n^3 = 5 + n$

$2A_0 + 6A_1 = 5$

$6A_1 = 1$

$A_1 = \frac{1}{6} \quad A_0 = 2$

$x_n^{(1)} = 2n^2 + \frac{1}{6}n^3$

Schließlich:

$x_n = x_n^{(h)} + \overset{(p)}{x_n^{(1)}} + \overset{(p)}{y_n^{(2)}}$

$= C_1 + C_2 n + 2n^2 + \frac{1}{6}n^3 + 3^n$

Bestimmung von $x_n^{(p)}$

(Fortsetzung Ordnung 2)

ii) „Methode des unbestimmten Ansatzes"

$$x_{n+2} + a\,x_{n+1} + b\,x_n = s_n$$

Ansatz abhängig von Störfunktion wählen

Gleichgewichtspunkt / Fixpunkt bei Ordnung 2

$$\bar{a} = C_1 \bar{a} + C_2 \bar{a} + g \text{ (nicht } g_n) \rightarrow \text{konstant}$$

Tesch

$$\bar{a} = \frac{g}{1 - C_1 - C_2}$$

$a_n = h_n + \bar{a}$

für

$a_n = C_1 a_{n-1} + C_2 a_{n-2} + g$

Ist S_n konstant dann führt der „unbestimmte Ansatz" $A = x_n^{(p)}$ auf die konstante Lösung $x_n^{(p)} = \frac{s}{1+a+b}$

Ist S_n nicht konstant dann führt der „unbestimmte Ansatz" A nach dem Typ von S_n in Form einer „Versuchslösung" mit unbest. Koeffiz. zum Einsetzen zur Partikulärlösung.

S_n	Versuchslösung $x_n^{(p)}$
1	A
r^n	Ar^n
$\sin(rn)$ oder $\cos(rn)$	$A \sin(rn)$ oder $A \cos(rn)$
n^k oder Polynom Grad k	$A_0 + A_1 n + A_2 n^2 + \ldots + A_k n^k$
$r^k \cdot r^n$	$r^n \cdot \odot$

Resonanzfall

wenn $x_n^{(p)}$ eine Funktion enthält die in $y_n^{(h)}$ ist, Ansatz mit n multiplizieren

Superpositionsprinzip

$x_{n+2} + a\,x_{n+1} + b\,x_n = c_1 s_n^{(1)} + c_2 s_n^{(2)}$ Inhomogene DGL

$x_n^{(1)}, x_n^{(2)}$ Lösungen (partikulär)

$x_n = c_1 x_n^{(1)} + c_2 x_n^{(2)}$ Ebenfalls Partikuläre Lösung mit Störfunktion $c_1 s_n^{(1)}, c_2 s_n^{(2)}$

2. Ordnung

$x_{n+2} + a\,x_{n+1} + b\,x_n = \boxed{S_n}$ → Störfunktion

Bestimmung von $x_n^{(h)}$

Lösungen $x_n^{(1)}, x_n^{(2)}$ nur gültig wenn

$$\begin{vmatrix} x_0^{(1)} & x_0^{(2)} \\ x_1^{(1)} & x_1^{(2)} \end{vmatrix} \neq 0$$

charakteristische Wurzeln λ_1, λ_2 bei Ansatz $\lambda^n = a_n$

i) $\lambda_1 \neq \lambda_2 \in \mathbb{R}$ $\quad x_n = C_1 \lambda_1^n + C_2 \lambda_2^n$

ii) $\lambda_1 = \lambda_2 \in \mathbb{R}$ $\quad x_n = C_1 \lambda_1^n + C_2 \lambda_1^n = (C_1 + C_2)\lambda_1^n$

iii) $\lambda_1 \cdot \lambda_2 \in \mathbb{R}$ $\quad \lambda_{1,2} = r \cdot (\cos\varphi \pm i \cdot \sin\varphi)$

$\lambda_1, \lambda_2 \in \mathbb{C}$

$$x_n = C_1 \cdot r^n (\cos n\varphi \,\textcircled{+}\, i \sin n\varphi) + C_2\, r^n (\cos n\varphi \,\textcircled{-}\, i \sin \varphi \cdot n) =$$

$$= r^n \Big(\underbrace{(C_1 + C_2)}_{D_1} \cos n\varphi + \underbrace{i\,(C_1 - C_2)}_{D_2} \sin n\varphi \Big)$$

$$x_n = r^n \left(D_1 \cos n\varphi + D_2 \sin n\varphi \right)$$

Beispiel

Fibonacci-Folge

$N_t = N_{t-1} + N_{t-2}$ $\quad$ Anfangswerte $N_0 = N_1 = 1$

$\lambda_{1,2} = \frac{1 \pm \sqrt{5}}{2}$

$N_t = C_1 \left(\frac{1 \pm \sqrt{5}}{2}\right)^t + C_2 \left(\frac{1 - \sqrt{5}}{2}\right)^t$

$C_1 = \frac{1 + \sqrt{5}}{2\sqrt{5}}$

$C_2 = \frac{-1 - \sqrt{5}}{2\sqrt{5}}$

Explizit:

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

Bestimmung von $x_n^{(p)}$

i) „Variation der Konstanten"

Beispiel

$$x_{n+1} = (n+1)x_n + 3(n+1)! \quad n \geq 0$$ Differenzengleichung

$$x_n^{(h)} = C\,n!$$ Homogene Allgemeinlösung

$$x_n^{(p)} = \boxed{C_n\, n!}$$ Ansatz

$$\downarrow$$

$$x_{n+1} = (n+1)x_n + 3(n+1)!$$

$$\underbrace{C_{n+1}(n+1)!}_{} = (n+1)\underbrace{C_n\, n!}_{} + 3(n+1)!$$

$$C_{n+1} = C_n + 3$$

wir wählen $C_0 = 0$

$$C_n = 3n$$

Δ Nebenrech.

$$\left(\begin{array}{l} x_n = x_{n-1} + 3 \\ x_n = 3n + a_0 \quad \text{also } x_n = 3n + \end{array} \right)$$

Daraus folgt:

$$x_n = x_n^{(h)} + x_n^{(p)} = \underbrace{C \cdot n!}_{} + \underbrace{3n \cdot n!}_{} = (c + 3n)\, n!$$

Beispiel

$$v_{n+1} = \frac{n+2}{n+1} v_n + 2$$

$$v_n^{(h)} = C \prod_{i=1}^{n-1} \frac{i+2}{i+1} = c\, \frac{n+1}{2}$$

$$v_n^{(p)} = C_n \frac{n+1}{2} \longrightarrow$$

$$v_{n+1} = \frac{n+2}{n+1} v_n + 2$$

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

$$\vdots$$

$$C_{n+1} = C_n + \frac{4}{n+2}$$

$$C_n = \sum_{l=1}^{n-1} \frac{4}{l+2} = \boxed{4\left(H_{n+1} - \frac{3}{2}\right)}$$

$$v_n^{(p)} = 4\left(H_{n+1} - \frac{3}{2}\right) \frac{n+1}{2} =$$

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

$v_1 = 0 \quad C = 0$

$$v_1 = 0 = \frac{1+2}{1+1} v_0 + 2$$

$$= \frac{3}{2} v_0 + 2$$

$$v_n = (2n+1)\left(H_{n+1} - \frac{3}{2}\right)$$

Differenzengleichungen

Lösungsgesamtheit : $\underset{\text{Allgemeine Lsg}}{x_n^{(h)}} + \underset{\text{partikulär Lsg (beliebig)}}{x_n^{(p)}} = x_n$

1. Ordnung

$$x_n = a^n \cdot x_0 + b \frac{a^n - 1}{a - 1}$$ -> allgemeine Lsg von $x_n = a\,x_{n-1} + \boxed{b}$ konstant

Beispiel

$$x_n = 2x_{n-1} + 1$$

$a = 2$
$b = 1$ $\rightarrow x_n = 2^n \cdot x_0 + 1\,\frac{2^n - 1}{2 - 1} = 2^n \underbrace{(x_0 + 1)} - 1 = 2^n \cdot C - 1$

C damit man Anfangswert nicht festlegen muss und bei x_3 anfangen kann bsws statt x_0

Angenommen $x_1 = 1$

$x_1 = 1 = 2^1 \cdot C - 1$ $\quad C = 1$

Berechnung von
$x_n^{(h)} = C \cdot \prod_{i=0}^{n-1} a_i$ für 1. Ordnung:

$$x_n = \underline{x_0} \cdot a_0 \cdot a_1 \cdot a_2 \cdot a_3 \cdot \ldots \cdot a_n =$$

$$= x_0 \cdot \prod_{i=0}^{n-1} a_i = \underbrace{x_0}_{C} \cdot a^n \text{ wenn } a = \text{konst.}$$

Beispiel

$$x_{n+1} = (n+1)\,x_n \quad n \geq 0$$

$$x_n^{(h)} = C \cdot \prod_{i=0}^{n-1} (i+1) = C\boxed{n!} \leftarrow x_3 = x_0 \underbrace{(0+1)}_{1} \underbrace{(1+1)}_{2} \underbrace{(2+1)}_{3} = x_0 \cdot \boxed{3!}$$

$x_n = 2n!$ wenn $x_0 = 2$

Aber weil es keine Störfunktion (inhomogenen Teil) gibt, benötigt man kein $x_n^{(p)}$

Wenn aber eine Störfunktion vorhanden ist, benötigt man eine Partikulärlösung.

Lineare Algebra – Vektoren

Vektorraum

- Multiplikation mit einem Skalar → abgeschlossen
- Vektoraddition → abgeschlossen

Linearkombination

$$\sum_{j=1}^{m} k_j \vec{a}_j = k_1 \vec{a}_1 + k_2 \vec{a}_2 + \ldots + k_m \vec{a}_m$$

- Die Menge der Vektoren ist linear unabhängig wenn die triviale Lösung $k_1 = k_2 = k_3 = \ldots = k_m = 0$ die einzige Lösung ist sodass die Linearkombination 0 ergibt. → Basis
- Linear abhängig genau wenn Vektoren vielfache voneinander sind

→ wichtig: es müssen nicht alle linear unabhängig sein:

Beispiel
$$\underbrace{k_1 \begin{pmatrix} 1 \\ 0 \end{pmatrix} + k_2 \begin{pmatrix} 0 \\ 1 \end{pmatrix}}_{\text{unabhängig}} + k_3 \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

Es gibt eine maximale Menge an Basisvektoren pro Vektorraum: Dimension dim(V)
Mit dieser Menge lässt sich jeder beliebige Vektor durch die Änderung der Koeffizienten / Koordinaten entwickeln

Jede Menge von linear unabhängigen Vektoren = minimales Erzeugenden-System
Klassisches Beispiel: kanonische Basisvektoren e_1, e_2, e_n

Teilräume $U \subseteq V$ (Untervektorräume)

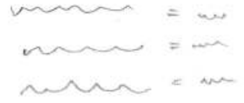
$$LH\{a_1, \ldots, a_m\} = \left\{ \sum_{j=1}^{m} k_j \vec{a}_j \mid k_j \in \mathbb{K} \right\} \subseteq V$$

Lineare Hülle
\# der Elemente in der linearen Hülle die Unterraum aufspannen = dim(U)

Kriterium:
$\vec{a}, \vec{b} \in U \rightarrow \vec{a} + \vec{b} \in U$
$\vec{a} \in U \rightarrow k \cdot \vec{a} \in U$

Lineare Algebra – Lineare Gleichungen

Lineares Gleichungssystem
über $\mathbb{K}$



$A \boxed{\vec{x}} = \vec{b}$

↑

Lösung lässt sich mit
Gauß-Jordan Algorithmus berechnen

$(A \mid \vec{b})$

Auch inverse Matrix! A^{-1}

$$\underset{\substack{\uparrow \\ \text{umformen}}}{(A \mid \mathbb{I})} \longrightarrow \underset{\substack{\uparrow \\ \text{Lösung}}}{(\mathbb{I} \mid A^{-1})}$$

„Rang" rg(A)

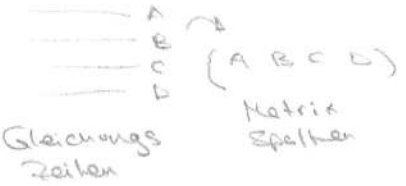
Zeilen / Spaltenrang = # der linear unabhängigen Zeilen / Spalten

Nullvektor by default abhängig

Gleichungssystem lösbar, wenn $\overset{\text{(Spalten)}}{\text{rang}(A)} = \overset{\text{(Spalten)}}{\text{rang}(A \vec{b})}$.

