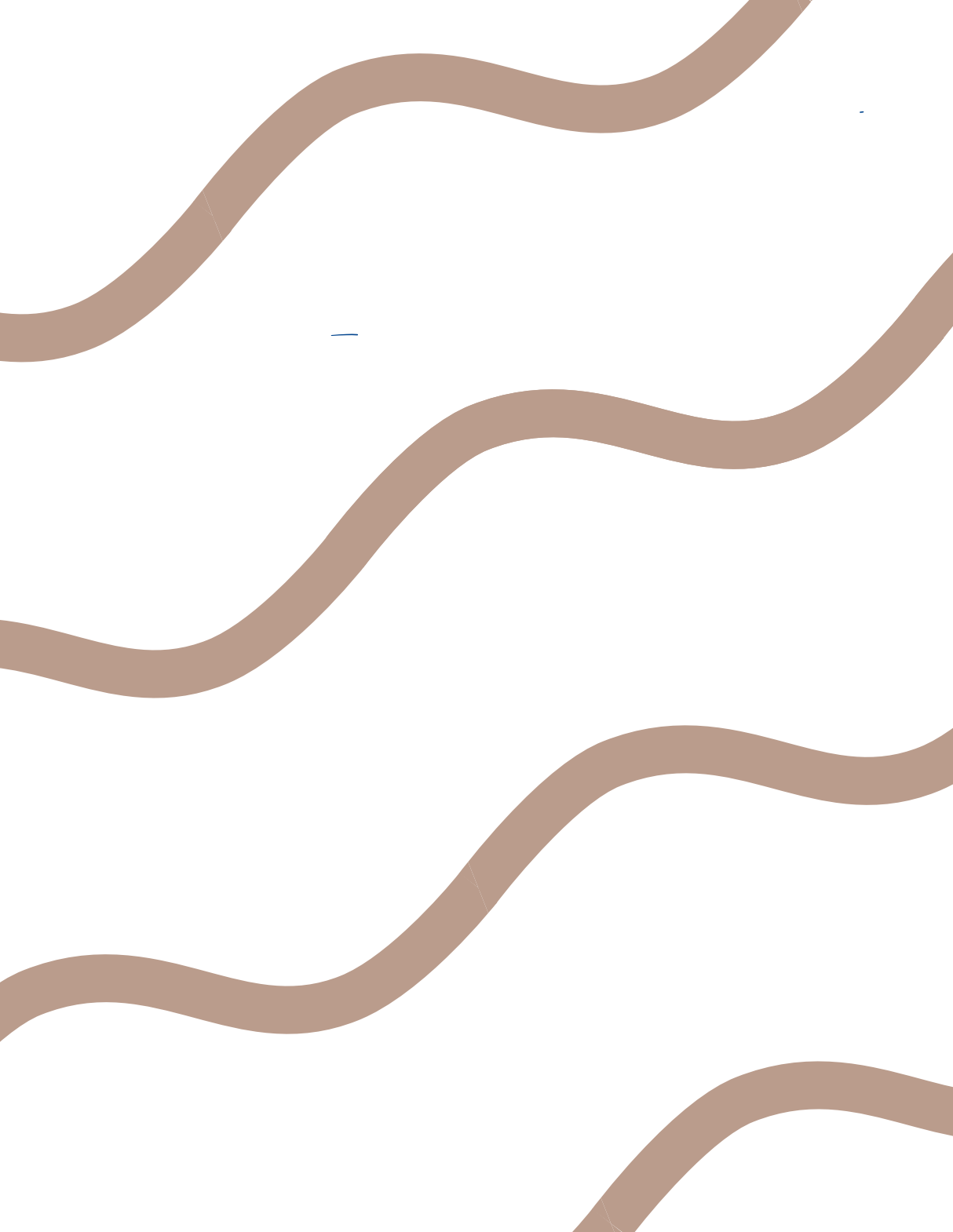




SYMBOLE

$\Rightarrow$	daraus folgt	Beispiel: n ist durch 4 teilbar $\Rightarrow n$ ist durch 2 teilbar			
$\Leftrightarrow$	genau dann, wenn	Beispiel: n ist eine gerade Zahl $\Leftrightarrow n$ ist durch 2 teilbar			
$\approx$	ungefähr gleich	Beispiel: $\frac{1}{3} \approx 0.33$	$\mathbb{R}^2$	<u>zweidimensionaler Raum</u>	Mathematische Formalisierung der Zeichenebene als $\mathbb{R} \times \mathbb{R}$. Ausgesprochen: "R zwei".
$\neq$	ungleich	Beispiel: $2 \neq 1$	$\mathbb{R}^3$	dreidimensionaler Raum	Formalisierung des dreidimensionalen Raumes als $\mathbb{R} \times \mathbb{R} \times \mathbb{R}$. Verallgemeinerung: $\mathbb{R}^n$ ($n = 4, 5, \dots$).
$<$	<u>kleiner</u>	Beispiel: $1 < 2$	$\vec{a}$	<u>Vektor</u>	Vektoren werden fett dargestellt. Beispiel: $\vec{a} = (3, 4)$.
$>$	<u>größer</u>	Beispiel: $2 > 1$	$ \dots $	<u>Betrag eines Vektors</u>	Beispiel: $ (3, 4) = 5$.
$\leq$	<u>kleiner-gleich</u>	Beispiel: $-x^2 \leq 0$ für jede reelle Zahl x	$\parallel$	parallel	Schreibweise: $\vec{a} \parallel \vec{b}$
$\geq$	<u>größer-gleich</u>	Beispiel: $x^2 \geq 0$ für jede reelle Zahl x	$\perp$	normal (orthogonal)	Schreibweise: $\vec{a} \perp \vec{b}$
$=$	<u>identisch</u>	Beispiel: $a \times a = a^2$	Δ	<u>Dreieck</u>	Schreibweise für das Dreieck mit Eckpunkten A, B und C : ΔABC . <i>Achtung:</i> Verwechslungsgefahr mit "Änderung" (s.u.)
$\pm$	<u>plus-minus</u>	Beispiel: Aus $x^2 = 4$ folgt $x = \pm 2$ (d.h. $x = -2$ oder $x = 2$)	$\sphericalangle$	<u>Winkel</u>	Schreibweise: $\sphericalangle CAB$ (für den Winkel mit Scheitel A).
$\{\dots\}$	<u>Menge</u>	Beispiel: $A = \{1, 4, 9, 16, 25\}$	$f(x)$	<u>Zuordnungsvorschrift für Funktionen</u>	Beispiel: Durch $f(x) = x^3$ ist eine Funktion $f: \mathbb{R} \rightarrow \mathbb{R}$ definiert.
$\mathbb{N}$ oder $\mathbb{N}_0$	<u>Menge der natürlichen Zahlen</u>	$\mathbb{N} = \{1, 2, 3, \dots\}$ <i>Achtung:</i> Manchmal wird die Null zur Menge $\mathbb{N}$ hinzugenommen.	$\circ$	<u>Verkettung von Funktionen</u>	$(f \circ g)(x) = f(g(x))$
$\mathbb{Z}$ oder $\mathbb{Z}_n$	<u>Menge der ganzen Zahlen</u>	$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$	$\rightarrow$	<u>Zuordnungsvorschrift für Funktionen</u>	Beispiel: Durch $f: x \rightarrow x^2$ ist eine Funktion $f: \mathbb{R} \rightarrow \mathbb{R}$ definiert.
$\mathbb{Q}$ oder $\mathbb{Q}_n$	<u>Menge der rationalen Zahlen</u>	Menge aller Bruchzahlen $\frac{m}{n}$ (wobei m, n ganzzahlig und $n \neq 0$)	$\rightarrow$	<u>asymptotisches Verhalten: "gegen"</u>	Beispiel: x^2 wächst für $x \rightarrow \infty$ ("x gegen Unendlich") über jede Schranke.
$\mathbb{R}$ oder $\mathbb{R}_n$	<u>Menge der reellen Zahlen</u>	Menge aller Zahlen mit Dezimaldarstellung	e	<u>Eulersche Zahl</u>	$e = 2.7182818284590452353602874713526 \dots \approx 2.718$
$\mathbb{C}$ oder $\mathbb{C}_n$	<u>Menge der komplexen Zahlen</u>	Menge aller $x + iy$ mit $x, y \in \mathbb{R}$	$ $	<u>bedingte Wahrscheinlichkeit</u>	Schreibweise: $p(A B)$
(a, b)	<u>offenes Intervall</u>	<i>Achtung:</i> Verwechslungsgefahr mit "geordnetes Paar" (s.u.)	$< \dots >$	<u>Erwartungswert</u>	Beispiel: $\langle a \rangle$ für den Erwartungswert der Zufallsvariable a . Eine andere Schreibweise dafür ist $E(a)$.
$[a, b]$	<u>abgeschlossenes Intervall</u>	$[a, b)$ und $(a, b]$ bezeichnen halboffene Intervalle.	μ	<u>Erwartungswert</u>	Öbliche Bezeichnung für den Erwartungswert einer Zufallsvariable.
∞	unendlich		σ^2	<u>Varianz</u>	Öbliche Bezeichnung für die Varianz einer Zufallsvariable.
$ \dots $	<u>Absolutbetrag</u>	Beispiele: $ 5 = 5, -6 = 6$	σ	<u>Standardabweichung</u>	Öbliche Bezeichnung für die Standardabweichung einer Zufallsvariable.
$\sqrt{\quad}$	<u>(Quadrat-)Wurzel</u>	Wird der Einfachheit halber oft auch als $\sqrt{\quad}$ geschrieben. Für (nicht-negative) reelle Zahlen ist sie immer ≥ 0 (z.B. $\sqrt{4} = 2$).	$'$	<u>Ableitung</u>	Beispiel: $(x^2)' = 2x$
π	Kreiszahl (Pi)	$\pi = 3.1415926535897932384626433832795 \dots \approx 3.14$	$''$	<u>Zweite Ableitung</u>	Beispiel: $(x^3)'' = 6x$
$\in$	<u>ist Element von</u>	Beispiel: $5 \in \mathbb{N}$	Δ	<u>Differenz, Änderung</u>	Differenzenquotient: $\Delta f / \Delta x$ <i>Achtung:</i> Verwechslungsgefahr mit "Dreieck" (s.o.)
$\notin$	<u>ist kein Element von</u>	Beispiel: $\frac{1}{2} \notin \mathbb{N}$	d	<u>Differential</u>	Ableitung ("Differentialquotient"): df/dx . Dies wird ausgesprochen als "df nach dx".
$\forall$	<u>für alle (für jedes)</u>	Beispiel: $x \cdot y = y \cdot x \quad \forall x, y \in \mathbb{R}$	d/dx	<u>Differenzieren</u>	Beispiel: $d(x^2)/dx = 2x$. Ausgesprochen: "d nach dx von ...".
$\exists$	<u>es existiert ein</u>	Beispiel: $\exists a \in \mathbb{R}$, sodaß gilt: $a^2 = 2$	d^2/dx^2	<u>Zweimal differenzieren</u>	Beispiel: $d^2(\sin x)/dx^2 = -\sin x$. Ausgesprochen: "d zwei nach dx-Quadrat von ...".
$ $	<u>für die gilt</u>	$\{x \mid \dots\}$ = Menge aller x , für die gilt $\dots$	$ $	<u>an der Stelle</u>	Beispiel: $(x^2)' _{x=5} = 10$
$\cap$	<u>Durchschnittsmenge</u>	$A \cap B = \{x \mid x \in A \text{ und } x \in B\}$	$\int \dots dx$	<u>unbestimmtes Integral</u>	Beispiel: $\int x^2 dx = x^3/3$
$\cup$	<u>Vereinigungsmenge</u>	$A \cup B = \{x \mid x \in A \text{ oder } x \in B\}$	$\int_a^b \dots dx$	<u>bestimmtes Integral</u>	Beispiel: $\int_0^3 x^2 dx = 9$
$\subseteq$	<u>ist Teilmenge von</u>	Beispiel: $\mathbb{N} \subseteq \mathbb{Z}$	$ $	<u>Differenz an den Stellen</u>	Wird für das <u>bestimmte</u> Integral verwendet. Beispiel: $\int_1^2 3x^2 dx = x^3 _1^2 = 2^3 - 1^3 = 7$
$\sup$	<u>ist Obermenge von</u>	Beispiel: $\mathbb{Z} \supseteq \mathbb{N}$			
$\setminus$	<u>Komplementärmenge</u>	$A \setminus B = \{x \in A \mid x \notin B\}$ Dafür sind auch die Schreibweisen $A \sim B$ und $A - B$ gebräuchlich.			
$^{\wedge}$	<u>hochstellen (Potenz)</u>	Beispiel: Schreibweise $x^{\wedge} 2$ anstelle von x^2			
$\wedge$	<u>logisches und</u>				
$\vee$	<u>logisches oder</u>				
$\neg$	<u>logisches nicht</u>				
$\{\}$	<u>leere Menge</u>	Dafür ist auch das Symbol $\emptyset$ gebräuchlich.			
$\cong$	<u>isomorph</u>	Kann im konkreten Fall verschiedene Bedeutungen haben, z.B., daß zwei Mengen "gleichmächtig" sind.			
(a, b)	<u>geordnetes Paar</u>	<i>Achtung:</i> Verwechslungsgefahr mit "offenes Intervall" (s.o.)			
$\times$	<u>kartesisches Produkt zweier Mengen</u>	$A \times B = \{(a, b) \mid a \in A, b \in B\}$. Ausgesprochen: "A kreuz B". Manchmal auch für die Multiplikation zweier Zahlen verwendet.			

Kapitel

1

Das interessanteste Axiom ist das **Induktionsaxiom 5**. Aus diesem leitet man das Beweisprinzip der **vollständigen Induktion** ab.

Es sei $P(n)$ eine **Eigenschaft**², die für eine **natürliche Zahl** n gelten **kann** oder **nicht** (siehe Beispiele 1.1 bis 1.3). Wir wollen untersuchen, ob $P(n)$ für **alle natürlichen Zahlen** wahr ist. Das Induktionsaxiom besagt, dass man dafür $P(0)$ überprüfen muss, also ob die natürliche Zahl 0 die Eigenschaft P hat, und dass man überprüfen muss, ob aus der Annahme, dass $P(n)$ gültig ist, auch die Gültigkeit von $P(n') = P(n+1)$ gefolgert werden kann.

$$\hookrightarrow P(0) \wedge (\forall n \in \mathbb{N} : P(n) \Rightarrow P(n+1)) \Rightarrow \forall n \in \mathbb{N} : (P(n))$$

Die Überprüfung von $P(0)$ wird auch als **Induktionsanfang** und der Schluss $P(n) \Rightarrow P(n+1)$ als **Induktionsschritt** bezeichnet, dabei nennt man $P(n)$ **Induktionsvoraussetzung** und $P(n+1)$ **Induktionsbehauptung**. △

Manchmal ist es auch günstiger, nicht nur den Schluss $P(n) \Rightarrow P(n+1)$ zu verwenden, sondern die **Information über alle vorigen** $P(k)$ zu nützen, d.h. man nimmt an, dass $P(0), P(1), \dots, P(n)$ gültig sind, und leitet daraus $P(n+1)$ ab. In der Schreibweise der Logik sieht diese Variante der vollständigen Induktion so aus:

$$P(0) \wedge (\forall n \in \mathbb{N} : (\forall k \leq n : P(k)) \Rightarrow P(n+1)) \implies \forall n \in \mathbb{N} : P(n).$$

Das Prinzip der Induktion ist auch Grundlage der so genannten **rekursiven Definition**. Man kann beispielsweise die Folge $a_n = 2^n$, $n \geq 0$, auch durch Angabe des ersten Elements $a_0 = 1$ und durch die rekursive Beziehung

$$a_{n+1} = 2a_n, \quad n \geq 0,$$

definieren. **Rekursive Definitionen** findet man in den verschiedensten Zusammenhängen. So werden z.B. die **Potenzen** x^n am einfachsten rekursiv definiert: $x^0 := 1$, $x^{n+1} := x^n x$ (für $n \geq 0$). Ein weiteres Beispiel sind die **Fibonacci-Zahlen** F_n , die üblicherweise durch $F_0 = 0$, $F_1 = 1$ und durch $F_{n+1} := F_n + F_{n-1}$ (für $n \geq 1$) definiert werden.

Das „Immerweiterzählen“ ist auch Grundlage des Rechnens mit natürlichen Zahlen. Die **Addition** von n mit 1 ist durch den **Nachfolger** von n gegeben: $n+1 = n'$. Entsprechend ist die Addition von n und 2 (dem Nachfolger von 1): $n+2 = n+1' = (n+1)'$. Allgemein definiert man in **rekursiver Weise**

$$n+k' = (n+k)'$$

Aus dem Induktionsaxiom folgt, dass damit die Addition von zwei beliebigen natürlichen Zahlen definiert wird, wenn man zusätzlich noch $n+0 = 0+n = n$ setzt.

Die **Multiplikation** zweier natürlicher Zahlen wird ebenso **rekursiv** definiert: $0 \cdot n = 0$, $1 \cdot n = n$, $2 \cdot n = n + n$ und allgemein

$$k' \cdot n = k \cdot n + n.$$

Satz 1.4 Für natürliche Zahlen $n, m, k \in \mathbb{N}$ gelten die folgenden Eigenschaften:

- (i) **Kommutativgesetz:** $n + m = m + n$, $n \cdot m = m \cdot n$,
- (ii) **Assoziativgesetz:** $(n + m) + k = n + (m + k)$, $(n \cdot m) \cdot k = n \cdot (m \cdot k)$,
- (iii) **Distributivgesetz:** $(n + m) \cdot k = n \cdot k + m \cdot k$,
- (iv) **Existenz eines neutralen Elements:** $n + 0 = 0 + n = n$, $n \cdot 1 = 1 \cdot n = n$.

Neben der Addition und der Multiplikation betrachtet man in den natürlichen Zahlen auch die **Subtraktion** und die **Division**. Ist $n \leq m$, so bezeichnet $k = m - n$ die **Differenz**, also jene natürliche Zahl mit $n + k = m$. Gibt es zu zwei natürlichen Zahlen m, n (mit $n \neq 0$) eine natürliche Zahl q mit $n \cdot q = m$, so sagt man, „ n teilt m “ und bezeichnet q als **Quotienten**, der durch $q = m : n = \frac{m}{n}$ geschrieben wird. Man überlegt sich leicht, dass Differenz und Quotient eindeutig bestimmt sind.

Blieben wir zunächst bei den **ganzen Zahlen $\mathbb{Z}$** . Sie wurden so konstruiert, dass man zu jeder natürlichen Zahl $n > 0$ auch die **negative Zahl $-n$** betrachtet. Damit kann man (ausgehend von 0) auch um **-1 immer weiterzählen** und erhält auch eine Fortsetzung der Ordnung der natürlichen Zahlen (siehe Abb. 1.2).

Im nächsten Schritt definiert man die **Addition** für alle ganzen Zahlen:

$$\begin{aligned} (-m) + (-n) &= -(m + n) && \text{für } m, n \geq 0, \\ m + (-n) &= (-n) + m = m - n && \text{für } 0 \leq n \leq m, \\ m + (-n) &= (-n) + m = -(n - m) && \text{für } 0 \leq m < n. \end{aligned}$$

Weiters wird der Begriff negative Zahl auch für alle ganzen Zahlen definiert, insbesondere setzt man **$-0 = 0$** und

$$-(-n) = n \quad \text{für } n > 0,$$

also z.B. **$-(-3) = 3$** . Jede ganze Zahl hat daher eine negative Zahl.

Mit dieser Festlegung wird die **Subtraktion**

$$n - m = n + (-m)$$

Eine ähnliche Idee liegt der Konstruktion der **rationalen Zahlen $\mathbb{Q}$** zu Grunde. Hier spielt der **Kehrwert $\frac{1}{r} = r^{-1}$** eine ähnliche Rolle wie zuvor die negative Zahl $-n$. Wieder ist es wichtig, den Kehrwert $r^{-1} = \frac{1}{r}$ jeder rationalen Zahl $r = \frac{m}{n} \neq 0$ zu kennen:

$$\left(\frac{m}{n}\right)^{-1} = \frac{1}{\frac{m}{n}} = \frac{n}{m}$$

Beispielsweise ist **$\left(\frac{1}{2}\right)^{-1} = 2$** . Damit ist (zunächst) für alle ganzen Zahlen m, n (mit $n \neq 0$) die Lösung von $n \cdot y = m$ durch $y = \frac{m}{n}$ gegeben. Neben dem Kehrwert einer rationalen Zahl definiert man auch die **negative Zahl $-r$** einer rationalen Zahl $r = \frac{m}{n}$:

$$-r = -\frac{m}{n} = \frac{-m}{n}$$

Schließlich führen wir die **Addition** und **Multiplikation** von zwei rationalen Zahlen $r = \frac{m}{n}$ und $s = \frac{k}{l}$ ein:

$$r + s = \frac{m}{n} + \frac{k}{l} = \frac{ml + nk}{nl} \quad \text{und} \quad r \cdot s = \frac{m}{n} \cdot \frac{k}{l} = \frac{m \cdot k}{n \cdot l}$$

Entsprechend definieren wir für zwei beliebige rationale Zahlen $r = \frac{m}{n}$, $s = \frac{k}{l}$ die **Subtraktion** und **Division**:

$$r - s = r + (-s) \quad \text{und} \quad r : s = \frac{r}{s} = r \cdot \frac{1}{s} \quad (s \neq 0).$$

Damit können wir die Gleichungen $s + x = r$ und $s \cdot y = r$ für alle rationalen Zahlen r, s lösen:

$$x = r - s \quad \text{und} \quad y = \frac{r}{s} \quad (s \neq 0).$$

In den **ganzen Zahlen** kann man daher **uneingeschränkt addieren, multiplizieren und subtrahieren**. In den **rationalen Zahlen** kommt noch die **uneingeschränkte Division** durch eine Zahl $\neq 0$ dazu. Man beachte, dass die Rechenregeln von Satz 1.4 in derselben Weise für $\mathbb{Z}$ und $\mathbb{Q}$ gelten. Zusätzlich kommt noch hinzu, dass wir **negative und reziproke Zahlen** bilden können.

↪ wechselseitig

Wie bereits angegeben, sind die **ganzen Zahlen geordnet**. Ebenso können die rationalen Zahlen geordnet werden. Dies wird an der so genannten **Zahlengeraden** verdeutlicht (siehe Abb. 1.3):

Für zwei rationale Zahlen $r = \frac{m}{n}$, $s = \frac{k}{l}$ (mit $n > 0$ und $l > 0$) definiert man

$$r = \frac{m}{n} < s = \frac{k}{l} \iff m \cdot l < n \cdot k.$$

Weiters beachte man, dass es zwischen je zwei rationalen Zahlen $r < s$ immer noch eine **rationale Zahl** gibt, die zwischen r und s liegt:

$$r < \frac{r+s}{2} < s.$$

Es sieht daher so aus, als ob die **rationalen Zahlen auf der Zahlengeraden keine Lücken haben**. Dies ist aber (bei genauerer Betrachtungsweise) **falsch**. Wir versuchen nun, die Gleichung

$$x^2 = 2$$

zu lösen. Dies ist jedoch überraschenderweise im Rahmen der rationalen Zahlen nicht möglich. Eine Lösung der Gleichung $x^2 = 2$ wird durch $x = \sqrt{2}$, die **Wurzel** von 2 bezeichnet. Eine Zahl, die **nicht rational** ist, heißt **irrational**.

Satz 1.5 Die Gleichung $x^2 = 2$ hat **keine Lösung in den rationalen Zahlen**, d.h. $\sqrt{2}$ ist **irrational**.

Beweis. Wir benutzen eine indirekte Vorgangsweise, den sogenannten **indirekten Beweis**. Wir nehmen an, es gäbe eine **rationale Lösung** $x = \frac{m}{n}$ und führen diese Annahme zu einem Widerspruch. Daraus folgt, dass es unmöglich ist, dass $x^2 = 2$ eine rationale Lösung hat.

