Mathematische Modellbildung

Skript zur Vorlesung Mathematische Modellbildung
für das Lehramt an Grund-, Haupt-, und Realschulen
an der Carl von Ossietzky Universität Oldenburg
im Sommersemester 2005

Cora Kohlmeier

27. Juni 2005

Inhaltsverzeichnis

1 Einführung

1.1 Was ist Modellbildung – mathematische Modellierung

Die mathematische Modellbildung oder mathematische Modellierung

- bezeichnet eine Methode
- ist nicht an eine spezielle Wissenschaft gebunden und wird in Naturwissenschaften und Technik und in der Ökonomie angewendet
- versucht Teile der Realität mathematisch begreifbar zu machen

(Natur)-Wissenschaft ist Modellierung: In der Wissenschaft werden Modelle aufgestellt, um eine vorgebenen Fragestellung zu beantworten.

Jedes Modelliervorhaben braucht eine Leitfrage oder ein Ziel!

Dies ist wichtig, da die Art und die Komplexität eines Modells von dieser Zielvorgabe abhängt. Ein Modell soll einen Teilaspekt der Realität so darstellen, dass es die Information liefern kann, die zur Beantwortung einer Leitfrage notwendig ist.
Beispiel:
Ein Klimamodell taugt nicht zur Wettervorhersage, ein Regentropfenmodell auch nicht.

1.2 Was ist ein Modell ?

Hierfür gibt es keine eindeutige Definition. Man könnte es wie folgt beschreiben:
Ein Modell ist ein Objekt oder Konzept, das benutzt wird, um einen realen Aspekt so darzustellen, dass er in Hinblick auf eine Zielfrage verstanden werden kann. Beispiele für Modelle sind:

- ein Landschaftsbild
- Landkarten
- Wettermodelle

1.2.1 Merkmale von Modellen

- Vereinfachung. Es werden nur die wesentlichen Aspekt durch das Modell beschrieben. Will man z.B. das Volumen eines Würfels berechnen, so ist dessen Farbe unwichtig.
- Skalierung in Raum und Zeit. Ein Atommodell stellt das Atom in einer Größe dar, die wir sehen können, ein Globus ist so klein, dass er bequem auf dem Schreibtisch stehen kann. Modelle zur Wettervorhersage müssen schneller sein als das Wetter selbst.
- Modelle haben einen begrenzten Gültigkeitsbereich, z.B. gelten die Newton'schen Gesetze nicht nahe der Lichtgeschwindigkeit

1.2.2 Arten von Modellen

- einfache Modelle, die Prinzipien erklären, z.B. Beschreibung des radioaktiven Zerfalls durch die Exponentialfunktion
- komplexe Modelle, wie z.B. Klimamodelle, die die Atmosphäre und die Ozeanströmungen berücksichtigen
- empirische Modelle, die einen funktionalen Zusammenhang zu Messdaten liefern
- prozessorientierte Modelle
- deterministische Modelle
- stochastische Modelle

Diese Einteilung ist nicht eindeutig! Z.B. Können einfache Modelle sowohl deterministisch als auch stochastisch gebildet werden.

1.2.3 Modell-Simulation

Ergebnisse von Modellen erhält man durch eine Simulation. Die Simulation liefert eine Realisierung des Modells. Das Modell gibt die Einsicht in die Zusammenhänge, die Simulation liefert ein Ergebnis, das z.B. mit Messdaten verglichen werden kann. Wird dieser Vergleich für ausreichend gut befunden, so kann das Modell den beschriebenen Sachverhalt reproduzieren. Zeigt der Vergleich von Simulationsergebnis mit den Daten Abweichungen, so muss dass Modell verbessert werden.

2 Empirische Modelle

Bei der empirischen Modellierung wird ausgehend von einem oder mehreren Datensätzen versucht, einen funktionalen Zusammenhang zu bestimmen, der diese Daten ausreichend gut reproduziert.

2.1 Parameteranpassung

Bei der Parameteranpassung wird eine Funktion vorgegeben und die Parameter der Funktion anhand der Messdaten bestimmt. Es seien z.B. folgende Werte für die Wassertemperatur an der Nordseeküste gegeben (Abbildung 2.1):.

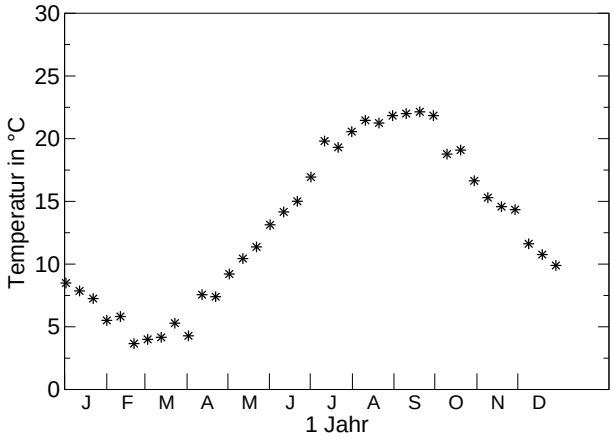
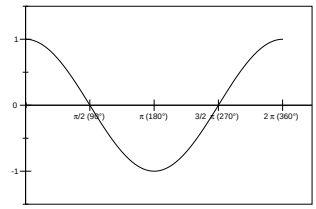


Abbildung 2.1: Jahresgang der Wassertemperatur an der Norseeküste (Beispiel)

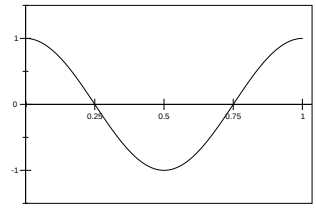
Diese Werte sollen nun durch eine Kosinusfunktion approximiert werden. Aus der Grafik erkennt man, dass der kälteste Zeitraum Mitte Februar bis Mitte März ist. Wir nehmen als kältesten Tag den Tag 60 an. Die kälteste gemessene Temperatur beträgt ca. 4 $°C$ die wärmste ca. 22 $°C$. Die Temperaturdifferenz beträgt somit 18 $°C$, die mittlere Temperatur ca. 13 $°C$.

Die Kosinusfunktion soll nun so verändert werden, dass sie zu den Daten passt:

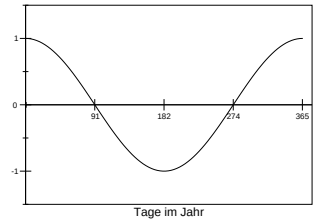
Die Kosinusfunktion: $T = \cos(t)$



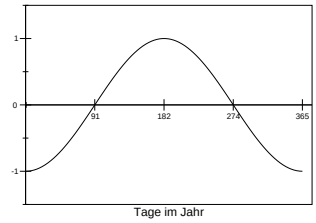
Skalierung auf $[0,1]$ $T = \cos(2\pi t)$



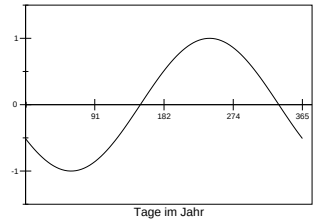
Skalierung auf 1 Jahr $T = \cos(\frac{2\pi t}{365})$



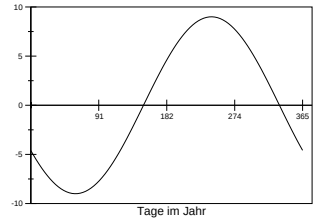
Im Winter soll es kalt sein $T = -\cos(\frac{2\pi t}{365})$



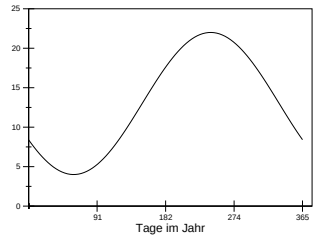
Der kälteste Tag ist Tag 60 $T = -\cos(\frac{2\pi(t-60)}{365})$



Die Amplitude beträgt 9 $^\circ C$ $T = -9\cos(\frac{2\pi(t-60)}{365})$



Der Mittelwert beträgt 13 $^\circ C$ $T = 13 - 9\cos(\frac{2\pi(t-60)}{365})$



Man erhält so eine Kurve, die recht gut zu den Daten passt (Abbildung 2.2).

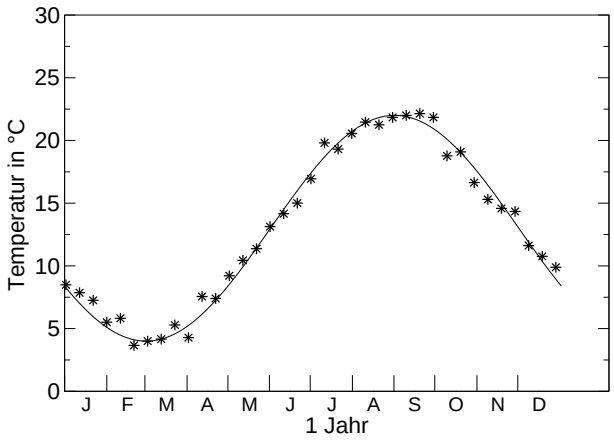


Abbildung 2.2: Jahresgang der Wassertemperatur an der Norseeküste und daran angepasste Kosinusfunktion.

2.2 Lineare Regression

Im vorherigen Beispiel haben wir die Parameter der Kosinuskurve anhand von wenigen Charaketristika, wie die Lage der Extrema bestimmt. Im folgenden wird ein Verfahren beschrieben, dass die Anpassung einer Geraden an gegebene Messwerte unter Berücksichtigung aller Messwerte erreicht.
Für das Wachstum einer Bohne seien folgende Messwerte für die Zeit in Tagen seit der Pflanzung und die zu dieser Zeit gemessene Höhe der Bohne gegeben:

Zeit in Tagen	3	5	10	15	20	30	40	50	60	70	80	100
Höhe in cm	0,5	1	2	7	15	30	70	130	170	230	248	252

In Abbildung 2.4 erkennt man, dass im Bereich zwischen dem 20. Tag und dem 70. Tag wahrscheinlich ein linearer Zusammenhang zwischen der Wachstumszeit und der Wachstumshöhe besteht. Diesen Zusammenhang kann man durch eine Geradengleichung beschreiben:

$$y = m \cdot x + b$$

Wir wollen nun m und b bestimmen. Dabei interessiert uns insbesondere m, die Steigung der Geraden. Sie ist ein Maß für die Wachstumsgeschwindigkeit. Eine solche Gerade kann man z.B. erhalten, wenn man zwei beliebige Punkte in diesem Bereich miteinander verbindet. Handelt es sich tatsächlich um einen linearen

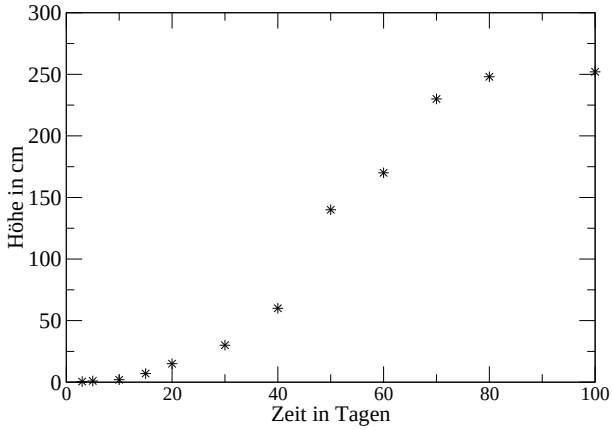


Abbildung 2.3: Wachstum einer Stangenbohne.

Zusammenhang und sind die Messungen nicht fehlerbehaftet, so kann man so die Steigung und damit die Wachstumsgeschwindigkeit erhalten. Liegen aber nicht alle Punkte auf dieser Geraden, so wird die Lage der Geraden von der Wahl der Punkte abhängen.
In der Realität wird aber weder das Wachstum exakt einem linearen Zusammenhang folgen (Bohnen wissen gar nicht, was das ist) noch wird man die Höhe derart exakt messen. In Abschnitt 2.2.1 wird daher ein Verfahren vorgestellt, eine Gerade zu bestimmen, die allen Punkten in diesem Bereich Rechnung trägt.
Aber nehmen wir mal beispielsweise die Gerade, die durch die Punkte bei t=20 und t=70 läuft, dann gilt:

$$\begin{aligned} 15 &= m \cdot 20 + b \\ 230 &= m \cdot 70 + b \end{aligned}$$

Auflösen ergibt $m = 4.3$ und $b = -71.0$.
Man kann die Steigung m auch erhalten, indem man ein Steigungsdreieck betrachtet:

$$m = \frac{\Delta y}{\Delta x} = \frac{230\,\text{cm} - 15\,\text{cm}}{70\,\text{Tage} - 20\,\text{Tage}}$$

Im betrachteten Zeitintervall wächst die Bohne also $4.3\,\text{cm}/\text{Tag}$.
Die Methode, nur zwei Punkte zu berücksichtigen, ist natürlich falsch, da sich Messfehler und Abweichungen in diesen Punkten stark auf die Lage der Geraden auswirken. Besser ist es alle Punkte zu berücksichtigen, die im Bereich des linearen Wachstums liegen. Hierzu gibt es die Methode der kleinsten Quadrate auch lineare Regression genannt.

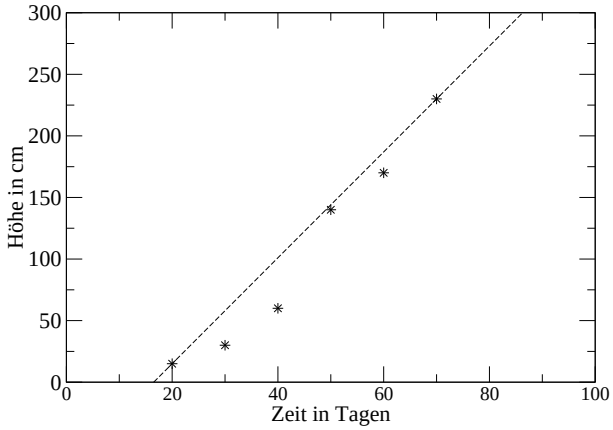


Abbildung 2.4: Wachstum einer Stangenbohne. Dargestellt sind die Messwerte und die Gerade, die durch die Punkte (20,15) und (70,230) geht.

2.2.1 Methode der kleinsten Quadrate

Seien $t_1 < t_2 < \cdots < t_n$ die n Zeitpunkte, an denen die n Messwerte $y_1, y_2, \cdots, y_n$ gemessen wurden. Der Datenbereich des Beispiels aus 2.2, in dem lineares Wachstum angenommen wird, ist durch

Zeit t_i	20	30	40	50	60	70
Höhe y_i	15	30	70	130	170	230

gegeben.
Es soll nun eine Gerade $y(t) = m \cdot t + b$ so bestimmt werden, dass die Summe der Quadrate der Abweichungen von Messdaten und Geraden minimal wird.

$$S(m,b) := \sum_{i=1}^{n} (y_i - y(t_i))^2 = \sum_{i=1}^{n} (y_i - (m \cdot t_i + b))^2$$

soll also minimal werden. Im Beispiel muss also

$$\begin{aligned} S(m,b) &:= (15 - (m \cdot 20 + b))^2 + (30 - (m \cdot 30 + b))^2 + (70 - (m \cdot 40 + b))^2 \\ &+ (130 - (m \cdot 50 + b))^2 + (170 - (m \cdot 60 + b))^2 + (230 - (m \cdot 70 + b))^2 \end{aligned}$$

minimal werden.

Anmerkung für Analytiker: Mit ein wenig Differentialrechnung kann man das Minimum dieser Funktion bestimmen, indem man die Ableitung von S nach m gleich null setzt und die Ableitung von S nach b gleich null setzt. Dann hat man zwei Gleichungen mit den zwei Unbekannten m und b und kann diese lösen (Formal muss man natürlich zeigen, dass es sich tatsächlich um ein Minimum handelt!).

Satz 2.2.1 Methode der keinsten Quadrate (lineare Regression)
Es seien n Messwerte $y_i, i = 1 \cdots n$ zu den Zeitpunkten $t_i, i = 1 \cdots n$ gegeben. Die Summe der Abstandsquadrate der Messwerte von der Geraden $y(t) = m \cdot t + b$ wird durch

$$m = \frac{n \cdot \sum_{i=1}^{n} t_i \cdot y_i - T \cdot Y}{n \cdot \sum_{i=1}^{n} t_i^2 - T \cdot T} \qquad b = \frac{1}{n}(Y - mT)$$

minimiert. Hierbei seien

$$T := \sum_{i=1}^{n} t_i = t_1 + \cdots + t_n \qquad Y := \sum_{i=1}^{n} y_i = y_1 + \cdots + y_n$$

Im Beispiel erhält man die Gerade

$$y = 4.44 \cdot t - 92.43$$

Das so bestimmte Wachstum beträgt also 4.44 cm/Tag. In Abbildung 2.5 sieht man, dass die Gerade zwar keinen der Messpunkte genau trifft, aber trotzdem besser ist als die Gerade in Abbildung 2.4. Dies liegt daran, dass Ausreisser weniger stark einfliessen. Das Verfahren der linearen Regression ist in vielen wissenschaftlichen

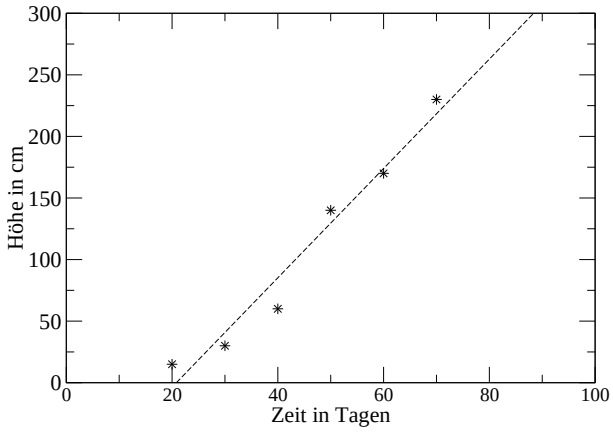


Abbildung 2.5: Wachstum einer Stangenbohne. Dargestellt sind die Messwerte, für die ein lineares Wachstum angenommen wird, und die Ausgleichgerade, die sich nach der Methode der kleinsten Quadrate ergibt.

Taschenrechnern und Tabellenkalulationsprogrammen implementiert.

2.3 Logarithmischer Zusammenhang am Beispiel der Karzinogenese

Häufig folgen natürliche Prozesse keinem linearen Zusammenhang. Am folgenden Beispiel soll gezeigt werden, wie die Methode der linearen Regression auf Prozesse angewendet werden kann, die einem logarithmischen Zusammenhang folgen.

Beispiel: Karzinogenese bei Ratten.

Durch Gabe von Diethylnitrosamin, kann bei Ratten Krebs ausgelöst werden. Je höher die tägliche Dosis ist, desto schneller entwicken die Ratten einen Tumor. Die Zeit von der Diethylnitrosamingabe bis zur Ausbildung des Tumors heisst Latenzzeit. Es besteht folgender Zusammenhang

Dosis in mg/kg/Tag	0.075	0.15	0.3	0.6	1.25	2.5	5.0	10.0
Latenzzeit in Tagen	1020	645	480	360	265	225	150	120

Auf den ersten Blick kann man nicht entscheiden, welcher Zusammenhang besteht (Abbildung 2.6).

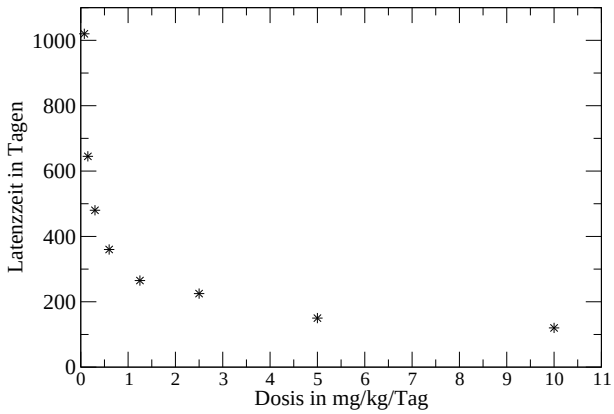


Abbildung 2.6: Karzinogenese bei Ratten. Aufgetragen sind die Dosis an Diethylnitrosamin und die zugehörige Zeit bis zur Ausbildung eines Tumors (Latenzzeit)

Trägt man die Datenpunkte doppelt logarithmisch auf so erkennt man den Zusammenhang (Abbildung 2.7). Doppelt logarithmisch bedeutet, dass sowohl die x- als auch die y-Achse logarithmisch sind. Hierbei ist es unerheblich, ob man die Achsenskalierungen logarithmisch wählt oder die Werte in der Tabelle logarithmiert und die Achsen linear skaliert (siehe Achsen in Abbildung 2.7). Es scheint ein linearer Zusammenhang zwischen dem Logarithmus der Dosis und dem Logarithmus der Latenzzeit zu bestehen:

$$log(Latenzzeit) = m \cdot log(Dosis) + b$$

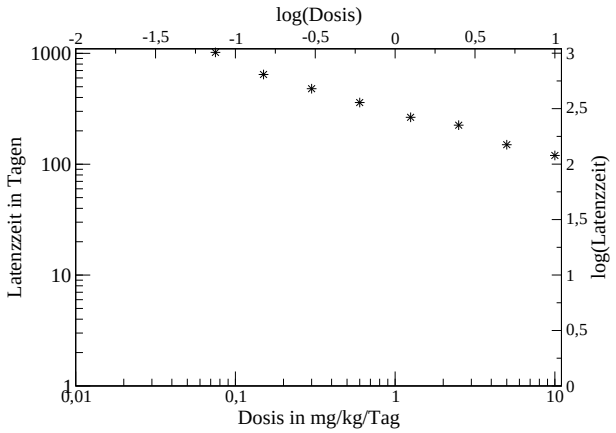


Abbildung 2.7: Karzinogenese bei Ratten. Aufgetragen sind die Dosis an Diethylnitrosamin und die zugehörige Zeit bis zur Ausbildung eines Tumors (Latenzzeit) in doppelt logarithmischer Darstellung

Die Parameter m und b kann man nun mit der Methode der kleinsten Quadrate bestimmen. Hierzu macht man sich zuerst die Wertetabelle der logarithmierten Werte. Man beachte, dass diese Werte keine Einheit haben!!:

log(Dosis)	-1.12	-0.82	-0.52	-0.22	0.1	0.4	0.7	1
log(Latenzzeit)	3.009	2.810	2.681	2.556	2.423	2.352	2.176	2.079

Man erhält $m = -0.42$ und $b = 2.48$.
Aus $log(Latenzzeit) = m \cdot log(Dosis) + b$ folgt

$$Latenzzeit = 10^{m \cdot log(Dosis)+b} = 10^b \cdot Dosis^m = e^{b \cdot ln(10)+m \cdot ln(Dosis)}$$

Dieser funktionale Zusammenhang ist in Abbildung 2.8 dargestellt. Man hat nun eine Funktion mit der man zu einer gegebenen Dosis die Latenzzeit bestimmen kann. In der Praxis wird die tatsächliche Latenzzeit davon abweichen (Ratten sind keine Computer). Auch weiss man nicht, welchen Gültigkeitsbereich das Gesetz hat (bei sehr hohen Dosen werden die Ratten vermutlich viel schneller Tumore entwickeln, bei sehr niedrigen eventuell gar keine).

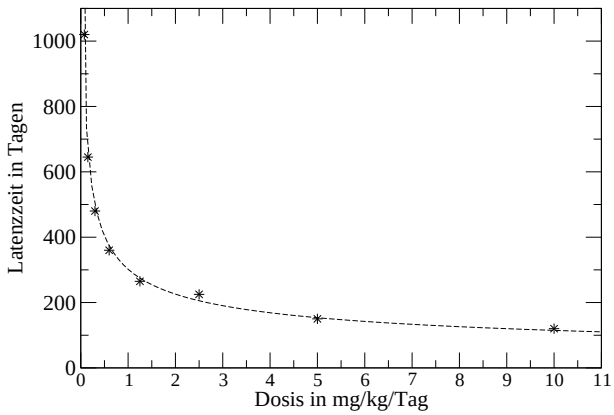


Abbildung 2.8: Karzinogenese bei Ratten. Aufgetragen sind die Dosis an Diethylnitrosamin und die zugehörige Zeit bis zur Ausbildung eines Tumors (Latenzzeit) sowie der funktionale Zusammenhang, der sich nach der Methode der kleinsten Quadrate ergibt.

3 Prozessorientierte Modelle

Im vorherigen Kapitel haben wir ausgehend von Messwerten einen funktionalen Zusammenhang hergestellt. Manchmal hat man aber das Problem, dass es keine Messungen gibt. In diesem Fall fragt man die Experten z.B. Biologen oder Physiker wie sich das System, das man durch ein Modell beschreiben möchte, verhält[1].

3.1 Freier Fall

Will man beschreiben, in welcher Höhe H sich eine fallende Kugel zur Zeit T befindet, wenn sie zur Zeit $t_0 = 0$ in der Höhe H_0 losgelassen wird, so wird man vom Physiker erfahren, dass dies durch das Fallgesetz beschrieben wird und von der Erdbeschleunigung g abhängt. Der Physiker sagt:

Die Geschwindigkeit v eines fallenden Körpers ist proportional zur Fallzeit t mit der Proportionalitätskonstanten g (bei Vernachlässigung der Reibung).

Man erhält also den funktionalen Zusammenhang

$$v(t) = g \cdot t$$

Die in einem Zeitintervall Δt zurückgelegte Strecke Δs ist durch

$$\Delta s = v(t) \cdot \Delta t$$

gegeben.

Tragen wir nun v in einem Geschwindigkeit-Zeitdiagramm auf, so erhält man die in dem Zeitintervall $[t, t + \Delta t]$ zurückgelegte Strecke Δs, indem man das Intervall mit dem Geschwindigkeitswert bei $t + \frac{\Delta t}{2}$ multipliziert. Dies entspricht gerade den Rechtecken in Abbildung 3.1.
Die Summe der Flächen aller dieser Rechtecke ergibt gerade die Fläche F des grauen Dreiecks in Abbildung 3.1 und beträgt

[1] Das Wissen der Experten basiert dabei im allgemeinen natürlich auch auf Messungen und deren Interpretation. Die Messdaten sind aber vielleicht im Laufe der Zeit verloren gegangen.

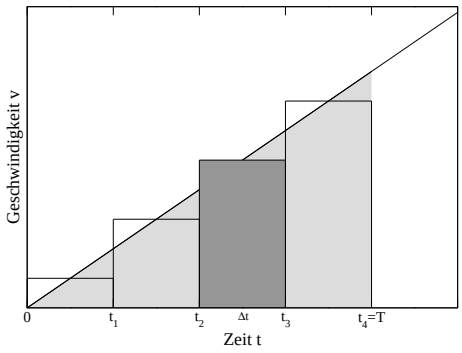


Abbildung 3.1: Geschwindigkeit-Zeit-Diagramm

$$F = \sum_{i=1}^{n} v(t_{i+\Delta t/2}) \cdot \Delta t = \frac{1}{2} T \cdot v(T) = \frac{1}{2} T \cdot g \cdot T = \frac{1}{2} g \cdot T^2$$

Hierbei ist $t_0 = 0$ und $t_n = T$. Diese Fläche beschreibt den seit t_0 zurückgelegten Weg, also $s(t) = \frac{1}{2} g \cdot t^2$.

Die Position der Kugel zur Zeit t beträgt dann $H(t) = H_0 - s(t)$. Das Minuszeichen rührt daher, dass die Kugel in Richtung Erdboden, also in Richtung geringerer Höhe, fällt. Die Höhe verringert sich also um die zurückgelegte Strecke. Unser gesuchtes Modell ist also durch

$$H(T) = H_0 - \frac{1}{2} \cdot g \cdot T^2$$

gegeben, wobei die Erdbeschleunigung $g = 9,81\,\mathrm{m/s^2}$ beträgt.

Genaugenommen muss man Δt infinitisimal klein machen, um das richtige Ergebnis zu erhalten. In diesem Beispiel ist die Funktion, unter der die Fläche bestimmt wird, linear, so dass das Ergebnis auch so stimmt.

Anmerkung für Analytiker: Die Momentangeschwindigkeit v ist die zeitliche Ableitung des Weges s, also

$$v(t) = \frac{ds(t)}{dt} = \dot{s}(t) = s'(t)\,.$$

Daraus ergibt sich für den Weg

$$s(t) = s(t_0) + \int_{t_0=0}^{t} v(x)\,dx = s_0 + \int_0^t g \cdot x\,dx = s_0 + \frac{1}{2} g \cdot x^2 |_0^t = s_0 + \frac{1}{2} g \cdot t^2$$

Die Abweichung im Vorzeichen rührt daher, dass wir hier angenommen haben, dass s und

v in dieselbe Richtung laufen. Ausserdem bezeichnet s hier wie üblich die Position zur Zeit t. $s(t_0)$ ist die Position zur Zeit t_0. Das Integral ist der in der Zeit von t_0 bis t zurückgelegte Weg.

3.2 Die Wurfparabel

Ein Fussball werde vom Boden aus mit einer vorgegebenen Anfangsgeschwindigkeit unter einem vorgegebenen Winkel geschossen.

Wie weit fliegt der Ball bis er zum erstem Mal wieder auf dem Boden aufkommt und wie hoch kommt er, wenn wir die Reibung vernachlässigen ?

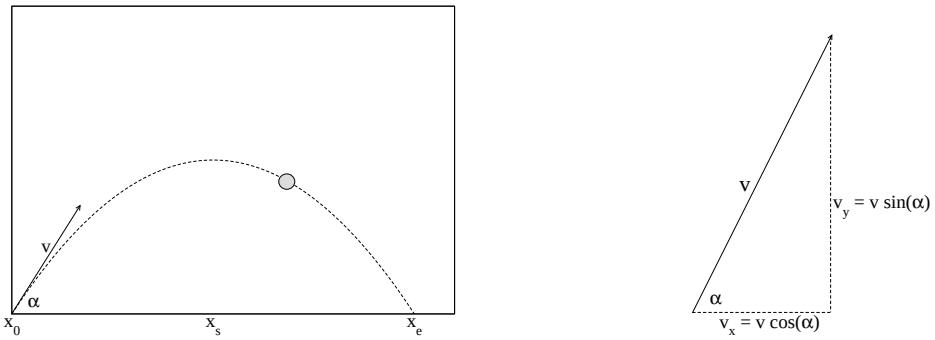


Abbildung 3.2: Die Wurfparabel und die Zerlegung der Geschwindigkeit v in die Komponenten v_x und v_y

Gegeben sei also der Winkel α, unter dem der Ball abgeschossen wird, und die Geschwindigkeit v zur Zeit $t_0 := 0$. Zunächst muss die Anfangsgeschwindigkeit v in ihre Komponenten zerlegt werden: Die zur Zeit t in x-Richtung zurückgelegte Strecke beträgt

$$x(t) = v_x \cdot t = v \cdot \cos\alpha \cdot t\,.$$

In y-Richtung wirkt die Schwerkraft, die zur Zeit t in y-Richtung zurückgelegte Strecke beträgt also (siehe Abschnitt 3.1)

$$y(t) = v_y \cdot t - \frac{g}{2} \cdot t^2 = v \cdot \sin\alpha \cdot t - \frac{g}{2} \cdot t^2\,.$$

Um nun zu bestimmen, wie weit der Ball fliegt, müssen wir herausfinden, bei welchem x-Wert y gerade null wird. Bisher haben wir aber nur Informationen darüber zu welcher Zeit, welcher x- bzw- y-Wert angenommen wird. Daher lösen wird die

Gleichung für x nach t auf und setzen das Ergebnis in die Gleichung für y ein.

Nehmen wir mal an, dass wir denn Ball nicht senkrecht in die Höhe schiessen, also $\alpha \neq 90\ ^\circ$ ist, und $\alpha \in [0,90[$ (damit gilt $\cos\alpha \neq 0$), so dürfen wir $x = v \cdot \cos\alpha \cdot t$ zu

$$t = \frac{x}{v \cdot \cos\alpha}$$

umstellen. Einsetzen ergibt

$$y(x) = \frac{\sin\alpha}{\cos\alpha} \cdot x - \frac{g}{2v^2 \cdot \cos^2\alpha} \cdot x^2 . \tag{3.1}$$

Man erhält also tatsächlich eine nach unten geöffnete Parabel. Die Schnittpunkte mit der x-Achse erhält man, indem man nun $y = 0$ setzt und nach x auflöst.

Man erhält die Lösungen x_0=0, den Abschusspunkt und

$$x_e = \frac{2v^2}{g} \cdot \sin\alpha \cdot \cos\alpha \qquad \text{, den Auftreffpunkt.} \tag{3.2}$$

Um nun die maximale Flughöhe zu ermitteln, müssen wir den y-Wert an der Scheitelstelle x_s der Parabel ermitteln. Aus Symmetriegründen gilt $x_s = x_e/2$ und die maximale Flughöhe y_s beträgt:

$$y_s = \frac{\sin\alpha}{\cos\alpha} \cdot x_s - \frac{g}{2v^2 \cdot \cos^2\alpha} \cdot x_s^2 . \tag{3.3}$$

Zahlenbeispiel: Der Abschusswinkel sei $\alpha = 40\ ^\circ$, die Anfangsgeschwindigkeit $v = 50\,\mathrm{km/h}$. Die Fallbeschleunigung beträgt auf der Erde $g = 9{,}81\,\mathrm{m/s^2}$.
Zuerst muss die Geschwindigkeit in die richtigen Einheiten umgerechnet werden:

$$50\,\frac{\mathrm{km}}{\mathrm{h}} = 50 \cdot \frac{1000\,\mathrm{m}}{3600\,\mathrm{s}} = \approx 13{,}89\,\frac{\mathrm{m}}{\mathrm{s}}$$

Einsetzen ergibt (Achtung: Winkel in Grad und nicht in Bogenmaß):

$$x_e \approx 19{,}36\,\mathrm{m} \qquad y_s \approx 4{,}06\,\mathrm{m}$$

Der Fussball fliegt 19,36 m weit und erreicht eine maximale Flughöhe von 4,06 m .

Betrachten wir nun den Fall, dass der Abschusspunkt nicht auf dem Boden, sondern in Höhe H vom Boden entfernt ist. Dann ist die Höhe des Balles durch

$$y(x) = H + \frac{\sin\alpha}{\cos\alpha} \cdot x - \frac{g}{2v^2 \cdot \cos^2\alpha} \cdot x^2 . \tag{3.4}$$

gegeben (vergleiche Gleichung 3.1).
Man erhält die Flugweite, indem $y(x) = 0$ gesetzt wird und die Gleichung nach x aufgelöst wird. Es existieren zwei Lösungen, die man durch Lösen der quadratischen Gleichung erhält:

$$x_{1,2} = \frac{v^2}{g}\cos\alpha \left(\sin\alpha \pm \sqrt{\sin^2\alpha + \frac{2gH}{v^2}} \right) , \tag{3.5}$$

von denen die positive die gesuchte Flugweite x_e ist.
Für $H = 0$ erhält man wiederum das Ergebnis aus 3.2.
Der Scheitelpunkt der Parabel liegt bei $\frac{x_1+x_2}{2}$. Er ist unabhängig von H:

$$x_s = \frac{v^2}{g} \cdot \sin\alpha \cdot \cos\alpha \tag{3.6}$$

Einsetzen von x_s in Gleichung 3.4 ergibt die maximale Flughöhe (vom Boden aus gemessen):

$$y_s = H + \frac{\sin\alpha}{\cos\alpha} \cdot x_s - \frac{g}{2v^2 \cdot \cos^2\alpha} \cdot x_s^2 . \tag{3.7}$$

3.3 Bakterienwachstum

Aus der Mikrobiologie ist bekannt, dass sich Bakterien einiger Arten alle 20 Minuten teilen. Wir nehmen an, dass sich dabei auch die Bakterienbiomasse alle 20 Minuten verdoppelt. Ein Bakterium hat in etwa einen Durchmesser von $0.5\,\mu$m.

Zielfrage: Wieviele Bakterien entstehen aus einer vorgegebenen Anzahl in einer vorgegebenen Zeit?

Anhand der uns zur Verfügung stehenden Information stellen wir folgendes Wachstumsmodell auf:

Bakterienzahl zur Zeit	$t_0 = 0\,\text{min}$	x_0
	$t_1 = 20\,\text{min}$	$x_1 = 2 \cdot x_0$
	$t_2 = 40\,\text{min}$	$x_2 = 2 \cdot x_1 = 2 \cdot 2 \cdot x_0$
	$\vdots$	$\vdots$
	$t_n = n \cdot 20\,\text{min}$	$x_n = 2 \cdot x_{n-1} = 2 \cdot \cdots \cdot 2 \cdot x_0 = 2^n \cdot x_0$

Man erhält das Wachstumsmodell des exponentiellen Wachstums in expliziter Darstellung

$$x_n = 2^n \cdot x_0 \,,$$

oder in impliziter (rekursiver) Darstellung

$$x_n = 2 \cdot x_{n-1} \,,$$

wobei jeweils x_0 als Anfangswert vorgegeben wird.

Anmerkung für Analytiker:
Beweis der expliziten Formel durch vollständige Induktion
Induktionsanfang: $n = 0 : x_0 = 2^0 \cdot x_0$
Induktionsschritt $n-1 \;\rightarrow n$:
Es gelte $x_{n-1} = 2^{n-1} \cdot x_0$, dann ist

$$x_n = 2 \cdot x_{n-1} = 2 \cdot 2^{n-1} \cdot x_0 = 2^n \cdot x_0 \,.$$

Überprüfung der Plausibilität des Modells

Wieviele Bakterien gibt es nach einem Tag und welches Volumen nehmen sie ein ?

Ein Tag hat $24 \cdot 3 \cdot 20$ Minuten, enspricht also 72 Zeitschritten. Unter der Annahme, dass zu Anfang ein Bakterium existiert, hat man nach 72 Zeitschritten

$$x_{72} = 2^{72} = 10^{72 \log 2} \approx 10^{21.674} \approx 4.7 \cdot 10^{21}$$

Bakterien.
Nun, solch eine Zahl sagt uns anschaulich nicht mehr viel. Schauen wir uns das Volumen an. Wir nehmen der Einfachheit halber an, dass die Bakterien kugelförmig sind und trotzdem dicht an dicht (ohne Lücken) gepackt liegen. Damit unterschätzen wir das tatsächliche Volumen.

Das Volumen V_B eines Bakteriums mit einem Durchmesser von
$d = 0.5\,\mu\text{m} = 0.5 \cdot 10^{-6}\,\text{m}$ beträgt

$$V_B = \frac{4}{3}\pi \left(\frac{d}{2}\right)^3 = \frac{4}{3}\pi \left(0.25 \cdot 10^{-6}\right)^3 m^3 = \frac{1}{48}\pi \cdot 10^{-18} m^3 \,.$$

Das Gesamtvolumen V beträgt also nach einem Tag

$$V = x_{72} \cdot V_B = 47 \cdot 10^{20} \cdot \frac{1}{48} \cdot \pi \cdot 10^{-18} m^3 \approx 3 \cdot 10^2\, m^3 \,.$$

Dieses Volumen entspricht einem Quader der Kantenlänge $3\,\text{m} \times 10\,\text{m} \times 10\,\text{m}$, also in etwa einem großen Seminarraum.
Vielleicht ist die von uns angenommene Wachstumsrate zu groß.
Bisher ist die Zahl der Bakterien, die pro Zeitschritt hinzukommt, genausogroß wie die Zahl bereits existierender Bakterien. Die Änderung der Zellzahl ist also zu jeder Zeit die Zellzahl selbst:

$$x_{n+1} = 2 \cdot x_n = x_n + x_n = x_n + 1 \cdot x_n$$

Die Wachstumsrate beträgt 1.
Vielleicht müssen wir diese Wachstumsrate verringen. Setzen wir anstelle von 1 nun den Parameter r ein, so erhalten wir folgendes Modell:

$$x_{n+1} = x_n + r \cdot x_n = (1 + r) \cdot x_n \qquad r \in \mathbb{R}^+$$

Wir erhalten nun folgende explizite Darstellung:

$$x_{n+1} = (1+r) \cdot x_n = (1+r) \cdot (1+r) \cdot x_{n-1} = \ldots = (1+r)^{n+1} \cdot x_0$$

oder anders geschrieben

$$x_n = x_0 \cdot (1+r)^n = x_0 \cdot e^{\ln(1+r)^n} = x_0 \cdot e^{n \cdot \ln(1+r)}$$

Es handelt sich hierbei um das Modell des exponentiellen Wachstums. Für jede positive Wachstumsrate r wächst die Zahl der Bakterien schliesslich über alle Grenzen. Also wächst die Bakterienzahl auch dann über alle Grenzen, wenn wir die Wachstumsrate verringeren (Abbildung 3.3).

