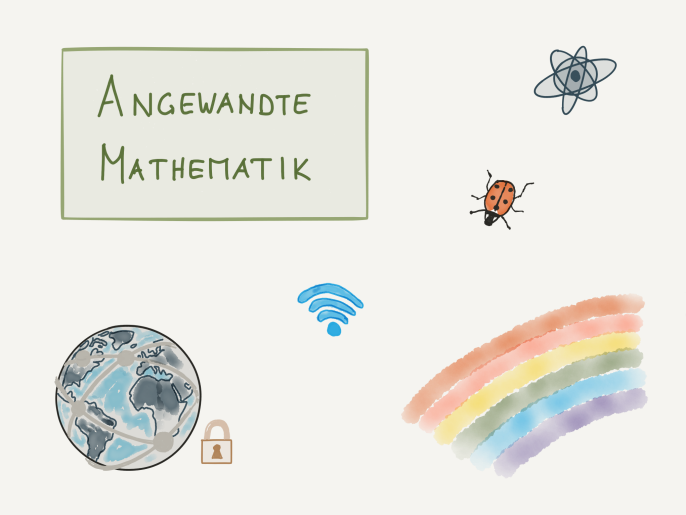


Protokoll einer SF Klasse

A 3000y Journey from the Greeks to Erwin Schroedinger

Jorma Wassmer

24. Januar 2020

Inhaltsverzeichnis

1 Getting Started

Please fasten your seatbelt!

- Natürliche Zahlen
$$\mathbb{N} = \{1, 2, 3, \dots\}$$
- Axiomatisierung von $\mathbb{N}$ (Text: Wozu in aller Welt Axiome?)
  - Axiome von Peano (mit „Induktionsaxiom“)
  - von Neumann ($\mathbb{N}_0$ via Mengen/Kardinalität)
- Primzahlen
$$\mathbb{P} = \{2, 3, 5, 7, 11, \dots\}$$
(Text: Gibt es eine mathematische DIN-Norm)
- Eindeutigkeit der Primfaktorzerlegung in $\mathbb{N} \setminus \{1\}$ (DNA von $n \in \mathbb{N} \setminus \{1\}$)
- ggT und kgV
  - Primfaktorzerlegung als Hilfsmittel zur Bestimmung von ggT und kgV
  - **Euklid'scher Algorithmus** zur Bestimmung des ggT

2 Ahh, the Primes

The Primes: like!

- Primzahlen spielen eine wichtige Rolle in der modernen Gesellschaft, nämlich bei der Verschlüsselung elektronischer Daten. (vgl. `MINT, dCulture`)
- Es gibt unendlich viele Primzahlen.
- Es gibt genug k-stellige Primzahlen. Die Anzahl Primzahlen bis zur Zahl $x \in \mathbb{N}\setminus\{1\}$ wird gut durch
$$\frac{x}{\ln(x)}$$
approximiert; und wird mit wachsendem x besser. (Text: Eine Million Dollar Belohnung: Wie sind die Primzahlen verteilt?)
- Verteilung der Primzahlen: The primes look random, but aren't.

Für jede natürliche Zahl kann überprüft werden, ob sie prim ist oder nicht (einfach Faktoren suchen); deterministisch. Die Verteilung der Primes auf dem Zahlenstrahl genügt aber jedem statistischen Test für randomness!

- Primzahlzwillinge, Primzahldrilling
- Indirekte und direkte Beweise (z.B. Übungen **4**,5,**9**,12,13,14)
- Lustiges:
  - Goldbach'sche Vermutung:

    Jede gerade natürliche Zahl grösser 3 lässt sich als Summe zweier Primzahlen schreiben.

    Der geneigte Leser googelt VINOGRADOV.
  - Primzahllücken (Übung 10)
  - Primzahlen in der Biologie (Übung 11)

3 Be Rational, Get Real

Viel „Handwaving"; wir können leider (noch) nicht alles beweisen.

- Rationale Zahlen
  - Definition
    $$\mathbb{Q} = \left\{ \frac{a}{b} \mid a \in \mathbb{Z}, b \in \mathbb{N} \right\}$$
  - Dezimaldarstellung abbrechend (Nenner hat Primfaktorzerlegung $2^n \cdot 5^m$) oder periodisch (Übungen 2 und 3)
  - Transformation Bruch $\leftrightarrow$ Dezimalzahl
  - Eine Menge $\mathbb{M}$ heisst **abzählbar unendlich**, wenn es eine Bijektion $f : \mathbb{N} \longrightarrow \mathbb{M}$ gibt.
  - $|\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}|$ (Text: Gross, grösser, am grössten)
  - $\mathbb{Q}$ hat „Löcher"
- Reelle Zahlen

  - irrational: Dezimaldarstellung ist nichtabbrechend und aperiodisch
  - $\mathbb{R}$ ist **überabzählbar unendlich**
  - Weiteres Musterbeispiel für einen indirekten Beweis (via Eindeutigkeit der Primfaktorzerlegung in $\mathbb{N} \setminus \{1\}$): $\sqrt{p} \notin \mathbb{Q}$ für p prim
  - Klassifikation **algebraisch** ($\sqrt{p}, \dots$) und **transzendent** ($\pi, e, \dots$) (Text: In der Mathematik gibt es Transzendenz, doch mit Mystik hat das nichts zu tun)
- Zahlensysteme
  - Additions- und Positionssysteme
  - Dezimalsystem: Basis 10, Ziffern: $0, 1, 2, \dots, 9$
  - allgemein: System zur Basis b: $a_n \cdot b^n + a_{n-1} \cdot b^{n-1} + \dots + a_1 \cdot b + a_0 \cdot b^0$
  - Komma trennt Übergang zu negativen Exponenten (Übung 15)
  - **Binärsystem** (computing): Basis 2, Ziffern: $0, 1$ (Übungen 13 und 14)
  - **Hexadezimalsystem**: Basis $16 = 2^4$, Ziffern: $0, 1, 2, \dots, 9, A, B, C, D, E, F$
  - Transformation binär $\leftrightarrow$ hexadezimal (Übung 28)

4 Digital Natives

Please, be up to date ...

- Computing (Übungen **16**,17,18,19)
  - *Bi*nary digi*t*, **Bit**: 2 Zustände (0 und 1)
  - 1 **Byte** $\sim$ 8 Bit: $2^8 = 256$ Zustände (00 bis FF, ASCII)
  - Schriftliche binäre Addition ($1 + 1 = 0$ behalte 1) (Text: Information optimal verpackt)
- **Nibbles** (4 Bit Blöcke) (Übung 20)
- Subtraktion definiert via Addition im Zyklus mit Vorzeichenbit
- Inverses Element: Element $\rightarrow$ Flip $\rightarrow$ Flip $+1 \rightarrow$ et voilˆ (Übungen 21,22,23,24,25)

5 Reminder Modulo

The good old times: Wie in der 4.ten Klasse ...

- Mathematische **Definition**:

$$a \equiv b \mod m \quad :\Leftrightarrow \quad a - b = k \cdot m$$

  für ein $k \in \mathbb{Z}$

- Eine **Äquivalenzrelation** $\sim$ auf einer Menge $\mathbb{M}$ ist eine Relation — und damit eine Teilmenge von $\mathbb{M} \times \mathbb{M}$ (Fragen bitte direkt an CŽline) —, welche folgende Bedingungen ($\forall a, b, c \in \mathbb{M}$) erfüllt:
  - Reflexivität: $a \sim a$
  - Symmetrie: $a \sim b \;\Rightarrow\; b \sim a$
  - Transitivität: $a \sim b$ und $b \sim c \;\Rightarrow\; a \sim c$
- Modulare Äquivalenz, $\equiv$, ist eine Äquivalenzrelation. Daher impliziert ein Modul m ebensoviele Äquivalenzklassen (**Restklassen** $0, \ldots, m-1$).
- Musterbeispiel für Beweis via Definition: Modulare Äquivalenz ist eine quivalenzrelation.
- Beim Umformen kann $\equiv$, bis auf Division, als Gleichheitszeichen aufgefasst werden. (Übung 1)
- Addition und Multiplikation modular kann separat ausgeführt werden. (Übung 1)
- Teilbarkeitsregeln für 3 und 11 im Dezimalsystem.
- Musterbeispiel für Beweis mit Rechenregeln: Teilbarkeit mit 3 und 11 dezimal (Übung 1)
- Eine **Gruppe** ist eine Menge $\mathbb{G}$ zusammen mit einer zweistelligen Verknüpfung

$$* : \mathbb{G} \times \mathbb{G} \to \mathbb{G} \quad \text{(Abgeschlossenheit)}$$

  so, dass folgende Axiome — für $a, b, c \in \mathbb{G}$ — erfüllt sind:
  - Assoziativität: $(a * b) * c = a * (b * c)$
  - Neutrales Element: $\exists\, e \in \mathbb{G}$ mit $a * e = e * a = a \quad \forall a \in \mathbb{G}$
  - Inverse Elemente: $\forall a \in \mathbb{G}\ \exists\, a^{-1} \in \mathbb{G}$, so dass $a * a^{-1} = a^{-1} * a = e$

- $(\mathbb{Z}_p^*, \cdot)$ mit p prim, die Menge aller Restklassen Modulo p ohne 0 mit Multiplikation, ist eine Gruppe. (Übungen 2 und 3)

6 On Groups and Checksums

Niemand hat eine Ahnung von Gruppen; oder \ignore Wassmer...

- erneut: Begriff der Gruppe
- **Verknüpfungstafeln** für ausgewählte $\mathbb{Z}_k^*$ mit Multiplikation erstellt
- Wichtigkeit der Gruppen
$$(\mathbb{Z}_p^*, \cdot)$$
mit p prim erkannt. Finde Beispiele und Übungen online.
- **Primitivwurzel/Erzeuger** zyklischer Gruppen definiert
- Kernidee moderner Verschlüsselung anhand $(\mathbb{Z}_{17}^*, \cdot)$ gesehen. (Übungen 2,3 & 4)
- übliche **Notation für Summen** mit
$$\Sigma$$
eingeführt
- Kernidee der **Prüfziffer**/Checksum anhand der alten ISBN-Nummer $a_1 a_2 \dots a_{10}$
$$\text{check digit: } a_{10} \equiv \sum_{k=1}^{9} k \cdot a_k \mod 11$$
verstanden
- Beweis „Erkennung eines Vertippers“ angeschaut. (Übung 4) Wichtigkeit des Primzahlmoduls erkannt.
- selbständiges Einsehen der „Erkennung eines Zahlendrehers“ (Übung 5)

7 Mathemaniacs

Erste Schritte in Mathematica...

- Wichtige Grundlagen in Mathematica
  - Mathematica ist case-sensitiv
  - vorhandene Funktionen beginnen mit Capital
  - Hilfe via Google und/oder „?“
  - Unterschied von **Zuweisung** („=“), **logischer Gleichheit** („==“) und **definitorischer Gleichheit** („:=“) eingesehen
  - selbstgebastelte Funktionen mit `Module` erstellt
    - `barcode`: Input erste 9 Ziffern alte ISBN und Output check digit
    - `checkISBN`: Input alte ISBN und Output True für korrekte Eingabe bzw. False für inkorrekte Eingabe auf Basis Auswertung der check digit
    - `osternGauss`: Input jahr und Output Datum Ostern für jahr
- Wichtigkeit von Kommentaren in Dokumenten/Programmen gepredigt
- `If-Then-Else`-Verzweigung verwendet (vgl. TR Programm `QuadrGl`)
- Begriffe **Syntax** und **Semantik** erwähnt

8 Caesar Cipher

Endlich Kryptologie... Übrigens, im Aquarium ist Mathematica installiert...

- **Kryptologie**: **Kryptographie** (Algorithmen) und Kryptoanalyse (knacken)
- Wichtige, aktuelle Anwendungen:
  - authentification
  - secrecy
  - integrity
  - liability
- **Brute Force**: Versuch zu knacken durch Ausprobieren aller möglichen Schlüssel
- Wir erwähnen Steganographie.

- Transpositionschiffre, bekannt als **Caesar Cipher** (26 Schlüssel):

  Verschiebung des Alphabets um t. Caesar Cipher ohne Angabe bedeutet $t = 3$.

- **Substitutionschiffre** (26! Schlüssel):

  Jedem Buchstaben des Klartext-Alphabets wird eindeutig ein Buchstabe des Cipher-Alphabets zugeordnet (bijektiv).

- Mathematica Fortsetzung:

  - **Datentypen** `Int`, `Char`, `String`, `List`
  - Weitere nützliche Funktionen: `ToCharacterCode`, `FromCharacterCode`
  - Module
    - `transEncode`[String *message*, Int *transposition*, Char *outputfilename*]
    - `transDecode`[Int *transposition*, Char *inputfilename*]

      en- bzw. decoden eine *message* mit Transposition *transposition* und legen eine Datei *outputfilename*.dat mit der cipher im aktuellen Notebookverzeichnis an bzw. lesen den Inhalt der Datei *inputfilename*.dat und returnen die message.

  bereitgestellt und ausprobiert.

9 Recap to Showdown

Get familiar with...

- Axiomatisierungen von $\mathbb{N}$ durchgedacht
- Euklid'scher Algorithmus inklusive Beweis nachvollzogen
- Primzahlen: Primzahlzwilling, Eindeutigkeit der Primfaktorzerlegung kennen
- Dezimaldarstellung von Elementen in $\mathbb{Q}$ und $\mathbb{R}$, Abzählbarkeit, algebraische Zahlen kennen
- Zahlensysteme, insbesondere $2, 10$ und 16 beherrschen.
- Begriff des Bytes und Umrechnungen binär $\leftrightarrow$ hexadezimal können

- Modulo: Rechenregeln beherrschen
- Begriff der Äquivalenzrelation mit induzierten Äquivalenzklassen kennen; insbesondere im Zusammenhang mit Modulo (Restklassen)
- Konzept des indirekten Beweises verstanden
- Gruppen beherrschen! Insbesondere die Gruppen $(\mathbb{Z}_p^*, \cdot)$
- Teilbarkeitsregeln und check sums verstanden

10 Friday the 13th

Fragen zu Zahlen, Gruppen und Modulo...

- Ferner Mathematica für die nächste Session auffrischen (siehe letzte und vorletzte Woche):
  - Module `transEncode[]` und `transDecode[]` lesen und anwenden können.
  - Sich mit dem Gedanken befassen, selber Module formulieren zu können. (Beispielsweise: Habe ich die Ostern nach Gauss bereits als Modul umgesetzt? Oder, kann ich jede Zeile im Modul `checkISBN[]` kommentieren/sprachlich ausformulieren?)

11 Now We Know

Antworten zu Zahlen, Gruppen und Modulo...

- Quintessenz aus der Prüfung:
  - **Quartastoff** wird vorausgesetzt.
  - Die **Skripts** werden sorgfältig gelesen; im Unterricht werden eventuell nicht alle Themen aus den ausgehändigten Dokumenten angesprochen.
  - Tauchen im Skript oder anderswo (Protokoll, Unterricht, ...) unbekannte Zeichen auf ($\exists$, $\forall$, ...), so werden diese selbstverständlich nachgeschlagen.
  - Haben Sie einen Satz oder einen Beweis nicht *vollständig* verstanden, so darf er nicht ad acta gelegt werden.

- Kreativität ist gerne gesehen, jedoch haben die Fragestellungen bzw. die Aufträge Priorität.
- Die Aufgabe wird sorgfältig gelesen.
- Es kann vorkommen, dass Sie mit etwas „Unbekanntem“ konfrontiert werden.

- Wir erweitern unseren **Caesar binär**. Das bringt erneut einige Mathematica-Funktionen mit sich.

12 403291461126605635584000000 keys? No problem...

PAMler are so good in patterns...

- Knacken monoalphabetisch verschlüsselter Texte
  - Kern: Buchstabenhäufigkeiten bleiben bei monoalphabetischer Verschlüsselung erhalten.
  - Im Deutschen ist `e` der häufigste Buchstabe; finde den Repräsentanten von `e`.
  - Weitere häufige Buchstaben (`ernstl`) können dann unter Einbezug häufiger n-gramme — im Allgemeinen — rasch zugeordnet werden.
- Mathematisches Hilfsmittel zur Sprachanalyse
  - Definition **Koinzidenzindex** κ

$$\kappa(T_x, T_y) = \sum_{i=1}^{n} \frac{\delta(x_i, y_i)}{n} \quad \text{mit} \quad \delta(x_i, y_i) = \begin{cases} 1 & \text{für } x_i = y_i \\ 0 & \text{für } x_i \neq y_i \end{cases}$$

  - In guter Näherung gilt

$$\kappa = \frac{\sum_{i=1}^{26} n_i^2}{n(n-1)}$$

  - Kunstsprache (laaanger Text, keine charakteristischen Häufigkeiten)

$$\kappa(T_x, T_y) = \frac{1}{26} \approx 3.85\%$$

13 Vigenère-Cipher? No problem...

PAMler are sooo good in patterns...

- Verschlüsselung eines Textes mit einem Schlüsselwort und dem **Vigenère-Quadrat**.
- Crash-Course Wahrscheinlichkeit:
  - Laplace: „günstig“ durch „möglich“
  - Gegenwahrscheinlichkeit: $P(\overline{A}) = 1 - P(A)$
  - Prozesse: oder $\sim +$, und $\sim \cdot$
- Knacken der polyalphabetischen Vigenère-Verschlüsselung mit Kasiski und Friedmann.
  - **Kasiski** guckt nach wiederholten Patterns und sucht den ggT ihrer Abstände. Es gilt, dass die Länge des verwendeten Schlüsselworts ein Vielfaches dieses Abstandes ist.
  - **Friedmann** gibt eine Abschätzung der Schlüsselwortlänge nach oben unter Verwendung des Koinzidenzindex der Sprache (message) und des Geheimtextes (cipher):

$$n \leq \frac{\kappa_m - 3.85}{\kappa_c - 3.85}$$

  - Ist die vermutete Schlüsselwortlänge n, wird der Text kanonisch in n Teiltexte unterteilt, die nun monoalphabetisch mit einer Transposition verschlüsselt sind. Man sucht in jedem der Teiltexte das „`e`“, woraus unmittelbar der Shift folgt, und findet so das Schlüsselwort.

