

Inhaltsverzeichnis

1 Einleitung	3
2 Logik	3
2.1 Junktoren	3
2.2 Wahrheitstafeln	4
2.3 Normalformen	4
2.4 Karnaugh-Veitch-Diagramme	6
2.5 Prädikatenlogik	8
3 Beweistechniken	8
3.1 Direkter und indirekter Beweis sowie Widerspruchsbeweis	8
3.2 Vollständige Induktion	9
4 Folgen und Reihen	9
5 Mengen	10
5.1 Definitionen und Allgemeines	10
5.2 Mengenoperationen	11
5.3 Kartesisches Produkt	11
6 Relationen und Abbildungen	12
6.1 Relationen	12
6.2 Abbildungen	12
6.3 Mächtigkeit von Mengen	13
7 Modulo-Rechnen	13
7.1 Definitionen und Allgemeines	13
7.2 Rechenregeln in Restklassen	14
7.3 Erweiterter Euklidscher Algorithmus	15
7.4 RSA Verschlüsselung	17
8 Lineare Algebra	18
8.1 Lineare Gleichungssysteme	18
8.2 Matrizen und Vektoren	21
8.3 Lineare Abbildungen	27
8.4 Geraden und Ebenen	28
8.5 Vektorräume	29

1 Einleitung

Nachfolgend finden Sie eine Zusammenfassung von Konzepten sowie Formeln zur Vorlesung Diskrete Mathematik für Informatik, Herbstsemester 2024. Diese Formelsammlung ist zur Prüfung zugelassen. Markierungen und handschriftliche Ergänzungen sind erlaubt.

2 Logik

2.1 Junktoren

Notationen

- ¬ Negation (nicht)
- ∧ Konjunktion (und)
- ∨ Disjunktion (*einschliessendes* oder)
- ⇒ Implikation (wenn ... dann ...)
- ↔ Äquivalenz (genau dann, wenn)

Anmerkung: Die Implikation $A \Rightarrow B$ ist nur falsch, wenn B falsch und A richtig ist.

Bindungsstärke

In aussagenlogischen Formeln gilt folgende Bindungsstärke:

¬ vor (∧, ∨) vor (⇒, ↔)

Im Zweifelsfall - oder zur Übersichtlichkeit - Klammern setzen.

Regeln in aussagenlogischen Formeln

$$\begin{aligned} \text{Kommutativität: } & A \wedge B \Leftrightarrow B \wedge A \\ & A \vee B \Leftrightarrow B \vee A \end{aligned}$$

$$\begin{aligned} \text{Assoziativität: } & (A \wedge B) \wedge C \Leftrightarrow A \wedge (B \wedge C) \\ & (A \vee B) \vee C \Leftrightarrow A \vee (B \vee C) \end{aligned}$$

$$\begin{aligned} \text{Distributivität: } & A \wedge (B \vee C) \Leftrightarrow (A \wedge B) \vee (A \wedge C) \\ & A \vee (B \wedge C) \Leftrightarrow (A \vee B) \wedge (A \vee C) \end{aligned}$$

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

Satz 2.1 (De Morgan). Für beliebige Aussagen A, B gilt:

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

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

2.2 Wahrheitstafeln

Definition 2.1 (Kontradiktion, Tautologie). 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.

Beispiel 2.1 (Tautologie). Für zwei Aussagen A und B ergibt sich für entsprechende aussagenlogische Formeln die folgende Wahrheitstabelle, wobei somit $(A \Rightarrow B) \Leftrightarrow (B \vee \neg A)$ eine Tautologie ist.

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

Beispiel 2.2 (Kontradiktion). Für zwei Aussagen A und B ergibt sich für entsprechende aussagenlogische Formeln die folgende Wahrheitstabelle, wobei somit $(A \Rightarrow B) \Leftrightarrow (\neg B \wedge A)$ eine Kontradiktion ist.

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

2.3 Normalformen

Definition 2.2 (Negationsnormalform). Eine aussagenlogische Formel steht in *Negationsnormalform*, wenn die Negation (das \neg) nur direkt vor Aussagen oder vor Konstanten steht.

Beispiel: $\neg A \wedge \neg B$ steht in Negationsnormalform, während $\neg(A \vee B)$ nicht.

Beispiel 2.3. Zur Illustration der folgenden Definitionen und Herleitungen verwenden wir folgendes Beispiel: Sei die Aussage

$$A \Leftrightarrow (X \wedge \neg Y) \vee (\neg X \wedge (Y \vee \neg Z))$$

mit folgender Wahrheitstafel.

Beachte, dass man direkt aus der Wahrheitstafel ablesen kann, dass die Aussage A genau dann wahr ist, wenn: (X wahr, Y falsch und Z wahr ist) oder (X wahr, Y falsch und Z falsch ist) oder (X falsch, Y wahr und Z wahr

ist) oder (X falsch, Y wahr und Z falsch ist) oder (X falsch, Y falsch und Z falsch ist).

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

Definition 2.3 (Verallgemeinerte Konjunktion). Eine *verallgemeinerte Konjunktion* ist

- eine einzelne Aussage oder seine Negation (also A oder $\neg A$) oder
- eine der logischen Konstanten T=wahr und F=falsch oder
- eine Konjunktion $A \wedge B$, falls A und B selbst verallgemeinerte Konjunktionen sind.

Definition 2.4 (Disjunktive Normalform). Die Aussage A liegt in *disjunktiver Normalform* vor, wenn sie eine verallgemeinerte Konjunktion ist, oder wenn sie eine Disjunktion von verallgemeinerten Konjunktionen ist.

Beispiel 2.4 (Disjunktive Normalform). Die Aussage $A \Leftrightarrow (X \wedge \neg Y) \vee (\neg X \wedge (Y \vee \neg Z))$ schreibt sich in disjunktiver Normalform durch Kombination mittels Disjunktion (“oder”, \vee) der Zeilen der Wahrheitstafeln, welche wahr sind, wie folgt:

$$\begin{aligned} A \Leftrightarrow & (X \wedge \neg Y \wedge Z) \vee (X \wedge \neg Y \wedge \neg Z) \vee (\neg X \wedge Y \wedge Z) \\ & \vee (\neg X \wedge Y \wedge \neg Z) \vee (\neg Y \wedge \neg Y \wedge \neg Z) \end{aligned}$$

Definition 2.5 (Verallgemeinerte Disjunktion). Eine *verallgemeinerte Disjunktion* ist

- eine einzelne Aussage oder seine Negation (also A oder $\neg A$) oder
- eine der logischen Konstanten T=wahr und F=falsch oder
- eine Disjunktion $A \vee B$, falls A und B selbst verallgemeinerte Disjunktionen sind.

Definition 2.6 (Konjunktive Normalform). Die Aussage A liegt in *konjunktiver Normalform* vor, wenn sie eine verallgemeinerte Disjunktion ist, oder wenn sie eine Konjunktion von verallgemeinerten Disjunktionen ist.

Beispiel 2.5 (Konjunktive Normalform). Die konjunktive Normalform der Aussage $A \Leftrightarrow (X \wedge \neg Y) \vee (\neg X \wedge (Y \vee \neg Z))$ leitet sich wie folgt her: Erstens kombiniere man mittels Disjunktion (“oder”, \vee) die Zeilen der Wahrheitstafel, welche falsch sind (dann ist A falsch); zweitens negiere man diese aussagenlogische Formel (dann ist A wahr); drittens wende man den Satz von de Morgan (ggf. mehrmals) an, bis die entsprechende Form folgt:

$$\begin{aligned}\neg A &\Leftrightarrow (X \wedge Y \wedge Z) \vee (X \wedge Y \wedge \neg Z) \vee (\neg X \wedge \neg Y \wedge Z) \\ A &\Leftrightarrow \neg((X \wedge Y \wedge Z) \vee (X \wedge Y \wedge \neg Z) \vee (\neg X \wedge \neg Y \wedge Z)) \\ A &\Leftrightarrow \neg(X \wedge Y \wedge Z) \wedge \neg(X \wedge Y \wedge \neg Z) \wedge \neg(\neg X \wedge \neg Y \wedge Z) \\ A &\Leftrightarrow (\neg X \vee \neg Y \vee \neg Z) \wedge (\neg X \vee \neg Y \vee Z) \wedge (X \vee Y \vee \neg Z)\end{aligned}$$

2.4 Karnaugh-Veitch-Diagramme

Aussagenlogische Formeln können auch mit den sog. Karnaugh-Veitch-Diagrammen vereinfacht werden. Aus der Wahrheitstafel wird zuerst eine disjunktive oder eine konjunktive Normalform abgeleitet und in das Karnaugh-Veitch-Diagramm eingetragen. Im Diagramm werden die einzelnen Aussagen zu Blöcken zusammengefasst, die mit einfacheren Aussagen charakterisiert werden können. Dies kann zum Beispiel mit der Minterm-Methode erfolgen.

Das Vorgehen wird anhand des folgenden Beispiels mit den $n = 3$ Aussagen A, B, C illustriert.

Beispiel 2.6 (Karnaugh-Veitch-Diagramm). Die Aussage G ist als Kombination der Aussagen A, B, C gegeben durch die folgende Wahrheitstafel:

A	B	C	G
w	w	w	w
w	w	f	f
w	f	w	w
w	f	f	f
f	w	w	w
f	w	f	f
f	f	w	w
f	f	f	w

Die disjunktive Normalform von G ergibt sich somit als

$$\begin{aligned}G &\Leftrightarrow (A \wedge B \wedge C) \vee (A \wedge \neg B \wedge C) \vee (\neg A \wedge B \wedge C) \\ &\quad \vee (\neg A \wedge \neg B \wedge C) \vee (\neg A \wedge \neg B \wedge \neg C).\end{aligned}$$

Die Erstellung des Karnaugh-Veitch-Diagrammes und eine Vereinfachung der aussagenlogischen Formel von G erfolgt nun wie folgt.

