
Kapitel I

Grundlagen

§1 Mengen und Aussagen

In der Wissenschaft ist es genau wie im täglichen Leben üblich, Begriffe, Dinge oder Lebewesen mit gemeinsamen Merkmalen durch Vergabe eines neuen Namens zu einem neuen Objekt zusammenzufassen:

So werden z.B. unter der Bezeichnung *Arachnida* oder *Spinnentiere* ca. 36 000 Tierarten zusammengefaßt.

Gewisse Elemente, deren Atome keine Elektronen aufnehmen oder abgeben können, bezeichnet man als *Edelgase*.

Das französische Volk ist ein Begriff für die Gesamtheit aller Menschen, deren Paß die französische Staatsangehörigkeit nachweist.

Auch in der Mathematik hat man schon immer Objekte zu neuen Begriffen zusammengefaßt: *die Gesamtheit aller Quadratzahlen, das Kontinuum der reellen Zahlen* usw. Wollte man Aussagen über die Gesamtheit und nicht über einzelne Objekte machen, so war man auf nicht einheitlich festgelegte und oft recht verkrampft wirkende Sprechweisen angewiesen, es war die Rede vom *Inbegriff* oder der *Mannigfaltigkeit* solcher Objekte. Dem machte **Georg Cantor** 1895 durch folgende Festlegung ein Ende.

Unter einer *Menge* verstehen wir jede Zusammenfassung M von bestimmten wohlunterschiedenen Objekten m unserer Anschauung oder unseres Denkens (welche die *Elemente* von M genannt werden) zu einem Ganzen.

Ist m ein Element der Menge M , so schreibt man heute:

$$m \in M$$

Cantors Mengenlehre war in ihrer ursprünglichen Form nicht widerspruchsfrei, das wurde später von Zermelo und Fraenkel korrigiert. Wir können und wollen hier auf die Details nicht eingehen, sondern uns lieber mit den Regeln befassen, nach denen Mengen gebildet werden können.

1. Mengenbildung durch Aufzählen der Elemente:

$\{0, 1\}$ ist die Menge mit den Elementen 0 und 1. Sie stimmt überein mit der Menge $\{0, 0, 1, 1, 1\}$, denn die Elemente sollen „wohlunterschieden“ sein, und wir können die mehrfach auftretenden Nullen oder Einsen nicht voneinander unterscheiden.

Definition.

Zwei Mengen M und N heißen *gleich*, wenn sie die gleichen Elemente besitzen. Man schreibt dann:

$$\boxed{M = N}$$

Also ist $\{0, 1\} = \{0, 0, 1, 1, 1\}$.

Will man der Menge $\{0, 1\}$ zur Abkürzung den Namen M geben, so schreibt man:

$$\boxed{M := \{0, 1\}}$$

Das soll heißen: M ist definiert als die Menge $\{0, 1\}$. Der Doppelpunkt muß immer auf der Seite des neu definierten Begriffes stehen.

Das Zeichen „:=“ wird auch in anderem Zusammenhang benutzt, wenn ein (komplizierter) Ausdruck mit einer Abkürzung versehen wird, z.B.:

$$\frac{a+b}{2} =: m(a, b).$$

Hier steht auf der linken Seite etwas Bekanntes, das künftig durch das neu eingeführte Symbol $m(a, b)$ ersetzt werden soll.

Als Abkürzungen für Mengen benutzen wir meist Großbuchstaben, die aber auch noch mit irgendwelchen Strichen, Akzenten oder Indizes versehen sein können, etwa A , A'' , \hat{A} , \tilde{A} , A_0 usw.

Beispiel :

$$A_{\text{klein}} := \{a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, y, z\}.$$

Weil es etwas mühsam ist, alle Buchstaben des Alphabets hinzuschreiben, wird man i.a. folgende abgekürzte Schreibweise wählen:

$$A_{\text{klein}} := \{a, b, c, \dots, z\}.$$

Problematisch wird es aber, wenn man auch eine unendliche Menge so aufschreiben will.

Definition.

$$\mathbb{N} := \{1, 2, 3, \dots\}$$

heißt die *Menge der natürlichen Zahlen*.

Hier ist nicht mehr klar, was die Pünktchen bedeuten. Wir haben zwar alle eine intuitive Vorstellung davon, wie es bei den natürlichen Zahlen weitergeht, aber die Intuition versagt wahrscheinlich bei Mengen wie etwa der folgenden:

$$M := \{3, 8, 24, 48, 120, \dots\}.$$

Oder wissen Sie, wie die nächste Zahl lautet?¹

Unendliche Mengen sollten wir möglichst mit Hilfe einer Konstruktionsvorschrift beschreiben. Bei der Menge \mathbb{N} könnte man das etwa folgendermaßen machen:

1. Die Zahl 1 ist ein Element von \mathbb{N} .
2. Zu jeder Zahl $n \in \mathbb{N}$ gibt es eine Nachfolgezahl $n^+ := n + 1$, die ebenfalls Element von \mathbb{N} und verschieden von all ihren Vorgängern ist.
3. Mit Ausnahme der 1 hat jede natürliche Zahl einen Vorgänger.

So haben wir das Bildungsgesetz für die natürlichen Zahlen exakt beschrieben, und es steht uns frei, den Zahlen auch noch Namen zu geben:

$$\begin{aligned} 2 &:= 1^+, \\ 3 &:= 2^+, \\ 4 &:= 3^+, \\ &\dots \end{aligned}$$

Nachdem wir nun wissen, wie man es eigentlich richtig macht, erlauben wir uns doch, einige gut bekannte unendliche Mengen in der etwas schlampigen aufzählenden Weise anzugeben.

Definition.

$\mathbb{Z} := \{0, \pm 1, \pm 2, \pm 3, \dots\}$ ist die *Menge der ganzen Zahlen*,

$\mathbb{Q} := \{0, \pm 1, \pm 2, \dots, \pm \frac{1}{2}, \pm \frac{3}{2}, \dots, \pm \frac{1}{3}, \pm \frac{2}{3}, \pm \frac{4}{3}, \dots\}$ ist die *Menge der rationalen Zahlen oder Brüche*.

Unmöglich wird diese Beschreibungsweise allerdings bei der Menge \mathbb{R} der reellen Zahlen. Wie man sich da behilft, untersuchen wir später.

2. Beschreibung von Mengen durch ihre Eigenschaften:

Die Menge $M := \{2, 4, 6, 8, \dots\}$ ist die Menge der geraden natürlichen Zahlen. Man schreibt das besser in folgender Form:

$$M := \{x \mid x \text{ ist eine gerade natürliche Zahl}\},$$

oder mathematischer:

$$M := \{x \in \mathbb{N} \mid 2 \text{ ist Teiler von } x\}.$$

Man sagt dazu

Menge der Elemente x aus \mathbb{N} mit der Eigenschaft „2 ist ein Teiler von x “.

¹Die Elemente haben die Gestalt $p^2 - 1$, wobei p jeweils eine Primzahl ist.

Ist X eine schon bekannte Grundmenge und $E(x)$ eine Eigenschaft, die Elementen $x \in X$ zukommen kann oder auch nicht, so ist auch $\{x \in X \mid E(x)\}$ wieder eine Menge, die aus genau denjenigen Elementen $x \in X$ besteht, die die Eigenschaft $E(x)$ haben. Man spricht vom Prinzip der „Aussonderung“.

Natürlich kommen nur nachprüfbar mathematisch sinnvolle Eigenschaften in Frage. Wir wollen das etwas präzisieren.

Eine *Aussage* (im mathematischen Sinne) ist eine Behauptung, die entweder wahr oder falsch ist.

Grundlage unserer Mathematik ist also die sogenannte zweiwertige Logik. Eine mathematische Aussage, die nicht wahr ist, muß falsch sein. Das stimmt zwar nicht mit der Erfahrung im Alltag überein, aber die Strukturen der zweiwertigen Logik lassen sich sehr schön mit elektronischen Schaltkreisen verwirklichen.

Um gültige Aussagen zu konstruieren, geht man am besten folgendermaßen vor:

- Elementare Aussagen sind „Gleichungen“ $a = b$ und „Element-Beziehungen“ $a \in A$.
- Komplexere Aussagen gewinnt man durch logische Verknüpfung von einfacheren Aussagen.

Bevor wir uns mit der Verknüpfung von Aussagen befassen, müssen wir noch etwas klarstellen.

$M = \{x \in X \mid E(x)\}$ ist eine Aussage, aber die beschreibende Eigenschaft $E(x)$ ist es im allgemeinen nicht, wegen der Variablen x . Erst wenn für x ein spezielles Element eingesetzt wird, erhält man eine wahre oder falsche Aussage. Man spricht deshalb von einer *Aussageform*. Wir werden aber diesen Unterschied zwischen Aussage und Aussageform nicht so genau beachten. Daß $E(x)$ wahr ist, soll dann jeweils bedeuten, daß $E(x)$ für jedes in Frage kommende Element x wahr ist.

Beispiel:

Die Menge M sei definiert durch $M := \{x \in \mathbb{R} \mid 2x - 7 = 15\}$. Wie jeder sofort sieht, ist $M = \{11\}$. Man überlege sich, warum im 1. Fall das Symbol „:=“ („ist definiert als“) und im 2. Fall das Symbol „=“ („ist gleich“) benutzt wurde!²

3. Logische Verneinung und Komplementärmenge:

Ist E eine Aussage (oder Aussageform), so bezeichnet man deren *logische Verneinung* mit $\neg E$. Wie man die Verneinung **inhaltsmäßig** bestimmt, werden wir nach und nach herausfinden. Aus der Sicht der formalen Logik kommt es zunächst nur auf die Wahrheitswerte an, und die werden durch eine sogenannte *Wahrheitstafel* festgelegt:

E	$\neg E$
w	f
f	w

²Beim 1. Mal wird M als neues Symbol eingeführt, beim 2. Auftreten ist M bereits bekannt, und es wird eine Aussage über M gemacht.

Die Wahrheitswerte werden durch die Verneinung ins Gegenteil verkehrt. Aber trotzdem sind die logische Verneinung und das umgangssprachliche Gegenteil zwei verschiedene Dinge.

Beispiel:

E sei die Aussage „Dieses Kleid ist weiß“, und F die Aussage „Dieses Kleid ist schwarz“. Ist E wahr, so ist F falsch. Ist aber E falsch, so braucht F noch lange nicht wahr zu sein, das Kleid könnte ja auch rot oder grün sein. Also ist F vielleicht das Gegenteil von E , aber sicher nicht die logische Verneinung.

Die Aussage „ E ist falsch“ ist aber die logische Verneinung der Aussage „ E ist wahr“, denn wir lassen ja keine andere Möglichkeit zu.

Bei Aussageformen muß man darauf achten, aus welchem Bereich die Variable gewählt werden soll. Betrachten wir etwa zwei Aussagen über Primzahlen p :³

$E(p)$: „ p ist ungerade“,

$F(p)$: „ $3p + 7 = 13$ “.

Man überzeugt sich leicht davon, daß $F(p)$ die logische Verneinung von $E(p)$ ist. Und das, obwohl man inhaltlich nur schwer einen Zusammenhang zwischen den beiden Aussagen finden kann. Es kommt eben nur auf die Wahrheitswerte an!

In gewissen Fällen hat man sogar spezielle Symbole für die logische Verneinung eingeführt.

1. $a \neq b$ bedeutet: $\neg(a = b)$.

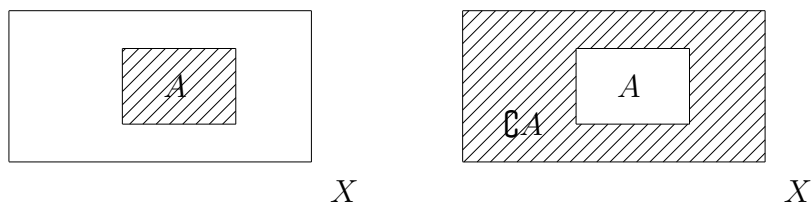
2. $x \notin A$ bedeutet: $\neg(x \in A)$.

Wie wird die logische Verneinung nun in der Mengenlehre benutzt?

Definition.

Sei X eine Grundmenge und $A = \{x \in X \mid E(x)\}$ eine mittels der Eigenschaft E aus X ausgesonderte Menge.

Dann heißt $A' := \{x \in X \mid \neg E(x)\}$ die *Komplementärmenge* (oder kurz das *Komplement*) von A in X . Man schreibt statt A' auch $\complement A$ oder $\complement_X(A)$.



4. Äquivalenz und Gleichheit:

Die Aussagen „ $x = 2$ “ und „ $3x + 7 = 13$ “ sind vom Wahrheitswert her nicht zu unterscheiden. Solche Aussagen wollen wir logisch äquivalent nennen. Und die Behauptung,

³ $p \in \mathbb{N}$ heißt *Primzahl*, wenn p genau 2 Teiler besitzt.

daß zwei Aussagen E und F logisch äquivalent sind, ist selbst wieder eine Aussage, die mit $E \iff F$ bezeichnet wird. Die zugehörige Wahrheitstafel ist etwas größer, da es hier 4 Möglichkeiten gibt:

E	F	$E \iff F$
w	w	w
w	f	f
f	w	f
f	f	w

Zwei Aussagen sind also genau dann äquivalent, wenn sie die gleichen Wahrheitswerte besitzen.

Die logische Äquivalenz von zwei Aussageformen $E(x)$ und $F(x)$ kann man auf zwei Weisen ausdrücken:

1. Für alle x aus (einer vorher festgelegten Grundmenge) X ist $E(x) \iff F(x)$.
2. $\{x \in X \mid E(x)\} = \{x \in X \mid F(x)\}$.

Das logische Äquivalenzzeichen steht zwischen Aussagen, das Gleichheitszeichen zwischen Objekten (d.h. zwischen Mengen oder Elementen).

Der Wahrheitswert einer Aussageform $E(x)$ hängt davon ab, was man für die Variable einsetzt. Dabei sind zwei Situationen so wichtig, daß man dafür eine besondere Symbolik eingeführt hat.

$$\boxed{\forall x \in X : E(x)}$$

ist eine Aussage, die bedeutet: „**Für alle** $x \in X$ **gilt** $E(x)$.“ Sie ist gleichbedeutend damit, daß $\{x \in X : E(x)\} = X$ ist. Durch Vorschaltung des sogenannten *Allquantors* \forall wird so aus einer Aussageform eine Aussage gemacht.

$$\boxed{\exists x \in X : E(x)}$$

ist eine Aussage, die bedeutet: „**Es existiert** (wenigstens) **ein** $x \in X$ **mit** $E(x)$. Das heißt, die Menge $\{x \in X : E(x)\}$ besitzt mindestens ein Element. Das Zeichen \exists nennt man den *Existenzquantor*.

Beispiel :

Sei \mathcal{H} die Menge der Hörer (und Hörerinnen) dieser Vorlesung, $E(x)$ die Aussageform „ x studiert die E-Technik im 1. Semester“. Dann werden wahrscheinlich viele unter Ihnen sein, für die $E(x)$ wahr ist, und einige, für die $E(x)$ falsch ist. Also kann man sagen:

„ $\forall x \in \mathcal{H} : E(x)$ “ ist eine falsche Aussage,
 „ $\exists x \in \mathcal{H} : E(x)$ “ ist eine wahre Aussage,
 aber auch „ $\exists x \in \mathcal{H} : \neg E(x)$ “ ist wahr.

Ferner überlegt man sich:

$$\neg(\forall x \in \mathcal{H} : E(x)) \iff \exists x \in \mathcal{H} : \neg E(x).$$

und:

$$\neg(\exists x \in \mathcal{H} : E(x)) \iff \forall x \in \mathcal{H} : \neg E(x).$$

Das Beispiel zeigt bereits das allgemeine Kochrezept, wie die mit \forall oder \exists quantifizierten Aussagen verneint werden.

Wir betrachten wieder eine abstrakte Menge $M := \{x \in X : E(x)\}$. Ist „ $\exists x \in X : E(x)$ “ eine wahre Aussage, so besitzt M mindestens ein Element. Aber was ist los, wenn diese Aussage falsch ist? Dann stellt sich heraus, daß die zuvor definierte Menge M überhaupt kein Element besitzt. Kann man Nichts zu etwas zusammenfassen? Ja, auch wenn das etwas pathologisch klingt. Damit keine widersprüchlichen Situationen eintreten können, läßt man so etwas zu.

Es gibt eine Menge, die kein Element besitzt. Weil jede Menge durch ihre Elemente festgelegt ist, kann es auch nur eine solche Menge geben.

Definition.

Man nennt die Menge, die kein Element besitzt, die *leere Menge* und bezeichnet sie mit dem Symbol \emptyset .

Um auszudrücken, daß eine Menge M keine Elemente besitzt, kann man nun auch sagen: $M = \emptyset$. Daraus folgt:

$$\exists x \in M \iff M \neq \emptyset.$$

5. Die logische Folgerung:

In diesem Abschnitt geht es nicht um die Konstruktion von Mengen, sondern um das wichtigste Werkzeug des Mathematikers, das logische Schließen.

Sind E und F Aussagen, so soll auch $E \implies F$ eine Aussage sein, die bedeutet: „Aus E folgt F .“

Wir versuchen, eine Wahrheitstafel aufzustellen. Da aus einer wahren Aussage durch richtiges Schließen wieder eine wahre Aussage gewonnen werden soll, muß die Wahrheitstafel zumindest so aussehen:

E	F	$E \implies F$
w	w	?
w	f	f
f	w	?
f	f	?

Wenn E und F die gleichen Wahrheitswerte besitzen, dann sind sie äquivalent. Wir stellen uns dann vor, daß man jede der beiden Aussagen aus der anderen logisch folgern kann. Also sollte in der ersten und der letzten Zeile der Tafel unter „ $E \implies F$ “ jeweils ein w stehen.

Jetzt müssen wir uns nur noch entscheiden, ob wir in der 3. Zeile ein w oder ein f setzen. Würden wir das f wählen, so würden wir die Wahrheitsverteilung der logischen Äquivalenz erhalten. Ist das sinnvoll? Wohl kaum, wie das folgende Beispiel zeigt:

Ist $E(n)$ die Aussage „ n ist ganz und durch 6 teilbar“ und $F(n)$ die Aussage „ n ist ganz und durch 2 teilbar“, so sollte ja wohl $E(n) \implies F(n)$ wahr sein. Es ist aber $E(8)$ falsch und $F(8)$ wahr, also $E(n)$ nicht äquivalent zu $F(n)$.

Das bedeutet, daß wir uns in der 3. Zeile für w entscheiden müssen.

Die Aussage „ $E \implies F$ “ bezeichnet man als *Implikation* oder *logische Folgerung*. Die zugehörige Wahrheitstafel sieht wie folgt aus:

E	F	$E \implies F$
w	w	w
w	f	f
f	w	w
f	f	w

Überraschend ist dabei die dritte und vierte Zeile. Aus einer falschen Aussage kann man alles folgern! Das liegt daran, daß die Implikation zunächst nichts mit Inhalten zu tun hat. Ihr Wahrheitsgehalt hängt rein formal vom Wahrheitsgehalt der beiden eingehenden Aussagen ab.

Beispiel :

Mit etwas Mühe kann man auch inhaltlich aus Quatsch (d.h. einer falschen Aussage) alles (insbesondere eine andere falsche Aussage) folgern.

Behauptung: „Wenn $2 \times 2 = 5$ ist, bin ich der Papst.“

Beweis: Wir setzen voraus, daß $2 \cdot 2 = 5$ ist. Andererseits folgt aus elementaren Rechenregeln:

$$2 \cdot 2 = (1 + 1) \cdot 2 = 1 \cdot 2 + 1 \cdot 2 = 2 + 2 = 4.$$

Also ist $4 = 5$. Wir bilden nun die Menge

$$M := \{\text{Motorrad, Krokodil, Petersdom, Papst, ich}\}.$$

Diese Menge besitzt 5 und daher auch 4 Elemente. Zwei der Elemente müssen gleich sein.

Die Elemente von M sind aus den Sparten „Fahrzeuge“, „Tiere“, „Bauwerke“ und „Personen“ gewählt, keine der Sparten hat mit einer der anderen etwas gemeinsam. Also können nur die beiden Personen gleich sein. Ich bin der Papst.

Wenn die logische Folgerung nur formal und nicht inhaltlich zu verstehen ist, so kann man natürlich nach ihrem Nutzen fragen. Die Antwort ergibt sich aus den folgenden Regeln:

- (Abtrennungsregel) Ist E wahr und $E \implies F$ wahr, so ist auch F wahr.
- (Syllogismus-Regel) Ist $E \implies F$ wahr und $F \implies G$ wahr, so ist auch $E \implies G$ wahr.

Beide Regeln kann man allein aus den Wahrheitstafeln herleiten! Die Syllogismus-Regel zeigt, wie man durch Verkettung von Implikationen neue bildet. Und die Abtrennungsregel zeigt, daß man mit Hilfe einer Implikation aus einer alten Wahrheit eine neue Wahrheit erhalten kann. Zusammen ermöglichen die Regeln es, aus vielen kleinen Folgerungen einen langen (direkten) Beweis aufzubauen.

