Diskrete Mathematik für Informatik 1 | DMI 1

Zusammenfassung

1. AUSSAGENLOGIK

Eine ***Aussage*** ist ein feststellender Satz, dem eindeutig einer der beiden Wahrheitswerte wahr oder falsch zugeordnet werden kann.»

Auch wenn der Wahrheitswert unbekannt ist, können Behauptungen Aussagen sein, wenn sie im Prinzip beweis- oder widerlegbar sind. Auch Behauptungen über die Zukunft können Aussagen sein. Für Aussagen werden oft Symbole (z.B. A, B, C, …) verwendet.

Wenn die Behauptung in eine «Wenn <Behauptung>, dann …» Form gebracht werden kann, handelt es sich um eine Aussage.

1.1. JUNKTOREN

¬ Negation *nicht*
∧ Konjunktion *und*
∨ Disjunktion *oder*
⇒ Implikation *wenn … dann …*
⇔ Äquivalenz *… genau dann, wenn …*

1.1.1. Negation / Verneinung / ¬

Die Negation einer Aussage ist genau dann wahr, wenn die Aussage falsch ist.

- Heute regnet es ⇒ Heute regnet es nicht
- $x > 1000 \Rightarrow x \leq 1000$
- A: $x < 7$ ⇒ ¬A: $\neg(x<7)$ oder ¬A: $x \geq 7$

A	*¬A*	*¬(¬A)*
w	f	w
f	w	f

1.1.2. Konjunktion / und / ∧

Die Konjunktion zweier Aussagen ist genau dann wahr, wenn beide Aussagen wahr sind.

- A: Heute regnet es. B: Die Lufttemperatur ist unter null. ⇒ A ∧ B: Heute regnet es und die Lufttemperatur ist unter null.
- A: $x < 3$, B: $y > 5$ ⇒ A ∧ B: $x < 3$ und $y > 5$

A	*B*	*A ∧ B*
w	w	w
w	f	f
f	w	f
f	f	f

Achtung: Mit der Konjunktion wird kein kausaler oder zeitlicher Zusammenhang berücksichtigt.
In der Aussagenlogik gilt A ∧ B ⇔ B ∧ A

1.1.3. Disjunktion / (einschliessliches) ODER / ∨

Die Disjunktion zweier Aussagen ist genau dann wahr, wenn mindestens eine der beiden Aussagen wahr ist.

- A: Heute regnet es. B: Die Lufttemperatur ist unter null. → A ∨ B: Heute regnet oder und die Lufttemperatur ist unter null.
- A: $x < 3$, B: $y > 5$ → A ∨ B: $x < 3$ oder $y > 5$ oder beides

A	***B***	***A ∨ B***
w	w	w
w	f	w
f	w	w
f	f	f

Eine ***Kontradiktion*** ist eine logische Aussage, die nie wahr ist. Alle Zeilen der Wahrheitstafel ergeben falsch. Eine ***Tautologie*** ist eine logische Aussage, die immer wahr ist. Alle Zeilen der Wahrheitstafel ergeben wahr.

1.1.4. Implikation / wenn x, dann y / ⇒

Wenn die Aussage A wahr ist, dann gilt auch die Aussage B. Aus A folgt B.
A ist hinreichend für B. B ist notwendig für A. A ist Voraussetzung / Annahme, B ist die Folgerung.

A	***B***	***A ⇒ B***
w	w	w
w	f	f
f	w	w
f	f	w

Abtrennungsregel: Wenn A wahr ist, und A ⇒ B wahr ist, dann ist auch B wahr. $(A \wedge (A \Rightarrow B)) \Rightarrow B$

1.1.5. Äquivalenz / y genau dann, wenn x / ⇔

Aussage A gilt genau dann, wenn B gilt. Es gilt A ⇒ B und B ⇒ A

A	***B***	***A ⇔ B***
w	w	w
w	f	f
f	w	f
f	f	w

Hinweis: ein senkrechter Strich $x \mid y$ bedeutet *x ist ein Teiler von y*

1.1.6. Bindungsstärke

Die Bindungsstärke legt fest, welche Junktoren in aussagenlogischen Formeln zuerst ausgeführt werden. Das ***Nicht*** hat die grösste Bindungsstärke, gefolgt von den beiden Junktoren ***Und*** und ***Oder***. Die kleinste Bindungsstärke besitzen die ***Implikationen*** und die ***Äquivalenz***.

1.2. AUSSAGENLOGISCHE FORMELN

A und B seien Aussagen. Die verknüpften Aussagen $\neg A$, $A \wedge B$, $A \vee B$, $A \Rightarrow B$ und $A \Leftrightarrow B$ sind ***aussagenlogische Formeln***. Die verknüpften Aussagen sind auch aussagenlogische Formeln, wenn A oder B bereits selbst aussagenlogische Formeln sind. Eine aussagenlogische Formel ist selbst wieder eine Aussage. Die logische Konstante W bedeutet «wahr» und F bedeutet «falsch».

SATZ 1: A, B, und C seien aussagenlogische Formeln. Dann gilt

1. Kommutativität: $A \wedge B \Leftrightarrow B \wedge A$, $A \vee B \Leftrightarrow B \vee A$
Wenn A und B zutreffen, gilt auch B und A. Wenn A oder B zutreffen, gilt auch B oder A (umgekehrt)

2. Assoziativität: $A \wedge (B \wedge C) \Leftrightarrow (A \wedge B) \wedge C$, $A \vee (B \vee C) \Leftrightarrow (A \vee B) \vee C$
Wenn A und (B und C) zutreffen, können die Klammern beliebig verschoben oder weggelassen werden (gleich bei oder)

3. Distributivität: $A \wedge (B \vee C) \Leftrightarrow (A \wedge B) \vee (A \wedge C)$, $A \vee (B \wedge C) \Leftrightarrow (A \vee B) \wedge (A \vee C)$
A und (B oder C) ist das gleiche wie (A und B) oder (A und C), A oder (B und C) ist das gleiche wie (A oder B) und (A oder C)

4. Absorption: $A \vee (A \wedge B) \Leftrightarrow A$, $A \wedge (A \vee B) \Leftrightarrow A$
A oder (A und B) ist das Gleiche wie A. A und (A oder B) ist das Gleiche wie A

5. Idempotenz: $A \vee A = A$, $A \wedge A = A$
A und A = A, A oder A = A

6. Doppelte Negation: $\neg(\neg A) \Leftrightarrow \neg\neg A \Leftrightarrow A$
Nicht nicht A ist gleich A

7. Konstanten: W = wahr, F = falsch. $A \vee W \Leftrightarrow W$, $A \wedge W \Leftrightarrow A$, $A \vee \neg A \Leftrightarrow W$
A oder wahr = wahr, A und wahr = A, A oder nicht A = wahr

Implikation ersetzen: $A \Rightarrow B$ kann man durch $\neg A \vee B$ ersetzen
Äquivalenz ersetzen: $A \Leftrightarrow B$ kann man durch $(A \wedge B) \vee (\neg A \wedge \neg B)$ ersetzen

SATZ 2: A, B und C seien aussagenlogische Formeln. Dann bedeutet $A \Rightarrow B \Rightarrow C$, dass beide Implikationen, sowohl $A \Rightarrow B$ als auch $B \Rightarrow C$ gelten. Formal kann man also schreiben: $(A \Rightarrow B \Rightarrow C) \Leftrightarrow (A \Rightarrow B) \wedge (B \Rightarrow C)$

SATZ 3 (DE MORGAN): Für beliebige Aussagen A und B gilt:
a) $\neg(A \wedge B) \Leftrightarrow \neg A \vee \neg B$ Nicht (A und B) ist das gleiche wie nicht A oder nicht B
b) $\neg(A \vee B) \Leftrightarrow \neg A \wedge \neg B$ *Nicht (A oder B) ist das gleiche wie nicht A und nicht B*

1.3. NORMALFORMEN

Dienen der Übersichtlichkeit – standardisierte Form

1.3.1. Negationsnormalform

Eine aussagenlogische Formel steht in Negationsnormalform, wenn die Negation ($\neg$) nur direkt vor Aussagen oder vor Konstanten steht.
Beispiel: $\neg(A \vee B)$ ist keine Negationsnormalform, $\neg A \wedge \neg B$ hingegen schon

1.3.2. Verallgemeinerte Konjunktion

Eine verallgemeinerte Konjunktion ist…

- Eine einzelne Aussage oder seine Negation (also A oder $\neg A$) oder

- Einer der logischen Konstante T=wahr oder F=falsch oder
- Eine Konjunktion $A \land B$, falls A und B selbst verallgemeinerte Konjunktionen sind

Eine Verbindung von Aussagen, Negationen und logischen Konstanten mit «und».
*Liegt immer in **Negationsnormalform** vor.*

1.3.3. Disjunktive Normalform

Eine Aussage liegt in disjunktiver Normalform vor, wenn sie eine **verallgemeinerte Konjunktion** ist, oder wenn sie eine Disjunktion von verallgemeinerten Konjunktionen ist.

*Eine Verbindung von **verallgemeinerten Konjunktionen** mit «oder».*

1.3.4. Verallgemeinerte Disjunktion

Eine verallgemeinerte Disjunktion ist…
- Eine einzelne Aussage oder seine Negation (also A oder ¬A) oder
- Einer der logischen Konstante T=wahr oder F=falsch oder
- Eine Disjunktion $A \lor B$, falls A und B selbst verallgemeinerte Disjunktionen sind

1.3.5. Konjunktive Normalform

Eine Aussage liegt in konjunktiver Normalform vor, wenn sie eine **verallgemeinerte Disjunktion** ist, oder wenn sie eine Konjunktion von verallgemeinerten Disjunktionen ist.

Beispiel: Aussage A: $(X \land \neg Y) \lor (\neg X \land (Y \lor \neg Z))$

X	*Y*	*Z*	*A*
w	w	w	**f**
w	w	f	**f**
w	f	w	**w**
w	f	f	**w**
f	w	w	**w**
f	w	f	**w**
f	f	w	**f**
f	f	f	**w**

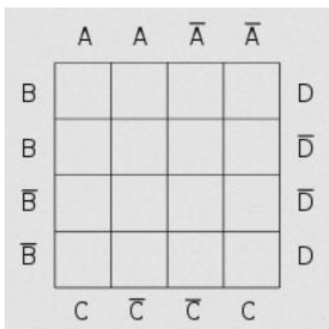
Um A in **disjunktiver Normalform** zu schreiben, werden die Zeilen der Tabelle ausgewertet, in denen A richtig ist. Um A in **konjunktiver Normalform** zu schreiben, werden die Zeilen der Tabelle ausgewertet, in denen A falsch ist.

Das heisst, die **konjunktive Normalform** wäre wie folgt:
$A \Leftrightarrow \neg ((X \land Y \land Z) \lor (X \land Y \land \neg Z) \lor (\neg X \land \neg Y \land Z))$

Daraus lässt sich mit der Regel von de Morgan eine **Negationsnormalform** erstellen:
$A \Leftrightarrow (\neg X \lor \neg Y \lor \neg Z) \land (\neg X \lor \neg Y \lor Z) \land (X \lor Y \lor \neg Z))$

1.4. KARNAUGH-VEITCH-DIAGRAMME

Aus der Wahrheitstafel wird eine **disjunktive** oder **konjunktive Normalform** abgeleitet und in das Diagramm eingetragen. Wir verwenden die Minterm-Methode.



1.4.1. Vorgehen:

1. Diagramm mit 2^n Zellen erzeugen. Bei n=3:

	B	**B**	**¬B**	**¬B**
A				
¬A				
	C	**¬C**	**C**	**¬C**

Die Beschriftungen müssen so gewählt sein, dass 2 benachbarte Zellen sich genau in einer Aussage unterscheiden.

2. Werte aus der Wahrheitstabelle eintragen. *Hier werden Beispielwerte verwendet*

	B	**B**	**¬B**	**¬B**
A	w	f	f	w
¬A	w	f	w	w
	C	**¬C**	**C**	**¬C**

3. Alle benachbarten w-Felder zu Blöcken in 2er-Potenz (2,4,8 etc.) zusammenfassen und vereinfachen. *Über den Rand hinaus gilt auch als benachbart. Alle w-Zellen müssen überdeckt werden, ohne dass eine f-Zelle überdeckt wird. Zellen dürfen mehrfach überdeckt werden.*

	B	**B**	**¬B**	**¬B**
A	w	f	f	w
¬A	w	f	w	w
	C	**¬C**	**C**	**¬C**

Im Beispiel gibt es folgende Nachbarn:
2 Felder unten rechts $(\neg A \land \neg B \land C) \lor (\neg A \land \neg B \land \neg C) \Leftrightarrow \neg A \land \neg B$
4 Felder ganz links und ganz rechts $(A \lor \neg A) \land (B \lor \neg B) \land C \Leftrightarrow C$
Zusammengefasst: $(\neg A \land \neg B) \lor C$

2. PRÄDIKATENLOGIK

Aussagen können auch von ***Variablen*** abhängen. Aussagen mit Variablen können *wahr* oder *falsch* sein, je nachdem, welche Variable eingesetzt wird. Es geht also um Aussagen, die ***«manchmal wahr»*** sind.