1. Ein Diagramm mit 2^n Zellen erzeugen und beschriften, wobei die Randbeschriftungen so gewählt werden müssen, dass 2 benachbarte Zellen sich genau in einer Aussage unterscheiden. Hier für $n = 3$:

	B	B	$\neg B$	$\neg B$
A				
$\neg A$				

	C	$\neg C$	$\neg C$	C
A				
$\neg A$				

2. Aus der Wahrheitstabelle die Wahrheitswerte ablesen und in das Diagramm eintragen. Eine disjunktive Normalform kann an der Wahrheitstabelle abgelesen werden und direkt in das Karnaugh-Veitch-Diagramm eingetragen werden. Am einfachsten trägt man zuerst die Wahrheitswerte ein, die am wenigsten häufig auftreten, hier also die Falsch-Werte.

	B	B	$\neg B$	$\neg B$
A		f	f	
$\neg A$		f		

	C	$\neg C$	$\neg C$	C
A				
$\neg A$				

	B	B	$\neg B$	$\neg B$
A	w	f	f	w
$\neg A$	w	f	w	w

	C	$\neg C$	$\neg C$	C
A				
$\neg A$				

3. Es folgt nun die Blockbildung nach folgendem Schema: Alle benachbarten w-Felder zu horizontalen oder vertikalen Blöcken zusammenfassen, die die Grösse einer 2er-Potenz besitzen. Hierbei gelten Zellen auch über den Rand als benachbart.

Bei der Minterm-Methode müssen alle w-Zellen durch solche Blöcke überdeckt werden, ohne dass eine f-Zelle überdeckt wird. Es können w-Zellen mehrfach überdeckt werden.

	B	B	$\neg B$	$\neg B$
A	w	f	f	w
$\neg A$	w	f	w	w
	C	$\neg C$	$\neg C$	C

In dem Beispiel können wir den 4er-Block C (blau) und den 2er-Block $\neg A \wedge \neg B$ (rot) nehmen und erhalten bei der Vereinfachung mit dem Karnaugh-Veitch-Diagramm als Ergebnis:

$$G \Leftrightarrow (\neg A \wedge \neg B) \vee C.$$

2.5 Prädikatenlogik

Definition 2.7 (Aussageform). Aussagen, deren Wahrheitswert von einer oder mehreren Variablen abhängt, heißen *Aussageformen*. Aussagen und Aussageformen bestehen aus dem *Subjekt* (ein konkretes Objekt oder ein Platzhalter) und dem *Prädikat* (einer Eigenschaft).

Beispiel 2.7 (Aussageform). $P(n)$: „ n ist eine Primzahl“. Man sagt: $P(n)$ ist ein Prädikat für (das Subjekt) $n \in \mathbb{N}$. Es ist ein einstelliges Prädikat.

Quantoren

Sei R eine Aussageform, d.h. $R(x)$ ein Prädikat für $x \in W$ für eine gegebene Menge W . Für alle: $\forall x \in W : R(x) \Leftrightarrow \neg \exists x \in W : \neg R(x)$
Es existiert: $\exists x \in W : \neg R(x) \Leftrightarrow \neg \forall x \in W : R(x)$

3 Beweistechniken

3.1 Direkter und indirekter Beweis sowie Widerspruchsbeweis

Zu zeigen: $A \Rightarrow B$.

Direkter Beweis: Ausgehend von A zeige direkt, dass B , z.B. mittels Äquivalenzumformungen.

Indirekter Beweis: Zeige, dass $\neg B \Rightarrow \neg A$. D.h. Ausgehend von $\neg B$ zeige, dass $\neg A$, z.B. mittels Äquivalenzumformungen.

Widerspruchsbeweis: Zeige, dass $A \wedge \neg B \Rightarrow F$ (falsch, false), d.h. zeige, dass A zusammen mit $\neg B$ nicht sein kann.

3.2 Vollständige Induktion

Behauptung/Aussage: $\forall n \in \mathbb{N}, n \geq n_0 : S(n)$, d.h. $S(n)$ gilt für alle $n \in \mathbb{N}$ mit $n \geq n_0$

1. Verankerung: $S(n_0)$, d.h. $S(n)$ gilt für den ersten Wert $n = n_0$, z.B. für $n = 0$ oder $n = 1$

2. Induktionsschritt: Es gilt zu zeigen, dass $S(k) \Rightarrow S(k+1)$, d.h. wenn $S(k)$ gilt, dann gilt auch $S(k+1)$

a) **Induktionsannahme:** $S(k)$, d.h. $S(k)$ sei richtig für k

b) **Induktionsbehauptung:** $S(k+1)$, d.h. $S(k+1)$ ist richtig

c) **Induktionsbeweis:** Verwenden von $S(k)$, um die Richtigkeit von $S(k+1)$ zu zeigen. Wähle hierzu je nach Situation einen direkten, indirekten oder Widerspruchs-Beweis.

4 Folgen und Reihen

Definition 4.1 (Folgen und Reihen). Eine *Folge* ist eine nummerierte Liste von Objekten (Folgegliedern, z.B. Zahlen). Eine *Reihe* ist die Summe von Folgegliedern einer Zahlenfolge.

Eine endliche bzw. unendliche Folge lässt sich schreiben als

$$(a_k)_{k=0 \dots n} = (a_0, a_1, a_2, \dots, a_n), \\ (a_k)_{k \in \mathbb{N}} = (a_0, a_1, a_2, \dots)$$

und die entsprechenden Reihen als:

$$\sum_{k=0}^n a_k = a_0 + a_1 + a_2 + \dots + a_n, \\ \sum_{k=0}^{\infty} a_k = a_0 + a_1 + a_2 + \dots$$

Beispiel 4.1 (Folgen und Reihen).

$$\sum_{k=1}^n k = 1 + 2 + \dots + (n-1) + n = \frac{n(n+1)}{2}, \\ \sum_{k=1}^{\infty} \frac{(-1)^{(k-1)}}{k} = 1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \dots = \ln(2).$$

Definition 4.2 (Direkte und rekursive Berechnungsformeln für Folgen). Eine Folge kann sowohl *direkt* wie auch *rekursiv* definiert werden. Die direkte Definition erfolgt über eine Funktion in Abhängigkeit des Index k für jedes Folgenglied

$$a_k = f(k), \forall k = 0, 1, 2, \dots, n \text{ (oder ggf. } \forall k \in \mathbb{N}),$$

während die rekursive Definition das (oder die) erste(n) Folgenglieder definiert und eine Funktion, wie man rekursiv zu den nächsten kommt, z.B. ist die Folge

$$\begin{aligned} a_0 &= 1, \\ a_1 &= 1, \\ a_k &= f(a_{k-2}, a_{k-1}) = a_{k-2} + a_{k-1}, \forall k \in \mathbb{N}, k > 1 \end{aligned}$$

die Fibonacci-Folge.

5 Mengen

5.1 Definitionen und Allgemeines

Definition 5.1 (Menge (Cantor)). Eine Menge M ist eine Zusammenfassung von bestimmten, wohl unterschiedenen Objekten zu einem Ganzen. Mengen können in *aufzählender Form*, z.B. $M_1 = \{1, 3, 5\}$, $M_2 = \{1, 4, 9, 16, 25, 36, \dots\}$ oder in *beschreibender Form*, z.B. $M_2 = \{x \in \mathbb{R} \mid x^2 = 1\}$, $M_3 = \{x \in G \mid E(x)\}$, wobei G die Grundmenge und E (eine) Eigenschaft(en) sind, notiert werden.

Definition 5.2 (Mächtigkeit). Die Mächtigkeit $|M|$ einer Menge M ist die Anzahl ihrer Elemente.

Beispiel 5.1 (Mächtigkeit einer Menge).

$$\begin{aligned} M &= \{a, b, c\}, \quad |M| = 3 \\ |\emptyset| &= 0 \end{aligned}$$

Definition 5.3 (Potenzmenge). Sei M eine Menge. Die Menge aller Teilmengen von M heisst *Potenzmenge* $P(M)$.

Beispiel 5.2 (Potenzmenge). $M = \{a, b, c\}$ hat die Teilmengen $\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}$. Somit:

$$P(M) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$$

Satz 5.1. Sei M eine Menge mit $|M| = n$. Die Potenzmenge enthält $|P(M)| = 2^{|M|} = 2^n$ Elemente.