Nun gibt es Aussagen, die man nicht beweisen kann, z.B. die elementaren Eigenschaften der natürlichen Zahlen. Da aber alle Menschen diese Eigenschaften anerkennen, legt man

sie als sogenannte *Axiome* fest. Die Axiome und die Gesetze der Logik sind die Spielregeln der Mathematik. Nachdem sie – mehr oder weniger willkürlich – festgelegt wurden, muß sich jeder daran halten.

Beispiel:

Ein Axiom für das Rechnen mit natürlichen Zahlen könnte z.B. lauten:

$$\forall n \in \mathbb{N} : 1 \cdot n = n.$$

Man kann daraus folgende wahre Implikation machen:

$$n \in \mathbb{N} \implies 1 \cdot n = n.$$

Hat man nun eine natürliche Zahl gegeben, etwa die 4, so ist $4 \in \mathbb{N}$ wahr, und auch die Implikation „ $4 \in \mathbb{N} \implies 1 \cdot 4 = 4$ “. Mit Hilfe der Abtrennungsregel schließt man daraus: $1 \cdot 4 = 4$.

Für den Anfänger ist hier kaum sichtbar, daß überhaupt etwas bewiesen wurde. Etwas deutlicher wird es in folgendem Beispiel:

Behauptung: $(-1) \cdot (-1) = 1$.

Beweis: Vorausgesetzt werden alle elementaren (als Axiome zu fordernden) Rechenregeln, insbesondere:

$$\begin{aligned} x \cdot (y + z) &= x \cdot y + x \cdot z, \\ x + y &= y + x, \\ x + (-x) &= 0, \\ x \cdot 1 &= x. \end{aligned}$$

Außerdem nehmen wir an, wir hätten schon folgende Regeln bewiesen:

Hilfssatz 1: $\forall x \in \mathbb{Z} : x \cdot 0 = 0$.

Hilfssatz 2: $\forall a \in \mathbb{Z} : (a + x = a + y \implies x = y)$.

Dann gilt:

$$(-1) + (-1) \cdot (-1) = (-1) \cdot 1 + (-1) \cdot (-1) = (-1) \cdot (1 + (-1)) = (-1) \cdot 0 = 0,$$

und genauso $(-1) + 1 = 1 + (-1) = 0$.

Also ist $(-1) + (-1) \cdot (-1) = (-1) + 1$, und mit der Implikation von Hilfssatz 2 ergibt sich daraus: $(-1) \cdot (-1) = 1$. \square

Nach diesem Schema verlaufen im Prinzip alle *direkten Beweise*.

Ein stärkeres Hilfsmittel ist der *indirekte Beweis* oder *Beweis durch Widerspruch*:

Gegeben ist eine Aussage A . Bewiesen werden soll B . Da das direkt zu schwierig ist, versucht man es indirekt und nimmt an, $\neg B$ wäre wahr. Das liefert zunächst eine zusätzliche nützliche Voraussetzung. Dann versucht man, aus A und $\neg B$ eine offensichtlich falsche Aussage C herzuleiten (den *Widerspruch*). Wenn das gelingt, ist die Implikation

$\neg B \implies C$ wahr, aber C falsch. Das geht nur, wenn $\neg B$ falsch ist, also B wahr. Damit ist man fertig!

Ein wichtiges Beispiel ist der Umgang mit dem Unendlichen. Eine Menge M heißt *endlich*, wenn sie nur endlich viele Elemente besitzt, wenn es also ein $n \in \mathbb{N}$ gibt, so daß M genau n Elemente enthält. Eine Menge heißt *unendlich*, wenn sie nicht endlich ist.

Z.B. ist $M := \{n \in \mathbb{Z} : 3 < n < 7\} = \{4, 5, 6\}$ eine Menge mit 3 Elementen, also endlich, aber $X := \{x \in \mathbb{Q} : 3 < x < 7\}$ ist unendlich. Letzteres können wir nur durch Widerspruch beweisen:

Beweis: Vorausgesetzt werden alle nötigen Regeln für das Rechnen mit rationalen Zahlen. Gezeigt werden soll, daß X unendlich ist. Wir führen Beweis durch Widerspruch und nehmen an, X ist endlich. Dann gibt es höchstens endlich viele rationale Zahlen q mit $3 < q < 4$. $\frac{7}{2}$ ist z.B. eine solche Zahl. Wir können diese endlich vielen Zahlen der Größe nach ordnen und erhalten in X eine kleinste rationale Zahl $q = \frac{a}{b}$ mit $3 < q < 4$, so daß zwischen 3 und q keine weitere rationale Zahl liegt. Aber $p := \frac{3+q}{2} = \frac{a+3b}{2b}$ ist eine rationale Zahl mit $3 < p < q$. Wir haben in X eine Zahl gefunden, die kleiner als q ist. Das ist der gewünschte Widerspruch. \square

Zum Schluß noch ein weiterer Begriff aus der Mengenlehre:

Definition.

Eine Menge A heißt *Teilmenge* einer Menge B (in Zeichen $A \subset B$), falls gilt: Jedes Element von A ist auch Element von B .

Man kann auch sagen:

$$A \subset B : \iff \forall x : x \in A \implies x \in B$$

6. Konjunktion und Schnittmenge:

Sind E und F Aussagen, so bezeichnet $E \wedge F$ deren *Konjunktion*, d.h. die Aussage, die genau dann wahr ist, wenn E und F beide wahr sind.

E	F	$E \wedge F$
w	w	w
w	f	f
f	w	f
f	f	f

Definition.

Sind A und B Mengen, so nennt man

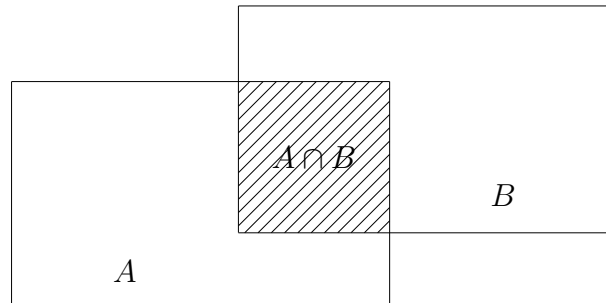
$$A \cap B := \{x : (x \in A) \wedge (x \in B)\}$$

die *Schnittmenge* oder den *Durchschnitt* von A und B .

Beispiel:

Sei $A := \{n \in \mathbb{Z} : 1 \leq n \leq 5\}$ und $B = \{n \in \mathbb{Z} : 3 < n < 8\}$. Dann ist

$$A \cap B = \{n \in \mathbb{Z} : 3 < n \leq 5\}.$$



I.1.1 Satz.

1. $A \cap B = B \cap A$ (Kommutativgesetz).
2. $A \cap (B \cap C) = (A \cap B) \cap C$ (Assoziativgesetz).
3. $A \cap \emptyset = \emptyset$.
4. $A \cap \complement_X(A) = \emptyset$.

7. Disjunktion und Vereinigung:

Sind E und F Aussagen, so bezeichnet $E \vee F$ deren *Disjunktion*, d.h. die Aussage, die genau dann wahr ist, sobald eine der beiden Aussagen E und F wahr ist.

E	F	$E \vee F$
w	w	w
w	f	w
f	w	w
f	f	f

Im Gegensatz zum üblichen Sprachgebrauch ist das logische „oder“ nicht ausschließend, also kein „entweder – oder“.

Definition.

Sind A und B Mengen, so nennt man

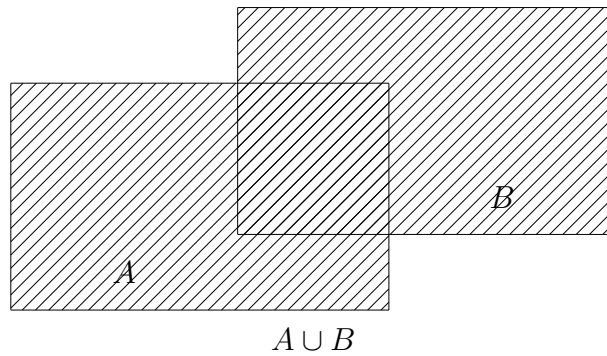
$$A \cup B := \{x : (x \in A) \vee (x \in B)\}$$

die *Vereinigung* von A und B .

Beispiel:

Sei $A := \{n \in \mathbb{Z} : 1 \leq n \leq 5\}$ und $B = \{n \in \mathbb{Z} : 3 < n < 8\}$. Dann ist

$$A \cup B = \{n \in \mathbb{Z} : 1 \leq n < 8\}.$$

**I.1.2 Satz.**

1. $A \cup B = B \cup A$ (Kommutativgesetz).
2. $A \cup (B \cup C) = (A \cup B) \cup C$ (Assoziativgesetz).
3. $A \cup \emptyset = A$.
4. $A \cup \complement_X(A) = X$.

8. Boolesche Algebra:

Die Begriffe „Kommutativgesetz“ und „Assoziativgesetz“ erinnern an die Algebra. Tatsächlich geht die Analogie noch weiter. Es gibt für Durchschnitt und Vereinigung **zwei** Distributivgesetze:

I.1.3 Satz.

1. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.
2. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

Der BEWEIS beruht auf den entsprechenden Regeln für die logischen Verknüpfungen \wedge und \vee . Setzt man nämlich

$$E(x) : \iff x \in A, \quad F(x) : \iff x \in B \quad \text{und} \quad G(x) : \iff x \in C,$$

so braucht man nur noch eine große Wahrheitstafel aufzustellen:

E	F	G	$F \vee G$	$E \wedge F$	$E \wedge G$	$E \wedge (F \vee G)$	$(E \wedge F) \vee (E \wedge G)$
w	w	w	w	w	w	w	w
w	w	f	w	w	f	w	w
w	f	w	w	f	w	w	w
w	f	f	f	f	f	f	f
f	w	w	w	f	f	f	f
f	w	f	w	f	f	f	f
f	f	w	w	f	f	f	f
f	f	f	f	f	f	f	f

Die Äquivalenz zwischen den beiden letzten Spalten liefert das erste Distributivgesetz.

Man beachte allerdings, daß hier \cap und \cup gleichberechtigt sind, während es in der Algebra zwischen $+$ und \cdot nur ein Distributivgesetz gibt.

I.1.4 Satz. Seien $A, B \subset X$. Dann gilt:

$$\begin{aligned} A \subset B &\iff A \cap B = A \\ &\iff A \cup B = B \\ &\iff B \cup \complement_X(A) = X. \end{aligned}$$

Den BEWEIS könnte man mit Wahrheitstafeln führen, wir wollen hier aber am Beispiel der ersten Äquivalenz ein anderes Verfahren vorführen.

Der Beweis einer Äquivalenz zerfällt in zwei Teile, nämlich den Beweis der Implikation „ \implies “ und den der Implikation „ \impliedby “.

1. Es sei $A \subset B$. Zu zeigen ist $A \cap B = A$.

Der Beweis der Mengengleichheit zerfällt wiederum in zwei Teile:

- (a) Sei $x \in A \cap B$. Dann gilt $(x \in A) \wedge (x \in B)$, insbesondere also $x \in A$.
- (b) Sei $x \in A$. Da nach Voraussetzung $A \subset B$ ist, gilt auch $x \in B$ und damit $x \in A \cap B$.

2. Nun setzen wir $A \cap B = A$ voraus. Zu zeigen ist $A \subset B$.

Sei $x \in A$. Nach Voraussetzung liegt x dann in $A \cap B$, und damit auch in B .

So einfach sind auch die anderen Äquivalenzen zu zeigen. □

I.1.5 Satz (de Morgansche Verneinungsregeln). Es ist

1. $\complement_X(A \cap B) = \complement_X(A) \cup \complement_X(B)$.
2. $\complement_X(A \cup B) = \complement_X(A) \cap \complement_X(B)$.

Die Mengengleichungen entsprechen den logischen Äquivalenzen

$$\begin{aligned} \neg(E \wedge F) &\iff (\neg E) \vee (\neg F) \\ \text{und} \quad \neg(E \vee F) &\iff (\neg E) \wedge (\neg F), \end{aligned}$$

und die sind wieder leicht mit Wahrheitstafeln zu verifizieren.

Beispiel:

Gesucht ist das Komplement der Menge $M := \{x \in \mathbb{Z} \mid 2 < x \leq 13\}$.

$x \leq 13$ ist gleichbedeutend mit der Aussage $(x < 13) \vee (x = 13)$. Daher gilt:

$$\begin{aligned} x \in \complement_{\mathbb{Z}}(M) &\iff \neg[(x > 2) \wedge ((x < 13) \vee (x = 13))] \\ &\iff \neg(x > 2) \vee (\neg(x < 13) \wedge \neg(x = 13)) \\ &\iff (x \leq 2) \vee ((x \geq 13) \wedge (x \neq 13)) \\ &\iff (x \leq 2) \vee (x > 13) \\ &\iff x \in \{x \in \mathbb{Z} \mid x \leq 2\} \cup \{x \in \mathbb{Z} \mid x > 13\}. \end{aligned}$$

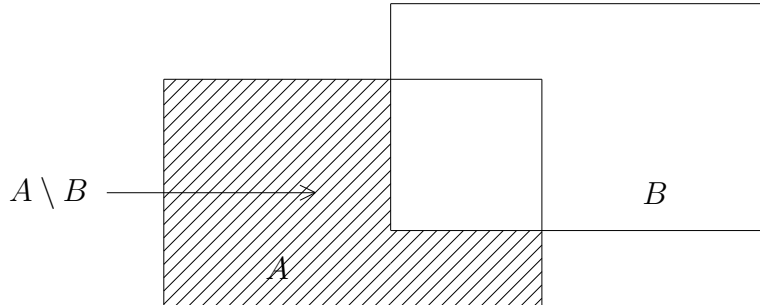
Daher ist

$$\complement_{\mathbb{Z}}(\{x \in \mathbb{Z} \mid 2 < x \leq 13\}) = \{x \in \mathbb{Z} \mid x \leq 2\} \cup \{x \in \mathbb{Z} \mid x > 13\}.$$

Der Vollständigkeit halber notieren wir noch:

$$A \setminus B := \{x \in A \mid x \notin B\} \quad \text{heißt die Differenz von } A \text{ und } B.$$

Dazu braucht B keine Teilmenge von A zu sein! Vielmehr ist $A \setminus B = \complement_A(A \cap B)$.



Definition.

Sei X eine beliebige Menge. Dann heißt $P(X) := \{A \mid A \subset X\}$ die *Potenzmenge* von X .

Hier bilden wir eine Menge aus Elementen, die noch nie zuvor zu einer Menge zusammengefaßt wurden. Daß das in diesem Falle geht, gehört zu den Axiomen der Mengenlehre. Übrigens trifft das auch auf die Existenz der Vereinigung zweier Mengen zu.

9. Kombinatorik und Induktion:

Definition.

Ist M eine endliche Menge, so bezeichnen wir mit $\#M$ die Anzahl ihrer Elemente. Ist M nicht endlich, so setzen wir $\#M := \infty$.

I.1.6 Satz.

Hat M genau n Elemente, so hat $P(M)$ 2^n Elemente.

BEWEIS: Für die leere Menge ist der Satz richtig, denn $P(\emptyset) = \{\emptyset\}$ hat $2^0 = 1$ Element. Wir können also voraussetzen, daß M mindestens ein Element besitzt. Wir untersuchen nun verschiedene Fälle:

1. Fall: $M = \{x_1\}$ hat genau ein Element. Dann ist $P(M) = \{\emptyset, \{x_1\}\}$, also $\#P(M) = 2 = 2^1$.

2. Fall: $M = \{x_1, x_2\}$ habe genau zwei Elemente. Dann ist

$$P(M) = \{\emptyset, \{x_1\}, \{x_2\}, \{x_1, x_2\}\},$$

also $\#P(M) = 4 = 2^2$.

3. Fall: $M = \{x_1, x_2, x_3\}$ habe genau 3 Elemente. Dann gilt:

$$\begin{aligned} P(M) &= \{\emptyset, \{x_1\}, \{x_2\}, \{x_3\}, \{x_1, x_2\}, \{x_1, x_3\}, \{x_2, x_3\}, M\} \\ &= \{\emptyset, \{x_1\}, \{x_2\}, \{x_1, x_2\}\} \cup \{\{x_3\}, \{x_1, x_3\}, \{x_2, x_3\}, \{x_1, x_2, x_3\}\} \\ &= P(\{x_1, x_2\}) \cup \{A \cup \{x_3\} \mid A \in P(\{x_1, x_2\})\}. \end{aligned}$$

Da $P(\{x_1, x_2\})$ 2^2 Elemente besitzt, folgt:

$P(M)$ besitzt $2^2 + 2^2 = 2 \cdot 2^2 = 2^3 = 8$ Elemente. Diese etwas umständlich anmutende Methode ist zugleich ein Rezept für den allgemeinen Fall:

Ist $M = \{x_1, \dots, x_{n-1}, x_n\}$ und $M' := \{x_1, \dots, x_{n-1}\}$, so ist $M = M' \cup \{x_n\}$. Aber dann ist

$$P(M) = P(M') \cup \{A \cup \{x_n\} \mid A \in P(M')\},$$

also

$$\#P(M) = \#P(M') + \#P(M') = 2 \cdot \#P(M') = 2 \cdot 2^{n-1} = 2^n,$$

sofern man den Fall der Mengen mit $n - 1$ Elementen schon abgehandelt hat. \square

Wir haben ein typisches Beispiel für einen *Induktionsbeweis* kennengelernt. Das allgemeine Prinzip sieht so aus:

Zu beweisen ist eine Aussage $E(n)$ für alle $n \in \mathbb{N}$ (oder alle $n \in \mathbb{N}_0 := \mathbb{N} \cup \{0\}$).

Induktionsanfang: Zeige $E(1)$ (bzw. $E(0)$ für $n \in \mathbb{N}_0$).

Induktionsschluß: Beweise für $n \geq 1$ die Implikation $E(n) \implies E(n+1)$ (bzw. $E(n-1) \implies E(n)$ für $n \in \mathbb{N}_0$).

Wohlgemerkt: Man braucht nicht zu zeigen, daß $E(n)$ wahr ist! Man muß nur zeigen, daß $E(n+1)$ automatisch aus $E(n)$ folgt.

Damit ist $E(n)$ für alle n bewiesen! Warum? Es gilt ja:

$$E(1) \wedge (E(1) \implies E(2)), \text{ also auch } E(2).$$

$$E(2) \wedge (E(2) \implies E(3)), \text{ also auch } E(3).$$

... u.s.w.

Auch wenn das unendlich viele Schritte sind, so gilt doch: Um eine der Aussagen $E(n)$ zu beweisen, reichen n Schritte aus. Und weil das für jedes beliebige n geht, hat man so auch $E(n)$ für alle n bewiesen.

Um den Induktionsbeweis zu verstehen, stelle man sich die natürlichen Zahlen als eine unendliche Reihe von Domino-Steinen vor. Kippt man den ersten Stein um und hat man dafür gesorgt, daß der $(n+1)$ -te Stein nahe genug beim n -ten Stein steht, so kippen alle Steine um.

Wir wollen jetzt folgende Aussage mit Induktion beweisen:

I.1.7 Satz. *Es gibt genau $n!$ Möglichkeiten, die Zahlen $1, 2, 3, \dots, n$ anzuordnen.*

Dabei ist $n! := 1 \cdot 2 \cdot 3 \cdot \dots \cdot n$ (und $0! := 1$).

BEWEIS: Nach dem Domino-Prinzip müssen wir zunächst den *Induktionsanfang* erledigen, also die Aussage $E(1)$ beweisen: „Es gibt genau eine Möglichkeit, die Zahl 1 anzuordnen“. Nun, das ist so evident, da brauchen wir gar nichts zu zeigen.

Im zweiten Schritt müssen wir den *Induktionsschluß* durchführen, d.h. wir müssen uns davon überzeugen, daß die Domino-Steine richtig stehen. Wenn man schon weiß, daß man die Zahlen $1, 2, 3, \dots, n$ auf genau $n!$ verschiedene Weisen anordnen kann, dann sieht

die Situation bei den Zahlen

$1, 2, 3, \dots, n, n+1$ folgendermaßen aus:

Es gibt $n!$ mögliche Anordnungen, bei denen die Zahl $n+1$ an letzter Stelle steht. Es kann aber auch jede andere Zahl zwischen 1 und n an letzter Stelle stehen, und für die verbliebenen n Zahlen stehen jedesmal wieder $n!$ mögliche Anordnungen zur Verfügung. Zusammen sind das $(n+1) \cdot n! = (n+1)!$ Möglichkeiten.

