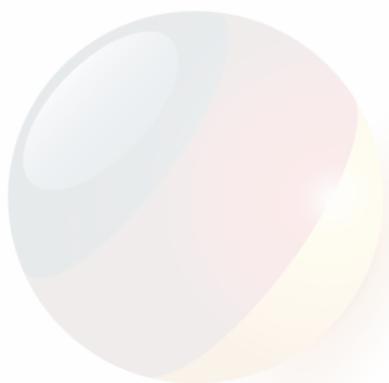




Studienbrief

Mathematik für Informatik I

Diskrete Mathematik und Lineare Algebra



Inhaltsverzeichnis

Vorwort	3
Inhaltsverzeichnis.....	5
Ergänzende Hinweise zum Studienbrief.....	9
Übergeordnete Lernziele des Studienmoduls.....	10
Teil I: Diskrete Mathematik	11
1 Mengenlehre	12
1.1 Mengenbegriff	13
1.2 Teilmengen.....	17
1.3 Mengenoperationen	18
2 Aussagenlogik.....	27
2.1 Allgemeingültigkeit und Tautologien.....	30
2.2 Quantoren.....	32
3 Beweisprinzipien	35
3.1 Direkter Beweis	36
3.2 Widerspruchsbeweise	37
3.2.1 Beweis durch Kontraposition.....	37
3.2.2 Indirekter Beweis	37
3.3 Äquivalenzbeweis.....	39
3.4 Beweis durch vollständige Induktion.....	40
4 Relationen, Abbildungen und Funktionen.....	44
4.1 Relation	44
4.1.1 Äquivalenzrelation	46
4.1.2 Äquivalenzklassen	49
4.1.3 Partition	50
4.1.4 Teilrelation und Teilordnung	51
4.2 Abbildungen, Funktionen, Bilder und Graphen.....	53
4.3 Abbildungseigenschaften	56
4.4 Verknüpfen und Umkehren von Abbildungen.....	58
4.5 Mächtigkeit von Mengen	62
5 Primzahlen und Teiler.....	66
5.1 Division mit Rest.....	66
5.2 Primfaktorzerlegung.....	68
5.2.1 Fundamentalsatz der Zahlentheorie	69
5.2.2 Primfaktorzerlegung großer Zahlen	69

5.3	Größter gemeinsamer Teiler.....	70
5.4	Euklidischer Algorithmus	71
5.5	Erweiterter Euklidischer Algorithmus	72
6	Modulare Arithmetik	75
6.1	Kongruenz.....	75
6.2	Restklassen	77
6.3	Modulare Addition und Multiplikation	79
7	Algebraische Strukturen.....	83
7.1	Gruppen.....	84
7.2	Ringe	86
7.3	Polynome.....	88
7.3.1	Polynomdivision	90
7.3.2	Horner-Schema.....	91
7.3.3	Abspaltung von Nullstellen.....	92
7.3.4	Anzahl von Nullstellen	93
7.3.5	Größter gemeinsamer Teiler von Polynomen.....	95
7.3.6	Euklidischer Algorithmus für Polynome.....	95
7.3.7	Reduzibilität.....	96
7.4	Körper.....	98
7.4.1	Polynome auf allgemeinen Körpern.....	101
7.4.2	Anwendungsbeispiel: Datensicherung.....	102
7.4.3	Anwendungsbeispiel: IBAN und ihre Prüfziffern.....	106
8	Anwendung: Algorithmen der Kryptografie.....	111
8.1	Erzeugen von Pseudozufallszahlen	111
8.1.1	Pseudo Random Number Generator (PRNGs)	112
8.1.2	True Random Number Generators (TRNGs)	113
8.2	Caesar-Verschlüsselung	114
8.3	AES-Verschlüsselung.....	115
8.4	RSA-Verschlüsselung.....	118
	Teil II Lineare Algebra	123
1	Grundlagen der Vektorrechnung.....	124
1.1	Tupel und Vektoren	124
1.2	Vektorräume.....	126
1.2.1	Vektoraddition.....	126
1.2.2	Multiplikation mit einem Skalar	127
1.2.3	Skalarprodukt	130
1.2.4	Kreuzprodukt.....	131
1.2.5	Länge und Betrag eines Vektors.....	134
1.2.6	Geometrische Objekte im Raum	138
1.3	Lineare Unabhängigkeit und Basis	141
1.3.1	Linearkombination	142
1.3.2	Lineare Unabhängigkeit.....	143
1.3.3	Basis, Entwicklungskoeffizienten und Koordinaten	144

