

# Diskrete Mathematik | DMI

## Zusammenfassung

### INHALTSVERZEICHNIS

<b>1. Aussagenlogik</b>	<b>3</b>
1.1. Glossar	3
1.2. Formeln	3
1.3. Rechenregeln	4
<b>2. Prädikatenlogik</b>	<b>4</b>
2.1. Glossar	4
<b>3. Beweisen</b>	<b>4</b>
3.1. Induktion	4
3.1.1. Techniken	5
<b>4. Direkte, iterative und rekursive Berechnungen</b>	<b>5</b>
4.1. Glossar	5
<b>5. Mengen</b>	<b>5</b>
5.1. Glossar	5
5.2. Rechenregeln	5
<b>6. Formeln, Abbildungen, Relationen</b>	<b>6</b>
6.1. Glossar	6
<b>7. Modulo-Rechnen</b>	<b>6</b>
7.1. Glossar	7
7.2. Rechenregeln	7
7.3. Primfaktorenzerlegung	7
7.4. Euklidischer Algorithmus	7
7.4.1. Beispiel	7
7.5. Erweiterter Euklidischer Algorithmus	8
7.5.1. Beispiel	8
7.6. Kleiner Fermat	8
7.7. Satz von Euler	8
7.7.1. Euler'sche $\varphi$ -Funktion (Totient)	8
7.7.1.1. Rechenregeln	9
7.8. RSA Verschlüsselung	9
<b>8. Lineare Algebra</b>	<b>9</b>
8.1. Glossar	9
8.2. Pivot-Gleichung	9
8.2.1. Glossar	10
8.3. Gauss-Tableau	10
8.4. Vektoren	11
8.4.1. Glossar	11
8.4.2. Vektorenrechnen	11
8.4.3. Rechenregeln	12
8.4.4. Kreuzprodukt	12
8.4.4.1. Eigenschaften	12

8.4.4.2. Geometrische Eigenschaften .....	12
8.4.5. Vektorraum .....	12
8.4.6. Lineare Abbildung .....	13
8.5. Matrizen .....	13
8.5.1. Glossar .....	13
8.5.2. Definition .....	14
8.5.3. Matrizen als Vektoren interpretieren .....	14
8.5.4. Matrizen transponieren .....	15
8.5.5. Matrixmultiplikation .....	15
8.5.6. Rechenregeln .....	16
8.6. Analytische Geometrie .....	16
8.6.1. Geraden .....	16
8.6.1.1. Parameterform .....	16
8.6.2. Ebenen .....	16
8.6.2.1. Parameterform .....	16
8.6.2.2. Normalenform / Koordinatenform .....	16
8.6.2.3. Hessesche Normalform .....	16

# 1. AUSSAGENLOGIK

## 1.1. GLOSSAR

<i>Begriff</i>	<i>Bedeutung</i>
Aussage	Feststellender Satz, dem eindeutig «wahr» oder «falsch» zugeordnet werden kann. Symbole wie <b>A, B, C...</b> werden dafür verwendet
Aussagenlogische Form	Kombination von Aussagen, verknüpft durch Junktoren
Aussageform	Aussagen verknüpft mit Variablen
Normalform	Standartisierte Aussagenlogische Formen (Formeln)
Negationsnormalform	$\neg$ steht ausschliesslich direkt vor Aussagen oder Konstanten
Verallgemeinerte Disjunktion	<ul style="list-style-type: none"> <li>– Einzelne Aussage oder Negation</li> <li>– wahr oder falsch</li> <li>– Disjunktion <math>A \vee B</math>, falls <b>A</b> und <b>B</b> selbst verallgemeinerte Disjunktionen sind</li> </ul>
Verallgemeinerte Konjunktion	<ul style="list-style-type: none"> <li>– Einzelne Aussage oder Negation</li> <li>– wahr oder falsch</li> <li>– Konjunktion <math>A \wedge B</math>, falls <b>A</b> und <b>B</b> selbst verallgemeinerte Konjunktionen sind</li> </ul>
Disjunktive Normalform	Disjunktion von (oder eine einzelne) verallgemeinerten Konjunktionen
Konjunktive Normalform	Konjunktion von (oder eine einzelne) verallgemeinerten Disjunktionen
Kontradiktion	Immer falsch
Tautologie	Immer wahr
Junktoren (/Konnektoren)	$\neg$ Negation $\wedge$ Konjunktion $\vee$ Disjunktion (einschliessliches oder!) $\Rightarrow$ Implikation $\Leftrightarrow$ Äquivalenz
Abtrennungsregel	$(A \wedge (A \Rightarrow B)) \Rightarrow B$
Bindungsstärke	$\neg$ vor $\wedge$ , $\vee$ vor $\Rightarrow$ , $\Leftrightarrow$