Jetzt sind wir mit dem Induktionsbeweis fertig! Aus der Aussage $E(1)$ folgt wegen des Induktionsschlusses die Aussage $E(2)$, hieraus dann die Aussage $E(3)$ usw. Die Domino-
steine kippen alle um! \square

Bevor wir zur nächsten Aussage kommen, führen wir das Summenzeichen ein:

Sind a_1, a_2, \dots, a_n irgendwelche (reelle) Zahlen, so setzt man

$$\sum_{i=1}^n a_i := a_1 + a_2 + \dots + a_n.$$

Allgemeiner ist dann

$$\sum_{i=k}^l a_i = a_k + a_{k+1} + \dots + a_{l-1} + a_l.$$

Im Falle $k > l$ erhält man dabei eine *leere Summe*, die wird $= 0$ gesetzt.

I.1.8 Satz. Für alle $n \in \mathbb{N}$ ist $\sum_{i=1}^n i = \frac{n(n+1)}{2}$.

BEWEIS: Wieder führen wir Induktion nach n :

$n = 1$: Die linke Seite ist $= 1$, und die rechte $= \frac{1 \cdot (1+1)}{2} = 1$.

$n \rightarrow n+1$: Es ist

$$\begin{aligned} \sum_{i=1}^{n+1} i &= \sum_{i=1}^n i + (n+1) = \frac{n(n+1)}{2} + (n+1) \\ &= \frac{n(n+1) + 2(n+1)}{2} = \frac{(n+1)(n+2)}{2}. \end{aligned}$$

\square

Solche Formeln werden gerne benutzt, um den Induktionsbeweis zu üben. Dabei ist keine Rede davon, wie man die Formel findet, und es wird auch verschwiegen, daß es einen viel einfacheren Beweis gibt:

Es ist nämlich

$$\begin{aligned} 2 \cdot \sum_{i=1}^n i &= 1 + 2 + \dots + n \\ &\quad + n + (n-1) + \dots + 1 \\ &= n(n+1). \end{aligned}$$

In dieser Form hat der kleine Gauß schon in der Schule das Problem gelöst, die Zahlen von 1 bis 100 zu addieren.

Sei nun wieder M eine Menge mit n Elementen und

$$P(M)_k := \{A \subset M \mid \#A = k\}.$$

Für $k > n$ ist diese Menge natürlich leer.

I.1.9 Satz. Für $1 \leq k \leq n$ ist $\#(P(M)_k) = \frac{n!}{k!(n-k)!}$.

BEWEIS: Wir wählen eine beliebige Anordnung x_1, \dots, x_n der Elemente von M (davon gibt es bekanntlich $n!$). Anschließend fassen wir die ersten k Elemente zu einer Teilmenge zusammen. Auf diese Weise erhalten wir sicherlich alle k -elementigen Teilmengen, aber sie treten mehrfach auf. Wenn wir die ersten k Elemente untereinander vertauschen (und dafür gibt es $k!$ Möglichkeiten), oder wenn wir die hinteren $n-k$ Elemente untereinander vertauschen (dafür gibt es $(n-k)!$ Möglichkeiten), dann ändert sich nichts an unserer Auswahl. Also gibt es $\frac{n!}{k!(n-k)!}$ Teilmengen von M mit k Elementen. \square

Definition.

Sei $0 \leq k \leq n$. Die Zahlen $\binom{n}{k} := \frac{n!}{k!(n-k)!}$ (in Worten: „ n über k “) nennt man *Binomialkoeffizienten*.

Hier sind einige Eigenschaften:

1. Es ist $\binom{n}{k} = \frac{(n-k+1) \cdot (n-k+2) \cdot \dots \cdot n}{1 \cdot 2 \cdot \dots \cdot k}$.
2. $\binom{n}{0} = \binom{n}{n} = 1$.
3. $\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}$.

Überprüfen wir die letzte Aussage: Es ist

$$\begin{aligned} \binom{n}{k} + \binom{n}{k-1} &= \frac{n!}{k!(n-k)!} + \frac{n!}{(k-1)!(n-k+1)!} \\ &= \frac{n! \cdot (n-k+1) + k \cdot n!}{k!(n-k+1)!} \\ &= \frac{n! \cdot (n+1)}{k!(n-k+1)!} \\ &= \frac{(n+1)!}{k!((n+1)-k)!} = \binom{n+1}{k}. \end{aligned}$$

Die gerade bewiesene Formel erlaubt eine besonders einfache Berechnung der Binomialkoeffizienten – ohne Multiplikation! Allerdings müssen die Koeffizienten der Reihenfolge

nach berechnet werden. Man kann sie dann in Form des sogenannten Pascalschen Dreiecks anordnen:

$$\begin{array}{ccccccc}
 n = 0 & & & & & & 1 \\
 n = 1 & & & & 1 & & 1 \\
 n = 2 & & & 1 & & 2 & & 1 \\
 n = 3 & & 1 & & 3 & & 3 & & 1 \\
 & & & & & & & & \dots
 \end{array}$$

Beispiel:

Beim Lotto müssen 6 Zahlen aus 49 ausgewählt werden. Nun ist

$$\binom{49}{6} = \frac{49!}{6!43!} = \frac{44 \cdot 45 \cdot 46 \cdot 47 \cdot 48 \cdot 49}{1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6} = 13\,983\,816.$$

Bei sovielen Möglichkeiten sollte man die Ausgabe für den nächsten Lottoschein vielleicht doch noch einmal überdenken.

Wir kommen nun zu dem Satz, der den Binomialkoeffizienten ihren Namen gab:

I.1.10 Satz. (*Binomische Formel*)

Für $a, b \in \mathbb{R}$ und $n \in \mathbb{N}$ ist

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

BEWEIS: Es ist $(a + b)^n = (a + b) \cdot (a + b) \cdot \dots \cdot (a + b)$, mit n Faktoren. Beim Ausmultiplizieren erhält man Terme der Gestalt

$$\dots + N(n, k) \cdot a^k \cdot b^{n-k} + \dots,$$

wobei $N(n, k)$ die Anzahl der Möglichkeiten bedeutet, aus k Klammern ein a und aus $n - k$ Klammern ein b zu holen. Aber jede dieser Möglichkeiten entspricht der Auswahl einer k -elementigen Teilmenge aus einer n -elementigen Menge (nämlich der Menge aller

n Klammern). Also ist $N(n, k) = \binom{n}{k}$. □

Für kleines n ist diese Formel wohlbekannt:

$$\begin{aligned}
 (a + b)^2 &= a^2 + 2ab + b^2, \\
 (a + b)^3 &= a^3 + 3a^2b + 3ab^2 + b^3.
 \end{aligned}$$

Eine Folgerung wollen wir noch notieren:

I.1.11 Folgerung. *Es ist*

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

Zum Beweis setze man einfach $a = b = 1$ in der binomischen Formel.

I.1.12 Satz. (Geometrische Summenformel)

Ist $q \neq 1$ eine reelle Zahl, so ist

$$\sum_{k=0}^n q^k = \frac{q^{n+1} - 1}{q - 1}.$$

BEWEIS: Man kann einfach ausmultiplizieren:

$$\begin{aligned} \left(\sum_{k=0}^n q^k \right) \cdot (q - 1) &= \sum_{k=0}^n q^{k+1} - \sum_{k=0}^n q^k \\ &= q^{n+1} - 1. \end{aligned}$$

Division durch $q - 1$ ergibt das Ergebnis. □

Der Trick mit den beiden Summen, wo sich die Summanden – bis auf das erste Glied der einen und das letzte Glied der anderen Summe – gegenseitig wegheben, kann häufig benutzt werden. Man spricht auch von „Teleskop-Summen“. Hier ist noch ein weiteres wichtiges Beispiel:

I.1.13 Satz. Ist $x \neq y$, so ist

$$\frac{x^n - y^n}{x - y} = \sum_{i=0}^{n-1} x^i y^{n-i-1}.$$

BEWEIS: Es ist

$$\begin{aligned} (x - y) \cdot \sum_{i=0}^{n-1} x^i y^{n-i-1} &= \\ &= \sum_{i=0}^{n-1} x^{i+1} y^{n-i-1} - \sum_{i=0}^{n-1} x^i y^{n-i} \\ &= (xy^{n-1} + \dots + x^{n-1}y + x^n) - (y^n + xy^{n-1} + \dots + x^{n-1}y) \\ &= x^n - y^n. \end{aligned}$$

□

Beispiele :

1. Der Fall $n = 2$ liefert die Formel

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

2. Ist $y = 1$, so erhält man

$$\frac{x^n - 1}{x - 1} = 1 + x + x^2 + \dots + x^{n-1}.$$

§2 Zahlen und Strukturen

Wir wollen nun die Menge \mathbb{R} der reellen Zahlen sorgfältiger untersuchen. Bisher konnten wir keine saubere Definition für \mathbb{R} angeben. Woran liegt das? Was sind die reellen Zahlen?

- Anschaulich entsprechen die reellen Zahlen den Punkten auf einer unendlichen Geraden. Aber damit wird das Problem nur verlagert. Wir können zwar aus der Anschauung viele Gesetzmäßigkeiten herleiten, aber ein exaktes mathematisches Vorgehen ist das nicht.
- Wir kennen die reellen Zahlen als unendliche Dezimalbrüche

$$\pm m_N m_{N-1} \dots m_0, m_{-1} m_{-2} m_{-3} \dots$$

Diese Darstellung ist nicht eindeutig und besonders wegen der Pünktchen problematisch. Außerdem lassen sich die Rechenverknüpfungen so nur schwer definieren, und ihre Gesetze sind noch schwerer nachzuweisen. Eine Theorie sollte aber möglichst einfach beginnen.

Denken wir etwa an das Kartenspiel „Skat“. Man kann es mit französischen Karten oder mit altdeutschen Karten spielen, es bleibt doch das gleiche Spiel. Wenn man jedoch die Regeln ändert, so ändert man das Spiel.

Betrachten wir also den Umgang mit den reellen Zahlen als ein Spiel. Wir müssen nicht wissen, was die Zahlen sind, wir müssen nur wissen, welche Regeln für den Umgang mit den Zahlen gelten. In der Mathematik nennt man solche Regeln *Axiome*. Wir werden versuchen, ein vollständiges Axiomensystem für \mathbb{R} aufzustellen. Ob es wirklich vollständig ist, überlassen wir allerdings den Experten.

1. Die Axiome der Addition

Je zwei reellen Zahlen x und y ist eine weitere reelle Zahl $x + y$ zugeordnet, ihre *Summe*.

1. **Assoziativgesetz:** $\forall x, y, z \in \mathbb{R} : (x + y) + z = x + (y + z).$
2. **Kommutativgesetz:** $\forall x, y \in \mathbb{R} : x + y = y + x.$
3. **Existenz der Null:** $\exists 0 \in \mathbb{R}$, so daß $\forall x \in \mathbb{R}$ gilt: $x + 0 = x.$
4. **Existenz des Negativen:** $\forall x \in \mathbb{R} \exists (-x) \in \mathbb{R}$ mit $x + (-x) = 0.$

Man kann aus diesen Axiomen andere Eigenschaften herleiten, z.B.:

I.2.1 Satz. Für alle $a, b \in \mathbb{R}$ besitzt die Gleichung

$$a + x = b$$

eine eindeutig bestimmte Lösung.

BEWEIS:

1. **Existenz:** Wir erraten eine Lösung und überprüfen, ob es wirklich eine ist. Sei $x := b + (-a)$. Dann ist tatsächlich

$$a + x = a + (b + (-a)) = a + ((-a) + b) = (a + (-a)) + b = 0 + b = b + 0 = b.$$

Wir haben nur die Axiome benutzt!

2. **Eindeutigkeit:** Seien x und y zwei Lösungen der Gleichung. Dann ist $a + x = b = a + y$, also

$$y = 0 + y = ((-a) + a) + y = (-a) + (a + y) = (-a) + (a + x) = ((-a) + a) + x = 0 + x = x.$$

Wir haben hier insbesondere die altbekannte Regel, daß man auf beiden Seiten einer Gleichung das Gleiche subtrahieren darf, aus den Axiomen hergeleitet. \square

I.2.2 Folgerung. *Es ist $-(-a) = a$ und $-(a + b) = (-a) + (-b)$.*

Der BEWEIS ist ganz einfach. Z.B. sind a und $-(-a)$ beides Lösungen der Gleichung $-a + x = 0$.

In \mathbb{Z} und in \mathbb{Q} gelten die gleichen Regeln für die Addition. Also reichen sie mit Sicherheit nicht aus, um \mathbb{R} auszuzeichnen. Allerdings ist die Menge \mathbb{N} (und auch \mathbb{N}_0) aus dem Rennen, denn dort gibt es kein Negatives.

2. Die Axiome der Multiplikation

Je zwei reellen Zahlen x und y ist eine weitere reelle Zahl $x \cdot y$ zugeordnet, ihr *Produkt*.

1. **Assoziativgesetz:** $\forall x, y, z \in \mathbb{R} : (x \cdot y) \cdot z = x \cdot (y \cdot z)$.
2. **Kommutativgesetz:** $\forall x, y \in \mathbb{R} : x \cdot y = y \cdot x$.
3. **Existenz der Eins:** $\exists 1 \in \mathbb{R}$, so daß $\forall x \in \mathbb{R}$ gilt: $x \cdot 1 = x$.
4. **Existenz des Inversen:** $\forall x \in \mathbb{R}$ mit $x \neq 0$ $\exists x^{-1} \in \mathbb{R}$ mit $x \cdot x^{-1} = 1$.

Die Gesetze sehen fast genauso aus wie bei der Addition, mit nur einer Ausnahme: Bei der Existenz des Inversen wird $x \neq 0$ vorausgesetzt. Warum das so sein muß, werden wir noch sehen.

Wie oben zeigt man auch hier, daß die Gleichung $a \cdot x = b$ stets eindeutig lösbar ist. Allerdings muß man $a \neq 0$ voraussetzen. Und es folgt dann:

Für $a \neq 0$ und $b \neq 0$ ist $(a^{-1})^{-1} = a$ und $(a \cdot b)^{-1} = a^{-1} \cdot b^{-1}$.

In \mathbb{Q} gelten die gleichen Regeln, aber \mathbb{Z} ist nun aus dem Spiel, denn die ganzen Zahlen besitzen i.a. kein ganzzahliges Inverses!

Viel weiter kommt man bei der Herleitung weiterer Regeln nicht, es fehlt eine Verbindung zwischen Addition und Multiplikation.

3. Das Axiom vom Distributivgesetz

Distributivgesetz: $\forall x, y, z \in \mathbb{R} : x \cdot (y + z) = x \cdot y + x \cdot z.$

Hierbei dürfen Addition und Multiplikation nicht vertauscht werden! Im Gegensatz zu den Mengenverknüpfungen \cup und \cap gibt es hier nur **ein** Distributivgesetz. Dies gilt übrigens auch in \mathbb{N} , \mathbb{Z} und \mathbb{Q} .

Die Mächtigkeit des Distributivgesetzes zeigen die folgenden Aussagen:

I.2.3 Satz.

1. $\forall x \in \mathbb{R} : x \cdot 0 = 0.$
2. $(-1) \cdot (-1) = 1.$
3. Ist $x \cdot y = 0$, so ist $x = 0$ oder $y = 0$.

BEWEIS: 1) Es ist $0 + 0 = 0$, also $x \cdot 0 = x \cdot (0 + 0) = x \cdot 0 + x \cdot 0$. Da aber auch $x \cdot 0 = x \cdot 0 + 0$ ist, folgt aus der eindeutigen Lösbarkeit der Gleichung die Aussage: $x \cdot 0 = 0$.

2) haben wir schon in §1 bewiesen, als Beispiel eines direkten Beweises.

3) Sei $x \cdot y = 0$. Wir machen eine Fallunterscheidung: Ist $x = 0$, so ist man fertig. Ist $x \neq 0$, so gibt es genau eine Lösung y der Gleichung $x \cdot y = 0$. Dies kann nur $y = 0$ sein.

□

Bemerkung: Wie gewohnt schreiben wir künftig auch xy statt $x \cdot y$, $x - y$ statt $x + (-y)$ und $\frac{x}{y}$ statt $x \cdot y^{-1}$

Dem aufmerksamen Hörer sollte etwas aufgefallen sein:

Die Mengen \mathbb{Z} , \mathbb{Q} und \mathbb{R} mit der Verknüpfung $+$, sowie die Mengen $\mathbb{Q}^* := \mathbb{Q} \setminus \{0\}$ und $\mathbb{R}^* := \mathbb{R} \setminus \{0\}$ mit der Verknüpfung \cdot haben die gleiche *Struktur*. Das wird richtig deutlich, wenn man die Gesetze ein wenig anders hinschreibt:

Definition.

Sei G eine Menge. Je zwei Elementen $x, y \in G$ sei auf eindeutige Weise ein Element $x * y \in G$ zugeordnet. Man nennt G eine *Gruppe*, wenn folgendes gilt:

1. $\forall a, b, c \in G$ gilt: $(a * b) * c = a * (b * c).$
2. $\exists e \in G$, so daß $\forall a \in G$ gilt: $a * e = a$
3. $\forall a \in G \exists a' \in G$ mit $a * a' = e.$

Ist sogar $a * b = b * a$ für alle $a, b \in G$, so spricht man von einer *kommutativen* oder *Abelschen Gruppe*.

Die „Verknüpfung“ $*$ kann je nach Situation als $+$, als \cdot oder auch ganz anders geschrieben werden. Es kommt nicht auf ihre Bedeutung an, sondern auf die Gültigkeit der Gruppengesetze. Man kann übrigens zeigen, daß das neutrale Element e und zu jedem $a \in G$ das Inverse a' eindeutig bestimmt ist. Und auch in einer nicht-kommutativen Gruppe ist immer $a * e = e * a$ und $a * a' = a' * a$.

Beispiele:

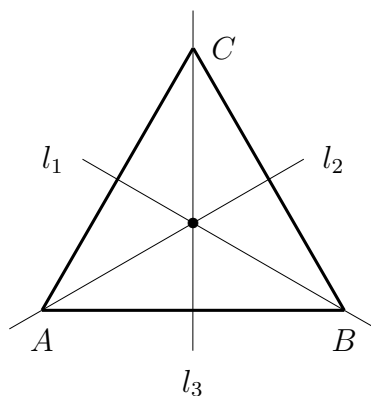
1. Die Zahlen haben schon mehrere Beispiele geliefert, etwa $(\mathbb{Z}, +)$ oder $(\mathbb{Q} \setminus \{0\}, \cdot)$.

Von \mathbb{R} verlangen wir ebenfalls, daß $(\mathbb{R}, +)$ und $(\mathbb{R} \setminus \{0\}, \cdot)$ jeweils kommutative Gruppen sind.

2. Ein Beispiel einer nicht kommutativen Gruppe konstruieren wir geometrisch. Wir betrachten ein gleichseitiges Dreieck mit den Symmetrieachsen l_1, l_2 und l_3 . Wollen wir das Dreieck so bewegen, daß es hinterher wieder mit sich selbst zur Deckung kommt, so bleiben uns 6 Möglichkeiten:

- D_0 : Drehung um 0° (d.h. keine Bewegung),
- D_{120} : Drehung um 120° ,
- D_{240} : Drehung um 240° ,
- S_1 : Spiegelung an der Achse l_1 ,
- S_2 : Spiegelung an der Achse l_2 ,
- S_3 : Spiegelung an der Achse l_3 .

Die Drehung um 360° überführt das Dreieck wieder in die Ausgangsposition, bewirkt also das gleiche wie D_0 .



Die Hintereinander-Ausführung von zwei solchen Transformationen ergibt zwangsläufig wieder eine solche. Also haben wir eine Verknüpfung (die wir mit $*$ bezeichnen), auf der Menge $G := \{D_0, D_{120}, D_{240}, S_1, S_2, S_3\}$. Diese Verknüpfung ist offensichtlich assoziativ, und eine Multiplikationstabelle kann man experimentell erstellen:

	D_0	D_{120}	D_{240}	S_1	S_2	S_3
D_0	D_0	D_{120}	D_{240}	S_1	S_2	S_3
D_{120}	D_{120}	D_{240}	D_0	S_3	S_1	S_2
D_{240}	D_{240}	D_0	D_{120}	S_2	S_3	S_1
S_1	S_1	S_2	S_3	D_0	D_{120}	D_{240}
S_2	S_2	S_3	S_1	D_{240}	D_0	D_{120}
S_3	S_3	S_1	S_2	D_{120}	D_{240}	D_0

D_0 ist das neutrale Element. Und da D_0 in jeder Zeile genau einmal vorkommt, besitzt jedes Element ein Inverses.

Damit ist G eine Gruppe. Sie ist aber nicht kommutativ, denn es ist z.B.

$$D_{120} * S_1 = S_3$$

und $S_1 * D_{120} = S_2.$

Die Welt ist voller Gruppenstrukturen, aber es gibt auch noch eine allgemeinere Struktur:

Definition.

Sei H eine nicht-leere Menge mit einer assoziativen Verknüpfung $*$. Dann nennt man H eine *Halbgruppe*.

Ein Element $e \in H$ mit $x * e = e * x = x$ für jedes $x \in H$ heißt *neutrales Element* von H .

