

1. AUSSAGENLOGIK

1.1. GLOSSAR

Begriff	Bedeutung
Aussage	Feststellender Satz, dem eindeutig «wahr» oder «falsch» zugeordnet werden kann. Symbole wie A, B, C, \dots werden dafür verwendet
Aussagenlogische Form	Kombination von Aussagen, verknüpft durch Junktoren
Aussageform	Aussagen verknüpft mit Variablen
Normalform	Standardisierte Aussagenlogische Formen (Formeln)
Negationsnormalform	- steht ausschliesslich direkt vor Aussagen oder Konstanten
Verallgemeinerte Disjunktion	- Einzelne Aussage oder Negation - wahr oder falsch - Disjunktion $A \vee B$, falls A und B selbst verallgemeinerte Disjunktionen sind
Verallgemeinerte Konjunktion	- Einzelne Aussage oder Negation - wahr oder falsch - Konjunktion $A \wedge B$, falls A und B selbst verallgemeinerte Konjunktionen sind
Disjunktive Normalform	Disjunktion von (oder eine einzelne) verallgemeinerten Konjunktionen Beispiel: $(A \wedge B \wedge C) \vee (A \wedge \neg B \wedge \neg C)$
Konjunktive Normalform	Konjunktion von (oder eine einzelne) verallgemeinerten Disjunktionen Beispiel: $(A \vee B \vee C) \wedge (A \vee \neg B \vee \neg C)$
Kontradiction	Immer falsch
Tautologie	Immer wahr
Junktoren (/Konnektoren)	- Negation - Konjunktion - Disjunktion (einschliessliches oder) - Implikation - Äquivalenz
Bindungsstärke	- vor \wedge, \vee vor $\Rightarrow, \Leftrightarrow$

1.2. FORMELN

$$(A \Rightarrow B) \Leftrightarrow (\neg B \Rightarrow \neg A) \quad (A \Leftrightarrow B) \Leftrightarrow (A \wedge B) \vee (\neg A \wedge \neg B) \quad (A \vee B) \Leftrightarrow (\neg A \Rightarrow B)$$

$$(A \Rightarrow B) \Leftrightarrow (\neg A \Rightarrow \neg B) \quad (A \Leftrightarrow B) \Leftrightarrow (A \Rightarrow B) \wedge (B \Rightarrow A)$$

1.3. RECHENREGELN

Begriff	Bedeutung
Abtrennungsregel	$(A \wedge (A \Rightarrow B)) \Rightarrow B$
Kommutativität	$(A \wedge B) \Leftrightarrow (B \wedge A)$ $(A \vee B) \Leftrightarrow (B \vee A)$
Assoziativität	$A \wedge (B \wedge C) \Leftrightarrow (A \wedge B) \wedge C$ $A \vee (B \vee C) \Leftrightarrow (A \vee B) \vee C$
Distributivität	$A \wedge (B \vee C) \Leftrightarrow (A \wedge B) \vee (A \wedge C)$ $A \vee (B \wedge C) \Leftrightarrow (A \vee B) \wedge (A \vee C)$
Absorption	$A \vee (A \wedge B) \Leftrightarrow A$ $A \wedge (A \vee B) \Leftrightarrow A$
Idempotenz	$A \vee A = A$ $A \wedge A = A$
Doppelte Negation	$\neg(\neg A) \Leftrightarrow A$
Konstanten	$W = \text{wahr}$ $F = \text{falsch}$
de Morgan	$\neg(A \wedge B) \Leftrightarrow \neg A \vee \neg B$ $\neg(A \vee B) \Leftrightarrow \neg A \wedge \neg B$

2. PRÄDIKATENLOGIK

2.1. GLOSSAR

Begriff	Bedeutung
Subjekt	«Konkretes Ding» / Stellvertreter einer Variable
Prädikat	«Eigenschaft», z.B. «ist eine Primzahl» Prädikate werden oft wie Funktionen geschrieben. Ist P ein Prädikat, dann bedeutet $P(x)$, dass x das Prädikat erfüllt. $P(x)$ ist eine Aussageform.
Quantor	\forall Allquantor (Für alle) \exists Existenzquantor (Es existiert)

3. BEWEISEN

3.1. INDUKTION

$$A(1) \wedge (A(n) \Rightarrow A(n+1)) \Rightarrow A(m), m \in \mathbb{N}$$

TODO: besseres Beispiel

Beispiel: $2 \mid (6^n)$

1) Verankerung: $n = 0$

- $2 \mid (6^0)$
- 2) Induktionsschritt $n \rightarrow n + 1$
 - $2 \mid (6^{n+1})$
 - a) Induktionsannahme: $2 \mid (6^n)$
 - b) Behauptung: $2 \mid (6^{n+1})$
 - c) Beweis: Verwendung der Annahme, um Richtigkeit der Behauptung zu zeigen $2 \mid (6^n + 6)$

3.1.1. Techniken

- 1) Direkter Beweis $f(n) = f_1(n) = f_2(n) = \dots = f_m(n) = g(n)$
- 2) Differenz gleich Null $f(n) - g(n) = 0 \Rightarrow f(n) = g(n)$
- 3) Äquivalenzumformung
- 4) Dritte Grösse (vereinfachen) $g(n) = h(n) = f(n)$

4. DIREKTE, ITERATIVE UND REKURSIVE BERECHNUNGEN

4.1. GLOSSAR

Begriff	Bedeutung
Folge	Nummerierte Liste von Objekten (Folgegliedern)

Reihe Summe von Folgegliedern einer Zahlenfolge

5. MENGEN

5.1. GLOSSAR

Begriff	Bedeutung
Aufzählend	$\{1, 2, 3\}$
Beschreibend	$\{x \in \mathbb{N}^* \mid x < 4\}$
Mächtigkeit	Anzahl Elemente einer Menge $ M $
Potenzmenge	Menge aller Teilmengen einer Menge $P(M)$ $ P(M) = 2^{ M }$
Teilermenge	$T(n) = \text{Menge der Teiler der Zahl } n$
Kartesisches Produkt	$A \times B = \{(a, b) \mid a \in A, b \in B\}$