## 1.2. FORMELN

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

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

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

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

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

$$\text{Abtrennungsregel: } A \wedge (A \Rightarrow B) \Rightarrow B$$

**1.3. RECHENREGELN**

<i>Begriff</i>	<i>Bedeutung</i>
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	$\neg(\neg A) \Leftrightarrow \neg\neg A \Leftrightarrow A$
Konstanten	$W = \text{wahr}$ $F = \text{falsch}$
???	$(A \Rightarrow B \Rightarrow C) \Leftrightarrow (A \Rightarrow B) \wedge (B \Rightarrow C)$
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**

<i>Begriff</i>	<i>Bedeutung</i>
Subjekt	– «Konkretes Ding» / Stellvertreter einer Variable
Prädikat	– «Eigenschaft», zB «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****TODO: MEHR BEWEISE****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

### 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	– $T(n) =$ 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:

$$\begin{aligned} \overline{\overline{A}} &= A \\ A \cap \overline{A} &= \emptyset \\ A \cup \overline{A} &= M \\ \overline{A \cap B} &= \overline{A} \cup \overline{B} \\ \overline{A \cup B} &= \overline{A} \cap \overline{B} \end{aligned}$$

## 6. FORMELN, ABBILDUNGEN, RELATIONEN

### 6.1. GLOSSAR

Begriff	Bedeutung
Funktion/Abbildung	<ul style="list-style-type: none"> <li>– Zuordnung, die jedem Element der Definitionsmenge <math>D</math> genau ein Element einer Zielmenge <math>Z</math> zuordnet.</li> <li>– Injektive Relation</li> <li>– <math>f : D \rightarrow Z</math></li> <li>– Abbildungen mit mehreren Argumenten: <math>f : A \times B \rightarrow Z, f(a, b) = y</math></li> </ul>
Graph	<ul style="list-style-type: none"> <li>– Menge von Paaren <math>(x, f(x))</math></li> <li>– <math>G \in D \times Z</math></li> </ul>
Relation	<ul style="list-style-type: none"> <li>– Teilmenge des Kartesischen Produktes mehrerer Mengen</li> <li>– <math display="block">A = \prod_{i=1}^n A_i,  A_i  = n_i \Rightarrow  A  = \prod_{i=1}^n n_i</math></li> <li>– Kleiner-Relation: <math>R_{&lt;} = \{(a, b) \mid a \in A, b \in B, a &lt; b\}</math></li> <li>– Gleich-Relation: <math>R_{=} = \{(a, b) \mid a \in A, b \in B, a = b\}</math></li> <li>– Kleiner-Gleich-Relation: <math>R_{\leq} = R_{=} \cup R_{&lt;} = \{(a, b) \mid a \in A, b \in B, a \leq b\}</math></li> </ul>
Surjektiv	– Alle Elemente der Definitions- und Zielmenge sind «verknüpft» / jedes Element der Bildmenge kommt als Bild vor
Injektiv	<ul style="list-style-type: none"> <li>– Alle Inputs haben eindeutige Outputs</li> <li>– <math>a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_2)</math></li> </ul>
Bijektiv	– Surjektiv und Injektiv
Reflexiv	<ul style="list-style-type: none"> <li>– Alle Elemente von <math>A</math> stehen zu sich selbst in Beziehung</li> <li>– <math>a \in A \Rightarrow (a, a) \in R</math></li> <li>– <math>A \Leftrightarrow A</math></li> </ul>