Es sei also $x = \frac{m}{n}$ eine rationale Lösung der Gleichung $x^2 = 2$, also $\left(\frac{m}{n}\right)^2 = 2$ oder $m^2 = 2n^2$. Wir können dabei auch o.B.d.A.⁵ annehmen, dass m und n nicht beide gerade sind.⁶ Denn wären m und n gerade, so könnte man wegen $x = \frac{m}{n} = \frac{m/2}{n/2}$ anstelle von m und n auch $m/2$ und $n/2$ betrachten und auf diesem Weg erzwingen, dass nach endlich vielen Schritten (eventuell neue) m und n nicht beide gerade sind.

Aus der Beziehung $m^2 = 2n^2$ folgt aber, dass m gerade ist. Denn wäre m ungerade, so müsste auch m^2 ungerade sein, was der Beziehung $m^2 = 2n^2$ widerspricht. Wir können daher $m = 2k$ setzen und erhalten $(2k)^2 = 4k^2 = 2n^2$ und schließlich $2k^2 = n^2$. Aus dieser

Gleichung folgt auch, dass n gerade sein muss.

Reelle Zahlen:

Üblicherweise werden natürliche Zahlen in ihrer **Dezimalentwicklung** angegeben, also z.B.

$$327 = (327)_{10} = 3 \cdot 10^2 + 2 \cdot 10^1 + 7 \cdot 10^0.$$

Es ist leicht zu sehen, dass jede natürliche Zahl n eindeutig in dieser Weise dargestellt werden kann als

$$n = c_k \cdot 10^k + c_{k-1} \cdot 10^{k-1} + \dots + c_1 \cdot 10^1 + c_0 \cdot 10^0 = (c_k c_{k-1} \dots c_1 c_0)_{10},$$

wobei die **Ziffern** $c_j \in \{0, 1, 2, \dots, 9\}$ sind. Bei **negativen Zahlen** setzt man einfach ein **Minuszeichen** davor, z.B. -327 .

Es ist aber nicht

möglich, alle rationalen Zahlen in der Form

$$r = c_k \cdot 10^k + c_{k-1} \cdot 10^{k-1} + \dots + c_1 \cdot 10^1 + c_0 \cdot 10^0 + c_{-1} \cdot 10^{-1} + \dots + c_{-m} \cdot 10^{-m} \\ = (c_k c_{k-1} \dots c_1 c_0 . c_{-1} \dots c_{-m})_{10},$$

also durch eine **endliche Dezimalentwicklung** darzustellen. Die Ziffern $c_{-1}, c_{-2}, \dots, c_{-m}$ werden auch als **Nachkommastellen** bezeichnet.

Man erfasst damit nur rationale Zahlen der Form $r = n/10^m$, wobei n und m natürliche Zahlen sind.

Desto genauer man die Zahlen bzw. Nachkommastellen betrachtet, desto präziser werden auch die Zahlen.
Man kann jedoch z.B. die Zahl $\sqrt{2}$ nicht in endlich vielen Schritten darstellen, weil $\sqrt{2} \notin \mathbb{Q} \Rightarrow$ irrational... eher unendliche Dezimalentwicklung.

In analoger Weise betrachtet man beliebige **unendliche Dezimalentwicklungen**

$$x = c_k \cdot 10^k + c_{k-1} \cdot 10^{k-1} + \dots + c_1 \cdot 10^1 + c_0 \cdot 10^0 + \sum_{m=1}^{\infty} c_{-m} \cdot 10^{-m}$$

mit (beliebigen) Ziffern $c_j \in \{0, 1, 2, \dots, 9\}$. Zu so einer unendlichen Dezimalentwicklung gehört immer eine so genannte **Intervallschachtelung** von Intervallen⁸ $I_m = [x'_m, x''_m]$, indem man die **unendliche Dezimalentwicklung** nach m Schritten abbricht.

Intervallschachtelungsverfahren kann **nicht nur für irrationale Zahlen** (wie $\sqrt{2}$) **sondern auch für rationale Zahlen** durchgeführt werden. Für $x = \frac{1}{3}$ oder $x = 5/11$ stellt sich beispielsweise heraus, dass diese Zahlen die unendliche Dezimalentwicklung

$$\frac{1}{3} = 0.333 \dots \quad \text{bzw.} \quad \frac{5}{11} = 0.454545 \dots$$

haben. Solche Entwicklungen werden **periodische Dezimalentwicklungen** genannt. Wenn die

Satz 1.6 Die **Dezimalentwicklung einer rationalen Zahl ist entweder endlich oder (schließlich) periodisch**. Sie ist **eindeutig**, wenn man die (schließlich) Periode $999 \dots$ **ausschließt**.

Beweis. Ist die **Dezimalentwicklung von x endlich**, so ist x offensichtlich eine **rationale Zahl**. Hat hingegen die Zahl x die (schließlich) periodische Dezimalentwicklung $x = (c_k c_{k-1} \dots c_1 c_0 . c_{-1} \dots c_{-m} p_1 \dots p_r p_1 \dots p_r \dots)_{10}$ mit Periode $p_1 \dots p_r$, so hat $10^r x - x = (c_k c_{k-1} \dots c_1 c_0 . c_{-1} \dots c_{-m} p_1 \dots p_r p_1 \dots p_r \dots)_{10}$ mit Periode $p_1 \dots p_r$, so hat $(10^r - 1)x$ eine **endliche Dezimalentwicklung**, also $(10^r - 1)x$ ist rational. Daher ist auch x rational.

Definition 1.7 Die Menge aller positiven und negativen, endlichen und unendlichen Dezimalentwicklungen – wobei Zahlen mit (schließlicher) Periode $999 \dots$ mit ihrer endlichen Dezimalentwicklung identifiziert werden – wird als die Menge $\mathbb{R}$ der **reellen Zahlen** bezeichnet.

Anschaulich gesprochen füllen die reellen Zahlen die Lücken auf der Zahlengeraden (siehe Abb. 1.3), die die rationalen Zahlen lassen. Aus der Dezimalentwicklung ergibt sich auch die natürliche Ordnung der reellen Zahlen (die sich auch graphisch auf der Zahlengeraden wieder spiegelt).

Jede reelle Zahl x kann auch eindeutig als Summe einer ganzen Zahl n und einer Zahl r mit $0 \leq r < 1$ dargestellt werden: $x = n + r$. Die ganze Zahl n wird durch $n = \lfloor x \rfloor = \max\{k \in \mathbb{Z} \mid k \leq x\}$ bestimmt und heißt **Ganzteil** von x , der verbleibende Rest $r = \{x\} = x - \lfloor x \rfloor$ **Bruchteil** von x . Weiters definieren wir den **Betrag** $|x|$ einer reellen Zahl als $|x| = \max\{x, -x\}$. Es ist also z.B. $|3| = 3$ und $|-5| = 5$.

Komplexe Zahlen:

Definition 1.8 Die Menge $\mathbb{C}$ der **komplexen Zahlen** besteht aus den formalen Summen der Form

$$z = a + ib \quad \text{mit } a, b \in \mathbb{R}.$$

Dabei heißt $a = \Re(z)$ auch **Realteil** und $b = \Im(z)$ **Imaginärteil** von z .

$i = \text{imaginäre Zahl}$

Beispielsweise ist $z = 3 + 2i$ eine komplexe Zahl mit Realteil $\Re(z) = 3$ und Imaginärteil $\Im(z) = 2$. Es erweist sich als günstig, komplexe Zahlen (in gewisser Analogie zur Zahlengeraden) in der Ebene, der so genannten **Gauß'schen Ebene** als **Zeiger** darzustellen (siehe Abb. 1.4). Dabei dienen Real- und Imaginärteil von $z = a + ib$ als **Koordinaten** der Spitze des Zeigers. Die Länge dieses Zeigers wird auch als **Betrag** $r = |z| = \sqrt{a^2 + b^2}$ von z und

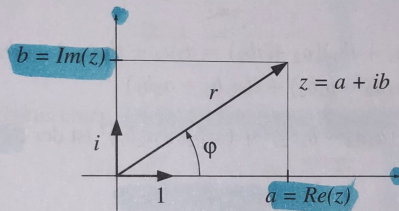


Abbildung 1.4 Die Gauß'sche Zahlenebene

der **Winkel** zur reellen Achse als **Argument** $\varphi = \arg(z)$ bezeichnet.⁹ Das Paar $[r, \varphi]$ bildet die **Polarkoordinaten** von z . Dabei ist das Argument nur bis auf ein ganzzahliges Vielfaches von 2π bestimmt, man sagt auch, es ist modulo 2π bestimmt. Mit Hilfe der Winkelfunktionen $\sin$ und $\cos$ gewinnt man einen direkten Zusammenhang zwischen der Darstellung einer komplexen Zahl $z = a + ib$ durch Real- und Imaginärteil und den Polarkoordinaten:

$$a = r \cos \varphi, \quad b = r \sin \varphi$$

bzw.¹⁰

$$r^2 = a^2 + b^2, \quad \tan \varphi = \frac{b}{a}$$

⁹Das Argument φ wird üblicherweise im **Bogenmaß** angegeben, d.h. der volle Winkel von 360° entspricht im Bogenmaß dem **Winkel** $\varphi = 2\pi$.

Addition von $\mathbb{C} \Rightarrow$ Realteil + Imaginärteil

$$\hookrightarrow z_1 = a_1 + ib_1 \text{ und } z_2 = a_2 + ib_2$$

$$\hookrightarrow z = z_1 + z_2 = (a_1 + a_2) + i(b_1 + b_2)$$

Zahlen. Weiters kann man uneingeschränkt subtrahieren, die negative Zahl $-z$ von $z = a + ib$ ist durch $-z = -a - ib$ gegeben. Weiters, und das ist bemerkenswert, kann man $-$ wie man wieder sofort nachrechnet – auch von jeder komplexen Zahl $z = a + ib \neq 0$ den Reziprokwert

$$\frac{1}{z} = \frac{a}{a^2 + b^2} - i \frac{b}{a^2 + b^2}$$

bilden, d.h. man kann in $\mathbb{C}$ uneingeschränkt durch Zahlen $\neq 0$ dividieren.

Der Reziprokwert kann mit Hilfe der **konjugiert komplexen Zahl** $\bar{z}$ von $z = a + ib$, die durch

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

definiert ist, noch einfacher angegeben werden:

$$\frac{1}{z} = \frac{\bar{z}}{z \cdot \bar{z}} = \frac{\bar{z}}{|z|^2}$$

Dabei haben wir bereits eine einfache Rechenregel für **konjugiert komplexe Zahlen** verwendet (nämlich $z \cdot \bar{z} = |z|^2$). Es gelten – wie man direkt sieht – noch weitere Rechenregeln:

$$\left. \begin{aligned} z_1 + z_2 &= \bar{z}_1 + \bar{z}_2, \\ z_1 \cdot z_2 &= \bar{z}_1 \cdot \bar{z}_2, \\ |z| &= \sqrt{z \cdot \bar{z}}, \\ \Re(z) &= \frac{z + \bar{z}}{2}, \\ \Im(z) &= \frac{z - \bar{z}}{2i}. \end{aligned} \right\}$$

Daraus gewinnt man übrigens einen **weiteren (einfachen) Beweis** für $|z_1 \cdot z_2| = |z_1| \cdot |z_2|$:

$$\left. \begin{aligned} |z_1 \cdot z_2|^2 &= z_1 \cdot z_2 \cdot \bar{z}_1 \cdot \bar{z}_2 \\ &= z_1 \cdot \bar{z}_1 \cdot z_2 \cdot \bar{z}_2 \\ &= |z_1|^2 \cdot |z_2|^2. \end{aligned} \right\}$$

Man beachte insbesondere, dass $z \cdot \bar{z} = |z|^2$ immer eine **reelle Zahl ≥ 0** ist.

Die Division z_1/z_2 komplexer Zahlen kann nun so gesehen werden, dass der **Quotient** mit $\bar{z}_2$ erweitert wird, so dass der **Nenner $z_2 \cdot \bar{z}_2$** insgesamt reell wird:

$$\frac{z_1}{z_2} = \frac{z_1 \cdot \bar{z}_2}{z_2 \cdot \bar{z}_2} = \frac{1}{z_2 \cdot \bar{z}_2} \cdot (z_1 \cdot \bar{z}_2).$$

Weiters gilt (wie bei der Multiplikation)

$$\left| \frac{z_1}{z_2} \right| = \frac{|z_1|}{|z_2|} \quad \text{und} \quad \arg\left(\frac{z_1}{z_2}\right) = \arg(z_1) - \arg(z_2) \bmod 2\pi.$$

Satz 1.12 (Fundamentalsatz der Algebra) Es seien $a_0, a_1, \dots, a_n$ komplexe Zahlen mit $a_n \neq 0$. Dann gibt es zum **Polynom**

$$p(z) = a_n z^n + a_{n-1} z^{n-1} + \dots + a_1 z + a_0$$

komplexe Zahlen $z_1, \dots, z_n$ mit

$$a_n z^n + \dots + a_0 = a_n (z - z_1) \cdot (z - z_2) \cdot \dots \cdot (z - z_n),$$

d.h. $z_1, \dots, z_n$ sind **Nullstellen** des Polynoms $p(z)$, also **Lösungen der Gleichung $p(z) = 0$** . Sie sind (bis auf die Reihenfolge) **eindeutig bestimmt**.

Für Polynome **dritten und vierten** Grades gibt es ähnlich wie bei der quadratischen Gleichung Lösungsformeln für diese Nullstellen. Es kann aber gezeigt werden, dass es für $n \geq 5$ keine allgemeinen (algebraischen) Lösungsformeln gibt. Man ist daher auf Approximationsverfahren angewiesen.

Aussagenlogik:

→ Aussage kann nur w oder f sein. => Prinzip vom ausgeschlossenen Dritten. (=zweiwertige Aussagenlogik)

1. **Konjunktion:** Aus zwei Aussagen wird durch Einfügen des Wortes **und** eine neue Aussage gewonnen, die Konjunktion der beiden Aussagen. Z.B. ist

„Es ist Winter, und es ist kalt.“

die Konjunktion der beiden Aussagen

„Es ist Winter.“ sowie „Es ist kalt.“

Die Konjunktion zweier Aussagen erhält genau dann den **Aussagewert w**, wenn die **beiden ursprünglichen Aussagen den Wert w** haben. In allen anderen Fällen erhält die Konjunktion daher den **Wert f**.

2. **Disjunktion:** Aus zwei Aussagen wird durch Einfügen des Wortes **oder** eine neue Aussage gewonnen, die Disjunktion der beiden Aussagen. Z.B. ist

„Die Straße ist nass, oder es regnet.“

die Disjunktion der beiden Aussagen

„Die Straße ist nass.“ sowie „Es regnet.“

Die Disjunktion zweier Aussagen erhält genau dann den **Aussagewert w**, wenn **wenigstens eine** der ursprünglichen Aussagen den Wert w hat. (Nur wenn **beide Aussagen den Wert f** haben, hat auch die Disjunktion den Wert f.)

3. **Implikation:** Aus zwei Aussagen wird durch Einfügen der Worte **wenn – dann** (bzw. **aus – folgt** oder **impliziert**) eine neue Aussage gewonnen, die Implikation der beiden Aussagen. Z.B. ist

„Wenn es regnet, dann ist die Straße nass.“

die Implikation der beiden Aussagen

„Es regnet.“ sowie „Die Straße ist nass.“

Die Implikation zweier Aussagen hat genau dann den **Wert f**, wenn die **erste Aussage den Wert w**, aber die **zweite den Wert f** hat. Man beachte, dass bei der Implikation die Reihenfolge wesentlich ist. Weiters hat eine Implikation immer den **Wert w**, wenn die **erste Aussage den Wert f** hat, unabhängig davon, wie die zweite Aussage lautet („ex falso quodlibet“).

4. **Äquivalenz:** Aus zwei Aussagen wird durch Einfügen der Worte **genau dann – wenn** (bzw. **dann und nur dann – wenn** oder **äquivalent**) eine neue Aussage gewonnen, die Äquivalenz der beiden Aussagen. Z.B. ist

„Die Straße ist genau dann nass, wenn es regnet.“

die Äquivalenz der beiden Aussagen

„Die Straße ist nass.“ sowie „Es regnet.“

Die Äquivalenz zweier Aussagen hat genau dann den **Wert w**, wenn den **beiden ursprünglichen Aussagen dieselben Wahrheitswerte** zugeordnet sind.

5. **Negation:** Fügt man in einer Aussage (an geeigneter Stelle) das Wort **nicht** ein, so entsteht eine neue Aussage, die Negation der ursprünglichen Aussage. Z.B. ist

„Es ist nicht Winter.“

die Negation der Aussage

„Es ist Winter.“

2. Äquivalente Formeln

Zur Vereinfachung der Notation ist es günstig, Aussagen durch Symbole $p_1, p_2, \dots$ zu bezeichnen und anstelle von „und“ das Symbol $\wedge$, anstelle von „oder“ das Symbol $\vee$, anstelle von „wenn – dann“ das Symbol $\Rightarrow$, anstelle von „genau dann – wenn“ das Symbol $\Leftrightarrow$ und anstelle von „nicht“ das Symbol $\neg$ zu verwenden. Die Symbole $\wedge, \vee, \Rightarrow, \Leftrightarrow, \neg$ werden in diesem Zusammenhang als **Junktoren** bezeichnet. Ist z.B.

Die Operationssymbole $\wedge, \vee, \Rightarrow, \Leftrightarrow, \neg$ können sinnvollerweise auch auf die Wahrheitswerte w und f angewandt werden. Daraus ergeben sich die nachstehenden Operationstabellen:

$\wedge$	w	f	$\vee$	w	f	$\Rightarrow$	w	f	$\Leftrightarrow$	w	f	$\neg$	w	f
w	w	f	w	w	w	w	w	f	w	w	f	f	w	f
f	f	f	f	w	f	f	w	w	f	f	w	w	f	w

Allgemein versteht man unter einer **Formel** einen Ausdruck, der aus Aussagenvariablen $p_1, p_2, \dots$ (oder auch $a, b, c, \dots$) und Junktoren $\wedge, \vee, \Rightarrow, \Leftrightarrow, \neg$, entsprechend geklammert, gebildet werden kann. Zwei Formeln F_1, F_2 heißen, wie gesagt, **semantisch** (oder **mathematisch**) **äquivalent**, also $F_1 \Leftrightarrow F_2$, wenn sie für alle Wahrheitsbelegungen von $p_1, p_2, \dots$ immer denselben Wahrheitswert haben. Eine Formel heißt **gültig** oder **Tautologie**, wenn sie für jede Belegung wahr ist, sie heißt **unerfüllbar** oder **Kontradiktion**, wenn sie für jede Belegung falsch ist, und sie heißt **erfüllbar**, wenn sie für mindestens eine Belegung wahr ist.

Im Folgenden werden einige dieser semantischen Äquivalenzen, die man auch als **logische Regeln** bezeichnen kann, angegeben:

- | | |
|--|---|
| (i) $a \wedge b \Leftrightarrow b \wedge a,$ | $a \vee b \Leftrightarrow b \vee a,$ |
| (ii) $a \wedge (b \wedge c) \Leftrightarrow (a \wedge b) \wedge c,$ | $a \vee (b \vee c) \Leftrightarrow (a \vee b) \vee c,$ |
| (iii) $a \wedge (a \vee b) \Leftrightarrow a,$ | $a \vee (a \wedge b) \Leftrightarrow a,$ |
| (iv) $a \wedge (b \vee c) \Leftrightarrow (a \wedge b) \vee (a \wedge c),$ | $a \vee (b \wedge c) \Leftrightarrow (a \vee b) \wedge (a \vee c),$ |
| (v) $\neg(a \wedge b) \Leftrightarrow \neg a \vee \neg b,$ | $\neg(a \vee b) \Leftrightarrow \neg a \wedge \neg b,$ |
| (vi) $a \wedge b \Leftrightarrow \neg(a \Rightarrow \neg b),$ | $a \vee b \Leftrightarrow \neg a \Rightarrow b,$ |
| (vii) $a \Leftrightarrow b \Leftrightarrow (a \Rightarrow b) \wedge (b \Rightarrow a)$
$\Leftrightarrow \neg((a \Rightarrow b) \Rightarrow \neg(b \Rightarrow a)),$ | |
| (viii) $a \Rightarrow b \Leftrightarrow \neg a \vee b,$ | $a \Leftrightarrow b \Leftrightarrow (a \wedge b) \vee (\neg a \wedge \neg b),$ |
| (ix) $a \Rightarrow b \Leftrightarrow \neg b \Rightarrow \neg a,$ | $\neg(a \Rightarrow b) \Leftrightarrow a \wedge \neg b.$ |

Besonders beachtenswert sind die Regeln (v) und (ix):

(v) wird **DeMorgan'sche Regel** genannt. Die Negation einer Disjunktion ist die Konjunktion der Negationen und umgekehrt (vergleiche auch mit dem einleitenden Beispiel).

(ix) ist die logische Grundlage des **indirekten Beweises**, der im Abschnitt 4. noch genauer besprochen wird.

Alle angegebenen Äquivalenzen (i)–(ix) können mit Hilfe geeigneter Wahrheitstabellen sofort bewiesen werden.

=> ... daraus folgt

... ist definiert

≡ ... identisch

! ... für die gilt

3. Prädikatenlogik

In vielen Anwendungsbereichen – und insbesondere in der Mathematik – haben so genannte **atomare** (d.h. unzerlegbare) **Aussagen** eine **Subjekt-Prädikat-Struktur**.

Allgemein bezeichnet man $P(x)$ als **Prädikat** (oder **Aussageform**) in der **Gegenstandsvariablen** x , wenn durch konkretes Einsetzen für x eine Aussage entsteht, der also ein Wahrheitswert zugeordnet werden kann. Beispielsweise entstehen aus $P(x) = „x \text{ ist groß}.“$ durch Einsetzen die Aussagen $P(\text{Alexander}) = „\text{Alexander ist groß}.“$ und $P(\text{Haus}) = „\text{Das Haus ist groß}.“$

Neben (einstelligen) Prädikaten $P(x)$ betrachtet man auch **mehrstellige Prädikate** der Form $Q(x_1, x_2, \dots, x_n)$. Beispielsweise ist

$$Q(x, y) = „x \text{ ist größer als } y.“$$

den. Viele (mathematische) Aussagen beginnen z.B. mit:

„Für alle ... gilt ...“ oder „Es gibt ein ..., so dass ...“

Ein wenig präziser (mit Hilfe eines Prädikats $P(x)$) dargestellt, sieht das so aus:

„Für alle x gilt $P(x)$.“ oder „Es gibt ein x , so dass $P(x)$.“

Vor dem Prädikat $P(x)$ steht ein so genannter **Quantor**, ein **Allquantor**, den wir mit „ $\forall$ “ abkürzen, oder ein **Existenzquantor**, den wir mit „ $\exists$ “ bezeichnen. Wir schreiben daher

$\forall x P(x)$ für alle

für die Aussage, dass alle möglichen x die Eigenschaft P haben, und

$\exists x P(x)$ Es existiert

dafür, dass es wenigstens ein x gibt, das die Eigenschaft P hat.

Der Wahrheitswert der Aussage $\forall x P(x)$ ist genau dann **w**, wenn die Aussage $P(x)$ für alle möglichen (eingesetzten) x den Wert **w** hat, entsprechend hat die Aussage $\exists x P(x)$ genau dann den Wert **w**, wenn es wenigstens ein x gibt, für das $P(x)$ den Wert **w** hat.