1.3.4 Dimension	144
1.4 Teilräume	146
1.4.1 Lineare Hülle	146
1.4.2 Teilraum und Untervektorraum	147
2 Matrizen und lineare Gleichungen	154
2.1 Lineares Gleichungssystem	154
2.2 Matrix.....	156
2.3 Transponation und Skalarprodukt.....	163
2.4 Transformation von Vektoren	167
2.5 Determinante.....	169
2.6 Gauß-Jordan-Algorithmus	173
2.6.1 Zeilenumformungen	173
2.6.2 Tabellen- und Stufenform	174
2.7 Rang einer Matrix.....	177
2.8 Inverse Matrix	179
2.8.1 Berechnung inverse Matrix nach Gauß-Jordan.....	179
2.8.2 Berechnung inverse Matrix nach Cramer.....	180
3 Lineare Abbildungen und Transformationen	190
3.1 Lineare Abbildung	190
3.2 Bild und Kern einer linearen Abbildung.....	193
3.3 Koordinatentransformation	199
3.3.1 Verkettete Abbildung	200
3.3.2 Umkehrbarkeit.....	201
3.3.3 Drehungen	201
4 Eigenwerte und Eigenvektoren	209
4.1 Das charakteristische Polynom	211
4.2 Diagonalisierbarkeit	214
4.3 Eigenwerte symmetrischer Matrizen	221
5 Anwendung: Computergrafik Pipeline	227
5.1 Object-to-World	229
5.2 World-to-View.....	231
5.3 View-to-Projection	233
5.3.1 Perspektivische Projektion	234
5.3.2 Orthogonale Projektion	237
5.4 Clipping	238
5.5 Transformationspipeline	239
Nachwort.....	241
Anhang	243
Lösungen und Kommentare zu den Übungen, Glossar und Literatur des Studienbriefs in ILIAS	243

1.1 Mengenbegriff

Der Begriff **Menge** ist in vielen Bereichen der Informatik von grundlegender Bedeutung, wie zum Beispiel bei Datenbanken, und geht auf Georg Cantor zurück (1845–1918). Er begründete die moderne Mengenlehre. Der Begriff sollte nicht mit dem umgangssprachlichen Begriff „eine Menge“ im Sinne von „viel“ verwechselt werden. Obwohl eine „Zusammenfassung von Objekten“ zwar intuitiv verständlich ist, wird der Begriff „Menge“ in der Mathematik dennoch wie folgt klar definiert:



Definition 1.1 – Menge, Elemente

Eine Menge M ist eine Zusammenfassung von bestimmten, wohl unterscheidbaren Objekten der Anschauung oder des Denkens, welche die Elemente von M genannt werden, zu einem Ganzen (Cantor, Zermelo & Fraenkel, 2013). Mengen sind selbst Objekte und können daher Elemente anderer Mengen sein.

Die Elemente einer Menge M werden in geschweiften Klammern eingeschlossen, z. B. $M = \{3, 2, 8, 1\}$. Ist ein Element x Teil einer Menge M , so schreiben wir $x \in M$, ansonsten $x \notin M$. Man spricht: „ M ist die Menge mit den Elementen 3,2,8 und 1“ bzw. „ x ist (kein) Element von M “ oder „ x (nicht) in M “.



Beispiel

Bertrand Russell (1872–1970) formulierte das berühmte „Barbier-Paradoxon“ (Russell, 1918). Eine Variante lautet:

Ein Physiotherapeut massiert nur Menschen, die sich nicht selbst massieren.

