

# MATHEMATIK IM ALLTAG

BEI PROF. DR. S. GOETTE, PROF. DR. W. SOERGEL, PHD S. KITCHEN UND DR.  
M. LISTING

In diesem Proseminar geht es darum, in unserem Alltag „versteckte“ Mathematik „wiederzuentdecken“. Jeder einzelne Vortrag beschreibt einen Gegenstand, eine Technik, ein Problem oder ein Phänomen des täglichen Lebens. Dabei soll zunächst erklärt werden, worum es geht, und wieso Mathematik ins Spiel kommt. Anschließend sollen die auftretenden Probleme mathematisch beschrieben und — wenn möglich — gelöst werden. Dazu sind oft neue mathematische Begriffe zu definieren oder Sätze zu beweisen. Ziel ist es, am Ende eines Vortrages das Thema aus mathematischer Sicht zu verstehen.

Die angegebene Literatur ist immer nur als Ausgangspunkt gedacht; die Vortragenden dürfen gern und sollten nach Möglichkeit zusätzliche Quellen suchen, um den Vortragsgegenstand oder die dafür benötigte Mathematik besser zu verstehen oder verwandte Teileaspekte mit aufzugreifen.

Es folgt eine Beschreibung der einzelnen Vorträge, geordnet nach Themenbereichen. Sollten Sie Interesse an einem Thema haben, das unten nicht aufgeführt ist, und zu dessen mathematischem Inhalt Sie Literatur kennen, dann schreiben Sie bitte rechtzeitig (mehrere Tage vor der Vorbesprechung) eine e-mail an den Dozenten. Falls das Thema in den Rahmen des Proseminars passt, dürfen Sie auch darüber vortragen.

## 1. RECHENVERFAHREN

Anwendungen der Mathematik im Alltag erfordern oftmals numerische Berechnungen. Die Verfahren, die hier vorgestellt werden sollen, kommen teilweise in anderen Vorträgen zum Einsatz. Grundkenntnisse in Numerik (oder Informatik) sind hilfreich, aber nicht notwendig.

**1. Additions- und Schiebe-Algorithmen.** Taschenrechner, vor allem ältere Modelle, verfügen über eine sehr einfache Hardware. In diesem Vortrag sollen daher Algorithmen vorgestellt werden, die die Exponentialfunktion, Winkel- und Hyperbelfunktionen und ihre Inversen mit möglichst einfachen Mitteln vergleichsweise schnell und vor allem zuverlässig ausrechnen.

*Literatur:* [15], [16], Stichworte jeweils CORDIC und BKM.

**2. Die Zahl  $\pi$ .** Es gibt viele Reihen, Iterationsverfahren, etc..., die gegen die Kreiszahl  $\pi$  konvergieren. Dieser Vortrag soll einige davon vorstellen und erklären, warum und wie schnell die Verfahren konvergieren.

*Literatur:* [16], Stichwort: Numerical approximations of  $\pi$ .

**3. Die diskrete Fouriertransformation.** Dieser Vortrag soll erklären, was eine diskrete Fouriertransformation ist und wie sie schnell berechnet werden kann. Außerdem sollten einige Anwendungen gegeben werden, jedoch nicht solche, die

in anderen Vorträgen (z.B. Abtasttheorem, Audio-Kompression, Kernspin) behandelt werden.

*Literatur:* [15], *Stichworte:* Schnelle Fourier-Transformation

## 2. DATENVERARBEITUNG/KRYPTOGRAPHIE

Kryptographie ist die Wissenschaft von der Verschlüsselung. Die folgenden zwei Vorträge behandeln Public-Key-Verschlüsselungsverfahren. Diese ermöglichen eine abhörsichere Kommunikation, ohne dass vorher geheime Vereinbarungen getroffen wurden. Public-Key-Verfahren beruhen auf sogenannten Falltürfunktionen, Funktionen, die leicht zu berechnen sind, für deren Umkehrung es aber keinen effizienten Algorithmus gibt.

**4. Der RSA-Code.** Die Multiplikation zweier Primzahlen ist einfach, jedoch eine große Zahl in Primfaktoren zu zerlegen, sprengt schnell die Kapazitäten eines jeden Rechners. Auf dieser Asymmetrie beruht der RSA-Code.

*Literatur:* [16], *Stichwort* „RSA“, [14]

*Vorkenntnisse:* Algebra

**5. Diskrete Logarithmen.** In endlichen zyklischen Gruppen mit gegebenem Erzeuger  $g$  lässt sich die Potenz  $h = g^n$  für gegebenes  $n$  schnell berechnen, während kein effizientes Verfahren bekannt ist, dass den „Logarithmus“  $n$  bei gegebenem  $h$  bestimmt. Hierauf basieren das Diffie-Hellmann-, das ElGamal- und das DSA-Verfahren.