Wohlgemerkt: In einer Halbgruppe muß kein neutrales Element existieren, aber es **kann** existieren. Wenn es existiert, dann ist es auch eindeutig bestimmt. Wichtig ist allerdings, daß man die Gültigkeit beider Gleichungen $x * e = x$ und $e * x = x$ fordern muß (im Gegensatz zur Gruppe, wo schon eine der Gleichungen reicht). Vor allem unterscheidet sich die Halbgruppenstruktur von der Gruppenstruktur darin, daß nicht jedes Element ein Inverses zu besitzen braucht.

Beispiele:

Menge:	Verknüpfung:	neutrales Element:
$P(M)$	\cup	\emptyset
$P(M)$	\cap	M
\mathbb{N}	$+$	nicht vorh.
\mathbb{N}_0	$+$	0
$\mathbb{Z} \setminus \{0\}$	\cdot	1
\mathbb{N}	ggT	nicht vorh.
\mathbb{N}	kgV	1
Strings $xyz \dots$	Verkettung	leerer String

Kehren wir zurück zur Axiomatik von \mathbb{R} . Wir haben gefordert, daß \mathbb{R} mit der Addition und $\mathbb{R} \setminus \{0\}$ mit der Multiplikation eine kommutative Gruppe bilden soll, und beide Verknüpfungen hängen über das Distributivgesetz zusammen.

Definition.

Ein *Körper* ist eine Menge K mit zwei Verknüpfungen $+$ und \cdot und zwei ausgezeichneten Elementen 0 und 1, so daß gilt:

1. K bildet mit $+$ eine kommutative Gruppe und 0 ist das zugehörige neutrale Element.
2. $K^* := K \setminus \{0\}$ bildet mit \cdot eine kommutative Gruppe und 1 ist das zugehörige neutrale Element.

3. Es gilt das Distributivgesetz.

Die rationalen Zahlen bilden den Körper \mathbb{Q} und auch \mathbb{R} ist auf Grund der bisherigen Axiome ein Körper. Weitere Beispiele kennen wir bisher noch nicht.

Aus den Axiomen folgt, daß jeder Körper zumindest die beiden (voneinander verschiedenen) Elemente 0 und 1 besitzt. Wieviele weitere Elemente er noch haben muß, ist zunächst nicht zu sehen. Wir wollen nun beweisen, daß man aus diesen beiden Elementen allein schon einen Körper basteln kann:

Sei $K_2 := \{0, 1\}$. Eine Addition und eine Multiplikation auf K_2 definiert man durch die folgenden Verknüpfungstabellen:

$$\begin{array}{c|cc} + & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array} \qquad \begin{array}{c|cc} \cdot & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & 1 \end{array}$$

Beide Verknüpfungen sind kommutativ, weil die Tabellen symmetrisch zur Diagonalen sind. Auch sieht man sofort, daß 0 das neutrale Element bzgl. der Addition und 1 das neutrale Element bzgl. der Multiplikation ist. Zu jedem $x \in K_2$ existiert das Negative (z.B. ist $-1 = 1$) und zu der 1 (dem einzigen Element $\neq 0$) existiert ein multiplikatives Inverses, es ist $1^{-1} = 1$.

Die Assoziativgesetze und das Distributivgesetz müssen in allen Fällen nachgeprüft werden, aber das ist nur eine Fleißaufgabe. K_2 ist tatsächlich ein Körper.

Was zunächst reichlich unsinnig anmutet, wird durchaus sinnvoll, wenn man die Dinge etwas anders interpretiert. Es gibt bekanntlich gerade und ungerade ganze Zahlen. Wir schreiben g für „gerade“ und u für „ungerade“. Ersetzen wir nun 0 durch g und 1 durch u , so erhalten wir die folgenden Tabellen:

$$\begin{array}{c|cc} + & g & u \\ \hline g & g & u \\ u & u & g \end{array} \qquad \begin{array}{c|cc} \cdot & g & u \\ \hline g & g & g \\ u & g & u \end{array}$$

Addieren wir etwa eine gerade und eine ungerade Zahl, so erhalten wir als Ergebnis eine ungerade Zahl. Auf diese Weise können wir die Tabellen interpretieren. Daß das so gut klappt, liegt an folgender Tatsache: Teilt man eine gerade Zahl durch 2, so bleibt der Rest 0. Teilt man eine ungerade Zahl durch 2, so bleibt der Rest 1. Addieren wir zwei Zahlen, so addieren sich die Reste. Aber den Rest 2 müssen wir wieder durch den Rest 0 ersetzen..

Die Menge \mathbb{Z} bildet mit $+$ und der Null eine kommutative Gruppe, und $\mathbb{Z} \setminus \{0\}$ bildet mit \cdot und der Eins eine (kommutative) Halbgruppe. Außerdem gilt das Distributivgesetz. Eine Menge mit einer solchen Struktur nennt man einen *Ring*. Jeder Körper ist natürlich insbesondere ein Ring, aber i.a. braucht in einem Ring nicht zu jedem $x \neq 0$ ein multiplikatives Inverses zu existieren.

Wir haben jetzt gesehen, daß \mathbb{R} ein Körper ist. Aber diese Eigenschaft zeichnet die reellen Zahlen nicht vor anderen Zahlbereichen wie etwa \mathbb{Q} aus. Wir brauchen also noch weitere Axiome.

4. Die Axiome der Anordnung

Es gibt eine Teilmenge $P \subset \mathbb{R}$ (die „Menge der positiven reellen Zahlen“), so daß gilt:

1. $a, b \in P \implies a + b \in P$ und $a \cdot b \in P$.
2. $\mathbb{R}^* = P \cup (-P)$, mit $-P := \{x \in \mathbb{R} \mid -x \in P\}$.

Bemerkung: Es ist $P \cap (-P) = \emptyset$.

Wäre nämlich $x \in P \cap (-P)$, so wäre $x \in P$ und $-x \in P$, also auch $0 := x + (-x) \in P$. Das ist aber nach Eigenschaft (2) nicht möglich.

Statt $x \in P$ schreibt man auch $x > 0$.

Weiter definiert man:

$$\begin{aligned} a < b & : \iff b - a > 0, \\ a \leq b & : \iff a < b \text{ oder } a = b, \\ a > b & : \iff b < a, \\ \text{und } a \geq b & : \iff a > b \text{ oder } a = b. \end{aligned}$$

So ist – im Gegensatz zur Umgangssprache – die Aussage „ $3 \geq 3$ “ mathematisch völlig korrekt.

I.2.4 Satz. *Ist $x \in \mathbb{R}$, so gilt genau eine der folgenden Aussagen:*

1. $x > 0$.
2. $x = 0$.
3. $x < 0$.

Außerdem gelten die folgenden Regeln:

$$\begin{aligned} a < b \text{ und } b < c & \implies a < c, \\ a < b \text{ und } c \text{ beliebig} & \implies a + c < b + c, \\ a < b \text{ und } c > 0 & \implies a \cdot c < b \cdot c, \\ a < b \text{ und } c < 0 & \implies a \cdot c > b \cdot c, \\ 0 < a < b & \implies 0 < \frac{1}{b} < \frac{1}{a}. \end{aligned}$$

Exemplarisch zeigen wir den Beweis der 2. Aussage: Ist $a < b$ und c beliebig, so ist $b - a > 0$ und daher auch $(b + c) - (a + c) = b - a > 0$, also $a + c < b + c$.

Gewisse Teilmengen von \mathbb{R} können durch Ungleichungen beschrieben werden:

Definition.

a, b seien reelle Zahlen mit $a < b$.

$$(a, b) := \{x \in \mathbb{R} \mid a < x < b\}$$

heißt *offenes Intervall* mit den Grenzen a und b ,

$$[a, b] := \{x \in \mathbb{R} \mid a \leq x \leq b\}$$

heißt *abgeschlossenes Intervall* mit den Grenzen a und b .

Beim abgeschlossenen Intervall gehören die Grenzen dazu, beim offenen nicht!⁴

Man beachte noch:

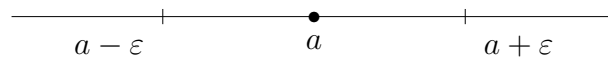
$a < x < b$ bedeutet eigentlich: $a < x$ **und** $x < b$.

Ein Punkt x liegt also genau dann *nicht* in (a, b) , wenn $x \leq a$ **oder** $x \geq b$ ist.

Speziell nennt man – für beliebiges $a \in \mathbb{R}$ und $\varepsilon > 0$ – die Menge

$$U_\varepsilon(a) := (a - \varepsilon, a + \varepsilon) = \{x \in \mathbb{R} \mid a - \varepsilon < x < a + \varepsilon\}$$

die ε -Umgebung von a .



Die Menge $\mathbb{R}_+ := \{x \in \mathbb{R} \mid x > 0\}$ heißt die *positive Halbgerade*,
und $\mathbb{R}_- := \{x \in \mathbb{R} \mid x < 0\}$ die *negative Halbgerade*.

Definition.

Der *Absolutbetrag* einer reellen Zahl ist gegeben durch

$$|a| := \begin{cases} a & \text{falls } a \geq 0 \\ -a & \text{falls } a < 0 \end{cases}$$

So ist z.B. $|3| = 3$ und $|-7| = 7$.

$|a - b| = |b - a|$ ist der Abstand von a und b auf der Zahlengeraden.

Für das Rechnen mit Beträgen haben wir die folgenden Regeln:

I.2.5 Satz.

1. $|a \cdot b| = |a| \cdot |b|$.
2. Es ist stets $-|a| \leq a \leq +|a|$.
3. Sei $c > 0$. Dann ist $|x| < c \iff -c < x < +c$.

⁴Für das offene Intervall (a, b) sind auch andere Symbole im Gebrauch, wie etwa $\langle a, b \rangle$ oder $]a, b[$.

4. Es gilt die **Dreiecks-Ungleichung**: $|a + b| \leq |a| + |b|$.

5. Es ist $|a - b| \geq |a| - |b|$.

Zum BEWEIS: (1) und (2) erhält man durch Fallunterscheidung.

3) Ist $|x| < c$, so ist $-|x| > -c$ und daher

$$-c < -|x| \leq x \leq |x| < c.$$

Die Umkehrung erledigt man wieder durch Fallunterscheidung.

Wegen (2) ist $-|a| - |b| \leq a + b \leq |a| + |b|$. Wegen (3) folgt daraus die Dreiecksungleichung.

Zum Beweis von (5) benutzt man einen beliebigen Trick:

Es ist $|a| = |(a - b) + b| \leq |a - b| + |b|$. □

Als Konsequenz aus (3) erhalten wir z.B.:

$$\begin{aligned} x \in U_\varepsilon(a) &\iff a - \varepsilon < x < a + \varepsilon \\ &\iff -\varepsilon < x - a < +\varepsilon \\ &\iff |x - a| < \varepsilon. \end{aligned}$$

Die ε -Umgebung von a ist also die Menge derjenigen x , deren Abstand von a kleiner als ε ist.

Alles, was wir bisher gemacht haben, funktioniert auch in \mathbb{Q} . Brauchen wir überhaupt einen größeren Zahlenbereich?

Irgendwann im Laufe der Schulzeit beweist man den Satz:

Es gibt keine rationale Zahl q mit $q^2 = 2$.

Na und? Dann braucht man sich mit Wurzeln überhaupt nicht herumzuplagen. Um so besser!

Leider kommt man mit diesem Standpunkt nicht so weit. Betrachten wir den Graphen der Funktion $f(x) := x^2 - 2$, so sehen wir, daß dieser Graph die x-Achse in zwei Punkten trifft. Punkte auf der x-Achse fassen wir als reelle Zahlen auf, und hier haben wir welche gefunden, die nicht rational sind. Wir können die als Schnittpunkte auftretenden Zahlen $\sqrt{2}$ und $-\sqrt{2}$ sehr genau durch rationale Zahlen von unten und oben approximieren, aber wir müssen dabei immer einen gewissen Fehler in Kauf nehmen. Wir brauchen also ein zusätzliches Axiom, das uns die Existenz der reellen Zahl $\sqrt{2}$ sichert.

5. Das Vollständigkeitsaxiom

M und N seien zwei nicht-leere Mengen reeller Zahlen, so daß $x \leq y$ für alle $x \in M$ und alle $y \in N$ gilt.

Dann existiert eine Zahl $c \in \mathbb{R}$ mit $x \leq c \leq y$ für $x \in M$ und $y \in N$.

Wir werden weiter unten zeigen, daß dieses Axiom ausreicht, um die Existenz von $\sqrt{2}$ zu beweisen.

Definition.

Eine Menge $M \subset \mathbb{R}$ heißt *nach oben* (bzw. *nach unten*) *beschränkt*, falls es eine reelle Zahl c gibt, so daß $x \leq c$ (bzw. $x \geq c$) für $x \in M$ ist. Die Zahl c nennt man dann eine *obere* (bzw. *untere*) *Schranke*.

M heißt *beschränkt*, wenn M nach oben und nach unten beschränkt ist.

Definition.

Sei $M \subset \mathbb{R}$ eine nach oben beschränkte Menge. Wenn die Menge aller oberen Schranken von M ein kleinstes Element a besitzt, so nennt man a *die kleinste obere Schranke* oder *das Supremum* von M (in Zeichen: $a = \sup(M)$).

Die größte untere Schranke einer nach unten beschränkten Menge M nennt man – wenn sie existiert – das *Infimum* von M (in Zeichen: $a = \inf(M)$).

Z.B. ist $\sup((a, b)) = b$ und $\sup([a, b]) = b$. Das Supremum einer Menge kann also zu der Menge gehören, braucht es aber nicht.

I.2.6 Satz. Sei $M \subset \mathbb{R}$ eine nicht-leere Menge.

1. Ist M nach oben beschränkt, so besitzt M ein Supremum.
2. Ist M nach unten beschränkt, so besitzt M ein Infimum.

BEWEIS: (für den ersten Teil)

Sei S die Menge der oberen Schranken von M . Nach Voraussetzung ist $S \neq \emptyset$, und für $x \in M$ und $y \in S$ ist $x \leq y$. Wegen des Vollständigkeitsaxioms gibt es ein $c \in \mathbb{R}$, so daß $x \leq c \leq y$ für $x \in M$ und $y \in S$ ist. Aber dann gehört c sogar zu S und ist damit die kleinste obere Schranke von M . \square

I.2.7 Satz (Prinzip von Archimedes).

Zu jeder reellen Zahl x gibt es ein $n \in \mathbb{N}$ mit $n > x$.

BEWEIS: Wir nehmen an, es gibt ein $x \in \mathbb{R}$, so daß $x \geq n$ für alle $n \in \mathbb{N}$ ist. Dann ist x eine obere Schranke für \mathbb{N} , und es existiert $a := \sup(\mathbb{N})$. Die Zahl $a - 1$ kann dann keine obere Schranke von \mathbb{N} mehr sein. Also gibt es ein $n_0 \in \mathbb{N}$ mit $n_0 > a - 1$. Aber dann ist $a < n_0 + 1$, und das ist ein Widerspruch! \square

I.2.8 Folgerung (ε -Prinzip).

Ist ε eine beliebige **positive** reelle Zahl, so gibt es ein $n \in \mathbb{N}$ mit $\frac{1}{n} < \varepsilon$.

BEWEIS: Ist $\varepsilon > 0$, so ist auch $x := \frac{1}{\varepsilon}$ eine positive reelle Zahl, und nach Archimedes gibt es ein $n \in \mathbb{N}$ mit $x < n$. Aber dann ist $\varepsilon = \frac{1}{x} > \frac{1}{n}$. \square

Beispiel:

Es ist $\inf\{\frac{1}{n} \mid n \in \mathbb{N}\} = 0$, denn 0 ist eine untere Schranke der Menge, aber jede Zahl $c > 0$ ist keine untere Schranke mehr.

Wie kann man nun die Existenz von $\sqrt{2}$ zeigen? Wir betrachten die Mengen

$$M := \{x \in \mathbb{R} \mid x > 0 \text{ und } x^2 < 2\}$$

$$\text{und } N := \{x \in \mathbb{R} \mid x > 0 \text{ und } x^2 > 2\}.$$

Es ist z.B. $\frac{14}{10} \in M$ und $\frac{15}{10} \in N$, also sind beide Mengen nicht leer. Außerdem überzeugt man sich leicht davon, daß $x \leq y$ für $x \in M$ und $y \in N$ ist.

Das Vollständigkeitsaxiom sichert die Existenz einer Zahl c zwischen M und N . Mit einem etwas kniffligen Widerspruchsbeweis zeigt man nun, daß $c^2 = 2$ sein muß:

Die Zahl $z := 2 - c^2$ muß > 0 , $= 0$ oder < 0 sein. Nehmen wir etwa an, $z > 0$, also $c \in M$. Die Idee ist nun, zu zeigen, daß dann auch noch $c + \varepsilon$ in M liegt, wenn man nur ε klein genug wählt. Das wäre der gewünschte Widerspruch, denn wir hätten ein $x \in M$ mit $x > c$ gefunden.

Es ist $(c + \varepsilon)^2 = c^2 + \varepsilon(2c + \varepsilon)$. Nach dem ε -Prinzip kann man zu jeder positiven reellen Zahl eine andere positive Zahl finden, die kleiner ist. Daher kann man erreichen, daß $\varepsilon(2c + \varepsilon) < z$ wird, also $(c + \varepsilon)^2 < 2$ (die Details ersparen wir uns hier).

Den Fall $z < 0$ führt man genauso zum Widerspruch, es bleibt nur: $z = 0$, also $c^2 = 2$.

Analog zeigt man:

I.2.9 Satz. *Zu jeder positiven reellen Zahl a und jedem $n \in \mathbb{N}$ gibt es genau eine positive Lösung der Gleichung $x^n = a$.*

Die Lösung bezeichnet man mit $\sqrt[n]{a}$ oder $a^{\frac{1}{n}}$.

In manchen Fällen kann man auch Wurzeln aus negativen Zahlen ziehen, z.B. ist

$$\sqrt[3]{-27} = -3.$$

§3 Folgen und Konvergenz

Wenn wir irgend ein **unendliches** System von reellen Zahlen a_1, a_2, a_3, \dots vorliegen haben, so sprechen wir von einer

Folge reeller Zahlen (a_n) .

Definition.

1. Eine Folge (a_n) heißt *konstant*, falls es ein $a \in \mathbb{R}$ gibt, so daß $a_n = a$ für alle $n \in \mathbb{N}$ ist.
2. Eine Folge (a_n) heißt

nach oben beschränkt (bzw. *nach unten beschränkt*),

falls es ein $c \in \mathbb{R}$ gibt, so daß für alle $n \in \mathbb{N}$ gilt:

$$a_n \leq c \quad (\text{bzw. } c \leq a_n).$$

3. (a_n) heißt *beschränkt*, falls (a_n) nach oben **und** nach unten beschränkt ist.
4. Eine Folge heißt *unbeschränkt*, falls sie nicht beschränkt ist. (Sie ist dann **entweder** *nicht* nach oben beschränkt **oder** *nicht* nach unten beschränkt **oder** in beiden Richtungen *nicht* beschränkt.)

Beispiele :

1. Durch $a_n := n$ wird die Folge der natürlichen Zahlen $1, 2, 3, 4, \dots$ gegeben. Das Prinzip des Archimedes besagt, daß diese Folge unbeschränkt ist.
2. Durch $a_n := (-1)^n$ erhält man die seltsame Folge

$$-1, +1, -1, +1, \dots .$$

Sie ist offensichtlich beschränkt, es werden ja nur die beiden Werte -1 und $+1$ angenommen.

Hinweis: Ist (a_n) eine Folge, so kann man dazu die Menge der Folgenglieder bilden: $M := \{a_n \mid n \in \mathbb{N}\}$. Diese Menge ist *etwas ganz anderes* als die Folge selbst. Die Folge in unserem Beispiel besitzt unendlich viele Glieder, die zugehörige Menge $M = \{-1, +1\}$ besteht aber nur aus 2 Elementen. Der Grund dafür liegt in der Mengendefinition. Kommt ein Objekt mehrfach als Element einer Menge vor, so darf es nur einmal gezählt werden! Bei einer Folge sind die Glieder dagegen schon durch ihre Nummer voneinander zu unterscheiden, die Werte dürfen ruhig gleich sein.

3. Durch $a_n := \frac{1}{n}$ wird die Folge der „Stammbrüche“ $1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \dots$ definiert. Diese Folge ist nach unten durch 0 und nach oben durch 1 beschränkt.

Die zuletzt betrachtete Folge hat eine bemerkenswerte Eigenschaft: Die Werte der Folgeglieder kommen der Null immer näher, ja, sogar beliebig nahe! Wie kann man das, was anschaulich klar ist, exakt formulieren? Tatsächlich wird der Wert 0 ja nie angenommen.