14 Vigenère Up- & Reloaded

Point of no return, soon...

- Herleitung der Friedmann Abschätzung lückenlos nachvollzogen.
- Erkannt, dass im PAM eine Aussage wie „lückenlos nachvollzogen“ ein Pleonasmus ist.
- Die Bedeutung der Wörter wie „verstanden“, „erkannt“, „nachvollzogen“ etc. verstanden.
- Repetitionslustige orientieren sich bitte am Protokoll und an den Prüfungsaufgaben.

15 Kasiski & Friedmann by hand

Vigenère, Kasiski & Friedmann... ✓

- Eingesehen, dass ein Spickzettel nicht eine SF Prüfung zu lösen vermag. Insbesondere nicht, wenn er am Vorabend der Prüfung geschrieben wurde.
- Vigenère abgeschlossen.

16 Mathematical Induction

De- and Induction...

- **Vollständige Induktion** als Beweismethode auf Aussagen, welche mit natürlichen Zahlen formuliert werden, anwenden können.
- Basis der vollständigen Induktion bildet das Induktionsaxiom von Peano. Die Durchführung kann in die drei Schritte
  (a) **Verankerung** (häufig $n = 1$)
  (b) **Schritt** ($n \to n + 1$)
  (c) Schluss

  aufgeteilt werden. (Übungen 2, **3**, 4, **5**)
- Nebenprodukte **Pascal-Dreieck** und „**Gauss-Trick**“ aufgesogen.

17 Enigma

$\alpha\iota\nu\iota\gamma\mu\alpha$

- Innenleben
  - 3 Walzen (aus 5)
  - 1 Reflektor (aus 2)
  - Steckbrett (mit maximal 13 Verbindungen)

- Breaking
  - Idee: die Polen Jerzy Rozycki und Henryk Zygalski finden einen Zusammenhang zwischen Cipher und Walzenlagen/-stellungen.
  - Tagesschlüsselsuche: Alan Turing im Bletchley Park mit dem „ersten“ Computer, der **Turing-Bombe**
  - Wichtig für die Schlüsselsuche durch eine Bombe ist es, wahrscheinliche Wörter des Ciphertexteszu erraten.

18 The Imitation Game

The Godfather of Computer Sciences... Alan Turing

19 From Unthinkable to Imaginary

Gauss is everywhere...

Formel von Tartaglia/Cardano zur Lösung von $ax^3 + bx^2 + cx + d = 0$:

- Dividiert man durch a und setzt man $y := x + \frac{b}{3a}$, so entsteht die Gleichung „Fior'schen Typs“
$$y^3 + 3py + 2q = 0$$
mit $3p = \frac{3ac-b^2}{3a^2}$ und $2q = \frac{2b^3}{27a^3} - \frac{bc}{3a^2} + \frac{d}{a}$.
- Die Anzahl der (reellen) Lösungen hängt vom Vorzeichen der Diskrimante $D := q^2 + p^3$ ab.
  - Ist $D > 0$, so hat die Gleichung eine reelle Lösung.
  - Ist $D < 0$, so hat die Gleichung drei verschiedene reelle Lösungen.
  - Für $D = 0$ hat die Gleichung die Lösung $y_1 = y_2 = y_3 = 0$, falls $p = 0 = q$ und zwei Lösungen, falls $q^2 = -p^3 \neq 0$.
- Die Lösungen sind $y_1 = u + v$, $y_2 = f_1u + f_2v$, $y_3 = f_2u + f_1v$, wobei $u = \sqrt[3]{-q + \sqrt{D}}$, $v = \sqrt[3]{-q - \sqrt{D}}$, und f_1 und f_2 die Lösungen der Gleichung $f^2 + f + 1 = 0$ sind, d.h. $f_{1,2} = 0.5(-1 \pm i\sqrt{3})$.

i heisst **imaginäre Einheit** und entspricht der Interpretation $i \sim \sqrt{-1}$. ein Fundament unserer heutigen Kultur mit zahllosen Anwendungen — folgt in Kürze.

- Es ist
$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$$
$\mathbb{C}$ ist ein sogenannter **algebraischer Abschluss** von $\mathbb{R}$.

- Erwähnt sei noch die schönste Formel der Welt:
$$e^{i\pi} + 1 = 0$$

- Übrigens:
  - Heute weiss man, dass für eine polynomiale Gleichung vom Grad 5 oder höher keine geschlossene Lösungsformel angegeben werden kann (bewiesen mit Gruppentheorie).
  - Cardano fand auch noch Lösungen für polynomiale Gleichungen vierten Grades...

20 Complex Numbers Are Easy to Handle

$\sqrt{-1} = i$ für den Laien...

- Definition der **imaginären Einheit** i via $i^2 = -1$. (Permanenzprinzip)

  In diesem Zusammenhang wird die Termumformung
$$-1 = i^2 = i \cdot i = \sqrt{-1} \cdot \sqrt{-1} = \sqrt{(-1) \cdot (-1)} = \sqrt{1} = 1 \quad ?!$$
  kritisch beäugt.

- **Imaginäre Zahl**: $i \cdot b$ mit $b \in \mathbb{R} \setminus \{0\}$

- **Komplexe Zahl**: $a + i \cdot b$ mit $a, b \in \mathbb{R}$. a heisst **Realteil**, b heisst **Imaginärteil**. Eine komplexe Zahl kann als Punkt in der Ebene — der sogenannten komplexen Ebene — aufgefasst werden.

- **Addition und Subtraktion** von komplexen Zahlen werden kanonisch definiert. D.h. rechne mit komplexen Zahlen wie mit reellen, aber unter der Voraussetzung, dass i ein Parameter ist, für den $i^2 = -1$ gilt.

- Wichtig — mit Blick auf die Physik und im Hinblick auf mathematische Modellierung — ist die **geometrische Interpretation der Addition** als „nacheinander

ausführen von Verschiebungen“; anders: „aneinander hängen von Pfeilen (Vektoren)“. Der Spielplatz ist ein 2D-Koordinatensystem, in dem die Achsen reell (Re) und imaginär (Im) heissen.

- Die Subtraktion kann auf die Addition mit inversem Element zurückgeführt werden:

$$z_1 - z_2 := z_1 + (-z_2)$$

- Schliesslich wird noch die Darstellung von $\sqrt{i}$ als komplexe Zahl, $a + ib$, gesucht. Alle finden $\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i =: z_1$, ✓. Niemand bemerkt, dass die Berechnung auch $-\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i =: z_2$ liefert....

  Fragen: Wieso ergeben sich rechnerisch die beiden Lösungen z_1 *und* z_2? Welche Lösungen kriegst du mit geometrischen Überlegungen? Und, wieso bevorzugt man z_1 als Darstellung von $\sqrt{i}$?

21 Complex Numbers Are Still Easy to Handle

$i^2 = -1$ for pros...

- Das **komplex Konjugierte** einer Zahl $z = a + ib$ ist

$$\bar{z} = a - ib,$$

  also ein Vorzeichenwechsel des Imaginärteils, und entspricht geometrisch einer Spiegelung an der reellen Achse.

- **Multiplikation** mit komplexen Zahlen ist nichts Neues. Bei der **Division** erweitert man den Quotienten mit dem komplex konjugierten des Divisors und vereinfacht.

- Unter dem **Betrag** $|z|$ einer komplexen Zahl $z = a + ib$ verstehen wir den Abstand vom Punkt $z = (a \,|\, b)$ zum Ursprung (Länge des Vektors). Nach Pythagoras haben wir

$$|z| = \sqrt{a^2 + b^2}.$$

- Den Winkel α zwischen dem Vektor z und der reellen Achse nennt man **Argument** von z. Er berechnet sich grundsätzlich durch

$$\alpha = \tan^{-1}\left(\frac{\mathrm{Im}\,(z)}{\mathrm{Re}\,(z)}\right)$$

- **Geometrisch** interpretiert man die Multiplikation zweier komplexer Zahlen als Addition der Argumente und Multiplikation der Beträge. Bei der Division werden entsprechen Argumente subtrahiert und Beträge dividiert.

- Quadratische Gleichungen — auch mit komplexen Koeffizienten — können wie bis anhin mit der Lösungsformel für quadratische Gleichungen gelöst werden.

22 On the Geometry of Complex Number Equations including Absolute Values

Saga like: „Separate the imaginary from the real and thou shall see ...“

- Wir beschäftigen uns mit der geometrischen Interpretation von Betragsgleichungen, welche komplexe Zahlen beinhalten, und bemerken, dass es manchmal hilfreich ist diese Betragsgleichungen umzuschreiben und/oder die komplexen Zahlen auszuschreiben: $z = a + ib$.

- Aus unseren Überlegungen folgt, dass wir einen Kreis mit Mittelpunkt M und Radius r in der komplexen Ebene wie folgt beschreiben können: Er ist die Menge aller $z \in \mathbb{C}$, welche
$$|z - M| = r$$
erfüllen.

- Quintessenz: Wer Algebra kann ist geometrisch im Vorteil.

23 Almighty e^x

Feed imaginary numbers in there, suddenly waves are coming out!

- Betrachtet man einen beliebigen Punkt $z = a + i \cdot b \in \mathbb{C}$, so stellt man fest, dass z auch über einen Abstand r vom Ursprung und einen Winkel φ (zwischen Pfeil und reeller Achse) angegeben werden kann. Wir notieren ohne Begründung dieses
$$z =: r \cdot e^{i \cdot \varphi}.$$
Diese Darstellung heisst **Polarform**.

- Wir werden sehen, dass e tatsächlich die Euler'sche Zahl ist.

- Mit Pythagoras und den trigonometrischen Funktionen sieht man leicht, wie man die kartesische Form $a + i \cdot b$ als Polarform $r \cdot e^{i \cdot \varphi}$ formuliert; und viceversa.

$a + i \cdot b \to$ polar

$$r = \sqrt{a^2 + b^2} \quad \text{und} \quad \varphi = \arctan\left(\frac{b}{a}\right)$$

$r \cdot e^{i\varphi} \to$ kartesisch

$$a = r \cdot \cos(\varphi) \quad \text{und} \quad b = r \cdot \sin(\varphi)$$

- Dadurch kriegen wir einen höchst interessanten Zusammenhang bzw. eine wunderschöne Interpretation von $e^{i\cdot\varphi}$. Denn man findet unmittelbar

  $$e^{i\cdot\varphi} = \cos(\varphi) + i \cdot \sin(\varphi)$$

  Also ist $e^{i\varphi}$ ein **Einheitszeiger**, denn

  $$\left|e^{i\varphi}\right| = \sqrt{\sin^2(\varphi) + \cos^2(\varphi)} = \sqrt{1} = 1 \quad \forall\varphi \in \mathbb{R}.$$

- Anders geschwärmt: Die Funktion e^x mit $x \in \mathbb{R}$ ist eine schöne Exponentialfunktion mit super Eigenschaften, von denen du bald mehr kennen lernen wirst. Faszinierend ist auch, dass e^{ix} eine schöne Wellenfunktion ist.

- Die Multiplikation von komplexen Zahlen, sagen wir z_1 und z_2, ist in Polarform einfach, denn wir haben Permanenz:

  $$z_1 \cdot z_2 = r_1 e^{i\varphi_1} \cdot r_2 e^{i\varphi_2} = r_1 r_2 e^{i(\varphi_1+\varphi_2)}$$

  Deshalb dividiert man analog.

- Wir wollen im Falle, dass wir Winkelfunktionen und e-Funktionen betrachten, stets das Bogenmass verwenden. (Begründung später)

- Ich formuliere jeweils überspitzt

  – „Es gibt nur eine Basis, und das ist e.“

  – „Es gibt nur einen Logarithmus, und das ist ln.“

  – „Es gibt nur ein Winkelmass, und das ist das Bogenmass.“

  Übrigens, wenn Sie in Mathematica `Log[x]` eintippen, dann wird $\ln(x)$ berechnet...

24 Symmetrische Verschlüsselung

sorry, forgot the security code...

- Allgemein zu Verschlüsselung → KERKHOFF

  > Die Sicherheit verschlüsselter Kommunikation darf nur vom verwendeten Schlüssel abhängen.

- Bei symmetrischen Verfahren sind die Schlüssel zum Ver- und Entschlüsseln gleich:

$$D_k(E_k(m)) = m$$

- Es gibt absolute Sicherheit → OneTimePad mit `XOR`
- `XOR`: binäre bitweise Addition ohne Rest

$\oplus$	0	1
0	0	1
1	1	0

- Beispiel IDEA, entworfen 1990 an der ETH Zürich, verwendet Gruppen mit den Operationen `XOR`, Addition $\mod (2^{16})$ und Multiplikation $\mod (2^{16}+1)$
- Beispiel DES, *Data Encryption Standard*, entworfen von IBM. Verschlüsselung erfolgt in Blöcken; die message wird ordentlich „durchgeschüttelt“.

25 RSA

Rivest, Shamir, Adleman

- Asymmetrische Verschlüsselung: Schlüssel zum Ver- und Entschlüsseln können verschieden sein.
- **RSA-Verschlüsselung**
  - Der **public key** hat zwei Komponenten: $(n \mid e)$.
    - n ist das Produkt zweier Primzahlen:

$$n = p \cdot q$$

      mit p, q random primes, die geheim gehalten werden.

* e ist fast beliebig wählbar. Wir definieren $r := (p-1)\cdot(q-1)$; dann muss

$$\mathrm{ggT}(e, r) = 1$$

erfüllt sein. (Sicherstellung der Existenz des Inversen d zu e Modulo r)

In der Praxis wählt man häufig, falls möglich, $e = 2^{16} + 1$, da durch diese Wahl e eine angenehme Binärdarstellung besitzt.

* Der public key wird öffentlich zugänglich gemacht, hence the name. Damit kann jeder messages m **verschlüsseln**, und zwar so:

$$c = m^e \mod n$$

– Der **private key** d bleibt geheim und dient dem Empfänger zum Entschlüsseln. d kann mit dem **erweiterten Euklid'schen Algorithmus** berechnet werden. Dazu muss man e und insbesondere r — also p und q — kennen. Wegen $\mathrm{ggT}(e, r) = 1$ wird der letzte nichttriviale Rest des Euklid'schen Algorithmus angewendet auf e und r gleich 1 sein. Danach stellt man den Rest 1 durch Substitution der vorangegangenen Reste als Linearkombination von e und r dar und liest d ab:

$$1 = x \cdot e + y \cdot r$$

mit $x, y \in \mathbb{Z}$. Offensichtlich ist nun $x = e^{-1} = d \mod r$.

– Mit meinem private key d kann nur ich mit $(n \mid e)$ verschlüsselte Nachrichten c **entschlüsseln**. Das geht so:

$$c^d \mod n = m$$

- Ein Angreifer kann dann Nachrichten knacken, wenn er n in seine Primfaktoren p und q zerlegen kann. Denn nur so kann er das Inverse Modulo $(p-1)(q-1)$ mit dem erweiterten Euklid'schen Algorithmus effizient berechnen. Die Sicherheit hängt also davon ab, dass man bis heute kein effizientes Verfahren zur Zerlegung einer Zahl in ihre Primfaktoren kennt.

- Es wurde die Frage gestellt, wieso man just zum Modul r das Inverse d von e sucht. Ein kleiner, unvollständiger Einblick gab
Satz 1 (Kleiner Fermat'scher Satz)**.** *Seien p prim und $a \in \mathbb{Z}$ mit* $\mathrm{ggT}(a, p) = 1$. *Dann gilt*

$$a^{p-1} \equiv 1 \mod p$$

Keine Bange, selbstverständlich werden wir allgemein beweisen, dass RSA funktioniert. Die dabei verwendeten Sätze, wie z.B. der kleine Fermat, werden wir ebenfalls verifizieren.

- Abschliessend ein Beispiel: Karo M. aus O. will mir eine Frage stellen, die sie aber gerne verschlüsselt übermitteln möchte. Ich sage unter der Bedingung zu, dass wir RSA verwenden...

  – Ich wähle zwei random primes $p = 17$ und $q = 23$ berechne $n = pq = 391$.

  – Als öffentlichen Exponenten wähle ich $e = 15$.

  – Zu diesem e will ich nun meinen private key d, der invers zu e modulo $(p-1)(q-1) = 352 =: r$ ist. Gibt es zu $e = 15$ ein Inverses Modulo $r = 352$? Die Antwort ist ja, weil nämlich $\mathrm{ggT}(e, r) = 1$ ist.

  – Jetzt berechne ich mein d mit dem erweiterten Euklid'schen Algorithmus

$$352 = 23 \cdot 15 + 7$$
$$15 = 2 \cdot 7 + 1$$

    der versprochene $\mathrm{ggT} = 1$ erscheint, den ich nun als Linearkombination des Moduls r und des öffentlichen Exponenten e dargestellt haben möchte, damit ich d ablesen kann. Also rückwärts Marsch

$$1 = 15 - 2 \cdot 7$$
$$1 = 15 - 2 \cdot (352 - 23 \cdot 15) = 15 - 2 \cdot 352 + 46 \cdot 15 = 47 \cdot 15 - 2 \cdot 352$$

    Da ja $e = 15$ und ich am Inversen d Modulo 352 interessiert bin, lese ich aus der letzten Gleichung $d = 47$ ab.

  – Ich gebe meinen public key $(n \,|\, e) = (391 \,|\, 15)$ öffentlich bekannt und Karo verschlüsselt damit die Frage: „Was ist eine Restklasse?“

  – Wegen des Moduls $n = 391$ beschliesst sie, buchstabenweise zu verschlüsseln (ASCII-Code 0-256). Wir betrachten nur den ersten Buchstaben, das `W`, was ASCII 87 dezimal entspricht.

  – Sie verschlüsselt

$$c = 87^{15} \mod 391 = 349$$

    und schickt mir 349...

  – Ich entschlüssle

$$m = 349^{47} \mod 391 = 87$$

    und erhalte `W`... und bin enttäuscht; solch eine Frage hätte man vor einem halben Jahr stellen müssen.