(erweiterter Koeffizienten-Matrix)

[weil sich $\vec{b}$ als Linearkombination der Spalten von A schreiben lassen sollte.]



wenn Rang der Matrix = # der Gleichungen

„Bild" Bild(A)

$\text{Bild}(A) = \{ A x \mid x \in \underbrace{\mathbb{K}^n}_{} \} \subseteq \underbrace{\mathbb{K}^m}_{}$ $\qquad F : \underbrace{\mathbb{K}^n}_{} \longmapsto \underbrace{\mathbb{K}^m}_{}$

(Abbildung) $\qquad F(x) = A x$

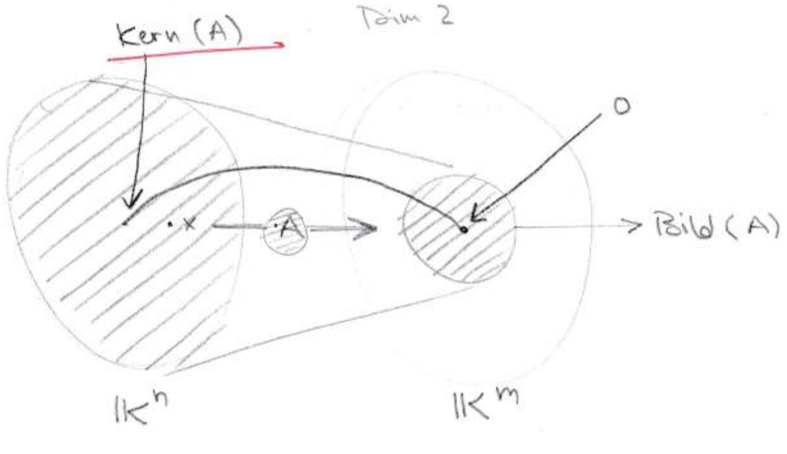
Teilraum von $\mathbb{K}^m$

der von den Spalten von A aufgespannt wird

Beispiel: $A = \begin{pmatrix} 0 & 1 \\ 2 & 6 \end{pmatrix}$

$\text{Bild}(A) = LH \underbrace{\left\{ \begin{pmatrix} 0 \\ 2 \end{pmatrix}, \begin{pmatrix} 1 \\ 6 \end{pmatrix} \right\}}_{\text{Dim } 2}$

$\dim(\text{Bild}(A)) = \text{rang}(A)$



⇒ Alle Elemente aus $K^n \cdot A$
⇒ Funktion Ax in $\mathbb{K}^m$.

Wenn $\text{Bild}(A) \not\subseteq \mathbb{K}^m$ sondern
$\text{Bild}(A) = \mathbb{K}^m$

„Kern A"

$$\ker(A) = \{ x \mid Ax = 0 \} \subseteq \mathbb{K}^n$$

$$Ax = 0$$

Alle Vektoren die auf 0 abgebildet werden.

Beispiel:

„Bestimmen Sie $\ker(A)$"

$$A = \begin{pmatrix} 1 & 1 & 2 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$$

$$Ax = 0$$

$$\boxed{\begin{matrix} x_1 + x_2 + 2x_3 = 0 \\ x_2 + x_3 = 0 \\ x_1 + x_3 = 0 \end{matrix} \xrightarrow{\text{Gauß Algorit.}} \begin{matrix} x_1 + x_3 = 0 \\ x_2 + x_3 = 0 \\ 0 = 0 \end{matrix}}$$

wenn $x_3 = t \in \mathbb{R}$

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} -t \\ -t \\ t \end{pmatrix}$$

Lösung!

$$\operatorname{Ker}(A) = LH\left\{ \begin{pmatrix} -1 \\ -1 \\ 1 \end{pmatrix} \right\}$$

Dimension 1

---

wenn $Ax = b$

$b \in \mathbb{K}^m$

$F: \mathbb{K}^n \longmapsto \mathbb{K}^m$

- Zumindest 1 Lösung wenn $b \in \text{Bild}(A)$
- Und man erhält alle anderen Lösungen durch

$x_0 + \text{Kern}(A) = x$

eindeutig wenn $\dim(\text{Kern}(A)) = 0$

Rangsatz

$$\underbrace{\dim(\text{Kern}(A))}_{\text{„Defekt"}} + \dim(\text{Bild}(A)) = n$$

Lineare Algebra – Matrizen und Lineare Abbildungen

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & & \vdots \\ \vdots & & \ddots & \\ a_{m1} & \cdots & & a_{mn} \end{pmatrix}$$

$A^{m,n}$ … m×n Matrix … ← Dimension

m = Zeile

n = Spalte

„Quadratische Matrix" … Zeilenanzahl = Spaltenanzahl

„Transponierte Matrix" … A^T

$$\begin{pmatrix} 1 & 3 & 5 \\ 2 & 4 & 6 \end{pmatrix}^T = \begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{pmatrix} \qquad (a_{ij})^T = (a_{ji})$$

hier:

11 → 11   21 → 12

12 → 21   22 → 22

13 → 31   23 → 32

✓

→ wenn $A = A^T$ → symmetrisch

„Adjungierte Matrix" … A^*

A^T und komplex konjugiert

„Einheitsmatrix" … $\mathbb{I}_n$

$(\vec{e}_1, \vec{e}_2, \vec{e}_3 \ldots \vec{e}_n)$

„Inverse Matrix" … A^{-1}

singulär ——— nicht invertierbar

regulär ——— invertierbar

→ jede Matrix hat nur 1 Inverses

$A \cdot A^{-1}$ oder $A^{-1} \cdot A = \mathbb{I}$

lässt sich mit einem Gleichungs-System berechnen oder

$Ax = B$

$x = B \cdot A^{-1}$

Lineare Abbildungen

$F: \mathbb{K}^n \longmapsto \mathbb{K}^m$ ← Vektorräume

$x \in \mathbb{K}^n \rightsquigarrow y = F(x) \in \mathbb{K}^m$

Anwendungsgebiet:

„Drehmatrix", Dreht Input um $\alpha°$

$$A = \begin{pmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{pmatrix}$$

$F(x) = A\,x$

„Verkettete Abbildungen"

$F: \mathbb{K}^l \longrightarrow \mathbb{K}^n \quad F(y) = \underline{A}y$

$G: \mathbb{K}^m \longmapsto \mathbb{K}^l \quad G(x) = \underline{B}x$

$$\left.\begin{matrix} F \circ G: \mathbb{K}^m \longrightarrow \mathbb{K}^n \\ \mathbb{K}^m \longmapsto \mathbb{K}^l \longmapsto \mathbb{K}^n \end{matrix}\right\} (F \circ G)(x) = \underline{AB}x$$

Bedingung:

$F(a + b) = F(a) + F(b)$

$F(k a) = k f(a)$

„Linear" wenn

$F(x) = A x$

jede Spalte von A lässt sich mit den Bildern der Standardbasisvektoren bestimmen:

$$A = \left(F(e_1), F(e_2), F(e_3), \ldots, F(e_n) \right)$$

„Affin" wenn

$F(x) = Ax + b$

„Umkehrbar" wenn

bei lineare Abbildung

$F(x) = Ax$ ein A^{-1} existiert

Sodass $x = A^{-1}y$

(auch linear)

Determinante

Es gilt: $\det(A) = \det(A^T)$

Zeile und Spalte kein Unterschied

„Entwicklung von Laplace"

Vorzeichenmatrix

$$\begin{pmatrix} + & - & + & - \\ - & + & - & \\ + & - & \dots & \\ - & & & \end{pmatrix} \leftarrow \pm a_{i1} \cdot \underbrace{\det(A^{i1})}_{\text{Matrix ohne Zeile } i\text{, Spalte } 1} \pm a_{i2} \cdot \det(A^{i2}) \dots$$

Invertierbarkeit

Quadratische Matrix A invertierbar genau dann wenn $\det(A) \neq 0$

Bedeutet eindeutige Lsg für $Ax = b$ weil $x = b A^{-1}$!

Beispiel: Bestimmen Sie λ sodass $x \neq \begin{pmatrix} 0 \\ 0 \end{pmatrix}$!

$$A = \begin{pmatrix} 1-\lambda & 2 \\ 2 & 1-\lambda \end{pmatrix}$$

$$\boxed{Ax = 0}$$

wenn $x = 0 \cdot A^{-1}$ und Matrix invertierbar ist, kann nur $\begin{pmatrix} 0 \\ 0 \end{pmatrix} = x$ die Lösung sein.

gesucht: λ sodass $\left| \begin{array}{l} A \neq \text{invertierbar} \\ \det(A) = 0 \end{array} \right.$

$$\det(A) = \underbrace{(1-\lambda)^2 - 4}$$

$$\begin{vmatrix} 1-\lambda & 2 \\ 2 & 1-\lambda \end{vmatrix}$$

→ Quadr. Gleich.; soll 0 ergeben

$\lambda_1 = -1$

$\lambda_2 = 3$ ✓

Inverse Matrix nach Formel

$$A^{-1} = \frac{1}{\det(A)} \cdot \tilde{A}$$

← Komplementäre Matrix mit Koeffizienten

$$\tilde{a}_{jk} = \underbrace{(-1)^{j+k}}_{\text{Vorzeichen}} \det(A^{kj})$$

erfüllt:

$$\tilde{A} \cdot A = A \cdot \tilde{A} = \det(A) \cdot \mathbb{I}$$

Eigenschaften der Determinante

- Zeile / Spalte nur 0 $\longrightarrow$ $\det(A) = 0$
- Zeile / Spalte$_1$ = Zeile / Spalte$_2$ $\longrightarrow$ $\det(A) = 0$
  oder linear abhängig
- $\det(kA) = \underset{\uparrow}{k^{\boxed{n}}} \det(A)$
  [n×n Matrix A]

$\det(A^{-1}) = \det(A)^{-1}$
aber $\det(AB) = \det(A) \cdot \det(B)$

(
- $\det(kA) \neq k\det(A)$
- $\det(A+B) \neq \det(A) + \det(B)$ $\longrightarrow$ (keine lineare Abbildung)
)

- Vertauschung von 2 Zeilen ändert Vorzeichen
- Multiplizieren einer Zeile mit k $\rightarrow$ $\det(A) \cdot k$
- Elementare Zeilenoperation $\rightarrow$ keine Auswirkung!