Stellen Sie sich vor, wir wären über das Problem in Streit geraten. Sie trauen ihrer Anschauung und glauben, daß die Folgeglieder der Null beliebig nahe kommen, ja, Sie haben an der Schule schon einmal gehört, daß die Folge der Stammbrüche gegen Null „konvergiert“, was auch immer das heißen mag. Ich dagegen bin skeptisch: „Wie nahe kommen die a_n der Null denn tatsächlich, etwa näher als $1/1000$?“

„Sicher!“, sagen Sie. „Wenn $n \geq 1001$ ist, dann ist $a_n = \frac{1}{n} \leq \frac{1}{1001} < 1/1000$.“

„Ja, aber kommen die a_n der Null auch näher als $1/3\,000\,000$?“

„Natürlich, sobald $n \geq 3\,000\,001$ ist.“

Und wenn wir nicht mit dem Streitgespräch aufhören, dann sind wir am Ende des Semesters immer noch dabei. Die Tatsache, daß Sie immer wieder eine passende Antwort finden, benutzen wir, um den Konvergenzbegriff exakt einzuführen.

Definition.

Eine Folge (a_n) konvergiert gegen die reelle Zahl a , falls gilt:

Zu jedem vorgegebenen $\varepsilon > 0$ gibt es eine Nummer n_0 , so daß für alle weiteren Nummern $n \geq n_0$ das a_n um weniger als ε von a entfernt ist.

In Formeln kann man das etwas kürzer ausdrücken:

$$\forall \varepsilon > 0 \exists n_0, \text{ so daß } \forall n \geq n_0 \text{ gilt: } |a - a_n| < \varepsilon.$$

Man nennt dann a den *Grenzwert* oder *Limes* der Folge und schreibt:

$$\lim_{n \rightarrow \infty} a_n = a.$$

Wenn die Folge nicht konvergiert, heißt sie *divergent*.

Die Verschachtelung von „Quantoren“ $\forall \dots \exists \dots \forall \dots$ bereitet zu Anfang Schwierigkeiten, und mancher lernt's nie. Deshalb kommt hier noch eine weitere Formulierung der Konvergenz:

Wir sagen, *fast alle Folgeglieder* a_n liegen in einer Menge M , wenn es höchstens endlich viele Ausnahmen gibt. Geht man die Folgeglieder der Reihe nach durch, so hat man irgendwann alle Ausnahmen hinter sich gebracht und damit ein n_0 erreicht, so daß für $n \geq n_0$ alle a_n in M liegen. Mit dieser Sprechweise können wir sagen:

(a_n) konvergiert genau dann gegen a , wenn gilt:

In jeder ε -Umgebung von a liegen fast alle a_n .

I.3.1 Satz.

$$\lim_{n \rightarrow \infty} \frac{1}{n} = 0.$$

BEWEIS: Wir müssen nur feststellen, daß in jeder ε -Umgebung fast alle Folgeglieder liegen.

Aber das ist genau die Aussage des ε -Prinzips. Ist nämlich ein beliebiges $\varepsilon > 0$ vorgegeben, so gibt es eine natürliche Zahl n_0 mit $\frac{1}{n_0} < \varepsilon$.

Ist nun $n \geq n_0$, so ist

$$\left| \frac{1}{n} - 0 \right| = \frac{1}{n} \leq \frac{1}{n_0} < \varepsilon.$$

Also ist alles bestens! □

Es kommt manchmal vor, daß eine Folge zwar nicht konvergiert, sich aber dennoch einem bestimmten Wert beliebig annähert.

Definition.

$a \in \mathbb{R}$ heißt *Häufungspunkt* der Folge (a_n) , falls gilt:

In jeder ε -Umgebung von a liegen unendlich viele Folgeglieder a_n .

Beispiele:

1. $1, 2, 3, 4, \dots$ hat keinen Häufungspunkt.
2. $1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \dots$ hat die 0 als einzigen Häufungspunkt. Der ist zugleich der Limes.
3. $a_n := (-1)^n = -1, +1, -1, +1, -1, \dots$ hat zwei Häufungspunkte, nämlich $+1$ und -1 . Sie konvergiert weder gegen $+1$ noch gegen -1 , weil sie sich immer wieder von diesen Punkten entfernt.

Man muß also sorgfältig unterscheiden, ob in einer Umgebung „nur“ unendlich viele oder sogar fast alle Folgeglieder liegen.

4. Die Folge

$$a_n := \begin{cases} n & \text{falls } n \text{ gerade} \\ \frac{1}{n} & \text{falls } n \text{ ungerade} \end{cases}$$

hat einen Häufungspunkt, nämlich die 0. Sie konvergiert aber nicht gegen 0, sie ist sogar unbeschränkt!

Ein Häufungspunkt ist also i.a. nicht der Grenzwert. Umgekehrt gilt aber offensichtlich:

Wenn die Folge (a_n) gegen $a \in \mathbb{R}$ konvergiert, dann ist a auch der einzige Häufungspunkt der Folge.

Wir kommen jetzt zu einem sehr wichtigen Satz über Folgen:

I.3.2 Satz von Bolzano–Weierstraß. *Jede beschränkte Folge (a_n) besitzt (mindestens) einen Häufungspunkt.*

Wir verzichten hier auf einen genauen Beweis. Man konstruiert – durch fortgesetzte Halbierung und geeignete Auswahl – eine Folge von abgeschlossenen Teilintervallen

$$I_0 \supset I_1 \supset I_2 \supset \dots,$$

so daß in jedem I_n unendlich viele Folgenglieder liegen. Die Intervalle müssen einen gemeinsamen Punkt x_0 besitzen, der sich als der gesuchte Häufungspunkt herausstellt.

I.3.3 Satz. *Eine Folge ist genau dann konvergent, wenn sie beschränkt ist und genau einen Häufungspunkt besitzt.*

Der einzige Häufungspunkt ist auch der Grenzwert.

Wir verzichten auch hier auf den Beweis.

Beispiel:

Sei $a_n := (-1)^n \frac{n}{n+1}$. Das ist die Folge

$$-\frac{1}{2}, \quad \frac{2}{3}, \quad -\frac{3}{4}, \quad \frac{4}{5}, \quad -\frac{5}{6}, \quad \dots$$

Für die positiven Terme $a_{2n} = \frac{2n}{2n+1}$ gilt:

$$|1 - a_{2n}| = \left| \frac{2n+1}{2n+1} - \frac{2n}{2n+1} \right| = \frac{1}{2n+1}.$$

Da $2n+1$ über alle Grenzen wächst, kommt $\frac{1}{2n+1}$ der Null beliebig nahe, d.h.:

Für alle $\varepsilon > 0$ liegen fast alle a_{2n} in $U_\varepsilon(1)$.

Also ist 1 ein Häufungspunkt der Folge. Genauso zeigt man, daß auch -1 ein Häufungspunkt ist. Aus dem Satz von oben folgt nun, daß (a_n) nicht konvergiert, also eine divergente Folge ist.

Im Beispiel ist zu sehen, daß es für jeden der beiden Häufungspunkte eine Teilfolge gibt, die gegen diesen Punkt konvergiert. Das ist ein allgemeingültiges Prinzip:

Ist a Häufungspunkt der Folge (a_n) , so gibt es eine Teilfolge von (a_n) , die gegen a konvergiert.

Wir haben gesehen, daß es schon bei relativ einfachen Folgen ziemlich mühsam ist, Häufungspunkte oder Grenzwerte zu bestimmen. Zum Glück gibt es eine Reihe von Regeln zur Berechnung von Grenzwerten, die wir hier ohne Beweis übernehmen:

I.3.4 Satz. *Die Folgen (a_n) bzw. (b_n) seien konvergent gegen a bzw. b . Dann gilt:*

$$\lim_{n \rightarrow \infty} a_n \pm b_n = a \pm b,$$

und $\lim_{n \rightarrow \infty} a_n \cdot b_n = a \cdot b.$

Sind b und alle $b_n \neq 0$, so ist

$$\lim_{n \rightarrow \infty} \frac{a_n}{b_n} = \frac{a}{b}.$$

Ist (x_n) eine weitere Folge und $a_n \leq x_n \leq b_n$ für alle n , so gelten folgende „Vergleichsregeln“:

1. Konvergiert (x_n) gegen x , so ist $a \leq x \leq b$.
2. Ist über (x_n) nichts bekannt, aber $a = b$, so folgt, daß (x_n) gegen a konvergiert.

Bisher sind wir mit dem Begriff „unendlich“ etwas zaghaft umgegangen. Wir wollen uns jetzt das Leben erleichtern:

Die *erweiterte Zahlengerade* $\overline{\mathbb{R}}$ besteht aus der Menge \mathbb{R} und zwei weiteren Elementen $-\infty$ und $+\infty$, die nicht zu \mathbb{R} gehören und auch voneinander verschieden sind:

$$\overline{\mathbb{R}} = \mathbb{R} \cup \{-\infty, +\infty\}.$$

Die Rechenregeln von \mathbb{R} dürfen nicht auf $-\infty$ und $+\infty$ angewandt werden, aber es gilt folgende Ordnungs-Beziehung:

$$\forall x \in \mathbb{R} : \quad -\infty < x < +\infty.$$

Insbesondere soll das auch bedeuten, daß $-\infty < +\infty$ ist.

Wir definieren jetzt:

$$\begin{aligned} \lim_{n \rightarrow \infty} a_n = +\infty & : \iff \forall c \in \mathbb{R} \text{ gilt: Fast alle } a_n \text{ sind } > c. \\ \lim_{n \rightarrow \infty} a_n = -\infty & : \iff \forall c \in \mathbb{R} \text{ gilt: Fast alle } a_n \text{ sind } < c. \end{aligned}$$

Beispiele :

1. $a_n := \frac{3n}{n+1} = \frac{3}{1+\frac{1}{n}}$ konvergiert gegen $\frac{3}{1+0} = 3$.
2. $a_n := \frac{n(n-2)}{5n^2+3} = \frac{n^2-2n}{5n^2+3} = \frac{1-2 \cdot \frac{1}{n}}{5+3 \cdot \frac{1}{n} \cdot \frac{1}{n}}$ konvergiert gegen $\frac{1}{5}$.

Der Trick ist immer der gleiche: Man kürzt die höchste Potenz von n heraus. Das geht allerdings nur so lange gut, wie diese höchste Potenz im Nenner auftritt. Enthält der Zähler n in höherer Potenz als der Nenner, so passiert z.B. folgendes:

$$a_n := \frac{n^3-1}{5+n} = \frac{n^2-\frac{1}{n}}{\frac{5}{n}+1} \text{ konvergiert gegen } +\infty.$$

3. Nun zu etwas komplizierteren Beispielen:

Sei $b \geq 1$ und $a_n := \sqrt[n]{b}$. Da $a_n \geq 1$ ist, können wir schreiben:

$$a_n = 1 + h_n, \text{ mit } h_n \geq 0.$$

Dann ist $b = (a_n)^n = (1 + h_n)^n \geq 1 + n \cdot h_n$, also

$$0 \leq h_n \leq \frac{b-1}{n}.$$

Daraus folgt, daß $\lim_{n \rightarrow \infty} h_n = 0$ und $\lim_{n \rightarrow \infty} a_n = 1$ ist.

4. Den Trick von oben sollte man sich merken, denn jetzt wird's noch schwieriger:

Sei $a_n := \sqrt[n]{n}$. Eine Vorhersage über das Ergebnis ist nicht so ohne weiteres möglich. Wir gehen wie beim vorigen Beispiel an die Sache heran, benutzen aber noch einen weiteren Trick:

Da $a_n > 1$ ist, ist $b_n := \sqrt{a_n} = 1 + h_n$ mit $h_n > 0$.

Dabei ist $b_n = \sqrt[n]{\sqrt{n}}$, also

$$\sqrt{n} = (b_n)^n = (1 + h_n)^n \geq 1 + n \cdot h_n.$$

Damit ist

$$h_n \leq \frac{\sqrt{n} - 1}{n} = \frac{1 - 1/\sqrt{n}}{\sqrt{n}} \leq \frac{1}{\sqrt{n}},$$

also

$$1 < a_n = (b_n)^2 = (1 + h_n)^2 = 1 + 2h_n + (h_n)^2 \leq 1 + \frac{2}{\sqrt{n}} + \frac{1}{n}.$$

Das bedeutet, daß (a_n) gegen 1 konvergiert.

5. Wir betrachten nun die Folge q^n für $q \in \mathbb{R}_+$.

- (a) Ist $q > 1$, also $q = 1 + h$ mit $h > 0$, so ist $q^n = (1 + h)^n \geq 1 + n \cdot h$, und dieser Ausdruck konvergiert gegen $+\infty$.
- (b) Ist $q = 1$, so ist $q^n = 1$ eine konstante Folge.
- (c) Sei $0 < q < 1$. Dann ist $\frac{1}{q} > 1$, also wächst $\left(\frac{1}{q}\right)^n$ über alle Grenzen. Daraus folgt: $\lim_{n \rightarrow \infty} q^n = 0$.

Eine ganz andere Klasse von Beispielen erhält man folgendermaßen:

$$\text{Sei } a_n := \sum_{i=0}^n q^i = \frac{q^{n+1} - 1}{q - 1} \quad (\text{für } q \neq 1).$$

Wir betrachten hier nur den Fall $q > 0$:

- 1. Ist $q > 1$, so ist q^n und damit erst recht $a_n = 1 + q + q^2 + \cdots + q^n$ unbeschränkt.
- 2. Ist $0 < q < 1$, so strebt $q^{n+1} = q \cdot q^n$ gegen Null, also a_n gegen $\frac{1}{q-1}$.

Es ist

$$\begin{aligned} a_1 &= 1 + q, \\ a_2 &= 1 + q + q^2, \\ a_3 &= 1 + q + q^2 + q^3, \\ &\vdots \end{aligned}$$

Im Grenzwert werden unendlich viele Terme addiert. Man spricht daher von einer *unendlichen Reihe* und schreibt

$$\lim_{n \rightarrow \infty} a_n = \sum_{i=0}^{\infty} q^i = \frac{1}{1-q}.$$

Wir werden zu einem späteren Zeitpunkt noch viele andere Reihen kennenlernen, das hier betrachtete Beispiel ist die sogenannte *geometrische Reihe*. Sie kommt in der Mathematik sehr häufig vor.

Beispiel:

Es ist

$$\sum_{i=0}^{\infty} \left(\frac{1}{2}\right)^i = \frac{1}{1-\frac{1}{2}} = 2,$$

also $\sum_{i=1}^{\infty} \left(\frac{1}{2}\right)^i = 1$. Das liefert die wundersame Formel

$$\boxed{\frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \frac{1}{16} + \dots = 1.}$$

Sie zeigt, warum Achilles bei seinem Wettlauf mit der Schildkröte doch gewonnen hat.

Eine andere wichtige Klasse von Folgen sind die monotonen Folgen:

Definition.

Eine Folge (a_n) heißt *monoton wachsend* (bzw. *monoton fallend*), falls gilt:

$$a_n \leq a_{n+1} \quad (\text{bzw. } a_n \geq a_{n+1}) \quad \text{für alle } n \in \mathbb{N}.$$

Z.B. ist die Folge $a_n := \frac{1}{n}$ monoton fallend, während die Folge $a_n := \sum_{i=0}^n q^i$ (mit $q > 0$) monoton wachsend ist.

I.3.5 Satz von der monotonen Konvergenz. Die Folge (a_n) sei monoton wachsend und nach oben beschränkt. Dann ist sie konvergent.

BEWEIS: Es gibt nach Voraussetzung eine reelle Zahl c , so daß $a_1 \leq a_n \leq c$ für alle $n \in \mathbb{N}$ ist. Also ist (a_n) beschränkt und besitzt nach dem Satz von Bolzano-Weierstraß einen Häufungspunkt a . Wir wollen zeigen, daß es der einzige Häufungspunkt und damit schon der Grenzwert ist.

Wenn es ein $n_0 \in \mathbb{N}$ mit $a_{n_0} > a$ gäbe, dann wäre wegen der Monotonie sogar $a_n > a$ für alle $n \geq n_0$, also für fast alle n . Wählt man dann ein ε mit $a < a + \varepsilon < a_{n_0}$, so können höchstens endlich viele a_n in $U_\varepsilon(a)$ liegen. Das widerspricht der Tatsache, daß a Häufungspunkt ist.

Also ist $a_n \leq a$ für alle $n \in \mathbb{N}$. Eine Zahl $b > a$ hat dann keine Chance mehr, Häufungspunkt von (a_n) zu sein. Wenn es aber ein $b < a$ gäbe, das Häufungspunkt ist, dann müßte – nach der gleichen Argumentation wie eben – schon $a_n \leq b$ für alle $n \in \mathbb{N}$ sein, und die

Zahl a könnte kein Häufungspunkt der Folge sein. Also besitzt (a_n) nur einen einzigen Häufungspunkt und ist damit konvergent! \square

Der Satz von der monotonen Konvergenz ist ein äußerst nützliches Kriterium, um die Konvergenz einer Folge zu beweisen. Ist die Konvergenz erst einmal gesichert, dann gibt es oftmals Mittel und Wege, auch noch den Grenzwert herauszubekommen.

Beispiel:

Es sei $a_1 := \sqrt{2}$, $a_2 := \sqrt{2 + \sqrt{2}}$, $a_3 := \sqrt{2 + \sqrt{2 + \sqrt{2}}}$ und allgemein $a_{n+1} := \sqrt{2 + a_n}$.

Das ist eine *rekursive Definition*. Daß auf diese Weise alle Folgenglieder bestimmt sind, ergibt sich unmittelbar aus dem Prinzip der vollständigen Induktion. Rekursive Formeln lassen sich besonders gut mit dem Computer bearbeiten.

Wir wollen zeigen, daß (a_n) monoton wachsend und nach oben durch 2 beschränkt ist.

Wegen der rekursiven Definition müssen wir fast zwangsläufig das Induktionsprinzip verwenden: Offensichtlich ist $a_1 = \sqrt{2} < 2$, und da $2 < 2 + \sqrt{2}$ ist, ist $a_1 < a_2$. Damit ist der Induktionsanfang erledigt.

1. Ist nach Induktionsvoraussetzung $a_n < 2$, so ist $a_n + 2 < 4$, und damit $a_{n+1} = \sqrt{a_n + 2} < \sqrt{4} = 2$. Das war ganz einfach.
2. Bei der Monotonie lautet die Induktionsvoraussetzung $a_n < a_{n+1}$. Aber dann ist $2 + a_n < 2 + a_{n+1}$, und damit

$$a_{n+1} = \sqrt{2 + a_n} < \sqrt{2 + a_{n+1}} = a_{n+2}.$$

Damit ist auch hier der Induktionsschluß vollzogen.

Aus dem Satz von der monotonen Konvergenz folgt jetzt, daß (a_n) konvergent ist. Mit einem einfachen Trick ermitteln wir den Grenzwert:

Mit (a_n) ist natürlich auch (b_n) mit $b_n := a_{n+1}$ konvergent. Beide Folgen konvergieren gegen den gleichen Grenzwert, eine reelle Zahl a . Nun ist $b_n = \sqrt{2 + a_n}$, also

$$a^2 = \left(\lim_{n \rightarrow \infty} b_n\right)^2 = \lim_{n \rightarrow \infty} (b_n)^2 = \lim_{n \rightarrow \infty} (2 + a_n) = 2 + a.$$

Das bedeutet, daß $a^2 - a - 2 = 0$ ist, also $a = \frac{1 \pm \sqrt{1 + 2 \cdot 4}}{2} = \frac{1 \pm 3}{2}$. Da alle Folgenglieder ≥ 0 sind, muß auch $a \geq 0$ sein, also $a = 2$.

Gelegentlich kann man auch neue (irrationale) Zahlen als Grenzwerte von Folgen einführen:

Es sei

$$a_n := \sum_{\nu=0}^n \frac{1}{\nu!} = 1 + 1 + \frac{1}{2} + \frac{1}{6} + \frac{1}{24} + \cdots + \frac{1}{n!}.$$

Es handelt sich mal wieder um eine Reihe, diesmal aber keine geometrische Reihe. Offensichtlich ist (a_n) monoton wachsend. Da die einzelnen Summanden ab einer gewissen Stelle stets schneller schrumpfen als die Summanden der geometrischen Reihe, dürfen wir vermuten, daß (a_n) konvergiert.

Tatsächlich ist

$$\frac{1}{\nu!} = \frac{1}{2} \cdot \frac{1}{3} \cdot \dots \cdot \frac{1}{\nu} < \frac{1}{2} \cdot \frac{1}{2} \cdot \dots \cdot \frac{1}{2} = \frac{1}{2^{\nu-1}},$$

also

$$\begin{aligned} a_n &< 1 + 1 + \sum_{\nu=2}^n \left(\frac{1}{2}\right)^{\nu-1} \\ &= 1 + \sum_{\mu=0}^{n-1} \left(\frac{1}{2}\right)^{\mu} \\ &= 1 + \frac{1 - \left(\frac{1}{2}\right)^n}{1 - \frac{1}{2}} \\ &< 1 + 2 = 3. \end{aligned}$$

Als beschränkte monotone Folge ist (a_n) konvergent, und der Grenzwert

$$e := \lim_{n \rightarrow \infty} a_n = \sum_{\nu=0}^{\infty} \frac{1}{\nu!}$$

heißt *Eulersche Zahl*.

