Mathematik 1

Prof. Dr.-Ing. Karin Landenfeld

1 Einführung und Grundlagen

Inhaltsverzeichnis des Kapitels 1

1.1 Einführung

Die **Mathematik** gehört zu den **ältesten Wissenschaften** und ist trotzdem gerade im Zeitalter der Computer äußerst wichtig. Bereits in der griechischen Antike entstanden in wissenschaftlicher Methodik die Grundlagen der Zahlentheorie, der Algebra, der Trigonometrie und der Infinitesimalrechnung.

Die Mathematik mit ihren Denkweisen und Techniken ist für die Ingenieurwissenschaften und die Informatik mit ihrer systematischen Verarbeitung von Informationen eine wichtige Grundlage. **Mathematische Beschreibungen, Methoden und Modelle** spielen überall eine Rolle, sowohl in der Formulierung und Untersuchung von Algorithmen als auch bei der Beschreibung und Lösung von technischen Problemen und dem Verständnis von informationstechnischen- und kommunikationstechnischen Anlagen.

Von Ingenieuren und Informatikern erwartet man die Lösung technischer und softwaretechnischer Probleme, d.h. sie benötigen **Kompetenz in Technik und Problemlösung**.

Beide Berufsgruppen sind wegen der Komplexität ihrer Aufgabenstellung daher massiv auf den Einsatz von Mathematik angewiesen. Die **Kenntnisse und die souveräne Handhabung der mathematischen Methoden ist wichtig** und uneingeschränkt nützlich. Sie müssen außerdem in der Lage sein, numerische Verfahren anzuwenden und deren Ergebnisse zu interpretieren.

Für Ingenieure und Informatiker ist die Mathematik ein „**Werkzeugkasten**", aus dem sie sich zum Problemverständnis und zur Problemlösung bedienen. Ohne Verständnis für das Problem und das Werkzeug ist die Benutzung des Werkzeugs aber im allgemeinen nicht möglich.

1.1.1 Inhaltsübersicht

Im Rahmen dieser Vorlesung wird das Grundwissen über die „höhere Mathematik" vermittelt. In den meisten Fällen wird auf den Beweis der Sätze zu Gunsten einer **Veranschaulichung des Sachverhaltes** verzichtet. **Beispiele und Aufgaben** sollen den Stoff verdeutlichen und die Handhabung einüben. Wichtig dabei ist, die Verknüpfung der Inhalte zu einem „Netzwerk des Verstehens". Häufig können **praktische Anwendungen** allerdings erst am Ende mehrerer theoretischer Abschnitte angegeben werden.

Die Veranstaltung der **Linearen Algebra** beinhaltet folgende Themen:

Kapitel 1: Einführung, Grundlagen, Mengen

Kapitel 2: Logik und Beweise

Kapitel 3: Vektoren und Matrizen

Kapitel 4: Lineare Gleichungssysteme

Kapitel 5: Determinanten und Eigenwerte

Kapitel 6: Zahlensysteme und Komplexe Zahlen

Im Rahmen der parallel stattfindenden Veranstaltung der **Analysis 1** sowie der **Analysis 2** werden folgende Inhalte vermittelt:

Kapitel 1: Grundlagen

Kapitel 2: Folgen und Grenzwerte

Kapitel 3: Funktionen

Kapitel 4: Differentialrechnung

Kapitel 5: Reihen, Potenzreihen und Taylorreihen

Kapitel 6: Integralrechnung

Kapitel 7: Fourierreihen

Kapitel 8: Mehrdimensionale Differential- und Integralrechnung

Kapitel 9: Differentialgleichungen

1.1.2 Skript

Das vorliegende „Skript“ enthält die wichtigsten Sätze und Definitionen zu den Vorlesungsinalten. **Herleitungen, Veranschaulichungen und Beispiele werden in der Vorlesung entwickelt.** Das „Skript“ ist erst dann vollständig, wenn es durch die Vorlesungsbeispiele und Herleitungen ergänzt wurde. Das Erstellen einer zusätzlichen Mitschrift ist hier empfehlenswert und sehr hilfreich.

Hinweise zum Skript

- Die Definitionen sind jeweils innerhalb eines Kapitels fortlaufend durchnummeriert. Die Kapitelnummer ist dieser fortlaufenden Nummerierung vorangestellt.
- Die Sätze sind in der gleichen Art und Weise in einer eigenen Nummerierung bezeichnet.
- Die Beispiele und Bemerkungen sind nicht durchnummeriert.
- In vielen Fällen wird auf einen Beweis der Sätze verzichtet und stattdessen eine Veranschaulichung der Aussage gegeben.

1.1.3 Literaturhinweise

Beiliegend eine Liste der für dieses Skript verwendeten Literatur in Form von Büchern oder Internetquellen. Diese Bücher und Online-Quellen können für Vertiefung der Inhalte zum Selbststudium verwendet werden.

- **Koch, Jürgen und Stämpfle, Martin**
  Mathematik für das Ingenieurstudium

  Hanser-Verlag, 3.Auflage, September 2015 (36,00 €)

  Bemerkung: sehr übersichtlich

- **Rießinger, Thomas**
  Mathematik für Ingenieure

  Springer Verlag, 10.Auflage 2017 (44,99 €)

  Bemerkung: umfangreicher Stoff, netter Schreibstil, sehr kleine Schrift, ergänzendes Übungsbuch

- **Papula, Lothar**
  Mathematik für Ingenieure und Naturwissenschaftler - Band 1 und 2 (Ein Lehr- und Arbeitsbuch für das Grundstudium)

  Verlag Vieweg, Band 1, 15.Auflage 2018 (29,99 €)

  Band 2, 14.Auflage 2015 (34,99 €)

  Bemerkung: sehr ausführlich beschriebene Inhalte, Beispiele und Lösungen im Buch, Standardwerk für Ingenieure

- **Papula, Lothar**
  Mathematische Formelsammlung für Ingenieure und Naturwissenschaftler

Verlag Vieweg, 12.Auflage 2017(29,99 €)

Bemerkung: ausführliche Beschreibungen

- **Westermann, Thomas**
  Mathematik für Ingenieure

  Springer Verlag, 8.Auflage 2020 (44,99 €)

  Bemerkung: übersichtlich, viele Anwendungsbeispiele

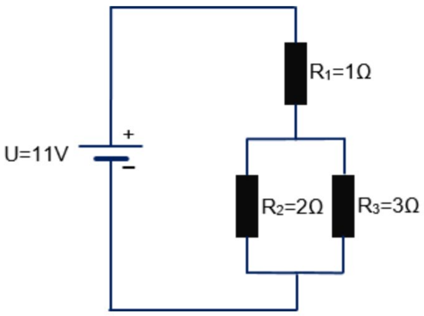
Online-Links:

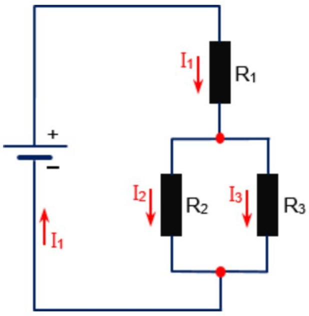
- www.mathe-online.at
- mo.mathematik.uni-stuttgart.de
- www.matheprisma.de
- http://www-hm.ma.tum.de/integration/branch.htm

1.2 Anwendungen der Mathematik

Die in den Veranstaltungen zur Mathematik vermittelten Grundlagen werden in verschiedenen Anwendungsvorlesungen in diesem oder in den folgenden Semestern benötigt. Einige Anwendungsbeispiele sind nachfolgend dargestellt.

Elektrische Schaltungen - Bestimmung der Ströme

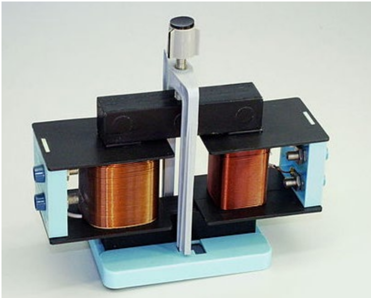




Mathematik:

- Vektoren und Matrizen
- Lineare Gleichungssysteme

Transformatoren - Komplexe Wechselstromrechnung

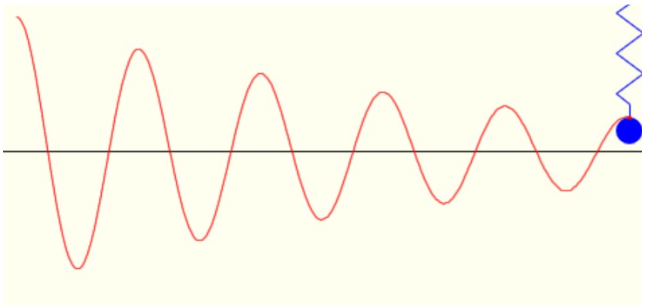
 

aus https://de.wikipedia.org/wiki/Komplexe_Wechselstromrechnung#Anwendung_und_Verallgemeinerung

Mathematik:

- Komplexe Zahlen
- Trigonometrische Funktionen
- Rechnen mit Potenzen

Federpendel

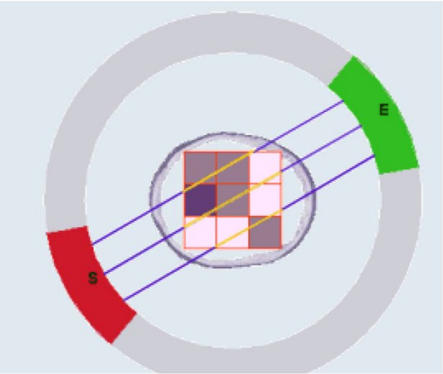


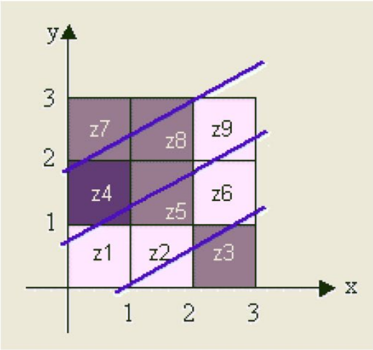
aus http://www.matheprisma.de/Module/Schwingu/

Mathematik:

- Harmonische Schwingungen
- Differentialgleichungen

Computer-Tomographie



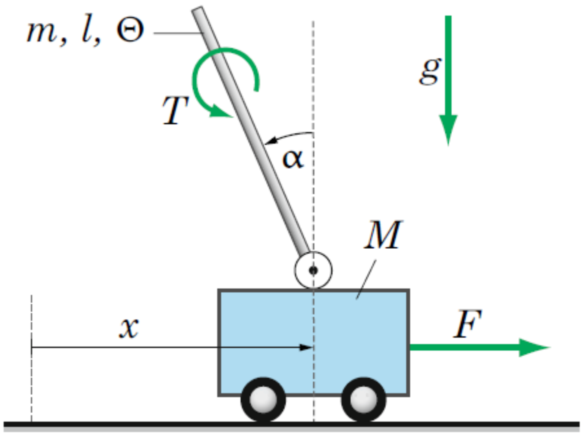


aus http://www.matheprisma.de/Module/CT

Mathematik:

- Lineare Gleichungssysteme
- Modellierung und numerische Lösungsverfahren

Segway – Balancieren mit Differentialgleichungen

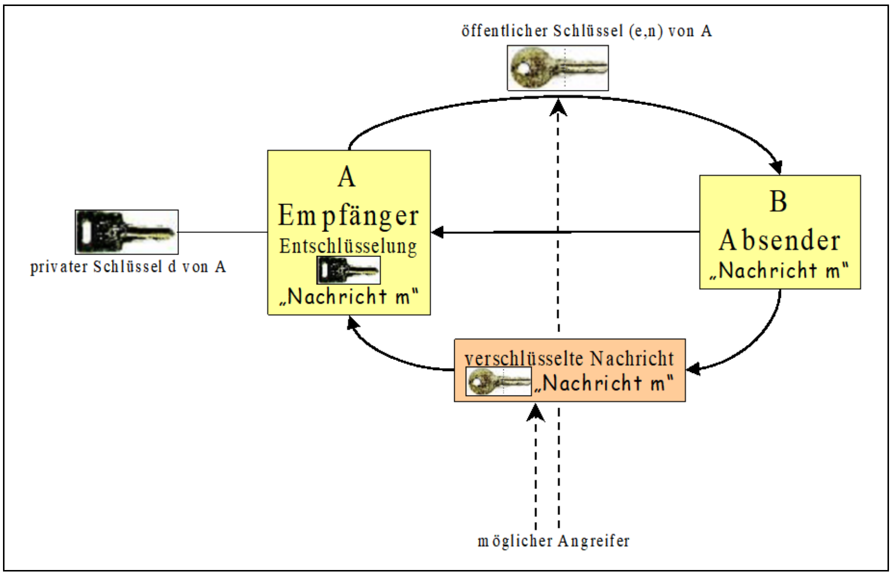


aus J. Härterich, A. Rooch, Das Mathe-Praxis-Buch, https://www.springer.com/gp/book/9783642383052

Mathematik:

- Matrizen und Lineare Gleichungssysteme
- Eigenwerte und Eigenvektoren
- Funktionen
- Differentialgleichungen
- Taylorreihen

Verschlüsselung mit dem RSA-Algorithmus



Mathematik:

- Primzahlen
- Grundlegende Eigenschaften natürlicher Zahlen
- Ein-eindeutige Zuordnungen

Die Mathematik bildet die Basis für die Verschlüsselungsalgorithmen der Krypthographie, so verwendet das RSA-Verfahren Primzahlen, den größten gemeinsamen Teiler (ggT) von zwei Zahlen und die Modulo-Funktion. Im Folgenden wird das RSA-Verfahren kurz dargestellt und anhand eines Beispiels erläutert. Die benötigten Begriffe der Mathematik werden in den nachfolgenden Kapiteln erläutert.

Das RSA-Verfahren ist ein public-key-Verfahren, das mit einem öffentlichen Schlüssel (public key) und einem privaten Schlüssel(private key) arbeitet. Der Empfänger einer Nachricht gibt seinen öffentlichen Schlüssel, mit dem alle an ihn gerichteten Nachrichten verschlüsselt werden, allgemein bekannt. Den zu diesem öffentlichen Schlüssel passenden privaten Schlüssel behält er für sich. Allein der Empfänger ist mit seinem privaten Schlüssel in der Lage die mit seinem öffentlichen Schlüssel verschlüsselten Nachrichten zu entschlüsseln.

Das **Funktionsprinzip der Schlüsselgenerierung** basiert auf der Primzahlenzerlegung:

→ Beide Schlüssel werden auf der Grundlage von zwei großen Primzahlen p und q erzeugt. Diese Primzahlen sind nur dem Empfänger bekannt und müssen geheim bleiben.

→ Der Empfänger sendet das Produkt $n = p \cdot q$ der beiden Primzahlen und einen passend ausgewählten öffentlichen Schlüssel e an den Sender.

→ Die Zahl e wird mit Hilfe der folgenden beiden Gleichungen bestimmt:

$$\varphi(n) = (p-1)(q-1) \;\; und \;\; ggT(e, \varphi(n)) = 1, \; d.h. \; e \; teilerfremd \; zu \; \varphi(n) \, .$$

→ Weiterhin wird eine natürliche Zahl d bestimmt mit $e \cdot d \bmod \varphi(n) = 1$.

Dann gilt: $\varphi(n) \mid (e \cdot d - 1)$ *bzw.* $e \cdot d = \varphi(n) \cdot k + 1$ *für eine natürliche Zahl* k.

→ Die Zahl d ist der private Schlüssel des Empfängers.

→ Das Paar (e,n) ist der öffentliche Schlüssel des Empfängers.

Die Verschlüsselung einer Nachricht m wird durch den Sender nach folgender Formel unter Verwendung des öffentlichen Schlüssels (e,n) durchgeführt:

→ $c := m^e \bmod n$

→ Somit ist c nun die verschlüsselte Nachricht m und kann an den Empfänger geschickt werden.

Der rechtmäßige Empfänger der Nachricht c ist nun mit Hilfe seines privaten Schlüssels d in der Lage diese Nachricht zu entschlüsseln:

→ Durch Potenzierung der Nachricht c mit seinem privaten Schlüssel d erhält er wieder die Originalnachricht m: $m = c^d \bmod n$

Beispiel:

→ Zielsetzung: Person B möchte an Person A eine Nachricht über einen sicheren Übermittlungsweg schicken.

Person A	**Person B**
1) Schlüsselbildung **Wahl von Primzahlen** ***pA*** = ***23*** ***qA*** = ***13*** (in der Realität mindestens 100 Stellen) **Berechnung** **nA** = pA * qA = 23 * 13 = **299** **φ (nA)** = (pA – 1) (qA – 1) = 22 * 12 = **264** **Wahl** ***eA*** = ***5*** *(gewählt mit den Bedingungen:* *1 < eA <* 264∧ ggT(eA,264) = 1) **Berechnung** **dA** so, dass eA * dA mod φ (nA) = 1 (5 * dA) mod 264 = 1 ⇒ **dA = 53** **Schlüssel** öffentlicher Schlüssel: **(eA, nA)=(5, 299)** privater Schlüssel : **dA = 53**	

2) Schlüsselverteilung

öffentlicher Schlüssel: **(eA, nA)=(5, 299)**

3) Verschlüsselung

Verschlüsselung der Nachricht

*Nachricht m = **99***

Formel: $c = m^{eA} \bmod nA$

$c = 99^5 \bmod 299 = 86$

*verschlüsselte Nachricht c = **86***

verschlüsselte Nachricht c wird an A übertragen

4) Entschlüsselung

Verwendung des

privaten Schlüssel : **dA = 53**

und des

öffentlichen Schlüssel: **(eA, nA)=(5, 299)**

$m = c^{dA} \bmod nA$

$m = 86^{53} \bmod 299 = 99$

entschlüsselte Meldung ist: m = 99

Weiterführende Literatur dazu ist zu finden unter: http://www.matheprisma.de/Module/RSA und https://kilchb.de/bsp_rsa.php.

1.3 Formelzeichen und Begriffe

1.3.1 Griechische Buchstaben

Alpha	α
Beta	β
Gamma	γ
Delta	δ
Epsilon	ε
Zeta	ζ
Eta	η
Theta	ϑ
Kappa	κ
Iota	ι
Lambda	λ
Mikron, My	μ

Ny	ν
Xi	ξ
Omikron	o
Pi	π
Rho	ρ
Sigma	σ
Tau	τ
Ypsilon	υ
Phi	φ
Chi	χ
Psi	ψ
Omega	ω

1.3.2 Zeichen und Begriffe

Begriff	**Darstellung**	**Beschreibung**	**Beispiel**
Summe	+	Addition Summand + Summand	3 + 4
Differenz	-	Subtraktion Minuend - Subtrahend	3 - 4
Produkt	$\cdot$ (*, x)	Multiplikation Faktor $\cdot$ Faktor	3 * 4
Quotient	: (/ , ÷)	Division Dividend : Divisor	3 : 4
Bruch	$\frac{x}{y}$	Division Zähler x und Nenner y	$\frac{3}{4}$

Begriff	**Darstellung**	**Beschreibung**	**Beispiel**
Kehrwert (Reziprokwert)	$\frac{1}{x}$	Division	Zähler 1 und Nenner x
Potenz	x^y	Potenzieren	Basis$^{\text{Exponent}}$ $2^5 = 32$
Wurzel/ Wurzel-wert	$\sqrt[y]{x}$	Radizieren (Wurzelziehen)	$\sqrt[Wurzelexponent]{Radikand}$ $\sqrt[2]{9} = 3$
n-Fakultät	n!	1 · 2·3 · .. · n	$4! = 1 \cdot 2 \cdot 3 \cdot 4 = 24$
n über k *Binomial-Koeffi-zient*	$\binom{n}{k}$	$\binom{n}{k} = \frac{n!}{(n-k)!k!}$ Anzahl k-elementiger Teilmengen einer n-ele-mentigen Menge	$\binom{4}{2} = \frac{4!}{(4-2)!2!} = 6$
Modulo	n mod m (n%m)	Rest der ganzzahligen Division von n und m	$14 \bmod 4 = 2$
teilt	n|m	n ist Teiler von m (bzw. m ist durch n ohne Rest teilbar)	$4 \mid 12$
gleich	=	Vergleich/ Zuweisung	$3 + 2 = 5$
ungleich	≠ (!=, <>)	Vergleich	$3 + 2 \neq 6$
kleiner	<	Vergleich	$3 + 2 < 6$
größer	>	Vergleich	$3 + 5 > 6$
kleiner gleich	≤ (<=)	Vergleich	$3 + 2 \leq 6$
größer gleich	≥ (>=)	Vergleich	$3 + 5 \geq 8$
Unendlich	∞	+∞ positiv unendlich -∞ negativ unendlich	
Pi Kreiskonstante	p (=3.1415..)		
Eulersche Zahl	e (=2.7182..)		