Wichtig:

$\det\underbrace{(\triangledown)}_{\text{Dreieckes Matrix}}$ = Produkt der Diagonalelemente

Beispiel

$$\begin{pmatrix} 2 & 1 & 3 \\ 4 & 0 & 5 \\ 7 & 6 & 8 \end{pmatrix} \rightarrow \begin{pmatrix} 2 & 1 & 3 \\ & -2 & -1 \\ & & -\frac{15}{4} \end{pmatrix} \rightarrow \det(A) = 2 \cdot (-2) \cdot \left(-\frac{15}{4}\right)$$

Skalarprodukt und Orthogonalität

Multiplikation von Vektoren

$\langle a, b\rangle = a^T \cdot b = a_1 b_1 + a_2 b_2 + a_3 b_3 \ldots$ = Skalar $\in \mathbb{R}$
Produkt

$\left.\begin{array}{l}\langle a, Ab\rangle = \langle A^T a, b\rangle \\ \langle Aa, b\rangle = \langle a, A^T b\rangle\end{array}\right\}$ wenn A quadratisch
Verschiebung von links $(A m, m)$ nach rechts $(m, A m)$

Länge / Norm von Vektor

$\overset{\shortparallel}{\text{Norm}}$

$\|\vec{a}\|^2 = \langle a, a\rangle$

Winkel

$\langle a, b\rangle = \|a\| \|b\| \cdot \cos(\underbrace{\varphi}_{})$

der kleinere Winkel zwischen a, b in der von ihnen aufgespannten Ebene

Erklärung:

α = Winkel zwischen $\vec{a}$ und x-Achse

$\vec{a} = (\|a\| \cdot \cos(\alpha), \|a\| \sin(\alpha))$

$\vec{b} = (\|b\| \cdot \cos(\alpha), (\|b\| \sin(\alpha))$

rechter Winkel

orthogonal $a \perp b$ wenn $\langle a, b\rangle = 0$ $\Longrightarrow \|a+b\|^2 = \|a\|^2 + \|b\|^2$

parallel $a \parallel b$ wenn $ka = b$

orthogonale Projektion

orthogonale Projektion eines Vektors in eine vorgegebene $\underbrace{\text{Richtung}}_{}$

bestimmt durch Einheits-Vektor e $(|e| = 1)$

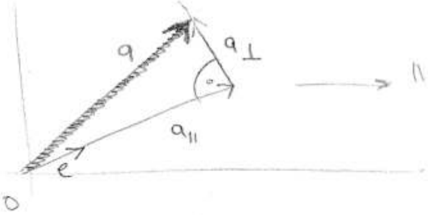
a wird in 2 Komponenten zerlegt:

$a = a_{\parallel} + a_{\perp}$

$\uparrow$ Parallel zu e (vielfaches von e)

$\uparrow$ Orthogonal zu e $\left(\begin{array}{l}\langle a_{\perp}, e\rangle = 0 \\ a_{\perp} = a - \langle e, a\rangle e\end{array}\right)$

$\longrightarrow a_{\parallel} \perp a_{\perp}$ $\langle a_{\parallel}, a_{\perp}\rangle = 0$



$\longrightarrow \|a\|^2 = \|a_{\parallel}\|^2 + \|a_{\perp}\|^2$

$a = a_{\perp} + a_{\parallel}$

Definition: |Projektionslänge von a auf e|

$a_{\parallel} = \overbrace{\langle e, a \rangle}\, e$ („Orthogonale" Projektion von a Richtung e

$a_{\perp} = a - \langle e, a \rangle e$ orthogonales Komplement von a Richtung e

$U^{\perp} = \{ a \in V \mid a \perp b$ für $\forall b \in U \}$ $U \subseteq V$

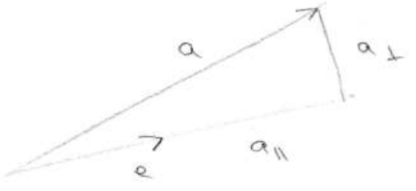
„Orthogonaler Komplement von U"

Alle Vektoren die auf Menge U orthogonal stehen.

weiters gilt

$a_{\parallel} \in LH\{e\}$

$a_{\perp} \in LH\{e\}^{\perp}$



$\|a\|^2 = \|a_{\parallel}\|^2 + \|a_{\perp}\|^2$

$\|a_{\parallel}\| \leq \|a\|$

Cauchy-Schwarz-Ungleichung

$b = \|b\| \cdot e$ ← Richtungsvektor $\|e\| = 1$

$|\langle a, b \rangle| = \underbrace{|\langle a, \|b\| e \rangle|}_{\text{Projektionslänge von a auf (b)} = \|b\| \cdot e} = \|b\| \cdot \underbrace{|\langle a, e \rangle|}_{\text{Projektionslänge a auf e mal b}} = \|b\| \cdot \underbrace{\|a_{\parallel}\|} \leq \|b\| \cdot \|a\|$

$\uparrow$ $= |\langle a, e \rangle|$ Projektionslänge a auf $e \cdot \|b\|$

$\underbrace{|\langle a, b \rangle|}_{\text{Projektion von a auf b}} \leq \|a\| \cdot \|b\|$

Projektion von a auf b $\leq$ Länge $\|a\|$ · Länge $\|b\|$

$\|a_{\parallel}\|$ als Näherung zu a

$\|e\| = 1$ normierter Einheitsvektor $x \in LH\{e\}$ (vielfaches von e)

$x = k \cdot e$

$\underbrace{\|a - x\|} \geq \|a_{\perp}\|$

→ Abschätzungsfehler = 0 wenn $x = a_{\parallel}$ weil $\|a - a_{\parallel}\| = \|a_{\perp}\|$

(wenn durch x approximiert wird)

Normalvektoren

in $\mathbb{R}^2$: Normalvektor von $e = (e_1, e_2)$:

$$\left.\begin{array}{l} \rightarrow n = (e_2, -e_1) \\ \rightarrow -n = (-e_2, e_1) \end{array}\right\} \langle e, n \rangle = 0$$

Parameterform → Normalvektorform

$\mathbb{R}^2$

Gerade

$\begin{pmatrix} x \\ y \end{pmatrix} = a + k \cdot \vec{e}$

e ... Richtungsvektor (e_1, e_2)

a ... Punkt (eigentlich $\overrightarrow{OA}$) (a_1, a_2)

n ... Normalvektor (n_1, n_2)

↳

$n_1 x + n_2 y = c$

$(c = a_1 n_1 + a_2 n_2)$ → wenn $\|n\| = 1$ dann ist das die Hess'sche Normalform der Gerade

In dieser Form ist $|c|$ der Abstand der Gerade vom Ursprung.

$\mathbb{R}^3$

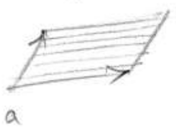
Ebene

$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = a + k_1 e_1 + k_2 e_2$

e_1, e_2 Richtungsvektor ... (e_1, e_2, e_3)

a ... Ortsvektor .... (a_1, a_2, a_3)

n ... Normalvektor .... (n_1, n_2, n_3)



↳

$x n_1 + y n_2 + z n_3 = c$

$(c = a_1 n_1 + a_2 n_2 + a_3 n_3)$ → wenn $\|n\| = 1$ Hess'sche Normalform der Ebene

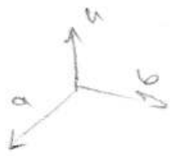
$|c|$ ... Abstand zum Ursprung

Wichtig

Gerade lässt sich nicht in Normalform in $\mathbb{R}^3$ angeben.

Deshalb nimmt man 2 Ebenen in Normalform die eine Gerade als Schnitt haben.

Vektorkreuzprodukt in $\mathbb{R}^3$



Normalvektor u von a und b

- $$a \times b = \begin{pmatrix} a_2 b_2 - a_3 b_2 \\ -(a_1 b_3 - a_2 b_1) \\ a_1 b_2 - a_2 b_1 \end{pmatrix}$$ wobei $a = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix}$ $b = \begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix}$

  $a, b \in \mathbb{R}^3$

  $a \nparallel b$

- $$\|a \times b\| = \|a\| \cdot \|b\| \, \underbrace{|\sin \varphi|}_{\text{Winkel zwischen a und b}}$$

- $a \times b = -b \times a$

Hyperebene (Verallgemeinerung)

n = Einheitsvektor in $\mathbb{R}^n$

$\langle x, n \rangle = x_1 n_1 + \ldots + x_n n_n = c$ „Normalform der Hyperebene"

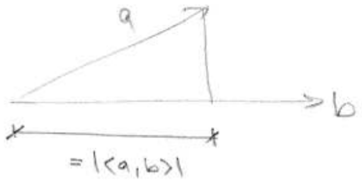
Falls $n = 3$ Ebene, $n = 2$ Gerade $\Big\}$ mit Normalvektor $\vec{n}$

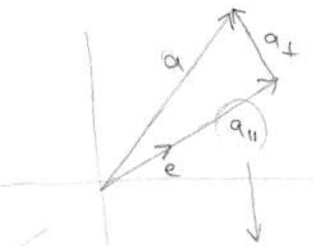
$|c|$ = Abstand der Hyperebene vom Ursprung

Cauchy-Schwarz-Ungleichung

$$\underbrace{|\langle a, b\rangle|}_{\text{Projektionslänge von a auf b}} \leq \|a\| \, \|b\|$$

↑ Gleichheit wenn a ∥ b





als Approximation zu a

Definition:

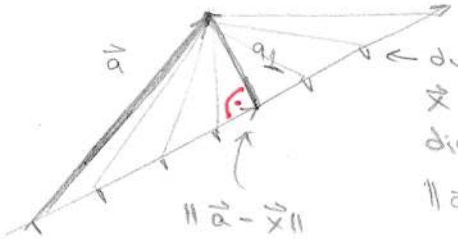
$\|\vec{e}\| = 1$

$x \in LH\{\vec{e}\}$

$\vec{x} = k \cdot \vec{e} \longrightarrow$ mit k kann $\vec{x} = \vec{a}_\parallel$

Es gilt:

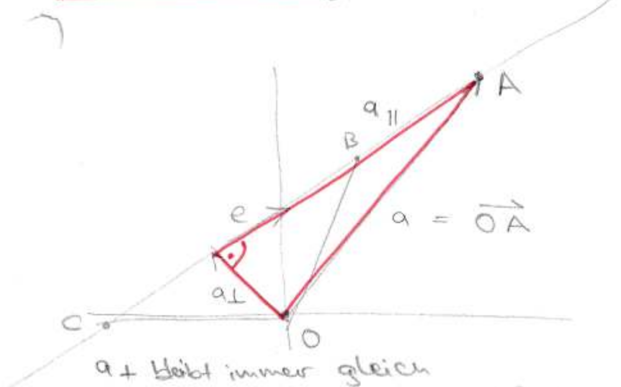
$\|\vec{a} - \vec{x}\| \geq \|a_\perp\|$



← durch verschiedene $\vec{x}$ ändert sich die Länge von $\|\vec{a} - \vec{x}\|$

$\|\vec{a} - \vec{x}\|$ ist am kürzesten wenn $= \|a_\perp\|$ und $\vec{x} = a_\parallel$

Bestimmung des Abstandes vom Ursprung $\vec{O}$



$a_\perp$ bleibt immer gleich (gilt für jeden Ortsvektor $\vec{OA}$)

Wenn man Abstand von $\vec{e}$ zu O bestimmen möchte ist $\vec{a}_\perp$ für jeden Ortsvektor $\vec{a}$ der auf einem Punkt A auf der Gerade $a_\parallel$ ist, immer gleich

und der kürzeste Weg!