5.2 Mengenoperationen

Vereinigung:	$A \cup B$	$= \{x \mid x \in A \vee x \in B\}$
Schnittmenge:	$A \cap B$	$= \{x \mid x \in A \wedge x \in B\}$
Differenz:	$A \setminus B$	$= \{x \mid x \in A \wedge x \notin B\}$
Symmetrische Differenz:	$A \Delta B$	$= \{x \mid (x \in A \cup B) \wedge (x \notin A \cap B)\}$
Komplement:	\bar{A}	$= \{x \mid x \notin A\}$ (Differenz bez. Grundmenge G)

Regeln für Mengenoperationen

Kommutativität:	$A \cap B$	$\Leftrightarrow B \cap A$
	$A \cup B$	$\Leftrightarrow B \cup A$
Assoziativität:	$(A \cap B) \cap C$	$\Leftrightarrow A \cap (B \cap C)$
	$(A \cup B) \cup C$	$\Leftrightarrow A \cup (B \cup C)$
Distributivität:	$A \cap (B \cup C)$	$\Leftrightarrow (A \cap B) \cup (A \cap C)$
	$A \cup (B \cap C)$	$\Leftrightarrow (A \cup B) \cap (A \cup C)$
Idempotenzgesetz:	$A \cup A$	$= A$
	$A \cap A$	$= A$
Verschmelzungsgesetz:	$A \cup (A \cap B)$	$= A$
	$A \cap (A \cup B)$	$= A$
Inklusion:	$A \subset B \Leftrightarrow (A \cap B) = A \Leftrightarrow (A \cup B) = B$	

Weitere Regeln:

$$\begin{aligned} \bar{\bar{A}} &= A \\ A \cap \bar{A} &= \emptyset \\ A \cup \bar{A} &= G, \text{ mit der Grundmenge } G \\ \overline{A \cap B} &= \bar{A} \cup \bar{B} \\ \overline{A \cup B} &= \bar{A} \cap \bar{B} \end{aligned}$$

5.3 Kartesisches Produkt

$A \times B$	$= \{(a, b) \mid a \in A \wedge b \in B\}$
$A_1 \times A_2 \times \dots \times A_n$	$= \prod_{i=1}^n A_i = \{(a_1, a_2, \dots, a_n) \mid a_i \in A_i, \forall i = 1, 2, \dots, n\}$
A^k	$= \underbrace{A \times A \times A \times \dots \times A}_{k \text{ Faktoren}}$

6 Relationen und Abbildungen

6.1 Relationen

Definition 6.1 (Relation). Eine *Relation* ist eine Teilmenge des kartesischen Produktes: $R \subset A_1 \times A_2 \times \cdots \times A_n = \prod_{i=1}^n A_i$

Definition 6.2 (reflexiv, symmetrisch, antisymmetrisch, transitiv). Eine Relation $R \subset A \times A$ ist:

- *reflexiv*, wenn $\forall a \in A : (a, a) \in R$,
- *symmetrisch*, wenn $\forall a, b \in A : (a, b) \in R \Rightarrow (b, a) \in R$,
- *antisymmetrisch*, wenn $\forall a, b \in A : ((a, b) \in R) \wedge ((b, a) \in R) \Rightarrow a = b$ bzw. $((a, b) \in R \wedge (a \neq b)) \Rightarrow (b, a) \notin R$,
- *transitiv*, wenn $\forall a, b, c \in A : (a, b) \in R \wedge (b, c) \in R \Rightarrow (a, c) \in R$.

Definition 6.3 (Äquivalenzrelation). Eine reflexive, symmetrische und transitive Relation heisst *Äquivalenzrelation*.

Definition 6.4 (Ordnungsrelation). Eine reflexive, antisymmetrische und transitive Relation heisst *Ordnungsrelation*.

6.2 Abbildungen

Definition 6.5 (Abbildung, Funktion). Eine *Abbildung* oder *Funktion* ist eine Zuordnung, die jedem Element einer *Definitionsmenge* D genau ein Element einer *Zielmenge* Z zuordnet. Ist f eine Abbildung mit Definitionsmenge D und Zielmenge Z , so schreibt man

$$\begin{aligned} f : D &\rightarrow Z \\ x &\mapsto z = f(x) \end{aligned}$$

Die Elemente von D heissen *Argumente*, die Elemente von Z heissen *Werte*. Die Wertemenge bzw. der *Wertebereich* W ist

$$W = \{z \in Z \mid \exists d \in D : f(d) = z\}.$$

Eine Abbildung $f : D \rightarrow Z$ kann als Relation $R \subset D \times Z$ verstanden werden, wobei es für jedes Element in D ein Element in Z gibt, welches in der Relation ist: $\forall d \in D \exists z \in Z : (d, z) \in R$. Das Element z ist namentlich $z = f(d)$.

Definition 6.6 (injektiv, surjektiv, bijektiv). Sei $f : D \rightarrow Z$ eine Abbildung von D nach Z . Dann ist f

- *injektiv*, wenn $\forall d_1, d_2 \in D : d_1 \neq d_2 \Rightarrow f(d_1) \neq f(d_2)$, d.h., zwei unterschiedliche Argumente werden stets auf unterschiedliche Werte abgebildet,
Beispiel: $f : \mathbb{N} \rightarrow \mathbb{N}, n \mapsto 2n$,
Gegenbeispiel: $f : \mathbb{R} \rightarrow \mathbb{R}, x \mapsto x^2$,
- *surjektiv*, wenn $\forall z \in Z \exists d \in D : f(d) = z$, d.h. jeder Zielwert wird durch mindestens ein Bild erreicht,
- *bijektiv* (umkehrbar), wenn injektiv und surjektiv.

6.3 Mächtigkeit von Mengen

Definition 6.7 (gleichmächtig, abzählbar). Zwei Mengen A und B heissen *gleichmächtig*, wenn es eine bijektive Abbildung von A nach B gibt.
Die Mächtigkeit von \mathbb{N} heisst *abzählbar unendlich*.

Satz 6.1 (gem. Cantor). Folgende Aussagen gelten:

- \mathbb{Z} ist abzählbar unendlich, d.h. die Mengen \mathbb{N} und \mathbb{Z} sind gleichmächtig,
- \mathbb{Q} ist abzählbar unendlich, d.h., die Mengen \mathbb{N} und \mathbb{Q} sind gleichmächtig,
- \mathbb{R} ist überabzählbar, d.h., es gibt keine bijektive Abbildung $\mathbb{N} \rightarrow \mathbb{R}$,
- Das Intervall $(0; 1)$ ist gleichmächtig wie \mathbb{R} .

7 Modulo-Rechnen

7.1 Definitionen und Allgemeines

Definition 7.1 (Teiler-Relation). Seien $a, b \in \mathbb{Z}$. Wir sagen, dass "b ein Teiler von a" ist (b teilt a) und schreiben $b \mid a$, wenn $\exists q \in \mathbb{Z} : b \cdot q = a$. Wir nennen sie auch die *Teiler-Relation* $T(b, a)$ auf $\mathbb{Z} \times \mathbb{Z}$. Es gilt also:

$$T(b, a) \Leftrightarrow b \mid a \Leftrightarrow \exists q \in \mathbb{Z} : b \cdot q = a.$$

Die Teiler-Relation ist eine Ordnungsrelation.

Definition 7.2 (Modulo-Relation). Seien $a, q, r \in \mathbb{Z}$. Die Relation

$$R_q(a, r) \Leftrightarrow q \mid a - r$$

heisst die *Modulo-Relation* und wir schreiben $a \equiv r \pmod{q}$ und sagen "a ist kongruent r modulo q".

Die Modulo-Relation ist eine Äquivalenzrelation.

Definition 7.3 (Restklassen). Die Modulo-Relation teilt, für ein gegebenes $q \in \mathbb{Z}$, die ganzen Zahlen \mathbb{Z} in q Äquivalenzklassen, sogenannte *Restklassen*, auf:

$$\mathbb{Z}_q = \{[0]_q, [1]_q, [2]_q, \dots, [q-1]_q\},$$

wobei

$$[r]_q = \{z \in \mathbb{Z} \mid z \equiv r \pmod{q}\}, \quad r = 0, 1, 2, \dots, q-1$$

Wir schreiben einfacher: $\mathbb{Z}_q = \{0, 1, 2, \dots, q-1\}$

Definition 7.4 (ggT, kgV). Seien zwei Zahlen $a, b \in \mathbb{Z}$. Der *grösste gemeinsame Teiler* $\text{ggT}(a, b)$ und das *kleinste gemeinsame Vielfache* $\text{kgV}(a, b)$ von a und b sind definiert als:

$$\begin{aligned} \text{ggT}(a, b) &= \max\{d \in \mathbb{N} \mid d \mid a \wedge d \mid b\}, \\ \text{kgV}(a, b) &= \min\{m \in \mathbb{N} \mid a \mid m \wedge b \mid m\}. \end{aligned}$$

Zudem gilt:

$$\text{kgV}(a, b) = \frac{a \cdot b}{\text{ggT}(a, b)}.$$

7.2 Rechenregeln in Restklassen

Satz 7.1 (Addition und Multiplikation). Wenn $a \equiv r_a \pmod{q}$ und $b \equiv r_b \pmod{q}$ dann ist

$$\begin{aligned} a + b &\equiv r_a + r_b \pmod{q}, \\ a \cdot b &\equiv r_a \cdot r_b \pmod{q}. \end{aligned}$$

Satz 7.2 (Kleiner Fermat). Sei $p \in \mathbb{N}$ eine Primzahl und $z \in \mathbb{Z} \setminus \{0\}$, so dass $\text{ggT}(z, p) = 1$. Dann gilt:

$$z^{p-1} \equiv 1 \pmod{p}.$$

Definition 7.5 (Multiplikatives Inverses). Seien $q \in \mathbb{N} \setminus \{0\}$ und $m \in \mathbb{N} \setminus \{0\}$. Dann heisst eine Zahl $n \in \mathbb{Z}$ mit $m \cdot n \equiv 1 \pmod{q}$ ein *multiplikatives Inverses* von m Modulo q . Man schreibt auch $n = m^{-1}$. Es gilt zudem:

Es gibt ein multiplikatives Inverses von m Modulo $q \Leftrightarrow \text{ggT}(q, m) = 1$.