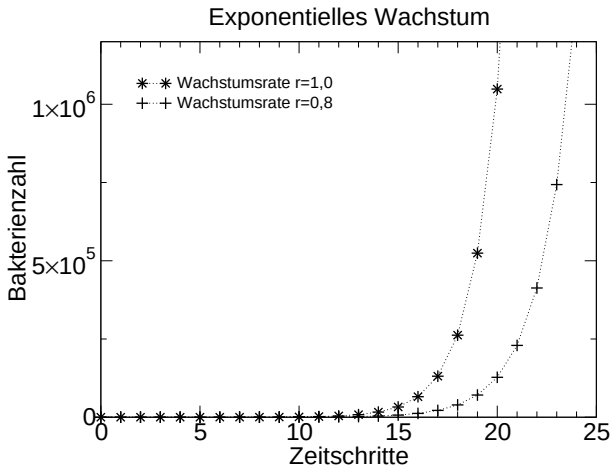


Abbildung 3.3: Vergleich des exponentiellem Wachstums für die Wachstumsrate $r = 1$ (*) und $r = 0,8$ (+).

Nun, irgendetwas ist also immer noch falsch. Wir haben bisher eine sehr grobe Zielfrage im Auge gehabt. Anfangs wurde nicht spezifiziert, für welche Zeiträume das Modell Gültigkeit haben soll. Wenn wir die Zahl der Bakterien nach wenigen Stunden bestimmen, so scheint das Modell plausible Ergebnisse zu lieferen (Übung).
Wir müssen also entweder den Gültigkeitsbereich einschränken oder das Modell an den gewünschten Gültigkeitsbereich anpassen. Zuerst stellt sich die Frage, warum der Gültigkeitsbereich eingeschränkt ist.
Bakterien brauchen zum Wachstum Nährstoffe und i.a. Sauerstoff. Lässt man eine Bakterienkultur in einer Petrischale auf Nährlösung wachsen, so wird die Nährlösung nach und nach verbraucht. Je dicker der Bakterienrasen wird, desto schlechter wer-

den innen liegende Zellen mit Sauerstoff und Nährstoffen versorgt. Es gibt also eine Nährstofflimitierung und eine Limitierung durch den zur Verfügung stehenden Platz. Bakterien werden also mit abnehmendem Nährstoff- und Raumangebot immer langsamer wachsen und sich dementsprechend auch immer seltener teilen.

Wir müssen die Wachstumsrate mit zunehmender Bakterienzahl abnehmen lassen , also

$$x_{n+1} = x_n + R(x_n) \cdot x_n$$

wobei R nun eine Funktion der Bakterienzahl ist, die monoton fallend sein soll, also z.B.

$$R(x) = 1 - \frac{x}{1000000}$$

Für sehr kleine Bakterienzahlen beträgt R nahezu 1, und wird immer kleiner, je mehr sich die Zahl der Bakterien einer Million nähert.

Wir erhalten also das verbesserte Modell:

$$x_{n+1} = x_n + \left(1 - \frac{x_n}{1000000}\right) \cdot x_n$$

Um nun nicht immer 1000000 schreiben zu müssen, setzen wir K=1000000.
K heisst Kapazität der Bakterienpopulation.

$$x_{n+1} = x_n + \left(1 - \frac{x_n}{K}\right) \cdot x_n$$

Dieses ist das Modell des logistischen Wachstums. Für kleine Bakterienzahlen wächst die Population nahezu ungebremst. Je größer die Population wird, desto langsamer wächst sie (Abbildung 3.4).

Auch das logistische Wachstum kann man verallgemeinern:

$$x_{n+1} = x_n + r \cdot \left(1 - \frac{x_n}{K}\right) \cdot x_n \qquad r \in \mathbb{R}^+ \tag{3.8}$$

Ist die Zellzahl sehr klein gegenüber der Maximalkapzität, beträgt die Wachstumsrate nun in etwa r.

Die rechte Seite kann man nun als Funktion der Zellzahl x schreiben. Sie gibt an,

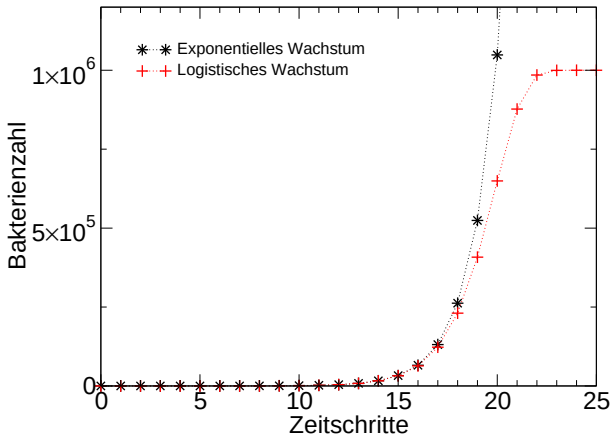


Abbildung 3.4: Vergleich zwischen exponentiellem Wachstum und logistischem Wachstum.

wie groß die Zellzahl im jeweils nächsten Zeitschritt ist:

$$f(x) = x + r \cdot \left(1 - \frac{x}{K}\right) \cdot x = -\frac{r}{K}x^2 + (1+r) \cdot x = (1+r) \cdot (1 - \frac{r}{(1+r) \cdot K} \cdot x) \cdot x$$

Die Zellzahl ist also als Funktion der Zellzahl im vorherigen Zeitschritt zu verstehen. Der Zeitschritt spielt nun keine Rolle mehr. In Abbildung 3.5 ist der Graph der Funktion f für $K = 1000000$ und $r = 1$ gegeben. Es handelt sich um eine nach unten geöffnete, gestauchte und nach rechts verschobene Parabel.
Es gilt:

- f(0)=0, d.h wenn keine Bakterien da sind, entstehen auch keine,
- f(K)=K, wenn die Bakterienzahl gerade gleich der Maximalkapazität ist, verändert sie sich nichts mehr,
- für $0 < x < K$, gilt $f(x) > x$, die Zellzahl nimmt zu,
- für $x > K$, gilt $f(x) < x$, die Zellzahl nimmt ab.

Zeichnet man zusätzlich die Gerade $y = x$ in den Graphen ein, so geben die Schnittpunkte des Graphen der Geraden mit dem Graphen der Funktion gerade die Zellzahlen an, bei denen sich nichts mehr ändert, also $f(x) = x$ gilt. In unserem Beispiel also, wenn

$$x + r \cdot \left(1 - \frac{x}{K}\right) \cdot x = x \quad \text{oder} \qquad r \cdot \left(1 - \frac{x}{K}\right) \cdot x = 0$$

gilt. Dies gilt für x=0 und x=K.

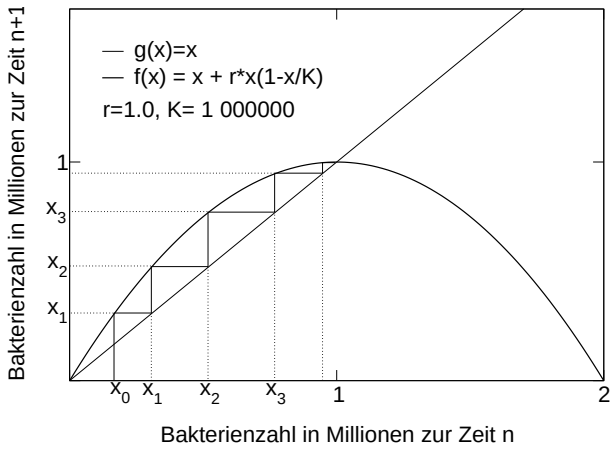


Abbildung 3.5: Graphische Lösung des Modells zum logistischen Wachstum.

Man kann das Modell auch graphisch simulieren. Dazu wählt man einen Anfangswert für die Zellzahlen und bestimmt die Zellzahlen der folgenden Schritte, wie in Abbildung 3.5 dargestellt.

3.4 Räuber-Beute-Modell

In diesem Abschnitt soll das Zusammenspiel zwischen einer Beutepopulation, z.B. Hasen und einer Räuberpopulation, z.B. Füchse simuliert werden (Abbildung 3.6. Hierzu machen wir folgende Annahmen.

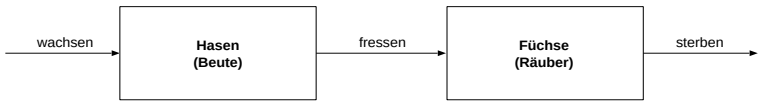


Abbildung 3.6: Diagramm des Räuber-Beute-Systems. Die Pfeile geben den Biomassenfluss an.

1. Die Hasen wachsen in jedem Zeitschritt in Abhängigkeit der Anzahl der aktuell vorhandenen Hasen.
2. Die Füchse fressen in jedem Zeitschritt einen Teil der Hasen, umso mehr, je mehr Hasen da sind.
3. Ein Teil der Füchse stirbt in jedem Zeitschritt.

Sei B_n (Beute) die Anzahl der Hasen und R_n (Räuber) die Anzahl der Füchse im Zeitschritt n

Zur Zeit 0 sei die Zahl der Hasen $B_0 = 200$, die Zahl der Füchse $R_0 = 20$.

Wir nehmen in Kauf, dass auch nicht-ganzzahlige Werte vorkommen können. Wen das stört, der kann als Einheit auch kg Hasen und kg Füchse wählen. Als Zeitschritt können wir z.B. 1 Tag wählen.
Das Wachstum der Hasen wird wie in Abschnitt 3.3 durch

$$B_{n+1} = B_n + r \cdot B_n$$

beschrieben. Hierbei ist r die Wachstumsrate der Hasen. Wir nehmen an, dass die Wachstumsrate der Hasen $r = 0.01$ pro Tag beträgt. Das bedeutet, dass die Hasenpoulation jeden Tag um 1 % wächst, wenn keine Hasen gefressen werden. Die Abnahme der Räuber ist durch

$$R_{n+1} = R_n - s \cdot R_n$$

beschrieben.Hierbei ist s die Sterberate der Räuber. Wir nehmen an, dass die Sterberate der Füchse $s = 0.05$ pro Tag beträgt .Das bedeutet, dass die Fuchspopulation jeden Tag um 5 % abnimmt, wenn nichts gefressen wird.
Nun müssen wir noch berücksichtigen, wieviel ein Fuchs frisst. Klar ist, dass er nichts zu fressen findet, wenn es keine Hasen gibt, und dass er umso mehr frisst, je mehr Hasen da sind (er muss dann nicht so lange suchen). Die Wachstumsrate der Füchse w wird also von der Hasenzahl abhängen $w = f(B)$, z.B.

$$w = b \cdot B$$

Setzen wir für den Parameter $b = 0.0004$, dann gilt bei 100 Hasen gerade $w = 0.04$. Stehen den Füchsen 100 Hasen als Nahrung zur Verfügung, kann ihre Population am Tag 4% wachsen (dies ist unrealistisch, aber es ist ein sehr einfaches Modell). Nun müssen wir nur noch die gefressenen Hasen bei den Hasen abziehen und bei den Füchsen addieren:

$$\begin{aligned} B_{n+1} &= B_n + r \cdot B_n - b \cdot B_n \cdot R_n \\ R_{n+1} &= R_n + b \cdot B_n \cdot R_n - s \cdot R_n \end{aligned} \tag{3.9}$$

Betrachtet man nun die Hasen- und Fuchszahl von Zeitschritt zu Zeitschritt (Abbildung 3.7[2]) so fällt folgendes auf: Beide Populationen oszillieren. Zuerst steigt die Zahl der Hasen. Dadurch steht den Füchsen mehr Nahrung zur Verfügung und ihre

[2] Um dieses Ergebnis zu erzielen, muss man einen kleineren Zeitschritt Δt wählen.

Zahl steigt kurz darauf ebenfalls. Dies reduziert die Zahl der Hasen wieder und den Füchsen steht wieder weniger Nahrung zur Verfügung usw..

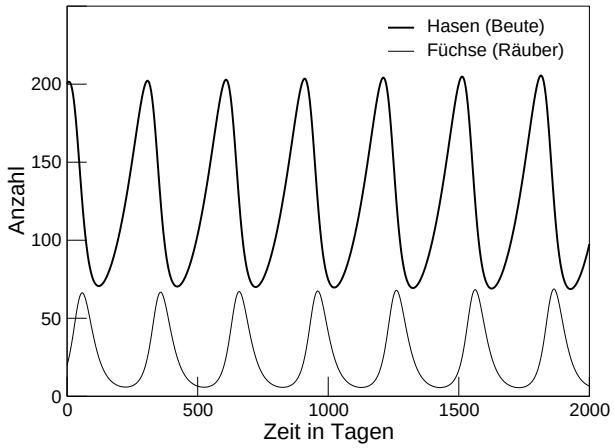


Abbildung 3.7: Lösungskurven des Räuber-Beute Systems. Die Kurven bestehen aus Einzelpunkten (kann man nicht sehen, da es zuviele sind), da das zugrundeliegende Modell ein Differenzengleichungsmodell ist.

Dieses Modell wurde in den zwanziger Jahren von Lotka und Volterra entwickelt und heisst auch Lotka-Volterra-Modell. Dieses Modell kann natürlich verbessert werden. Folgende Verbesserungen fallen einem sofort ein:

- Die Hasen dürfen nicht unbegrenzt wachsen, wenn keine Füchse da sind. Es muss eine Maximalkapazität wie in Abschnitt 3.3 geben.
- Die Füche müssen satt werden. Die Zunahme der Wachstumsrate der Füchse darf nicht linear von der Zahl der Hasen abhängen.
- Nur ein Teil der Hasen kann als Nahrung verwertet werden (Fell und Knochen werden ausgeschieden).

Verbessern wir das Modell nun dahingehend, dass wir eine Maximalkapazität für Hasen berücksichtigen. In diesem Fall wird das Wachstum der Hasen durch Gleichung 3.8 beschrieben, und das vollständige Modell lautet:

$$\begin{aligned} B_{n+1} &= B_n + r \cdot B_n \cdot \left(1 - \frac{B_n}{K}\right) - b \cdot B_n \cdot R_n \\ R_{n+1} &= R_n + b \cdot B_n \cdot R_n - s \cdot R_n \end{aligned} \tag{3.10}$$

Das Modell ist mit $\Delta t = 0.1$ gelöst.

$$\begin{aligned} B_{n+1} &= B_n + (r \cdot B_n - b \cdot B_n \cdot R_n) \cdot \Delta t \\ R_{n+1} &= R_n + (b \cdot B_n \cdot R_n - s \cdot R_n) \cdot \Delta t \end{aligned}$$

Die Modellergebnisse sind in Abbildung 3.8 für $K = 250$ und $K = 500$ dargestellt (andere Parameter wie bisher). Die Osszillationen sind nun mehr oder weniger stark gedämpft. Die Zahl der Hasen und Füchse strebt letztlich auf konstante Werte zu.

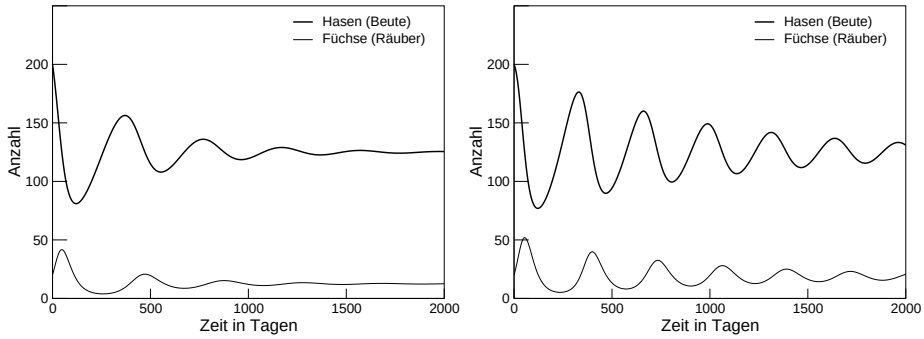


Abbildung 3.8: Lösungskurven des Räuber-Beute Systems mit einer Maximalkapazität für die Hasen (Beute) von $K = 250$ (links) und $K = 500$ (rechts).

Auch dies ist nicht unbedingt realistisch. Weitere Modifikationen des Modells können aber zu einem realistischeren Modellverhalten führen
Leider können diese Modifikationen im Rahmen dieser Vorlesung nicht näher untersucht werden. Dies ist Gegenstand der Vorlesungen „Mathematischen Modellierung“ und „Dynamische Systeme“.

Anmerkung für Analytiker: Dieses Modell instabil. Letztlich wird die Zahl der Hasen und Füchse immer stärker oszillieren. Dies wird man in Grenzen los, wenn man das System als Differenzialgleichungssystem berechnet. Trotzdem bleibt es ein singuläres Modell, da es stabil aber nicht asymptotisch stabil ist.

4 Wie arbeitet ein Computer?

Wie kommt ein Taschenrechner auf $\sqrt{2} = 1.4142135\cdots$?
Es stellt sich also die Frage, wie man eine Zahl x findet, für die $x^2 = 2$ gilt.
Schauen wir uns das ganze mal grafisch an. Die Fläche eines Quadrats mit der Kantenlänge a beträgt $F = a^2$. Ist nun die Fläche F gegeben und gefragt , wie groß ist die Kantenlänge a des Quadrats ist, so lautet die Lösung $a = \sqrt{F}$. Wir haben also quasi dasselbe Problem.
Beginnen wir mit einem Rechteck. Wählen wir als erste grobe Schätzung für eine Kantenlänge den Wert x_0, so muss die andere Kante die Länge $\frac{F}{x_0}$ haben, damit die Fläche F herauskommt, denn $F = x_0 \cdot \frac{F}{x_0}$. Im allgemeinen wird nun aber die eine Kante länger als die andere sein. (Wenn nicht sind wir schon fertig, denn dann haben wir bereits ein Quadrat und die gesuchte Kantenlänge.).

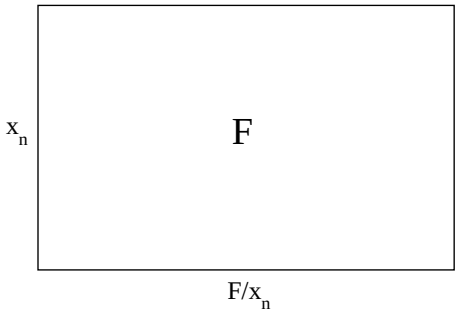


Abbildung 4.1: Idee des Heron-Verfahrens

Wir werden x bestimmt verbessern, wenn wir den Mittelwert der beiden Kantenlängen als eine Kante wählen. Wir setzen also

$$x_1 = \frac{1}{2}\left(x_0 + \frac{F}{x_0}\right)$$

und wiederholen das Verfahren:

$$x_{n+1} = \frac{1}{2}\left(x_n + \frac{F}{x_n}\right) \tag{4.1}$$

Dies machen wir nun so oft, bis die von uns gewünsche Genauigkeit der Lösung erreicht ist, also $x_{n+1} \approx \frac{F}{x_{n+1}}$ gilt.

Die Vorschrift 4.1 heisst Heron-Verfahren. Das Verfahren basiert darauf, dass mit einem Wert in der Nähe der Lösung gestartet wird, der Schritt für Schritt verbessert wird.

Solch ein Verfahren (oder ein ähnliches) ist in fast jedem Taschenrechner enthalten, man sagt auch implementiert. Ein solches Verfahren approximiert die Lösung Schritt für Schritt. Das Verfahren, dass ein Taschenrechner benutzt ist also ein Näherungsverfahren. Und damit sind wir beim wichtigsten Punkt überhaupt:

Ein Computer kann nicht genau rechnen!

Nun, was bedeutet dies ?
Will man eine Zahl, z.B. π in den Taschenrechner eingeben, so ist irgendwann Schluss. Manche Taschenrechner haben 8 Stellen andere 10, Computer eventuell beliebig aber endlich viele. Da π unendlich viele Nachkommastellen hat, kann man gar nicht erwarten, dass ein Rechner das kann, man könnte es ja nicht mal richtig eingeben. Welche Konsequenzen hat das?

Wenn man eine Berechnungen durchführt, werden also Fehler gemacht. Diese können Abbruchsfehler sein, die dadurch entstehen, dass die tatsächliche Zahl mehr stellen hat, als der Rechner bearbeiten kann. Oder es werden Fehler gemacht, weil ein Verfahren, z.B. das Heron-Verfahren zum Wurzelziehen, nur eine gewisse Anzahl mal wiederholt wird. Was nun ?

Die Numerik liefert zu allen Verfahren Abschätzungen, wie groß diese Fehler sind. So kann man sich zu einem gegebenen Problem das Verfahren heraussuchen, das für dieses Problem genau genug arbeitet. Man kann also Computern doch mehr anfangen als eMails zu verschicken. Nur, wie bringe ich dem Computer etwas bei, das er noch nicht kann? Hierzu ein kleiner Ausflug in die Funktionsweise des Computers:

Ein Computer versteht keine Zahlen und Buchstaben. Auch das muss ihm erst beigebracht werden. Glücklicherweise haben das schon andere für uns erledigt. Auch ist es nicht selbstverständlich, dass wir etwas auf der Tastatur schreiben und dies dann auf dem Bildschirm zu sehen ist.

Die Grundidee der Umsetzung aller Eingaben in einen für den Computer verständliche Sprache sind die zwei Zustände „Strom an“ (1) und „Strom aus“ (0). Wir machen nun einen Riesenschritt und landen beim Binärsystem.

Im Alltag rechnen wir im Dezimalsystem. Wir haben uns so daran gewöhnt, dass es uns gar nicht mehr bewusst ist. Wir stellen Zahlen durch die Ziffern $0-9$ dar. Sei eine Zahl a durch die Ziffernfolge $a_3a_2a_1a_0$ beschrieben, so ist a_0 der Koeffizient zu 10^0, a_1 zu 10^1, a_2 zu 10^2 und a_3 zu 10^3:

$$a = a_3 \cdot 10^3 + a_2 \cdot 10^2 + a_1 \cdot 10^1 + a_0 \cdot 10^0$$

Was ist nun, wenn unser Zahlensystem nicht aus den Ziffern $0-9$ sondern nur aus den Ziffern 0 und 1 besteht? In diesem Fall ist mit einer Zahl b mit der Ziffernfolge $b_1b_2b_3b_4$, wobei die b_i nur 0 oder 1 sein können, folgendes gemeint:

$$b = b_3 \cdot 2^3 + b_2 \cdot 2^2 + b_1 \cdot 2^1 + b_0 \cdot 2^0$$

Wir können somit die Zahl b, die in der Binärdarstellung $b_1b_2b_3b_4$ angegeben ist, in das Dezimalsystem umrechnen, zum Beispiel

$$11010_{BIN} = 1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0_{DEC} = 26_{DEC}$$

Im Binärsystem tauchen nur die Ziffern 0 und 1 auf, denn schon die 2 kann man als $1 \cdot 2^1$ schreiben.

Man kann also alle Zahlen nur mit den Ziffern 0 und 1 darstellen. Ausserdem kann man Zahlsysteme für jede beliebige Ziffernzahl angeben, z.B. heisst das System bestehend aus den Ziffern 0,1,2 Ternärsystem.

$$12020_{TER} = 1 \cdot 3^4 + 2 \cdot 3^3 + 0 \cdot 3^2 + 2 \cdot 3^1 + 0 \cdot 3^0_{DEC} = 141_{DEC}$$

In der Computerei bedeutend sind das Oktalsystem (0-7) und das Hexadezimalsystem bestehen aus 16 Ziffern. Hier nimmt man zu den Ziffern $0-9$ noch die Ziffern A,B,C,D,E,F zur Hilfe. A steht für 10, B für 11 usw.

$$12AC_{HEX} = 1 \cdot 16^3 + 2 \cdot 16^2 + 10 \cdot 16^1 + 12 \cdot 16^0_{DEC} = 4780_{DEC}$$

Man kann also mit dem Binärsystem alle Zahlen durch die Zustände „Strom an“ (1) und „Strom aus“ (0) darstellen. Durch die Codierung von Buchstaben und Sonderzeichen durch Zahlen kann man also alles darstellen, was man so braucht.

Im Binärsystem kann man nun wie in jedem Zahlsystem rechnen. Betrachten wir zunächst das Dezimalsystem. Beim schriftlichen Addieren zweier Zahlen machen

wir immer dann einen Übertrag, wenn das Ergebnis 9 übersteigt:

$$\begin{array}{rrr} & 1 & 5 \\ + & 1_1 & 7 \\ \hline & 3 & 2 \end{array}$$

Genauso verfahren wir beim Addieren zweier Zahlen im Binärsystem, nur dass man jetzt schon einen Übertrag machen muss, wenn das Ergebnis 1 übersteigt:

$1_{BIN} + 1_{BIN} = 10_{BIN}$

$$\begin{array}{rrrrrr} & & 1 & 1 & 0 & 1 \\ + & & 1_1 & 1_1 & 1_1 & 1 \\ \hline & 1 & 1 & 1 & 0 & 0 \end{array}$$

Multiplizieren im Binärsystem funktioniert ähnlich wie im Dezimalsystem, man muss nur mit den mehrfachen Überträgen aufpassen, daher schreibt man sich die größere der beiden Zahlen am besten nach vorne:

$$\begin{array}{rrrrrrrrrr} & 1 & 1 & 0 & 1 & 1 & * & 1 & 1 & 0 \\ \hline & & & 1 & 1 & 0 & 1 & 1 & & \\ & & & & 1 & 1 & 0 & 1 & 1 & \\ + & & & & & & & & & 0 \\ \hline & & 1 & 1 & 1 & 1 & 1 & & & \\ \hline & & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \end{array}$$

Die Zwischenzeile gibt die Überträge bei der Addition an. Muss man mehr Zeilen addieren, so können sich weitere Überträge ergeben:

$$\begin{array}{rrrrrrrrrr} 1 & 1 & 1 & 1 & * & 1 & 1 & 0 & 1 & 1 \\ \hline & & 1 & 1 & 1 & 1 & & & & \\ & & & 1 & 1 & 1 & 1 & & & \\ & & & & & & & 0 & & \\ & & & & & 1 & 1 & 1 & 1 & \\ + & & & & & & 1 & 1 & 1 & 1 \\ \hline & & 1 & & 1 & & & & & \\ & 1 & 1 & & 1 & & 1 & 1 & & \\ \hline & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \end{array}$$

Nun sind noch einige Begriffe zu klären. Eine Speicherzelle im Computer kann den Zustand 0 oder 1 annehmen. Eine solche Speicherzelle beinhaltet also ein Bit (kurz

für binary digit, eine Binärziffer). Will man nun größere Zahlen speichern, braucht man wie oben gesehen mehrere Bits.

Ein Oktett von Bits (also 8 Bits) bezeichnet man als Byte. Gebräuchlich sind hierbei die Vorsilben „kilo“(k), „Mega“(M), „Giga“(G) und „Tera“(T).
Hierbei bezeichnet ein kByte allerdings nicht, wie zu erwarten wäre, 1000 Byte sondern 2^{10} Byte = 1024 Byte. Ein Megabyte sind dann $1024 \cdot 1024$ Byte usw.[1]

Eine CD-ROM mit 640 MB hat dann also
$640 \cdot 1024 \cdot 1024$ Byte = $640 \cdot 1024 \cdot 1024 \cdot 8$ Bit.

Auf die weitere hardwaremäßige Umsetzung können wir im Rahmen der Vorlesung leider nicht eingehen, wir springen daher direkt zur Programmierung.

4.1 Einführung in die Programmierung

Wie bereits erläutert, versteht der Computer nur „Strom an“ und „Strom aus“. Damit wir uns aber nicht mit Nullen und Einsen herumschlagen müssen, gibt es Programmiersprachen. Programmiersprachen sind Sprachen, die für uns mehr oder weniger leicht erlernbar sind, und unsere Befehle (über einige Zwischenstufen) in die benötigten Nullen und Einsen umsetzen. Programmiersprachen bestehen aus Vokabeln, die gewisse Anweisungen codieren und je nach Sprache unterschiedlich sein können.
Im folgenden wird die alte Sprache BASIC (Beginner’s All-purpose Symbolic Instruction Code) vorgestellt. BASIC ist zwar heutzutage nicht mehr aktuell, bietet aber den Vorteil, dass man die Grundprinzipien der Programmierung sehr gut damit erklären kann. Im übrigen gibt es BASIC kostenlos im Internet, so dass jeder damit arbeiten kann. Man findet im Internet verschieden BASICs. Diese kann man als unterschiedliche Dialekte auffassen. Sie sind sich größtenteils sehr ähnlich, besitzen aber häufig Erweiterungen der „Ursprache“, die sehr nützlich sind. Im folgenden wird SmallBasic[2] benutzt.
Die folgende Einführung ersetzt keinesfalls einen Programmierkurs, sondern kann nur einen Einblick in die Funktionsweise einer Programmiersprache geben.

[1] Bei übertragenen Datenmengen pro Zeiteinheit werden hingegen Zehnerpotenzen zugrundegelegt, so dass 1 kBit/s = 10^3 Bit/s = 1000 Bit/s (1 Kilobit/Sekunde) sind.

[2] SmallBasic ist von Nicholas D. Christopoulos. Es ist sogenannte Freeware unter der GNU Public License. Man findet es unter http://smalbasic.sf.net

Ein SmallBasic-Programm besteht aus einer Abfolge von Anweisungen. Man schreibt diese Anweisungen in eine Datei und speichert sie. Der Dateiname soll dabei die Extension (das nach dem Punkt) `bas` haben, z.B. `myfirst.bas`. Unter Linux kann man das Programm „laufen lassen“, indem man

```
sbasic myfirst
```

eingibt. Das Programm wird nun Zeile für Zeile abgearbeitet.

Unter Windows gibt es ein GUI (graphical user interface, graphische Benutzerschnittstelle), das SBPad[3]. Nach Aufruf von Smallbasic wird das GUI geöffnet und man kann gleich im Editor (Karteikarte Editor) losschreiben. Wenn man nun `File/Save` auswählt, wird das Geschriebene in einer Datei gespeichert und erhält automatisch die Extension `.bas`.

Durch Ausführen von `Program/Run` kann man das Programm „laufen lassen“. Die Ausgabe des Programms erscheint auf der Karteikarte Output.

SmallBasic kann natürlich ganz normal rechnen. Will man 3+8 rechnen, so muss man

```
PRINT 3+8
```

im Editor eingeben und durch `Run` laufenlassen. Der Output ist dann

```
11
```

Der Befehl `print` dient dazu, dass das Ergebnis ausgegeben wird. Gibt man nur `3+8` ein, erhält man eine Fehlermeldung, dass SmallBasic diesen Befehl nicht kennt.

Häufig will man das Ergebnis aber gar nicht ausgeben sondern im weiteren Verlauf des Programms benutzen. Dazu kann man das Ergebnis einer Variablen zuweisen. Will man das Ergebnis in der Variablen a speichern, so muss man

```
a = 3+5
```

eingeben. Mit diesem Befehl wird für die Variable `a` Speicherplatz eingerichtet, in den das Ergebnis geschrieben wird.

Betrachten wir folgendes Programm

```
a = 3+3
a = a+1
PRINT a
```

[3] Das ausführbare Programm heisst `SBpad.exe` und liegt je nach Installation meistens in `C:\programme\smallbasic`

Nach `Run` erscheint im Ausgabefenster das Ergebnis 7. Wie kommt dies? Nach Abarbeitung der ersten Ziele steht in `a` eine 6. In der zweiten Zeile wird zu dem Wert in `a` 1 addiert und das Ergebnis wieder `a` zugewiesen. Nun hat `a` den Wert 7. Die zweite Zeile ist also nicht im mathematischen Sinn zu verstehen. Das Gleichheitszeichen darf hier nicht als Äquivalenzrelation verstanden werden, sondern symbolisiert eine Zuweisung. Das Ergebnis des Ausdrucks, der rechts vom Gleichheitszeichen steht, wird der Variabeln auf der linken Seite zugewiesen. Daher führt die Zeile `a+1=a` zu einer Fehlermeldung.
Was nützt einem nun eine Programmiersprache? Solche Rechnungen kann ein Taschenrechner doch viel bequemer ausführen!
Häufig muss man ähnliche Rechenschritte oft hintereinander ausführen. Will man z.B. die Zahlen von eins bis 100 aufaddieren (und kennt die Gaußsche Formel nicht), so ist das sehr mühsam. Mit einer Programmiersprache ist das auch ohne Gaußsche Formel sehr einfach.
In einer Programmiersprache gibt es viele Befehle, die einem das Leben leicht machen. Um Befehle mehrfach hintereinander auszuführen gibt es sogenannte Schleifen:

```
FOR i=1 TO 5
   print i
NEXT i
```

Das Beispiel zeigt die sogenannte `FOR-NEXT-` Schleife. Man wählt eine Laufvariable (hier *i*), die initialisiert wird (`i=1`) und einen Endwert (5) bis zu dem die Schleife abgearbeitet werden soll. Das Ende der Schleife ist durch den Befehl `NEXT` gekennzeichnet. Beim Programmlauf wird in der `FOR`-Zeile *i* auf 1 gesetzt, dann wird die Anweisung zwischen `FOR` und `NEXT`-Zeile abgearbeitet und dann wieder nach oben gesprungen. Dies wird sooft wiederholt bis `i` den Endwert erreicht hat. Das Ergebnis dieses Programms ist

```
1
2
3
4
5
```

Nun können wird die Zahlen von 1 bis 10 addieren:

```
summe=0
FOR i=1 TO 10
   summe= summe+i
NEXT i
PRINT summe
```

In der ersten Zeile wird die Variable `summe` initialisiert. Dies ist wichtig, da innerhalb der Schleife die Variable auf der rechten Seite auftritt. Vergisst man die Initialisierung, hat `summe` keinen Wert und kann folglich auch nicht verrechnet werden. In der Schleife wird der aktuelle Wert von `i` zum aktuellen Wert von `summe` addiert und das Ergbnis in `summe` gespeichert. Nach Verlassen der Schleife wird das Ergebnis ausgegeben.
Als nächstes wollen wird das Programm hübsch machen. Es soll uns nach einer Zahl fragen, bis zu der alle natürlichen Zahlen von 1 an aufaddiert werden sollen, und das Ergebnis ausgeben.

```
PRINT "Dieses Programm berechnet die Summe der Zahlen von 1 bis N"
INPUT "Bitte N eingeben:", n
summe=0
FOR i=1 TO n
    summe= summe+i
NEXT i
PRINT "Ergebnis:", summe
```

Die erste Zeile gibt einen sogenannten String aus. Ein String ist eine Zeichenkette. Diese wird in Gänsefüßchen gesetzt. In der zweiten Zeile wird mit dem `INPUT`-Befehl ebenfalls zuerst ein String ausgegeben und dann auf die Eingabe gewartet. Im Ausgabefenster erscheint bis hierhin:

```
Dieses Programm berechnet die Summe der Zahlen von 1 bis N
Bitte N eingeben:
```

Nun kann man z.B. 5 eingeben. Danach wird das Programm automatisch weiter abgearbeitet und es erscheint

```
Ergebnis: 15
```

Bis jetzt muss man für n eine natürliche Zahl eingeben. Gibt man z.B. 5.5 ein, so ist das Ergbnis auch 15, da die FOR-NEXT Schleife nachsieht, ob $\texttt{i} \leq \texttt{n}$ gilt, und

dass ist auch für n=5.5 der Fall (da Programmiersprachen der englischen Notation folgen, werden Kommazahlen wie beim Taschenrechner mit einem Punkt statt einem Komma eingegeben). Trotzdem ist das Verhalten des Programms nicht schön. Besser wäre es, es würde überprüfen, ob `n` richtig eingegeben wurde. Wir wollen das Programm nur dann ausführen, wenn `n` eine natürliche Zahl ist. Dazu müssen wir zuerst überprüfen, ob der ganzahlige Anteil von `n` gleich `n` selbst ist. Der ganzzahlige Anteil von `n` wird durch `INT(n)` berechnet. Zur Abfrage braucht man eine sogenannte `IF`-Anweisung:

```
PRINT "Dieses Programm berechnet die Summe der Zahlen von 1 bis N"
INPUT "Bitte N eingeben:", n
IF n=INT(n) THEN
summe=0
FOR i=1 TO n
   summe= summe+i
NEXT i
PRINT "Ergebnis:", summe
ENDIF
```

Zwischen `IF` und `THEN` steht eine Aussage, die wahr oder falsch sein kann. Man beachte, dass in diesem Zusammenhang das Gleichheitszeichen im mathematischen Sinne gebraucht wird. Ist die Aussage wahr, dann wird alles zwischen `IF` und `ENDIF` ausgeführt, sonst nicht.
Jetzt fehlen noch zwei Sachen. Erstens wollen wird, dass es eine Meldung gibt, wenn ein falsches `n` eingegeben wird, und zweitens müssen wir abfangen, dass ein n kleiner als 1 eingegeben wird. Es müssen also zwei Bedingungen gleichzeitig erfüllt sein, nämlich `n>1` und `n=INT(n)`. Dies erreicht man durch

```
...
IF n=INT(n) AND n>1 THEN
...
```

Eine Meldung soll erscheinen, wenn mindestens eine der beiden Aussagen falsch ist. Dann ist aber nach der Aussagenlogik auch die gesamte Aussage falsch. Man muss im Programm also eine Meldung ausgeben, wenn die Aussage zwischen `IF` und `THEN` falsch ist . Die erreicht man, wenn man die `IF` Bedingung um eine `ELSE` Anweisung erweitert.

```
PRINT "Dieses Programm berechnet die Summe der Zahlen von 1 bis N"
INPUT "Bitte N eingeben:", n
IF n=INT(n) AND n>1 THEN
summe=0
FOR i=1 TO n
   summe= summe+i
NEXT i
PRINT "Ergebnis:", summe
ELSE
PRINT "Die Eingabe ist unzulässig!"
ENDIF
```

Alles, was nunzwischen `ELSE` und `ENDIF` steht, wird ausgeführt, wenn die Aussage zwischen `IF` und `THEN` falsch ist.
Nun wollen wir das Programm ja nicht jedesmal neu starten, wenn eine falsche Eingabe gemacht wurde.
Hierzu gibt es eine weitere Schleifenart, die sogenannte `WHILE`-Schleife. Bei einer `WHILE`-Schleife werden Anweisungen zwischen `WHILE` und `WEND` solange ausgeführt, solange eine Bedingung wahr ist.

```
a=1
WHILE a<1.3
   a=a+0.1
   print a
WEND
```

Die Ausgabe des Programms ist

```
1.1
1.2
1.3
```

Der letzte Schleifendurchlauf findet bei a=1.2 statt. Dann wird aber a noch um 0.1 erhöht und erst dann ausgegeben. Damit können wir das Programm verbessern:

```
PRINT "Dieses Programm berechnet die Summe der Zahlen von 1 bis N"
OK=0
WHILE OK=0
INPUT "Bitte N eingeben:", n
```

```
IF n=INT(n) AND n>1 THEN
summe=0
FOR i=1 TO n
   summe= summe+i
NEXT i
PRINT "Ergebnis:", summe
OK=1
ELSE
PRINT "Die Eingabe ist unzulässig!"
ENDIF
WEND
```

Wenn eine zulässige Zahl eingegeben wurde, wird OK auf 1 gesetzt und die Schleife damit beendet. Anderenfalls wird nach erneuter Eingabe gefragt.
Man kann in BASIC diese `WHILE`-Schleife auch durch eine Sprunganweisung ersetzen. Da dies aber ein veralteter Programmierstil ist, der zu sehr unübersichtlichen Programmen führt, wollen wir darauf nicht näher eingehen.