26 RSA Works

... dank einem 400-jährigen Satz aus der Zahlentheorie...

- Die **Euler'sche Φ-Funktion** einer Zahl $n \in \mathbb{N}$ ist die Anzahl teilerfremde Zahlen kleiner oder gleich n.

$$\Phi(n) := \text{card}(\{\, k \in \mathbb{N} \mid 1 \leq k \leq n, \text{ggT}(k,n) = 1 \,\})$$

- Ist p prim, dann gilt

$$\Phi(p) = p - 1$$

  was man durch einfaches Zählen beweist.

- Φ ist multiplikativ. Insbesondere gilt für p, q prim

$$\Phi(p \cdot q) = (p-1) \cdot (q-1)$$

  was man durch Zählen beweist.

- Der **Satz von Euler** sagt, dass für $\text{ggT}(a,n) = 1$ gilt

$$a^{\Phi(n)} \mod n \equiv 1$$

- Für den Beweis der Korrektheit von RSA reicht grundsätzlich der enger gefasste **Satz 2** (Kleiner Fermat'scher Satz)**.** *Seien p prim und $a \in \mathbb{Z}$. Dann gilt*

$$a^p \equiv a \mod p$$

  Eine Induktion über a für fixes p beweist die Aussage. Dabei taucht das Problem der Teilbarkeit von Koeffizienten der Form

$$\frac{p!}{k! \cdot (p-k)!} =: \binom{p}{k}$$

  mit $1 \leq k \leq p-1$ auf. Man kann einsehen, dass diese Koeffizienten allesamt Vielfache von p sind.

- Der Ausdruck $\binom{p}{k}$ heisst **Binomialkoeffizient** und man sagt „p tief k".

- Eine weitere Anwendung des Pascaldreiecks wird sichtbar:
  Bemerkung. Mit der Definition $0! := 1$ liefert das Pascaldreieck also die Werte der Binomialkoeffizienten.

- Damit ist der Beweis, dass tatsächlich für random primes p, q mit $e \cdot d \mod r = 1$ immer

$$m^{e \cdot d} \mod n = m$$

  gilt nur noch Formsache; RSA funktioniert!

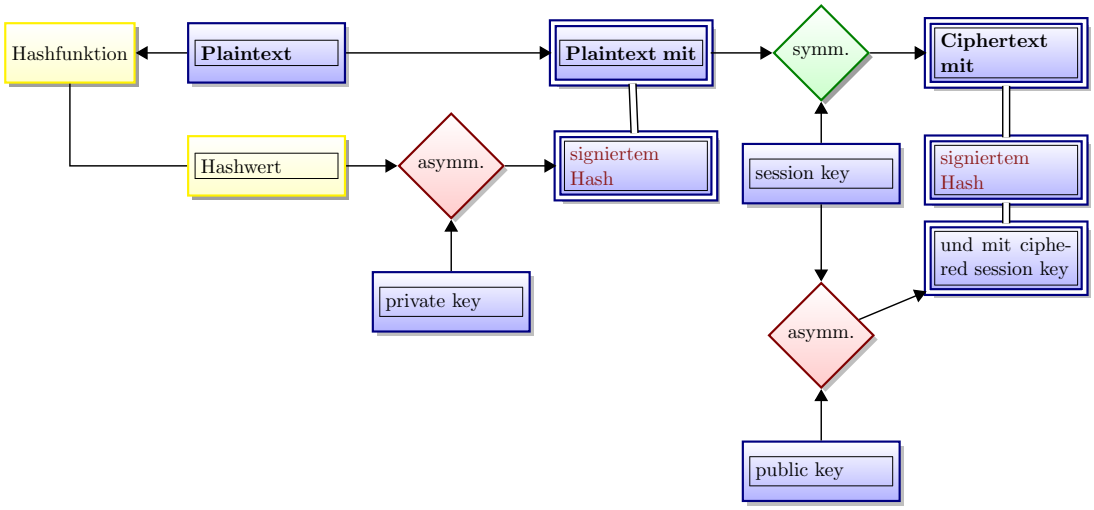


Abbildung 1: ciphered message mit signed hash ready to send

27 Sign the Hash

`...RSA` vice-versa

- Wir erkennen — vorzugsweise unter Einsicht eines Schemas wie Abbildung 1 auf Seite 27 — wie RSA, zusammen mit einer Hashfunktion, zum **Unterschreiben** und Überprüfen der **Integrität** einer message eingesetzt werden kann.
- **Hashfunktionen** sind vereinfacht gesagt Funktionen, die zu einem Input einen Output fester Länge liefern und sehr empfindlich auf Änderungen des Inputs reagieren. Bekannte Beispiele für unsere Zwecke sind die ISBN-Prüfziffer, MD5, SHAxx, CRC32 ...
- Wir basteln uns ein Beispiel, bei dem die Kommunikationspartner Zyril B. aus M. und SŽline H. aus M. das Prozedere durchspielen; mit dem Unterschied, dass der Text nicht symmetrisch, sondern RSA verschlüsselt wird. Als Prüfziffer wird der Barcode $\sum_k k \cdot a_k \mod 11$ verwendet. Die message soll dann mindestens zweistellig sein, da sonst die Prüfziffer nicht amüsant ist.
  - Zyril wählt $p = 17, q = 23, e_Z = 15$ und veröffentlicht $(n_Z \,|\, e_Z) = (391 \,|\, 15)$, hält sein $d_Z = 47$ geheim.
  - SŽline nimmt in ihrer Euphorie $p = 11, q = 19, e_S = 7$ und veröffentlicht $(n_S \,|\, e_S) = (209 \,|\, 7)$, hält ihr $d_S = 103$ geheim.
  - SŽline will die message `Lach` senden, signieren und integrieren und verschlüsselt

Buchstabe für Buchstabe des ASCII-Codes $\{76, 97, 99, 104\}$

– Sie verschlüsselt die message mit Zyrils public key

$$c = \{83, 180, 198, 128\}$$

berechnet den Hashwert für die message

$$\sum_k k \cdot a_k \mod 11 = 7$$

und unterschreibt diese checksum mit ihrem private key d_S

$$7^{103} \mod 209 = 178$$

Abschliessend schickt sie also die verschlüsselte message $\{83, 180, 198, 128\}$ und den unterschriebenen Hashwert 178 an Zyril.

– Zyril hat eine Nachricht erhalten und entschlüsselt $\{83, 180, 198, 128\}$ mit seinem private key 47 und erhält $\{76, 97, 99, 104\}$, was `Lach` bedeutet. Ist diese Nachricht wirklich von SŽline, und wurde diese Nachricht nicht manipuliert?

Zyril nimmt 178, entschlüsselt mit SŽlines public key $(209 \mid 7)$

$$178^7 \mod 209 = 7$$

und wendet die vereinbarte Hashfunktion auf `Lach` an, was ebenfalls 7 ergibt. Daraus kann er schliessen, dass die Nachricht mit an zu Sicherheit grenzender Wahrscheinlichkeit von SŽline stammt und nicht manipuliert worden ist.

28 Some Thoughts on RSA

. . . we can do better

- 4096 bit sind i.A. 1024 Hexadezimalstellen.
- Byteweise RSA-Verschlüsselung ist monoalphabetisch.
- Die Multiplikativität der Euler'schen Φ-Funktion haben wir nur für Primzahlen gezeigt.
- Ein Element von $\langle \mathbb{Z}_p^*, \cdot \rangle$ ist nicht automatisch Primitivwurzel.
- Ein Element $p-1$ von $\langle \mathbb{Z}_p^*, \cdot \rangle$ ist für $p > 3$ sicher keine Primitivwurzel, da $p-1 \equiv -1 \mod p$.
- Man definiert $0! = 1$.

29 RSA Simulation mit Mathematica

Illidan Stormrage: „You are not prepared!“

- Es ist *unmöglich* RSA zu programmieren, wenn noch Fragen zu RSA offen sind!
- Man generiert zwei Module
  - Ein Modul `exportRSAkey`, das einen public key erzeugt und den private key berechnet. Der public key soll als Liste in ein file exportiert werden.
  - Das andere Modul `importRSAkey` soll einen public key aus einem file importieren, damit man messages verschlüsseln kann.
- Es ist mit Blick auf die nächste Doppellektion natürlich von Vorteil, wenn der public key eines Adressaten im Mathematica Notebook aufgerufen werden kann ($\rightarrow$ Verschlüsselung).
- Der eigene Exponenten, das eigene Modul und der private key sollten natürlich auch im Mathematica Notebook als Variablen aufgerufen werden können ($\rightarrow$ Entschlüsselung, Signatur).
- Eine mögliche Umsetzung der key Generierung in Mathematica meinerseits könnte folgen.

30 RSA Simulation mit Mathematica fortgesetzt

. . . bald sind Sommerferien. . .

- Man generiert zwei weitere Module
  - Ein Modul `encryptRSA` soll einen Text verschlüsseln und in einem file ablegen.
  - Das andere Modul `decryptRSA` soll ein file importieren und den Text entschlüsseln.
- Bravo an Luca, Fabian und Carola, die das gesteckte Ziel beinahe in der Doppelstunde erreicht haben.
- Bis nächste Stunde sollten alle mindestens das Modul formuliert haben, das einen key generiert und exportiert.
- Man sollte die Erfahrung gemacht haben, dass Programmieren auch mit schritt-

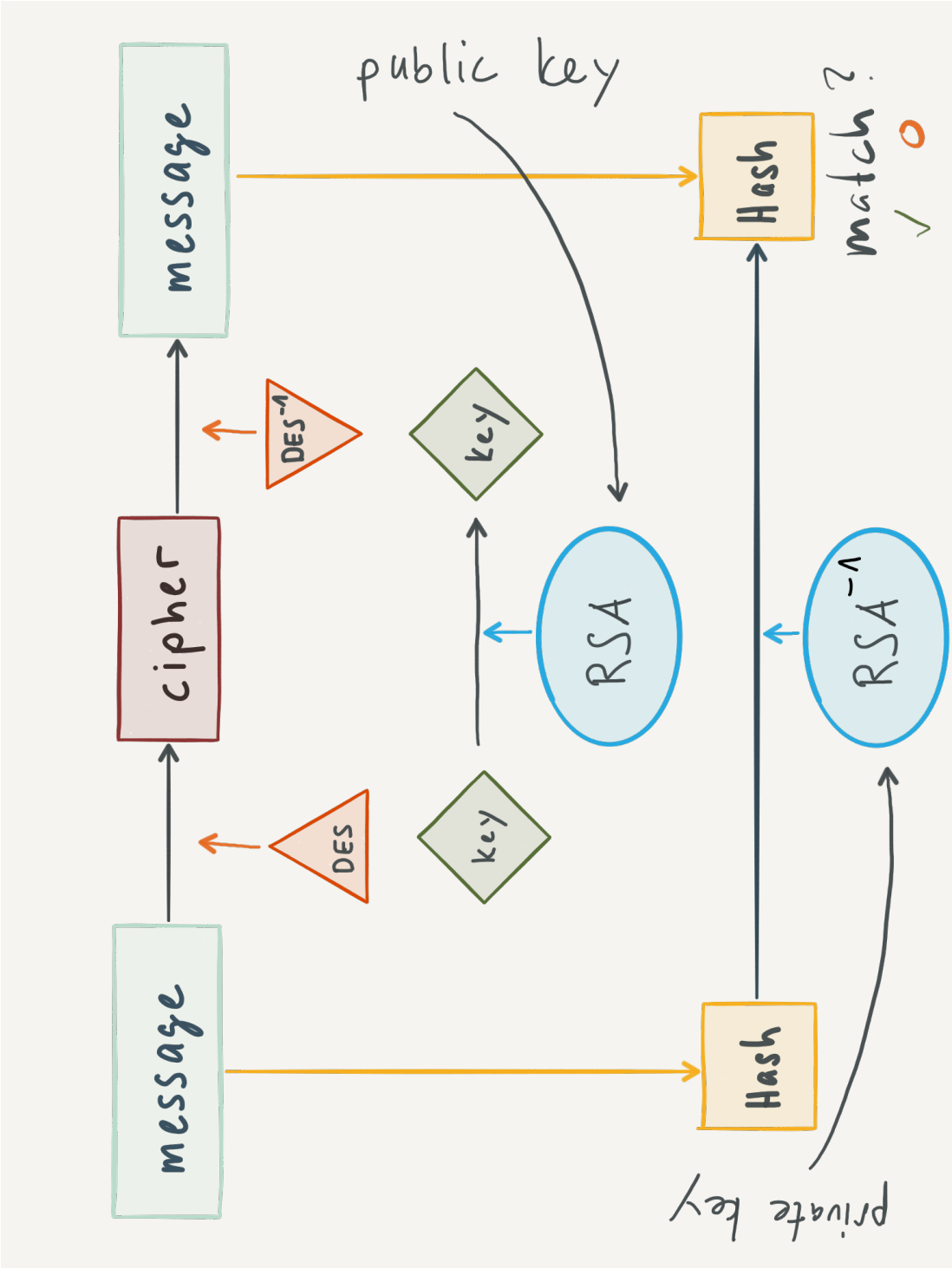
weisem Ausprobieren und hartnäckiger Fehlersuche zu tun hat.

- Möglicherweise folgt eine mögliche Umsetzung der gestellten Aufgaben meinerseits.

31 Let's Play!

. . . rock'n'roll, gogogo!

- Wir spielen `RSA` mit verschlüsselten und signierten Nachrichten. . .
- . . . und freuen uns auf die Ferien!
- Nach den Sommerferien starten wir mit Affinen Abbildungen.


message
public key
Hash
match?
yes
DES⁻¹
key
cipher
RSA
RSA⁻¹
DES
key
message
Hash
private key

```
Clear["Global`*"]

generateKeys[outfilename_] := Module[{p, q, myr, exportdir},
    (* generiert einen RSA-Schlüssel;
    Input: Dateiname für den public key.
       Returns n,e,d (als Variable myn,mye,d innerhalb des notebooks aufrufbar)
     und speichert den public key (e,n) in filename (uses .dat ending) *)
    Clear[myn, mye, d]; (* Clear für erneuten Aufruf *)
    d = 1; (* initial value zur Fehlerunterdrückung falls if-condition false *)
    p = Prime[Random[Integer, {10^9, 10^10}]]; (* random primes *)
    q = Prime[Random[Integer, {10^9, 10^10}]];
    mye = 2^16 + 1; (* public exponent *)
    myn = p * q; (* public module *)
    myr = (p - 1) * (q - 1); (* module to get inverse *)
    If[GCD[mye, myr] == 1, (* check existance of inverse *)
     d = PowerMod[mye, -1, myr], (* calculate private key *)
     Print["Pech gehabt mit Verschlüsselungsexponent e"]];
    exportdir =
     ToFileName[{NotebookDirectory[]}, StringJoin[ToString[outfilename], ".dat"]];
    (* Textfile filename, enthält e und n *)
    Export[exportdir, {myn, mye}]; (* export to file *)
    Print["Public Key exportiert nach: " exportdir];
    Clear[p, q]; (* vaporize primes *)
    Print["Deinen public und private key kannst
       du innerhalb des Notebooks mit myn, mye und d abfragen."];
  ];

generateKeys["bobspublickey"]
```

```
Public Key exportiert nach:
 /Users/waj/Dropbox/Module/Angewandte Mathematik/04 Kryptologie Neu/RSA
   mit Mathematica/bobspublickey.dat
Deinen public und private key kannst du innerhalb des Notebooks mit myn, mye und d abfragen.
```

```
bobe = mye
bobn = myn
bobd = d
```