Definition 7.6 (Eulersche φ -Funktion). Die Eulersche φ -Funktion auch *Totient* genannt, ist definiert als $\varphi(n) = \text{Anzahl Zahlen } m \in \mathbb{N} \text{ mit } 1 \leq m \leq n \text{ und } \text{ggT}(n, m) = 1$. Es gelten zudem folgende Beziehungen:

- (i) Sei $p \in \mathbb{N}$ eine Primzahl. Dann ist $\varphi(p) = p - 1$.
- (ii) Sei $p \in \mathbb{N}$ eine Primzahl und $n \in \mathbb{N} \setminus \{0\}$. Dann ist $\varphi(p^n) = p^{n-1}(p - 1)$.
- (iii) Seien $m, n \in \mathbb{N} \setminus \{0\}$ und $\text{ggT}(n, m) = 1$. Dann ist $\varphi(nm) = \varphi(n)\varphi(m)$.
- (iv) Wenn $\mathbb{Z}_n^* = \{z \in \mathbb{Z}_n \mid z \text{ hat ein multiplikatives Inverses in } \mathbb{Z}_n\}$, dann gilt

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

Satz 7.3 (Euler). Seien $n \in \mathbb{N} \setminus \{0\}$ und $z \in \mathbb{Z}$ mit $\text{ggT}(z, n) = 1$. Dann ist

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

7.3 Erweiterter Euklidscher Algorithmus

Gegeben sind $a, b \in \mathbb{N}$. Der Euklidsche Algorithmus berechnet den $\text{ggT}(a, b)$ und der erweiterte Euklidsche Algorithmus liefert zusätzlich zwei ganze Zahlen $s, t \in \mathbb{Z}$, so dass $\text{ggT}(a, b) = s \cdot a + t \cdot b$.

Wenn $\text{ggT}(a, b) = 1$, lässt sich so das multiplikative Inverse von $a \pmod{b}$ oder von $b \pmod{a}$ berechnen, denn es gilt dann $s \cdot a \equiv 1 \pmod{b}$ und $t \cdot b \equiv 1 \pmod{a}$ und somit ist z.B. s das multiplikative Inverse von $a \pmod{b}$.

Algorithmus 7.1 (erweiterter Euklidscher Algorithmus). Gegeben seien $a, b \in \mathbb{N}$.

Initialisierung: Setze $k = 0, x_0 = a, y_0 = b$ sowie $(u_0, s_0, v_0, t_0) = (1, 0, 0, 1)$.

Iteration: Verwende den ganzzahligen Quotienten q_k mit Rest r_k der Division von x_k durch y_k , um die Folgen x_k, y_k, q_k, r_k sowie u_k, s_k, v_k, t_k von natürlichen Zahlen wie folgt zu konstruieren:

Repetiere bis $r_k = 0$:

$$\begin{aligned}
 q_k &= x_k \text{ div } y_k \quad (\text{ganzzahlige Division}), \\
 r_k &= x_k \text{ mod } y_k = x_k - q_k \cdot y_k, \\
 x_{k+1} &= y_k, \\
 y_{k+1} &= r_k, \\
 u_{k+1} &= s_k, \\
 s_{k+1} &= u_k - q_k \cdot s_k, \\
 v_{k+1} &= t_k, \\
 t_{k+1} &= v_k - q_k \cdot t_k, \\
 k &= k + 1.
 \end{aligned}$$

Resultat: Wenn $r_k = 0$, dann gilt:

$$\begin{aligned}
 \text{ggT}(a, b) &= y_k \\
 \text{ggT}(a, b) &= s_k \cdot a + t_k \cdot b.
 \end{aligned}$$

Anmerkung: Das zweite Resultat gilt so, wenn bei der Initialisierung $x_0 \geq y_0$ gewählt wurde. Ansonsten tauschen sich die Rollen von s_k und t_k .

Wenn $\text{ggT}(a, b) = 1$ ist $s_k \cdot a \equiv 1 \pmod{b}$, d.h. s_k ist das multiplikative Inverse von a Modulo b und $t_k \cdot b \equiv 1 \pmod{a}$, d.h. t_k ist das multiplikative Inverse von b Modulo a .

Zur Umsetzung eignet sich die folgende Tabellenform:

	x	y	$q = x \text{ div } y$	$r = x \text{ mod } y$	
Init	a	b	$a \text{ div } b$	$a \text{ mod } b$	
...					
k	x_k	y_k	$q_k = x_k \text{ div } y_k$	$r_k = x_k \text{ mod } y_k$	
$k+1$	$x_{k+1} = y_k$	$y_{k+1} = r_k$	
...					...
Result	...	$\text{ggT}(a, b)$...	0	

	u	s	v	t
1	0	0	0	1
...				
u_k	s_k	v_k	t_k	
$u_{k+1} = s_k$	$s_{k+1} = u_k - q_k s_k$	$v_{k+1} = t_k$	$t_{k+1} = v_k - q_k t_k$	
...	s	...	t	

7.4 RSA Verschlüsselung

Die RSA-Verschlüsselung (nach Rivest, Shamir und Adleman) ist ein Public-Key Verfahren, bei welchem Botschaften mit einem öffentlichen Schlüssel verschlüsselt werden, die aber nur mit dem privaten Schlüssel (effizient) entschlüsselt werden können.

Algorithmus 7.2 (RSA Verschlüsselung). Das RSA-Verfahren kann wie folgt implementiert werden.

- (i) Wähle zwei Primzahlen $p, q \in \mathbb{N}$, zum Beispiel $p = 3, q = 11$, und berechne das Produkt $n = pq$.
- (ii) Berechne $\varphi(n) = \varphi(p)\varphi(q) = (p-1)(q-1)$, hier im Beispiel $\varphi(n) = 20$.
- (iii) Wähle eine Zahl $a, 0 \leq a < \varphi(n)$ mit $\text{ggT}(a, \varphi(n)) = 1$, zum Beispiel $a = 3$.
- (iv) Berechne das multiplikative Inverse von a in $\mathbb{Z}_{\varphi(n)}$, d.h. bestimme $b, 0 < b < \varphi(n)$ mit $a \cdot b \equiv 1 \pmod{\varphi(n)}$, hier im Beispiel $3 \cdot b \equiv 1 \pmod{20} \Rightarrow b = 7$.
- (v) Veröffentliche den öffentlichen Schlüssel $n = 33, b = 7$ und behalte den privaten Schlüssel $n = 33, a = 3$ geheim.
- (vi) Vereinbare eine Buchstaben-Tabelle, um Buchstaben eindeutig einer Zahl zuzuordnen.

Eine Nachricht verschlüsselt sich nun, indem für jeden Buchstaben einer Nachricht die zugehörige Zahl c zu $\tilde{c} = c^b \pmod{n}$ verschlüsselt wird. Zum Beispiel mit $c = 13$ folgt $\tilde{c} = 13^7 \pmod{33} \equiv 7$. Die Nachricht bzw. die Zahl \tilde{c} kann dann entschlüsselt werden mit $c = \tilde{c}^a \pmod{n}$. Im Beispiel $7^3 \pmod{33} \equiv 13$.

Die Schwierigkeit, einen Code zu knacken, besteht darin, die Zahl n in die zwei (in der Anwendung sehr grossen) Primzahlen zu zerlegen, um $\varphi(n)$ berechnen zu können. Wenn $\varphi(n)$ bekannt ist, kann zu einem öffentlichen Schlüssel n, b der private Schlüssel n, a schnell berechnet werden, indem a als das multiplikative Inverse zu b in $\mathbb{Z}_{\varphi(n)}$ berechnet wird, d.h. $a \cdot b \equiv 1 \pmod{\varphi(n)}$.

8 Lineare Algebra

8.1 Lineare Gleichungssysteme

Definition 8.1 (Lineares Gleichungssystem). Ein *lineares Gleichungssystem* mit m Gleichungen und n Unbekannten über einem Skalarkörper, hier \mathbb{R} , schreibt sich als

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n &= b_1 \\ a_{21}x_1 + a_{22}x_2 + \dots + a_{2n}x_n &= b_2 \\ \vdots &\quad \vdots & \vdots & \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n &= b_m \end{aligned}$$

mit $a_{i,j}, b_i \in \mathbb{R}, i = 1, 2, \dots, m, j = 1, 2, \dots, n$, und in Matrixschreibweise als $A\vec{x} = \vec{b}$ mit

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix} \in \mathbb{R}^{m \times n}, \vec{x} = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} \in \mathbb{R}^n, \vec{b} = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{bmatrix} \in \mathbb{R}^m.$$

Ein lineares Gleichungssystem heisst *homogen*, wenn $\vec{b} = \vec{0}$ und *inhomogen* sonst.

Algorithmus 8.1 (Gauss und Gauss-Jordan Algorithmus). Ein lineares Gleichungssystem löst sich mit dem Gauss oder dem *Gauss-Jordan Algorithmus*. Sei ein lineares Gleichungssystem mit m Gleichungen und n Unbekannten:

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n &= b_1 \\ a_{21}x_1 + a_{22}x_2 + \dots + a_{2n}x_n &= b_2 \\ \vdots &\quad \vdots & \vdots & \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n &= b_m \end{aligned}$$

Wir konstruieren nun die erweiterte Koeffizientenmatrix (d.h. die Tableau-Form des Gleichungssystems) $[A|\vec{b}]$ wie folgt:

$$\begin{array}{cccc|c} x_1 & x_2 & \cdots & x_n & 1 \\ \hline a_{11} & a_{12} & \cdots & a_{1n} & b_1 \\ a_{21} & a_{22} & \cdots & a_{2n} & b_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} & b_m \end{array}$$

Das Ziel ist nun, mittels elementarer Zeilenumformungen das System in die Zeilenstufenform (Gauss Algorithmus) oder die reduzierte Zeilenstufenform (Gauss-Jordan Algorithmus) zu bringen. D.h.