Selbstverständlich kann man Prädikate mit Junktoren untereinander bzw. mit gewöhnlichen Aussagen verbinden und, solange noch **freie Gegenstandsvariable** vorhanden sind, Quantoren anwenden. Führt man dies mit Aussagensymbolen $(p_1, p_2, \dots)$ und Prädikatsymbolen $(P_1, P_2, \dots)$ durch, so erhält man wieder eine **Formel**. Beispielsweise ist

$$\forall x_1 ((P_1(x_1) \wedge p_1) \Rightarrow (\exists x_2 (P_2(x_2) \wedge p_2) \Rightarrow P_3(x_1, x_2)))$$

In ähnlicher Weise wie in der Aussagenlogik gibt es auch in der Prädikatenlogik (semantische) Äquivalenzen, von denen wir einige auflisten:

- (x) $\forall x \forall y P(x, y) \iff \forall y \forall x P(x, y)$, $\exists x \exists y P(x, y) \iff \exists y \exists x P(x, y)$,
- (xi) $a \wedge \forall x P(x) \iff \forall x (a \wedge P(x))$, $a \vee \exists x P(x) \iff \exists x (a \vee P(x))$,
- (xii) $a \wedge \exists x P(x) \iff \exists x (a \wedge P(x))$, $a \vee \forall x P(x) \iff \forall x (a \vee P(x))$,
- (xiii) $\neg (\forall x P(x)) \iff \exists x \neg P(x)$, $\neg (\exists x P(x)) \iff \forall x \neg P(x)$.

Während die Äquivalenz zweier Formeln der Aussagenlogik mit Hilfe von Wahrheitstafeln stets in endlich vielen Schritten entschieden werden kann, gibt es in der Prädikatenlogik i. Allg. kein endliches Verfahren, um die Äquivalenz zweier Formeln zu überprüfen.

Bei mathematischen Aussagen verwendet man auch **Quantoren**, um über Elemente einer Menge eine Aussage zu treffen. So schreibt man

$$\forall x \in E : P(x)$$

dafür, dass alle Elemente $x \in E$ die Eigenschaft P haben. Man kann dies auch als Kurzschreibweise für $\forall x ((x \in E) \Rightarrow P(x))$ sehen. Entsprechend ist

$$\exists x \in E : P(x)$$

eine Kurzschreibweise für $\exists x ((x \in E) \wedge P(x))$.

4. Elementare Beweistechniken

Ein wesentliches Kennzeichen der Mathematik ist, dass alle Aussagen (bzw. mathematischen Sätze) **bewiesen** werden müssen. Ein mathematischer Satz hat üblicherweise eine **Implikationsstruktur** $a \Rightarrow b$, wobei a die **Voraussetzungen** in eine Aussage zusammenfasst und b die **eigentliche Aussage** des Satzes ist. Einfache Beispiele sind:

Wenn x eine gerade ganze Zahl ist, dann ist x^2 auch eine gerade ganze Zahl.

oder

Wenn für reelle Zahlen x, y die Beziehung $x^2 \neq y^2$ gilt, dann gilt auch $x \neq y$.

Ein Beweis ist nun eine **Kette von Schlussfolgerungen** (die natürlich alle logischen Regeln folgen müssen), aus denen dann schließlich der Satz folgt.

Ein **direkter Beweis** lässt die Aussagen a, b der Implikation $a \Rightarrow b$ unverändert, d.h. man geht von a aus und schließt daraus b . Beispielsweise betrachten wir die erste obige Aussage:

Beweis. Ist x eine gerade (ganze) Zahl, dann kann x in der Form $x = 2 \cdot y$ geschrieben werden, wobei y wieder eine ganze Zahl ist. Es folgt dann $x^2 = (2y)^2 = 4y^2 = 2(2y^2)$. Da y eine ganze Zahl ist, ist auch $y' = 2y^2$ eine ganze Zahl und folglich ist wegen der Darstellung $x^2 = 2y'$ die Zahl x^2 eine gerade Zahl. $\square$

Im Unterschied zum direkten Beweis geht der **indirekte Beweis** nicht von der Struktur $a \Rightarrow b$ aus, sondern ersetzt sie durch die so genannte **Kontraposition** $\neg b \Rightarrow \neg a$, die zur **ursprünglichen Implikation** $a \Rightarrow b$ äquivalent ist. Im indirekten Beweis wird die Kontraposition $\neg b \Rightarrow \neg a$ bewiesen, woraus aber auch der ursprüngliche Satz $a \Rightarrow b$ folgt. Beispielsweise ist die Kontraposition des zweiten obigen Beispiels:

Wenn für reelle Zahlen x, y die Beziehung $x = y$ gilt, dann gilt auch $x^2 = y^2$.

Der Beweis dieser Implikation ist evident. Also ist damit auch der ursprüngliche Satz bewiesen.

In vielen Fällen, wird ein indirekter Beweis nicht so geführt, dass die Kontraposition explizit angegeben wird. Man *nimmt an*, dass b nicht gilt (also dass $\neg b$ gilt) und zeigt, dass $\neg b$ mit a im **Widerspruch** steht, also mit a nicht vereinbar ist. Das heißt natürlich nichts anderes, als dass $\neg a$ bewiesen wird. In diesem Beispiel könnte das etwa so lauten:

Beweis. Angenommen es wäre $x = y$, dann folgt daraus $x^2 = y^2$, was mit $x^2 \neq y^2$ im Widerspruch steht. Also ist $x \neq y$. $\square$

Neben mathematischen Sätzen mit einer Implikationsstruktur $a \Rightarrow b$ gibt es auch Sätze, die eine **Äquivalenz** $a \Leftrightarrow b$ ausdrücken. In diesem Fall muss also neben $a \Rightarrow b$ auch $b \Rightarrow a$ gelten. Beispielsweise können wir die Frage stellen, ob das zweite obere Beispiel in diesem Sinn erweiterbar ist, ob der Satz

Für reelle Zahlen x, y gilt $x^2 \neq y^2$ genau dann, wenn $x \neq y$ gilt.

richtig ist? Das kann man relativ einfach mit einem so genannten **Gegenbeispiel** beantworten. Es gilt $(-2)^2 = 2^2$, aber $-2 \neq 2$. Anders ausgedrückt, die Implikation $b \Rightarrow a$ ist nicht richtig. Man beachte, dass hier nur ein einziges Beispiel ausreichend war, die Implikation zu falsifizieren, während es nicht ausreichend ist, für den Nachweis der (richtigen) Implikation $a \Rightarrow b$ eines (oder mehrere) Beispiele anzugeben.

1.4. MENGEN

Definition 1.38 (Cantor) Eine **Menge** ist eine Zusammenfassung von wohl unterschiedenen Objekten unserer Anschauung oder unseres Denkens zu einem Ganzen.

Definition 1.40 Die Objekte x , die in einer Menge A zusammengefasst werden, bezeichnet man als **Elemente** der Menge A . Man sagt auch, dass x in A enthalten ist, und schreibt $x \in A$. Ist x in A nicht enthalten, so schreibt man dafür $x \notin A$. Die Menge $\emptyset$, die keine Elemente enthält, heißt **leere Menge**.

Eine Menge heißt **endlich**, wenn sie endlich viele Elemente enthält, andernfalls heißt sie **unendlich**. Für eine endliche Menge A bezeichnet man mit $|A|$ bzw. $\#A$ die **Anzahl** der Elemente von A .

Definition 1.41 Eine Menge A heißt **Teilmenge** einer Menge B , im Zeichen $A \subseteq B$, wenn jedes Element x aus A auch in B enthalten ist. Zwei Mengen A, B sind **gleich**, also $A = B$, wenn sie dieselben Elemente enthalten.

Satz 1.42 Zwei Mengen A, B sind genau dann **gleich**, wenn sowohl A **Teilmenge** von B als auch B **Teilmenge** von A ist, d.h.

$$A = B \iff A \subseteq B \wedge B \subseteq A.$$

Es gibt verschiedene Möglichkeiten, eine Menge anzugeben. Die einfachste Möglichkeit ist die **aufzählende Darstellung**, z.B. $A = \{1, 2, 3\}$, die sich aber nur für endliche (und gelegentlich für abzählbare) Mengen eignet. Die häufigste Form ist die **beschreibende Darstellung**

$$A = \{x \mid P(x)\},$$

wobei $P(x)$ ein Prädikat in der freien Variablen x ist. Die Menge A enthält nun jene x , für die $P(x)$ gilt. Beispielsweise ist $\{x \mid x \in \mathbb{Z} \wedge 1 \leq x \leq 3\}$ die Menge $\{1, 2, 3\}$. Verlangt man, dass die zu beschreibende Menge A **Teilmenge** einer Menge E sein soll, d.h. $P(x)$ hat die Form $x \in E \wedge Q(x)$, so wird anstelle $A = \{x \mid x \in E \wedge Q(x)\}$ einfach

$$A = \{x \in E \mid Q(x)\}$$

Die Definition einer Menge impliziert, dass ein Element x nur einmal in eine Menge A aufgenommen werden kann, x ist entweder in A enthalten oder nicht in A enthalten. Es ist aber oft sinnvoll, „verallgemeinerte Mengen“ zu betrachten, wo die Elemente mit einer gewissen Vielfachheit auftreten, z.B. $A = \{1, 1, 2, 2, 2, 3, 4, 4\}$. Solche Objekte werden als **Multimengen** bezeichnet.

Ein wichtiges Merkmal einer Menge ist, **wieviele Elemente sie enthält**. Es geht also um ihre Größe bzw. ihre **Kardinalität**. Für endliche Mengen ist dies begrifflich kein wirkliches Problem, anders ist es bei so genannten unendlichen Mengen.

Um dies präzise zu fassen, definiert man zunächst, wann zwei Mengen A und B **gleichmächtig** (oder gleich groß) sind: nämlich wenn es eine **bijektive** (also eins-zu-eins) **Zuordnung** zwischen den Elementen von A und B gibt. D.h. jedes Element aus A hat eine **Entsprechung** in B und umgekehrt.¹⁹ Beispielsweise sind die Mengen $\{0, 1, 2\}$ und $\{a, b, c\}$ gleichmächtig. Dasselbe gilt aber auch für die Mengen $\{0, 1, 2, 3, \dots\}$ und $\{0, 2, 4, 6, \dots\}$. Jede natürliche Zahl x aus der ersten Menge kann mit der geraden Zahl $2x$ aus der zweiten Menge verknüpft werden. Während das erste Beispiel unmittelbar klar ist, gibt das zweite zum Nachdenken Anlass.

Die zweite Menge ist doch ein echter Teil der ersten. Wie können sie dann gleich groß sein? Das Problem ist, dass diese Mengen unendlich sind und das führt auch zur Antwort.

Wie kann man aber zwischen endlich und unendlich präzise unterscheiden? Dazu stellt man zunächst fest (oder definiert es einfach), dass für jede natürliche Zahl n die Mengen $\{k \in \mathbb{N} : k < n\} = \{0, 1, 2, \dots, n-1\}$ genau n Elemente enthalten, d.h. sie haben die Mächtigkeit n . Jede Menge A , die nun gleichmächtig zu einer Menge dieser Art ist, wird dann als endlich bezeichnet (und ihre Kardinalität ist dann die entsprechende natürliche Zahl n). Jede andere Menge, die zu keiner dieser Mengen gleichmächtig ist, wird als unendlich bezeichnet. Beispielsweise ist die Menge $\mathbb{N} = \{0, 1, 2, \dots\}$ der natürlichen Zahlen eine unendliche Menge.

Eine wichtige Klasse von Mengen sind jene, die zu $\mathbb{N}$ gleichmächtig sind, diese nennt man **abzählbare Mengen**. Das sind also jene Mengen A , wo es möglich ist, die Elemente „durchzunummerieren“: $A = \{a_0, a_1, a_2, \dots\}$ (alle a_j sind voneinander verschieden). Wir haben bereits gesehen, dass die geraden natürlichen Zahlen $\{0, 2, 4, 6, \dots\}$ abzählbar sind. Es sind aber auch – was erst beim zweiten Blick klar wird – die ganzen Zahlen $\mathbb{Z} = \{0, 1, -1, 2, -2, \dots\}$ und die rationalen Zahlen $\mathbb{Q} = \{0, 1, -1, 2, -2, \frac{1}{2}, -\frac{1}{2}, 3, -3, \frac{1}{3}, -\frac{1}{3}, \frac{3}{2}, -\frac{3}{2}, \frac{2}{3}, -\frac{2}{3}, \dots\}$ abzählbar. Es gibt auch überabzählbare Mengen, also unendliche Mengen, wo es nicht mehr möglich ist, die Elemente durchzunummerieren. Beispielsweise sind die reellen Zahlen überabzählbar.

2. Mengenoperationen

Definition 1.43 Die Vereinigung $A \cup B$ zweier Mengen A, B enthält genau jene Elemente x , die in A oder in B enthalten sind, d.h.

$$A \cup B = \{x \mid x \in A \vee x \in B\}.$$

Der Durchschnitt $A \cap B$ zweier Mengen A, B enthält genau jene Elemente x , die sowohl in A als auch in B enthalten sind, d.h.

$$A \cap B = \{x \mid x \in A \wedge x \in B\}.$$

Es ist oft notwendig, nicht nur zwei oder endlich viele Mengen zu vereinigen, sondern ein ganzes System von Mengen. Dafür verwendet man die folgende Notation.

Definition 1.44 Sei I eine Menge (Indexmenge), und für alle $i \in I$ sei A_i eine Menge. Dann ist durch

$$\bigcup_{i \in I} A_i = \{x \mid \exists i \in I : x \in A_i\}$$

die Vereinigung aller $A_i, i \in I$, und durch

$$\bigcap_{i \in I} A_i = \{x \mid \forall i \in I : x \in A_i\}$$

der Durchschnitt aller $A_i, i \in I$, definiert.

Wie im Abschnitt 1. schon angedeutet wurde, ist es oft sinnvoll, nur Teilmengen einer „großen Menge“, eines Universums E zu betrachten. Die folgende Definition ist nur in einem solchen Kontext anzuwenden.

Definition 1.45 Sei $A \subseteq E$. Dann bezeichnet

$$A' = \{x \in E \mid x \notin A\}$$

das **Komplement** von A .

Manchmal wird auch die Bezeichnung $\bar{A}$ für das Komplement verwendet.

Satz 1.46 Seien A, B, C und $A_i, i \in I$, Teilmengen einer Menge E . Dann gelten die folgenden Rechenregeln:

- | | |
|---|--|
| (i) $A \cup B = B \cup A,$ | $A \cap B = B \cap A,$ |
| (ii) $A \cup (B \cap C) = (A \cup B) \cap C,$ | $A \cap (B \cup C) = (A \cap B) \cup C,$ |
| (iii) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C),$ | $A \cup (B \cap C) = (A \cup B) \cap (A \cup C),$ |
| (iii)' $A \cap \bigcup_{i \in I} A_i = \bigcup_{i \in I} (A \cap A_i),$ | $A \cup \bigcap_{i \in I} A_i = \bigcap_{i \in I} (A \cup A_i),$ |
| (iv) $A \cup \emptyset = A,$ | $A \cap E = A,$ |
| (v) $A \cup A' = E,$ | $A \cap A' = \emptyset,$ |
| (vi) $A \cup A = A,$ | $A \cap A = A,$ |
| (vii) $A \cup E = E,$ | $A \cap \emptyset = \emptyset,$ |
| (viii) $A \cup (A \cap B) = A,$ | $A \cap (A \cup B) = A,$ |
| (ix) $(A \cup B)' = A' \cap B',$ | $(A \cap B)' = A' \cup B',$ |
| (ix)' $(\bigcup_{i \in I} A_i)' = \bigcap_{i \in I} A_i',$ | $(\bigcap_{i \in I} A_i)' = \bigcup_{i \in I} A_i',$ |

Die Regel (i) nennt man auch **Kommutativgesetz**, (ii) **Assoziativgesetz**, (iii) **Distributivgesetz**, (viii) **Verschmelzungsgesetz** und (ix) **DeMorgan'sche Regel**.

Definition 1.47 Die **Mengendifferenz** $A \setminus B$ zweier Mengen A, B enthält genau jene Elemente x , die in A , aber nicht in B enthalten sind, d.h.

$$A \setminus B = \{x \mid x \in A \wedge x \notin B\}.$$

Die **symmetrische Differenz** $A \Delta B$ zweier Mengen A, B ist durch

$$\begin{aligned} A \Delta B &= (A \setminus B) \cup (B \setminus A) \\ &= (A \cup B) \setminus (A \cap B) \end{aligned}$$

gegeben.

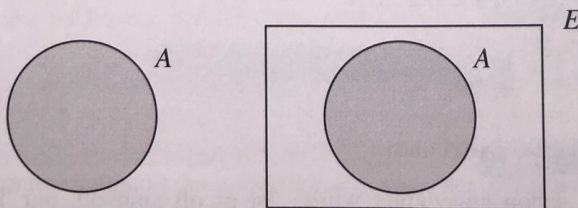


Abbildung 1.6 Venn diagramm einer Menge A ohne bzw. mit Universum E

Es ist oft nützlich, eine Menge A bildlich durch ein so genanntes **Venn-Diagramm** (vgl. Abb. 1.6) darzustellen.

Auf diesem Weg lassen sich die Mengenoperationen **Vereinigung, Durchschnitt, Komplement, Mengendifferenz und symmetrische Differenz** auf **einfache Art** graphisch verdeutlichen (siehe Abb. 1.7).

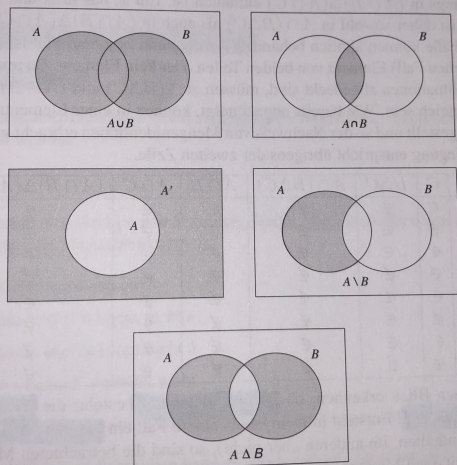


Abbildung 1.7 Mengenoperationen

3. Mengenidentitäten

Mengenidentitäten sind **allgemeine Gleichungen für Mengen**, also z.B. $A \cup B = B \cup A$ oder $A = A \cup (A \cap B)$. Definitionsgemäß sind **zwei Mengen gleich**, wenn sie **dieselben Elemente** enthalten. Wie im Beweis von Satz 1.42 kann dies oft auf **logische Regeln** zurückgeführt werden. So ist etwa die logische Formel $x \in A \vee x \in B$ zur Formel $x \in B \vee x \in A$ äquivalent. Daher folgt direkt

$$A \cup B = \{x \mid x \in A \vee x \in B\} = \{x \mid x \in B \vee x \in A\} = B \cup A$$

Elementartafel:

A	B	C	$B \Delta C$	$A \cap (B \Delta C)$	$A \cap B$	$A \cap C$	$(A \cap B) \Delta (A \cap C)$
∈	∈	∈	∅	∅	∈	∈	∅
∈	∈	∅	∈	∈	∈	∅	∈
∈	∅	∈	∈	∈	∅	∈	∈
∈	∅	∅	∅	∅	∅	∅	∅
∅	∈	∈	∅	∅	∅	∅	∅
∅	∈	∅	∈	∅	∅	∅	∅
∅	∅	∈	∈	∅	∅	∅	∅
∅	∅	∅	∅	∅	∅	∅	∅

Potenzmenge:

↳ Menge aller Teilmengen von A .

Potenzmenge $P(M)$ zu einer Menge

$$M = \{1, 2\}$$

$$P(M) = \{ \emptyset, \{1\}, \{2\}, \{1, 2\} \}$$

$$M = \{1, 2, 3\}$$

$$P(M) = \{ \emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\} \}$$

Relationsbegriff:

Zwei Elemente a, b einer Menge stehen miteinander in einer gewissen **Relation** (wobei die Reihenfolge eine Rolle spielen kann) oder eben nicht. Um diesen **Relationsbegriff** mathematisch streng zu fassen, benötigt man den Begriff des geordneten Paares von Elementen und des **kartesischen Produkts** von Mengen.

Definition 1.51 Ein **geordnetes Paar** (a, b) zweier Elemente a, b , die nicht unbedingt voneinander verschieden sein müssen, fasst diese zu einem neuen Element zusammen, wobei die Reihenfolge wesentlich ist, d.h. $(a, b) = (c, d)$ ist gleichbedeutend mit $a = c$ und $b = d$. Das **kartesische Produkt** $A \times B$ zweier Mengen A, B ist die Menge aller geordneten Paare (a, b) mit $a \in A$ und $b \in B$, d.h.

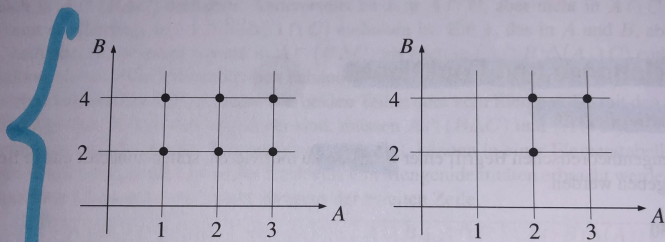
$$A \times B = \{ (a, b) \mid a \in A \wedge b \in B \}.$$

In derselben Weise definiert man auch das Produkt $A_1 \times A_2 \times \dots \times A_n$ von endlich vielen Mengen $A_1, A_2, \dots, A_n$ als die Menge aller (geordneten) n -tupel $(a_1, a_2, \dots, a_n)$ mit $a_j \in A_j$ ($1 \leq j \leq n$). Sind alle Mengen A_j gleich einer Menge A , so schreibt man statt $A \times A \times \dots \times A$ auch A^n .

Beispiel 1.52 Sei $A = \{1, 2, 3\}$ und $B = \{2, 4\}$. Dann ist

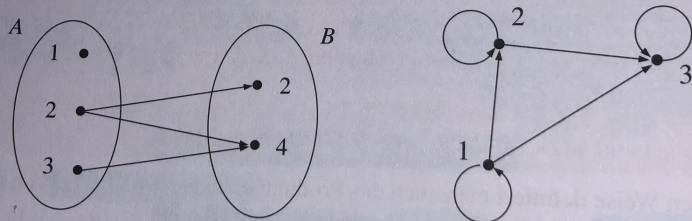
$$A \times B = \{(1, 2), (1, 4), (2, 2), (2, 4), (3, 2), (3, 4)\}.$$

Dies lässt sich auch „kartesisch“ darstellen, siehe Abb. 1.8. $\triangle$



Definition 1.53 Eine **Relation** R zwischen zwei Mengen A und B ist eine Teilmenge des kartesischen Produkts $A \times B$. Ist $A = B$ so spricht man von einer **binären Relation** auf A . Anstelle von $(a, b) \in R$ schreibt man auch aRb , anstelle von $(a, b) \notin R$ auch $a \not R b$.

1. **Kartesische Darstellung:** In der kartesischen Darstellung von $A \times B$ werden nur jene Elemente (= Punkte) von $A \times B$ markiert, die der Relation $R \subseteq A \times B$ angehören
2. **Pfeildiagramm:** Die Mengen A, B werden durch Venndiagramme dargestellt und Paare $(a, b) \in R$ durch einen Pfeil verbunden



3. **Graph einer binären Relation:** Da bei einer binären Relation $A = B$ gilt (d.h. $R \subseteq A \times A = A^2$), reicht es, die Menge A nur einmal zu repräsentieren. Paare $(a, b) \in A \times A$, die in Relation stehen, werden nun ähnlich wie beim Pfeildiagramm miteinander verbunden. Der **Graph** $G(R)$ besteht daher aus einer Menge von **Punkten** entsprechend den Elementen aus A und einer Menge von **gerichteten Kanten**, die genau jene Punkte miteinander verbinden, die in Relation stehen.