Unterprogramme

Nun werden Programme recht schnell unübersichtlich. Daher ist es gut Funktionen zu schreiben, die einen Teil der Berechnungen ausführen und das Ergebnis zurückgeben.
Wollen wir z.B. die Kreisfläche für verschiedene Radien berechnen, so ist es hilfreich eine Funktion zu schreiben, die ganz allgemein die Kreisfläche als Funktion des Radius zurückgibt:

```
FUNC flaeche(r)
 flaeche =
END
```

Am Ende der Funktion muss eine Variable, die genauso heisst, wie die Funktion selbst, den Rückgabewert, also das Ergebnis, enthalten. Um nun die Fläche der Kreise mit den Radien 0,1; 0,2;0,3;0,4 und 0,5 zu bestimmen, schreibt man folgendes Programm

```
REM Funktion zur Bestimmung der Kreisfläche
FUNC flaeche(r)
  flaeche = PI*r^2
```

```
END

REM Hauptprogramm
FOR i=1 TO 5
   radius = i/10
   PRINT "Radius=", radius,"Fläche=", flaeche(radius)
NEXT
```

Die erste Zeile ist eine sogenannte REM-Zeile. REM steht für Remark (Bemerkung). Zeilen, die mit REM anfangen, werden bei der Programmausführung ignoriert.

Das Hauptprogramm kann einfacher gestaltet werden, indem man in der FOR-NEXT-Schleife eine Schrittweite angibt:

```
REM Hauptprogramm
FOR i=0.1 TO 0.5 STEP 0.1
      PRINT "Radius=", i,"Fläche=", flaeche(i)
NEXT
```

Das Heron-Verfahren

Ein Anwendungsbeispiel ist das bereits erwähnte Heron-Verfahren zum Wurzelziehen. Wir müssen dem Programm eine Zahl angeben, aus der die Wurzel gezogen werden soll. Diese Zahl darf nicht negativ sein. Dann müssen wir einen Startwert vorgeben, der nicht null sein darf, und die Anzahl der Schritte wie oft die Iteration durchgeführt werden soll. Eine Möglichkeit dies zu tun ist

```
PRINT "Berechnung der Wurzel:"

F=-1
WHILE F<0
   INPUT "Bitte (nichtnegative) Zahl eingeben:", F
WEND

INPUT "Bitte Anzahl der Schritte eingeben:", N

x=0
WHILE x=0
```

```
  INPUT "Bitte Startwert (ungleich 0)  eingeben:", x
WEND

FOR i=1 TO N
   x=0.5*(x+F/x)
NEXT i

PRINT "Eine Wurzel von ";F;" ist ungefähr  "; x; "."
```

Räuber-Beute-System

Wir können jetzt auch das Räuber-Beute-System aus Abschnitt 3.4 programmieren. Der Programmcode ist in Abbildung 4.2 gegeben.
Als erstes fällt bei dem Programm das ' Zeichen auf. Dies ist eine Kurzform von `REM`, damit man nicht soviel tippen muss. Im ersten Teil des Programms werden Parameter, Endzeit und Startwere für die Zustandsvariablen gesetzt. Innerhalb der Zeitschleife werden für Räuber und Beute die neuen Werte aus den vorherigen bestimmt und geplottet. Der Befehl `PSET i, 500-xneu` setzt einen Punkt im Ausgabefenster, wobei der erste Wert den Wert auf der x-Achse und der zweite den Wert auf der y-Achse ist. Der zweite Wert beträgt hier 500-xneu und nicht nur xneu, da der Nullpunkt des Grafikfensters in der oberen linken Ecke liegt. Eine weitere Besonderheit des `PSET`-Befehls ist, dass er nur mit ganzzahligen Werten arbeitet. Gegebenenfalls muss man die Werte, die man darstellen will, skalieren. Die Anweisung zur Darstellung der Räuber-Werte enthält einen dritten Parameter. Dieser steuert die Farbe der Ausgabe. Das Ergebnis ist in Abbildung 4.2 dargestellt.
Dieses Ergebnis ist natürlich nicht schön. Das liegt daran, dass SmallBasic nur sehr eingeschränkt grafikfähig ist. Es fehlen Achsen und Beschriftungen. Besser wäre es, wenn man die Ergebnisse in eine Datei schreibt und mit einem leistungsfähigeren Programm weiterbearbeitet. Dies kann z.B. Excel sein.

Folgendes Programm schreibt die Zahlen von 1 bis 5 und deren Quadrate in die Datei `ergebnis.csv`:

```
OPEN "ergebnis.csv" FOR OUTPUT AS #1
FOR i=1 TO 5
     PRINT #1,i,i^2
NEXT
CLOSE #1
```

```
' Raeuber-Beute System nach Lotka-Volterra
' x: Beute
' y: Raeuber

' Laufzeit
tend=1000
' Schrittweite
dt=1

' Startzeit
t0=0
' Startwert fuer x
x0=200
' Startwert fuer y
y0=20

' Parameter
' Wachstumsrate der Beute
r=0.01
' Fressfaktor
b=0.0004
' Sterberate des Raeubers
m=0.05

' Initialisierung
xalt=x0
yalt=y0

' Zeitschleife
for i=0 to tend/dt
   xneu= xalt + (r*xalt -b*xalt*yalt)*dt
   yneu= yalt + (b*xalt*yalt -m*yalt)*dt

   pset i, 500-xneu
   pset i,500-yneu,1

   xalt=xneu
   yalt=yneu
next
```

Abbildung 4.2: Programm zum Räuber-Beute-Modell aus Abschnitt 3.4.

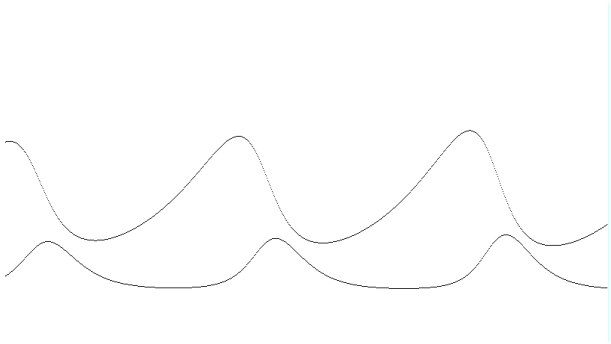


Abbildung 4.3: Ausgabe des Programms in 4.2.

Insgesamt schreibt jeder `PRINT` Befehl eine Zeile in die Datei mit der Kanalnummer `#1`, die einzelnen Einträge sind durch ein Tab getrennt. Wenn die Ausgabedatei die Extension `.csv` besitzt, kann man sie mit Excel lesen.

Man kann natürlich auch Daten aus einer Datei auslesen. Dies geschieht mit folgendem Programm:

```
OPEN "ergebnis.csv" FOR INPUT AS #1
WHILE NOT EOF(1)
  INPUT #1, a, b
  PRINT a,b
WEND
CLOSE #1
```

Wichtig ist, dass die Datei existiert und tatsächlich pro Zeile zwei Einträge vorhanden sind. Die WHILE Schleife stellt sicher, dass solange Daten gelesen werden, wie welche vorhanden sind. `EOF` steht für end-of-file. `WHILE NOT EOF(1)` bedeutet, dass die Schleife solange durchlaufen wird, solange das Ende der Datei die mit Kanalnummer 1 geöffnet wurde, nicht erreicht ist. Die Ergebnisse werden mit dem INPUT Befehl in die Variablen a und b gelesen und danach mit PRINT ausgegeben. Nun werden bei jedem Durchlauf a und b überschrieben. Am Ende stehen also nur die letzten Einträge zur Verfügung. Will man aber alle Einträge im Programm zur Verfügung haben, so kann man Arrays (Felder) benutzen. Arrays sind so etwas wie Vektoren. Man kann über eine Nummer auf die jeweilige Komponente zugreifen.
Wissen wir, wieviele Zeile in unserer Datei stehen, dann kann man Felder entsprechender Größe anlegen und die Werte aus der Datei in die Felder einlesen. Nehmen wir an, dass 5 Zeilen in der Datei stehen, dann können wir mit folgendem Programm die Werte einlesen.

```
DIM a(5)
DIM b(5)

OPEN "ergebnis.csv" FOR INPUT AS #1
FOR i=1 TO 5
  INPUT #1, a(i), b(i)
NEXT i
CLOSE #1

PRINT a(3),b(3)
```

Als Beispiel werden am Ende die Werte aus der dritten Zeile ausgegeben.
Damit haben wir einige Grundlagen der Programmierung zusammen. In anderen Programmiersprachen läuft es ganz ähnlich, auch wenn die Befehle meistens etwas anders heissen. Wichtig dabei ist, dass einige Programmiersprachen zwischen Groß- und Kleinschreibung unterscheiden, andere nicht. Die Grafikfähigkeit der verschiedenen Sprachen ist sehr unterschiedlich. Daher ist es wichtig zu verstehen, wie man Ergebnisse in Dateien schreibt. Man ist dann unabhängig von der jeweiligen Sprache und kann die Ergebnisse anderweitig weiterverarbeiten.

5 Wahrscheinlichkeitsrechnung

5.1 Zufall und Wahrscheinlichkeit

Im täglichen Leben passieren immer wieder Dinge zufällig. Dies bedeutet, dass wir die Geschehnisse nicht vorhersagen können. Wir gehen morgens aus dem Haus und wissen nicht, was tags passiert. Wir sind uns aber im allgemeinen ziemlich sicher dass nichts Schlimmes wie z.B. ein Unfall passiert. Dagegen sind wir uns gerade in Oldenburg absolut nicht sicher, dass wir nicht nass werden. Woher haben wir dieses Wissen, obwohl wir manchmal trocken bleiben und leider auch mal einen Unfall haben? Aus Erfahrung wissen wir, dass es in Oldenburg häufig regnet. Die Wahrscheinlichkeit, nass zu werden, ist hoch. Aus Unfallstatistiken wissen wir, das die Gefahr einen Unfall zu erleiden gering ist.

Bei einem Würfelspiel vertrauen wir auf die Zufälligkeit des Würfels. Nur wenn die Wahrscheinlichkeiten für alle Spieler gleich sind (alle würfeln mit demselben Würfel) und die Wahrscheinlichkeit für alle Augenzahlen gleich sind, macht das Spiel Sinn. Würden alle Spieler immer nur Dreier (oder Sechser oder Einser) würfeln, wäre es kein Glücksspiel mehr, es wäre langweilig.

Bei Massenproduktionen kann man nicht alle Produkte testen. Man wählt zufällig einige aus, überprüft sie und schliesst von dem Ergebnis auf die gesamte Produktion.

In der Medizin werden Medikamente zugelassen, wenn sie an einer ausreichend großen Anzahl an Patienten wirkungsvoll waren. Damit wird die Wahrscheinlichkeit, dass ein Medikament hilft, wenn man es einnimmt, bestimmt. Ausserdem muss das Auftreten von Nebenwirkungen im Rahmen bleiben. „Im Rahmen bleiben„ bedeutet in diesem Zusammenhang, dass die Nebenwirkungen nur bei einer geringen Anzahl der Patienten auftreten und nicht bedrohlich sind. Damit wird die Wahrscheinlichkeit, dass Nebenwirkungen auftreten, wenn man das Medikament einnimmt, bestimmt. Trotzdem gibt es keine absolute Sicherheit. Ein zugelassenes Medikament kann wirkungslos bleiben oder Nebenwirkungen haben.

Den Ursprung der Wahrscheinlichkeitsrechnung findet man bei den Glücksspielen im 17. Jahrhundert.

Beispiel 5.1.1 Das Drei-Würfel-Problem

Es wir mit drei Würfeln (schwarz, rot, weiss) gleichzeitig gewürfelt. Wie gross ist die Chance (Wahrscheinlichkeit), die Augensumme 11 bzw. 12 zu würfeln. *Chevalier de Méré* (1607-1684) vermutete, dass die Chance die Augenzahl 11 zu würfeln

genauso gross ist, wie die Augenzahl 12 zu würfeln. Er löste das Problem auf folgende Weise:
Er betrachtete alle Augenzahlen, die in der Summe 11 bzw 12 ergeben:

Augensumme 11	Augensumme 12
6-4-1	6-5-1
6-3-2	6-4-2
5-5-1	6-3-3
5-4-2	5-5-2
5-3-3	5-4-3
4-4-3	4-4-4

Nun in der Praxis zeigt sich, dass die Augensumme 11 häufiger auftritt als die 12.
Blaise Pascal (1623-1662) löste das Problem: Pascal erkannte, dass es nicht nur darauf ankommt, dass die Augensumme stimmt, sondern dass es auch darauf ankommt auf welche Weisen diese Augensumme zustande kommt. Hierzu betrachten wir die Würfel getrennt:
Das Tripel 6-3-2 kann wie folgt realisiert werden:

schwarz	rot	weiss
6	3	2
6	2	3
3	6	2
3	2	6
2	6	3
2	3	6

Tripel, die aus drei verschiedenen Zahlen bestehen, können auf 6 verschiedene Weisen erzeugt werden.
Das Tripel 5-5-1 kann wie folgt realisiert werden:

schwarz	rot	weiss
5	5	1
5	1	5
1	5	5

Tripel, die aus zwei verschiedenen Zahlen bestehen, können auf 3 verschiedene Weisen erzeugt werden.
Das Tripel 4-4-4 kann nur durch:

schwarz	rot	weiss
4	4	4

erzeugt werden.

Damit ergeben sich folgende Möglichkeiten:

Augensumme 11	Möglichkeiten	Augensumme 12	Möglichkeiten
6-4-1	6	6-5-1	6
6-3-2	6	6-4-2	6
5-5-1	3	6-3-3	3
5-4-2	6	5-5-2	3
5-3-3	3	5-4-3	6
4-4-3	3	4-4-4	1
Summe	27	Summe	25

□

Man muss also das Problem, das man zu lösen hat, genauer ansehen und ein Modell von den realen Begebenheiten machen. Betrachten wir zunächst ein einfacheres Problem, den Münzwurf.

Beispiel 5.1.2 Münzwurf
Wird eine Münze geworfen, so landet diese zufällig so, dass entweder Adler oder Zahl oben liegt („auf dem Rand stehen“ vergessen wir mal). Es gibt also die zwei Fälle Adler (A) oder Zahl (Z). Wir fassen diese Fälle zu einer Ergebnismenge Ω zusammen. Damit besteht unsere Ergebnismenge aus den Elementen A und Z:

$$\Omega = \{A, Z\}$$

Das Ereignis „A tritt ein“ schreiben wir als Menge $\{A\}$.
Ist die Münze nicht gezinkt, also A und Z gleich wahrscheinlich so ist die Wahrscheinlichkeit für das Eintreten von A gleich der Wahrscheinlichkeit für das Eintreten von Z gleich $\frac{1}{2}$:

$$P(\{A\}) = \frac{1}{2} \qquad \text{und} \qquad P(\{Z\}) = \frac{1}{2}$$

Beispiel 5.1.3 Würfeln
Für das Würfeln mit einem Würfel ergibt sich die Ergebnismenge

$$\Omega = \{1,2,3,4,5,6\}$$

Ist der Würfel nicht gezinkt, gilt:

$$P(\{1\}) = P(\{2\}) = P(\{3\}) = P(\{4\}) = P(\{5\}) = P(\{6\}) = \frac{1}{6}$$

Nun kann man nicht nur sogenannte Elementarereignisse betrachten, sondern auch zusammengesetzte, wie z.B. $A = \{2,4,6\}$, also das Ereignis „das Ergebnis ist eine gerade Augenzahl“. Da es insgesamt 6 verschiedene Ausgänge gibt, von denen 3 gerade sind, steht zu vermuten, dass

$$P(\{2,4,6\}) = \frac{1}{2}$$

ist.

Wie haben wir das bestimmt? Wir betrachten die Anzahl der für das Ereignis A günstigen Ausgänge und teilen die durch die Anzahl der möglichen Fälle:

$$P(A) = \frac{\text{Anzahl der für das Ereignis A günstigen Ausgänge}}{\text{Anzahl der möglichen Ausgänge}}$$

$P(A)$ ist die Wahrscheinlichkeit, mit der das Ereignis A eintritt. Dies funktioniert aber nur dann, wenn alle Ergebnisse gleich wahrscheinlich sind (Gleichverteilung, Laplace-Verteilung).
Nun, formalisieren wir das ganze ein wenig.

Definition 5.1.1 Sei $\Omega \neq \emptyset$, endlich, die Ergebnismenge.

- Eine Teilmenge A von Ω ($A \subseteq \Omega$) heisst **Ereignis**.
- Eine einelementige Teilmenge von Ω heisst **Elementarerereignis**.
- Die Teilmenge Ω selbst heisst **sicheres Ereignis**.
- Die leere Menge $\emptyset$ heisst **unmögliches Ereignis**.

- zwei Ereignisse A und B heissen **unvereinbar**, wenn die Mengen A und B disjunkt sind.
- Ist A eine Teilmenge von Ω, so heisst $\overline{A} = \Omega \setminus A$ **Gegenereignis** zu A.

Ein Ereignis ist also ein Element der Potenzmenge von Ω. Ein Ereignis A ist eingetreten, wenn das beobachtete Ergebnis ω des Zufallsexperiments in der Teilmenge A enthalten ist ($\omega \in A$). Ist z.B. das Ereignis A das Ereignis, eine gerade Zahl zu würfeln, also $A = \{2,4,6\}$, so ist mit der Realisierung $\omega = 2$ das Ereignis A eingetreten.

Beispiel 5.1.4 Würfeln mit zwei Würfeln
Es seien zwei unterscheidbare Würfel (z.B. rot und schwarz) gegeben. Uns interessiert die Wahrscheinlichkeit, die Augensumme 9 zuwürfeln. Ein geeigneter Ergebnisraum ist durch

$$\Omega = \{(1,1),(1,2),(1,3),(1,4),(1,5),(1,6),(2,1),\ldots,(6,5),(6,6)\}$$

gegeben. Hierbei beschreibt die erste Zahl in jedem 2-Tupel die Augenzahl des roten, und die zweite Zahl die Augenzahl des schwarzen Würfels. Insgesamt gibt es also 36 Elementarereignisse.
Das Ereignis, die Augensumme 9 zu werfen wird durch

$$A = \{(3,6),(4,5),(5,4),(6,3)\}$$

beschrieben. Damit beträgt die Wahrscheinlichkeit für die Augensumme 9 :
$P(A) = \frac{4}{36}$. □

5.1.1 Das Axiomensystem von Kolmogoroff

Bisher sind wir davon ausgegangen, dass die Wahrscheinlichkeit für alle Elemetarereignisse gleich ist. Dies muss aber nicht der Fall sein.

Beispiel 5.1.5 Gezinkter Würfel
In einen Holzwürfel sei eine Stahlkugel eingelassen, so dass er folgende Wahrscheinlichkeiten liefert:

$$P(1) = \frac{1}{12} \qquad P(2) = P(3) = P(4) = P(5) = \frac{1}{6} \qquad P(6) = \frac{3}{12}$$

Das Axiomensystem von Kolmogoroff verallgemeinert den Wahrscheinlichkeit-Begriff und formalisiert ihn:

Definition 5.1.2 Sei $\Omega \neq \emptyset$ endliche Ergebnismenge, und sei

$$P : \mathcal{P}(\Omega) \to \mathbb{R}$$

eine Abbildung P der Potenzmenge $\mathcal{P}(\Omega)$. P heisst **Wahrscheinlichkeitsmaß** (oder Wahrscheinlichkeitsverteilung), wenn gilt

1. $P(A) \geq 0$ für alle $A \in \mathcal{P}(\Omega)$; Nichtnegativität
2. $P(\Omega) = 1$; Normierung
3. $P(A \cup B) = P(A) + P(B)$ für alle disjunkten $A, B \in \mathcal{P}(\Omega)$; Additivität

$P(A)$ heisst **Wahrscheinlichkeit** von A.
Das Paar (Ω, P) heisst **Wahrscheinlichkeitsraum**.

Folgerungen

Satz 5.1.1 Sei A Ereignis des Wahrscheinlichkeitsraums (Ω, P) , dann gilt

$$P(\overline{A}) = 1 - P(A)$$

Beweis A und $\overline{A}$ sind unvereinbar, damit gilt nach dem dritten Axiom $P(A \cup \overline{A}) = P(A) + P(\overline{A})$. Nach Axiom 2 gilt $P(A \cup \overline{A}) = P(\Omega) = 1$. Es folgt $P(A) + P(\overline{A}) = 1$. ■

Satz 5.1.2 Die Wahrscheinlichkeit eines Ereignisses A nimmt nur Werte zwischen Null und Eins an: $0 \leq P(A) \leq 1$

Beweis Sei $A \in \mathcal{P}(\Omega)$. Nach Axiom 1 gilt $P(A) \geq 0$. Nach Satz 5.1.1 gilt $P(\overline{A}) = 1 - P(A)$ und damit $P(A) = 1 - P(\overline{A}) \leq 1$. ■

Satz 5.1.3 Die Wahrscheinlichkeit des unmöglichen Ereignisses $\emptyset$ ist Null: $P(\emptyset) = 0$.

Beweis Es gilt $\overline{\Omega} = \emptyset$. Nach Satz 5.1.1 gilt $P(\emptyset) = P(\overline{\Omega}) = 1 - P(\Omega) = 0$. ■

Das dritte Axiom lässt sich erweiteren:

Satz 5.1.4 Sind die Ereignisse $A_1, \cdots, A_n$ paarweise unvereinbar, d.h. $A_i \cap A_j = \emptyset$ für $i \neq j$ mit $i, j \in \{1, 2, \cdots, n\}$, dann gilt:

$$P(\bigcup_{i=1}^{n} A_i) = \sum_{i=1}^{n} P(A_i)$$

Beweis Übung ■

Beispiel 5.1.6 Nochmal der gezinkte Würfel
Der gezinkte Würfel liefert:

$$P(1) = \frac{1}{12} \qquad P(2) = P(3) = P(4) = P(5) = \frac{1}{6} \qquad P(6) = \frac{3}{12}$$

Wie groß ist die Wahrscheinlichkeit, eine gerade Zahl zu würfeln?

Da die Ereignisse $\{2\}$, $\{4\}$, $\{6\}$ unvereinbar sind gilt nach Satz 5.1.4,

$$P(\{2,4,6\}) = P(\{2\}) + P(\{4\}) + P(\{6\}) = \frac{1}{6} + \frac{1}{6} + \frac{3}{12} = \frac{7}{12}$$

Wie groß ist die Wahrscheinlichkeit, eine ungerade Zahl oder eine Primzahl zu würfeln?

$A = \{2,3,5\}$ beschreibt das Ereignis, eine Primzahl zu würfeln, mit

$$P(A) = P(\{2\}) + P(\{3\}) + P(\{5\}) = \frac{1}{6} + \frac{1}{6} + \frac{1}{6} = \frac{6}{12}$$

$B = \{1,3,5\}$ beschreibt das Ereignis, eine ungerade Zahl zu würfeln, mit

$$P(B) = P(\{1\}) + P(\{3\}) + P(\{5\}) = \frac{1}{12} + \frac{1}{6} + \frac{1}{6} = \frac{5}{12}$$

Das Ereignis, eine ungerade Zahl oder eine Primzahl zu würfeln ist durch $A \cup B = \{1,2,3,5\}$ beschrieben, und es gilt

$$P(A \cup B) = P(\{1\}) + P(\{2\}) + P(\{3\}) + P(\{5\}) = \frac{1}{12} + \frac{1}{6} + \frac{1}{6} + \frac{1}{6} = \frac{7}{12}$$

Damit ist

$$\frac{7}{12} = P(A \cup B) \neq P(A) + P(B) = \frac{11}{12}$$

Der Grund hierfür liegt darin, dass die Ereignisse A und B nicht unvereinbar sind, denn die Zahlen 3 und 5 sind zugleich ungerade und prim. Bei der Summenbildung werden ihre Wahrscheinlichkeit also doppelt berücksichtigt. Man muss also die Wahrscheinlichkeit der Elemente, die sowohl in A als auch in B liegen einmal abziehen.
Die Menge aller Elemente, die sowohl in A als auch in B liegen, ist aber gerade die Schnittmenge $A \cap B = \{3,5\}$, mit

$$P(A \cap B) = P(\{3\}) + P(\{5\}) = \frac{1}{6} + \frac{1}{6} = \frac{2}{6}$$

und es gilt

$$P(A \cup B) = P(A) + P(B) - P(A \cap B) = \frac{6}{12} + \frac{5}{12} - \frac{4}{12} = \frac{7}{12}$$

Satz 5.1.5 Seien A, B Ereignisse des Wahrscheinlichkeitsraum (Ω, P), dann gilt

$$P(A \cup B) = P(A) + P(B) - P(A \cap B)$$

Bemerkung: Sind die Ereignisse A und B unvereinbar so reduziert sich Satz 5.1.5 auf das dritte Axiom, denn es gilt $A \cap B = \emptyset$, also mit Satz 5.1.3 $P(A \cap B) = 0$.

5.1.2 Laplace-Verteilung (Gleichverteilung)

Die Laplace-Verteilung ist dadurch gekennzeichnet, dass alle Ausgänge gleich wahrscheinlich sind. Wir hatten uns bereits anschaulich folgendes Wahrscheinlichkeits-

maß überlegt:

$$P(A) = \frac{\text{Anzahl der für das Ereignis A günstigen Ausgänge}}{\text{Anzahl der möglichen Ausgänge}}$$

P erfüllt die drei Kolmogoroffschen Axiome:

1. $P(A) \geq 0$ für alle $A \in \mathcal{P}(\Omega)$, denn die Anzahl der günstigen Ausgänge ist größer oder gleich null.

2. $P(\Omega) = 1$, denn für $A = \Omega$ ist die Anzahl der günstigen Ausgänge gleich der Anzahl der möglichen.

3. $P(A \cup B) = P(A) + P(B)$ für alle disjunkten $A, B \in \mathcal{P}(\Omega)$: Sei $g(A)$ die Anzahl der günstigen Fälle von A und $g(B)$ die Anzahl der günstigen Fälle von B. Da A und B unvereinbar sind, gilt $g(A \cup B) = g(A) + g(B)$. Mit der Anzahl m der möglichen Fälle gilt nun also

$$P(A \cup B) = \frac{g(A \cup B)}{m} = \frac{g(A) + g(B)}{m} = \frac{g(A)}{m} + \frac{g(B)}{m} = P(A) + P(B)$$

Ist $\Omega = \{\omega_1, \cdots, \omega_n\}$ eine nichtleere, endliche Ergebnismenge mit den Elementarereignissen $\omega_1, \cdots, \omega_n$ und $A \in \mathcal{P}(\Omega)$. Die für A günstigen Ausgänge sind gerade die Elementarereignisse, die in A enthalten sind. Es ist also (wegen der Unvereinbarkeit der Elementarereignisse):

$$P(A) = \sum_{\omega_i \in A} P(\{\omega_i\}) \qquad \text{für alle } A \in \mathcal{P}(\Omega), A \neq \emptyset$$

Damit ist folgende Definition sinnvoll:

Definition 5.1.3 Sei $\Omega = \{\omega_1, \cdots, \omega_n\}$ eine nichtleere, endliche Ergebnismenge mit den Elementarereignissen $\omega_1, \cdots, \omega_n$. Die durch

$$P(\{\omega\}) = \frac{1}{|\Omega|} \qquad \text{für alle } \omega \in \Omega$$

definierte Wahrscheinlichkeitverteilung heisst **Laplace-Verteilung** oder **Gleichverteilung**. (Ω, P) heisst **Laplacescher Wahrscheinlichkeitsraum**.

Bemerkung: Für $P(\{\omega\})$ schreibt man auch kurz $P(\omega)$.

5.2 Kombinatorik

Bisher haben wir uns formal überlegt, wie ein Wahrscheinlichkeitsraum aussieht. Um nun Wahrscheinlichkeiten zu berechnen, muss man nun die Anzahl der günstigen Augänge und die Anzahl der möglichen Fälle kennen.
Diese Anzahlbestimmung ist Gegenstand der Kombinatorik. Die Kombinatorik liefert Strategien, geschickt zu zählen.

5.2.1 Kombinatorisches Zählen

Die einfachste Möglichkeit, eine Anzahl zu bestimmen, ist das Abzählen. Will man die Anzahl von Äpfeln in einer Schale bestimmen, so ordnet man jedem Apfel fortlaufend beginnend bei Eins eine natürliche Zahl zu, man zählt die Anzahl der Äpfel durch.
Formal ordnet man den Elementen einer endlichen Menge die Ziffern 1,2, ... zu. Es darf kein Element mehrfach belegt werden oder ausgelassen werden. Eine Menge A hat genau dann n Elemente, wenn es eine bijektive Abbildung der Menge A auf die Menge $\{i|\ i \in \mathbb{N}, i \leq n\}$ gibt. Man bezeichnet die Mächtigkeit der Menge mit $|A| = n$. Ist $A = \emptyset$, so definiert man $|A| = 0$.
Bei vielen Problemstellungen ist das Abzählen mühsam. Sind z.B Bodenfliesen rechteckig angeordnet (Abbildung 5.1), so wird man die Fliesen nicht Abzählen, sondern die Anzahl der Fliesen in einer Reihe mal der Anzahl der Reihen nehmen.

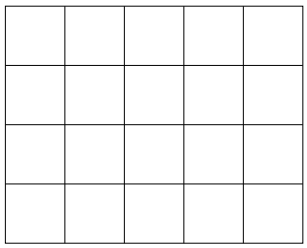


Abbildung 5.1: 4 Reihen mit jeweils 5 Fliesen ergibt $4 \cdot 5 = 20$ Fliesen.

Es gibt Probleme, bei denen die Zählstrategie nicht so offensichtlich ist.

Beispiel 5.2.1 Klamotten
Nehmen wir an wir stehen vor dem Kleiderschrank und haben folgendes zur Auswahl: Zwei verschiedene Jacken (Regenjacke (R) und Windjacke (W) , drei verschiedene T-Shirts (blau (B), bchwarz (S) und gelb (G) und zwei verschiedene Hosen (lang (L) und kurz (K)). Wieviele Kombinationen gibt es?

Zu den zwei Hosen gibt es jeweils drei Möglichkeiten an T- Shirts. Macht insgesamt sechs Möglichkeiten. Zu diesen sechs Möglichkeiten kann man nun jeweils aus den zwei Jacken wählen, macht insgesamt 12 Möglichkeiten (Abbildung 5.2). Es spielt hierbei keine Rolle, ob wir zuerst das T-Shirt, die Hose oder die Jacke auswählen.

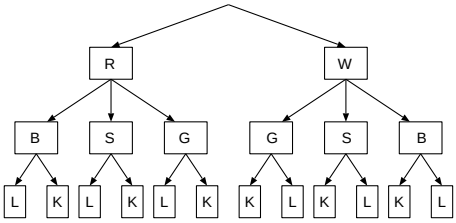


Abbildung 5.2: Auswahlmöglichkeiten aus zwei Jacken (R,W, 2 Äste), 3 T-Shirts (B,S,G, 3 Äste) und zwei Hosen (K,L, 2 Äste)

Beispiel 5.2.2 Bauklötze

Wieviele verschiedene Türme aus drei verschiedenfarbigen Bauklötzen kann man bauen? Hat man drei Bauklötze (rot,grün und blau), so kann man diese wie folgt anordnen: Für den untersten gibt es drei Möglichkeiten, für den mittleren bleiben noch zwei, der letzte wird oben draufgelegt. Insgesamt gibt es also $3 \cdot 2 \cdot 1 = 6$ Möglichkeiten (Abbildung 5.3).

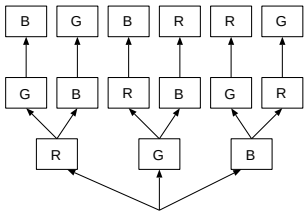


Abbildung 5.3: Anordnung von drei verschiedenfarbigen (r,g,b) Bauklötzen.

Beispiel 5.2.3 PIN

Bei der 4-stelligen Geheimzahl einer Bank (PIN, persönliche Identifikationsnummer) kann jede Stelle die Ziffern 0-9 annehmen[1]. Es gibt also für jede Stelle 10 Möglichkeiten. Zu jeder Ziffer an der ersten Stelle gibt es 10 Möglichkeiten für die zweite Ziffer usw. Insgesamt gibt es also 10^4 Möglichkeiten. Im Unterschied zum Klamotten-Beispiel sind hier die Realisierungen für jede Stelle gleich □

[1] In der Realität gibt es vermutlich keine Geheimzahlen, die mit 0, 00 oder 000 beginnen. Dies soll uns hier aber nicht stören.

Man erhält das Fundamentalprinzip des Zählens:

Satz 5.2.1 Fundamentalprinzip des Zählens
Es sei die n-gliedrige Sequenz $a_1\ a_2\ \ldots\ a_n$ zu bilden, wobei es für die i-te Stelle a_i k_i Realisierungen gibt ($i = 1, \ldots, n$).
Dann gibt es insgesamt $k_1 \cdot k_2 \cdot \ldots \cdot k_n$ verschiedene n-gliedrige Sequenzen.

Man kann dieses Prinzip auch anders betrachten. Will man eine PIN knacken, so muss man die einzelnen Stellen durch Versuche ermitteln. Das Gesamt-„Experiment“ PIN-Knacken besteht also aus vier Teilversuchen mit jeweils 10 möglichen Ausgängen.

Satz 5.2.2 Fundamentalprinzip des Zählens (alternativ)
Besteht ein Experiment aus n Teilversuchen, bei dem der i-te Teilversuch k_i mögliche Ergebnisse hat ($i = 1, \ldots, n$), dann hat das Experiment insgesamt
$k_1 \cdot k_2 \cdot \ldots \cdot k_n$ verschiedene mögliche Ergebnisse.

Hierbei sind die Teilversuche voneinander unabhängig (siehe auch Satz 5.2.6). Im folgenden Abschnitt betrachten wir ein Beispiel, bei dem die Einzelergebnisse nicht unabhängig sind. Bei den PINs wäre dies der Fall, wenn eine Ziffer nicht mehrfach auftreten dürfte.

5.2.2 Permutationen ohne Wiederholung

Beispiel 5.2.4 Eiskugeln
Ein Eishörnchen mit zwei verschiedenen Sorten Eis (Schoko und Vanille) kann auf zwei Arten gebaut werden: Die erste Kugel ist Vanille, dann ist die zweite Kugel Schoko. Oder die erste Kugel ist Schoko, dann ist die zweite Kugel Vanille. Wir haben also für die erste Kugel die freie Auswahl, die zweite ist dann klar. Betrachten wir nun 3 Sorten (Schoko, Vanille, Nuss) und drei Kugeln: Die erste Kugel ist beliebig wählbar, z.B. Nuss. Dann bleiben für die zweite Kugel zwei Möglichkeiten (Schoko oder Vanille) . Wählt man eine davon aus, ist die letzte Kugel festgelegt. Man hat also für die erste Kugel 3, für die zweite 2 und die dritte 1 Möglichkeit. Man hat also $1 \cdot 2 \cdot 3 = 6$ Möglichkeiten. Eine vierte Kugel (Zitrone) kann nun bei jeder Kombination vor die erste, zweite, dritte Kugel oder oben drauf gesetzt werden.

Für jede bisherige Kombination kommen dann 4 weitere hinzu also, $1 \cdot 2 \cdot 3 \cdot 4 = 24$ Möglichkeiten.

Unter Berücksichtigung der Reihenfolge können 4 verschiedenen Dinge also auf $1 \cdot 2 \cdot 3 \cdot 4$ Arten angeordnet werden (siehe auch Beispiel 5.2.2). Wir schreiben $1 \cdot 2 \cdot 3 \cdot 4 = 4!$ □

Eine Anordnung von Dingen mit Berücksichtigung der Reihenfolge nennt man Permutation ohne Wiederholung. Der Begriff ohne Wiederholung bedeutet, dass jedes Ding nur einmal ausgewählt werden kann. Dies wird deutlich, wenn man das „Experiment“ als Urnenmodell betrachtet. Aus einer Urne mit n Kugeln, die sich in ihrer Farbe unterscheiden, werden nacheinander n-Kugeln gezogen. Jede mögliche Farbanordnung ist dann eine Permutation.

Definition 5.2.1 Permutation ohne Wiederholung
Sei eine n-elementige Menge gegeben. Eine Anordnung von n Elementen aus dieser Menge, die jedes Element genau einmal enthält, heisst n-Permutation ohne Wiederholung aus einer Menge von n Elementen. Im Urnenmodell handelt es sich dabei um eine geordnete Stichprobe vom Umfang n aus einer Urne mit n unterscheidbaren Kugeln.

Definition 5.2.2 Fakultät
Das Produkt $1 \cdot 2 \cdot 3 \cdot \cdots \cdot n$ bezeichnen wir mit $n!$ (sprich: n Fakultät).
Man setzt $0! = 1$.

Satz 5.2.3 Permutation ohne Wiederholung
Unter Berücksichtigung der Reihenfolge lassen sich n verschiedene Dinge auf $n!$ verschiedene Arten anordnen.

Beweis durch vollständige Induktion
Induktionsverankerung $n = 1$:
Ein Element kann nur auf eine Weise angeordnet werden: 1=1!

Induktionsschritt von $n \to n+1$:
Es gelte: n Elemente lassen sich auf $n!$ Arten anordnen. Ein weiteres Element kann jeweils vor dem ersten, zweiten, ... , nten Element eingeordnet werden oder an das Ende gestellt werden. D.h. zu jeder Permutation von n Elementen gibt es $n+1$ weitere Möglichkeiten. Damit beträgt die Anzahl der Permutationen von $n+1$ Elementen nach Induktionsannahme $(n+1) \cdot n! = (n+1)!$. ■

Beispiel 5.2.5 Fußball
Beim Fussball stehen bei der Nationalhymne die 10 Feldspieler in beliebiger Reihenfolge nebeneinander. Wie gross ist die Wahrscheinlichkeit, dass Kuranyi neben Ballack steht? Es gibt insgesamt 10! Möglichkeiten, wie die 10 Feldspieler stehen können. Die günstigen Fälle sind die, wo Kuranyi und Ballack auf den Plätzen (1,2), (2,3), ..., (9,10) stehen. Die anderen 8 Spieler können dann beliebig auf den anderen Plätzen stehen. Für jedes der 9 Platzpaare gibt es wiederum jeweils 2 Möglichkeiten. Insgesamt gibt es also $2 \cdot 9 \cdot 8!$ günstige Permutationen. Die Wahrscheinlichkeit P beträgt also

$$P = \frac{2 \cdot 9 \cdot 8!}{10!} = \frac{2 \cdot 9 \cdot 8!}{10 \cdot 9 \cdot 8!} = \frac{2}{10}.$$

Beispiel 5.2.6 Eiskugeln: 2 Kugeln aus 5 Sorten ohne Doppelte
Es gebe die Eissorten Schoko, Vanille, Nuss, Erdbeer und Zitrone. Ein Hörnchen mit zwei Kugeln kann auf $5 \cdot 4 = 20$ Arten gebildet werden, wobei z.B. Schoko-Vanille und Vanille-Schoko unterschieden werden. □

Definition 5.2.3 k-Permutation ohne Wiederholung aus n Elementen
Sei eine n-elementige Menge gegeben. Eine Anordnung von k ($k < n$) Elementen aus dieser Menge, und die jedes Element höchstens einmal enthält, heisst **k-Permutation ohne Wiederholung** aus einer Menge von n Elementen.

Im Urnenmodell handelt es sich dabei um eine geordnete Stichprobe vom Umfang k aus einer Urne mit n unterscheidbaren Kugeln.

Satz 5.2.4 k-Permutation ohne Wiederholung aus n Elementen
Unter Berücksichtigung der Reihenfolge lassen sich k Elemente aus einer n-

elementigen Menge auf

$$n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot (n-(k-1)) = \frac{n!}{(n-k)!}$$

verschiedene Arten anordnen.

Beispiel 5.2.7 Nehmen wir nun an, dass wir ein Eis aus 3-mal Vanille 2-mal Schoko und 4-mal Nuss haben. Insgesamt haben wir also 9 Kugeln Eis. Nummerieren wir die Kugeln durch, so gibt es insgesamt 9! Möglichkeiten, die Kugeln anzuordnen. Da aber einige gleich sind, kann man einige Permuationen nicht voneinander unterscheiden, z.B. ist die Permutation

$V_1\ V_2\ V_3\ S_1\ S_2\ N_1\ N_2\ N_3\ N_4$ von

$V_2\ V_1\ V_3\ S_1\ S_2\ N_1\ N_2\ N_3\ N_4$ nicht zu unterscheiden.

Die Frage ist nun, wieviele unterscheidbare Kombinationen existieren? Die 3 Kugeln Vanilleeis anzuordnen geht auf 3! Arten, die 2 Schoko auf 2!, und die 4 Nuss auf 4! Arten. Man erhält also insgesamt $3! \cdot 2! \cdot 4!$ Möglichkeiten.
Damit bleiben insgesamt $\frac{9!}{3! \cdot 2! \cdot 4!}$=1260 Möglichkeiten. □

Satz 5.2.5 n Dinge, von denen jeweils $n_1, n_2, \ldots, n_r$ gleich sind, und für die $n_1 + n_2 + \ldots + n_r = n$ gilt, lassen sich auf

$$\frac{n!}{n_1! \cdot n_2! \cdot \ldots \cdot n_r!}$$

verschiedene Arten anordnen.