Begriff	**Darstellung**	**Beschreibung**	**Beispiel**
Betrag	|x|	Betrag einer Zahl x	$\|x\| = \begin{cases} x, & wenn\ x \geq 0 \\ -x, & wenn\ x \leq 0 \end{cases}$
Signum von x	sgn(x)	Vorzeichen einer Zahl x	$\operatorname{sgn}(x) = \begin{cases} 1, & wenn\ x > 0 \\ 0, & wenn x = 0 \\ -1, & wenn\ x < 0 \end{cases}$
Determinante	$\begin{vmatrix} 1 & 4 \\ -2 & 6 \end{vmatrix}$	Determinante einer Matrix	
Summenzeichen	$\sum$		Beispiel: Summe der Zahlen 1-4 $\sum_{i=1}^{4} i = 1+2+3+4$
Produktzeichen	$\prod$		Beispiel: Produkt der Zahlen 1-4 $\prod_{i=1}^{4} i = 1 \cdot 2 \cdot 3 \cdot 4$
Menge	$\{...\}$	Zusammenfassung einzelner Objekte zu einem Ganzen	$\{1,2,4,8\}$
Element von	$\in$	Objekt ist in einer Menge enthalten	$2 \in \{1,2,4,8\}$
Natürliche Zahlen	$\mathbb{N}$	{1,2,3,…}	
Natürliche Zahlen mit 0	$\mathbb{N}_0$	{0,1,2,3,…}	
Ganze Zahlen	$\mathbb{Z}$	{…, -3,-2,-1,0,1,2,3,…}	
Rationale Zahlen	$\mathbb{Q}$	Menge aller Brüche $\mathbb{Q} = \left\{ \begin{matrix} \ldots, -\frac{2}{1}, -\frac{1}{2}, -\frac{1}{1}, 0, \\ \frac{1}{1}, \frac{1}{2}, \frac{2}{2}, \frac{1}{3}, \frac{2}{3}, \ldots \end{matrix} \right\}$ $= \left\{ \frac{p}{q} \middle\| p \in \mathbb{Z}, q \in \mathbb{N} \right\}$	
Reelle Zahlen	$\mathbb{R}$	Menge aller Dezimalzahlen	

Name	Darstellung	Beschreibung	Beispiel
Komplexe Zahlen	$\mathbb{C}$	Zahlen $a + jb$ mit $a, b \in \mathbb{R}$, wobei $j^2 = -1$.	Beispiel: $z = 3 - j0.5$
Allquantor	$\forall$	für alle	Beispiel: $\forall x \in \{2,4,6,8\}$ *gilt* $2 \mid x$
Existenzquantor	$\exists$	es gibt	Beispiel: $\forall x \in \{2,3,4,5,7\}$ *gilt* $2 \mid x$
Vereinigung Durchschnitt	$\cup$ $\cap$	Vereinigung bzw. Durchschnitt zweier Mengen	Beispiel: $\{1,3\} \cup \{2,4\} = \{1,2,3,4\}$ $\{1,3\} \cap \{2,3\} = \{3\}$
Leere Menge	$\varnothing$	$\{ \}$	
Teilmenge	$\subset$ / $\subseteq$		Beispiel: $\{1,3\} \subset \{1,2,3\}$
Vektor	$\vec{v}, \underline{v}, \boldsymbol{v}$	Vektorvariable mit verschiedenen Schreibweisen	
Vektor	$\vec{v} = \begin{pmatrix} \dots \\ \dots \\ \dots \end{pmatrix}$	Vektor in Komponenten-darstellung	Beispiel: Koordinaten im Raum $\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 5 \end{pmatrix}$
Gauß-Klammer / Abrundungs-funktion	$\lfloor x \rfloor$	Ordnet einer reellen Zahl x die größte ganze Zahl zu, die kleiner oder gleich x ist.	$\lfloor x \rfloor = \max\{k \in \mathbb{Z} \mid k \le x\}$ $= floor(x)$
Aufrundungs-funktion	$\lceil x \rceil$	Ordnet einer reellen Zahl x die kleinste ganze Zahl zu, die größer oder gleich x ist.	$\lceil x \rceil = \min\{k \in \mathbb{Z} \mid k \ge x\}$ $= ceil(x)$

Bemerkung: Rechnen mit Fakultäten

$\frac{(n+1)!}{n!} = n+1$ zum Beispiel $\frac{7!}{6!} = 7$

$\frac{(n+1)!}{(n-1)!} = n(n+1)$ zum Beispiel $\frac{10!}{8!} = 9 \cdot 10 = 90$

Bemerkung: Rechenregeln mit Summen

(1) Zusammenfassen von Summen

$$\sum_{k=0}^{n} A(k) + \sum_{k=0}^{n} B(k) = \sum_{k=0}^{n} (A(k) + B(k))$$

(2) Multiplikation mit konstanten Elementen

$$c \cdot \sum_{k=0}^{n} A(k) = \sum_{k=0}^{n} (c \cdot A(k))$$

(3) Indexverschiebung

$$\sum_{k=0}^{n} A(k) = \sum_{k=1}^{n+1} A(k-1)$$

(4) Abspaltung des letzten Summanden

$$\sum_{k=1}^{n} A(k) = \left(\sum_{k=1}^{n-1} A(k) \right) + A(n)$$

Bemerkung: Ende eines Beweises

q.e.d. Diese Buchstaben stehen häufig am Ende eines Beweises für „quod erat demonstrandum“ , was bedeutet „Was zu beweisen war“

□ Für das Ende eines Beweises wird aber auch ein kleines Quadrat verwendet.

1.4 Zahlen, Teiler und Vielfache

In diesem Kapitel wollen wir uns passend zur Anwendung der Verschlüsselung mit der RSA-Verfahren aus dem letzten Kapitel die notwendigen mathematischen Grundlagen anschauen. Wir schauen uns die Begriffe Primzahlen, Teilbarkeit, größter gemeinsamer Teiler (ggT) und kleinstes gemeinsames Vielfaches (kgV) sowie die Division mit Rest an.

1.4.1 Teiler und Vielfache

Grundlage für diese Begriffe bilden die natürlichen Zahlen $\mathbb{N} = \{1,2,3,4,...\}$ und die ganzen Zahlen $\mathbb{Z} = \{...,-4,-3,-2,-1,0,1,2,3,4,...\}$.

Die natürlichen Zahlen sind bezüglich der Addition und der Multiplikation abgeschlossen, d.h. beide Operationen anwendet auf natürlichen Zahlen haben ebenfalls wieder ein Ergebnis in den natürlichen Zahlen.

Beispiel: $3+4=7 \quad und \quad 3*4=12$

Das ist bei der Subtraktion und Division nicht für alle natürlichen Zahlen der Fall, sondern es gibt Beispiele, in denen das Ergebnis dann keine natürliche Zahl mehr ist.

Beispiel: $3-4=-1 \quad und \quad 3/4=0.75$

Für die Division werden innerhalb der natürlichen und ganzen Zahlen die folgenden Begriffe und Regeln definiert.

Definition 1.1: Teiler und Vielfaches

Eine Zahl $a \in \mathbb{Z}$ heißt **durch** $b \in \mathbb{Z}, b \neq 0$ **teilbar**,
wenn es eine ganze Zahl $q \in \mathbb{Z}$ gibt, so dass $a = b \cdot q$ ist.

Diese Eigenschaft kann gesprochen über verschiedene Sätze ausgedrückt werden:

„in Zeichen $b \mid a$, gesprochen b teilt a“

„b ist ein Teiler von a.“

„a ist ein Vielfaches von b“

„Die Zahl b passt genau q - mal in die Zahl a.“

Beispiel:

$28 \; ist \; durch \; 7 \; teilbar$

$7 \; teilt \; 28, \; geschrieben \; 7 \mid 28$

$28 = 7 \cdot 4 \quad "7 \; passt \; genau \; 4-mal \; in \; die \; 28"$

Satz 1.1: Teilbarkeitsregeln

1. Gilt $c \mid b$ und $b \mid a$, so gilt auch $c \mid a$:
2. Gilt $b_1 \mid a_1 \;\; und \;\; b_2 \mid a_2$, so gilt auch $b_1 b_2 \mid a_1 a_2$

Beispiel:

1. $3 \mid 6 \;\; und \;\; 6 \mid 18 \Rightarrow 3 \mid 18$
2. $3 \mid 6 \;\; und \;\; 4 \mid 8 \Rightarrow 12 \mid 48$

Ist die Division nicht ganzzahlig innerhalb der natürlichen bzw. ganzen Zahlen möglich, so werden zusätzliche Begriffe definiert.

Definition 1.2: Division mit Rest

Für zwei ganze Zahlen $a, b \in \mathbb{Z}$ mit $b \neq 0$ gibt es genau eine Darstellung

$a = b \cdot q + r$ mit $q, r \in \mathbb{Z}$ und $0 \leq r < b$, $\;\; falls \;\; b > 0$

und $0 \leq r < -b$, $\;\; falls \;\; b < 0$.

a heißt Dividend, b Divisor
und r Rest der ganzzahligen Division von a durch b.

Definition 1.3: modulo, Rest der ganzzahligen Division

$a \bmod b$ ist der Rest, den a bei der Division durch b lässt,

d.h. wenn $a = b \cdot q + r$ mit $q, r \in \mathbb{Z}$ und $0 \leq r < b$

so ist $a \bmod b = r$.

Beispiel:

$9 \bmod 2 = 1 \Leftrightarrow 9 = 2 \cdot 4 + 1$

1 ist der Rest der ganzzahligen Division von 9 durch 2.

1.4.2 ggt und kgV

Der **größte gemeinsamer Teiler**, kurz **ggT**, ist die größte natürliche Zahl, die zwei oder mehrere ganze Zahlen ohne Rest teilt. Nachfolgend sind einige Definitionen dargestellt, die diese Eigenschaft formal beschreiben.

Definition 1.4: größter gemeinsamer Teiler ggT

Sind $a,b,d \in \mathbb{Z}$ und gilt $d\,|\,a$ und $d\,|\,b$,
so heißt d **gemeinsamer Teiler** von a und b.

Wenn für jeden anderen gemeinsamen Teiler c von a und b gilt: $c\,|\,d$,
so heißt d **größter gemeinsamer Teiler** von a und b
und wird mit $d = ggt(a,b)$ bezeichnet.

Beispiele:

(1) ggT(12,18)=6, denn $6\,|\,12$ und $6\,|\,18$
2 und 3 sind weitere Teiler von 12 und 18, aber beides sind kleinere Zahlen und sind als Faktor in der 6 enthalten, denn $2\,|\,6$ und $3\,|\,6$.
Es gibt keine größere Zahl als 6, die sowohl 12 als auch 18 teilt.

(2) ggT(100,20)=20,

(3) ggT(-4,14)=2

(4) ggT(3,8)=1

Wie können wir den größten gemeinsamen Teiler zweier gegebener Zahlen in einfacher und übersichtlicher Art und Weise ermitteln?

Dieses ermöglicht der Euklidische Algorithmus, den wir uns nachfolgend genauer anschauen. Zuvor jedoch blicken wir auf den nachfolgenden Satz, der die Basis für den Euklidischen Algorithmus bildet und diesen begründet.

Satz 1.2:
Seien *a* und *b* ganze Zahlen mit $a \neq 0$. Seien *q* und *r* Zahlen, für die gilt: $b = q \cdot a + r$.

Dann gilt ***ggT(b,a)=ggT(a,r)*** .

Die Aussage des Satzes ist die Folgende:

Suchen wir den größten gemeinsamen Teiler von zwei Zahlen a und b und wir zusätzlich wissen, dass b bei der ganzzahligen Division durch a den Rest r lässt, so reicht es, dass wir den ggT von a und r suchen, da dieser gleich dem ggT von a und b ist.

Euklidischer Algorithmus zur Berechnung des ggT:

Der ggT kann mittels des Euklidischen Algorithmus berechnet werden.

Eingangsgrößen sind zwei natürliche Zahlen *a* und *b*. Bei der Berechnung verfährt man nach Euklid wie folgt:

1. setze *m* = *a*; *n* = *b*
2. ist *m* < *n*, so vertausche *m* und *n*
3. berechne *r* mit $m = q \cdot n + r$ (d.h. r ist Rest der ganzzahligen Division)
4. setze *m* = *n*, *n* = *r*
5. ist *r* ≠ 0 fahre fort mit Schritt 2 , ist *r=0*, dann ist *m* der gesuchte ggT

Nach Ablauf des Verfahrens hat man **mit *m* den ggT von *a* und *b* gefunden**.