Beispiele:

A(n): 5 | n, 5 ist ein Teiler von n

B(n): $1 + 2 + 3 + 4 + \ldots + n = \sum_{k=1}^{n} = \frac{1}{2} n\,(n+1), n \in \mathbb{N}$

R(X): der Weg X führt nach Rom.

2.1. AUSSAGEFORMEN

Aussagen, deren Wahrheitswert von einer oder mehreren Variablen abhängt, heissen Aussageformen.

- Wenn in eine Aussageform der Wert einer Variablen eingesetzt wird, dann erhalten wir eine Aussage, die eindeutig entweder wahr oder falsch ist.
- Aussageformen sind unbestimmt, weil nicht bestimmt ist, welcher Wert für eine Variable eingesetzt wird.
- Was in eine Aussageform eingesetzt wird, muss für die Aussageform geeignet sein, muss also ein zulässiges Subjekt sein. *A(m): m ist Primzahl. m=7 ist wahr, m=8 ist falsch, m=7.8 ist nicht zulässig*

2.2. PRÄDIKAT

Aussagen und Aussageformen bestehen aus zwei Teilen: Dem Subjekt und dem Prädikat.
Subjekt: «konkretes Ding» oder Stellvertreter für «konkretes Ding»
Prädiktat: «Eigenschaft», die ein Ding haben kann.

- Einstelliges Prädikat: «ist eine Primzahl» ist die Eigenschaft der natürlichen Zahlen.
  P(n) ist ein Prädikat für ℕ.
- Zweistelliges Prädikat: «ist Teiler von» ist eine Eigenschaft, die ein Paar von natürlichen Zahlen besitzen kann. *T(n,m) ist ein Prädikat für zwei natürliche Zahlen* (zweistelliges Prädikat
- Dreistelliges Prädikat: T(k,n,m): k teilt das Produkt von n und m

Anmerkung:
Prädikate und Aussageformen werden in Mengenbeschreibungen verwendet, um die Menge zu charakterisieren: $M = \{(x, y) \in \mathbb{R}^2 | \boldsymbol{x + 2 = 7 - y}\}$

2.3. QUANTOREN

Bei Aussagen, die Variablen enthalten, sind 2 Fälle besonders wichtig:

- Gilt die Aussageform für ***alle*** zugelassenen Werte der Variablen?
- Gilt die Aussageform für ***einen*** der zugelassenen Werte der Variablen?

Beispiel: Die Summe S(n) aller natürlichen Zahlen von 1 bis n ist $S(n) = \frac{1}{2}n(n+1)$. Das gilt für alle natürlichen Zahlen. Das bedeutet:

- ***Allquantor:*** $\forall n \in \mathbb{N}$ gilt $S(n) = \frac{1}{2}n(n+1)$ «für ***alle*** n aus den natürlichen Zahlen gilt…»
- ***Existenzquantor:*** $\exists n \in \mathbb{N}$ gilt $S(n) = \frac{1}{2}n(n+1)$ «es gibt ***eine*** natürliche Zahl n, für die gilt…»

Der Existenzquantor mach in diesem Beispiel wenig Sinn, da der Allquantor auch verwendet werden kann. Beispiel für eine sinnvolle Verwendung des Existenzquantors: «Es gibt ein Schiff, das uns über den Fluss bringen kann»

2.4. BEWEISEN

Ein Beweis zeigt die Gültigkeit einer Behauptung unter gewissen Voraussetzungen und Annahmen:

- ***Direkter Beweis:*** $A \Rightarrow B$
- ***Indirekter Beweis:*** $\neg B \Rightarrow \neg A$
- ***Widerspruchsbeweis:*** $A \wedge \neg B \Rightarrow F$
- ***Vollständige Induktion:*** $A(1) \wedge \big(A(n) \Rightarrow A(n+1)\big) \Rightarrow A(m), m \in \mathbb{N}$
- ***Vollständige Fallunterscheidung:*** Wenn $A \Leftrightarrow A_1 \vee A_2 \vee \ldots A_n$ und es gilt, dass $(A_1 \Rightarrow B) \wedge (A_2 \Rightarrow B) \wedge \ldots \wedge (A_n \Rightarrow B)$ ist, dann gilt auch $A \Rightarrow B$
- ***Schubfachprinzip:*** Wenn n + 1 Gegenstände (Objekte) auf n Schubladen (Kategorien) verteilt werden, dann befinden sich in mindestens einem Schubfach 2 Gegenstände.
- ***Diagonalverfahren (Georg Cantor):*** Anzahl rationaler Zahlen ist genau so gross wie die Anzahl natürlicher Zahlen.

3. VOLLSTÄNDIGE INDUKTION

Wie kann man natürliche Zahlen mathematisch exakt festlegen?

3.1. PEANO-AXIOME:

- Null ist eine natürliche Zahl.
- Zu jeder natürlichen Zahl n gibt es genau einen Nachfolger n_0, der auch eine natürliche Zahl ist.
- Null ist nicht Nachfolger einer natürlichen Zahl.
- Jede natürliche Zahl ist Nachfolger höchstens einer natürlichen Zahl.
- Die Menge der natürlichen Zahlen ist die kleinste Menge, die die Zahl Null und mit jeder natürlichen Zahl auch ihren Nachfolger enthält.

3.2. DAS SCHEMA DER VOLLSTÄNDIGEN INDUKTION

1. ***Verankerung:*** Es wird geprüft, ob A(n) für den ersten Wert richtig ist. Ob also die Aussage $A(n_0)$ gilt.
   Z.B. für $n_0 = 0$ oder für $n_0 = 1$
2. ***Induktionsschritt:*** n -> n + 1
   Es wird gezeigt: wenn A(n) gilt, dann gilt auch A(n+1). Als Formel: $A(n) \Rightarrow A(n+1)$
   a. Induktionsannahme: A(n) sei richtig für n
   b. Induktionsbehauptung: A(n+1)
   c. Induktionsbeweis: es wird die Aussage A(n) verwendet, um die Richtigkeit der Behauptung A(n+1) zu zeigen.

3.3. BEISPIEL ANHAND DER SUMMENFORMEL

$$\boldsymbol{S(n)}\colon \sum_{k=1}^{n} \boldsymbol{k} = \frac{\mathbf{1}}{\mathbf{2}} * \boldsymbol{n} * (\boldsymbol{n} + \mathbf{1})$$

1. **Induktionsanfang (Verankerung), hier für $n_0 = 1$**

Linke Seite:

$$\sum_{k=1}^{1} \boldsymbol{k} = \mathbf{1}$$

Rechte Seite:

$$\frac{1}{2} * 1 * (1+1) = \mathbf{1}$$

Die Summenformel gilt für n0 = 1.

2. **Induktionsschritt n -> n+1**

a. Induktionsannahme: $\boldsymbol{S(n)}\colon \sum_{k=1}^{n} \boldsymbol{k} = \frac{\mathbf{1}}{\mathbf{2}} * \boldsymbol{n} * (\boldsymbol{n} + \mathbf{1})$

b. Induktionsbehauptung: $\boldsymbol{S(n+1)}\colon \sum_{k=1}^{n+1} \boldsymbol{k} = \frac{\mathbf{1}}{\mathbf{2}} * (\boldsymbol{n} + \mathbf{1}) * (n + \mathbf{2})$

c. Induktionsbeweis:

Wir nehmen die linke Seite der Induktionsbehauptung und teilen diese Summe in zwei Teile, sodass für den einen Teil die Induktionsannahme eingesetzt werden kann:

$$\sum_{k=1}^{n+1} \boldsymbol{k} = \left(\sum_{k=1}^{n} k\right) + n + 1$$

Dann setzen wir die Induktionsannahme ein:

$$\sum_{k=1}^{n+1} \boldsymbol{k} = \frac{1}{2} * n * (n+1) + n + 1$$

Multiplizieren und klammern ½ aus:

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

Und schreiben die Klammer als Produkt:

$$\sum_{k=1}^{n+1} \boldsymbol{k} = \frac{1}{2} * (n+1) * (n+2)$$

Damit haben wir die Induktionsbehauptung gezeigt und die Gültigkeit der Summenformel für alle natürlichen Zahlen $n \geq 1$ bewiesen.

4. MENGEN

P(M)	Potenzmenge	Alle möglichen Resultate als Mengen + leere Menge	$M = \{a, b, c\}$ $P(M) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$
|M|	Mächtigkeit	Anzahl Resultate	$\|M\| = 3$ (In der Menge M sind 3 Elemente a, b & c) $\|P(M)\| = 2^n = 2^3 = 8$
∈	Enthalten in	kann Elemente & Mengen vergleichen	
⊂	Teilmenge von	kann nur Mengen vergleichen. Jede Menge ist eine Teilmenge von sich selbst. Echte Teilmenge: wenn nicht identisch	$Wenn\ gilt: A \subset B \wedge B \subset A, dann\ ist\ A = B.$
{}	Leere Menge	Menge, die keine Elemente beinhaltet. Ist Teilmenge jeder anderen Menge.	

4.1. SCHREIBWEISEN MENGEN

- ***Aufzählende Form:*** Die Elemente einer Menge werden zwischen geschweiften Klammern aufgezählt {1, 2, 3} oder {2, 4, 6, 8, …}
- ***Beschreibende Form:*** Durch {X ∈ G | E(x)} wird die Menge bezeichnet, die aus allen Elementen x einer Grundmenge G besteht, die die Eigenschaft E besitzen. Z.B. alle reellen Zahlen, die die Gleichung x^2 = 1 lösen, bilden die Lösungsmenge $\{x \in \mathbb{R} \mid x^2 = 1\}$

4.2. VEREINIGUNG

Wenn A und B Mengen sind, dann bezeichnen wir: 1. Die Vereinigung von A und B ist die Menge mit allen Objekten, die Element von A oder Element von B sind.

$$A \cup B = \{x \mid x \in A \vee x \in B\}$$

4.3. DURCHSCHNITT / SCHNITTMENGE

Der Durchschnitt von A und B ist die Menge mit allen Objekten, die sowohl Element von A als auch Element von B sind.

$$A \cap B = \{x \mid x \in A \wedge x \in B\}$$

Rechenregeln für Durchschnitt und Vereinigung:
Satz 9: Für Mengen A, B und C gelten die folgenden Gesetze:

Kommutativgesetz:

$$A \cap B = B \cap A$$
$$A \cup B = B \cup A$$

Assoziativgesetz:

$$A \cap (B \cap C) = (A \cap B) \cap C$$
$$A \cup (B \cup C) = (A \cup B) \cup C$$

Idempotenzgesetz:

$$A \cap A = A$$
$$A \cup A = A$$

Verschmelzungsgesetz:

$$A \cup (A \cap B) = A$$
$$A \cap (A \cup B) = A$$

Distributivgesetz:

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$
$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

4.4. KOMPLEMENT UND DIFFERENZ

Sei A eine Teilmenge einer Obermenge M. Dann heisst die Menge $\bar{A} := \{x \in M \mid x \notin A\}$ das ***Komplement*** von A bezüglich der Obermenge M.

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

$$\bar{\bar{A}} = A$$
$$A \cap \bar{A} = \emptyset$$
$$A \cup \bar{A} = M$$
$$\overline{A \cap B} = \bar{A} \cup \bar{B}$$
$$\overline{A \cup B} = \bar{A} \cap \bar{B}$$

Die Differenz von zwei Mengen A und B besteht aus allen Elementen von A, die nicht in B sind, und wird definiert durch $A \backslash B = \{x \in A \mid x \notin B\}$

Das Komplement besitzt die grösste Bindungsstärke, gefolgt von den anderen Mengen-Operatoren Vereinigung, Durchschnitt und Mengendifferenz. Es gilt: $^{-}\ vor\ \cup, \cap, \backslash$.