$\|a_\perp\|$ = kürzester Abstand der Gerade zum Ursprung!

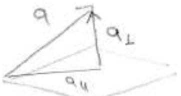
$a_\perp$ ist der Normalvektor der Gerade $a_\parallel$.

Satz:

Sei $u_1, \ldots u_m \in V$ ein Orthonormalsystem gilt für jeden $x \in LH\{u_1, \ldots u_m\}$:

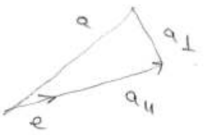
$\|a - x\| \geq \|a_\perp\|$

$\|a - a_\parallel\| \boxed{=} \|a_\perp\|$



Wenn man Ebene nicht verlassen darf ist $a_\parallel$ die beste Annäherung

Orthogonalentwicklungen



Bisher: Zerlegung bezüglich $\vec{e}$

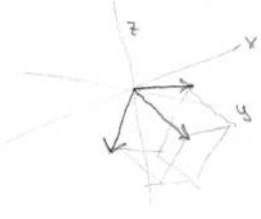
Jetzt : Zerlegung bezüglich $u_1 \dots u_m$

„Orthonormalsystem" aus Orthonormalbasis

Wie Basisvektoren nur $u_1, u_2, \dots, u_m \in V$ mit Länge 1 und normal zueinander

$$\langle u_j, u_k \rangle = \begin{cases} \text{wenn } u_j = u_k \ \dots 1 \\ \text{wenn } u_j \neq u_k \ \dots 0 \end{cases}$$

→ können verdrehte Koordinatenachsen sein



Linear unabhängig und max. Anzahl = Dim(V)

Orthogonalentwicklung

Vektor wird nicht mit Linearkombination sondern mit Orthogonalentwicklung zerlegt.

$$\vec{a} = \sum_{j=1}^{n \leftarrow \dim(V)} \underbrace{\langle u_j, a \rangle}_{\substack{\text{Projektions} \\ \text{Länge} \\ \text{auf } u_j}} \cdot \underbrace{u_j}_{\text{Richtung}}$$

kanonische Basis

Beispiel: $\left.\begin{matrix} u_1 = e_1 \\ u_2 = e_2 \\ u_3 = e_3 \end{matrix}\right\} \# = 3$

$$\vec{a} = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} = \sum_{j=1}^{3} \langle u_j, a \rangle \cdot u_j =$$

Projektionslänge + Richtung

X - Achse $\langle u_1, a \rangle \cdot u_1 +$

y - Achse $\langle u_2, a \rangle \cdot u_2 +$

Z - Achse $\langle u_3, a \rangle \cdot u_3$

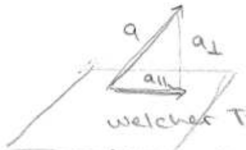
(Wenn man nicht nach allen n Dimensionen entwickelt sondern $m < n$
→ Teilraum von V)

↓

Vektor = (Komponente im Teilraum) + (Komponente außerhalb von Teilraum)

$a_\parallel$ $a_\perp$

$$a_\parallel = \sum_{j=1}^{m} \langle u_j, a \rangle u_j \qquad a_\perp = a - a_\parallel$$



welcher Teil des Vektors würde aus $\mathbb{R}_2$ bestehen?

$a_\parallel \in LH\{u_1, \dots, u_m\}$

↪ Orthogonale Projektion von $\vec{a}$ auf $LH\{u_1 \dots u_m\}$ → quasi Schatten

$a_\parallel$

Wichtig: $a_\perp$ = kürzester Abstand von a zu Teilraum

$a_\perp \in LH\{u_1, \dots, u_m\}^\perp$ → damit auch $a_\parallel$

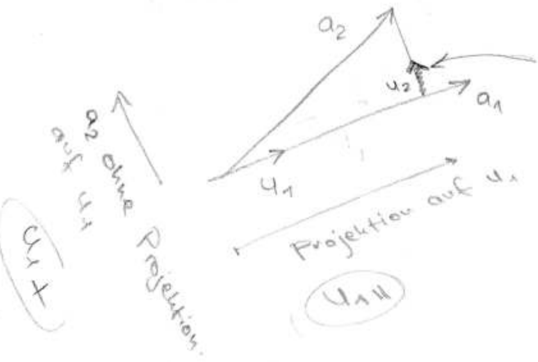
Wie man ein Orthonormalsystem aus linear unabhängigen Orthonormalbasis bilden kann!

[$a_1, a_2, a_3, a_4, \dots, a_m$: beliebiger linear unabhängiger Vektor]

$$u_1 = \frac{a_1}{\|a_1\|}$$ → Länge auf 1 normiert

$$u_2 = \frac{a_2 - \langle u_1, a_2 \rangle u_1}{\|a_2 - \langle u_1, a_2 \rangle u_1\|}$$

Bildet Vektor, der normal zu u_1 steht (wird normiert auf 1)



$$\overbrace{a_2 - \underbrace{\langle u_1, a_2 \rangle \cdot u_1}_{\text{Projektion auf } u_1}}$$

Wiederholen bis dim(V):

Gram-Schmidt-Verfahren

$a_1, a_2, \dots, a_m \in V$

linear unabhängige Vektoren

$$v_k = \frac{a_k - \sum_{j=1}^{k-1} \langle u_j, a_k \rangle u_j}{\| \text{——} \| \text{——} \|} \qquad 1 \leq k \leq m$$

→ Bildet Orthonormalsystem mit gleicher linearer Hülle

$LH \{a_1, \dots, a_{\underline{k}}\} =$

$LH \{u_1, \dots, v_{\underline{k}}\}$

Lineare Unabhängigkeit der a_m muss nicht geprüft werden.

→ wenn a_1, a_2 linear abhängig sind:

$a_2 - \langle u_1, a_2 \rangle u_1 = 0$ $\qquad \longmapsto$ ← Projektion = Vektor selbst.

Wenn $a_1 = k \cdot a_2$ dann ergibt die Projektion immer ein vielfaches der anderen

Orthogonale Transformationen

U = reele quadratische Matrix

wenn $U^T = U^{-1}$ → „U = orthogonale Matrix"

Lineare Abbildung, die dazu gehört:

$F: V \to V$

$F(x) = Ux$

„orthogonale Transformation"

- erhaltet Skalarprod:

$\langle Ua, Ub \rangle = \langle a, b \rangle$

$\langle Ua, Ub \rangle =$

$\langle a, \underbrace{U^T}_{\overset{\|}{U^{-1}}} U b \rangle = \langle a, b \rangle$

Spalten sind Orthogonale Basis

$U = (u_1, u_2, u_3 \dots, u_n)$

↑ Spaltenvektoren

Davaus folgt:
keine Änderung von
- Länge
- Winkel

Beispiel:

Drehungen, Spiegelungen

Beweis:

angenommen $U =$

$$\begin{pmatrix} u_1 & u_2 & u_3 \\ u_1 & u_2 & u_3 \\ u_1 & u_2 & u_3 \end{pmatrix} \text{ dann}$$

$$U^T = \begin{pmatrix} u_1 & u_1 & u_1 \\ u_2 & u_2 & u_2 \\ u_3 & u_3 & u_3 \end{pmatrix}$$

$$\text{Vektor } \underset{\substack{\uparrow \\ \text{beliebig}}}{x} \cdot U^T = \begin{pmatrix} \langle u_1, x \rangle \\ \langle u_2, x \rangle \\ \langle u_3, x \rangle \end{pmatrix}$$

$F^{-1}(x) = U^{-1}x = U^T x$ ← Umkehrabbildung auch orthogonal

$(U^T)^{-1} = (U^{-1})^T$

wenn x aber $= u_j$ (beliebig)

$$\underset{1 \leq j \leq n}{u_j} \cdot \underset{\substack{\uparrow \\ \text{Spalten} \\ \text{von } U = u_j}}{U^T} = \begin{pmatrix} \langle u_1, u_j \rangle \\ \langle u_2, u_j \rangle \\ \langle u_3, u_j \rangle \end{pmatrix} \Rightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \mathbb{I}_n$$

→ Davaus folgt:
$U^T = U^{-1}$
nur wenn Spalten von U die u_n sind.

Anwendung von U

wenn $u_1, \dots, u_n$ die Spalten von U sind:

$U_T \cdot x$ → gibt die Projektionslänge auf jede Orthogonalbasis!

$\langle u_1, x \rangle$

Beispiel für Anwendung : Bild-Kompression

orthogonale Matrix C : Diskrete Kosinustransformation (DCT)

$$c_{jk} = \sqrt{\frac{2 - \delta_{1k}}{n}} \cdot \cos\left(\frac{(2j-1)(k-1)\pi}{2n}\right) \quad \text{mit} \quad \delta_{jk} = \begin{cases} 1, & \text{für } j=k \\ 0, & \text{für } j \neq k \end{cases}$$

Abbildung:

$y = C^T x$

$x = C y$ (Umkehrabbildung)

[Ziel: JPEG Kompression, Annäherung der Vektoren durch Projektion auf Teilraum]

Beispiel:

$n = 2$

$C = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ → orthogonale Transformation

$\underset{u_1}{\begin{pmatrix} 1 \\ 1 \end{pmatrix}} \quad \underset{u_2}{\begin{pmatrix} 1 \\ -2 \end{pmatrix}}$ → Basis

Eigenschaften von Orthogonalen Matrizen:

$|\det(U)| = 1$

$U_1 \cdot U_2 = U_3$ (Produkt von 2 orthogonalen Matrizen ist orthogonal)

„Spaltenorthogonal"

Anzahl der u in $(u_1, \dots, u_m)$ kleiner als $\dim(V) = n$ $\longrightarrow$ $m < n$

$Q = (u_1, u_2, \dots, u_m)$ Beispiel in $\mathbb{R}^2$: $Q = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix}$ $m=2$ $n=3$

Es gilt: $Q^T \cdot Q = \mathbb{I}_m$ denn die Spalten von Q bilden ein Orthogonalsystem

Beispiel in $\mathbb{R}^3$: $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \mathbb{I}_m$

$\longrightarrow$ Aber $Q \cdot Q^T \neq \mathbb{I}_m$: $\begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \Rightarrow$ Error weil nicht quadratisch

$\longrightarrow$ Während bei $U = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ sowohl Zeilen als auch Spalten orthogonal sind, trifft das bei Q nicht zu!