Symmetrisch	<ul style="list-style-type: none"> <li>– <math>(a, b) \in R \wedge (b, a) \in R</math></li> <li>– <math>(A \Leftrightarrow B) \Leftrightarrow (B \Leftrightarrow A)</math></li> </ul>
Transitiv	<ul style="list-style-type: none"> <li>– <math>(a, b) \in R \wedge (b, c) \in R \Rightarrow (a, c) \in R</math></li> <li>– <math>(A \Leftrightarrow B) \wedge (B \Leftrightarrow C) \Rightarrow (A \Leftrightarrow C)</math></li> </ul>
Äquivalenzrelation	<ul style="list-style-type: none"> <li>– reflexiv, symmetrisch und transitiv</li> <li>– <math>\Leftrightarrow, =</math></li> </ul>
Irreflexiv	– $a \in A \Rightarrow \neg(a, a) \in R$
Asymmetrisch	– $(a, b) \in R \Rightarrow \neg(b, a) \in R$
Antisymmetrisch	– $((a, b) \in R) \wedge ((b, a) \in R) \Rightarrow a = b$
Ordnungsrelation	<ul style="list-style-type: none"> <li>– reflexiv, antisymmetrisch und transitiv</li> <li>– <math>\leq</math></li> </ul>
Symmetrische Differenz	<ul style="list-style-type: none"> <li>– <math>A \Delta B = \{x \in G \mid (x \in A \cup B) \wedge \neg(x \in A \cap B)\}</math></li> <li>– <math>A \Delta B = (A \cup B) \setminus (A \cap B)</math></li> <li>– <math>(A \Delta B) \Delta C = A \Delta (B \Delta C)</math></li> </ul>

## 7. MODULO-RECHNEN

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

## 7.1. GLOSSAR

Begriff	Bedeutung
Teiler-Relation	<ul style="list-style-type: none"> <li>Für <math>a, b \in \mathbb{Z}</math> ist die Teiler-Relation <math>b \mid a \Leftrightarrow T(b, a) \Leftrightarrow \exists q \in \mathbb{Z} : bq = a</math></li> <li><math>b \mid a \Leftrightarrow -b \mid a</math></li> <li><math>b \mid a \Leftrightarrow b \mid -a</math></li> <li>Ordnungsrelation auf <math>\mathbb{N}</math></li> </ul>
Modulo-Relation	Für $a, q, r \in \mathbb{Z}$ ist die Modulo-Relation $R_q(a, r) \Leftrightarrow q \mid a - r \Leftrightarrow a \equiv r \pmod{q}$
$\sim$	<ul style="list-style-type: none"> <li>«relates to»</li> <li><math>a \sim b \Leftrightarrow (a, b) \in R</math></li> </ul>
Quotient, Rest	<p>Zu jeder Zahl <math>a \in \mathbb{Z}</math> und jeder Zahl <math>b \in \mathbb{Z}</math> gibt es eindeutig bestimmte Zahlen <math>q, r \in \mathbb{Z}</math> mit <math>a = q \cdot b + r, 0 \leq r &lt; b</math></p> <p>Bsp: <math>7 = 2 \cdot 3 + 1</math></p> <p><math>q</math> heisst <b>Quotient</b></p> <p><math>r</math> heisst <b>Rest</b></p>
Restklassen	<ul style="list-style-type: none"> <li><math>[b]_q = \{a \in \mathbb{Z} \mid a \equiv b \pmod{q}, q &gt; 0\}</math></li> <li><math>\mathbb{Z}_q = \{[0]_q, [1]_q, [2]_q, \dots, [q-1]_q\} = \underbrace{\{0, 1, 2, 3, \dots, q-1\}}_{\text{Vereinfachung}}</math></li> </ul>
Multiplikatives Inverses	Für $a \in \mathbb{Z}_q$ ist $b \in \mathbb{Z}_q$ das <b>multiplikative inverse</b> von $a$ , wenn $a \cdot b \equiv 1 \pmod{q}$
Nullteiler	Wenn für $a, b \in \mathbb{Z}_q : ab \equiv 0 \pmod{q}$ und $a \not\equiv 0 \pmod{q} \wedge b \not\equiv 0 \pmod{q}$ , heissen $a, b$ <b>Nullteiler</b>