1. Jeder führende Eintrag einer Zeile (das erste nicht-Null Element von links) ist 1, die sogenannte *führende Eins*,
2. In jeder Spalte sind unterhalb jeder führenden Eins alle Elemente gleich Null (Zeilenstufenform),
3. Die führende Eins ist das einzige Element ungleich Null in seiner Spalte, d.h. oberhalb und unterhalb sind alle Elemente gleich Null (reduzierte Zeilenstufenform).

Elementare Zeilenumformungen beinhalten:

- Vertauschen von Zeilen,
- Multiplikation einer Zeile mit einem Skalar $\lambda \in \mathbb{R} \setminus \{0\}$,
- Addition (eines vielfachen) einer Zeile zu einer anderen.

Es gibt auch die Möglichkeit, Spalten zu tauschen; dann muss man sich den Spaltentausch aber merken bzw. verfolgen, welche Spalte zu welcher Variablen gehört.

Der Gauss-Algorithmus stoppt bei der Zeilenstufenform und löst das Gleichungssystem danach von unten nach oben durch Rückwärtseinsetzen.

Beim Gauss-Jordan Algorithmus werden die Lösungen direkt aus der reduzierten Zeilenstufenform abgelesen.

Beispiel 8.1 (Gauss-Jordan Algorithmus). Sei das folgende lineare Gleichungssystem:

$$2x + 4y - 2z = 2$$

$$4x + 4y - 12z = 16$$

$$2x + 5y - 4z = 7$$

mit der erweiterten Koeffizientenmatrix

$$\begin{array}{ccc|c} x & y & z & 1 \\ \hline 2 & 4 & -2 & 2 \\ 4 & 4 & -12 & 16 \\ 2 & 5 & -4 & 7 \end{array}$$

Schritt 1: Teilen wir die erste Zeile durch 2, um den führenden Eintrag zu 1 zu machen.

$$\begin{array}{ccc|c} x & y & z & 1 \\ \hline 1 & 2 & -1 & 1 \\ 4 & 4 & -12 & 16 \\ 2 & 5 & -4 & 7 \end{array}$$

Schritt 2: Subtrahieren wir 4-mal die erste Zeile von der zweiten Zeile und 2-mal die erste Zeile von der dritten Zeile.

$$\begin{array}{ccc|c} x & y & z & 1 \\ \hline 1 & 2 & -1 & 1 \\ 0 & -4 & -8 & 12 \\ 0 & 1 & -2 & 5 \end{array}$$

Schritt 3: Teilen wir die zweite Zeile durch -4 , um den führenden Eintrag auf 1 zu bringen.

$$\begin{array}{ccc|c} x & y & z & 1 \\ \hline 1 & 2 & -1 & 1 \\ 0 & 1 & 2 & -3 \\ 0 & 1 & -2 & 5 \end{array}$$

Schritt 4: Subtrahieren wir das 1-fache der zweiten Zeile von der dritten Zeile.

$$\begin{array}{ccc|c} x & y & z & 1 \\ \hline 1 & 2 & -1 & 1 \\ 0 & 1 & 2 & -3 \\ 0 & 0 & -4 & 8 \end{array}$$

Schritt 5: Teilen wir die dritte Zeile durch -4 , um den führenden Eintrag auf 1 zu bringen.

$$\begin{array}{ccc|c} x & y & z & 1 \\ \hline 1 & 2 & -1 & 1 \\ 0 & 1 & 2 & -3 \\ 0 & 0 & 1 & -2 \end{array}$$

Die Zeilenstufenform ist erreicht. Für den *Gauss-Algorithmus* liest sich nun die Lösung $z = -2$ aus der letzten Zeile ab. Durch Rückwärtseinsetzen von z in die zweite Zeile und Verschieben dieses Eintrages auf die rechte Seite ergibt sich dann $y = -3 - 2z = 1$. Schliesslich folgt mit ähnlicher Prozedur in der ersten Zeile $x = 1 - 2y + z = -3$.

Der *Gauss-Jordan Algorithmus* geht wie folgt weiter:

Schritt 6: Subtrahieren wir 2-mal die dritte Zeile von der zweiten Zeile und addieren wir 1-mal die dritte Zeile zur ersten.

$$\begin{array}{ccc|c} x & y & z & 1 \\ \hline 1 & 2 & 0 & -1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & -2 \end{array}$$

Schritt 7: Subtrahieren wir 2-mal die zweite Zeile von der ersten Zeile.

$$\begin{array}{ccc|c} x & y & z & 1 \\ \hline 1 & 0 & 0 & -3 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & -2 \end{array}$$

Die Lösung des Systems liest sich nun direkt aus dem Schlusstableau ab: $x = -3, y = 1$ und $z = -2$.

Satz 8.1 (Lösungstrichotomie). Ein lineares Gleichungssystem hat entweder keine, eine oder unendlich viele Lösungen. Wenn es unendlich viele Lösungen gibt, gibt es (mind. eine) freie Variable(n).

Das Schlusstableau am Ende des Gauss-Jordan Algorithmus zeigt uns, in welchem Fall wir sind: Gibt es Zeilen, wo die linke Seite Null ist und die rechte Seite ungleich Null, gibt es keine Lösung, gibt es hingegen Nullzeilen (linke und rechte Seite = 0), so gibt es unendlich viele Lösungen. In den anderen Fällen gibt es genau eine Lösung.

Definition 8.2 (reguläres Gleichungssystem). Ein lineares Gleichungssystem heisst *regulär*, wenn es genau eine Lösung hat.

Definition 8.3 (Rang). Der *Rang* eines linearen Gleichungssystems ist gleich der Anzahl bestimmter Variablen des Gleichungssystems. Dies ist gleich der Anzahl führender Einsen im Schlusstableau des Gauss-Jordan Algorithmus.

8.2 Matrizen und Vektoren

Seien $\vec{u}, \vec{v} \in \mathbb{R}^n$ zwei Vektoren mit Dimension n . Wir schreiben:

$$\vec{u} = \begin{bmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{bmatrix} = [u_i]_{i=1,2,\dots,n} \in \mathbb{R}^n, \quad \vec{v} = \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix} = [v_i]_{i=1,2,\dots,n} \in \mathbb{R}^n.$$

Definition 8.4 (Norm). Die *Norm* eines Vektors \vec{v} , auch Länge oder Betrag genannt, ist definiert als

$$|\vec{v}| = \sqrt{\sum_{i=1}^n v_i^2}$$

Definition 8.5 (Skalarprodukt). Das *Skalarprodukt* der Vektoren \vec{u}, \vec{v} ist definiert als

$$\begin{aligned} \vec{u} \bullet \vec{v} &= \sum_{i=1}^n u_i v_i \\ &= |\vec{u}| \cdot |\vec{v}| \cdot \cos(\phi), \end{aligned}$$

wobei ϕ der Winkel zwischen \vec{u} und \vec{v} ist.

Definition 8.6 (Kreuzprodukt). Das *Kreuzprodukt* zweier Vektoren $\vec{u}, \vec{v} \in \mathbb{R}^3$ ist definiert, so dass $\vec{w} = \vec{u} \times \vec{v} \in \mathbb{R}^3$ die folgenden drei Bedingungen erfüllt:

- \vec{w} steht senkrecht auf \vec{u} und \vec{v} ,
- Die Vektoren $\vec{u}, \vec{v}, \vec{w}$ bilden in dieser Reihenfolge ein Rechtssystem,
- Die Norm $|\vec{w}|$ entspricht der Fläche des von \vec{u} und \vec{v} aufgespannten Parallelogramms.

Das Kreuzprodukt lässt sich wie folgt berechnen:

$$\vec{w} = \vec{u} \times \vec{v} = \begin{bmatrix} u_1 \\ u_2 \\ u_3 \end{bmatrix} \times \begin{bmatrix} v_1 \\ v_2 \\ v_3 \end{bmatrix} = \begin{vmatrix} u_1 & v_1 & \vec{e}_1 \\ u_2 & v_2 & \vec{e}_2 \\ u_3 & v_3 & \vec{e}_3 \end{vmatrix} = \begin{bmatrix} u_2 v_3 - u_3 v_2 \\ u_3 v_1 - u_1 v_3 \\ u_1 v_2 - u_2 v_1 \end{bmatrix}.$$

Seien zudem $A \in \mathbb{R}^{m \times r}$ eine m mal r Matrix, d.h. eine Matrix mit m Zeilen und r Spalten und $B \in \mathbb{R}^{r \times n}$ eine r mal n Matrix. Wir schreiben:

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1r} \\ a_{21} & a_{22} & \cdots & a_{2r} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mr} \end{bmatrix} = [a_{ij}]_{\substack{i=1,2,\dots,m \\ j=1,2,\dots,r}} \in \mathbb{R}^{m \times r},$$

$$B = \begin{bmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{r1} & b_{r2} & \cdots & b_{rn} \end{bmatrix} = [b_{ij}]_{\substack{i=1,2,\dots,r \\ j=1,2,\dots,n}} \in \mathbb{R}^{r \times n}.$$

Definition 8.7 (Matrix Addition und Multiplikation mit einem Skalar). Matrizen werden addiert (oder subtrahiert), indem man sie elementweise addiert (oder subtrahiert). Eine Matrix wird mit einem Skalar $\lambda \in \mathbb{R}$ multipliziert, indem jedes Element mit λ multipliziert wird. Analoges gilt für Vektoren.