4.4.1. Beispiele

a) $A \cap \overline{A \cup B \cup C} = A \cap \left(\bar{A} \cap \bar{B} \cap \bar{C}\right) = A \cap \bar{A} \cap \bar{B} \cap \bar{C} = \varnothing \cap \bar{B} \cap \bar{C} = \varnothing$

b) $A \setminus (A \setminus B) = A \setminus \left(A \cap \bar{B}\right) = A \cap \overline{A \cap \bar{B}} = A \cap \left(\bar{A} \cup B\right) =$

$= \left(A \cap \bar{A}\right) \cup (A \cap B) = A \cap B$

c) $\left(A \cup \bar{C}\right) \cap \overline{B \cap C} \cap \overline{\left(\bar{A} \cup B\right) \cap \bar{C}} =$

$= \left(A \cup \bar{C}\right) \cap \left(\bar{B} \cup \bar{C}\right) \cap \left(\overline{\bar{A} \cup B} \cup C\right)$

$= \left(\left(A \cap \bar{B}\right) \cup \bar{C}\right) \cap \left(\left(A \cap \bar{B}\right) \cup C\right)$

$= \left(A \cap \bar{B}\right) \cup \left(\bar{C} \cap C\right) = A \cap \bar{B}$

5. RELATIONEN UND ABBILDUNGEN

Eine ***Relation*** zwischen den nicht-leeren Mengen A und B ist eine Teilmenge des kartesischen Produktes AxB.

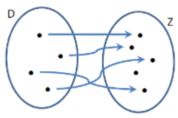
Eine ***Abbildung*** ist eine Formel, der sämtliche Werte im Definitionsbereich einem Zielbereich zugeordnet werden (analog Funktion in Analysis) und kein Input mehrere Outputs ergibt. Ist f eine Abbildung mit Definitionsmenge D und Zielmenge Z, so schreibt man f : D -> Z. Die Elemente von D heissen Argumente oder Stellen, die Elemente von Z heissen Werte.

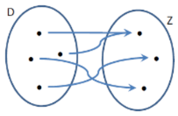
Der ***Graph einer Funktion*** f ist die Menge aller Punkte, deren Koordinaten (x,y) die Funktionsgleichung von f erfüllen. G kann man als eine Menge von Paaren (x, f(x)) auffassen.

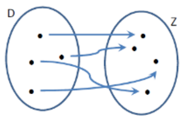
Definitionsmenge = **Urbild**, Zielmenge = **Bildmenge**

5.1. INJEKTIV, SURJEKTIV, BIJEKTIV

- ***Injektiv:*** Die Abbildung *f : D -> Z , a -> f(a)* heisst injektiv, wenn für je zwei verschiedene Elemente a_1, a_2 von A auch die Bilder verschieden sind. Alle Inputs müssen eindeutige Outputs ergeben.
- ***Surjektiv:*** Die Abbildung *f: D -> Z, a -> f(a)* heisst surjektiv, wenn jedes Element der Bildmenge als Bild vorkommt.
- ***Bijektiv:*** Die Abbildung *f: D -> Z, a -> f(a)* heisst bijektiv, wenn f sowohl injektiv als auch surjektiv ist.







6. MODULO-RECHNEN

Für $a, q, r \in \mathbb{Z}$ heisst die Relation $R_q(a,r) \Leftrightarrow q \mid a - r \Leftrightarrow a \equiv r \bmod q$ die ***modulo Relation***. Man sagt «a ist gleich r modulo q».

Wenn $a \equiv r \bmod b$ ist, dann ist a gleich r plus ein Vielfaches von b.

$a = 35, b = 12$
$a \equiv r \bmod b \Leftrightarrow a = q * b + r \Rightarrow r \in \{\dots, -13, -1, 11, 23, \dots\}$

Beispiele:

$\mathbf{33 * 2 \; mod \; 7} = 66 \; mod \; 7 \Rightarrow 66 \; durch \; 7 - wieviel \; Rest?, 63 \; geht \; durch \; 7, dh \; Rest = 3 \Rightarrow \underline{3 \; mod \; 7}$

$\mathbf{2 + 33 \; mod \; 7} = 35 \; mod \; 7 \;\; \Rightarrow 35 \; durch \; 7 - wieviel \; Rest? \; \Rightarrow 0$

$\mathbf{2^{33} mod \; 7} = (2^3)^{11} \;\; = 8^{11} \;\; \Rightarrow das \; Gleiche \; wie \; 1^{11}(-7) \Rightarrow 1$

Zwei wichtige Regeln beim Modulo-Rechnen mit Potenzen sind das Auseinandernehmen von Potenzen und das «Reinziehen»

Potenzen auseinandernehmen	***«Reinziehen»***
$2^{100} \; mod \; 3$	$a^n \; mod \; k = (a \; mod \; k)^n \; mod \; k$
$= 2^{2*50} \; mod \; 3$	Der Term in der Klammer kann zuerst berechnet werden:
$= (2^2)^{50} \; mod \; 3$	$4^{50} \; mod \; 3 = (4 \; mod \; 3)^{50} \; mod \; 3$
$= 4^{50} \; mod \; 3$	$= (1)^{50} \; mod \; 3 = 1 \; mod \; 3 = 1$

Seien $a \equiv r_a \; mod \; q$ und $b \equiv r_b mod \; q$. Dann ist
$a + b \equiv r_a + r_b \; mod \; q$
$a * b \equiv r_a * r_b \; mod \; q$

Beispiel:

$2 + 4 + 6 + 8 \; mod \; 3 \equiv 2 + 1 + 0 + 2 \; mod \; 3 \equiv 5 \; mod \; 3 \equiv \underline{2 \; mod \; 3}$

Kleiner Fermat

Sei $p \in \mathbb{N}$ eine Primzahl und $x \in \mathbb{Z} \backslash \{0\}$ mit ggT(x,p) = 1.
Dann ist: $\boldsymbol{x}^{p-1} \equiv 1 \; mod \; \boldsymbol{p}$

Beispiel: $\boldsymbol{p} = \mathbf{2} \;\; \Rightarrow 1^{2-1} \equiv \underline{1 \; mod \; \mathbf{2}}$

Beispiel: $\boldsymbol{p} = \mathbf{5} \;\; \Rightarrow$

$\mathbf{1}^{5-1} \equiv 1 \; mod \; \mathbf{5}$

$\mathbf{2}^{5-1} \equiv 16 \;\; \equiv 1 \; mod \; \mathbf{5}$

$\mathbf{3}^{5-1} \equiv 81 \;\; \equiv 1 \; mod \; \mathbf{5}$

$\mathbf{4}^{5-1} \equiv 256 \;\; \equiv 1 \; mod \; \mathbf{5}$

Damit lassen sich sehr hohe Potenzen berechnen.

Beispiel: $2^{98} mod \; 5 \equiv ?$ Weil p = 5 eine Primzahl ist, ist $2^4 \equiv 1 \; mod \; 5$. Dann schreiben wir
$2^{98} mod \; 5 \equiv 2^{4*24+2} \equiv (2^4)^{24} * 2^2 \equiv 1^{24} * 4 \;\; \equiv \underline{4 \; mod \; 5}$.

Oder kürzer:

$98 \equiv 2 \; mod \; 4 \;\; \Rightarrow 2^{98} \equiv 2^2 \equiv \underline{4 \; mod \; 5}$

Satz von Euler

Sei $n \in \mathbb{N}\backslash\{0\}$ und $z \in \mathbb{Z}$ mit ggT(z,n) = 1. Dann ist $z^{\varphi(n)} \equiv 1 \; mod \; n$

Eulersche φ-Funktion

Sei $n \in \mathbb{N}$ und $\mathbb{Z}_n^* = \{x \in \mathbb{Z}_n \mid x \; hat \; ein \; multiplikatives \; Inverses \; in \; \mathbb{Z}_n\}$. Dann berechnet sich die Eulersche φ-Funktion als

$\varphi(n) =$ Anzahl Zahlen $m \in \mathbb{N}$ mit $1 \leq m \leq n$ und ggT(n,m) = 1 *=> Anzahl der teilerfremden Zahlen zwischen 0 und n*

$\varphi(n) =$ Anzahl Elemente $x \in \mathbb{Z}_n$ mit multiplikativem Inversen

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

Formen zur Berechung:

1. Sei $n \in \mathbb{N}$ eine Primzahl: Dann ist $\varphi(n) = n - 1$

2. Sei $n \in \mathbb{N}$ eine Primzahl und $p \in \mathbb{N}\backslash\{0\}$: Dann ist $\varphi(n^p) = n^{p-1} * (n-1)$

3. Seien $m, n \in \mathbb{N}\backslash\{0\}$ und ggT(m,n) = 1: Dann ist $\varphi(n * m) = \varphi(n) * \varphi(m)$

Beispiel 1: $\varphi(11) = 10$

Beispiel 2: $\varphi(5^3) = 5^2 * 4 = 25 * 4 = 100$

Beispiel 3: $\varphi(2 * 47) = \varphi(2) * \varphi(47) = 1 * (47 - 1) = 46$

Multiplikatives Inverses

Seien $q \in \mathbb{N}, q \neq 0$ und $m \in \mathbb{N}, m \neq 0$. Dann gilt:

Es gibt eine Zahl $n \in \mathbb{N}$ mit $m * n \equiv 1 \; mod \; q \Leftrightarrow ggT(q, m) = 1$

Beispiel: Multiplikatives Inverse von **7** in $\mathbb{Z}_{11}$: $7 * x \equiv 1 \; mod \; 11$

X kann auf 2 Arten berechnet werden. Entweder durch Durchprobieren oder durch den erweiterten euklidischen Algorithmus.

Durchprobieren:

$7 * 1 - 1 = 6 \Rightarrow$ nicht durch 11 teilbar

$7 * 2 - 1 = 13 \Rightarrow$ nicht durch 11 teilbar

…

$7 * 8 - 1 = 55 \Rightarrow$ durch 11 teilbar, **x = 8**

Erweiterter euklidischer Algorithmus: Siehe unten, danach das letzte Resultat von t (in diesem Fall -3) durch Modulo der Zahl in der Originalrechnung nehmen.

$-3 \; mod \; 11 = \frac{|-3|}{11} = \boldsymbol{Rest \; 8}$ = multiplikatives Inverses von 7 in $\mathbb{Z}_{11}$

7. EUKLIDISCHER ALGORIGHMUS (MODULO)

Gibt ggT (grösster gemeinsamer Teiler) & kgV (kleinstes gemeinsames Vielfaches) aus.

Wenn der ggT von zwei Zahlen 1 ist, sind die beiden Zahlen ***teilerfremd*** (sie haben keinen gemeinsamen Teiler). Bei geraden Zahlen sind alle kleineren geraden Zahlen **nicht** teilerfremd. Bei Primzahlen sind alle Zahlen kleiner als die Primzahl teilerfremd. Die Zahl 1 ist bei jeder Zahl teilerfremd.

Teilerfremde Zahlen der Zahlen 1-10

1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*
1	1	1,2	1,3	1,2,3,4	1,5	1,2,3,4,5,6	1,3,5,7	1,2,4,5,7,8	1,3,7,9

7.1. PRIMFAKTORZERLEGUNG

12 = 2 * ~~2~~ * ~~3~~, 18 = ~~2~~ * ~~3~~ * 3 => 2 * 3 = 6 => ggT. (12 * 18) / 6 = 36 => kgV

Bei grossen Zahlen sehr rechenaufwendig. Deshalb bestimmen wir den ggT mit dem Euklidischen Algorithmus, und das kgV aus (a*b) / ggT(a,b)

Euklidischer Algorithmus (ggT finden)

Seien $a, b \in \mathbb{N}, a \neq b, a \neq 0, b \neq 0$

Initialisierung: Setze $\boldsymbol{x := a}, \boldsymbol{y := b}$ und $\boldsymbol{q := x\ div\ y}$ (wie oft passt y in x)und $\boldsymbol{r := x - q * y}$ (d.h. bestimme q und r so, dass $x = q * y + r$ ist.

Wiederhole, bis r = 0 ist.