## 7.2. RECHENREGELN

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

## 7.3. PRIMFAKTORENZERLEGUNG

Begriff	Bedeutung
$\text{ggT}(a, b)$	$\max\{d \in \mathbb{N} \mid d \mid a \wedge d \mid b\}$
$\text{kgV}(a, b)$	<ul style="list-style-type: none"> <li><math>\min\{m \in \mathbb{N} \mid a \mid m \wedge b \mid m\}</math></li> <li><math>\frac{ab}{\text{ggT}(a, b)}</math></li> </ul>
Teilerfremd	<ul style="list-style-type: none"> <li>Zwei Zahlen <math>a, b \in \mathbb{N}</math> heissen <b>Teilerfremd</b>, wenn <math>\text{ggT}(a, b) = 1</math></li> <li>Sei <math>p \in \mathbb{N}</math> eine Primzahl und <math>q \in \mathbb{N}, q &lt; p, q \neq 0</math> dann ist <math>\text{ggT}(p, q) = 1</math></li> </ul>

## 7.4. EUKLIDISCHER ALGORITHMUS

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

Initialisierung: Setze  $x := a, y := b$  und  $q := x, r := x - q \cdot y$  (d.h. bestimme  $q$  und  $r$  so, dass  $x = q \cdot y + r$  ist)

Wiederhole bis  $r = 0$  ist

Ergebnis:  $y = \text{ggT}(a, b)$

## 7.4.1. Beispiel

$\text{ggT}(122, 72), a = 122, b = 72$

– Init:  $x_0 = a = 122, y_0 = b = 72$

– Iteration:

	$x_i = y_{i-1}$	$y_i = r_{i-1}$	$q_i = x_i \text{ div } y_i$	$r_i = x_i \bmod y_i = x_i - q_i \cdot y_i$
$i = 0$	122	72	1	50
$i = 1$	72	50	1	22 Muster: $r_{i+1} < r_i$
$i = 2$	50	22	2	6
$i = 3$	22	6	3	4
$i = 4$	6	4	1	2
$i = 5$	4	$2 = \text{ggT}(122, 72)$	2	0 (immer 0 am Schluss)

### 7.5. ERWEITERTER EUKLIDISCHER 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:  $t \cdot v \equiv 1 \bmod a$

#### 7.5.1. Beispiel

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

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

Daraus folgend:

- $\text{ggT}(99, 79) + 1 + 4 \cdot 99 + (-5) \cdot 79 \Leftrightarrow 396 - 395 = 1$
- $-5$  ist mult. Inv. von  $79$  in  $\mathbb{Z}_{99}$
- $4$  ist mult. Inv. von  $99$  in  $\mathbb{Z}_{79}$

### 7.6. KLEINER FERMAT

Sei  $p \in \mathbb{N}$  eine Primzahl und  $x \in \mathbb{Z} \setminus \{0\}$  mit  $\text{ggT}(x, p) = 1$