5.2. RECHENREGELN

Für die Mengen A und B in der Obermenge M gelten die folgenden Aussagen:

$$\begin{array}{llll} A \setminus \emptyset = A & A \cup \bar{A} = M & A \setminus B = A \cap \bar{B} & (A \setminus B) \setminus C = A \setminus (B \cup C) \\ A \setminus A = \emptyset & \bar{A} \cup \bar{A} = \bar{A} \cap \bar{B} & \bar{A} \setminus B = \bar{A} \cup B & A \setminus (B \setminus C) = (A \setminus B) \cup (A \cap C) \\ \bar{\bar{A}} = A & \bar{A} \cap \bar{B} = \bar{A} \cup \bar{B} & (A \setminus B) \cup (A \cap B) = A & A \setminus (A \setminus B) = A \cap B \\ A \cap \bar{A} = \emptyset & A \setminus \bar{A} = A \cap B & A \setminus (A \setminus B) = \emptyset & A \setminus (A \setminus B) = A \cap B \end{array}$$

6. FORMELN, ABBILDUNGEN, RELATIONEN

6.1. GLOSSAR

Begriff	Bedeutung
Funktion/Abbildung	Zuordnung, die jedem Element der Definitionsmenge D genau ein Element einer Zielmenge Z zuordnet. Injektive Relation: $f : D \rightarrow Z$ Abbildungen mit mehreren Argumenten: $f : A \times B \rightarrow Z, f(a, b) = y$
Graph	Menge von Paaren $(x, f(x))$ $G \in D \times Z$
Relation	Teilmenge des Kartesischen Produktes mehrerer Mengen $A = \bigcup_{i=1}^n A_i, A_i = n_i \Rightarrow A = \prod_{i=1}^n n_i$ - Kleiner-Relation: $R_c = \{(a, b) \mid a \in A, b \in B, a < b\}$ - Gleich-Relation: $R_e = \{(a, b) \mid a \in A, b \in B, a = b\}$ - Kleiner-Gleich-Relation: $R_s = R_c \cup R_e = \{(a, b) \mid a \in A, b \in B, a \leq b\}$
Surjektiv	Alle Elemente der Definitionsmenge und Zielmenge sind «verknüpft» / jedes Element der Bildmenge kommt als Bild vor
Injektiv	Alle Inputs haben eindeutige Outputs $a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_2)$
Bijektiv	Surjektiv und Injektiv
Reflexiv	Alle Elemente von A stehen zu sich selbst in Beziehung $a \in A \Rightarrow (a, a) \in R$ $A \subseteq A$
Symmetrisch	$(a, b) \in R \wedge (b, a) \in R$ $(A \leftrightarrow B) \Leftrightarrow (B \leftrightarrow A)$
Transitiv	$(a, b) \in R, (b, c) \in R \Rightarrow (a, c) \in R$ $(A \leftrightarrow B) \wedge (B \leftrightarrow C) \Rightarrow (A \leftrightarrow C)$
Äquivalenzrelation	reflexiv, symmetrisch und transitiv $\Leftrightarrow, =$

Begriff	Bedeutung
Irreflexiv	$a \in A \Rightarrow \neg(a, a) \in R$
Asymmetrisch	$(a, b) \in R \Rightarrow \neg(b, a) \in R$
Antisymmetrisch	$((a, b) \in R \wedge (b, a) \in R) \Rightarrow a = b$
Ordnungsrelation	reflexiv, antisymmetrisch und transitiv \leq
Symmetrische Differenz	$AAB = \{x \in G \mid (x \in A \wedge x \in B) \wedge \neg(x \in A \cap B)\}$ $AAB = (A \cup B) \setminus (A \cap B)$ $(A \Delta B) \Delta C = A \Delta (B \Delta C)$

7. MODULO-RECHNEN

Die Modulo-Relation ist eine Äquivalenzrelation auf \mathbb{Z} .

7.1. GLOSSAR

Begriff	Bedeutung
Teiler-Relation	Für $a, b \in \mathbb{Z}$ ist die Teiler-Relation $b \mid a \Leftrightarrow T(b, a) \Leftrightarrow \exists q \in \mathbb{Z} : bq = a$ $b \mid a \Leftrightarrow -b \mid a$ $b \mid a \Leftrightarrow b \mid -a$ Ordnungsrelation auf \mathbb{N}
Modulo-Relation	Für $a, q, r \in \mathbb{Z}$ ist die Modulo-Relation $R_q(a, r) \Leftrightarrow q \mid a - r \Leftrightarrow a \equiv r \pmod{q}$
Quotient, Rest	Zu jeder Zahl $a \in \mathbb{Z}$ und jeder Zahl $b \in \mathbb{Z}$ gibt es eindeutig bestimmte Zahlen $q, r \in \mathbb{Z}$ mit $a = q \cdot b + r, 0 \leq r < b$ Bsp: $7 = 2 \cdot 3 + 1$ q heißt Quotient r heißt Rest
Restklassen	$[b]_q = \{a \in \mathbb{Z} \mid a \equiv b \pmod{q}\}, q > 0$ $\mathbb{Z}_q = \{[0]_q, [1]_q, [2]_q, \dots, [q-1]_q\} = \{0, 1, 2, \dots, q-1\}$ Vereinfachung
Multiplikatives Inverses	Für $a \in \mathbb{Z}_q$ ist $b \in \mathbb{Z}_q$ das multiplikative Inverses von a , wenn $a \cdot b \equiv 1 \pmod{q}$
Nullteiler	Wenn für $a, b \in \mathbb{Z}_q : ab \equiv 0 \pmod{q}$ und $a \not\equiv 0 \pmod{q} \wedge b \not\equiv 0 \pmod{q}$, heissen a, b Nullteiler

7.2. RECHENREGELN

- 1) $(a + b) \pmod{n} = ((a \pmod{n}) + (b \pmod{n})) \pmod{n}$
- 2) $(a - b) \pmod{n} = ((a \pmod{n}) - (b \pmod{n})) \pmod{n}$
- 3) $(a \cdot b) \pmod{n} = ((a \pmod{n}) \cdot (b \pmod{n})) \pmod{n}$
- 4) $a^d \pmod{n} = (a^{d-x} \cdot a^x) \pmod{n} = ((a^{d-x} \pmod{n}) \cdot (a^x \pmod{n})) \pmod{n}$

7.3. PRIMFAKTORENZERLEGUNG

Begriff	Bedeutung
ggT(a, b)	$\max\{d \in \mathbb{N} \mid d \mid a \wedge d \mid b\}$
kgV(a, b)	$\min\{m \in \mathbb{N} \mid a \mid m \wedge b \mid m\}$ $\frac{ab}{\text{ggT}(a, b)}$
Teilerfremd	Zwei Zahlen $a, b \in \mathbb{N}$ heissen Teilerfremd, wenn $\text{ggT}(a, b) = 1$ Sei $p \in \mathbb{N}$ eine Primzahl und $q \in \mathbb{N}, q < p, q \neq 0$ dann ist $\text{ggT}(p, q) = 1$