„Orthogonaler Projektor"

$Q \cdot Q^T \cdot \vec{x}$

$$Q \cdot \underbrace{Q^T \cdot a}_{} = Q \begin{pmatrix} \langle u_1, a \rangle \\ \vdots \\ \langle u_m, a \rangle \end{pmatrix} = \sum_{j=1}^{m} \langle u_j, a \rangle \cdot u_j = a_{\parallel}$$

Richtung

Länge

Die gesamte Projektion von a auf Unterraum $U_1, \dots, U_m$ zusammenaddiert.

Symmetrische Matrix mit der Eigenschaft $P^2 = P \cdot P = P$ heißt orthogonaler Projektor.

Beweis bei QQ^T:

— $P^T = P$ $\quad (\underbrace{QQ^T}_{})^T = (Q^T)^T Q^T = \underbrace{QQ^T}_{}$

— $P^2 = P$ $\quad (QQ^T) \cdot (QQ^T) = Q \mathbb{I}_m Q^T = QQ^T$

QQ^T ist die Struktur eines jeden orthogonalen Projektors.

$$a = \underbrace{a_{\parallel}}_{Pa} + \underbrace{a_{\perp}}_{(\mathbb{I} - P)a}$$

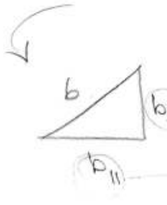
wichtig: $a_{\parallel} \in \text{Bild}(P)$ und $a_{\perp} \in \text{Bild}(\mathbb{I} - P)$ sind orthogonal, (da $\langle a_{\parallel}, a_{\perp} \rangle = \langle Pa, (\mathbb{I} - P)a \rangle = \langle a, P(\mathbb{I} - P)a \rangle = \langle a, (P - P^2)a \rangle = 0$)

Anwendung

$Ax = b$ mit QR-Zerlegung lösen:

- Gleichungssystem nur lösbar wenn $b \in \text{Bild}(A)$.
- wenn $b \notin \text{Bild}(A)$ dann Approximation durch Projektion:

Wir suchen $\|Ax - b\|$ mit dem geringsten Wert.



$\longrightarrow$ $b_\perp$ orthogonal zu Bild (A) mit geringstem Fehler

$\longrightarrow$ $b_\parallel \in \text{Bild}(A)$ → benutzen zum Lösen

Pythagoras:

$$\|Ax - b\|^2 = \|Ax - b_\parallel\|^2 + \|b_\perp\|^2$$

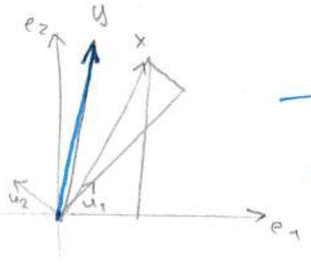
$\|Ax - b_\parallel\|$ lösen

Interessante Idee

Matrix $\boxed{U^{-1}}$ dreht Punkte um 45° gegen den Uhrzeigersinn

$f(x) = U^{-1} x = \textcircled{y}$

↑



Entweder : y = Neuer Punkt der gedreht ist $\Rightarrow y = \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix}$

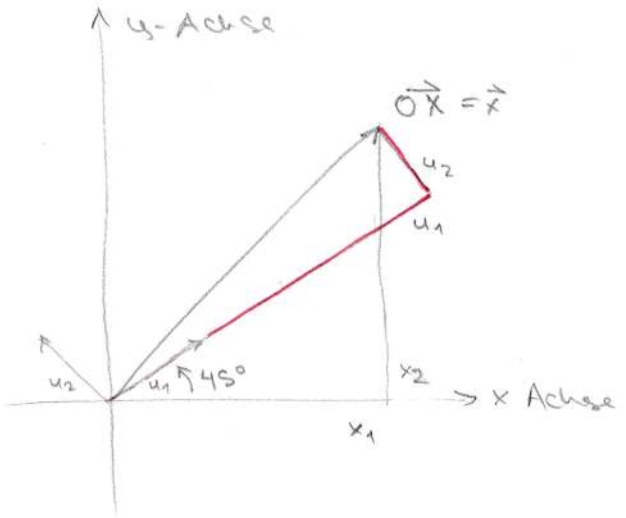
Oder : y = Beschreibung von x aus einer um 45° gedrehten Perspektive,

Sodass

$x = y_1 \cdot u_1 + y_2 \cdot u_2 + y_3 \cdot u_3$

Beispiel

3D-Welt, Spielerperspektive dreht sich 45° gegen Uhrzeigersinn um x_3 Achse. Objekte müssen nun bezüglich der neuen Perspektive beschrieben werden



$$x = \begin{pmatrix} 1 \\ 3 \\ 4 \end{pmatrix}$$

$$U = \begin{pmatrix} u_1 & u_2 & u_3 \end{pmatrix}$$

$$\begin{array}{ccc} \downarrow & \downarrow & \downarrow \end{array}$$

$$U = \begin{pmatrix} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$U^T = U^{-1} = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Neue Koordinaten

$$\boxed{x'} = U^{-1} \cdot \underset{\substack{\uparrow \\ x}}{\begin{pmatrix} 1 \\ 3 \\ 4 \end{pmatrix}} = \begin{pmatrix} 2\sqrt{2} \\ \sqrt{2} \\ 4 \end{pmatrix} \begin{array}{l} \rightarrow x'_1 \\ \rightarrow x'_2 \\ \rightarrow x'_3 \end{array}$$

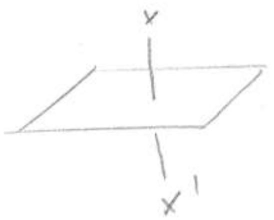
Neue Beschreibung durch Linearkombination

$$\underset{x}{\begin{pmatrix} 1 \\ 3 \\ 4 \end{pmatrix}} = \underbrace{2\sqrt{2}}_{x'_1} \cdot u_1 + \underbrace{\sqrt{2}}_{x'_2} \cdot u_2 + \underbrace{4}_{x'_3} \cdot u_3$$

$$x \rightarrow \boxed{U^{-1}} \rightarrow x'$$

$$x' \rightarrow \boxed{U} \rightarrow x$$

Beispiel 2

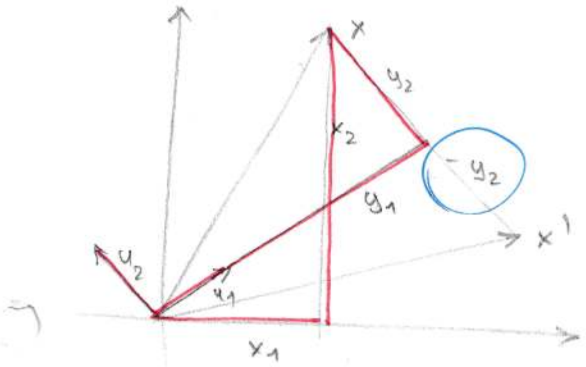


Punkt X ($\overrightarrow{OX} = \vec{x}$) wird an Ebene $x_1 - x_2 = 0$ anhand der spiegelnden Matrix A gespiegelt

Lineare Abbildungen

$S(x) = \underline{A}x = x'$ Spiegelt x (funktioniert nur bez e_1, e_2, e_3)

$K(x) = \underline{U}^T x = U^{-1} x = y$ beschreibt x aus der Perspektive U



Angabe:

Vektor x soll gespiegelt werden und anhand der alten und neuen Basis beschrieben werden.

$$x = \begin{pmatrix} 1 \\ 3 \\ 4 \end{pmatrix} \quad E = (e_1 \ e_2 \ e_3) \quad U = (u_1 \ u_2 \ u_3)$$

$$A = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Wichtiges zu K(x):

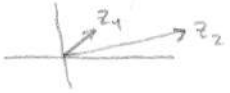
$K(x) = U^{-1} x = y$

$K(y)^{-1} = U y = x$

Diese Transformation durch Multiplikation der Spalten von U mit Koordinaten von x ist nur möglich, weil $U^T = U^{-1}$ (also die Elemente orthogonal zueinander sind)

Sonst müsste man zur Umschreibung in eine andere Linearkombination (zB z) die Koeffizienten einzeln berechnen.

$x = \textcircled{k_1} z_1 + \textcircled{k_2} z_2 + \textcircled{k_3} z_3$



Lösung:

x Spiegeln: $S(x) = Ax = x'$

$$x \quad \rightarrow \quad x'$$
$$\begin{pmatrix} 1 \\ 3 \\ 4 \end{pmatrix} \quad \begin{pmatrix} 3 \\ 1 \\ 4 \end{pmatrix}$$

---

x umwandeln zu y $K(x) = U^{-1} x = y$

y umwandeln zu x $K(x)^{-1} = U y = x$

x spiegeln zu x' $S(x) = Ax = x'$

x' umwandeln zu y' $K(x') = U^{-1} x' = y'$

$$y \quad \rightarrow \quad y'$$
$$\begin{pmatrix} 2\sqrt{2} \\ \sqrt{2} \\ 4 \end{pmatrix} \quad \begin{pmatrix} 2\sqrt{2} \\ \boxed{-\sqrt{2}} \\ 4 \end{pmatrix}$$

$$K(x) = U^{-1} x' = \begin{pmatrix} 2\sqrt{2} \\ -\sqrt{2} \\ 4 \end{pmatrix}$$

System E System U

$3e_1 + e_2 + 4e_3 = 2\sqrt{2}\, u_1 - \sqrt{2}\, u_2 + 4 u_3$

3 1 4 $2\sqrt{2}$ $-\sqrt{2}$ 4

Vereinfachte Formel laut Buch!

$$y' = U^{-1}\underbrace{x'} = U^{-1}\underbrace{Ax} = U^{-1}A\underbrace{Uy}_{=x},$$

Neue Matrix die

$y \to x \to x' \to y'$

$B = U^{-1} A U$

$By = U^{-1} A U y = y'$

Definition

"Ähnliche Matrizen"

Bsp.: $f(x) = Ax = x'$

$f(y) = Bx = y'$

Beide Matrizen spiegeln, aber A spiegelt bezüglich $[E]$ und B spiegelt bezüglich $[U]$

(Äquivalenzrelation)

Man sagt 2 Matrizen (quadratisch) sind ähnliche $\cong$ Matrizen wenn gilt:

$$\boxed{B = U^{-1} A U}$$

Eigenwerte und Eigenvektoren

Diagonalmatrizen sind leichter handzuhaben.

Manche Matrizen sind diagonalisierbar.

Vorheriges Beispiel

$$B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = U^{-1} A U$$

Gesucht zu jeder Matrix A:

eine Transformation U sodass $U^{-1} A U$ eine Diagonalmatrix ist

$$U^{-1} A U = \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix} \quad \Big| \cdot U$$

$$A U = \operatorname{diag}(\lambda_1, \dots, \lambda_n) \cdot U$$

$$AU = \left(Au_1 \; Au_2 \dots Au_n \right) = \left(\lambda_1 u_1 \; \lambda_2 u_2 \dots \lambda_n u_n \right)$$

$$Au_j = \lambda_j u_j \qquad 1 \leq j \leq n$$

Beispiel

$$A = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \in \mathbb{R}^2$$

$$Au = \lambda u \qquad | -\lambda u$$

$$Au - \lambda u = 0 \qquad | \; u \text{ herausheben}$$

$$\underbrace{(A - \lambda \cdot \mathbb{I}_2)}_{\text{darf nicht invertierbar sein!}} \underbrace{u}_{\neq 0} = \vec{0}$$

Gesucht: λ, u dass die Gleichung erfüllt.

