

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: $(A \vee B \vee C) \wedge (A \vee \neg B \vee \neg C)$
Kontradiktion	Immer falsch
Tautologie	Immer wahr
Junktoren (/Konnektoren)	- Negation - Konjunktion - Disjunktion (einschliessliches oder) - Implikation - Äquivalenz
Bindungsstärke	- vor \wedge, \vee vor $\Rightarrow, \Leftrightarrow$

1.2. FORMELN

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

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

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

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

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:

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

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
----------	--

$$A = \prod_{i=1}^n A_i, |A_i| = n_i \Rightarrow |A| = \prod_{i=1}^n n_i$$

- Kleiner-Relation: $R_< = \{(a, b) \mid a \in A, b \in B, a < b\}$
- Gleich-Relation: $R_ = = \{(a, b) \mid a \in A, b \in B, a = b\}$
- Kleiner-Gleich-Relation: $R_ \leq = R_< \cup R_ = = \{(a, b) \mid a \in A, b \in B, a \leq b\}$

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 $a \in A \Rightarrow (a, a) \in R$
----------	---

Symmetrisch	$(a, b) \in R \wedge (b, a) \in R$ $(A \Leftrightarrow B) \Leftrightarrow (B \Leftrightarrow A)$
-------------	---

Transitiv	$(a, b) \in R \wedge (b, c) \in R \Rightarrow (a, c) \in R$ $(A \Rightarrow B) \wedge (B \Rightarrow C) \Rightarrow (A \Rightarrow C)$
-----------	---

Äquivalenzrelation	reflexiv, symmetrisch und transitiv \Leftrightarrow
--------------------	---

Irreflexiv	$a \in A \Rightarrow \neg(a, a) \in R$
------------	--

Begriff	Bedeutung
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	$\Delta B = \{x \in G \mid (x \in A \vee B) \wedge \neg(x \in A \wedge B)\}$ $\Delta B = (A \cup B) \setminus (A \cap B)$ $\Delta(A \Delta B) \Delta C = A \Delta(B \Delta C)$

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 $b \mid a \Leftrightarrow T(b, a) \Leftrightarrow \exists q \in \mathbb{Z} : bq = a$ $b \mid a \Leftrightarrow a \mid b \mid a$ $b \mid a \Leftrightarrow \neg b \mid a$
Modulo-Relation	Für $a, q, r \in \mathbb{Z}$ ist die Modulo-Relation $R_q(a, r) \Leftrightarrow q \mid a - r \Leftrightarrow a \equiv r \pmod{q}$ $\Leftrightarrow \text{relates to } a - b \Leftrightarrow (a, b) \in R$
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 $a = qb + r$, $0 \leq r < b$ Bsp: $7 = 2 \cdot 3 + 1$ q heißt Quotient r heißt Rest
Restklassen	$[b]_q = \{a \in \mathbb{Z} \mid a \equiv b \pmod{q}\}$ $\mathbb{Z}_q = \{[0]_q, [1]_q, [2]_q, \dots, [q-1]_q\} = \{0, 1, 2, \dots, q-1\}$
Multiplikatives Inverses	Für $a \in \mathbb{Z}_q$ ist $a^{-1} \in \mathbb{Z}$ das multiplikative Inverse 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 $a \not\equiv 0 \pmod{q}$ und $b \not\equiv 0 \pmod{q}$, heissen a, b Nullteiler
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

x = y ₋₁	y = r ₋₁	q = x div y	r = x mod y = x - q · y
i = 0	122	72	1
i = 1	72	50	1
i = 2	50	22	2
i = 3	22	6	3
i = 4	6	4	1
i = 5	4	2 = ggT(122, 72)	0 (immer 0 am Schluss)

7.5. ERWEITETER 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

$$\text{ggT}(99, 79)$$

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

Daraus folgend:

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

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

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

7.6. KLEINER FERMAT

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

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

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

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

Daraus folgend:

$$-\text{ggT}(x, p) = 1 \quad \Leftrightarrow x^{n(p-1)} \equiv x \pmod{p}$$

$$-\text{ggT}(x, p) = 1 \quad \Leftrightarrow x^{1 \mod (p-1)} \equiv x \pmod{p}$$

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) Sei $n \in \mathbb{N}$ eine Primzahl, dann $\varphi(n) = n - 1$ 2) Sei $n \in \mathbb{N}$ eine Primzahl und $p \in \mathbb{N} \setminus \{0\}$, dann $\varphi(n^p) = n^{p-1} \cdot (n - 1)$ 3) Seien $m, n \in \mathbb{N} \setminus \{0\}$ und $\text{ggT}(m, n) = 1$, 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: $z^b \pmod{n} \Leftrightarrow c^a \pmod{n}$ Sidenote: Fürs Alphabet muss n grösser sein als 26

8. LINEARE ALGEBRA

3b1b <3

8.1. GLOSSAR

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

8.2. PIVOT-GLEICHUNG

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

8.3. GAUSS-TABLEAU

	x_1	x_2	x_3	1	
I	1	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 $\vec{b} = \begin{pmatrix} -6 \\ -4 \\ -2 \end{pmatrix}$ 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