7.4. EUKLIDSCHER ALGORITHMUS

Seien $a, b \in \mathbb{N}, a \neq b, a \neq 0, b \neq 0$	Initialisierung: Setze $x := a, y := b, q := x \div y, r := x - q \cdot y, (u, s, v, t) = (1, 0, 0, 1)$ (d.h. bestimme q und r so, dass $x = q \cdot y + r$ ist)
Wiederhole bis $r = 0$ ist	
Ergebnis: $y = \text{ggT}(a, b) = s \cdot a + t \cdot b$	
Wenn $\text{ggT}(a, b) = 1$ ist, dann folgt: $t \cdot v \equiv 1 \pmod{a}$	

7.5. ERWEITERTER EUKLIDSCHER ALGORITHMUS

Seien $a, b \in \mathbb{N}, a \neq b, a \neq 0, b \neq 0$	Initialisierung: Setze $x := a, y := b, q := x \div y, r := x - q \cdot y, (u, s, v, t) = (1, 0, 0, 1)$ (d.h. bestimme q und r so, dass $x = q \cdot y + r$ ist)
Wiederhole bis $r = 0$ ist	
Ergebnis: $y = \text{ggT}(a, b) = s \cdot a + t \cdot b$	
Wenn $\text{ggT}(a, b) = 1$ ist, dann folgt: $t \cdot v \equiv 1 \pmod{a}$	

7.5.1. Beispiel

ggT(99,79)

	$x = y_{-1}$	$y = r_{-1}$	$q = x \div y$	$r = x_i - q_i \cdot y_i$	$u = s_{-1}$	$s = u_{-1} - q_{-1} \cdot s_{-1}$	$v = t_{-1}$	$t = v_{-1} - q_{-1} \cdot t_{-1}$
$i = 0$	99	79	1	20	1	0	0	1
$i = 1$	79	20	3	19	0	1	1	-1
$i = 2$	20	19	1	1	-3	-1	4	
$i = 3$	19	1	19	0	-3	4	4	-5

Daraus folgend:

$$-\text{ggT}(99, 79) = 4 \cdot 99 + (-5) \cdot 79 \Leftrightarrow 396 - 395 = 1$$

$$-99 + (-5) = 94 \text{ ist mult. Inv. von 79 in } \mathbb{Z}_{99}$$

$$-79 + 4 = 83 \text{ ist mult. Inv. von 99 in } \mathbb{Z}_{79}$$

7.6. KLEINER FERMAT

Sei $p \in \mathbb{N}$ eine Primzahl und $x \in \mathbb{Z} \setminus \{0\}$ mit

$$\text{ggT}(x, p) = 1$$

Dann ist $x^{p-1} \equiv 1 \pmod{p}$

Daraus folgend:

$$x^{p-1} \equiv 1 \pmod{p} \quad | \cdot x^n$$

$$\Leftrightarrow x^{n(p-1)} \equiv 1 \pmod{p} \quad | \cdot x$$

$$\Leftrightarrow x^{1+n(p-1)} \equiv x \pmod{p}$$

$$\Leftrightarrow x^{1 \pmod{p-1}} \equiv x \pmod{p}$$

7.7. SATZ VON EULER

Sei $n \in \mathbb{N} \setminus \{0\}$ und $z \in \mathbb{Z}$ mit $\text{ggT}(z, n) = 1$. Dann ist $z^{\varphi(n)} \equiv 1 \pmod{n}$.7.7.1. Euler'sche φ -Funktion (Totient)Sei $n \in \mathbb{N} \setminus \{0\}$ und $\mathbb{Z}_n^* = \{x \in \mathbb{Z}_n \mid x \text{ hat ein multiplikatives Inverses in } \mathbb{Z}_n\}$.Dann heisst $\varphi(n)$:

$$\begin{aligned} \varphi(n) &= \text{Anz. Elemente in } \mathbb{Z}_n \text{ mit mult. Inversen} \\ &= \text{Anz. Zahlen } 1 \leq q \leq n \text{ mit } \text{ggT}(q, n) = 1 \\ &= |\mathbb{Z}_n^*| \end{aligned}$$

7.7.1.1. Rechenregeln

$$1) \text{ Sei } n \in \mathbb{N} \text{ eine Primzahl, dann } \varphi(n) = n - 1$$

$$2) \text{ Sei } n \in \mathbb{N} \text{ eine Primzahl und } p \in \mathbb{N} \setminus \{0\}, \text{ dann } \varphi(n^p) = n^{p-1} \cdot (n - 1)$$

$$3) \text{ Seien } m, n \in \mathbb{N} \setminus \{0\} \text{ und } \text{ggT}(m, n) = 1, \text{ dann } \varphi(n \cdot m) = \varphi(n) \cdot \varphi(m)$$

7.8. RSA VERSCHLÜSSELUNG

1) Wähle 2 Primzahlen p, q 2) Berechne $n = p \cdot q$ 3) Berechne $\varphi(n) = (p - 1)(q - 1)$ 4) Wähle a, b so, dass $a \cdot b \equiv 1 \pmod{\varphi(n)}$ 5) Vergesse $p, q, \varphi(p \cdot q)$. Brauchen wir nicht und riskieren nur, dass uns jemand hacktPublic key ist nun n, b , Private key ist n, a Verschlüsseln: $c^a \pmod{n}$ Entschlüsseln: $z^b \pmod{n} \Leftrightarrow c^{ab} \pmod{n}$ Sidenote: Fürs Alphabet muss n grösser sein als 26

8. LINEARE ALGEBRA

3b1b <3

8.1. GLOSSAR

Begriff	Bedeutung
Lineares Gleichungssystem (LGS)	
Homogenes LGS	$M \cdot \vec{x} = \vec{0}$
Inhomogenes LGS	$M \cdot \vec{x} = \vec{b}$
Lineare Abbildung	$L : \mathbb{R}^p \rightarrow \mathbb{R}^m$ $\vec{x} \mapsto M \vec{x}$ $\text{kern}(L) = \{\vec{0}\} \Leftrightarrow L \text{ ist injektiv}$
Kern	Lösungsmenge des Homogenen LGS = $\{\vec{x} \in \mathbb{R}^n \mid L(\vec{x}) = \vec{0}\}$
Koeffizientenmatrix	