Ablauf	***x***	***y***	$\boldsymbol{q} := x\ div\ y$	$\boldsymbol{r} := x - q * y$
Initialisierung	122	72	1	122 – 72 = 50
1. Wiederholung	72	50	1	72 – 50 = 22
2. Wiederholung	50	22	2	50 – 44 = 6
3. Wiederholung	22	6	3	22 – 18 = 4
4. Wiederholung	6	4	1	6 – 4 = 2
5. Wiederholung	4	2 = ggT	2	0

Erweiterter Euklidischer Algorithmus (ggT finden und als Linearkombination darstellen)

Seien $a, b \in \mathbb{N}, a \neq b, a \neq 0, b \neq 0$

Initialisierung: Setze $\boldsymbol{x := a}, \boldsymbol{y := b}, \boldsymbol{q := x\ div\ y}$ (wie oft passt y in x), $\boldsymbol{r := x - q * y}$ (d.h. bestimme q und r so, dass $x = q * y + r$ ist), und *(u, s, v, t) = (1,0,0,1)*

Wiederhole, bis r = 0 ist.

x = y aus der vorangegangenen Zeile

y = r aus der vorangegangenen Zeile

q = x div y, **r = x mod y** = x-y*q

u = s aus der vorangegangenen Zeile

s = u – q * s mit u, q & s aus der vorangegangenen Zeile

v = t aus der voangegangenen Zeile

t = v – q * t mit v, q & t aus der vorangegangenen Zeile

Ergebnis: In der letzten Zeile gilt y = ggT, s * a + t * b. Wenn ggT = 1 ist, dann folgt: t*b = 1 mod a

Ablauf	***x***	***y***	$\boldsymbol{q} := x\ div\ y$	$\boldsymbol{r} := x - q * y$	***u***	***s***	***v***	***t***
Initialisierung	99	79	1	99 – 79 = 20	1	0	0	1
1. Wiederholung	79	20	3	79 – 60 = 19	0	1 – **1** * 0 = **1**	1	0 – **1** * 1 = **-1**
2. Wiederholung	20	19	1	20 – 19 = 1	1	0 – **3** * 1 = **-3**	-1	1 – **3** * -1 = **4**
3. Wiederholung	19	1	19	19 – 19 = **0**	-3	1 – 1*-3 = **4**	4	-1 – 1*4 = **-5**

Bedeutet: $\mathbf{4} * \mathbf{99} + \mathbf{-5} * \mathbf{79} = \mathbf{1}\ (s * x + t * y = kgV)$

$$\boldsymbol{kgV} = \frac{x * y}{ggt(x, y)} = \frac{99 * 79}{1} = \underline{7821}$$

8. RSA-VERSCHLÜSSELUNG

Die RSA-Verschlüsselung ist ein Public-Key-Verfahren. Funktionsprinzip: Sie vergeben einen öffentlichen Schlüssel, mit dem jeder Botschaften an Sie so verschlüsseln kann, dass nur Sie sie entschlüsseln können.

8.1. PUBLIC & PRIVATE KEY ERHALTEN

1. ***Zwei Primzahlen (p,q) multiplizieren*** zum Produkt n: $n = p * q = 3 * 11 = 33$

2. Die Eulersche ***φ-Funktion von n berechnen.*** $\varphi(p * q)$ ergibt dasselbe Resultat und da beide Zahlen Primzahlen sind, kann einfach $(p - 1) * (q - 1)$gerechnet werden.
$\varphi(n) = \varphi(p * q) = \varphi(3) * \varphi(11) = (3 - 1) * (11 - 1) = 2 * 10 = 20$

3. Eine ***beliebige Zahl a zwischen 1 und $\varphi(n)$ auswählen***, die mit $\boldsymbol{\varphi(n)}$teilerfrend ist:
z.B. a = 3, Test: ggt(20,3)=1

4. Das ***multiplikative Inverse b*** von a in $\mathbb{Z}_{\varphi(n)}$ berechnen $a * b \equiv 1 \, mod \, \varphi(n)$
$3 * b \equiv 1 \, mod \, 20$
Kleinstmögliche Zahl $3 * 7 = 21, \frac{21-1}{20} = 1$ => durch **20** teilbar, also $b = 7$

5. Nun haben wir den ***Public Key (b & n)*** und den ***Private Key(a)*** zur Verschlüsselung:
$b = 7, n = 33 \; und \; a = 3$

8.2. TEXT VERSCHLÜSSELN

1. ***Buchstabentabelle*** generieren, zum Beispiel

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

2. Text in ***Zahlen aus Tabelle umwandeln***: T = 20, E = 5, S = 19, T = 20

3. Zahlen mit b ***potenzieren*** und ***Modulo*** **n** rechnen:
$20^7 \, mod \, 33 \equiv 26, \; 5^7 mod \, 33 \equiv 14, \; 19^7 mod \, 33 \equiv 13$

4. Nun kann die ***Nachricht*** «26, 14, 13, 26» ***gesendet*** werden.

8.3. TEXT ENTSCHLÜSSELN

1. ***Dieselbe Buchstabentabelle*** wie beim Verschlüsseln verwenden.

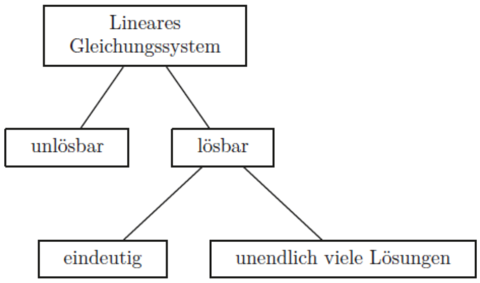
2. Die empfangene Nachricht mit a ***potenzieren*** und ***Modulo*** **n** rechnen:
$26^3 \, mod \, 33 \equiv 20, \; 14^3 \, mod \, 33 \equiv 5 \;\; 13^3 \, mod \, 33 \equiv \; 19$

3. Zahlen in Buchstaben umwandeln: 20 = **T**, 5 = **E**, 19 = **S**, 20 = **T**

9. LINEARE ALGEBRA

Allgemein ist eine linare Gleichung in einer Variablen x von der Form $ax = b$, wobei a, b reelle Konstanten sind. Eine lineare Gleichung in n Variablen $x_1,\ x_2, \dots, x_n$ hat die Gestalt $a_1x_1 + a_2x_2 + \cdots + a_nx_n = b$, wobei $a_1,\ a_2, \dots, a_n$ und b ***reelle Konstanten*** sind.

9.1. LINEARES GLEICHUNGSSYSTEM MIT ZWEI UNBEKANNTEN



Die beiden Gleichungen unten bilden ein lineares Gleichungssystem mit zwei Unbekannten.

$$x_1 - 2x_2 = 1$$
$$3x_1 + 2x_2 = 11$$

Bei einem Gleichungssystem wie unten, lässt sich erkennen, dass das System ***unendlich viele Lösungen*** hat:

$$x_1 + 2x_2 = 4 \qquad \Rightarrow x_1 = 4 - \ 2x_2$$
$$0x_1 + 0x_2 = 0$$

Für die freie Variable x_2 kann man einen beliebigen Parameter $t\ \in \mathbb{R}$ wählen. Die unendlich vielen Lösungen haben somit die parametrisierte Form

$$x_1 = 4 - \ 2t, x_2 = t$$

10. MATRIZEN (LINEARE ALGEBRA)

Ein lineare Gleichungssystem kann auch als Matrizen ausgedrückt werden.

Zum Beispiel das Geichunggsystem oben (Hinterste Spalte ist die Lösung):

$$A = \begin{bmatrix} 1 & -2 & 1 \\ 3 & 2 & 11 \end{bmatrix}$$

Anzahl Zeilen = m, hier 2; Anzahl Spalten = n, hier 3 (mit Lösung).

Besteht eine Matrix aus einer ***einzigen Spalte***, so heisst sie ***Spaltenmatrix***, besteht sie aus einer ***einzigen Zeile,*** ist sie eine ***Zeilenmatrix***. Eine (1,1)-Matrix ist sowohl Zeilen- als auch Spaltenmatrix und wird auch als ***Skalar*** bezeichnet.

Vertauscht man Zeilen und Spalten einer Matrix, so erhölt man die ***transponierte Matrix***.

Spaltenmatrizen
werden mit Kleinbuchstaben angeschrieben. Sie können auch mit ***Vektoren*** identifiziert werden.

$$a = \begin{bmatrix} a_1 \\ a_2 \\ \dots \\ a_n \end{bmatrix}$$

Einheitsmatrix
Quadratische Diagonalmatrix, deren Diagonalelemente alle gleich 1 sind

$$E = \begin{bmatrix} 1 & & & \\ & 1 & & \\ & & \dots & \\ & & & 1 \end{bmatrix}$$

Obere und untere Dreiecksmatrix
Eine ***obere Dreiecksmatrix*** hat ***unterhalb der Diagonale nur Nullen***. Eine ***untere Dreiecksmatrix*** hat ***oberhalb der Diagonale nur Nullen***.

10.1. RECHNEN MIT MATRIZEN

Zwei Matrizen sind gleich, wenn sie dieselbe Ordnung haben und die einander entsprechenden Elemente übereinstimmen.

$A = \begin{bmatrix} 1 & x \\ y & -2 \end{bmatrix}$ und $B = \begin{bmatrix} 1 & -1 \\ 2 & -2 \end{bmatrix}$ sind ***gleich***, wenn $x = -1$ und $y = 2$.

Addition und Subtraktion (Linearkombination)
Sind A und B zwei Matrizen gleicher Ordnung, so ist ihre Summe $A + B$ diejenige Matrix, die durch ***Addition der einander entsprechenden Elemente*** entsteht. Subtraktion funktioniert analog.

$$A = \begin{bmatrix} 1 & 2 & 3 \\ -1 & 4 & 2 \end{bmatrix} \text{ und } B = \begin{bmatrix} 0 & 2 & -4 \\ -2 & 1 & 3 \end{bmatrix}$$

$$A + B = \begin{bmatrix} 1 + 0 & 2 + 2 & 3 + (-4) \\ -1 + (-2) & 4 + 1 & 2 + 3 \end{bmatrix} = \begin{bmatrix} 1 & 4 & -1 \\ -3 & 5 & 5 \end{bmatrix}$$

Multiplikation (Produkt)
Das Matrizenprodukt berechnet sich durch Zeile von A * Spalte von B.

$$A = \begin{bmatrix} 2 & 0 \\ 6 & 8 \end{bmatrix} \text{ und } B = \begin{bmatrix} 5 & 7 & 8 \\ 9 & 10 & 11 \end{bmatrix}$$

	$B = \begin{bmatrix} 5 & 7 & 8 \\ 9 & 10 & 11 \end{bmatrix}$
$A = \begin{bmatrix} 2 & 0 \\ 6 & 8 \end{bmatrix}$	$C = \begin{bmatrix} c_{11} & c_{12} & c_{13} \\ c_{21} & c_{22} & c_{23} \end{bmatrix}$

$c_{11} = 2 * 5 + 0 * 9 = 10$ $\quad c_{12} = 2 * 7 + 0 * 10 = 14$ $\quad c_{13} = 2 * 8 + 0 * 11 = 16$
$c_{21} = 6 * 5 + 8 * 9 = 102$ $\quad c_{22} = 6 * 7 + 8 * 10 = 122$ $\quad c_{23} = 6 * 8 + 8 * 11 = 136$

Achtung: Das Matrizenprodukt ist nur für Matrizen A und B mit der Eigenschaft «Spalten von A gleich Zeilen von B» definiert.

Inverse
Die inverse Matrix A^{-1} ist die Matrix, die multipliziert mit der ursprünglichen Matrix A die Einheitsmatrix E ergibt. Besitzt eine quadratische Matrix eine ***Inverse***, so ist diese ***eindeutig bestimmt***. Das lineare quadratische Gleichungssystem $Ax = b$ hat genau dann eine ***eindeutige Lösung*** $x = A^{-1}b$, wenn A ***invertierbar*** (regulär) ist.

Bei 2x2 Matrix

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \frac{1}{ad - bc} * \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

Bei 3x3 Matrix

$$A = \begin{bmatrix} 2 & 0 & 1 \\ 4 & 1 & 2 \\ 4 & 2 & 0 \end{bmatrix}$$

1. Die ***Einheitsmatrix neben die ursprüngliche Matrix A schreiben***. Ab jetzt wird diese erweiterte Matrix als Gesamtpaket betrachtet.

$$A = \begin{bmatrix} 2 & 0 & 1 & | & 1 & 0 & 0 \\ 4 & 1 & 2 & | & 0 & 1 & 0 \\ 4 & 2 & 0 & | & 0 & 0 & 1 \end{bmatrix}$$

2. Matrix ***umformen***, dass ***links die Einheitsmatrix*** ist (mit dem Gauss-Jordan-Algorithmus)

$$A = \begin{bmatrix} 1 & 0 & 0 & | & 1 & -0.5 & 0.25 \\ 0 & 1 & 0 & | & -2 & 1 & 0 \\ 0 & 0 & 1 & | & -1 & 1 & -0.5 \end{bmatrix}$$

3. Invertierte Matrix ***ablesen***.

$$A^{-1} = \begin{bmatrix} 1 & -0.5 & 0.25 \\ -2 & 1 & 0 \\ -1 & 1 & -0.5 \end{bmatrix}$$

10.2. ELEMENTARE UMFORMUNGEN UND ZEILENSTUFENFORMEN

Unter einer elementaren Gleichungsumformung versteht man eine der drei grundlegenden Operationen:

- Gleichungen ***vertauschen***
- Gleichung mit einer Konstante ($\neq 0$) ***multiplizieren***
- ***Addition*** eines Vielfachen einer Gleichung zu einer anderen Gleichung

> Elementare Gleichungsumformungen ***ändern nicht die Lösungsmenge*** eines linearen Gleichungssystems.