Man beachte, dass im Graph einer Relation auch so genannte **Schlingen** auftreten können, das sind Kanten, die von $a \in A$ wieder auf a zeigen (a steht mit sich selbst in Relation: aRa).

Äquivalenzrelation:

Die Grundidee von Äquivalenzrelationen ist, gewisse Elemente als gleichwertig (also äquivalent) zu betrachten, also z.B. Schrauben gleicher Länge (Beispiel 1.50 (c)) oder ganze Zahlen a, b mit $a \equiv b \pmod{m}$ (Beispiel 1.56 (c)). Die formalen Kriterien sind die folgenden.

Definition 1.55 Eine binäre Relation R auf einer Menge A heißt **Äquivalenzrelation**, wenn folgende drei Eigenschaften erfüllt sind:

- Reflexivität:** $\forall a \in A : aRa$, = reflexiv
- Symmetrie:** $\forall a, b \in A : aRb \Rightarrow bRa$, = symmetrisch
- Transitivität:** $\forall a, b, c \in A : (aRb \wedge bRc) \Rightarrow aRc$, = transitiv

In der kartesischen Darstellung einer Relation R äußert sich die Reflexivität dadurch, dass die 1. Hauptdiagonale (1. Mediane) in der Relation enthalten ist. Ist die Relation symmetrisch, so ist die kartesische Darstellung symmetrisch zur 1. Hauptdiagonale, d.h. R geht durch Spiegelung an der 1. Hauptdiagonale in sich über. Die Transitivität hat in der kartesischen Darstellung keine offensichtliche Entsprechung.

Stellt man eine Relation R als Graph $G(R)$ dar, so entspricht einer reflexiven Relation ein Graph, bei dem jeder Punkt (Knoten) mit einer Schlinge ausgestattet ist. Bei einer symmetrischen Relation treten die Kanten (mit Ausnahme der Schlingen) gepaart auf. Zu einer Kante von a nach b gibt es immer auch eine Gegenkante von b nach a . Ebenso lässt sich die Transitivität sofort übersetzen.

Ein entsprechender Sachverhalt gilt ganz allgemein. Äquivalenzrelationen zerlegen die Grundmenge in so genannte Äquivalenzklassen. Dies soll nun präzisiert werden.

Definition 1.57 Ein System von nichtleeren Teilmengen A_i ($i \in I$) einer Menge A heißt **Partition** oder **Zerlegung** von A , wenn die A_i ($i \in I$) paarweise disjunkt sind, d.h.

$$A_i \cap A_j = \emptyset \quad \text{für } i \neq j,$$

und A die Vereinigung

$$A = \bigcup_{i \in I} A_i$$

Definition 1.58 Sei R eine Äquivalenzrelation auf A . Für $a \in A$ heißt die Menge

$$K(a) = \{b \in A \mid bRa\}$$

die von a erzeugte **Äquivalenzklasse**.

Man beachte, dass wegen der Reflexivität immer $a \in K(a)$ gilt, insbesondere ist $K(a)$ nicht leer.

Satz 1.59 Sei R eine Äquivalenzrelation auf A . Dann bilden die (verschiedenen) Äquivalenzklassen der Elemente von A eine Partition von A .

Sei umgekehrt A_i ($i \in I$) eine Partition von A und bezeichne $\tilde{K}(a)$ ($a \in A$) jene Teilmenge A_j der Partition mit $a \in A_j$. Definiert man aRb genau für jene $a, b \in A$, für die $\tilde{K}(a) = \tilde{K}(b)$ gilt, so ist R eine Äquivalenzrelation mit $K(a) = \tilde{K}(a)$ für alle $a \in A$.

Beweis. Es sei zunächst R eine Äquivalenzrelation auf der Menge A , und es sei $\mathcal{K} = \{K(a) | a \in A\}$ das System der dazugehörigen Äquivalenzklassen. Offensichtlich gilt $K(a) \subseteq A$ und wegen der Reflexivität $a \in K(a)$. Daher ist $K(a)$ für kein $a \in A$ leer. Weiters folgt daraus auch $\bigcup_{a \in A} K(a) = A$. Es bleibt also zu zeigen, dass verschiedene Äquivalenzklassen $K(a) \neq K(b)$ kein Element gemeinsam haben, also disjunkt sind. Wäre etwa $c \in K(a) \cap K(b)$, so folgt cRa und cRb und wegen der Symmetrie und Transitivität auch aRb . Aus aRb folgt aber

unmittelbar (wieder wegen der Symmetrie und Transitivität) $K(a) = K(b)$, was aber ausgeschlossen wurde.

Für den zweiten Teil des Beweises muss nur nachgeprüft werden, ob die definierte Relation R reflexiv, symmetrisch und transitiv ist. Das ist eine leichte Übung. Aus $\tilde{K}(a) = \tilde{K}(a)$ folgt aRa , und die offensichtlich richtigen Aussagen $\tilde{K}(a) = \tilde{K}(b) \implies \tilde{K}(b) = \tilde{K}(a)$ und $\tilde{K}(a) = \tilde{K}(b) \wedge \tilde{K}(b) = \tilde{K}(c) \implies \tilde{K}(a) = \tilde{K}(c)$ implizieren Symmetrie und Transitivität. $\square$

3. Halbordnungen

Eine zweite wichtige Klasse von binären Relationen sind Halbordnungen. Die Grundidee ist hier, auf einer Menge A eine „Hierarchie“ einzuführen. Formal verlangt man für diese Hierarchie die folgenden Eigenschaften.

Definition 1.60 Eine binäre Relation R auf einer Menge A heißt **Halbordnung oder partielle Ordnung**, wenn folgende drei Eigenschaften erfüllt sind:

- (i) **Reflexivität:** $\forall a \in A : aRa$,
- (ii) **Antisymmetrie:** $\forall a, b \in A : (aRb \wedge bRa) \implies a = b$, = antisymmetrisch
- (iii) **Transitivität:** $\forall a, b, c \in A : (aRb \wedge bRc) \implies aRc$.

Definition 1.61 Eine Halbordnung R auf einer Menge A heißt **Totalordnung**, wenn je zwei Elemente vergleichbar sind.

Wie jede binäre Relation kann man natürlich auch Halbordnungen durch einen Graphen darstellen. Viele der darzustellenden Kanten sind allerdings redundant, sie lassen sich aus den definierenden Eigenschaften leicht wieder rekonstruieren. Führt man die folgenden drei Schritte durch, so erhält man aus dem Graphen $G(R)$ einer Halbordnung R das **Hasse-Diagramm** der Relation R : nächste Seite $\rightarrow$

„redundant“ = „mehrfach vorhanden“

- Weglassen aller Schlingen.
- Weglassen aller Kanten, die sich aufgrund der Transitivitätsbedingung rekonstruieren lassen.
D.h.: nur die unmittelbaren Nachbarn von a werden mit einer Kante verbunden.
- Weglassen aller Orientierungen. Wegen der Antisymmetrie kann für $a \neq b$ entweder aRb oder bRa gelten, aber nie beides zugleich.

Oft wird eine Halbordnung auf einer endlichen Menge nur durch Angabe des Hassediagramms definiert.

Abschließend werden noch zwei Begriffe betrachtet, die erst bei unendlichen Halbordnungen wirklich relevant werden, nämlich das Hausdorffsche Maximalitätsprinzip und die transfiniten Induktion.

Eine **Kette** K einer Halbordnung (H, R) ist eine Teilmenge von H , die mit der Relation R eine Totalordnung bildet. Eine Kette heißt **maximal**, wenn es nicht möglich ist, K um ein Element von H zu erweitern, so dass R wieder eine Totalordnung bildet. (Beispielsweise ist $K = \{\emptyset, \{1, 2\}, \{1, 2, 3\}\}$ eine Kette von $P(\{1, 2, 3\}, \subseteq)$, aber keine maximale Kette, da man z.B. das Element $\{2\}$ noch ergänzen kann. Nimmt man diese dazu, erhält man eine maximale Kette.) Das **Hausdorffsche Maximalitätsprinzip** besagt, dass jede Halbordnung eine maximale Kette besitzt. Dies ist für endliche Halbordnungen evident, für unendliche Halbordnungen allerdings nicht. Es stellt sich heraus, dass die Richtigkeit des Hausdorffsche Maximalitätsprinzips äquivalent zum Auswahlaxiom ist.

Ein Element m einer Teilmenge S einer Halbordnung H heißt **Minimum**, wenn für alle Elemente $s \in S$ die Relation mRs gilt. Beispielsweise ist 0 das Minimum der natürlichen

Zahlen $\mathbb{N}$ als Teilmenge in der Halbordnung der ganzen Zahlen $\mathbb{Z}$. Eine Totalordnung (H, R) heißt **Wohlordnung**, wenn jede nicht-leere Teilmenge S von H ein Minimum besitzt. Neben jeder endlichen Totalordnung bildet beispielsweise die Halbordnung $(\mathbb{N}, \leq)$ eine Wohlordnung. Denn es gilt: jede nicht-leere Teilmenge der natürlichen Zahlen hat ein kleinstes Element.

Es sei nun $A(x)$ ein Prädikat (das für $x \in H$ definiert ist). Das Prinzip der **transfiniten Induktion** für Wohlordnungen lautet nun:

$$\forall x \in H : ((\forall y R x, y \neq x : A(y)) \Rightarrow A(x)) \implies \forall x \in H : A(x)$$

Funktionen:

Definition 1.64 Seien A, B zwei nichtleere Mengen. Eine **Funktion** oder **Abbildung** $f : A \rightarrow B$ von A nach B ist ein Tripel (A, B, R_f) , wobei $R_f \subseteq A \times B$ eine Relation ist mit der Eigenschaft, dass zu jedem $a \in A$ genau ein $b \in B$ mit aR_fb existiert. Man schreibt dafür $b = f(a)$. Die Menge $R_f = \{(a, f(a)) \mid a \in A\} \subseteq A \times B$ bezeichnet man auch als **Graph der Funktion** $f : A \rightarrow B$.

Definition 1.65 Eine Funktion $f : A \rightarrow B$ heißt **injektiv** oder **Injektion**, wenn es zu jedem $b \in B$ höchstens ein $a \in A$ mit $b = f(a)$ gibt, d.h. $a_1 \neq a_2$ impliziert $f(a_1) \neq f(a_2)$.

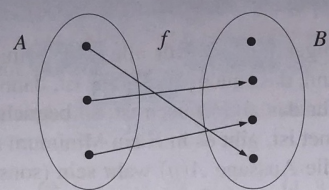


Abbildung 1.12 Injektive Funktion

Eine Funktion $f : A \rightarrow B$ heißt **surjektiv** oder **Surjektion**, wenn es zu jedem $b \in B$ mindestens ein $a \in A$ mit $b = f(a)$ gibt.

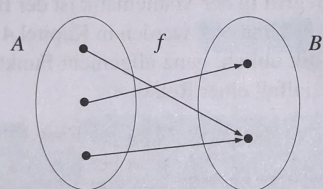


Abbildung 1.13 Surjektive Funktion

Eine Funktion $f : A \rightarrow B$ heißt **bijektiv** oder **Bijektion**, wenn es zu jedem $b \in B$ genau ein $a \in A$ mit $b = f(a)$ gibt.

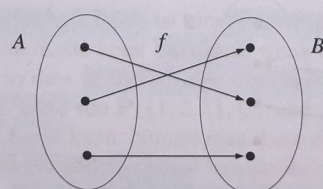


Abbildung 1.14 Bijektive Funktion

Offensichtlich ist eine Funktion $f : A \rightarrow B$ genau dann bijektiv, wenn sie injektiv und surjektiv ist.

Satz 1.67 Haben zwei endliche Mengen A, B gleich viele Elemente, d.h. $|A| = |B|$, dann ist eine injektive Funktion $f : A \rightarrow B$ auch surjektiv und damit bijektiv. Entsprechend ist eine surjektive Funktion $f : A \rightarrow B$ auch injektiv und ebenfalls bijektiv.

Satz 1.70 Sind die Funktionen $f : A \rightarrow B$ und $g : B \rightarrow C$ beide injektiv (bzw. surjektiv bzw. bijektiv), so ist auch $g \circ f : A \rightarrow C$ injektiv (bzw. surjektiv bzw. bijektiv).

Definition 1.71 Eine Funktion $f^{-1} : B \rightarrow A$ heißt die zu der Funktion $f : A \rightarrow B$ **inverse Funktion** (oder **Umkehrfunktion**), wenn $f^{-1} \circ f = \text{id}_A$ und $f \circ f^{-1} = \text{id}_B$ gilt. Dabei bezeichnet id_A die **identische Funktion** auf einer Menge A , d.h. $\text{id}_A(a) = a$ für alle $a \in A$.

Satz 1.73 Eine Funktion $f : A \rightarrow B$ besitzt genau dann eine inverse Funktion $f^{-1} : B \rightarrow A$, wenn f bijektiv ist. Die inverse Funktion f^{-1} ist dann auch bijektiv.

Kapitel



2

1. Grundaufgaben der Kombinatorik

Für alle Abzählverfahren gelten die folgenden drei einfachen Grundregeln.

- (i) **Summenregel.** Besteht die Menge A aus m Elementen und die Menge B aus n Elementen und haben A und B keine gemeinsamen Elemente, so besteht die Vereinigung von A und B aus $m + n$ Elementen:

$$A \cap B = \emptyset \implies |A \cup B| = |A| + |B|.$$

- (ii) **Produktregel.** Besteht die Menge A aus m Elementen und die Menge B aus n Elementen, so gibt es genau $m \cdot n$ Möglichkeiten, Elemente von A und B zu kombinieren, also geordnete Paare zu bilden:

$$|A \times B| = |A| \cdot |B|.$$

- (iii) **Gleichheitsregel.** Gibt es eine bijektive Entsprechung der Elemente der Mengen A und B , so sind A und B gleich groß:

$$\exists f : A \rightarrow B \text{ bijektiv} \iff |A| = |B|.$$

Definition 2.3 Unter der **Fakultät einer natürlichen Zahl** $n \geq 1$ (bzw. unter n -**Faktorielle**) versteht man das Produkt

$$n! = 1 \cdot 2 \cdot 3 \cdots (n-1) \cdot n.$$

Weiters setzt man $0! = 1$.

Der **Binomialkoeffizient** $\binom{n}{k}$ (in Worten „ n über k “) wird für natürliche Zahlen n, k mit $0 \leq k \leq n$ durch

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

definiert. Für $n \geq 0$ und $k < 0$ oder $k > n$ setzt man $\binom{n}{k} = 0$.

Man beachte die rekursive Beziehung $(n+1)! = n! (n+1)$. Diese ist auch im Fall $n = 0$ richtig.

Viele kombinatorische Probleme lassen sich auf **Anordnungsprobleme** und **Auswahlprobleme** zurückführen, wobei bei **Anordnungen** die Reihenfolge der betrachteten Objekte eine Rolle spielt, bei **Auswahlen** hingegen nicht. Die folgenden sechs kombinatorischen Grundaufgaben beziehen sich genau auf diese Fälle.

Im Folgenden sei $A = \{a_1, a_2, \dots, a_n\}$ eine Menge mit n Elementen.

- (i) **Anordnungen ohne Einschränkung.** Die Menge A^k der geordneten k -Tupel wird als die Menge der Anordnungen von Elementen von A der Länge k interpretiert. Hier ist die Reihenfolge der Elemente natürlich wesentlich. Wegen der Produktregel gilt jedenfalls

$$|A^k| = |A|^k = n^k. \quad (2.1)$$

Manchmal bezeichnet man A^k auch als **Variationen mit Wiederholung** oder als „geordnete Auswahl“ von k Elementen aus A mit Zurücklegen. Der Begriff „Zurücklegen“ kommt davon, dass es in der Kombinatorik üblich ist, eine Menge A als „Urne“ und die Elemente als „Kugeln“ bildlich zu beschreiben. Die k -Tupel aus A^k können nun als geordnete Auswahlen von k Elementen aus A interpretiert werden, wobei man bei jedem Schritt wieder alle Elemente („Kugeln“) zur Verfügung hat, also das gewählte Element („Kugel“) wieder zurückgelegt worden ist.

(ii) **Anordnungen verschiedener Elemente.** Die geordneten k -Tupel von Elementen von A , wobei alle Elemente verschieden sind, werden als **Variationen ohne Wiederholung** oder – wieder mit Hilfe des Urnenbildes – als „geordnete Auswahlen“ von k Elementen aus A ohne Zurücklegen bezeichnet. Offensichtlich muss hier $k \leq n$ gelten. Für die Berechnung der Anzahl dieser Möglichkeiten kann man wieder die Produktregel verwenden, allerdings in einer leicht modifizierten Form. Für die Auswahl der ersten „Kugel“ hat man alle Elemente aus A zur Verfügung, also n Möglichkeiten. Für die zweite Stelle kann das zuerst gewählte Element nicht verwendet werden, es bleiben daher $n - 1$ Möglichkeiten, usw. Insgesamt ergeben sich

$$n \cdot (n - 1) \cdot (n - 2) \cdots (n - k + 1) = \frac{n!}{(n - k)!} \quad (2.2)$$

(iii) **Permutationen einer Menge.** Eine Permutation π einer Menge A ist eine bijektive Funktion $\pi : A \rightarrow A$. Besteht die Menge A aus n Elementen, etwa $A = \{a_1, a_2, \dots, a_n\}$, so wird π auch durch Angabe der Bilder $\pi(a_1), \pi(a_2), \dots, \pi(a_n)$ beschrieben. Wegen der Bijektivität muss jedes Element aus A in dieser Auflistung genau einmal auftreten. Eine Permutation von A entspricht daher genau einer Anordnung der Elemente von A , wobei jedes Element genau einmal auftritt. Mit derselben Überlegung wie vorhin erkennt man, dass es

$$n! \quad (2.3)$$

verschiedene Permutationen einer n -elementigen Menge gibt.

Beispielsweise gibt es $3! = 6$ Möglichkeiten, 3 Gläser gefüllt mit Bier, Schnaps und Wein nacheinander zu leeren: $A = \{B, S, W\}$,

BSW, BWS, SBW, SWB, WBS, WSB.

(iv) **Permutationen einer Multimenge.** Ein etwas allgemeineres Problem ist es, Anordnungen der Elemente von A zu betrachten, wobei man vorgibt, wie oft ein Element auftreten soll. Man spricht hier auch von **Permutationen einer Multimenge**. Fordert man, dass das Element a_i genau k_i -mal auftreten soll ($1 \leq i \leq n$), so gibt es

$$\frac{(k_1 + k_2 + \cdots + k_n)!}{k_1! k_2! \cdots k_n!} \quad (2.4)$$

Möglichkeiten solcher Anordnungen. Dies lässt sich folgendermaßen begründen. Unterscheidet man zunächst die k_i gleichen Elemente a_i ($1 \leq i \leq n$), so gibt es $(k_1 + k_2 + \cdots + k_n)!$ mögliche Anordnungen. Davon führen aber (wegen der Produktregel) insgesamt $k_1! k_2! \cdots k_n!$ Anordnungen zur selben ursprünglich gesuchten Anordnung, da alle Umordnungen unter den k_i Elementen a_i ($1 \leq i \leq n$) dieselbe (gesuchte) Anordnung ergeben.

Beispielsweise können 2 Gläser Bier, 1 Glas Schnaps und 1 Glas Wein in $4!/(2! 1! 1!) = 12$ verschiedenen Reihenfolgen getrunken werden:

BBSW, BBWS, BSBW, BWBS, BSWB, BWSB, SBBW, WBBS, SBWB, WBSB, SWBB, WSBB.

(v) **Auswahlen einer Teilmenge.** Eine (ungeordnete) Auswahl von k verschiedenen Elementen einer Menge A ist nichts anderes als eine Teilmenge von A der Größe k . In der Kombinatorik wird so eine Auswahl auch als **Kombination ohne Wiederholung** bezeichnet. Hier gibt es

$$\frac{n!}{k!(n-k)!} = \binom{n}{k} \quad (2.5)$$

Möglichkeiten. Das kann auf verschiedene Arten begründet werden. Z.B. entsprechen die k -elementigen Teilmengen einer n -elementigen Menge den Binärzahlen der Länge n mit k Einsen, also genau den Permutationen einer Multimenge von k Einsen und $(n-k)$ Nullen. Eine andere Begründung ist, dass genau $k!$ Anordnungen verschiedener Elemente einer Auswahl entsprechen.

Es ist auch üblich, die Elemente von A gedanklich in eine Urne zu geben und sie als verschiedene „Kugeln“ zu interpretieren. Eine Auswahl von k Elementen entspricht dann einfach dem „gleichzeitigen“ Entnehmen von k Kugeln aus der Urne. Im Gegensatz dazu wird – bildlich gesprochen – bei einer Anordnung eine „Kugel“ nach der anderen aus der Urne genommen.

Beispielsweise gibt es $\binom{45}{6} = 45!/(6!39!) = 8\,145\,060$ mögliche Lottotipps „6 aus 45.“ Ein Tipp entspricht einer 6-elementigen Teilmenge von $A = \{1, 2, \dots, 45\}$.

(vi) **Auswahlen einer Teilmultimenge.** Entsprechend betrachtet man auch Auswahlen von Elementen einer Menge A , wo die Elemente von A mehrfach auftreten können, also Teilmultimengen der Multimenge $\tilde{A}$, in der jedes Element von A beliebig oft vorkommt. Solche Anordnungen werden auch als **Kombinationen mit Wiederholung** bezeichnet. Hier kann wieder das Bild der „Urne“ verwendet werden. Man stelle sich eine Urne vor, in der jedes Element von A nicht nur einmal, sondern beliebig oft vorhanden ist, d.h. in der Urne sind unendlich viele „Kugeln“ vom Typ a_1 , unendlich viele „Kugeln“ vom Typ a_2 etc. Entnimmt man nun dieser Urne in einem Satz k „Kugeln“, so entspricht dies genau so einer Auswahl.

Da die Reihenfolge keine Rolle spielt, können wir diese Kugeln der Reihe nach anordnen, zuerst die Kugeln vom Typ a_1 , dann die Kugeln vom Typ a_2 , usw. Insgesamt sind dies k Kugeln. Wir wollen nun diese Kugeln alle weiß färben. Damit geht allerdings die Information, welche Kugeln von welchem Typ sind, verloren. Um diese Information nicht zu verlieren, setzen wir $n-1$ schwarze „Trennkugeln“ ein. Wir illustrieren das an einem einfachen Beispiel: Sei $A = \{a_1, a_2, a_3, a_4\}$ eine Menge mit $n = 4$ Elementen und

$$a_1, a_1, a_1, a_2, a_2, a_4, a_4$$

eine Auswahl von $k = 7$ Elementen. Nach Einfügen von $n-1 = 3$ schwarzen Kugeln an den Schnittstellen erhalten wir zunächst folgendes Bild:

$$a_1, a_1, a_1, \bullet, a_2, a_2, \bullet, \bullet, a_4, a_4$$

Jetzt kann man die Elemente (= Kugeln) von A alle weiß färben:

$$\circ, \circ, \circ, \bullet, \circ, \circ, \bullet, \bullet, \circ, \circ$$

Offensichtlich ist es sofort möglich, aus dieser Anordnung von $k+n-1$ Kugeln die Auswahl $a_1, a_1, a_1, a_2, a_2, a_4, a_4$ eindeutig zu rekonstruieren. Wegen der Gleichheitsregel ist daher die Anzahl der Auswahlmöglichkeiten von Elementen von A genau der Anzahl der Permutationen von k weißen Kugeln $\circ$ und $n-1$ schwarzen Kugeln $\bullet$:

$$\frac{(n+k-1)!}{k!(n-1)!} = \binom{n+k-1}{k}. \quad (2.6)$$

Wir geben noch eine weitere Interpretation solcher Auswahlen. Um eine ungeordnete Anordnung von Elementen $a_1, a_2, \dots, a_n$ zu beschreiben, ist es ausreichend zu wissen, wie oft die Elemente vorkommen, die Reihenfolge spielt ja keine Rolle. Sei also k_i die Anzahl, wie oft a_i vorkommt ($1 \leq i \leq n$), dann wird eine ungeordnete Auswahl von k Elementen auch durch das n -Tupel $(k_1, k_2, \dots, k_n)$ von natürlichen Zahlen mit der Eigenschaft $k_1 + k_2 + \dots + k_n = k$ beschrieben. Das heißt, eine Kombination mit Wiederholung entspricht auch einer **Komposition** einer natürlichen Zahl in n Summanden $k_i \geq 0$. Beispielsweise gibt es $(4 + 7 - 1)! / (7! (4 - 1)!) = 120$ Möglichkeiten, die Zahl $k = 7$ als (geordnete) Summe von $n = 4$ Zahlen $k_i \geq 0$ darzustellen. Ein Beispiel wäre $7 = 3 + 2 + 0 + 2$.