8.2. PIVOT-GLEICHUNG

$$\begin{array}{ll} (\text{I}) & 1x_1 + 1x_2 + 1x_3 = -6 \\ (\text{II}) & x_1 + 2x_2 + 3x_3 = -10 \\ (\text{III}) & 2x_1 + 3x_2 + 6x_3 = -18 \\ \Rightarrow & \\ (\text{I}') & 1x_1 + 1x_2 + 1x_3 = -6 \\ (\text{II}') & 1x_2 + 2x_3 = -4 \\ (\text{III}') & 1x_2 + 4x_3 = -6 \\ \Rightarrow & \\ (\text{I}'') & 1x_1 + 1x_2 + 1x_3 = -6 \Rightarrow x_1 = -6 - x_2 - x_3 = -6 + 2 + 1 = -3 \\ (\text{II}'') & 1x_2 + 2x_3 = -4 \xrightarrow{\text{Rückwärtssubstitution}} x_2 = -4 - 2x_3 = -4 + 2 = -2 \\ (\text{III}'') & 1x_2 + 4x_3 = -6 \xrightarrow{\text{Rückwärtssubstitution}} x_3 = -6 + 2 = -4 \end{array}$$

8.3. GAUSS-TABLEAU

TODO: beispiel nullzeile

	x_1	x_2	x_3	1	
I	1		1	-6	
II	1	2	3	-10	-(I)
III	2	3	6	-18	-2(II)
					=
I'	1	1	1	-6	
II'	0	1	2	-4	
III'	0	1	4	-6	-(II')
					=
I''	1	1	1	-6	
II''	0	1	2	-4	
III''	0	0	2	-2	$\cdot \frac{1}{2}$
					=
I'''	1	1	1	-6	-(III'')
II'''	0	1	2	-4	-2(III'')
III'''	0	0	1	-1	
					=

Koeffizientenmatrix $A = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}$

	x_1	x_2	x_3	1	
I'''	1	1	0	-5	-(II'')
II'''	0	1	0	-2	
III'''	0	0	1	-1	
					=
	1	0	0	-3	
	0	1	0	-2	
	0	0	1	-1	

Ergebnisvektor $\vec{b} = \begin{pmatrix} -6 \\ -4 \\ -1 \end{pmatrix}$ Lösungsvektor $\vec{x} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$ Lineares Gleichungssystem $A \cdot \vec{x} = \vec{b}$ p = Anzahl Pivot-Variablen.Wenn $b_{p+1} = \dots = b_m = 0$ dann ist das LGS lösbar (homogenes Gleichungssystem), sonst unlösbar.Wenn $p = n$ dann hat LGS genau eine Lösung.Wenn $p < n$ dann hat LGS unendlich viele Lösungen.

8.4. VEKTOREN

8.4.1. Glossar

Begriff	Bedeutung
Vektor	Liste von Zahlen
Nullvektor	$\vec{0} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$
Ortsvektor	Ortsvektor \vec{p} vom Nullpunkt des Koordinatensystems $\begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$ zum Punkt P
Richtungsvektor	Richtungsvektor \vec{AB} vom Punkt A zum Punkt B ist $\vec{b} - \vec{a}$

Begriff

Bedeutung

Linearkombination der Variablen x_1, x_2, x_3 (Bsp. $3 \cdot x_1 - 2 \cdot x_2 + 4 \cdot x_3 = -6$). Vektoren werden jeweils mit einer Zahl multipliziert und miteinander summiertLineare Unabhängigkeit $\vec{v}_1, \vec{v}_2, \dots, \vec{v}_n$ heissen linear Unabhängig, wenn die Gleichung $\lambda_1 \cdot \vec{v}_1 + \lambda_2 \cdot \vec{v}_2 + \dots + \lambda_n \cdot \vec{v}_n = \vec{0}$ genau eine Lösung hat, nämlich $\lambda_1 = \lambda_2 = \dots = \lambda_n = 0$
 $\begin{pmatrix} \vec{v}_1 & \dots & \vec{v}_n \end{pmatrix} \cdot \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_n \end{pmatrix} = \vec{0}$ eindeutig lösbar = $\vec{v}_1, \dots, \vec{v}_n$ sind linear unabhängig

Vektorprodukt/Kreuzprodukt

$$\vec{a} \times \vec{b} = \vec{c}$$

$$\begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} \times \begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix} = \begin{pmatrix} a_2 b_3 - a_3 b_2 \\ a_3 b_1 - a_1 b_3 \\ a_1 b_2 - a_2 b_1 \end{pmatrix}$$

Skalarprodukt

$$\vec{a} \cdot \vec{b} = c$$

$$\begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} \cdot \begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix} = a_1 \cdot b_1 + a_2 \cdot b_2 + a_3 \cdot b_3$$

Orthogonale Projektion

$$\text{Betrag/Länge eines Vektors}$$

$$\vec{a} = \begin{pmatrix} 2 \\ -3 \\ 5 \end{pmatrix}$$

$$|\vec{a}| = \sqrt{2^2 + (-3)^2 + 5^2} = \sqrt{38}$$

Normalenvektor = Vektorprodukt?

8.4.2. Vektorenrechnen

Addition:

$$\vec{v} + \vec{w} = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} + \begin{pmatrix} 5 \\ -9 \\ 4 \end{pmatrix} = \begin{pmatrix} 1+5 \\ 2+(-9) \\ 3+4 \end{pmatrix} = \begin{pmatrix} 6 \\ -7 \\ 7 \end{pmatrix}$$

Multiplikation mit reellen Zahlen (=Skalare):

$$3 \cdot \vec{v} = 3 \cdot \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} = \begin{pmatrix} 3 \cdot 1 \\ 3 \cdot 2 \\ 3 \cdot 3 \end{pmatrix} = \begin{pmatrix} 3 \\ 6 \\ 9 \end{pmatrix}$$

8.4.3. Rechenregeln

Falls die Vektoren senkrecht zueinanderstehen, ist das Skalarprodukt gleich 0

$$\lambda \vec{0} = \vec{0}$$

$$\vec{v} + \vec{0} = \vec{v}$$

$$-\vec{v} + \vec{v} = \vec{0}$$

$$(\lambda \mu) \vec{v} = \lambda (\mu \vec{v}) = \lambda \mu \vec{v}$$

$$\lambda (\vec{v} + \vec{w}) = \lambda \vec{v} + \lambda \vec{w}$$

$$\vec{v} + (\vec{u} + \vec{w}) = (\vec{v} + \vec{u}) + \vec{w} = \vec{v} + \vec{u} + \vec{w}$$