Zeilenstufenform
Durch elementare Zeilenumformungen kann man nun jede Matrix auf ***Zeilenstufenform*** bringen. Eine Matrix hat Zeilenstufenform, wenn folgende Eigenschaften erfüllt sind:

- Alle Zeilen, die nur ***Nullen*** enthalten, stehen in den ***untersten Zeilen*** der Matrix.
- Wenn eine Zeile nicht nur aus Nullen besteht, so ist die ***erste von Null verschiedene Zahl eine Eins*** (führende Eins).
- In zwei aufeinanderfolgenden Zeilen, die nicht nur aus Nullen bestehen, steht die ***führende Eins der unteren Zeile rechts von der führenden Eins der oberen Zeile***.

$$\begin{bmatrix} \mathbf{1} & 4 & 3 & 7 \\ 0 & \mathbf{1} & 5 & 2 \\ 0 & 0 & \mathbf{1} & 9 \end{bmatrix}$$

Die Zeilenstufenform kann dann wieder als Gleichung geschrieben werden. Dabei entspricht jede Spalte einer Variable (hier x_n).

$$\begin{bmatrix} 1 & 0 & 0 & 4 & -1 \\ 0 & 1 & 0 & 2 & 6 \\ 0 & 0 & 1 & 3 & 2 \end{bmatrix} \rightarrow \left| \begin{matrix} x_1 & & & + 4x_4 = & -1 \\ & x_2 & & + 2x_4 = 6 \\ & & x_3 & + 3\,x_4 = 2 \end{matrix} \right|$$

Die führenden Einsen werden so zu ***führenden Variablen***, die übrigen (hier x_4) werden zu ***freien Variablen***. Nun kann man die freien Variablen auf die rechte Seite subtrahieren, um die Gleichungen nach den führenden Variablen aufzulösen.

$$\left| \begin{matrix} x_1 = & -1 - 4x_4 \\ x_2 = 6 - 2x_4 \\ x_3 = 2 - 3x_4 \end{matrix} \right|$$

Reduzierte Zeilenstufenform

Besitzt eine Matrix Zeilenstufenform und gilt noch zusätzlich, dass eine Spalte, die eine führende Eins enthält, keine weiteren von Null verschiedenen Einträge enthält, dann hat sie reduzierte (normierte) Zeilenstufenform.

$$\begin{bmatrix} \mathbf{1} & 0 & 0 & 4 \\ 0 & \mathbf{1} & 0 & 7 \\ 0 & 0 & \mathbf{1} & -1 \end{bmatrix} \Rightarrow x_1 = 4, x_2 = 7, x_3 = -1$$

-> Siehe Gauss-Jordan-Algorithmus

11. GAUSS-(JORDAN-)ALGORITHMUS (LINEARE ALGEBRA)

Damit lässt sich ein lineares Gleichungssystem in (reduzierte) Zeilenstufenform bringen.

Gauss -Verfahren (Zeilenstufenform)

1. Wir bestimmen die am ***weitesten links stehende Spalte***, die von Null verschiedene Werte enthält.

$$\begin{bmatrix} \mathbf{1} & 1 & 2 & 9 \\ \mathbf{2} & 4 & -3 & 1 \\ \mathbf{3} & 6 & -5 & 0 \end{bmatrix}$$

2. Die oberste Zahl in der ersten Spalte darf ***keine Null*** sein. Sonst mit anderen Zeile ***vertauschen***.

3. Ist a das erste Elemente der in Schritt 1 gefundenen Spalte, dann dividieren wir die erste Zeile durch a, um die ***führende Eins zu erzeugen***. (falls zB. 3 $\Rightarrow Zeile$ / 3)

4. Wir addieren ***passende Vielfache der ersten Zeile zu den übrigen Zeilen***, um unterhalb der führenden Eins Nullen zu erzeugen.

$$\begin{bmatrix} 1 & 1 & 2 & 9 \\ 2 & 4 & -3 & 1 \\ 3 & 6 & -5 & 0 \end{bmatrix} \begin{matrix} \\ +(-2 * erste\ Zeile) \\ +(-\ 3 * erste\ Zeile) \end{matrix}$$

ergibt:

$$\begin{bmatrix} \mathbf{1} & 1 & 2 & 9 \\ \mathbf{0} & 2 & -7 & -17 \\ \mathbf{0} & 3 & -11 & -27 \end{bmatrix}$$

5. Wir wenden die ersten vier Schritte auf den Teil der Matrix an, den wir durch Streichen der ersten Zeile erhalten, und ***wiederholen dieses Verfahren***, bis die erweiterte Koeffizientenmatrix Zeilenstufenform hat.

$$\begin{bmatrix} 1 & 1 & 2 & 9 \\ 0 & 2 & -7 & -17 \\ 0 & 3 & -11 & -27 \end{bmatrix} * 1/2$$

$$\begin{bmatrix} 1 & 1 & 2 & 9 \\ 0 & 1 & -7/2 & -17/2 \\ 0 & 3 & -11 & -27 \end{bmatrix} + (-3 * zweite\ Zeile)$$

$$\begin{bmatrix} 1 & 1 & 2 & 9 \\ 0 & 1 & -7/2 & -17/2 \\ 0 & 0 & -1/2 & -3/2 \end{bmatrix} * -2$$

$$\begin{bmatrix} 1 & 1 & 2 & 9 \\ 0 & 1 & -7/2 & -17/2 \\ 0 & 0 & 1 & 3 \end{bmatrix}$$

6. Wir lösen das System in Zeilenstufenform durch ***Rückwärtssubstitution***.

$$x = 9 - y - 2z \ \Rightarrow 9 - 2 - 6 = \underline{1}$$

$$y = -\frac{17}{2} + \frac{7}{2}z \ \Rightarrow y = -\frac{17}{2} + \frac{21}{2} = \frac{4}{2} = \underline{2}$$

$$z = 3$$

Gauss -Jordan-Verfahren (reduzierte Zeilenstufenform)

1. Schritte ***1-5 vom Gauss-Jordan-Verfahren*** durchführen.

2. Mit der letzten nicht verschwindenden Zeile beginnend, addiere man geeignete Vielfache jeder Zeile zu den darüber liegenden Zeilen, um ***über den führenden Einsen Nullen zu erzeugen***.

$$\begin{bmatrix} 1 & 1 & 2 & 9 \\ 0 & 1 & -7/2 & -17/2 \\ 0 & 0 & 1 & 3 \end{bmatrix} \begin{array}{l} +(-2*dritte\ Zeile) \\ +(7/2*dritte\ Zeile) \\ \end{array}$$

$$\begin{bmatrix} 1 & 1 & 0 & 3 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 3 \end{bmatrix} \begin{array}{l} +(-1*zweite\ Zeile) \\ \\ \end{array}$$

$$\begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 3 \end{bmatrix}$$

Nun kann die Lösung direkt ***abgelesen werden*** $z = 3, y = 2, x = 1$

Pivotsuche

Man kann bei den Matrizen auch die Zeilen ***vertauschen***, wenn sich dadurch das Verfahren einfacher anwenden lässt, das muss man sich jedoch merken und am Schluss wieder ***zurücktauschen***.

11.1. ZU GAUSS-ALGORITHMUS UND DETERMINANTE

- Das ***Tauschen von benachbarten Zeilen*** führt in der Determinante zu ***Vorzeichenwechseln***.
- ***Multiplikation*** einer Zeile mit $c \in \mathbb{R}$ führt zu $c * det\,(A)$.
- ***Addition eines Vielfachen einer Zeile*** zu einer anderen ***ändert die Determinante nicht***.

12. VEKTOREN

12.1. BEGRIFFE

- ***Ortsvektor:*** Vektor vom Ursprung zu einem Punkt $\overrightarrow{OP}$
- ***Normalenvektor:*** Vektor, der im 90°-Winkel zu einem anderen Vektor steht.
- ***Parameterform:*** Möglichkeit, um eine Gerade oder eine Ebene darzustellen. Dabei wird ein Stütz- und ein Richtungsvektor benötigt.
- ***Stützvektor:*** Vorder Vektor in der Parameterform, fast immer Ortsvektor. Definiert den «Startpunkt» des Vektors.
- ***Richtungsvektor:*** Hinterer Vektor in der Parameterform. Definiert die Länge und Richtung des Vektors und kann mithilfe des Parameters t beliebig skaliert werden.

Rechenregeln für geometrische Vektoren

1. Kommutativität: $u + v = v + u$

2. Assoziativität: $(u + v) + w = u + (v + w)$

3. Nullvektor: Für jeden Vektor v gilt $v + o = v$

4. Existenz negativer Vektoren: Zu jedem Vektor v gibt es einen Gegenvektor $-v$ mit $v + (-v) = o$.

12.2. SKALARES VIELFACHES

Für einen Vektor $v \neq 0$ und eine reelle Zahl $r \neq 0$ bezeichnet man mit dem skalaren Vielfachen $r * v$ den Vektor, dessen Pfeile:

- ***Parallel*** zu den Pfeilen von v sind
- $|r|$***-mal so lang*** wie die Pfeile von v sind
- ***Gleich gerichtet*** zu den Pfeilen von v sind, falls $\boldsymbol{r > 0}$, ***entgegengesetzt*** gerichtet zu den Pfeilen von v, falls $\boldsymbol{r < 0}$ ist.

Die Verknüpfung eines Skalars mit einem Vektor nenne man ***skalare Multiplikation***. Dafür gelten folgende Regeln:

Rechenregeln für skalare Multiplikation

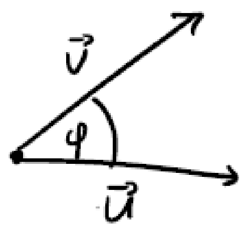
Für alle reellen Zahlen c, d und für alle geometrischen Vektoren $\mathrm{u}, \mathrm{v}, \mathrm{w}$ gelten die folgenden Eigenschaften:

1. Distributivität: $c * (v + w) = (c * v) + (c * w)$
2. Distributivität: $(c + d) * v = (c * v) + (d * v)$
3. Assoziativität: $c * (d * v) = (c * d) * v$
4. $1 * v = v$
5. $v * w = w * v$
6. $(u + v) * w = u * w + v * w$
7. $(c * w) * v = w * (c * v) = c * (w * v)$

12.3. SKALARPRODUKT

Mit dem Skalarprodukt lassen sich ***zwei Vektoren miteinander multiplizieren***, die ***gleich gross*** sind. Als Ergebnis erhält man eine ***reelle Zahl***, die ***Skalar*** genannt wird.

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



Damit lässt sich auch der ***Winkel zwischen Vektoren*** berechnen:

$$\vec{u} * \vec{v} = |\vec{u}| * |\vec{v}| * \cos(\varphi)$$

$$\Rightarrow \cos(\varphi) = \frac{\vec{u} * \vec{v}}{|\vec{u}| * |\vec{v}|}$$

Eigenschaften

- $\vec{u} * \vec{v}$ ist ***positiv***, wenn $0 \leq \varphi < 90°$ (***spitzer Winkel***)
- $\vec{u} * \vec{v}$ ist ***0***, wenn $\varphi = 90°$(***rechter Winkel***, orthogonal)
- $\vec{u} * \vec{v}$ ist ***negativ***, wenn $\varphi > 90°$(***stumpfer Winkel***)
- $\vec{u} * \vec{v} = 0$, wenn $\vec{u} = 0$ oder $\vec{v} = 0$

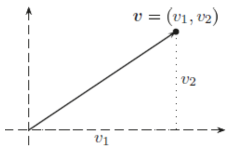
12.4. ORTHOGONALE VEKTOREN

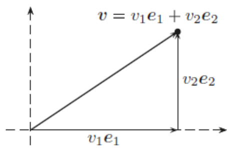
Stehen zwei Vektoren ***senkrecht aufeinander***, so nennt man das auch ***orthogonal***. Wenn wir noch vereinbaren, dass der Nullvektor senkrecht zu jedem Vektor ist, erhalten wir:

Zwei Vektoren u und v sind genau dann ***orthogonal***, wenn $\boldsymbol{u * v = 0}$ ist.