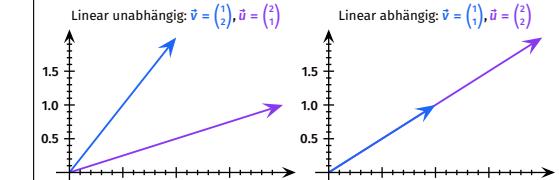
Begriff	Bedeutung
Vektor	Liste von Zahlen
Nullvektor	$\vec{0} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$
Ortsvektor	Ortsvektor \vec{p} vom Nullpunkt des Koordinatensystems $\begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$ zum Punkt P

Richtungsvektor	Richtungsektor \vec{AB} vom Punkt A zum Punkt B ist $\vec{b} - \vec{a}$
	$A = (1; 1), B = (2; 3), \vec{AB} = \begin{pmatrix} 1 \\ 3 \end{pmatrix}$

Linear kombination 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 summiert

Begriff

Bedeutung

Lineare 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
 $\lambda_1 = \lambda_2 = \dots = \lambda_n = 0$
 $\begin{pmatrix} \vec{v}_1 & \dots & \vec{v}_n \end{pmatrix} \cdot \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} = \vec{0}$ eindeutig lösbar = $\vec{v}_1, \dots, \vec{v}_n$ sind linear unabhängig

Skalarprodukt

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

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

8.4.2. Vektorenrechnen

Addition:

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

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

$$\begin{aligned} \lambda \vec{v} &= \lambda \vec{u} + \lambda \vec{w} \\ (\lambda \mu) \vec{v} &= \lambda (\mu \vec{v}) = \lambda \mu \vec{v} \\ \lambda(\vec{v} + \vec{w}) &= \lambda \vec{v} + \lambda \vec{w} \\ \vec{v} + (\vec{u} + \vec{w}) &= (\vec{v} + \vec{u}) + \vec{w} = \vec{v} + \vec{u} + \vec{w} \end{aligned}$$

8.4.4. Kreuzprodukt

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

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

8.4.4.1. EigenschaftenAnti-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**

$\vec{a} \times \vec{b}$ steht immer senkrecht auf \vec{a} und auf \vec{b} .
 $\vec{a}, \vec{b}, \vec{a} \times \vec{b}$ bilden ein Rechtssystem

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

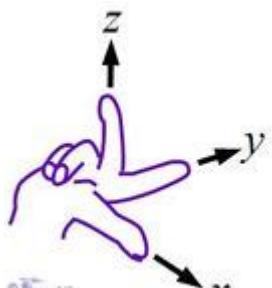


Abbildung 1: Rechtssystem

8.4.5. VektorraumEin Vektorraum ist eine Menge V mit den Rechenoperationen:

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

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

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:

– $\alpha \odot (u \oplus v) = (\alpha \odot u) \oplus (\alpha \odot v)$ – $(\alpha + \beta) \odot v = (\alpha \odot v) \oplus (\beta \odot v)$ – $(\alpha \cdot \beta) \odot v = \alpha \odot (\beta \odot v)$ – $1 \odot v = v$ 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

Beispiel

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

mit den Eigenschaften

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

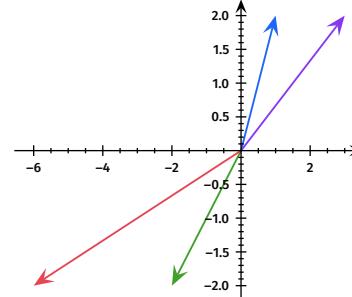
Für jede lineare Abbildung $L : \mathbb{R}^n \rightarrow \mathbb{R}^m$ gibt es eine (Abbildungs) Matrix $M \in \mathbb{R}^{m \times n}$ mit der Eigenschaft, dass $L(\vec{x}) = M\vec{x}$

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

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

$$M = \begin{pmatrix} -2 & 0 \\ 0 & -1 \end{pmatrix}, \vec{a} = \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \vec{b} = \begin{pmatrix} 3 \\ 2 \end{pmatrix}$$

$$\vec{c} = M\vec{a} = \begin{pmatrix} -2 \\ -2 \end{pmatrix}, \vec{d} = M\vec{b} = \begin{pmatrix} -6 \\ -2 \end{pmatrix}$$



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

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

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

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

$$\begin{pmatrix} 1 \\ 4 \\ 5 \end{pmatrix}^T = (1 \ 4 \ 5)$$

8.5.4. Matrizen transponierenTransponierte 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

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

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

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

8.5.6. MatrixmultiplikationMeistens 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:

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

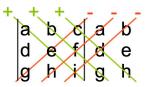
$$x = \frac{\det \begin{pmatrix} e & b \\ f & d \end{pmatrix}}{\det \begin{pmatrix} a & b \\ c & d \end{pmatrix}} = \frac{ed - fb}{ad - cb}$$

$$y = \frac{\det \begin{pmatrix} a & e \\ c & f \end{pmatrix}}{\det \begin{pmatrix} a & b \\ c & d \end{pmatrix}} = \frac{af - ce}{ad - cb}$$