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

Daraus folgend:

$$\begin{aligned}
 x^{p-1} &\equiv 1 \bmod p & | \quad ()^n \\
 \Leftrightarrow x^{n(p-1)} &\equiv 1 \bmod p & | \cdot x \\
 \Leftrightarrow x^{1+n(p-1)} &\equiv x \bmod p \\
 \Leftrightarrow x^{1 \bmod (p-1)} &\equiv x \bmod p
 \end{aligned}$$

### 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  $z^{\varphi(n)} \equiv 1 \bmod n$ .

#### 7.7.1. Euler'sche $\varphi$ -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  $\varphi(n)$ :



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

Falls  $p$  Primzahl ist, dann ist  $\varphi(p) = p - 1$

#### 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 hackt

Public key ist nun  $n, b$ , Private key ist  $n, a$

Sidenote: Fürs Alphabet muss  $n$  grösser sein als 26

## 8. LINEARE ALGEBRA

### 8.1. GLOSSAR

Begriff	Bedeutung
Lineares Gleichungssystem (LGS)	
Koeffizientenmatrix	
Ergebnisvektor	
Lösungsvektor	
Transponieren	

### 8.2. PIVOT-GLEICHUNG

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

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} -3 \\ -2 \\ -1 \end{pmatrix}$$

### 8.2.1. Glossar

Begriff	Bedeutung
Pivot-Variable	

### 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  $\hat{\mathbf{b}} = \begin{pmatrix} -6 \\ -4 \\ -1 \end{pmatrix}$  Lösungsvektor  $\hat{\mathbf{x}} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$  Lineares Gleichungssystem  $A \cdot \hat{\mathbf{x}} = \hat{\mathbf{b}}$

$p$  = Anzahl Pivot-Variablen.

Wenn  $b_{p+1} = \dots = b_m = 0$  dann ist das LGS lösbar (homogenes Gleichungssystem), sonst unlösbar.

Wenn  $p = n$  dann hat LGS genau eine Lösung.

Wenn  $p < n$  dann hat LGS unendlich viele Lösungen.

## 8.4. VEKTOREN

### 8.4.1. Glossar

Begriff	Bedeutung
Vektor	Liste von Zahlen
Nullvektor	$\vec{0} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$
Ortsvektor	Ortsvektor $\vec{p}$ vom Nullpunkt des Koordinatensystems $\begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$ zum Punkt $P$
Richtungsvektor	Richtungsvektor $\vec{AB}$ vom Punkt $A$ zum Punkt $B$ ist $\vec{b} - \vec{a}$
Linearkombination	Linearkombination der Variablen $x_1, x_2, x_3$ (Bsp. $3 \cdot x_1 - 2 \cdot x_2 + 4 \cdot x_3 = -6$ ). Vektoren werden jeweils mit einer Zahl multipliziert und miteinander summiert
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 $\lambda_1 = \lambda_2 = \dots = \lambda_n = 0$ $\begin{pmatrix} \uparrow & \dots & \uparrow \\ \vec{v}_1 & \dots & \vec{v}_n \\ \downarrow & \dots & \downarrow \end{pmatrix} \cdot \vec{\lambda} = \vec{0}$ eindeutig lösbar $\Rightarrow \vec{v}_1, \dots, \vec{v}_n$ sind linear unabhängig
Vektorprodukt/Kreuzprodukt	$\vec{a} \times \vec{b} = \vec{c}$ $\begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} \times \begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix} = \begin{pmatrix} a_2 b_3 - a_3 b_2 \\ a_3 b_1 - a_1 b_3 \\ a_1 b_2 - a_2 b_1 \end{pmatrix}$
Skalarprodukt	$\vec{a} \cdot \vec{b} = c$ $\begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} \cdot \begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix} = a_1 \cdot b_1 + a_2 \cdot b_2 + a_3 \cdot b_3$
Orthogonale Projektion	
Betrag/Länge eines Vektors	$\vec{a} = \begin{pmatrix} 2 \\ -3 \\ 5 \end{pmatrix}$ $ \vec{a}  = \sqrt{2^2 + (-3)^2 + 5^2} = \sqrt{38}$
Normalenvektor	= Vektorprodukt?