5.2.3 Permutationen mit Wiederholung

Bisher trat jedes Element in den Permutationen höchstens einmal auf. Jetzt betrachten wir Permutationen, bei denen Elemente auch mehrfach vorkommen dürfen (z.B. 2 Kugeln Vanilleeis):

Definition 5.2.4 k-Permutation mit Wiederholung aus n Elementen
Sei eine n-elementige Menge gegeben. Eine Sequenz von k Elementen aus dieser Menge, wobei an jeder Stelle ein beliebiges Element der Menge stehen darf, heisst **k-Permutation mit Wiederholung** aus einer Menge von n Elementen.

Im Urnenmodell handelt es sich dabei um eine geordnete Stichprobe vom Umfang k aus einer Urne mit n unterscheidbaren Kugeln, wobei die gezogene Kugel jeweils in die Urne zurückgelegt wird.

Satz 5.2.6 k-Permutation mit Wiederholung aus n Elementen
Unter Berücksichtigung der Reihenfolge lassen sich k Elemente aus einer n-elementigen Menge auf

$$n^k$$

verschiedene Arten anordnen, wenn Wiederholungen der Elemente zulässig sind.

Beispiel 5.2.8 Eiskugeln: 2 Kugeln aus 5 Sorten mit Doppelten
Es gebe die Eissorten Schoko, Vanille, Nuss, Erdbeer und Zitrone. Ein Hörnchen mit zwei Kugeln kann auf $5^2 = 25$ Arten gebildet werden, wobei z.B. Schoko-Vanille und Vanille-Schoko unterschieden werden. Hier sind zum Beispiel ohne doppelte Sorten gerade die fünf Anordnungen hinzugekommen, in denen beide Kugeln gleich sind.

5.2.4 Kombinationen ohne Wiederholung

Nun ist es ja einigen Menschen völlig egal, ob sie ein Schoko-Vanille-Zitrone-Eis oder ein Zitrone-Vanille-Schoko-Eis bekommen, Haupsache drei Sorten. Wir betrachten nun also den Fall, dass die Elemente der Stichprobe verschiedenen sind, es aber nicht auf die Reihenfolge ankommt.

Betrachten wir zunächst die Anzahl der Möglichkeiten unter Berücksichtigung der Reihenfolge. In diesem Fall gibt es nach Satz 5.2.4 bei n Sorten und k Kugeln

$\frac{n!}{(n-k)!}$ Anordnungen. Bei 5 Sorten und 3 Kugeln sind das 60 Möglichkeiten, wobei Zitrone-Schoko-Vanille, Vanille-Schoko-Zitrone, etc. verschiedene Anordnungen sind. Jede Dreierkombination kann nach Satz 5.2.3 auf 3! verschiedene Arten dargestellt werden. Damit ergibt sich die Zahl der Möglichkeiten ohne Berücksichtigung der Reihenfolge zu $\frac{60}{3!} = 10$.

Definition 5.2.5 k-Kombination ohne Wiederholung aus n Elementen
Sei eine n-elementige Menge gegeben. Eine Sequenz von k Elementen aus dieser Menge, die jedes Element höchstens einmal enthält, heisst **k-Kombination ohne Wiederholung** aus einer Menge von n Elementen. Hierbei ist die Reihenfolge der Elemente egal.

Im Urnenmodell handelt es sich dabei um eine ungeordnete Stichprobe vom Umfang k aus einer Urne mit n unterscheidbaren Kugeln, ohne Zurücklegen.

Satz 5.2.7 k-Kombination ohne Wiederholung aus n Elementen
Ohne Berücksichtigung der Reihenfolge lassen sich k Elemente aus einer n-elementigen Menge auf

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

verschiedene Arten anordnen, wenn keine Wiederholungen der Elemente zulässig sind.

Definition 5.2.6 Binomialkoeffizient
Die Zahlen

$$\binom{n}{k} := \frac{n!}{(n-k)! \cdot k!} \qquad \text{sprich: n über k}$$

heissen Binomialkoeffizienten. Mit der Definition $0! = 1$ gilt $\binom{n}{0} = 1$.

Beispiel 5.2.9 Lotto
Beim Lotto „6 aus 49“ werden aus 49 Zahlen nacheinander 6 gezogen. Da die Spieler auf ihrem Lottoschein keine Reihenfolge angeben, kommt es auf diese auch

nicht an. Wie groß ist nun die Wahrscheinlichkeit für einen Sechser im Lotto?

Es handelt sich hierbei um eine ungeordnete Stichprobe vom Umfang 6 aus einer Urne mit 49 unterscheidbaren Kugeln. Damit ist die Anzahl der möglichen Kombinationen $\binom{49}{6} = 13983816$. Da nur eine Kombination die richtige ist, beträgt die Wahrscheinlichkeit

$$P(\text{„6 richtige“}) = \frac{1}{\binom{49}{6}} = \frac{1}{13983816} \approx 0,00000007\,,$$

also in etwa 1 zu 14 Millionen.

Es gibt auch noch die Zusatzzahl: 5 richtige plus Zusatzzahl bedeutet, dass die sechste Zahl die Zusatzzahl ist. Um von den gezogenen 6 Zahlen nur 5 richtig zu haben gibt es $\binom{6}{5} = 6$ Möglichkeiten, nämlich die erste falsch zu haben oder die zweite oder ... die sechste. Da die sechste Zahl die Zusatzzahl sein muss, gibt es genau $\binom{6}{5}$ günstige Fälle. Damit beträgt die Wahrscheinlichkeit

$$P(\text{„5 richtige plus Zusatzzahl“}) = \frac{\binom{6}{5}}{\binom{49}{6}} = \frac{6}{13983816} \approx 0,0000004\,.$$

Nun ist es ja auch noch gut, 5 Richtige zu haben. Die sechste Zahl muss dann aus den 42 verbleibenden stammen (nämlich 49 Zahlen ohne die 6 Gewinnzahlen und ohne die Zusatzzahl). Es gibt also $42 \cdot \binom{6}{5}$ günstige Möglichkeiten.

Damit beträgt die Wahrscheinlichkeit

$$P(\text{„5 Richtige“}) = \frac{\binom{6}{5} \cdot 42}{\binom{49}{6}} = \frac{252}{13983816} \approx 0,00002\,.$$

Bei 4 Richtigen muss man berücksichtigen, dass für die verbleibenden zwei falschen Zahlen zwei aus 43 gewählt werden dürfen (die Zusatzzahl hat bei weniger als 5 Richtigen keine Bedeutung):

$$P(\text{„4 richtige“}) = \frac{\binom{6}{4} \cdot \binom{43}{2}}{\binom{49}{6}} = \frac{13545}{13983816} \approx 0,001\,.$$

Wahrscheinlichkeit beim mehrmaligen Ziehen ohne Zurücklegen

Betrachten wir noch einmal das Lotto Beispiel „6 aus 49“ . Um 4 richtige zu ziehen, haben wird zuerst die Anzahl der Möglichkeiten bestimmt. Dies waren $\binom{49}{6}$. Dann haben wird die Anzahl der Kombinationen bestimmt, 4 Zahlen aus den 6 Richtigen zu ziehen. Dies waren $\binom{6}{4}$. Zu jeder dieser Kombination gibt es dann noch beliebige Kombinationen aus den restlichen Zahlen $\binom{43}{2}$, so dass

$$P(\text{„4 richtige“}) = \frac{\binom{6}{4} \cdot \binom{43}{2}}{\binom{49}{6}}$$

gilt.
Man kann dieses Experiment auch in Form eines Urnenmodells betrachten. Eine Urne enthalte 49 Kugeln, von denen 6 schwarz und 43 weiss sind. Die 6 schwarzen sind die Richtigen. Aus der Urne werden 6 Kugeln gezogen ohne sie jeweils nach dem Zug zurückzulegen. Die Wahrscheinlichkeit, dass unter den 6 gezogenen Kugeln gerade 4 schwarze sind, beträgt dann $\frac{\binom{6}{4}\cdot\binom{49-6}{6-4}}{\binom{49}{6}} = \frac{\binom{6}{4}\cdot\binom{43}{2}}{\binom{49}{6}}$.
Allgemein gilt der

Satz 5.2.8 Eine Urne enthalte N Kugeln, von denen M schwarz und $N-M$ weiss sind. Aus der Urne werden n ($n \leq N$) Kugeln gezogen ohne sie jeweils nach dem Zug zurückzulegen. Die Wahrscheinlichkeit, dass unter den n gezogenen Kugeln gerade k schwarze sind, beträgt

$$p_k = \frac{\binom{M}{k} \cdot \binom{N-M}{n-k}}{\binom{N}{n}} \qquad \text{für} \quad 0 \leq k \leq \min(M,n)\,.$$

In Abschnitt 5.7.2 werden wir sehen, dass es sich um eine hypergeometrische Verteilung handelt.

Beispiel 5.2.10 Qualitätskontrolle
In einer Produktion von 10 Festplatten sind 4 fehlerhaft. Es werden zwei Platten zufällig ausgewählt. Wie groß ist die Wahrscheinlichkeit dabei k=0,1,2 defekte Platten zu erwischen. Wir betrachten die defekten Platten als schwarz, die funktionsfähigen als weiss. Mit N=10 M=4 und n=2 gilt:

$$p_0 = \frac{\binom{4}{0} \cdot \binom{6}{2}}{\binom{10}{2}} = \frac{1 \cdot 15}{45} = \frac{5}{15}$$

$$p_1 = \frac{\binom{4}{1} \cdot \binom{6}{1}}{\binom{10}{2}} = \frac{4 \cdot 6}{45} = \frac{8}{15}$$

$$p_2 = \frac{\binom{4}{2} \cdot \binom{6}{0}}{\binom{10}{2}} = \frac{6 \cdot 1}{45} = \frac{2}{15}$$

Für eine Qualitätskontrolle muss das ganze natürlich andersherumlaufen. Man wählt zwei Platten aus, schaut nach, ob sie defekt sind und bestimmt für 0,1,..,10 defekte Platten die Wahrscheinlichkeiten, dass gerade diese Anzahl fehlerhaft ist. Dieses Verfahren ist natürlich nur bei sehr viel größeren Stückzahlen und Stichproben aussagekräftig.
Angenommen man wählt aus 20 Festplatten zufällig drei aus. Von diesen ist eine fehlerhaft, dann ergeben sich folgende Wahrscheinlichkeiten:

$$P(1 \text{ defekt}) = \frac{\binom{1}{1} \cdot \binom{19}{2}}{\binom{20}{3}} = 0,15 \qquad P(6 \text{ defekt}) = \frac{\binom{6}{1} \cdot \binom{14}{2}}{\binom{20}{3}} = 0,48$$

$$P(2 \text{ defekt}) = \frac{\binom{2}{1} \cdot \binom{18}{2}}{\binom{20}{3}} = 0,27 \qquad P(7 \text{ defekt}) = \frac{\binom{7}{1} \cdot \binom{13}{2}}{\binom{20}{3}} = 0,48$$

$$P(3 \text{ defekt}) = \frac{\binom{3}{1} \cdot \binom{17}{2}}{\binom{20}{3}} = 0,36 \qquad P(8 \text{ defekt}) = \frac{\binom{8}{1} \cdot \binom{12}{2}}{\binom{20}{3}} = 0,46$$

$$P(4 \text{ defekt}) = \frac{\binom{4}{1} \cdot \binom{16}{2}}{\binom{20}{3}} = 0,42 \qquad P(9 \text{ defekt}) = \frac{\binom{9}{1} \cdot \binom{11}{2}}{\binom{20}{3}} = 0,43$$

$$P(5 \text{ defekt}) = \frac{\binom{5}{1} \cdot \binom{15}{2}}{\binom{20}{3}} = 0,46 \qquad P(10 \text{ defekt}) = \frac{\binom{10}{1} \cdot \binom{10}{2}}{\binom{20}{3}} = 0,39$$

...

Die Wahrscheinlichkeit ist am größten für sechs oder sieben Festplatten. □

5.2.5 Kombinationen mit Wiederholung

Nun fehlt uns noch die letzte Möglichkeit ein Eis zu bestellen. Wir können aus 5 Sorten drei Kugeln wählen, wobei uns die Reihenfolge egal ist und wir auch mit 3 mal Schoko etc. oder 2 mal Vanille und 1 mal Zitrone glücklich sind.

Definition 5.2.7 k-Kombination mit Wiederholung aus n Elementen
Sei eine n-elementige Menge gegeben. Eine Sequenz von k Elementen aus dieser Menge, heisst **k-Kombination mit Wiederholung** aus einer Menge von n Elementen, wobei Wiederholungen der Elemente zulässig sind . Die Reihenfolge der Elemente ist egal.

Im Urnenmodell handelt es sich dabei um eine ungeordnete Stichprobe vom Umfang k aus einer Urne mit n unterscheidbaren Kugeln, mit Zurücklegen.

Satz 5.2.9 k-Kombination mit Wiederholung aus n Elementen
Ohne Berücksichtigung der Reihenfolge lassen sich k Elemente aus einer n-elementigen Menge auf

$$\binom{n+k-1}{k}$$

verschiedene Arten anordnen, wobei Wiederholungen der Elemente zulässig sind.

Um dies zu verstehen müssen wir ein wenig ausholen. Sei also n die Anzahl der Eissorten und k die Anzahl der Kugeln in der Eistüte. Die Anzahl der Möglichkeiten, eine bestimmte Kombination zu bilden, hängt davon ab wieviel Doppelte, Dreifache etc. vorkommen. Sind alle Kugeln gleich, gibt es nur eine Permutation zu dieser Kombination, sind alle verschieden gibt es nach Satz 5.2.7 $\binom{n}{k}$. Nun ist es mühsam, dies für alle Fälle dazwischen zu berechnen. Daher führen wir das Problem darauf zurück, dass alle Kugeln verschieden sind.

Nummerieren wir zuerst die Eissorten durch, dann ist $\mathbb{A} = \{1,...,n\}$ die Anzahl der Eissorten. Eine Realisierung ist dann durch $(\omega_1,\ldots,\omega_k)$ mit $\omega_1,\ldots,\omega_k \in \mathbb{A}$ gegeben. Zu einer Kombination wählen wird diejenige Permutation aus, in der die Kugeln sortiert sind, also $\omega_1 \leq \omega_2 \leq \ldots \leq \omega_k$ gilt. Das Problem besteht darin, dass die Beziehung kleiner oder gleich und nicht kleiner heisst. Daher bilden wird die ω_i's so auf $\tilde{\omega}_i$'s ab, dass für diese gerade $\tilde{\omega}_1 < \tilde{\omega}_2 < \ldots < \tilde{\omega}_k$ gilt, $\tilde{\omega}_i = \omega_i + i - 1$:

$$\begin{array}{cccc} \omega_1 & \omega_2 & \cdots & \omega_k \\ \downarrow & \downarrow & \cdots & \downarrow \\ \tilde{\omega}_1 = \omega_1 + 1 - 1 & \tilde{\omega}_2 = \omega_2 + 2 - 1 & \cdots & \tilde{\omega}_k = \omega_k + k - 1 \end{array}$$

Durch diese Zuordnung wird die Menge

$$\Omega = \{(\omega_1, \ldots, \omega_k) \in \mathbb{A}^k | \omega_1 \leq \omega_2 \leq \ldots \leq \omega_k\}$$

bijektiv auf die Menge

$$\tilde{\Omega} = \{(\tilde{\omega}_1, \ldots, \tilde{\omega}_k) \in \mathbb{B}^k | \tilde{\omega}_1 < \tilde{\omega}_2 < \ldots < \tilde{\omega}_k\}$$

mit $\mathbb{B} = \{1, ..., n+k-1\}$ abgebildet. Damit gilt $|\Omega| = |\tilde{\Omega}|$.
$\tilde{\Omega}$ ist nun der Ergebnisraum zu dem Experiment k Kugeln aus $n+k-1$ ohne Wiederholung und ohne Berücksichtigung der Reihenfolge auszuwählen. Damit gibt es nach Satz 5.2.7

$$\binom{n+k-1}{k}$$

Möglichkeiten.

Im Beispiel beträgt die Anzahl der Kombinationen von drei aus fünf Sorten 35.

5.2.6 Wahrscheinlichkeit beim mehrmaligen Ziehen mit Zurücklegen

Man kann dieses Experiment auch wieder in Form eines Urnenmodells betrachten. Eine Urne enthalte N Kugeln, von denen M schwarz und $N-M$ weiss sind. Betrachten wir den Fall, dass die Kugeln jeweils vor dem nächsten Zug zurückgelegt werden. Wie groß ist nun die Wahrscheinlichkeit bei n Zügen genau k schwarze zu erwischen? Jetzt ist bei jedem Zug die Wahrscheinlichkeit, eine schwarze Kugel zu erwischen, gleich. Damit handelt es sich beim Ziehen von n Kugeln um n Einzelexperimente.
Wir betrachten die Permutation, bei der die ersten k Kugeln schwarz und die letzten (n-k) weiss sind. Hiervon gibt es $M^k \cdot (N-M)^{n-k}$ Möglichkeiten. Nämlich M Möglichkeiten im ersten Zug eine schwarze zu ziehen, mal M Möglichkeiten im

zweiten Zug eine schwarze zu ziehen,..,. mal M Möglichkeiten im k-ten Zug eine schwarze zu ziehen, mal $N-M$ Möglichkeiten im $k+1$-ten Zug eine weisse zu ziehen, ..., mal $N-M$ Möglichkeiten im n-ten Zug eine weisse zu ziehen.
Wir haben bisher aber nur die eine geordnete Permutation betrachtet, die aus k schwarzen und $(n-k)$ weissen Kugeln besteht. Nummerieren wir die Kugeln durch, so gibt es nach Satz 5.2.7 $\binom{n}{k}$ Permutationen, die aus k schwarzen und $(n-k)$ weissen Kugeln bestehen.
Damit beträgt die Anzahl der günstigen Fälle $\binom{n}{k} \cdot M^k \cdot (N-M)^{n-k}$. Die Anzahl aller n-Permutationen beträgt nach Satz 5.2.6 N^n. Damit beträgt die Wahrscheinlichkeit, genau k schwarze Kugeln zu ziehen,

$$p_k = \frac{\binom{n}{k} \cdot M^k \cdot (N-M)^{n-k}}{N^n} = \binom{n}{k} \cdot \left(\frac{M}{N}\right)^k \cdot \left(1-\frac{M}{N}\right)^{n-k}.$$

Hierbei ist nun $\frac{M}{N}$ die Wahrscheinlichkeit, bei einmaligem Ziehen eine schwarze Kugel zu erwischen. Es gilt also der Satz

Satz 5.2.10 Eine Urne enthalte N Kugeln, von denen M schwarz und $N-M$ weiss sind. Aus der Urne werden n ($n \leq N$) Kugeln gezogen und jeweils nach jedem Zug zurückgelegt. Die Wahrscheinlichkeit, dass unter den n gezogenen Kugeln gerade k schwarze sind, beträgt

$$p_k = \binom{n}{k} \cdot \left(\frac{M}{N}\right)^k \cdot \left(1-\frac{M}{N}\right)^{n-k}.$$

In Abschnitt 5.7.1 werden wir sehen, dass es sich um eine Binomialverteilung handelt.

5.2.7 Zusammenfassung

In der Tabelle sind jeweils die Anzahlen der Permuationen bzw. Kombinationen angegeben. Es sei $k \leq n$ und $0! = 1$.

Ziehen von k Kugeln aus n	ohne Zurücklegen	mit Zurücklegen
mit Berücksichtigung der Reihenfolge	$\frac{n!}{(n-k)!}$	n^k
ohne Berücksichtigung der Reihenfolge	$\binom{n}{k}$	$\binom{n+k-1}{k}$

5.3 Bedingte Wahrscheinlichkeit

Häufig stehen Informationen zu einem Zufallsexperiment vorab zur Verfügung. Kennt man z.B beim Skat die eigenen Karten, so hat man dadurch schon Informationen über die des Gegners. Hat man selbst 2 Asse, kann der Gegner keine drei mehr haben. Die Wahrscheinlichkeit für 3 Asse beim Gegner unter der Bedingung, dass man selber zwei hat, ist also null (Asse im Ärmel zählen nicht!). Im folgenden soll die bedingte Wahrscheinlichkeit definiert weren. Für ein Laplace Experiment, bei dem alle Elementarereignisse gleich wahrscheinlich sind, ist dies naheliegend:

Betrachten wir hierzu einen Würfel. Gesucht sei die Wahrscheinlichkeit, eine Drei zu würfeln unter der Bedingung, dass das Ergebnis ungerade ist. Wenn wir schon wissen, dass die Zahl ungerade ist, kommen nur noch drei Zahlen in Frage. Die Wahrscheinlichkeit, eine Drei gewürfelt zu haben, ist also $\frac{1}{3}$. Sei $A = \{3\}$ das Ereignis, eine Drei zu würfeln, und $B = \{1,3,5\}$. Die Anzahl der günstigen Ergebnisse beträgt also $|A \cap B| = 1$. Die Anzahl der möglichen Ergebnisse beträgt $|B| = 3$. Damit beträgt die gesuchte Wahrscheinlichkeit $\frac{|A \cap B|}{|B|}$. Diese Wahrscheinlichkeit heisst nun die bedingte Wahrscheinlichkeit von A unter der Bedingung B und wird mit $P(A|B)$ bezeichnet. Es gilt

$$P(A|B) = \frac{|A \cap B|}{|B|} = \frac{\frac{|A \cap B|}{|\Omega|}}{\frac{|B|}{|\Omega|}} = \frac{P(A \cap B)}{P(B)}$$

Wir definieren nun auch für beliebige Wahrscheinlichkeitsräume (Ω, P) die bedingte Wahrscheinlichkeit $P(A|B)$:

Definition 5.3.1 Bedingte Wahrscheinlichkeit
Ist (Ω, P) ein endlicher Wahrscheinlichkeitsraum und B ein Ereignis mit $P(B) > 0$, so heisst

$$P(A|B) := \frac{P(A \cap B)}{P(B)}$$

die **bedingte Wahrscheinlichkeit** von A unter der Bedingung B.

Aus Definition 5.3.1 ergibt sich sofort

$$P(A|B) = \frac{P(B|A) \cdot P(A)}{P(B)}, \text{ denn } P(B|A) = \frac{P(A \cap B)}{P(A)}$$

Man hat zu zeigen, dass die Definition der bedingten Wahrscheinlichkeit den drei Kolmogoroffschen Axiomen nach Definition 5.1.2 genügt, also dass durch

$$P(.|B) : \mathcal{P}(\Omega) \rightarrow \mathbb{R} \tag{5.1}$$

$$A \mapsto P(A|B) := \frac{P(A \cap B)}{P(B)} \tag{5.2}$$

ein Wahrscheinlichkeit-Maß auf $\mathcal{P}(\Omega)$ definiert ist. Zum Beweis siehe Stochastik Lehrbücher.

Beispiel 5.3.1 Würfeln mit zwei unterscheidbaren Würfeln
Es werde mit zwei unterscheidbaren (schwarz und weiss) Würfeln gleichzeitig gewürfelt. Wie groß ist die Wahrscheinlichkeit , dass die Augensumme größer 9 ist unter der Bedingung, dass die Augenzahl des schwarzen Würfels kleiner als 6 ist?

Das Experiment ist durch folgenden Wahrscheinlichkeitsraum beschrieben:

$$\Omega = \{(i, j) | i, j \in \{1, 2, \ldots, 6\}\}$$

mit $|\Omega| = 36$. Hierbei beschreibe die erste Komponente den schwarzen und die zweite den weissen Würfel.
Es sei A das Ereignis, eine Augensumme größer 9 zu würfeln:

$$A = \{(i, j) \,|\, i + j > 9 \quad i, j \in \{1, 2, \ldots, 6\}\} = \{(4,6), (5,5), (5,6), (6,4), (6,5), (6,6)\}$$

Damit gilt $P(A) = \frac{6}{36} = \frac{1}{6}$.
Es sei B das Ereignis, dass die Augenzahl des schwarzen Würfels kleiner 6 ist. Dies sind alle Tupel, bei denen die erste Zahl nicht 6 ist. Es gilt also $|B| = 30$.

Die für beide Ereignisse günstigen Ausgänge sind durch $A \cap B = \{(4,6), (5,5), (5,6)\}$ mit $|A \cap B| = 3$ gegeben.

Damit beträgt die bedingte Wahrscheinlichkeit

$$P(A|B) = \frac{\frac{3}{36}}{\frac{30}{36}} = \frac{3}{30} = \frac{1}{10}$$

Beispiel 5.3.2 Schultest
Bei einem Schultest hat es folgendes Ergebnis gegeben.

	bestanden (B)	nicht bestanden	
Mädchen (A)	30	20	50
Jungen	40	40	80
	70	60	130

Wählt man nun ein Kind zufällig aus, so ist dies durch den Ergebnisraum Ω, der alle Kinder enthält, beschrieben und es gilt $|\Omega| = 130$.
Die Wahrscheinlichkeit, ein Mädchen zu wählen, beträgt:

$$P(A) = \frac{|A|}{|\Omega|} = \frac{50}{130}$$

Betrachtet man nun nur die Kinder, die bestanden haben, so ist die Wahrscheinlichkeit, ein Mädchen zu wählen:

$$P(A|B) = \frac{|A \cap B|}{|B|} = \frac{30}{70}$$

Betrachtet man nun nur die Kinder, die nicht bestanden haben, so ist die Wahrscheinlichkeit, ein Mädchen zu wählen:

$$P(A|\overline{B}) = \frac{|A \cap \overline{B}|}{|B|} = \frac{20}{60}$$

Die Wahrscheinlichkeit, ein Mädchen zu wählen, ergibt sich auch, wenn man die Wahrscheinlichkeiten der unvereinbaren Ereignisse $A \cap B$ und $A \cap \overline{B}$ addiert:

$$P(A) = P(A \cap B) + P(A \cap \overline{B}) = \frac{30}{130} + \frac{20}{130} = \frac{50}{130}$$

Die kann man auch durch

$$P(A) = P(A|B) \cdot P(B) + P(A|\overline{B}) \cdot P(\overline{B}) = \frac{30}{70} \cdot \frac{70}{130} + \frac{20}{60} \cdot \frac{60}{130}$$

ausdrücken. □

Es gilt:

Satz 5.3.1 Totale Wahrscheinlichkeit zweier Ereignisse
Zerfällt die Ergebnismenge Ω in die zwei Ereignisse B und $\overline{B} = \Omega \setminus B$, und ist $P(B) > 0$ und $P(\overline{B}) > 0$, so gilt für die Wahrscheinlichkeit eines Ereignisses A:

$$P(A) = P(A|B) \cdot P(B) + P(A|\overline{B}) \cdot P(\overline{B})$$

Beweis Übung ■

Eine Veranschaulichung in Form eines Baumdiagramms ist in Abbildung 5.5 gegeben.

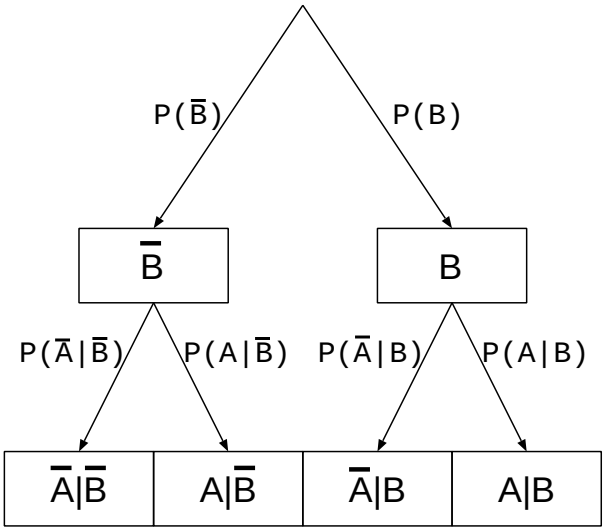


Abbildung 5.4: Baumdiagramm zur Veranschaulichung der totalen Wahrscheinlichkeit.

Beispiel 5.3.3 Hochbegabtentest Ein Test auf Hochbegabtheit ergibt bei 90 % aller Hochbegabten ein positives Testergebnis. Aber es werden auch 5% der Normalbegabten durch diesen Test als hochbegabt eingestuft. Relevantere Tests haben ergeben, dass 1% aller Kinder hochbegabt sind[2].
Wie groß ist die Wahrscheinlichkeit, dass ein Kind hochbegabt ist, falls der Test positiv ist ?

[2]Die Zahlen sind frei erfunden und nicht wissenschaftlich belegt

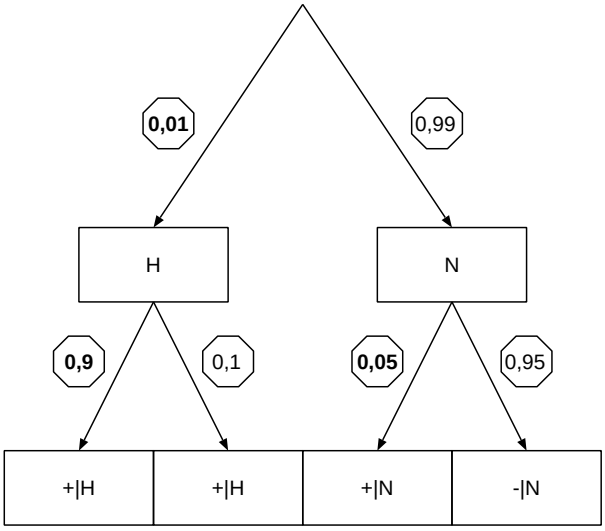


Abbildung 5.5: Baumdiagramm zum Hochbegabtentest. H steht für hochbegabt, N für normalbegabt. Ein positives Testergebis ist mit +, ein negatives mit - gekennzeichnet. Die direkt aus der Aufgabenstellung resultierenden Zahlen sind fett gedruckt.

Es sei H das Ereignis, hochbegabt, und + das Ereignis, positiv getestet zu sein. Es sei $N := \overline{H}$, das Ereignis, normalbegabt, und $- := \overline{+}$ das Ereignis, negativ getestet worden zu sein. Es gilt:
$P(H) = 0,01$ (1%)
$P(+|H) = 0,9$ (90 %)
$P(+|N) = 0,05$ (5%)

$$\begin{aligned} P(+) &= P(+|H) \cdot P(H) + P(+|N) \cdot P(N) \\ &= 0,9 \cdot 0,01 + 0,05 \cdot 0,99 = 0,009 + 0,0495 = 0,0585 \end{aligned}$$

Gesucht ist nun die Wahrscheinlichkeit, hochbegabt zu sein, unter der Bedingung, dass der Test positiv ist:

$$\begin{aligned} P(H|+) &= \frac{P(H \cap +)}{P(+)} = \frac{P(+|H) \cdot P(H)}{P(+)} \\ &= \frac{0,9 \cdot 0,01}{0,0585} \approx 0,1538 \end{aligned}$$

Die gesuchte Wahrscheinlichkeit beträgt ca. 15,38 %. □

Nach Definition 5.3.1 gilt $P(A \cap B) := P(A|B) \cdot P(B)$.
Dies kann man verallgemeinern:

Satz 5.3.2 Sind $A_1, \ldots, A_n$ Ereignisse mit $P(A_1 \cap \ldots \cap A_{n-1}) > 0$, dann ist

$$P(A_1 \cap \ldots \cap A_n) =$$

$$P(A_1) \cdot P(A_2|A_1) \cdot P(A_3|A_1 \cap A_2) \cdot \ldots \cdot P(A_n|A_1 \cap \ldots \cap A_{n-1})$$

Sind die Teilmengen $B_1, B_2, \ldots, B_n$ von Ω paarweise disjunkt und gilt $\bigcup_{i=1}^{n} B_i = \Omega$, so heissen $B_1, B_2, \ldots, B_n$ eine Zerlegung von Ω.

Satz 5.3.3 Satz von Bayes
Sei (Ω, P) ein endlicher Wahrscheinlichkeitsraum. Bilden die Ereignisse $B_1, B_2, \ldots, B_n$ eine Zerlegung von Ω mit $P(B_i) > 0$, für alle $i = 1, 2, \ldots, n$, so gilt für ein Ereignis $A \in \mathcal{P}(\Omega)$

$$P(A) = \sum_{i=1}^{n} P(A|B_i) \cdot P(B_i) \; .$$

5.4 Stochastische Unabhängigkeit

Greifen wir noch einmal das Beispiel „Würfeln mit zwei Würfeln auf“. Es werde wieder mit zwei unterscheidbaren (schwarz und weiss) Würfeln gleichzeitig gewürfelt. Es seien Ω und A wie in obigem Beispiel gegeben. Es ist nun die Wahrscheinlichkeit gesucht, dass die Augensumme größer 9 ist unter der Bedingung, dass der schwarze Würfel eine 4 ist:

$$A = \{(4,6),(5,5),(5,6),(6,4),(6,5),(6,6)\} \qquad P(A) = \frac{1}{6}$$

$$B = \{(4,1),(4,2),(4,3),(4,4),(4,5),(4,6)\} \qquad P(B) = \frac{1}{6}$$

Damit ist $A \cap B = \{(4,6)\}$, also $P(A \cap B) = \frac{1}{36}$ und $P(A|B) = \frac{P(A \cap B)}{P(B)} = \frac{1}{6}$.
Dieses Ergebnis ist interessant, denn es gilt $P(A|B) = P(A)$ und damit
$P(A) \cdot P(B) = P(A \cap B)$. Das Ereignis A tritt unabhängig von B ein.

Definition 5.4.1 Stochastische Unabhängigkeit
Ist (Ω, P) ein endlicher Wahrscheinlichkeitsraum. Die Ereignisse A, B heissen **stochastisch unabhängig** genau dann, wenn gilt:

$$P(A \cap B) = P(A) \cdot P(B)$$

Beispiel 5.4.1 Schultest 2
Bei einem weiteren Schultest hat es folgendes Ergebnis gegeben.

	bestanden (B)	nicht bestanden	
Mädchen (A)	60	20	80
Jungen	30	10	40
	90	30	120

Die Wahrscheinlichkeit, ein Mädchen auszuwählen beträgt

$$P(A) = \frac{80}{120} = \frac{2}{3}$$

Die Wahrscheinlichkeit, ein Kind auszuwählen , dass bestanden hat, beträgt

$$P(B) = \frac{90}{120} = \frac{3}{4}$$

Betrachet man hier die Wahrscheinlichkeit, ein Mädchen, dass bestanden hat, auszuwählen, so gilt:

$$P(A \cap B) = \frac{60}{120} = \frac{1}{2}$$

Somit gilt

$$P(A \cap B) = P(A) \cdot P(B)$$

Die Ereignisse, ein Mädchen auszuwählen und ein Kind, das bestanden hat auszuwählen, sind stochastisch unabhängig. □

Man kann die Definition auf endlich viele Ereignisse übertragen:

Definition 5.4.2 Stochastische Unabhängigkeit von n Ereignissen
Ist (Ω, P) ein endlicher Wahrscheinlichkeitsraum. Eine endliche Familie von Er-

eignissen $\{A_i | i \in I\}$ heisst **stochastisch unabhängig**, wenn für jede endliche Teilfamilie $J \subset I$ gilt:

$$P(\bigcap_{i \in J} A_i) = \prod_{i \in J} P(A_i)$$

Anmerkungen:

1. Aus $P(A_1 \cap A_2 \cap \ldots \cap A_n) = P(A_1) \cdot P(A_2) \cdot \ldots \cdot P(A_n)$ folgt nicht zwingend die stochastische Unabhängigkeit der Ereignisse $A_1, A_2, \ldots, A_n$ (siehe Übung)

2. Sind n Ereignisse stochastisch unabhängig, so gilt dies auch für jedes Ereignispaar.

3. Stochastische Unabhängigkeit ist etwas anderes als Unvereinbarkeit. Ersteres ist über die Wahrscheinlichkeiten definiert, letzteres bedeutet $A \cap B = \emptyset$.

4. Stochastische Unabhängigkeit bedeutet, dass eine Bedingung B keinen stochastischen Einfluss auf ein Ereignis A hat. Dies bedeutet aber nicht, dass in der Realität kein Einfluss besteht. Man wird beim wiederholten Ausführen eines Experiments (z.B. 3 mal eine Münze werden) davon ausgehen, dass die Einzelexeprimente unabhängig voneinander sind. In der Realität handelt es sich aber erstmal nur um getrennte Experimente, von denen man annimmt, dass die zugehörigen Ereignisse auch stochastisch unabhängig sind. Dies ist aber eine Modellannahme.

5.5 Beispiele

Beispiel 5.5.1 Diabetes
In einer Population seien 60 % Frauen. Der Anteil der Frauen, die an Diabetes leiden betrage 1%, der Anteil der Männer, die an Diabetes leiden, betrage 5%.

1. Wie groß ist die Wahrscheinlichkeit , dass eine zufällig ausgewählte Person an Diabetes leidet

2. Sind die Ereignisse „Die Person ist weiblich“ und „ die Person leidet an Diabetes“ stochastisch unabhängig

3. Ein zufällig ausgewählte Person hat Diabetes. Wie groß ist die Wahrscheinlichkeit , dass die Person weiblich ist.

Lösung:
Es gibt folgende Ereignisse
F : „die ausgewählte Person ist eine Frau“, mit $P(F) = 0.6$
M : „die ausgewählte Person ist ein Mann“, mit $P(M) = 0.4$
D: „die ausgewählte Person hat Diabetes“
G: „die ausgewählte Person ist gesund“

Gegeben sind weiterhin $P(D|F) = 0.01$ und $P(D|M) = 0.05$.
Das Baumdiagramm in Abbildung 5.6 veranschaulicht die Situation.

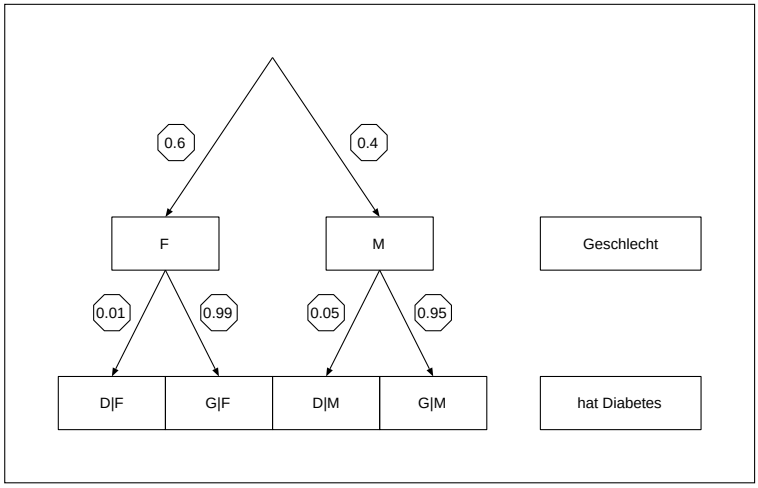


Abbildung 5.6: Baumdiagramm zur Veranschaulichung der bedingten Wahrscheinlichkeiten

1. Gesucht ist $P(D)$: Da die Ereignisse F und M unvereinbar sind gilt

$$\begin{aligned} P(D) &= P(D \cap F) + P(D \cap M) = P(D|F) \cdot P(F) + P(D|M) \cdot P(M) \\ &= 0,01 \cdot 0,6 + 0,05 \cdot 0,4 = 0,026 \end{aligned}$$ □

Die Wahrscheinlichkeit , dass eine zufällig ausgewählte Person an Diabetes leidet, beträgt 2,6 %.

2. Die Ereignisse F und D sind stochastisch unabhängig, wenn $P(D|F) = P(D)$ gilt. $P(D|F) = 0.01$, $P(D) = 0.026$, damit sind die Ereignisse nicht stochastisch unabhängig.
3. Gesucht ist die Wahrscheinlichkeit $P(F|D)$.

$$P(F|D) = \frac{P(D|F) \cdot P(F)}{P(D)} = \frac{0,01 \cdot 0,6}{0,026} = 0,231$$

Die Wahrscheinlichkeit , dass eine zufällig ausgewählte Person, die an Diabetes leidet, weiblich ist beträgt 23,1 %.