Neben den gerade besprochenen Anordnungs- und Auswahlproblemen gibt es noch weitere kombinatorische Grundaufgaben, wie z.B. **Aufteilungsprobleme**, also Probleme, die sich darauf beziehen, eine Menge in Teilmengen aufzuteilen, also eine **Partition** zu erzeugen.

Beispielsweise werden die Anzahl der möglichen Partitionen einer n -elementigen Menge in k Teile durch die so genannten **Stirlingzahlen 2. Art**

$$S_{n,k} = \frac{1}{k!} \sum_{j=0}^k (-1)^{k-j} \binom{k}{j} j^n, \quad (0 \leq k \leq n),$$

gezählt. Diese Zahlen erfüllen auch die Rekursion

$$S_{n+1,k} = S_{n,k-1} + k S_{n,k}$$

(mit den Anfangsbedingungen $S_{n,n} = 1$, $n \geq 0$, und $S_{n,0} = 0$, $n \geq 1$). Die Anzahl aller möglichen Partitionen einer n -elementigen Menge werden als **Bellzahlen**

$$B_n = \sum_{k=0}^n S_{n,k}$$

bezeichnet. Diese erfüllen die Rekursion:

$$B_{n+1} = \sum_{k=0}^n \binom{n}{k} B_k$$

(mit der Anfangsbedingung $B_1 = 1$).

In der Zahlentheorie betrachtet man auch **Zahlpartitionen**, also die Aufteilung einer natürlichen Zahl n in Summanden. Beispielsweise kann die Zahl $n = 4$ auf folgende Arten zerlegt werden:

$$1 + 1 + 1 + 1, \quad 1 + 1 + 2, \quad 2 + 2, \quad 1 + 3, \quad 4;$$

also $p(4) = 5$. Man beachte, dass $1 + 3$ und $3 + 1$ nicht unterschieden werden, die Reihenfolge der Summanden also keine Rolle spielt. Die Anzahl $p(n)$ aller möglichen Zahlpartitionen einer natürlichen Zahl n wird als **Partitionsfunktion** bezeichnet. Bezeichnet man mit $p(n, k)$ die Anzahl der Zahlpartitionen von n in genau k Summanden, so gilt die Rekursion

$$p(n, k) = p(n - k, k) + p(n - 1, k - 1)$$

(mit den Anfangsbedingungen $p(n, 1) = p(n, n) = 1$) und $p(n)$ ist dann durch $p(n) = \sum_{k=1}^n p(n, k)$ gegeben.

Eine weitere grundlegende kombinatorische Technik ist das **Schubfachprinzip**. Wie bei Partitionen teilt man eine n -elementige Menge in k paarweise disjunkte Teilmengen auf, wobei – im Unterschied zu einer Partition – die Teilmengen auch leer sein können. Man kann auch sagen, man verteilt n Objekte auf k „Schubfächer“. Das Schubfachprinzip sagt nun, dass im Fall $n > k$ wenigstens eine der Teilmengen (oder Schubfächer) mehr als ein Element enthalten muss. (Andernfalls wäre nämlich $k \geq n$.) Mit der selben Idee kann man sogar sagen, dass bei einer Aufteilung von n Elementen in k Teilmengen wenigstens eine der Teilmengen $\lceil n/k \rceil$ Elemente enthalten muss.

Der binomische Lehrsatz

Eine der bekanntesten Formeln in der Mathematik ist

$$(a+b)^2 = a^2 + 2ab + b^2.$$

Im Grunde ist dies nur ein Spezialfall eines allgemeinen Satzes, des *binomischen Lehrsatzes*.

Wenn man nämlich höhere Potenzen ausrechnen will, z.B.

$$(a+b)^3$$

oder

$$(a+b)^4$$

wird der Rechenaufwand sehr groß, wenn man einfach ausmultipliziert. Letzterer Term ausmultipliziert ergibt etwa

$$a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4.$$

Man erkennt, wie kompliziert das Ausmultiplizieren wird. Deswegen versuchen wir eine allgemeine Formel für

$$(a+b)^n$$

zu ermitteln.

Es gilt

$$(a+b)^n = \underbrace{(a+b) * (a+b) * \dots * (a+b)}_{n\text{-mal}}$$

Wenn man alle Klammern ausmultipliziert, bekommt man eine Reihe von Termen, die wir Schritt für Schritt bestimmen. Beim Ausmultiplizieren wird 1 Faktor der 1. Klammer mit je 1 Faktor aller anderen Klammern multipliziert (dabei werden alle möglichen Kombinationen durchlaufen), und dann wird aufsummiert.

Wenn man dies bei

$$(a+b)^n = \underbrace{(a+b) * (a+b) * \dots * (a+b)}_{n\text{-mal}}$$

macht, ergibt das

$$\underbrace{(a+b) * (a+b) * \dots * (a+b)}_{n\text{-mal}} = a^n + na^{n-1}b + \frac{n(n-1)}{2!}a^{n-2}b^2 + \frac{n(n-1)(n-2)}{3!}a^{n-3}b^3 + \dots + \frac{n(n-1)\dots(n-m+1)}{m!}a^{n-m}b^m + \dots + nab^{n-1} + b^n.$$

Die Koeffizienten der Terme $a^{n-k}b^k$ sind

$$1, n, \frac{n(n-1)}{2!}, \dots, \frac{n(n-1)\dots(n-k+1)}{k!}, \dots, \frac{n(n-1)}{2!}, n, 1$$

welche man auch auf folgende Weise anschreiben kann

$$\binom{n}{0}, \binom{n}{1}, \binom{n}{2}, \dots, \binom{n}{k}, \dots, \binom{n}{2}, \binom{n}{1}, \binom{n}{0}$$

was gleich

$$\binom{n}{0}, \binom{n}{1}, \binom{n}{2}, \dots, \binom{n}{k}, \dots, \binom{n}{n-2}, \binom{n}{n-1}, \binom{n}{n}$$

ist.

Also gilt

$$(a+b)^n = \binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \dots + \binom{n}{n-1}ab^{n-1} + \binom{n}{n}b^n$$

bzw.

$$(a+b)^n = \sum_{k=0}^n \binom{n}{k} a^{n-k} b^k \quad \text{Binomischer Lehrsatz}$$

Satz 2.4 Die Binomialkoeffizienten erfüllen die Eigenschaften

- (i) $\binom{n}{0} = \binom{n}{n} = 1,$
- (ii) $\binom{n}{k} = \binom{n}{n-k},$
- (iii) $\binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1}.$

Pascal'sches Dreieck:

	k=0	k=1	k=2	k=3	k=4	k=5...
n=0	1					
n=1	1	1				
n=2	1	2	1			
n=3	1	3	3	1		
n=4	1	4	6	4	1	
n=5	1	5	10	10	5	1
⋮						

→ Erste Spalte 0, Hauptdiagonale 1
→ restliche Felder: Summe aus Zahl darüber und links darüber

$$\sum_{k=0}^n \binom{n}{k} = 2^n$$

Hintergrund davon und somit Binomialkoeff.:
Binomischer LS:

$$n \geq 0$$

x, y beliebig aus $\mathbb{C}$

$$\sum_{k=0}^n \binom{n}{k} x^{n-k} y^k = (x+y)^n \rightarrow \text{Beweis durch vollständige Induktion}$$

Beispiel: $x=y=1 \dots n=3$

$$(x+y)^3 = \binom{3}{0}x^3 + \binom{3}{1}x^2y + \binom{3}{2}xy^2 + \binom{3}{3}y^3 = x^3 + 3x^2y + 3xy^2 + y^3$$

3. Inklusions-Exklusions-Prinzip

Im letzten Teilabschnitt über Kombinatorik beschäftigen wir uns mit der allgemeinen Summenregel für die Berechnung von $|A \cup B|$, wenn A und B auch gemeinsame Elemente haben können (und mit entsprechenden Verallgemeinerungen für mehrere Mengen). Man überzeugt sich leicht, dass etwa die Beziehung

$$|A \cup B| = |A| + |B| - |A \cap B|$$

gilt, d.h. zur Bestimmung der Anzahl der Elemente von $A \cup B$ addiert man zunächst die Anzahl der Elemente von A und von B (Inklusion) und subtrahiert danach jene Elemente, die man einmal zuviel aufgenommen hat (Exklusion). Man kann dieses Prinzip folgendermaßen exakt

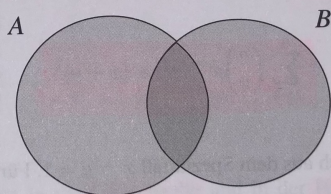


Abbildung 2.1 Vereinigung von zwei Mengen A und B

fassen (siehe Abb. 2.1):

$$\begin{aligned} |A \cup B| &= |A \setminus B| + |A \cap B| + |B \setminus A| \\ &= |A \setminus B| + |A \cap B| + |B \setminus A| + |A \cap B| - |A \cap B| \\ &= |A| + |B| - |A \cap B|. \end{aligned}$$

Die Situation wird bei drei Mengen etwas aufwändiger. Jedenfalls erhält man (nach einer kleinen Rechnung)

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|.$$

Es zeigt sich schon, wie das **Inklusions-Exklusions-Prinzip** im allgemeinen aussehen wird. Tatsächlich gilt der folgende Satz.

Satz 2.6 (Inklusions-Exklusions-Prinzip oder Siebformel) Es seien $A_1, A_2, \dots, A_n$ endliche Mengen. Dann gilt

$$\begin{aligned} \left| \bigcup_{i=1}^n A_i \right| &= |A_1 \cup A_2 \cup \dots \cup A_n| \\ &= \sum_{i=1}^n |A_i| - \sum_{1 \leq i < j \leq n} |A_i \cap A_j| + \sum_{1 \leq i < j < k \leq n} |A_i \cap A_j \cap A_k| \\ &\quad \mp \dots + (-1)^{n-1} |A_1 \cap A_2 \cap \dots \cap A_n| \\ &= \sum_{\emptyset \neq I \subseteq \{1, 2, \dots, n\}} (-1)^{|I|-1} \left| \bigcap_{i \in I} A_i \right|. \end{aligned}$$

Beweis. Man benützt das Beweisprinzip der vollständigen Induktion. Die Siebformel ist (wie bereits bemerkt) für $n = 1$ und $n = 2$ (und auch für $n = 3$) richtig. Man nehme nun an, sie sei für ein $n \geq 2$ richtig, dann folgt

für ein $n \geq 2$ richtig, dann folgt

$$\begin{aligned}
 \left| \bigcup_{i=1}^{n+1} A_i \right| &= \left| \bigcup_{i=1}^n A_i \cup A_{n+1} \right| \\
 &= \left| \bigcup_{i=1}^n A_i \right| + |A_{n+1}| - \left| \bigcup_{i=1}^n A_i \cap A_{n+1} \right| \\
 &= \sum_{\emptyset \neq I \subseteq \{1, 2, \dots, n\}} (-1)^{|I|-1} \left| \bigcap_{i \in I} A_i \right| + |A_{n+1}| - \sum_{\emptyset \neq I \subseteq \{1, 2, \dots, n\}} (-1)^{|I|-1} \left| \bigcap_{i \in I} A_i \cap A_{n+1} \right| \\
 &= \sum_{\emptyset \neq J \subseteq \{1, 2, \dots, n+1\}} (-1)^{|J|-1} \left| \bigcap_{j \in J} A_j \right|.
 \end{aligned}$$

□

Für die Anwendungen ist folgende Variante des Inklusions-Exklusions-Prinzips auch von Interesse. Wir setzen jetzt voraus, dass alle Mengen A_i in einem „Universum“ E enthalten

sind.¹ Dann gilt für das Komplement von $A_1 \cup A_2 \cup \dots \cup A_n$

$$\begin{aligned}
 \left| \bigcap_{i=1}^n A_i^c \right| &= \left| \left(\bigcup_{i=1}^n A_i \right)^c \right| = |E| - \left| \bigcup_{i=1}^n A_i \right| \\
 &= |E| - \sum_{\emptyset \neq I \subseteq \{1, 2, \dots, n\}} (-1)^{|I|-1} \left| \bigcap_{i \in I} A_i \right| \\
 &= \sum_{I \subseteq \{1, 2, \dots, n\}} (-1)^{|I|} \left| \bigcap_{i \in I} A_i \right|,
 \end{aligned}$$

wobei der leere Durchschnitt als $\{x \in E \mid \forall i \in \emptyset : x \in A_i\} = E$ gedeutet wird. Zum Beispiel ergibt sich für $n = 2$:

$$|A' \cap B'| = |E| - |A| - |B| + |A \cap B|.$$

1. Grundlegende graphentheoretische Begriffsbildungen

Definition 2.10 Ein **Graph** $G = (V, E)$ besteht aus einer endlichen Knotenmenge $V = V(G)$ und einer endlichen Kantenmenge $E = E(G)$.^a Dabei ist eine **Kante** $e \in E(G)$ entweder **gerichtet**, d.h. ein geordnetes Paar $e = (v_1, v_2)$ von zwei **Knoten** $v_1, v_2 \in V(G)$, oder **ungerichtet**, d.h. ein ungeordnetes Paar $e = \{v_1, v_2\} = v_1 v_2$ von zwei Knoten $v_1, v_2 \in V(G)$. Im gerichteten Fall heißt v_1 **Anfangsknoten** und v_2 **Endknoten** von e .

Sind alle Kanten $e \in E(G)$ gerichtet, so spricht man von einem **gerichteten Graphen**, sind hingegen alle Kanten $e \in E(G)$ ungerichtet, so heißt G **ungerichteter Graph**.

^aEs können auch Graphen mit unendlicher Knoten- bzw. unendlicher Kantenmenge betrachtet werden.

In Definition 2.10 sind auch Kanten der Form (v, v) (bzw. $\{v, v\} = \{v\} = vv$) zugelassen. So eine Kante heißt **Schlinge**. In vielen Zusammenhängen ist es sinnvoll, eine ungerichtete Kante $e = \{v_1, v_2\}$ als Zusammenfassung zweier gerichteter Kanten, also $e = \{(v_1, v_2), (v_2, v_1)\}$ zu sehen (vgl. Abb. 2.3).

Ein Graph ist übrigens eine alternative Beschreibung einer binären Relation auf einer Menge V . Dabei beschreibt ein gerichteter Graph eine allgemeine Relation und ein ungerichteter Graph eine symmetrische Relation.

Sind zwei Knoten v, w eines Graphen durch eine Kante verbunden, so heißen v und w auch **adjazent**. Weiters **inzidieren** Knoten v, w mit einer Kante, die sie verbindet. Die Anzahl der Knoten eines Graphen G wird auch mit $\alpha_0(G) = |V(G)|$ und die Anzahl der Kanten mit $\alpha_1(G) = |E(G)|$ bezeichnet.

Es ist auch möglich, Graphen mit **Mehrfachkanten** zu betrachten. Hier kann man aber Kanten nicht mehr mit Paaren von Knoten identifizieren. Einer allgemeinen Kante e werden zwei Knoten v_1, v_2 zugeordnet, die als Anfangs- bzw. Endknoten interpretiert werden können. Zwei verschiedene Kanten können daher (in diesem Rahmen) durchaus dieselben Anfangs- und Endknoten besitzen.

Definition 2.11 Ein Graph $G = (V, E)$ heißt **schlicht oder einfach**, wenn G keine Schlingen und keine Mehrfachkanten enthält.

Definition 2.12 In einem schlichten ungerichteten Graphen G heißen die zu $v \in V(G)$ adjazenten Knoten

$$\Gamma(v) = \{w \in V(G) \mid vw \in E(G)\}$$

Nachbarn von v . Die Anzahl

$$d(v) = |\Gamma(v)| = |\{w \in V(G) \mid vw \in E(G)\}|$$

der Nachbarn von $v \in V(G)$ ist der **Knotengrad** von $v \in V(G)$.

In einem gerichteten Graphen G heißen die Elemente von

$$\Gamma^+(v) = \{w \in V(G) \mid (v, w) \in E(G)\}$$

Nachfolger des Knotens $v \in V(G)$ und

$$\Gamma^-(v) = \{w \in V(G) \mid (w, v) \in E(G)\}$$

Vorgänger von $v \in V(G)$. $\Gamma(v) = \Gamma^+(v) \cup \Gamma^-(v)$ bilden die Nachbarn von $v \in V(G)$. Die Anzahl

$$d^+(v) = |\Gamma^+(v)| = |\{w \in V(G) \mid (v, w) \in E(G)\}|$$

der Nachfolger von $v \in V(G)$ ist der **Weggrad** von v , also die Anzahl der Kanten, die von v wegführen. Die Anzahl

$$d^-(v) = |\{w \in V(G) \mid (w, v) \in E(G)\}|$$

der Vorgänger von $v \in V(G)$ ist der **Hingrad** von v , also die Anzahl der Kanten, die zu v hinführen.

Man beachte, dass bei gerichteten Graphen in dieser Definition Schlingen zugelassen sind.

Lässt man auch im ungerichteten Fall Schlingen zu, so müssen diese bei der Gradberechnung doppelt gezählt werden.

Satz 2.13 (Handschlaglemma) In einem schlichten ungerichteten Graphen G gilt

$$\sum_{v \in V(G)} d(v) = 2|E(G)|.$$

In einem gerichteten Graphen G gilt hingegen

$$\sum_{v \in V(G)} d^+(v) = \sum_{v \in V(G)} d^-(v) = |E(G)|.$$

Beweis. In einem **schlichten ungerichteten Graphen** verbindet jede Kante genau zwei verschiedene Knoten. Denkt man sich alle Kanten in der Mitte „aufgeschnitten“, so zerfällt der Graph in lauter „Sterne“, wobei die Anzahl der „Halbkanten“, die mit einem Knoten verbunden sind, genau dem Grad des jeweiligen Knoten entspricht. Bildet man daher die Summe über alle Knotengrade, so wird jede Kante zweimal gezählt.

Bildet man hingegen bei einem gerichteten Graphen die Summe über alle Weggrade, so zählt man jede Kante genau einmal. Entsprechendes gilt für die Hingrade. $\square$

Definition 2.14 Ein Graph $G' = (V', E')$ heißt **Teilgraph** eines Graphen $G = (V, E)$ wenn $V' \subseteq V$ und $E' \subseteq E$ gelten.

Ein Teilgraph $G' = (V', E')$ eines Graphen $G = (V, E)$ heißt **induzierter Teilgraph**, wenn E' alle Kanten aus E enthält, für die Anfangs- und Endknoten in V' liegen, d.h., E' muss nicht extra angegeben werden, sondern wird durch Vorgabe von G und V' induziert.

Definition 2.15 Eine Folge von Kanten $e_1, e_2, \dots, e_k \in E(G)$ eines ungerichteten Graphen G heißt **Kantenfolge**, wenn es Knoten $v, v_1, v_2, \dots, v_{k-1}, w \in V(G)$ mit

$$e_1 = vv_1, e_2 = v_1v_2, \dots, e_{k-1} = v_{k-2}v_{k-1}, e_k = v_{k-1}w$$

gibt, d.h., man kann die Kanten $e_1, e_2, \dots, e_k$ „ohne Absetzen“ durchlaufen. Man sagt auch, dass die Kantenfolge e_j ($1 \leq j \leq k$) die Knoten v und w verbindet. Die Anzahl k der Kanten ist die **Länge** der Kantenfolge. Eine Kantenfolge der Länge 0 besteht aus keiner Kante und wird als **leere Kantenfolge** bezeichnet. Sie verbindet jeden Knoten mit sich selbst.

Eine Folge von Kanten $e_1, e_2, \dots, e_k \in E(G)$ eines gerichteten Graphen G heißt **Kantenfolge**, wenn für je zwei aufeinander folgende Kanten e_j, e_{j+1} ($1 \leq j < k$) der Endknoten von e_j mit dem Anfangsknoten von e_{j+1} übereinstimmt, d.h., es gibt Knoten $v, v_1, v_2, \dots, v_{k-1}, w$ mit

$$e_1 = (v, v_1), e_2 = (v_1, v_2), \dots, e_{k-1} = (v_{k-2}, v_{k-1}), e_k = (v_{k-1}, w).$$

Wiederum spricht man von einer Kantenfolge, die die Knoten v und w verbindet, v ist der Anfangsknoten und w der Endknoten. Ebenso ist k die Länge der Kantenfolge.

Ein Knoten w ist von einem Knoten v aus **erreichbar**, wenn es eine Kantenfolge gibt, die v mit w verbindet.

Eine Kantenfolge $e_1, e_2, \dots, e_k \in E(G)$ in einem Graphen G heißt **Kantenzug**, wenn alle Kanten e_j ($1 \leq j \leq k$) voneinander verschieden sind.

Eine Kantenfolge $e_1, e_2, \dots, e_k \in E(G)$ in einem Graphen G heißt **Weg** (in einem ungerichteten Graphen) bzw. **Bahn** (in einem gerichteten Graphen), wenn alle Knoten, die durch die Kantenfolge $e_1, e_2, \dots, e_k$ durchlaufen werden, voneinander verschieden sind.

Eine Kantenfolge, die einen Knoten $v \in V(G)$ mit sich selbst verbindet, heißt **geschlossen**.

Eine geschlossene Kantenfolge in einem ungerichteten Graphen heißt **Kreis**, wenn alle Knoten dieser Kantenfolge mit Ausnahme von v , der gleichzeitig Anfangs- und Endknoten ist, voneinander verschieden sind und keine Kante mehrfach vorkommt. (Der Zusatz, dass keine Kante mehrfach vorkommt, ist nur notwendig, um die Kantenfolge $e_1 = vv_1, e_2 = v_1v$ auszuschließen.) Eine geschlossene Kantenfolge in einem gerichteten Graphen heißt **Zyklus**, wenn alle Knoten dieser Kantenfolge mit Ausnahme von v voneinander verschieden sind.

Satz 2.16 Werden in einem Graphen G zwei verschiedene Knoten v, w durch eine Kantenfolge verbunden, so gibt es auch einen Weg (bzw. eine Bahn), der (die) v mit w verbindet und nur Kanten aus der ursprünglichen Kantenfolge enthält.

Satz 2.17 Gibt es in einem ungerichteten Graphen G zwei verschiedene Knoten v, w und zwei verschiedene Wege, die diese Knoten verbinden, dann gibt es einen Kreis positiver Länge, der nur Kanten aus diesen beiden Wegen enthält.

Gibt es in einem gerichteten Graphen G eine geschlossene Kantenfolge positiver Länge, so gibt es auch einen Zyklus positiver Länge, der nur Kanten aus der ursprünglichen geschlossenen Kantenfolge enthält.