Beispiel des Euklidischen Algorithmus:

$Bestimmung\ des\ ggT\ von\ a = 105\ und\ b = 63$

m	n	q	r
105	63		
105	63	1	42
63	42	1	21
42	21	2	0
$\boxed{21}$			

$21\ ist\ der\ ggT\ von\ 63\ und\ 105$

Das **kleinste gemeinsame Vielfache**, kurz **kgV**, ist die kleinste natürliche Zahl, die zwei oder mehrere ganze Zahlen ohne Rest teilt. Nachfolgend sind einige Definitionen dargestellt, die diese Eigenschaft formal beschreiben.

Definition 1.5: kleinstes gemeinsames Vielfaches kgV

Sind $a, b, d \in \mathbb{Z}$

Eine Zahl $d \in \mathbb{Z}$ heißt **kleinstes gemeinsames Vielfaches** von a und b, bezeichnet $kgV(a,b)$ wenn folgende Bedingungen erfüllt sind:

(1) Sowohl a als auch von b sind Teiler von d **:** $a \mid d$ und $b \mid d$

(2) Es gibt keine kleinere Zahl, für die die Eigenschaft (1) erfüllt ist.

1.4.3 Primzahlen und Primfaktorzerlegung

Definition 1.6: Primzahl

Eine natürliche Zahl p wird eine Primzahl genannt, falls p>1 ist und 1 und p die einzigen natürlichen Zahlen sind, die p teilen.

Definition 1.7: Primfaktorzerlegung

Unter der **Primfaktorzerlegung**, auch als **Zerlegung in Primfaktoren** bezeichnet, versteht man die Darstellung einer natürlichen Zahl $a \in \mathbb{N}$ als Produkt von Primzahlen

$$a = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_n \quad \text{mit} \quad Primzahlen\ \ p_1, p_2, p_3, \ldots, p_n\ , n \in \mathbb{N}$$

Die in der Primfaktorzerlegung einer Zahl auftretenden Primzahlen $p_1, p_2, p_3, \ldots, p_n$ nennt man die **Primfaktoren** dieser Zahl.

Beispiele:

1200 = 2 · 2 · 2 · 2 · 3 · 5 · 5 = $2^4 \cdot 3 \cdot 5^2$ mit Primfaktoren 2, 3, 5

6936 = 2 · 2 · 2 · 3 · 17 · 17 = $2^3 \cdot 3 \cdot 17^2$ mit Primfaktoren 2, 3, 17

Satz 1.3: Fundamentalsatz der Arithmetik

Der **Fundamentalsatz der Arithmetik** besagt, dass jede natürliche Zahl eine Primfaktorzerlegung besitzt und dass diese, bis auf die Reihenfolge der Faktoren, eindeutig ist.

Bemerkungen:

(1) Treten gleiche Primfaktoren mehrfach auf, so werden sie entweder im Produkt mehrfach aufgeführt oder sie werden mit ihrer Potenzdarstellung geschrieben.

(2) Die Primfaktorzerlegung einer Primzahl *p* besteht aus dem einzigen Faktor *p*.

(3) Eine natürliche Zahl, die nicht selbst Primzahl ist, nennt man **zusammengesetzt**; ihre Primfaktorzerlegung besteht aus mehr als einem Faktor (möglicherweise auch mehrmals demselben).

(4) Die Primfaktorzerlegung großer Zahlen ist kein triviales Problem.

(5) Lässt man auch negative Exponenten zu, dann ist sogar jede positive rationale Zahl eindeutig als Produkt von Primzahl-Potenzen darstellbar.

$$\frac{1200}{6936} = \frac{2 \cdot 5^2}{17^2}$$

Satz 1.4: Primfaktorzerlegung zur Berechnung des ggT und des kgV

Den größten gemeinsamen Teiler ggT und auch das kleinste gemeinsame Vielfache kgV kann man auch aus der Primfaktorzerlegung von *a* und *b* bestimmen.

Für den **ggT(a,b)** verwendet man **alle Primfaktoren, die *a* und *b* gemeinsam haben**, und multipliziert diese. („Schnittmenge der Primfaktoren“)

Kommen Faktoren mit einem Exponenten vor, wird jeweils der kleinste Exponent genommen.

Für das **kgV(a,b)** wird **jeder Primfaktor mit dem jeweils höchsten Exponenten** verwendet, und anschließend multipliziert. („Obermenge der Primfaktoren“)

Kommen Faktoren mit einem Exponenten vor, wird jeweils der größte Exponent genommen.

Beispiel:

$a = 63 = 3*3*7$
$b = 105 = 3*5*7$
ggT $(63, 105) = 3*7 = 21$
kgV $(63, 105) = 3*3*5*7 = 315$

Satz 1.5: ggT und kgV

Für zwei Zahlen $a, b \in \mathbb{N}$ gilt der folgende Zusammenhang für den größten gemeinsamen Teiler ggT(a,b) und kgV(a,b):

$$kgV(a,b) = \frac{a \cdot b}{ggT(a,b)}$$

Beispiel:

$a = 63 = 3*3*7$
$b = 105 = 3*5*7$
ggT $(63, 105) = 3*7 = 21$
kgV $(63, 105) = \frac{63 \cdot 105}{21} = \frac{\cancel{3}*3*\cancel{7} \cdot 3*5*7}{\cancel{3}*\cancel{7}} = 315$

1.5 Mengen

Wir beginnen mit einer Wiederholung der Grundbegriffe der Mengenlehre.

1.5.1 Definitionen und Beschreibungen

Definition 1.8: Menge (Georg Cantor, 1845-1918)

Eine **Menge** ist eine Zusammenfassung von genau bestimmten, unterscheidbaren Objekten zu einem Ganzen. Diese Objekte heißen **Elemente der Menge**.

Wir schreiben

$x \in M$, falls x ein Element von M ist und

$x \notin M$, falls x kein Element von M ist.

Die Anzahl der Elemente in einer Menge bezeichnet man als **Mächtigkeit der Menge** und notiert dieses mit den "senkrechten Strichen" um die Menge: |M|

Bemerkung:

- Es muss dabei eindeutig bestimmbar sein, ob ein Objekt zu einer Menge gehört oder nicht.
- Mengen werden üblicherweise mit lateinischen Großbuchstaben und deren Elemente mit Kleinbuchstaben angegeben.

Beispiel:

(1) Die Menge der Sonntage im Jahr ist eine Menge im mathematischen Sinn gemäß Definition 1.1 .

(2) Die Menge Wasser im Regenfass ist hingegen keine Menge im mathematischen Sinn, da sie keine unterscheidbaren Objekte enthält.

(3) Die Menge der natürlichen Zahlen ist eine Menge gemäß Definition 1.1.

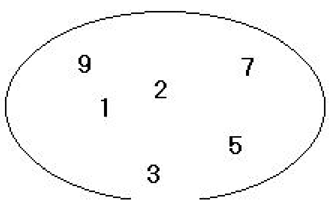
Beschreibung von Mengen

Eine Beschreibung von Mengen auf unterschiedliche Art und Weise möglich

(1) Graphisch durch so genannte Venn-Diagramme

Es können hier die Elemente direkt angegeben werden. Man kann aber auf eine direkte Eingabe der Elemente verzichten, wenn nur die Lage verschiedener Mengen zueinander dargestellt werden soll.

Beispiel:



(2) Aufzählend durch Aufzählung aller Elemente innerhalb einer Mengenklammer

$M = \{ Aufzählung \;\; aller \;\; Elemente \}$

Beispiel: $M = \{1,2,3,5,7,9\}$

(3) Beschreibend durch Angabe der Eigenschaften der Elemente

$M = \{ x | \; x \; hat \; bestimmte \; Eigenschaft \; e \}$

(gelesen: M ist die Menge aller x, für die gilt: x hat die Eigenschaft e)

Beispiel: $M = \{ x | \; x \; ist \; eine \; geometrische \; Figur \}$

$M = \{ x | x \; ist \; eine \; natürliche \; Zahl \; mit \; x \le 3 \} = \{1,2,3\}$

$[a,b] = \{ x | a \le x \le b \}$ (abgeschlossenes Intervall)

$(a,b) = \{ x | a < x < b \}$ (offenes Intervall)

1.5.2 Mengenbeziehungen

Definition 1.9: Leere Menge

Es gibt genau eine Menge ohne Elemente, die leere Menge $\varnothing$.

Definition 1.10: Teilmenge

Eine Menge N, die nur Elemente einer Menge M enthält, heißt **Teilmenge** (oder Untermenge) von M. Teilmenge (Schreibweise $N \subseteq M$) bedeutet:

$N \subseteq M$, falls gilt $x \in N \Rightarrow x \in M$.

Schreibweise: Falls explizit die Gleichheit von Menge du Teilmenge ausgeschlossen sein soll, so schreiben wir

$N \subset M$, falls N eine **echte Teilmenge** von M ist (d.h. $N \subseteq M$ und $N \neq M$)

Beispiel:

$M = \{1, a, K\}, N = \{1, a\} \;\; mit \; N \subseteq M \; und \; sogar \; N \subset M$.

Definition 1.11: Mengengleichheit

Zwei Mengen sind genau dann gleich, wenn sie dieselben Elemente enthalten.

Die Gleichheit der Mengen M und N (Schreibweise M = N) bedeutet:

M = N, falls gilt $x \in M$ genau dann, wenn $x \in N$ (d.h. $x \in M \Leftrightarrow x \in N$),

d.h. falls gilt: $M \subseteq N \; und \; N \subseteq M$.

Beispiel:

(1) Sei $M = \{x | x \in \mathbb{N} \; und \; x \leq 3\}$ und $N = \{1,2,3\}$, dann gilt $M = N$.

(2) Sei $M = \{x | x \in \mathbb{Z} \; und \; x \leq 3\}$ und $N = \{1,2,3\}$, dann gilt $M \neq N$, aber $N \subseteq M$.

Satz 1.6: Aussagen zu Teilmengen

(1) Jede Menge hat die Menge selbst und die leere Menge als Teilmenge.

(2) Die leere Menge hat nur sich selbst als Teilmenge.

(3) Eine Menge mit n Elementen hat 2^n Teilmengen.

Definition 1.12: Mengensystem

Eine Menge von Mengen heißt auch Mengensystem.

Beispiel:

$\{\{1,2\},\{1\},\{3\}\}$ und $\{\{1,2\},\{A\},\{\square, \bigcirc, \triangle\},\varnothing\}$ sind Mengensysteme.

Definition 1.13: Potenzmenge

Die Menge aller Teilmengen einer Menge M heißt **Potenzmenge zu M**: $P(M) := \{X | X \subseteq M\}$.

Die Potenzmenge einer Menge M mit n Elementen hat 2^n Elemente.

Beispiel:

Sei $M = \{0,1,2\}$, dann ist $P(M) := \{\varnothing,\{0\},\{1\},\{2\},\{0,1\},\{0,2\},\{1,2\},\{0,1,2\}\}$ und enthält 8 Teilmengen als Elemente.

Bemerkungen:

- Man beachte den Unterschied zwischen $\in$ und $\subseteq$:
  $x \in M, \{x\} \subseteq M, X \in P(M) \; mit \; X \subseteq M$.
- Ein Symbol $M \subset N$ bedeutet bei manchen Autoren $M \subseteq N$ und bei anderen $M \subseteq N$ und $M \neq N$.