Beispiel 5.5.2 Kinder, Kinder
Die Geschlechterverteilung von Kindern soll gleichverteilt sein. Eine Mutter mit zwei Kindern sagt:
1. Mein erstes Kind ist ein Junge
2. Ich habe mindestens einen Jungen
Wie gross ist jeweils die Wahrscheinlichkeit, dass die Mutter auch ein Mädchen hat?
Lösung:
Es handelt sich um ein Laplace Experiment mit $\Omega = \{(ww),(mm),(mw),(mm)\}$.
Das Ereignis mindestens ein Mädchen zu haben: $M = \{(ww),(wm),(mw)\}$.
Das Ereignis als erstes Kind eine Jungen zu haben: $J_1 = \{(mw),(mm)\}$.
Das Ereignis mindestens einen Jungen zu haben ist durch $J = \{(wm),(mw),(mm)\}$.
Damit beträgt

$$P(M|J_1) = \frac{|M \cap J_1|}{|J_1|} = \frac{1}{2} \qquad \text{und} \qquad P(M|J) = \frac{|M \cap J|}{|J|} = \frac{2}{3}$$

Beispiel 5.5.3 ZONK - Das Ziegenproblem
In einer Fernsehshow gibt es drei Tore. Hinter zweien steht eine Ziege bzw. der ZONK, hinter einem der Hauptgewinn, ein Auto. Der Kandidat darf ein Tor auswählen. Danach öffnet der Moderator eines der beiden anderen Tore mit einer Ziege dahinter (zufällig, falls beide Tore eine Ziege verbergen). Danach darf der Kandidat seine Entscheidung noch einmal ändern. Ist es sinvoll, die ursprüngliche Entscheidung zu verwerfen und zu wechseln?
Lösung:
Berachtung als dreistufiges Experiment:
a: Das Auto wird zufällig hinter ein Tor gestellt
k: Der Kandidat wählt ein Tor
m: Der Moderator öffnet ein Tor

$\Omega = \{(a,k,m) |\ a,k,m \in \{1,2,3\}\}$

Ereignis „Auto steht hinter Tor i “: $A_i = \{(a,k,m) | \, a = i\}$
Ereignis „Kandidat wählt Tor i “: $K_i = \{(a,k,m) | \, k = i\}$
Ereignis „Moderator öffnet Tor i “: $M_i = \{(a,k,m) | \, m = i\}$

Verglichen werden müssen nun die Wahrscheinlichkeit dafür, bei Wechsel des Tores zu gewinnen bzw. die ursprüngliche Entscheidung beizubehalten.

Bleibt man bei der ursprüngliche Wahl, so hat die Entscheidung des Moderators keinen Einfluss. Die Wahrscheinlichkeit zu gewinnen beträgt $\frac{1}{3}$.

Das Auto steht mit einer Wahrscheinlichkeit von $\frac{2}{3}$ hinter einem der beiden anderern Tore. Der Moderator öffnet das Ziegentor 2, wir wählen daraufhin 3. Die Wahrscheinlichkeit beträgt also dann $\frac{2}{3}$.

Und nun formal:

Das Baumdiagramm in Abbildung 5.7 veranschaulicht die Situation.

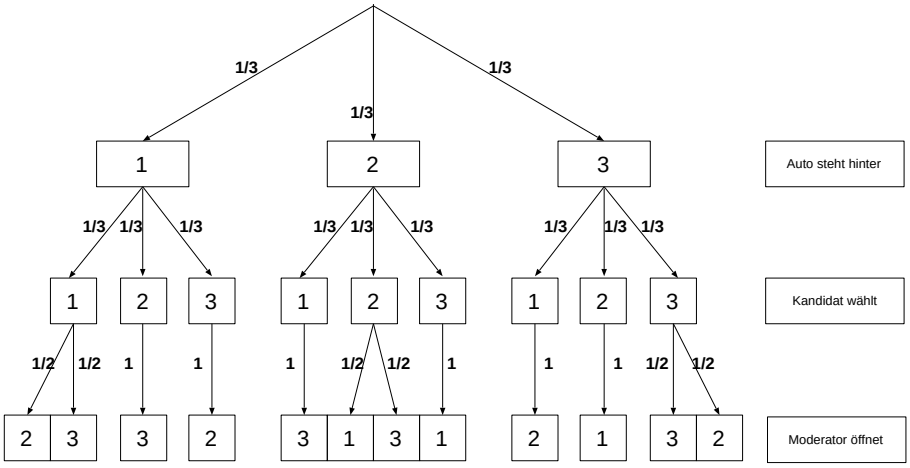


Abbildung 5.7: Baumdiagramm zum Ziegenproblem

Mit $p(a,k,m) := P(\{(a,k,m)\})$ gilt z.B.

$$p(2,1,3) = \frac{1}{3} \cdot \frac{1}{3} \cdot 1 \qquad p(1,1,3) = \frac{1}{3} \cdot \frac{1}{3} \cdot \frac{1}{2}$$

Die Wahrscheinlichkeit, bei Wechsel zu gewinnen ist z.B.

$$P(A_2 | K_1 \cap M_3) = \frac{P(A_2 \cap K_1 \cap M_3)}{P(K_1 \cap M_3)} = \frac{p(2,1,3)}{p(2,1,3) + p(1,1,3)} = \frac{1/9}{1/9 + 1/18} = \frac{2}{3}$$

Man erhält die Wahrscheinlichkeit, bei Wechsel zu gewinnen, in dem man die Wahr-

scheinlichkeiten aller Ereignisse addiert, bei denen alle 3 Zahlen verschieden sind:

$$p(1,2,3)+p(1,3,2)+p(2,1,3)+p(2,3,1)+p(3,1,2)+p(3,2,1)=6\cdot\frac{1}{3}\cdot\frac{1}{3}\cdot 1=\frac{2}{3}$$

Die Wahrscheinlichkeit, bei ursprünglicher Entscheidung zu gewinnen, ist z.B.

$$P(A_1|K_1\cap M_3)=\frac{P(A_1\cap K_1\cap M_3)}{P(K_1\cap M_3)}=\frac{p(1,1,3)}{p(2,1,3)+p(1,1,3)}=\frac{1/18}{1/9+1/18}=\frac{1}{3}$$

Man erhält die Wahrscheinlichkeit, bei ursprünglicher Entscheidung zu gewinnen, in dem man die Wahrscheinlichkeiten aller Ereignisse addiert, deren ersten beiden Zahlen gleich sind und die dritte davon verschieden:

$$p(1,1,2)+p(1,1,3)+p(2,2,1)+p(2,2,3)+p(3,3,1)+p(3,3,2)==6\cdot\frac{1}{3}\cdot\frac{1}{3}\cdot\frac{1}{2}=\frac{1}{3}$$

5.6 Bernoulli-Experimente

Bisher haben wir nur Experimente betrachtet, bei denen alle Elementarereignisse die gleiche Wahrscheinlichkeit besitzen. Im folgenden sollen Zufallsexperimente betrachtet werden, deren Ergebnismenge aus zwei Elementen besteht, wobei die Wahrscheinlichkeiten der Ergebnisse nicht zwingend gleich sein müssen. Bei der Qualitätskontrolle ist z.B. die Wahrscheinlichkeit, dass ein Werkstück fehlerhaft ist, deutlich kleiner als die Wahrscheinlichkeit, dass es fehlerfrei ist (hoffentlich, sonst hat das Unternehmen ein Problem!!).

Definition 5.6.1 Bernoulli Experiment
Ein Zufallsexperiment, dessen Ergebnisraum aus genau zwei Elementen besteht, heisst **Bernoulli Experiment**.

Die beiden Ergebnisse werden häufig mit Treffer oder Niete bezeichnet und durch „1“ und „0“ dargestellt.
Die Wahrscheinlichkeit für einen Treffer sei $p := P(\{1\}) = P(1)$. Dann ist die Wahrscheinlichkeit für eine Niete $q := 1 - p$.

Beispiel 5.6.1 Würfeln einer 6
Beim Experiment „Würfeln einer 6“ ist $p = \frac{1}{6}$ und $q = \frac{5}{6}$. □

Nun interessiert im allgemeinen nicht der Ausgang eines einzigen Bernoulli Experiments, sondern die Hintereinanderschaltung vieler gleichartiger Experimente.

Definition 5.6.2 Bernoulli-Kette
Ein Zufallsexperiment, bei dem ein Bernoulli-Experiment n-mal hintereinander ausgeführt wird, heisst **Bernoulli Kette der Länge** n.

Ist $\tilde{\Omega}$ der Ergebnisraum des Bernoulli-Experiments, so ist

$$\Omega = \tilde{\Omega}^n = \underbrace{\tilde{\Omega} \times \ldots \times \tilde{\Omega}}_{n-mal}$$

der Ergebnisraum der Bernoulli-Kette.

Beispiel 5.6.2 Wiederholt eine Münze werfen
Wird eine Münze n-mal hintereinander geworfen, so stellen sich folgende Fragen?

1. Wie groß ist die Wahrscheinlichkeit, dass beim k-ten Wurf erstmals Zahl eintritt?

2. Wie groß ist die Wahrscheinlichkeit, dass mindestens einmal Zahl eintritt?

3. Wie groß ist die Wahrscheinlichkeit, k-mal Zahl zu werfen? □

Die Wahrscheinlichkeit, Zahl zu werfen, sei p (bei einer verbogenen Münze muss nicht zwingend $p = 1/2$ gelten).
Der Ergebnisraum ist durch

$$\Omega = \{(\omega_1, \ldots, \omega_n) | \, \omega_i \in \{Z, K\} \; i = 1, \ldots n\}$$

gegeben. Ein Elementarereignis besteht also aus einem n-Tupel.

1. Beim k-ten Wurf erstmals Zahl

Hierzu müssen die ersten $k-1$ Versuche Kopf zeigen und der k-te Versuch muss Zahl zeigen:

$$P(\underbrace{K, K, ..., K}_{k-1-mal}, Z) = (1-p)^{k-1} \cdot p$$

2. Mindestens einmal Zahl

Mindestens einmal Zahl zu werfen ist gleichbedeutend mit nicht nur Kopf werden. Die Wahrscheinlichkeit nur Kopf zu werden beträgt

$$P(\underbrace{K, K, ..., K}_{n-mal}) = (1-p)^n$$

Damit beträgt die Wahrscheinlichkeit P, mindestens einmal Zahl zu werfen

$$P = 1 - (1-p)^n$$

3. k-mal Zahl

Die Wahrscheinlichkeit, dass an den ersten k-Stellen Zahl und an den weiteren Stellen Kopf eintritt ist $p^k \cdot (1-p)^{n-k}$. Dies ist aber nur eine Permutation bei der k-mal Zahl eintritt. Insgesamt gibt es $\binom{n}{k}$ Permutationen. Es handelt sich um eine k-Kombination ohne Wiederholung. Aus n-Elementen kann man ohne Berücksichtigung der Reihenfolge auf $\binom{n}{k}$ Arten k Elemente auswählen.

Man erhält die Wahrscheinlichkeit für k Treffer bei einer Kettenlänge n:

$$P_{k,n} = \binom{n}{k} \cdot p^k \cdot (1-p)^{n-k}$$

Beispiel 5.6.3 Irrfahrt
Ein Teilchen bewege sich auf den Punkten $0, \pm 1, \pm 2, \ldots$ auf der x-Achse. In jedem Schritt springt es mit der Wahrscheinlichkeit p nach rechts und mit der Wahrscheinlichkeit q=1-p nach links. Das Teilchen starte im Punkt 0. Wie gross ist die Wahrscheinlichkeit, dass es nach 11 Schritten im Punkt (a) +3, (b) -4 ist?
Um in 11 Schritten im Punkt 3 zu landen muss es 7 Schritte nach rechts und 4 Schritte nach links machen. Um 4 Schritte nach links zu machen, gibt es $\binom{11}{4}$ Möglichkeiten. Die Wahrscheinlichkeit beträgt somit

$$P = \binom{11}{4} p^7 q^4$$

Nach 11 Schritten auf Position -4 zu gelangen ist unmöglich, die Wahrscheinlichkeit beträgt also 0. Dies kann man sich wie folgt klar machen: Ist L die Anzahl der Schritte nach links und R die Anzahl der Schritte nach rechts, so muss $R+L = 11$ und $R-L = -4$ gelten. Dies hat aber keine ganzzahlige Lösung. □

5.7 Zufallsvariable, Verteilung und Verteilungsfunktion

Wir haben bisher die Elemente der Ergebnismenge betrachtet und ihre Wahrscheinlichkeit bestimmt. Im Falle eines Würfels haben wir die Augenzahl dabei jeweils mit der natürlichen Zahl identifiziert, die der Augensumme entspricht. Beim Werfen einer Münze haben wird K oder Z geschrieben und die ggf. mit 0 und 1 identifiziert. Im folgenden soll dies nun formalisiert werden:

Definition 5.7.1 Zufallsvariable
Sei (Ω, P) ein Wahrscheinlichkeitsraum mit abzählbarer Ergebnismenge Ω. Eine Funktion

$$\begin{array}{rcl} X : \Omega & \longrightarrow & \mathbb{R} \\ \omega & \mapsto & X(\omega) \end{array} \tag{5.3}$$

heisst **Zufallsvariable auf** Ω. Eine Zufallsvariable wird auch zufällige Variable oder Zufallsgröße genannt.

Der Name rührt daher, dass das Ergebnis ω des Zufallsexperiments zufällig ist. Damit ist auch $X(\omega)$ zufällig. X selbst ist eine eindeutige Zuordnung, denn steht ω erst einmal fest, ist auch $X(\omega)$ bestimmt.

Definition 5.7.2 Diskrete Zufallsvariable
Eine Zufallsvariable X mit abzählbarer Wertemenge $X(\Omega)$ heisst diskret.

Im Beispiel des Münzwurfs ist $\Omega = \{Z,K\}$. Durch $X(\{Z\}) = 1$ und $X(\{Z\}) = 0$ wird eine diskrete Zufallsvariable definiert.

Eine Zufallsvariable X mit überabzählbarer Wertemenge $X(\Omega)$ heisst stetig. Ein Beispiel für eine stetige Zufallsvariable ist z.B. die Lebensdauer einer Glühbirne.

Definition 5.7.3 Wahrscheinlichkeitsverteilung
Sei (Ω,P) ein Wahrscheinlichkeitsraum mit endlicher oder abzählbarer Ergebnismenge Ω und $X :\rightarrow \mathbb{R}$ eine diskrete Zufallsvariable auf Ω, dann heisst das durch

$$P_X(\{k\}) := P(\{\omega \in \Omega | X(\omega) = k\}), \qquad k \in \mathbb{R}$$

definierte Wahrscheinlichkeitmaß P_X die **Wahrscheinlichkeitsverteilung** (oder kurz: Verteilung) der Zufallsvariablen X.

Für $P_X(\{k\})$ schreibt man auch kurz $P(X = k)$.
Die Verteilung eines Würfels ist in Abbildung 5.8 dargestellt.
Häufig interessiert die Wahrscheinlichkeit, dass eine Zufallsvariable Werte annimmt, die kleiner als ein vorgegebener Wert x sind. Dies Wahrscheinlichkeit ist durch $P(X \leq x)$ gegeben. Für beliebige x ist somit eine Funktion definiert:

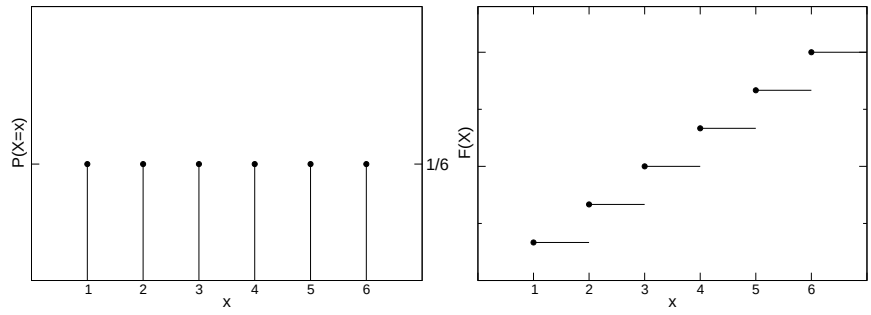


Abbildung 5.8: Verteilung (links) und Verteilungsfunktion (rechts) des Laplace Würfels

Definition 5.7.4 Verteilungsfunktion
Sei X eine diskrete Zufallsvariable, dann heisst die Funktion

$$\begin{aligned} F : \mathbb{R} &\longrightarrow [0,1] \\ x &\mapsto F(x) := P(X \leq x) := \sum_{x_i \leq x} P(X = x_i) \end{aligned} \tag{5.4}$$

Verteilungsfunktion der Zufallsvariablen X.

Die Verteilungsfunktion F ist monoton steigend.
Es gilt $P(a < x \leq b) = F(b) - F(a)$.
Die Verteilungsfunktion eines Würfels ist in Abbildung 5.8 dargestellt.

5.7.1 Binomialverteilung

Betrachten wir noch einmal das n-malige Werfen einer Münze. In Abschnitt 5.2.6 hatten wir die Wahrscheinlichkeit bestimmt, genau k-mal Zahl zu werfen. Beschreiben wir das Experiment durch die Zufallsvariable X, die die Werte $0, 1, \ldots, n$ annehmen kann (Anzahl der Zahlwürfe), dann ist

$$P(X = k) = \binom{n}{k} \cdot p^k \cdot (1-p)^{n-k}.$$

Definition 5.7.5 Binomialverteilung
Sei X eine diskrete Zufallsvariable, die die Werte $0, 1, \ldots, n$ annehmen kann. X heisst **binominalverteilt** mit den Parametern $n \in \mathbb{N}$ und p, $0 < p < 1$, genau dann,

wenn gilt

$$P(X=k) = \binom{n}{k} \cdot p^k \cdot (1-p)^{n-k} =: B_{n;p}(k)\,.$$

Der Name der Binomialverteilung folgt aus der Analogie zum Binomischen Satz:

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} \cdot a^k \cdot b^{n-k}\,.$$

Die Binomialkoeffizienten erhält man aus dem Pascalschen Dreieck

$$\begin{array}{lccccccccccccccccc}
n=0 & & & & & 1 & & & & & & & & \binom{0}{0} & & & & \\
n=1 & & & & 1 & & 1 & & & & & & \binom{1}{0} & & \binom{1}{1} & & & \\
n=2 & & & 1 & & 2 & & 1 & & & & \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} & & \\
n=3 & & 1 & & 3 & & 3 & & 1 & & \binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3} & \\
n=4 & 1 & & 4 & & 6 & & 4 & & 1 & \binom{4}{0} & & \binom{4}{1} & & \binom{4}{2} & & \binom{4}{3} & & \binom{4}{4} \\
\vdots & & & & & & & & & & & & & & & & & &
\end{array}$$

Die Verteilung ist in Abbildung 5.10 für $n = 20$ und $p = 0,05$ bzw. $p = 0,5$ gegeben. Ist die Wahrscheinlichkeit $p = 0,5$, liegt also ein Laplace Experiment zugrunde, so ist die Verteilung symmetrisch.

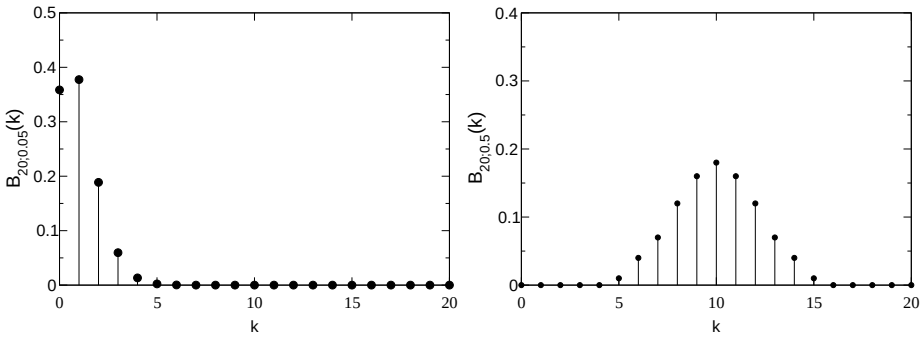


Abbildung 5.9: Binomialverteilung für $n = 20$ und $p = 0,05$ (links) bzw. $p = 0,5$ (rechts).

Beispiel 5.7.1 Blumenzwiebeln
Man erhält Blumenzwiebeln in Packungsgröße von 20 Stück. Der Händler gibt eine 90%ige Garantie, dass die Zwiebeln keimen. Man weiss aus Erfahrung, dass 5 % der Zwiebeln nicht keimen. Wie groß ist die Wahrscheinlichkeit, dass eine zufällig ausgewählte Packung die Garantie nicht erfüllt.

Lösung:
Man nimmt an, dass das Keimen der Zwiebeln voneinander unabhängig ist, so ist die Wahrscheinlichkeit, dass genau k Zwiebeln nicht keimen

$$B_{20;0,05}(k) = P(X = k) = \binom{20}{k} \cdot 0,05^k \cdot 0,95^{20-k}.$$

Die Garantie ist nicht erfüllt, wenn mehr als 2 Zwiebeln nicht keimen.

$$P(X > 2) = 1 - P(X \leq 2) = 1 - (P(X = 0) + P(X = 1) + P(X = 2)) \approx 0,08$$

Damit ist mit einer Wahrscheinlichkeit von 8% die Keimgarantie nicht erfüllt. □

5.7.2 Hypergeometrische Verteilung

Im Beispiel 5.7.1 haben wird angenommen, dass es sich bei den einzelnen Blumenzwiebeln um voneinander unabhängige Experimente handelt. Betrachet wir nun noch einmal das Beispiel 5.2.10. Man hat eine Lieferung von 10 Festplatten und möchte wissen, ob die Lieferung in Ordnung ist, so testet wählt man eine gewisse Anzahl aus und testet sie. In diesem Fall verändert sich die Wahrscheinlichkeit, eine defekte Platte zu erwischen, jeweils mit der Anzahl der bisher ausgewählten Platten. Es handelt sich um ein Experiment ohne Wiederholung wie in Abschnitt 5.2.4.

Definition 5.7.6 Hypergeometrische Verteilung
Eine Zufallsvariable X heisst **hypergeometrisch verteilt** mit den Parametern $N, M, n \in \mathbb{N}$, $1 \leq n \leq N$ und $0 \leq K \leq N$, genau dann, wenn gilt

$$H_{N;M;n}(k) = P(X = k) = \frac{\binom{M}{k} \cdot \binom{N-M}{n-k}}{\binom{N}{n}} \qquad \text{für} \quad 0 \leq k \leq \min(M, n)\,.$$

In Abbildung sind zwei Beispiel für hypergeometrische Verteilungen gegeben.

Für sehr große Werte von N bezogen auf n kann die hypergeometrische Verteilung durch eine Binomialverteilung approximiert werden (Abbildung 5.11).Die Wahrscheinlichkeit p für die Binomialverteilung ergibt sich aus dem Quotienten von N und M aus der hypergeometrischen Verteilung: $p = \frac{M}{N}$.

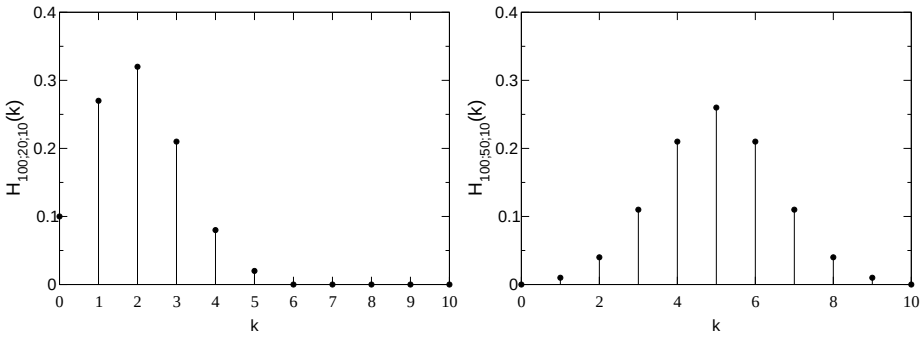


Abbildung 5.10: Hypergeometrische Verteilung für $N = 100$, $M = 20$ und $n = 10$ (links) bzw. $N = 100$, $M = 50$ und $n = 10$ (rechts).

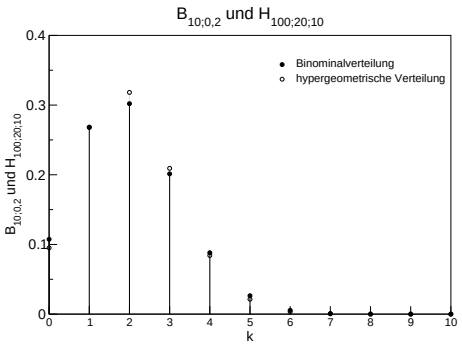


Abbildung 5.11: Vergleich der Binomialverteilung $B_{10;0,2}$ (schwarz) mit der hypergeometrischen Verteilung $H_{100;20;10}$ (weiss).

5.8 Erwartungswert und Varianz diskreter Zufallsvariablen

5.8.1 Erwartungswert

Betrachten wir noch einmal das Beispiel mit einem Würfel zu würfeln. Wir wissen dass die Wahrscheinlichkeit für jede Augezahl $\frac{1}{6}$ beträgt. Bei einem Glücksspiel ist man an der Gewinnerwartung interessiert oder anders ausgedrückt, man möchte wissen, ob das Spiel fair ist.

Beispiel 5.8.1 Gummibärchen
Beim einmaligen Würfeln mit einem Laplace-Würfel beträgt der Einsatz 5 Gummibärchen. Ich gebe also meinem Mitspieler 5 Bärchen. Bei einer geraden Augenzahl erhalte ich soviele Bärchen wie Augen von meinem Mitspieler, bei einer ungeraden doppelt soviel wie Augen. Die Frage ist nun inwieweit das Spiel fair ist, d.h. ob beide Spieler die gleiche Gewinnerwartung haben. Es ergibt sich folgende Situation:

Augenzahl	1	2	3	4	5	6
Bärchenzahl	2	2	6	4	10	6
Wahrscheinlichkeit	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{6}$

Wir betrachten die Zufallsvariable X, die die Anzahl der erhaltenen Bärchen angibt:

x_i	2	4	6	10
$P(X = x_i)$	$\frac{2}{6}$	$\frac{1}{6}$	$\frac{2}{6}$	$\frac{1}{6}$

Die erwartete Bärchenzahl ergibt sich nun, indem wir jeweils die Wahrscheinlichkeit für eine bestimmte Bärchenzahl mit der Bärchenzahl multiplizieren und das ganze aufsummieren:

$$E(X) = 2 \cdot \frac{2}{6} + 4 \cdot \frac{2}{6} + 6 \cdot \frac{2}{6} + 10 \cdot \frac{1}{6} = \frac{30}{6} = 5$$

Das Spiel kann somit als fair angesehen werden, da der Einsatz gerade 5 Bärchen betragen hat. □

Bemerkung: In vielen Büchern sind Beispiele von Glücksspielen um Geld. Dieses ist aber aus pädagogischer Sicht nicht für die Schule geeignet!! Insgesamt sollte darauf verzichet werden Glücksrad-, Roulette- oder Pokerbeispiele in der Schule zu behandeln. Sinnvoll halte ich hingegen die Behandlung von Lotto, da fast jeder damit in Kontakt kommt. Eine Auseinandersetzung mit den Gewinnchancen ist also wünschenswert.

Definition 5.8.1 Erwartungswert (bei endlicher Wertemenge)
Sei X eine diskreten Zufallsvariable, die die Werte $x_1, \ldots, x_n$ annimmt.

$$E(X) := x_1 \cdot P(X = x_1) + \cdots + x_n \cdot P(X = x_n) = \sum_{i=1}^{n} x_i \cdot P(X = x_i)$$

heisst **Erwartungswert** von X. Der Erwartungswert wird auch mit μ bezeichnet.

Es handelt sich beim Erwartungswert um eine gewichtete Summe der Werte. Die Gewichte sind gerade die Wahrscheinlichkeiten.
Sind die möglichen Ergebisse nicht genauer spezifiziert, und ist X eine zufällige Variable auf dem (Ω, P) , dann schreibt man auch:

$$E(X) = \sum_{\omega \in \Omega} X(\omega) \cdot P(\omega)$$

Beispiel 5.8.2 Erwartungswert des Würfels
Beim einmaligem Werfen eines Laplace-Würfels beträgt die erwartete Augenzahl

$$E = 1 \cdot \frac{1}{6} + 2 \cdot \frac{1}{6} + 3 \cdot \frac{1}{6} + 4 \cdot \frac{1}{6} + 5 \cdot \frac{1}{6} + 6 \cdot \frac{1}{6} = 3,5$$

Satz 5.8.1 Sei X eine diskrete Zufallsvariable und $a, b \in \mathbb{R}$, dann gilt

$$E(aX + b) = a \cdot E(X) + b$$

Beweis Nimmt die Zufallsvariable X die Werte $x_1, \ldots, x_n$ an, so gilt

$$\begin{aligned} E(aX+b) &= \sum_{i=1}^{n} (ax_i + b) \cdot P(X = x_i) \\ &= a \cdot \left(\sum_{i=1}^{n} x_i \cdot P(X = x_i) \right) + b \cdot \underbrace{\sum_{i=1}^{n} P(X = x_i)}_{=1} = a \cdot E(X) + b \end{aligned}$$

■

Definiert man für zwei diskrete Zufallsvariabeln X und Y auf derselben Ergebnismenge Ω ihre Summe $X + Y$ durch

$$(X+Y)(\omega) = X(\omega) + Y(\omega), \qquad \omega \in \Omega\,,$$

so gilt:

Satz 5.8.2 Seien X, Y zwei diskrete Zufallsvariablen auf derselben Ergebnismenge Ω so gilt

$$E(X+Y) = E(X) + E(Y)$$

Beweis Übung ■

Beispiel 5.8.3 Münzwurf
Betrachtet wird eine Bernoulli-Kette der Länge 2:

$\Omega = \{Adler, Zahl\}$
1. Münzwurf: $X(Adler) = 1$, $X(Zahl) = 0$
2. Münzwurf: $Y(Adler) = 1$, $Y(Zahl) = 0$

Es gelte $P(X = 1) = P(Y = 1) = p$:
$E(X) = 1 \cdot P(X = 1) + 0 \cdot P(X = 0) = 1 \cdot p + 0 \cdot (1 - p) = p$, $E(Y)$ analog
Es gilt also $E(X) + E(Y) = p + p = 2p$

$X + Y$ nimmt die Werte 0,1,2 an, wobei gilt:
$P(X + Y = 0) = \binom{2}{0} \cdot p^0 \cdot (1 - p)^2 = (1 - p)^2$
$P(X + Y = 1) = \binom{2}{1} \cdot p^1 \cdot (1 - p)^1 = 2 \cdot p \cdot (1 - p)$
$P(X + Y = 2) = \binom{2}{2} \cdot p^2 \cdot (1 - p)^0 = p^2$

$E(X + Y) = 0 \cdot (1 - p)^2 + 1 \cdot 2 \cdot p \cdot (1 - p) + 2 \cdot p^2 = 2p - 2p^2 + 2 \cdot p^2 = 2p$ □

5.8.2 Varianz

Der Erwartungswert einer Zufallsvariablen gibt Auskunft über die Lage der Verteilung. Eine weiter Kenngröße ist die „Breite“ der Verteilung. Hierzu werden die Abweichungen der einzelnen Werte x_i vom Erwartungswert μ betrachtet. Analog zur Methode der kleinsten Quadrate (2.2.1) werden nun nicht alle Abstände sondern die Abstandsquadrate aufsummiert und dabei mit der jeweiligen Wahrscheinlichkeit gewichtet:

Definition 5.8.2 Varianz (bei endlicher Wertemenge) Sei X eine diskrete Zufallsvariable, die Werte $x_1, \ldots, x_n$ annimmt.

$$V(X) := E((X - E(X))^2) = \sum_{i=1}^{n} (x_i - E(X))^2 \cdot P(X = x_i)$$

heisst **Varianz** von X. Die Varianz wird auch mit σ^2 bezeichnet.
Die positive Quadratwurzel $\sigma = \sqrt{\sigma^2}$ heisst **Standardabweichung** oder **Streuung** von X.

anders ausgedrückt:

$$V(X) := E((X - E(X))^2) = \sum_{\omega \in \Omega} (X(\omega) - E(X))^2 \cdot P(\omega)$$

Beispiel 5.8.4 Varianz des Würfels
Beim einmaligen Werfen eines Laplace-Würfels beträgt die Varianz

$$\begin{aligned} V &= (1-3,5)^2 \cdot \frac{1}{6} + (2-3,5)^2 \cdot \frac{1}{6} + (3-3,5)^2 \cdot \frac{1}{6} \\ &+ (4-3,5)^2 \cdot \frac{1}{6} + (5-3,5)^2 \cdot \frac{1}{6} + (6-3,5)^2 \cdot \frac{1}{6} \\ &= \frac{17,5}{6} \approx 2,92 \end{aligned}$$

□

Satz 5.8.3 Sei X eine diskrete Zufallsvariable, die Werte $x_1, \ldots, x_n$ annimmt, und μ deren Erwartungswert, dann gilt

$$V(X) = E(X^2) - \mu^2$$

Beweis

$$\begin{aligned} V(X) &= E((x-\mu)^2) = \sum_{i=1}^{n} (x_i - \mu)^2 \cdot P(X = x_i) \\ &= \sum_{i=1}^{n} (x_i^2 - 2x_i\mu + \mu^2) \cdot P(X = x_i) \\ &= \sum_{i=1}^{n} x_i^2 \cdot P(X = x_i) - 2\mu \sum_{i=1}^{n} x_i \cdot P(X = x_i) + \mu^2 \sum_{i=1}^{n} P(X = x_i) \\ &= \sum_{i=1}^{n} x_i^2 \cdot P(X = x_i) - 2\mu \cdot \mu + \mu^2 \cdot 1 \\ &= E(X^2) - \mu^2 \end{aligned}$$

■

Beispiel 5.8.5 Varianz des Würfels
Beim einmaligen Werfen eines Laplace-Würfels gilt

$$E(X^2) = \sum_{i=1}^{6} i^2 \cdot P(X = i) = 1 \cdot \frac{1}{6} + 4 \cdot \frac{1}{6} + 9 \cdot \frac{1}{6} + 16 \cdot \frac{1}{6} + 25 \cdot \frac{1}{6} + 36 \cdot \frac{1}{6} = \frac{91}{6} \approx 15,17$$

$$V(X) = 15,17 - 3,5^2 = 2,92$$

Satz 5.8.4 Sei X eine diskrete Zufallsvariable und $a, b \in \mathbb{R}$, dann gilt

$$V(aX + b) = a^2 \cdot V(X)$$

Beweis Übung ■

Satz 5.8.5 Seien X, Y zwei diskrete Zufallsvariablen auf derselben Ergebnismenge Ω und sind X und Y **unabhängige** Zufallsvariablen, dann gilt

$$V(X + Y) = V(X) + V(Y)$$

5.8.3 Erwartungswert und Varianz der Binomialverteilung

Seien X_i, $i = 1, \ldots, n$ Zufallsvariable, die die Werte 0 und 1 annehmen können, und sei $P(X_i = 1) = p$ f.a. $i = 1, \ldots, n$.
Für den Erwartungswert von X_i gilt

$$E(X_i) = 1 \cdot P(X_i = 1) + 0 \cdot P(X_i = 0) = p$$

Für die Varianz gilt nach Satz 5.8.3 mit $1 - p =: q$

$$\begin{aligned} V(X_i) &= E(X_i^2) - (E(X_i))^2 = 1^2 \cdot P(X_i = 1) + 0^2 \cdot P(X_i = 0) - p^2 \\ &= p - p^2 = p \cdot (1 - p) = pq \end{aligned}$$

Die Zufallsvariable $X = \sum_{i=1}^{n} X_i$ ist binominalverteilt und es gilt

$$E(X) = E(\sum_{i=1}^{n} X_i) = \sum_{i=1}^{n} E(X_i)) = np$$

Da die Einzelexperimente der Kette voneinander unabhängig sind, gilt

$$V(X) = \sum_{i=1}^{n} V(X_i) = npq$$

5.9 Tschebyscheffsche Ungleichung

Erwartungswert und Varianz sind Größen, die Informationen über eine Verteilung geben. Die Varianz ist ein Maß für die Streuung einer Verteilung. Man kann also fragen, inwieweit die Werte einer Zufallsvariablen vom Erwartungswert abweichen, und vermuten, dass dies etwas mit der Varianz zu tun hat.
Sei also eine Schranke A vorgegeben. Wir wollen nun wissen, wie groß die Wahrscheinlichkeit ist, dass X Werte ausserhalb des Intervalls $[E(X)-a, E(X)+a]$ annimmt, also $|X-E(X)| \geq a$ gilt.
Hierzu liefert die Tschebyscheffsche Ungleichung eine Abschätzung:

Satz 5.9.1 Tschebyscheffsche Ungleichung
Sei X eine diskrete Zufallsvariable mit Erwartungswert $E(X)$ und Varianz $V(X)$, dann gilt für jedes $a > 0$

$$P(|X-E(X)| \geq a) \leq \frac{V(X)}{a^2}$$

Beweis Sei $A = \{\omega \in \Omega |\ |X(\omega)-E(X)| \geq a\}$, dann gilt

$$\begin{aligned} V(X) &= \sum_{\omega\in\Omega} P(\{\omega\})[X(\omega)-E(X)]^2 \\ &\geq \sum_{\omega\in A} P(\{\omega\})[X(\omega)-E(X)]^2 \\ &\geq \sum_{\omega\in A} P(\{\omega\})\cdot a^2 \\ &= P(A)\cdot a^2 \end{aligned}$$

■

Beispiel 5.9.1 Beim einmaligen Würfeln gilt $E = 3,5$ und $V = \frac{35}{12}$.
Für $a = 2,5$ gilt

$$A = \{\omega \in \Omega |\ |X(\omega)-E(X)| \geq a\} = \{1;6\} \text{ mit } P(A) = \frac{1}{3} \approx 0,33$$

. Nach der Tschebyscheffschen Ungleichung gilt:

$$P(A) \leq \frac{V(x)}{2,5^2} = \frac{35}{12\cdot 6,25} = \frac{7}{15} \approx 0,47$$

Für $a = 1,5$ gilt

$$A = \{\omega \in \Omega | \; |X(\omega) - E(X)| \geq a\} = \{1;2;5;6\} \text{ mit } P(A) = \frac{2}{3} \approx 0,67$$

Nach der Tschebyscheffschen Ungleichung gilt:

$$P(A) \leq \frac{V(x)}{2,5^2} = \frac{35}{12 \cdot 2,25} = \frac{35}{27} \approx 1,3$$

Dies ist sowieso klar.

Man sieht, dass die Abschätzung sehr grob ist. Ein Nutzen der Gleichung liegt bei der Qualitätskontrolle.