Man sieht sofort, daß $2 < e \leq 3$ ist. Eine genauere Analyse ergibt

$$e = 2.718281\dots,$$

und man kann relativ leicht zeigen, daß e irrational ist.

Als nächstes untersuchen wir die Folge

$$b_n := \left(1 + \frac{1}{n}\right)^n \quad (b_1 = 2, b_2 = 2.25, b_3 = 2.37\dots, \dots).$$

Mit der binomischen Formel erhalten wir:

$$\begin{aligned} b_n &= \sum_{k=0}^n \binom{n}{k} \frac{1}{n^k} = \sum_{k=0}^n \frac{1}{k!} \cdot \frac{(n-k+1) \cdot \dots \cdot (n-1)n}{n^k} \\ &= \sum_{k=0}^n \frac{1}{k!} \cdot \frac{n}{n} \cdot \frac{n-1}{n} \cdot \frac{n-2}{n} \cdot \dots \cdot \frac{n-k+1}{n} \\ &= \sum_{k=0}^n \frac{1}{k!} \cdot \left(1 - \frac{1}{n}\right) \left(1 - \frac{2}{n}\right) \cdot \dots \cdot \left(1 - \frac{k-1}{n}\right) \\ &< \sum_{k=0}^n \frac{1}{k!} < e. \end{aligned}$$

Also ist (b_n) nach oben beschränkt durch die Eulersche Zahl. Weiter gilt:

$$\begin{aligned}
 b_{n+1} &= \left(1 + \frac{1}{n+1}\right)^{n+1} = \sum_{k=0}^{n+1} \binom{n+1}{k} \frac{1}{(n+1)^k} \\
 &= \sum_{k=0}^{n+1} \frac{1}{k!} \cdot \frac{(n+1)n(n-1) \cdots (n-k+2)}{(n+1)^k} \\
 &\geq \sum_{k=0}^n \frac{1}{k!} \cdot \frac{n}{n+1} \cdot \frac{n-1}{n+1} \cdots \frac{n-(k-2)}{n+1} \\
 &> \sum_{k=0}^n \frac{1}{k!} \cdot \frac{n-1}{n} \cdots \frac{n-(k-1)}{n} \\
 &= b_n.
 \end{aligned}$$

Damit ist (b_n) monoton wachsend, also konvergent gegen eine Zahl $e^* \leq e$. Um den Grenzwert näher zu bestimmen, brauchen wir einen Trick! Ist $m \geq 2$ irgend eine feste natürliche Zahl und $n > m$, so gilt:

$$\begin{aligned}
 b_n &= \sum_{k=0}^n \frac{1}{k!} \cdot \frac{n-1}{n} \cdots \frac{n-(k-1)}{n} \\
 &\geq \sum_{k=0}^m \frac{1}{k!} \cdot \left(1 - \frac{1}{n}\right) \left(1 - \frac{2}{n}\right) \cdots \left(1 - \frac{k-1}{n}\right).
 \end{aligned}$$

Läßt man $n \rightarrow \infty$ gehen (bei festem m), so erhält man:

$$e^* = \lim_{n \rightarrow \infty} b_n \geq \sum_{k=0}^m \frac{1}{k!}, \text{ für jedes } m \geq 2.$$

Also ist schließlich $e^* \geq e$, und damit

$$e = \lim_{n \rightarrow \infty} \left(1 + \frac{1}{n}\right)^n = \sum_{k=0}^{\infty} \frac{1}{k!}.$$

So haben wir zwei verschiedene Darstellungen der Eulerschen Zahl gewonnen.

§ 4 Der Abbildungsbegriff

A und B seien zwei Mengen. Dann kann man je ein Element $x \in A$ und ein Element $y \in B$ zu einem *Paar* (x, y) zusammenfassen. Man nennt x die *erste Komponente* und y die *zweite Komponente* des Paares (x, y) . Es kommt auf die Reihenfolge an, d.h., es gilt:

$$(a, b) = (c, d) \iff a = c \text{ und } b = d.$$

Die Menge aller möglichen Paare nennt man die *Paarmenge*, *Produktmenge* oder das *kartesische Produkt* von A und B und schreibt dafür $A \times B$. Es gilt also:

$$A \times B = \{(x, y) \mid x \in A \text{ und } y \in B\}.$$

Das kartesische Produkt von A mit sich selbst bezeichnet man auch mit A^2 . Hier muß besonders auf die Reihenfolge der Komponenten geachtet werden. Sind x, y zwei verschiedene Elemente von A , so ist zwar $\{x, y\} = \{y, x\}$, aber $(x, y) \neq (y, x)$! Man spricht deshalb manchmal auch ausdrücklich von einem *geordneten Paar*.

Sind drei Mengen A, B und C gegeben, so kann man Elemente $x \in A, y \in B$ und $z \in C$ zu (geordneten) *Tripeln* (x, y, z) zusammenfassen. Die Menge aller solcher Tripel wird mit $A \times B \times C$ bezeichnet.

Sind schließlich n Mengen A_1, \dots, A_n und Elemente $x_i \in A_i$ gegeben, so kann man diese zu sogenannten *n -Tupeln* (x_1, x_2, \dots, x_n) zusammenfassen. Die Menge aller dieser n -Tupel wird mit $A_1 \times \dots \times A_n$ bezeichnet.

Die Menge $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ nennt man auch die *Euklidische Ebene*, und $\mathbb{R}^3 = \mathbb{R} \times \mathbb{R} \times \mathbb{R}$ den *Euklidischen Raum*.

Ist $P_0 = (x_0, y_0)$ ein Punkt im \mathbb{R}^2 , so nennt man x_0 die *x -Koordinate* oder *Abszisse* und y_0 die *y -Koordinate* oder *Ordinate* von P_0 . Der Punkt $O := (0, 0)$ heißt der *Nullpunkt* oder *Koordinatenursprung*.

Sind $P_1 := (x_1, y_1)$ und $P_2 := (x_2, y_2)$ zwei Punkte in der Ebene, so ist die Verbindungsstrecke von P_1 und P_2 die Hypotenuse eines rechtwinkligen Dreiecks mit den Katheten $|y_2 - y_1|$ und $|x_2 - x_1|$. Ihre Länge

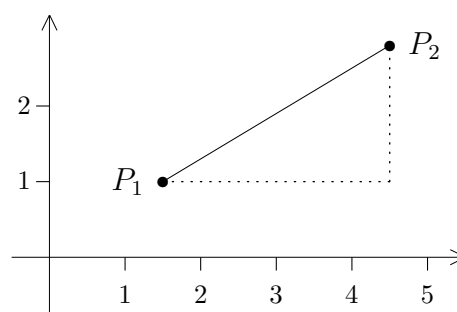
$$d(P_1, P_2) := \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}.$$

nennt man den *Abstand* oder die *Distanz* von P_1 und P_2 .

Wir wollen uns einige geometrische Figuren ansehen:

1. Geraden:

Jede Menge der Gestalt $L = \{(x, y) \in \mathbb{R}^2 \mid ax + by = s\}$ mit reellen Zahlen a, b, s und $(a, b) \neq (0, 0)$ nennt man eine *Gerade* (in der Ebene). Ist $s = 0$, so geht die



Gerade durch den Ursprung. Ist $a = 0$, so verläuft sie „horizontal“, im Falle $b = 0$ „vertikal“.

2. Kreise:

Sei $P_0 = (x_0, y_0)$ ein fester Punkt und $r > 0$ eine reelle Zahl. Die Menge $K_r(P_0)$ aller Punkte $P = (x, y)$, die von P_0 den festen Abstand r haben, bezeichnet man als den *Kreis um P_0 mit Radius r* :

$$K_r(P_0) := \{P \in \mathbb{R}^2 \mid d(P, P_0) = r\} = \{(x, y) \in \mathbb{R}^2 \mid (x - x_0)^2 + (y - y_0)^2 = r^2\}.$$

Speziell nennt man $S^1 := K_1(O)$ den *Einheitskreis*.

3. Kreisscheiben:

Ist $P_0 = (x_0, y_0) \in \mathbb{R}^2$ und $r > 0$, so nennt man die Menge

$$\begin{aligned} D_r(P_0) &:= \{P \in \mathbb{R}^2 \mid d(P, P_0) < r\} \\ &= \{(x, y) \in \mathbb{R}^2 \mid (x - x_0)^2 + (y - y_0)^2 < r^2\} \end{aligned}$$

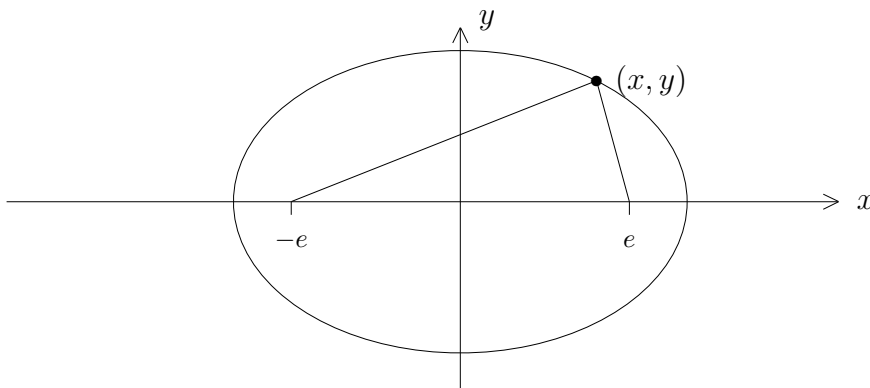
die (*offene*) *Kreisscheibe um P_0 mit Radius r* . Ersetzt man „ $<$ “ durch „ \leq “, so spricht man von einer *abgeschlossenen Kreisscheibe*. Sie wird mit $\overline{D_r(P_0)}$ bezeichnet. Es gilt:

$$\overline{D_r(P_0)} = D_r(P_0) \cup K_r(P_0).$$

4. Ellipsen:

Es seien P_1, P_2 zwei feste Punkte der Ebene und $a > e := \frac{1}{2}d(P_1, P_2)$. Die Menge aller Punkte P mit $d(P, P_1) + d(P, P_2) = 2a$ nennt man eine *Ellipse* mit den *Brennpunkten* P_1 und P_2 . Die Zahl e heißt die *lineare Exzentrizität* der Ellipse.

Wir leiten eine Gleichung für die Punkte der Ellipse her und setzen dabei voraus, daß $P_1 = (-e, 0)$ und $P_2 = (e, 0)$ ist. Durch eine Verschiebung und eine Drehung um den Nullpunkt (also eine „euklidische Bewegung“ oder Kongruenzabbildung) kann man das erreichen.



Für einen Punkt (x, y) auf der Ellipse gilt dann:

$$\sqrt{(e+x)^2 + y^2} + \sqrt{(e-x)^2 + y^2} = 2a,$$

also

$$e^2 + 2ex + x^2 + y^2 = 4a^2 - 4a\sqrt{(e-x)^2 + y^2} + e^2 - 2ex + x^2 + y^2.$$

Zusammengefaßt ergibt das:

$$ex - a^2 = -a\sqrt{(e-x)^2 + y^2},$$

also

$$(ex)^2 - 2ea^2x + a^4 = a^2(e^2 - 2ex + x^2 + y^2).$$

Vereinfacht man noch einmal, so erhält man

$$a^2y^2 + (a^2 - e^2)x^2 = a^2(a^2 - e^2).$$

Setzt man $b^2 := a^2 - e^2$, so wird daraus die Gleichung $a^2y^2 + b^2x^2 = a^2b^2$, also

$$\boxed{\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1.}$$

Setzt man $y = 0$ ein, so wird $x = \pm a$, und im Falle $x = 0$ wird $y = \pm b$. Man nennt a und b die beiden *Halbachsen* der Ellipse.

5. Allgemeine Kurven:

Ist $F(x, y)$ ein algebraischer Term, der x und y als Variable enthält, so nennt man die Menge $\{(x, y) \in \mathbb{R}^2 \mid F(x, y) = 0\}$ i.a. eine *ebene Kurve*. Oben haben wir verschiedene Beispiele gesehen:

$$\begin{aligned} F(x, y) = ax + by - s & : \text{ Gerade,} \\ F(x, y) = (x - x_0)^2 + (y - y_0)^2 - r^2 & : \text{ Kreis,} \\ F(x, y) = a^2y^2 + b^2x^2 - a^2b^2 & : \text{ Ellipse.} \end{aligned}$$

Manchmal ist der Begriff „Kurve“ allerdings auch verfehlt, wie etwa

$$\{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 0\} = \{(0, 0)\}$$

zeigt.

Wir kommen nun zu einem der wichtigsten Begriffe der Mathematik:

Definition.

A und B seien zwei beliebige Mengen. Unter einer *Abbildung von A nach B* versteht man eine Vorschrift, durch die **jedem Element $x \in A$ genau ein Element $y \in B$** zugeordnet wird.

Die Zuordnungsvorschrift sei mit dem Buchstaben f bezeichnet.

Dann schreibt man:

$$\boxed{f : A \rightarrow B}$$

Wird dem Element $x \in A$ das Element $x \in B$ zugeordnet, so drückt man das durch $f(x) = y$ oder $f : x \mapsto y$ aus.

Die Menge A nennt man den *Definitionsbereich* von f . Sie ist wesentlicher Bestandteil der Abbildung f und wird daher auch gerne mit D_f bezeichnet. Die Menge B nennt man *Wertebereich*, *Wertevorrat* oder *Zielmenge*.

Beispiel :

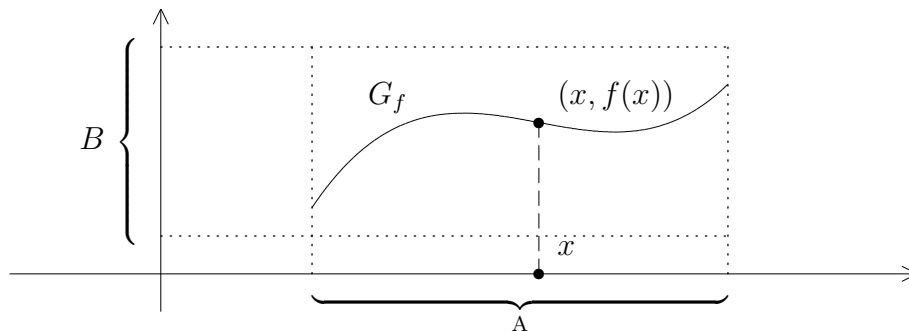
Sei A die Menge der Hörer der Vorlesung und B die Menge der Plätze im Hörsaal. Wenn sich alle Hörer hingesetzt haben, ist eine Zuordnung von A nach B hergestellt. In der nächsten Woche wird die Zielmenge voraussichtlich gleich geblieben sein, aber der Definitionsbereich und die Zuordnungsvorschrift können sich ändern. Also ergibt sich auch eine andere Abbildung.

Definition.

Ist $f : A \rightarrow B$ eine Abbildung, so versteht man unter dem *Graphen* von f die Menge

$$G_f := \{(x, y) \in A \times B \mid y = f(x)\} = \{(x, f(x)) \mid x \in A\}.$$

Ist etwa $A \subset \mathbb{R}$ und $B \subset \mathbb{R}$, so kann man den Graphen sehr einfach aufzeichnen:



Die typischen Eigenschaften einer Abbildung sind leicht zu erkennen:

1. Da jedem $x \in A$ etwas zugeordnet werden soll, muß jede vertikale Gerade, die A trifft, auch den Graphen treffen.
2. Da jedem x nur ein y zugeordnet werden kann, darf eine vertikale Gerade den Graphen auch stets nur einmal treffen.

Ist der Wertebereich einer Abbildung eine Menge von **Zahlen**, so sagt man an Stelle von „Abbildung“ meistens „Funktion“. Das ist allerdings nur eine Tradition, keine feste Vorschrift. Und der Begriff „Zahl“ kann dabei recht weit ausgelegt werden.

Der Graph einer reellwertigen Funktion f mit $D_f \subset \mathbb{R}$ ist eine Menge der Gestalt

$$\{(x, y) \in \mathbb{R}^2 \mid y - f(x) = 0\},$$

also eine Kurve. Umgekehrt ist jedoch noch lange nicht jede Kurve im \mathbb{R}^2 der Graph einer Funktion, wie etwa das Beispiel eines Kreises zeigt.⁵

⁵Es gibt vertikale Geraden, die $2 \times$ treffen.

Definition.

Sei $f : A \rightarrow B$ eine Abbildung. Ist $M \subset A$ eine Teilmenge, so nennt man die Menge

$$f(M) := \{f(x) \mid x \in M\} \subset B$$

das *Bild* (oder die *Bildmenge*) von M unter f .

Man darf die Bildmenge nicht mit dem Wertebereich verwechseln. Im Beispiel mit den Hörern der Vorlesung ist die Bildmenge die Menge der besetzten Plätze.

Beispiele :

1. Entscheidender Bestandteil einer Abbildung ist die Zuordnungsvorschrift. Sie kann als Funktionsterm, in Form einer eindeutig lösbaren Gleichung oder auch durch einen Algorithmus gegeben werden.

Sei etwa $A := \mathbb{N} \times \mathbb{N}$ und $B := \mathbb{N}$. Jedem Element (n, m) des Definitionsbereichs soll als Wert der größte gemeinsame Teiler $\text{ggT}(n, m)$ zugeordnet werden. Wie kann man diese Zuordnung angeben? Man braucht eine Vorschrift zur eindeutigen Berechnung des ggT . Eine Möglichkeit ist die Zerlegung der Zahlen n und m in Primfaktoren. Anschließend kann $\text{ggT}(n, m)$ mit Hilfe einer Formel ermittelt werden. Leichter durchführbar ist der „Euklidische Algorithmus“:

Sei etwa $n > m$. Dann kann man fortgesetzt ganzzahlig mit Rest dividieren:

$$\begin{aligned} n &= q_0 \cdot m + r_1, & \text{mit } 0 \leq r_1 < m, \\ m &= q_1 \cdot r_1 + r_2, & \text{mit } 0 \leq r_2 < r_1, \\ r_1 &= q_2 \cdot r_2 + r_3, & \text{mit } 0 \leq r_3 < r_2, \\ &\vdots \\ r_{N-2} &= q_{N-1} \cdot r_{N-1} + r_N, & \text{mit } 0 \leq r_N < r_{N-1}, \\ r_{N-1} &= q_N \cdot r_N. \end{aligned}$$

Da $n > m > r_1 > r_2 > \dots \geq 0$ ist, muß die Division irgendwann aufgehen, der Prozeß also abbrechen. Und offensichtlich gilt:

$$r_N = \text{ggT}(r_{N-1}, r_N) = \text{ggT}(r_{N-2}, r_{N-1}) = \dots = \text{ggT}(n, m).$$

Da jeder Schritt eindeutig ist, liefert der Algorithmus eine Abbildung.

2. Sei $A = B = \mathbb{R}^2$, $(a, b) \in \mathbb{R}^2$ fest gewählt. Durch

$$T_{(a,b)}(x, y) := (x + a, y + b)$$

wird eine Abbildung $T_{(a,b)} : A \rightarrow A$ definiert, eine sogenannte *Translation* oder *Verschiebung*. Einen Graphen kann man hier nicht gut zeichnen. Eine anschauliche Vorstellung kann man trotzdem gewinnen, indem man in der Ebene eine Reihe von Punkten jeweils durch einen Pfeil mit ihrem Bildpunkt verbindet. Man sieht dann, daß durch $T_{(a,b)}$ die gesamte Ebene um einen bestimmten Betrag in einer bestimmten Richtung parallel verschoben wird.

Von ähnlicher Art sind auch die folgenden Abbildungen:

Ist λ eine positive reelle Zahl, so nennt man $H_\lambda : A \rightarrow A$ mit

$$H_\lambda(x, y) := (\lambda x, \lambda y)$$

eine *Streckung*, *Homothetie* oder *Skalierung*.

Die Abbildung $S : A \rightarrow A$ mit $S(x, y) := (x, -y)$ nennt man die *Spiegelung an der x-Achse*.

3. Sei M eine beliebige Menge. Die *identische Abbildung* auf M wird durch $\text{id}_M(x) := x$ definiert. Sie bewirkt überhaupt nichts! Trotzdem werden wir sie später brauchen, so wie wir ja auch die leere Menge oder die Zahl Null gebraucht haben.

Definition.

Es sei $f : A \rightarrow B$ eine beliebige Abbildung.