12.5. KOORDINATEN- UND KOMPONENTENFORM

Ist $v = (v_1, v_2) \in \mathbb{R}^2$, so sind v_1 und v_2 die Koordinaten des Vektors v und $\boldsymbol{v = (v_1, v_2)}$ seine ***Koordinatenform*** (links im Bild). Eine andere Darstellungsform erhalten wir mit den natürlichen Einheitsvektoren e_1 und e_2. Das Skalarprodukt des Einheitsvektors e_1 mit dem Vektor v ergbit die erste Koordinate v_1 von v: $v * e_1 = (v_1, v_2) * (1,0) = v_1 * 1 + v_2 * 0 = v_1$.





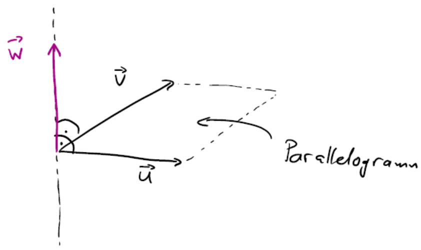
Der Vektor $(v * e_1)e_1 = v_1e_1$ ist der orthogonale Projektionsvektor von v auf e_1. Den Vektor v kann man daher folgendermassen schreiben (***Komponentenform***, rechts im Bild):

$$v = (v_1, v_2) = (v_1, 0) + (0, v_2) = v_1(1,0) + v_2(0,1) = \boldsymbol{v_1e_1 + v_2e_2}$$

12.6. KREUZPRODUKT

Existiert nur im Raum $\mathbb{R}^3$. Unter dem ***Kreuzprodukt*** $u \times v$ zweier räumlicher Vektoren u und v versteht man den eindeutig bestimmten Vektor mit folgenden drei Eigenschaften $(u \times v \text{ wird in } Bild\ als\ w\ bezeichnet)$

- $u \times v$ ist ***sowohl zu u als auch zu v orthogonal*** (steht senkrecht auf beide)
- Die ***Länge des Vektors*** $u \times v$ ist ***gleich dem Produkt aus den Längen der Vektoren u und v und dem Sinus*** des von ihnen eingeschlossenen Winkels: $|u \times v| = |u||v| \sin(\varphi)\ mit\ 0° \leq \varphi \leq 180°$
- Die Vektoren u, v und $u \times v$ bilden in dieser Reihenfolge ein ***Rechtssystem***.

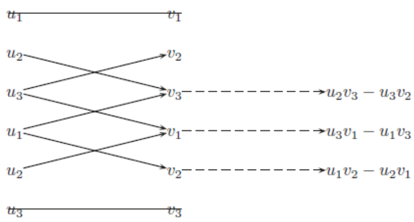


Weiter gilt:

- Die ***Länge des Kreuzproduktes*** $u \times v$ entspricht dem ***Flächeninhalt*** des von den Vektoren u und v aufgespannten ***Parallelogramms*** (Vektorprodukt).
- Wenn das ***Kreuzprodukt Null*** ergibt, so sind die Vektoren ***parallel***.

Kreuzprodukt berechnen

$$\vec{u} \times \vec{v} = \begin{pmatrix} u_1 \\ u_2 \\ u_3 \end{pmatrix} \times \begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix} = \begin{pmatrix} u_2v_3 - u_3v_2 \\ u_3v_1 - u_1v_3 \\ u_1v_2 - u_2v_1 \end{pmatrix}$$



Rechenregeln des Kreuzproduktes

Sind u, v und w beliebige Vektoren im Raum und c eine reelle Zahl, so gilt:

1. Anti-Kommutativität: $u \times v = -(v \times u)$
2. Distributivität: $u \times (v + w) = (u \times v) + (u \times w)$
3. Distributivität: $(u + v) \times w = (u \times w) + (v \times w)$
4. Assoziativität: $c(u \times v) = (cu) \times v = u \times (cv)$
5. $u \times 0 = 0 \times u = 0$

13. LINEARE ABBLIDUNGEN

Eine Abbildung $L: V \to W$ heisst linear, wenn sie mit den Vektorraum-Verknüpfungen $+$ und $*$ in V und W verträglich ist, das heisst, wenn es gleichgültig ist, ob ich zwei Vektoren in V erst addiere und dann die Summe nach W abbilde oder ob ich sie erst abbilde und dann ihre Bilder addiere; entsprechend für die skalare Multiplikation.

Eine ***Abbildung L von $\mathbb{R}$ nach $\mathbb{R}$ ist linear***, wenn sie die Form $\boldsymbol{L(x) = ax,\ x \in \mathbb{R}}$ hat, wobei a ein reeller Parameter ist.

Der Graph einer linearen Funktion von $\mathbb{R}$ nach $\mathbb{R}$ ist eine Gerade und geht durch den Koordinatenursprung, dabei ist ***a die Steigung*** der Geraden. L ist nur dann eine lineare Abbildung, wenn der Graph von L eine Gerade ist und durch den Koordinatenursprung geht.

Jede reelle lineare Funktion $L: \mathbb{R} \to \mathbb{R}$ hat die folgenden Eigenschaften:
Für alle $\mathrm{x, y, c} \in \mathbb{R}$ gilt:
1. $\mathrm{L(x+y)} = L(x) + L(y)$
2. $\mathrm{L(cx)} = cL(x)$
3. $\mathrm{L(0)} = 0$
Beispiel: $\mathrm{f}(p * x + q * y) = p * f(x) + q * f(y)$

Eine Abbildung ist nur linear, wenn diese Bedingungen zutreffen.

Matrizen und lineare Abbildungen
1. Eine Lineare Abbildung L wird ***eindeutig durch eine Matrix*** A dargestellt.
2. Eine Matrix A ***erzeugt eine lineare Abbildung*** L.
Das heisst, Lineare Abbildungen und Matrizen sind «dasselbe» (Lineare Abbildung ist eine Funktion und eine Matrize ein rechteckiges Zahlensystem)

Zu beachten: Die Addition $x + y$ findet im Vektorraum $\mathbb{R}^n$ statt, während die Addition $L(x) + L(y)$ im Vektorraum $\mathbb{R}^m$ stattfindet.

Sei L eine lineare Funktion. Dann:

$$e_1 = \begin{bmatrix} 1 \\ 0 \\ 0 \\ \dots \\ 0 \end{bmatrix}, e_2 = \begin{bmatrix} 0 \\ 1 \\ 0 \\ \dots \\ 0 \end{bmatrix}, x = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ \dots \\ x_n \end{bmatrix}, A = [L(e_1) \quad L(e_2) \quad \dots \quad L(e_n)]$$

Die Matrix besteht aus den Bildern der kanonischen Einheitsvektoren.

$$A\,x = A(x_1e_1 + x_2e_2 + \dots + x_ne_n) = x_1Ae_1 + x_2Ae_2 + \dots + x_nAe_n = x_1L(e_1) + \dots + x_nL(e_n) = L(x)$$

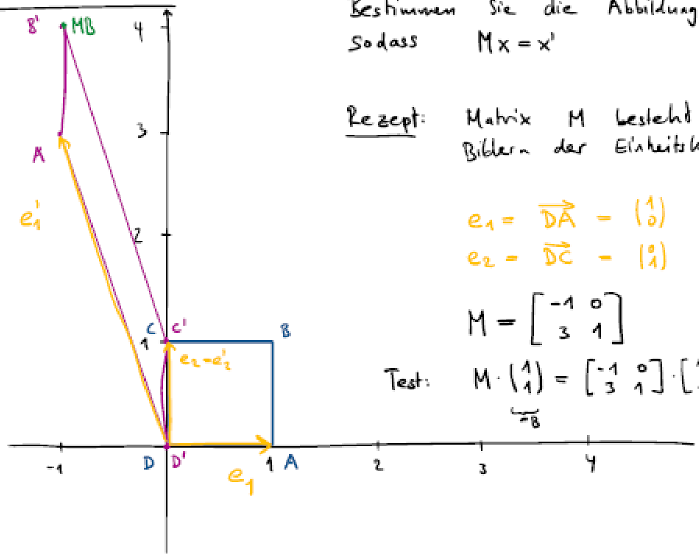
13.1. NULLABBILDUNG

Es ist O die (m, n)-Nullmatrix und o der Nullvektor im $\mathbb{R}^m$. Dann gilt für jeden Vektor $\mathrm{x} \in \mathbb{R}^n$:

$\boldsymbol{O(x) = Ox = o,}$

also bildet die Multiplikation mit der Nullmatrix O jeden Vektor des $\mathbb{R}^n$ in den Nullvektor des $\mathbb{R}^m$ ab. O heisst Nullabbildung von $\mathbb{R}^n$ nach $\mathbb{R}^m$.

Beispiele (siehe Ergänzungen)



Bestimmen Sie die Abbildungsmatrix M sodass $Mx = x'$

Rezept: Matrix M besteht aus den Bildern der Einheitsvektoren

$e_1 = \overrightarrow{DA} = \binom{1}{0}$

$e_2 = \overrightarrow{DC} = \binom{0}{1}$

$M = \begin{bmatrix} -1 & 0 \\ 3 & 1 \end{bmatrix}$

Test: $M \cdot \underbrace{\binom{1}{1}}_{=B} = \begin{bmatrix} -1 & 0 \\ 3 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \begin{bmatrix} -1 \\ 4 \end{bmatrix} = B'$

Gegeben: Punkte Original (Rechteck) und Bild (Parallelogramm):

$A = (1;-1), B = (1;1), C = (-1;1), D = (-1;-1)$

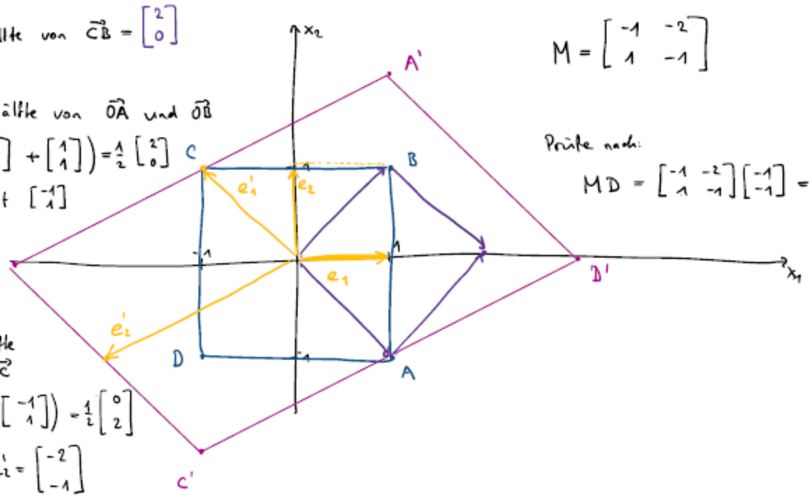
$A' = (1;2), B' = (-3;0), C' = (-1;-2), D' = (3;0)$

Gesucht: Abbildungsmatrix M, so dass gilt: $M \cdot \vec{x} = \vec{x}'$

e_1 ist die Hälfte von $\overrightarrow{CB} = \begin{bmatrix} 2 \\ 0 \end{bmatrix}$ d.h. $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$

e_1 ist die Hälfte von $\overrightarrow{OA}$ und $\overrightarrow{OB}$ d.h. $\frac{1}{2}\left(\begin{bmatrix} 1 \\ -1 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \end{bmatrix}\right) = \frac{1}{2}\begin{bmatrix} 2 \\ 0 \end{bmatrix}$

Bild von e_1 ist $\begin{bmatrix} -1 \\ 1 \end{bmatrix}$



e_2 ist die Hälfte von $\overrightarrow{OB}$ und $\overrightarrow{OC}$

$e_2 = \frac{1}{2}\left(\begin{bmatrix} 1 \\ 1 \end{bmatrix} + \begin{bmatrix} -1 \\ 1 \end{bmatrix}\right) = \frac{1}{2}\begin{bmatrix} 0 \\ 2 \end{bmatrix}$

Bild von $e_2 = e_2' = \begin{bmatrix} -2 \\ -1 \end{bmatrix}$

$M = \begin{bmatrix} -1 & -2 \\ 1 & -1 \end{bmatrix}$

Prüfe nach:

$MD = \begin{bmatrix} -1 & -2 \\ 1 & -1 \end{bmatrix}\begin{bmatrix} -1 \\ -1 \end{bmatrix} = \begin{bmatrix} 3 \\ 0 \end{bmatrix} = D'$ ✓

14. GERADEN UND EBENEN

Eine Gerade hat keinen Start- oder Endpunkt (sonst wäre es eine Strecke).