$\lambda \in \mathbb{C}$ Eigenwert

$u \in \mathbb{C}^n$ zugehöriger Eigenvektor von A

$u \neq \vec{0}$

$\vec{u} \neq \vec{0}$ weil der Nullvektor nicht linear unabhängig ist.

→ sonst: $u = \vec{0} \cdot (A - \lambda \cdot \mathbb{I}_2)^{-1}$

$u = \vec{0}$

Nicht invertierbar bedeutet: $\det(A - \lambda \cdot \mathbb{I}) = 0$ (→ siehe Formel für A^{-1} invertierung)

„Charakteristisches Polynom"

$$\chi_A(\lambda) = \det(A - \lambda \mathbb{I}) \; (= 0)$$

↑ wir suchen λ

$\det(A - \lambda \mathbb{I})$ bildet ein Polynom. Nullstellen sind λ_n

Eigenwerte

↓

einsetzen)

$(A - \lambda_j \mathbb{I}) u = 0$

↓

Eigenvektoren berechnen

↓

Auf 1 Länge normieren

Beispiel 14.6) Eigenwerte und Eigenvektoren

$A = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$ $\qquad U^{-1} A U = \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix} \quad | \cdot U$

$$A U = U \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix}$$

$$(A u_1 \ \dots \ A u_n) = (\lambda_1 u_1 \ \dots \ \lambda_n u_n)$$

$$A u_j = \lambda_j u_1 \qquad 1 \leq j \leq n \longrightarrow \text{weil Spalten übereinstimmen}$$

$$A u = \lambda u$$

$$A u - \lambda u = 0 \quad | \, u \text{ herausheben}$$

$$(A - \lambda \cdot \mathbb{I}_n) \cdot u = 0$$

weil $u \neq 0$ darf $(A - \lambda \mathbb{I}_n)$ nicht invertierbar sein,

daher: $\det(A - \lambda \mathbb{I}_n) \cdot \cancel{u} = 0$ ← „charakteristisches Polynom"

$$\det(A - \lambda \mathbb{I}_n) = 0$$

$$\det\left(\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} - \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}\right) = 0$$

$$\det \begin{pmatrix} 1-\lambda & 1 \\ 1 & 1-\lambda \end{pmatrix} = 0$$

$$\begin{vmatrix} 1-\lambda & 1 \\ 1 & 1-\lambda \end{vmatrix} = (1-\lambda)^2 - 1^2 = 0$$

$$\cancel{1^2} - 2\lambda + \lambda^2 - \cancel{1^2} = 0$$

$$(-2+\lambda)\lambda = 0$$

$$\underbrace{\lambda_1 = 0 \quad \lambda_2 = 2}_{\text{Eigenwerte}}$$

→ zurücksetzen in die urspr. Gleichung

$$(A - \lambda \cdot \mathbb{I}_n) \cdot \underbrace{u}_{\text{Eigenvektor}} = 0$$

$$\left(\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} - \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}\right) u = 0$$

$$\begin{pmatrix} 1-\lambda & 1 \\ 1 & 1-\lambda \end{pmatrix} \cdot \begin{pmatrix} u_x \\ u_y \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

Für $\lambda_2 = 2$

$$(1-2) u_x + u_y = 0$$

$$u_x + (1-2) u_y = 0$$

$$u_x = u_y$$

$$\begin{pmatrix} t \\ t \end{pmatrix} \quad \forall t \in \mathbb{R}$$

Normiert:

$$\frac{\begin{pmatrix} t \\ t \end{pmatrix}}{\sqrt{2t^2}} = 1$$

Für $\lambda_1 = 0$

$$\Leftrightarrow (1-0) \cdot u_x + u_y = 0$$

$$u_x + (1-0) u_y = 0$$

$u_x = -u_y$ für alle $u \in \mathbb{R}$

$$\begin{pmatrix} t \\ -t \end{pmatrix} \quad \forall t \in \mathbb{R}$$

Normiert:

$$\frac{\begin{pmatrix} t \\ -t \end{pmatrix}}{\sqrt{2t^2}} = 1$$

Eigenwerte λ und Eigenvektoren $\vec{u}$

Alg Vielf. = Geometr Vielf. → diagonalisierbar

$A = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \quad \ldots \lambda_1 = 0 \rightarrow u_1 = \begin{pmatrix} t \\ -t \end{pmatrix} \; \forall t \in \mathbb{R}$

$\lambda_2 = 2 \rightarrow u_2 = \begin{pmatrix} t \\ t \end{pmatrix} \; \forall t \in \mathbb{R}$

$\lambda_1 : \; 1, \; 1$

$\lambda_2 : \; 1, \; 1$ ✓

$A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \ldots \lambda_1 = \lambda_2 = 1$ → Alle Vektoren außer Nullvektor kann man beliebig bilden

$\lambda : 2, 2$ ✓

$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \ldots \lambda_1 = \lambda_2 = 1$ nur ein Eigenvektor: $u_1 = \begin{pmatrix} t \\ 0 \end{pmatrix}$

$\lambda : 2, 1$ ✗ nicht diagonalis.

$A = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix} \quad \ldots$ Komplexe Nullstellen $\lambda_1 = i$, $\lambda_2 = -i$

$-i u_1 - u_2 = 0$

$u_1 - i u_2 = 0$

$\nearrow \lambda_1 = i \quad 1, 1$ ✓

$t \begin{pmatrix} i \\ 1 \end{pmatrix} \; t \in \mathbb{C}$

$\searrow \lambda_2 = -i \quad 1, 1$ ✓

$t \begin{pmatrix} -i \\ 1 \end{pmatrix} \; t \in \mathbb{C}$

Eigenwerte:
Nullstellen des charakteristischen Polynoms → Eigenvektoren: Zugehörige

$\underbrace{\hphantom{Nullstellen des}}$

Für $n \times n$ Matrix
maximal n Eigenwerte

Anzahl der λ_j die vorkommen

„Algebraische Vielfachheit des Eigenwerts λ_j"

Anzahl der zugehörigen linear unabhängigen Eigenvektoren von λ_j

„Geometrische Vielfachheit des Eigenwerts λ_j"

↓

- linear unabhängig
- bilden Teilraum durch $LH\{\mathrm{Kern}(A - \lambda_j \mathbb{I})\}$
- Geometrische Vielfachheit = dim(Eigenraum)

$f(u) = (A - \lambda_j \mathbb{I}) \cdot u = 0$

↓

„Eigenraum" beinhaltet alle möglichen Eigenvektoren.

- $\det(A) = \lambda_1 \cdot \lambda_2 \cdots \lambda_n$
- Summe diagonale A
  trace(A) = tr(A)

$tr(A) = \sum_{j=1}^{n} a_{jj} = \sum_{j=1}^{n} \lambda_j$

Eigenwerte und Eigenvektoren

$$U^{-1} A U = \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix}$$

gesucht: λ und u (Spalten von U) dass A diagonalisierbar ist.

- Die Eigenvektoren sind linear unabhängig, es muss aber genug von ihnen geben damit U invertierbar ist

$\downarrow$

A ist diagonalisierbar wenn U invertierbar ist

U ist invertierbar wenn:

algebraische Vielfachheit = geometr. Vielfachheit.

$U^{-1} A U$

1. Koordinatentransform. in U
2. Ausführung von A
3. Zurücktransformieren

$\Rightarrow$ Ähnliche Matrix zu A die aber diagonal ist.

- Ähnliche Matrizen haben gleiche charakter. Polynome:

$B = U^{-1} A U$ $\quad$ $\det(B - \lambda \mathbb{I}) = \det(U^{-1} A U - \lambda U^{-1} \mathbb{I} U) =$

$\det(U^{-1}(A - \lambda\mathbb{I}) U) = \det(U^{-1}) \det(A - \lambda \mathbb{I}) \det(U) =$

$\det(A - \lambda \mathbb{I})$

- A und AT haben gleiche charakt. Polynome

$\det(A^T - \lambda \mathbb{I}) = \det(A^T - (\lambda \mathbb{I})^T) = \det((A - \lambda\mathbb{I})^T) = \det(A - \lambda\mathbb{I})$

Symmetrische Matrizen und ihre Eigenwerte / Eigenvektoren

Symmetrisch: $A^T = A$

- Eigenwerte sind reel $\lambda \in \mathbb{R}$
- Eigenvektoren sind orthogonal $u_1 \perp u_2$ → können orthonormalbasis bilden wenn man sie normiert
- Immer diagonalisierbar

„Positiv definit"

$\langle x, Ax \rangle = x^T \cdot A x > 0 \quad x \neq 0 \quad x \in \mathbb{R}^n$ → Alle Eigenwerte positiv

„negativ definit"

$\langle x, A \rangle = x^T \circ A x < 0 \quad x \neq 0 \quad x \in \mathbb{R}^n$ → Alle Eigenwerte negativ

Überblick

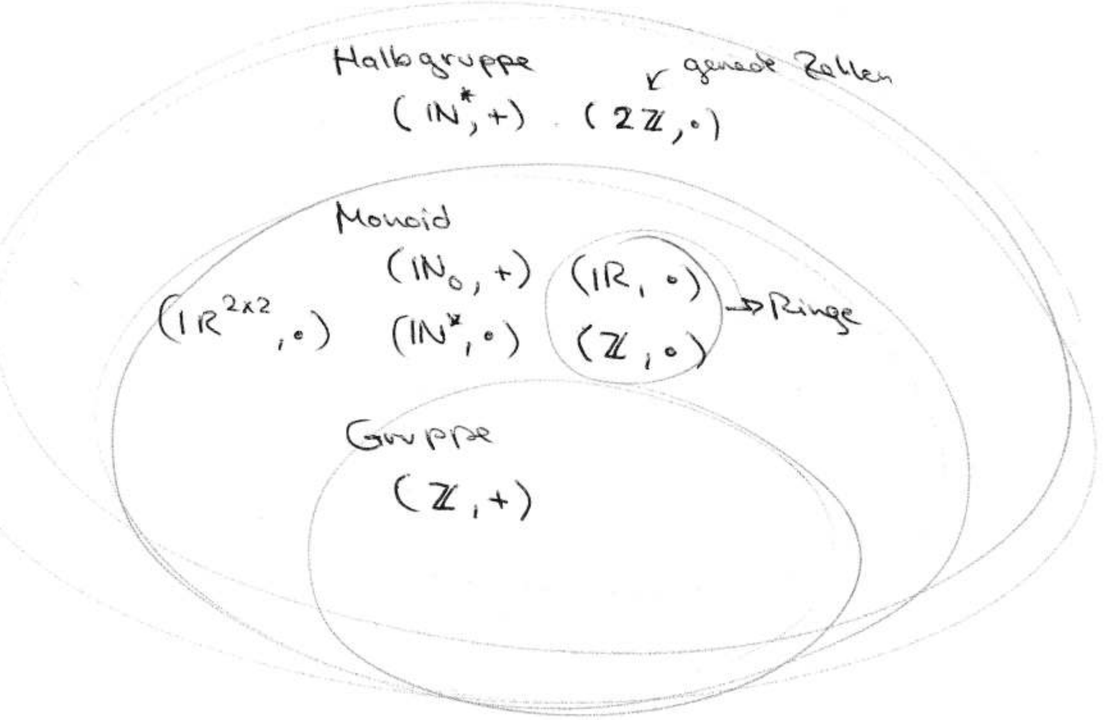
$(\mathbb{Z}, \circ)$ keine Gruppe weil nicht alle Elemente ein multiplikativ inverses Element haben zB $3 \rightarrow 3^{-1} = \frac{1}{3} \in \mathbb{Q}$

