Skript
Mathematik & Informatik

Sammlung von Theoremen, Definitionen, Algorithmen, Code-Schnipseln
und Strukturen
für die behandelten Themen in den Leistungskursen
Mathematik und Informatik

Nottuln, 2013

Autor

Alexander Pietz
Stand: 13. März 2014

Hans-Böckler Berufskolleg
Münster

Inhaltsverzeichnis

Abbildungsverzeichnis

Teil I.

Mathematik

1. Analysis

1.1. Differenzialrechnung

1.1.1. Änderungsraten

1.1.2. Ableitungsfunktion

1.1.3. Kurvendiskussion

1.1.4. Gauß Algorithmus

1.2. Integralrechung

Die Integralrechnung ist die Umkehrung der Differentiation und dient zur Berechnung von Flächen. Man unterscheidet zwischen unbestimmten und das bestimmten Integralen:

1.2.1. Das bestimmte Integral

Das bestimmte Integral einer Funktion ordnet dieser einen Zahlwert zu. Bildet man das bestimmte Integral einer reellen Funktion in einer Variablen, so lässt sich das Ergebnis im zweidimensionalen Koordinatensystem als Flächeninhalt der Fläche, die zwischen dem Graphen der Funktion, der x-Achse und den begrenzenden Parallelen zur y-Achse liegt, deuten. Hierbei zählen Flächenstücke unterhalb der x-Achse negativ. Man spricht vom orientierten Flächeninhalt. Diese Konvention wird gewählt, damit das bestimmte Integral eine lineare Abbildung ergibt, was sowohl für theoretische Überlegungen als auch für konkrete Berechnungen eine zentrale Eigenschaft des Integralbegriffs darstellt.

1.2.2. Das unbestimmte Integral

tbd

2. Stochastik

Mit dem Wort „Zufall“ gibt der Mensch nur seiner Unwissenheit Ausdruck.

(Pierre Simon Marquis de Laplace)

2.1. Wahrscheinlichkeitsrechnung

2.1.1. Das Urnenexperiment

Beim **Urnenexperiment** wird ein fiktives Gefäß, eine *Urne*, mit einer Anzahl Kugeln gefüllt, welche anschließend zufällig gezogen werden. Damit ist gemeint, dass bei jedem Zug alle in der Urne befindlichen Kugeln die gleiche Wahrscheinlichkeit haben, ausgewählt zu werden (Laplace-Experiment). Dadurch kann die Bestimmung interessierender Wahrscheinlichkeiten auf die Lösung kombinatorischer Abzählprobleme zurückgeführt werden. Viele wichtige Wahrscheinlichkeitsverteilungen, wie beispielsweise die Binomialverteilung, können mit Hilfe von Urnenmodellen hergeleitet und veranschaulicht werden.

Lemma 2.1.1. In der Urne befinden sich n Kugeln, von denen k gezogen werden.

Das Ziehen kann auf zwei verschiedene Arten erfolgen:

- Eine Kugel wird gezogen und wieder zurückgelegt.
- Nach dem Ziehen der Kugel wird diese nicht wieder zurückgelegt.

2.1.2. Abzählende Kombinatorik

Die abzählende Kombinatorik ist ein Teilbereich der Kombinatorik, der sich mit der Bestimmung der Anzahl möglicher Anordnungen oder Auswahlen

- unterscheidbarer oder nicht unterscheidbarer Objekte (d. h. „ohne“ bzw. „mit“ Wiederholung derselben Objekte) sowie
- mit oder ohne Beachtung ihrer Reihenfolge (d. h. „geordnet“ bzw. „ungeordnet“)

beschäftigt. In der modernen Kombinatorik werden diese Auswahlen oder Anordnungen auch als Abbildungen betrachtet, so dass sich die Aufgabe der Kombinatorik in diesem Zusammenhang im Wesentlichen darauf beschränken kann, diese Abbildungen zu zählen. Für das Rechnen mit Wahrscheinlichkeiten auf der Basis des Wahrscheinlichkeitsbegriffs von Laplace bildet die Kombinatorik eine wichtige Grundlage.
Ein verblüffendes Phänomen der Kombinatorik ist, dass sich oftmals wenige Objekte auf vielfältige Weise kombinieren lassen. Beim Zauberwürfel können beispielsweise die

26 Elemente auf rund 43 Trillionen Arten kombiniert werden. Dieses Phänomen wird oft als kombinatorische Explosion bezeichnet und ist auch die Ursache für das so genannte Geburtstagsparadoxon.
Alles in allem gibt es also zunächst einmal drei (oder auch nur zwei) verschiedene Fragestellungen, die ihrerseits noch einmal danach unterteilt werden, ob es unter den ausgewählten Elementen auch Wiederholungen gleicher Elemente geben darf oder nicht. Ist ersteres der Fall, spricht man von Kombinationen, Variationen oder Permutationen mit Wiederholung, andernfalls solchen ohne Wiederholung. Stellt man sich schließlich vor, dass die ausgewählten Elemente dabei einer Urne oder Ähnlichem entnommen werden, wird dementsprechend auch von Stichproben mit oder ohne Zurücklegen gesprochen:

	Ohne Wiederholung bzw. Zurücklegen	Mit Wiederholung bzw. Zurücklegen
Mit Berücksichtigung der Reihenfolge und k = n	Permutation ohne Wiederholung	Permutation mit Wiederholung
Mit Berücksichtigung der Reihenfolge und k < n	Variation ohne Wiederholung	Variation mit Wiederholung
Ohne Berücksichtigung der Reihenfolge und k < n	Kombination ohne Wiederholung	Kombination mit Wiederholung

Permutation

Ohne Wiederholung Eine Permutation ohne Wiederholung ist eine Anordnung von n Objekten, die alle unterscheidbar sind. Nachdem es für das erste Objekt n Platzierungsmöglichkeiten gibt, kommen für das zweite Objekt nur noch $n-1$ Möglichkeiten in Betracht, für das dritte Objekt nur mehr $n-2$ und so weiter bis zum letzten Objekt, dem nur noch ein freier Platz bleibt. Die Anzahl der möglichen Permutationen von n Objekten wird demnach durch die Fakultät

$$n! = n \cdot (n-1) \cdot \ldots \cdot 1$$

angegeben.

Mit Wiederholung Eine Permutation mit Wiederholung ist eine Anordnung von n Objekten, von denen manche nicht unterscheidbar sind. Sind genau k Objekte identisch, dann sind diese auf ihren Plätzen vertauschbar, ohne dass sich dabei eine neue Reihenfolge ergibt. Auf diese Weise sind genau $k!$ Anordnungen gleich. Die Anzahl der Permutationen von n Objekten, von denen k identisch sind, ist demnach durch

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

gegeben.

Variation

Ohne Wiederholung Bei einer Variation ohne Wiederholung sollen k von n Objekten (mit $k \leq n$) auf k verfügbare Plätze platziert werden, wobei jedes Objekt nur höchstens einen Platz einnehmen darf. Es gibt für den ersten Platz n mögliche Objekte, für den

zweiten Platz $n-1$ Objekte usw. bis zum k-ten Platz, für den es noch $n-k+1$ mögliche Objekte gibt. Insgesamt gibt es also

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

mögliche Anordnungen.

Mit Wiederholung Bei einer Variation mit Wiederholung werden aus n Objekten k Objekte unter Beachtung der Reihenfolge ausgewählt, wobei Objekte auch mehrfach ausgewählt werden können. Nachdem jedes der n Objekte auf jedem der k Plätze der Auswahl erscheinen kann, gibt es demzufolge

$$\underbrace{n \cdot \ldots \cdot n}_{k\text{-mal}} = n^k$$

mögliche Anordnungen.

Kombination

Ohne Wiederholung Bei einer Kombination ohne Wiederholung geht man zunächst von einer Variation ohne Wiederholung aus, für die es bei k von n auszuwählenden Elementen $\frac{n!}{(n-k)!}$ Möglichkeiten gibt. Nun aber können die k ausgewählten Elemente ihrerseits auf $k!$ verschiedene Weisen angeordnet werden. Wenn diese verschiedenen Anordnungen allesamt keine Rolle spielen, also immer wieder als die gleiche Auswahl von Elementen gelten sollen, müssen wir das erhaltene Ergebnis noch einmal durch $k!$ teilen und erhalten damit nur noch

$$\frac{n!}{(n-k)!\,k!} = \frac{n(n-1)(n-2)\ldots(n-k+1)}{k!} = \binom{n}{n-k} = \binom{n}{k}$$

Möglichkeiten. Die Notation wird auch als *Binomialkoeffizient* bezeichnet.

Mit Wiederholung Sollen aus einer Menge von n Elementen k Elemente ausgewählt werden, wobei ihre Reihenfolge weiterhin ohne Belang sein soll, sie sich aber nun auch wiederholen dürfen, wie das z. B. beim Ziehen mit Zurücklegen möglich ist, ergibt sich für die Zahl der Möglichkeiten folgende Formel :

$$\frac{(n+k-1)!}{(n-1)!\,k!} = \binom{n+k-1}{k} = \binom{n+k-1}{n-1}$$

Der Binomialkoeffizient

Der **Binomialkoeffizient** ist eine mathematische Funktion, mit der sich eine der Grundaufgaben der Kombinatorik lösen lässt. Er gibt an, auf wie viele verschiedene Arten man k Objekte aus einer Menge von n verschiedenen Objekten auswählen kann (ohne Zurücklegen, ohne Beachtung der Reihenfolge). Der Binomialkoeffizient ist also die Anzahl der k-elementigen Teilmengen einer n-elementigen Menge.

Beispiel 2.1.1. "49 über 6ïst z. B. die Anzahl der möglichen Ziehungen beim Lotto (ohne Berücksichtigung der Zusatzzahl).

Ein Binomialkoeffizient hängt von zwei Zahlen n und k ab. Er wird mit dem Symbol $\binom{n}{k}$ geschrieben und als "n über k“, "k aus n“ oder "n tief k“ gesprochen. Die englische Abkürzung nCr für *from n choose r* findet sich als Beschriftung auf Taschenrechnern und somit auch auf dem TI.

Definition 2.1.1. Handelt es sich bei n um eine nichtnegative ganze Zahl mit $n \geq k$, so kann man die aus der Kombinatorik bekannte Definition verwenden:

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

$$\binom{n}{0} = \binom{n}{n} = 1$$

$$\binom{n}{1} = \binom{n}{n-1} = n$$

2.1.3. Zufallsgröße und Wahrscheinlichkeitsverteilung

In der Stochastik ist eine **Zufallsgröße** eine Variable, deren Wert vom Zufall abhängig ist. Eine Zufallsgröße lässt sich formal als Funktion beschreiben, die den Ergebnissen eines Zufallsexperiments Werte (so genannte Realisierungen) zuordnet.

Zufallsgröße $X = X(\omega)$ sind funktional abhängig von einer den Zufall repräsentierenden Größe ω. Zum Beispiel kann ω das zufällige Ergebnis eines Münzwurfs sein. Dann kann zum Beispiel eine Wette auf den Ausgang eines Münzwurfs mithilfe einer Zufallsgröße modelliert werden. Angenommen, es wurde auf Zahl gewettet, und wenn richtig gewettet wurde, wird 1 EUR ausgezahlt, sonst nichts. Sei X die Auszahlungssumme. Da der Wert von X vom Zufall abhängt, ist X eine Zufallsgröße. Sie bildet die Menge der Wurfergebnisse $\{\text{Kopf}, \text{Zahl}\}$ auf die Menge der möglichen Auszahlungsbeträge $\{0, 1\}$ ab:

$$X(\omega) = \begin{cases} 0, & \text{wenn } \omega = \text{Kopf}, \\ 1, & \text{wenn } \omega = \text{Zahl}. \end{cases}$$

Wettet man bei zwei Münzwürfen beide Male auf Kopf und bezeichnet die Kombination der Ausgänge der Münzwürfe mit $\omega = (\omega_1, \omega_2)$, so lassen sich beispielsweise folgende Zufallsgrößen untersuchen:

- $X_1(\omega) := X(\omega_1) \in \{0, 1\}$ als Auszahlung nach der ersten Wette,
- $X_2(\omega) := X(\omega_2) \in \{0, 1\}$ als Auszahlung nach der zweiten Wette,
- $S(\omega) := X(\omega_1) + X(\omega_2) \in \{0, 1, 2\}$ als Summe der beiden Auszahlungen.

Zufallsgrößen selbst werden üblicherweise mit einem Großbuchstaben bezeichnet (hier X_1, X_2, S), während man für die Realisierungen die entsprechenden Kleinbuchstaben verwendet (so beispielsweise für $\omega = (\text{Zahl}, \text{Kopf})$ die Realisierungen $x_1 = 1, x_2 = 0, s = 1$).
Im Beispiel hat die Menge $\Omega = \{\text{Kopf}, \text{Zahl}\}$ eine konkrete Interpretation. In der weiteren Entwicklung der Wahrscheinlichkeitstheorie ist es oft zweckmäßig, die Elemente von Ω als abstrakte Repräsentanten des Zufalls zu betrachten, ohne ihnen eine konkrete Bedeutung zuzuweisen, und dann sämtliche zu modellierende Zufallsvorgänge als Zufallsgröße zu erfassen.

Erwartungswert

Definition 2.1.2. Eine Zufallsgröße X nehme die Werte $a_1, a_2, .., a_m$ mit den Wahrscheinlichkeiten $P(X = a_1), P(X = a_2), ...P(X = a_m)$ an. Dann wird der zu erwartende Mittelwert $E(X)$ der Verteilung als *Erwartungswert der Zufallsgröße X* bezeichnet. Es gilt:

$$\mu = \mathrm{E}(X) = \sum_{i=1}^{m} a_i * P(X = a_i)$$

Varianz

Definition 2.1.3. Gegeben sei ein quantitatives Merkmal mit den Merkmalsausprägungen $x_1, x_2, .., x_m$ und den zugehörigen relativen Häufigkeiten $h(x_1), h(x_2), .., h(x_m)$. Dann gilt für die Varianz:

$$s^2 = (\sum_{i=1}^{m} x_i^2 * h(x_i)) - \mu^2$$

2.1.4. Satz von Bayes

Sei A ein Ereignis, das uns interessiert, und B eine Bedingung, unter der wir das Ereignis betrachten. Dann gilt:

Definition 2.1.4. *Die Wahrscheinlichkeit $P_B(A)$ für A unter der Bedingung B* berechnet sich wie folgt:

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

Mehrfeldtafel

Mehrfeldtafeln sind Tabellen, die die absoluten oder relativen Häufigkeiten von Kombinationen bestimmter Merkmalsausprägungen enthalten. Kontingenz hat dabei die Bedeutung des gemeinsamen Auftretens von zwei Merkmalen. Das bedeutet, es werden Häufigkeiten für mehrere miteinander durch 'und' oder 'sowie' verknüpfte Merkmale dargestellt. Diese Häufigkeiten werden ergänzt durch deren Randsummen, die die sogenannten **Randhäufigkeiten** bilden.

Vierfeldertafel

Unter einer **Vierfeldertafel** versteht man eine vereinfachte Kontingenztafel , die Zahlenwerte der möglichen Ergebnisse eines durchgeführten Tests auf einen Blick präsentiert.
Die Vierfeldtafel bildet sich nach dem *Satz von Bayes* wie folgt:

Merkmal	A	$\bar{A}$	Summe
B	$P(A \cap B)$	$P(A \cap B)$	$P(B)$
B	$P(A \cap B)$	$P(A \cap B)$	$P(B)$
Summe	$p(A)$	$P(\bar{A})$	1

Stochastische Unabhängigkeit

Stochastische Unabhängigkeit ist ein Konzept, welches die Vorstellung von sich nicht gegenseitig beeinflussenden Zufallsereignissen formalisiert. Sind zwei Ereignisse stochastisch unabhängig, dann ändert sich die Wahrscheinlichkeit dafür, *dass das eine eintritt, nicht, wenn das andere eintritt* (beziehungsweise nicht eintritt).
Insbesondere Ereignisse, die mit positiver Wahrscheinlichkeit eintreten und sich gegenseitig ausschließen oder bedingen, sind voneinander abhängig. Dass Ereignisse sich gegenseitig ausschließen, wird häufig mit deren Unabhängigkeit verwechselt.

Stehen die Wahrscheinlichkeiten in den Spalten oder in den Zeilen einer Vierfeldertafel im gleichen festen Zahlenverhältnis, dann sind die zugehörigen Merkmale voneinander unabhängig; sonst sind sie voneinander abhängig.

Gilt für zwei Ereignisse A,B, dass $P(A \cap B) = P(A) * P(B)$, d.h. also dass $P(B) = P_A(B)$, dann nennt man A,B **stochastisch voneinander unabhängig**, sonst **stochastisch voneinander abhängig**.

Sensitivität Die Sensitivität (auch Richtig-Positiv-Rate, Empfindlichkeit oder Trefferquote) gibt den Anteil der korrekt als positiv klassifizierten Objekte an der Gesamtheit der tatsächlich positiven Objekte an. Beispielsweise entspricht Sensitivität bei einer medizinischen Diagnose dem Anteil an tatsächlich Kranken, bei denen die Krankheit auch erkannt wurde.

Spezifität Die Spezifität (auch Richtig-Negativ-Rate oder kennzeichnende Eigenschaft) gibt den Anteil der korrekt als negativ klassifizierten Objekte an der Gesamtheit der in Wirklichkeit negativen Objekte an. Beispielsweise gibt die Spezifität bei einer medizinischen Diagnose den Anteil der Gesunden an, bei denen auch festgestellt wurde, dass keine Krankheit vorliegt.

Umkehrung des Baumdiagramms Vertauscht man die Reihenfolge der betrachteten Merkmale bei einem Baumdiagramm, dann erhält man das so genannte **umgekehrte Baumdiagramm**. Die Wahrscheinlichkeiten, die an den einzelnen Pfaden stehen, unterscheiden sich im Allgemeinem bei einem Baumdiagramm und seiner Umkehrung, denn sie beziehen sich auf verschiedene Merkmale und daher auf verschiedene Teilgesamtheiten.

Dagegen stimmen die Pfadwahrscheinlichkeiten bis auf die Reihenfolge überein, da sie die Wahrscheinlichkeiten der inneren Felder derselben Vierfeldtafel sind.