Definition der Determinante:

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

Definition über Eigenschaften:

Komponenten von A : a_{ij} i : Zeilenindex, j : Spaltenindex. Bsp: $a_{23} = 7$ **8.5.3. Matrizen als Vektoren interpretieren** $\rightarrow A$ ist ein 6-Dimensional VR (Vektorraum)

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

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

\mathbb{R}^n 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 ZeilenvektoreZu A gehörige Spaltenvektore

$$\det(\mathbb{1}) = 1$$

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

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

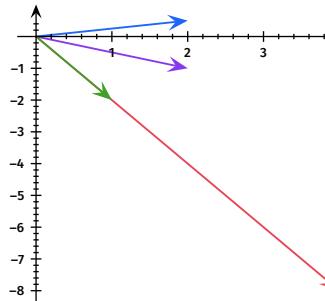
$\det M = 0$ wenn $M \geq 2$ nicht linear unabhängige Zeilen hat. Heisst: Transformierte Vektoren auch linear abhängig.

$$M = \begin{pmatrix} 1 & -2 \\ -2 & 4 \end{pmatrix}, \det(M) = 0$$

$$\vec{d} = \begin{pmatrix} 2 \\ 1 \\ 2 \end{pmatrix}, \vec{b} = \begin{pmatrix} 2 \\ -1 \\ 1 \end{pmatrix}$$

$$\vec{c} = M\vec{d} = \begin{pmatrix} 1 \\ -2 \\ 2 \end{pmatrix}, \vec{d} = M\vec{b} = \begin{pmatrix} 4 \\ -8 \\ 2 \end{pmatrix}$$

$\Rightarrow \vec{c}$ linear abhängig zu \vec{d}



Bsp:

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

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

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

Bsp:

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

$$= -2(2-3) + 0 - 4(-1)$$

$$= 2 + 4 = 6$$

$$\text{Vorzeichen: } \begin{pmatrix} + & - & + & - & \dots \\ - & + & - & + & \dots \\ + & - & + & - & \dots \\ - & + & - & + & \dots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

$$\text{Vorgehen: } \begin{pmatrix} 0 & 2 & 1 \\ 1 & 0 & 1 \\ 3 & 4 & 2 \end{pmatrix} \rightarrow -2 \det \begin{pmatrix} 1 & 1 \\ 3 & 2 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 2 & 1 \\ 1 & 0 & 1 \\ 3 & 4 & 2 \end{pmatrix} \rightarrow 0 \det \begin{pmatrix} 0 & 1 \\ 3 & 2 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 2 & 1 \\ 1 & 0 & 1 \\ 3 & 4 & 2 \end{pmatrix} \rightarrow -4 \det \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

Weitere Eigenschaften:

- Die Determinante wechselt beim Vertauschen von Zeilen ihr Vorzeichen

- Wenn wir zu einer Zeile einer Matrix ein Vielfaches einer anderen Zeile dazuzählen, ändert die Determinante ihren Wert nicht

$$\Rightarrow \det(M) \underset{\text{Gauss}}{=} (-) \det \begin{pmatrix} \lambda_1 & * & * \\ 0 & \ddots & * \\ 0 & 0 & \lambda_n \end{pmatrix} = \lambda_1 \cdot \dots \cdot \lambda_n$$

Weiteres:

$$\det(\lambda M) = \lambda^n \det(M), M \in \mathbb{R}^{n \times n}$$

$$\det \begin{pmatrix} A & * \\ 0 & B \end{pmatrix} = \det(A) \cdot \det(B)$$

$$\det(A \cdot B) = \det(A) \cdot \det(B)$$

$$\det(A^{-1}) = \frac{1}{\det(A)}$$

$$\det(A^T) = \det(A)$$

$$\text{Volumen eines Spats} = \det \begin{pmatrix} \uparrow & \uparrow & \uparrow \\ \vec{a} & \vec{b} & \vec{c} \\ \downarrow & \downarrow & \downarrow \end{pmatrix}$$

$$= \vec{a} \cdot (\vec{b} \times \vec{c})$$

$$\text{Volumen} = \text{Grundfläche} \cdot \text{Höhe}$$

$$= |\vec{b} \times \vec{c}| \cdot |\vec{a}| \cdot \cos(\varphi)$$

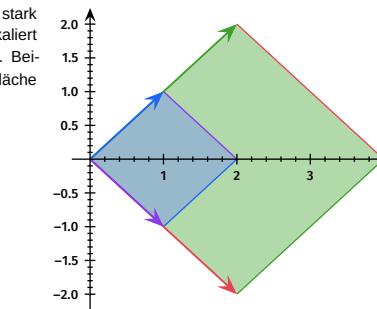
$$= |\vec{a} \cdot (\vec{b} \times \vec{c})|$$

Determinante im 2D-Raum sagt aus, wie stark eine Fläche auf dem Koordinatensystem skaliert wird sobald durch die Matrix transformiert. Beispiel: $\det \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} = 4$ bedeutet, dass die Fläche vierfach wird.