$(\mathbb{R}, \circ)$ keine Gruppe, 0 hat kein inverses Element
$(\mathbb{R}^*, \circ)$ ist eine Gruppe

Axiome einer Gruppe:

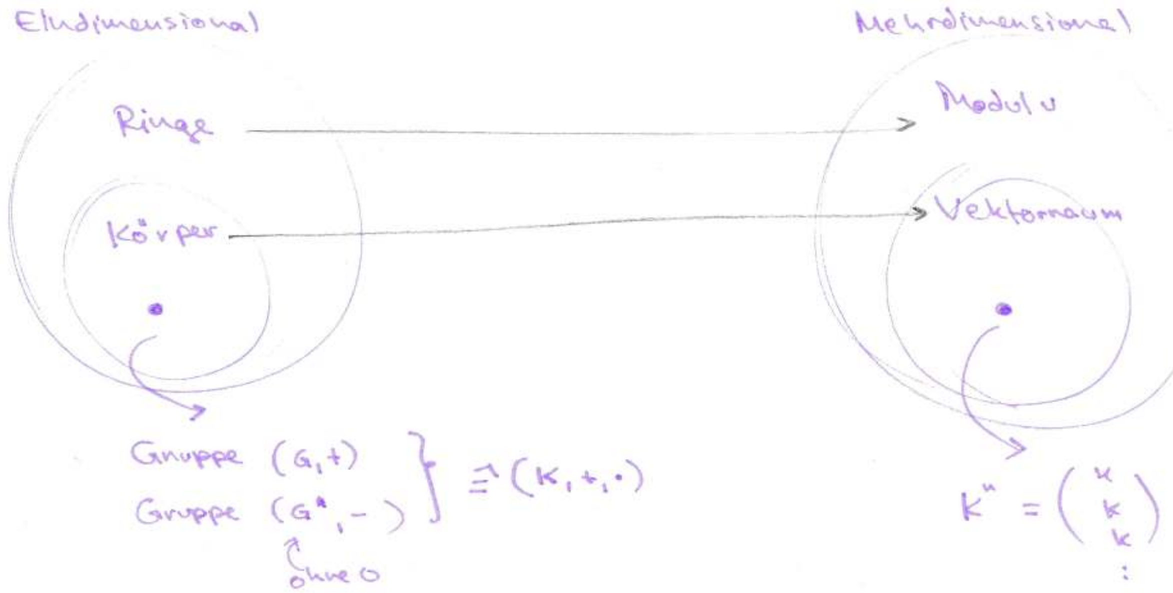
0) Abgeschlossenheit
1) Assoziativität
} Halbgruppe } Monoid } Gruppe
2) neutrales Element e
3) g^{-1} inverses Element

(4) kommutativität $a \circ b = b \circ a$) → nur abel'sche Gruppe



Überblick

Gruppe	Körper	Ring	Vektor Raum	Modul
$(S_n, \circ)$ $(\mathbb{Z}, +)$ $(\mathbb{Z}^*, \cdot)$	$\mathbb{Q}, \mathbb{R}, \mathbb{C}$	$\mathbb{Z}/m\mathbb{Z}$	$\mathbb{Q}^n$ $\mathbb{R}^n$ $\mathbb{C}^n$	$\mathbb{Z}^n$ $(\mathbb{Z}/m\mathbb{Z})^n$
nur 1 Operator (oder 2 mit Umkehroperat.)	Alle Operatoren $+, -, \cdot, \div$	3 Operatoren $+, -, \cdot$ (ohne $\div$)	Körper mit n potenziert	Ringe mit n potenziert



Wir brauchen algebraische Strukturen (modern algebra) damit wir Gleichungen in verschiedenen Rahmen lösen können.

- $2x = 1$: ist nicht mit ganzen Zahlen (int) lösbar!
- $3 + x = 5$: lässt sich mit Gruppen lösen (nur 1 Operator)
- $3 + 2x = 5$: lässt sich mit Körper lösen.

0) Abgeschlossenheit:

bei einem Gruppoid / einer binärer algebraischer Struktur

$$A \times A \rightarrow A$$

$$(a,b) \in A \rightarrow (a \circ b) \in A \qquad \left.\begin{matrix}\textcircled{a}\\ \textcircled{b}\end{matrix}\right\} \xrightarrow{\text{zuweisung}} (a \circ b)$$

(wenn $B \subseteq A$ und $a,b \in B$
dann muss $(a \circ b) \in B$)

1) Assoziativgesetz

$$(a \circ b) \circ c = a \circ (b \circ c)$$

2) neutrales Element

$\exists!\ e \in A$ sodass für alle $a \in A$

$$e \circ a = a \circ e = a$$

- bei Addition 0
- bei Multiplikation 1

3) inverses Element

$$a \rightarrow a'$$

$$a \circ a' = e$$

- bei Addition $-a$
- bei Multiplikation a^{-1}

4) Kommutativgesetz

$$a \circ b = b \circ a$$

Gruppen

(Körper, Operator)
(A , ∘)

wenn 4 gilt: „kommutative ... [Bezeichnung]"
kommutative Gruppe = abel'sche Gruppe / Gruppoid

Halbgruppe	1)
Monoid	1) 2)
Gruppe	1) 2) 3)
Gruppoid	1) 2) 3) 4)

↳ binäre algebraische Struktur / Operation (weil nur + und −)

Elementare Begriffe der Zahlentheorie

$a \equiv b \mod m$: a und b sind kongruent modulo m, sie sind in derselben Restklasse $\overline{a \mod m}$

$a - b = km$ sie unterscheiden sich um ein Vielfaches von m

(es ist egal ob $a > b$ oder $b < a$)

Rechenregln:

$a \equiv b \mod m$

$c \equiv d \mod m$

$a + c \equiv b + d \mod m$ →

$a \cdot c \equiv b \cdot d \mod m$

Beispiel:

$2 \equiv 12 \mod 5$

$3 \equiv 13 \mod 5$

$2 + 3 \equiv 25 \mod 5$

warum?

$a \equiv b \mod m$ .... gleicher Rest

$a = qm + r_1$

$b = pm + r_r$

$c \equiv d \mod m$ .... gleicher Rest

$c = km + r_2$

$d = hm + r_2$

gemeinsam ergibt das:

$a + c = (qm + r_1) + (km + r_2)$

$b + d = (pm + r_1) + (hm + r_2)$

$(q + k)m + (r_1 + r_2) = (p + h)m + (r_1 + r_2)$

$(q + k)m = p + k)m$

ModuloRechnung bei Prüfziffern :

ISBN, Zehnstellige Zahl

$a - bcd - efghi - \boxed{p}$

↑ Prüfziffer

Beispiel:

ISBN: 3-446-19873-p wie muss die Prüfziffer lauten?

$10 \cdot 3 + 9 \cdot 4 + 8 \cdot 4 + 7 \cdot 6 + 6 \cdot 1 + 5 \cdot 9 + 4 \cdot 8 + 3 \cdot 7 + 2 \cdot 3 + 1 \cdot p \equiv 0 \mod 11$

$\underbrace{250}_{\% 11} + p \equiv 8 + p \equiv 0 \mod 11$

$8 + p \equiv 0 \mod 11 \quad | -8$

$p \equiv -8 \mod 11 \longrightarrow p = -8 = 3$

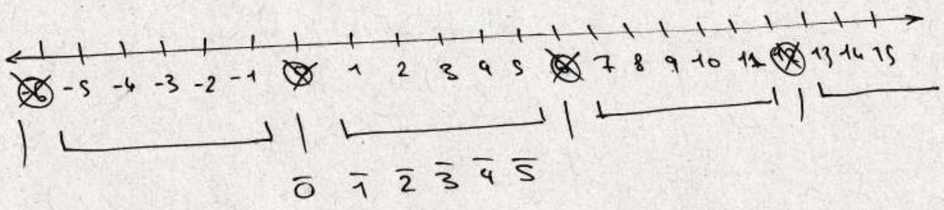
Alle möglichen Reste die bei mod m entstehen können → Restklassen

$\mathbb{Z}_m = \{ \bar{0}, \bar{1}, \dots, \overline{m-1} \}$

Eine Restklasse $\bar{r} := \{ r + m \cdot n \mid n \in \mathbb{Z} \}$

Man schreibt auch $\mathbb{Z} / m\mathbb{Z}$ statt $\mathbb{Z}_m$

Angenommen $\mathbb{Z}/6\mathbb{Z}$ bei $m=6$



$\varnothing =$ vielfachen von 6

Es gibt

1. additiv inverse sodass $a + [\text{add. inv. } a] \equiv 0 \mod m$
2. multiplikativ inverse (Kehrwerte) sodass $a \cdot [\text{Kehrwert } a] \equiv 0 \mod m$

Beispiel

~~additiv - Inverse zu 2 bei m=6~~

Multiplikativ Inverses von 2 bei m=6

$2 \equiv 1 \mod 6$

~~$2 \equiv 1 \quad 2 = 1 + 6n$~~

~~$1 = 6n$~~

$2 \cdot [\text{inv}] = 1 + 6n$

$2 \cdot [\text{inv}] - 6n = 1 \Rightarrow 2([\text{inv}] - 3n) = 1$

$[\text{inv}] - 3n = 1/2$

$[\text{inv}] = 1/2 + 3n$

↑

[inv] kann nicht ganzzahlig sein

Problem:

2 kann kein Inverses haben
weil 2 und 6 nicht
Teilerfremd sind!

Satz:
genau dann wenn
~~Kehrwert und~~ e und
m Teilerfremd sind

Elementare Begriffe der Zahlentheorie:

1) $a + \textcircled{x} \equiv b \mod m$ | + (additiv Inverses von a)

$\textcircled{x} \equiv b + (-a) \mod m$

2) $a \cdot \textcircled{x} \equiv b \mod m$ | · (multiplikativ Inverses vor a)

$\textcircled{x} = \left(\frac{1}{a}\right) \cdot b \mod m$

→ a und m müssen aber teilerfremd sein!

$ggT(a, m) = 1$ bedeutet sie sind teilerfremd

3) Bei $a \cdot c \equiv b \cdot c \mod m$ durch c kürzen

[Wenn $c \in \mathbb{Z}_m^*$ ist (ein multiplikativ Inverses besitzt)
dann darf man kürzen]

also wenn: $ggT(c, m) = 1$

$\mathbb{Z}_{primzahl} = \mathbb{Z}^*_{primzahl}$
da Primzahl mit allen Restklassen teilerfremd ist!