65 537

7 107 498 970 806 166 200 991

5 826 702 430 598 089 200 785

```
generateKeys["jormaspublickey"]
```

```
Public Key exportiert nach:
 /Users/waj/Dropbox/Module/Angewandte Mathematik/04 Kryptologie Neu/RSA
   mit Mathematica/jormaspublickey.dat
Deinen public und private key kannst du innerhalb des Notebooks mit myn, mye und d abfragen.
```

```
importPublicKey[infilename_] := Module[{bobKeys},
    (* Importiert public key aus file filename,
    und speichert n unter bobn und e unter bobe innerhalb des Notebooks *)
    bobKeys = Flatten[Import[ToFileName[{NotebookDirectory[]},
         StringJoin[ToString[infilename], ".dat"]], "Data"]]; (* construct filename *)
    bobn = bobKeys[[1]]; (* get public module *)
    bobe = bobKeys[[2]]; (* get public exponent *)
    Print["Importierter public key (bobn, bobe): ", bobn, ", ", bobe];
  ];
```

```
importPublicKey["bobspublickey"]
```

```
Importierter public key (bobn, bobe): 7 107 498 970 806 166 200 991, 65 537
```

```
myEncryptRSA[msg_, e_, n_, outfilename_] := Module[{mbyte, ciphertemp},
    (* Input: message, exponent, module, filename.
      Chiffriert eine Message mit e und
     n und speichert die cipher unter cipherout in filename.
      Returns cipher als String repräsentiert binär,
    damit "hoffentlich" kompatibel mit jedem Textverarbeitungsprogramm *)
    Clear[cipherout]; (* Clear für erneuten Aufruf *)
    mbyte = Fold[#1 * 256 + #2 &, 0, ToCharacterCode[msg]];
    (* message im 256er System (bytes) *)
    ciphertemp = Function[x, PowerMod[x, e, n]] /@ IntegerDigits[mbyte, n];
    (* Blockverschlüsselung im n-er-System *)
    cipherout = Fold[#1 * n + #2 &, 0, ciphertemp]; (* cipherstring im n-er System *)
    bblocks = Ceiling[(DigitCount[cipherout, 2, 0] + DigitCount[cipherout, 2, 1]) / 8];
    (* Länge der Binärzahl messen → fürs padding *)
    bytestring = IntegerString[cipherout, 2, 8 * bblocks]; (* Binärzahl mit padding *)
    exportdir = ToFileName[{NotebookDirectory[]},
      StringJoin[ToString[outfilename], ".dat"]]; (* generate ciphered messagefile *)
    Export[exportdir, bytestring];
    Print["Cipher exportiert nach: ", exportdir];
   ];
```

```
message = "Real check now if the whole
   thing, inlcuding signing of messages and integrity, works."
```

```
Real check now if the whole thing, inlcuding signing of messages and integrity, works.
```

```
cipher = myEncryptRSA[message, mye, myn, "bobtojorma"]
```

```
Cipher exportiert nach: /Users/waj/Dropbox/Module/Angewandte
   Mathematik/04 Kryptologie Neu/RSA mit Mathematica/bobtojorma.dat
```

```
myDecryptRSA[infilename_, d_, n_] :=
  Module[{temp, temp1, temp2, temp3, msgtemp, id, bobcipher},
   (* Entschlüsselt cipher, die mit einem public key
     verschlüsselt wurde. Input Message als Zahl im Binär-System,
    n und private key d oder public key e. Returns orignal Message *)
    bobcipher = Flatten[Import[ToFileName[{NotebookDirectory[]},
        StringJoin[ToString[infilename], ".dat"]], "Data"]]; (* construct filename *)
    temp = FromDigits[Flatten[bobcipher], 2]; (* liest den String als Binärzahl ein *)
    temp1 = IntegerDigits[temp]; (* kreiert die Liste der Digits *)
    temp2 = Fold[#1 * 2 + #2 &, 0, temp1]; (* berechnet den dezimalen Wert *)
    temp3 = IntegerDigits[temp2, n]; (* macht Blöcke im n-er-System *)
    msgtemp = Function[x, PowerMod[x, d, n]] /@ temp3; (* decrypt *)
    id = IntegerDigits[Fold[#1 * n + #2 &, 0, msgtemp], 256]; (* Liste mit Bytes *)
    FromCharacterCode[id]
   ];
```

```
myDecryptRSA["bobtojorma", d, myn]
```

```
Real check now if the whole thing, inlcuding signing of messages and integrity, works.
```

```
(*******************************************************************************)
```

```
getHash[msg_] := Module[{mlist, lmlist, hash},
  (* Hash nach Barcode Muster. Input Message und Output Zahl Mod 7;
  +2 um 0 und 1 zu vermeiden *)
  Clear[mlist, hash, lmlist]; (* clear für erneuten Aufruf *)
  mlist = ToCharacterCode[msg]; (* generiert Byte-Code der Message *)
  lmlist = Length[mlist]; (* Listenlänge für die Checksum bestimmen *)
  hash = (Mod[Sum[k * mlist[[lmlist - k + 1]], {k, 1, 10}], 7] + 2)]
  (* Checksum über die Message *)
```

```
getHash[message]
```

```
4
```

```
Hash[message, "CRC32"](* built-in hash-function *)
```

```
2 997 428 377
```

```
exportSigniert[msg_, outfilename_] := Module[{exportdir, mbyte, ciphertemp},
    (* Input: message
      Verschlüsselt message mit public key bobe und bobn,
    berechnet fingerprint mit CRC32 und signiert fingerprint mit private d und myn.
      Return file filename mit cipher und singiertem fingerprint *)
    mbyte = Fold[#1 * 256 + #2 &, 0, ToCharacterCode[msg]]; (* message im 256er System *)
    ciphertemp = Function[x, PowerMod[x, bobe, bobn]] /@ IntegerDigits[mbyte, bobn];
    (* Blockverschlüsselung mit Länge bobn *)
    cipherout = Fold[#1 * bobn + #2 &, 0, ciphertemp]; (* cipherstring im bobn-er System *)
    edhash = Hash[msg, "CRC32"]; (* fingerprint mit CRC32 der message *)
    edhash = PowerMod[edhash, d, myn];
    (* signierter fingerprint mit private exponent d *)
    exportdir = ToFileName[{NotebookDirectory[]},
      StringJoin[ToString[outfilename], ".dat"]]; (* Export der signierten Nachricht *)
    Export[exportdir, {cipherout, edhash}];
    Print["Verschlüsselte und signierte Nachricht exportiert nach: ", exportdir];
   ];
```

```
exportSigniert[message, "jormatobobsigniert"]
```

```
Verschlüsselte und signierte Nachricht exportiert nach:
 /Users/waj/Dropbox/Module/Angewandte Mathematik/04
   Kryptologie Neu/RSA mit Mathematica/jormatobobsigniert.dat
```

```
importSigniert[infilename_] := Module[{incoming, temp, msgtemp, id, hashtest},
    incoming = Flatten[Import[ToFileName[{NotebookDirectory[]},
        StringJoin[ToString[infilename], ".dat"]], "Data"]]; (* construct filename *)
    incmessage = incoming[[1]];
    inchash = incoming[[2]];
    temp = IntegerDigits[incmessage, myn]; (* message in n-er-Blöcke *)
    msgtemp = Function[x, PowerMod[x, d, myn]] /@ temp; (* decrypt *)
    id = IntegerDigits[Fold[#1 * myn + #2 &, 0, msgtemp], 256]; (* Byte-Blöcke *)
    msg = FromCharacterCode[id];
    Print["Importierte Cipher:" msg];
    inchash = PowerMod[inchash, bobe, bobn]; (* prepare to test authentity *)
    hashtest = TrueQ[Hash[msg, "CRC32"] == inchash]; (* integrity and authentity test *)
    Print["Hash- and Authentitytest:" hashtest];
   ];
```

```
importSigniert["jormatobobsigniert"]
```

```
Importierte Cipher:
 Real check now if the whole thing, inlcuding signing of messages and integrity, works.
```

```
Hashtest: True
```

32 Abbildungen

. . . one to rule them all. . .

- **bijektiv** heisst: zu jedem Bild y gibt es genau ein Urbild x. Ist eine Abbildung bijektiv, so ist sie umkehrbar!
- **Verkettung** von Abbidlungen schreiben wir

  $$\beta \circ \alpha$$

  (sprich „beta Ring alpha“). Beachte, dass diese Schreibweise von rechts nach links gelesen wird; es wird also zuerst α und danach β auf ein Element angewendet.
- Erster Kontakt mit der Formulierung von Abbildungen in der Ebene

  $$\alpha : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$$

- Formulierung der grundlegenden Abbildungen: Translation, Streckung, Scherung, Spiegelung.

$$\tau : \begin{cases} x' = x & + t_x \\ y' = & y + t_y \end{cases} \qquad \zeta : \begin{cases} x' = x & + y \cdot \tan(\varphi) \\ y' = y & \end{cases}$$

$$\sigma : \begin{cases} x' = kx & \\ y' = & ky \end{cases} \qquad \varrho : \begin{cases} x' = x & \\ y' = & -y \end{cases}$$

33 Getting used to

. . . gemütlicher Freitag Morgen. . .

- bis und mit Übung 7

34 Fixpoints

. . . immun gegenüber α sein. . .

- Abbildungen von Geraden am Beispiel der Punktspiegelung an $(-2\,|\,4)$ angeschaut.

- Begriffe **Fixpunkt**, **Fixgerade** und **Fixpunktgerade** eingeführt.
- einige Übungen bis 13 gelöst (insbesondere Inversion am Kreis)

35 Ursprungsaffinitäten

. . . watch the basis under α

- Affine Ursprungsaffinitäten
  - $(0\,|\,0)$ ist Fixpunkt
  - geradentreu
  - parallelentreu
  - teilverhältnistreu
- Jede Ursprungsaffinität kann als Verkettung der „Grundabbildungen“
  - Streckung
  - Achsenspiegelung
  - Scherung
  - Rotation um φ mit Zentrum $(0\,|\,0)$

    $$\varrho : \begin{cases} x' = \cos(\varphi) \cdot x & -\sin(\varphi) \cdot y \\ y' = \sin(\varphi) \cdot x & +\cos(\varphi) \cdot y \end{cases}$$

    formuliert werden.
- Wir haben uns davon überzeugt, dass die Bilder der Basisvektoren zeigen, wie die Abbildungsgleichung aussieht. Sei $\vec{v} = x \cdot \vec{e_x} + y \cdot \vec{e_y}$ ein Punkt bzw. sein Ortsvektor, dann ist das Bild $\vec{v'} = x \cdot \vec{e'_x} + y \cdot \vec{e'_y}$. Es gilt dann

  $$\alpha : \begin{cases} x' = e'_{xx} \cdot x & +e'_{yx} \cdot y \\ y' = e'_{xy} \cdot x & +e'_{yy} \cdot y \end{cases}$$

36 Von A bis det

. . . expectation vs. reality. . .

- Matrizenschreibweise für Ursprungsaffinitäten registriert, und in Erinnerung gerufen, dass die Spaltenvektoren den Bildern der Einheitsvektoren entsprechen:

$$\begin{pmatrix} e'_{xx} & e'_{yx} \\ e'_{xy} & e'_{yy} \end{pmatrix}$$

- Die Addition ist komponentenweise wie in $\mathbb{R}$ definiert. Man sieht leicht, dass die Matrizen mit Addition eine kommutative Gruppe bilden.

- Die Multiplikation ist umständlicher definiert, entspricht aber just der Verkettung von Ursprungsaffinitäten:

$$A \cdot B = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \cdot \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{12} + a_{12}b_{22} \\ a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{12} + a_{22}b_{22} \end{pmatrix}$$

- Die Determinante det einer 2×2-Matrix A ist die Zahl

$$\det(A) := a_{11}a_{22} - a_{21}a_{12}$$

- Nebst diversen andern Facts, die an der Determinante abgelesen werden können, ist für uns Gold Wert:

  > Die Matrizen, welche $\det(A) \neq 0$ haben, sind als Ursprungsaffinitäten aufgefasst bijektiv; die Umkehrung gilt auch!

- Einfach genial: Die Menge der regulären Matrizen bilden zusammen mit der Multiplikation eine Gruppe und sind isomorph zur Menge der bijektiven Ursprungsaffinitäten mit Operation Verkettung.

37 Anwendungsbeispiel Matrizen

. . . Erste Tranche Affine Abbildungen überblicken. . .

- Wir rechnen ein Beispiel der Verkettung zweier Ursprungsäffinitäten mit Matrizen durch.

38 EW & EV

. . . now we're talking. . .

- Wir sehen die **Eigenwert-/Eigenvektorgleichung** zur Matrix A

$$A \cdot \vec{r} = \lambda \cdot \vec{r}$$

  die uns Auskunft zu Fixgeraden (Fixpunktgeraden für $\lambda = 1$) gibt.

- Das **Charakteristische Polynom** von A,

$$\chi(A) = \lambda^2 - \text{Spur}(A) + \det A$$

  liefert uns *Eigenwerte* λ und die Koordinatengleichungen

$$\begin{aligned}(a_{11} - \lambda)x + a_{12}y &= 0\\ a_{21}x + (a_{22} - \lambda)y &= 0\end{aligned}$$

  zugehörige *Eigenvektoren* $\vec{r}$ zu den Eigenwerten λ.

39 Anwendungen EV & EW

... der Goldene Schnitt...

- Wir betrachten zwei voneinander abhängige Folgen mit linearen rekursiven Formen. Formuliere dieses System mit einer Matrix...

- Wir leiten die explizite Definition der k-ten Position der Fibonacci-Folge her.

40 Raus in den $\mathbb{R}^n \times \mathbb{R}^n$

... nicht nur Gauss kann was...

- Entwicklungssatz von Laplace zur Determinantenberechnung:

$$\sum_i (-1)^{i+j} a_{ij} \cdot \det(A_{ij})$$

  Entwicklung nach der j-ten Spalte, oder

$$\sum_j (-1)^{i+j} a_{ij} \cdot \det(A_{ij})$$

  nach der i-ten Zeile.

- Regel von Sarrus zur Berechnung der Determinante einer 3×3-Matrix gesehen.

- Für die Übungen wurde das charakteristische Polynom einer 3×3-Matrix bereitgestellt:
$$\chi_A = \lambda^3 - \text{Spur}(A) \cdot \lambda^2 + (\det(A_{11}) + \det(A_{22}) + \det(A_{33})) \cdot \lambda - \det(A)$$

41 Komplexe Funktionen & Impedanz

... geht ja fast wie Affine Abbildungen...

- Repetition der wichtigsten Facts zu komplexen Zahlen
  - $$i^2 = -1$$
    i imaginäre Einheit
  - Normal- & Polarform
    $$a + i \cdot b = r \cdot e^{i\varphi}$$
    einer komplexen Zahl $z \in \mathbb{C}$
  - Gauss-Ebene $\mathbb{C}$, reelle Achse, imaginäre Achse
  - Addition eher in Normalform, Multiplikation eher in Polarform
  - $re^{i\varphi} = r(\cos(\varphi) + i \cdot \sin(\varphi))$
  - Schönste Formel der Welt
    $$e^{i \cdot \pi} + 1 = 0$$
- Möbius-Transformation $f : \mathbb{D} \longrightarrow \mathbb{C}$ mit
$$f(z) = \frac{az + b}{cz + d} \quad (a, b, c, d \in \mathbb{R})$$
wobei $ad - bc \neq 0$
- Jede Möbiustransformation kann in die Grundoperationen Translation, Drehstreckung und Inversion zerlegt werden:
$$z + c, re^{i\varphi}, \frac{1}{z}$$
- Eine Möbiustransformation konserviert die Kreise (eine Gerade wird als Kreis mit unendlichem Radius aufgefasst).
- Es wurde versucht — mit wenig Erfolg— die Impedanz eines RLC-Seriekreises zu begründen.

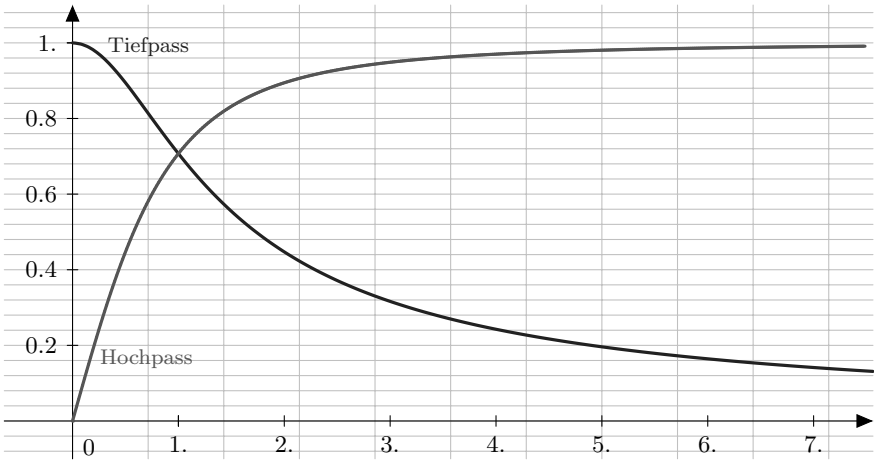


Abbildung 2: Typische Kennkurve eines Hoch- bzw. Tiefpassfilters

42 RC mit Wechselspannung

... Hochpass, Tiefpass...

- Herleitung der Impedanz eines Kondensators

$$Z_C = -\frac{1}{\omega C} \cdot i$$

- Hochpass-/Tiefpasseigenschaften für einen RC-Serie mit Wechselspannung $U(t) = U_0 \cdot e^{i\omega t}$
- Amplitudenverhälnisse der Teilspannungen U_R bzw. U_C ($x = \omega RC$)

$$\text{Tiefpass} : \frac{1}{\sqrt{1+x^2}}, \text{ Hochpass: } \frac{1}{\sqrt{1+\frac{1}{x^2}}}$$

Das sieht dann qualitativ wie in Abbildung 2 auf Seite 40 aus.

43 Iterationen

... neues Thema, alte Begriffe...

- **Iterieren** einer Funktion f bedeutet, dass man auf einen Startwert x_0 immer wieder f anwendet. Wir schreiben dann z.B.

$$f(f(f(x_0))) =: f^{(3)}(x_0)$$

- Beim Iterieren durchläuft ja der Startwert x_0 reelle Werte. Diese Folge nennt man Bahn oder **Orbit** von f für den Startwert x_0.

- Natürlich interessieren uns wieder Werte, für die man trotz f an Ort und Stelle tritt — sogenannte Fixpunkte — oder Werte, für die man nach einigen Iterationen wiederum erreicht. Wir unterscheiden darum **Fixpunkte der Periode** 1, der Periode 2, etc.

$$f^{(k)}(x) = x$$

44 Übungen zu Iterationen

... das x nicht vergessen...

- und täglich grüssen die Fixpunkte...

- und wieder ein Semester um...

45 Mathematica Reloaded

... shift enter...

- erste Vorbereitungen zu Iterationen mit `Mathematica` im Hinblick auf Modellierung realer Systeme

- Befehle: `Nestlist, Listplot, Solve, Manipulate`

46 Intermezzo QT à la „gspür mi“

... this is another world... oh, no, it's the matrix...

- ... fragte ich mich immer wieder, ob die Natur wirklich so absurd sei, wie sie uns durch diese Atomexperimente erschien...

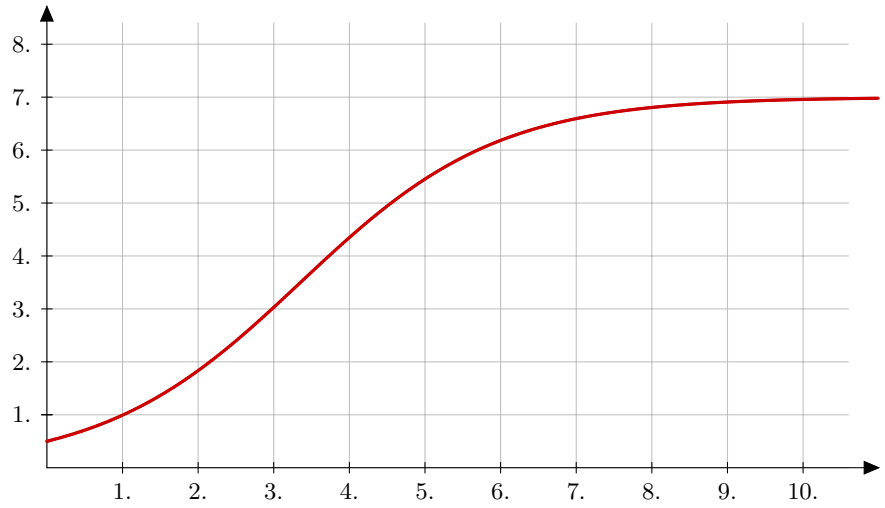


Abbildung 3: Beispiel einer logistischen Wachstumskurve

- jain. „Blue or red pill?“ Take blue and taste your steak, take red and learn about nature.