$$M = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \vec{d} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \vec{b} = \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

$$\vec{c} = M\vec{d} = \begin{pmatrix} 2 \\ 2 \end{pmatrix}$$

$$\vec{d} = M\vec{b} = \begin{pmatrix} 2 \\ -2 \end{pmatrix}$$



8.5.8. Eigenwerte

$$\text{Gegeben: } A = \begin{pmatrix} 1 & 1 \\ -2 & 4 \end{pmatrix}$$

\vec{x} heisst Eigenvektor zum Eigenwert λ

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

$$\begin{pmatrix} 1 & 1 \\ -2 & 4 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 2 \\ 2 \end{pmatrix} = 2 \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

Gegeben: Matrix $A \in \mathbb{R}^{n \times n}$

Ein Vektor $\vec{v} \neq \vec{0}$ heisst Eigenvektor zum Eigenwert λ , wenn $A\vec{v} = \lambda\vec{v}$ ist.

$$A\vec{v} - \lambda\vec{v} = 0$$

$$\Leftrightarrow (A - \lambda\mathbb{1})\vec{v} = 0$$

Wenn λ gegeben ist, ist das ein homogenes lineares Gleichungssystem in \vec{v} . Davon suchen wir nicht-triviale Lösungen ($\vec{v} \neq \vec{0}$).

λ heisst Eigenwert von $A \Leftrightarrow A - \lambda\mathbb{1}$ ist singulär $\Leftrightarrow \text{rang}(A - \lambda\mathbb{1}) < n \Leftrightarrow \det(A - \lambda\mathbb{1}) = 0$

Wenn $A \in \mathbb{R}^{n \times n}$, dann ist $\det(A - \lambda\mathbb{1})$ ein Polynom von Grad n . (Charakteristisches Polynom). Eigenwerte sind Nullstellen des charakteristischen Polynoms.

$$A = \begin{pmatrix} 1 & 1 \\ -2 & 4 \end{pmatrix}$$

$$\det(A - \lambda\mathbb{1})$$

$$= \det \begin{pmatrix} 1-\lambda & 1 \\ -2 & 4-\lambda \end{pmatrix}$$

$$= (1-\lambda)(4-\lambda) - (-2) \cdot 1$$

$$= \lambda^2 - 5\lambda + 4 + 2$$

$$= \lambda^2 - 5\lambda + 6$$

= Charakteristisches Polynom

Nullstelle des char. Polynoms

$$\lambda^2 - 5\lambda + 6 = 0$$

$$\Leftrightarrow \lambda = \frac{5 \pm \sqrt{25-24}}{2}$$

$$\Leftrightarrow \lambda = \frac{5 \pm 1}{2}$$

$$\Leftrightarrow \lambda \in \{3, 2\}$$

Eigenwerte von A sind $\lambda = 2$ und $\lambda = 3$

Für diese Zahlen ist die Matrix $A - \lambda\mathbb{1}$ singulär, d.h. die Gleichung $(A - \lambda\mathbb{1})\vec{v} = \vec{0}$ hat nicht-triviale Lösungen. Diese heissen Eigenvektoren.

8.5.9. Eigenwert $\lambda = 2$

$$(A - 2\mathbb{1}) = \begin{pmatrix} 1 & 1 \\ -2 & 4 \end{pmatrix} - \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} -1 & 1 \\ -2 & 2 \end{pmatrix}$$

$$(A - 3\mathbb{1}) = \begin{pmatrix} 1 & 1 \\ -2 & 4 \end{pmatrix} - \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix} = \begin{pmatrix} -2 & 1 \\ -2 & 1 \end{pmatrix}$$

Matrizen haben Rang von 1

$$(A - 2\mathbb{1})\vec{v} = \vec{0}$$

$$(A - 3\mathbb{1})\vec{v} = \vec{0}$$

$$\begin{array}{c|c|c} v_1 & v_2 & 1 \\ \hline -1 & 1 & 0 \\ -2 & 2 & 0 \end{array}$$

$$\begin{array}{c|c|c} v_1 & v_2 & 1 \\ \hline -2 & 1 & 0 \\ -2 & 1 & 0 \end{array}$$

$$\Rightarrow -v_1 + v_2 = 0$$

$$\Rightarrow v_1 = v_2$$

$$\vec{v} = \begin{pmatrix} v_1 \\ v_2 \end{pmatrix} = \begin{pmatrix} \mu \\ \mu \end{pmatrix} = \mu \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

$$\vec{v} = \mu \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \mu \neq 0$$

Für alle $\mu \neq 0$ ist \vec{v} ein Eigenvektor zum Eigenwert $\lambda = 3$.

8.5.11. Diagonalisierbar

$A \in \mathbb{R}^{n \times n}$ heisst diagonalisierbar, wenn es eine invertierbare Matrix X gibt, so dass $X^{-1}AX = D$ (D ist eine Diagonalmatrix $\begin{pmatrix} \lambda_1 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \lambda_n \end{pmatrix}$)

Wenn A diagonalisierbar ist, dann sind die Spalten von X linear unabhängige Eigenvektoren, also eine Basis von \mathbb{R}^n , die nur aus Eigenvektoren von A besteht.