Nun die Frage: Gehört er zu der Menge der Therapeuten, die sich selbst massieren? Beim Versuch, diese Frage zu beantworten, ergibt sich ein Widerspruch. Angenommen, ein Therapeut massiert sich selbst. Dann gehört er zu denen, die er aber laut Aussage nicht massiert, was der Annahme selbst widerspricht. Angenommen, es gilt das Gegenteil, das heißt, er massiert sich nicht selbst, dann erfüllt er selbst die Eigenschaft der Menschen, die er massiert. Das widerspricht jedoch wieder der Annahme, dass er ja nur Menschen massiert, die sich nicht selbst massieren.

Die gestellte Frage kann also nicht eindeutig beantwortet werden.

Es wurde später gezeigt, dass es in der Mathematik solche nicht entscheidbaren Fragen geben muss (Gödel, 1931). Für die Anwendungen in diesem Kurs ist die Definition einer Menge von Cantor jedoch völlig ausreichend.

Mengen sind **gleich** („=“), wenn sie dieselben Elemente beinhalten. Die Reihenfolge und Wiederholungen der Elemente einer Menge spielen keine Rolle. Es wird also nicht

2 Aussagenlogik



Lernziele

Nach der Bearbeitung des Kapitels

- kennen Sie die grundlegenden Definitionen und Eigenschaften der Logik, um Wissen so zu repräsentieren, dass daraus formal Schlüsse gezogen werden können.
- kennen Sie die Grundlagen boolescher Algebra, um logische Verknüpfungen formalisieren und interpretieren zu können.
- können Sie Wahrheitstabeln für verschiedene Aussagen erstellen und damit logische Zusammenhänge sichtbar machen.
- kennen Sie die verschiedenen Tautologien und Gesetze der Aussagenlogik.
- können Sie mithilfe von Quantoren und Junktoren spezifische Objekte oder Situationen präzise formulieren.

Die **Aussagenlogik** ist ein Zweig der **Logik**. Der Bereich beschäftigt sich mit Aussagen, die wahr oder falsch sein können, und dem Argumentationsfluss. Zusammengesetzte Aussagen werden gebildet, indem Aussagen durch logische Zusammenhänge miteinander verbunden werden. Anwendungsfelder finden sich besonders in der Informatik, wie bei Fallunterscheidungen im Programmiercode, bei der Wissensmodellierung im Bereich der Künstlichen Intelligenz, bei logischen Schaltungen im Hardwarebereich, aber auch beim automatisierten Beweisen oder Testen von Software.



Definition 2.1 – Aussage

Eine logische Aussage ist ein Satz in einer menschlichen oder auch künstlichen Sprache (z.B. Programmiersprachen), dem eindeutig einer der beiden Wahrheitswerte „wahr“ (1, w, true) oder „falsch“ (0, f, false) zugeordnet werden kann. Aussagen ohne logische Verbindungen werden als atomare Aussagen bezeichnet.



Formeln 2.1

Wir definieren folgende Verknüpfungen (oder Junktoren) von Aussagen:

- i. Negation („nicht A“):
 - $\neg A$
- ii. Konjunktion („A und B“):
 - $A \wedge B$

- iii. Disjunktion („A oder B“):
 - $A \vee B$
- iv. Kontravalenz/ausschließende Disjunktion („entweder A oder B“, „XOR“):
 - $A \oplus B$
- v. Implikation („A impliziert B“ oder „wenn A, dann B“):
 - $A \Rightarrow B$
 - $A \Rightarrow B \neq B \Rightarrow A$
- vi. Äquivalenz („A ist äquivalent zu B“ oder „genau dann A, wenn auch B“):
 - $A \Leftrightarrow B$

Tab. 2: Wahrheitswertetafel der Aussagenlogik (© BSA/DHfPG).