Definition 2.18 Sei G ein Graph mit Knotenmenge $V(G) = \{v_1, v_2, \dots, v_n\}$. Die **Adjazenzmatrix** $A(G) = (a_{ij})$ ist eine quadratische $n \times n$ -Matrix mit

$$a_{ij} = \begin{cases} 1 & \text{für } (v_i, v_j) \in E(G) \text{ bzw. } v_i v_j \in E(G), \\ 0 & \text{sonst.} \end{cases}$$

Man beachte, dass die Adjazenzmatrix eines ungerichteten Graphen immer symmetrisch ist, also $a_{ij} = a_{ji}$. Schlingen äußern sich in der Adjazenzmatrix durch Einträge $a_{ii} = 1$ in der Diagonalen. Schlichte ungerichtete Graphen haben daher eine symmetrische Adjazenzmatrix mit verschwindender Diagonale $a_{ii} = 0$. Es ist auch sinnvoll, Graphen mit Mehrfachkanten eine Adjazenzmatrix zuzuordnen, wo a_{ij} die Anzahl der Kanten von v_i nach v_j bezeichnet.

Mit Hilfe der Adjazenzmatrix $A(G)$ eines Graphen lassen sich die Knotengrade ablesen. Ist G schlicht und ungerichtet, so gilt

$$d(v_i) = \sum_{j=1}^n a_{ij} = \sum_{j=1}^n a_{ji}.$$

Ist G gerichtet, so gilt entsprechend

$$d^+(v_i) = \sum_{j=1}^n a_{ij} \quad \text{und} \quad d^-(v_i) = \sum_{j=1}^n a_{ji}.$$

Weiters kann mit Hilfe der Potenzen der Adjazenzmatrix (vergleiche mit Definition 3.22) die Erreichbarkeit beschrieben werden. Ist nämlich $a_{ij}^{[k]}$ die Anzahl der Kantenfolgen der Länge k von v_i nach v_j , so ist (siehe Übungsaufgabe 3.13)

$$A(G)^k = (a_{ij}^{[k]}),$$

d.h., ist das (i, j) -te Element der k -ten Potenz von $A(G)$ positiv, so gibt es eine Kantenfolge von v_i nach v_j . In diesem Fall folgt nach Satz 2.16, dass es auch einen Weg (bzw. eine Bahn) von v_i nach v_j gibt. Die Länge eines Weges (bzw. einer Bahn) kann aber nicht länger als $|E|$ bzw. $|V| - 1$ sein. Berechnet man also

$$C = (c_{ij}) = \sum_{k=0}^m A(G)^k \quad \text{mit} \quad m = \min\{|E(G)|, |V(G)| - 1\},$$

so ist v_j von v_i genau dann erreichbar, wenn $c_{ij} > 0$ ist.

Definition 2.20 Ein ungerichteter Graph G heißt **zusammenhängend**, wenn es zwischen je zwei Knoten $v, w \in V(G)$ eine Kantenfolge von v nach w gibt. Die maximalen zusammenhängenden Teilgraphen eines ungerichteten Graphen G heißen (**Zusammenhangs-)** **Komponenten** von G .

Ein Graph G ist daher genau dann zusammenhängend, wenn er nur aus einer Zusammenhangskomponente besteht.

Definition 2.21 Ein gerichteter Graph G heißt **stark zusammenhängend**, wenn für je zwei verschiedene Knoten $v, w \in V(G)$ eine (gerichtete) Kantenfolge von v nach w existiert. Ein gerichteter Graph G heißt **schwach zusammenhängend**, wenn für je zwei verschiedene Knoten $v, w \in V(G)$ eine Folge von Kanten existiert, die bei Missachtung der Richtung der Kanten v und w verbindet.

Die maximalen stark zusammenhängenden Teilgraphen eines gerichteten Graphen G heißen **starke Zusammenhangskomponenten** oder **Komponenten des starken Zusammenhangs** von G . Entsprechend heißen die maximalen schwach zusammenhängenden Teilgraphen eines gerichteten Graphen G **schwache Zusammenhangskomponenten** oder **Komponenten des schwachen Zusammenhangs** von G .

Mit Hilfe der Potenzen $A(G)^k$ der Adjazenzmatrix $A(G)$ kann man – wie oben ausgeführt wurde – berechnen, wieviele verschiedenen Kantenfolgen (der Länge k) es zwischen zwei Knoten eines Graphen G gibt. Bei Kantenfolgen dürfen aber Kanten mehrfach verwendet werden. Ein anderes Problem ist es, die Anzahl der verschiedenen Wege zwischen zwei Knoten zu bestimmen, oder noch mehr, die maximale Anzahl von kantendisjunkten Wegen zwischen zwei Knoten zu bestimmen. Die Antwort auf diese Frage wird vom **Satz von Menger** gelöst.

Satz 2.22 Sei G ein ungerichteter Graph und v, w zwei verschiedene Knoten. Dann ist die maximale Anzahl von kantendisjunkten Wegen, die v und w verbinden gleich der minimalen Anzahl von Kanten, die man aus G entfernen muss, um v und w in G zu trennen.

2. Bäume, Wälder und azyklische Graphen

Definition 2.23 Ein schlichter ungerichteter Graph W , der keine Kreise positiver Länge enthält, heißt **Wald**. Ein Wald T , der auch zusammenhängend ist, heißt **Baum**.

Offensichtlich sind die Zusammenhangskomponenten eines Waldes Bäume. Man beachte, dass es in einem Baum T zu je zwei Knoten v, w genau einen Weg von v nach w gibt. Da T zusammenhängend ist, muss es einen Weg von v nach w geben. Gäbe es aber einen weiteren Weg, so müsste es (wegen Satz 2.17) auch einen Kreis positiver Länge geben, was aber definitionsgemäß ausgeschlossen ist. Die Länge dieses Weges bezeichnet man als den **Abstand** $d_T(v, w)$ zwischen den Knoten v und w .

Satz 2.24 Für einen Baum T gilt

$$\alpha_0(T) = \alpha_1(T) + 1. \quad (2.10)$$

Entsprechend gilt für einen Wald W mit k Komponenten

$$\alpha_0(W) = \alpha_1(W) + k. \quad (2.11)$$

Beweis. Es genügt, die Beziehung (2.10) für einen Baum zu zeigen. Bei einem Wald gilt (2.10) dann für jede der k Komponenten, und (2.11) folgt durch Summation.

Der Nachweis von (2.10) erfolgt nun mit vollständiger Induktion über die Anzahl $n = \alpha_0(T)$ der Knoten von T . Offensichtlich gilt (2.10) für $n = 1$. Man nehme nun an, dass (2.10) für alle Bäume mit n Knoten gilt. Ist nun T ein Baum mit $\alpha_0(T) = n + 1$ Knoten, so hat T sicher einen Knoten v mit Knotengrad $d(v) = 1$, einen so genannten „Endknoten“ (vergleiche mit Übungsaufgabe 2.24). Entfernt man diesen Knoten v gemeinsam mit der einzigen Kante, die von v wegführt, so erhält man wieder einen Baum T' mit $\alpha_0(T') = \alpha_0(T) - 1 = n$ und $\alpha_1(T') = \alpha_1(T) - 1$. (Man beachte, dass T' wieder zusammenhängend ist.) Aus der Induktionsvoraussetzung folgt $\alpha_0(T') = \alpha_1(T') + 1$ und damit $\alpha_0(T) = \alpha_0(T') + 1 = \alpha_1(T') + 2 = \alpha_1(T) + 1$. $\square$

Zeichnet man in einem Baum einen Knoten $w \in V(T)$ als so genannte **Wurzel** aus, so kann man sich die Struktur eines Baumes sehr einfach verdeutlichen. Platziert man in einer graphischen Darstellung die **Nachbarn von w oberhalb von w** und deren **Nachbarn** (mit der Ausnahme w) **wieder darüber**, usw., so entsteht tatsächlich ein Bild, das einem „Baum“ ähnelt (vergleiche mit Abb. 2.8). Man beachte, dass hier tatsächlich von **jedem Knoten in neue Knoten** verzweigt wird, da ein Baum definitionsgemäß kreisfrei ist. Manchmal wird ein Wurzelbaum auch als **gerichteter Graph** interpretiert, in dem **alle Kanten von der Wurzel weg gerichtet** sind.

Wurzelbäume spielen in der Informatik eine große Rolle. So bilden z.B. die Ordner auf der Festplatte in einem Computer einen Wurzelbaum. Man unterscheidet in Wurzelbäumen zwischen **externen Knoten** (die auch **Blätter** oder **Endknoten** genannt werden), das sind Knoten vom **Knotengrad 1**, und **internen Knoten**. (Die Wurzel betrachtet man als **externen Knoten**, wenn sie **Grad 0** hat, sonst zählt sie zu den internen Knoten.) Diese Unterscheidung ist insbesondere bei so genannten **Binärbäumen** von Bedeutung, die z.B. als Datenstrukturen (binäre oder digitale Suchbäume, TRIES etc.) auftreten. Bei **Binärbäumen** haben alle Knoten (mit Ausnahme der Wurzel) **Knotengrad 1 oder 3**, die **Wurzel hat Knotengrad 2** (bzw. 0, wenn der Baum nur aus der Wurzel besteht). Ein interner Knoten v hat daher Knotengrad 3, jener Nachbarknoten, der auf der Verbindung zur Wurzel liegt, heißt **Vorgänger** von v , und die beiden anderen Nachbarknoten heißen **Nachfolger** von v , wobei die „**Links-Rechts-Reihenfolge**“ der beiden

Nachfolger eine Rolle spielt; vergleiche auch mit Abb. 2.8, wo die externen Knoten eines Binärbaums durch $\square$ und die internen Knoten durch $\circ$ dargestellt werden.

Verlangt man bei gerichteten Graphen, dass es **keine Zyklen (positiver Länge)** gibt, so führt dies zu so genannten **azyklischen Graphen**:

Definition 2.25 Ein gerichteter Graph $G = (V, E)$ heißt **azyklisch** wenn er **keine Zyklen positiver Länge** enthält.

Wie das Beispiel in Abbildung 2.9 zeigt, unterscheiden sich azyklische Graphen deutlich von Bäumen oder Wäldern. Allerdings ist es sehr leicht, algorithmisch zu entscheiden, ob ein azy-

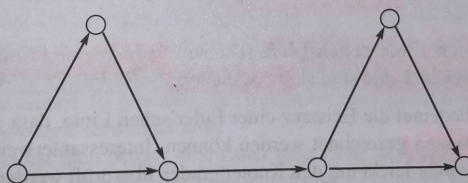


Abbildung 2.9 Azyklischer Graph

klischer Graph vorliegt oder nicht. Der Grund dafür ist die folgende Eigenschaft:

Satz 2.26 Jeder azyklische Graph G besitzt einen Knoten $v \in V(G)$ mit **Weggrad $d^+(v) = 0$** (und entsprechend auch einen Knoten $w \in V(G)$ mit **Hingrad $d^-(w) = 0$**).

Beweis. In einem azyklischen Graphen ist jede (gerichtete) Kantenfolge eine **beschränkte Länge**. Dann wenn eine Kantenfolge immer wieder verlängert werden könnte, würde man irgendwann einen Knoten ein zweites Mal erreichen und erhielte eine **Zyklus**. Es gibt daher eine Kantenfolge **maximaler Länge**. Der Endknoten v dieser Kantenfolge muss dann **Weggrad $d^+(v) = 0$** haben, entsprechend der **Anfangsknoten w Hingrad $d^-(w) = 0$** . $\square$

Findet man beispielsweise keinen Knoten v mit $d^+(v) = 0$, so ist der Graph sicher nicht azyklisch. Andernfalls kann man Knoten v mit $d^+(v) = 0$ aus dem Graphen entfernen und erhält einen kleineren Graphen, der genau dann azyklisch ist, wenn der ursprüngliche Graph azyklisch ist. Nun führt man dies iterativ durch. Wenn schließlich alle Knoten entfernt werden,

Graph azyklisch ist oder nicht. Man beachte, dass anstelle des Entferns die entsprechenden Knoten markiert werden:

1. (a) Bestimme alle Knoten v mit Weggrad $d^+(v) = 0$ und markiere diese mit $\oplus$.
 (b) Wurde in 1.(a) kein solcher Knoten gefunden, so ist G **nicht azyklisch** $\rightarrow$ ENDE.
2. (a) Sind bereits alle Knoten von G mit $\oplus$ markiert, so ist G **azyklisch** $\rightarrow$ ENDE.
 (b) Suche (unmarkierte) Knoten, von denen nur Kanten zu schon markierten führen und markiere diese mit $\oplus$.
3. (a) Wurde in 2.(b) mindestens ein Knoten markiert, so wiederhole 2.
 (b) Wurde in 2.(b) kein Knoten markiert, so ist G **nicht azyklisch** $\rightarrow$ ENDE.

3. Euler'sche und Hamilton'sche Linien

Definition 2.27 Eine Kantenfolge in einem (gerichteten oder ungerichteten) Graphen G heißt **Euler'sche Linie**, wenn sie jeden Knoten und jede Kante enthält, und zwar jede Kante genau einmal. Ein Graph wird als **Euler'scher Graph** bezeichnet, wenn er eine Euler'sche Linie besitzt.

Bei einer **geschlossenen Euler'schen Linie** stimmen Anfangs- und Endknoten überein, bei einer **offenen Euler'schen Linie** sind sie verschieden.

Grob gesprochen bedeutet die Existenz einer Euler'schen Linie, dass die Kanten von G , in einem Zug "ohne Absetzen" gezeichnet werden können. Interessanterweise kann die Existenz einer Euler'schen Linie sehr leicht mit den Knotengraden überprüft werden. Es ist also möglich, durch eine „lokale Bedingung“ eine „globale Eigenschaft“ zu erhalten.

Satz 2.28 Ein ungerichteter Graph G besitzt genau dann eine geschlossene Euler'sche Linie, wenn G zusammenhängend ist und alle Knotengrade $d(v)$ ($v \in V(G)$) gerade sind.

Ein ungerichteter Graph G besitzt genau dann eine offene Euler'sche Linie, wenn G zusammenhängend ist und mit der Ausnahme von zwei Knoten $w_1, w_2 \in V(G)$ mit ungeradem Knotengrad alle übrigen Knotengrade $d(v)$ ($v \in V(G) \setminus \{w_1, w_2\}$) gerade sind.

Satz 2.29 Ein gerichteter Graph G besitzt genau dann eine geschlossene Euler'sche Linie, wenn G schwach zusammenhängend ist und für alle Knoten $v \in V(G)$ Hin- und Weggrad gleich sind: $d^+(v) = d^-(v)$.

Ein gerichteter Graph G besitzt genau dann eine offene Euler'sche Linie, wenn G schwach zusammenhängend ist und mit der Ausnahme von zwei Knoten $w_1, w_2 \in V(G)$, für die $d^+(w_1) = d^-(w_1) + 1$ und $d^+(w_2) = d^-(w_2) - 1$ gilt, bei allen übrigen Knoten $v \in V(G) \setminus \{w_1, w_2\}$ Hin- und Weggrad gleich sind: $d^+(v) = d^-(v)$.

Definition 2.30 Eine Kantenfolge in einem (gerichteten oder ungerichteten) Graphen G heißt **Hamilton'sche Linie**, wenn sie jeden Knoten (mit der möglichen Ausnahme, dass Anfangs- und Endpunkt übereinstimmen) genau einmal enthält. Ein Graph wird als **Hamilton'scher Graph** bezeichnet, wenn er eine Hamilton'sche Linie besitzt.

Bei einer **geschlossenen Hamilton'schen Linie** stimmen Anfangs- und Endknoten überein, bei einer **offenen Hamilton'schen Linie** sind sie verschieden.

Im Gegensatz zu den Euler'schen Linien gibt es (bis heute) noch kein allgemeines Kriterium für die Existenz von Hamilton'schen Linien. Es gibt aber viele Sätze, die hinreichende Bedingungen für die Existenz einer Hamilton'schen Linie angeben. Als Beispiel dafür sei der folgende Satz (ohne Beweis) angegeben.

Satz 2.31 Sei G ein schlichter ungerichteter Graph mit n Knoten, so dass für alle Knotenpaare $x, y \in V(G)$, die in G nicht durch eine Kante verbunden sind, d.h. $(x, y) \notin E(G)$,

$$d(x) + d(y) \geq n$$

gilt. Dann gibt es in G eine geschlossene Hamilton'sche Linie.

Planare Graphen:

4. Planare Graphen

Definition 2.32 Ein Graph G heißt **planar** oder **eben**, wenn G kreuzungsfrei in der Ebene $\mathbb{R}^2$ dargestellt werden kann, d.h. die **Kurven**, die die **Kanten** repräsentieren, haben außer in jenen **Punkten**, die die **Knoten** repräsentieren, **keine weiteren Schnittpunkte**.

Satz 2.33 (Eulersche Polyederformel) Für einen zusammenhängenden planaren Graphen G gilt

$$\alpha_0(G) - \alpha_1(G) + \alpha_2(G) = 2. \quad (2.12)$$

Beweis: Man wähle

$$\alpha_0(P) - \alpha_1(P) + \alpha_2(P) = 2,$$

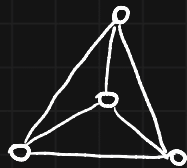
wobei $\alpha_0(P)$ die Anzahl der **Eckpunkte**, $\alpha_1(P)$ die Anzahl der **Kanten** und $\alpha_2(P)$ die Anzahl der **Flächen** des Polyeders P bezeichnen.

Aus der eben geführten Überlegung ergibt sich auch die folgende Eigenschaft.

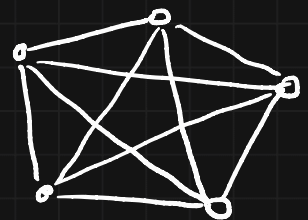
Satz 2.34 Ein Graph lässt sich genau dann kreuzungsfrei in der Ebene darstellen, wenn er **kreuzungsfrei auf einer Kugeloberfläche darstellbar** ist.

Satz 2.35 (Satz von Kuratowski) Ein Graph G ist genau dann **nicht planar**, wenn er einen **Teilgraphen** enthält, der aus **K_5 oder $K_{3,3}$** durch eventuelle Unterteilung (von Kanten) entsteht. (Dabei ist eine Unterteilung ein Graph, der aus G dadurch hervorgeht, dass in einer oder in mehreren Kanten von G zusätzliche Knoten eingefügt werden.)

Planarer Graph:



Nicht planarer Graph:



sind. Beispielsweise ist eine zulässige Färbung eine Färbung, bei der so dass benachbarte Knoten verschiedene Farben haben. Die **chromatische Zahl** $\chi(G)$ eines Graphen ist dann die **minimale Anzahl von Farben**, die benötigt wird, um die Knoten eines Graphen zulässig zu färben. Beispielsweise ist $\chi(K_n) = n$. Im Allgemeinen ist es außerordentlich schwer, die chromatische Zahl eines Graphen zu bestimmen.

Für planare Graphen gilt allerdings der **Vierfarbensatz**.

Satz 2.36 Für planare Graphen G gilt $\chi(G) \leq 4$.

Netzwerke sind gerichtete oder ungerichtete Graphen $G = (V, E)$, wo jeder Kante $e \in E$ ein **Wert** $w(e) \in \mathbb{R}$ zugeordnet wird. Dieser Wert kann je nach Anwendung als Länge, Kosten, Kapazität, Gewicht etc. gedeutet werden. Netzwerke spielen gerade in den Anwendungen der

Definition 2.37 Ein **spannender Baum** T eines schlichten ungerichteten zusammenhängenden Graphen G ist ein Baum mit $V(T) = V(G)$ und $E(T) \subseteq E(G)$, d.h. er enthält dieselben Knoten wie G und gewisse Kanten von G .

Ein **Gerüst** oder **spannender Wald** W eines schlichten ungerichteten Graphen G ist ein Wald mit $V(W) = V(G)$ und $E(W) \subseteq E(G)$ und denselben Zusammenhangskomponenten wie G , d.h., schränkt man W auf eine Zusammenhangskomponente K von G ein, so ist diese Einschränkung ein spannender Baum von K .

Ist G ein bewerteter Graph, so bezeichnet man ein Gerüst W als **minimales Gerüst**, wenn die Summe aller Kantengewichte des Gerüsts

$$w(W) = \sum_{e \in E(W)} w(e)$$

unter allen möglichen Gerüsten von G kleinstmöglich ist.

Ein Graph hat üblicherweise sehr viele verschiedene Gerüste. Beispielsweise hat der so genannte **vollständige Graph** K_n aus n Knoten und allen möglichen $n(n-1)/2$ Kanten n^{n-2}

Dijkstra-Algorithmus:

1. Man setze $l(v_0) = 0$, $l(v) := \infty$ für alle $v \in V \setminus \{v_0\}$, $U = \{v_0\}$ und $u = v_0$.
2. Für alle $v \in V \setminus U$ mit $(u, v) \in E$, die $l(v) > l(u) + w(u, v)$ erfüllen, setze man $p(v) := u$ und

$$l(v) := l(u) + w(u, v).$$

3. Man bestimme $m = \min_{v \in V \setminus U} l(v)$. Falls $m = \infty$, dann terminiere, andernfalls wähle einen Knoten $z \in V \setminus U$ mit $l(z) = m$ und setze $U := U \cup \{z\}$ und $u := z$.
4. Ist $U = V$, so wird der Algorithmus beendet. Andernfalls gehe zu Schritt 2.

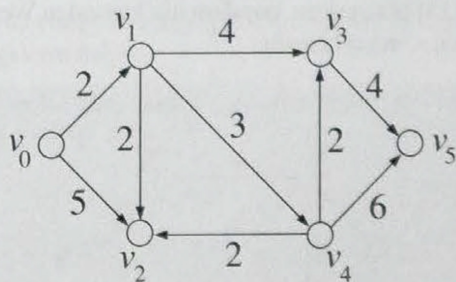


Abbildung 2.17 Netzwerk zum Dijkstra-Algorithmus

Im ersten Durchlauf des Algorithmus werden folgende Operationen durchgeführt:

1. $l(v_0) = 0$ und $l(v_1) = l(v_2) = l(v_3) = l(v_4) = l(v_5) = \infty$, $U = \{v_0\}$ und $u = v_0$.
2. $l(v_1) = \min\{\infty, 0 + 2\} = 2$, $p(v_1) = v_0$; $l(v_2) = \min\{\infty, 0 + 5\} = 5$, $p(v_2) = v_0$.
3. $m = 2$, $z = v_1$, $U = \{v_0, v_1\}$, $u = v_1$.
4. Fortsetzung bei Schritt 2.

	v_0	v_1	v_2	v_3	v_4	v_5	Auswahl	Vorgänger
0	0	∞	∞	∞	∞	∞	v_0	
1		2	5	∞	∞	∞	v_1	v_0
2			4	6	5	∞	v_2	v_1
3				6	5	∞	v_4	v_1
4				6		11	v_3	v_1
5						10	v_5	v_3

Da alle Distanzen $d(v_0, v)$ berechnet wurden, kann man auch den so genannten **Entfernungsbaum** (siehe Abb. 2.18) bestimmen, aus dem die kürzesten Wege bzw. Bahnen von v_0 zu allen Endknoten v abgelesen werden können. $\triangle$

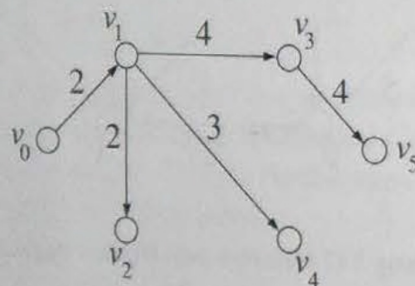


Abbildung 2.18 Entfernungsbaum bezüglich v_0 in einem Netzwerk

Algebraische Strukturen: Binäre Operatoren

Definition 2.40 Sei A eine nichtleere Menge. Eine **binäre Operation** $\circ$ auf A ist eine Abbildung $A \times A \rightarrow A$, d.h., je zwei Elementen $a, b \in A$ wird ein Element $a \circ b$ zugeordnet. Das Paar $(A, \circ)$ heißt dann **binäre algebraische Struktur** oder **Gruppoid**.

Definition 2.42 Die folgenden Gesetzmäßigkeiten können für eine algebraische Struktur $(A, \circ)$ zusätzlich definiert werden.