Allgemeine Multiplikationsregel $A_1, A_2, ..., A_3$ sind Ereignisse einer Ergebnismenge S. Dann gilt:

$$P(A_1 \cap A_2 \cap ... \cap A_K) = P(A_1) * P_{A_1}(A_2) * P_{A_1 \cap A_2}(A_2) * ... * P_{A_1 \cap A_2 \cap ... \cap A_k}(A_2)$$

Satz der totalen Wahrscheinlichkeit Fasst man gleiche Pfad-Enden zusammen, so gilt für die neue Pfadwahrscheinlichkeit:

$$P(B) = P(A \cap B) + P(\bar{A} \cap B) = P(A) * P_A(B) + P(\bar{A}) * P_{\bar{A}}(B)$$

Aus der Summe von Produkten lässt sich ablesen, wie sich das Ergebnis B ßusammensetzt"(ein Pfad über das Ereignis A, ein Pfad über das Ereignis $\bar{A}$)
Allgemein erhält man analog:

$$P(B) = P(A_1) * P_{A_1}(B) + P(A_2) * P_{A_2}(B) + ... + P(A_n) * P_{A_n}(B) = \sum_{i=1}^{n} P(A_i) * P_{A_i}(B)$$

2.1.5. Die Binomialverteilung

Die Binomialverteilung ist eine der wichtigsten diskreten Wahrscheinlichkeitsverteilungen.

Sie beschreibt die Anzahl der Erfolge in einer Serie von gleichartigen und unabhängigen Versuchen, die jeweils genau zwei mögliche Ergebnisse haben (Ërfolg“ oder "Misserfolg“). Solche Versuchs-Serien werden auch Bernoulli-Prozesse genannt.

Ist p die Erfolgswahrscheinlichkeit bei einem Versuch und die Anzahl der Versuche n, dann bezeichnet man mit $B_{n,p}(k)$ die Wahrscheinlichkeit, genau k Erfolge zu erzielen.

Die Binomialverteilung und der Bernoulli-Versuch können mit Hilfe des Galtonbretts veranschaulicht werden. Dabei handelt es sich um eine mechanische Apparatur, in die man n Kugeln wirft. Diese fallen dann zufällig in eines von mehreren Fächern, wobei die Aufteilung der Binomialverteilung entspricht. Je nach Konstruktion sind unterschiedliche Parameter p möglich.

Eigenschaften

Definition Die Wahrscheinlichkeitsverteilung mit der Wahrscheinlichkeitsfunktion

$$B_{n,p}(k) = \binom{n}{k} p^k (1-p)^{n-k} beik = 0, 1, \ldots, n$$

heißt die **Binomialverteilung** zu den Parametern n (Anzahl der Versuche) und $p \in [0, 1]$ (der Erfolgs- oder Trefferwahrscheinlichkeit).

Symmetrie Die Binomialverteilung ist in den Spezialfällen $p = 0, p = 0{,}5$ und $p = 1$ symmetrisch und ansonsten asymmetrisch.

Erwartungswert Die Binomialverteilung besitzt den Erwartungswert $n * p$.

Varianz Die Binomialverteilung besitzt die Varianz $n * p * (1 - p)$.

Sigma - Umgebungen

Der Abstand vom Erwartungswert zur x-Koordinate eines Wendepunkts heißt Standardabweichung und wird mit σ (lies: sigma) bezeichnet. Mit Mitteln der Analysis kann $\sigma = \sqrt{n * p * (1 - p)}$ bestimmt werden.

Für n-stufige Bernoulli-Versuche gilt under der sog. Laplace-Bedingung $\sigma > 3$:
Die Wahrscheinlichkeit, dass die Anzahl der Treffer in der 2 σ-Umgebung des Erwartungswerts liegt, beträgt ca. $0,954$, für die 3 σ-Umgebung sind es ca. $0,997$

Standardisierung einer Zufallsgröße

Eine Zufallsgröße mit dem Erwartungswert 0 und der Varianz 1 heißt standardisiert. Jede Zufallsgröße lässt sich mit Hilfe der Transformation standardisieren:

1. Die Höhen der Rechtecke in der Histogrammdarstellung müssen mit dem Faktor σ multipliziert werden, da die Rechtecksbreiten um den Faktor $1/\sigma$ verändert werden.

2. Durch die Standardisierung wir bei der Verteilungsfunktion nur die Lage der Sprungstellen, nicht deren Höhe verändert.

Die Normalverteilung

Die Bedeutung der Normalverteilung beruht unter anderem auf dem zentralen Grenzwertsatz, der besagt, dass eine Summe von n unabhängigen, identisch verteilten Zufallsvariablen mit endlicher Varianz im Grenzwert $n \to \infty$ normalverteilt ist. Das bedeutet, dass man Zufallsvariablen dann als normalverteilt ansehen kann, wenn sie durch Überlagerung einer großen Zahl von unabhängigen Einflüssen entstehen, wobei jede einzelne Einflussgröße einen im Verhältnis zur Gesamtsumme unbedeutenden Beitrag liefert.
Die Standardabweichung σ beschreibt die Breite der Normalverteilung und hängt mit der Halbwertsbreite zusammen. Es gilt näherungsweise:

Im Intervall der Abweichung $\pm\sigma$vom Mittelwert sind 68,27 % aller Messwerte zu finden,
Im Intervall der Abweichung $\pm 2\sigma$ vom Mittelwert sind 95,45 % aller Messwerte zu finden,
Im Intervall der Abweichung $\pm 3\sigma$ vom Mittelwert sind 99,73 % aller Messwerte zu finden.

Und ebenso lassen sich umgekehrt für gegebene Wahrscheinlichkeiten die maximalen Abweichungen vom Mittelwert finden:

50 % aller Messwerte haben eine Abweichung von höchstens $0{,}675\sigma$ vom Mittelwert,
90 % aller Messwerte haben eine Abweichung von höchstens $1{,}645\sigma$ vom Mittelwert,
95 % aller Messwerte haben eine Abweichung von höchstens $1{,}960\sigma$ vom Mittelwert,
99 % aller Messwerte haben eine Abweichung von höchstens $2{,}576\sigma$ vom Mittelwert.

Die **Dichtefunktion** der Standardnormalverteilung ist

$$\varphi(x) = \frac{1}{\sqrt{2\pi}} e^{-\frac{1}{2}x^2}$$

Das Bernoulli-Experiment

Zufallsgrößen mit einer **Bernoulli-Verteilung** benutzt man zur Beschreibung von zufälligen Ereignissen, bei denen es nur zwei mögliche Versuchsausgänge gibt. Einer der Versuchsausgänge wird meistens mit Erfolg bezeichnet und der komplementäre Versuchsausgang mit Misserfolg. Die zugehörige Wahrscheinlichkeit p für einen Erfolg nennt man Erfolgswahrscheinlichkeit und $q = 1 - p$ die Wahrscheinlichkeit eines Misserfolgs. Beispiele:

Werfen einer Münze: Kopf (Erfolg), $p = 1/2$, und Zahl (Misserfolg), $q = 1/2$.

Werfen eines Würfels, wobei nur eine "6" als Erfolg gewertet wird: $p = 1/6$, $q = 5/6$.

Qualitätsprüfung (einwandfrei, nicht einwandfrei).

Erwartungswert Die Bernoulli-Verteilung mit Parameter p hat den Erwartungswert:

$$\mathrm{E}(X) = p$$

Varianz Die Bernoulli-Verteilung besitzt die Varianz:

$$\mathrm{Var}(X) = p(1-p) = pq$$

, denn:

$$\mathrm{E}\left(X^2\right) - \mathrm{E}(X)^2 = p - p^2 = p \cdot (1-p) = pq$$

Beziehung zur Binomialverteilung Die Bernoulli-Verteilung ist ein Spezialfall der Binomialverteilung für $n = 1$. Mit anderen Worten, die Summe von unabhängigen Bernoulli-verteilten Zufallsgrößen mit identischem Parameter p genügt der Binomialverteilung. Die Binomialverteilung ist die n-fache Faltung der Bernoulli-Verteilung mit gleicher Wahrscheinlichkeit ,p.

Die Bernoulli-Kette

Eine **Bernoulli-Kette** ist ein zeitlich diskreter stochastischer Prozess, der aus einer endlichen oder abzählbar-unendlichen Folge von unabhängigen Versuchen mit Bernoulli-Verteilung besteht, das heißt, für jeden der Zeitpunkte 1, 2, 3, ... wird "ausgewürfelt", ob ein Ereignis mit Wahrscheinlichkeit p eintritt, oder nicht.
Der Prozess kann durch eine Folge von Zufallsvariablen X_1, X_2, X_3,..., beschrieben werden, von denen jede mit der konstanten Wahrscheinlichkeit p den Wert $X = 1$ (Erfolg) und mit der Wahrscheinlichkeit $q = 1 - p$ den Wert $X = 0$ (Misserfolg) annimmt.
Die Anzahl k erfolgreicher Versuche nach Durchführung von insgesamt n Versuchen; sie folgt einer Binomialverteilung.

Beispiel 2.1.2. Ein betrunkener Fußgänger bewegt sich bei jedem Schritt mit der Wahrscheinlichkeit p vorwärts, mit der Wahrscheinlichkeit q rückwärts. Man interessiert sich für die Entfernung vom Ausgangspunkt $2k - n$. Ein solches Modell wird in der Physik als eindimensionale Zufallsbewegung (Random Walk) bezeichnet.

Die Zufallsvariable k, die angibt, wie viele von n Bernoulli-Versuchen erfolgreich waren, folgt der Binomialverteilung. Wir leiten diese Verteilung anhand eines Beispiels her:

Beim Würfeln werde die Sechs als Erfolg gewertet; die Erfolgswahrscheinlichkeit ist also $p = 1/6$, die komplementäre Misserfolgswahrscheinlichkeit $q = 5/6$. Gefragt sei nun nach der Wahrscheinlichkeit, in $n = 5$ Würfen genau $k = 2$ Sechsen zu werfen.

Antwort: Die Wahrscheinlichkeit, erst zwei Sechsen, dann drei Nicht-Sechsen zu werfen, ist p^2q^3. Da es auf die Reihenfolge aber nicht ankommt, ist diese Wahrscheinlichkeit zu multiplizieren mit der Anzahl der Möglichkeiten, zwei (ununterscheidbare) Sechserwürfe auf fünf Würfe zu verteilen. Der Kombinatorik zufolge ist diese Anzahl durch den Binomialkoeffizienten "5 über 2" gegeben; die gesuchte Wahrscheinlichkeit lautet also:

$$B(2|p, 5) = \binom{5}{2} p^2 q^{5-2}.$$

Davon verallgemeinert, lautet die Wahrscheinlichkeit, in n Bernoulli-Versuchen genau k mal Erfolg zu haben,

$$B(k|p, n) = \binom{n}{k} p^k q^{n-k}$$

mit $q = 1 - p$. Diese Funktion heißt **Binomialverteilung**.

Das Histogramm

Ein **Histogramm** ist eine graphische Darstellung der Häufigkeitsverteilung metrisch skalierter Merkmale. Es erfordert die Einteilung der Daten in Klassen, die eine konstante oder variable Breite haben können. Bei Bernulli-Versuchen bietet sich zunächst eine konstante Breite von 1 an. Es werden direkt nebeneinander liegende Rechtecke von der Breite der jeweiligen Klasse gezeichnet, deren Flächeninhalte die (relativen

oder absoluten) Klassenhäufigkeiten darstellen. Die Höhe jedes Rechtecks stellt dann die (relative oder absolute) Häufigkeitsdichte dar, also die (relative oder absolute) Häufigkeit dividiert durch die Breite der entsprechenden Klasse.

2.2. Beurteilende Statistik

In der Beurteilenden Statistik versucht man, aus den bei mehrmaligen Durchführungen eines Zufallsexperimentes aufgetretenen Ergebnissen auf die unbekannte, dem Zufallsexperiment tatsächlich zugrundeliegende Wahrscheinlichkeitsverteilung zu schließen.

2.2.1. Hypothesentest

Das Testen von Hypothesen ist immer ein Vorgang, den man in mehrere Schritte unterteilen kann:

1. Formulierung der Nullhypothese H_0 und der Alternativhypothese H_1
2. Festlegung des Signifikanzniveaus
3. Bestimmung des Annahme- und Ablehnungsbereichs der Nullhypothese
4. Ziehung der Stichprobe
5. Treffen der Testentscheidung und Interpretation:
6. Liegt das Ergebnis der Stichprobe innerhalb des Annahmebereichs, wird H_0 angenommen, anderenfalls abgelehnt

Für das Aufstellen der Hypothesen gilt:

- Was ich zeigen oder beweisen will, gehört in die Alternativhypothese
- Das Gleichheitszeichen gehört immer in die Nullhypothese
- Beim aufstellen der Nullhypothese geht man davon aus, “Alles bleibt beim alten, nichts hat sich geändert”

3. Zahlentheorie

Mathematiker sind Betriebsunfälle der Natur.

(Werner Fuld)

Hinweis [1]

3.1. Teilbarkeit

Definition 3.1.1. Eine ganze Zahl b heißt durch eine ganze Zahl $a \neq 0$ teilbar, falls es ein $x \in \mathbb{Z}$ gibt, so dass $b = ax$ ist, und wir schreiben $a \mid b$. Man nennt a einen Teiler von b ,und b heißt Vielfaches von a. Falls b nicht durch a teilbar ist, schreiben wir $a \nmid b$

3.2. Kongruenzen

In diesem Kapitel studieren wir die Theorie der Kongruenzen. Kongruenzen beschreiben Teilbarkeitsrelationen. Man findet sie auch im täglichen Leben: Uhren geben die Stunden entweder modulo 12 oder modulo 24 an. Die Wochentage rechnen wir modulo 7 und die Monate modulo 12. Sobald wir die richtigen Werkzeuge bereit gestellt haben, können wir genauso gut mit Kongruenzen rechnen wie mit Gleichungen.

Definition 3.2.1. Sei m eine natürliche Zahl und seien a, b ganze Zahlen. Wir sagen, dass a kongruent zu b modulo m ist, falls $m \mid (b-a)$. (Äquivalent: es existiert ein $k \in Z$ mit $b = a + km$.) Wir schreiben: $a \equiv b \pmod{m}$. Die Zahl m heißt der Modul der Kongruenz. Zum Beispiel ist $200 \equiv 11 \pmod{9}$, da 9 ein Teiler von $200 - 11 = 189$ ist. Anders formuliert: 200 und 11 haben den gleichen Rest nach Division durch 9, nämlich 2.

Satz 3.2.1. *Kongruenz ist eine Äquivalenzrelation, d.h. es gelten die folgenden Eigenschaften:*

Reflexivität $a \equiv a \pmod{m}$*, für alle* $a \in Z$*,*

Symmetrie *Falls* $a \equiv b \pmod{m}$*, so gilt auch* $b \equiv a \pmod{m}$*,*

Transitivität *Falls* $a \equiv b \pmod{m}$ *und* $b \equiv c \pmod{m}$*, so gilt auch* $a \equiv c \pmod{m}$*.*

[1] Teilweise entnommen aus [Bou10] und [MR10]

3.3. Nullteiler

In der *abstrakten Algebra* ist ein Nullteiler eines Ringes R ein vom Nullelement 0 verschiedenes Element a, für das es ein vom Nullelement 0 verschiedenes Element b gibt, so dass $ab = 0$.

3.4. Größter gemeinsamer Teiler

Definition 3.4.1. Der ggT zweier ganzer Zahlen a und b ist eine ganze Zahl m mit der Eigenschaft, dass sie Teiler sowohl von a als auch von b ist und dass jede ganze Zahl, die ebenfalls die Zahlen a und b teilt, ihrerseits Teiler von m ist.

3.5. Kleinstes gemeinsames Vielfaches

Definition 3.5.1. Das *kleinste gemeinsame Vielfache* zweier ganzer Zahlen m und n ist die kleinste natürliche Zahl, die sowohl Vielfaches von m als auch Vielfaches von n ist.

3.6. Euklidscher Algorithmus

Der **erweiterte euklidische Algorithmus** berechnet neben dem größten gemeinsamen Teiler $\mathrm{ggT}(a, b)$ zweier natürlicher Zahlen a und b noch zwei ganze Zahlen s und t, die die folgende Gleichung erfüllen:

$$\mathrm{ggT}(a, b) = s \cdot a + t \cdot b$$

Das Haupteinsatzgebiet des erweiterten euklidischen Algorithmus ist die Berechnung der **inversen Elemente in ganzzahligen Restklassenringen**, denn wenn der Algorithmus das Tripel $(d = \mathrm{ggT}(a, b), s, t)$ ermittelt, ist entweder $d = 1$ und damit $1 \equiv t \cdot b \pmod{a}$, t also das *multiplikative Inverse* von b modulo a, oder aber $d \neq 1$, was bedeutet, dass b modulo a kein Inverses hat.

3.7. Primfaktorzerlegung

Die Primfaktorzerlegung ist die Darstellung einer natürlichen Zahl n als Produkt aus Primzahlen, die dann als Primfaktoren von n bezeichnet werden.

Definition 3.7.1. Sei n eine natürliche Zahl. Eine Zahl p heißt Primfaktor von n,

- wenn p ein Teiler von n ist und
- p eine Primzahl ist.

Die Primfaktorzerlegung ist die Darstellung der Zahl n als Produkt ihrer Primfaktoren. Da die Multiplikation kommutativ und assoziativ ist, ist die Reihenfolge der Primfaktoren aus Sicht der Zahlentheorie unwichtig. Die Primfaktorzerlegung der Eins kann als leeres Produkt betrachtet werden. Wenn n selbst eine Primzahl ist, so ist sie selbst

ihr einziger Primfaktor. Gibt es mehr als einen Primfaktor, so wird n zusammengesetzte Zahl genannt. Die Null ist niemals Teil der multiplikativen Gruppe und wird von solchen Betrachtungen ausgeschlossen.
Mehrfach auftretende Primfaktoren können mittels Exponenten-Schreibweise zusammengefasst werden.

3.8. Satz von Euler-Fermat

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

3.8.1. Kleiner fermatscher Satz

$$a^p \equiv a \pmod{p}$$

Ist a kein Vielfaches von p gilt:

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

3.9. Eulersche Phi-Funktion

Die eulersche Phi-Funktion ist eine zahlentheoretische Funktion. Sie gibt für jede natürliche Zahl n an, wie viele zu n teilerfremde natürliche Zahlen es gibt, die nicht größer als n sind:

$$\varphi(n) := \left|\{a \in \mathbb{N} \mid 1 \leq a \leq n \wedge \mathrm{ggT}(a,n) = 1\}\right|$$

3.9.1. Eigenschaften und Berechnung

Allgemein lässt sich der Wert der eulerschen Phi-Funktion aus der Primfaktorzerlegung berechnen:

Multiplikative Funktion Für teilerfremde Zahlen m und n gilt:

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

Berechnung für Primzahlen Da eine Primzahl p nur durch 1 und sich selbst teilbar ist, ist sie zu den Zahlen 1 bis $p-1$ teilerfremd. Weil sie größer als 1 ist, ist sie außerdem *nicht* zu sich selbst teilerfremd. Es gilt daher

$$\varphi(p) = p - 1.$$

3.10. Gruppen, Ringe, Körper

Siehe hierzu bitte Anhang .1 auf Seite 65.