Definition 8.8 (Matrixprodukt). Das *Matrixprodukt* von A mit B ist definiert als

$$AB = \begin{bmatrix} a_{11} & \cdots & a_{1r} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mr} \end{bmatrix} \cdot \begin{bmatrix} b_{11} & \cdots & b_{1n} \\ \vdots & \ddots & \vdots \\ b_{r1} & \cdots & b_{rn} \end{bmatrix} = \begin{bmatrix} \sum_{k=1}^r a_{1k} b_{k1} & \cdots & \sum_{k=1}^r a_{1k} b_{kn} \\ \vdots & \ddots & \vdots \\ \sum_{k=1}^r a_{mk} b_{k1} & \cdots & \sum_{k=1}^r a_{mk} b_{kn} \end{bmatrix},$$

d.h., $C = AB \in \mathbb{R}^{m \times n}$ und das Element von $C = AB$ in Zeile i und Spalte j berechnet sich aus der i -ten Zeile von A und der j -ten Spalte von B als

$$c_{ij} = \sum_{k=1}^r a_{ik} b_{kj}, \quad i = 1, 2, \dots, m, j = 1, 2, \dots, n.$$

Als Spezialfall ist das Produkt einer Matrix $C \in \mathbb{R}^{m \times n}$ mit einem Vektor $u \in \mathbb{R}^n$ definiert als:

$$C \cdot \vec{u} = \begin{bmatrix} c_{11} & \cdots & c_{1n} \\ \vdots & \ddots & \vdots \\ c_{m1} & \cdots & c_{mn} \end{bmatrix} \cdot \begin{bmatrix} u_1 \\ \vdots \\ u_n \end{bmatrix} = \begin{bmatrix} \sum_{k=1}^n c_{1k} u_k \\ \vdots \\ \sum_{k=1}^n c_{mk} u_k \end{bmatrix}.$$

Definition 8.9 (Diagonal- und Einheitsmatrix). Eine *Diagonalmatrix* $D \in \mathbb{R}^{m \times n}$ ist eine Matrix, für welche alle Elemente außerhalb der Diagonalen Null sind. Die *Einheitsmatrix* $E \in \mathbb{R}^{n \times n}$ ist eine quadratische Diagonalmatrix mit Ordnung n und Diagonalelementen gleich Eins, d.h.

$$D = [d_{ij}] \text{ mit } \begin{cases} d_{ii} \in \mathbb{R}, \\ d_{ij} = 0, i \neq j. \end{cases} \quad E = [e_{ij}] \text{ mit } \begin{cases} e_{ii} = 1, \\ e_{ij} = 0, i \neq j. \end{cases}$$

Definition 8.10 (Reguläre Matrix). Eine quadratische Matrix $A \in \mathbb{R}^{n \times n}$ heisst *regulär*, wenn das Gleichungssystem $A\vec{x} = \vec{b}$ für jeden Vektor \vec{b} eine eindeutige Lösung hat. Ansonsten heisst die Matrix *singulär*.

Definition 8.11 (Inverse Matrix). Das *Inverse* einer regulären Matrix $A \in \mathbb{R}^{n \times n}$ ist diejenige Matrix A^{-1} , so dass

$$A^{-1}A = AA^{-1} = E.$$

Für $A \in \mathbb{R}^{2 \times 2}$ lässt es sich wie folgt berechnen:

$$A^{-1} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \frac{1}{ad - cb} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$$

Definition 8.12 (transponierte Matrix, symmetrische Matrix). Die *transponierte Matrix* einer Matrix $A = [a_{ij}] \in \mathbb{R}^{m \times n}$ ist

$$A^T = [a_{ji}] \in \mathbb{R}^{n \times m}.$$

Eine Matrix heiss *symmetrisch*, wenn $A = A^T$.

Definition 8.13 (Idempotent). Eine Matrix $A = \mathbb{R}^{n \times n}$ heisst *idempotent*, wenn $A^2 = A \cdot A = A$.

Eine symmetrische, idempotente Matrix ist eine *orthogonale Projektionsmatrix*.

Definition 8.14 (linear Abhängig). Die m -dimensionalen Vektoren $\vec{v}_1, \dots, \vec{v}_n$ mit $\vec{v}_i \in \mathbb{R}^m, i = 1, 2, \dots, n$ heißen *linear abhängig*, wenn es eine nichttriviale Linearkombination gibt, die verschwindet, d.h. wenn es Skalare $\lambda_1, \lambda_2, \dots, \lambda_n$ gibt, die nicht alle = 0 sind, und für die gilt

$$\lambda_1 \vec{v}_1 + \lambda_2 \vec{v}_2 + \dots + \lambda_n \vec{v}_n = \vec{0}.$$

Definition 8.15 (Rang). Der *Rang* einer Matrix A ist die maximale Zahl linear unabhängiger Zeilen oder Spalten von A . Er wird $\text{rank}(A)$ abgekürzt (von engl. rank).

Definition 8.16 (Spur). Die *Spur* einer Matrix $A = [a_{ji}] \in \mathbb{R}^{n \times n}$ ist die Summe ihrer Diagonalelemente und wird mit $\text{tr}(A)$ abgekürzt (von engl. trace).

$$\text{tr}(A) = \sum_{k=1}^n a_{kk}.$$

Definition 8.17 (Determinante). Die *Determinante* ist eine Kennzahl, an der sich ablesen lässt, ob eine Matrix regulär oder singulär ist.

Die Determinante von Matrizen der Ordnung 2 und 3 lässt sich wie folgt berechnen:

$$A \in \mathbb{R}^{2 \times 2} : \det(A) = \begin{vmatrix} a & b \\ c & d \end{vmatrix} = a \cdot d - c \cdot b,$$

$$B \in \mathbb{R}^{3 \times 3} : \det(B) = \begin{vmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \\ b_{31} & b_{32} & b_{33} \end{vmatrix} = +b_{11}b_{22}b_{33} + b_{12}b_{23}b_{31} + b_{13}b_{21}b_{32} - b_{31}b_{22}b_{13} - b_{32}b_{23}b_{11} - b_{33}b_{21}b_{12}.$$

Für eine Matrix $A = [a_{ij}] \in \mathbb{R}^{n \times n}$ mit beliebiger Ordnung n kann die Determinante schrittweise über die Entwicklung (gem. *Entwicklungssatz von Laplace*) nach der i -ten Zeile oder j -ten Spalte erfolgen:

$$\begin{aligned} \det(A) &= \sum_{k=1}^n (-1)^{k+i} a_{ik} \det(A_{ik}), \\ &= \sum_{k=1}^n (-1)^{j+k} a_{kj} \det(A_{kj}), \end{aligned}$$

wobei $A_{ik} \in \mathbb{R}^{(n-1) \times (n-1)}$ die *Minormatrix* ist, welche aus der Matrix A durch entfernen der Zeile i und der Spalte k entsteht. Analoges gilt für A_{kj} .

Satz 8.2 (Determinante und Regularität). Eine quadratische Matrix ist genau dann regulär, wenn ihre Determinante nicht Null ist.

Somit ist auch ein Gleichungssystem mit n Unbekannten und n Gleichungen mit den Koeffizienten a_{ij} genau dann eindeutig lösbar, wenn für die Koeffizientenmatrix $A = [a_{ji}]$ gilt, dass $\det(A) \neq 0$.

Rechenregeln für die Determinante

Die Determinante wird durch elementare Zeilenoperationen des Gauss-Jordan Algorithmus wie folgt beeinflusst:

- $\det(A)$ ändert sich nicht bei einer Zeilenaddition,
- Wird eine Zeile mit $\lambda \in \mathbb{R} \setminus \{0\}$ multipliziert, dann gilt dies auch für die Determinante: $\lambda \cdot \det(A)$,
- Vertauscht man in einer Matrix zwei Zeilen, dann ändert sich das Vorzeichen von $\det(A)$.

Die Determinante ist für spezielle Matrizen sehr einfach zu berechnen:

- Die Determinante einer Einheitsmatrix ist gleich Eins: $\det(E) = 1$,
- Sind in einer Matrix A zwei Zeilen gleich oder linear abhängig voneinander, dann ist $\det(A) = 0$,
- Sind in einer Matrix A zwei Spalten gleich oder linear abhängig voneinander, dann ist $\det(A) = 0$,
- Hat eine Matrix A eine Nullzeile, dann ist $\det(A) = 0$,
- Hat eine Matrix A eine Spalte nur mit Nullen, dann ist $\det(A) = 0$,

- Die Determinante einer Diagonalmatrix ist gegeben durch das Produkt ihrer Diagonalelemente.

Es bestehen zudem folgende Beziehungen:

- $\det(A^T) = \det(A)$,
- $\det(AB) = \det(A)\det(B)$,
- $\det(A^{-1}) = \det(A)^{-1}$.

Definition 8.18 (Determinante als Homomorphismus). Die Determinante bildet quadratische Matrizen in Zahlen ab und führt Produkte von Matrizen in Produkte von Zahlen über:

$$\begin{aligned}\det : \mathbb{R}^{n \times n} &\rightarrow \mathbb{R} \\ A &\mapsto \det(A)\end{aligned}$$

mit den Eigenschaften, dass $\det(AB) = \det(A)\det(B)$, $\det(I) = 1$ und $\det(A^{-1}) = \det(A)^{-1}$. Eine solche Abbildung, welche die wesentlichen Eigenschaften der algebraischen Struktur erhält, heißt ein *Homomorphismus*.

Hinweis: Ein umkehrbarer Homomorphismus nennt sich *Isomorphismus*.