(i) **Assoziativgesetz:** Für alle $a, b, c \in A$ gilt

$$(a \circ b) \circ c = a \circ (b \circ c).$$

(ii) **Existenz eines neutralen Elements:** Es gibt ein $e \in A$ mit der Eigenschaft, dass für alle $a \in A$ gilt

$$e \circ a = a \circ e = a.$$

(iii) **Existenz inverser Elemente:** Für alle $a \in A$ gibt es ein $a' \in A$ mit

$$a \circ a' = a' \circ a = e,$$

wobei e das neutrale Element aus (ii) bezeichnet.

(iv) **Kommutativgesetz:** Für alle $a, b \in A$ gilt

$$a \circ b = b \circ a.$$

Benutzt man für das binäre Operationssymbol das **Malzeichen** $\cdot$, so schreibt man für das inverse Element von a auch a^{-1} , verwendet man hingegen das **Pluszeichen** $+$, so bezeichnet man das inverse Element von a durch $-a$.

Satz 2.44 In einer algebraischen Struktur $(A, \circ)$ gibt es **höchstens ein neutrales Element**, und in jeder assoziativen algebraischen Struktur gibt es zu jedem Element **höchstens ein inverses Element**.

Definition 2.45 Eine algebraische Struktur $(A, \circ)$ heißt

- (i) **Halbgruppe**, wenn sie assoziativ ist, also (i) aus Definition 2.42 erfüllt,
- (ii) **Monoid**, wenn sie assoziativ ist und ein **neutrales Element** besitzt, also (i) und (ii) aus Definition 2.42 erfüllt, und
- (iii) **Gruppe**, wenn sie assoziativ ist, ein **neutrales Element** und zu jedem Element ein **Inverses** besitzt, also (i), (ii) und (iii) aus Definition 2.42 erfüllt.

Erfüllt eine der Strukturen Gruppoid, Halbgruppe, Monoid bzw. Gruppe auch das **Kommutativgesetz (iv)**, so heißt sie **kommutative(s) Gruppoid, Halbgruppe, Monoid bzw. Gruppe**.

Kommutative Gruppen werden auch als **abelsche Gruppen**⁴ bezeichnet.

Definition 2.50 Eine (nichtleere) Teilmenge $U \subseteq G$ einer Gruppe $(G, \circ)$ heißt **Untergruppe** von G , wenn $(U, \circ)$ selbst eine Gruppe ist. Man schreibt dafür auch $(U, \circ) \leq (G, \circ)$ oder nur $U \leq G$.

Man beachte, dass es **immer zwei so genannte triviale Untergruppen** gibt: $\{e\} \leq G$ und $G \leq G$.

Definition 2.52 Sei $(G, \circ)$ Gruppe, U Untergruppe von G und $a \in G$. Dann heißt

$$a \circ U = \{a \circ u \mid u \in U\}$$

Linksnebenklasse von U in G und

$$U \circ a = \{u \circ a \mid u \in U\}$$

Rechtsnebenklasse von U in G .

Analoges gilt für die Rechtsnebenklassen. Wir werden uns gleich davon überzeugen, dass es **immer gleich viele Links- wie Rechtsnebenklassen** gibt. So können wir den **Index einer Untergruppe** definieren.

Definition 2.53 Sei $(G, \circ)$ eine endliche Gruppe und $U \leq G$. Die **Anzahl der Links- bzw. Rechtsnebenklassen** von U in G wird als **Index** $|G : U|$ von G nach U bezeichnet. Die **Anzahl** $|G|$ der Elemente einer Gruppe wird als **Ordnung** von G bezeichnet.

Satz 2.54 (Satz von Lagrange) Ist $(G, \circ)$ endliche Gruppe, so ist die **Ordnung** $|U|$ einer Untergruppe $U \leq G$ stets **Teiler der Gruppenordnung** $|G|$, und es gilt $|G : U| = |G|/|U|$.

Definition 2.55 Sei $(G, \circ)$ Gruppe mit neutralem Element e . Für $a \in G$ werden die **Potenzen** a^n von a mit $n \in \mathbb{Z}$ folgendermaßen definiert:

$$a^n = \begin{cases} e & \text{für } n = 0, \\ a & \text{für } n = 1, \\ a^{n-1} \circ a & \text{rekursiv für } n > 1, \\ (a^{-1})^{-n} & \text{für } n < 0. \end{cases}$$

$$a^{n+m} = a^n \circ a^m \quad \text{und} \quad (a^m)^n = a^{mn}.$$

mit $a^k = e$. Dies motiviert die folgende Definition.

Definition 2.56 Sei $(G, \circ)$ Gruppe und $a \in G$. Sind alle Potenzen a^n ($n \in \mathbb{Z}$) voneinander verschieden, so hat a **unendliche Ordnung** $\text{ord}_G(a) = \infty$. Andernfalls bezeichnet man

$$\text{ord}_G(a) = \min\{k > 0 \mid a^k = e\}$$

als **Ordnung** von a . Das Element a hat dann **endliche Ordnung**.

Satz 2.57 (Kleiner Fermat'scher Satz) Für jedes Element $a \in G$ einer **endlichen Gruppe** $(G, \circ)$ gilt $a^{|G|} = e$.

Definition 2.58 Eine **Untergruppe** N einer Gruppe G heißt **Normalteiler**, wenn die **Links- und Rechtsnebenklassen** übereinstimmen. Man schreibt dafür kurz $N \trianglelefteq G$.

Offensichtlich ist jede Untergruppe einer kommutativen Gruppe G ein Normalteiler. Weiters ist jede Untergruppe N mit Index $|G : N| = 2$ Normalteiler, da es in diesem Fall nur zwei Links- bzw. Rechtsnebenklassen gibt.

Definition 2.59 Sei N Normalteiler einer Gruppe G und bezeichne G/N die Menge der Nebenklassen von G nach N . Dann wird durch die Operation

$$(a \circ N) \circ (b \circ N) = (a \circ b) \circ N$$

eine Gruppenoperation auf G/N definiert. Die Gruppe $(G/N, \circ)$ heißt **Faktorgruppe** von G nach N .

Definition 2.61 Eine Abbildung $\varphi : G \rightarrow H$ zwischen zwei Gruppen $(G, \circ)$ und $(H, \star)$ heißt **Homomorphismus** (oder **Gruppenhomomorphismus**), wenn für alle $a, b \in G$ gilt

$$\varphi(a \circ b) = \varphi(a) \star \varphi(b).$$

Ist φ bijektiv, so heißt φ **Isomorphismus**. Die inverse Abbildung $\varphi^{-1} : H \rightarrow G$ ist dann auch ein Isomorphismus. Existiert zwischen zwei Gruppen G, H ein Isomorphismus, so heißen G und H **isomorph**, und man schreibt dafür $G \cong H$.

Satz 2.63 Ist $\varphi : G \rightarrow H$ ein Gruppenhomomorphismus, so wird das neutrale Element e_G von G auf das neutrale Element e_H von H abgebildet, d.h. $\varphi(e_G) = e_H$. Weiters gilt $\varphi(a^{-1}) = \varphi(a)^{-1}$ für alle $a \in G$.

Definition 2.64 Sei $\varphi : G \rightarrow H$ ein Gruppenhomomorphismus. Das Urbild $\varphi^{-1}(\{e_H\})$ des neutralen Elements e_H wird als **Kern** von φ bezeichnet:

$$\ker(\varphi) = \{a \in G \mid \varphi(a) = e_H\}.$$

Weiters nennt man

$$\varphi(G) = \{b \in H \mid \exists a \in G : \varphi(a) = b\}$$

Bild von G unter φ .

Satz 2.65 Sei $\varphi : G \rightarrow H$ ein Gruppenhomomorphismus. Dann ist $\ker(\varphi)$ ein Normalteiler von G und $\varphi(G)$ eine Untergruppe von H .

Satz 2.66 (Homomorphiesatz) Sei $\varphi : G \rightarrow H$ ein Gruppenhomomorphismus. Dann ist die Faktorgruppe $G/\ker(\varphi)$ zum Bild $\varphi(G)$ isomorph:

$$G/\ker(\varphi) \cong \varphi(G).$$

Die Nebenklasse $a \circ \ker(\varphi) \in G/\ker(\varphi)$ entspricht dem Element $\varphi(a) \in \varphi(G)$.

Wir betrachten wieder die symmetrische Gruppe S_n aller $n!$ Permutationen der Zahlen $\{1, 2, \dots, n\}$, also alle bijektiven Funktionen $\pi : \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}$. Es gibt verschiedene Darstellungen von Permutationen. Üblich ist vor allem die **zweizeilige Darstellung**. Hier wird $\pi \in S_n$ durch eine zweizeilige Matrix

$$\pi = \begin{pmatrix} 1 & 2 & 3 & \dots & n-1 & n \\ \pi(1) & \pi(2) & \pi(3) & \dots & \pi(n-1) & \pi(n) \end{pmatrix}$$

dargestellt, also z.B. durch

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix}.$$

$$\pi^{-1} = \begin{pmatrix} 3 & 5 & 4 & 1 & 2 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 3 & 2 \end{pmatrix}.$$

Ist $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 1 & 3 \end{pmatrix}$ eine weitere Permutation, so bestimmt sich

$$\sigma \circ \pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 1 & 4 & 2 \end{pmatrix},$$

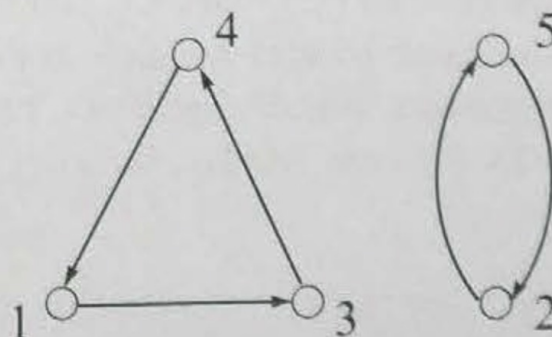


Abbildung 2.19 Grafische Darstellung einer Permutation

In den ganzen Zahlen $\mathbb{Z}$ verwendet man (wenigstens) zwei verschiedene binäre Operationen, die Addition und die Multiplikation. Bezüglich der Addition ist $\mathbb{Z}$ eine Gruppe und bezüglich der Multiplikation ein Monoid. Man erfasst aber die Struktur der ganzen Zahlen $\mathbb{Z}$ (bezüglich Addition und Multiplikation) nicht vollständig, wenn man die Strukturen $(\mathbb{Z}, +)$ und $(\mathbb{Z}, \cdot)$ nur getrennt betrachtet. Es gelten auch Rechenregeln wie das **Distributivgesetz**

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c),$$

wo Addition und Multiplikation gemeinsam auftreten.

Definition 2.68 Eine **algebraische Struktur** $(R, +, \cdot)$ mit zwei binären Operation heißt **Ring**, wenn die folgenden drei Eigenschaften erfüllt sind:

- (i) $(R, +)$ ist eine kommutative Gruppe (mit neutralem Element 0),
- (ii) $(R, \cdot)$ ist eine Halbgruppe, und
- (iii) es gelten die **Distributivgesetze**:

$$\begin{aligned} a \cdot (b + c) &= a \cdot b + a \cdot c \\ (a + b) \cdot c &= a \cdot c + b \cdot c \end{aligned} \quad \text{für alle } a, b, c \in R.$$

Besitzt R bezüglich $\cdot$ ein neutrales Element (siehe oben), so nennt man **R Ring mit Einselement**, und ist R bezüglich $\cdot$ kommutativ, so nennt man **R kommutativen Ring**.

Definition 2.71 Ein **kommutativer Ring** mit Einselement ohne Nullteiler heißt **Integritätsring**.

In einem beliebigen Ring R kann man stets durch Elemente $a \in R$ kürzen, die ein multiplikatives Inverses a^{-1} besitzen. Solche Elemente heißen auch **Einheiten**. Es ist direkt nachzurechnen, dass die Menge aller Einheiten R^* von R eine (multiplikative) Gruppe bildet, die so genannte **Einheitengruppe** von R . Beispielsweise ist $\mathbb{Z}^* = \{-1, 1\}$.

In Abschnitt 1.2 (siehe Satz 1.30) wurde bereits gezeigt, dass $\mathbb{Z}_m^*$ genau aus jenen Restklassen $\bar{a}$ besteht, welche die Eigenschaft $\text{ggT}(a, m) = 1$ erfüllen. Außerdem gilt $|\mathbb{Z}_m^*| = \varphi(m)$, wobei $\varphi(m)$ die Euler'sche φ -Funktion bezeichnet (siehe Definition 1.33). Man beachte insbesondere, dass für eine Primzahl $p \in \mathbb{P}$ die Beziehung $\varphi(p) = p - 1$ gilt, d.h., alle Elemente aus $\mathbb{Z}_p$ außer $\bar{0}$ sind Einheiten. Diese Beobachtung führt uns zu einer weiteren zentralen algebraischen Struktur.

Definition 2.73 Ein kommutativer Ring $(K, +, \cdot)$ mit Einselement $1 \neq 0$, in dem jedes Element $a \neq 0$ eine Einheit ist, also ein multiplikatives Inverses besitzt, heißt ein **Körper**.

Eine algebraische Struktur $(K, +, \cdot)$ ist also genau dann ein Körper, wenn $(K, +)$ und $(K \setminus \{0\}, \cdot)$ kommutative Gruppen sind und die Distributivgesetze gelten.

Satz 2.75 Jeder Körper ist ein Integritätsring, und jeder endliche Integritätsring ist ein Körper.

gangspunkt ist die Division

Satz 2.77 Seien $a(x)$ und $b(x)$ zwei Polynome mit Koeffizienten aus einem Körper K , und sei $b(x) \neq 0$. Dann gibt es Polynome $q(x), r(x) \in K[x]$ mit

$$a(x) = b(x)q(x) + r(x),$$

wobei $r(x)$ entweder das Nullpolynom ist oder $\text{grad}(r(x)) < \text{grad}(b(x))$.

Satz 2.78 Sei K ein Körper, ferner sei $q(x) \in K[x]$ ein Polynom mit Koeffizienten aus K und $\text{grad}(q(x)) \geq 1$. Dann ist der Faktorring $(K[x]/q(x)K[x], +, \cdot)$ genau dann ein Körper, wenn das Polynom $q(x)$ irreduzibel über K ist, d.h., wenn $q(x)$ nicht als Produkt zweier Polynome $a(x), b(x) \in K[x]$ mit kleinerem Grad (als $q(x)$) dargestellt werden kann.

Definition 2.80 Eine algebraische Struktur $(M, \wedge, \vee)$ heißt **Verband**, wenn folgende Eigenschaften erfüllt sind:

- (i) $(M, \wedge)$ ist eine kommutative Halbgruppe,
- (ii) $(M, \vee)$ ist eine kommutative Halbgruppe, und
- (iii) es gelten die **Verschmelzungsgesetze**

$$a = a \wedge (a \vee b),$$

$$a = a \vee (a \wedge b)$$

für alle $a, b \in M$.

$$a \wedge a = a \wedge (a \vee (a \wedge b)) = a$$

und ebenso $a \vee a = a$.

Satz 2.83 Sei $(M, \wedge, \vee)$ ein Verband. Dann wird durch

$$a \leq b \iff a = a \wedge b$$

auf M eine Halbordnung definiert. In dieser Halbordnung gibt es zu je zwei Elementen ein **Infimum**, nämlich $\inf(a, b) = a \wedge b$, und ein **Supremum** $\sup(a, b) = a \vee b$.

Ist umgekehrt $\leq$ eine Halbordnung auf M mit der Eigenschaft, dass es zu je zwei Elementen ein Infimum und ein Supremum gibt, so ist M mit den Operationen $a \wedge b = \inf(a, b)$ und $a \vee b = \sup(a, b)$ ein Verband.

Definition 2.86 Ein Verband $(M, \wedge, \vee)$ heißt **distributiver Verband**, wenn die **Distributivgesetze**

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c),$$

$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$$

für alle $a, b, c \in M$ gelten.

Kapitel



Definition 2.88 Ein distributiver Verband $(M, \wedge, \vee)$ heißt **Boole'sche Algebra**, wenn er die folgenden beiden zusätzlichen Eigenschaften besitzt:

- (i) Es gibt ein neutrales Element $1 \in M$ bezüglich $\wedge$, und es gibt ein neutrales Element $0 \in M$ bezüglich $\vee$, d.h. $(M, \wedge)$ und $(M, \vee)$ sind Monoide.
- (ii) Zu jedem $a \in M$ gibt es ein Komplement $a' \in M$ mit

$$a \vee a' = 1 \quad \text{und} \quad a \wedge a' = 0.$$

Satz 2.89 Eine Boole'sche Algebra $(M, \wedge, \vee)$ hat die folgenden Eigenschaften:

- (i) Für alle $a \in M$ gilt $a \vee 1 = 1$ und $a \wedge 0 = 0$.
- (ii) Gelten für ein $b \in M$ die Beziehungen $a \vee b = 1$ und $a \wedge b = 0$, so ist $a' = b$.
- (iii) Für alle $a \in M$ gilt $(a')' = a$.
- (iv) Für alle $a, b \in M$ gelten die **DeMorgan'schen Regeln**

$$(a \wedge b)' = a' \vee b',$$

$$(a \vee b)' = a' \wedge b'.$$

Vektoren:

Ein (Spalten-)Vektor x im n -dimensionalen (reellen) Raum $\mathbb{R}^n$ hat die Form

$$x = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$$

$\mathbb{R}^2 = \left\{ x = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \mid x_1, x_2 \in \mathbb{R} \right\}$ und $\mathbb{R}^3 = \left\{ x = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \mid x_1, x_2, x_3 \in \mathbb{R} \right\}$
die Ebene und den 3-dimensionalen Anschauungsraum.

Zwei Vektoren $x, y \in K^n$ werden koordinatenweise addiert:

$$x + y = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} x_1 + y_1 \\ x_2 + y_2 \\ \vdots \\ x_n + y_n \end{pmatrix}.$$

Geometrisch entspricht die Vektoraddition der aus der Physik bekannten Parallelogrammregel für die Addition von Kräften (vergleiche mit Abb. 3.2).

Weiters können Vektoren mit einem beliebigen Faktor $\lambda \in K$ (also einem Skalar) multipliziert werden:

$$\lambda \cdot x = \lambda \cdot \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} \lambda x_1 \\ \lambda x_2 \\ \vdots \\ \lambda x_n \end{pmatrix}.$$

Spezielle Vektoren sind der Nullvektor 0 und der additiv inverse Vektor $-x$:

$$0 = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad -x = (-1) \cdot x = \begin{pmatrix} -x_1 \\ -x_2 \\ \vdots \\ -x_n \end{pmatrix}.$$

angewandt dann:

Definition 3.2 Sei K ein Körper und $(V, +)$ eine abelsche Gruppe. Weiters werde jedem $\lambda \in K$ und $x \in V$ ein Produkt $\lambda \cdot x \in V$ zugeordnet.

Die algebraische Struktur $(V, +, K)$ heißt **Vektorraum** oder **linearer Raum** über K , wenn die folgenden Eigenschaften (für alle $\lambda, \mu \in K$ und $x, y \in V$) erfüllt sind:

- (i) $\lambda \cdot (x + y) = \lambda \cdot x + \lambda \cdot y$,
- (ii) $(\lambda + \mu) \cdot x = \lambda \cdot x + \mu \cdot x$,
- (iii) $(\lambda \mu) \cdot x = \lambda \cdot (\mu \cdot x)$,
- (iv) $1 \cdot x = x$.

Definition 3.5 Sei $(V, +, K)$ ein Vektorraum und U eine nichtleere Teilmenge von V . Bildet $(U, +, K)$ wieder einen Vektorraum, dann heißt U **Unterraum** oder **Teilraum** von V .

106

Definition 3.6 Sei U ein Unterraum eines Vektorraums V und x_0 ein Vektor aus V . Die Menge

$$N = x_0 + U = \{x_0 + u \mid u \in U\}$$

heißt **Nebenraum** von U .

Definition 3.7 Es seien $v_1, v_2, \dots, v_n$ Elemente eines Vektorraums V (über dem Körper K) und $\lambda_1, \lambda_2, \dots, \lambda_n \in K$. Dann heißt die Summe

$$\lambda_1 \cdot v_1 + \lambda_2 \cdot v_2 + \dots + \lambda_n \cdot v_n = \sum_{i=1}^n \lambda_i \cdot v_i$$

Linearkombination der Vektoren $v_1, v_2, \dots, v_n$. Die Skalare $\lambda_1, \lambda_2, \dots, \lambda_n \in K$ heißen **Koeffizienten** der Linearkombination. Eine Linearkombination heißt **trivial**, wenn alle Koeffizienten $\lambda_i = 0$ sind ($1 \leq i \leq n$). Andernfalls heißt sie **nichttrivial**.

Die **lineare Hülle** $[M]$ einer nichtleeren Teilmenge M von V ist die Menge aller Vektoren, die durch Linearkombinationen von (endlich vielen) Vektoren aus M gebildet werden können. Weiters setzt man $[\emptyset] = \{0\}$.

Satz 3.8 Sei M eine Teilmenge eines Vektorraums V . Dann ist die lineare Hülle $[M]$ ein Unterraum von V , und zwar der (bezüglich der mengentheoretischen Inklusion) **kleinste Unterraum**, der alle Vektoren von M enthält.

linear unabhängig. Dieser Begriff

Definition 3.9 Eine Menge M von Vektoren heißt **linear unabhängig**, wenn kein Vektor aus M als Linearkombination der anderen Vektoren aus M dargestellt werden kann, also für alle $v \in M$ gilt

$$v \notin [M \setminus \{v\}].$$

Andererseits heißt eine Menge M von Vektoren **linear abhängig**, wenn es möglich ist, einen Vektor aus M als Linearkombination von anderen Vektoren aus M darzustellen, wenn es also einen Vektor $v \in M$ gibt mit

$$v \in [M \setminus \{v\}].$$

Beispiel 3.10 Die Vektoren (bzw. die Menge der Vektoren)

$$e_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, e_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \dots, e_n = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix} \in K^n$$

sind (ist) linear unabhängig. Beispielsweise ist bei jeder Linearkombination von $e_2, e_3, \dots, e_n$ die erste Koordinate 0, also kann e_1 nicht als Linearkombination von $e_2, e_3, \dots, e_n$ dargestellt werden.

Die Vektoren $e_1, e_2, \dots, e_n$ bilden auch die (so genannte) **kanonische Basis** $E = \{e_1, e_2, \dots, e_n\}$ von K^n . $\triangle$

Beispiel 3.11 Die drei Vektoren (und auch die Menge der drei Vektoren)

$$v_1 = \begin{pmatrix} 1 \\ 3 \\ 4 \end{pmatrix}, v_2 = \begin{pmatrix} 1 \\ 2 \\ 2 \end{pmatrix}, v_3 = \begin{pmatrix} -1 \\ 0 \\ 2 \end{pmatrix}$$

3.1 Vektoren

109

sind (ist) linear abhängig. Es gilt nämlich

$$v_3 = 2 \cdot v_1 - 3 \cdot v_2.$$

$\triangle$

Satz 3.12 Eine Menge $M = \{v_1, v_2, \dots, v_n\}$ von Elementen eines Vektorraums V ist genau dann linear unabhängig, wenn nur die triviale Linearkombination den Nullvektor darstellt:

$$\lambda_1 \cdot v_1 + \lambda_2 \cdot v_2 + \dots + \lambda_n \cdot v_n = 0 \implies \lambda_1 = \lambda_2 = \dots = \lambda_n = 0.$$

M ist genau dann linear abhängig, wenn es eine nichttriviale Linearkombination gibt, die den Nullvektor darstellt:

$$\exists (\lambda_1, \lambda_2, \dots, \lambda_n) \neq (0, 0, \dots, 0) \text{ mit } \lambda_1 \cdot v_1 + \lambda_2 \cdot v_2 + \dots + \lambda_n \cdot v_n = 0.$$

Man beachte, dass dieser Satz wortwörtlich auch für Listen von Vektoren gilt.