Satz 5.9.2 Sei X eine diskrete Zufallsvariable, die die Werte 0 und 1 annehmen kann und $P(X = 1) = p$ gilt. Bei einer Bernoulli-Kette der Länge n gilt für die Zufallsvariable $\overline{X}$, die den Mittelwert von X angibt,

$$P(|\overline{X} - E(X)| \geq a) \leq \frac{V(X)}{n \cdot a^2}$$

Beweis Nach Abschnitt 5.8 und 5.8.3

$$E(\overline{X}) = E(\frac{1}{n}\sum_{i=1}^{n} X) = \frac{1}{n}E(X) = \frac{1}{n}np = p = E(X)\,.$$

Da die Einzelexperimente der Kette voneinander unabhängig sind, gilt

$$V(\overline{X}) = V(\frac{1}{n}\sum_{i=1}^{n} X) = \frac{1}{n^2}\sum_{i=1}^{n} V(X) = \frac{1}{n^2}npq = \frac{pq}{n} = \frac{V(X)}{n}\,.$$

Damit gilt nach Satz 5.9.1 die Behauptung. ■

Beispiel 5.9.2 Ein Hersteller verspricht, dass höchstens 5% seiner Produkte fehlerhaft sind. Es werden aus der Gesamtproduktion Stichproben der Größe 100, 1000, 10000 genommen. Mit höchstens welcher Wahrscheinlichkeit finden die Tester jeweils mindestens 10% defekte Produkte?
Gehen wir davon aus, dass die Stichproben deutlich kleiner sind als die Grundgesamtheit, so kann man eine Binomialverteilung annehmen. Ist nun p die Wahrscheinlichkeit für ein fehlerhaftes Produkt (laut Herstellerangabe $\leq 0,05$), so gilt

nach 5.8.3 $E(X) = p$ und $V(X) = pq$. Die Tschebyscheffschen Ungleichung liefert

$$P(|\overline{X} - E(X)| \geq a) = P(|\overline{X} - p| \geq a) \leq \frac{pq}{n \cdot a^2}$$

Ist der Erwartungswert $p = 5\%$ und wählt man für a ebenfalls 5%, so ist das in der Ungleichung betrachtete Intervall, der Bereich von 0% bis 10%. Man erhält also eine Aussage darüber, mit über die Wahrscheinlichkeit, dass die Stichprobe mehr als 10% Ausschuss enthält (kleiner null geht ja nicht).
Für die verschiedenen Stichprobengrößen erhält man

$n = 100$ $P < 19\%$
$n = 1000$ $P < 1,9\%$
$n = 10000$ $P < 0,19\%$

Die Wahrscheinlichkeit mehr als 10% Ausschuß zu erwischen, wenn die erwartete Ausschusshäufigkeit bei 5% liegt, hängt von der Stichprobengröße ab. Je größer die Stichprobengröße desto kleiner ist die Wahrscheinlichkeit. □

5.10 Stetige Zufallsvariablen

Kann eine Zufallsvariable nicht nur diskrete Werte annehmen, spricht man von einer stetigen Zufallsvariablen. In diesem Fall kann man die Wahrscheinlichkeit dafür, dass ein bestimmter Wert angenommen wird, nicht angeben. Stattdessen kann man Aussagen darüber machen, dass ein Wert innerhalb eines bestimmten Intervalls angenommen wird.
Anstelle einer Verteilung wird nun eine Dichtefunktion betrachtet. Die Fläche unterhalb der Dichtefunktion beträgt 1. Die Fläche unterhalb der Dichtekurve innerhalb eines Intervalls gibt gerade die Wahrscheinlichkeit an, dass ein Wert innerhalb des Intervalls angenommen wird.
Ein berühmtes Beispiel ist die Gaußsche Glockenkurve. Eine Zufallsvariable, deren Dichte die Gaußsche Glockenkurve ist, heisst normalverteilt (Abbildung 5.12).

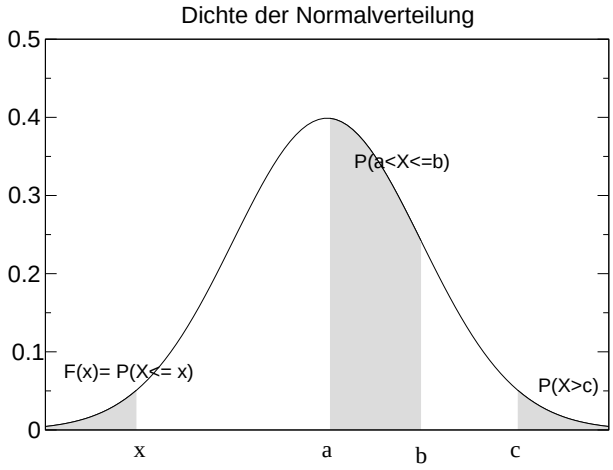


Abbildung 5.12: Dichte der Normalverteilung: Gaußsche Glockenkurve

6 Kryptologie

Die Kryptologie ist die Wissenschaft, Methoden zur Ver- und Entschlüsselung von Daten zu entwickeln. Man unterscheidet zwischen der Krytographie, der Entwicklung von Schlüsselsystemen, und der Kryptoanalyse, der Entschlüsselung. Man bezeichnet die Verschlüsselung auch als Chiffrierung, die Entschlüsselung als Dechiffrierung.

Internet und die Online-Dienste übertragen Nachrichten unverschlüsselt. Will man vermeiden, dass Dritte Dinge mitlesen können, wie z.B. die Kreditkartennummer beim Online-Shopping, oder das Klausurergebnis beim Abrufen der Ergebnisse übers Internet, so braucht man ein Kryptosystem. Auch muss man sich sicher sein, dass eine Nachricht auch tatsächlich von der Person stammt, von der sie vorgibt zu sein, so braucht man eine sichere Signatur.

In den letzten Jahren hat sich hierbei insbesondere das Kryptosystem Pretty Good Privacy, auch als PGP bekannt, durchgesetzt.

Die Kryptologie reicht mehrere tausend Jahre zurück. Schon Julius Cäsar benutzte eine spezielle Methode der monoalphabetischen Chiffrierung. Er verschob die Buchstaben seines Klartexts um 3 Stellen bezüglich des Alphabetes nach links:

Klartext:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Schlüssel:	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Damit wird aus „Hundefutter“ KXQGHIXWWHU .

Im Jahr 1466 hat L.B. Alberti erstmals den polyalphabetischen Schlüssel beschrieben.

Im zweiten Weltkrieg benutzen die Deutschen eine Chiffrieung mittels einer Maschine, bei der sich Walzen mit eingravierten Buchstaben drehten. Durch Veränderung der elektrischen Kontakte konnte man den Code, also die Größe der Verschiebung für jeden einzelnen Buchstaben verschieben. Der Empfänger besaß eine ähnliche Maschine, die sogenannte ENIGMA, in die er den Code eingegeben hat und dann durch Eingabe des verschlüsselten Textes den Klartext erhalten hat. Die Deutschen waren sich ihrer Sache sehr sicher. Insbesondere wurde dieses Verfahren zur Verschlüsselung aller Informationen der U-Boot-Flotte benutzt.

Da die Anzahl der Codes begrenzt war und England über pfiffige Kryptoannalytiker wie Alan Turing verfügte, konnten mit Hilfe der ersten leistungsfähigen Rechner sowie einer von einem deutschen U-Boot erbeuteten ENIGMA (allerdings ohne Code-Tabellen) die feindlichen Botschaften entschlüsselt werden. So hat die Com-

putertechnik und die Mathematik entscheidend zur Entscheidung des Krieges beigetragen.
Heutzutage ist die Kryptologie nicht mehr wegzudenken. Insbesondere bei im Geldverkehr spielt die Verschlüsselung eine entscheidende Rolle.
Letztlich ist der Grund für Verschlüsselungen, bestimmte Informationen vor Fremdzugriff zu schützen. Besteht aber seitens Dritter ein Interesse an diese Informationen zu gelangen, so wird es immer ausgefeiltere Methoden der Kryptonanalytik geben.

6.1 Monoalphabetische Verschlüsselung

Bei der monoalphabetische Verschlüsselung wird jedem Buchstaben des Alphabets genau ein anderer Buchstabe zu geordnet. Man hat also nach Satz 5.2.3 $26! \approx 4 \cdot 10^{26}$ Anordnungen von 26 Buchstaben. Da die Anordnung, die dem Alphabet entspricht entfällt, bleiben $26! - 1$ mögliche Schlüssel. Die einfachste Möglichkeit ist die bereits erwähnte Verschiebechiffrierung. Dieser Code ist einfach zu knacken, man muss nur die 25 Verschiebemöglichkeiten, die das Alphabet zulässt, durchprobieren.
Eine bessere Verschlüsselung bietet die Zuordnung eines beliebigen Buchstabens. Mit der Verschlüsselung

Klartext:	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Schlüssel:	W F U M Q T V Z S Y I P L A K B C X H D O N G R E J

erhält man aus
KATZEN MOEGEN KEIN HUNDEFUTTER
den verschlüsselten Text
IWDJQA LKQVQA IQSA ZOAMQTODDQX

Wie kann man nun eine Botschaft entschlüsseln? Angenommen Sie fangen im Matheunterricht ein Briefchen mit folgendem Text ab:

```
GSX DXQTTQA OAH OL AQOA OZX FQS LSX. MWAA IKQAAQA GSX MSQ
HBSUIJQDDQP TOQX LKXVQA NKXFQXQSDQA. GSX AQZLQA WL
FQHDQA MQA VPQSUZQA UKMQ GSQ ZQODQ MWTOQX. MWAA
LWUZD QH ASUZDH, GQAA MSQ JQDDQP VQTOAMQA GQXMQA.
MSQ QXMIOAMQWXFQSD HKPPDQ HK SL IWHDQA HQSA.
HOBS, VXOHH JWIH
```

Wie können wir diesen Text entschlüsseln?
1. Zählen der Buchstabenhäufigkeiten

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
27	2	0	13	0	4	6	13	5	3	6	7	12	1	11	5	42	0	17	5	5	4	8	15	0	6

Wir vergleichen diese Häufigkeiten mit den üblichen Häufigkeiten eines deutschen Texts, die man aus langen Texten erhält. Diese Tabelle kann natürlich je nach Text variieren:

A	B	C	D	E	F	G	H	I	J	K	L	M
5.91	1.85	2.83	5.36	17.70	1.67	2.81	4.34	7.67	0.18	1.49	3.94	2.66
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
10.68	2.33	0.84	0.02	7.33	6.27	6.16	4.28	0.98	1.49	0.04	0.08	1.08

Angegeben ist jeweils die Häufigkeit in Prozent.

Die Reihenfolge der Häufigsten Buchstaben ist also „ENISRAT...“.
Mit dieser Tabelle kommt man nun weiter. Der häufigste Buchstabe in deutschen Texten ist E. Man kann also vermuten, dass das E durch Q verschlüsselt wird. Genauso kann man auf die Verschlüsselung von N durch A und von I durch S schließen. Wir erhalten somit

```
GSX DXQTTQA OAH OL AQOA OZX FQS LSX. MWAA IKQAAQA GSX MSQ
_I_ __E__EN _N_ __ NE_N ___ _EI _I_. __NN __ENNEN _I_ _IE
HBSUIJQDDQP TOQX LKXVQA NKXFQXQSDQA. GSX AQZLQA WL
__I___E__E_ __E_ ____EN ____E_EI_EN. _I_ _E__EN __
FQHDQA MQA VPQSUZQA UKMQ GSQ ZQODQ MWTOQX. MWAA
_E__EN _EN __EI__EN ___E _IN _E__E ____E_. __NN
LWUZD QH ASUZDH, GQAA MSQ JQDDQP VQTOAMQA GQXMQA.
_____ E_ NI____, _ENN _IE _E__E_ _E__N_EN _E__EN.
MSQ QXMIOAMQWXFQSD HKPPDQ HK SL IWHDQA HQSA.
_IE E____N_E___EI_ _____E __ __ ____EN _EIN.
HOBS, VXOHH JWIH
___I, _____ ____
```

Diese Zuordnung muss natürlich noch nicht richtig sein, da unser Text sehr kurz ist und die Häufigkeiten nicht mit den üblichen übereinstimmen müssen. Ein Hinweis auf die Richtigkeit ist das Auftreten der Kombination EN, die im Deutschen

tatsächlich sehr häufig am Wortende auftritt.

Betrachtet man den Text genauer, sieht man, dass das 5. Wort NEIN oder NEUN heissen könnte. Da das I bereits belegt ist, versuchen wir es also mit der Zuordnung O zu U. Weiterhin tritt die Kombination MWAA mehrfach auf, die könnte also WANN oder DANN heissen. Auf alle Fälle macht die Zuordnung W zu A Sinn.

Als häufiger Buchstabe tritt in deutschen Texten noch das R auf. Da R häufig am Wortende auftritt und in Kombination mit E vorkommt, liegt die Vermutung nahe, dass R durch X codiert wird.

```
GSX DXQTTQA OAH OL AQOA OZX FQS LSX. MWAA IKQAAQA GSX MSQ
_IR _RE__EN UN_ U_ NEUN U_R _EI _IR. _ANN __ENNEN _IR _IE
HBSUIJQDDQP TOQX LKXVQA NKXFQXQSDQA. GSX AQZLQA WL
__I___E__E_ _UER __R_EN __R_E_EI_EN. _IR _E__EN A_
FQHDQA MQA VPQSUZQA UKMQ GSQ ZQODQ MWTOQX. MWAA
_E__EN _EN __EI__EN ___E _IE _EU_E _A_UER. _ANN
LWUZD QH ASUZDH, GQAA MSQ JQDDQP VQTOAMQA GQXMQA.
_A___ E_ NI____, _ENN _IE _E__E_ _E_UN_EN _ER_EN.
MSQ QXMIOAMQWXFQSD HKPPDQ HK SL IWHDQA HQSA.
_IE ER__UN_EAR_EI_ _____E __ __ _A__EN _EIN.
HOBS, VXOHH JWIH
_U_I, __U__ _A__
```

Nun sehen wir schon klarer. Betrachtet man die Kombinationen GSX, MWAA und GQXMQ kann eigentlich nur W durch G und D durch M codiert werden, also

```
GSX DXQTTQA OAH OL AQOA OZX FQS LSX. MWAA IKQAAQA GSX MSQ
WIR _RE__EN UN_ U_ NEUN U_R _EI _IR. DANN __ENNEN WIR DIE
HBSUIJQDDQP TOQX LKXVQA NKXFQXQSDQA. GSX AQZLQA WL
__I___E__E_ _UER __R_EN __R_EREI_EN. WIR _E__EN A_
FQHDQA MQA VPQSUZQA UKMQ GSQ ZQODQ MWTOQX. MWAA
_E__EN DEN __EI__EN __DE WIE _EU_E DA_UER. DANN
LWUZD QH ASUZDH, GQAA MSQ JQDDQP VQTOAMQA GQXMQA.
_A___ E_ NI____, WENN DIE _E__E_ _E_UNDEN WERDEN.
MSQ QXMIOAMQWXFQSD HKPPDQ HK SL IWHDQA HQSA.
DIE ERD_UNDEAR_EI_ _____E __ I_ _A__EN _EIN.
HOBS, VXOHH JWIH
_U_I, _RU__ _A__
```

Das Wort OAH (UN_) könnte UND oder UNS heissen. Da das D schon weg ist, nehmen wir also die Zurdnung von H zu S. Das Wort OL (U_) kann eigentlich nur UM heissen also L wird zu M. Zusammen mit der NEUN dahinter könnte es eine Uhrzeit sein. Wäre dies richtig könnte OZX (U_R) UHR heissen und somit wäre dann H durch Z codiert.
Da es sich um eine Schülerbrief handelt, liegt die Vermutung nahe, dass QXMIO-AMQWXFQSD (ERD_UNDEAR_EI_) ERDKUNDEARBEIT bedeutet. Fragen wir den Erdkundelehrer doch mal, ob eine Arbeit anliegt ;). Damit wird dann I zu K F zu B und D zu T:

```
GSX DXQTTQA OAH OL AQOA OZX FQS LSX. MWAA IKQAAQA GSX MSQ
WIR TRE__EN UNS UM NEUN UHR BEI MIR. DANN K_ENNEN WIR DIE
HBSUIJQDDQP TOQX LKXVQA NKXFQXQSDQA. GSX AQZLQA WL
__I_K_ETTE_ _UER __R_EN __RBEREITEN. WIR NE_MEN AM
FQHDQA MQA VPQSUZQA UKMQ GSQ ZQODQ MWTOQX. MWAA
BESTEN DEN __EI__EN __DE WIE _EUTE DA_UER. DANN
LWUZD QH ASUZDH, GQAA MSQ JQDDQP VQTOAMQA GQXMQA.
MA__T E_ NI__T_, WENN DIE _ETTE_ _E_UNDEN WERDEN.
MSQ QXMIOAMQWXFQSD HKPPDQ HK SL IWHDQA HQSA.
DIE ERDKUNDEARBEIT S___TE S_ IM KASTEN SEIN.
HOBS, VXOHH JWIH
SU_I, _RUSS _AKS
```

Nun, das zweite Wort kann eigentlich nur TREFFEN heissen. Jetzt ist es an der Zeit, die letzten Vokale zu verteilen und nach CK, CH und SCH Ausschau zu halten. Sinnvoll erscheint, dass K durch O codiert wird . Für CH könnte UZ stehen.
Weiss man nun noch, dass der berühmt-berüchtigte Peter auch Zaks gerufen wird, so ist das Ende klar. J codiert Z und V codiert G.

```
GSX DXQTTQA OAH OL AQOA OZX FQS LSX. MWAA IKQAAQA GSX MSQ
WIR TREFFEN UNS UM NEUN UHR BEI MIR. DANN KOENNEN WIR DIE
HBSUIJQDDQP TOQX LKXVQA NKXFQXQSDQA. GSX AQZLQA WL
S_ICKZETTE_ _UER _ORGEN _ORBEREITEN. WIR NE_MEN AM
FQHDQA MQA VPQSUZQA UKMQ GSQ ZQODQ MWTOQX. MWAA
BESTEN DEN __EICHEN CODE WIE HEUTE DAFUER. DANN
LWUZD QH ASUZDH, GQAA MSQ JQDDQP VQTOAMQA GQXMQA.
MACHT ES NICHTS, WENN DIE ZETTE_ _EFUNDEN WERDEN.
```

```
MSQ QXMIOAMQWXFQSD HKPPDQ HK SL IWHDQA HQSA.
DIE ERDKUNDEARBEIT SO__TE SO IM KASTEN SEIN.
HOBS, VXOHH JWIH
SU_I, GRUSS ZAKS
```

Nun das war's wohl mit der Erkundearbeit:

```
WIR TREFFEN UNS UM NEUN UHR BEI MIR. DANN KOENNEN WIR DIE
SPICKZETTEL FUER MORGEN VORBEREITEN. WIR NEHMEN AM
BESTEN DEN GLEICHEN CODE WIE HEUTE DAFUER. DANN
MACHT ES NICHTS, WENN DIE ZETTEL GEFUNDEN WERDEN.
DIE ERDKUNDEARBEIT SOLLTE SO IM KASTEN SEIN.
SUPI, GRUSS ZAKS
```

Die Dechiffrierung ist also eine Mischung aus Statistik, Intuition und Vorinformation. Diese Vorinformation besteht hier darin, dass wir wissen, dass es sich um Schülerbelange handelt und dass wir deren Spitznamen kennen
Wie hätten die Schüler den Code verbessern können?

1. Je kürzer der Text desto schwieriger die Entschlüsselung
2. Vermeidung von Satzzeichen und Leerzeichen oder diese einfach mitverschlüsseln
3. Verschleierung der Häufigkeiten. Zuordnung von mehreren Geheimtextzeichen (z.B. Zahlenpaare) zu einem Buchstaben und zwar so viele wie der Häufigkeit entspricht
4. den Schlüssel variieren (siehe 6.2)

Ein gewisser Herr Bauer hat einmal gesagt:

„Ein ideal für die Chiffrierung vorbereiteter Klartext ist orthographisch falsch, sprachlich knapp und stilistisch grauenhaft.“

Die Entschlüsselung des Textes hängt von der Sprache ab, in der der Text verfasst wurde. Wie sind bisher davon ausgegangen, dass der Text auf deutsch geschrieben wurde, und haben die Häufigkeitstabelle für deutsche Texte verwendet. Für englische Texte sieht diese Verteilung anders aus.

6.2 Polyalphabetische Verschlüsselung

Bei der polyalphabetischen Verschlüsselung wir nicht nur ein Code sondern mehrere verwendet. Man kann zum Beispiel für jeden Buchstaben einen anderen Schlüssel verwenden. Zum Beispiel kann das Wort ABBA mit folgenden Schüsseln zu HINT codiert werden:

Klartext	A	B	C	D	E	...
1. Schlüssel	**H**	L	K	D	F	
2. Schlüssel	G	**I**	R	A	V	...
3. Schlüssel	B	**N**	R	W	Q	...
4. Schlüssel	**T**	V	Z	G	X	...

Der Vorteil besteht darin, dass die Häufigkeiten der einzelnen Schlüssel verschleiert werden. Problematisch hierbei ist, dass der Empfänger alle verwendeten Schlüssel kennen muss. Ein berühmtes Verfahren der polyalphabetischen Verschlüsselung, bei der nur ein einziges Schlüsselwort übermittelt werden muss, ist die Vigenére-Chiffrierung. Hierbei wird das Schlüsselwort, z.B. HAMSTER periodisch über den Klartext geschrieben.

```
HAMSTERH AMSTE RHAMS
SCHNAPPI MACHT SPASS
ZCTFTTGP MMUAX JWAEK
```

Jeder Buchstabe wird dann mit dem Schlüssel codiert, der dem jeweiligen Buchstaben des Schlüsselworts, dem Schlüsselbuchstaben, entspricht. Dies ist die Zeile im Vigenére-Quadrat (Abbildung 6.1), die mit dem Schlüsselbuchstaben beginnt. Im Beispiel wird das S in Schnappi mit der H-Zeile codiert. Das bedeutet, man geht in die Zeile, die mit H beginnt, bestimmt im Klartextalphabet, dass über dem Quadrat steht, die Spalte in der der zu codierende Buchstabe steht und nimmt als Ergebnis den Buchstaben, der im Schnittpunkt von Zeile und Spalte steht.
Die Kryptoanalyse der Vigenére-Chiffrierung ist einfach, sofern das Schlüsselwort relativ kurz und der Text relativ lang ist. Die Idee der Entschlüsselung basiert darauf, dass man den Abstand wiederkehrender Buchstabengruppen bestimmt und daraus auf die Länge des Schlüsselwortes schließt. Hat man die Länge bestimmt, weiss man, welche Buchstaben mit dem gleichen Schlüssel codiert wurden. Betrachtet man die Häufigkeitsverteilung innerhalb aller Spalten, die mit gleichem Schlüssel codiert wurden, so wird der am häufigsten auftretende Buchstabe das E codieren. Damit kennt man die Schlüsselzeile und somit den Schlüsselbuchstaben.

```
a b c d e f g h i j k l m n o p q r s t u v w x y z

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
B C D E F G H I J K L M N O P Q R S T U V W X Y Z A
C D E F G H I J K L M N O P Q R S T U V W X Y Z A B
D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
E F G H I J K L M N O P Q R S T U V W X Y Z A B C D
F G H I J K L M N O P Q R S T U V W X Y Z A B C D E
G H I J K L M N O P Q R S T U V W X Y Z A B C D E F
H I J K L M N O P Q R S T U V W X Y Z A B C D E F G
I J K L M N O P Q R S T U V W X Y Z A B C D E F G H
J K L M N O P Q R S T U V W X Y Z A B C D E F G H I
K L M N O P Q R S T U V W X Y Z A B C D E F G H I J
L M N O P Q R S T U V W X Y Z A B C D E F G H I J K
M N O P Q R S T U V W X Y Z A B C D E F G H I J K L
N O P Q R S T U V W X Y Z A B C D E F G H I J K L M
O P Q R S T U V W X Y Z A B C D E F G H I J K L M N
P Q R S T U V W X Y Z A B C D E F G H I J K L M N O
Q R S T U V W X Y Z A B C D E F G H I J K L M N O P
R S T U V W X Y Z A B C D E F G H I J K L M N O P Q
S T U V W X Y Z A B C D E F G H I J K L M N O P Q R
T U V W X Y Z A B C D E F G H I J K L M N O P Q R S
U V W X Y Z A B C D E F G H I J K L M N O P Q R S T
V W X Y Z A B C D E F G H I J K L M N O P Q R S T U
W X Y Z A B C D E F G H I J K L M N O P Q R S T U V
X Y Z A B C D E F G H I J K L M N O P Q R S T U V W
Y Z A B C D E F G H I J K L M N O P Q R S T U V W X
Z A B C D E F G H I J K L M N O P Q R S T U V W X Y
```

Abbildung 6.1: Das Vigenére-Quadrat zur polyalphabetischen Verschlüsselung.

6.3 Asymmetrische Verschlüsselung

Die Gefahren der mono- und polyalphabetischen Verschlüsselung liegen in der Übermittlung der Schlüssel. Bei der Public Key Verschlüsselung besitzt der Sender ein solches Wort nicht, sondern benutzt einen allen Nutzern zur Verfügung stehendes Codewort des Empfängers, den öffentlichen Schlüssel. Nur der Empfänger besitzt den geheimen Schlüssel, mit dem die Nachricht dann dechiffriert werden kann. Es gibt also einen Schlüssel zur Verschlüsselung, der öffentlich ist, und einen zur Entschlüsselung, der geheim ist. Daher rührt der Name asymmetrische Verschlüsselung. Der Vorteil besteht darin, dass der geheime Schlüssel nicht verschickt werden muss.

Eine bekannte Public-Key-Kodierung geht auf Rivest, Shamir und Adleman zurück und heisst entsprechend der Anfangsbuchstaben RSA-Algorithmus.

6.3.1 Der RSA-Algorithmus

Die Grundlage dieses Algorithmus findet sich in der Zahlentheorie.

Erzeugung der Schlüssel

Zuerst werden der öffentliche und der private Schlüssel erzeugt. Ziel ist es, die Schlüssel so zu gestalten, dass es praktisch unmöglich ist, den private key aus dem public key zu rekonstruieren. Man nutzt hierbei aus, dass die Primfaktorzerlegung sehr großer Zahlen sehr schwierig und zeitaufwändig sit.
Der private Schlüssel besteht aus einer ganzen positiven Zahl d, der öffentliche aus den zwei ganzen positiven Zahlen e und n.

Privater Schlüssel	$d \in \mathbb{Z}^+$
Öffentlicher Schlüssel	$e, n \in \mathbb{Z}^+$

Um diese Zahlen zu bestimmen, werden zwei große Primzahlen p, q gewählt und

$$n = p \cdot q \qquad p, q \text{ Primzahlen}$$

gesetzt. Die Zahl e wird so bestimmt, dass sie mit der Zahl $(p-1)\cdot(q-1)$ keinen gemeinsamen Teiler hat, also

$$ggT(e, (p-1)\cdot(q-1)) = 1\,.$$

Der private Schlüssel ist dann die Zahl d, die folgende Bedingungen erfüllt:

$$d \leq (p-1)\cdot(q-1)$$

$$e \cdot d \bmod (p-1)\cdot(q-1) = 1$$

Letzters bedeutet, dass $e \cdot d$ geteilt durch $(p-1)\cdot(q-1)$ den Rest 1 ergibt (vgl. B.2).

Bestimmung von e (Teil des öffentlichen Schlüssels)
Man probiert so lange, bis man eine Zahl e gefunden hat, für die
$ggT(e, (p-1)\cdot(q-1)) = 1$ gilt. Dies kann ein Computer erledigen.

Die Bestimmung des ggT kann man entweder über eine Primfaktorzerlegung oder über den euklidschen Algorithmus (Anhang B.3) erledigen.

Bestimmung des privaten Schlüssels d

Zu e,$p-1$ und $q-1$ muss d bestimmt werden, so dass

$e \cdot d \bmod (p-1) \cdot (q-1) = 1$

gilt. Dies funktioniert mit dem erweitereten Eulerschen Algorithmus (siehe Anhang B.4).

Anschließend werden die Zahlen p, q vernichtet bzw. gelöscht.

Anwendung der Schlüssel

Der Klartext wird in Form einer Zahl dargestellt, die nicht größer als n ist. Man kann z.B. jedem Buchstaben die Position im Alphabet zuordnen und diese dann einzeln verschlüsseln.

Um die Zahl z zu verschlüsseln, wird mit Hilfe des öffentlichen Schlüssels e, n der Divisionsrest

$$c := z^e \bmod n$$

bestimmt. Diese Zahl c ist nun der Geheimtext, der zum Klartext z gehört.

Der Empfänger dechiffriert c, indem er den privaten Schlüssel d anwendet und $c^d \bmod n$ bestimmt. Es gilt:

$$z = c^d \bmod n$$

Beweis Satz von Euler ■

Warum ist das RSA-Verfahren recht sicher?

Wenn man mit sehr großen Primzahlen p, q beginnt, wird n sehr groß sein. Um den Schlüssel d zu bestimmen, muss man eine Primfaktorzerlegung von n durchführen, um $p-1$ und $q-1$ zu erhalten. Dieses ist für große Zahlen sehr aufwändig.

Beispiel 6.3.1 Dieses Beispiel ist natürlich nicht realistisch, da sehr kleine Primzahlen gewählt werden.

Wir wählen $p = 17$ und $q = 13$. Dann ist $n = 221$.

Wähle $e = 41$, dann erfüllt e

$$ggT(e,(p-1)\cdot(q-1)) = 1\,.$$

Für $d = 89$ gilt

$$d \leq (p-1)\cdot(q-1)$$

und

$$e \cdot d \bmod (p-1)\cdot(q-1) = 1 \qquad \text{siehe Anhang B.4}$$

Soll nun die Zahl 7 verschlüsselt werden, so gilt:

$$c = 7^e \bmod n = 7^{41} \bmod 221$$

Um dies nun endgültig auszurechnen, müssen wir ein wenig tricksen. Hierzu zerlegen wir 7^{41}, indem wir den Exponenten im Zweiersystem darstellen:

$$\begin{aligned} 41 &= 1\cdot 2^5 + 0\cdot 2^4 + 1\cdot 2^3 + 0\cdot 2^2 + 0\cdot 2^1 + 1\cdot 2^0 \\ &= 32 + 8 + 1 \end{aligned}$$

Es gilt $7^{41} = 7^{32}\cdot 7^8 \cdot 7^1$.
Nun bestimmen wird die Kongruenzen modulo 221 nach Satz B.2.1

$$\begin{aligned} 7 &\equiv 7 \\ 7^2 = 7\cdot 7 &\equiv 7\cdot 7 = 49 \\ 7^4 = 7^2\cdot 7^2 &\equiv 49\cdot 49 = 2401 \equiv 191 \\ 7^8 = 7^4\cdot 7^4 &\equiv 191\cdot 191 = 36481 \equiv 16 \\ 7^{16} = 7^8\cdot 7^8 &\equiv 16\cdot 16 = 256 \equiv 35 \\ 7^{32} = 7^{16}\cdot 7^{16} &\equiv 35\cdot 35 = 1225 \equiv 120 \end{aligned}$$

$$7^{41} = 7^{32}\cdot 7^8\cdot 7^1 \equiv 120\cdot 16\cdot 7 = 13440 \equiv 180$$

Die Verschlüsselung der Zahl 7 ist also 180.

Zum Dechiffrieren müssen wir

$$180^d \bmod n = 180^{89} \bmod 221$$

bestimmen.

$$\begin{aligned} 89 &= 1\cdot 2^6 + 1\cdot 2^4 + 1\cdot 2^3 + 0\cdot 2^2 + 0\cdot 2^1 + 1\cdot 2^0 \\ &= 64 + 16 + 8 + 1 \end{aligned}$$

□

Es gilt $180^{89} = 180^{64}\cdot 180^{16}\cdot 180^{8}\cdot 180^{1}$.

Nun bestimmen wird die Kongruenzen modulo 221:

$$\begin{aligned} 180 &\equiv 180 \\ 180^2 &\equiv 180\cdot 180 \equiv 134 \\ 180^4 &\equiv 134\cdot 134 \equiv 55 \\ 180^8 &\equiv 55\cdot 55 \equiv 152 \\ 180^{16} &\equiv 152\cdot 152 \equiv 120 \\ 180^{32} &\equiv 120\cdot 120 \equiv 35 \\ 180^{64} &\equiv 35\cdot 35 \equiv 120 \end{aligned}$$

$$180^{89} = 180^{64}\cdot 180^{16}\cdot 180^{8}\cdot 180^{1} \equiv 120\cdot 120\cdot 152\cdot 180 = 393984000 \equiv 7$$

6.3.2 Die Sicherheit von RSA

6.4 Digitale Unterschrift

Mit Hilfe eine Verschlüsselungsverfahrens wie z.B. RSA lässt sich eine digitale Unterschrift realisieren. Im Falle von RSA verschlüsselt „unterschreibt“ man eine Nachricht, indem man einen Unterschriftstext z.B eine Zahl z mit dem geheimen Schlüssel d codiert.

$$c := z^d \bmod n$$

Nun verschickt man die verschlüsselte Unterschrift c und die Klartextunterschrift z zusammen mit der Nachricht. Der Empfänger überprüft nun mit dem öffentlichen Schlüssel, ob

$$c^e \bmod n = z$$

gilt. Damit ist für ihn klar, dass z mit dem geheimen Schlüssel des Versenders, den ja auch nur dieser kennt, verschlüsselt wurde. Damit stammt die Nachricht also tatsächlich vom Versender selbst.
Man kann natürlich die Nachricht selbst zusätzlich verschlüsseln und davon nur den Code verschicken.

6.5 PGP- pretty good privacy

PGP ist ein kostenlos erhältliches Programm, das ursprünglich von Philip Zimmermann entwickelt wurde. Grundlegend für PGP ist, dass jeder Benutzer einen geheimen Schlüssel besitzt, ebenso wie die Kopien der öffentlichen Schlüssel seiner potientiellen Partner, mit denen er kommunizieren will. PGP bietet folgende Dienste:

1. digitale Unterschrift
2. Verschlüsselung der Nachricht
3. Komprimierung der Daten
4. Aufbereitung von Dateien für E-Mail
5. Aufteilung und Zusammensetzen von Dateien

6.5.1 Öffentliche Schlüssel

PGP führt eine Liste der öffentlichen Schlüssel aller Teilnehmer, mit denen man kommunizieren will. Diese sind auf dem Rechner gespeichert. Zu jedem Schlüssel gehören folgende Informationen:

1. der öffentliche Schlüssel
2. die Benutzerkennung oder der Name des Besitzers des öffentlichen Schlüssels
3. eine eindeutige Schlüsselnummer
4. weitere Informationen

Anhand der Benutzerkennung oder der Schlüsselnummer wird der öffentlichen Schlüssel des Benutzers identifiziert und ausgewählt.

6.5.2 Geheime Schlüssel

Um PGP zu benutzen, benötigt man mindestens einen geheimen Schlüssel. Man kann auch mehrere Schlüssel unterschiedlicher Länge haben. Je nach Wichtigkeit der Nachricht kann ein kurzer oder langer Schlüssel verwendet werden. Diese Auswahl hat dann Auswirkungen auf die Dauer der Ver- und Entschlüsselung.

6.5.3 Erzeugung eines Schlüsselpaares

Nach der Installation erzeugt PGP ein Schlüsselpaar. Wie beim RSA-Verfahren bereits beschrieben, erzeugt PGP ein zusammengehöriges Schlüsselpaar mit einem öffentlichen und einem geheimen Schlüssel. Hat PGP beide Schlüssel erzeugt, wird der öffentliche mit der Benutzerkennung und einer Schlüsselnummer versehen.
PGP verschlüsselt den geheimen Schlüssel so, dass er nur zusammen mit einem Mantra (Passwort) benutzt werden kann.
Wann immer man den geheimen Schlüssel benutzen möchte, fragt PGP nach dem Mantra. Wird dieses korrekt eingegeben, entschlüsselt PGP ihn mit dem Mantra. Wenn PGP den geheimen Schlüssel benutzt hat, wird er sofort wieder gelöscht.
Sollte es passieren, dass jemand den geheimen Schlüssel entwendet (z.B. auf Diskette kopiert), nützt ihm dieser nichts ohne das Mantra. Deshalb sollte man sich sein Mantra nur merken, aber niemals niederschreiben.

7 Zinsrechnung

7.1 Zinseszins

Ein Kapital von K=1000 € wird mit einem Jahreszinsatz von p= 2,5 % über 8 Jahre verzinst. Die Zinsen werden nach jedem Jahr dem Kapital zugeschlagen. Wie groß ist das Kapital nach n=8 Jahren?
Nach einem Jahr beträgt das Kapital $K + K \cdot p = K \cdot (1 + p)$,
nach zwei Jahren $K \cdot (1 + p) \cdot (1 + p)$, nach n Jahren beträgt das Kapital

$$K \cdot (1 + p)^n .$$

Nach 8 Jahren hat man $1000 \cdot 1,025^8$ €=1218,40 €.
Würde man die Zinsen nach jedem Jahr abheben, und somit keine Zinseszinsen erhalten, so betrüge das Kapital inklusive abgehobener Zinsen nach n Jahren

$$K + n \cdot p \cdot K = K \cdot (1 + n \cdot p) .$$

Nach 8 Jahren hätte man 1200 €.

Bemerkung: Es handelt sich bei der Verzinsung mit Zinseszins um einen Wachstumsprozess wie in Abschnitt 3.3. Geht man von einem „Kapital“ von x_0 Bakterien und einem Zinssatz von p=100 % =1 aus, so hat man nach n Jahren (Zeitschritten)

$$x_n = x_0 \cdot (1 + p)^n = x_0 \cdot 2^n$$

Bakterien.

7.2 Unterjährige Verzinsung

Werden die Zinsen nicht erst am Ende eines Jahres gezahlt, sondern monatlich, so gibt es verschiedene Arten dies zu tun.
Es werde ein Kapital von K=100 € für ein Jahr zu einem Jahreszinsatz von p=6% angelegt. Der relative monatliche Zinssatz beträgt dann $p_m = \frac{p}{12}$. Damit beträgt das Kapital nach einem Jahr

$$K_1 = K \cdot (1 + p_m)^{12} = K \cdot (1 + \frac{p}{12})^{12} = 106,17 €$$

Der effektive Zinssatz[1] beträgt also 6,17 %.
Will man erreichen, dass der effektive Jahreszinssatz dem nominellen Jahreszinsatz p=6% entspricht, muss

$$K \cdot (1+p) = K \cdot (1+p_k)^{12}$$

gelten. Hierbei heisst p_k der zum Jahreszinssatz konforme Monatszinssatz und es gilt:

$$p_k = (1+p)^{\frac{1}{12}} - 1$$

7.3 Stetige Verzinsung

Im vorherigen Abschnitt sind wir davon ausgegangen, dass die Zinsen monatlich gezahlt werden. Was aber passiert mit dem effektiven Zinssatz, wenn das Kapital mit einem wöchentlichen, täglichen, stündlichen Zinssatz etc. verzinst wird?
Es sei p der nominelle Jahreszinsatz und *n* die Anzahl der Zinsperioden, in die das Jahr eingeteilt wird. Bei monatlicher Zinszahlung gilt also n=12, bei wöchentlicher n=52 usw. Das Kapital nach einem Jahr beträgt dann abhängig von n:

$$K_1 = K \cdot (1+\frac{p}{n})^n$$

Man erhält folgende Werte für K= 100 € und p= 10%:

n	1	12	52	1248
K_1 in €	110,000	110,471	110,506	$110,51\overline{6}$

Wenn man (bei gleichbleibendem nominellen Zinssatz) die Anzahl der Zinsperioden vergrößert, wird das Endkapital immer größer. Es gibt aber eine obere Grenze. Man kann zeigen, dass die Folge $(1+\frac{p}{n})^n$ für n gegen Unendlich gegen e^p konvergiert. Damit liegt die Grenze im Zahlenbeispiel bei $K_1 = 110,517$ €.

7.4 Ratensparen

Die Eltern der kleinen Susi legen jeden Monat 50 € in einem Ratensparbuch für ihre Ausbildung fest. Sie beginnen damit bei ihrer Geburt. Der effektive Jahreszinssatz

[1] In der Realität berechnet sich der effektive Zinssatz komplizierter. Beim effektiven Zinsatz werden sämtliche Gebühren etc., berücksichtigt.

beträgt 3%. Die Zinsen werden monatlich gutgeschrieben. Wieviel Geld erhält Susi an ihrem 18. Geburtstag?

Da der effektive Jahreszins 3% beträgt, beträgt der konforme Monatszinssatz $p_k = (1+0.03)^{\frac{1}{12}} - 1$. Der Wert der ersten Rate B beträgt nach einem Monat

$$B \cdot (1+p_k) = B \cdot \left(1 + 1.03^{\frac{1}{12}} - 1\right) = B \cdot 1.03^{\frac{1}{12}}$$

Nach n Monaten beträgt der Wert der ersten Rate

$$B \cdot (1+p_k)^n = B \cdot \left(1 + 1.03^{\frac{1}{12}} - 1\right)^n = B \cdot \left(1.03^{\frac{1}{12}}\right)^n$$

Wir haben jeden Monat den Faktor $c = 1.03^{\frac{1}{12}}$ zu berücksichtigen.