A	B	$\neg A$	$\neg B$	$A \wedge B$	$A \vee B$	$A \oplus B$	$A \Rightarrow B$	$B \Rightarrow A$	$A \Leftrightarrow B$
1	1	0	0	1	1	0	1	1	1
1	0	0	1	0	1	1	0	1	0
0	1	1	0	0	1	1	1	0	0
0	0	1	1	0	0	0	1	1	1



Beispiel

Hier ein paar Beispiele für Aussagen:

- „ $1 + 3 = 4$ “ ist eine wahre Aussage.
- „9 ist eine Primzahl“ ist eine falsche Aussage.
- „Es ist noch sehr früh“ ist keine Aussage, da kein eindeutiger Wahrheitswert zugeordnet werden kann.
- A : „Die Geraden g und h schneiden sich.“
- $\neg A$: „Die Geraden g und h schneiden sich **nicht**.“
- $\neg(\neg A)$: „Es ist **nicht** wahr, dass die Geraden g und h sich **nicht** schneiden.“
- Die Konjunktion der wahren Aussage $A =$ „8 ist eine gerade Zahl“ mit der falschen Aussage $B =$ „8 ist durch 5 teilbar“ ist die falsche Aussage $A \wedge B =$ „8 ist eine gerade Zahl **und** durch 5 teilbar“.
- Die Disjunktion der wahren Aussage $0 < 1$ und der falschen Aussage $0 = 1$ ist die wahre Aussage $0 \leq 1$, sprich „0 ist kleiner **oder** gleich 1“.
- Die Aussage „**Wenn** $3 < 2$ ist, **dann** ist $2 < 1$ “ ist wahr, obwohl sie eine Implikation zweier falscher (Teil-)Aussagen ist. Die Implikation ist wahr, wenn beide Aussagen wahr sind oder wenn die erste Aussage falsch ist.
- Die Äquivalenzverknüpfung der falschen Aussage „Die Tonne ist eine Längeneinheit“ mit der wahren Aussage „1000 Meter ergeben einen Kilometer“ ist die falsche Aussage „Die Tonne ist **dann und nur dann** eine

Längeneinheit, **wenn** 1000 Meter einen Kilometer ergeben“. Die Äquivalenz zweier Teilaussagen ist nur wahr, wenn entweder beide Teilaussagen wahr oder beide falsch sind.

- „Diese Aussage ist falsch.“ Durch die spezielle Art des Bezugs auf sich selbst kann der Satz weder wahr noch falsch sein und ist deshalb keine Aussage.



Merke

Beachten Sie, dass die Disjunktion nicht mit einer Kontravalenz (ausschließende Disjunktion, „entweder oder“) verwechselt werden sollte. Somit ist eine Disjunktion zweier Wahrheitswerte auch wahr, wenn beide Werte wahr sind. Man spricht hier auch von einer einschließenden Disjunktion.

Eine Implikation ist immer wahr, wenn die Prämisse falsch ist. In der Aussagenlogik können aus falschen Aussagen auch wahre Aussagen folgen, wie zum Beispiel:

„Wenn $1 = 2$ (falsch), dann ist Berlin die Hauptstadt von Frankreich (falsch)“
→ wahr!

„Wenn $1 = 2$ (falsch), dann ist Paris die Hauptstadt von Frankreich (wahr)“
→ wahr!

„Wenn $1 < 2$ (wahr), dann ist Berlin die Hauptstadt von Frankreich (falsch)“
→ falsch!

„Wenn $1 < 2$ (wahr), dann ist Paris die Hauptstadt von Frankreich (wahr)“
→ wahr!



Übung 2.1

Handelt es sich hier um Aussagen? Wenn ja, sind sie wahr oder falsch?

1. Moskau ist die Hauptstadt von Finnland.
2. $32 + 9 = 41$
3. 1 ist kleiner als 2.
4. Vielen Dank!
5. $x^2 - 4 = 0$
6. Delfine sind Säugetiere und leben auf dem Land.
7. Wenn eine Zahl 20 gerade ist, dann ist sie auch durch 7 teilbar.
8. Wenn London in Frankreich liegt, dann ist Schnee schwarz.
9. Immer wenn es regnet, sind auch Wolken am Himmel.