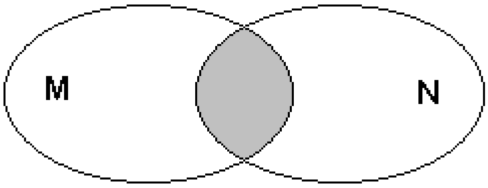
1.5.3 Operationen mit Mengen

Definition 1.14: Durchschnitt von Mengen

Die Durchschnittsmenge zweier Mengen M und N ist die Menge aller Elemente, die sowohl zu M als auch zu N gehören:

$$M \cap N := \{x \mid x \in M \text{ und } x \in N\}$$

M und N heißen **disjunkte Mengen**, falls $M \cap N = \varnothing$.

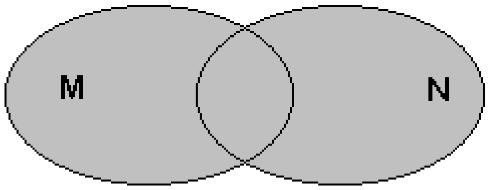


Durchschnittsmenge

Definition 1.15: Vereinigung von Mengen

Die Vereinigungsmenge zweier Mengen M und N ist die Menge aller Elemente, die zu M oder zu N (oder zu beiden) gehören:

$$M \cup N := \{x \mid x \in M \text{ oder } x \in N\}$$



Vereinigungsmenge

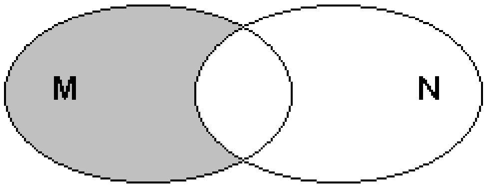
Bemerkung:

- Das deutsche Wort „oder" ist im täglichen Sprachgebrauch nicht eindeutig. Es kann zwei verschiedene Bedeutungen haben:
  1. „ausschließendes oder" bzw. „exklusives oder": $x \in M \text{ oder } x \in N$, aber x ist nicht Element von beiden.
  2. „nicht ausschließendes oder" bzw. „inklusives oder": $x \in M \text{ oder } x \in N$ oder x ist Element von beiden.
- In der Mathematik ist stets das „**inklusive oder**" gemeint, wenn nicht explizit etwas anderes angegeben ist.

Definition 1.16: Differenzmenge

Die Differenzmenge zweier Mengen M und N ist die Menge aller Elemente, die zu M aber nicht zu N gehören:

$$M \setminus N := \{x \mid x \in M \text{ und } x \notin N\}.$$

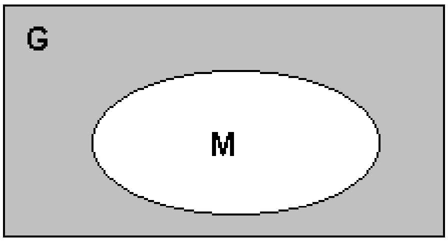


Differenzmenge

Definition 1.17: Komplement

Die Komplementmenge einer Menge M (bezüglich der Grundmenge G) ist die Menge aller Elemente von G, die nicht zu M gehören:

$$\overline{M} := \{x \mid x \in G \text{ und } x \notin M\}.$$



Komplement

Bemerkung:

Die betrachteten Mengen sind stets Teilmengen einer vorgegebenen Grundmenge G sind. Man schreibt dieses jedoch nicht immer explizit auf.

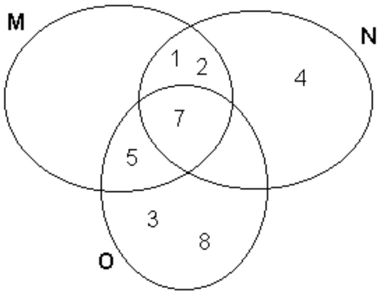
Beispiel:

Gegeben sei das folgende Venn-Diagramm der Mengen M, N und O mit

$M := \{1,2,5,7\}$,

$N := \{1,2,4,7\}$,

$O := \{3,5,7,8\}$



Durchschnittsmengen:

$M \cap N := \{1,2,7\}$ $\quad M \cap O := \{5,7\}$ $\quad N \cap O := \{7\}$

Vereinigungsmengen:

$M \cup N := \{1,2,5,7,4\}$ $\quad M \cup O := \{1,2,5,7,3,8\}$ $\quad N \cup O := \{1,2,4,7,5,3,8\}$

Differenzmengen:

$M \setminus N := \{5\}$ $\quad M \setminus O := \{1,2\}$ $\quad N \setminus O := \{1,2,4\}$

$N \setminus M := \{4\}$ $\quad O \setminus M := \{3,8\}$ $\quad O \setminus N := \{3,5,8\}$

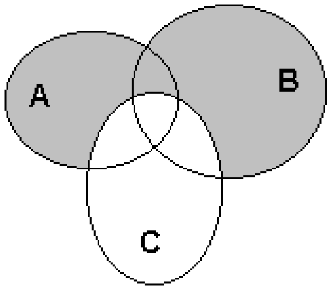
Komplementärmengen (in Bezug auf die Grundmenge $M \cup N \cup O$):

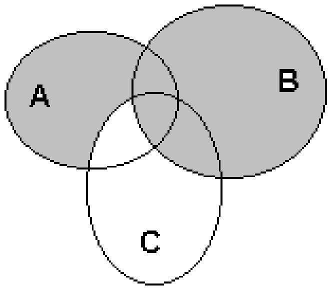
$\overline{M} := \{3,8,4\}$ $\quad \overline{O} := \{1,2,4\}$ $\quad \overline{N} := \{5,3,8\}$

Beispiel:
Mittels der Venn-Diagramme kann geprüft werden, ob folgende Mengenformel gültig ist:

$$(A \cup B) \setminus C = (A \setminus C) \cup B$$

Nach Erstellung des Venn-Diagramms ist klar, dass diese Mengengleichung falsch ist.





Es gilt aber: $(A \cup B) \setminus C \subseteq (A \setminus C) \cup B$

Definition 1.18: Mächtigkeit einer Menge

Die Anzahl der Elemente einer endlichen Menge M wird mit $|M|$ bezeichnet und die **Mächtigkeit** (auch Länge oder Kardinalität) von M genannt.

Satz 1.7: Mächtigkeiten von Mengen

(1) Sind M und N disjunkte endliche Mengen, so gilt $|M \cup N| = |M| + |N|$.

(2) Für alle endlichen Mengen M und N gilt: $|M \cup N| = |M| + |N| - |M \cap N|$.

(3) Für alle endlichen Mengen M und N gilt: $|M \setminus N| = |M| - |M \cap N| = |M \cup N| - |N|$.

(4) Für alle endlichen Mengen M gilt: $|P(M)| = 2^{|M|}$

Beispiele:

$|\{1,2,3\}| = 3,\ |\varnothing| = 0,\ |\{\varnothing\}| = 1$

$M = \{1,2,3,4\}$, $N = \{1,3,5\}$

$|M \cup N| = |M| + |N| - |M \cap N| = 4 + 3 - 2 = 5$

1.5.4 Grundgesetze der Mengenalgebra

Satz 1.8: Rechengesetze bei Mengen

Seien M, N, O Mengen, dann gilt:

Kommutativgesetze $M \cap N = N \cap M$ beim Durchschnitt

$M \cup N = N \cup M$ bei der Vereinigung

Assoziativgesetze $(M \cap N) \cap O = M \cap (N \cap O)$ beim Durchschnitt

$(M \cup N) \cup O = M \cup (N \cup O)$ bei der Vereinigung

Distributivgesetze $M \cup (N \cap O) = (M \cup N) \cap (M \cup O)$ 1.Distributivgesetz

$M \cap (N \cup O) = (M \cap N) \cup (M \cap O)$ 2.Distributivgesetz

Beispiele:

Seien Mengen M = $\{1, 2, 3\}$, N = $\{2, 4, 6\}$, O = $\{2, 4, 7\}$ gegeben, dann gilt

für die Kommutativität

$M \cap N = N \cap M = \{2\}$ und $M \cup N = N \cup M = \{1, 2, 3, 4, 6\}$

für die Assoziativität:

"$\cap$": $\{1, 2, 3\} \cap (\{2, 4, 6\} \cap \{2, 4, 7\}) \overset{\overset{\text{zu zeigen}}{!}}{=} (\{1, 2, 3\} \cap \{2, 4, 6\}) \cap \{2, 4, 7\}$

$\{1, 2, 3\} \cap \{2, 4\} = \{2\} \cap \{2, 4, 7\}$

$\{\ 2\ \} = \{\ 2\ \}$ *q.e.d.*

"$\cup$": $\{1, 2, 3\} \cup (\{2, 4, 6\} \cup \{2, 4, 7\}) \overset{!}{=} (\{1, 2, 3\} \cup \{2, 4, 6\}) \cup \{2, 4, 7\}$

$\{1, 2, 3\} \cup \{2, 4, 6, 7\} = \{1, 2, 3, 4, 6\} \cup \{2, 4, 7\}$

$\{1, 2, 3, 4, 6, 7\} = \{1, 2, 3, 4, 6, 7\}$ *q.e.d.*

für die Distributivität:

1.*Distributivgesetz*

$$\{1, 2, 3\} \cup (\{2, 4, 6\} \cap \{2, 4, 7\}) \overset{\overset{\text{zu zeigen}}{!}}{=} (\{1, 2, 3\} \cup \{2, 4, 6\}) \cap (\{1, 2, 3\} \cup \{2, 4, 7\})$$

$$\{1, 2, 3\} \cup (\{2, 4\}) = (\{1, 2, 3, 4, 6\}) \cap (\{1, 2, 3, 4, 7\})$$

$$\{1, 2, 3, 4\} = \{1, 2, 3, 4\} \quad q.e.d.$$

2.*Distributivgesetz*

$$\{1, 2, 3\} \cap (\{2, 4, 6\} \cup \{2, 4, 7\}) \overset{\overset{\text{zu zeigen}}{!}}{=} (\{1, 2, 3\} \cap \{2, 4, 6\}) \cup (\{1, 2, 3\} \cap \{2, 4, 7\})$$

$$\{1, 2, 3\} \cap (\{2, 4, 6, 7\}) = (\{2\}) \cup (\{2\})$$

$$\{\ 2\ \} = \{\ 2\ \} \quad q.e.d.$$

Satz 1.9:

Sei M Teilmenge einer Grundmenge G, dann gilt:

(1) $\overline{\overline{M}} = M$ (**doppeltes Komplement**)

(2) $\overline{M} \cup M = G \quad und \quad \overline{M} \cap M = \emptyset$

(3) $M \cap M = M$ (**Idempotenzgesetz für Durchschnitt**)

$M \cap \emptyset = \emptyset$

$M \cap G = M$ (G ist **neutrales Element für Durchschnitt**)

$M \cap N = N \;\; mit \;\; N \subseteq M$

(4) $M \cup M = M$ (**Idempotenzgesetz für Vereinigung**)

$M \cup \emptyset = M$ ($\emptyset$ ist **neutrales Element für Vereinigung**)

$M \cup G = G$

$M \cup N = M \;\; mit \;\; N \subseteq M$

Beispiel:

$G = \{1,2,3,4,5,6,7,8,9\} \; und \; M = \{1,2,3\}$,

$dann \; ist \; \overline{M} = \{4,5,6,7,8,9\} \; das \; Komplement \; von \; M \; in \; G$,

$\overline{\overline{M}} = \{1,2,3\} \; das \; Komplement \; von \; \overline{M} \; in \; G.$