8.4.4. Kreuzprodukt

$$\vec{a} \times \vec{b} = \begin{pmatrix} a_x \\ a_y \\ a_z \end{pmatrix} \times \begin{pmatrix} b_x \\ b_y \\ b_z \end{pmatrix}$$

$$\begin{array}{l} \cancel{a_x} \times \cancel{b_x} \\ \cancel{a_y} \times \cancel{b_y} \\ \cancel{a_z} \times \cancel{b_z} \end{array} \Rightarrow \begin{array}{l} a_y b_z - a_z b_y \\ + a_z b_x - a_x b_z \\ + a_x b_y - a_y b_x \end{array} \Rightarrow \vec{a} \times \vec{b} = \begin{pmatrix} a_y b_z - a_z b_y \\ a_z b_x - a_x b_z \\ a_x b_y - a_y b_x \end{pmatrix}$$

8.4.4.1. Eigenschaften

Anti-kommutativ: $\vec{a} \times \vec{b} = -\vec{b} \times \vec{a}$. Konsequenz: $\vec{a} \times \vec{a} = -\vec{a} \times \vec{a} = \vec{0}$ Distributiv: $\vec{a} \times (\vec{b} + \vec{c}) = \vec{a} \times \vec{b} + \vec{a} \times \vec{c}$ Gemischt-assoziativ: $\lambda(\vec{a} \times \vec{b}) = (\lambda \vec{a}) \times \vec{b} = \vec{a} \times (\lambda \vec{b})$ Das Kreuzprodukt ist nicht assoziativ. $\vec{a} \times \vec{b} \times \vec{c}$ darf man nicht! $(\vec{a} \times \vec{b}) \times \vec{c} \neq \vec{a} \times (\vec{b} \times \vec{c})$

8.4.4.2. Geometrische Eigenschaften

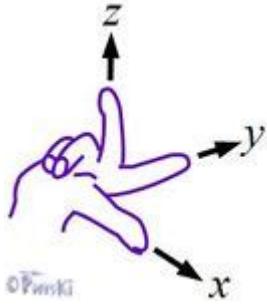
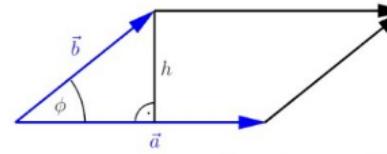


Abbildung 1: Rechtssystem

$\vec{a} \times \vec{b}$ steht immer senkrecht auf \vec{a} und auf \vec{b} .

$\vec{a}, \vec{b}, \vec{a} \times \vec{b}$ bilden ein Rechtssystem

$|\vec{a} \times \vec{b}| = \text{Flächeninhalt des durch } \vec{a} \text{ und } \vec{b} \text{ aufgespannten Parallelogramms} = |\vec{a}| \cdot |\vec{b}| \cdot \sin(\varphi)$

Abbildung 2: Flächeninhalt $h \cdot a$

8.4.5. Vektorraum

Ein Vektorraum ist eine Menge V mit den Rechenoperationen:

$$\oplus : V \times V \rightarrow V, (\vec{v}, \vec{w}) \mapsto \vec{v} \oplus \vec{w}$$

$$\circ : \mathbb{R} \times V \rightarrow V, (\lambda, \vec{v}) \mapsto \lambda \circ \vec{v}$$

Mit den Eigenschaften:

- Vektoraddition:
Assoziativgesetz: $u \oplus (v \oplus w) = (u \oplus v) \oplus w$
Existenz eines neutralen Elements $0_V \in V$ mit $v \oplus 0_V = 0_V \oplus v = v$
Existenz eines **inversen Elements** $-v \in V$ mit $v \oplus (-v) = (-v) \oplus v = 0_V$
- Kommutativgesetz: $v \oplus u = u \oplus v$
- Skalarmultiplikation:
 $\alpha \circ (u \oplus v) = (\alpha \circ u) \oplus (\alpha \circ v)$
 $(\alpha + \beta) \circ v = (\alpha \circ v) \oplus (\beta \circ v)$
 $(\alpha \cdot \beta) \circ v = \alpha \circ (\beta \circ v)$
- $1 \circ v = v$ für das **Einselement** $1 \in K$ des **Skalkörpers**

Gelten diese Eigenschaften für die Teilmenge eines grösseren Vektorraums W , so nennt man V **Untervektorraum** von W . Heisst: Man hat nur dann einen Untervektorraum V , wenn die Produkte der Multiplikation oder Addition der Elemente dieses Raumes auch in V liegen. Untervektorräume sind also unendliche Räume mit n Dimensionen weniger, zB $W = 3$ -Dimensionaler Vektorraum, $V = 2$ -Dimensionaler Untervektorraum.

Kern von $A = U = \{\vec{x} \in \mathbb{R}^n \mid A\vec{x} = \vec{0}\}$, $A \in \mathbb{R}^{m \times n}$ ist ein Untervektorraum von \mathbb{R}^n .

8.4.6. Lineare Abbildung

Eine Lineare Abbildung ist eine Funktion

$$L : \begin{cases} \mathbb{R}^n \rightarrow \mathbb{R}^m \\ \vec{x} \mapsto L(\vec{x}) \end{cases}$$

mit den Eigenschaften

$$L(\vec{x} + \vec{y}) = L(\vec{x}) + L(\vec{y})$$

$$L(\lambda \vec{x}) = \lambda L(\vec{x})$$

Für jede lineare Abbildung $L : \mathbb{R}^n \rightarrow \mathbb{R}^m$ gibt es eine (Abbildungs) Matrix $M \in \mathbb{R}^{m \times n}$ mit der Eigenschaft, dass $L(\vec{x}) = M\vec{x}$

$$M = \begin{pmatrix} m_{11} & \dots & m_{1n} \\ \vdots & \ddots & \vdots \\ m_{m1} & \dots & m_{mn} \end{pmatrix}$$

$$m_{ij} = \vec{e}_i \cdot L(\vec{e}_j)$$

8.5. MATRIZEN

8.5.1. Glossar

Begriff	Bedeutung
Spaltenvektoren	Spalten der Matrix als Vektoren
Zeilenvektoren	Zeilen der Matrix als Vektoren
Rang	Wieviele Spaltenvektoren einer Matrix linear unabhängig sind
Nullmatrix	$0 = \begin{pmatrix} 0 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 0 \end{pmatrix}$
Quadratische Matrix	$M \in \mathbb{R}^{n \times n}$ Gleichviele Zeichen und Spalten