47 Rettet die Wale

. . . Manipulate. . .

- Wir modellieren ein gecaptes, zu Beginn exponentielles Wachstum mit

$$x_{n+1} = x_n + r \cdot x_n \cdot (S - x_n)$$

  wobei x_n die Population zur Zeit n, r ein Mass für das Wachstum und S die Sättigungsgrenze bezeichnen.

  Das sieht dann etwa so aus wie in Abbildung 3 auf Seite 42.

- `Mathematica` stellt verschiedene, hilfreiche Funktionen zum Iterieren und Problemelösen bereit; beispielsweise `NestList`, `ListPlot`, `Manipulate`, `Solve`, ...

- Man überlegt sich, wie absolute und prozentuale Fangquote ins Model einfliessen.

- Die Wenigsten wagen eine Quintessenz. . .

48 Logistisches Wachstumsmodel unter der Lupe

. . . from capped to chaos. . . und . . . yes, *we* want. . .

- *Wir* iterieren
$$W(x) = x + qx(S - x)$$
und finden unter Variation von q Instanzierungen von beschränktem Wachstum über sprunghaftes Verhalten bis hin zum Chaos.

- *Wir* reskalieren die logistische Gleichung um sie für eine Analyse handlicher parat zu haben:
$$f_r(x) := rx(1 - x)$$
Im „neuen“ r steckt die Information aus dem Walfangmodel; $1 + rS$.

- *Wir* haben ferner mit $f_r : [0, 1] \longrightarrow [0, 1]$ unbeschränkte Iteration erzwungen, woraus $r \in [0, 4]$ folgte. Das ist ein wichtiges Datum, deshalb hier noch mal zentriert: Will man
$$f_r : [0, 1] \longrightarrow [0, 1]$$
so muss
$$0 \leq r \leq 4$$

- *Wir* wollen noch einsehen, dass wegen der Isomorphie (Gleichgestaltigkeit) zwischen $(0, 1)$ und $\mathbb{R}$ dies keine Einschränkung für die Analyse des logistischen Wachstumsmodells ist. Die Nullstellen 0 und 1 können beispielsweise als $-\infty$ und $+\infty$ interpretiert werden, so dass $(0, 1)$ zu $[0, 1]$ erweitert wird.

  Übrigens ist, nebst andern Möglichkeiten, zum Beispiel
$$f(x) = \frac{e^{2x} - 1}{e^{2x} + 1} =: \tanh(x)$$
ein schöner Isomorphismus (strukturerhaltende, bijektive Abbildung), da nebst $f(0) = 0$ auch $f'(0) = 1$ gilt. Ferner erhält f auch die Ordnung.

- Los gehts. . . auf eine fantastische Reise. . . *wir* zusammen. . .

49 Logistische Gleichung analysiert

. . . „ja aber de isch ja das munzig chli. . .

- Wir verwenden eine einfache, starke Version des Banach’schen Fixpunktsatzes

Satz 3. *Sei $\mathbb{I} \subset \mathbb{D} \subset \mathbb{R}$ ein Intervall und $x_0 \in \mathbb{I}$. Ferner gelte $\forall x \in \mathbb{I}$: $\exists M$ mit $-1 < M < 1$, so dass $|f'(x)| < M$. Dann gilt für jeden Startwert $x_0 \in \mathbb{I}$: Die Folge $< x_k >$ konvergiert und der Grenzwert ist ihr Fixpunkt.*

Beweis. Verwende Mittelwertsatz. □

- Fixpunkte erster Ordnung sind

$$x_1^* = 0 \quad \text{und} \quad x_2^* = 1 - \frac{1}{r}$$

und weil ihre Ableitungen $f'(x_1^*) = r$ und $f'(x_2^*) = 2 - r$ sind, bietet sich für die Attraktorbetrachtung die Fallunterscheidung $0 < r < 1$ und $1 < r < 3$.

50 Feigenbaum und Chaos

... endlich wieder Polynomdivision...

- Für $3 < r < 4$ werden Fixpunkte der Ordnung 2 attraktiv, nämlich

$$x_{3,4}^* = \frac{(r+1) \pm \sqrt{(r+1)(r-3)}}{2r},$$

konkret im Bereich $3 < r < 1 + \sqrt{6}$.

- Wir bemerken, dass die sogenannten Bifurkation in immer kürzeren Abständen folgen. Diese Folge der Verzeigungen $< r_k >$ konvergiert und man findet numerisch

$$\lim_{k \to \infty} r_k = 3.569945\ldots$$

Ab dort herrscht Chaos mit zwischenzeitlichen Unterbrüchen.

- Obige Betrachtung führt uns zum Feigenbaumdiagramm.

51 Fraktale

... most famous: Mandelbrotmenge!

- Wir sehen die Mandelbrotmenge, i.e. die Menge aller Punkte $c \in \mathbb{C}$, so dass

$$f(z) = z^2 + c$$

unter Iteration mit $z_0 = 0$ nicht divergiert.

- Diese Menge ist verwandt mit der logistischen Gleichung (siehe Abbildung 4 auf Seite 46)
- Eine „Fahrt“ in die Mandelbrotmenge zu DJ Dimsas Funktionality 2.
- In der Mandelbrotmenge divergiert f, sobald für ein z $|f(z)| > 2$ gilt; dies hilft beim Programmieren.
- Wir lernen noch das Newton-Verfahren zur Nullstellenbestimmung kennen. Nämlich gilt für eine gutmütige Funktion f, dass die Folge

  $$x_{k+1} = x_k - \frac{f(x_k)}{f'(x_k)}$$

  gegen eine Nullstelle konvergiert.

52 Masern

...Jorma, läbe dini Ching no...

- Zurück zum Modellieren mit Iteration. Wir sehen anhand des Masern-Moduls mit der Populationsaufteilung „empfänglich“, „infektiös“, „immun“, wie wir periodisch auftretende Epidemien modulieren könnten.

  $$x_{k+1} = f \cdot x_k y_k \tag{1}$$
  $$y_{k+1} = x_k - f \cdot x_k y_k + B \tag{2}$$
  $$z_{k+1} = z_k + y_k \tag{3}$$

- Erstaunlicherweise hat die unscheinbare „Geburtenrate“ B Einfluss auf Höhe und Frequenz der Peaks!

53 Räuber-Beute Modell von Lotka-Voltera

...ahh, endlich kommen die Marienkäfer...

- Klassiker Hasen–Luchse
- Populationen x und y in Wechselwirkung beschreiben wir einfach so

  $$x_{n+1} = x_n(1 + a) - b \cdot x_n \cdot y_n$$
  $$y_{n+1} = y_n(1 - c) + d \cdot x_n \cdot y_n$$

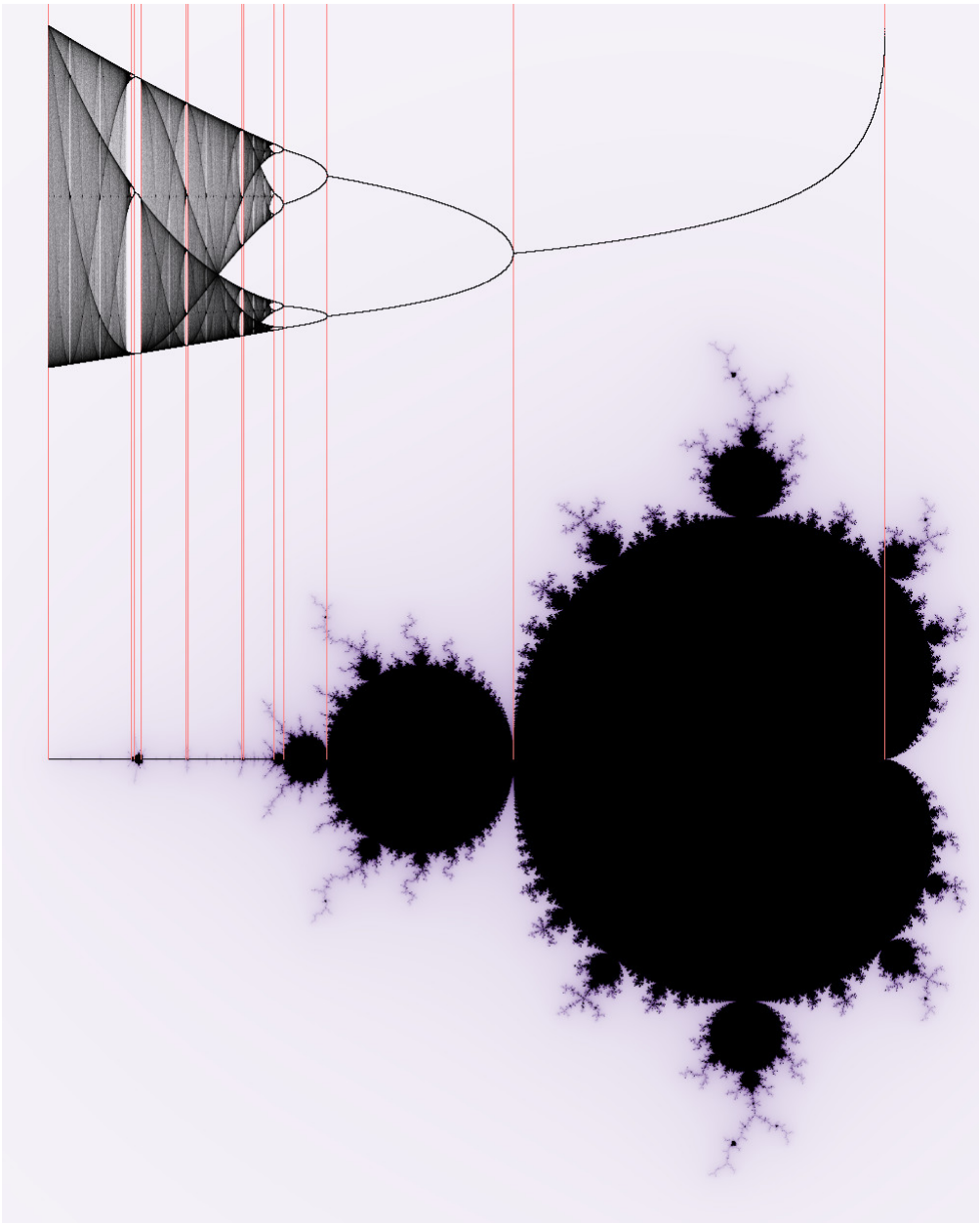


Abbildung 4: Feigenbaum-Diagramm und Mandelbrotmenge

Wir erhalten periodische Schwankungen, die sich aufschaukeln können.

- Beim Marienkäfer–Läuse–Problem arbeiten wir zusätzlich mit Gift, das auf beide Populationen die gleiche Wirkung hat.
- Weitere Erweiterungen sind denkbar...

54 Crash Course Integral

...mut scho bisl ableite könne...

- Integrieren ist das „Gegenteil“ vom Ableiten. Das heisst: Lerne richtig, sicher und schnell ableiten. Übe das! Lerne alle Regeln auswendig!
- Wichtige Ableitungen und Ableitungsregeln
  - $(e^x)' = e^x$
  - $(\sin(x))' = \cos(x)$
  - $(\cos(x))' = -\sin(x)$
  - $(\ln(x))' = \frac{1}{x}$
  - Produktregel: $(f \cdot g)' = f' \cdot g + f \cdot g$
  - Kettenregel: $(f(g))' = f'(g) \cdot g$
- Ableitung/Differential bedeutet **momentane Änderung**/Tangentensteigung. Aufleiten/Integrieren bedeutet globale Änderung/Flächenwert.
- Schreibweisen ausgehend von Leibniz/Newton
  - Vorteil der Schreibweise: Du kannst damit rechnen wie mit Variablen
  - Limit Steigungsdreieck: $\lim_{\Delta x \to 0} \frac{\Delta f}{\Delta x} =: \frac{df}{dx} = \frac{d}{dx} \cdot f$
  - Differentialoperator: $\frac{d}{dx}$
  - Ortsableitung $\frac{\partial}{\partial x} f(x,t) =: f'(x,t)$ und Zeitableitung $\frac{\partial}{\partial t} f(x,t) =: \dot{f}(x,t)$
  - Stammfunktion: $\int f(x)\,dx = F(x) + c$ mit $F'(x) = f(x)$

- Hauptsatz der Integral- & Differentialrechnung:

$$\int_a^b f(x)\,dx = F(x)|_a^b = F(b) - F(a)$$

55 Differentialgleichungen: erster Einblick

$\ldots \dot{N} = \lambda \cdot N \to N_0 \cdot e^{\lambda t}$ und $\ddot{\varphi} = -\frac{g}{L} \cdot \varphi \to A \cdot e^{i\sqrt{\frac{g}{L}} \cdot t} \ldots$

- Klassiker **Radioaktiver Zerfall**. Modell: Die momentane Änderung der Stoffmenge ist proportional zur aktuell vorhandenen Stoffmenge

$$\dot{N}(t) = -\lambda \cdot N(t)$$

  Als Lösung erhalten wir

$$N(t) = N_0 \cdot e^{-\lambda t}$$

- Klassiker **Mathematisches Pendel**. Modell: ohne Störfaktoren und mit dem Auslenkungswinkel φ erhält man

$$\ddot{\varphi}(t) = -\frac{g}{L} \cdot \varphi(t)$$

  wobei die für kleine Auslenkungswinkel φ die Näherung $\sin(\varphi(t)) \approx \varphi(t)$ motiviert wurde.

  Die Lösung ist — natürlich — eine Schwingung

$$\varphi(t) = A \cdot e^{i\sqrt{\frac{g}{L}} \cdot t}$$

56 Logistisches Wachstum

…scho wider…

- Klassiker **Logistische Gleichung**. Modell: Geburtenrate B, Sterberate D, Populationsgrösse P, Stressfaktor S führt zu

$$\dot{p} = (B - D) \cdot p - S \cdot p^2$$

  Das lösen wir ähnlich wie die Zerfallsgeschichte, aber müssen uns zusätzlich der Partialbruchzerlegung bedienen. Schliesslich finden wir mit $B - D =: \beta$

$$p(t) = \frac{p_0 \beta}{S p_0 + (\beta - S p_0) e^{\beta(t - t_0)}}$$

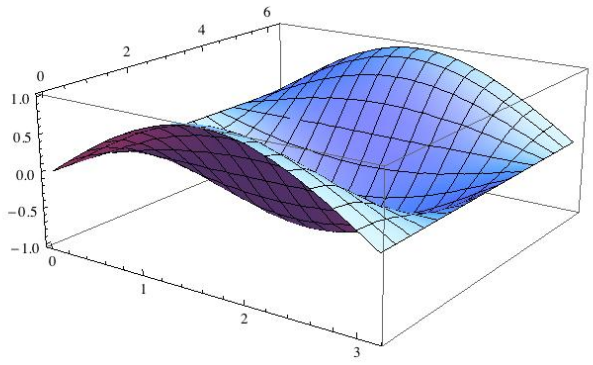


Abbildung 5: Schwingende Saite mit fixen Enden in Zeit- und Ortsabhängigkeit

- Der Plot veranschaulicht logistisches Wachstum.
- Bemerkung: Stationäre Lösungen sind übrigens 0 und $\frac{\beta}{S}$, was den altbekannten Fixpunkten (Repeller und Attraktor) bei den Walen entspricht. Den Wert $\frac{\beta}{S}$ bezeichneten wir als Sättigungs- oder Kapazitätsgrenze. Man schreibt deshalb auch oft, mit $K := \frac{\beta}{S}$,

$$p(t) = \frac{Kp_0}{p_0 + (K - p_0)e^{-\beta(t-t_0)}}$$

57 Weitere Differentialgleichungen

...DGLs im Alltag? JA!...

- Seil mit fixen Enden

$$\frac{\partial^2 u}{\partial x} = \lambda \frac{\partial^2 u}{\partial t^2}$$

  Eine Lösung ist zum Beispiel $u(x,t) = \sin(nx) \cdot \cos(nt)$ (siehe Abbildung 5 auf Seite 49).

- Wärmeleitungsgleichung

$$\frac{\partial u}{\partial t} = \lambda \frac{\partial^2 u}{\partial x^2}$$

  Eine Lösung ist zum Beispiel $u(x,t) = e^{nt} \cdot \sin(nx)$ (siehe Abbildung **??** auf Seite 50).

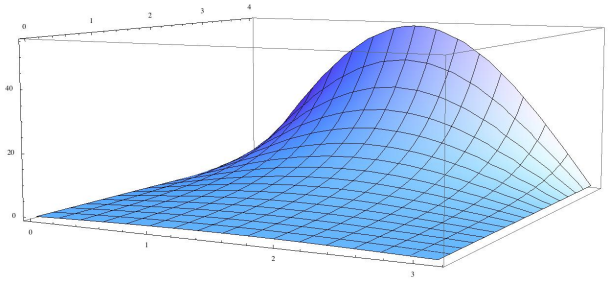


Abbildung 6: Temperaturverlauf mit isolierten Enden in Zeit- und Ortsabhängigkeit

58 Fourierreihe

... Schwingungsanteile von f ...

- Trigonometrische Basisfunktionen

$$1, \quad \sin(nx), \quad \cos(nx)$$

- Skalarprodukt abstrakter:

$$\langle f, g \rangle := \int_{-\pi}^{\pi} f(x) \cdot g(x)\, dx$$

- Orthogonalität $\langle f, g \rangle = 0$, Normierung $\sqrt{\langle f, f \rangle}$ und Beweis der paarweisen Orthogonalität der trigonometrischen Basisfunktionen. Dazu verwenden wir die fundamentale Beziehung $e^{ix} = \cos(x) + i \cdot \sin(x)$.