Satz 1.10: De Morgansche Regeln

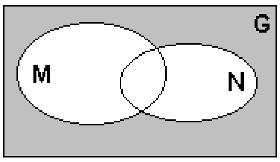
Seien M und N Teilmengen einer Grundmenge G, dann gilt:

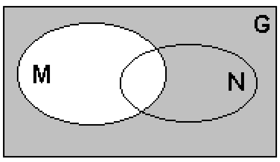
$$\overline{(M \cup N)} = \overline{M} \cap \overline{N} \quad und \quad \overline{(M \cap N)} = \overline{M} \cup \overline{N}$$

Erläuterung der De Morganschen Regeln anhand der Venn-Diagramme:

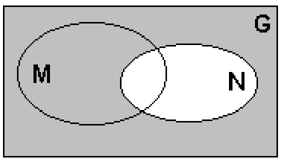
Erste De Morgansche Regel

linke Seite





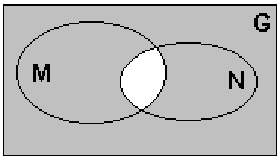
1. Term der rechten Seite

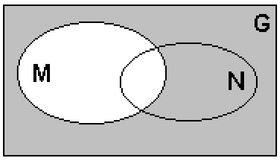


2.Term der rechten Seite

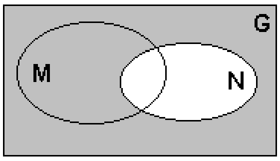
Zweite De Morgansche Regel

linke Seite





1. Term der rechten Seite



2.Term der rechten Seite

Beispiel:

Die aufgestellten Regeln erlauben es, komplizierte Ausdrücke zu vereinfachen.

$$(A\cap B)\cup\left(\overline{\overline{A}\cup B}\right)=$$

$$(A\cap B)\cup\left(\overline{\overline{A}}\cap\overline{B}\right)= \qquad (\textit{gilt nach der ersten De Morganschen Regel Satz } 1.10)$$

$$(A\cap B)\cup\left(A\cap\overline{B}\right)= \qquad (\textit{gilt nach dem Satz } 1.9 \textit{ doppeltes Komplement})$$

$$A\cap\left(B\cup\overline{B}\right)= \qquad (\textit{gilt nach dem Distributivgesetz Satz } 1.8)$$

$$A \qquad (\textit{gilt nach dem Satz } 1.9)$$

Bemerkung:

- Mengenalgebraische Ausdrücke sind in der Regel durch konsequente Klammerung klar definiert.
- Wenn in Ausdrücken keine Klammern gesetzt sind, so gilt die Konvention:

  Komplement vor *Durchschnitt* vor *Vereinigung bzw. Differenz*
- Somit sind die folgenden Ausdrücke äquivalent:

$$A\cup B\cap C\cup D\cap E \quad\Leftrightarrow\quad \big(A\cup(B\cap C)\big)\cup(D\cap E)$$

In der nachfolgenden Definition eines kartesischen Produktes werden Paare aus jeweils zwei Elementen von zwei verschiedenen Mengen gebildet. Die Paare aller möglichen Kombinationen werden in einer Menge, genannt kartesisches Produkt, zusammengefasst. Das kartesische Produkt bildet die Grundlage für das Kapitel 1.2 „Relationen“, in dem aus diesen Paaren gewisse Paare mit speziellen Eigenschaften herausgesucht werden.

Definition 1.19: kartesisches Produkt

Seien M und N Mengen. Das ***kartesische Produkt*** $M \times N$ von M und N ist die Menge aller Paare mit erstem Element aus M und zweitem Element aus N:

$$M \times N := \{(m,n) | m \in M \text{ und } n \in N\}.$$

Beispiele:

(1) A={Menge aller Autos}, B={Menge aller Autobesitzer}, dann enthält

$$A \times B := \{(a,b) | a \text{ ist ein Auto und } b \text{ ist ein Autobesitzer}\}$$

alle möglichen Kombinationen (Auto, Autobesitzer).

(2) Das kartesische Produkt der Mengen A := { u, v } und B := { 2, 7, 0} ist die Menge

$$A \times B := \{(u,2),(u,7),(u,0),(v,2),(v,7),(v,0)\}.$$

Das kartesische Produkt enthält 6 Elemente.

(3) Als kartesisches Koordinatensystem wird das kartesische Produkt $\mathbb{R} \times \mathbb{R}$ bezeichnet ($\mathbb{R}$ ist die Menge der *reellen Zahlen*), in dem jeder Punkt einer Ebene durch zwei *Koordinaten* x und y dargestellt werden kann.

Satz 1.11: (Mächtigkeit des kartesischen Produkts zweier Mengen)

Seien M und N endliche Mengen, dann gilt:

$$|M \times N| = |M| \cdot |N|$$

Definition 1.20: n-faches kartesisches Produkt

Seien M_i Mengen, dann ist das n-fache ***kartesische Produkt*** $M_1 \times M_2 \times M_3 \times ... \times M_n$ definiert als die Menge aller n-Tupel mit i-tem Element aus M_i für i=1,...,n:

$$M_1 \times M_2 \times ... \times M_n := \{(m_1, m_2, ..., m_n) | m_i \in M_i\}.$$

1.5.5 Der Binomialkoeffizient

Der Binomialkoeffizient gibt die Anzahl der Teilmengen mit k Elemeten einer Menge mit n Elementen an.

Definition 1.21: Binomialkoeffizient

Für $n,k \in \mathbb{N}_0$ mit $n \geq k$ definiert man den Binomialkoeffizienten n über k

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

Insbesondere gilt $\binom{0}{0} := 1$, $\binom{n}{n} := 1$, $\binom{n}{0} := 1$ (da $0! = 1$ gilt).

Satz 1.12:

Seien $n,k \in \mathbb{N}_0$ und $n \geq k$. Dann gilt für den Binomialkoeffizienten n über k die folgende Rekursion:

$$\binom{n}{k} = \begin{cases} 1 & , \textit{falls } k = 0, k = n \\ \binom{n-1}{k} + \binom{n-1}{k-1} & , \textit{sonst} \end{cases}$$

Bemerkung:

- Hinter dieser rekursiven Vorschrift verbirgt sich die Möglichkeit, den Binomialkoeffizienten mit Hilfe des **Pascal´schen Dreieck**s zu berechnen.
- Jeder Koeffizient ergibt sich als Summe der beiden schräg darüber stehenden Koeffizienten

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

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

$$\binom{2}{0} = 1 \qquad \binom{2}{1} = 2 \qquad \binom{2}{2} = 1$$

$$\binom{3}{0} = 1 \qquad \binom{3}{1} = 3 \qquad \binom{3}{2} = 3 \qquad \binom{3}{3} = 1$$

$$\binom{4}{0} = 1 \qquad \binom{4}{1} = 4 \qquad \binom{4}{2} = 6 \qquad \binom{4}{3} = 4 \qquad \binom{4}{4} = 1$$

Beispiele:

$$\binom{8}{5} = \frac{8!}{5!(8-5)!} = \frac{8!}{5!3!} = \frac{6 \cdot 7 \cdot 8}{3!} = 56 \quad \textit{und} \quad \binom{8}{5} = \binom{7}{5} + \binom{7}{4} = 21 + 35 = 56$$

Satz 1.13: Eigenschaften des Binomialkoeffizienten

Seien $n,k \in \mathbb{N}_0$ und $n \geq k$. Dann gilt für den Binomialkoeffizienten n über k:

1. $\binom{n}{k} = \binom{n}{n-k}$
2. $\sum_{k=0}^{n} \binom{n}{k} = |P(M)| = 2^n$, d.h. die Anzahl der Teilmengen einer n-elementigen Menge ist gleich der Summe der Binomialkoeffizienten, also einer Zeile im Pascalschen Dreieck.

Satz 1.14: Binomischer Lehrsatz (oder Binomialsatz)

Für $n \in \mathbb{N}_0$ und $a,b \in \mathbb{R}$ gilt:

$$\begin{aligned}(a+b)^n &= \binom{n}{0}a^n + \binom{n}{1}a^{n-1}b^1 + \binom{n}{2}a^{n-2}b^2 + \ldots + \binom{n}{n-1}a^1b^{n-1} + \binom{n}{n}b^n \\ &= \sum_{k=0}^{n} \binom{n}{k} a^{n-k}b^k\end{aligned}$$

Bemerkung:

Für n = 2 erhalten wir die bekannten Binomischen Formel, siehe auch im nachfolgenden Abschnitt.

1.5.6 Binomische Formeln

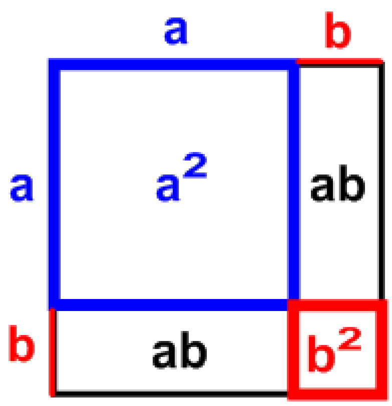
$(a+b)^2 = a^2 + 2ab + b^2 \quad 1.\textit{Binomische Formel}$

$(a-b)^2 = a^2 - 2ab + b^2 \quad 2.\textit{Binomische Formel}$

$(a-b)(a+b) = a^2 - b^2 \quad 3.\textit{Binomische Formel}$

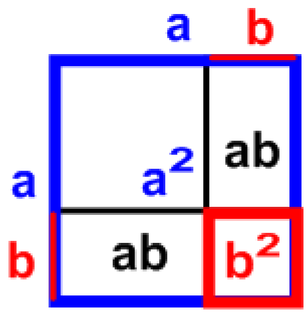
Veranschaulichung der 1.Binomischen Formel

$(a+b)^2 = a^2 + 2ab + b^2 \quad 1.\textit{Binomische Formel}$



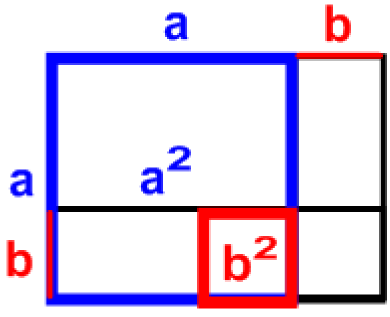
Veranschaulichung der 2.Binomischen Formel