4 Relationen, Abbildungen und Funktionen



Lernziele

Nach der Bearbeitung des Kapitels

- können Sie mathematische Abbildungen und Relationen formal beschreiben, um die Grundlagen von Konzepten wie relationalen Datenbanken verstehen zu können.
 - können Sie den Begriff „Relation“ definieren und gegenüber Abbildungen und Funktion abgrenzen.
 - kennen Sie die verschiedenen Formen von Relationen und können eine Menge in Klassen unterteilen.
 - kennen Sie die Besonderheiten und Eigenschaften von Abbildungen und können diese anwenden.
 - können Sie bestimmen, ob eine Relation reflexiv, symmetrisch oder transitiv ist.
 - können Sie Abbildungen umkehren und/oder miteinander verknüpfen und kennen die Kriterien für Injektivität, Surjektivität und Bijektivität.
 - können Sie die Mächtigkeit bzw. Abzählbarkeit von Mengen bestimmen.
-

Mithilfe von Relationen kann man die Elemente zweier Mengen in Beziehung zueinander setzen. Des Weiteren kann eine Menge in Klassen unterteilt werden, sodass „ähnliche“ Elemente in derselben Klasse liegen. Die Elemente innerhalb einer Klasse können geordnet werden und als spezieller Ausschnitt einer Menge einem besseren Verständnis dienen. In der Informatik sind solche Fragestellungen besonders bei relationalen Datenbanken wichtig, wenn man zum Beispiel aus der Menge aller Mitglieder eines Fitnessstudios nur einen Überblick über alle Männer im Alter von 30 bis 40 Jahre haben möchte.

4.1 Relation

Relationen in der Mathematik gelten als Beziehungen, bei denen stets klar ist, ob sie existieren oder nicht. Genauer gesagt, zwei Elemente können also nicht „teilweise“ in einer Relation zueinanderstehen:



Definition 4.1 – Relation, Umkehrrelation

Seien A, B nichtleere Mengen. Dann ist eine Relation R auf $A \times B$ eine Teilmenge:

$$R \subset A \times B = \{ (x, y) \mid x \in A, y \in B \}$$

Für alle $(x, y) \in R$ sagt man „ x steht in Relation R zu y “ und schreibt auch xRy .

Zu jeder Relation R existiert eine zugehörige Umkehrrelation R^{-1} :

$$R^{-1} := \{ (y, x) \in B \times A \mid (x, y) \in R \}$$

Man bildet die Umkehrrelation einer Relation, indem man Vor- und Nachbereich vertauscht, das heißt für xRy gilt $yR^{-1}x$.

Objekte, die in Relation zueinanderstehen, bilden also ein Tupel, welches Element der Relation ist. Wenn nicht ausdrücklich etwas anderes angegeben ist, versteht man unter einer Relation eine „zweistellige“ (oder „binäre“) Relation, also eine Beziehung zwischen je zwei Dingen. Die Tupel sind in diesem Fall geordnete Paare.



Beispiel

Sei M die Menge der Mitglieder eines Fitnessstudios und K die Menge der Fitnesskurse. Dann ist

$$R = \{ (m, k) \mid m \text{ belegt den Fitnesskurs } k \}$$

eine Relation R auf $M \times K$ und

$$R^{-1} = \{ (k, m) \mid \text{Fitnesskurs } k \text{ hat Teilnehmer } m \}$$

Andere Beispiele:

- Umkehrrelation der Relation „ist Nachfolger von“ ist die Relation „ist Vorgänger von“.
- Umkehrrelation der Relation „ist größer als“ ist die Relation „ist kleiner als“.
- Umkehrrelation der Relation „lehrt“ ist die Relation „wird gelehrt von“.

$$A = \begin{pmatrix} \vdots \\ a_i \\ \vdots \\ a_j \\ \vdots \end{pmatrix} \mapsto \begin{pmatrix} \vdots \\ a_i \\ \vdots \\ a_j + \lambda \cdot a_i \\ \vdots \end{pmatrix}$$

- Vertauschen der i -ten Zeile mit der j -ten Zeile:

$$A = \begin{pmatrix} \vdots \\ a_i \\ \vdots \\ a_j \\ \vdots \end{pmatrix} \mapsto \begin{pmatrix} \vdots \\ a_j \\ \vdots \\ a_i \\ \vdots \end{pmatrix}$$

2.6.2 Tabellen- und Stufenform

Als ersten Schritt wird das Gleichungssystem in eine sogenannte **Tabellenform** gebracht. Die Tabellenform bietet in den meisten Fällen eine übersichtlichere Darstellung. In der Tabelle trägt man dann die Skalare, also die Werte vor den Variablen, ein.