- **Fourierreihe**: Sei f relativ gutmütig und auf $[-\pi, \pi]$ definiert. Dann nennen wir die Darstellung

$$f(x) = \frac{a_0}{2} + \sum_{n=1}^{\infty} (a_n \cos(nx) + b_n \sin(nx))$$

  die Fourierreihe von f.

- Die **Fourierkoeffizienten** finden wir via

$$a_0 = \frac{1}{\pi} \int_{-\pi}^{\pi} f(x)\, dx, \quad a_n = \frac{1}{\pi} \int_{-\pi}^{\pi} f(x) \cos(nx)\, dx, \quad b_n = \frac{1}{\pi} \int_{-\pi}^{\pi} f(x) \sin(nx)\, dx$$

  (Herleitung siehe Unterricht)

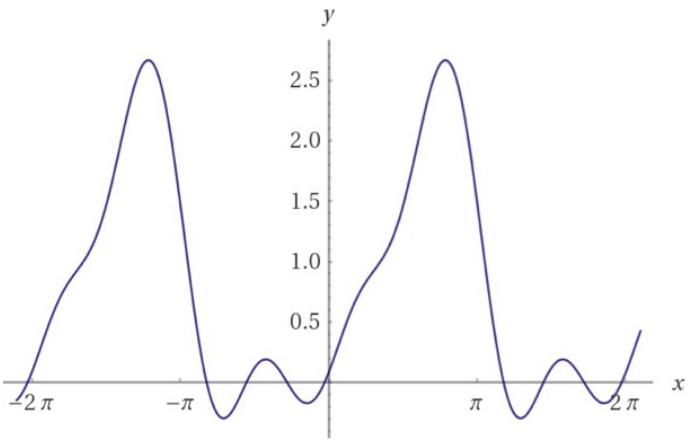


Abbildung 7: Approximation einer Sägezahnfunktion mit Fourier

59 DGL System 2×2

... und täglich grüssen EW & EV...

- DGL $y'(x) = g(x) \cdot y(x)$ mit Separation der Variablen, wie Zerfall....
- Für ein lineares **Differatialgleichungsystem** erster Ordnung finden wir — mit entsprechendem Ansatz —, dass die Lösung auf die bekannte Eigenwert-Eigenvektorengleichung führt. Mit dem entsprechenden Ansatz erkennen wir die Lösung

$$x(t) = c_{1x}e^{\lambda_1 \cdot t} + c_{2x}e^{\lambda_2 \cdot t}$$
$$y(t) = c_{1y}e^{\lambda_1 \cdot t} + c_{2y}e^{\lambda_2 \cdot t}$$

  wobei λ_1 und λ_2 die Eigenwerte und $\vec{c_1}$, $\vec{c_2}$ die Eigenvektoren repräsentieren.

60 Recap, recap, recap...

...und täglich grüssen die Fourierreihen...

- viele, sehr viele Beispiele zu Fourierreihen...mit vielen, sehr vielen plots...
- Die Herleitung der Fourierkoeffizienten führt zur Idee des frequency fishing.
- irgendwann dann der Schritt zur kurzen Präsentation der **Fouriertransformation**

$$\mathcal{F}(k) := \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} f(x) e^{-ikx}\, dx$$

und dem *frequency fishing*. Das Amplitudenspektrum wurde nur berührt und die Geschichte dann mangels Interesse fallen gelassen, obwohl eine anschauliche geogebra.org-Animation einer Signalanalyse gezeigt wurde.

61 Separation der Variablen

...y zu dy und x zu dx

- Gleichungen der Form

$$y' = g(x) \cdot y$$

separiert man im Sinne

$$y' = \frac{dy}{dx} = g(x)y \;\rightarrow\; \frac{1}{y} dy = g(x) dx$$

integriert auf beiden Seiten (Integrationskonstante nicht vergessen) und löst schliesslich nach $y = y(x)$ auf. Dies ergibt eine klassische „e hoch“ Lösung.

62 Lineare, inhomogene Differentialgleichungen

...eine Erweiterung...

- Die Differentialgleichung hat die Form

$$y' = g(x) \cdot y + s(x)$$

mit dem sogenannten **Störterm** $s(x)$.

- Die Gesamtlösung ergibt sich, indem man die zugehörige **homogene** Gleichung $y' = g(x) \cdot y$ allgemein löst, y_{hom}, und dazu eine **partikuläre** Lösung, y_{part}, von $y' = g(x) \cdot y + s(x)$ addiert: kurz

$$y = y_{hom} + y_{part}.$$

  Der Beweis erfolgte im Unterricht.

- Manchmal ist es schwierig, eine partikuläre Lösung zu erraten. Abhilfe schafft die **Variation der Konstanten**. Dabei wird die Integrationskonstante der homogenen Lösung als Funktion von x angesetzt und anschliessend die zu lösende Differentialgleichung „neu ausgewertet“. Alle Puzzlestücke wurden im Unterricht zusammen gefügt.

- Beispiel aus dem Unterricht: Zu lösen ist

$$y' = y + x$$

  Die homogene Gleichung ist $y' = y$ mit fast trivialer Lösung

$$y_{hom}(x) = y_0 e^x$$

  (kurze Überlegung oder Separation der Variablen).

  Um eine partikuläre Lösung zu finden, wird nun die Integrationskonstante y_0 als Funktion von x angesetzt, $y_0(x)$.

  Nun ist $y_{hom} = y_0(x)e^x =: y$ und damit $y' = y_0'(x)e^x + y_0(x)e^x$, gemäss Produktregel. Eingesetzt in die zu lösende Gleichung hat man

$$y_0'(x)e^x + y_0(x)e^x = y_0(x)e^x + x$$

  woraus unmittelbar $y_0'(x)e^x = x$ folgt. Dies wollen wir nach der Integrationskonstanten y_0 auflösen. Kurze Umformung liefert:

$$y_0 = \int x \cdot e^{-x}\, dx$$

  Da es sich um ein moderates Produkt handelt, verwenden wir partielle Integration und erhalten

$$y_0 = -e^{-x}(1 + x) + C$$

  Also wird y_{hom} unter Variation zu y_{part} und damit zur Gesamtlösung

$$y(x) = y_{hom} + y_{part} = y_0 e^x + (-e^{-x}(1 + x) + C) \cdot e^x = K \cdot e^x - x - 1$$

  mit $K = y_0 + C$.

Abbildung 8: Vermeers Disciples at Emmaus

63 Altersbestimmung eines Gemäldes

... Vermeer oder Van Meegeren?

- Im Folgenden ultra ausführlich...
- Die Geschichte, basierend auf einer Fallstudie von Brown (1979), führt zur Altersbestimmung via Messung des in der Farbe „Weiss“ enthaltenen ^{210}Pb. Long story short, es ist die Gleichung
$$\dot{N}(t) = -\lambda N(t) + R$$
zu lösen, um dann mit einer Messung das Alter abzuschätzen. Dies ist eine lineare, inhomogene DGL. Daher lösen wir zuerst die homogene Gleichung
$$\dot{N}(t) = -\lambda N(t),$$
bestimmen anschliessend unter Variation der Integrationskonstanten eine partikuläre Lösung, um schliesslich $N(t) = N_{hom}(t) + N_{part}(t)$ zu bilden. Diesen Typ homogene Gleichung haben wir schon gefühlte 1000-mal gelöst. Bestimmte Integration liefert
$$N_{hom}(t) = N_0 \cdot e^{-\lambda(t-t_0)}.$$
Jetzt setzen wir die Integrationskonstante als Funktion von t an, um eine partikuläre Lösung zu finden:
$$N_{part}(t) = N_0(t) \cdot e^{-\lambda(t-t_0)}$$
Es folgt mit der Produktregel
$$\dot{N}_{part}(t) = \dot{N}_0(t) \cdot e^{-\lambda(t-t_0)} + N_0(t) \cdot (-\lambda) e^{-\lambda(t-t_0)}$$

Dieser Ansatz soll ja

$$\dot{N}(t) = -\lambda N(t) + R$$

lösen. Wir setzen ein:

$$\dot{N_0}(t) \cdot e^{-\lambda(t-t_0)} + N_0(t) \cdot (-\lambda) e^{-\lambda(t-t_0)} = -\lambda N_0(t) \cdot e^{-\lambda(t-t_0)} + R$$

Daraus folgt:

$$\begin{aligned} \dot{N_0}(t) \cdot e^{-\lambda(t-t_0)} &= R \\ \dot{N_0}(t) &= R \cdot e^{\lambda(t-t_0)} \\ N_0(t) &= R \cdot \frac{1}{\lambda} e^{\lambda(t-t_0)} + C \end{aligned}$$

Da wir „bloss“ an einer partikulären Lösung interessiert sind, können wir $C = 0$ setzen. Das $N_0(t)$ in unserem partikulären Ansatz eingesetzt ergibt:

$$\begin{aligned} N_{part}(t) &= R \cdot \frac{1}{\lambda} e^{\lambda(t-t_0)} \cdot e^{-\lambda(t-t_0)} \\ N_{part}(t) &= R \cdot \frac{1}{\lambda} \\ N_{part}(t) &= \frac{R}{\lambda} \end{aligned}$$

Tja, diese partikuläre Lösung hätten wir auch erraten können...

Jetzt dürfen wir die Gesamtlösung noch zusammensetzen:

$$N(t) = N_{hom}(t) + N_{part}(t) = N_0 \cdot e^{-\lambda(t-t_0)} + \frac{R}{\lambda}$$

An dieser Stelle bietet sich ein Check der Lösung an; bitte sehr...

Die Alterbestimmung gestaltet sich aufgrund grosser Schwankungen der Messresultate am Gestein bzw. der Farbe als schwierig; glücklicherweise müssen wir aber nicht das genaue Alter des Gemäldes bestimmen. Um es als echt oder gefälscht zu klassifizieren, reicht die Abschätzung, ob es jung ($\sim$ 30 a) oder alt ($\sim$ 300 a) ist. Im Falle eines alten Gemäldes erwartet man minütlich pro cm^2 weniger als 30 000 Zerfälle für dieses „Weiss“. Es wurde am Gemälde $\lambda N = 8.5$ und $R = 0.8$ gemessen. Die Halbwertszeit von ^{210}Pb ist 22.3 Jahre, womit man λ bestimmt. Nehmen wir an, das Gemälde sei $t - t_0 = 300$ Jahre alt. Damit ergibt sich nach unseren Berechnungen für die Anzahl Zerfälle, als das Bild gemalt wurde:

$$\begin{aligned} N &= N_0 \cdot e^{-\lambda(t-t_0)} + \frac{R}{\lambda} \\ \lambda N &= \lambda N_0 \cdot e^{-\lambda(t-t_0)} + R \\ \lambda N_0 &= \lambda N \cdot e^{\lambda(t-t_0)} - R \cdot e^{\lambda(t-t_0)} \\ \lambda N_0 &\approx 86\,000 \end{aligned}$$

Dieses Gemälde wurde sicher nicht im 17. Jhdt. von Vermeer gemalt.

- Die zweite Challenge
$$y' = \frac{y-2}{x-1} + 2x - 2$$
kommentiere ich knackiger.

  Homogen:
$$y' = \frac{y-2}{x-1}$$
  Es folgt
$$\begin{aligned} \frac{1}{y-2}dy &= \frac{1}{x-1}dx \\ \ln(y-2) &= \ln(x-1) + C \\ y-2 &= e^c(x-1) \\ y &= k(x-1)+2 \end{aligned}$$
  Partikuläre Lösung mit Variation:
$$\begin{aligned} y &= k(x)(x-1)+2 \\ y' &= k'(x)(x-1)+k(x) \end{aligned}$$

  Eingesetzt:
$$\begin{aligned} k'(x)(x-1)+k(x) &= \frac{k(x)(x-1)+2-2}{x-1} + 2x - 2 \\ k'(x)(x-1)+k(x) &= \frac{k(x)(x-1)}{x-1} + 2x - 2 \\ k'(x)(x-1)+k(x) &= k(x) + 2x - 2 \\ k'(x)(x-1) &= 2x-2 \\ k'(x) &= \frac{2(x-1)}{x-1} \\ k'(x) &= 2 \\ k(x) &= 2x + C \end{aligned}$$
  Mit $C = 0$ folgt $y = 2x(x-1)+2 = 2x^2-2x+2$ als partikuläre Lösung. Insgesamt erhalten wir
$$y(x) = k(x-1) + 2 + 2x^2 - 2x + 2 = 2x^2 + (k-2)x + 4 - k$$
  Wiederum bringt dir ein Check Routine.

- Jo'l und Mathieu freuen sich auf weitere Kapital Differentialgleichungen mit ihren wunderbaren Anwendungen...

64 Exakte Differentialgleichungen

...versteht noch nicht?...macht nichts!...wird dann schon verstehen...später... vielleicht...

- Eine Gleichung vom Typ
$$P(x,y) + Q(x,y) \cdot \frac{dy}{dx} = 0,$$
wobei $\frac{\partial P}{\partial y} = \frac{\partial Q}{\partial x}$ (**Integrabilitätsbedingung**), heisst **exakt**.

- Sodann findet man via
$$\int P\,dx \quad \text{und} \quad \int Q\,dy$$
die Lösung $F(x,y)$, das sogenannte **Potential**, durch Anpassen der Integrationskonstanten $C(y)$ bzw. $C(x)$.

- Für das Potential $F : G \subset \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ gilt dann $\nabla F = \begin{pmatrix} P \\ Q \end{pmatrix}$.

- Illustrativ sind die **Niveaulinien** von F. Man erhält sie, indem $F(x,y) = k$ nach x oder y aufgelöst wird.

- Ist die Gleichung von obigem Typ aber erfüllt die Integrabilitätsbedingung nicht, so kann man manchmal einen sogenannten **integrierenden Faktor** $M(x,y)$ finden, so dass
$$M(x,y)(P(x,y) + Q(x,y) \cdot \frac{dy}{dx}) = 0$$
exakt wird. Die Lösung erfüllt dann auch
$$P(x,y) + Q(x,y) \cdot \frac{dy}{dx} = 0.$$

- Beispiel: Wir lösen
$$(-x) + y \cdot y' = 0,$$
also
$$(-x) \cdot dx + y \cdot dy = 0.$$
Wegen $\frac{\partial(-x)}{\partial y} = \frac{\partial y}{\partial x} = 0$ ist diese DGL exakt. Wir integrieren
$$\int (-x)\,dx = -\frac{1}{2}x^2 + C(y)$$
und
$$\int y\,dy = \frac{1}{2}y^2 + C(x).$$

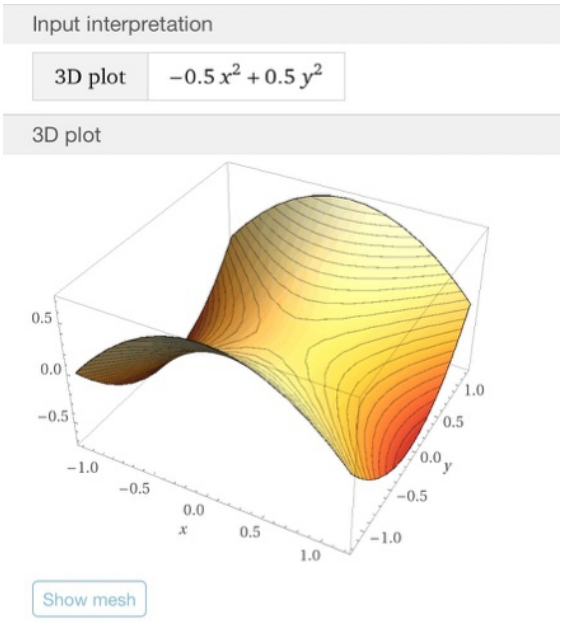


Abbildung 9: Potenzial $F = -\frac{1}{2}x^2 + \frac{1}{2}y^2$ mit einigen Niveaulinien

Anpassen der Integrationskonstanten führt zum Potential

$$F(x, y) = -\frac{1}{2}x^2 + \frac{1}{2}y^2.$$

Niveaulinien finden wir durch lösen von

$$-\frac{1}{2}x^2 + \frac{1}{2}y^2 = k$$

nach y. Wir erhalten als mögliche Lösung

$$y = \sqrt{x^2 + 2k}.$$

Das Potential ist in Abbildung 9 auf Seite 58 zu sehen.

65 Taylorreihen

. . . alle Funktionen sind ganzrational. . .

- Betrachtet man eine Reihe $f(x) = a_0 + a_1x + a_2x^2 + \dots$ zusammen mit ihren Ableitungen und wertet an der Stelle $x = 0$ aus, so findet man, dass $f^{(k)}(0) = k! \cdot a_k$, wobei $f^{(k)}$ die k-te Ableitung von f bezeichnet. Dies führt zur Idee, dass

eine gutmütige Funktion f an einer Stelle x_0 gut durch eine Polynomfunktion approximiert wird; die sogenannte **Taylorreihe** von f:

$$f(x) = \sum_{k=0}^{\infty} \frac{f^{(k)}}{k!} \cdot (x - x_0)^k.$$

Insbesondere hat man für $x_0 = 0$ die sogenannte **MacLaurin-Reihe**

$$f(x) = \sum_{k=0}^{\infty} \frac{f^{(k)}}{k!} \cdot x^k.$$

- Beispiel: Die MacLaurin-Reihe von $f(x) = e^x$ ist wegen $f^{(k)}(0) = 1$

$$f(x) = 1 + x + \frac{1}{2}x^2 + \frac{1}{6}x^3 + \frac{1}{24}x^4 + \cdots = \sum_{k=0}^{\infty} \frac{1}{k!} \cdot x^k.$$

  Die Taylorreihe bei $x_0 = 2$ ist wegen $f^{(k)}(2) = e^2$

$$f(x) = \sum_{k=0}^{\infty} \frac{e^2}{k!} \cdot (x - 2)^k.$$

- Weitere Betrachtungen zeigen, dass man Potenzreihen summieren/subtrahieren, multiplizieren/dividieren, in ihnen substituieren und differenzieren darf, um weitere Reihen zu erhalten.