1. f heißt *injektiv* (oder *eineindeutig*), falls gilt:

$$x_1 \neq x_2 \implies f(x_1) \neq f(x_2).$$

2. f heißt *surjektiv* (oder eine *Abbildung auf B*), falls gilt:

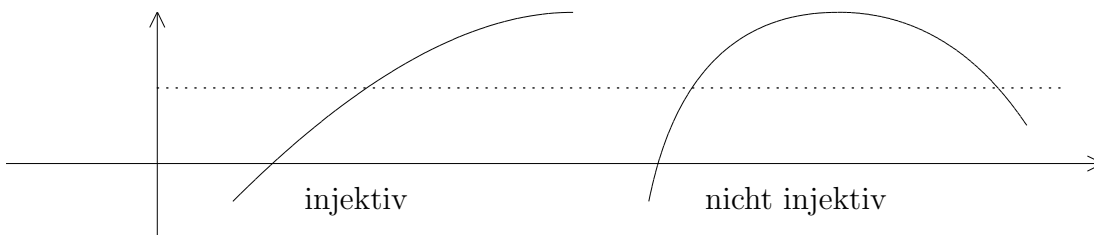
$$\forall y \in B \exists x \in A \text{ mit } f(x) = y.$$

3. f heißt *bijektiv*, falls f injektiv und surjektiv ist.

f ist also genau dann injektiv, wenn die Gleichung $f(x) = y$ bei gegebenem y – wenn überhaupt – eindeutig lösbar ist. Und f ist genau dann surjektiv, wenn die Gleichung $f(x) = y$ für jedes y aus dem Wertebereich lösbar ist (aber nicht unbedingt eindeutig).

Im Falle einer reellen Funktion kann man sich diese Eigenschaften an Hand des Graphen G_f veranschaulichen:

f ist genau dann injektiv, wenn der Graph von jeder horizontalen Geraden höchstens einmal getroffen wird. Und f ist genau dann surjektiv, wenn jede horizontale Gerade, die B trifft, auch den Graphen G_f trifft.



Statt eine Aussage der Gestalt $(E \implies F)$ zu zeigen, kann man auch die dazu äquivalente Aussage $(\neg F \implies \neg E)$ beweisen. Das nennt man „Beweis durch Kontraposition“. Das Verfahren ist dem Widerspruchsbeweis sehr ähnlich.

Man weist Injektivität deshalb meist nach folgendem Schema nach: $f(x_1) = f(x_2) \implies x_1 = x_2$.

Die Surjektivität nachzuweisen bedeutet, den Zuordnungsprozeß rückgängig zu machen. In der Praxis läuft das oft auf das Lösen von Gleichungen hinaus.

Beispiele:

1. $f: \mathbb{R} \rightarrow \mathbb{R}$ mit $f(x) := mx + t$ und $m \neq 0$ ist injektiv und surjektiv, also bijektiv.

Wir können das Beweisschema an diesem Beispiel besonders gut zeigen:

Injektivität: Sei $f(x_1) = f(x_2)$. Dann ist $mx_1 + t = mx_2 + t$, also $m(x_1 - x_2) = 0$. Da ein Produkt nur dann verschwindet, wenn wenigstens einer der beiden Faktoren verschwindet, muß $x_1 - x_2 = 0$ sein, also $x_1 = x_2$.

Surjektivität: Sei $y \in \mathbb{R}$ vorgegeben. Wir suchen ein $x \in \mathbb{R}$ mit $f(x) = y$, müssen also die Gleichung $mx + t = y$ nach x auflösen. Das ist leicht getan: $x = \frac{1}{m}(y - t)$.

2. $f: \mathbb{R} \rightarrow \mathbb{R}$ mit $f(x) := x^2$ ist weder injektiv noch surjektiv.

Wie führt man den Beweis solcher negativer Aussagen?

Injektivität: Es ist $-1 \neq 1$, aber $f(-1) = 1 = f(1)$. Also ist f nicht injektiv.

Surjektivität: Ist $x \in \mathbb{R}$, so ist $x^2 > 0$. Also kann z.B. $y = -1$ nicht als Wert vorkommen. f ist nicht surjektiv.

3. Surjektivität kann man immer durch Verkleinern der Zielmenge erreichen. So ist z.B. $f: \mathbb{R} \rightarrow \mathbb{R}_+ \cup \{0\}$ mit $f(x) := x^2$ surjektiv.

Injektivität kann man manchmal durch Verkleinern des Definitionsbereichs erreichen.

Ist $f: A \rightarrow B$ eine Abbildung und $T \subset A$, so definiert man die *Einschränkung* von f auf T durch $(f|_T)(x) := x$.

Ist $f: \mathbb{R} \rightarrow \mathbb{R}$ definiert durch $f(x) := x^2$, so ist $f|_{\mathbb{R}_+}: \mathbb{R}_+ \rightarrow \mathbb{R}$ injektiv und $f|_{\mathbb{R}_+}: \mathbb{R}_+ \rightarrow \mathbb{R}_+$ sogar bijektiv.

4. Die Abbildung $\text{ggT}: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ ist surjektiv (denn es ist ja z.B. $\text{ggT}(a, a) = a$), aber nicht injektiv, denn es ist z.B. $\text{ggT}(15, 9) = 3 = \text{ggT}(33, 12)$.
5. Seien A, B zwei **endliche** Mengen mit $\#(A) = n$ und $\#(B) = m$. Ist $f: A \rightarrow B$ injektiv, so ist auch $\#(f(A)) = n$, also $n \leq m$. Ist $f: A \rightarrow B$ surjektiv, so muß $m \leq n$ sein. Eine bijektive Abbildung zwischen A und B kann es also nur dann geben, wenn $n = m$ ist. Ist das aber der Fall, so ist eine Abbildung $f: A \rightarrow B$ schon dann bijektiv, wenn f injektiv oder surjektiv ist.

Wir betrachten nun **bijektive** Abbildungen von $\{1, \dots, n\}$ auf sich. Solche Abbildungen nennt man auch *Permutationen*. Man schreibt eine Permutation f üblicherweise in der Form

$$f = \begin{pmatrix} 1 & 2 & \dots & n \\ f(1) & f(2) & \dots & f(n) \end{pmatrix}.$$

Die Werte $f(1), \dots, f(n)$ bestimmen – in dieser Anordnung – die Abbildung f . Dabei stellen sie nichts anderes als eine mögliche Anordnung der Zahlen $1, \dots, n$ dar. Also gibt es genau $n!$ Permutationen der Zahlen $1, \dots, n$. Wir bezeichnen die Menge aller dieser Permutationen mit S_n . So ist z.B.

$$S_3 = \left\{ \begin{pmatrix} 123 \\ 123 \end{pmatrix}, \begin{pmatrix} 123 \\ 132 \end{pmatrix}, \begin{pmatrix} 123 \\ 213 \end{pmatrix}, \begin{pmatrix} 123 \\ 231 \end{pmatrix}, \begin{pmatrix} 123 \\ 312 \end{pmatrix}, \begin{pmatrix} 123 \\ 321 \end{pmatrix} \right\}.$$

Wird n größer, so wird auch der Umgang mit den Permutationen aus S_n komplizierter. Eine gewisse Hilfe ist dann die „Zykel-Schreibweise“. Wir demonstrieren das an einem Beispiel:

$$\text{Sei } f := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 7 & 4 & 5 & 1 & 2 & 6 \end{pmatrix} \in S_7.$$

Beginnen wir mit der 1. Die 1 wird auf 3 abgebildet, die 3 auf die 4, die 4 auf die 5 und die 5 wieder auf die 1. Das ergibt einen abgeschlossenen *Zykel*, den man mit $(1, 3, 4, 5)$ bezeichnet. Damit ist aber noch nicht alles abgehandelt, was die Abbildung f tut. Die nächstgrößere Zahl nach der 1, die noch nicht vorkam, ist die 2. Mit ihr beginnen wir das Spiel erneut: Die 2 wird auf die 7 abgebildet, die 7 auf die 6 und die 6 wieder auf die 2. Das ergibt den Zykel $(2, 7, 6)$. Da nun alle Zuordnungen von f berücksichtigt wurden, schreiben wir:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 7 & 4 & 5 & 1 & 2 & 6 \end{pmatrix} = (1, 3, 4, 5)(2, 7, 6).$$

Wird eine Zahl i auf sich abgebildet, so führt das auf einen „Einer-Zykel“ (i). Solche Zykel schreibt man normalerweise nicht hin. Wenn allerdings f die Identität ist, also jedes Element auf sich abgebildet wird, so besteht f nur aus Einer-Zykeln, und man muß wenigstens einen davon hinschreiben:

$$\text{id}_{\{1, \dots, n\}} = (1).$$

Bei reellwertigen Funktionen besitzen wir ein etwas handlicheres Kriterium für die Injektivität. Wir betrachten eine Funktion, deren Definitionsbereich ein Intervall ist. Dabei fassen wir den Intervall-Begriff recht allgemein:

$[a, b]$, $[a, b)$, $(a, b]$, (a, b) , $(-\infty, b)$, $(-\infty, b]$, (a, ∞) , $[a, \infty)$ und $\mathbb{R} = (-\infty, \infty)$ sind allesamt Intervalle.

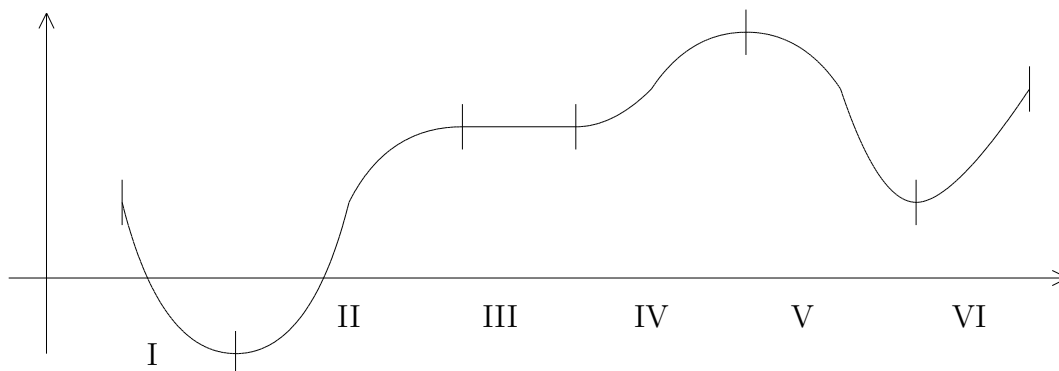
Definition.

Sei $I \subset \mathbb{R}$ ein Intervall. Eine Funktion $f : I \rightarrow \mathbb{R}$ heißt *monoton wachsend* (bzw. *streng monoton wachsend*), falls für $x_1, x_2 \in I$ mit $x_1 < x_2$ gilt:

$$f(x_1) \leq f(x_2) \quad (\text{bzw. } f(x_1) < f(x_2)).$$

Analog definiert man „(streng) monoton fallend“.

Normalerweise zeigt eine Funktion auf verschiedenen Abschnitten unterschiedliches Monotonieverhalten:



In den Bereichen (I) und (V) fällt f streng monoton, in den Bereichen (II), (IV) und (VI) wächst f streng monoton, und in (III) ist f konstant, also zugleich monoton wachsend und fallend, aber nicht streng monoton.

Offensichtlich gilt: Ist f auf D_f streng monoton (wachsend oder fallend), so ist f dort injektiv.

Betrachten wir z.B. $f(x) := x^3$ und $x_1 < x_2$. Dann ist

$$f(x_2) - f(x_1) = (x_2)^3 - (x_1)^3 = (x_2 - x_1) \cdot (x_1^2 + x_1x_2 + x_2^2).$$

Haben x_1, x_2 das gleiche Vorzeichen, so ist der Ausdruck in der rechten Klammer > 0 , und da auch $x_2 - x_1 > 0$ ist, muß $f(x_1) < f(x_2)$ sein. Ist jedoch $x_1 < 0 < x_2$, so ist auch $f(x_1) < 0 < f(x_2)$. Also ist $x \mapsto x^3$ streng monoton wachsend und damit erst recht injektiv.

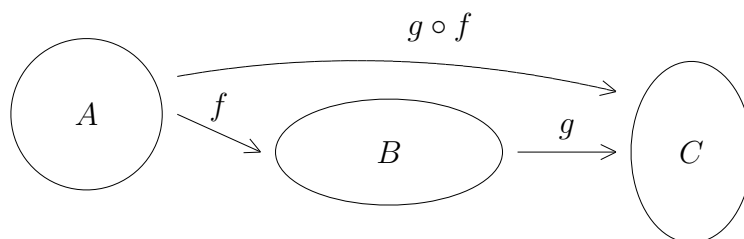
Im übrigen ist $x \mapsto x^3$ auch surjektiv. Zu jeder positiven reellen Zahl a gibt es eine positive Zahl x mit $x^3 = a$. Aber dann ist auch $-a = (-x)^3$.

Bemerkung: Eine streng monotone Funktion ist injektiv. Umgekehrt braucht eine injektive Funktion aber nicht streng monoton zu sein. Man sagt dann, die strenge Monotonie ist ein *hinreichendes Kriterium* für die Injektivität, aber kein *notwendiges Kriterium*.

Definition.

A, B und C seien irgendwelche Mengen. Sind Abbildungen $f : A \rightarrow B$ und $g : B \rightarrow C$ gegeben, so kann man diese Zuordnungen hintereinander ausführen und so zu einer neuen Abbildung $g \circ f : A \rightarrow C$ verknüpfen, mit

$$g \circ f(x) := g(f(x)).$$



Beispiele :

1. Die Funktionen $f, g : \mathbb{R} \rightarrow \mathbb{R}$ seien definiert durch $f(x) := x^2 + 2x$ und $g(y) := y + 1$.
Dann gilt:

$$\begin{aligned} g \circ f(x) &= f(x) + 1 = x^2 + 2x + 1, \\ f \circ g(y) &= g(y)^2 + 2g(y) = (y + 1)^2 + 2(y + 1) = y^2 + 4y + 3. \end{aligned}$$

Im allgemeinen ist also $f \circ g \neq g \circ f$. Bei beliebigen Abbildungen sind darüber hinaus die beiden Verknüpfungen $f \circ g$ und $g \circ f$ nicht unbedingt gleichzeitig definiert.

2. Sind $T_{(a,b)} : (x, y) \mapsto (x+a, y+b)$ und $T_{(c,d)} : (x, y) \mapsto (x+c, y+d)$ zwei Translationen der Ebene, so ist $T_{(c,d)} \circ T_{(a,b)} = T_{(a+c, b+d)} : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ wieder eine Translation.

Weil die Addition in \mathbb{R} kommutativ ist, gilt:

$$T_{(c,d)} \circ T_{(a,b)} = T_{(a,b)} \circ T_{(c,d)}.$$

3. Ist $S : (x, y) \mapsto (x, -y)$ die Spiegelung an der x-Achse, so ist $S \circ S(x, y) = (x, y)$, also $S \circ S = \text{id}_{\mathbb{R}^2}$.

Sind $\sigma := \begin{pmatrix} 1 & \cdots & n \\ \sigma(1) & \cdots & \sigma(n) \end{pmatrix}$ und $\tau := \begin{pmatrix} 1 & \cdots & n \\ \tau(1) & \cdots & \tau(n) \end{pmatrix}$ zwei Permutationen, so kann man sie zu einer neuen Permutation $\sigma \circ \tau$ miteinander verknüpfen, mit

$$\sigma \circ \tau = \begin{pmatrix} 1 & \cdots & n \\ \sigma(\tau(1)) & \cdots & \sigma(\tau(n)) \end{pmatrix}.$$

So ist z.B.

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Man beachte, daß die Permutationen von rechts nach links abzuarbeiten sind! Die rechte (innere) Permutation bildet z.B. die 1 auf die 3 ab, und die linke (äußere) Permutation bildet dann die 3 auf die 2 ab. Im Ergebnis auf der anderen Seite der Gleichung muß deshalb unter der 1 die 2 stehen.

Normalerweise ist die Verknüpfung von Permutationen nicht kommutativ. Wenn wir allerdings die Menge $\{1, \dots, n\}$ in zwei disjunkte Teilmengen M und N aufteilen können, so daß die Permutation σ nur die Zahlen aus M verändert und τ nur die Zahlen aus N , dann spielt die Reihenfolge keine Rolle, es ist $\sigma \circ \tau = \tau \circ \sigma$. Das hat Konsequenzen für die Zykel-Schreibweise. Die Aufteilung einer Permutation in mehrere Zyklen bedeutet, daß sich die gegebene Permutation aus mehreren einfacheren Permutationen verknüpfen läßt, und die Reihenfolge spielt dabei keine Rolle. Es ist also z.B.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 7 & 4 & 5 & 1 & 2 & 6 \end{pmatrix} = (1, 3, 4, 5) \circ (2, 7, 6) = (2, 7, 6) \circ (1, 3, 4, 5).$$

Eine Permutation heißt *Transposition* oder *Vertauschung*, wenn nur zwei Zahlen miteinander vertauscht werden und alle anderen fest bleiben, wenn sie also nur aus einem „Zweier-Zykel“ besteht, z.B.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 3 & 1 & 5 \end{pmatrix} = (1, 4)$$

I.4.1 Satz. *Jede Permutation läßt sich als endliche Verknüpfung von Transpositionen schreiben.*

BEWEIS: Da wir jede Permutation als Folge von Zyklen schreiben können, reicht es zu zeigen, daß sich jeder beliebige Zykel aus endlich vielen Zweier-Zykeln zusammensetzen läßt.

Betrachten wir also einen beliebigen Zykel (i_1, i_2, \dots, i_k) in einer Permutation f . Dann ist

$$f(i_\nu) = i_{\nu+1} \text{ für } \nu = 1, 2, \dots, k-1, \text{ und } f(i_k) = i_1.$$

Der Zweier-Zykel (i_1, i_2) vertauscht nur i_1 mit i_2 und läßt alles andere fest. Führt man anschließend den Zweier-Zykel (i_1, i_3) aus, so wird insgesamt i_1 auf i_2 , i_2 auf i_3 und i_3 auf i_1 abgebildet. So kann man fortfahren bis zu der Kombination

$$(i_1, i_k) \circ \dots \circ (i_1, i_3) \circ (i_1, i_2),$$

die i_1 auf i_2 , i_2 auf i_3 usw. und schließlich i_{k-1} auf i_k und i_k auf i_1 abbildet. Also ist

$$(i_1, i_2, \dots, i_k) = (i_1, i_k) \circ \dots \circ (i_1, i_3) \circ (i_1, i_2).$$

Man beachte aber, daß es hier auf die Reihenfolge ankommt, weil die einzelnen Zweier-Zykel nicht paarweise disjunkt sind. \square

Das oben versteckte Verfahren zur Auflösung einer Permutation in Transpositionen liefert ein eindeutiges Ergebnis. Leider sind auch andere Verfahren denkbar, und die Zerlegung einer Permutation in Transpositionen ist nicht eindeutig bestimmt. So ist z.B.

$$\begin{aligned} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} &= (1, 2) \circ (1, 4) \circ (1, 3) \\ &= (2, 4) \circ (1, 3) \circ (2, 3) \\ &= (2, 4) \circ (1, 2) \circ (2, 3) \circ (1, 3) \circ (1, 2). \end{aligned}$$

Allerdings gilt:

I.4.2 Satz. *Wird eine Permutation auf zweierlei Weisen durch eine Folge von Transpositionen erzeugt, so ist die Anzahl der benötigten Vertauschungen entweder in beiden Fällen gerade oder in beiden Fällen ungerade.*

Der Beweis ist nicht ganz einfach und wird deshalb weggelassen.

Definition.

Eine Permutation $\sigma \in \mathcal{S}_n$ heißt *gerade*, wenn sie sich aus einer geraden Anzahl von Vertauschungen zusammensetzt. Andernfalls heißt sie *ungerade*. Wir setzen

$$\text{sgn}(\sigma) := \begin{cases} +1 & \text{falls } \sigma \text{ gerade ist,} \\ -1 & \text{falls } \sigma \text{ ungerade ist,} \end{cases}$$

und nennen diese Zahl das *Signum* der Permutation.

Dann ist etwa

$$\begin{aligned} \operatorname{sgn} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 4 & 3 & 5 \end{pmatrix} &= \operatorname{sgn}[(3, 4)] = -1, \\ \operatorname{sgn} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 2 & 5 \end{pmatrix} &= \operatorname{sgn}[(1, 3) \circ (2, 4)] = +1 \\ \text{und } \operatorname{sgn} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix} &= \operatorname{sgn}[(1, 3, 4) \circ (2, 5)] \\ &= \operatorname{sgn}[(1, 4) \circ (1, 3) \circ (2, 5)] = -1. \end{aligned}$$

Das Signum einer Permutation wird uns später bei den Determinanten wieder begegnen.

I.4.3 Satz. *Eine Abbildung $f : A \rightarrow B$ ist genau dann bijektiv, wenn es eine weitere Abbildung $g : B \rightarrow A$ gibt, so daß $g \circ f = \operatorname{id}_A$ und $f \circ g = \operatorname{id}_B$ ist.*

BEWEIS: Ist f bijektiv, so gibt es wegen der Surjektivität zu jedem $y \in B$ ein $x \in A$ mit $f(x) = y$, und wegen der Injektivität ist dieses x eindeutig bestimmt. Also gibt es eine eindeutige Zuordnung $y = f(x) \mapsto x$. Diese Zuordnung ist eine Abbildung g von B nach A . Offensichtlich ist $g(f(x)) = x$ und $f(g(y)) = f(g(f(x))) = f(x) = y$, also $g \circ f = \operatorname{id}_A$ und $f \circ g = \operatorname{id}_B$.