Begriff	Bedeutung
Diagonalmatrix	(immer quadratisch und symmetrisch): $D = \begin{pmatrix} x_1 & 0 & 0 & 0 \\ 0 & x_2 & 0 & 0 \\ 0 & 0 & x_3 & 0 \\ 0 & 0 & 0 & x_4 \end{pmatrix}, d_{ij} = 0 \text{ für } i \neq j$
Einheitsmatrix	(immer diagonal): $E = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$
Symmetrische Matrix	(immer quadratisch): $A = A^T, a_{ij} = a_{ji} \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 4 & 4 \\ 3 & 4 & 1 \end{pmatrix}$
Obere Dreiecksmatrix	$O = \begin{pmatrix} x_1 & x_2 & x_3 \\ 0 & x_2 & x_3 \\ 0 & 0 & x_3 \end{pmatrix}, o_{ij} = 0 \text{ für } i > j$
Kovarianzmatrix	immer symmetrisch
Reguläre Matrix	Quadratische Matrix mit höchstem Rang (Rang = Anzahl Spalten/Reihen)
Singuläre Matrix	Quadratische Matrix mit kleinerem Rang (Rang < Anzahl Spalten/Reihen)
Invertierbare Matrix	Für $A \in \mathbb{R}^{n \times n}$ heisst A invertierbar, wenn es eine Matrix A^{-1} gibt, so dass $A \cdot A^{-1} = A^{-1} \cdot A = \text{Einheitsmatrix } (E)$. Dies ist der Fall, wenn A Regular ist.

8.5.2. Definition

Matrix mit 2 Zeilen und 3 Spalten

$$A = \begin{pmatrix} 1 & 4 & 5 \\ 2 & 3 & 7 \end{pmatrix} \in \mathbb{R}^{2 \times 3}$$

Komponenten von A : a_{ij}

i: Zeilenindex, j: Spaltenindex. Bsp: $a_{23} = 7$

8.5.3. Matrizen als Vektoren interpretieren

→ A ist ein 6-Dimensionaler VR (Vektorraum)

$$\text{Variante 1: } \begin{pmatrix} a_{11} \\ a_{12} \\ a_{13} \\ a_{14} \\ a_{15} \\ a_{16} \end{pmatrix} = \begin{pmatrix} 1 \\ 4 \\ 5 \\ 2 \\ 3 \\ 7 \end{pmatrix}, \text{ Variante 2: } \begin{pmatrix} a_{11} \\ a_{12} \\ a_{13} \\ a_{14} \\ a_{15} \\ a_{16} \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \\ 4 \\ 3 \\ 5 \\ 7 \end{pmatrix}$$

$$\mathbb{R}^n \text{ interpretiere als } \begin{cases} \mathbb{R}^{n \times 1} \rightarrow \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \text{ Spaltenvektor} \\ \mathbb{R}^{1 \times n} \rightarrow (a_1 \ a_2 \ \dots \ a_n) \text{ Zeilenvektor} \end{cases}$$

Zu A gehörige Zeilenvektoren $\vec{a}_1 = (1 \ 4 \ 5), \vec{a}_2 = (2 \ 3 \ 7)$

$$A = \begin{pmatrix} \leftarrow \vec{a}_1 \rightarrow \\ \leftarrow \vec{a}_2 \rightarrow \end{pmatrix} = \begin{pmatrix} 1 & 4 & 5 \\ 2 & 3 & 7 \end{pmatrix}$$

Zu A gehörige Spaltenvektoren $\vec{a}_1 = \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \vec{a}_2 = \begin{pmatrix} 4 \\ 3 \end{pmatrix}, \vec{a}_3 = \begin{pmatrix} 5 \\ 7 \end{pmatrix}$

$$A = \begin{pmatrix} \uparrow \vec{a}_1 \uparrow \vec{a}_2 \uparrow \vec{a}_3 \\ \downarrow \quad \downarrow \quad \downarrow \end{pmatrix} = \begin{pmatrix} 1 & 4 & 5 \\ 2 & 3 & 7 \end{pmatrix}$$

8.5.4. Matrizen transponieren

Transponierte Matrix $A \in \mathbb{R}^{m \times n}$ wäre: $A^T \in \mathbb{R}^{n \times m}$

$$A = (a_{ij}), A^T = (a_{ji})$$

Rolle von Zeile und Spalte vertauscht: $a_{ij} \rightarrow a_{ji}$

Bsp:

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 2 \\ 3 & 1 \end{pmatrix} \in \mathbb{R}^{3 \times 2}, A^T = \begin{pmatrix} 1 & 0 & 3 \\ 0 & 2 & 1 \end{pmatrix} \in \mathbb{R}^{2 \times 3}, \begin{pmatrix} 1 \\ 4 \\ 5 \end{pmatrix}^T = (1 \ 4 \ 5)$$

8.5.5. Matrizen invertieren

$$A = \begin{pmatrix} -1 & -2 \\ 3 & 1 \end{pmatrix}$$

$$\begin{pmatrix} -1 & -2 \\ 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 2 \\ 3 & 1 \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 2 \\ 0 & -5 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 3 & 1 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 2 \\ 0 & -5 \end{pmatrix} \begin{pmatrix} -1 & 0 \\ \frac{3}{5} & -\frac{1}{5} \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} -\frac{1}{5} & \frac{2}{5} \\ \frac{3}{5} & -\frac{1}{5} \end{pmatrix}$$

$$A^{-1} = \begin{pmatrix} -\frac{1}{5} & \frac{2}{5} \\ \frac{3}{5} & -\frac{1}{5} \end{pmatrix}$$

8.5.6. Matrixmultiplikation

Meistens nicht kommutativ ($A \cdot B \neq B \cdot A$)