4. Lineare Algebra / Analytische Geometrie

Jedes Problem, das ich gelöst hatte, wurde zu einer Regel, mit deren Hilfe später weitere Probleme gelöst werden konnten.

(René Descartes)

4.1. Matrizenrechnung

Eine Matrix ist ein rechteckiges Schema, dessen Elemente üblicherweise Zahlen, aber auch andere mathematische Elemente wie Variablen oder Funktionen sein können. Sie besteht aus m Zeilen und n Spalten. Matrizen können beliebige Dimensionalität besitzen.

4.1.1. Notation

Eine **Matrix** A vom Typ (m, n) mit Zahlen, die in m Zeilen und n Spalten angeordnet sind:

$$A_{m,n} = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m,1} & a_{m,2} & \cdots & a_{m,n} \end{pmatrix}$$

Man schreibt: $A_{m,n} = (a_{i,k})_{m,n}$ mit $i = 1, 2, .., m$ und $k = 1, 2, .., n$.

Matrizen, die aus lauter Nullen bestehen, nennt man **Nullmatrix**. Man schreibt dafür auch O.

$$O_{mn} = \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{pmatrix}.$$

4.1.2. Matrizenaddition

Zwei Matrizen können addiert werden, wenn sie vom selben Typ sind, das heißt, wenn sie dieselbe Anzahl von Zeilen und dieselbe Anzahl von Spalten besitzen. Seien A und B Matrizen über einer Menge R, dessen abelsche Gruppe ein Ring ist.[1]. Jedes Element

[1] lt. Ringtheorie Voraussetzung zur Addition von Matrizen[Art98]

der Summenmatrix ist die Summe der Elemente der Matrizen A und B:

$$A + B = (a_{ij} + b_{ij}) = \begin{pmatrix} a_{11} + b_{11} & \cdots & a_{1n} + b_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} + b_{m1} & \cdots & a_{mn} + b_{mn} \end{pmatrix}$$

Die Einheitsmatrix

Die Einheitsmatrix ist eine quadratische Matrix, auf der alle Elemente den Wert Null haben, bis auf die Elemente, die auf der Diagonale (von links oben nach unten rechts) liegen und den Wert Eins haben.

$$I_n = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{pmatrix}$$

Beachte, dass 0 das Nullelement und 1 das Einselement des jeweiligen Ringes, über den die Matrix gebildet wird, sind.

4.1.3. Skalarmultiplikation

Bei der Skalarmultiplikation der Matrix A wird jedes Element der Matrix mit einem Skalar λ multipliziert.

$$\lambda \cdot A = \lambda \cdot \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} = \begin{pmatrix} \lambda \cdot a_{11} & \dots & \lambda \cdot a_{1n} \\ \vdots & \ddots & \vdots \\ \lambda \cdot a_{m1} & \dots & \lambda \cdot a_{mn} \end{pmatrix}$$

Für die Skalarmultiplikation gelten folgende Gesetze:

1. $1 * A = A$
2. $0 * A = O$
3. $(r * s) * A = r * (s * A)$
4. $(r + s) * A = r * A + s * A$

Die Skalarmultiplikation ist nicht mit dem Skalarprodukt zu verwechseln!

4.1.4. Multiplikation von Matrizen

Genau dann dürfen zwei Matrizen A und B miteinander multipliziert werden, wenn gilt:

Definition 4.1.1. A hat m Zeilen und n Spalten, und B hat n Zeilen und s Spalten. Das Ergebnis hat dann m Zeilen und s Spalten, also $A * B \in M_{ms}$.

Seien formal:

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}, B = \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{m1} & b_{m2} & \cdots & b_{mn} \end{pmatrix}$$

Dann gilt:

$$AB = \left(\sum_{j=1}^{n} a_{ij} b_{jk} \right) = \begin{pmatrix} \sum_{j=1}^{n} a_{1j} b_{j1} & \sum_{j=1}^{n} a_{1j} b_{j2} & \cdots & \sum_{j=1}^{n} a_{1j} b_{js} \\ \sum_{j=1}^{n} a_{2j} b_{j1} & \sum_{j=1}^{n} a_{2j} b_{j2} & \cdots & \sum_{j=1}^{n} a_{2j} b_{js} \\ \vdots & \vdots & \ddots & \vdots \\ \sum_{j=1}^{n} a_{mj} b_{j1} & \sum_{j=1}^{n} a_{mj} b_{j2} & \cdots & \sum_{j=1}^{n} a_{mj} b_{js} \end{pmatrix}$$

Die Matrizenmultiplikation ist nicht kommutativ, d. h. im Allgemeinen gilt $B \cdot A \neq A \cdot B$. Die Matrizenmultiplikation ist allerdings assoziativ:

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

Die Matrizenaddition und Matrizenmultiplikation genügen zudem den beiden Distributivgesetzen:

$$(A + B) \cdot C = A \cdot C + B \cdot C$$

für alle $l \times m$-Matrizen A, B und $m \times n$-Matrizen C sowie

$$A \cdot (B + C) = A \cdot B + A \cdot C$$

für alle $l \times m$-Matrizen A und $m \times n$-Matrizen B, C.

4.1.5. Transponierung von Matrizen

Die Transponierte einer $m \times n$-Matrix $A = (a_{ij})$ ist die $n \times m - Matrix A^T = (a_{ji})$, das heißt zu

$$A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix}$$

ist

$$A^T = \begin{pmatrix} a_{11} & \dots & a_{m1} \\ \vdots & \ddots & \vdots \\ a_{1n} & \dots & a_{mn} \end{pmatrix}$$

die Transponierte. Man schreibt also die erste Zeile als erste Spalte, die zweite Zeile als zweite Spalte usw.

4.1.6. Inverse Matrizen

Satz 4.1.1. *Die Matrix* $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *hat das Inverse*

$$M^{-1} = \frac{1}{a*d-b*c} * \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

wenn $a*d-b*c \neq 0$.

Definition 4.1.2. Gegeben ist die Matrix $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Der Term

$$det(M) = a*d-b*c$$

heißt Determinante.

Die Inverse der transponierten Matrix entspricht der Transponierten der inversen Matrix:

$$\left(A^T\right)^{-1} = \left(A^{-1}\right)^T$$

Die Inverse einer Matrix A ist ebenfalls invertierbar. Die Inverse der Inversen ist gerade wieder die Matrix selbst:

$$\left(A^{-1}\right)^{-1} = A$$

4.1.7. Affine Abbildungen in $\mathbb{R}^2$

Eine affine Abbildung α ist eine Abbildung der Form

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

$$\overrightarrow{x} \longmapsto A\overrightarrow{x} + \overrightarrow{v} \text{ mit } det(a) \neq 0$$

Sie ordnet einem Urbildpunkt $P(x \mid y)$ einen Bildpunkt $P'(x' \mid y')$ zu. Eine affine Abbildung ist umkehrbar; man spricht auch von einer eindeutigen Abbildung. Abgekürzt schreibt man

$$\overrightarrow{x'} = A\overrightarrow{x} + \overrightarrow{v}$$

oder in Matrixschreibweise

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} * \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} e \\ f \end{pmatrix}$$

Der Vektor $\overrightarrow{v} = \begin{pmatrix} e \\ f \end{pmatrix}$ heißt **Verschiebungsvektor** der linearen Abbildung.

Beachte: Es handelt sich nur um eine umkehrbare Abbildung, wenn gilt:

$$det\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) \neq 0$$

Eine Abbildung lässt sich durch die erneute Abbildung mit dem Inversen der Abbildungsmatrix umkehren.

4.1.8. Wichtige bekannte Abbildungen in Matrizenschreibweise

Die wichtigsten Abbildungen in Tabellenform zusammengefasst:

Abbildung	Matrix
Spiegelung x-Achse	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
Spiegelung y-Achse	$\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$
Spiegelung an der Diagonalen $y = x$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
Punktspiegelung am Ursprung	$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$
Zentrische Streckung mit Zentrum im Ursprung	$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$
Scherung x-Achse	$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$
Scherung y-Achse	$\begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}$
Drehung mit Drehzentrum im Ursprung	$\begin{pmatrix} cos(\alpha) & -sin(\alpha) \\ sin(\alpha) & cos(\alpha) \end{pmatrix}$

4.1.9. Verkettung affiner Abbildungen

Da die Multiplikation von Matrizen nicht kommutativ ist, muss man Obacht geben, ob eine Gleichung von links oder von rechts mit einer Matrix multipliziert wird.
Gegeben seien nun die beiden Abbildungen

$$\alpha\colon \overrightarrow{x'} = A * \overrightarrow{x} + \overrightarrow{v}$$

$$\beta\colon \overrightarrow{x'} = B * \overrightarrow{x} + \overrightarrow{w}$$

Dann gilt:

$$\alpha \circ \beta\colon \overrightarrow{x''} = A * (B * \overrightarrow{x} + \overrightarrow{w}) + \overrightarrow{v}$$

$$\beta \circ \alpha\colon \overrightarrow{x''} = B * (A * \overrightarrow{x} + \overrightarrow{v}) + \overrightarrow{w}$$

Man beachte, dass bei $\alpha \circ \beta$ zuerst β und dann erst α auf $\overrightarrow{x}$ angewendet wird, also $(\alpha \circ \beta) = \alpha(\beta(x))$.

4.1.10. Fixelemente

Als Fixelemente einer Abbildung bezeichnet man in der Geometrie Mengen des Definitionsbereiches, die auf sich selbst abgebildet werden. Zu ihnen gehören unter Anderem:

Fixpunkte $P \mapsto P$

Fixpunktgeraden $P \mapsto P$ für alle Punkte einer Geraden g. Alle Punkte der Geraden sind also Fixpunkte der Abbildung.

Fixgeraden $g \mapsto g$ (nicht aber zwingend $P \mapsto P$für $P \in g$, etwa bei Umkehrung der Orientierung: hier gibt es nur einen Fixpunkt; Fixpunktgeraden sind spezielle Fixgeraden)

Fixelemente sind die Symmetrieachsen (bzw. -punkte und sonstige Elemente) einer geometrischen Symmetrie.

4.1.11. Eigenwerte und Eigenvektoren

Ein **Eigenvektor** einer Abbildung ist in der linearen Algebra ein vom Nullvektor verschiedener Vektor, dessen Richtung durch die Abbildung nicht verändert wird. Ein Eigenvektor wird also nur gestreckt und man bezeichnet den Streckungsfaktor als **Eigenwert** der Abbildung.
Es gilt:

$$A \cdot x = \lambda x$$

Den Faktor λ nennt man dann den zugehörigen *Eigenwert*. Diese Gleichung kann man auch in der Form $A \cdot x = \lambda\, E \cdot x$ schreiben.

Berechnung der Eigenwerte

Die Gleichung $(A - \lambda E) \cdot x = 0$ definiert die Eigenwerte und stellt ein homogenes lineares Gleichungssystem dar. Da $x \neq 0$ vorausgesetzt wird, ist dieses genau dann lösbar, wenn $\det(A - \lambda E) = 0$ gilt.

Definition 4.1.3. Man bezeichnet $\det(A - \lambda E) = (a - \lambda) \cdot (d - \lambda) - c \cdot b$ als das *charakteristische Polynom* der Matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

Satz 4.1.2. *Die Nullstellen des charakteristischen Polynoms sind die Eigenwerte von* A.

Berechnung der Eigenvektoren

Für einen Eigenwert λ lassen sich die Eigenvektoren aus der Gleichung

$$(A - \lambda E) \cdot x = 0$$

bestimmen. Jeweils die Eigenwerte einsetzen; anschließend die Gleichung in Koordinatenform mit Hilfe eines Gleichungssystemes lösen. Jeder Eigenwert hat einen Eigenvektor.

4.1.12. Homogene Koordinaten für zweidimensionale Objekte

Objekte in der Ebene werden normalerweise durch kartesische Koordinaten dargestellt. Man kann auch homogene Koordinaten verwenden. sie haben einen großen Vorteil:

```
Durch homogene Koordinaten kann man alle geometischen Transformationen
        einheitlich durch Matrizenmultiplikation darstellen.
```

Man erweitert dazu den Ortsvektor durch eine dritte Koordinate mit dem Wert 1, die bei der Darstellung um Koordinatensystem gar nicht berücksichtigt wird. Die Abbildungsmatrizen ergänzt man um eine zusätzliche Zeile und Spalte. Aus der gewohnten Abbildungsgleichung $\alpha\colon \begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} v_x \\ v_y \end{pmatrix}$ wird dann in homogenen Koordinaten:

$$\alpha\colon \begin{pmatrix} x' \\ y' \\ 1 \end{pmatrix} = \begin{pmatrix} a & b & v_x \\ c & d & v_y \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ 1 \end{pmatrix} = \begin{pmatrix} a \cdot x + b \cdot y + v_x \\ c \cdot x + d \cdot y + v_y \\ 1 \end{pmatrix}$$

4.2. Vektorielle Geometrie

4.2.1. Vektoren im Raum

Was ist ein Vektor?

Physik Pfeile, Kräfte, Bewegung

Mathematik $(1, n)Matrix$, oder:

Definition 4.2.1. Ein Vektor ist ein Repäsentant einer Klasse von Pfeilen. Er ist bestimmt durch: Länge und Richtung.

Definition 4.2.2. Ein Ortsvektor ist „ortsgebunden“.

$$\text{Fußpunkt} \longmapsto \text{Spitze}.$$

Der Fußpunkt eines Ortsvektors liegt im Nullpunkt. Der Gegenvektor $\overrightarrow{v}^{-1} = -\overrightarrow{v}$ ist das additive Inverse zum Vektor $\overrightarrow{v}$.

Notation

Punkt: $P(a|b|c)$

Ortsvektor : $\overrightarrow{OP} = \overrightarrow{P} = \begin{pmatrix} a \\ b \\ c \end{pmatrix}$

Addition von Vektoren

1. Fußpunkt von $\overrightarrow{b}$ an Spitze von $\overrightarrow{a}$
2. Ergebnis $\overrightarrow{a} + \overrightarrow{b}$ vom Fußpunkt von $\overrightarrow{a}$ zur Spitze von $\overrightarrow{b}$
3. $\overrightarrow{a} + \overrightarrow{b} = \overrightarrow{b} + \overrightarrow{a}$

Subtraktion von Vektoren

1. Spitze von $\overrightarrow{a}$ an Spitze von $\overrightarrow{b}$ anlegen.
2. Ergebnis $\overrightarrow{a} - \overrightarrow{b}$ geht vom Fußpunkt von $\overrightarrow{a}$ zum Fußpunkt von $\overrightarrow{b}$.

oder *Addition* mit dem *Gegenvektor*: $\overrightarrow{a} + (-\overrightarrow{b})$

Linearkombination

Unter einer Linearkombination versteht man in der linearen Algebra einen Vektor, der sich durch gegebene Vektoren unter Verwendung der Vektoraddition und der skalaren Multiplikation ausdrücken lässt.

Definition 4.2.3. Es seien endlich viele Vektoren $v_1, \ldots, v_n$ gegeben. Dann nennt man jeden Vektor v, der sich in der Form

$$v = a_1 v_1 + a_2 v_2 + \cdots + a_n v_n = \sum_{i=1}^{n} a_i v_i$$

schreiben lässt eine Linearkombination von $v_1, \ldots, v_n$. Die Faktoren in der obigen Darstellung nennt man die Koeffizienten der Linearkombination. Auch die Darstellung selbst wird als Linearkombination bezeichnet.

Betrag von Vektoren

In kartesischen Koordinaten kann die Länge von Vektoren nach dem Satz des Pythagoras berechnet werden:

Definition 4.2.4.

$$a = |\vec{a}| = \sqrt{{a_1}^2 + {a_2}^2 + {a_3}^2}$$

Dies entspricht der sog. euklidischen Norm. Die Länge lässt sich in einer alternativen Schreibweise auch als die Wurzel des Skalarprodukts angeben:

Definition 4.2.5.

$$a = |\vec{a}| = \sqrt{\vec{a} \cdot \vec{a}}$$

Vektoren der Länge 1 heißen *Einheitsvektoren*. Hat ein Vektor die Länge 0, so handelt es sich um den *Nullvektor*.

Definition 4.2.6. Es seien endlich viele Vektoren $v_1, \ldots, v_n$ gegeben. Dann nennt man jeden Vektor v, der sich in der Form

$$v = a_1 v_1 + a_2 v_2 + \cdots + a_n v_n = \sum_{i=1}^{n} a_i v_i$$

schreiben lässt eine Linearkombination von $v_1, \ldots, v_n$. Die Faktoren in der obigen Darstellung nennt man die Koeffizienten der Linearkombination. Auch die Darstellung selbst wird als Linearkombination bezeichnet.

4.2.2. Geraden im Raum

Was ist eine Gerade?

Definition 4.2.7. Eine gerade Linie oder kurz Gerade ist ein Element der Geometrie. Die kürzeste Verbindung zweier Punkte ist gerade und wird als Strecke bezeichnet. Eine gerade, unendlich lange, unendlich dünne und in beide Richtungen unbegrenzte Linie nennt man eine Gerade.
Hilberts Axiomensystem besagt:
`Zwei voneinander verschiedene Punkte` P `und` Q `bestimmen stets eine Gerade` g.

Parameterdarstellung

Unter der Parameterdarstellung (oder auch Parameterform) einer Geradengleichung versteht man die Form

$$\vec{r} = \overrightarrow{r_0} + t \cdot \vec{u}$$

t ist hierbei der reelle Parameter, der Vektor $\overrightarrow{r_0}$ ist der Ortsvektor eines Punktes P_0 auf der Geraden. Dieser Punkt heißt Aufpunkt oder Stützpunkt, seinen Ortsvektor $\overrightarrow{r_0}$ nennt man dann *Stützvektor*. Den Vektor $\overrightarrow{u}$ in der Geradengleichung nennt man den *Richtungsvektor* der Geraden.