Es gilt:
monatliche Rate : $B = 50\,€$
Laufzeit: $n = 12 \cdot 18 = 216$ Monate
Kapitalzins: 3% p.a., daraus ergibt sich $c = 1.03^{\frac{1}{12}}$

Monat	Rate	Wert der Rate nach dem Monat	Kapital nach dem Monat
1	B	$B \cdot c^n$	$B \cdot c^n$
2	B	$B \cdot c^{n-1}$	$B \cdot (c^n + c^{n-1})$
3	B	$B \cdot c^{n-2}$	$B \cdot (c^n + c^{n-1} + c^{n-2})$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
n	B	$B \cdot c^1$	$B \cdot (c^n + c^{n-1} + c^{n-2} + \ldots + c^1)$

Damit beträgt das Kapital E nach n Monaten(vgl. B.1.1):

$$\begin{aligned} E &= B \cdot \sum_{k=1}^{n} c^k = B \cdot \sum_{k=0}^{n-1} c^{k+1} \\ &= B \cdot c \cdot \sum_{k=0}^{n-1} c^k = B \cdot c \cdot \frac{c^n - 1}{c - 1} \end{aligned}$$

Das angesparte Kapital, das Susi erhält, beträgt $E = 50 \cdot c \cdot \frac{c^{216}-1}{c-1} = 14275,92\,€$.
Im Vergleich dazu beträgt die eingezahlte Summe $216 \cdot 50\,€ = 10800\,€$.

7.5 Kredit

Wir wollen einen Kredit von 6000 € für ein Auto aufnehmen und diesen innerhalb der nächsten 3 Jahre zurückzahlen. Hierbei sollen jeden Monat gleich hohe Raten gezahlt werden. Die Rückzahlung beginnt am Ende des Monats, in dem wir den Kredit aufgenommen haben.

Die HAIBANK macht uns ein Angebot mit einem jährlichen (effektiven) Kreditzins von 6%. Wie hoch sind die monatlichen Raten?

Für die Schulden fallen monatliche Zinsen an. Da der Jahreszins 6% beträgt, müssen die aktuellen Schulden jeden Monat mit $c = 1.06^{\frac{1}{12}}$ multipliziert werden. Dann ergibt sich nach einem Jahr der Faktor $(1.06^{\frac{1}{12}})^{12} = 1.06$. Ohne Rückzahlung sind dann die Schulden um 6% gestiegen. Wir haben folgende Situation:

Schulden zu Kreditbeginn: $S = 6000$ €
Laufzeit: $n = 36$ Monate
Kreditzins: $p = 6\%$ daraus ergibt sich $c = 1.06^{\frac{1}{12}} \approx 1,00487$
Rückzahlungsrate am Ende des Monats: R (gesucht)

Monat	**Schulden am Ende des Monats**
1	$S \cdot c - R$
2	$(S \cdot c - R) \cdot c - R = S \cdot c^2 - R \cdot c - R$
3	$((S \cdot c - R) \cdot c - R) \cdot c - R = S \cdot c^3 - R \cdot c^2 - R \cdot c - R$
$\vdots$	$\vdots$
n	$S \cdot c^n - R \cdot c^{n-1} - \ldots - R \cdot c^2 - R \cdot c - R$
	$= S \cdot c^n - R \cdot (c^{n-1} + \ldots + c^2 + c + 1)$

Bei dem Ausdruck in der Klammer handelt es sich um eine geometrische Summe und es gilt nach Satz B.1.1

$$c^{n-1} + \ldots + c^2 + c + 1 = \frac{c^n - 1}{c - 1}$$

Nach 36 Monaten soll die Restschuld null sein, also

$$S \cdot c^n - R \cdot \frac{c^n - 1}{c - 1} = 0$$

damit ergibt sich für die Rate

$$R = S \cdot c^n \cdot \frac{c - 1}{c^n - 1}$$

Im Zahlenbeispiel gilt

$$R = 6000 \cdot (1.06^{\frac{1}{12}})^{36} \cdot \frac{1.06^{\frac{1}{12}} - 1}{(1.06^{\frac{1}{12}})^{36} - 1} \text{€} = 182,10 \text{€}$$

Man hat also insgesamt ca. 6556 € zu zahlen.
Anmerkung: Bei der Kreditberechnung findet man in Schulbüchern häufig die Berechnung mit dem relativen Monatszinssatz. In diesem Fall beträgt der Faktor

$$c = (1 + \frac{p}{12}) = 1 + \frac{0.06}{12} = 1.005$$

und es gilt

$$R = 182,53 \text{€}$$

Man hat also insgesamt ca. 6571 € zu zahlen.

7.6 Altersvorsorge

Eine Referendarin möchte mit 25 anfangen, für das Alter vorzusorgen. Hierzu will sie beginnend mit dem 25. Geburtstag monatlich Geld zurücklegen. Ziel ist es mit 65 Jahren eine zusätzliche Rente zu erhalten, die sich den steigenden Lebenshaltungskosten anpasst. Der Vermögensberater der Bank empfiehlt eine Absicherung, bei der sie anfangs eine zusätzliche Rente von 1000 € erhält, die sich jedes Jahr um 2% erhöht, wobei die Rentensteigerung jeden Monat stattfinden soll. Das eingezahlte Kapital wird mit einem festen (effektiven) Zinssatz von 3% p.a. verzinst. Weiterhin schlägt der Berater vor, die Raten monatlich zu erhöhen, so dass von Jahr zu Jahr 2% mehr eingezahlt wird. Der Berater empfiehlt weiterhin eine Laufzeit von 30 Jahren, so dass sie bis zum Alter von 95 Jahren die Rente beziehen kann. Wie hoch ist nun die anfängliche monatliche Belastung
Wir berechnen zuerst das Kapital K, das bis zum 65. Geburtstag angespart sein muss. Wir haben folgende Situation:

Grundrente zu Beginn: $R = 1000$ €
Laufzeit: $n = 360$ Monate
Kapitalzins: 3% daraus ergibt sich $c = 1.03^{\frac{1}{12}}$
Rentensteigerung: 2% daraus ergibt sich der Rentensteigerungsfaktor $b = 1.02^{\frac{1}{12}}$
Gesamtkapital mit 65: K (gesucht)

Betrachten wir das für den k-ten Rentenmonat benötigte Kapital K_k:
Da das angesparte Kapital für die vorhergehenden k-1 Monate verzinst wird, beträgt das im k-ten Monat verfügbare Kapital

$$K_k \cdot c^{k-1}$$

Dieser Betrag muss nun gleich dem im k-ten Monat benötigten sein: Da sich die Grundrente R jeden Monat erhöhen soll, müssen wir diese k-1-mal mit dem Steigerungsfaktor multiplizieren. Die Rente im k-ten Monat beträgt also $R \cdot b^{k-1}$. Gleichsetzen ergibt:

$$K_k \cdot c^{k-1} = R \cdot b^{k-1}$$

Das für den k-ten Monat benötigte Kapital, das zu Rentenbeginn zur Verfügung stehen muss, beträgt also

$$K_k = R \cdot \left(\frac{b}{c}\right)^{k-1}$$

Für die Laufzeit von n-Rentenmonaten ergibt sich also ein benötigtes Gesamtkapital von

$$K = \sum_{k=1}^{n} K_k = R \cdot \sum_{k=1}^{n} \left(\frac{b}{c}\right)^{k-1} = R \cdot \sum_{k=0}^{n-1} \left(\frac{b}{c}\right)^{k} = R \cdot \frac{\left(\frac{b}{c}\right)^{n} - 1}{\frac{b}{c} - 1}$$

Im Zahlenbeispiel beträgt das benötigte Kapital

$$K = 1000 \cdot \frac{\left(\frac{1.02}{1.03}\right)^{\frac{360}{12}} - 1}{\left(\frac{1.02}{1.03}\right)^{\frac{1}{12}} - 1} \text{€} \approx 312228,32 \text{€}$$

Nun können wir berechnen, wie hoch die anfängliche Beitragsrate B ist. Wir haben folgende Situation:

Benötigtes Kapital: $K = 312228,32$ €
Laufzeit: $n = 480$ Monate
Kapitalzins: 3% p.a., daraus ergibt sich $c = 1.03^{\frac{1}{12}}$
Beitragssteigerung: 2% p.a., daraus ergibt sich der Steigerungsfaktor $b = 1.02^{\frac{1}{12}}$
Höhe der ersten Beitragsrate: B (gesucht)

Monat	Rate	Wert der Rate nach dem Monat	Kapital nach dem Monat
1	B	$B \cdot c^n$	$B \cdot c^n$
2	$B \cdot b$	$B \cdot b \cdot c^{n-1}$	$B \cdot (c^n + b \cdot c^{n-1})$
3	$B \cdot b^2$	$B \cdot b^2 \cdot c^{n-2}$	$B \cdot (c^n + b \cdot c^{n-1} + b^2 \cdot c^{n-2})$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
n	$B \cdot b^{n-1}$	$B \cdot b^{n-1} \cdot c^1$	$B \cdot (c^n + b \cdot c^{n-1} + b^2 \cdot c^{n-2} + \cdots + b^{n-1} \cdot c^1)$

damit beträgt das Kapital E nach n Monaten:

$$\begin{aligned} E &= \sum_{k=0}^{n-1} B \cdot b^k \cdot c^{n-k} = B \cdot c^n \cdot \sum_{k=0}^{n-1} B \cdot b^k \cdot c^{-k} \\ &= B \cdot c^n \cdot \sum_{k=0}^{n-1} \left(\frac{b}{c}\right)^k = B \cdot c^n \cdot \frac{\left(\frac{b}{c}\right)^n - 1}{\frac{b}{c} - 1} = B \cdot c \cdot \frac{b^n - c^n}{b - c} \end{aligned}$$

Diese Summe muss nun dem benötigten Kapital entprechen. Damit gilt für die anfängliche Beitragsrate B:

$$B = K \cdot \frac{1}{c} \cdot \frac{b - c}{b^n - c^n}$$

Im Zahlenbeispiel beträgt die erste Beitragszahlung $B \approx 240,74$ €, und die letzte $B \cdot b^{479} \approx 530,69$ €.

8 Numerische Verfahren

8.1 Flächenbestimmung

8.1.1 Flächenbestimmung nach der Mittelpunktsformel

Im Beispiel aus Abschnitt 3.1 wurde die Fläche unter der Kurve nach der sogenannten Mittelpunktsformel bestimmt. Mit dieser Formel lassen sich Flächen unter beliebigen Kurven approximativ bestimmen:

Es sei folgende Situation gegeben: Gesucht ist die Fläche F, die nach unten durch die x-Achse, nach oben durch die Funktion f(x) und nach rechts und links durch Senkrechten bei x=a und x=b begrenzt ist.

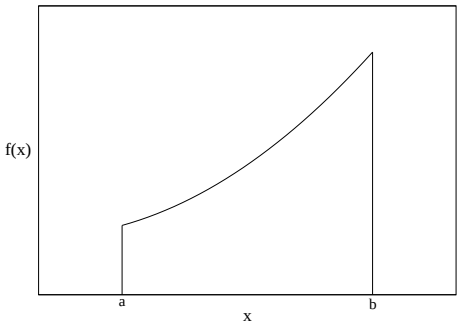


Abbildung 8.1: Flächenbestimmung unter einer Kurve

Die Fläche unter der Kurve wird näherungsweise bestimmt, indem das Gebiet in n senkrechte Streifen eingeteilt wird und der obere krumme Rand jeden Streifens durch eine Strecke ersetzt wird, so dass Rechtecke entstehen. Die Streifen werden alle gleich breit gewählt: $h := (b-a)/n$. Die Gesamtfläche ergibt sich aus der Summe der Flächen aller Rechtecke. Zur Flächenberechnung eines Rechtecks R_i wird dessen Höhe $f(x_i + \frac{h}{2})$ in der Mitte des Streifens herangezogen:

$$R_i = h \cdot f(x_i + \frac{h}{2}) \quad i = 1 \cdots n$$

Für die Gesamtsumme bei n Streifen gilt dann

$$Q_n^{Mi}[f] = h \cdot \left[f(x_1 + \frac{h}{2}) + f(x_2 + \frac{h}{2}) + \cdots + f(x_n + \frac{h}{2}) \right],$$

wobei $x_1 = a$ und $x_n + h = b$ gilt.

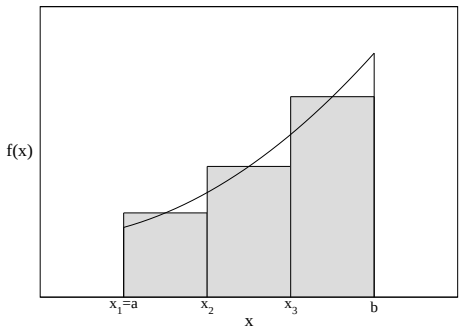


Abbildung 8.2: Flächenbestimmung nach der Mittelpunktsformel

8.1.2 Flächenbestimmung nach der Trapezformel

Ähnlich zur Mittelpunktsformel kann man die Fläche unter einer Kurve auch durch die sogenannte Trapezformel approximieren. Hierbei wird, wie der Name schon sagt, die Fläche von Trapezen abgedeckt und diese aufsummiert. Zur Flächenberechnung eines Trapezes T_i wird dessen durchschnittliche Höhe $(f(x_{i+1}) + f(x_i))/2$ herangezogen:

$$T_i = \frac{h}{2} \cdot (f(x_{i+1}) + f(x_i))) \quad i = 1 \cdots n$$

Für die Gesamtsumme bei n Streifen gilt dann

$$Q_{n+1}^{Tr}[f] = \frac{h}{2} \cdot [f(x_1) + 2f(x_2) + \cdots + 2f(x_n) + f(x_{n+1})] \,,$$

wobei $x_1 = a$ und $x_{n+1} = b$ gilt.
Der Index $n+1$ ergibt sich aus der Tatsache, dass bei n Streifen $n+1$ Stützstellen berücksichtigt werden.

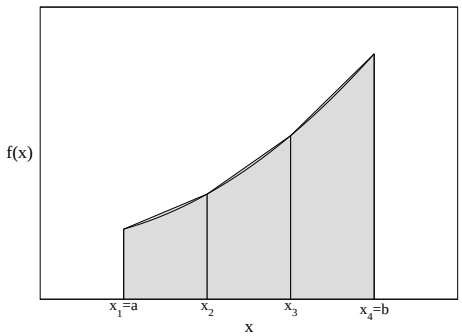


Abbildung 8.3: Flächenbestimmung nach der Trapezformel

Anmerkung für Analytiker: Die Zahlenfolgen $(Q_{n+1}^{Tr}[f])_n$ und $(Q_n^{Mi}[f])_n$, $n \in \mathbb{N}$ konvergieren gegen das Riemannsche Integral, falls dieses existiert.

8.1.3 Flächenbestimmung nach der Kästchenzählmethode

Um beliebige Flächen zu bestimmen kann die gesuchte Fläche mit einem Gitter überdeckt werden. Man zählt nun alle Kästchen, die die Fläche überdecken oder berühren. Die Gesamtfläche ergibt sich aus der Anzahl der Kästchen multipliziert mit der Fläche eines Kästchens.

8.1.4 Flächenbestimmung durch Wiegen

Man zeichnet die Fläche auf einen Karton dessen Fläche F_K bekannt ist (ausmessen) und wiegt diesen. Dann schneidet man die gesuchte Fläche aus und wiegt sie ebenfalls. Die Fläche ergibt sich aus dann zu

$$F = \frac{M}{M_K} \cdot F_K \,,$$

wobei M die Masse der Fläche und M_K die Masse des Kartons ist.

8.2 Das Horner-Schema

Das Berechnen von Polynomen höherer Ordnung ist mühsam. Betrachtet man z.B. das Polynom

$$p(x) = 3x^5 + 4x^4 + 2x^3 - 3x^2 - 7x + 5 \,,$$

so muss man folgende Rechenoperationen ausführen:

$3 \cdot x \cdot x \cdot x \cdot x \cdot x$	5 Multiplikationen
$4 \cdot x \cdot x \cdot x \cdot x$	4 Multiplikationen
$2 \cdot x \cdot x \cdot x$	3 Multiplikationen
$3 \cdot x \cdot x$	2 Multiplikationen
$7 \cdot x$	1 Multiplikationen
	3 Additionen
	2 Subtraktionen

Dies macht zusammen 20 Rechenoperationen. Bedenkt man, dass bei jeder Operation Rundungsfehler auftreten können (ganz zu Schweigen von Rechenfehlern, wenn man es von Hand macht) stellt sich die Frage, ob man die Rechnung effizienter ausführen kann. Hierzu klammern wir x so oft es geht aus:

$$\begin{aligned} p(x) &= 3x^5+4x^4+2x^3-3x^2-7x+5 \\ &= (3x^4+4x^3+2x^2-3x-7)x+5 \\ &= \cdots \\ &= ((((3x+4)x+2)x-3)x-7)x+5 \end{aligned}$$

Insgesamt müssen nun noch 10 Rechenoperationen ausgeführt werden.
Schematisch kann man diese Rechnung nun ganz einfach durchführen: Man schreibt die Koeffizienten in die erste Zeile (nicht die Nullen vergessen, falls welche auftreten):
Dann fängt man links an. In den Spalten wird addiert, das Ergebnis mit x multipliziert und in die zweite Zeile der nächsten Spalte geschoben. (In der ersten Spalte wird der Eintrag nur in die dritte Zeile übertagen). In der dritten Zeile der letzen Spalte steht dann das Ergebnis.
Für das Beispiel sieht dies wie folgt aus, wobei die Pfeile jeweils die Multiplikation mit x andeuten sollen:

	3	4	2	-3	-7	5
$+$		$3x$	$(3x+4)x$	$((3x+4)x+2))x$	$(((3x+4)x+2))x-3)x$	$((((3x+4)x+2))x-3)x-7)x$
	$3\nearrow$	$3x+4\nearrow$	$2+(3x+4)x+2\nearrow$	$((3x+4)x+2))x-3\nearrow$	$((((3x+4)x+2))x-3)x-7)\nearrow$	$((((\mathbf{3x+4})\mathbf{x+2}))\mathbf{x-3})\mathbf{x-7})\mathbf{x+5}$

Für $x = 2$ berechnet sich das Ergebnis also wie folgt:

	3	4	2	-3	-7	5
$+$		6	20	44	82	150
	$3\nearrow$	$10\nearrow$	$22\nearrow$	$41\nearrow$	$75\nearrow$	**155**

8.3 Das Newton-Verfahren

In Abschnitt haben wir uns die Frage gestellt, wie t ein Taschenrechner auf $\sqrt{2} = 1.4142135\cdots$ kommt und haben dabei das Heron-Verfahren kennengelernt.

Allgemein stellt sich die Frage, wie man zu einem Polynom die Nullstellen findet? Im Beispiel von $\sqrt{2}$ suchen wir die Nullstellen von $p(x) = x^2 - 2$.
Dieses Problem kann man wie folgt angehen (Abbildung 8.4):
Gestartet wird in der Nähe der Nullstelle mit x_0. Gesucht ist nun die Tangente $g_0(x)$

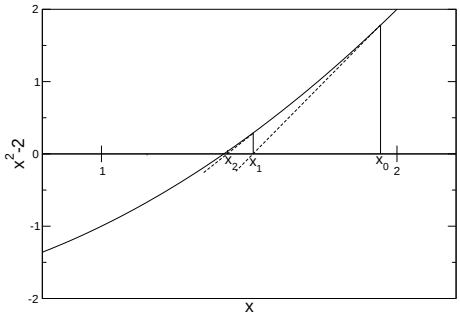


Abbildung 8.4: Idee des Newton-Verfahrens

an den Graphen $p(x)$. Die Tangente hat folgende Eigenschaften

- $g_0(x_0) = p(x_0)$
- die Steigung der Tangente stimmt mit der Steigung von p an der Stelle x_0 überein

Der nächste Schritt wird dann berechnet, indem die Nullstelle der Tangente bestimmt wird und an dieser Stelle wieder eine Tangente an den Graphen der Funktion angelegt wird, und so weiter.

Sei $g_0(x) = m_0 \cdot x + b_0$.
Die Nullstelle x_1 der Tangente ergibt sich aus $g_0(x_1) = m_0 \cdot x_1 + b_0 = 0$:

$$x_1 = -\frac{b_0}{m_0} \tag{8.1}$$

Aus $g_0(x_0) = p(x_0)$ folgt $p(x_0) = m_0 \cdot x_0 + b_0$ und damit

$$b_0 = p(x_0) - m_0 \cdot x_0 \,.$$

Einsetzen in Gleichung 8.1 ergibt

$$x_1 = -\frac{p(x_0) - m_0 \cdot x_0}{m_0} = x_0 - \frac{p(x_0)}{m_0} \tag{8.2}$$

Man erhält eine Iterationsfolge, die sich der Nullstelle nähert:

$$x_{n+1} = x_n - \frac{p(x_n)}{m_n} \tag{8.3}$$

Es bleibt das Problem, die Steigungen m_n der Geraden zu bestimmen.

Anmerkung für Analytiker: Eigentlich ist man schon fertig. Da die Steigung der Geraden in x_n gerade der Steigung der Funktion p an der Stelle x_n entspricht, und die Steigung von p gerade die Ableitung p' ist, lautet das Newton-Verfahren

$$x_{n+1} = x_n - \frac{p(x_n)}{p'(x_n)}\,.$$

Um die Steigung der Funktion p (und damit auch der Geraden) zu bestimmen, gehen wir davon aus, dass sich die Steigung der Funktion p in der Nähe der betrachteten Stelle nur geringfügig ändert. Sei x_0 die Stelle, an der die Steigung m_0 bestimmt werden soll, und sei $\varepsilon > 0$ klein, dann gilt (Abbildung 8.5):

$$m_0 \approx \frac{p(x_0+\varepsilon) - p(x_0)}{\varepsilon}\,.$$

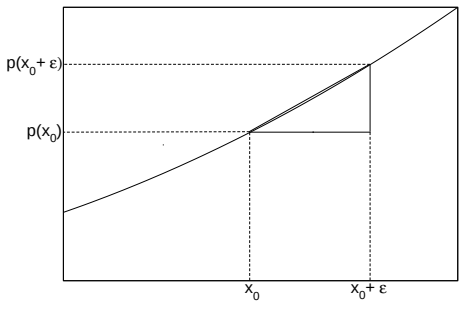


Abbildung 8.5: Bestimmung der Steigung von p an der Stelle x_0 über das Steigungsdreieck.

Für das Beispiel $p(x) = x^2 - F$ gilt

$$m_0 \approx \frac{((x_0+\varepsilon)^2 - F) \;-\; (x_0^2 - F)}{\varepsilon} = \frac{2x_0\varepsilon + \varepsilon^2}{\varepsilon} = 2x_0 + \varepsilon\,.$$

Da ε klein ist, kann man alle Terme, die ε enthalten, vernachlässigen und erhält somit die Steigung $m_0 = 2x_0$: Dieses Verfahren funktioniert nur bei bestimmten Funktionen, wie z.B. den Polynomen.

Anmerkung für Analytiker: Für beliebige differenzierbare Funktionen funktioniert das Verfahren, wenn man den Grenzwert
$\lim_{\varepsilon \to 0} \frac{2 \cdot x_0 \cdot \varepsilon + \varepsilon^2}{\varepsilon} = \lim_{\varepsilon \to 0} 2x_0 + \varepsilon = 2x_0$ betrachetet. Dieser Grenzwert ist gerade die Ableitung (Steigung).

Für das Beispiel $p(x) = x^2 - F$ erhält man also folgende Iteration:

$$\begin{aligned} x_{n+1} &= x_n - \frac{x_n^2 - F}{2x_n} \\ &= \frac{1}{2}\left(2x_n - \frac{x_n^2 - F}{x_n}\right) \\ &= \frac{1}{2}\left(2x_n - x_n + \frac{F}{x_n}\right) \\ &= \frac{1}{2}\left(x_n + \frac{F}{x_n}\right). \end{aligned} \tag{8.4}$$

Das Ergebnis ist also dasselbe wie beim Heron-Verfahren in Gleichung 4.1.

Satz 8.3.1 Newton Verfahren für Polynome
Es sei ein Polynom $p(x) = a_m \cdot x^m + \cdots + a_1 \cdot x + a_0$, $m \in \mathbb{N}$ gegeben. Die Lösung der Gleichung $p(x) = 0$ bestimmt man, indem man eine Schätzung x_0 der Nullstelle vorgibt und p durch die Tangente an den Graphen in x_0 approximiert und deren Nullstelle bestimmt. Dieser Wert x_1 wird als nächster Schätzwert der Nullstelle gewählt, usw:

$$x_{n+1} = x_n - \frac{p(x_n)}{m(x_n)}$$

mit

$$m(x) = m \cdot a_m \cdot x^{m-1} + \cdots + 2a_2 \cdot x^2 + a_1$$

Mit dem Horner-Schema und dem Newton-Vefahren kann man nun leicht die Nullstellen eines Polynoms bestimmen.

Beispiel: Bestimmung der Nullstellen von $p(x) = 3x^4 - 6x^3 + 2x^2 - 5x + 1$

Zuerst machen wir eine Wertetabelle (und zeichnen den Graphen, um besser zu sehen, ob es noch mehr Nullstellen gibt), um eine Abschätzung der Nullstellen zu erhalten.

x	-1.0	-0.5	0.0	0.5	1.0	1.5	2.0	2.5
p(x)	17.0	4.9	1.0	-1.6	-5.0	-7.1	-1.0	24.4

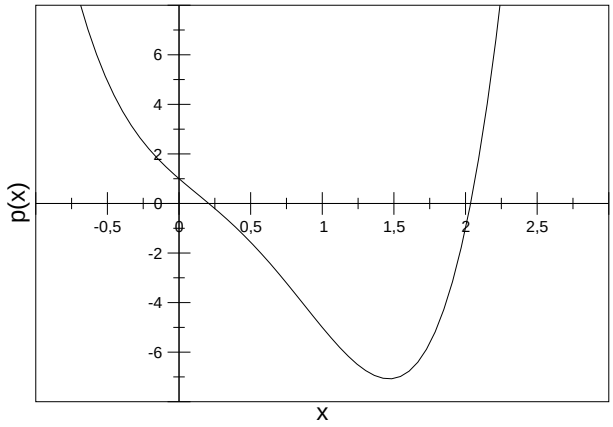


Abbildung 8.6: Der Graph von $p(x) = 3x^4 - 6x^3 + 2x^2 - 5x + 1$.

Als Startwerte für die Iteration kommen $x_0 = 2$ und $x_0 = 0$ in Frage.

Bestimmung der Nullstelle in der Nähe von $x_0 = 2$:

Nach 8.3.1 gilt

$$x_1 = x_0 - \frac{p(x_0)}{m(x_0)}$$

Zuerst muss also das Polynom $p(x) = 3x^4 - 6x^3 + 2x^2 - 5x + 1$ an der Stelle $x_0 = 2$ ausgewertet werden. Mit dem Hornerschema erhält man $p(x_0) = -1$:

	3	-6	2	-5	1
+		6	0	4	-2
	$3\nearrow$	$0\nearrow$	$2\nearrow$	$-1\nearrow$	$\mathbf{-1}$

Nun muss noch das Steigungspolynom

$$m(x) = 3 \cdot 4x^3 - 6 \cdot 3x^2 + 2 \cdot 2x - 5 = 12x^3 - 18x^2 + 4x - 5$$

an der Stelle $x_0 = 2$ ausgewertet werden. Mit dem Hornerschema erhält man $m(x_0) = 27$:

	12	−18	4	−5
+		24	12	32
	12 ↗	6 ↗	16 ↗	**27**

Man erhält also als erste Näherung für die erste Nullstelle

$$x_1 = 2 - \frac{-1}{27} = \frac{55}{27} \approx 2.0370$$

Mit diesem Wert kann man das Verfahren nun wiederholen, um ein genaueres Ergebnis zu erhalten.
Der exakte Wert beträgt auf vier Nachkommastellen gerundet 2,03526.

Bestimmung der Nullstelle in der Nähe von $x_0 = 0$:

Zur Bestimmung der zweiten Nullstelle starten wir bei $x_0 = 0$. Dies ist besonders einfach, da man $p(0)$ und $m(0)$ direkt ausrechnen kann, und man erhält als erste Näherung:

$$x_1 = 0 - \frac{-1}{-5} = \frac{1}{5} = 0.2$$

Der nächste Schritt ergibt $p(x_1) = \frac{23}{625}$:

	3	−6	2	−5	1
+		$\frac{3}{5}$	$-\frac{27}{25}$	$\frac{23}{125}$	$-\frac{602}{625}$
	3 ↗	$-\frac{27}{5}$ ↗	$\frac{23}{25}$ ↗	$\frac{602}{125}$ ↗	$\mathbf{\frac{23}{625}}$

Es ist besser mit Brüchen zu rechnen, um Rundungsfehler zu vermeiden!!

und $m(x_1) = -\frac{603}{125}$:

	12	-18	4	-5
$+$		$\frac{12}{5}$	$-\frac{78}{25}$	$\frac{223}{125}$
	$12\ \nearrow$	$-\frac{78}{5}\ \nearrow$	$\frac{22}{25}\ \nearrow$	$-\mathbf{\frac{603}{125}}$

Man erhält also als Näherung für die zweite Nullstelle

$$x_2 = \frac{1}{5} - \frac{\frac{23}{625}}{-\frac{603}{125}} = \frac{626}{3015} \approx 0.2076$$

Der exakte Wert beträgt auf vier Nachkommastellen gerundet 0,2076.

9 Fraktale

9.1 Fraktale und fraktale Dimension

Betrachten wir folgende Vorschrift: Wir nehmen das Intervall $[0,1]$ und schneiden im ersten Schritt das mittlere Drittel also das Intervall $[\frac{1}{3},\frac{2}{3}[$ heraus. Übrig bleiben die Intervalle $[0,\frac{1}{3}[$ und $[\frac{3}{3},1]$. Mit diesen Intervallen Verfahren wir genauso. Aus jedem der beiden Intervalle wird jeweils wieder das mittlere Drittel herausgeschnitten usw. (siehe Abbildung 9.1).

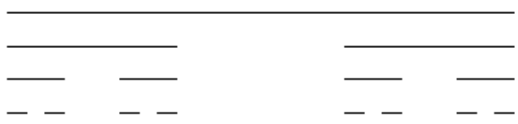


Abbildung 9.1: Die Cantor-Menge entsteht indem man in jedem Intervall das mittlere Drittel wegstreicht.

Die Frage ist, was übrig bleibt, wenn man dieses Verfahren unendlich oft anwendet. Das Bild, das dabei entsteht nennt man auch Limesbild (von Limes: Grenzwert). Obwohl jedes einzelne Objekt eine Strecke ist, besteht das Limesbild aus isolierten Punkten. Limesbilder können also ganz andere Eigenschaften haben als die Objekte, die zu ihrer Entstehung führen:
Betrachten wir hierzu ein Quadrat der Kantenlänge 1. Wir schneiden nun sukzessive Quadrate heraus, so dass eine Treppe entsteht (Abbildung 9.2): Bestimmt man die Treppenlänge (von der oberen linken zur unteren rechten Ecke) so beträgt die Länge in jedem Schritt 2. Je öfter man das Verfahren wiederholt, umso mehr nähert sich die Treppe der Diagonalen (Limesbild). Die Diagonale hat aber die Länge $\sqrt{2}$.

Abbildung 9.2: Die Treppenlänge beträgt für jeden Schritt 2. Die Diagonale als Limesbild hat die Länge $\sqrt{2}$.

Betrachten wir noch einmal die Cantor-Menge. Jedes Intervall, dass entsteht, sieht, bis auf einen Skalierungsfaktor, aus wie das Original. Die Cantor-Menge ist selbstähnlich.

Definition 9.1.1 Eine Figur wird **selbstähnlich** genannt, wenn Teile der Figur kleine Kopien der ganzen Figur sind.

Ein weiters Beispiel für eine selbstähnliche Figur ist die Koch'sche Kurve, auch Schneeflockenkurve genannt. Sie entsteht aus einem gleichseitigen Dreieck, bei dem man auf das mittlere Drittel jeder Seite ein weiteres Dreick aufsetzt und die überschüssigen Linien wegstreicht (siehe 9.3).

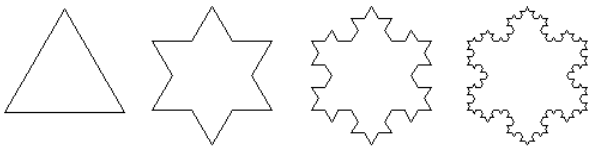


Abbildung 9.3: Die Schneeflockenkurve entsteht indem auf jede Seite eines gleichseitigen Dreiecks in der Mitte ein gleichseitiges Dreieck mit einem Drittel der ursprünglichen Seitenlänge aufgesetzt wird.

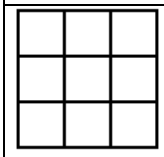
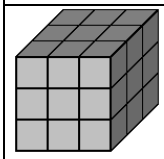
Betrachet man eine Seite des Dreicks und setzt die erste Seitenlänge gleich eins, so verlängert sich die Seitenlänge in jedem Schritt um ein Drittel. Letzlich wird die Seite und damit die gesamte Kurve unendlich lang.

Um dieses etwas besser zu verstehen betrachten wir zunächst die für uns vertauten Objekte Strecke, Quadrat und Würfel.

Bei einer Strecke, die in drei gleiche Teile eingeteilt wird beträgt die Länge jeder einzelnen Strecke ein Drittel der Ursprungslänge, logisch.

Teilt man die Seiten eines Quadrats in drei gleiche Teile, so entstehen insgesamt 9 Quadrate, von denen jedes eine Fäche hat, die einem Neuntel der Ursprungsfläche entspricht.

Teilt man die Kanten eines Würfels in drei gleiche Teile, so entstehen insgesamt 27 Würfel, von denen jeder ein Volumen hat, das einem Siebenundzwanzigstel des Ursprungsvolumen entspricht. Wir erhalten folgende Tabelle:

Objekt	Skalierungsfaktor s	Anzahl N	Beziehung
	3	3	$3^1 = 3$
	3	9	$3^2 = 9$
	3	27	$3^3 = 27$

Man erhält die Beziehung

$$s^D = N \text{ , oder } D = \frac{\log N}{\log s}$$

wobei D die Dimension des Objektes ist.
Führt man dasselbe Verfahren für die Cantor-Menge und die Schneeflockenkurve durch, so erhält man:

Objekt	Skalierungsfaktor s	Anzahl N	Beziehung
	3	2	$3^x = 2$
	3	4	$3^x = 4$

Bestimmt man jeweils den unbekannten Exponenten x, so erhält man für die Cantormenge den Wert $x = \frac{\log 2}{\log 3} = 0,631$, für die Schneeflockenkurve $x = \frac{\log 4}{\log 3} = 1,262$. Nach obigen Überlegungen handelt es sich bei diesen Werten um die Dimension der Objekte. Man erhält einen Dimensionbegriff, bei dem auch nicht-ganzzahlige Werte zugelassen sind, die fraktale Dimension:
Fraktale Dimension der Cantor-Menge: $D \approx 0,631$
Fraktale Dimension der Schneeflockenkurve: $\approx 1,262$

Die bisherigen Überlegungen passen damit gut zusammen. Die Cantormenge, deren Limesbild aus isolierten Punkten und nicht mehr aus Strecken besteht, hat eine Dimension zwischen Punkt (D=0) und Strecke (D=1), die Schneeflockenkurve, deren Länge unendlich ist, hat eine Dimension zwischen Strecke (D=1) und Fläche (D=2).

Ein weiters bekanntes Fraktal ist das Sierpinski-Dreieck[1]. Es entsteht aus einem gleichseitigen Dreick, aus dem man sukzessive Dreiecke entfernt (Abbildung 9.4).

Abbildung 9.4: Sierpinski-Dreieck.

Beim Sierpinski-Dreieck wird bei einer Verdopplung der linearen Ausdehnung (der-Sietenlänge), also einem Skalierungsfaktor von s=2, eine Verdreifachung des Ausgangsbildes erreicht, also N=3. damit hat das Sierpinski-Dreieck die faktale Dimension $D = \frac{\log 3}{\log 2} \approx 1,585$. Die Dimension liegt also zwischen der einer Strecke und der einer Fläche.

9.2 Das Chaos-Spiel

9.2.1 Cantor Menge

Man kann selbstähnliche Fraktale auch über ein Chaos-Spiel erreichen. Es sei die Strecke $\overline{AB}$ gegeben. Ein Floh hüpft auf dieser Strecke nach folgenden Regeln umher: Er startet in der Mitte (oder bei $\frac{2}{3}$) und wirft eine Münze. Bei Kopf spring er in Richtung A und zwar genau $\frac{2}{3}$ der Entfernung bis A, Bei Zahl springt er in Richtung B und zwar genau $\frac{2}{3}$ der Entfernung bis B. Diese Regel wird beliebig oft wiederholt. Wählt man A=0 und B=1, erhält man folgendes Schema:

Kopf: $x_{neu} = \frac{1}{3} \cdot x_{alt}$
Zahl: $x_{neu} = x_{alt} + \frac{2}{3} \cdot (1 - x_{alt}) = \frac{2}{3} + \frac{1}{3} \cdot x_{alt}$
Stellt man diese Folge graphisch dar, so entsteht nach und nach die Cantor-Menge. Ein Programm hierzu ist in 9.6 angegeben.
Startet der Floh auf einem Punkt der Cantor-Menge, z.B. $x_0 = \frac{2}{3}$, so ergibt sich folgende Folge, für die Münzwürfe KKZKZ... $x_0 = \frac{2}{3}$
$x_1 = \frac{1}{3} \cdot x_0 = \frac{1}{3} \cdot \frac{2}{3} = \frac{2}{9}$
$x_2 = \frac{2}{3} + \frac{1}{3} \cdot x_1 = \frac{2}{3} + \frac{1}{3} \cdot \frac{2}{9} = \frac{20}{27}$

[1] Waclaw Sierpinski (1882-1969)

$x_3 = \frac{1}{3} \cdot \frac{20}{27} = \frac{20}{81}$

Betrachtet man diese Zahlen im Ternärsystem, so stellt man fest, dass die Ziffer 1 nicht vorkommt und dass sich von Schritt zu Schritt eine Null (bei Kopf) oder eine Zwei (bei Zahl) hinter dem Komma dazwischenschiebt:

$x_0 = \frac{2}{3} = 2 \cdot 3^{-1} = 0,2_{TER}$
$x_1 = \frac{2}{9} = 0 \cdot 3^{-1} + 2 \cdot 3^{-2} = 0,02_{TER}$
$x_2 = \frac{20}{27} = 2 \cdot 3^{-1} + 0 \cdot 3^{-2} + 2 \cdot 3^{-3} = 0,202_{TER}$
$x_2 = \frac{20}{81} = 0 \cdot 3^{-1} + 2 \cdot 3^{-2} + 0 \cdot 3^{-3} + 2 \cdot 3^{-4} = 0,0202_{TER}$

9.2.2 Sierpinski Dreick

Ein Archäologe hat ein dreieckiges Gebiet abgesteckt, in dem er Dino-Knochen vermutet. Da er keine Ahnung hat wo, fängt er an einem beliebigen Ort im Dreieck an zu graben. Den nächsten Ort wäht er aus, indem er zuerst eine Ecke auswählt und dann den Mittelpunkt zwischen dieser Ecke und seiner aktuellen Position als neuen Grabungsort bestimmt. Trägt man die Grabungsorte auf, so entsteht nach und nach das Sierpinski-Dreieck. Ein Programm hierzu ist in 9.6 angegeben.

9.2.3 Der Farn

Zur Erzeugung des Farns wird ausgehend von einem Startpunkt (x_0, y_0) eine von vier affinen Abbildung ausgewählt, die auf den Punkt losgelassen wird. In jedem Schritt wird zufällig eine der vier Abbildungen ausgewählt. Um ein gleichmäßiges Bild zu erhalten, wird eine Abbildung umso häufiger ausgewählt, je größer ihr Bild (ihre Determinante) ist, das sie erzeugt. Die Abbildungen:

$$\begin{pmatrix} x_{neu} \\ y_{neu} \end{pmatrix} = \begin{pmatrix} 0,85 & 0,04 \\ -0.04 & 0,85 \end{pmatrix} \cdot \begin{pmatrix} x_{alt} \\ y_{alt} \end{pmatrix} + \begin{pmatrix} 0 \\ 1,6 \end{pmatrix}$$

$$\begin{pmatrix} x_{neu} \\ y_{neu} \end{pmatrix} = \begin{pmatrix} 0,2 & -0,26 \\ 0,23 & 0,22 \end{pmatrix} \cdot \begin{pmatrix} x_{alt} \\ y_{alt} \end{pmatrix} + \begin{pmatrix} 0 \\ 1,6 \end{pmatrix}$$

$$\begin{pmatrix} x_{neu} \\ y_{neu} \end{pmatrix} = \begin{pmatrix} -0,15 & 0,28 \\ 0,26 & 0,24 \end{pmatrix} \cdot \begin{pmatrix} x_{alt} \\ y_{alt} \end{pmatrix} + \begin{pmatrix} 0 \\ 0,44 \end{pmatrix}$$

$$\begin{pmatrix} x_{neu} \\ y_{neu} \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0,16 \end{pmatrix} \cdot \begin{pmatrix} x_{alt} \\ y_{alt} \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

Dieses Verfahren zur Erzeugung selbstähnlicher Abbildungen nennt man iteriertes Funktionensystem (IFS). Ein Programm hierzu ist in 9.6 angegeben.