14.1. DARSTELLUNGEN VON GERADEN

Sind eine Gerade und zwei Punkte P und Q auf dieser gegeben, so gilt: Für einen beliebigen Punkt X der Geraden ist $x = \overrightarrow{OX} = \overrightarrow{OP} + \overrightarrow{PX}$ der Ortsvektor. Da P, Q und X auf derselben Geraden liegen, sind $\overrightarrow{PX}$ und $\overrightarrow{PQ}$ Vielfache voneinander.

Parameterform

Jede Gerade in der Ebene oder im Raum lässt sich durch eine Gleichung der Form

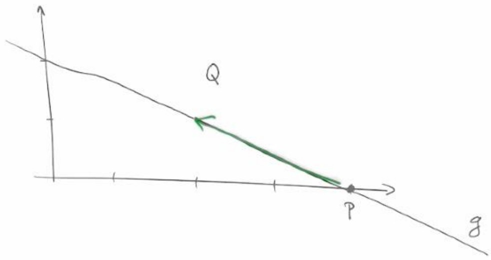
$\boldsymbol{x} = \vec{\boldsymbol{p}} + \boldsymbol{t}\vec{\boldsymbol{u}}, \qquad \boldsymbol{t} \in \mathbb{R}$

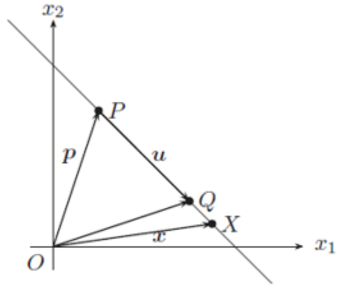
Beschreiben. Hierbei ist p ein **Stützvektor**, $u \neq o$ ein **Richtungsvektor** und t ein reeller Parameter.

Beispiel: $P = (4{,}0), Q = (2{,}1)$

$x = \begin{pmatrix} 4 \\ 0 \end{pmatrix} + t\begin{pmatrix} \mathbf{-2} \\ 1 \end{pmatrix}$

$L = \{\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 4-2t \\ t \end{pmatrix}, t \in \mathbb{R}\}$





Achtung: bei t() sind die Zahlen nicht gleich Q, sondern der Abstand von P zu Q.

Koordinatenform

Jede Gerade in der x_1, x_2-Ebene lässt sich durch eine Koordinatengleichung

$\boldsymbol{ax_1 + bx_2 - d = 0}$ oder $\boldsymbol{(a, b) * (x_1, x_2) - d = 0}$

Beschreiben, bei der mindestens einer der beiden Koeffizienten a und b ungleich Null ist.

Beispiel von oben in Koordinatenform

In Komponentengleichung umwandeln:

$x_1 = 4 - 2t$

$x_2 = 0 + t$

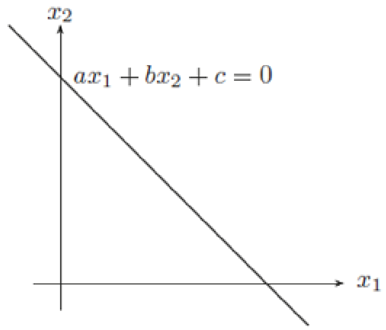
Ersetze t mit 2. Gleichung, die nach t aufgelöst wurde

$x_1 = 4 - 2x_2$

Danach noch umstellen:

$x_1 + 2x_2 - 4 = 0$

--> ist eine parameterfreie Darstellung und nicht eindeutig.



Es lässt sich auch hier der Normalenvektor n ablesen: $\boldsymbol{a}x_1 + \boldsymbol{b}x_2 - 4 = 0$

$n = \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \end{pmatrix}$

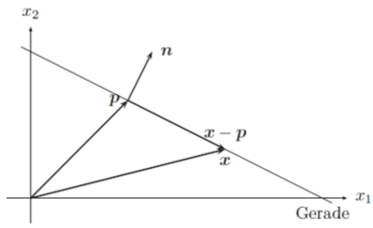
Normalenform

Jede Gerade in der Ebene lässt sich durch eine Normalengleichung

$\boldsymbol{(x - p) * n = 0}$ oder $\boldsymbol{x * n = p * n}$

Beschreiben. Hierbei ist p ein Stützvektor und n ein Normalenvektor.

Normalenvektor steht ***senkrecht*** zur Geraden.



Beispiel von oben in Normalenform:

$\vec{n}$ ist $\vec{u}$ von der Parameterform, gedreht und zweite Komponente negiert.

Skalarprodukt

$\left(\vec{x} - \begin{pmatrix} 4 \\ 0 \end{pmatrix}\right) * \begin{pmatrix} 1 \\ 2 \end{pmatrix} = 0 \Leftrightarrow$

$\vec{x} * \begin{pmatrix} 1 \\ 2 \end{pmatrix} - (4 \;\; 0) * \begin{pmatrix} 1 \\ 2 \end{pmatrix} = 0 \Leftrightarrow$

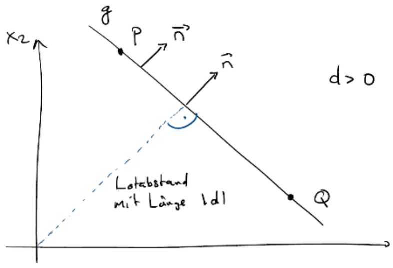
$\vec{x} * \begin{pmatrix} 1 \\ 2 \end{pmatrix} - \mathbf{4} = 0 \Leftrightarrow$ vereinfachte Normalengleichung

--> ist eine parameterfreie Darstellung und nicht eindeutig.

Hessesche Normalform

Ist ein Spezialfall der Normalenform für Geraden oder Ebenen.
Weil bei der Hesse Normalform ein **normierter Vektor** verwendet wird, kann man einen Abstand besonders gut berechnen.

$\boldsymbol{\vec{n} * \vec{x} - d = 0}$ mit $|\boldsymbol{\vec{n}}| = \boldsymbol{1}$



Eigenschaften:

$d > 0$: $\vec{n}$ vom Ursprung weg
$d < 0$: $\vec{n}$ zum Ursprung hin
$d = 0$: Gerade geht durch Ursprung

Beispiel von oben in Hessescher Normalenform:

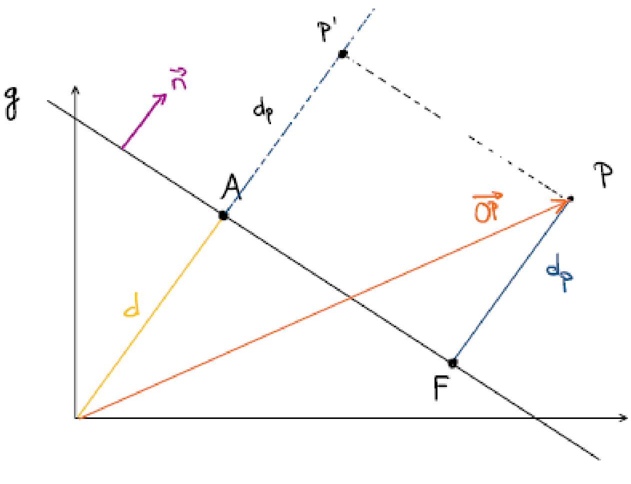
$\vec{n} = \begin{pmatrix} 1 \\ 2 \end{pmatrix} \Rightarrow |\vec{n}| = \sqrt{1^2 + 2^2} = \sqrt{5}$

-> Der Vektor muss um den Faktor $\sqrt{5}$ gekürzt werden

$$\vec{n_0} = \frac{1}{\sqrt{5}}\vec{n} = \frac{1}{\sqrt{5}}\begin{pmatrix} 1 \\ 2 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{5}} \\ \frac{2}{\sqrt{5}} \end{pmatrix} \Rightarrow$$

$$\begin{pmatrix} \boldsymbol{\frac{1}{\sqrt{5}}} \\ \boldsymbol{\frac{2}{\sqrt{5}}} \end{pmatrix} * \boldsymbol{\vec{x}} - \boldsymbol{\frac{4}{\sqrt{5}}} = \boldsymbol{0}$$

14.2. ABSTAND VON PUNKT ZU GERADE



$$\vec{OP} = \vec{OA} + \vec{AF} + \vec{FP}$$

$$\vec{FP} = \vec{OP} - \vec{OA} - \vec{AF}$$

$$\begin{aligned} \vec{FP} \cdot \vec{n} &= (\vec{OP} - \vec{OA} - \vec{AF}) \cdot \vec{n} \\ &= \vec{OP} \cdot \vec{n} - \vec{OA} \cdot \vec{n} - \underbrace{\vec{AF} \cdot \vec{n}}_{=0} \\ &= (d + d_p) - d \\ &= d_p \end{aligned}$$

$$|\vec{FP} \cdot \vec{n}| = |d_p|$$

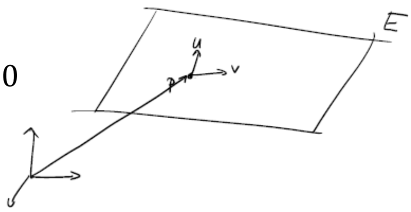
$\vec{x} \cdot \vec{n} - d = 0$ Hessesche Normalform $(|\vec{n}| = 1)$

$d_p = |\vec{p} \cdot \vec{n} - d|$ Abstand Punkt P zu Gerade g

$|\vec{n}| = 1$!

14.3. IN DER EBENE

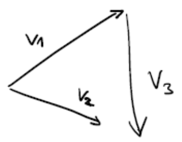
$\vec{u}, \vec{v}$ nicht parallel



- ***Parameterform:*** $\vec{x} = \vec{p} + s\vec{u} + t\vec{v}$
- ***Koordinatengleichung:*** $(a\ b\ c) * \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} - d = 0 \Leftrightarrow \vec{n} * \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} - d = 0$
- ***Normalengleichung:*** $(\vec{x} - \vec{p}) * \vec{n} - d = 0$
- ***Hessesche Normalengleichung:*** $|\vec{n}| = 1$

14.4. LINEARE UNABHÄNGIGKEIT

$\mathbb{R}^2$ Ebene



$\vec{V_3} = c_1 \vec{V_1} + c_2 \vec{V_2}$

$0 = c_1 \vec{V_1} + c_2 \vec{V_2} - \vec{V_3}$

$0 = c_1 \vec{V_1} + c_2 \vec{V_2} + c_3 \vec{V_3}$

Linearkombination von $\vec{V_1}, \vec{V_2}, \vec{V_3}$

Die Menge $\{\vec{v_1}, \vec{v_2}, \dots, \vec{v_r}\}$ ist ***linear abhängig***, wenn es eine Linearkombination

$$\sum_{i=1}^{r} c_i \vec{v_i} = \vec{0}$$

gibt, mit mindestens einem Koeffizienten $c_i \neq 0$

Die Menge $\{\vec{v_1}, \vec{v_2}, \dots, \vec{v_r}\}$ ist ***linear unabhängig***, wenn

$$\sum_{i=1}^{r} c_i \vec{v_i} = \vec{0}$$

nur für $c_i = 0$ lösbar ist.

Bzw. genau dann, wenn das lineare Gleichungssystem

$c_1\vec{v_1} + c_2\vec{v_2} + \dots + c_r\vec{v_r} = \vec{0}$

Eine eindeutige Lösung hat, nämlich $c_1 = c_2 = \dots = c_r = 0$

Beispiel

$\overrightarrow{v_1} = \begin{bmatrix}1\\2\\1\end{bmatrix}, \overrightarrow{v_2} = \begin{bmatrix}1\\0\\2\end{bmatrix}, \overrightarrow{v_3} = \begin{bmatrix}1\\1\\0\end{bmatrix}$

Kann $\vec{v} = \begin{bmatrix}2\\1\\5\end{bmatrix}$ als Linearkombination von $\{\overrightarrow{v_1}, \overrightarrow{v_2}, \overrightarrow{v_3}\}$ dargestellt werden?

Wenn ja, dann ist $\{\overrightarrow{v_1}, \overrightarrow{v_2}, \overrightarrow{v_3}, \vec{v}\}$ linear abhängig.