$a_{11} \cdot v_1 + \dots + a_{1n} \cdot v_n = b_1$	\Rightarrow	v_1	v_2	...	v_n	\vec{b}
\vdots		a_{11}	a_{12}	...	a_{1n}	b_1
$a_{m1} \cdot v_1 + \dots + a_{mn} \cdot v_n = b_m$		\vdots	\vdots	\vdots	\vdots	\vdots
		a_{m1}	a_{m2}	...	a_{mn}	b_m

Abb. 25: Darstellung eines linearen Gleichungssystems in Tabellenform (© BSA/DHfPG).

Als nächsten Schritt soll die eben aufgestellte Tabellenform in eine sogenannte **Stufenform** umgewandelt werden. Sobald die Tabelle in eine Stufenform gebracht wurde, kann das Gleichungssystem durch einfaches Einsetzen der einzelnen Variablen in die Zeilen gelöst werden. Um eine Tabelle in Stufenform zu bringen, können einzelne Zeilen mit einer Konstanten multipliziert werden oder ganze Zeilen miteinander addiert oder subtrahiert werden.

v_1	v_2	...	v_n	\vec{b}	\Rightarrow	v_1	v_2	...	v_n	\vec{b}
a_{11}	a_{12}	...	a_{1n}	b_1		*	*	*	*	*
\vdots	\vdots	\vdots	\vdots	\vdots		\vdots	*	*	*	*
\vdots	\ddots	\ddots	\vdots	\vdots		0	\ddots	*	*	*
a_{m1}	a_{m2}	...	a_{mn}	b_m		0	0	...	*	*

Abb. 26: Darstellung einer Stufenform (Dreiecksmatrix) nach Zeilenumformungen (© BSA/DHfPG).

Die Stufenform wäre ausreichend, um daraus die Determinante einer Matrix zu berechnen. Um jedoch das gesamte Gleichungssystem zu lösen, muss durch geschickte Zeilenumformungen eine Einheitsmatrix hergestellt werden. Dies geschieht durch Einsetzen der jeweiligen Variablen nacheinander von unten nach oben.

v_1	v_2	...	v_n	\vec{b}		v_1	v_2	...	v_n	\vec{b}
*	*	*	*	*	→	1	0	...	0	*
⋮	*	*	*	*		⋮	1	0	⋮	*
0	⋮	*	*	*		0	⋮	1	0	*
0	0	...	*	*		0	0	...	1	*

Abb. 27: Darstellung einer Einheitsmatrix nach Zeilenumformungen (© BSA/DHfPG).



Beispiel

Gegeben sei folgende Matrix, dessen Determinante mittels **Gauß-Jordan-Algorithmus** berechnet werden soll:

$$A = \begin{pmatrix} 1 & 3 & 4 \\ 0 & 0 & 2 \\ 2 & 0 & 7 \end{pmatrix} \xrightarrow{II \leftrightarrow III} \begin{pmatrix} 1 & 3 & 4 \\ 2 & 0 & 7 \\ 0 & 0 & 2 \end{pmatrix} \xrightarrow{II^* = II - 2 \cdot I} \begin{pmatrix} 1 & 3 & 4 \\ 0 & -6 & -1 \\ 0 & 0 & 2 \end{pmatrix}$$

Nach nur drei Zeilenumformungen konnte eine obere Dreiecksmatrix hergestellt werden. Daraus ergeben sich folgende Änderungen der Determinante:

- Das **Vorzeichen** ändert sich durch das Vertauschen der Zeile *II* und *III*
- Keine Änderungen durch das Subtrahieren des Vielfachen der Zeile *I*

Somit lässt sich die Determinante von *A* folgendermaßen direkt von der oberen Dreiecksmatrix ablesen:

$$\det(A) = (-1) \cdot (1 \cdot (-6) \cdot 2) = 12$$