4.2.3. Gegenseitige Lage von Geraden im Raum

Eine Gerade kann zu einer anderen Gerade entweder **parallel** liegen, einen **Schnittpunkt** mit ihr haben oder **identisch** mit ihr sein. Gilt keine dieser Lagebeziehungen, sind die Geraden **windschief** zueinander.

4.2.4. Ebenen im Raum

Definition 4.2.8. Bei einer Ebene handelt es sich um ein unbegrenzt ausgedehntes flaches zweidimensionales Objekt.

- Hierbei bedeutet unbegrenzt ausgedehnt und flach, dass zu je zwei Punkten auch eine durch diese verlaufende Gerade vollständig in der Ebene liegt.
- Zweidimensional bedeutet, dass – abgesehen von enthaltenen Geraden – kein echter Teilraum ebenfalls diese Eigenschaft hat.

Parameterform

Bei der Parameterform oder Punktrichtungsform wird eine Ebene durch einen Stützvektor $\overrightarrow{p}$ und zwei Richtungsvektoren $\overrightarrow{u}$ und $\overrightarrow{v}$ beschrieben:

$$E : \overrightarrow{x} = \overrightarrow{u} + r \cdot \overrightarrow{v} + s \cdot \overrightarrow{w} \mid r, s \in \mathbb{R}$$

Koordinatenform

Bei der Koordinatenform wird eine Ebene durch vier reelle Zahlen a, b, c und d in Form einer linearen Gleichung beschrieben:

$$E : ax_1 + bx_2 + cx_3 = d \mid \vec{x} \in \mathbb{R}^3$$

Normalenform

Bei der Normalenform wird eine Ebene durch einen Stützvektor $\vec{p}$ und einen Normalenvektor $\vec{n}$ beschrieben

$$E : (\vec{x} - \vec{p}) \cdot \vec{n} = 0 \mid \vec{x} \in \mathbb{R}^3$$

Die Normalenform kann als Ausgangspunkt sowohl für die Parameterform, als auch die Koordinatenform verwendet werden. Umgewandelt wird wie folgt:

Parameterform $\longrightarrow$ Normalenform

1. Parameterform: $E : \overrightarrow{x} = \overrightarrow{u} + r \cdot \overrightarrow{v} + s \cdot \overrightarrow{w}$
2. Normalenvektor per Kreuzprodukt (siehe 4.2.8) bestimmen: $\vec{n} = \vec{v} \times \vec{w}$
3. Normalenform bildet sich folgendermaßen: $E : (\vec{x} - \vec{u}) \cdot \vec{n} = 0$

Normalenform $\longrightarrow$ Parameterform

1. Normalenform: $E : (\vec{x} - \vec{u}) \cdot \vec{n} = 0$
2. Mit $\vec{v}$ und $\vec{w}$ werden nun 2 Vektoren gesucht, die jeweils orthogonal zum Normalenvektor $\vec{n}$ stehen. Zwei Vektoren sind senkrecht, wenn ihr Skalarprodukt 0 ergibt:
$$\vec{n} \cdot \vec{v} = 0, \vec{n} \cdot \vec{w} = 0$$
3. Man wähle nun je 2 Koordinaten von $\vec{v}$ und $\vec{w}$ beliebig und bestimme die Letzte. Beispielhaft:
$$\vec{n} \cdot \begin{pmatrix} v_1 \\ 1 \\ 1 \end{pmatrix} = 0, \vec{n} \cdot \begin{pmatrix} w_1 \\ 1 \\ 2 \end{pmatrix} = 0$$
4. Paremeterform bildet sich folgendermaßen: $E : \overrightarrow{x} = \overrightarrow{u} + r \cdot \overrightarrow{v} + s \cdot \overrightarrow{w}$

Koordinatenform $\longrightarrow$ Normalenform Der Normalenvektor $\vec{n}$ kann anhand der Vorfaktoren sofort abgelesen werden. Es muss noch ein Ortsvektor $\vec{p}$ gefunden werden. Dazu müssen x_1, x_2 und x_3 so gewählt werden, dass die Gleichung erfüllt ist. Man wählt einfach x_2 und x_3 als 1 und löst die Gleichung nach x_1 auf.

Normalenform $\longrightarrow$ Koordinatenform Hier genügt ein einfaches Ausmultiplizieren:

$$E : (\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} - \begin{pmatrix} u_1 \\ u_2 \\ u_3 \end{pmatrix}) \cdot \begin{pmatrix} n_1 \\ n_2 \\ n_3 \end{pmatrix} = 0$$

$$\Leftrightarrow \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \cdot \begin{pmatrix} n_1 \\ n_2 \\ n_3 \end{pmatrix} - \begin{pmatrix} u_1 \\ u_2 \\ u_3 \end{pmatrix} \cdot \begin{pmatrix} n_1 \\ n_2 \\ n_3 \end{pmatrix} = 0$$

$$\Leftrightarrow \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \cdot \begin{pmatrix} n_1 \\ n_2 \\ n_3 \end{pmatrix} = \begin{pmatrix} u_1 \\ u_2 \\ u_3 \end{pmatrix} \cdot \begin{pmatrix} n_1 \\ n_2 \\ n_3 \end{pmatrix}$$

$$\Rightarrow n_1 \cdot x_1 + n_2 \cdot x_2 + n_3 \cdot x_3 = u_1 \cdot n_1 + u_2 \cdot n_2 + u_3 \cdot n_3$$

Achsenabschnittsform

Bei der Achsenabschnittsform wird eine Ebene durch drei Achsenabschnitte a_1,a_2 und a_3 beschrieben:

$$E : \frac{x_1}{a_1} + \frac{x_2}{a_2} + \frac{x_3}{a_3} = 1 \Big| \vec{x} \in \mathbb{R}^3$$

Hierbei sind $(a_1, 0, 0)$, $(0, a_2, 0)$ und $(0, 0, a_3)$ die Schnittpunkte der Ebene mit den drei Koordinatenachsen. Diese Schnittpunkte werden auch Spurpunkte genannt, ihre Verbindungsstrecken liegen auf den Spurgeraden und bilden das Spurdreieck. Die Achsenabschnittsform kann aus der Koordinatenform mittels Division durch d errechnet werden. Verläuft eine Ebene parallel zu einer oder zwei Koordinatenachsen, dann fallen die entsprechenden Terme in der Achsenabschnittsform weg.

4.2.5. Gegenseitige Lage von Ebenen im Raum

Ebenen können entweder eine oder keine Schnittgerade besitzen. Ist beides nicht der Fall, sind sie identisch.

4.2.6. Gegenseitige Lage von Ebenen und Geraden im Raum

Eine Gerade kann zu einer Ebene entweder parallel liegen, ein Teilraum der Ebene sein, oder sie durchstoßen.

4.2.7. Das Skalarprodukt

Das Skalarprodukt ordne zwei Vektoren eine Zahl (Skalar) zu. Geometrisch berechnet man das Skalarprodukt zweier Vektoren $\vec{a}$ und $\vec{b}$ nach der Formel

$$\vec{a} \cdot \vec{b} = |\vec{a}|\,|\vec{b}|\,\cos\sphericalangle(\vec{a}, \vec{b})$$

Dabei bezeichnen $|\vec{a}|$ und $|\vec{b}|$ jeweils die Beträge der Vektoren. Mit$\cos\sphericalangle(\vec{a}, \vec{b}) = \cos\varphi$ wird der Kosinus des von den beiden Vektoren eingeschlossenen Winkels φ bezeichnet.

Definition 4.2.9. In einem kartesischen Koordinatensystem gilt:

$$\vec{a} \cdot \vec{b} = a_1\,b_1 + a_2\,b_2 + a_3\,b_3$$

Kennt man die kartesischen Koordinaten der Vektoren, so kann man mit dieser Formel das Skalarprodukt ausrechnen und mit der obigen Formel dann den Winkel zwischen den beiden Vektoren.

4.2.8. Das Kreuzprodukt

Das Kreuzprodukt ist eine Verknüpfung, die im zwei Vektoren wieder einen Vektor zuordnet. Um es von anderen Produkten, insbesondere vom Skalarprodukt, zu unterscheiden, wird es mit einem Malkreuz als Multiplikationszeichen geschrieben. Das Kreuzprodukt der Vektoren $\vec{a}$ und $\vec{b}$ ist ein Vektor, der senkrecht auf der von den beiden Vektoren aufgespannten Ebene steht und mit ihnen ein Rechtssystem bildet. Die Länge dieses Vektors entspricht dem Flächeninhalt des Parallelogramms, das von den Vektoren $\vec{a}$ und $\vec{b}$ aufgespannt wird.

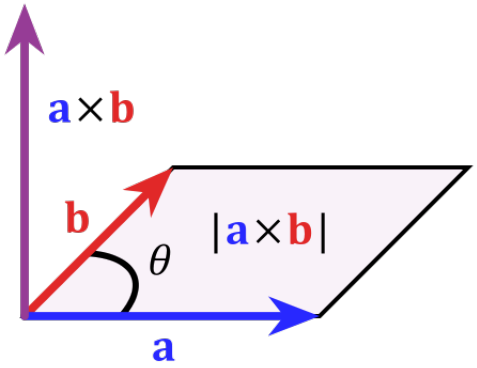

Abbildung 4.1.: Das Kreuzprodukt zweier Vektoren

Definition 4.2.10. Das Krauzprodukt ist definiert als:

$$\vec{a} \times \vec{b} = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} \times \begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix} = \begin{pmatrix} a_2 b_3 - a_3 b_2 \\ a_3 b_1 - a_1 b_3 \\ a_1 b_2 - a_2 b_1 \end{pmatrix}$$

4.2.9. Projektion

Trifft Licht auf einen Körper, so wird es absorbiert oder reflektiert. Dadurch entsteht in der Grundebene ein Schatten des Körpers. Genau dies ist das Prinzip der Projektion.

Parallelprojektion

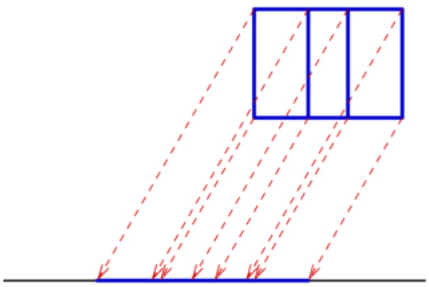

Abbildung 4.2.: Die Parallelprojektion

Definition 4.2.11. Eine Parallelprojektion ist eine Abbildung von Punkten des dreidimensionalen Raums auf Punkte einer gegebenen Ebene, wobei die Projektionsstrahlen zueinander parallel sind.

Vergleich: Sonnenstrahlen aus größter Entfernung.
Sei $\vec{v} = \begin{pmatrix} a \\ b \\ c \end{pmatrix}$ der Richtungsvektor der Parallelprojektion. Ein Bildpunkt P hat den Ortsvektor $\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$. Die Gerade der Projektion lautet dann $\vec{x} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} + r \cdot \begin{pmatrix} a \\ b \\ c \end{pmatrix}$. Der Bildpunkt P' ergibt sich durch Bestimmung des Schnittpunktes der Geraden mit der Projektionssebene. Ist dies beispielsweise die xy-Ebene, so muss der Schnittpunkt P' bei $(p \mid q \mid 0)$ sein. Man berechnet das r für $x_3 = 0$ und löst damit die anderen Koordinaten.

Zentralprojektion

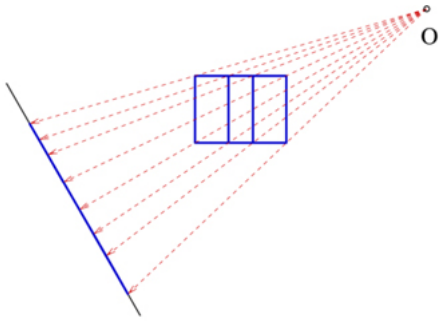

Abbildung 4.3.: Die Zentralprojektion

Definition 4.2.12. Im Gegensatz zur Parallelprojektion, wo man parallele Strahlen zur Projektion auf eine Ebene (Bildtafel) verwendet, benutzt man bei der Zentralprojektion Geraden durch einen festen Punkt O, dem Fluchtpunkt.

Vergleich: Scheinwerferlicht.
Die Methode entspricht die der Parallelprojektion, nur die Gerade der Projektion wird definiert als Gerade zwischen O und P.

Teil II.

Informatik

5. Software-Engineering

> Wenn du dir die Anwender deiner Programme als Idioten vorstellst, werden auch nur Idioten deine Programme verwenden.
>
> *(Linus Torvalds)*

Softwaretechnik beschäftigt sich mit der Herstellung bzw. Entwicklung von Software, der Organisation und Modellierung der zugehörigen Datenstrukturen und dem Betrieb von Softwaresystemen. Balzert beschreibt die Softwaretechnik als "Zielorientierte Bereitstellung und systematische Verwendung von Prinzipien, Methoden und Werkzeugen für die arbeitsteilige, ingenieurmäßige Entwicklung und Anwendung von umfangreichen Softwaresystemen"[Bal96].
Doch was muss ein gutes System ausmachen? Letztendlich ist ein gutes System eines, das den Bedürfnissen des Anwenders gerecht wird. Das System muss deshalb... [ABMG+05]

nützlich und nutzbar sein. Es muss dem Anwender das Leben möglichst stark erleichtern.

zuverlässig sein. Es soll möglichst wenig Fehler enthalten.

flexibel sein. Das System muss leicht an geänderte Anforderungen des Benutzers anpassbar sein. Die Fehler müssen leicht zu beheben sein.

kostengünstig sein, nicht nur in der Anschaffung, sondern auch im Unterhalt.

verfügbar sein. Das System muss auf jetzigen und zukünftigen Zielplattformen (Hardware, Betriebssystemen etc.) lauffähig bzw. leicht adaptierbar sein. Zur Verfügbarkeit gehört natürlich auch, dass das Softwareprodukt überhaupt existiert und zwar zu dem Zeitpunkt, zu dem es zum Einsatz kommen soll.

5.1. Phasen der Softwareentwicklung

In der Softwaretechnik läuft der Entwicklungsprozess eines Softwareprojektes in Phasen ab. Es gibt verschiedene Phasenmodelle, die auch die Zusammenarbeit zwischen den verschienden Beiteiligten regeln.
Das Urmodell ist das so genannte Wasserfallmodell, welches ein rein sequenzielles Vorgehen vorsah:

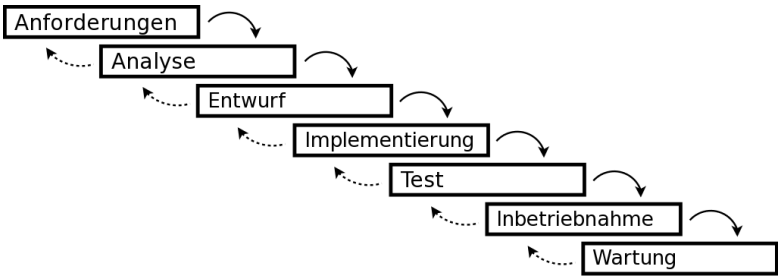

Abbildung 5.1.: Das Wasserfallmodell

Das Spiralmodell hingegen, ist ein generisches Vorgehensmodell, bei dem das Management immer wieder eingreifen kann, da man sich spiralförmig voran entwickelt:

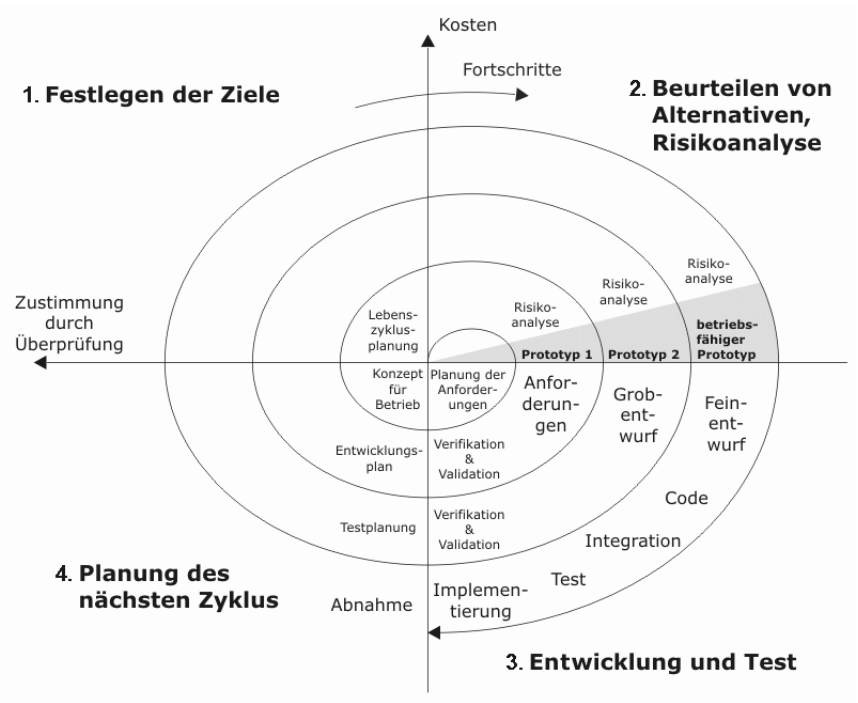

Abbildung 5.2.: Spiralmodell nach Boehm

5.2. UML

Die **Unified Modeling Language** (Vereinheitlichte Modellierungssprache), kurz UML, ist eine grafische Modellierungssprache zur Spezifikation, Konstruktion und Dokumentation von Software-Teilen und anderen Systemen. Bei Modellierung handelt es sich um eine partielle, subjektive Abbildung eines Abschnitts der realen Welt. [Klu11] In der UML gibt es folgende Diagramme:

- Strukturdiagramme
  - Klassendiagramm -Class Diagram
  - Objektdiagramm - Object Diagram
  - Komponentendiagramm - Component Diagram
  - Paketdiagramm - Package Diagram
  - Kompositionsstrukturdiagramm - Composite Structure Diagram
  - Verteilungsdiagramm - Deployment Diagram
- Verhaltensdiagramme
  - Aktivitätsdiagramm - Activity Diagram
  - Anwendungsfalldiagramm - Use Case Diagram
  - Zustandsdiagramm -State Machine Diagram
  - Interaktionsdiagramme
    - Interaktionsübersichsdiagramm - Interaction Overview Diagram
    - Sequenzdiagramm - Sequence Diagram
    - Kommunikationsdiagramm - Communication Diagram
    - Zeitverlaufsdiagramm - Timing Diagram