*Literatur:* [14]; [15], *Stichworte* „Diffie-Hellman-Schlüsselaustausch“, „Elgamal-Kryptosystem“

*Vorkenntnisse:* Algebra

**6. Quantencomputer und der Shor-Algorithmus.** Zwar ist der Quantencomputer noch fern der Realisierung, man weiß aber, welche Rechenoperationen einem Quantencomputer möglich wären. So gibt es einen effizienten Algorithmus zur Primfaktorzerlegung mittels eines Quantencomputers, den Shor-Algorithmus.

*Literatur:* [16], *Stichwort* „Shor algorithm“

*Vorkenntnisse:* Algebra. Auch Quantenmechanik I ist hilfreich.

## 3. DATENVERARBEITUNG/MUSIK

**7. Schwingungen und das Abtasttheorem.** Das Abtasttheorem ist in der Signalverarbeitung von zentraler Bedeutung. Es kommt überall dort zum Tragen, wo man analoge Signale digital übertragen möchte, z.B. beim Anhören einer CD oder beim digitalen Telefonieren. Das Abtasttheorem besagt, dass bei einem Signal mit Bandbreite  $B$ , Abtasten mit einer Frequenz  $f > 2B$  ausreicht, um daraus das Signal fehlerfrei rekonstruieren zu können. In dem Vortrag soll dieses Theorem bewiesen werden. Dafür ist die Fourieranalyse das wichtigste mathematische Hilfsmittel. Außerdem soll erklärt werden, wie dies auf den CD-Spieler anzuwenden ist.

*Literatur:* [15], *Stichwort:* Nyquist-Shannon-Abtasttheorem [16], *Stichwort:* Nyquist-Shannon-sampling theorem [1], *Kapitel:* Schwingungen, p.193-202

**8. Audio-Kompression.** Audio-Formate wie MP3, AAC oder Vorbis komprimieren die digital erfassten Klangdaten, indem kaum oder gar nicht hörbare Teile des Audiosignals weggelassen werden. Ein wichtiger Bestandteil ist dabei immer eine modifizierte diskrete Kosinustransformation (MDCT). Dieser Vortrag soll diese Transformation und ihre Inverse einführen. Darüberhinaus können die benutzten Kompressionsverfahren und die im Zusammenhang damit auftretenden Probleme beschrieben werden.

*Literatur:* [15], [16], *Stichworte:* MP3, MDCT, Vorbis

**9. Fehlerkorrigierende Codes.** Um die „Mathematik einer CD“ zu verstehen, sollen in diesem Vortrag die Grundlagen der Codierungstheorie erläutert werden. Der erste effiziente fehlerkorrigierende Code wurde von B. W. Hamming eingeführt, der sogenannte Hammingcode. Das Codierungssystem, das auf einer CD verwendet wird, ist ein Reed-Solomon-Code.

*Literatur:* [1], [14]

#### 4. WIRTSCHAFT UND GESELLSCHAFT

**10. Spieltheorie I — das Nash-Gleichgewicht.** Mit Spieltheorie kann man nicht nur Spiele im üblichen Sinne, sondern unterschiedlichste strategische Konfliktsituationen beschreiben. Zunächst sollte erklärt werden, was mit „Spiel“ und „reinen“ und „gemischten Strategien“ gemeint ist. Ein Nash-Gleichgewicht besteht aus Strategien für alle beteiligten Spieler, so dass es sich für keinen Spieler lohnt, die Strategie zu wechseln, wenn die Mitspieler ihre Strategie beibehalten. Der Vortrag soll zeigen, dass Nash-Gleichgewichte in gemischten Strategien immer existieren.

*Literatur:* [11], [5], [10]

*Vorkenntnisse:* Topologie ist hilfreich (Brouwerscher Fixpunktsatz)

**11. Spieltheorie II — das Minimax-Theorem.** Für Nullsummenspiele mit zwei Spielern hat von Neumann schon vor Nash die Existenz eines Nash-Gleichgewicht in gemischten Strategien bewiesen. In diesem Vortrag soll ein Algorithmus vorgestellt werden, der ein Nash-Gleichgewicht findet.