$(a-b)^2 = a^2 - 2ab + b^2 \quad 2.\textit{Binomische Formel}$



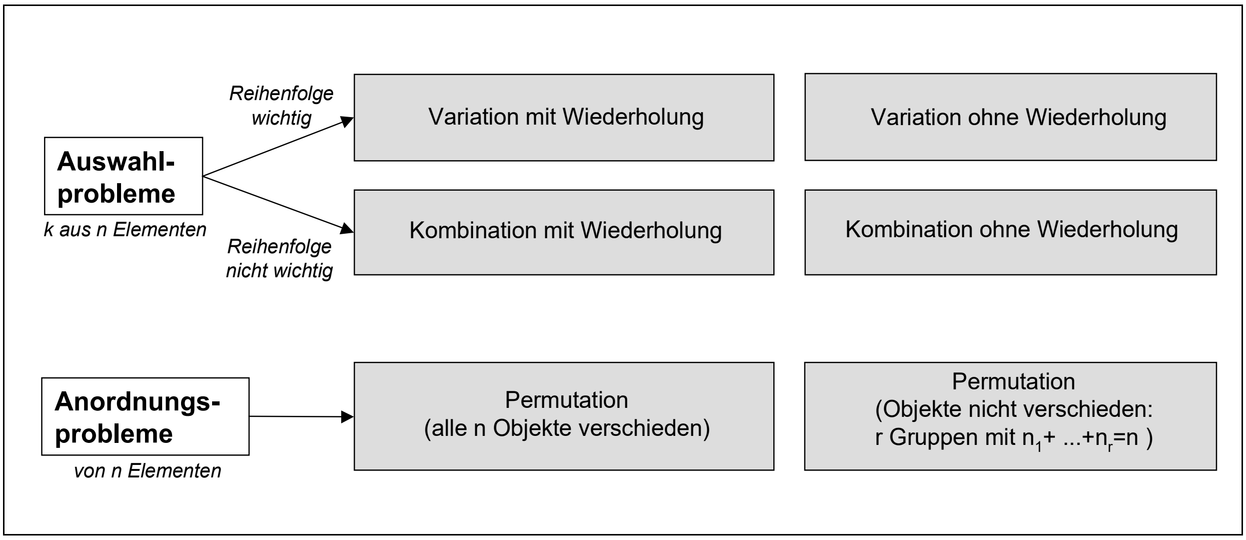
Veranschaulichung der 3.Binomischen Formel

$(a-b)(a+b) = a^2 - b^2 \quad 3.\textit{Binomische Formel}$



1.6 Grundelemente der Kombinatorik

Die Kombinatorik untersucht Anordnungen und Auswahlmengen von Objekten endlicher Mengen. Sie ist grundlegend für die Wahrscheinlichkeitstheorie und war früher auch Teil der Wahrscheinlichkeitstheorie. Sie wird jetzt aber eigenständig betrachtet.



1.6.1 Permutationen

Der nachfolgende Satz bildet die Grundlage für die Permutationen.

Satz 1.15: Das allgemeine Zählprinzip

Es seien Mengen $M_1, M_2, ..., M_n$ mit den Mächtigkeiten $|M_1| = m_1, |M_2| = m_2, ..., |M_n| = m_n$ gegeben. Für die Konstruktion von n-Tupeln $(x_1, x_2, ..., x_n)$ mit $x_i \in M_i$ gibt es $m_1 \cdot m_2 \cdot ... \cdot m_n$ verschiedene Möglichkeiten.

Beispiel:

Besteht ein Autokennzeichen $\boxed{HH\boxed{A}\boxed{K}\boxed{146}}$ nach dem Zulassungsbezirk aus ein oder zwei Buchstaben und einer dreistelligen Zahl: $\boxed{-}\boxed{-}\boxed{---} = (x_1, x_2, x_3)$ mit x_1 aus der Menge der 26 Buchstaben, x_2 aus der Menge der 26 Buchstaben oder kein Buchstabe und x_3 einer 3-stelligen Zahl zwischen 1 und 999, dann gibt es

$m_1 \cdot m_2 \cdot m_3 = 26 \cdot 27 \cdot 999 = 701298$ Fahrzeuge, die zugelassen werden können.

Definition 1.22: Permutation

Eine Permutation einer nicht leeren Menge M mit $|M| = n$ Elementen ist eine bijektive Abbildung auf sich selbst: $p: M \to M \quad i \to p(i)$.

Mit dieser bijektiven Abbildung erzielt man eine (veränderte) Anordnung der Elemente der Menge.

Beispiel:

Gegeben sei die Menge $M = \{1,2,3\} \ mit \ |M| = 3$. Die nachfolgenden bijektiven Abbildungen $p: M \to M \quad i \to p(i)$ mit

$$\begin{matrix} 1 \to 1 & 1 \to 1 & 1 \to 2 & 1 \to 2 & 1 \to 3 & 1 \to 3 \\ 2 \to 2\,, & 2 \to 3\,, & 2 \to 1\,, & 2 \to 3\,, & 2 \to 1\,, & 2 \to 2 \\ 3 \to 3 & 3 \to 2 & 3 \to 3 & 3 \to 1 & 3 \to 2 & 3 \to 1 \end{matrix}$$

erzeugen die folgenden 6 verschiedenen als n-Tupel notierten Anordnungen der Menge $M = \{1,2,3\}$:

$$(1,2,3), (1,3,2), (2,1,3), (2,3,1), (3,1,2), (3,2,1)$$

Satz 1.16:

Die Elemente einer Menge M mit n verschiedenen Elementen lassen sich auf genau $n!$ verschiedene Arten anordnen, d.h. es gibt $P_n = n!$ Permutationen.

Bemerkung: Definition Fakultät

Für $n \in \mathbb{N}$ ist $n! := 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n$ und für 0 wird definiert: $0! = 1$.

Veranschaulichung von Satz 1.16:

Bei der Anordnung von n Objekten hat man für die Besetzung der ersten Stelle n Möglichkeiten. Für jede dieser Möglichkeiten hat man dann für die zweite Stelle noch (n-1) Möglichkeiten zur Besetzung der Stelle übrig, da das n-te Element ja schon an der ersten Stelle steht. Entsprechend hat man zur Besetzung der zweiten Stelle noch (n-2) Elemente zur Verfügung. Zur Besetzung der vorletzten Stelle hat man noch 2 Elemente zur Auswahl und für die letzte Stelle dann noch genau 1 Element zur Verfügung, so dass die Gesamtzahl der Möglichkeiten sich aus der Multiplikation

$$n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot 2 \cdot 1 = n!$$

ergibt.

Dieses wird auch aus dem vorhergehenden Beispiel ersichtlich.

Satz 1.17:

Gegeben sei eine Menge M mit n Elementen, wobei nur r Elemente verschieden sind mit jeweils $n_1, n_2, ..., n_r$ gleichen Elementen und $n_1 + n_2 + ... + n_r = n$, d.h. r Gruppen mit $n_1, n_2, ..., n_r$ gleichen Elementen. Dann gibt es $P_{n_1, n_2, ..., n_r} = \frac{n!}{n_1! \cdot n_2! \cdot ... \cdot n_r!}$ Permutationen.

Veranschaulichung am Beispiel:

Das Wort „SASS“ hat 4 Buchstaben und würde nach Satz 1.16 $4! = 24$ Permutationen besitzen, wenn alle Buchstaben unterscheidbar wären. Das „S“ ist jedoch 3-mal vorhanden und nicht unterscheidbar. Es gibt insgesamt nur $\frac{4!}{1! \cdot 3!} = 4$ unterscheidbare „Wörter“, nämlich „SASS“, „ASSS“, „SSAS“, „SSSA“.

1.6.2 Variationen

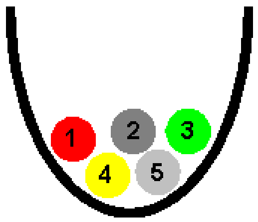
Definition 1.23: Variation

Gegeben sei eine Menge M mit n Elementen. Eine Auswahl von k Elementen dieser Menge (auch Stichprobe genannt) heißt eine **Variation**, wenn die **Reihenfolge der Elemente von Bedeutung** ist. Speziell nennt man sie

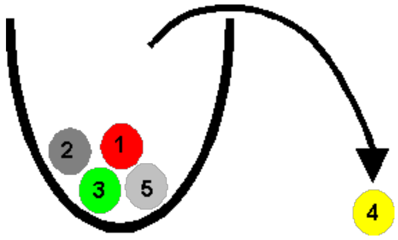
- eine **Variation ohne Wiederholung**, wenn die Elemente der Menge M nur höchstens einmal vorkommen dürfen.
- Eine **Variation mit Wiederholung**, wenn die Elemente der Menge M mehrfach vorkommen dürfen.

Das Urnenmodell: Ziehen mit Zurücklegen mit Beachtung der Reihenfolge

Problemstellung: Eine Urne enthält fünf verschieden farbige Kugeln. Es werden nacheinander drei Kugeln gezogen, wobei jede Kugel nach dem Ziehen sofort wieder in die Urne zurückgelegt wird.
Wie viele verschiedene Ergebnisse sind bei dieser Vorgehensweise möglich?

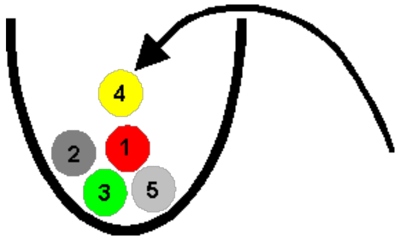


Ausgangspunkt: Eine Urne mit den fünf verschieden farbigen Kugeln.

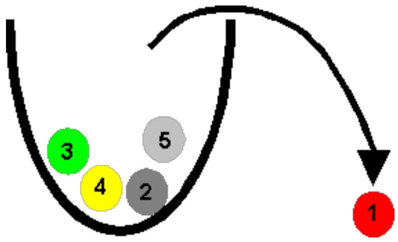


Von diesen fünf Kugeln wird nun eine beliebige Kugel zufällig herausgegriffen: In unserem Fall die gelbe Kugel.

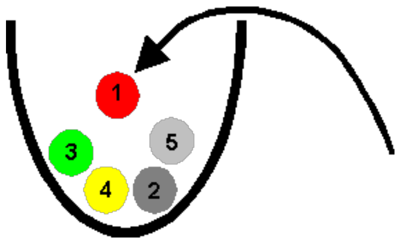
Da aber fünf verschiedene Kugeln in unserer Urne lagen, hatten wir für diesen Zug auch **5 Möglichkeiten**, eine dieser fünf Kugeln zu ziehen.



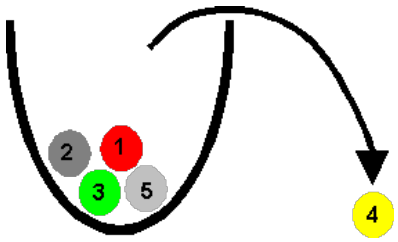
Nun wird die eben gezogene Kugel wieder zu den anderen Kugeln in die Urne **zurückgelegt**.
Man hat nun wieder alle fünf verschiedenen Kugeln in der Urne.



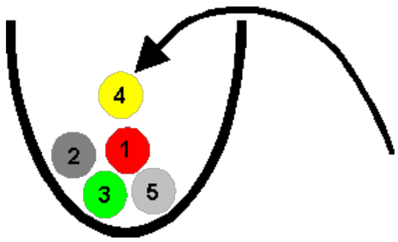
Jetzt wird ein zweites Mal gezogen. Durch das Zurücklegen der -in unserem Fall gelben- Kugel hat man wieder alle fünf Kugeln in der Urne und somit auch wieder **5 Möglichkeiten** für den zweiten Zug.
Diesmal wird die rote Kugel gezogen.



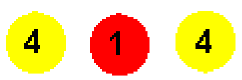
Wie eben wird nun die gezogene -rote- Kugel wieder zu den anderen Kugeln in die Urne **zurückgelegt**, so dass man wieder alle fünf verschiedene Kugeln in der Urne hat.



Nun wird ein drittes und letztes Mal gezogen. Auch hier hat man durch das Zurücklegen wieder alle fünf Kugeln zur Auswahl.
Somit hat man auch wieder **5 Möglichkeiten**, die dritte Kugel zu ziehen.
In unserem Fall erwischen wir erneut die gelbe Kugel, was nur durch das Zurücklegen möglich wurde.