Beispiel 3.13 Wir möchten nochmals untersuchen, ob die drei Vektoren v_1, v_2, v_3 bzw. die Menge $M = \{v_1, v_2, v_3\}$ der Vektoren aus Beispiel 3.11 linear unabhängig oder linear abhängig sind. Dazu betrachten wir

$$\lambda_1 \cdot \begin{pmatrix} 1 \\ 3 \\ 4 \end{pmatrix} + \lambda_2 \cdot \begin{pmatrix} 1 \\ 2 \\ 2 \end{pmatrix} + \lambda_3 \cdot \begin{pmatrix} -1 \\ 0 \\ 2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

Anders angeschrieben ist dies ein lineares Gleichungssystem:

$$1\lambda_1 + 1\lambda_2 - 1\lambda_3 = 0,$$

$$3\lambda_1 + 2\lambda_2 + 0\lambda_3 = 0,$$

$$4\lambda_1 + 2\lambda_2 + 2\lambda_3 = 0.$$

Dieses Gleichungssystem hat z.B. die nichttriviale Lösung $\lambda_1 = 2, \lambda_2 = -3, \lambda_3 = -1$. Die Vektoren sind also (wie wir bereits aus Beispiel 3.11 wissen) linear abhängig. $\triangle$

Definition 3.15 Eine Teilmenge B eines Vektorraums V heißt **Basis** von V , wenn sie linear unabhängig ist und ihre lineare Hülle $[B]$ gleich V ist.

Jeder Vektor x aus V lässt sich eindeutig als Linearkombination von Vektoren der Basis darstellen. Die Koeffizienten dieser Linearkombination heißen **Koordinaten** von x bezüglich der Basis B .

Satz 3.16 (Austauschlemma) Es sei $M = \{v_1, v_2, \dots, v_n\}$ eine Menge von Vektoren und $a = \mu_1 \cdot v_1 + \dots + \mu_n \cdot v_n$ eine Linearkombination dieser Vektoren. Weiter sei $M' = (M \setminus \{v_j\}) \cup \{a\} = \{v_1, \dots, v_{j-1}, a, v_{j+1}, \dots, v_n\}$ für ein j mit $\mu_j \neq 0$. Dann ist M genau dann linear unabhängig, wenn M' linear unabhängig ist, und es gilt immer $[M'] = [M]$.

begründet den Begriff der Dimension

Definition 3.17 Besitzt ein Vektorraum V eine endliche Basis B , so ist die **Dimension** $\dim V$ gleich der Anzahl $|B|$ der Vektoren von B . Besitzt V keine endliche Basis, so heißt er **unendlichdimensional**.

Matrizen:

Definition 3.20 Unter einer $m \times n$ -Matrix $A = (a_{ij})$ mit Koeffizienten aus einem Körper K versteht man ein rechteckiges Schema

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

aus m Zeilen und n Spalten mit Eintragungen $a_{ij} \in K$. Die Menge aller $m \times n$ -Matrizen mit Eintragungen aus K wird mit $K^{m \times n}$ bezeichnet. Eine Matrix $A \in K^{n \times n}$ mit gleicher Spalten- und Zeilenanzahl heißt **quadratisch**.

Definition 3.21 Ist $A \in K^{m \times n}$ eine $m \times n$ -Matrix, so bezeichnen wir mit A^T die zu A **transponierte Matrix**. Sie ist eine $n \times m$ -Matrix und geht aus A dadurch hervor, dass Zeilen und Spalten vertauscht werden, d.h., die erste Spalte von A ist die erste Zeile von A^T , usw.

Eine quadratische Matrix $A = (a_{ij}) \in K^{n \times n}$ heißt **symmetrisch**, wenn

$$A^T = A$$

ist, d.h., wenn $a_{ij} = a_{ji}$ für alle $1 \leq i, j \leq n$ gilt.

Beispielsweise ist

$$A_2^T = \begin{pmatrix} 1 & 2 \\ 5 & 7 \\ 0 & 2 \end{pmatrix}^T = \begin{pmatrix} 1 & 5 & 0 \\ 2 & 7 & 2 \end{pmatrix},$$

Symmetrisch

Definition 3.22 Sind $A = (a_{ij}) \in K^{m \times n}$ und $B = (b_{jk}) \in K^{n \times q}$ zwei Matrizen, wobei die Anzahl der Spalten der ersten gleich der Anzahl der Zeilen der zweiten ist, so wird durch

$$c_{ik} = a_{i1}b_{1k} + a_{i2}b_{2k} + \dots + a_{in}b_{nk} = \sum_{j=1}^n a_{ij}b_{jk}$$

eine Matrix in $K^{m \times q}$ definiert, die als **Produkt** $A \cdot B = (c_{ik})$ der Matrizen A und B bezeichnet wird.

Wir illustrieren diese formale Definition an einem einfachen Beispiel:

$$A_1 \cdot A_2 = \begin{pmatrix} 1 & 5 & 2 \\ 3 & 2 & 1 \\ 0 & 1 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 5 & 7 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 1 \cdot 1 + 5 \cdot 5 + 2 \cdot 0 & 1 \cdot 2 + 5 \cdot 7 + 2 \cdot 2 \\ 3 \cdot 1 + 2 \cdot 5 + 1 \cdot 0 & 3 \cdot 2 + 2 \cdot 7 + 1 \cdot 2 \\ 0 \cdot 1 + 1 \cdot 5 + 2 \cdot 0 & 0 \cdot 2 + 1 \cdot 7 + 2 \cdot 2 \end{pmatrix} = \begin{pmatrix} 26 & 41 \\ 13 & 22 \\ 5 & 11 \end{pmatrix}.$$

$$x \cdot y = \begin{pmatrix} x_1 & x_2 & \cdots & x_n \end{pmatrix} \cdot \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} = x_1 y_1 + x_2 y_2 + \cdots + x_n y_n$$

Definition 3.23 Sei $n \geq 1$ eine ganze Zahl. Unter der n -dimensionalen Einheitsmatrix $I_n \in K^{n \times n}$ versteht man die Matrix

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

d.h., die Spalten von I_n sind die Vektoren $e_1, e_2, \dots, e_n$ der kanonische Basis.

Die Einheitsmatrix hat auch die Eigenschaft, dass nur in der Diagonale Elemente stehen, die von Null verschieden sind. Allgemein betrachtet man so genannte Diagonalmatrizen

$$\text{diag}(\lambda_1, \lambda_2, \dots, \lambda_n) = \begin{pmatrix} \lambda_1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & \lambda_2 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \lambda_3 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & \lambda_{n-1} & 0 \\ 0 & 0 & \cdots & 0 & 0 & \lambda_n \end{pmatrix}.$$

Entsprechend spricht man von oberen bzw. unteren Dreiecksmatrizen, wenn alle Elemente unterhalb bzw. oberhalb der Diagonale 0 sind.

Im folgenden Satz

Satz 3.24 A, B, C bezeichnen Matrizen, I die Einheitsmatrix (jeweils in passender Dimension) und λ einen Skalar. Dann gelten die folgenden Rechenregeln:

- (i) $A \cdot I = I \cdot A = A$,
- (ii) $(A \cdot B) \cdot C = A \cdot (B \cdot C)$,
- (iii) $(A + B) \cdot C = A \cdot C + B \cdot C$,
- (iv) $A \cdot (B + C) = A \cdot B + A \cdot C$,
- (v) $(\lambda \cdot A) \cdot B = A \cdot (\lambda \cdot B) = \lambda \cdot (A \cdot B)$,
- (vi) $(A + B)^T = A^T + B^T$,
- (vii) $(A \cdot B)^T = B^T \cdot A^T$,
- (viii) $(\lambda \cdot A)^T = \lambda \cdot A^T$.

Definition 3.25 Sei $A \in K^{n \times n}$ eine quadratische Matrix. Sie heißt **invertierbar** oder **regulär**, wenn es eine Matrix $A^{-1} \in K^{n \times n}$ gibt mit

$$A \cdot A^{-1} = A^{-1} \cdot A = I_n.$$

Die Matrix A^{-1} heißt dann die zu A **inverse Matrix**. Nicht invertierbare Matrizen werden auch als **singulär** bezeichnet.

Satz 3.26 Es seien A und B zwei invertierbare Matrizen in $K^{n \times n}$. Dann sind $A \cdot B$ und A^T ebenfalls invertierbar, und es gilt

- (i) $(A \cdot B)^{-1} = B^{-1} \cdot A^{-1}$,
- (ii) $(A^T)^{-1} = (A^{-1})^T$.

Satz 3.27 Eine quadratische Matrix $A \in K^{n \times n}$ ist genau dann invertierbar, wenn ihre Spalten (oder Zeilen) linear unabhängig sind, also eine Basis von K^n bilden.

3. Rang einer Matrix

Definition 3.28 Der **Spaltenrang** $\text{rg}(A)$ einer Matrix $A \in K^{m \times n}$ ist die Dimension der linearen Hülle der Spalten von A . Der **Zeilenrang** einer Matrix $A \in K^{m \times n}$ ist die Dimension der linearen Hülle der Zeilen von A , also der Spaltenrang von A^T .

Interessanterweise stimmen Spaltenrang und Zeilenrang immer überein, wie wir im Rahmen des Beispiels 3.32 zeigen werden. Man spricht daher allgemein vom **Rang einer Matrix**.

Satz 3.29 Für jede Matrix $A \in K^{m \times n}$ stimmen Spalten- und Zeilenrang überein, also

$$\text{rg}(A) = \text{rg}(A^T).$$

Beispiel 3.33 Es soll die inverse Matrix A^{-1} von

$$A = \begin{pmatrix} 1 & 2 & 0 \\ 0 & 2 & 1 \\ 3 & 5 & 0 \end{pmatrix}$$

bestimmt werden. Durch elementare Spaltenumformungen erhält man

$$\begin{pmatrix} 1 & 2 & 0 \\ 0 & 2 & 1 \\ 3 & 5 & 0 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ 3 & -1 & 0 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 2 \\ 3 & 0 & -1 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 3 & 0 & -1 \end{pmatrix}$$

$$\rightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & -2 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & -2 \end{pmatrix}$$

$$\rightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 3 & 0 & 1 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 2 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 2 \end{pmatrix}$$

$$\rightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -6 & 1 & 2 \end{pmatrix}$$

Die inverse Matrix A^{-1} ist also

$$A^{-1} = \begin{pmatrix} -5 & 0 & 2 \\ 3 & 0 & -1 \\ -6 & 1 & 2 \end{pmatrix}.$$

Lineare Abbildungen:

Wir betrachten zunächst eine Matrix $A \in K^{m \times n}$ und die Zuordnung

$$x \in K^n \mapsto f(x) = A \cdot x \in K^m.$$

Diese Abbildung $f: K^n \rightarrow K^m$ hat folgende zwei Eigenschaften:

- (i) $f(x+y) = A \cdot (x+y) = A \cdot x + A \cdot y = f(x) + f(y),$
- (ii) $f(\lambda \cdot x) = A \cdot (\lambda \cdot x) = \lambda \cdot (A \cdot x) = \lambda \cdot f(x).$

Definition 3.34 Eine Abbildung $f: V \rightarrow W$ zwischen zwei Vektorräumen V und W (über demselben Körper K) ist **linear**, wenn sie die folgenden beiden Eigenschaften (für $x, y \in V$ und $\lambda \in K$) hat:

- (i) $f(x+y) = f(x) + f(y),$
- (ii) $f(\lambda \cdot x) = \lambda \cdot f(x).$

Satz 3.35 (Fortsetzungssatz) Es sei V ein n -dimensionaler Vektorraum und die Menge $B = \{b_1, b_2, \dots, b_n\}$ eine Basis von V . Weiters sei W ein Vektorraum, $f: V \rightarrow W$ linear, und $c_j = f(b_j)$, $1 \leq j \leq n$, bezeichnen die Bilder der Basisvektoren.

Ist $x = x_1 \cdot b_1 + x_2 \cdot b_2 + \dots + x_n \cdot b_n$, d.h., hat x die Koordinaten $x_1, x_2, \dots, x_n \in K$, so gilt

WTF is das?

$$f(x) = x_1 \cdot f(b_1) + x_2 \cdot f(b_2) + \dots + x_n \cdot f(b_n) = x_1 \cdot c_1 + x_2 \cdot c_2 + \dots + x_n \cdot c_n.$$

Umgekehrt vermittelt diese Formel bei beliebiger Wahl von $c_j \in W$ stets eine lineare Abbildung $f: V \rightarrow W$.

Definition 3.37 Es sei $f: V \rightarrow W$ eine lineare Abbildung. Die Mengen

$$\ker(f) = \{x \in V \mid f(x) = 0\} \quad \text{und} \quad f(V) = \{f(x) \mid x \in V\}$$

heißen **Kern** und **Bild** von f . Die Dimension des Kerns und des Bilds sind der **Defekt** und der **Rang** von f :

$$\text{def}(f) = \dim(\ker(f)) \quad \text{und} \quad \text{rg}(f) = \dim(f(V)).$$

Satz 3.38 (Rangformel) Es sei V ein endlichdimensionaler Vektorraum und $f: V \rightarrow W$ eine lineare Abbildung. Dann gilt

$$\text{rg}(f) + \text{def}(f) = \dim V.$$

lineare Gleichungssysteme:

Definition 3.40 Seien $m, n \geq 1$ ganze Zahlen und K ein Körper. Weiters seien Elemente $a_{ij} \in K$ ($1 \leq i \leq m, 1 \leq j \leq n$) und $b_i \in K$ ($1 \leq i \leq m$) gegeben. Dann heißt ein System der Form

$$\begin{array}{ccccccc} a_{11}x_1 & + & \cdots & + & a_{1n}x_n & = & b_1 \\ a_{21}x_1 & + & \cdots & + & a_{2n}x_n & = & b_2 \\ \vdots & & \vdots & & \vdots & & \vdots \\ a_{m1}x_1 & + & \cdots & + & a_{mn}x_n & = & b_m \end{array} \quad (3.5)$$

lineares Gleichungssystem in den Unbekannten $x_1, x_2, \dots, x_n \in K$. Sind alle $b_1 = b_2 = \dots = b_m = 0$, so heißt das lineare Gleichungssystem **homogen**, sonst **inhomogen**.

Satz 3.41 (Satz von Kronecker-Capelli) Sei $A \in K^{m \times n}$ und $b \in K^m$. Dann ist das lineare Gleichungssystem $Ax = b$ genau dann lösbar, wenn

$$\text{rg}(A) = \text{rg}(A \ b).$$

Satz 3.42 Sei $A \in K^{m \times n}$ und $b \in K^m$. Ist das lineare Gleichungssystem $Ax = b$ lösbar, so gibt es $s = n - \text{rg}(A)$ linear unabhängige Vektoren $x_1, \dots, x_s \in \ker(f) \subseteq K^n$, d.h. Lösungen des homogenen linearen Gleichungssystems $A \cdot x = 0$, so dass alle Lösungen von $A \cdot x = b$ durch die Menge

$$\{x_0 + t_1x_1 + \cdots + t_sx_s \mid t_1, \dots, t_s \in K\}$$

gegeben sind, wobei x_0 eine beliebige, aber fest gewählte Lösung von $A \cdot x = b$ ist.

Satz 3.43 Sei $A \in K^{m \times n}$, $f(x) = A \cdot x$ und $b \in K^m$.

Ist f surjektiv, d.h. $\text{rg}(f) = \text{rg}(A) = m$, so ist das lineare Gleichungssystem $A \cdot x = b$ für alle rechten Seiten $b \in K^m$ lösbar.

Ist f injektiv, d.h. $\text{rg}(f) = \text{rg}(A) = n$, so ist $\ker(f) = \{0\}$, und das lineare Gleichungssystem $A \cdot x = b$ hat höchstens eine Lösung.

Ein wichtiger Spezialfall ist jener, wo die Matrix $A \in K^{n \times n}$ quadratisch ist. Ist A zusätzlich regulär, also invertierbar, so ist das lineare Gleichungssystem $A \cdot x = b$ für jede rechte Seite $b \in K^n$ eindeutig lösbar, und die Lösung ist gegeben durch

$$x = A^{-1} \cdot b.$$

Gauß'sches Eliminationsverfahren

↳ Nach der unten Dreiecksmatrix

Beispiel ↓

Beispiel 3.46 Es soll das lineare Gleichungssystem

$$\begin{aligned}
 x_1 + 2x_2 - 2x_3 + 3x_4 &= 3 \\
 2x_1 + 5x_2 + x_4 &= 4 \\
 3x_1 + 8x_2 + 2x_3 - x_4 &= 5 \\
 x_1 + 4x_2 + 6x_3 - 7x_4 &= -1
 \end{aligned} \tag{3.9}$$

über einem Körper K vollständig gelöst werden. Die Koeffizientenmatrix A und die rechte Seite b sind

$$A = \begin{pmatrix} 1 & 2 & -2 & 3 \\ 2 & 5 & 0 & 1 \\ 3 & 8 & 2 & -1 \\ 1 & 4 & 6 & -7 \end{pmatrix} \quad \text{und} \quad b = \begin{pmatrix} 3 \\ 4 \\ 5 \\ -1 \end{pmatrix}.$$

Durch elementare Zeilenumformungen der erweiterten Matrix $(A|b)$ erhält man eine Matrix der Form (3.8):

$$\left(\begin{array}{cccc|c} 1 & 2 & -2 & 3 & 3 \\ 2 & 5 & 0 & 1 & 4 \\ 3 & 8 & 2 & -1 & 5 \\ 1 & 4 & 6 & -7 & -1 \end{array} \right) \rightarrow \left(\begin{array}{cccc|c} 1 & 2 & -2 & 3 & 3 \\ 0 & 1 & 4 & -5 & -2 \\ 0 & 2 & 8 & -10 & -4 \\ 0 & 2 & 8 & -10 & -4 \end{array} \right) \rightarrow \left(\begin{array}{cccc|c} 1 & 2 & -2 & 3 & 3 \\ 0 & 1 & 4 & -5 & -2 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array} \right).$$

Im ersten Schritt wird das (-2) -fache der ersten Zeile zur zweiten Zeile addiert, etc. Ziel ist es, in der jeweiligen Spalte unterhalb des Diagonalelements „Nullen zu erzeugen“. (Man kann die entsprechenden Rechnungen auch im Gleichungssystem (3.9) durchführen. Im ersten Schritt wird dabei in der 2., 3. und 4. Gleichung die Unbekannte x_1 „eliminiert.“)

Das ursprüngliche lineare Gleichungssystem ist daher äquivalent zu

$$\begin{aligned}
 x_1 + 2x_2 - 2x_3 + 3x_4 &= 3 \\
 x_2 + 4x_3 - 5x_4 &= -2
 \end{aligned}$$

und wegen des Satzes von Kronecker-Capelli (Satz 3.41) auch lösbar. Setzt man $x_3 = t_1$ und $x_4 = t_2$, so errechnet man

$$\begin{aligned}
 x_2 &= -2 - 4x_3 + 5x_4 \\
 &= -2 - 4t_1 + 5t_2, \\
 x_1 &= 3 - 2x_2 + 2x_3 - 3x_4 \\
 &= 7 + 10t_1 - 13t_2.
 \end{aligned}$$

Alle Lösungen sind daher durch

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 7 \\ -2 \\ 0 \\ 0 \end{pmatrix} + t_1 \begin{pmatrix} 10 \\ -4 \\ 1 \\ 0 \end{pmatrix} + t_2 \begin{pmatrix} -13 \\ 5 \\ 0 \\ 1 \end{pmatrix} \tag{3.10}$$

mit $t_1, t_2 \in K$ gegeben.

Selbstverständlich hätte man mit einer weiteren Zeilenumformung auch zu einer Matrix der Form (3.6) umformen können:

$$\left(\begin{array}{cccc|c} 1 & 2 & -2 & 3 & 3 \\ 0 & 1 & 4 & -5 & -2 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array} \right) \rightarrow \left(\begin{array}{cccc|c} 1 & 0 & -10 & 13 & 7 \\ 0 & 1 & 4 & -5 & -2 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array} \right).$$

Die Lösung (3.10) erhält man dann ohne weitere Rechnung aus Satz 3.44.

△

Determinanten:

Definition 3.54 Die **Determinante** einer quadratischen Matrix $A = (a_{ij}) \in K^{n \times n}$ ist durch

$$\det A = \sum_{\pi \in S_n} \operatorname{sgn}(\pi) a_{\pi(1)1} a_{\pi(2)2} \cdots a_{\pi(n)n}$$

gegeben. (S_n bezeichnet die Menge aller Permutationen der Zahlen $1, 2, \dots, n$ und $\operatorname{sgn}(\pi)$ das Vorzeichen einer Permutation π , vergleiche mit Beispiel 2.13.)

Für $n = 3$ gibt es $3! = 6$ Permutationen. Nach kurzer Rechnung erhält man die Form

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31} - a_{12}a_{21}a_{33} - a_{11}a_{23}a_{32}. \quad (3.12)$$

die so genannte **Regel von Sarrus**:

Entwicklungssatz (Satz 3.62) kennenlernen, der

Satz 3.56 Eine Matrix $A \in K^{n \times n}$ ist genau dann invertierbar, wenn

$$\det A \neq 0.$$

Sind also die Spalten oder Zeilen von A linear abhängig oder sind zwei Spalten oder Zeilen sogar gleich, so ist $\det A = 0$.

Die folgenden beiden Sätze geben weitere Eigenschaften der Determinante an. Insbesondere ist Satz 3.58 für die praktische Berechnung einer Determinante von Bedeutung.

Satz 3.57

- (i) Für beliebige Matrizen $A, B \in K^{n \times n}$ gilt
$$\det(A \cdot B) = \det A \cdot \det B.$$
- (ii) Ist $A \in K^{n \times n}$ invertierbar, so berechnet sich die Determinante der inversen Matrix durch
$$\det(A^{-1}) = (\det A)^{-1}.$$
- (iii) Für $A \in K^{n \times n}$ gilt
$$\det(A^T) = \det A.$$

Satz 3.58

- (i) Multipliziert man eine Spalte/Zeile einer Matrix A mit einem Faktor $\lambda \in K$, so ist die Determinante der neuen Matrix $\det A' = \lambda \det A$.
- (ii) Addiert man zu einer Spalte/Zeile einer Matrix das Vielfache einer anderen Spalte/Zeile, so verändert sich der Wert der Determinante nicht.
- (iii) Vertauscht man in einer Matrix A zwei Spalten/Zeilen, so ist die Determinante der neuen Matrix $\det A' = -\det A$.

Mit elementaren Spalten- und Zeilenumformungen kann jede Matrix in eine obere Dreiecksmatrix umgeformt werden. Wegen Satz 3.58 verändert sich dabei der Wert der Determinante in kontrollierter Art und Weise. Damit kann jede Determinante (auch ohne explizite Kenntnis von S_n) berechnet werden.

Beispiel 3.59 Die Determinante der Matrix

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}$$

berechnet sich nach geeigneten elementaren Zeilenumformungen zu

$$\begin{vmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{vmatrix} = \begin{vmatrix} 1 & 2 & 3 \\ 0 & -3 & -6 \\ 0 & -6 & -12 \end{vmatrix} = \begin{vmatrix} 1 & 2 & 3 \\ 0 & -3 & -6 \\ 0 & 0 & 0 \end{vmatrix} = 0.$$

△

Definition 3.60 Sei $A \in K^{n \times n}$. Unter dem **Kofaktor** A_{ij} ($1 \leq i, j \leq n$) versteht man die Determinante jener Matrix, die dadurch hervorgeht, dass man die j -te Spalte durch den Vektor e_i der kanonischen Basis ersetzt.