Das umgekehrte gilt auch. Das erlaubt uns, X zu konstruieren.

$$X^{-1}AX = D$$

$$\Leftrightarrow AX = XD$$

$$\Leftrightarrow AX = X \begin{pmatrix} \lambda_1 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \lambda_n \end{pmatrix}$$

$$\Leftrightarrow A \begin{pmatrix} \vec{v}_1 & \vec{v}_2 & \vec{v}_n \end{pmatrix} = \begin{pmatrix} \vec{v}_1 & \vec{v}_2 & \vec{v}_n \end{pmatrix} \begin{pmatrix} \lambda_1 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \lambda_n \end{pmatrix}$$

$$\Leftrightarrow \begin{pmatrix} A\vec{v}_1 & A\vec{v}_2 & A\vec{v}_n \end{pmatrix} = \begin{pmatrix} \lambda_1\vec{v}_1 & \lambda_2\vec{v}_2 & \lambda_n\vec{v}_n \end{pmatrix}$$

$$\Leftrightarrow A\vec{v}_1 = \lambda_1\vec{v}_1 \wedge A\vec{v}_2 = \lambda_2\vec{v}_2 \wedge \dots \wedge A\vec{v}_n = \lambda_n\vec{v}_n$$

$$(A \cdot B) \cdot C = A \cdot (B \cdot C) = A \cdot B \cdot C$$

$$(A + B) \cdot C = A \cdot C + B \cdot C$$

$$C \cdot (A + B) = C \cdot A + C \cdot B$$

$$E \cdot A = A \cdot E = A \text{ für } A \in \mathbb{R}^{n \times n}$$

$$(A^T)^T = A$$

$$(A + B)^T = A^T + B^T$$

$$(AA)^T = \lambda A^T$$

$$(A \cdot B)^T = B^T \cdot A^T$$

8.5.13. Alternative Berechnungsstrategie von Eigenwerten

$$\text{Mean } m = \frac{1}{2} \text{tr} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \frac{a+d}{2} = \frac{\lambda_1 + \lambda_2}{2}$$

$$\text{Product } p = \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc = \lambda_1 \lambda_2$$

$$\lambda_{1,2} = m \pm \sqrt{m^2 - p}$$

8.6.1. Geraden

8.6.1.1. Parameterform (Punktrichtungsform)

$$g: \vec{x} = \begin{pmatrix} p \\ 1 \end{pmatrix} + t \cdot \begin{pmatrix} \vec{PX} \\ 1 \end{pmatrix}, t \in \mathbb{R}$$

$$g_{bsp}: \vec{x} = \begin{pmatrix} 4 \\ 2 \end{pmatrix} + t \cdot \begin{pmatrix} -1 \\ 2 \end{pmatrix}$$

Aus Koordinatenform umwandeln: Richtungsvektor steht senkrecht zum Normalenvektor

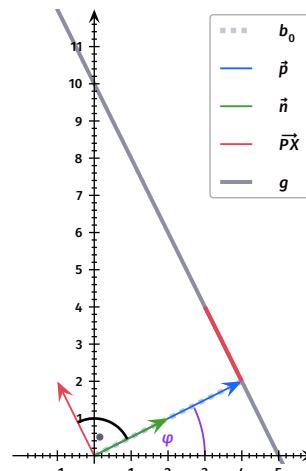
8.6.1.2. Koordinatenform

$$g: ax + by + c = 0$$

$$g_{bsp}: 2x + y - 10 = 0$$

Aus Parameterform umwandeln:

$$\begin{aligned} x &= 4 - 1t \\ y &= 2 + 2t \\ t &= 4 - x \\ y &= 2 + 2(4 - x) = 10 - 2x \\ \Leftrightarrow 2x + y - 10 &= 0 \end{aligned}$$



8.6.1.3. Normalenform

$$g: \left(\vec{x} - \begin{pmatrix} p \\ 1 \end{pmatrix} \right) \cdot \begin{pmatrix} \vec{n} \\ 0 \end{pmatrix} = 0$$

$$g_{bsp}: \left(\vec{x} - \begin{pmatrix} 4 \\ 2 \end{pmatrix} \right) \cdot \begin{pmatrix} 2 \\ 1 \end{pmatrix} = 0$$

Aus Koordinatenform umwandeln (\vec{p} bleibt gleich):

$$2x + 1y - 10 = 0 \Rightarrow \vec{n} = \begin{pmatrix} 2 \\ 1 \end{pmatrix}$$

8.6.1.4. Hessesche Normalenform

$$g: \vec{x} \cdot \vec{n}_0 - b_0 = 0$$

$$g_{bsp}: \vec{x} \cdot \frac{1}{\sqrt{5}} \begin{pmatrix} 2 \\ 1 \end{pmatrix} - \frac{10}{\sqrt{5}} = 0$$