- Der Taylor-Reihe von $\sin(x)$ um 0 sind wir bereits begegnet:

$$\sin(x) = x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} + \ldots.$$

  In Abbildung 10 auf Seite 60 sieht man die ersten paar Taylor-Approximationen.

66 Potenzreihenansatz

...Das ist was für Physiker.... Mathematicians want the real gem!...

- Taylorreihen können einen auf die Idee bringen, eine Differentialgleichung mit einer **Potenzreihe** zu lösen.

- Beispiel: Wir lösen

$$\ddot{x} = g$$

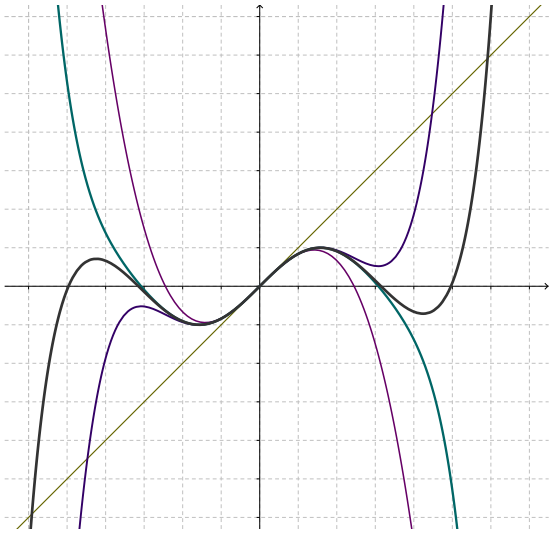


Abbildung 10: Taylor-Approximationen von $\sin(x)$

mit einem Potenzreihenansatz.

Sei $x(t) = a_0 + a_1 t + a_2 t^2 + a_3 t^3 + \dots$. Daraus folgt $\dot{x}(t) = a_1 + 2a_2 t + 3a_3 t^2 + 4a_4 t^4 \dots$ und $\ddot{x}(t) = 2a_2 + 6a_3 t + 12a_4 t^2 + 20a_5 t^3 + \dots$. Nun setzen wir ein

$$2a_2 + 6a_3 t + 12a_4 t^2 + 20a_5 t^3 + \dots = g$$

und vergleichen die Koeffizienten der entsprechenden Potenzen in t:

$$2a_2 = g, \quad 6a_3 = 0, \quad 12a_4 = 0 \quad \dots.$$

Es folgt $a_2 = \frac{1}{2}g$ und $a_k = 0$ für $3 \leq k$. Beachte, dass a_0 und a_1 keiner Bedingung unterworfen werden. Deshalb haben wir wie erwartet

$$x(t) = a_0 + a_1 t + \frac{1}{2} g t^2$$

als Lösung. Wir haben ja die Gleichung „Beschleunigung ist konstant g“ gelöst.

67 Regel von De L'Hôpital

... sehr elegant, sehr elegant...

- Beim Bestimmen von Grenzwerten kann die **Regel von De L'H$^{\text{TM}}$pital** helfen. Sucht man $\lim_{x \to x_0} \frac{f(x)}{g(x)}$ und ist für $x \to x_0$ entweder $f(x) = g(x) = 0$ oder

$f(x) = g(x) = \pm\infty$, so gilt

$$\lim_{x \to x_0} \frac{f(x)}{g(x)} = \lim_{x \to x_0} \frac{f'(x)}{g'(x)}.$$

- Ein Beweis kann via Taylorreihen geführt werden.
- Beispiel:

$$\lim_{x \to 0} \frac{\sin(x)}{x} = \lim_{x \to 0} \frac{\cos(x)}{1} = \frac{1}{1} = 1.$$

68 Grad, Div, Rot

. . . and mathematics explains all of this. . .

- Wir führen zuerst den **Nabla-Operator** ein:

$$\nabla := \begin{pmatrix} \frac{\partial}{\partial x} \\ \frac{\partial}{\partial y} \\ \frac{\partial}{\partial z} \end{pmatrix}.$$

- Salopp: Der **Gradient** ist ein Vektor, der für Punkte eines Skalarfelds in Richtung des steilsten Anstiegs zeigt. Wir definieren für $F : \mathbb{D} \subset \mathbb{R}^n \longrightarrow \mathbb{R}$

$$\text{grad}(F) := \nabla \cdot F = \begin{pmatrix} \frac{\partial F}{\partial x} \\ \frac{\partial F}{\partial y} \\ \frac{\partial F}{\partial z} \end{pmatrix}.$$

- Salopp: Die **Divergenz** gibt für ein Vektorfeld an, wie die stark Vektoren in einer kleinen Umgebung eines Punktes auseinander laufen. Wir definieren für $S = \begin{pmatrix} S_x(x,y,z) \\ S_y(x,y,z) \\ S_z(x,y,z) \end{pmatrix}$

$$\text{div}(S) := \nabla \cdot S = \frac{\partial S_x}{\partial x} + \frac{\partial S_y}{\partial y} + \frac{\partial S_z}{\partial z}.$$

- Salopp: Die **Rotation** für ein Strömungsfeld gibt in jedem Punkt die doppelte Winkelgeschwindigkeit an. Wir definieren für $S = \begin{pmatrix} S_x(x,y,z) \\ S_y(x,y,z) \\ S_z(x,y,z) \end{pmatrix}$

$$\text{rot}(S) := \nabla \times S = \begin{pmatrix} \frac{\partial S_z}{\partial y} - \frac{\partial S_y}{\partial z} \\ \frac{\partial S_x}{\partial z} - \frac{\partial S_z}{\partial x} \\ \frac{\partial S_y}{\partial x} - \frac{\partial S_x}{\partial y} \end{pmatrix}$$

- Integralsatz von Gauss:
$$\int_V \operatorname{div}(\vec{S})\, dV = \oint_A \vec{S}\, d\vec{A}$$

- Zirkulationssatz von Stokes:
$$\oint_A \operatorname{rot}(\vec{S})\, d\vec{A} = \oint_U \vec{S}\, d\vec{s}$$

69 Einige Begriffe aus der Mathematik

. . . Definition, Definition, . . .

- Ein **Körper** $\mathbb{K}$ ist eine Menge versehen mit zwei binären, inneren Verknüpfungen $+$ und $\cdot$, als Addition und Multiplikation bezeichnet, für die gilt:
  - $(\mathbb{K}, +)$ ist eine abelsche Gruppe.
  - $(\mathbb{K} \setminus \{e_+\}, \cdot)$ ist eine abelsche Gruppe.
  - $\cdot$ ist distributiv über $+$.

- Es seien V eine Menge und $(\mathbb{K}, +, \cdot)$ ein Körper, $\oplus : V \times V \longrightarrow V$ (Vektoraddition) eine innere und $\odot : \mathbb{K} \times V \longrightarrow \mathbb{K}$ (Skalarmultiplikation) eine äussere Verknüpfung. Man nennt das Tripel $(V, \oplus, \odot)$ einen **Vektorraum** über dem Körper $\mathbb{K}$ — kurz $\mathbb{K} - VR$ — wenn gilt:
  - $(V, \oplus)$ ist eine abelsche Gruppe.
  - $\odot$ ist distributiv über $\oplus$.
  - $(\alpha + \beta) \odot v = (\alpha \odot v) \oplus (\beta \odot v)$ und $(\alpha \cdot \beta) \odot v = \alpha \odot (\beta \odot v)$
  - $e. \odot v = v$

  Wir notieren von nun an Vektoraddition und Skalarmultiplikation ohne „Ringe“. Die Interpretation ergibt sich aus dem Kontext. Ferner bezeichnen wir Elemente des Vektorraumes mit lateinischen und Elemente des Skalarkörpers mit griechischen Buchstaben. Die neutralen Elemente bezeichnen wir kanonisch mit 0 bzw. 1.

- Ein **Skalarprodukt**, $\langle \cdot, \cdot \rangle : V \times V \longrightarrow \mathbb{R}$ auf einem $\mathbb{R}$-VR ist eine positiv definite, symmetrische Billinearform.

  Das heisst, $\forall a, b, c \in V$ und $\forall \lambda \in \mathbb{R}$ gilt:

- $\langle a, a\rangle \geq 0$ und $\langle a, a\rangle = 0 \implies a = 0_{\oplus}$
- $\langle a, b\rangle = \langle b, a\rangle$
- $\langle a + b, c\rangle = \langle a, c\rangle + \langle b, c\rangle$ und $\langle \lambda a, b\rangle = \lambda\langle a, b\rangle$; analog im zweiten Argument.

- Eine **Norm**, $||\cdot|| : V \longrightarrow \mathbb{R}_0^+$, ist eine Abbildung, so dass $\forall x, y, \in V$ und $\forall \lambda \in \mathbb{K}$ gilt:
  - $||x|| = 0 \implies x = 0$ (definit)
  - $||\lambda x|| = |\lambda|\,||x||$ (absolut homogen)
  - $||x + y|| \leq ||x|| + ||y||$ (subadditiv)
- Sei X eine Menge. Dann heisst eine Abbildung $d : X \times X \longrightarrow \mathbb{R}$ eine **Metrik**, falls $\forall x, y, z \in X$
  - $d(x, y) \geq 0$ und $d(x, y) = 0 \Leftrightarrow x = y$ (positiv definit)
  - $d(x, y) = d(y, x)$ (symmetrisch)
  - $d(x, y) \leq d(x, z) + d(z, y)$ (Dreiecksungleichung)

  (X, d) heisst metrischer Raum, wenn d eine Metrik auf X ist.
- Falls T eine Menge von Teilmengen von X ist, so dass
  - $\emptyset, X \subset T$
  - $\cup_i T_i \in T$
  - $\cap_{i\in\{1,\ldots,n\}} T_i \in T$

  so heisst T eine **Topologie** auf X. (X, T) heisst topologischer Raum und die Elemente $T_k \in T$ heissen **offene Mengen** des topologischen Raumes.
- Gegeben sei eine offene Menge $U \subseteq \mathbb{R}^n$, ein Punkt $x_0 \in U$ und eine Funktion $f : U \longrightarrow \mathbb{R}^m$. Die Funktion f heisst im Punkt x_0 **total differenzierbar**, falls eine lineare Abbildung $l : \mathbb{R}^n \longrightarrow \mathbb{R}^m$ existiert, so dass für die Abbildung $H : \mathbb{R}^n \longrightarrow \mathbb{R}^m$ mit $H(h) = f(x_0 + h) - f(x_0)$ gilt:

$$\lim_{h\to 0} \frac{||r(h)||}{||h||} = 0,$$

  wobei $r(h) := f(x_0 + h) - f(x_0) - l(h)$.

  Existiert l, so ist l eindeutig bestimmt und man nennt sie kurz die Ableitung von f

im Punkt x_0. Man schreibt $f'(x_0)$. Existiert l $\forall x_0 \in \mathbb{R}^n$, so heisst f überall/global differenzierbar; oder einfach differenzierbar.

- Sei $M \subset \mathbb{R}^n$ offen und $f : M \longrightarrow \mathbb{R}$. Falls für ein $x_0 \in M$ und ein $i \in \{1, \ldots, n\}$

$$\frac{\partial f}{\partial x_i}(x_0) := \lim_{h \to 0} \frac{f(x_1, \ldots, x_i + h, \ldots, x_n) - f(x_1, \ldots, x_n)}{h}$$

existiert, so nennt man diesen Quotienten **partielle Ableitung** von f in der i-ten Variablen an der Stelle x_0.
Satz 4. *Existieren alle partiellen Ableitungen von $f : M \longrightarrow \mathbb{R}$ im Punkt x_0 und sind dort stetig, dann ist f total ableitbar in x_0.*

- Seien (X, d_X) und (Y, d_Y) metrische Räume, $f : X \longrightarrow Y$ und $x_0 \in X$. f heisst **stetig** in x_0, falls

$$\forall \epsilon > 0 \quad \exists \delta > 0 \text{ so, dass } \forall x \in X \text{ mit } d_X(x, x_0) < \delta \text{ gilt: } d_Y(f(x), f(x_0)) < \epsilon.$$

- Sei $\langle \cdot, \cdot \rangle$ das handelsübliche Skalarprodukt auf $\mathbb{R}^n$ und $f : \mathbb{R}^n \longrightarrow \mathbb{R}$ partiell differenzierbar im Punkt $x_0 \in \mathbb{R}^n$. Der eindeutig bestimmte Vektor $\text{grad}(f(x_0))$ gegeben durch

$$d\,f(x_0) \cdot h = \langle \text{grad}(f(x_0)), h \rangle$$

mit $h \in \mathbb{R}^n$ heisst **Gradient** von f im Punkt x_0.

70 Wunderschöne Einsichten

. . . ein Vektor ist nicht immer ein „Pfeil“. . .

- Wir werden in Kürze sehen, dass ein Vektor nicht zwingend ein Pfeil sein muss. Deshalb schreiben wir ab dem letzten Abschnitt auch keine Pfeile mehr über die lateinischen Bezeichnungen der Vektorraumelemente.

- Hat man in einem $\mathbb{R}$-VR ein Skalarprodukt $\langle \cdot, \cdot \rangle$ definiert, so impliziert dieses in kanonischer Weise eine Norm via $|| \cdot || := \sqrt{\langle \cdot, \cdot \rangle}$, welche ihrerseits in kanonischer Weise eine Metrik impliziert, durch $d(x, y) := ||x - y||$. Diese Metrik impliziert in kanonischer Weise wiederum eine Topologie, $T := \{M \subset V \mid \forall x \in M \ \exists \epsilon > 0 \text{ mit } U_\epsilon(x) \subset M\}$ wobei $U_\epsilon(x) := \{y \in V \mid d(x, y) < \epsilon\}$.

- Beispiel: Wir definieren im $\mathbb{R}$-VR $\mathbb{R}^3$ das Standardskalarprodukt

$$\langle v, w \rangle := v_x w_x + v_y w_y + v_z w_z.$$

Dieses ist positiv definit, symmetrisch und billinear (check!). Dann ist die Norm $||v|| = \sqrt{\langle v, v \rangle} = \sqrt{v_x^2 + v_y^2 + v_z^2}$ (check!), was wir als Länge von v kennen. Die

Metrik $d(v,w) = ||v-w|| = \sqrt{(v_x-w_x)^2+(v_y-w_y)^2+(v_z-w_z)^2}$ (check!) beschreibt den Abstand der Punkte v und w (als Ortsvektoren aufgefasst). Die Topologie entspricht der Menge aller offenen Kugeln (ohne Rand/Oberfläche) um alle Punkte des 3D-Raumes.

- Eine endliche Familie von Vektoren $v_1, \ldots, v_n$ heisst **linear unabhängig**, wenn

$$\alpha_1 v_1 + \cdots + \alpha_n v_n = 0 \implies \alpha_1 = \cdots = \alpha_n = 0.$$

- Eine (Hamel-)**Basis** ist eine linear unabhängige Menge von Vektoren, die den ganzen VR mit Linearkombinationen erzeugt. (Linearkombination bedeutet: Du nimmst die Basisvektoren und darfst $\oplus$ und $\odot$ brauchen.)

- Beispiel: $\{e_x, e_y, e_z\}$ ist eine Basis des $\mathbb{R}$-VR $\mathbb{R}^3$.

- Sei ein Skalarprodukt $\langle \cdot, \cdot \rangle$ auf einem $\mathbb{R}$-VR gegeben. $v, w \in V$ heissen **orthogonal**, falls

$$\langle v, w \rangle = 0.$$

  Eine Basis heisst orthogonal, falls alle Basisvektoren paarweise orthogonal sind.

  Eine orthogonale Basis heisst **orthonormal**, falls für alle Basisvektoren b_i gilt: $||b_i|| = 1$.

- Beispiel: $\{e_x, e_y, e_z\}$ ist eine Orthonormalbasis (check!).

71 Der „Fourierreihen-Vektorraum“

- Eine 2π-periodische Funktion lässt sich als Reihen mit einer Konstanten und sin & cos Termen approximieren. (Dies kann leicht auf Funktionen mit beliebiger Periode erweitert werden.) Man hat

$$f(x) = \frac{a_0}{2} + \sum_{k=1}^{\infty} (a_k \cos(kx) + b_k \sin(kx)),$$

  wobei für $k \in \mathbb{N}$

$$a_0 = \frac{1}{\pi} \int_{-\pi}^{\pi} f(x)\, dx$$

$$a_k = \frac{1}{\pi} \int_{-\pi}^{\pi} f(x) \cos(kx)\, dx$$

$$b_k = \frac{1}{\pi} \int_{-\pi}^{\pi} f(x) \sin(kx)\, dx$$

- Beispiel: $\{\frac{1}{2}, \sin(kx), \cos(kx)\}$ ist eine Orthonormalbasis für den VR der 2π-periodischen Funktionen mit Skalarprodukt

$$\langle f, g\rangle := \frac{1}{\pi}\int_{-\pi}^{\pi} f(x)\cdot g(x)\,dx$$

(check!). Hier sind also die Vektorraumelemente Funktionen! Linearkombinationen entsprechen den Fourierreihen von Funktionen.

Jetzt kann man auch Norm, Metrik und eventuell Topologie induzieren...; viel Spass!

72 Maxwell-Gleichungen

...and God said...and there was light...