Definition 8.19 (Eigenwert, Eigenvektor). Sei $A \in \mathbb{R}^{n \times n}$ eine quadratische Matrix mit Ordnung n , $\vec{w} \in \mathbb{R}^n \setminus \{\vec{0}\}$ ein Vektor ungleich dem Nullvektor und $\lambda \in \mathbb{R}$. Wenn

$$A \cdot \vec{w} = \lambda \cdot \vec{w},$$

dann ist λ ein *Eigenwert* und \vec{w} ein *Eigenvektor* von A .

Definition 8.20 (Charakteristisches Polynom). Sei $A \in \mathbb{R}^{n \times n}$ eine beliebige und $E \in \mathbb{R}^{n \times n}$ die Einheitsmatrix mit Ordnung n . Das Polynom

$$p(\lambda) = \det(A - \lambda \cdot E)$$

nennt sich das *charakteristische Polynom* der Matrix A .

Die Eigenwerte einer Matrix sind die Nullstellen ihres charakteristischen Polynoms.

Satz 8.3 (Cramersche Regel). Sei ein reguläres lineares Gleichungssystem mit n Gleichungen und n Unbekannten $A\vec{x} = \vec{b}$. Die Lösung ist gegeben durch

$$x_i = \frac{\det(A_i)}{\det(A)}, \quad \forall i = 1, 2, \dots, n,$$

wobei die Matrix A_i aus A entsteht, indem die i -te Spalte von A durch die rechte Seite \vec{b} ersetzt wird.

8.3 Lineare Abbildungen

Definition 8.21 (Lineare Abbildung). Eine Abbildung $L : \mathbb{R}^n \rightarrow \mathbb{R}^m$ ist *linear*, wenn für alle $\vec{x}, \vec{y} \in \mathbb{R}^n$ und $\lambda \in \mathbb{R}$ gilt, dass

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

Satz 8.4 (Lineare Abbildungen und Matrizen). Ist eine Matrix $A \in \mathbb{R}^{m \times n}$ gegeben, dann ist die Abbildung

$$\begin{aligned}L : \mathbb{R}^n &\rightarrow \mathbb{R}^m \\ \vec{x} &\mapsto A\vec{x}\end{aligned}$$

linear. Ist umgekehrt $L : \mathbb{R}^n \rightarrow \mathbb{R}^m$ eine lineare Abbildung, dann gibt es genau eine Matrix $A \in \mathbb{R}^{m \times n}$ mit $L(\vec{x}) = A\vec{x}, \forall \vec{x} \in \mathbb{R}^n$.

Lineare Abbildungen in \mathbb{R}^2

Eine lineare Abbildung von \mathbb{R}^2 nach \mathbb{R}^2 mit zugehörige Abbildungsmatrix $A = [a_{ij}] \in \mathbb{R}^{2 \times 2}$ lässt sich wie folgt schreiben:

$$\begin{aligned}L : \mathbb{R}^2 &\rightarrow \mathbb{R}^2 \\ \vec{x} = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} &\mapsto L(\vec{x}) = \vec{y} = \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}.\end{aligned}$$

Satz 8.5 (Abbildung der Einheitsvektoren). Für eine lineare Abbildung ist die zugehörige Abbildungsmatrix $A = [a_{ij}] \in \mathbb{R}^{n \times n}$ spaltenweise bestimmt durch die Bilder der Einheitsvektoren, weil (hier am Beispiel einer Abbildung von \mathbb{R}^2 nach \mathbb{R}^2) gilt:

$$\begin{aligned}L(\vec{e}_1) &= \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} a_{11} \\ a_{21} \end{bmatrix}, \\ L(\vec{e}_2) &= \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} a_{12} \\ a_{22} \end{bmatrix}.\end{aligned}$$

Beispiel 8.2 (Drehung). Eine Drehung um den Nullpunkt und den Winkel ϕ im mathematisch positiven Sinne (gegen den Uhrzeigersinn) ist gegeben durch die Abbildungsmatrix

$$D = \begin{bmatrix} \cos(\phi) & -\sin(\phi) \\ \sin(\phi) & \cos(\phi) \end{bmatrix}.$$

Beispiel 8.3 (Abbildung gegeben durch das Bild zweier Punkte). Die lineare Abbildung $L : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ welche die Punkte $A = (a_1, a_2), B = (b_1, b_2)$ auf die Punkte $A' = (a'_1, a'_2), B' = (b'_1, b'_2)$ abbildet, ist gegeben durch die Abbildungsmatrix

$$M = \begin{bmatrix} a'_1 & b'_1 \\ a'_2 & b'_2 \end{bmatrix} \cdot \begin{bmatrix} a_1 & b_1 \\ a_2 & b_2 \end{bmatrix}^{-1}.$$

8.4 Geraden und Ebenen

Geraden (in der Ebene oder im Raum) und Ebenen (im Raum) können über Vektoren definiert werden.

Definition 8.22 (Gerade in Parameterform). Sei $\vec{p} \in \mathbb{R}^n$ ein *Stützvektor* und $\vec{u} \in \mathbb{R}^n \setminus \{\vec{0}\}$ ein *Richtungsvektor*. Dann ist die Gerade durch den Punkt P mit $\overrightarrow{OP} = \vec{p}$ in Richtung \vec{u} in *Parameterform* definiert als:

$$\vec{x}(t) = \vec{p} + t\vec{u}, \quad t \in \mathbb{R}.$$

Definition 8.23 (Gerade in Normalenform). Sei $\vec{p} \in \mathbb{R}^n$ ein *Stützvektor* und $\vec{n} \in \mathbb{R}^n \setminus \{\vec{0}\}$ ein *Normalenvektor*. Dann ist die Gerade durch den Punkt P mit $\overrightarrow{OP} = \vec{p}$ in Richtung \vec{u} mit $\vec{u} \perp \vec{n}$ in *Normalenform* definiert als:

$$(\vec{x} - \vec{p}) \bullet \vec{n} = 0 \quad \text{oder} \quad \vec{x} \bullet \vec{n} = \vec{p} \bullet \vec{n}.$$

Definition 8.24 (Gerade in Koordinatenform). Eine Gerade in der Ebene \mathbb{R}^2 lässt sich auch in *Koordinatenform* geben:

$$ax + by + c = 0, \quad a, b, c \in \mathbb{R},$$

wobei mindestens einer der beiden Koeffizienten $a \neq 0$ oder $b \neq 0$.

Definition 8.25 (Ebene in Parameterform). Seien $\vec{p} \in \mathbb{R}^n$ ein *Stützvektor* und $\vec{u}, \vec{v} \in \mathbb{R}^n \setminus \{\vec{0}\}$ zwei nicht parallele *Spannvektoren*. Dann ist die Ebene durch den Punkt P mit $\overrightarrow{OP} = \vec{p}$, welche durch die Richtungen \vec{u}, \vec{v} aufgespannt wird, in *Parameterform* definiert als:

$$\vec{x}(t) = \vec{p} + s\vec{u} + t\vec{v}, \quad s, t \in \mathbb{R}.$$

Definition 8.26 (Ebene in Normalenform). Sei $\vec{p} \in \mathbb{R}^n$ ein *Stützvektor* und $\vec{n} \in \mathbb{R}^n \setminus \{\vec{0}\}$ ein *Normalenvektor*. Dann ist die Ebene durch den Punkt P mit $\overrightarrow{OP} = \vec{p}$ mit Normalenvektor \vec{n} in *Normalenform* definiert als:

$$(\vec{x} - \vec{p}) \bullet \vec{n} = 0 \quad \text{oder} \quad \vec{x} \bullet \vec{n} = \vec{p} \bullet \vec{n}.$$

Definition 8.27 (Ebene in Koordinatenform). Eine Ebene im Raum \mathbb{R}^3 lässt sich auch in *Koordinatenform* geben:

$$ax + by + cz + d = 0, \quad a, b, c, d \in \mathbb{R},$$

wobei mindestens einer der drei Koeffizienten $a \neq 0, b \neq 0$ oder $c \neq 0$.

Definition 8.28 (Vereinfachte und Hessesche Normalenform). Sei $\vec{p} \in \mathbb{R}^n$ ein Stützvektor und $\vec{n} \in \mathbb{R}^n \setminus \{\vec{0}\}$ ein Normalenvektor und eine Gerade oder Ebene definiert durch ihre Normalenform als:

$$(\vec{x} - \vec{p}) \bullet \vec{n} = 0.$$

Die *vereinfachte Normalenform* ist dann:

$$\vec{x} \bullet \vec{n} - b = 0, \quad \text{mit } b = \vec{p} \bullet \vec{n}$$

und die *Hessesche Normalenform* ist gegeben durch:

$$\vec{x} \bullet \vec{n}_0 - b_0 = 0, \quad \text{mit } \vec{n}_0 = \frac{\vec{n}}{|\vec{n}|}, b_0 = \frac{b}{|\vec{n}|},$$

d.h. die Hessesche Normalenform ist eine Normalenform mit normiertem Normalenvektor, d.h. $|\vec{n}_0| = 1$.