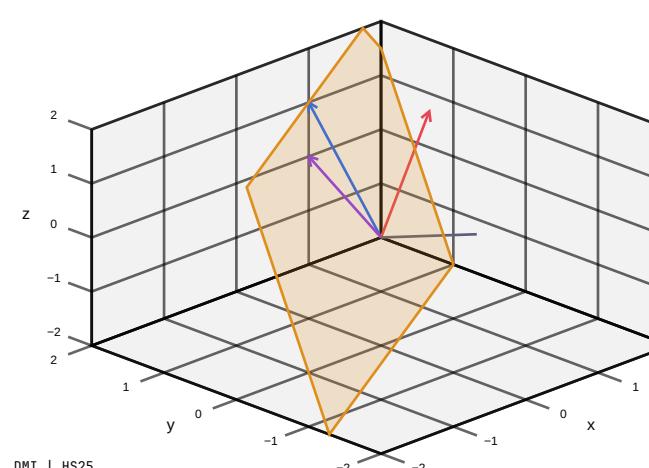
b_0 = Abstand der Geraden g vom Ursprung.

8.6.1.5. Abstand berechnen

Abstand a von Punkt P zur Geraden $\vec{x} \cdot \vec{n}_0 - b_0 = 0$

$$a = \vec{p} \cdot \vec{n}_0 - b_0$$

8.6.2. Ebenen



8.6.2.1. Parameterform

$$E: \vec{x} = \begin{pmatrix} p \\ 1 \end{pmatrix} + s \cdot \begin{pmatrix} \vec{AB} \\ 1 \end{pmatrix} + t \cdot \begin{pmatrix} \vec{AC} \\ 1 \end{pmatrix}, s, t \in \mathbb{R}$$

$$E_{bsp}: \vec{x} = \begin{pmatrix} 0 \\ 1 \\ 2 \end{pmatrix} + s \cdot \begin{pmatrix} 3 \\ 2 \\ 1 \end{pmatrix} + t \cdot \begin{pmatrix} -1 \\ 0 \\ 2 \end{pmatrix}$$

8.6.2.2. Normalenform

$$E: \left(\vec{x} - \begin{pmatrix} p \\ 1 \end{pmatrix} \right) \cdot \begin{pmatrix} \vec{n} \\ 0 \end{pmatrix} = 0$$

$$E_{bsp}: \left(\vec{x} - \begin{pmatrix} 0 \\ 1 \\ 2 \end{pmatrix} \right) \cdot \begin{pmatrix} 4 \\ -7 \\ 2 \end{pmatrix} = 0$$

Aus Parameterform umwandeln (\vec{p} bleibt gleich):

$$\vec{n} = \begin{pmatrix} 3 \\ 2 \\ 1 \end{pmatrix} \times \begin{pmatrix} -1 \\ 0 \\ 2 \end{pmatrix} = \begin{pmatrix} 4 \\ -7 \\ 2 \end{pmatrix}$$

8.6.2.3. Koordinatenform

$$E: ax + by + cz + d = 0$$

$$E_{bsp}: 4x - 7y + 2z + 3 = 0$$

Aus Normalenform umwandeln (ausmultiplizieren):

$$\begin{pmatrix} x - 0 \\ y - 1 \\ z - 2 \end{pmatrix} \cdot \begin{pmatrix} 4 \\ -7 \\ 2 \end{pmatrix} = 0 = 4x - 7y + 2z + 3$$

8.6.2.4. Vereinfachte Normalenform

$$E: \vec{x} \cdot \begin{pmatrix} \vec{n} \\ 0 \end{pmatrix} - \frac{b}{|\vec{n}|} = 0$$

$$E_{bsp}: \vec{x} \cdot \begin{pmatrix} 4 \\ -7 \\ 2 \end{pmatrix} + 3 = 0$$

Aus Koordinatenform umwandeln: $1x - 7y + 2z + 3 = 0$

$$\vec{x} \cdot \begin{pmatrix} 1 \\ -7 \\ 2 \end{pmatrix} + 3 = 0$$

8.6.2.5. Hessesche Normalenform

$$E: \vec{x} \cdot \begin{pmatrix} \vec{n}_0 \\ 1 \end{pmatrix} - \frac{b_0}{|\vec{n}|} = 0$$

$$E_{bsp}: \vec{x} \cdot \frac{1}{\sqrt{69}} \begin{pmatrix} 4 \\ -7 \\ 2 \end{pmatrix} - \frac{3}{\sqrt{69}} = 0$$

Aus Normalenform umwandeln:

$$b = 3, |\vec{n}| = \sqrt{69}, \vec{n}_0 = \frac{1}{\sqrt{69}} \begin{pmatrix} 4 \\ -7 \\ 2 \end{pmatrix}, b_0 = \frac{3}{\sqrt{69}}$$

8.6.2.6. Abstand berechnen

Abstand a von Punkt Q zur Ebene $\vec{x} \cdot \vec{n}_0 - b_0 = 0$

$$a = \vec{q} \cdot \vec{n}_0 - b_0$$

Abstand von Punkt $P(2, 8, 2)$ zur Ebene $E: 2x - y + 4z = 1$

$$\begin{aligned} \vec{n} &= \begin{pmatrix} 2 \\ -1 \\ 4 \end{pmatrix} \\ |\vec{n}| &= \sqrt{21} \\ \frac{2x - y + 4z - 1}{\sqrt{21}} &= \frac{2 \cdot 2 - 1 \cdot 8 + 4 \cdot 2 - 1}{\sqrt{21}} \\ &= \frac{3}{\sqrt{21}} \end{aligned}$$