$\begin{bmatrix}2\\1\\5\end{bmatrix} = c_1 \begin{bmatrix}1\\2\\1\end{bmatrix} + c_2 \begin{bmatrix}1\\0\\2\end{bmatrix} + c_3 \begin{bmatrix}1\\1\\0\end{bmatrix} \Leftrightarrow \begin{bmatrix}1 & 1 & 1 & & 2\\2 & 0 & 1 & & 1\\1 & 2 & 0 & & 5\end{bmatrix} \Rightarrow$ Lässt sich mit dem Gauss-Algorithmus lösen

Beispiel

$\overrightarrow{v_1} = \begin{bmatrix}1\\2\\3\end{bmatrix}, \overrightarrow{v_2} = \begin{bmatrix}2\\5\\7\end{bmatrix}, \overrightarrow{v_3} = \begin{bmatrix}2\\4\\6\end{bmatrix}$

$? * \begin{bmatrix}1\\2\\3\end{bmatrix} + ? * \begin{bmatrix}2\\5\\7\end{bmatrix} + ? * \begin{bmatrix}2\\4\\6\end{bmatrix} = \begin{bmatrix}0\\0\\0\end{bmatrix}$, mindestens 1 Koeffizient darf nicht 0 sein, damit ***linear abhängig***

Wenn ein Vektor ein Vielfaches von einem anderen Vektor ist, geht das gut

$$\mathbf{-2} * \begin{bmatrix}1\\2\\3\end{bmatrix} + \mathbf{0} * \begin{bmatrix}2\\5\\7\end{bmatrix} + \mathbf{1} * \begin{bmatrix}2\\4\\6\end{bmatrix} = \begin{bmatrix}0\\0\\0\end{bmatrix}$$

Beispiel für linear unabhängige Vektoren wären die kanonischen Einheitsvektoren.

$\overrightarrow{v_1} = \begin{bmatrix}1\\0\\0\end{bmatrix}, \overrightarrow{v_2} = \begin{bmatrix}0\\1\\0\end{bmatrix}, \overrightarrow{v_3} = \begin{bmatrix}0\\0\\1\end{bmatrix}$

14.5. BASIS EINES VEKTORRAUMS

Die Vektoren $v_1, v_2, \dots, v_n$ bilden genau dann eine Basis des Vektorraumes V, wenn jeder Vektor v aus V als eindeutige Linearkombination der Vektoren $v_1, v_2, \dots, v_n$ dargestellt werden kann. ***Die Dimension eines Vektorraumes V ist gleich der Anzahl der Vektoren einer Basis für V. Hierfür schreiben wir $\boldsymbol{Dim(V)}$.***

Ein Vektorraum V ist endlich dimenstional, wenn eine Basis für V aus nur endlich vielen Vektoren besteht, sonst ist V unendlich dimensional.

Die Menge $M = \{v_1, v_2, \dots, v_n\}$ ist eine Basis für $\mathbb{R}^n$ genau dann, wenn jeder Vektor $v \in \mathbb{R}^n$ als eindeutige Linearkombination dargestellt werden kann. M ist linear unabhängig.

14.6. DETERMINANTE

Die Determinante gibt an, ***wie viel grösser die Fläche einer Form sein wird, wenn sie mit dieser Matrix multipliziert wird (nur bei quadratischen Matrizen)***. Ist die Determinante ***negativ***, wird die Form ***gespiegelt***. Wenn entweder eine ***Zeile / Spalte null*** ist oder zwei ***Zeilen/Spalten übereinstimmen*** oder zwei ***Zeilen/Spalten linear abhängig*** sind, ***ist die Determinante 0***.

$$\det(AB) = \det(A) * \det(B)$$

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

2x2 Matrix

$$det(A) = det \begin{bmatrix} a & b \\ c & d \end{bmatrix} = a * d - b * c$$

3x3 Matrix: Regel von Sarrus

$$\begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix} \begin{matrix} a & b \\ d & e \\ g & h \end{matrix} = a * e * i + b * f * g + c * d * h - \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix} \begin{matrix} a & b \\ d & e \\ g & h \end{matrix} = g * e * c - h * f * a - i * d * b$$

$$\Rightarrow \det(A) = \det \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix} = a * e * i + b * f * g + c * d * h - g * e * c - h * f * a - i * d * b$$

Dreiecksmatrix

$$\det \begin{bmatrix} a & b & c \\ 0 & e & f \\ 0 & 0 & i \end{bmatrix} = a * e * i$$

Bei grösseren Matrizen: Auf kleinere zurückführen.

Laplacescher Entwicklungssatz

Schritt 1: Jedem Element in der Matrix ein Plus oder Minus zuordnen, abwechslungsweise, beim Plus beginnend:

$$A = \begin{bmatrix} a^+ & b^- & c^+ \\ d^- & e^+ & f^- \\ g^+ & h^- & i^+ \end{bmatrix}$$

Schritt 2: Wir rechnen die Determinante von der ersten Zeile. Man nimmt den ersten Eintrag, a^+ und rechnet $+a *$ die Determinante von den Spalten und Zeilen, die a nicht beinhalten.

$$A = \begin{bmatrix} a^+ & b^- & c^+ \\ d^- & e^+ & f^- \\ g^+ & h^- & i^+ \end{bmatrix} \Rightarrow +a * \det \begin{bmatrix} e & f \\ h & i \end{bmatrix}$$

Das wiederholt man mit den anderen Einträgen der ersten Zeile:

$$A = \begin{bmatrix} a^+ & b^- & c^+ \\ d^- & e^+ & f^- \\ g^+ & h^- & i^+ \end{bmatrix} \Rightarrow -d * \det \begin{bmatrix} b & c \\ h & i \end{bmatrix}, A = \begin{bmatrix} a^+ & b^- & c^+ \\ d^- & e^+ & f^- \\ g^+ & h^- & i^+ \end{bmatrix} \Rightarrow +g * \det \begin{bmatrix} b & c \\ e & f \end{bmatrix}$$

ergibt:

$$\det(A) = +a * \det \begin{bmatrix} e & f \\ h & i \end{bmatrix} - d * \det \begin{bmatrix} b & c \\ h & i \end{bmatrix} + g * \det \begin{bmatrix} b & c \\ e & f \end{bmatrix}$$

Cramersche Regel

Ein Lineares Gleichungssystem $Ax = b$ ist gegeben, mit $\det(A) \neq 0$. Dann ist die Lösung x eindeutig bestimmt ($x = A^{-1}b$) und kann berechnet werden mit:

$$x = \begin{bmatrix} x_1 \\ \dots \\ x_j \\ \dots \\ x_n \end{bmatrix}, \quad x_j = \frac{\det(\hat{A}_j)}{\det(A)}, mit\ \hat{A}_j = \text{Matrix mit Spalte } j \text{ ersetzt durch } b.$$

Beispiel

$$A = \begin{bmatrix} 1 & -2 \\ -4 & 3 \end{bmatrix} \qquad b = \begin{bmatrix} -1 \\ 2 \end{bmatrix} \qquad \det(A) = 1 \cdot 3 - (-4) \cdot (-2) = 3 - 8 = -5$$

$$x = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \quad \text{mit} \quad x_1 = \frac{\det\begin{pmatrix} -1 & -2 \\ 2 & 3 \end{pmatrix}}{\det(A)} = \frac{(-3+4)}{-5} = \frac{1}{-5} = -0.2$$

$$x_2 = \frac{\det\begin{pmatrix} 1 & -1 \\ -4 & 2 \end{pmatrix}}{\det(A)} = \frac{2-4}{-5} = \frac{-2}{-5} = 0.4$$

$$x = \begin{bmatrix} -0.2 \\ 0.4 \end{bmatrix}$$

15. EIGENWERTE UND EIGENVEKTOREN

Definition

$\boldsymbol{A} \in \mathbb{R}^{\boldsymbol{n} \times \boldsymbol{m}}, \boldsymbol{x} \in \mathbb{R}^{\boldsymbol{n}}, \boldsymbol{x} \neq \boldsymbol{0}, \lambda \in \mathbb{R}$

Wenn $Ax = \lambda x$ erfüllt ist, dann nennen wir λ ***Eigenwert*** und x ***Eigenvektor***.

(λ, x) ist ein Eigenpaar («sie gehen immer zusammen, existieren nicht separat»)

Eigenvektor: es reicht einen geeigneten Vektor zu wählen, weil gestreckte Eigenvektoren sind wieder Eigenvektoren: $A(cx) = cAx = c\lambda x = \lambda(cx)$

-> Wähle Eigenvektor so, dass er einfache Komponenten hat, bzw $|x| = 1$

Beispiel

$$A = \begin{bmatrix} 1 & 1 \\ -2 & 4 \end{bmatrix}, x = \begin{bmatrix} 1 \\ 1 \end{bmatrix} \Rightarrow Ax = \begin{bmatrix} 1 * 1 & + & 1 * 1 \\ -2 * 1 & + & 4 * 1 \end{bmatrix} = \begin{bmatrix} 2 \\ 2 \end{bmatrix} = 2x \Rightarrow Ax = \underbrace{\lambda}_{Eigenwert} * \underbrace{x}_{Eigenvektor}$$

15.1. BERECHNUNG

Gegeben eine Matrix $\boldsymbol{A} \in \mathbb{R}^{\boldsymbol{n} \times \boldsymbol{m}}$

$$\left(\underbrace{A}_{Matrix} - \overbrace{\lambda}^{Skalar} * \underbrace{E}_{Einheitsmatrix} \right) x = 0$$

Die Lösungen von $\mathbf{det}(\boldsymbol{A} - \boldsymbol{\lambda E}) = \mathbf{0}$ sind Eigenwerte von A.

Beispiel: Bestimme Eigenwerte von A:

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

$$\det(A - \lambda E) = \det\left(\begin{bmatrix} 1 & 1 \\ -2 & 4 \end{bmatrix} - \begin{bmatrix} \lambda & 0 \\ 0 & \lambda \end{bmatrix}\right) = \det\left(\begin{bmatrix} 1-\lambda & 1 \\ -2 & 4-\lambda \end{bmatrix}\right) = (1-\lambda)(4-\lambda) - (-2) * 1 =$$

$$4 - 5\lambda + \lambda^2 + 2 = \lambda^2 - 5\lambda + 6 = (\lambda - 3)(\lambda - 2) = 0 \Rightarrow \underline{\text{Eigenwerte: } \lambda_1 = 2, \lambda_2 = 3}$$

Satz

$\boldsymbol{A \in \mathbb{R}^{n \times m}}$, mit r verschiedenen Eigenwerte mit $v_1, v_2, \dots, v_r$ zugehörigen Eigenvektoren.
Dann gilt: $v_1, v_2, \dots, v_r$ sind linear unabhängig.

Spezialfall: Wenn es $n = r$ paarweise verschiedene Eigenwerte gibt (So viele Eigenwerte wie Dimensionen), dann gibt es n linear unabhängige Eigenvektoren. Diese bilden eine ***Basis***.

Bei einer ***Dreiecksmatrix*** sind die ***Diagonalelemente gleich den Eigenwerten***.

15.2. DIAGONALISIERUNG EINER MATRIX

Umwandlung einer Matrix in eine Diagonalmatrix.

$$A = \begin{bmatrix} 2 & 1 & 1 \\ 0 & 3 & 0 \\ 0 & 2 & 4 \end{bmatrix}$$

Schritt 1: Finden der Eigenwerte (λ)

$$X(\lambda) = \begin{bmatrix} \mathbf{2-\lambda} & 1 & 1 \\ 0 & \mathbf{3-\lambda} & 0 \\ 0 & 2 & \mathbf{4-\lambda} \end{bmatrix}$$

$$= (2-\lambda) * (3-\lambda) * (4-\lambda) + \cancel{1 * 0 * 0} + \cancel{1 * 0 * 2} - \cancel{1 * (3-\lambda) * 0} - \cancel{0 * 2 * (2-\lambda)} - \cancel{(4-\lambda) * 1 * 0}$$

$$= (2-\lambda) * (3-\lambda) * (4-\lambda)$$

-> Die Eigenwerte sind die Nullstellen, die Nullstellen sind dort, wo eine Klammer = 0 ist.

Eigenwerte: $\lambda_1 = 2,\ \lambda_2 = 3,\ \lambda_3 = 4.$

Schritt 2: Diagonalisierbarkeit prüfen:

- Die Matrix ist ***quadratisch***
- Das ***charakteristische Polynom hat n Nullstellen*** *(in diesem Fall: 3x3 Matrix, 3 Nullstellen (λ), also erfüllt)*
- Die algebraische und geometrische Vielfachheit der Eigenwerte sind gleich *(Anzahl Eigenwerte und Eigenvektoren ist gleich)*

Schritt 3: Diagonalmatrix aufschreiben

$$D = \begin{bmatrix} \lambda_1 & 0 & 0 \\ 0 & \lambda_2 & 0 \\ 0 & 0 & \lambda_3 \end{bmatrix} = \begin{bmatrix} 2 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 4 \end{bmatrix}$$