### 8.4.2. Vektorenrechnen

Addition:

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

Multiplikation mit reellen Zahlen (=Skalare):

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

### 8.4.3. Rechenregeln

Falls die Vektoren senkrecht zueinanderstehen, ist das Skalarprodukt gleich 0

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

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

$$-\vec{v} = -1 \cdot \vec{v}$$

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

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

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

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

### 8.4.4. Kreuzprodukt

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

#### 8.4.4.1. Eigenschaften

Anti-kommutativ:  $\vec{a} \times \vec{b} = -\vec{b} \times \vec{a}$ . Konsequenz:  $\vec{a} \times \vec{a} = -\vec{a} \times \vec{a} = \vec{0}$

Distributiv:  $\vec{a} \times (\vec{b} + \vec{c}) = \vec{a} \times \vec{b} + \vec{a} \times \vec{c}$

Gemischt-assoziativ:  $\lambda(\vec{a} \times \vec{b}) = (\lambda\vec{a}) \times \vec{b} = \vec{a} \times (\lambda\vec{b})$

Das Kreuzprodukt ist **nicht** assoziativ.  $\vec{a} \times \vec{b} \times \vec{c}$  darf man nicht!  $(\vec{a} \times \vec{b}) \times \vec{c} \neq \vec{a} \times (\vec{b} \times \vec{c})$

#### 8.4.4.2. Geometrische Eigenschaften

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

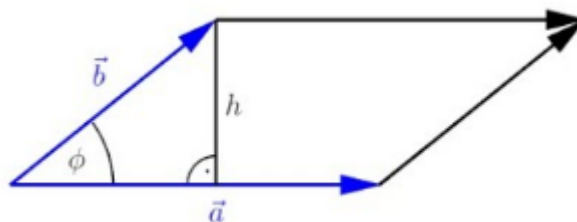


Abbildung 2: Flächeninhalt  $h \cdot a$

### 8.4.5. Vektorraum

Ein Vektorraum ist eine Menge  $V$  mit den Rechenoperationen:

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

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

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 zu  $v \in V$  **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

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

mit den Eigenschaften

$$\begin{aligned} L(\vec{x} + \vec{y}) &= L(\vec{x}) + L(\vec{y}) \\ L(\lambda \vec{x}) &= \lambda L(\vec{x}) \end{aligned}$$

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

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

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

### 8.5. MATRIZEN

#### 8.5.1. Glossar

Begriff	Bedeutung
Spaltenvektoren	Spalten der Matrix als Vektoren
Zeilenvektoren	Zeilen der Matrix als Vektoren
Rang	Wieviele Spaltenvektoren einer Matrix linear unabhängig sind

Begriff	Bedeutung
Nullmatrix	$\mathbf{0} = \begin{pmatrix} 0 & \dots & 0 \\ \vdots & \vdots & \vdots \\ 0 & \dots & 0 \end{pmatrix}$
Quadratische Matrix	$\mathbf{M} \in \mathbb{R}^{n \times n}$ Gleichviele Zeilen und Spalten
Diagonalmatrix	(immer quadratisch und symmetrisch): $\mathbf{D} = \begin{pmatrix} x_1 & 0 & 0 & 0 \\ 0 & x_2 & 0 & 0 \\ 0 & 0 & x_3 & 0 \\ 0 & 0 & 0 & x_4 \end{pmatrix}, d_{ij} = 0 \text{ für } i \neq j$
Einheitsmatrix	(immer diagonal): $\mathbf{E} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$
Symmetrische Matrix	(immer quadratisch): $\mathbf{A} = \mathbf{A}^T, a_{ij} = a_{ji}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 4 & 4 \\ 3 & 4 & 1 \end{pmatrix}$
Obere Dreiecksmatrix	$\mathbf{O} = \begin{pmatrix} x_1 & x_2 & x_3 \\ 0 & x_4 & x_5 \\ 0 & 0 & x_6 \end{pmatrix}, o_{ij} = 0 \text{ für } i > j$
Kovarianzmatrix	immer symmetrisch
Reguläre Matrix	Quadratische Matrix mit höchstem Rang (Rang = Anzahl Spalten/Reihen)
Singuläre Matrix	Quadratische Matrix mit kleinerem Rang (Rang < Anzahl Spalten/Reihen)
Invertierbare Matrix	Für $\mathbf{A} \in \mathbb{R}^{n \times n}$ heisst $\mathbf{A}$ invertierbar, wenn es eine Matrix $\mathbf{A}^{-1}$ gibt, so dass $\mathbf{A} \cdot \mathbf{A}^{-1} = \mathbf{A}^{-1} \cdot \mathbf{A} = \text{Einheitsmatrix (E)}$ . Dies ist der Fall, wenn $\mathbf{A}$ Regulär ist.
Kern	
Determinante	