*Literatur:* [5], [10]

**12. Der Satz vom Diktator.** Nach Wahlen oder Abstimmungen entsteht bei den Beteiligten manchmal das Gefühl, dass das Abstimmungsverfahren zu einem „ungerechten“ Ergebnis geführt hat. Verschiedene mathematische Kriterien für „Gerechtigkeit“ an ein solches Verfahren können unvereinbar sein. Der Satz von Arrow, umgangssprachlich auch Satz vom Diktator, ist ein Beispiel dafür. Der Vortrag soll diesen Satz erklären und beweisen und eventuell verwandte Sätze vorstellen.

*Literatur:* [16], *Stichwort* „Arrow’s impossibility theorem“

**13. Sitzzuteilungsverfahren.** Nach einer Bundestagswahl wird anhand der abgegebenen Stimmen und mit Hilfe eines Auszählverfahrens eine Sitzverteilung für das Parlament festgelegt. Mittlerweile ist seit Gründung der Bundesrepublik das dritte solche Verfahren in Kraft. In diesem Vortrag soll auf den Unterschied zwischen Divisor- und Quotenverfahren eingegangen werden, sowie auf den Unmöglichkeitssatz von Balinski und Young.

*Literatur:* [15], Stichworte „Sitzzuteilungsverfahren“, „Unmöglichkeitssatz von Balinski und Young“.

## 5. NAVIGATION UND KARTOGRAPHIE

**14. Das Global Positioning System.** Das vom amerikanischen Militär entwickelte GPS ist heute das am meisten verbreitete Satellitennavigationssystem. Dieser Vortrag soll die Funktionsweise des GPS erklären und auch beschreiben, wie in der Praxis die Positionen der Satelliten festgestellt werden, und wie der Empfänger aus den gemessenen Daten seine Position bestimmt.

*Literatur:* [16], [15] Stichwort: „Global Positioning System“

**15. Kartographie.** Da die Erde nicht flach ist, gibt es keine wirklich maßstabstreuen Karten. In diesem Vortrag soll zunächst die Mercatorprojektion (unter der Annahme, dass die Erde eine Kugel ist) und ihre Bedeutung für die Schifffahrt erklärt werden. Anschließend sollte auf modernere, verwandte Kartensysteme (Gauß-Krüger und UTM) eingegangen werden.

*Literatur:* [15], Stichwort: Gauß-Krüger-Koordinaten, [16], Stichworte: Mercator projection, UTM

**16. Algorithmen zur Routenplanung.** Bei der Routenplanung geht es darum, einen optimalen Weg zwischen einem Start und einem Zielort zu finden. Dabei hängt der Begriff „optimal“ im Allgemeinen von verschiedenen Parametern ab, z.B. versucht man einen Weg unter Zeitminimierung, Kostenminimierung sowie über bestimmte Zwischenorte zu realisieren. Mathematisch wird dieses Problem mit Hilfe der Graphentheorie betrachtet. Eine optimale Lösung kann man dann mit Hilfe des Dijkstra-Algorithmus bestimmen.

*Literatur:* [1]

## 6. GEOMETRIE IM ALLTAG

**17. Knoten.** Knoten finden in der Praxis vielseitig Anwendung. Deshalb ist das Knüpfen bestimmter Knoten auch eine der Prüfungsleistungen bei der Segel-, Kletterausbildung, bei der Feuerwehr und beim THW. In der Mathematik ist die Knotentheorie ein Teilgebiet der Topologie. Mit Hilfe der Physik kann man aber auch mathematisch erklären, ob ein bestimmter Knoten einfach lösbar ist, oder wie gut ein Knoten hält. Im Vortrag soll eine Einführung in die Knotentheorie gegeben werden.

*Literatur:* [1], [8], [9]

**18. Kugelpackungen.** Das Ziel einer dichtesten Kugelpackung besteht darin, möglichst viele gleichartige Kugeln in ein gegebenes Volumen zu packen. Dabei gibt es aber zwei verschiedene Problemstellungen: die Anzahl der Kugeln ist „klein“ oder die Anzahl der Kugeln ist sehr groß (bzw. unendlich). In Dimension  $n = 3$  ist bei einer Anzahl von weniger als 56 Kugeln die Wurstpackung optimal (obwohl im Alltag meistens unpraktisch). Im Vortrag geht es darum, optimale Packungen mit sehr großer beziehungsweise unendlicher Stückzahl in Dimension  $n = 2$  und  $n = 3$  zu betrachten.

*Literatur:* [1]

**19. Gelenke.** Auch in mechanischen Gelenkmechanismen steckt Mathematik. James Watt konstruierte für seine Dampfmaschine einen Mechanismus, der eine pendelnde Kreisbewegung näherungsweise in eine geradlinige Auf- und Abbewegung überführt. Erst knapp hundert Jahre später wurde das Problem exakt von Peaucellier gelöst.