9.3 Mehrfach-Verkleinerungs-Kopierer, MRCM

Man kann selbstähnliche Fraktale auch mit einem gedachten Mehrfach-Verkleinerungs-Kopierer (Multiple Reduction Copy Machine, MRCM) erzeugen. Denken wir uns einen Kopierer, der das Original verkleinert und es dann dreimal auf die Kopie bringt, wobei die verkleinerten Bilder im Dreieck angeordnet werden (Abbildung 9.5). Nimmt man die enstandene Kopie als neue Vorlage und wiederholt dieses Verfahren, so erscheint wieder das Sierpinski-Dreieck, unabhängig davon, was für ein Bild ursprünglich auf dem Original war.

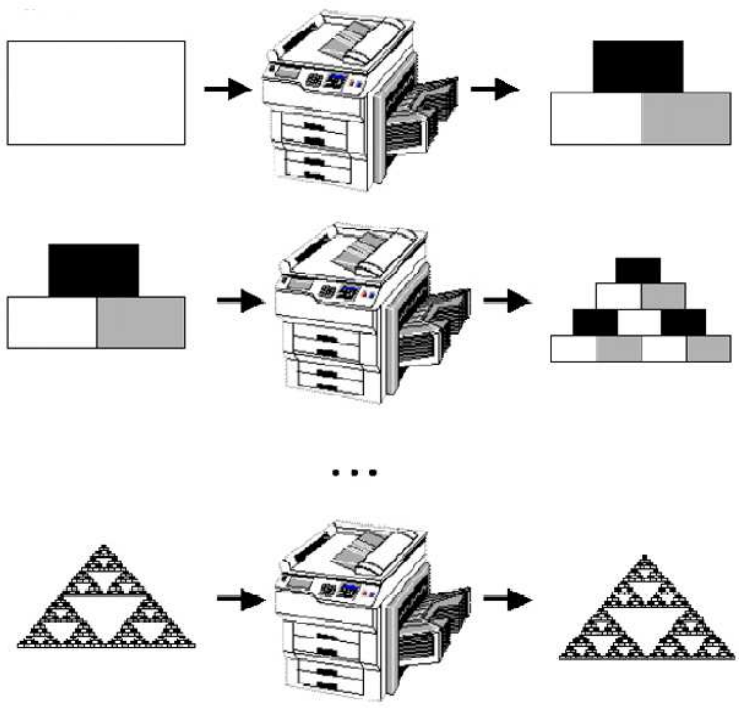


Abbildung 9.5: Entstehung des Sierpinski-Dreiecks mit dem Mehrfach-Verkleinerungs-Kopierer .

Stellt man sich nun einen Kopierer vor, der aus einem Quadrat in der ersten Stufe das Bild in Abbildung 9.6, rechts, erzeugt so entsteht bei wiederholter Anwendung

das Bild in Abbildung 9.6, rechts.

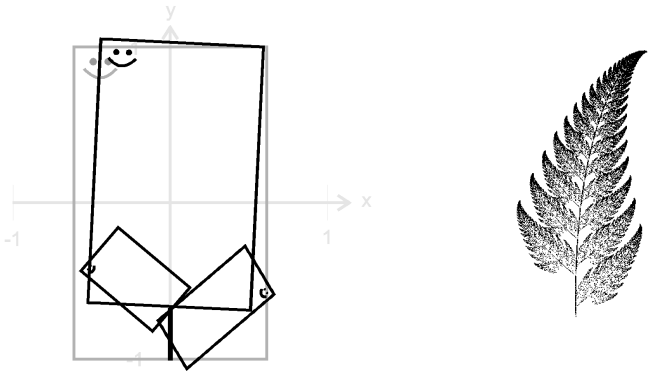


Abbildung 9.6: Entstehung des Farns. Die Vorschrift des Kopierers (links) und das Limesbild (rechts).

9.4 Die Mandelbrot-Menge

Die Mandelbrot-Menge ist nach Benoit B. Mandelbrot (1924-) benannt und wird manchmal auch als Apfelmännchen bezeichnet. Sie ist eine Teilmenge der komplexen Ebene $\mathbb{C}$. Die komplexe Ebene besteht aus komplexen Zahlen z, die sich aus einem Realteil a und einem Imaginärteil b zusammensetzen:

$$z = a + i \cdot b \qquad \text{mit} \qquad i = \sqrt{-1}$$

Der Betrag einer komplexen Zahl beträgt $|z| = \sqrt{a^2 + b^2}$
Die Mandelbrot-Menge ist wie folgt definiert:

$$M = \{c \in \mathbb{C} \mid (z_n) \text{ bleibt beschränkt}, \; z_{n+1} = z_n^2 + c, z_0 = c\}$$

Praktisch kann man die Konvergenz bzw. die Divergenz bestimmen, indem man für jeden Punkt der Ebene nachschaut, ob die Werte der Iteration den Kreis um Null mit dem Radius 2 nach einer bestimmten Zeit verlassen.
Hierzu bestimmt man den Abstand der komplexen Zahl vom Ursprung und überprüft, ob dieser kleiner als zwei ist: $|z_n - 0| < 2$
Nach einer bestimmten Zeit bedeutet hierbei, dass man eine Anzahl an Iterationsschritten vorgibt. Bleiben alle Werte der Iteration innerhalb des Kreises, so zäht man den Ausgangspunkt zur Menge. Je größer man die Anzahl wählt, desto genauer kann man die Menge bestimmen.

Ein Bild der Mandelbrot-Menge ist in Abbildung **??** gegeben. Ein Programm hierzu findet sich in 9.6. Die hübschen Farben, die man auf anderen Bildern häufig sieht ergeben sich, wenn man die Punkte, für die die Iteration divergiert (weiss in Abbildung **??**), je nach Divergenzgeschwindigkeit unterschiedlich einfärbt.

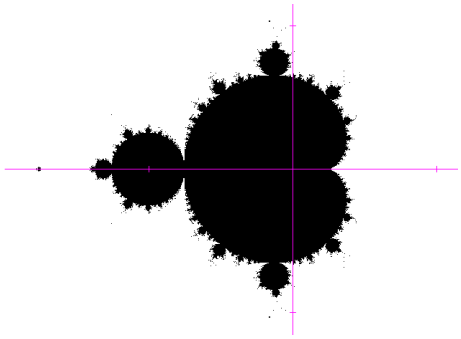


Abbildung 9.7: Mandelbrot-Menge.

Eng verwandt mit der Mandelbrot-Menge sind die Julia-Mengen. Die Julia-Menge ist nach Gaston M. Julia (1893- 1978) benannt. Die Julia-Menge zu einem Punkt c ist eine Teilmenge der komplexen Ebene, die durch

$$J_c = \{z \in \mathbb{C} \mid (z_n) \text{ bleibt beschränkt}, \;\; z_{n+1} = z_n^2 + c, z_0 = z\}$$

definiert ist.
Der Unterschied zur Mandelbrot-Menge besteht darin, dass ein Punkt c vorgegeben wird und für jeden Punkt z der Ebene nachgeschaut wird, ob die Iterationsfolge konvergiert. Man erhält also für jedes c eine Julia-Menge. Interessanterweise sind die Julia-Mengen, deren c-Wert der Mandelbrot-Menge angehört, zusammenhängende Mengen. Die Julia-Mengen, deren c-Wert ausserhalb der Mandelbrot-Menge liegen, bestehen aus isolierten Punkten. Unter diesem Aspekt kann man die Mandelbrot-Menge als Inhaltsverzeichnis der Julia-Mengen auffassen.

9.5 Anwendungen

Auf den ersten Blick erscheinen Fraktale als ganz hübsch, aber nicht sonderlich nützlich. In den letzten Jahren hat es aber eine ganze Reihe von praktischen Anwendungen gegeben:

- Die Küstenlänge von England hat die Dimension $D \approx 1,23$.

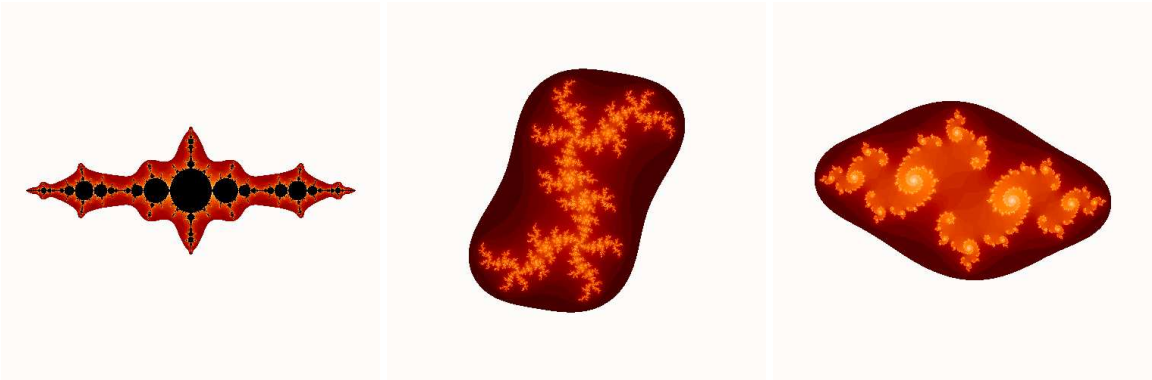


Abbildung 9.8: Julia-Mengen zu den Punkten c=1,28 (links) c= 0,334 - 0,528 i (Mitte) und c= -0,776 + 0,216 i (rechts).

- Misst man den Grundumsatz (Stoffwechsel) S von Lebewesen und trägt diesen doppelt-logarithmisch über der Körpermasse M auf, so ergibt sich ein linearer Zusammenhang. Daraus kann man die Dimension schließen, wenn man annimmt, dass die Masse proportional zum Volumen ist und das Volumen prortional zur dritten Potenz der linearen Ausdehnung. Man erhält eine Dimension $D \approx 2,25$.
- Die Dimension der Hirnhaut, d.h. der Hirnoberfläche ist $D \approx 2,79$.
- Die Verästelungen der Bronchien sind nahezu selbstähnlich. Es ergibt sich eine Dimension von $D \approx 2,8$. Bei der Dosierung von Medikamenten muss dies berücksichtigt werden

9.6 Programme

9.6.1 Cantor-Floh

SmallBasic -Programm zur Erzeugung der Cantor-Menge:

```
'Initialisierung
randomize(1)
cls
'Skalierungsfaktor fuer die Ausgabe
scale=400
'Anzahl der Schritte
N=100
'Startpunkt
x =2/3
 for j = 1 to N
 'Zufallszahl erzeugen (1 oder 2)
    p=int(2*rnd)+1
    if p=1 then
       x=x/3
    else
        x=2/3+x/3
    endif
    ' Linie zeichnen
    line 100+scale* x,100,100+scale* x,200,  color p
 next j
end
```

9.6.2 Sierpinski-Dreieck

SmallBasic -Programm zur Erzeugung der Sierpinski-Menge:

```
'Initialisierung
randomize(1)
cls
'Skalierungsfaktor fuer die Ausgabe
scale=4
'Anzahl der Schritte
N=10000
'Eckpunkte
DIM px(3)
DIM py(3)
px(1)=0
py(1)=0
px(2)=100
py(2)=0
px(3)=50
py(3)=87
'Startpunkt
x =50
y =50
 for j = 1 to N
    'Zufallszahl erzeugen (1,2 oder 3)
    p=int(3*rnd)+1
    x=(x+px(p))/2
    y=(y+py(p))/2
    pset 100+scale* x,400 -scale*y  color p
    next j
end
```

9.6.3 Farn

SmallBasic -Programm zur Erzeugung des Farns:

```
cls
scale=50
' Startwert
xalt = 1
yalt = 0
FOR i = 1 to 100000
   q = 100*rnd
  IF q<1 THEN
      x=0
      y=0.16*yalt
   ELSEIF q<85 and q>=1 THEN
     x = .85*xalt + .04*yalt
     y = -.04*xalt + .85*yalt + 1.6
   ELSEIF q>85 and q<93 THEN
      x = .2*xalt - .26*yalt
      y = .23*xalt +.22*yalt + 1.6
    ELSEIF q>=93 THEN
      x = -.15*xalt + .28*yalt
      y = .26*xalt +.24*yalt + .44
  ENDIF
  pset 300+scale*x,600-scale*y color 2
  xalt=x
  yalt=y
NEXT i
END
```

9.6.4 Mandelbrot-Menge

SmallBasic -Programm zur Erzeugung der Mandelbrotmenge.

```
' Iteration c=c*c+c
' c=c_re +c_im
cls
scale=200
minx=-2
maxx=0.5
miny=-1.2
maxy=1.2
acc=50
fine=0.005
FOR c_im=miny to maxy step fine
   FOR c_re=minx to maxx step fine
      'Iterationsstartwert
       zx=c_re
       zy=c_im
       count=0
       WHILE (zx*zx+zy*zy<4) AND count<acc
          tempx=zx*zx-zy*zy+c_re
          zy=2*zx*zy+c_im
          zx=tempx
           count=count+1
        WEND
        if count>=acc THEN
                  PSET 500+scale*c_re,250- scale*c_im
        endif
   NEXT
NEXT
END
```

10 Zelluläre Automaten

Bei der Beschreibung von Prozessen in der Natur spielt nicht nur die Veränderung der Zustandsgrößen im Laufe der Zeit eine Rolle. Häufig möchte man zusätzlich auch Informationen über die räumliche Verteilung haben. Stellt man sich eine Rasenfläche vor, und möchte man die Grasmenge auf dieser Fläche modellieren, so kann man natürlich ein Modell entwickeln, dass die Grasmenge auf dieser Fläche im Laufe der Jahreszeiten beschreibt. Dann hat man aber keinerlei Informationen darüber, ob auf dieser Rasenfläche an einigen Stellen braune Stellen oder dicke Grasbüschel existieren. Hierzu benötigt man ein Modell, dass die Grasfläche räumlich beschreibt. Hierzu kann man die Rasenfläche zum Beispiel in Quadrate einteilen. Man kann nun Wachstumsregeln aufstellen, die das Graswachstum beschreiben. Ist z.B. ein Quadrat von braunen Stellen umgeben, d.h., dass auf den Nachbarquadraten sehr wenig Gras ist, so wird das Gras auch in der Mitte schlecht wachsen, da der Schutz vor Wind fehlt. Sind um ein Quadrat dicke Grasbüschel, so werden die Nährstoffe knapp und auch dann kann das Gras schlecht wachsen.

10.0.5 Conway's Life

Ein erstes solches Modell, genannt LIFE, wurde von Conway im Jahre 1970 zur Beschreibung einer fiktiven Bevölkerung beschrieben. Jedes Quadrat, auch Zelle genannt, kann hierbei zwei Zustände annehmen, tot (0) oder lebendig (1). Conway hat nun folgende Regeln aufgestellt:

1. Eine Zelle wird geboren, wenn sie drei lebende Nachbarn hat.
2. Eine Zelle bleibt am Leben, wenn sie zwei oder drei lebende Nachbarn hat.
3. Eine Zelle stirbt sie an Vereinsamung oder Überbevölkerung, wenn sie weniger als zwei oder mehr als drei lebende Nachbarn hat.
4. Nachbarn sind die 8 Zellen um eine Zelle herum.

Mit diesen Regeln ergeben sich interessante Ergebnisse. Es gibt Konstellationen, die sich über die Zeit nicht ändern, andere die Zyklen durchlaufen, welche die sich über das Feld bewegen (Gleiter) und solche, die in gewissen Abständen Gleiter aussenden.

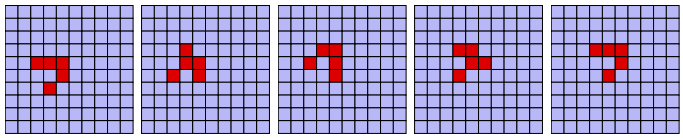


Abbildung 10.1: Gleiter in Life

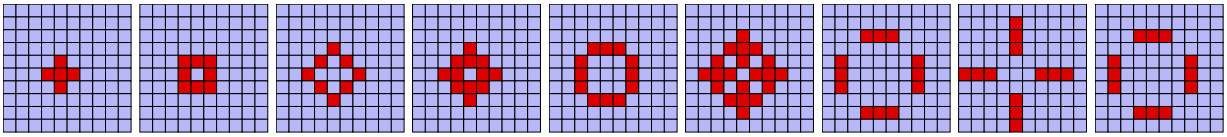


Abbildung 10.2: Zyklus in Life

SmallBasic -Programm für Conway's Life

Auch wenn es heute üblich ist, zelluläre Automaten in objektorientierten Sprachen wie z.B. Java zu programmieren, hier ein Programmbeispiel in SmallBasic :

```
' Anzahl der Zellen in einer Zeile
nmax=30
'Anzahl der Schritte
tmax = 100
RANDOMIZE(1)
'Initialisierung der Felder
DIM life(1 TO nmax,1 TO nmax)
DIM save(1 TO nmax,1 TO nmax)
'Skalierungsfaktor fuer die Ausgabe
scale=10
'Zufaelliger Anfangszustand
FOR i=1 TO nmax
   FOR j=1 TO nmax
     life(i,j)=int(2*RND)
   NEXT j
NEXT i
' Zeitschleife
FOR t=1 TO tmax
CLS
FOR i=1 TO nmax
   FOR j=1 TO nmax
      ' Ausgabe der lebenden Zellen
```

```
      IF life(i,j)=1 THEN  CIRCLE 100+scale*i,500 -scale*j , scale/2  FILLED
      ' Umspeichern
      save(i,j)=life(i,j)
      life(i,j)=0
  NEXT j
NEXT i

FOR i=1 TO nmax
   FOR j=1 TO nmax
'Bestimmung der Nachbarindizes
   k= i-1
   l= j-1
   m= i+1
   n= j+1
' Setzen der Randindizes
      IF i=1 THEN k=nmax
      IF i=nmax THEN m=1
      IF j=1 THEN l=nmax
      IF j=nmax THEN n=1
' Bestimmung der Nachbarn von i,j
    nachbarn= save(k,l)+save(i,l)+save(m,l)+save(k,j)
    nachbarn=nachbarn+save(m,j)+save(k,n)+save(i,n)+save(m,n)
'Eine Zelle wird bei 3 Nachbarn geboren
'und  ueberlebt bei 2 oder 3 Nachbarn
     IF nachbarn=3  THEN life(i,j)=1
     IF nachbarn=2  THEN life(i,j)=save(i,j)
   NEXT j
NEXT i
NEXT t
END
```

10.0.6 Per Bak's Sandhaufen

Ein weiteres berühmtes Beispiel ist der Sandhaufen von Per Bak. Auf einen Sandhaufen wird ein Sandkorn gestreut. Nun gibt es zwei Möglichkeiten. Entweder das Sandkorn bleibt liegen wo es hingefallen ist, oder es löst eine Lawine aus. Man nimmt nun an, dass das Sandkorn liegen bleibt, wenn weniger als 3 Sandkörner an

der Stelle liegen. Eine Lawine wird ausgelöst, wenn mehr als drei Sandkörner an der Stelle liegen. Kommt ein viertes hinzu wird der Sand auf die Nachbarzellen verteilt. Es wird jeweils ein Korn auf die Zellen rechts und links und oben und unten verteilt. Diese können dann weiter abrutschen. Man kann nun untersuchen ,wie lang die Lawinen werden. Immer dann, wenn keine Lawine mehr rollt, wird ein neues Sandkorn auf die Fläche ge gestreut. An der Rändern fallen die Sandkörner herunter

10.0.7 Zirkulärer Raum

Der zirkuläre Raum ist ein berühmtes Beispiel für Selbstorganisation. Nach einer geringen Anzahl von Schritten bilden sich Strukturen heraus.

- Es gibt N mögliche Zustände
- Der Zustand der Zelle wird um Eins erhöht, wenn mindestens ein Nachbar den Zustand der Zelle plus Eins hat.
- Jede Zelle hat 4 Nachbarn (links, rechts, oben und unten)
- Der Zustand 0 wird mit dem Zustand N gleichgesetzt

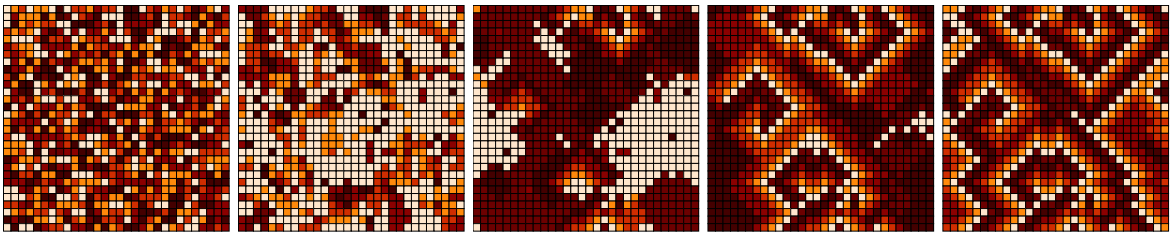


Abbildung 10.3: Selbstorganisation im zirkulären Raum mit N=6 Zuständen. Zwischen den Bildern liegen jeweils 6 Generationen

10.0.8 Charakteristika von zelluären Automaten

Allgemein kann man die Charakteristika von zelluären Automaten wie folgt beschreiben:

- Entwicklung in Raum und Zeit
- diskrete Anzahl an Zellen
- endliche Anzahl an Zuständen für jede Zelle (kann man aufweichen)
- Änderung der Zustände in diskreten Zeitschritten
- Zustand hängt von den Nachbarzellen ab.

10.0.9 Nachbarschaftsbeziehungen

Der Zustand einer Zelle hängt von den Zuständen seiner Nachbarn ab. Man kann verschiedene Nachbarschaftsbeziehungen betracheten.

- 4 Nachbarn (oben,unten, rechts und links)
- 8 Nachbarn (alle direkt angrenzenden Zellen)
- die Zelle selbts kann zu den nachbarn gezäht werden
- entferntere Zellen werden hinzugenommen

Randbedingungen

Man kann, wie bei Per Bak die Ränder offen lassen, so dass die Randzellen einfach weniger Nachbarn haben. In diesem Fall wird der Zustand der Randzellen je nach Automat anders ausfallen als der der Zellen in der Mitte. Will man dies vermeiden schliesst man das Feld zu einem Torus. Dann haben alle Zellen gleich viele Nachbarn.

A Funktionen

Eine Funktion f ist eine Vorschrift, die jedem Element einer Menge D genau ein Element der Menge W zuordnet. Die Menge D heisst Definitionsbereich, die Menge W Wertebereich:

$$\begin{array}{rcl} f : D & \longrightarrow & W \\ x & \mapsto & f(x) \end{array} \tag{A.1}$$

x heisst unabhängige Variable oder Argument. Eine Funktion wird auch Abbildung genannt.

Die Menge aller Punkte $G := \{(x, f(x)) | x \in D\}$ der Funktion (A.1) heisst Graph der Funktion.

Beispiel A.0.1

$$\begin{array}{rcl} f : [0,5] & \longrightarrow & \mathbb{R} \\ x & \rightarrow & x^2 \end{array} \tag{A.2}$$

Das Argument x ist anschaulich gesehen ein Platzhalter und ist beliebig durch einen anderen Buchstaben austauschbar. Durch

$$\begin{array}{rcl} f : [0,5] & \longrightarrow & \mathbb{R} \\ t & \rightarrow & t^2 \end{array}$$

ist dieselbe Funktion wie in (A.2) definiert.

In der Schule schreibt man statt $f(x)$ häufig einfach y. Wenn klar ist, welches in der Vorschrift die unabhängige Variable ist, so ist das ok:

$$y = 5 \cdot x^2 \tag{A.3}$$

Aber was ist,wenn die Vorschrift $y = a \cdot b^2$ geben ist. Man kann so nicht erkennen, ob a, b oder sogar beide als Argumente dienen sollen. Möglicherweise ist a ein Parameter, der einen festen Wert hat, und b das Argument oder umgekehrt. Daher

wird das Argument in der Vorschrift mit angegeben:

$$y(b) = a \cdot b^2$$

Ist nun $a = 5$, so haben wie dieselbe Vorschrift wie in (A.3).

Nun gibt es einige Konventionen, die aber nicht strikt eingehalten werden:

So weiss man im Allgemeinen, dass bei $y = mx + b$ eine Geradengleichung gemeint ist, mit dem Argument x, der Steigung m und dem Abzissenwert b. Meistens ist, wenn nicht anders angegeben x die unabhängige Variable.

In der Physik gibt es häufig Funktionen, in denen t als Argument auftritt. In den meisten Fällen ist damit die Zeit gemeint.

Anmerkung für Analytiker: Bildet man die Ableitung einer Funktion, so ist mit der Schreibweise y' die Ableitung nach dem (einzigen) Argument gemeint, dies ist meistens x. Insbesondere beschreibt $f'(x)$ die Ableitung der Funktion f nach x. Will man dies besonders hervorheben so schreibt man $\frac{d}{dx} f(x)$. In der Physik wird häufig die Ableitung nach der Zeit, die sogenannte Zeitableitung, mit einem Punkt dargestellt:

$$\dot{f}(t) := \frac{d}{dt} f(t) \, .$$

Ist der Definitionsbereich einer Abbildung $\mathbb{N}$, so nennt man die Abbildung eine Folge und schreibt

$$\begin{aligned} a : \mathbb{N} &\longrightarrow W \\ n &\mapsto a_n \, . \end{aligned}$$

oder kurz $(a_n)_{n \in \mathbb{N}}$.

A.1 Polynome

Abbildungen der Form $p(x) = a_m \cdot x^m + \cdots + a_1 \cdot x + a_0$, $m \in \mathbb{N}$ heissen Polynome. Berühmtestes Beispiel ist die Normalparabel $p(x) = x^2$ mit $m = 2$, $a_2 = 1$ und $a_1 = a_0 = 0$.

A.2 Periodische Funktionen – Winkelfunktionen

Eine Funktion heisst periodisch mit der Periodenlänge p , wenn für alle $x \in D$ $f(x+p) = f(x)$ gilt. Beispiele für periodische Funktionen sind die Winkelfunktionen (trigonometrische Funktionen) Sinus und Kosinus.

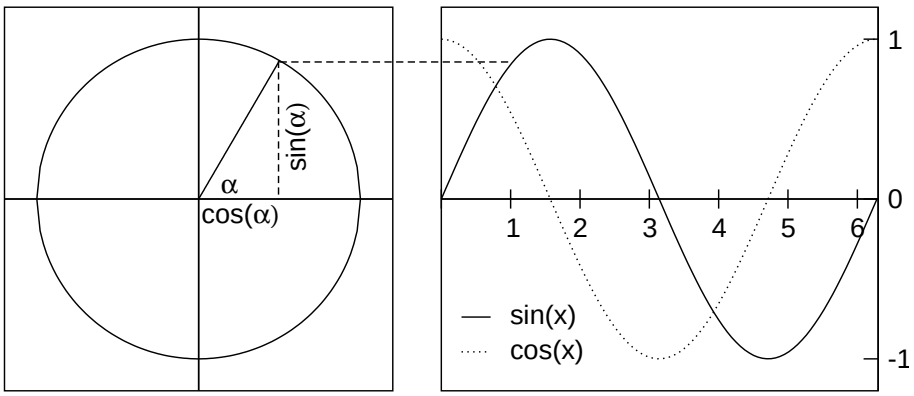


Abbildung A.1: Der Einheitskreis und die Winkelfunktionen

Betrachtet man im Einkeitskreis, das in Abbildung A.1 dargestellte Dreieck, so ist die Länge der Hypotenuse 1. Der resultierende Abschnitt auf der x-Achse ist also der Kosinus, des Winkels α, der Abschnitt auf der y-Achse ist der Sinus.

Die Steigung der Geraden beträgt $\frac{\sin(\alpha)}{\cos(\alpha)} = \tan(\alpha)$.

Das Argument der Winkelfunktionen kann sowohl in Grad als auch in Bogenmaß (Radiant) angegeben werden. Ein Vollkreis von 360° entspricht dabei 2πrad.

Wichtige Werte der Sinus und Kosinusfunktion:

Grad	0	30	45	60	90	180	270	360
Bogenmaß	0	$\pi/6$	$\pi/4$	$\pi/3$	$\pi/2$	π	$3\pi/2$	2π
Sinus	0	$1/2$	$\sqrt{2}/2$	$\sqrt{3}/2$	1	0	-1	0
Kosinus	1	$\sqrt{3}/2$	$\sqrt{2}/2$	$1/2$	0	-1	0	1

Eigenschaften der Sinus und Kosinusfunktion:

Periodenlänge 2π	$\sin(x) = \sin(x+2\pi)$ $\cos(x) = \cos(x+2\pi)$
Sinus ist symmetrisch zum Ursprung	$\sin(-x) = -\sin(x)$
Kosinus ist symmetrisch zur y-Achse	$\cos(x) = \cos(-x)$
sind gegeneinander um $\pi/2$ verschoben	$\cos(x) = \sin(x+\pi/2)$
Schnittpunkte bei $x = \pi/4 + n \cdot \pi, n \in \mathbb{Z}$	$\sin(\pi/4) = \cos(\pi/4)$

Bemerkung: Berechnet man Sinus und Kosinus mit dem Taschenrechner so muss man aufpassen, dass die Einstellung stimmt. Ist der Taschenrechner auf Gradmaß (DEG) eingestellt, muss man den Winkel in Grad eingeben, steht er auf Bogenmaß (RAD) so muss er in Bogenmaß angegeben werden.

B Weiteres

B.1 Geometrische Summe

Satz B.1.1 Geometrische Summe
Für alle $n \in \mathbb{N}$ und $c \neq 1$ gilt

$$\sum_{k=0}^{n-1} c^k = 1 + c + c^2 + \ldots + c^{n-2} + c^{n-1} = \frac{c^n - 1}{c - 1}$$

Beweis Multiplizieren der linken Seite mit $c-1$ ergibt

$$\begin{aligned} & c^{n-1} \cdot (c-1) + c^{n-2} \cdot (c-1) + \ldots + c^2 \cdot (c-1) + c \cdot (c-1) + 1 \cdot (c-1) \\ = \; & c^n - c^{n-1} + c^{n-1} - c^{n-2} + \ldots + c^3 - c^2 + c^2 - c + c - 1 \\ = \; & c^n - 1 \end{aligned}$$

■

B.2 Modulo-Rechenregeln

Definition B.2.1 Modulo
Seien $a, b \in \mathbb{Z}$, $n \in \mathbb{N}$. a heisst kongruent zu b modulo n, in Zeichen:

$$a \equiv b \pmod{n},$$

genau dann, wenn n die Differenz $a - b$ teilt (in Zeichen: $n \mid a - b$).

Es gibt also ein $k \in \mathbb{Z}$, so dass $a = k \cdot n + b$ gilt.

Modulo ist eine Äquivalenzrelation, d.h. reflexiv, symmetrisch und transitiv. Die kleinste nicht-negative Zahl in jeder Restklasse heisst Repräsentant. Der Kongruenzbegriff kann als Verfeinerung des Teilbarkeitsbegriffs aufgefasst werden, den $n \mid a$ ist gleichbedeutend mit $a \equiv 0 \pmod{n}$. In den Fällen, in denen die Division durch n nicht aufgeht, werden Reste charakterisiert.

Beispiel B.2.1 Tageszeiten
Ein Beispiel für Modulo-Rechnungen sind die Tageszeiten, die durch die Ziffern 1 bis 12 bzw. 1 bis 24 dargestellt werden. □

Definition B.2.2 Modulo-Operator
Seien $a, b, n \in \mathbb{Z}$, $n > 1$ und $0 \leq b < n$.
$a \bmod n = b$, genau dann, wenn $a \equiv b \pmod{n}$

Der Modulo-Operator gibt den Rest bei Divison durch n an.

Satz B.2.1 Seien $a, b, c, d, n \in \mathbb{Z}$, $n > 1$.
Aus $a \equiv b \pmod{n}$ und $c \equiv d \pmod{n}$ folgt:

$a + c \equiv b + d \pmod{n}$
$a \cdot c \equiv b \cdot d \pmod{n}$

Insbesondere gilt für $j \in \mathbb{N}$: $a^j \equiv b^j \pmod{n}$

Satz B.2.2 Seien $a, c, n \in \mathbb{Z}$, $n > 1$.
Ist $ggT(n, c) = 1$, so gilt:
Aus $a \cdot c \equiv b \cdot c \bmod n$ folgt $a \equiv b \bmod n$

B.3 Euklidscher Algorithmus

Der Euklidsche Algorithmus ist ein Verfahren zur Bestimmung des ggT zweier Zahlen $a, b \in \mathbb{N}$. Wir starten, indem wir $r_0 := a$ und $r_1 := b$ setzen. Nun berechnen wir die Division mit Rest, wobei die $c_i \in \mathbb{N}$ sein sollen.

$$\begin{array}{lcll} r_0 & = & c_1 \cdot r_1 + r_2 & 0 < r_2 < r_1 \\ r_1 & = & c_2 \cdot r_2 + r_3 & 0 < r_3 < r_2 \\ \vdots & & \vdots & \\ r_{n-2} & = & c_{n-1} \cdot r_{n-1} + r_n & 0 < r_n < r_{n-2} \\ r_{n-1} & = & c_n \cdot r_n & \end{array}$$

Behauptung: $r_n = ggT(a,b)$

Beweis Sei $z \in \mathbb{Z}$ mit $z|a$ und $z|b$. Eine solche Zahl z existiert, da $z = 1$ die Bedingung erfüllt. Es gilt also $z|r_0$ und $z|r_1$. Damit muss nach der ersten Zeile auch $z|r_2$ gelten usw. , und somit auch $z|r_n$. Da dies für jeden Teiler von a und b gilt, gilt es auch für $z = ggT(a,b)$, also

$$ggT(a,b)|r_n \qquad \text{und damit} \qquad ggT(a,b) \leq r_n \, .$$

Wenn nun $r_n|a$ und $r_n|b$ gilt sind wir fertig, da dann $r_n \leq ggT(a,b)$ gilt.
Aus der letzten Zeile folgt $r_n|\, r_{n-1}$, aus der vorletzten $r_n|\, r_{n-2}$, ..., $r_n|\, r_1$,$r_n|\, r_0$.

Damit gilt $r_n = ggT(a,b)$.

Beispiel B.3.1 Bestimmung von $ggT(147,56)$

$$\begin{aligned} 147 &= 2 \cdot 56 + 35 \\ 56 &= 1 \cdot 35 + 21 \\ 35 &= 1 \cdot 21 + 14 \\ 21 &= 1 \cdot 14 + 7 \\ 14 &= 2 \cdot 7 \end{aligned}$$

Also $ggT(147,56) = 7$. □

B.4 Erweiterter Euklidscher Algorithmus

Um den privaten Schlüssel d beim RSA-Verfahren zu bestimmen, ist die Gleichung

$$e \cdot d \bmod (p-1)(q-1) = 1$$

bei gegebenem e,p und q zu lösen.

Beispiel B.4.1 Es sei $e = 41$, $p = 17$, $q = 13$, dann ist $(p-1)(q-1) = 192$.
Zu lösen ist also

$$41d \bmod 192 = 1$$

Zuerst führen wir den Euklidsche Algorithmus für 192 und 41 durch:

$$\begin{aligned} 192 &= 4 \cdot 41 + 28 \\ 41 &= 1 \cdot 28 + 13 \\ 28 &= 2 \cdot 13 + 2 \\ 13 &= 6 \cdot 2 + 1 \end{aligned}$$

Nun löst man die Gleichungskette umgekehrt auf:

$$\begin{aligned} 1 &= 13 - 6 \cdot 2 && \text{Umformung der 4. Zeile} \\ &= 13 - 6 \cdot (28 - 2 \cdot 13) && \text{Umformung der dritten Zeile und Einsetzen} \\ &= 13 \cdot 13 - 6 \cdot 28 && \text{Zusammenfassen} \\ &= 13 \cdot (41 - 1 \cdot 28) - 6 \cdot 28 && \text{Umformen der zweiten Zeile und Einsetzen} \\ &= 13 \cdot 41 - 19 \cdot 28 && \text{Zusammenfassen} \\ &= 13 \cdot 41 - 19 \cdot (192 - 4 \cdot 41) && \text{Umformen der ersten Zeile und Einsetzen} \\ &= 89 \cdot 41 - 19 \cdot 192 && \text{Zusammenfassen} \end{aligned}$$

Damit gilt $89 \cdot 41 = 19 \cdot 192 + 1$, also $41 \cdot 89 \bmod 192 = 1$, und es gilt $d = 89$. □

B.5 Mengenlehre

Definition B.5.1 Gegeben seien zwei Mengen A und B

- Die Menge A heisst genau dann **Teilmenge** von B, wenn jedes Element x von A auch Element von B ist. (in Zeichen $A \subseteq$B). Ist A Teilmenge von B und $A \neq B$, so heisst A **echte Teilmenge** von B (in Zeichen $A \subset B$).
- Die Menge aller Elemente, die zu A und B gehören, heisst **Schnittmenge** von A und B (in Zeichen $A \cap B$, gelesen: A geschnitten B):

  $$A \cap B = \{x | x \in A \text{ und } x \in B\}$$

- Die Menge aller Elemente, die zu A oder B gehören, heisst **Vereinigungsmenge** von A und B (in Zeichen $A \cup B$, gelesen: A vereinigt B):

  $$A \cup B = \{x | x \in A \text{ oder } x \in B\}$$

- Die Menge aller Elemente, die zu A und nicht zu B gehören, heisst **Differenzmenge** (in Zeichen $A \setminus B$, gelesen: A ohne B):

  $$A \setminus B = \{x | x \in A \text{ und } x \notin B\}$$

- Ist B Teilmenge von A ($B \subseteq$A), so heisst die Differenzmenge $A \setminus B$ auch **Komplementärmenge** von B bezogen auf A (in Zeichen $\overline{B}$, gelesen B quer).
- A und B heissen **disjunkt**, wenn ihr Durchschnitt leer ist ($A \cap B = \emptyset$

Definition B.5.2 Sei $\Omega \neq \emptyset$, Ω endlich.

- Die Menge aller Teilmengen von Ω heisst **Potenzmenge** von Ω und wird mit $\mathcal{P}(\Omega)$ bezeichnet.

Satz B.5.1 Die Mächtigkeit der Potenzmenge $|\mathcal{P}(\Omega)|$ einer n-elementigen Menge Ω beträgt 2^n.

Beweis durch vollständige Induktion
Induktionsverankerung $n = 1$:
Besteht Ω aus einem Element, so ist $\{\emptyset, \Omega\}$ die Potenzmenge von Ω. Damit gilt $|\mathcal{P}(\Omega)| = 2$
Induktionsschritt von $n \to n+1$:
Sei die Mächtigkeit der Potenzmenge einer n-elementigen Menge 2^n. Sei Ω n+1-elementig und sei $x \in \Omega$. Dann ist die Mächtigkeit der Potenzmenge der Menge $\Omega \setminus \{x\}$ nach Induktionsvoraussetzung 2^n. Wir können nun zu jeder Menge in $\mathcal{P}(\Omega \setminus \{x\})$ x hinzufügen und erhalten weitere 2^n Mengen. Damit gilt $|\mathcal{P}(\Omega)| = 2 \cdot 2^n = 2^{n+1}$. ■

Satz B.5.2 Mengengesetze
Seien A, B, C Mengen dann gilt:

Kommutativgesetz
$A \cup B = B \cup A$
$A \cap B = B \cap A$

Assoziativgesetz
$A \cup (B \cup C) = (A \cup B) \cup C$
$A \cap (B \cap C) = (A \cap B) \cap C$

Distributivgesetz
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

Gesetz von de Morgan
$\overline{A \cup B} = \overline{A} \cap \overline{B}$
$\overline{A \cap B} = \overline{A} \cup \overline{B}$

$A \cup \emptyset = A$
$A \cap \emptyset = \emptyset$