- Herz des Elektromagnetismus, die **Maxwell-Gleichungen** mit Leiter/Ladungen im Vakuum
  - $\nabla\cdot\vec{E} = \frac{\rho}{\epsilon_0}$ (Gauss)
  - $\nabla\cdot\vec{B} = 0$ (Gauss)
  - $\nabla\times\vec{E} = -\frac{\partial\vec{B}}{\partial t}$ (Stokes)
  - $\nabla\times\vec{B} = \mu_0\vec{j} + \epsilon_0\mu_0\frac{\partial\vec{E}}{\partial t}$ (Stokes & Maxwell)
- Die Maxwell-Gleichungen im Vakuum
  - $\nabla\cdot\vec{E} = 0$
  - $\nabla\cdot\vec{B} = 0$
  - $\nabla\times\vec{E} = -\frac{\partial\vec{B}}{\partial t}$
  - $\nabla\times\vec{B} = \epsilon_0\mu_0\frac{\partial\vec{E}}{\partial t}$

  führen zur Einsicht, dass es elektromagnetische Transversalwellen geben muss, wobei die Ausbreitungsrichtung, B und E paarweise senkrecht aufeinander stehen.
- Mit $\nabla\times(\nabla\times\vec{E}) = \nabla(\nabla\cdot\vec{E}) - \triangle\vec{E}$, wobei $\triangle$ den **Laplace-Operator** bezeichnet, folgt nach kurzer Rechnung die Ausbreitungsgeschwindigkeit einer elektromagnetischen Welle:

$$c = \frac{1}{\sqrt{\epsilon_0\mu_0}} \approx 299\,792\,458\,\mathrm{m/s}.$$

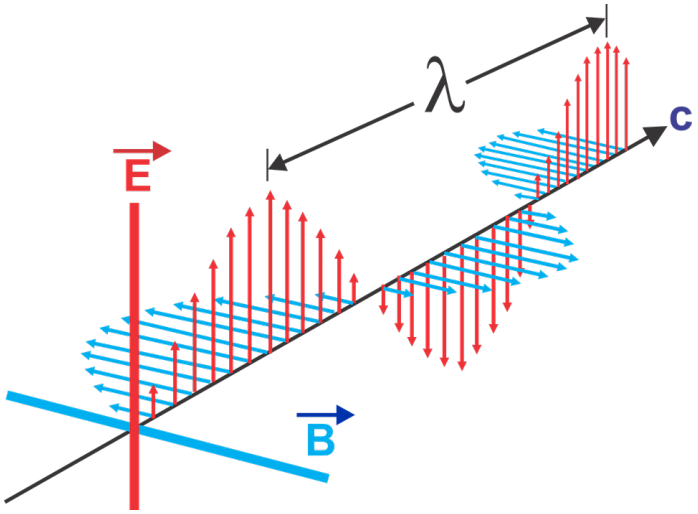


Abbildung 11: Skizze einer elektromagnetischen Welle im Fernfeld

73 Mathematische Einblicke in die Quantentheorie

...und täglich grüssen die VRs...

- Quantenmechanische Teilchen können als Elemente des Hilbertraums $\mathcal{L}^2$ beschrieben werden. Die Vektoren sind Wellenfunktionen, Ψ, welche absolut quadratintegrierbar sind. Das Skalaprodukt ist gegeben durch

$$\langle f, g \rangle = \int \overline{f(x)} g(x)\, dx.$$

  Zwischen dem Ortsraum und dem Impulsraum wechselt man mit der Fouriertransformation

$$\Phi(p) = \frac{1}{\sqrt{2\pi\hbar}} \int \Psi(x) e^{-\frac{ipx}{\hbar}}\, dx$$

$$\Psi(x) = \frac{1}{\sqrt{2\pi\hbar}} \int \Phi(p) e^{\frac{ipx}{\hbar}}\, dp$$

  Ein Teilchen, das sich bewegt, entspricht einem Element/Vektor des Hilbertraums $\mathcal{L}^2$. Die Addition entspricht der Überlagerung von Zuständen.

  Wie kommt man auf diese Elemente des Hilbertraums?

- Erwin Schrödinger postulierte 1926 die **Schrödingergleichung**

$$i\hbar \cdot \frac{\partial \Psi}{\partial t} = \hat{H} \cdot \Psi$$

  wobei $\hat{H}$ den **Hamiltonoperator** bezeichnet, welcher die Energien beschreibt.

- Mit dem **Impulsoperator**
$$\frac{\hat{p}^2}{2m}$$
beschreibt man die kinetische Energie und mit der Bezeichnung $V(x)$ für ein Potential lautet die Schrödingergleichung
$$i\hbar \cdot \frac{\partial \Psi}{\partial t} = [-\frac{\hbar^2}{2m}\triangle + V(x)] \cdot \Psi$$

- Ein Separationsansatz in Zeit und Ort mit konstanter Energie E führt zu den Lösungen
$$\varphi(t) = A \cdot e^{-\frac{-iE}{\hbar}}$$
für die Zeitabhängigkeit und für einen Potentialtopf der Breite a, in dem das Teilchen gefangen ist,
$$u(x) = -u_0 \cdot \frac{2mE}{\hbar^2} \sin(\frac{2mE}{\hbar^2} \cdot x + \delta)$$
für die Ortsabhängigkeit. Schliesslich erhält man unter Einbindung der Nebenbedingungen und mit der Normierung (wegen der Interpretation als Aufenthaltswahrscheinlichkeit) die Lösung
$$\Psi(x,t) = \sqrt{\frac{2}{a}} \cdot \sin(\frac{n\pi}{a} \cdot x) \cdot e^{-\frac{iE_n}{\hbar} \cdot t}$$
zu den diskreten **Energieeigenwerten** $E_n = \frac{\hbar^2\pi^2}{2ma^2} \cdot n^2$ mit $n \in \mathbb{N}$.

- Nun könnte man sich weitere Fragen stellen...

74 Freie Schwingung

...I like Complex Numbers...

- Wir betrachten eine Masse m an einer Feder mit Federkonstante k und fragen nach der Funktion des Ortes $y(t)$. Zur Bewegungsgleichung
$$\ddot{y} + \frac{k}{m} \cdot y = 0$$
finden wir kurze Zeit später deren Lösung
$$y(t) = y_0 \cdot \sin(\omega_0 \cdot t + \varphi_0),$$
wobei $\omega_0 = \sqrt{\frac{k}{m}}$ die **Eigenfrequenz** bezeichnet.

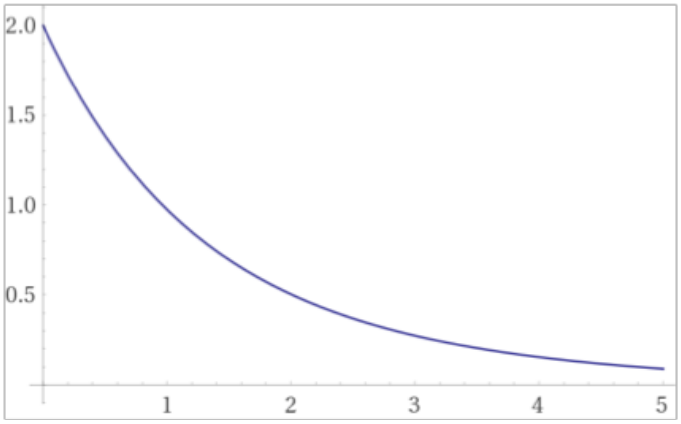


Abbildung 12: Kriechfall einer gedämpften Schwingung

75 Freie gedämpfte Schwingung

. . . etwas realistischer. . .

- Mit dem Reibungskoeffizienten α notieren wir die Bewegungsgleichung

$$\ddot{y} + \frac{\alpha}{m} \cdot \dot{y} + \frac{k}{m} \cdot y = 0.$$

- Die Lösung führt, mit der **Dämpfungskonstanten** $\beta = \frac{\alpha}{2m}$, zur („gedämpften“) Frequenz $\omega_d = -\beta \pm \sqrt{\beta^2 - \omega_0^2}$, die eine Fallunterscheidung Nahe legt.

  – $\beta^2 - \omega_0^2 > 0$: Die allgemeine Lösung für diesen Kriechfall ist

$$y(t) = c_1 e^{\omega_{d1} t} + c_2 e^{\omega_{d2} t}.$$

  – $\beta^2 - \omega_0^2 < 0$: Die allgemeine Lösung für diesen schwingenden Fall ist

$$y(t) = A e^{-\beta t} \cdot \sin(\omega_d \cdot t + \varphi_0),$$

  wobei $\omega_a = \sqrt{\omega_0^2 - \beta^2}$ für die „reduzierte“ Frequenz der gedämpften Schwingung stehen soll. Das sieht dann aus wie in Abbildung 13 auf Seite 70.

  – $\beta^2 - \omega_0^2 = 0$: In diesem Fall erhalten wir, nach möglichem kurzen Ausschlag, einen Kriechfall. In der Literatur findet man den Namen aperiodischer Grenzfall. Die allgemeine Lösung sieht so aus:

$$y(t) = (c_1 t + c_2) \cdot e^{-\beta \cdot t},$$

  illustriert in Abbildung 14 auf Seite 70.

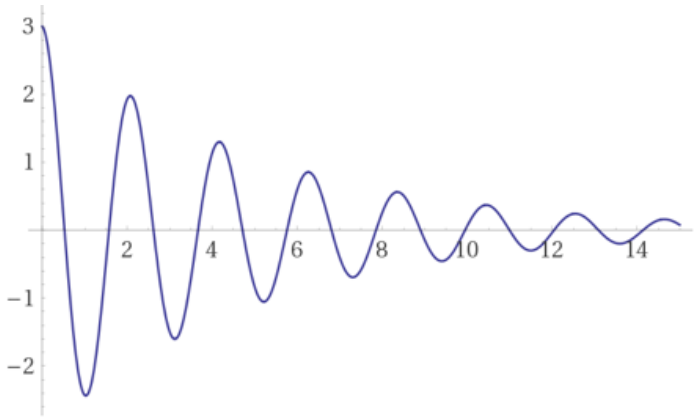


Abbildung 13: Gedämpfte Schwingung

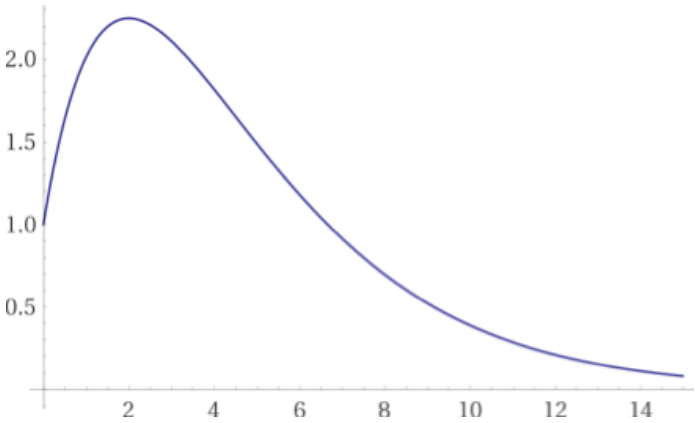


Abbildung 14: Aperiodischer Grenzfall einer gedämpften Schwingung

76 Erzwungen gedämpfte Schwingung

...Qualitativ logo...Jetzt quantitativ...

- Die Lösung der Bewegungsgleichung

$$m \cdot \ddot{y} + \alpha \cdot \dot{y} + k \cdot y = F_{ext}$$

wollen wir speziell für eine periodische Anregung suchen. Wir kennen bereits aus der vorherigen Section die Lösung der homogenen Gleichung.

- Etwas später finden wir die Anregung $F_0 \cos(\omega_a \cdot t)$ die partikuläre Lösung

$$y_p(t) = \frac{\frac{F_0}{m}}{\omega_0^2 - \omega_a^2 + i \cdot 2\beta\omega_a} \cdot e^{i\omega_a \cdot t}.$$

- Die Amplitude ist

$$\frac{F_0}{m\sqrt{(\omega_0^2 - \omega_a^2)^2 + (2\beta\omega_a)^2}}$$

und die Phase

$$\arctan(-\frac{2\beta\omega_a}{\omega_0^2 - \omega_a^2}).$$

- Weil Amplitude und Frequenz von der Anregungsfrequenz abhängen, und die Amplitudenfunktion ein Maximum hat (Resonanz), bestimmen wir letzteres. Die maximale Amplitude

$$\frac{F_0}{2m\beta\sqrt{\omega_0^2 - \beta^2}}$$

haben wir bei einer Frequenz von

$$\omega_{a_{max}} = \sqrt{\omega_0^2 - 2\beta^2}.$$

- Die allgemeine Lösung hat die Form

$$y(t) = Ae^{-\beta t}\sin(\omega_d t + \varphi_0) + \frac{F_0}{m\sqrt{(\omega_0^2 - \omega_a^2)^2 + (2\beta\omega_a)^2}}\cos(\omega_a t + \arctan(-\frac{2\beta\omega_a}{\omega_0^2 - \omega_a^2}).$$

Abbildung 15 auf Seite 72 zeigt den charakteristischen „Einschwingvorgang„ und die folgende Periodizität mit der Eingangsfrequenz.

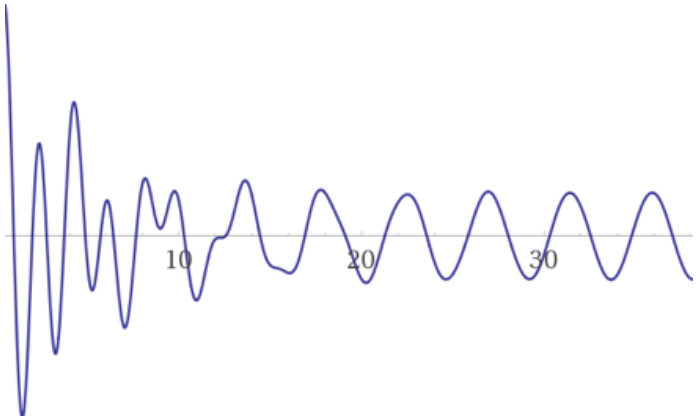


Abbildung 15: Erzwungen gedämpfte Schwingung

77 RLC (in Serie)

. . . einfach genial. . .

- Man will für eine bekannte, angelegte Spannung $U_{in}(t)$ den Strom $I(t)$ in einem RLC-Seriekreis (siehe Abbildung 16 auf Seite 73) kennen. Man findet die Differentialgleichung
$$\dot{U}_{in} = R \cdot \dot{I} + L \cdot \ddot{I} + \frac{1}{C} \cdot I.$$
Diese Gleichung hat prinzipiell dieselbe Form wie die Gleichung zur gedämpften Feder mit externem Antrieb.

- Bei „beliebegem“ Input löst man die Differentialgleichung numerisch. Bei einer angelegten Wechselspannung
$$U_{in}(t) = U_0 \cdot e^{i\omega t}$$
lässt sich die vorliegende Gleichung mit einem Ansatz der Form
$$I(t) = I_0 \cdot e^{i(\omega t + \varphi)}$$
lösen, da wir analog zur Feder mit externem Antrieb vorgehen.

- Nach kurzer Rechnung findet man (für diese Situation wie in Abbildung 16 auf Seite 73) den „komplexen Widerstand“, aka die **Impedanz**,
$$Z = R + i\omega L - \frac{i}{\omega C}.$$
Für die Stromamplitude folgt $I_0 = \frac{U_0}{|Z|}$ und für die Phase $\varphi = -\varphi_Z$.

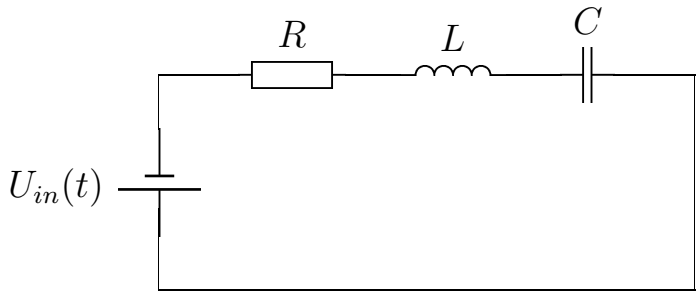


Abbildung 16: Schema eines RLC-Seriekreises

- Man sieht, dass im Falle $\omega = \frac{1}{\sqrt{LC}}$ I_0 maximal wird (Resonanz / Thomson-Frequenz). Bei kleinen Frequenzen sperrt der Kondensator (kapazitiv), bei hohen Frequenzen die Spule (induktiv). Den reellen Anteil der Impedanz Z nennt man **Wirkwiderstand**, den imaginären Anteil **Blindwiderstand**. Der Betrag $|Z|$ heisst **Scheinwiderstand**.

78 Hinweise zu Beispielen

...high noon soon...

Im Sinne einer themenübergreifenden Repetition können folgende Module eingeordnet werden:

- Das Warteschlangenproblem bei Burger-King
- Eigenfrequenzen gekoppelter Wagons
- Berechnung der Page-Ranking Eigenvektoren von Google
- ...

Andere, grössere oder schöne Module sind:

- Basics der Algebra: Gruppen
- Pretty Good Privacy mit RSA
- Die explizite Fibonacci-Formel vai Diagonalmatrizen und Basiswechsel
- Von den Walen zur Mandelbrotmenge

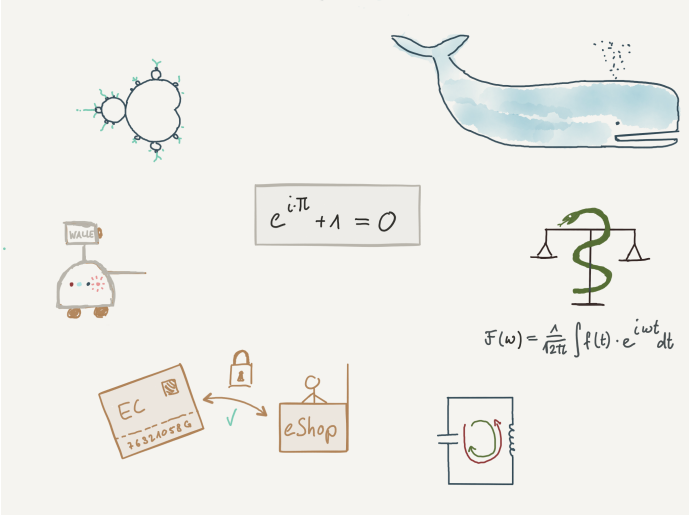


Abbildung 17: Illustration ausgewählter AM-Themen

- Frequency-Phishing mit Fourier
- Basics der linearen Algebra: Vektorräume
- „Disciples at Emmaus“: Altersbestimmung eines Gemäldes
- Die Raketengleichung: Von Nutzlasten und anderen Problemen...

Abbildungsverzeichnis