Satz 8.6 (Abstand eines Punktes von einer Geraden oder Ebene). Sei eine Gerade oder Ebene gegeben durch ihre Hessesche Normalenform

$$\vec{x} \bullet \vec{n}_0 - b_0 = 0.$$

Ein Punkt P mit Ortsvektor $\overrightarrow{OP} = \vec{p}$ hat den folgenden Abstand a von der Geraden oder Ebene:

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

8.5 Vektorräume

Definition 8.29 (Vektorraum). Ein reeller *Vektorraum* (reeller linearer Raum) besteht aus einer Menge V von Elementen, die wir Vektoren nennen, die folgenden Regeln, *Vektorraumaxiome* genannt, genügen:

- (i) *Verknüpfung von Vektoren*. Es gibt eine Verknüpfung $+$ auf V , welche je zwei Vektoren $\vec{u}, \vec{v} \in V$ einen Vektor $\vec{u} + \vec{v} \in V$ zuordnet, sodass für alle $\vec{u}, \vec{v}, \vec{w} \in V$ die folgenden Eigenschaften erfüllt sind:

- *Kommutativität*: $\vec{u} + \vec{v} = \vec{v} + \vec{u}$,

- *Assoziativitat:* $\vec{u} + (\vec{v} + \vec{w}) = (\vec{u} + \vec{v}) + \vec{w}$,
- *Nullvektor:* Es existiert ein Nullvektor $\vec{0}$, so dass $\vec{u} + \vec{0} = \vec{u}$,
- *Existenz negativer Vektoren:* Zu jedem $\vec{v} \in V$ gibt es einen Vektor $-\vec{v} \in V$, so dass $\vec{v} + (-\vec{v}) = \vec{0}$.

(ii) *Verknpfung von reellen Zahlen und Vektoren.* Fur jeden Vektor $\vec{v} \in V$ und jede reelle Zahl $c \in \mathbb{R}$ ist ein Vektor $c \cdot \vec{v} \in V$ definiert. Diese Bildung des skalaren Vielfachen ist so, dass fur alle $c, d \in \mathbb{R}$ und fur alle Vektoren $\vec{u}, \vec{v} \in V$ die folgenden Eigenschaften gelten:

- *Distributivitat:* $c \cdot (\vec{u} + \vec{v}) = c \cdot \vec{u} + c \cdot \vec{v}$,
- *Distributivitat:* $(c + d) \cdot \vec{u} = c \cdot \vec{u} + d \cdot \vec{u}$,
- *Assoziativitat:* $c \cdot (d \cdot \vec{v}) = (c \cdot d) \cdot \vec{v}$,
- $1 \cdot \vec{v} = \vec{v}$.

Definition 8.30 (Lineare Hulle). Fur die Vektoren $\vec{v}_1, \vec{v}_2, \dots, \vec{v}_k \in \mathbb{R}^n$ heisst die Menge all ihrer Linearkombinationen

$$\text{span}(\vec{v}_1, \vec{v}_2, \dots, \vec{v}_k) = \left\{ \vec{u} \in \mathbb{R}^n \mid \exists \lambda_1, \lambda_2, \dots, \lambda_k \in \mathbb{R} \text{ mit } \vec{u} = \sum_{i=1}^k \lambda_i \vec{v}_i \right\}$$

die *lineare Hulle* von $\vec{v}_1, \vec{v}_2, \dots, \vec{v}_k$.

Definition 8.31 (Basis, Dimension eines Vektorraumes). Die Menge $\{\vec{v}_1, \vec{v}_2, \dots, \vec{v}_k\}$ mit $\vec{v}_k \in \mathbb{R}^n$ heisst genau dann eine *Basis* von \mathbb{R}^n , wenn

- $\text{span}(\vec{v}_1, \vec{v}_2, \dots, \vec{v}_k) = \mathbb{R}^n$,
- $\vec{v}_1, \vec{v}_2, \dots, \vec{v}_k$ linear unabhangig sind.

Jede Basis von \mathbb{R}^n enthalt genau n Vektoren. Umgekehrt nennt sich die Anzahl Basisvektoren eines Vektorraumes die *Dimension des Vektorraumes*. Entsprechend hat \mathbb{R}^n die Dimension n .

Definition 8.32 (kanonische Basis). Die Menge $K = \{\vec{e}_1, \vec{e}_2, \dots, \vec{e}_n\}$ mit den Vektoren

$$(\vec{e}_i)_j = \begin{cases} 1, & i = j \\ 0, & i \neq j \end{cases} \quad i = 1, 2, \dots, n$$

ist die *kanonische Basis* von \mathbb{R}^n . Jeder Vektor $\vec{v} \in \mathbb{R}^n$ schreibt sich dann als:

$$\vec{v} = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} = v_1 \vec{e}_1 + v_2 \vec{e}_2 + \dots + v_n \vec{e}_n.$$

Satz 8.7 (Basistransformation). Sei $K = \{\vec{e}_1, \vec{e}_2, \dots, \vec{e}_n\}$ die kanonische Basis von \mathbb{R}^n und $B = \{\vec{b}_1, \vec{b}_2, \dots, \vec{b}_n\}$ eine weitere Basis von \mathbb{R}^n , wobei die Basisvektoren \vec{b}_i durch ihre Koeffizienten in der kanonischen Basis gegeben sind. Sei ein Vektor $\vec{v} \in \mathbb{R}^n$, der sich in der Basis B als \vec{v}_B schreibt. Die Transformation in die kanonischen Basis ausgedrckt als Vektor \vec{v}_K berechnet sich aus

$$\vec{v}_K = M_{BK} \vec{v}_B,$$

Wobei die Spalten der Matrix M_{BK} aus Koeffizienten der Vektoren \vec{b}_i in der kanonischen Basis bestehen.

Seien zwei Basen von \mathbb{R}^n gegeben durch $B = \{\vec{b}_1, \vec{b}_2, \dots, \vec{b}_n\}$ und $C = \{\vec{c}_1, \vec{c}_2, \dots, \vec{c}_n\}$, wobei ihre Basisvektoren durch die Koeffizienten in der kanonischen Basis gegeben sind. Sei ein Vektor $\vec{v} \in \mathbb{R}^n$, der sich in der Basis B als \vec{v}_B schreibt. Die Transformation in die Basis C ausgedrckt als Vektor \vec{v}_C berechnet sich aus

$$\vec{v}_C = M_{CK}^{-1} M_{BK} \vec{v}_B.$$

0.1. ERWEITETER EUKLIDSCHER ALGORITHMUS

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

Initialisierung: Setze $x := a, y := b, q := x \div y, r := x - q \cdot y, (u, s, v, t) = (1, 0, 0, 1)$ (d.h. bestimme q und r so, dass $x = q \cdot y + r$ ist)

Wiederhole bis $r = 0$ ist

Ergebnis: $y = \text{ggT}(a, b) = s \cdot a + t \cdot b$

Wenn $\text{ggT}(a, b) = 1$ ist, dann folgt: $t \cdot v \equiv 1 \pmod{a}$

0.1.1. 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}

0.2. KLEINER FERMAT

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

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

Daraus folgend:

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

0.3. SATZ VON EULER

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

0.3.1. Euler'sche φ -Funktion (Totient)

Sei $n \in \mathbb{N} \setminus \{0\}$ und $\mathbb{Z}_n^* = \{x \in \mathbb{Z}_n \mid x \text{ hat ein multiplikatives Inverses in } \mathbb{Z}_n\}$. Dann heisst $\varphi(n)$:

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

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

0.3.1.1. 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 $\varphi(n \cdot m) = \varphi(n) \cdot \varphi(m)$

Georgiy Shevoroshkin

0.3.2. Kreuzprodukt

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

~~$a_x \times b_x$~~ $\Rightarrow a_y b_z - a_z b_y$
 ~~$a_y \times b_y$~~ $\Rightarrow + a_z b_x - a_x b_z$
 ~~$a_z \times b_z$~~ $\Rightarrow + a_x b_y - a_y b_x$

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

0.4. MATRIZEN

0.4.1. Glossar

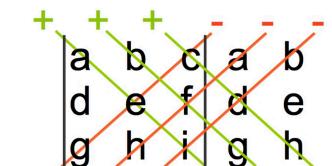
Begriff	Bedeutung
Rang	Wieviele Spaltenvektoren einer Matrix linear unabhängig sind
Nullmatrix	$0 = \begin{pmatrix} 0 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 0 \end{pmatrix}$
Quadratische Matrix	$M \in \mathbb{R}^{n \times n}$ Gleichviele Zeichen und Spalten
Diagonalmatrix	(immer quadratisch und symmetrisch): $D = \begin{pmatrix} x_1 & 0 & 0 & 0 \\ 0 & x_2 & 0 & 0 \\ 0 & 0 & x_3 & 0 \\ 0 & 0 & 0 & x_4 \end{pmatrix}, d_{ij} = 0 \text{ für } i \neq j$
Einheitsmatrix	(immer diagonal): $E = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$
Symmetrische Matrix	(immer quadratisch): $A = A^T, a_{ij} = a_{ji}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 4 & 4 \\ 3 & 4 & 1 \end{pmatrix}$
Obere Dreiecksmatrix	$O = \begin{pmatrix} x_1 & x_2 & x_3 \\ 0 & x_4 & x_5 \\ 0 & 0 & x_6 \end{pmatrix}, o_{ij} = 0 \text{ für } i > j$
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 $A \in \mathbb{R}^{n \times n}$ heisst A invertierbar, wenn es eine Matrix A^{-1} gibt, so dass $A \cdot A^{-1} = A^{-1} \cdot A = \text{Einheitsmatrix (E)}$. Dies ist der Fall, wenn A Regulär ist.

0.4.2. Determinante

1 × 1 Matrix : $\det(a) = a$

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

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



Bsp:

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

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

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

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

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

$$= 2 + 4 = 6$$

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

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

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

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

Weitere Eigenschaften:

- Die Determinante wechselt beim Vertauschen von Zeilen ihr Vorzeichen
- Wenn wir zu einer Zeile einer Matrix ein Vielfaches einer anderen Zeile dazuzählen, ändert die Determinante ihren Wert nicht

Weiteres:

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

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

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

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

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