5.2.1. Das Klassendiagramm

Klassendiagramme stellen die statische Struktur eines Systems dar. Sie zeigen die Klassen, die Eigenschaften der Klassen (Attribute), das Verhalten (Operationen) der Klassen und die Beziehungen zwischen den Klassen. Sie sind der zentrale Diagrammtyp der UML und werden in allen Phasen der Softwareentwicklung eingesetzt. Die Notation lautet wie folgt:

Die Klasse

Eine Klasse kann als Rechteck dargestellt werden, das den Klassennamen enthält. Üblicherweise bestehen Klassen aus drei Bereichen; der obere Bereich enthält den Stereotyp, das Paket zu dem die Klasse gehört und den Namen. Im mittleren Bereich werden die Attribute angegeben und im unteren Bereich stehen die Operationen der Klasse. Die Syntax für die Deklaration von Attributen lautet:

$$[Sichtbarkeit]Name[: Typ][= Wert]$$

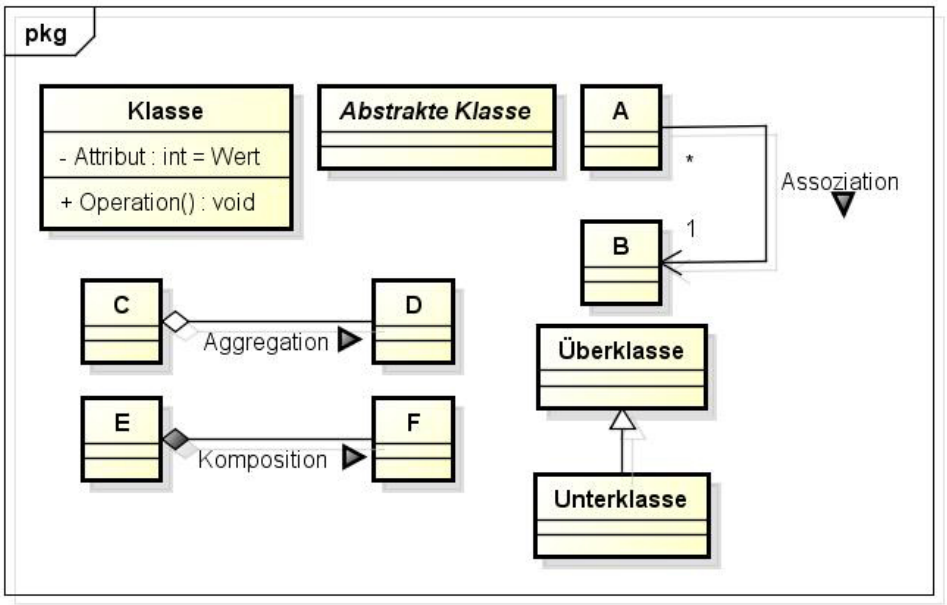

Abbildung 5.3.: Beispiel-Klassendiagramm

Die Syntax für die Deklaration von Operationen lautet :

$$[Sichtbarkeit]Name[(Parameterliste)][: Returntyp]$$

Dabei gibt die Sichtbarkeit an, wie die Sichtbarkeit eines Elementes relativ zu seiner Umgebung ist. Die Sichtbarkeit gibt also an, welche Elemente auf ein Attribut, bzw. auf eine Operation zugreifen können. Der Zugriff auf ein Attribut definiert den lesenden und schreibenden Zugriff auf das Attribut; die Sichtbarkeit von Operationen gibt an, welche Elemente die Operation aufrufen können. Folgende Sichtbarkeitsmodi sind definiert:

public Jedes andere Element hat Zugriff.

private Der Zugriff ist auf die Objekte der Klasse selbst beschränkt

protected Zugriff besteht nur für die definierende Klasse und die Vererbungslinien, die von ihr ausgehen.

package Das Element ist sichtbar für alle Klassen, die sich im selben Paket befinden.

Listing 5.1: Implementierung Klasse

```
1 public class Klasse
2 {
3   private int Attribut;
4   public void Operation() {
5   [...]
6 }
```

Abstrakte Klasse

Der Name einer abstrakten Klasse wird kursiv geschrieben. Alternativ kann die Eigenschaft abstract angegeben werden.

Listing 5.2: Implementierung abstrakte Klasse

```
1 public abstract class AbstrakteKlasse [...]
```

Es gibt zudem auch noch statische Klassen & Attribute, welche in der UML unterstrichen dargestellt werden.

Die Assoziation

Eine Linie zwischen den Klassen stellt eine Assoziation dar. Eine Assoziation ist eine Beziehung zwischen Klassen. Die Objekte der Klassen kommunizieren über die Assoziationen miteinander. Die Assoziation kann einen Namen haben. Ein Pfeil an dem Assoziationsnamen gibt die Leserichtung des Namens an. An den Assoziationsenden können die Rollen der beteiligten Klassen und die Multiplizität angegeben werden. Mit einem Pfeil an der Assoziation kann die Navigationsrichtung angegeben werden. Der Pfeil drückt die Zugriffsrichtung der Objekte aus. Objekt A greift auf B zu, B greift nie auf A zu. Die Impelemtationsmöglichkeiten hängen von der Situation und Multiplizität ab.

Vererbung

Die Vererbung ist ein Grundkonzept objektorientierter Programmiersprachen und dient der Wiederverwendung von Quellcode. Sie wird verwendet um Eigenschaften einer Oberklasse an Unterklassen zu vererben. Alle Eigenschaften (Attribute und Operationen) der Oberklasse, die für die Unterklasse sichtbar sind, werden an diese vererbt. Sie sind in der Unterklasse benutzbar, als wären sie in der Klasse selbst definiert. Die Unterklassen dürfen weitere, speziellere Eigenschaften haben. Aus der Sichtweise der Oberklasse sind die Unterklassen immer speziellere Klassen; aus der Sichtweise der Unterklassen ist die Oberklasse die allgemeinere, generellere Klasse. Deshalb wird die Vererbung auch Generalisierung oder Spezialisierung genannt. Vererbungsbeziehungen werden mit einem Pfeil dargestellt. Die Pfeilspitze zeigt auf die Oberklasse. Die Oberklasse vererbt ihre Eigenschaften an die Unterklasse(n).

Listing 5.3: Implementierung Vererbung

```
1 public class Oberklasse { [...] }
2 public class Unterklasse extends Oberklasse { [...] }
```

Aggregation

Die Aggregation wird verwendet um zwischen Klassen eine Teile-Ganzes-Beziehung aufzubauen. Die Raute befindet sich an dem Ende des Ganzen. Die Aggregation ist eine spezielle Art der Assoziation. Da das Ganze die Teile enthält, sollten am Assoziationsende der Teile ein Navigationspfeil stehen. Da die Aggregation eine Spezialform der Assoziation ist, wird sie wie eine Assoziation implementiert. - Je nach Multiplizitäten.

Komposition

Die Komposition als Sonderfall der Aggregation beschreibt ebenfalls die Beziehung zwischen einem Ganzen und seinen Teilen. Der Unterschied zur Aggregation ist, dass die Existenz eines Objekts, das Teil eines Ganzen ist, von der Existenz des Ganzen abhängig ist. Ein Objekt kann dabei immer nur Teil maximal eines Ganzen sein (Multiplizität 0..1 oder 1).
In Java gibt es verschiedene Möglichkeiten, eine Komposition zu implementieren. Dabei ist jedoch keine Optimal, da sich die Funtkionsweise von Java mit der erwünschten Umsetzung der Komposition widerspricht.

1. a erschafft b, damit kein Anderer b kennt; a verwendet den Konstruktor von b mit "einfachen" Datentypen
2. Wir legen eine Kopie des enthaltenen Objektes an
3. Klasse B wird in A definiert

Die Beispielhafte Implementation erfolgt folgendermaßen:

1. :

Listing 5.4: Implementierung durch Erschaffung des Teils vom Ganzen

```
1  public class Ganzes
2  {
3    Teil b1, b2;
4    public Ganzes(...)
5     {
6        b1 = new Teil(...);
7        b2 = new Teil(...);
8     }
9  }
10 public class Teil{ [...] }
11
```

2. :

Listing 5.5: Implementierung durch Anlegen einer Kopie

```
1  public class Ganzes
2  {
3    Teil b1, b2;
4    public Ganzes(Teil b1, Teil b2)
5     {
6        this.b1 = new Teil(b1);
7        this.b2 = new Teil(b2);
8     }
9  }
10 public class Teil
11 {
12   public Teil(Teil t)
13   {
14     //kopiere das bergebene Objekt t
15   }
16 }
17
```

3. :

Listing 5.6: Implementierung durch enthaltene Klassen

```
1     public class Ganzes
2     {
3       public class Teil{ [...] }
4       Teil b1, [...]
5     }
6
```

6. Sortieralgorithmen

Teilweise übernommen aus www.sortieralgorithmen.de.

6.1. Bubblesort

Der Name "Bubblesort"kommt von bubble (dt. Blase), da man seine Funktionsweise sehr gut anhand von langsam aufsteigenden Luftblasen in einer Wassersäule erklären kann.

Listing 6.1: Bubblesort

```
1  public static int[] bubblesort(int[] zusortieren) {
2    int temp;
3    for(int i=1; i<zusortieren.length; i++) {
4      for(int j=0; j<zusortieren.length-i; j++) {
5        if(zusortieren[j]>zusortieren[j+1]) {
6          temp=zusortieren[j];
7          zusortieren[j]=zusortieren[j+1];
8          zusortieren[j+1]=temp;
9        }
10     }
11   }
12   return zusortieren;
13 }
```

Ein Feld wird einmal vollständig durchlaufen. Dabei werden die jeweiligen Nachbarelemente miteinander verglichen und ggf. ausgetauscht. Am Ende befindet sich das größte Element am Ende des Feldes. Dieser Schritt wird nun mit dem kleineren Teilfeld (Feld ohne das letzte Element) wiederholt und wiederholt und ... Und irgendwann sind wir fertig und die Elemente sind sortiert.
In einer Wassersäule befinden sich unterschiedlich große Luftblasen. Die unterste Luftblase steigt nun langsam auf. Während sie an kleineren problemlos vorbeikommt, wird sie durch größere gestoppt. Durch den Zusammenprall setzt sich die größere Luftblase in Bewegung, bis auch diese gestoppt wird oder am oberen Säulenende ankommt. Nun setzt sich abermals die unterste Luftblase in Bewegung bis ... Und wenn die Wassersäule eine endliche Anzahl Luftblasen enthält, dann kann irgendwann keine Luftblase mehr aufsteigen, da sich über ihr eine noch größere befindet. Die Luftblasen sind dann der größe nach von unten (klein) nach oben (groß) sortiert.
Eine Seifenblase kann genau zwei Elemente in sich einschließen. Diese Seifenblase steigt nun langsam auf. Das schwerere der beiden Elemente in der Blase kann nicht nach oben getragen werden und fällt unten raus, während oben ein neues Element hineinkommt. Dadurch trägt die Seifenblase das leichteste Element bis ganz nach oben. Hier zerplatzt die Seifenblase und unten entsteht eine neue.
Aufgrund der Vergleiche benachbarter Elemente wird dieses Verfahren auch als “Sortierung durch Nachbarvergleiche” bezeichnet.

6.2. Selectionsort

Der Name SSelectsort"kommt von selection (dt. Auswahl), da in jedem Schritt das größte (oder kleinste) Element selektiert wird.

Listing 6.2: Bubblesort

```
public static int[] selectionsort(int[] zusortieren) {
  for (int i = 0; i < zusortieren.length - 1; i++) {
    for (int j = i + 1; j < zusortieren.length; j++) {
      if (zusortieren[i] > zusortieren[j]) {
        int temp = zusortieren[i];
        zusortieren[i] = zusortieren[j];
        zusortieren[j] = temp;
      }
    }
  }
  return zusortieren;
}
```

Ein Feld wird einmal vollständig durchlaufen. Dabei wird durch einfache Vergleiche das größte Element herausgesucht (selektiert) und zum Schluss an das Feldende gepackt. Dieser Schritt wird nun mit dem kleineren Teilfeld (Feld ohne das letzte Element) wiederholt und wiederholt und ... Und irgendwann sind wir fertig und die Elemente sind sortiert.
Aufgrund der Auswahl von Elementen wird dieses Verfahren auch als “Sortierung durch Auswahl” bezeichnet.

6.3. Insertionsort

Der Name Ïnsertsort"kommt von insertion (dt. Einfügen), da in jedem Schritt ein Element in eine bereits sortierte Gruppe von Elementen eingefügt wird.

Listing 6.3: Bubblesort

```
public static int[] insertionSort(int[] zusortieren) {
  int temp;
  for (int i = 1; i < zusortieren.length; i++) {
    temp = zusortieren[i];
    int j = i;
      while (j > 0 && zusortieren[j - 1] > temp) {
        zusortieren[j] = zusortieren[j - 1];
        j--;
      }
    zusortieren[j] = temp;
  }
  return zusortieren;
}
```

Ein kleineres bereits sortiertes Teilfeld wird um ein Element erweitert. Dieses neu hinzugekommene Element wird durch Vergleiche und Verschiebungs- oder Vertauschungsoperationen an die “richtige” Stelle dieses größeren Teilfeldes eingefügt. Dieser Schritt wird wiederholt, bis das Teilfeld maximal ist (also dem Gesamtfeld entspricht). Dann sind wir fertig und die Elemente sind sortiert.
Bei einem Kartenspiel bekommt man nacheinander eine bestimmte Anzahl von Karten

ausgehändigt. Erst hat man eine in der Hand, dann werden es zwei, drei, vier, ... Damit man da den Überblick behält sorgt man am besten dafür, daß die Karten sortiert in der Hand liegen. Kommt eine neue Karte hinzu, wird diese direkt an die richtige Position gesteckt.
Aufgrund des Einfügens von Elementen in eine sortierte Menge wird dieses Verfahren auch als “Sortierung durch Einfügen” bezeichnet.

6.4. Quicksort

Der Name "Quicksort"kommt von quick (dt. schnell) und spielt auf sein (in der Regel) phantastisches Laufzeitverhalten an.

Listing 6.4: Quicksort mit Privot-Element rechts

```
1  public void quickSort(int links, int rechts, int feld[]) {
2    int i=links, j=rechts-1;
3    int pivot;
4    if (rechts>links) {
5      pivot = feld[rechts];
6      while (i<j) {
7        while (feld[i] < pivot && i < rechts) {i++;}
8        while (feld[j] > pivot && j > links)  {j--;}
9        if(i<j) exchange(i,j,feld);
10     }
11   exchange(i,rechts,feld);
12   quickSort(links,i-1, feld);
13   quickSort(i+1,rechts, feld);
14   }
15 }
```

Ein Feld wird in zwei (in der Regel unterschiedlich große) Teilfelder aufgeteilt, die Elemente werden dabei so vertauscht, daß alle Elemente des linken Teilfeldes kleiner (oder gleich) den Elementen des rechten Teilfeldes sind. Die einzelnen Teilfelder werden dann wieder sortiert... Und irgendwann sind wir fertig und das gesamte Feld liegt sortiert vor.
Die Aufteilung eines Feldes in zwei Teilfelder geschieht aufgrund von Vergleichen mit einem speziellen (Am Anfang der Teilung gewählten) Pivotelement. Deshalb wird dieses Verfahren auch als “Sortierung durch Pivotisierung” oder “Sortierung durch Partitionierung” bezeichnet.

6.5. Laufzeitanalyse

6.5.1. Die O-Notation

Für die Effizienzanalyse von Algorithmen wird eine spezielle mathematische Notation verwendet, die als O-Notation bezeichnet wird. Die O-Notation erlaubt es, Algorithmen auf einer höheren Abstraktionsebene miteinander zu vergleichen. Algorithmen können mit Hilfe der O-Notation unabhängig von Implementierungsdetails, wie Programmiersprache, Compiler und Hardware-Eigenschaften, verglichen werden.

Definition 6.5.1. Die Funktion $T(n) = O(g(n))$, wenn es positive Konstanten c und n_0 gibt, so dass $T(n) \leq c \cdot g(n)$ für alle $n \geq n_0$.

Wichtig ist, dass $O(n^2)$ eine Menge darstellt, weshalb die Schreibweise $2n + n^2 \in O(n^2)$ besser ist als die Schreibweise $n^2 + 2n = O(n^2)$.

Klassifikation von Algorithmen

Notation	**Komplexitätsklasse**	**Anschauliche Beschreibung**
$O(1)$	konstant	Die meisten Anweisungen in einem Programm werden nur einmal oder eine konstante Anzahl von Malen wiederholt.
$O(logn)$	logarithmisch	Verdoppelt sich das Argument[1], wächst die Laufzeit um ca. einen konstanten Betrag.
$O(n)$	linear	Verdoppelt sich das Argument, verdoppelt sich auch die ungefähre Laufzeit.
$O(n^2)$	quadratisch	Verdoppelt sich das Argument, vervierfacht sich die ungefähre Laufzeit.
$O(2^n)$	exponentiell	Erhöht sich das Argument um eins, verdoppelt sich die ungefähre Laufzeit.

6.5.2. Stabilität von Sortieralgorithmen

Definition 6.5.2. Ein stabiles Sortierverfahren ist ein Sortieralgorithmus, der die *Reihenfolge der Datensätze, deren Sortierschlüssel gleich sind, bewahrt.*

Wenn bspw. eine Liste alphabetisch sortierter Personendateien nach dem Geburtsdatum neu sortiert wird, dann bleiben unter einem stabilen Sortierverfahren alle Personen mit gleichem Geburtsdatum alphabetisch sortiert.