### 8.5.2. Definition

Matrix mit 2 Zeilen und 3 Spalten

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

Komponenten von  $\mathbf{A}$ :  $a_{ij}$

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

### 8.5.3. Matrizen als Vektoren interpretieren

→  $\mathbf{A}$  ist ein 6-Dimensionaler VR (Vektorraum)

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

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

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

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

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

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

#### 8.5.4. Matrizen transponieren

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

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

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

Bsp:

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 2 \\ 3 & 1 \end{pmatrix} \in \mathbb{R}^{3 \times 2}$$

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

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

#### 8.5.5. Matrixmultiplikation

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

$B$  muss genau gleich viele Zeilen haben wie  $A$  Spalten

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

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

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

### 8.5.6. Rechenregeln

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

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

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

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

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

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

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

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

## 8.6. ANALYTISCHE GEOMETRIE

[beste playlist](#)

### 8.6.1. Geraden

#### 8.6.1.1. Parameterform

$$g: \vec{x} = \underbrace{\begin{pmatrix} 4 \\ 5 \\ 1 \end{pmatrix}}_{\text{Ortsvektor } \vec{p}} + t \cdot \underbrace{\begin{pmatrix} -2 \\ 1 \\ 6 \end{pmatrix}}_{\text{Richtungsvektor } \vec{p}\vec{x}}, t \in \mathbb{R}$$

### 8.6.2. Ebenen

#### 8.6.2.1. Parameterform

$$E: \vec{x} = \underbrace{\begin{pmatrix} 4 \\ 5 \\ 1 \end{pmatrix}}_{\text{Ortsvektor } \vec{o}} + s \cdot \underbrace{\begin{pmatrix} -2 \\ 1 \\ 6 \end{pmatrix}}_{\text{Spannvektor } \vec{AB}} + t \cdot \underbrace{\begin{pmatrix} -1 \\ 5 \\ 4 \end{pmatrix}}_{\text{Spannvektor } \vec{AC}}, s, t \in \mathbb{R}$$

#### 8.6.2.2. Normalenform / Koordinatenform

$$E = \left[ \begin{pmatrix} x \\ y \\ z \end{pmatrix} - \underbrace{\begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}}_{\text{Punkt auf Ebene}} \right] \cdot \underbrace{\begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix}}_{\vec{n} \text{ Orthogonal zur Ebene}} = 0$$

$$\Rightarrow x - 1 - z + 3 = 0$$

#### 8.6.2.3. Hessesche Normalform

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



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

$$|\vec{n}| = \sqrt{21}$$

$$\frac{2x - y + 4z - 1}{\sqrt{21}}$$

$$\Rightarrow \frac{2 \cdot 2 - 1 \cdot 8 + 4 \cdot 2 - 1}{\sqrt{21}} \\ = \frac{3}{\sqrt{21}}$$