Die eben gezogen Kugel wird wieder in die Urne zurückgelegt.



Wir haben also die folgende Reihenfolge gezogen.

Doch dies ist nur eine von vielen Möglichkeiten:

Beim **ersten** Ziehen hat man **5** Möglichkeiten.

Beim **zweiten** Ziehen hat man wiederum **5** Möglichkeiten

Beim **dritten** Ziehen existieren wieder **5** Möglichkeiten

Insgesamt: 5 * 5 * 5 = 125 Möglichkeiten

Verallgemeinerung:

Betrachtet man eine Urne mit **n** (statt 5) Kugeln, aus der **k**-mal (statt 3-mal) gezogen wird, so erhält man folgenden Merksatz:

> Die Anzahl der Möglichkeiten, **k** Kugeln aus **n** Kugeln mit Zurücklegen mit Berücksichtigung der Reihenfolge zu ziehen, ist n^k.

Satz 1.18: Variation mit Wiederholung

Gegeben sei eine Menge M mit n verschiedenen Elementen. Es existieren ${}^{w}V_n^k = n^k$ Variationen mit Wiederholung.

Veranschaulichung: (Geordnetes Ziehen mit Zurücklegen)

Aus einer Urne mit n Kugeln werden nacheinander k Kugeln gezogen und das Ergebnis in fester Reihenfolge aufgeschrieben. Vor jeder Ziehung wird die zuvor gezogene Kugel wieder in die Urne zurückgelegt. Die Anzahl der Möglichkeiten ist n^k.

Beispiel: Zeichencodierung

Sei n=2, nämlich die Menge $M = \{0,1\}$. Dann lassen sich durch ein Datenelement von k Bit Länge genau 2^k Zeichen darstellen. Jeder Variation kann also ein Zeichen zugeordnet werden. Ist k=8, also ein Byte, dann können damit $2^8 = 256$ Zeichen codiert werden. In zwei Byte (k=16) können $2^{16} = 65536$ Zeichen dargestellt werden.

Satz 1.19: Variation ohne Wiederholung

Gegeben sei eine Menge M mit n verschiedenen Elementen. Es existieren $V_n^k = \frac{n!}{(n-k)!} = n \cdot \ldots \cdot (n-k+1)$ Variationen ohne Wiederholung.

Veranschaulichung: (Geordnetes Ziehen ohne Zurücklegen)

Aus einer Urne mit n Kugeln werden nacheinander k Kugeln gezogen und in fester Reihenfolge abgelegt. Die Anzahl der Möglichkeiten ist $n \cdot \ldots \cdot (n-k+1)$

Beispiel: Pferdewette

Die Möglichkeiten einer Einlaufwette beim Pferderennen lassen sich aus der Formel für einer Variation ohne Wiederholung berechnen, denn beim Pferderennen wird aus einer gegebenen Menge von Pferden (z.B. n=15) die Reihenfolge des Einlaufes der ersten Pferde (z.B. k=5) vorhergesagt. Die Anzahl der Möglichkeiten einer solchen Vorhersage ist $V_{15}^5 = \frac{15!}{(15-5)!} = 15 \cdot \ldots \cdot (15-5+1) = 15 \cdot 14 \cdot 13 \cdot 12 \cdot 11 = 360360$.

1.6.3 Kombinationen

Definition 1.24: Kombination

Gegeben sei eine Menge M mit n Elementen. Eine Auswahl von k Elementen dieser Menge (auch Stichprobe genannt) heißt eine **Kombination**, wenn die **Reihenfolge der Elemente ohne Bedeutung** ist. Speziell nennt man sie

- eine **Kombination ohne Wiederholung**, wenn die Elemente der Menge M nur höchstens einmal vorkommen dürfen.
- Eine **Kombination mit Wiederholung**, wenn die Elemente der Menge M mehrfach vorkommen dürfen.

Satz 1.20: Kombination mit Wiederholung

Gegeben sei eine Menge M mit n verschiedenen Elementen. Es existieren ${}^{w}C_n^{\,k} = \binom{n+k-1}{k} = \frac{n+k-1!}{(n-1)!\cdot k!}$ Kombinationen mit Wiederholung.

Veranschaulichung: (Ungeordnetes Ziehen mit Zurücklegen)

Aus einer Urne mit n Kugeln werden nacheinander k Kugeln gezogen. Vor jeder Ziehung wird die zuvor gezogene Kugel wieder in die Urne zurückgelegt. Die Anzahl der Möglichkeiten ist ${}^{w}C_n^{\,k} = \binom{n+k-1}{k} = \frac{n+k-1!}{(n-1)!\cdot k!}$.

Beispiel: Würfelexperiment

Bei einem Würfelexperiment wird mit zwei Würfeln geworfen. Welche möglichen Kombinationen an Augenzahlen gibt es für die gefallenen Würfel?

Es handelt sich hierbei um eine Kombination mit Wiederholung. Die zwei Würfel (k=2) sind nicht unterscheidbar und die Menge, aus der „gezogen“ wird, hat die Mächtigkeit n=6. Daher sind die möglichen Würfe über die Formel ${}^{w}C_6^{\,2} = \binom{6+2-1}{2} = \frac{(6+2-1)!}{(6-1)!\cdot 2!} = \frac{7\cdot 6}{2} = 21$ bestimmbar.

Satz 1.21: Kombination ohne Wiederholung

Gegeben sei eine Menge M mit n verschiedenen Elementen. Es existieren $C_n^{\,k} = \binom{n}{k} = \frac{n!}{(n-k)!\cdot k!}$ Kombinationen ohne Wiederholung.

Veranschaulichung: (Ungeordnetes Ziehen ohne Zurücklegen)

Man stellt sich dabei das Ziehen von k Kugeln aus einer Urne mit n Kugeln vor. Die gezogenen Kugeln werden nicht wieder zurückgelegt. Die Anzahl der Möglichkeiten ist

$$C_n^{\,k} = \binom{n}{k} = \frac{n!}{(n-k)! \cdot k!}$$

Beispiel: Zahlenlotto

Das typische Beispiel für eine Kombination ohne Wiederholung ist das Zahlenlotto 6 aus 49, bei dem 6 Zahlen (k=6) aus 49 Zahlen (n=49) ohne Berücksichtigung einer Reihenfolge gezogen werden. Für diese Ziehung der Zahlen gibt es $C_{49}^{\,6} = \binom{49}{6} = \frac{49!}{(49-6)! \cdot 6!} = \frac{49 \cdot 48 \cdot 47 \cdot 46 \cdot 45 \cdot 44}{6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1} = 13.983.816$ Möglichkeiten.

1.6.4 Zusammenfassung: Permutation-Variation-Kombination

Auswahlprobleme

Variation mit Wiederholung

$$\boxed{{}^{w}V_n^{\,k} = n^k}$$

Variation ohne Wiederholung

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

Sonderfall k=n: Permutation

Kombination mit Wiederholung

$$\boxed{{}^{w}C_n^{\,k} = \binom{n+k-1}{k} = \frac{n+k-1!}{(n-1)! \cdot k!}}$$

Kombination ohne Wiederholung

$$\boxed{C_n^{\,k} = \binom{n}{k} = \frac{n!}{(n-k)! \cdot k!}}$$

Anordnungsprobleme

Permutation
(alle n Objekte verschieden)

$$\boxed{P_n = n!}$$

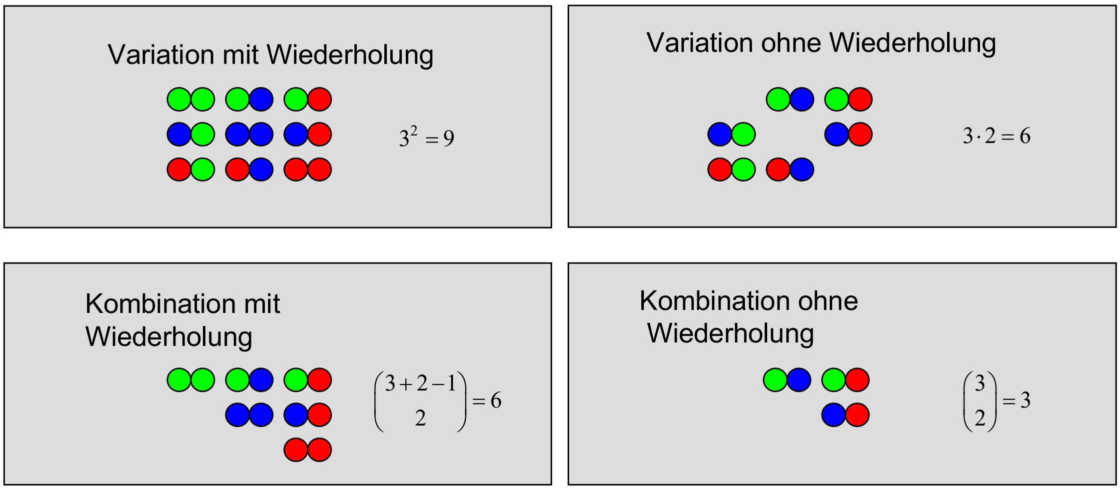
Permutation
(Objekte nicht verschieden:
r Gruppen mit $n_1 + \ldots + n_r = n$)

$$\boxed{P_{n_1, n_2, \ldots, n_r} = \frac{n!}{n_1! \cdot n_2! \cdot \ldots \cdot n_r!}}$$

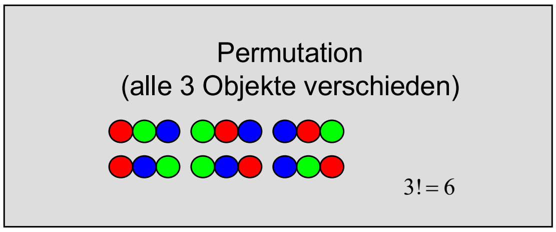
Beispiel:

In einer Urne befinden sich eine grüne, eine blaue und eine rote Kugel.

(a) In der nachfolgenden Abbildung sind die verschiedenen Möglichkeiten bei zweimaligem Ziehen (k=2) aus den 3 Kugeln (n=3) dargestellt.



(b) In der nachfolgenden Abbildungen sind die möglichen Anordnungen dieser 3 verschieden farbigen Kugeln dargestellt.



Ausblick: Wahrscheinlichkeiten

Die Wahrscheinlichkeitsrechnung beschäftigt sich mit den Gesetzmäßigkeiten vom zufälligen Eintreten bestimmter Ereignisse aus einer vorgegebenen Ereignismenge und findet Anwendung in vielen Bereichen der Naturwissenschaft, der Technik und der Ökonomie.

Definition 1.25: Wahrscheinlichkeit eines Ereignisses

Die Wahrscheinlichkeit für ein bestimmtes Ereignis ist definiert als

$$p = \frac{Anzahl\ der\ "günstigen"\ Fälle}{Anzahl\ der\ "möglichen"\ Fälle} = \frac{A_g}{A_m}.$$

Beispiel:

Die Wahrscheinlichkeit beim Lotto 6 aus 49 genau 6 Richtige zu erzielen ist:

$$p = \frac{A_g}{A_m} = \frac{1}{\binom{49}{6}} = \frac{1}{13.983.816} = 0.00000007$$