6.5.3. Zusammenstellung der beschriebenen Sortieralgorithmen

Algorithmus	Laufzeitklasse		stabil?
	worst	best	
BubbleSort	n^2	n	✓
SelectionSort	n^2	n^2	✓
InsertSort	n^2	n	✓
QuickSort	$nlogn$	$nlogn$	⁄

[1] Beispielsweise die Länge eines zu sortierenden Arrays

7. Dynamische Datenstrukturen

tbd

8. Modellieren und Implementieren kontextbezogener Problemstellungen als Netzwerkanwendungen

8.1. Netzwerkprotokolle

tbd

8.1.1. TCP/IP-Referenzmodell

tbd

8.2. Kryptologie

Die Kryptologie ist die Wissenschaft der Verschlüsselung und der Entschlüsselung von Informationen. Auch die Analyse der unterschiedlichen kryptografischen Verfahren, d. h ihre Stärken und Schwächen, zählt zur Kryptologie.
In der Kryptologie gibt es wie in der Netzwerktechnik ein Schichtenmodell, mit Ebenen, die auf einander Aufbauen und voneinander abhängig sind:

Bedrohungen
Ziele
Protokolle
Mechanismen
kryptogr. Algorithmen

8.2.1. Schutzziele

In der Informatik gibt es bestimmte Dinge, die man vor Angriffen schützen will. Die klassischen Schutzziele sind:[1]

Verfügbarkeit eines Dienstes, den man anbietet sollte auch tatsächlich gewährleistet sein. Denial of Service Attacken versuchen gerade dies zu verhindern. Ein konkretes Beispiel mit dem damit verbundenen wirtschaftlichen Schaden wäre, dass Sie ein Produkt auf einer Auktionsplattform, sagen wir einen Sportwagen anbieten. Erfahrungsgemäß

[1] Entnommen aus [Klu11]

steigt der Preis vor allem in der letzten Stunde vor dem Ende der Auktion. Wie würden Sie reagieren, wenn die Auktionsplattform in der letzten Stunde nicht verfügbar ist und ihr Wagen für den Spottpreis von 100 Euro den Besitzer wechselt? Wie stände es mit dem allgemeinen Vertrauen in eine solche Auktionsplattform?

Vertraulichkeit bedeutet, dass bestimmte Informationen nur berechtigten Personen auch Verfügung stehen. Dies betrifft natürlich auch Nachrichten die über öffentliche Netze versandt werden.

Integrität bedeutet, dass Informationen nicht von Unbefugten unberechtigt und unbemerkt verändert werden. Ob diese Informationen veprtraulich sind oder nicht, spielt hierbei keine Rolle. Beim Betreiben einer Webseite haben Sie in der Regel ein großes Interesse an Öffentlichkeit. Sie wären aber sicherlich nicht erfreut für ungewollt für ein zwielichtiges Produkt zu werben.

Verbindlichkeit ist eigentlich kein klassisches Schutzziel, sondern ist erst im letzten Jahrzehnt bedingt durch digitale Signaturen hinzugekommen. Es bedeutet, dass der Sender einer Information später nicht leugnen kann, dass diese Information von ihm versendet wurde. Dies ist z.B. beim Kauf von Produkten im Netz für den Verkäufer ein interessantes Thema.

8.2.2. Protokolle

Ein Protokoll ist ein verteilter Algorithmus, der durch eine Folge von Schritten definiert wird, die exakt die Aktionen spezifiziert, die zwei oder mehr Partner ausführen müssen, um ein bestimmtes Sicherheitsziel zu erreichen. Chiffren, digitale Signaturen, Einweg-Hashfunktionen, Pseudozufallszahlen-Generatoren sind wichtige Werkzeuge bzw. Bausteine, die genutzt werden können, um Protokolle aufzubauen.
Die Verwendung sicherer kryptographischer Bausteine garantiert keineswegs ein sicheres Protokoll. Ein **Protokoll- oder Mechanismus-Fehler** liegt vor, wenn es einem Angreifer gelingt, ein mit dem Protokoll bzw. Mechanismus angestrebtes Sicherheitsziel zu vereiteln, ohne daß er dazu die als Basis verwendeten Algorithmen (z.B. Chiffren und Einweg-Hashfunktionen) brechen muss. Real eingesetzte Protokolle sind deshalb sehr sorgfältig zu entwerfen und zu implementieren, wobei es auf die kleinsten Details ankommen kann. Zur Vermeidung unnötiger Risiken sollte man Protokolle und deren Implementierungen (Programme und Bibliotheken) einsetzen, die einer gründlichen öffentlichen Analyse unterzogen wurden und die allgemein als sicher angesehen werden.
`TBD: Beispiel für Protokolle`

8.2.3. Mechanismen

Kryptologische Mechanismen bezeichnen die Art der kryptografischen Algorithmen, die in den Protokollen verwendet werden.
Die wichtigsten sind:

Symmetrische Verschlüsselung

Beide Teilnehmer verwenden bei einer symmetrischen Verschlüsselung den selben Schlüssel, sowohl um den Klartext zu verschlüsseln, als auch um den Ciphertext wieder zu entschlüsseln. Bei einigen Verfahren sind die Schlüssel zwar nciht die Selben, können jedoch auf einfachste Art aus dem jeweiligen Gegenschlüssel berechnet werden. Der große Nachteil symmetrischer Verfahren liegt in der Nutzung ein- und desselben Schlüssels zur Ver- und Entschlüsselung, d. h. neben der verschlüsselten Information muss auch der Schlüssel übermittelt werden. Das Problem beim Einsatz symmetrischer Verfahren ist, dass der Schlüssel über einen sicheren Kanal übertragen werden muss, denn die Sicherheit des Verfahrens hängt von der Geheimhaltung des Schlüssels ab. Früher wurde der Schlüssel typischerweise durch einen Boten persönlich überbracht. Seit den 1970er Jahren sind mit dem Diffie-Hellman-Schlüsselaustausch asymmetrische Schlüsselaustauschprotokolle bekannt, mit denen auch über einen abgehörten Kanal Schlüssel sicher übertragen werden können. Eine weitere Möglichkeit ist der Einsatz asymmetrischer Verschlüsselungsverfahren um den symmetrischen Schlüssel selbst zu verschlüsseln und ihn so geschützt auch über einen unsicheren Kanal übertragen zu können. Bei der Kommunikation können mit dieser hybriden Verschlüsselung also die Vorteile (beispielsweise die höhere Geschwindigkeit) der symmetrischen Verschlüsselung ausgenutzt werden, während der Schlüssel durch die asymmetrische Verschlüsselung vor dem Zugriff eines Angreifers geschützt wird.

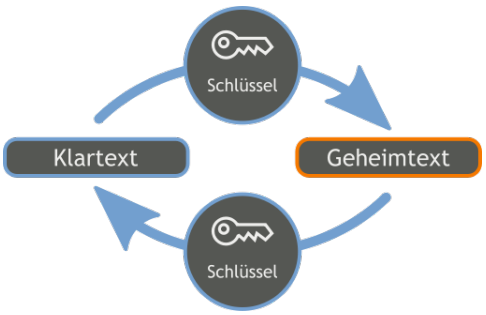

Abbildung 8.1.: Verschlüsselung und Entschlüsselung mit dem gleichen Schlüssel

Asymmetrische Verschlüsselung

Beide Teilnehmer verwenden bei einem asymmetrischen Verschlüsselungsverfahren im Gegensatz zu symmetrischen Verschlüsselungen keinen gemeinsamen geheimen Schlüssel. Ein Benutzer erzeugt ein Schlüsselpaar, das aus einem privaten Schlüssel und einem öffentlichen Schlüssel besteht. Der öffentliche Schlüssel ermöglicht es jedem, Daten für den Inhaber des privaten Schlüssels zu verschlüsseln, oder ihn zu authentifizieren. Der private Schlüssel ermöglicht es seinem Inhaver, mit dem öffentlchen Schlüssel verschlüsselte Daten zu entschlüsseln oder digitale Signaturen zu erzeugen. Der entscheidende Vorteil von asymmetrischen Verfahren ist, dass sie das Schlüsselverteilungsproblem vermindern. Bei symmetrischen Verfahren muss vor der Verwendung ein Schlüssel über einen sicheren, d. h. abhörsicheren und manipulationsgeschützten, Kanal ausgetauscht werden. Da der öffentliche Schlüssel nicht geheim ist, muss bei asymmetrischen Verfahren der Kanal nicht abhörsicher sein; wichtig ist nur, dass der öffentliche Schlüssel dem Inhaber des dazugehörigen geheimen Schlüssels zweifelsfrei zugeordnet werden kann. Dazu kann beispielsweise eine vertrauenswürdige Zertifizierungsstelle ein digitales Zertifikat ausstellen, welches den öffentlichen Schlüssel dem privaten Schlüssel(inhaber)

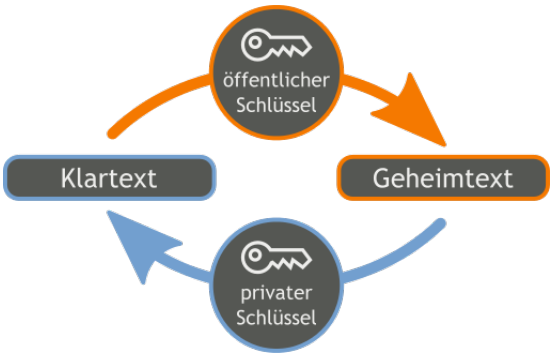

Abbildung 8.2.: Verschlüsselung mit öffentlichem Schlüssel und Entschlüsselung mit privatem Schlüssel

zuordnet. Als Alternative dazu kann auch ohne zentrale Stelle durch gegenseitiges Zertifizieren von Schlüsseln ein sog. Web of Trust aufgebaut werden.

Hashfunktionen

Eine **Hashfunktion** ist eine Abbildung, die eine große Eingabemenge (die Schlüssel) auf eine kleinere Zielmenge (die Hashwerte) abbildet – sie ist daher nicht injektiv. Dabei kann die Eingabemenge auch Elemente mit unterschiedlichen Längen enthalten, die Elemente der Zielmenge haben dagegen meist eine feste Länge. In der Kryptologie werden Hashfunktionen verwendet, um den Inhalt übertragener Daten zu verifizieren. Hier wird daher zusätzlich gefordert, dass Kollisionen sehr schwer zu finden sind, damit modifizierte Daten nicht zufällig den gleichen Hashwert besitzen wie das Original. Eine sog. „Kollision“ tritt dann auf, wenn zwei verschiedenen Eingabedaten derselbe Hashwert zugeordnet wird. Da die Menge der möglichen Hashwerte meist kleiner ist als die der möglichen Eingaben, sind solche Kollisionen dann prinzipiell unvermeidlich, weshalb es Verfahren zur Kollisionserkennung geben muss. Eine gute Hashfunktion zeichnet sich dadurch aus, dass sie für die Eingaben, für die sie entworfen wurde, möglichst wenige Kollisionen erzeugt.

8.2.4. Kryptographische Algorithmen

Wir definieren uns:

- den Klartext M
- den Ciphertext C
- den Schlüssel K, beziehungsweise die Schlüsselpaare (e, N) und (d, N), wobei e der öffentliche Schlüssel und d der private Schlüssel ist.
- die Verschlüsselungsfunktion $C = E(M)$
- die Entschlüsselungsfunktion $M = D(C)$

Caesar

Die Caesar-Verschlüsselung ist ein symmetrisches, monoalphabetisches Verschlüsselungsverfahren. Bei der Verschlüsselung wird jeder Buchstabe des Klartexts auf einen Geheimtextbuchstaben abgebildet. Diese Abbildung ergibt sich, indem man die Zeichen eines geordneten Alphabets um eine bestimmte Anzahl zyklisch nach rechts verschiebt (rotiert). Die Anzahl der verschobenen Zeichen bildet den Schlüssel, der für die gesamte Verschlüsselung unverändert bleibt.
Man bildet alle Zeichen des gewünschten Alphabets auf einen Restklassenring ab. Dann gilt monographisch für jeden Buchstaben des Textes:

$$E_K(M) = (M + K) \mod 26$$

$$D_K(C) = (C - K) \mod 26$$

Vigenère

Die Vigenère-Verschlüsselung ist ein symmetrisches, polyalphabetisches Verschlüsselungsverfahren. Die Verschlüsselung arbeitet ähnlich wie die Caesar-Verschlüsselung. Der Schlüssel ist hier ein String von mehreren Buchstaben des verwendeten Alphabets. Jeder Buchstabe des Textes wird mit der Ordnung des jeweiligen Buchstabens des Schlüssels nach dem Caesar-Prinzip substituiert.
Verwendet man das Vigenère-Quadrat, kann man den Geheimtext direkt ablesen. Die Ordnung des Schlüssels und die des Textes stehen in der ersten Reihe und Spalte. Der Ciphertext befindet sich im Körper.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
0	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
1	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
2	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
3	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
4	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
5	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
6	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
7	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
8	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
9	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
10	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
11	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
12	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
13	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
14	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
15	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
16	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
17	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
18	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
19	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
20	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
21	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
22	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
23	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
24	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
25	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

RSA

Die RSA-Verschlüsselung ist ein asymmetrisches Verschlüsselungsverfahren. Es wird zunächst vom Empfänger der Nachricht ein Schlüsselpaar generiert.

1. Wähle zufällig und stochastisch unabhängig zwei Primzahlen $p \neq q$.
2. Berechne den RSA-Modul $N = p \cdot q$.
3. Berechne die Eulersche φ-Funktion von N: $\varphi(N) = (p-1) \cdot (q-1)$.
4. Wähle eine zu $\varphi(N)$ teilerfremde Zahl e, für die gilt $1 < e < \varphi(N)$.
5. Berechne den Entschlüsselungsexponenten d als Multiplikatives Inverses von e bezüglich des Moduls $\varphi(N)$. Es gilt also:

$$e \cdot d \equiv 1 \mod \varphi(N)$$

Nun werden p, q und $\varphi(N)$ verworfen. Dann gilt:

$$E_{(e,N)}(M) = (M^e) \mod N$$

$$D_{(d,N)}(C) = (C^d) \mod N$$

Affine Verschlüsselung

Bei der affinen Verschlüsselung wird der Klartext, Buchstabe für Buchstabe, nach einer bestimmten mathematischen Formel verschlüsselt. Siehe dazu auch 4.1.7.

8.2.5. Angriffe auf kryptographische Algorithmen

Es gibt verschiedene Angriffsarten, die auf kryptographische Algorithmen ausgeführt werden können:[2]

Ciphertext-only-Angriff Der Kryptoanalytiker verfügt über den Chiffretext mehrerer Nachrichten, die mit demselben Verschlüsselungsalgorithmus chiffriert wurden.

Known-plaintext-Angriff Der Kryptoanalytiker verfügt nicht nur über diverse Chiffretexte, sondern darüber hinaus auch über die zugehörigen Klartexte.

Chosen-plaintext-Angriff Der Kryptoanalytiker verfügt nicht nur über die Chiffretexte und Klartexte diverser Nachrichten, sondern kann darüber hinaus den zu verschlüsselnden Klartext selber festlegen.

Kryptoanalyse mit Gewalt Der Kryptoanalytiker bedroht, erpresst oder quält jemanden solange, bis er ihm den Schlüssel verrät. Bestechung wird gelegentlich Ängriff mit gekauftem Schlüssel"genannt.

[2] Entnommen aus [Klu11]

9. Relationale Datenbanken

Definition 9.0.1. Eine *Datenbank* ist eine selbstständige, auf Dauer und flexiblen und sicheren Gebrauch ausgelegte Datenorganisation, die sowohl eine Datenbasis als auch eine zugehörige Datenverwaltung umfasst. Eine Datenbank dient dazu, eine große Menge von Daten strukturiert zu speichern und zu verwalten.

Grundsätzlich kann man sich eine **relationale Datenbank** als eine Sammlung von Tabellen – den *Relationen* – vorstellen, in welchen Datensätze abgespeichert sind. Jeder Datensatz ist eine Zeile *(Tupel)* in einer Tabelle. Jedes Tupel besteht aus einer Menge von Attributwerten, den Spalten der Tabelle. Das Relationenschema legt dabei die Anzahl und den Typ der Attribute für eine Relation fest.

Satz 9.0.1. *Die **referentielle Integrität** besagt, dass Attributwerte eines Fremdschlüssels auch als Attributwert des Primärschlüssels vorhanden sein müssen. Somit dürfen Datensätze (über ihre Fremdschlüssel) nur auf existierende Datensätze verweisen.*

9.0.6. Begriffsvergleich

UML	**ER-Diagramm**	**Relationenmodell**	**Datenbank**
Klasse	Entitätstyp	Relationstyp	Kopfzeile
Objekt	Entität	Tupel	Zeile
Objektmenge, Instanzmenge	Entitätsmenge	Relation	Tabelle
Assoziation	funktionale Beziehung	Fremdschlüssel	Spalte(-nüberschrift)
Attribut	Attribut	Attribut	Spaltenüberschrift
Attributwert	Attributwert	Attributwert	Zelle

9.1. Normalisierung

Man "normalisiert" Datenbanken, um Anomalien zu beseitigen oder Redundanzen zu minimieren.

9.1.1. 1. Normalform

Definition 9.1.1. Eine Relation befindet sich in **1. Normalform**, wenn alle Attribute einen atomaren Wertebereich haben (atomar sind).

9.1.2. 2. Normalform

Definition 9.1.2. Eine Attribut B ist von einem Attribut A **funktional abhängig**, wenn durch jeden Wert von A eindeutig ein Wert von B bestimmt wird.

$$A \to B$$

Definition 9.1.3. Eine Attribut B ist von einer Attributkombination (A_1, A_2) **voll funktional abhängig**, wenn B von der Kombination (A_1, A_2) funktional abhängig ist, nicht aber bereits von A_1 oder A_2.

Definition 9.1.4. Eine Relation befindet sich in **2. Normalform**, wenn sie in der 1. Normalform ist und zusätzlich jedes Nichtschlüsselattribut vom Primärschlüssel voll funktional abhängig ist und nicht bereits von einem Teil des Schlüsselattributs.

Regel zum Prüfen der Bedingung: Wenn Attribute *von einem Teil des Schlüssels eindeutig identifiziert werden*, dann liegt keine 2. Normalform vor!
Schrittfolge zur Herstellung der zweiten Normalform:

1. Primärschlüssel der gegebenen Relation festlegen, falls dieser nur aus einem Attribut besteht, so liegt bereits 2. NF vor.
2. Untersuchung, ob aus Teilschlüsselattributen bereits weitere Attribute folgen. Falls nicht liegt bereits die 2. NF vor. Falls Abhängigkeiten gefunden werden, dann
3. Neue Relation bilden, die das Teilschlüsselattribut und alle von diesem abhängigen Nichtschlüsselattribute enthält. Das Teilschlüsselattribut wird in der neuen Relation der Primärschlüssel.
4. Löschen der ausgelagerten Nichtschlüsselattribute in der Ausgangsrelation.
5. Vorgang ab 2. wiederholen, bis alle Nichtschlüsselattribute vom gesamten Schlüssel funktional abhängig sind.