9. VORGEHENSWEISE, UM

9.1. DIAGONALE UND FLÄCHE BERECHNEN

Gegeben: $A = (0; 1; 0), B = (2; 1; 0), C = (0; 0; 1), D = (1; 0; 0)$

$$\text{Diagonale } \vec{BD} = \vec{r}_B - \vec{r}_D = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} - \begin{pmatrix} 2 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} -1 \\ -1 \\ 0 \end{pmatrix}$$

$$\text{Fläche } F = \left| (\vec{r}_B - \vec{r}_A) \times (\vec{r}_D - \vec{r}_A) \right| = \left| \begin{pmatrix} 2 \\ 0 \\ 0 \end{pmatrix} \times \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix} \right| = \left| \begin{pmatrix} 0 \\ 0 \\ -2 \end{pmatrix} \right| = 2$$

9.2. ABBILDUNGSMATRIX BERECHNEN

Gegeben: $A = (-1; -1), B = (1; 1), A' = (2; 1), B' = (0; 1)$

$$M_U = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}, M_B = \begin{pmatrix} 2 & 0 \\ 1 & 1 \end{pmatrix}, M_U^{-1} = \frac{1}{2} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$$

$$M = M_B \cdot M_U^{-1} = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$$

$$\text{Note: } A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \Rightarrow A^{-1} = \frac{1}{ad-bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

9.3. NULLTEILER VON \mathbb{Z}_n FINDEN

Multiplikationstabelle?

Können nicht Teilerfremd zu n sein.

9.4. ELEMENTE VON \mathbb{Z}_n FINDEN (MULT. INV. IN \mathbb{Z}_n)

Multiplikationstabelle?

$$9.5. |\mathbb{Z}_n| \text{ BERECHNEN}$$

$$|\mathbb{Z}_n| = \varphi(n)$$

9.6. LÖSUNGSMENGE GAUSS-TABLEAU MIT NULLZEILE

$$\dots$$

$$\begin{array}{|ccc|} \hline 1 & 0 & 2 & 3 \\ \hline 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 4 \\ \hline \end{array}$$

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

$$\dots$$

$$\begin{array}{|ccc|} \hline 1 & 0 & 2 & 3 \\ \hline 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ \hline \end{array} \quad L(A, \vec{b}) = \left\{ \vec{x} \in \mathbb{R}^3 \mid \vec{x} = \begin{pmatrix} 3 \\ 0 \\ 0 \end{pmatrix} + t \cdot \begin{pmatrix} -2 \\ 1 \\ 1 \end{pmatrix}, t \in \mathbb{R} \right\}$$

9.7. DISJUNKTIVE/KONJUNKTIVE NORMALFORM ANGEBEN

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

$$\begin{aligned} \neg R &= (A \wedge B \wedge C) \vee (A \wedge \neg B \wedge C) \\ \Leftrightarrow R &= \neg(A \wedge B \wedge C) \wedge \neg(A \wedge \neg B \wedge C) \\ \Leftrightarrow R &= (\neg A \vee \neg B \vee \neg C) \wedge (\neg A \vee B \vee \neg C) \end{aligned}$$

9.8. $x^y \bmod p$ BERECHNEN

Kleiner Fermat: $x^{p-1} \equiv 1 \pmod p, \text{ggT}(x, p) = 1, p$ ist Primzahl

Satz von Euler: $x^{\varphi(p)} \equiv 1 \pmod p, \text{ggT}(x, p) = 1$

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

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

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

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

Georgiy Shevoroshkin

ggT(22,32) = 2 \Rightarrow gibt kein mult. Inv.

9.10. AUS GERADEN G₁ UND G₂ FOLGENDES HERAUSFINDEN:

Gegeben: G₁ = (2; 3) $\cdot \vec{x} - 1 = 0$, G₂ = (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

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

Hessesche Normalenform

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

$$G_2 = \left(\frac{3}{5}; \frac{4}{5} \right) \cdot \vec{x} + 1 = 0$$

Abstand

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

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

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

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

b₁ < 0 \wedge a₁ > 0 \Rightarrow verschiedene Seiten

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

b₂ > 0 \wedge a₂ > 0 \Rightarrow dieselben Seiten

$$\text{Schnittpunkt mit x-Achse berechnen: } g = \vec{x} \cdot \begin{pmatrix} \frac{4}{5} \\ \frac{3}{5} \end{pmatrix} - \frac{2}{5} = 0$$

$$\text{x-Achse } S = (s_x; 0) \text{ einsetzen: } \begin{pmatrix} s_x \\ 0 \end{pmatrix} \cdot \begin{pmatrix} \frac{4}{5} \\ \frac{3}{5} \end{pmatrix} - \frac{2}{5} = 0 \Leftrightarrow s_x = \frac{1}{2} \Rightarrow S = \left(\frac{1}{2}; 0 \right)$$

$$\text{Schnittpunkt zweier Geraden berechnen: } g_1: \vec{x} = \begin{pmatrix} -3 \\ -4 \end{pmatrix} + s_1 \begin{pmatrix} 2 \\ 1 \end{pmatrix}, g_2: \vec{x} = \begin{pmatrix} 4 \\ 1 \end{pmatrix} + s_2 \begin{pmatrix} -1 \\ 1 \end{pmatrix}$$