Beispiel:

$10 \equiv 40 \mod 6 \quad | \cdot \frac{1}{5} \qquad ggT(5,6) = 1$

$2 \equiv 8 \mod 6 \quad \cancel{| \cdot \frac{1}{2}} \qquad ggT(2,6) \neq 1$

Modulo - Rechnen

Wiederholung

mit Modulo n, $n = 7$ bei $\mathbb{Z}/n\mathbb{Z}$

Mo	DI	MI	DO	FR	SA	SO
				...	-2	-1
0	1	2	3	4	5	6
7	8	9	10	11	...	

Wenn man sich 7 Spalten bewegt = dann rutscht man nur eine Zeile herunter

Beispiel: Man fängt bei Montag an:

$x = 8 \Rightarrow 7 \cdot 1 + 1$ = effektiv 1

$x = 701 \Rightarrow 7 \cdot 100 + 1$ = effektiv 1

$x = 100 = 7 \cdot 14 + 2$ = effektiv 2

} 7 = Spaltenanzahl

Notation

Alle Vertreter der Äquivalenzklasse 0

$$\mathbb{Z}/n\mathbb{Z} = \{ \underset{\overset{\shortparallel}{[7]}}{[0]}, \underset{\overset{\shortparallel}{[8]}}{[1]}, [2], \dots, [n-1] \}$$

$[0] = [7]$

$0 \equiv 7 \pmod 7$

$1000 \equiv 300 \equiv 20 \equiv -1 \pmod 7$

Aufgrund von „Wohldefiniertheit" rechnen sowohl davor als auch danach möglich:

$$\underset{\overset{\shortparallel}{10 \cdot 4}}{3 \cdot 4} \quad \underset{= 40}{= 12} \qquad \underset{40 \equiv 5 \equiv -2}{12 \equiv 5 \equiv -2}$$

Definition: Ordnung und Index

$(G, \circ)$ ― endliche Gruppe

$(U, \circ)$ ― Untergruppe von G

$|G : U|$ ― Index: Anzahl der Links/Rechtsnebenklassen

Beispiel:

$G := \mathbb{Z}$

$U := m\mathbb{Z}$ mit $m = 3$ $\quad \frac{G}{U} = \mathbb{Z}/m\mathbb{Z} \quad |\mathbb{Z}/3\mathbb{Z}| = 3$

$\{\bar{0}, \bar{1}, \bar{2}\}$

Satz von Lagrange:

Es gilt zu beweisen:

„Es gibt gleich viele Links wie Rechtsnebenklassen"

„G wird in m gleich großen Teilmengen unterteilt"

$$\left.\begin{array}{l} U \to a \circ U \\ U \to a \circ a \end{array}\right\}$$ bijektive Abbildung: $|U| = |U \circ a|$ und $|a \circ U|$

Es gilt: $|G : U| = |G| \backslash |U| \quad | \cdot |U|$

$$|U| \cdot \underbrace{|G : U|}_{\text{natürliche Zahl}} = |G|$$

Also $|U| \cdot m = |G|$

$|U|$ teilt $|G|$ in m gleich große Teilmengen

$\bar{a} = a + m\mathbb{Z}$ und $m\mathbb{Z} = \bar{0}$

$\bar{0} = 0 + m\mathbb{Z}$

$\bar{1} = 1 + m\mathbb{Z}$ $\quad \{a, \pm(m+a), \pm(2m+a) \dots\}$ →

$\bar{2} = 2 + m\mathbb{Z}$ $\quad m = 3$

bei $|\mathbb{Z}/3\mathbb{Z}|$ ist $m = 3$

$\bar{0} = \{0, \pm(3+0), \pm(2 \cdot 3 + 0), \pm \dots\}$

$\bar{1} = \{1, \pm(3+1), \pm(2 \cdot 3 + 1), \pm \dots\}$

$\bar{2} = \{2, \pm(3+2), \pm(2 \cdot 3 + 2), \pm \dots\}$

$\bar{0} = 0 \mod 3$

$\bar{1} = 1 \mod 3$

$\bar{2} = 2 \mod 3$

Potenzieren definiert

rekursiv

$$a^n = \begin{cases} e & \text{für } n=0 \quad \text{(das neutrale Element)} \\ a & \text{für } n=1 \\ a^{n-1} \circ a & \text{rekursiv für } n>1 \\ (a^{-1})^{-n} & \text{rekursiv für } n<1 \end{cases}$$

Bei Additionsoperator = Multiplikation

$a^n = n \cdot a \qquad a^3 = a + a + a$

Bei Multiplikationsoperator = Potenzieren

$$a^n = a^n \qquad a^3 = a \cdot a \cdot a \longrightarrow \underline{a^{n+m} = a^n \circ a^m} \quad (a^m)^n = a^{m \cdot n}$$

Menge der Potenzen $\underline{\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\} = \text{Untergruppe von } G}$

$$P(\langle a \rangle) = \{\ldots a^{-1}, a^0, a^1, a^2, a^3, \ldots\}$$

Diese von a erzeugte Untergruppe ist kommutativ wegen $a^n \circ a^m = a^{n+m}$

$a^m \circ a^n = a^{m+n}$

G ist noch nicht definiert aber
diese Untergruppe von G ist kommutativ auch wenn G es nicht ist.

Alle Elemente von $\langle a \rangle$ sind eine Teilmenge von G die als Kopie der ganzen Zahlen $\mathbb{Z}$ gesehen werden kann

$$\textcircled{\mathbb{Z}} \swarrow a^n$$

Es müssen nicht alle Potenzen verschieden sein!

$a^m = a^n$ mit $m < n$

$a^m = a^n \mid \cdot a^{-m}$

$e = a^{n-m}$ ↳ es gibt also auch eine ganze Zahl $k>0$ mit der man das Inverse von n bilden kann!

$e = a^k$ → für alle Elemente gibt es eine Potenz mit der sie wieder zum neutralen Element werden

Definition: Die Ordnung $\mathrm{ord}_G(a)$

bei einer Untergruppe $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$ oder $\langle a \rangle = \{a^n \mid 0 \leq n < \mathrm{ord}_G(a)\}$

wenn gilt:

$$a^n = a^m \quad | \circ (a^{-m})$$

$$a^n \circ a^{-m} = a^m \circ a^{-m}$$

$$a^{n-m} = e$$

↗ es muss also eine Zahl geben mit der, wenn die Menge endlich ist

$$\mathrm{ord}_G(a) := \underset{\substack{\uparrow \\ \text{die kleinste Zahl}}}{\min} \{n \in \mathbb{N} \mid a^n = e\}$$

$$a^{\mathrm{ord}_G(a)} = e$$

$$|\langle a \rangle| = \mathrm{ord}_G(a)$$

Sonst wenn Menge unendlich ist und nicht zyklisch ist $\mathrm{ord}_G(a) := \infty$

Definition: unendliche Ordnung

Wenn $(G, \circ)$ nur unterschiedliche $a \in G \Rightarrow$ alle a^n $(n \in \mathbb{Z})$ unterschiedlich

$\mathrm{ord}_G(a) = \infty$

Beispiel: Gruppe $(\mathbb{Z}, +)$ $\quad \langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$

a	...	-2	-1	0	1	2	...
$\mathrm{ord}(a)$	...	∞	∞	1	∞	∞	...

wegen 0^1

↗ weil man nie auf 0 kommen könnte

Definition: endliche Ordnung

Bei $\langle a \rangle = \{a^n \mid 0 \leq n < \mathrm{ord}_G(a)\}$ bzw zyklischen Untergruppen trifft die Definition zu!

Beispiel: $\underbrace{(\mathbb{Z}/4\mathbb{Z}}, +) = G$

$\{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$ → wobei jede dieser Elemente eine eigene Untergruppe erzeugt:

$$\langle 0 \rangle = \{0^n \mid 0 \leq n < \mathrm{ord}_G(0)\}$$

$$\langle 1 \rangle = \{1^n \mid 0 \leq n < \mathrm{ord}_G(1)\}$$

$$\langle 2 \rangle = \{2^n \mid 0 \leq n < \mathrm{ord}_G(2)\}$$

$$\langle 3 \rangle = \{3^n \mid 0 \leq n < \mathrm{ord}_G(3)\}$$

$\langle 0 \rangle = \{0\}$ $\quad |\langle 0 \rangle| = 1$ $\quad \mathrm{ord}_G(0) = 1 = 0^1$ $\quad 0 \equiv 0 \bmod 4$

$\langle 1 \rangle = \{0,1,2,3\}$ $\quad |\langle 1 \rangle| = 4$ $\quad \mathrm{ord}_G(1) = 4 = 1+1+1+1$ $\quad 4 \equiv 0 \bmod 4$

$\langle 2 \rangle = \{0,2\}$ $\quad |\langle 2 \rangle| = 2$ $\quad \mathrm{ord}_G(2) = 2 = 2+2$ $\quad 4 \equiv 0 \bmod 4$

$\langle 3 \rangle = \{0,3,6,9\}$ $\quad |\langle 3 \rangle| = 4$ $\quad \mathrm{ord}_G(3) = 4 = 3+3+3+3$ $\quad 12 \equiv 0 \bmod 4$

Gruppe : $(\mathbb{Z}/4\mathbb{Z}, +)$

Zyklische Untergruppen $\langle 0 \rangle, \langle 1 \rangle, \langle 2 \rangle, \langle 3 \rangle$

periorisch mit periode $\mathrm{ord}_G(a)$

weil $a^{n+\mathrm{ord}_G(a)} = a^n + a^{\mathrm{ord}\,G(a)} = a^n + e$

$\mathrm{ord}_G(a)$ teilt $|G|$:

vergleiche kleiner Fermat'scher Satz:

Für teilerfremde Zahlen $\mathrm{ggT}(a,m) = 1$ gilt

$a^{\varphi(m)} \equiv 1 \bmod m$ $\quad$ also: $a^{\varphi(m)} \bmod m = 1$

Euler'sche φ-Funktion:

\# der invertierbaren (a^{-1}) Restklassen mod m

$\varphi(m) = |\{a \in \mathbb{Z} \mid 1 \leq a \leq m,\ \mathrm{ggT}(a,m) = 1\}|$

Beispiel

$\varphi(6) = 2$ weil bei $\mathbb{Z}/6\mathbb{Z} = \{\cancel{0}, \textcircled{1}, \cancel{2}, \cancel{3}, \cancel{4}, \textcircled{5}\} \rightarrow a^2 \equiv 1 \bmod 6$

$\varphi(5) = 4$ weil bei $\mathbb{Z}/5\mathbb{Z} = \{\cancel{0}, \textcircled{1}, \textcircled{2}, \textcircled{3}, \textcircled{4}\} \rightarrow a^4 \equiv 1 \bmod 5$

wenn:

$\mathrm{ggT}(a,m) = 1$

Beispiel:

$\mathrm{ggT}(7,6) = 1$

$7^2 = 49 \equiv 1 \bmod 6$ ✓

$(6 \cdot 8 = 48)$

gilt für jede beliebige Zahl