9.1.3. 3. Normalform

Definition 9.1.5. Eine Relation befindet sich in **3. Normalform**, wenn sie in der 2. Normalform ist und zusätzlich jedes Nichtschlüsselattribut nicht transitiv vom Primärschlüssel abhängig ist, d.h. aus keinem Nichtschlüsselattribut folgt ein anderes Nichtschlüsselattribut.

Regel zum Prüfen der Bedingung: Wenn aus einem *Nichtschlüsselattribut ein anderes Nichtschlüsselattribut folgt*, dann liegt keine 3. Normalform vor!
Schrittfolge zur Herstellung der dritten Normalform:

1. Untersuchung, ob aus Nichtschlüsselattributen andere Nichtschlüsselattribute folgen. Falls nicht liegt bereits die 3. NF vor. Falls Abhängigkeiten gefunden werden, dann
2. Neue Relation bilden, die das Nichtschlüsselattribut (wird nun Primärschlüssel der neuen Relation) und die von ihm abhängigen Attribute enthält.

3. Löschen der ausgelagerten Nichtschlüsselattribute mit Ausnahme des Attributes, das in der neuen Relation Primärschlüssel ist.

4. Vorgang ab 2. wiederholen, bis keine Abhängigkeiten mehr bestehen

9.2. Das Entity-Relationship-Modell

9.2.1. Elemente des ER-Modells und deren Darstellung

Entität und Attribut

Definition 9.2.1. Eine **Entität** ist ein eindeutig identifizierbares Objekt oder ein eindeutig identifizierbarer Sachverhalt der realen Welt oder der Vorstellungswelt. Die Entität wird durch ihre **Attribute** bestimmt. Die bei einer bestimmten Entität auftretenden Werte sind **Attributwerte**.
Ein **Entitätstyp** ist eine *abstrakte Beschreibung einer Menge von Entitäten mit gleichen Attributen*. Die Beschreibung enthält einen Typnamen und eine Menge von Attributen. Eine Entität ist ein eindeutig identifizierbares Element des Entitätstyps.

⇢ In der grafische Notation im Entity-Relationship-Diagramm wird der Entitätstyp als bezeichnetes **Rechteck** dargestellt. Seine Attribute werden Ellipsen dargestellt, die eine Verbindung zum Entitätstyp haben.

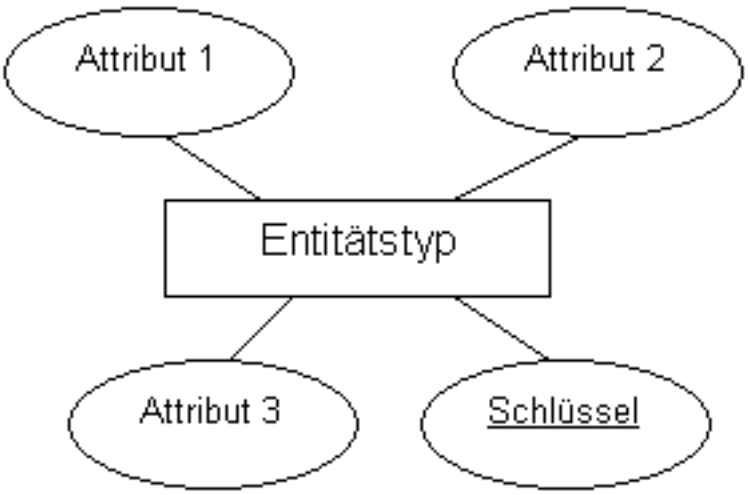

Abbildung 9.1.: Darstellung von Entitätstypen und zugehörigen Attributen

Schlüssel

Definition 9.2.2. Der **Primärschlüssel** ist eine minimale Kombination von Attributen, durch deren Werte jede Entität eindeutig identifiziert wird. Die Werte dürfen sich während der Existenz der Entität nicht ändern. Wir unterscheiden zwischen:

einfacher Schlüssel der Primärschlüssel besteht aus einem Attribut

zusammengesetzter Schlüssel der Primärschlüssel besteht aus mehreren Attributen, jedes Attributbezeichnet man als Teilschlüsselattribut.

künstlicher Schlüssel das Attribut wurde zusätzlich für den Entitätstyp erschaffen (ID,..).

⇢ Im Entity-Relationship-Modell werden die Attribute des Schlüssels unterstrichen.

Beziehungen

Definition 9.2.3. Eine **Beziehung** verbindet eine oder mehrere Entitäten miteinander. Assoziieren stets zwei Entitäten miteinander, so spricht man von *binärer Beziehung*. Ein **Beziehungstyp** umfasst alle Beziehungen, die gleichartig und wechselseitig zwischen zwei Entitätstypen bestehen. Ein Beziehungstyp kann Attribute besitzen.

⇢ Für die Darstellung von Beziehungstypen nutzt man das Rautensymbol und notiert darin den Beziehungstyp als Name.

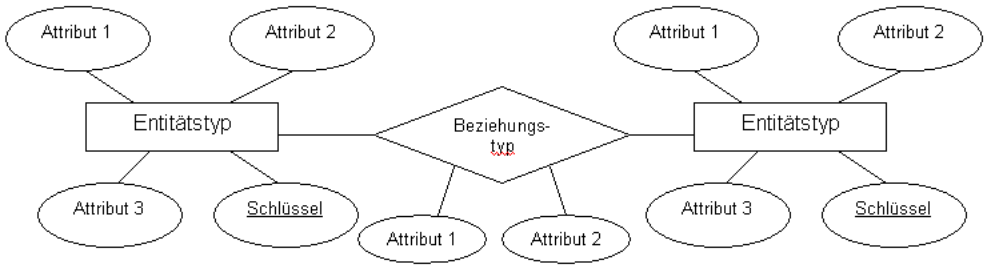

Abbildung 9.2.: Darstellung von Beziehungstypen und zugehörigen Attributen

Kardinalität und Optionalität

Definition 9.2.4. Die **Kardinalität** zwischen dem Entitätstyp 1 und dem Entitätstyp 2 gibt an, wie viele Entitäten des Entitätstyps 2 höchstens mit einer Entität des Entitätstyps 1 in Beziehung stehen.

Für die Datenstrukturierung interessieren nicht die genauen Zahlen, sondern nur die durch die Chen-Notation vorgegebenen Typen

- höchstens eine Entität (1),
- mehrere Entitäten (n oder m).

Da der Beziehungstyp wechselseitig ist, wird die Kardinalität durch zwei Angaben vollständig beschrieben.
In der *modifizierten Chen-Notation* lässt sich die **Optionalität** durch Hinzufügen eines *cs (von engl. can)* darstellen.

9.3. Das Relationenmodell

9.3.1. Notation

Die Notation erfolgt folgendermaßen:

Entitätstyp(Primärschlüssel, Nichtschlüsselattribut, ↑Fremdschlüssel)

9.3.2. Regeln für die Transformation des ERM in das relationale Datenbankmodell

1. Entitätstypen:
   - Jeder Entitätstyp wird in ein eigenes Relationsschema (Tabelle) abgebildet.
   - Schlüssel werden kenntlich gemacht.
2. Beziehungstypen:
   - Jeder Beziehungstyp wird in ein eigenes Relationsschema abgebildet.
   - Die Primärschlüssel der beiden beteiligten Entitätstypen werden zusätzliche Attributen des Relationsschemas.
   - Der (Teil-)Schlüssel des Relationsschemas bildet sich in Abhängigkeit von der Kardinalität wie folgt:

Typ	Schlüssel
1:1	einer der Primärschlüssel der beiden beteiligten Entitätstypen
1:n	der Primärschlüssel des zweiten Entitätstyps (also der "n-Entität")
n:m	beide Primärschlüssel der beteiligten Entitätstypen in neuem Relationstyp

9.4. MySQL

9.4.1. SQL-Operationen

SQL (Structured Query Language) ist eine Programmiersprache der 4. Generation und *die* Sprache zum Aufbau, zur Verwaltung und zur Abfrage von relationalen Datenbanken. Sie wurde von IBM im Rahmen eines Forschungsprojektes entwickelt und 1987 international standardisiert. (Fast) alle Datenbanksysteme arbeiten mit dieser Sprache.

Befehle zur Definition von Tabellen und anderer Datenstrukturen

Listing 9.1: Databank erzeugen

```
1 CREATE DATABASE "datenbankname";
```

Listing 9.2: Tabelle erzeugen

```
1 CREATE TABLE "Tabellen_Name"
2 ("Spalte 1" "Datentyp_Spalte_1",
3 "Spalte 2" "Datentyp_Spalte_2",
4 ... );
```

Listing 9.3: Tabelle löschen

```
DROP TABLE "Tabellen_Name";
```

Listing 9.4: Tabellenaufbau ändern

```
ALTER TABLE "Tabellen_Name"
[Alter Spezifikation];
```

[Alter Spezifikation] hängt von der Art der gewünschten Änderung ab. Für die oben aufgeführten Anwendungszwecke lauten die entsprechenden Anweisungen:

- Spalte hinzufügen: ADD “Spalte 1” “Datentyp für Spalte 1”
- Spalte löschen: DROP “Spalte 1”
- Spaltenname ändern: CHANGE “alter Spaltenname” “neuer Spaltenname” “Datentyp für neuen Spaltennamen”
- Datentyp einer Spalte ändern: MODIFY “Spalte 1“ ”neuer Datentyp“

Befehle zur Datenmanipulation und Datenabfrage

tbd

Listing 9.5: Tabelle abfragen

```
SELECT {spalten | *}
  FROM tabelle [alias] [tabelle [alias]] ...
    [WHERE {bedingung | unterabfrage}]
      [GROUP BY spalten]
      [ORDER BY spalten [ASC | DESC]...];
```

Die Syntax lässt sich wie folgt verstehen:

Klausel	Erläuterung
SELECT	**Wähle** die Werte aus der/den Spalte(n)
FROM	... **aus** der Tabelle bzw. den Tabellen ...
WHERE	... **wobei** die Bedingung(en) erfüllt sein soll(en) ...
GROUP BY	... und **gruppiere** die Ausgabe von allen Zeilen mit gleichem Attributwert zu einer einzigen ...
ORDER BY [ASC/DESC]	... und **sortiere** nach den Spalten *[auf- bzw. absteigend]*.

Bedingungen lassen sich mit **AND**, **OR** und **NOT** verknüpfen. Das **Sternsymbol** steht als Wildcard für eine beliebige Folge von Zeichen. Soll ein einzelnes Zeichen ausgeblendet werden, so benutzt man das Fragezeichen als Joker.

Operator	Erklärung
= < <= >= > <>	vergleicht ein Attributwert mit einem anderen bzw. Konstante auf Gleichheit, kleiner als, kleiner gleich, größer gleich, größer, Ungleichheit
BETWEEN ... AND ...	vergleicht, ob der Attributwert zwischen zwei Grenzen liegt
IN (..., ..., ...)	vergleicht, ob der Attributwertein Element der Menge ist
LIKE	vergleich von Zeichenketten anhand von Ähnlichkeitsoperatoren mit Unterscheidung auf Groß- und Kleinschreibung: %: Platzhalter für beliebiege Zeichen _: Platzhalter für ein Zeichen
IS (NOT) NULL	prüft, ob ein Attributwert (nicht) undefiniert ist

Listing 9.6: Inner Join

```
1 SELECT "Spaltenliste"
2   FROM "Haupttabelle"
3   INNER JOIN "NebenTabelle" ON "Bedingung2;
```

Der Join gibt im Gegensatz zum Select an genau zwei Tabellen nicht das kartesisches Produkt ($A \times B$) der beiden Tabellen aus.

9.4.2. Datentypen in MySql (Auswahl)

char(n) Zeichenkette mit n Zeichen $n \leq 255$, Rest wird mit 0en aufgefüllt

varchar(n) Zeichenkette von variabler Länge $m \leq 255$

text Text mit maximaler Länge: 65.535

date Datum

year Yahr

integer(n) Ganzzahl

float(m) Gleitkommazahl, m Nachkommastellen

decimal(n,m) Festkommazahl n Stellen und m Nach dem Komma

boolean Wahrheitswert

Teil III.

Anhang

Literaturverzeichnis

[ABMG+05] Andelfinger, Urs ; Bühler, Frank ; Michael Guist, Stephan K. ; Raffius, Gerhard ; Schestag, Inge ; Weber, Wolfgang ; Winkler, Gerhard:
Softwaretechnik - Vorlesungsskript / Hochschule Darmstadt.
2005. –
Forschungsbericht

[Art98] Artin, Michael:
Algebra.
Inhaltlich unveränd. Nachdr. der geb. dt. Erstausg. von 1993.
Basel ; Boston ; Berlin : Birkhäuser, 1998 (Grundstudium Mathematik ;).
`http://digitool.hbz-nrw.de:1801/webclient/DeliveryManager?pid=1811130&custom_att_2=simple_viewer`. –
ISBN 3–7643–5938–2. –
Verfasserangabe: Michael Artin. Aus dem Engl. übers. von Annette A'Campo ; 1998 ; Quelldatenbank: HBZOEB ; Format:marcform: print ; Umfang: XIII, 705 S. ; graph. Darst. ; 24 cm

[Bal96] Balzert, Helmut:
Lehrbuch der Software-Technik.
Heidelberg u.a. : Spektrum, Akad. Verl., 1996 (Lehrbücher der Informatik).
`http://digitool.hbz-nrw.de:1801/webclient/DeliveryManager?pid=3709381&custom_att_2=simple_viewer`. –
ISBN 3–8274–0301–4. –
Verfasserangabe: Helmut Balzert ; Erschienen: Bd. 1 - 2 ; Quelldatenbank: HBZ

[Bou10] Bouw, Prof. Dr. Irene I.:
Elementare Zahlentheorie, Vorlesungsskript / Universität Ulm.
Version: 2010.
`http://hbbk-ilias.de/ilias.php?ref_id=66988&cmd=sendfile&cmdClass=ilrepositorygui&cmdNode=bu&baseClass=ilrepositorygui`.
2010. –
Forschungsbericht

[Klu11] Kluth, Thomas:
LK Informatik Version 0.2.9.4 / Hans-Böckler Berufskolleg.
2011. –
Forschungsbericht

[MR10] Maier, Prof. Dr. H. ; Reck, Dipl.-Math. Hans-Peter:

Angewandte Diskrete Mathematik, Vorlesungsskript / Institut für Zahlentheorie und Wahrscheinlichkeitstheorie Universität Ulm.
2009/10. –
Forschungsbericht

Index

.1. Gruppen, Ringe, Körper

Entnommen aus dem Propädeutikum der Universität Leipzig.

5. Gruppen, Ringe, Körper

5.1. Gruppen

Die Gruppentheorie, als mathematische Disziplin im 19. Jahrhundert entstanden, ist ein Wegbereiter der modernen Mathematik. Beispielsweise folgt die Gruppe, die aus den Drehungen eines regulären n-Ecks in der Ebene um Vielfache des Winkels 360°/n besteht, denselben Gesetzen wie die Addition der ganzen Zahlen modulo n. Neutrales Element – entsprechend der Null bei der Addition – ist die Drehung um einen Winkel von 0° (die Nicht-Drehung).

Gruppen werden in der Mathematik verwendet, um vom Rechnen mit konkreten Zahlen zu abstrahieren (*sprich*: um mit Symbolen anstelle von Zahlen zu rechnen). Entsprechend besteht eine Gruppe aus einer Menge von abstrakten Dingen oder Symbolen und einer „Rechenvorschrift" (Verknüpfung), die angibt, wie mit diesen Dingen umzugehen ist.
Genauer gesagt: Von einer Gruppe spricht man, falls für eine Menge zusammen mit einer Verknüpfung je zweier Elemente dieser Menge, zum Beispiel „$a \times b$", die folgenden weiteren Anforderungen erfüllt sind:
Die Verknüpfung zweier Elemente der Menge ist wiederum ein Element derselben Menge (*Abgeschlossenheit*).
Die Klammerung beim Ausrechnen ist unerheblich (*Assoziativität*): $a\times(b\times c) = (a\times b)\times c$ für alle a,b,c.
Es gibt ein Element e in der Menge, das nichts bewirkt (*neutrales Element*): $a \times e = e \times a = a$ für alle a.
Zu jedem Element a gibt es ein „Spiegelbild" (*inverses Element*) a^* mit der Eigenschaft, beim Verknüpfen mit a das neutrale Element zu ergeben: $a \times a^* = a^* \times a = e$.
Spezialfall: Wenn man zudem noch die Operanden vertauschen darf, also stets $a \times b = b \times a$ gilt (*Kommutativität*), dann liegt eine abelsche oder kommutative Gruppe vor.

Beispiele für abelsche Gruppen sind

- die ganzen Zahlen $\mathbb{Z}$ mit der Addition „+" als Verknüpfung und der Null als neutralem Element,
- die rationalen Zahlen $\mathbb{Q}$ ohne Null mit der Multiplikation „×" als Verknüpfung und der Eins als neutralem Element. Die Null muss hierbei ausgeschlossen werden, da sie kein inverses Element besitzt: „1/0" ist nicht definiert.

Die sehr allgemeine Definition von Gruppen ermöglicht es, nicht nur Mengen von Zahlen mit entsprechenden Operationen als Gruppen aufzufassen, sondern auch andere abstrakte Dinge und Symbole, die die geforderten Eigenschaften erfüllen wie zum Beispiel die Menge der Drehungen und Spiegelungen (Symmetrietransformationen), durch die ein n-Eck auf sich selbst abgebildet wird, mit der Hintereinanderausführung der Transformationen als Verknüpfung.

5.1.1. Mathematische Definition des Gruppenbegriffs

Ein Paar $(G, *)$ mit einer Menge G und einer inneren zweistelligen Verknüpfung
$*: G \times G \to G, (a,b) \mapsto a * b$ heißt ***Gruppe***, wenn folgende ***Axiome*** erfüllt sind:

- *Abgeschlossenheit:* Für alle Gruppenelemente a und b gilt: $(a * b) \in G$
- *Assoziativität*: Für alle Gruppenelemente a, b und c gilt: $(a * b) * c = a * (b * c)$.
- *Neutrales Element*: Es gibt ein neutrales Element $e \in G$, mit dem für alle Gruppenelemente a gilt: $a * e = e * a = a$.
- *Inverses Element*: Zu jedem Gruppenelement a existiert ein Element $a^{-1} \in G$ mit $a*a^{-1} = a^{-1}*a = e$.

Eine Gruppe $(G, *)$ heißt *abelsch* oder *kommutativ*, wenn die Verknüpfung $*$ symmetrisch ist, d. h., wenn zusätzlich das folgende Axiom erfüllt ist:

- *Kommutativität*: Für alle Gruppenelemente a und b gilt $a * b = b * a$.