B muss genau gleich viele Zeilen haben wie A Spalten

$$A \in \mathbb{R}^{m \times l}, B \in \mathbb{R}^{l \times n}, C = A \cdot B \in \mathbb{R}^{m \times n}$$

$$c_{ij} = \sum_{k=1}^l a_{ik} b_{kj}$$

$$\begin{pmatrix} 2 & 3 & 1 \\ 4 & -1 & 7 \end{pmatrix} \cdot \begin{pmatrix} 6 & 4 \\ 1 & 0 \\ 8 & 9 \end{pmatrix} = \begin{pmatrix} (2 \cdot 6 + 3 \cdot 1 + 1 \cdot 8) & (2 \cdot 4 + 3 \cdot 0 + 1 \cdot 9) \\ (4 \cdot 6 + -1 \cdot 1 + 7 \cdot 8) & (4 \cdot 4 + -1 \cdot 0 + 7 \cdot 9) \end{pmatrix} = \begin{pmatrix} 23 & 17 \\ 79 & 79 \end{pmatrix}$$

8.5.7. Determinante

Determinante einer quadratischen Matrix ist eine reelle Zahl

$$1 \times 1 \text{ Matrix: } \det(a) = a$$

$$2 \times 2 \text{ Matrix: } \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - cb$$

$$3 \times 3 \text{ Matrix: } \det \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{31}a_{22}a_{13} - a_{32}a_{23}a_{11} - a_{33}a_{21}a_{12}$$

Bsp:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} e \\ f \end{pmatrix}$$

$$x = \frac{\det(f \ b)}{\det(c \ d)} = \frac{ed - fb}{ad - cb}$$

$$y = \frac{\det(a \ e)}{\det(c \ d)} = \frac{af - ce}{ad - cb}$$

Definition der Determinante:

$$\det : \begin{cases} \mathbb{R}^{n \times n} \rightarrow \mathbb{R} \\ M \mapsto \det(M) \end{cases}$$

Definition über Eigenschaften:

$$\det(1) = 1$$

$$\det \begin{pmatrix} \dots & \vec{a}_1 & \dots \\ \dots & \lambda \vec{a}_k & \dots \\ \dots & \vec{a}_n & \dots \end{pmatrix} = \lambda \det \begin{pmatrix} \dots & \vec{a}_1 & \dots \\ \dots & \vec{a}_k & \dots \\ \dots & \vec{a}_n & \dots \end{pmatrix}$$

$$\det \begin{pmatrix} \dots & \vec{a}_1 & \dots \\ \dots & \vec{a}_k + \vec{b}_k & \dots \\ \dots & \vec{a}_n & \dots \end{pmatrix} = \det \begin{pmatrix} \dots & \vec{a}_1 & \dots \\ \dots & \vec{a}_k & \dots \\ \dots & \vec{a}_n & \dots \end{pmatrix} + \det \begin{pmatrix} \dots & \vec{a}_1 & \dots \\ \dots & \vec{b}_k & \dots \\ \dots & \vec{a}_n & \dots \end{pmatrix}$$

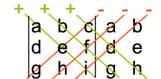
$\det M = 0$ wenn M 2 gleiche Zeilen hat

$$\det \begin{pmatrix} 1 & 2 & 3 \\ 8 & 10 & 12 \\ 1 & 1 & 4 \end{pmatrix} = 2 \det \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 1 & 1 & 4 \end{pmatrix}$$

$$\det \begin{pmatrix} 1 & 2 & 3 \\ 8 & 10 & 12 \\ 1 & 1 & 4 \end{pmatrix} = \det \begin{pmatrix} 1 & 0 & 0 \\ 8 & 10 & 12 \\ 1 & 1 & 4 \end{pmatrix} + \det \begin{pmatrix} 0 & 2 & 3 \\ 8 & 10 & 12 \\ 1 & 1 & 4 \end{pmatrix}$$

$$\det \begin{pmatrix} 1 & 2 & 3 \\ 8 & 10 & 12 \\ 1 & 1 & 4 \end{pmatrix} = \det \begin{pmatrix} 1 & 0 & 0 \\ 8 & 10 & 12 \\ 1 & 1 & 4 \end{pmatrix} + 2 \det \begin{pmatrix} 0 & 1 & 0 \\ 8 & 10 & 12 \\ 1 & 1 & 4 \end{pmatrix} + 3 \det \begin{pmatrix} 0 & 0 & 1 \\ 8 & 10 & 12 \\ 1 & 1 & 4 \end{pmatrix}$$

Bsp:



Georgiy Shevoroshkin
9.3. NULLTEILER VON \mathbb{Z}_n FINDEN

Multiplicationstabelle?
Können nicht Teilerfremd zu n sein.

Können nicht Teilerfremd zu n sein.
9.4. ELEMENTE VON \mathbb{Z}_n^* FINDEN (MULT. INV. IN \mathbb{Z}_n)

Multiplicationstabelle?

9.5. $|\mathbb{Z}_n^*|$ BERECHNEN
 $|\mathbb{Z}_n^*| = \varphi(n)$

9.6. LÖSUNGSMENGE GAUSS-TABLEAU MIT NULLZEILE
⇒ Unlösbar

1	0	2	3
0	1	1	0
0	0	0	4

$$x_1 = 3 - 2t, x_2 = -t, x_3 = t$$

1	0	2	3
0	1	1	0
0	0	0	4

9.7. DISJUNKTIVE/KONJUNKTIVE NORMALFORM ANGEBEN

Wahrheitstafel. Für konjunktive Normalform zuerst disjunktive erstellen, danach negieren und umformen. Beispiel:

$$\neg R = (A \wedge B \wedge C) \vee (A \wedge \neg B \wedge C) \Leftrightarrow R = \neg(A \wedge B \wedge C) \wedge \neg(A \wedge \neg B \wedge C) \Leftrightarrow R = (\neg A \vee \neg B \vee \neg C) \wedge (\neg A \vee B \vee \neg C)$$

9.8. $x^y \bmod p$ BERECHNEN
Rechenregeln Totient ($\varphi(p)$)

9.9. ZAHL $x \in \mathbb{Z}_n$ FINDEN, FÜR DIE $y \cdot x \equiv 1 \bmod n$ GILT (MULT. INV.)

Falls $\text{ggT}(y, n) \neq 1 \Rightarrow$ gibt kein mult. Inv. Ansonsten: Euklidischer Algorithmus.

Beispiel: $x \in \mathbb{Z}_{32}, 21 \cdot x \equiv 1 \bmod 32$

x	y	q	r	u	s	v	t
32	21	1	11	1	0	0	1
21	11	1	10		1	-1	
11	10	1	1		-1	2	
10	1	10	0		2	-3	

$$\Rightarrow x = -3 + 32 = 29$$

Beispiel: $x \in \mathbb{Z}_{32}, 22 \cdot x \equiv 1 \bmod 32$

$\text{ggT}(22, 32) = 2 \Rightarrow$ gibt kein mult. Inv.