Einen der Parameter berechnen:

$$-3 + 2s_1 = 4 - s_2$$

$$-4 + 2s_1 = 3 - s_2$$

$$-1 + 1s_1 = 1 + s_2$$

$$\text{Einsetzen: } \begin{pmatrix} -3 \\ -4 \end{pmatrix} + 3 \begin{pmatrix} 2 \\ 1 \end{pmatrix} = \begin{pmatrix} 3 \\ 2 \end{pmatrix} \Rightarrow S = (3; 2; 2)$$

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:

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

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

Hessesche Normalenform der Ebene E:

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

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

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

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

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

Befindet sich Punkt P auf derselben Seite wie der Ursprung: Ja, falls Abstand von P und Abstand von (0; 0; 0) gleiches Vorzeichen haben

Steht der Vektor \vec{v} senkrecht auf der Ebene: Ja, falls vielfaches vom Normalenvektor

9.12. ABSTAND ZWEIER EBENEN BERECHNEN

$$\text{Gegeben: } E_1 = \vec{x} \cdot \begin{pmatrix} 1 \\ -1 \\ 2 \end{pmatrix} - \frac{5}{\sqrt{6}} = 0, E_2 = \vec{x} \cdot \begin{pmatrix} 1 \\ -1 \\ 2 \end{pmatrix} + \frac{1}{\sqrt{6}} = 0$$

$$\text{Abstand: } |d_1 - d_2| = \frac{6}{\sqrt{6}} = \sqrt{6}$$

$$\text{Gegeben: } E_1 = 6x + 2y + 4z = 0, E_2 = 3x + y + 2z - 4 = 0$$

Punkt P $\in E_1$ wählen: y = z = 2 \Rightarrow x = 4

$$\text{Normalenvektor der Ebene } E_2 \text{ finden: } \begin{pmatrix} 3 \\ 1 \\ 2 \end{pmatrix}$$

$$l: \vec{x} = \begin{pmatrix} 4 \\ 2 \\ 2 \end{pmatrix} + s \begin{pmatrix} 3 \\ 1 \\ 2 \end{pmatrix}$$

$$l \text{ einsetzen: } 3(4 + 3s) + (2 + 1s) + 2(2 + 2s) - 4 = 0 \Leftrightarrow s = -1$$

$$\overrightarrow{OF} = \begin{pmatrix} 4 \\ 2 \\ 2 \end{pmatrix} - 1 \cdot \begin{pmatrix} 3 \\ 1 \\ 2 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$$

$$\text{Abstand: } |\overrightarrow{PF}| = \left| \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} - \begin{pmatrix} 4 \\ 2 \\ 2 \end{pmatrix} \right| = \left| \begin{pmatrix} -3 \\ -1 \\ -2 \end{pmatrix} \right| = \sqrt{14}$$

9.13. AUS NORMALENVEKTOR UND PUNKT EINE EBENE ERSTELLEN

$$\text{Gegeben: } \vec{n} = \begin{pmatrix} 3 \\ 4 \\ 0 \end{pmatrix}, P = (1; -1; 1)$$

$$\text{Vereinfachte Normalenform: } \begin{pmatrix} 3 \\ 4 \\ 0 \end{pmatrix} \cdot \vec{x} - b = 0$$

$$\begin{pmatrix} 3 \\ 4 \\ 0 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ -1 \\ 1 \end{pmatrix} - b = 0 \Rightarrow b = 3 - 4 = -1$$

$$\text{Vereinfachte Normalenform mit } b \text{ eingesetzt: } \begin{pmatrix} 3 \\ 4 \\ 0 \end{pmatrix} \cdot \vec{x} + 1 = 0$$

$$|\vec{n}| = 5, b_0 = \frac{1}{5}$$

$$\text{Hessesche Normalenform: } \frac{1}{5} \begin{pmatrix} 3 \\ 4 \\ 0 \end{pmatrix} \cdot \vec{x} + \frac{1}{5} = 0$$

9.14. 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: $x^a \bmod n$

9.15. ALLE ELEMENTE VON R = {(a, b) $\in M \times M$ | a · b $\equiv 1 \pmod{x}$ }

9.16. ALLE ELEMENTE VON R = {(a, b) $\in \mathbb{Z}_x^* \times \mathbb{Z}_x^*$ | a · b $\equiv y \pmod{x}$ }

Falls y teilerfremd zu x: Multiplikationstabelle mit Fremdelementen zu x erstellen.

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

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

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

9.17. LÖSUNG VON M · $\vec{x} = \vec{y}$ ZU \vec{x}
 $\vec{x} = M^{-1} \cdot \vec{y}$