5.1.2. Bemerkungen zur Notation

Häufig wird für die Verknüpfung $*$ das Symbol $\cdot$ benutzt, man spricht dann von einer multiplikativ geschriebenen Gruppe. Das neutrale Element heißt dann *Einselement* und wird durch 1 symbolisiert. Wie auch bei der gewöhnlichen Multiplikation üblich, kann in vielen Situationen der Malpunkt weggelassen werden.
Die Gruppeneigenschaften lassen sich auch additiv notieren, indem für die Verknüpfung $*$ das Symbol + benutzt wird. Das neutrale Element heißt dann Nullelement und wird durch 0 symbolisiert. Das zum Gruppenelement a inverse Element wird in einer additiv geschriebenen Gruppe nicht durch a^{-1}, sondern durch $-a$ symbolisiert. Üblich ist die additive Schreibweise bei abelschen Gruppen, während nicht abelsche oder beliebige Gruppen zumeist multiplikativ geschrieben werden.
Ist die Verknüpfung klar, so schreibt man für die Gruppe häufig nur G.

5.1.3. Ordnung einer Gruppe

Die Mächtigkeit (Kardinalität) $|G|$ der Trägermenge der Gruppe nennt man *Ordnung der Gruppe* oder kurz *Gruppenordnung*. Für endliche Mengen ist dies einfach die Anzahl der Elemente.

5.1.4. Ordnung von Elementen

Ergibt ein Element a der Gruppe, endlich viele Male n mit sich selbst verknüpft, das neutrale Element 1, d. h. gilt für ein geeignetes n: $a^n = 1$, so nennt man das kleinste derartige n die Ordnung des Elements a. Falls kein solches n existiert, sagt man, dass a unendliche Ordnung hat. In beiden Fällen entspricht die Ordnung des Elements der Ordnung der von ihm erzeugten Untergruppe.
Davon ausgehend kann man zeigen, dass die Ordnung jedes Elements einer endlichen Gruppe endlich ist und die Gruppenordnung teilt (Satz von Lagrange).

5.1.5. Untergruppen

Ist H eine Teilmenge der Trägermenge G einer Gruppe $(G, *)$ und ist $(H, *)$ selbst eine Gruppe, so nennt man H eine Untergruppe von G.
Hierzu ein wichtiger Satz (Satz von Lagrange): Die Ordnung (Anzahl der Elemente) jeder Untergruppe H einer endlichen Gruppe G ist ein Teiler der Ordnung der Gruppe G. Ist speziell $|G|$ eine Primzahl, dann hat G nur die (trivialen) Untergruppen $\{e\}$ (bestehend aus dem neutralen Element) und G selbst.

5.1.6. Beispiele für Gruppen

- Alle Zahlenbereiche (außer $\mathbb{N}$) bezüglich der Addition
- $\mathbb{Q}\backslash\{0\}$, $\mathbb{R}\backslash\{0\}$ und $\mathbb{C}\backslash\{0\}$ bezüglich Multiplikation
- $S_M := \{f: M \longrightarrow M \wedge f \text{ bijektiv}\}$ bezüglich der Hintereinanderausführung von Abbildungen (symmetrische Gruppe)
- Alle regulären Matrizen über den reellen bzw. komplexen Zahlen bezüglich Multiplikation
- Ist M = {1,2,3}, so kann man die Menge aller bijektiven Abbildungen von M auf M als Gruppe der ***Permutationen*** (Vertauschungen der Anordnung der Elemente) betrachten.

5.1.7. Halbgruppe und Monoid

Es gibt auch Verallgemeinerungen der Gruppentheorie. Dabei wird auf einzelne Axiome der Gruppe verzichtet.
Beispiele dafür sind die Definitionen der Halbgruppe und des Monoids:
Für Halbgruppen wird nur die Assoziativität verlangt.
Existiert in einer Halbgruppe ein neutrales Element, so spricht man von einem Monoid.

Beispiele und Gegenbeispiele

$(\mathbb{N}_0, +, 0)$ ist ein Monoid

$(\mathbb{N}, \cdot, 1)$	ist ein Monoid.
$(\mathbb{N}, :, 1)$	ist kein Monoid, da die Division nicht assoziativ ist.
$(\mathbb{Z}, +, 0)$	(die Menge der ganzen Zahlen mit der Addition) ist ein Monoid
$(\mathbb{Z}, -, 0)$	ist kein Monoid, da die Subtraktion nicht assoziativ ist.
$(\mathbb{R}^{n\times n}, \cdot, E)$	(die Menge der n×n-Matrizen mit der üblichen Matrizenmultiplikation und der Einheitsmatrix *E*) ist ein nichtkommutatives Monoid.
$(\mathbb{R}^3, \times, \vec{0})$	(der dreidimensionale reelle Raum mit dem Vektorprodukt) ist kein Monoid, da das Assoziativgesetz verletzt ist: Bezeichnen wir mit e_i den i-ten Einheitsvektor, so ist $(e_1 \times e_1) \times e_2 = 0$, aber $e_1 \times (e_1 \times e_2) = -e_2$.
$(n\mathbb{Z}, +, 0)$	(die Menge der Vielfachen der ganzen Zahl n mit der Addition) ist ein Monoid.
$(\mathbb{Q}_+, +, 0)$	(die Menge der nichtnegativen rationalen Zahlen mit der Addition) ist ein Monoid.

5.2. Ringe

Ein Ring ist eine Menge R mit zwei inneren binären Verknüpfungen „+“ und „·“, sodass gilt:

- (R, +) ist eine abelsche Gruppe,
- (R, ·) ist eine Halbgruppe,
- Die Distributivgesetze $a \cdot (b + c) = a \cdot b + a \cdot c$ und $(a + b) \cdot c = a \cdot c + b \cdot c$ sind für alle *a*,*b*,*c* ∈ *R* erfüllt.

Das neutrale Element 0 von (R, +) heißt Nullelement von R.
Ein Ring heißt kommutativ, falls er bezüglich der Multiplikation kommutativ ist.

5.2.1. Unter-/Oberring

Eine nichtleere Untermenge U eines Ringes R heißt Unterring von R, wenn U zusammen mit den beiden auf U eingeschränkten Verknüpfungen von R wieder ein Ring ist.
Ein Ring S heißt Oberring oder Erweiterung eines Ringes R, wenn R ein Unterring von S ist.

5.2.2. Einselement

Besitzt ein Ring ein neutrales Element bezüglich der Multiplikation, so nennt man dieses die Eins oder das Einselement des Ringes. Dieses Element wird meist mit 1 bezeichnet und hat die Eigenschaft
$1 \cdot a = a \cdot 1 = a \quad \forall a \in R.$
Ein Ring mit Einselement (oder kurz: Ring mit Eins) wird auch **unitärer Ring** genannt.

5.2.3. Abschwächung der Axiome

Wenn ein Ring eine Eins besitzt, dann muss nicht gefordert werden, dass die Addition kommutativ ist. Diese Eigenschaft folgt dann aus den restlichen Ringaxiomen. Für alle *a*,*b* ∈ *R* gilt:
$$a + a + b + b = 1 \cdot a + 1 \cdot a + 1 \cdot b + 1 \cdot b = (1+1) \cdot a + (1+1) \cdot b = (1+1) \cdot (a+b) =$$
$$1 \cdot (a+b) + 1 \cdot (a+b) = a + b + a + b$$
Addiert man diese Gleichung von links mit $(-a)$ und von rechts mit $(-b)$, so erhält man:
$a + b = b + a$.
Insgesamt wurden mit Ausnahme des Assoziativgesetzes der Multiplikation alle Axiome eines unitären Rings benutzt. Die Argumentation ist also auch für nicht-assoziative unitäre Ringe gültig.

5.2.4. Invertierbarkeit, Einheit

Existiert in einem Ring mit Eins zu einem Element *x* ein Element *y*, so dass $y \cdot x = 1$ (bzw. $x \cdot y = 1$) gilt, so nennt man *y* ein Linksinverses (bzw. Rechtsinverses) von *x*. Besitzt *x* sowohl Links- als auch Rechtsinverses, so nennt man *x* invertierbar oder Einheit des Ringes. Die Menge der Einheiten eines Ringes R mit

Eins wird gewöhnlich mit R* bezeichnet. R* bildet bezüglich der Ringmultiplikation eine Gruppe – die Einheitengruppe des Ringes.
In kommutativen Ringen mit Eins (insbesondere Integritätsringen) definiert man alternativ die Einheiten auch als diejenigen Elemente, die die Eins teilen. Dass *x* die Eins teilt, heißt nämlich dass es *y* gibt mit $y \cdot x = x \cdot y = 1$. Man sieht, dass die Eigenschaft, Teiler von Eins zu sein, und die Eigenschaft, invertierbar zu sein, hier dasselbe bedeuten. Diese Alternativdefinition funktioniert aber erst in kommutativen Ringen, da erst dort die Teilbarkeit erklärt wird.

5.2.5. Beispiele

Das wichtigste Beispiel eines Ringes ist die Menge $(\mathbb{Z},+,\cdot)$ der ganzen Zahlen mit der üblichen Addition und Multiplikation. Es handelt sich dabei um einen nullteilerfreien kommutativen Ring mit Einselement, also einen Integritätsring.

Ebenso bildet $(\mathbb{Q},+,\cdot)$ der rationalen Zahlen mit der üblichen Addition und Multiplikation einen Ring. Da in diesem Fall nicht nur $(\mathbb{Q},+)$, sondern auch $(\mathbb{Q}\backslash\{0\},\cdot)$ eine abelsche Gruppe bildet, liegt sogar ein Körper vor; es handelt sich dabei um den Quotientenkörper des Integritätsringes $(\mathbb{Z},+,\cdot)$.

Kein Ring ist die Menge $(\mathbb{N},+,\cdot)$ der natürlichen Zahlen mit der üblichen Addition und Multiplikation, da die Addition über den natürlichen Zahlen nicht invertierbar ist.

Weitere wichtige Beispiele von Ringen sind

- Restklassenringe,
- Polynomringe und
- quadratische Matrizen mit fixer Dimension.

Insbesondere Restklassenringe und quadratische Matrizen liefern Beispiele von Ringen, die nicht nullteilerfrei sind.
Quadratische Matrizen sind darüber hinaus ein Beispiel eines Rings, bei dem die Multiplikation nicht kommutativ ist.

Ein Beispiel eines Rings ohne Eins sind die geraden ganzen Zahlen, ebenso bilden alle ganzen Zahlen, die Vielfache einer gegebenen ganzen Zahl größer eins sind, einen Ring ohne Eins.
Allgemein ist jedes echte **Ideal** eines Rings ein Ring ohne Eins.

Aber was ist ein **Ideal**?

Um auch für *nichtkommutative* Ringe geeignete Begriffe zu haben, unterscheidet man zwischen Links-, Rechtsidealen und zweiseitigen Idealen:
Es sei I eine Teilmenge eines Ringes R. I heißt dann Linksideal, wenn gilt:

1: Die Null des Ringes liegt in I.

2: $\forall a,b \in I : (a-b) \in I.$

3L: Für jedes $a \in I$ und $r \in R$ gilt: $r \cdot a \in I$.

Entsprechend ist I ein Rechtsideal, wenn für I neben 1 und 2 auch gilt:

3R: Für jedes $a \in I$ und $r \in R$ gilt: $a \cdot r \in I$.

I nennt man schließlich zweiseitiges Ideal oder nur kurz **Ideal**, falls I Links- und Rechtsideal ist, also 1, 2, 3L und 3R erfüllt.

5.3. Körper

Ein Körper ist im mathematischen Teilgebiet der Algebra eine ausgezeichnete algebraische Struktur, in der die Addition, Subtraktion, Multiplikation und Division wie bei den „normalen“ (reellen) Zahlen durchgeführt werden können.
Die Bezeichnung Körper wurde im 19. Jahrhundert von Richard Dedekind eingeführt.

5.3.1. Allgemeine Definition

Ein Tripel (K,+,·), bestehend aus einer Menge K und zwei binären Verknüpfungen „ + “ und „·“ (die üblicherweise Addition und Multiplikation genannt werden), ist genau dann ein Körper, wenn folgende Eigenschaften erfüllt sind:

- (K,+) ist eine abelsche Gruppe (mit Neutralelement 0)
- ($K \setminus \{0\}$,·) ist eine abelsche Gruppe (mit Neutralelement 1)
- $a \cdot (b + c) = a \cdot b + a \cdot c$ und $(a + b) \cdot c = a \cdot c + b \cdot c$ (Distributivgesetz)

5.3.2. Einzelaufzählung der benötigten Axiome

Ein Körper muss also folgende Einzelaxiome erfüllen:

Additive Eigenschaften:

- $a + (b + c) = (a + b) + c$ (Assoziativgesetz)
- $a + b = b + a$ (Kommutativgesetz)
- Es gibt ein Element $0 \in K$ mit $0 + a = a$ (neutrales Element)
- Zu jedem $a \in K$ existiert das additive Inverse $(-a)$ mit $(-a) + a = 0$

Multiplikative Eigenschaften:

- $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (Assoziativgesetz)
- $a \cdot b = b \cdot a$ (Kommutativgesetz)
- Es gibt ein Element $1 \in K$ mit $1 \cdot a = a$ (neutrales Element), und es ist $1 \neq 0$.
- Zu jedem $a \in K \setminus \{0\}$ existiert das multiplikative Inverse a^{-1} mit $a^{-1} \cdot a = 1$

Zusammenspiel von additiver und multiplikativer Struktur:

- $a \cdot (b + c) = a \cdot b + a \cdot c$ (Links-Distributivgesetz)

Das Rechts-Distributivgesetz $(a + b) \cdot c = a \cdot c + b \cdot c$ folgt dann aus den übrigen Eigenschaften:
$(a + b) \cdot c = c \cdot (a + b) = c \cdot a + c \cdot b = a \cdot c + b \cdot c$

5.3.3. Definition als spezieller Ring

Ein kommutativer unitärer Ring, der nicht der Nullring ist, heißt ein Körper, wenn in ihm jedes von Null verschiedene Element multiplikativ invertierbar ist.
Anders formuliert, ist ein Körper ein kommutativer unitärer Ring K, in dem die Einheitengruppe K^* gleich $K \setminus \{0\}$, also maximal groß, ist.

Bemerkungen

Die Definition sorgt dafür, dass in einem Körper in der "gewohnten" Weise Addition, Subtraktion und Multiplikation funktionieren (und die Division mit Ausnahme der verbotenen Division durch 0):
Das Inverse von a bezüglich der Addition ist $-a$ und wird meist das additiv Inverse zu a oder auch das Negative von a genannt.

Das Inverse von a bezüglich der Multiplikation ist a^{-1} und wird das (multiplikativ) Inverse zu oder der Kehrwert von a genannt.
0 ist das einzige Element des Körpers, das keinen Kehrwert hat, die multiplikative Gruppe eines Körpers ist also $K^\times = K \setminus \{0\}$.

Anmerkung: Die Bildung des Negativen eines Elementes hat nichts mit der Frage zu tun, ob das Element selbst negativ ist; beispielsweise ist das Negative der reellen Zahl −2 die positive Zahl 2. In einem allgemeinen Körper gibt es keinen Begriff von negativen oder positiven Elementen. (Siehe auch geordneter Körper.)

5.3.4. Verallgemeinerung: Schiefkörper

Verzichtet man auf die Bedingung, dass die Multiplikation kommutativ ist, so gelangt man zur Struktur des Schiefkörpers. Es gibt jedoch auch Autoren, die für einen Schiefkörper explizit voraussetzen, dass die Multiplikation nicht kommutativ ist. In diesem Fall ist ein Körper nicht mehr zugleich Schiefkörper. Ein Beispiel ist der Schiefkörper der *Quaternionen*, der kein Körper ist.
Andererseits gibt es Autoren, so Bourbaki, die Schiefkörper als Körper und die hier besprochenen Körper als kommutative Körper bezeichnen.

5.3.5. Eigenschaften

- Es gibt genau eine „0“ (Null-Element, neutrales Element bzgl. der Körper-Addition) und eine „1“ (Eins-Element, neutrales Element bzgl. der Körper-Multiplikation) in einem Körper.
- Jeder Körper ist ein Ring. Die Eigenschaften der multiplikativen Gruppe heben den Körper aus den Ringen heraus. Wenn die Kommutativität der multiplikativen Gruppe nicht gefordert wird, erhält man den Begriff des Schiefkörpers.
- Jeder Körper ist ein Vektorraum über sich selbst (das heißt mit sich selbst als zugrundeliegendem Skalarkörper).
- Jeder Körper ist nullteilerfrei. Das heißt, dass ein Produkt zweier Elemente des Körpers genau dann 0 ist, wenn mindestens einer der beteiligten Faktoren 0 ist.

5.3.6. Beispiele

Bekannte Beispiele für Körper sind

- die Menge der rationalen Zahlen $(\mathbb{Q},+,\cdot)$,
- die Menge der reellen Zahlen $(\mathbb{R},+,\cdot)$ und
- die Menge der komplexen Zahlen $(\mathbb{C},+,\cdot)$

jeweils mit der üblichen Addition und Multiplikation.

Weitere Beispiele sind

- endliche Körper und
- die Körper der *p-adischen* Zahlen.

Kein Beispiel für einen Körper ist die Menge der ganzen Zahlen $(\mathbb{Z},+,\cdot)$: Zwar ist $(\mathbb{Z},+)$ eine Gruppe mit neutralem Element 0 und jedes $a \in \mathbb{Z}$ besitzt das additive Inverse $-a$, aber $(\mathbb{Z} \setminus \{0\},\cdot)$ ist keine Gruppe. Immerhin ist 1 das neutrale Element, aber außer zu 1 und −1 gibt es keine multiplikativen Inversen (zum Beispiel ist $3^{-1} = 1/3$ keine ganze, sondern eine echt rationale Zahl). Die ganzen Zahlen bilden lediglich einen Integritätsring, dessen Quotientenkörper die rationalen Zahlen sind.

Ein Beispiel für einen **endlichen Körper** ist der Restklassenkörper $\mathbb{Z}_5$. Nachfolgend sind die Additionstabelle und die Multiplikationstabelle für den Körper $\mathbb{Z}_5$ angegeben.
($\mathbb{Z}_5$ ist der Körper der Restklassen modulo 5 im Bereich der ganzen Zahlen $\mathbb{Z}$!)

Additionstabelle

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Multiplikationstabelle

*	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1