9.10. AUS GERADEN G_1 UND G_2 FOLGENDES HERAUSFINDEN:
Gegeben: $G_1 = (2; 3) \cdot \vec{x} - 1 = 0, G_2 = (3; 4) \cdot \vec{x} + 5 = 0, P = (1; 1)$

Welche Gerade liegt näher an Punkt P :

Hessesche Normalenform

$$\left| \begin{pmatrix} 2 \\ 3 \end{pmatrix} \right| = \sqrt{13}$$

$$G_1 = \frac{1}{\sqrt{13}} \cdot (2; 3) \cdot \vec{x} - \frac{1}{\sqrt{13}} = 0$$

Abstand

$$a_1 = \frac{1}{\sqrt{13}} \cdot (2; 3) \cdot \left(\begin{pmatrix} 1 \\ 1 \end{pmatrix} \right) - \frac{1}{\sqrt{13}} = \frac{4}{\sqrt{13}}$$

Hessesche Normalenform

$$\left| \begin{pmatrix} 3 \\ 4 \end{pmatrix} \right| = 5$$

$$G_2 = \left(\frac{3}{5}; \frac{4}{5} \right) \cdot \vec{x} + 5 = 0$$

Abstand

$$a_2 = \left(\frac{3}{5}; \frac{4}{5} \right) \cdot \left(\begin{pmatrix} 1 \\ 1 \end{pmatrix} \right) + 5 = \frac{12}{5}$$

$$\frac{4}{\sqrt{13}} < \frac{12}{5} \Rightarrow G_1$$

Wo schneiden sich die Geraden: Koordinatengleichung

$$2s_x + 3s_y = 1$$

$$3s_x + 4s_y = -5$$

$$S = (-19; 13)$$

Für welche Gerade liegt P auf derselben Seite wie der Ursprung: Ursprung in HNF einsetzen

$$\text{Abstand } b_1 = \frac{1}{\sqrt{13}} \cdot (2; 3) \cdot \left(\begin{pmatrix} 0 \\ 0 \end{pmatrix} \right) - \frac{1}{\sqrt{13}} = -\frac{1}{\sqrt{13}}$$

$b_1 < 0 \wedge a_1 > 0 \Rightarrow$ verschiedene Seiten

Abstand

$$b_2 = \left(\frac{3}{5}; \frac{4}{5} \right) \cdot \left(\begin{pmatrix} 0 \\ 0 \end{pmatrix} \right) + 1 = 1$$

$b_1 > 0 \wedge a_1 > 0 \Rightarrow$ dieselben Seiten

9.11. EBENEN

Gegeben: Punkte $A = (-1; 1; 4), B = (-7; 3; 1), C = (2; 1; 5)$

Ebene $E \in \mathbb{R}^3$ verläuft durch oben genannte Punkte. Gib sie in Parameterform unter Verwendung des Ortsvektors zum Punkt A als Stützvektor an:

$$\vec{AB} = \begin{pmatrix} -6 \\ 2 \\ -3 \end{pmatrix}, \vec{AC} = \begin{pmatrix} 3 \\ 0 \\ 1 \end{pmatrix}$$

$$E: \begin{pmatrix} -1 \\ 1 \\ 4 \end{pmatrix} + s \begin{pmatrix} -6 \\ 2 \\ -3 \end{pmatrix} + t \begin{pmatrix} 3 \\ 0 \\ 1 \end{pmatrix}$$

Hessesche Normalenform der Ebene E :

$$\vec{n} = \begin{pmatrix} -6 \\ 2 \\ -3 \end{pmatrix} \times \begin{pmatrix} 3 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 2 \\ -3 \\ -6 \end{pmatrix}$$

$$|\vec{n}| = 7, \vec{n}_0 = \begin{pmatrix} \frac{2}{7} \\ -\frac{3}{7} \\ -\frac{6}{7} \end{pmatrix}, b_0 = \begin{pmatrix} -1 \\ 1 \\ 4 \end{pmatrix} \cdot \vec{n}_0 = -\frac{29}{7}$$

$$E: (\vec{x} - \vec{a}) \cdot \vec{n}_0 = 0 \Leftrightarrow \vec{x} \cdot \vec{n}_0 - b_0 = 0$$

$$\text{Abstand des Punktes } Q = (10; 2; -1) \text{ von der Ebene } E: \begin{pmatrix} 10 \\ 2 \\ -1 \end{pmatrix} \cdot \vec{n}_0 - b_0$$

$$\text{Für welchen Wert von } z \text{ liegt } R = (-4; 1; z) \text{ auf der Ebene } E: \begin{pmatrix} -4 \\ 1 \\ z \end{pmatrix} \cdot \vec{n}_0 - b_0 = 0$$

9.12. RSA VERSCHLÜSSELUNG

Gegeben: $n = 119$

Zahlen angeben, die als Schlüssel infrage kommen: Teilerfremd zu $\varphi(n)$

Zum Schlüssel a den Schlüssel b berechnen: Euklidischer Algorithmus mit $\varphi(n), a$

Mit dem Schlüssel a die Zahl x ent- / verschlüsseln: $x^a \bmod n$

9.13. ALLE ELEMENTE VON $R = \{(a, b) \in M \times M \mid a \cdot b \equiv 1 \pmod{x}\}$

9.14. ALLE ELEMENTE VON $R = \{(a, b) \in \mathbb{Z}_n^* \times \mathbb{Z}_n^* \mid a \cdot b \equiv y \pmod{x}\}$

Falls y teilerfremd zu x : Multiplicationstabelle mit Fremdteilern zu x erstellen.

.	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

Beispiel: $R = \{(a, b) \in \mathbb{Z}_{12}^* \times \mathbb{Z}_{12}^* \mid a \cdot b \equiv 7 \pmod{12}\}$

$$= \{(1, 7), (5, 11), (7, 1), (11, 5)\}$$

9.15. LÖSUNG VON $M \cdot \vec{x} = \vec{y}$ ZU \vec{x}

$$\vec{x} = M^{-1} \cdot \vec{y}$$

9.16. EIGENWERTE DER MATRIX M BERECHNEN

9.17. EIGENVEKTOREN DER MATRIX M BERECHNEN