*Literatur:* [6], [13],[3]

**20. Planetenbewegung.** Der Ursprung der Infinitesimalrechnung ist eng verknüpft mit Newton's Erkenntnis, daß sich die Kepler'schen Gesetze der Planetenbewegung herleiten lassen aus Newton's Gesetz "Kraft=Masse×Beschleunigung" zusammen mit dem Gesetz, daß die Gravitationskraft umgekehrt proportional ist zum Quadrat des Abstands. Das soll für Studierende ohne zweites Fach Physik erklärt werden, also wohl am besten von einem Studierenden, dessen zweites Fach nicht Physik ist.

*Literatur:* [12], 1.1-1.3

*Vorkenntnisse:* Analysis II.

## 7. ANDERE THEMEN

**21. Kernspin-Tomographie.** In einem Kernspin-Tomographen werden bestimmte Atomkerne (meist Wasserstoffatomkerne) im menschlichen Körper durch Magnetfelder angeregt. Die Messung der elektro-magnetischen Felder, welche die angeregten Atome erzeugen, läßt sich mathematisch als die Radon-Transformierte der Dichtefunktion der Atome interpretieren. Um ein inneres Bild des Körpers zu erstellen, muss man also die Radon-Transformation invertieren.

*Literatur:* [4], Kapitel 1.7, 2.2, 5.3 [15], Stichwort: Magnetresonanztomographie [16], Stichworte: nuclear magnetic resonance, magnetic resonance imaging

*Vorkenntnisse:* Analysis III.

**22. Röntgenkristallographie.** In der Röntgenkristallographie schießt man Röntgenstrahlen auf ein Kristallgitter. Die Wellenlänge der Röntgenstrahlen ist kurz genug, um ein Beugungsmuster zu erzeugen, wenn sie in der Probe gestreut werden. Man benutzt das Muster und die Intensität der Streuung, um mithilfe der Fourier-Transformation die Elektronendichte für den Kristall zu bestimmen.

*Literatur:* [16], Stichwort: X-ray crystallography, [7], [2]

*Vorkenntnisse:* Analysis III.

**23. Benford's Gesetz.** Bei den Zahlen einer Steuererklärung treten typischerweise die ersten Ziffern nicht alle mit derselben Häufigkeit auf. Ähnliches gilt auch in anderen Zusammenhängen. Diese Erfahrung soll diskutiert und begründet werden. Sie wird eingesetzt, um Betrügereien auf die Spur zu kommen.

*Literatur:* : <http://www.educ.ethz.ch/unt/um/mathe/ana/benford>

*Vorkenntnisse:* Analysis I, etwas Analysis III.

## LITERATUR

- [1] M. Aigner, E. Behrends (Hrsg.), Alles Mathematik — von Pythagoras zum CD-Player, Vieweg, 2000

- [2] A. Authier, *Dynamical theory of X-ray diffraction*, International Union of Crystallography Monographs on Crystallography No. 11. Pp. xviii + 661, Oxford: Oxford University Press, 2001
- [3] H.S.M. Coxeter, *Introduction to Geometry*, Wiley, 1969
- [4] S. Deans, *The Radon Transform and some of its Applications*, Krieger, 1993
- [5] M. Dresher, *The Mathematics of Games of Strategy*, Dover Publications, 1981
- [6] D. Hilbert, S. Cohn-Vossen, *Anschauliche Geometrie*, Wiss. Buchgesellschaft, 1973
- [7] M. v. Laue: *Röntgenstrahlinterferenzen*. Akademische Verlagsanstalt, 1960.
- [8] C. Livingston, *Knot theory*, MAA, 1993
- [9] L.H. Kauffman, *Knoten*, Spektrum, 1995
- [10] P. Morris, *Introduction to Game Theory*, Springer 1994
- [11] J. F. Nash, *Non-cooperative games*, Ann. Math. 54 (1951), 286–295
- [12] H. R. Petry, B. C. Metsch, *Theoretische Mechanik*, Oldenbourg 2005
- [13] H. Rademacher, O. Toeplitz, *Von Zahlen und Figuren*, Springer 1968
- [14] R.-H. Schulze, *Codierungstheorie*, Vieweg 2003
- [15] Wikipedia, *Die freie Enzyklopädie*, Wikimedia foundation, <http://de.wikipedia.org/>
- [16] Wikipedia: *The free Encyclopedia*, Wikimedia foundation, <http://en.wikipedia.org/>  
Cambridge University Press 1995