Man nennt g auch die *Umkehrabbildung* zu f und bezeichnet sie mit f^{-1} . Es gilt also:

$$\begin{aligned} f^{-1} \circ f &= \operatorname{id}_A \\ \text{und } f \circ f^{-1} &= \operatorname{id}_B. \end{aligned}$$

Sei nun umgekehrt ein $g : B \rightarrow A$ mit den angegebenen Eigenschaften vorhanden. Wir müssen zeigen, daß f bijektiv ist.

- 1) Ist $y \in B$, so ist $f(g(y)) = y$, also f surjektiv.
- 2) Ist $f(x_1) = f(x_2)$, so ist $x_1 = g(f(x_1)) = g(f(x_2)) = x_2$, also f injektiv. □

Dieses Kriterium ist sehr nützlich. Z.B. ist die Translation $T = T_{(a,b)} : (x, y) \mapsto (x+a, y+b)$ bijektiv, weil man sofort eine Umkehrabbildung angeben kann:

$$T^{-1} : (x, y) \mapsto (x - a, y - b).$$

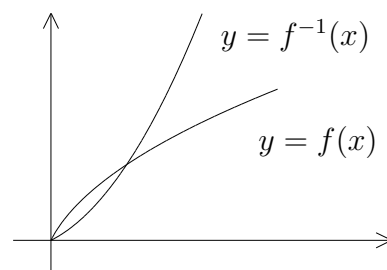
Beispiele :

1. Sei $f : \mathbb{R} \rightarrow \mathbb{R}$ definiert durch $f(x) := mx + t$, mit $m \neq 0$. Dann ist

$$f^{-1}(y) = \frac{1}{m}(y - t).$$

2. Sei $f : \mathbb{R}_+ \rightarrow \mathbb{R}_+$ definiert durch $f(x) := x^2$. Dann ist $f^{-1}(y) = \sqrt{y}$.

Den Graphen der Umkehrfunktion f^{-1} zu einer reellwertigen Funktion f erhält man übrigens, indem man den Graphen von f an der Winkelhalbierenden spiegelt.



I.4.4 Satz. Sei M eine beliebige Menge. Dann bilden die bijektiven Abbildungen von M auf sich eine Gruppe.

BEWEIS: Sei \mathcal{G} die Menge aller bijektiven Abbildungen von M auf sich. Wir müssen zunächst zeigen, daß die Verknüpfung von Abbildungen assoziativ ist. Das ist aber leicht:

Seien $f, g, h \in \mathcal{G}$, $x \in M$ beliebig. Dann ist

$$((f \circ g) \circ h)(x) = (f \circ g)(h(x)) = f(g(h(x))) = f((g \circ h)(x)) = (f \circ (g \circ h))(x).$$

Als neutrales Element können wir die identische Abbildung id_M benutzen. Und da jedes Element $f \in \mathcal{G}$ bijektiv ist, existiert dazu die Umkehrabbildung f^{-1} , die wieder in \mathcal{G} liegt. Offensichtlich ist f^{-1} das Inverse zu f bezüglich der Verknüpfung von Abbildungen. \square

Insbesondere ist also die Menge S_n der Permutationen eine Gruppe, die sogenannte *n-te symmetrische Gruppe*.

Gruppen bijektiver Abbildungen sind i.a. nicht kommutativ. Manchmal können aber Teilmengen solcher Gruppen kommutative „Untergruppen“ bilden, wie etwa die Gruppe der Translationen des \mathbb{R}^2 .

Wir wollen nun kurz untersuchen, wann es zwischen zwei verschiedenen Mengen eine bijektive Abbildung geben kann. Dafür gibt es sogar eine besondere Bezeichnung:

Definition.

Zwei Mengen A und B heißen *gleichmächtig*, wenn es eine bijektive Abbildung $f : A \rightarrow B$ gibt.

Eine Menge ist *endlich*, wenn sie gleichmächtig zu einer Menge der Gestalt $\{1, \dots, n\}$ ist. Zwei endliche Mengen sind genau dann gleichmächtig, wenn sie gleich viel Elemente enthalten.

Die einfachste unendliche Menge, die wir bisher kennen, ist die Menge \mathbb{N} der natürlichen Zahlen. Wir nennen nun eine Menge M *abzählbar*, wenn sie gleichmächtig zu \mathbb{N} ist. Man kann dann M in folgender Form schreiben:

$$M = \{a_1, a_2, a_3, \dots\}.$$

So ist z.B. die Menge \mathbb{Z} der ganzen Zahlen abzählbar:

$$\begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & 6 & \dots \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \dots \\ 0 & 1 & -1 & 2 & -2 & 3 & \dots \end{array}$$

Die bijektive Abbildung $\mathbb{N} \rightarrow \mathbb{Z}$ ist demnach gegeben durch

$$1 \mapsto 0, \quad 2k \mapsto k \text{ und } 2k + 1 \mapsto -k \text{ für } k \geq 1.$$

Problematischer wird es bei der Menge \mathbb{Q} der rationalen Zahlen. Sie liegen „dicht“ in der Menge aller reellen Zahlen, d.h., man kann jede reelle Zahl beliebig genau durch rationale Zahlen approximieren. Trotzdem gelingt es, sie abzuzählen, mit dem sogenannten Cantorschen Diagonalverfahren:

Definition.

Es sei eine Familie $\mathcal{M} = (M_\lambda)_{\lambda \in L}$ gegeben. Dann definiert man:

$$\begin{aligned} \bigcup_{\lambda \in L} M_\lambda &:= \{x \mid \exists \lambda \in L \text{ mit } x \in M_\lambda\}, \\ \bigcap_{\lambda \in L} M_\lambda &:= \{x \mid \forall \lambda \in L \text{ ist } x \in M_\lambda\}. \end{aligned}$$

Die meisten Sätze über endliche Durchschnitte und Vereinigungen lassen sich nun verallgemeinern. Es gilt z.B.:

I.4.5 Satz. Sei $(M_\lambda)_{\lambda \in L}$ eine Familie von Teilmengen einer Menge X . Dann ist

$$\mathfrak{C}_X \left(\bigcup_{\lambda \in L} M_\lambda \right) = \bigcap_{\lambda \in L} \mathfrak{C}_X(M_\lambda).$$

BEWEIS:

$$\begin{aligned} x \in \mathfrak{C}_X \left(\bigcup_{\lambda \in L} M_\lambda \right) &\iff \neg \left(x \in \bigcup_{\lambda \in L} M_\lambda \right) \\ &\iff \neg (\exists \lambda \in L \text{ mit } x \in M_\lambda) \\ &\iff \forall \lambda \in L : x \in \mathfrak{C}_X(M_\lambda) \\ &\iff x \in \bigcap_{\lambda \in L} \mathfrak{C}_X(M_\lambda). \end{aligned}$$

□

§5 Reelle Funktionen

Dieser Abschnitt behandelt zum großen Teil Schulstoff. Er dient der Wiederholung, auf Beweise wird weitgehend verzichtet. In der Vorlesung wurde manches noch knapper behandelt.

1. Affin-lineare Funktionen:

$f : \mathbb{R} \rightarrow \mathbb{R}$ sei definiert durch

$$f(x) := mx + t, \text{ mit } m \neq 0.$$

So etwas nennt man eine *affin-lineare Funktion*, und der Graph ist die Gerade $\{(x, y) \in \mathbb{R}^2 \mid mx - y = -t\}$. Eine vertikale Gerade kann nicht der Graph einer affin-linearen Funktion sein. Warum nicht? ⁶

Der Graph geht genau dann durch den Nullpunkt, wenn $t = 0$ ist. Dann spricht man von einer *linearen Funktion* oder auch von einer *proportionalen Zuordnung* (mit dem *Proportionalitätsfaktor* m).

2. Quadratische Funktionen:

$f : \mathbb{R} \rightarrow \mathbb{R}$ sei definiert durch

$$f(x) := ax^2 + bx + c, \text{ mit } a \neq 0.$$

Das ist eine *quadratische Funktion*, und ihr Graph ist eine sogenannte „Parabel“. Was kann man über die Gestalt dieser Parabel sagen?

1. Die Lösungen der quadratischen Gleichung $f(x) = 0$ sind die „Nullstellen“ von f , also die Schnittpunkte von G_f mit der x-Achse:

$$x_{1,2} = \frac{1}{2a} \cdot (-b \pm \sqrt{b^2 - 4ac}).$$

Die Größe $\Delta := b^2 - 4ac$ nennt man die *Diskriminante*. Ist $\Delta < 0$, so gibt es keine (reelle) Lösung. Ist $\Delta = 0$, so fallen die beiden Lösungen zusammen.

2. Nach dem Prinzip der quadratischen Ergänzung kann man schreiben:

$$f(x) = a \cdot \left[x^2 + 2 \cdot \frac{b}{2a} x + \left(\frac{b}{2a}\right)^2 - \frac{b^2 - 4ac}{4a^2} \right] = a((x - \alpha)^2 - \beta),$$

mit $\alpha := -\frac{b}{2a}$ und $\beta := \frac{\Delta}{4a^2}$. Dann ergibt sich sofort:

$$f(\alpha - x) = f(\alpha + x),$$

d.h., G_f liegt symmetrisch zur vertikalen Geraden $\{(x, y) \mid x = \alpha\}$.

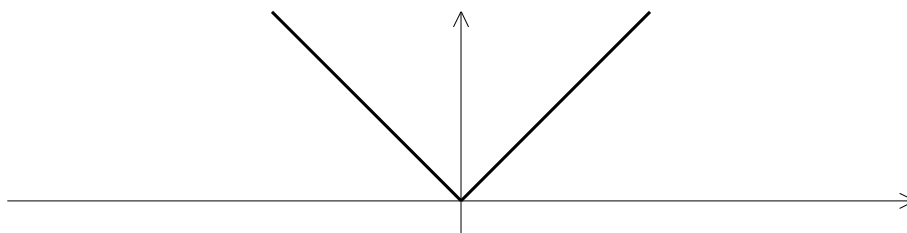
⁶Weil $m \neq 0$ ist!

3. Es ist $f(\alpha) = -a\beta$. Ist $a > 0$, so ist $f(x) \geq -a \cdot \beta = -\frac{\Delta}{4a}$, und die Parabel ist nach oben geöffnet.

Ist $a < 0$, so ist $f(x) \leq -a \cdot \beta$ und G_f nach unten geöffnet.

3. Die Betragsfunktion:

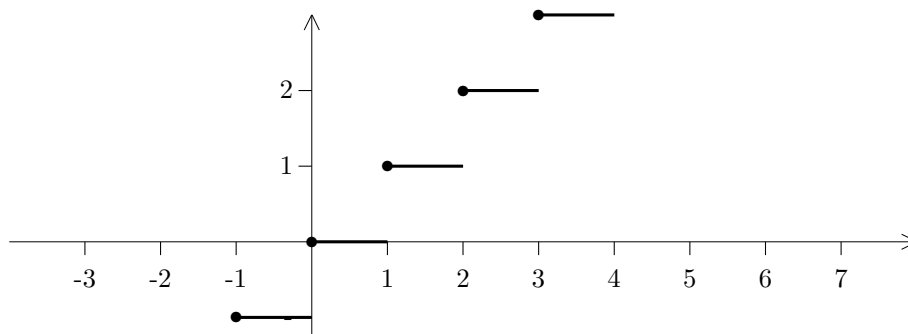
Die Funktion $f(x) := |x|$ hat folgenden Graphen:



4. Die Gauß-Klammer:

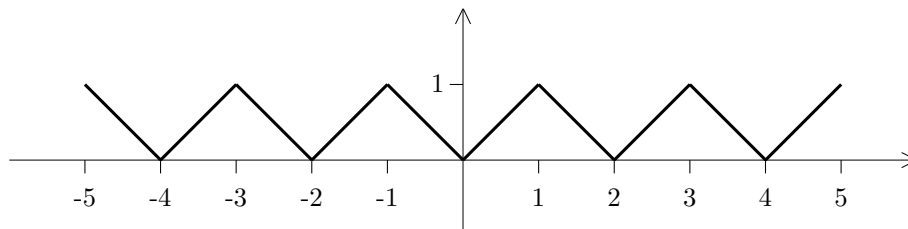
Für eine reelle Zahl x sei $[x]$ die größte ganze Zahl $n \in \mathbb{Z}$ mit $n \leq x$. Man spricht auch von der „Gauß-Klammer“. Z.B. ist $[3.5] = 3$, $[37] = 37$ und $[-\frac{20}{7}] = -3$.

Die Funktion $f(x) := [x]$ hat dann folgende Gestalt:



5. Die Zickzack-Funktion:

Wir wollen die Definition der Funktion finden, deren Graph die folgende Zickzackkurve ist:



Der Graph von f besteht aus Geradenstücken. Ist $2n \leq x < 2n + 1$, so ist $f(x) = x - 2n$. Ist $2n + 1 \leq x < 2n + 2$, so ist $f(x) = -x + (2n + 2)$. Zusammen ergibt das:

$$f(x) = \begin{cases} x - 2n & \text{für } 2n \leq x < 2n + 1 \\ -x + (2n + 2) & \text{für } 2n + 1 \leq x < 2n + 2. \end{cases}$$

6. Polynome:

Eine Funktion der Gestalt

$$p(x) := \sum_{i=0}^n a_i x^i = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0$$

mit Koeffizienten $a_i \in \mathbb{R}$ heißt *reelles Polynom*. Die Nummer n des höchsten nicht verschwindenden Koeffizienten nennt man den *Grad des Polynoms*.

So ist etwa $\text{grad}(x - x^4) = 4$.

Das „Nullpolynom“ $f(x) \equiv 0$ hat eigentlich keinen Grad, wird aber manchmal definitionsgemäß mit dem Grad $-\infty$ versehen..

Eine konstante Funktion $f(x) \equiv c$ mit $c \neq 0$ ist ein Polynom vom Grad 0.

Bemerkung: Durch $f(x) := c$ wird **jedem** Argument x der Wert c zugeordnet. Man schreibt dann auch $f(x) \equiv c$ („ $f(x)$ identisch c “) oder $f = c$.

Ist hingegen f schon auf irgend eine Weise eingeführt worden, so bedeutet die Gleichung $f(x) = c$ (ohne den Doppelpunkt), daß f an der Stelle x den Wert c annimmt, in x also eine c -Stelle besitzt. Besonders interessieren einen die Nullstellen, also die Lösungen der Gleichung $f(x) = 0$, während die Funktion $f(x) \equiv 0$ (das Nullpolynom) höchst langweilig ist.

Polynome können – wie andere reelle Funktionen – addiert und multipliziert werden, das Ergebnis ist jeweils wieder ein Polynom:

$$\text{Sei } f(x) := \sum_{i=0}^n a_i x^i \quad \text{und} \quad g(x) := \sum_{j=0}^m b_j x^j.$$

Ist $n = m$, so definiert man $f + g$ durch

$$(f + g)(x) := f(x) + g(x) = \sum_{i=0}^n (a_i + b_i) x^i.$$

Ist $n \neq m$, etwa $n > m$, so ergänzt man in g noch die Terme $b_{m+1} x^{m+1}, \dots, b_n x^n$, mit $b_{m+1} = \dots = b_n = 0$, und verfährt dann wie oben.

In jedem Fall kann man $f \cdot g$ definieren durch

$$\begin{aligned} (f \cdot g)(x) &:= f(x) \cdot g(x) = \sum_{k=0}^{n+m} \left(\sum_{i+j=k} a_i b_j \right) x^k \\ &= a_0 b_0 + (a_1 b_0 + a_0 b_1) x + (a_2 b_0 + a_1 b_1 + a_0 b_2) x^2 + \cdots + a_n b_m x^{n+m}. \end{aligned}$$

Hieraus ergeben sich die Grad-Formeln:

1. $\text{grad}(f \cdot g) = \text{grad}(f) + \text{grad}(g)$.
2. $\text{grad}(f + g) \leq \max(\text{grad}(f), \text{grad}(g))$.

Eins der wichtigsten Hilfsmittel in der Theorie der Polynome ist die *Division mit Rest*:

I.5.1 Satz (Division mit Rest für Polynome). Es seien f, g Polynome mit $\text{grad}(g) \leq \text{grad}(f)$. Dann gibt es Polynome q und r , so daß gilt:

1. $f = q \cdot g + r$.
2. Entweder ist $r = 0$, oder es ist $0 \leq \text{grad}(r) < \text{grad}(g)$.

Ist $r = 0$, so geht die Rechnung auf, und man sagt, f ist durch g teilbar.

Rechenbeispiel:

$$\begin{array}{r}
 (x^5) : (x^3) = x^2 \\
 \underline{x^5 } \\
 +4x^4 \\
 \underline{-4x^4} \\
 -16x^3 \\
 \underline{16x^3} \\
 +64x^2 \\
 \underline{-61x^2} \\
 -2x \\
 +7
 \end{array}$$

↑ Dies hat einen Grad < 3

Also ist $f(x) = (x^2 - 4x + 16) \cdot g(x) + (-61x^2 - 2x + 7)$.

I.5.2 Satz. Sei $p(x)$ ein Polynom vom Grad n und c eine Nullstelle von p . Dann gibt es ein Polynom $q(x)$ vom Grad $n - 1$, so daß gilt:

$$p(x) = (x - c) \cdot q(x).$$

Man kann also einen „Linearfaktor“ $(x - c)$ abspalten.

BEWEIS: Es ist $p(c) = 0$, also

$$\begin{aligned}
 p(x) &= p(x) - p(c) = (a_n x^n + \cdots + a_0) - (a_n c^n + \cdots + a_0) \\
 &= a_n (x^n - c^n) + a_{n-1} (x^{n-1} - c^{n-1}) + \cdots + a_1 (x - c),
 \end{aligned}$$

und dieses Polynom ist durch $(x - c)$ teilbar, nach der Formel

$$x^k - c^k = (x - c) \cdot \sum_{i=0}^{k-1} x^i c^{k-i-1}.$$

□

Beispiel:

Sei $p(x) := x^5 - 2x^4 - x + 2$. Durch Probieren stellt man schnell fest, daß p bei $x = 1$ eine Nullstelle besitzt. Durch Polynomdivision erhält man, daß

$$p(x) = (x - 1) \cdot (x^4 - x^3 - x^2 - x - 2)$$

ist. Zur Probe kann man ausmultiplizieren.

Definition.

Sei $p(x)$ ein Polynom vom Grad $n \geq 0$. Eine Zahl c heißt k -fache Nullstelle von p , falls es ein Polynom $q(x)$ vom Grad $n - k$ gibt, so daß gilt:

1. $p(x) = (x - c)^k \cdot q(x)$.
2. $q(c) \neq 0$.

Man nennt k dann die *Vielfachheit* der Nullstelle c .

Bemerkung: Da $q(c) \neq 0$ sein soll, kann q nicht das Nullpolynom sein. Also muß gelten: $n - k \geq 0$, d.h. $k \leq n$.

I.5.3 Satz. Sei $p(x)$ ein Polynom vom Grad $n \geq 0$.

1. p besitzt höchstens n Nullstellen (mit Vielfachheit gezählt).
2. Sind c_1, \dots, c_m die verschiedenen Nullstellen von p , $m \leq n$, mit Vielfachheiten k_1, \dots, k_m , so ist

$$p(x) = (x - c_1)^{k_1} \cdot \dots \cdot (x - c_m)^{k_m} \cdot q(x),$$

mit $k_1 + \dots + k_m \leq n$ und einem Polynom q ohne Nullstellen.

Zum BEWEIS dividiert man sukzessive alle Nullstellen heraus, bis nur noch ein Polynom ohne Nullstellen übrigbleibt. Dessen Grad ist $= n - (k_1 + \dots + k_m) \geq 0$.

Beispiel:

Sei $p(x) = x^7 - 2x^6 + 3x^5 - 4x^4 + 2x^3$.

Offensichtlich ist $p(x) = x^3 \cdot q_1(x)$, mit $q_1(x) := x^4 - 2x^3 + 3x^2 - 4x + 2$.

Da $q_1(0) \neq 0$ ist, hat p in $x = 0$ eine Nullstelle der Vielfachheit 3.

Probieren zeigt, daß $q_1(1) = 0$ ist. Polynomdivision ergibt:

$$q_1(x) = (x - 1) \cdot q_2(x), \text{ mit } q_2(x) := x^3 - x^2 + 2x - 2.$$

Da auch $q_2(1) = 0$ ist, kann man noch einmal durch $(x - 1)$ dividieren und erhält:

$$q_1(x) = (x - 1)^2 \cdot q_3(x), \text{ mit } q_3(x) := x^2 + 2.$$

$q_3(x)$ besitzt keine Nullstelle mehr. Also ist

$$p(x) = x^3 \cdot (x - 1)^2 \cdot (x^2 + 2)$$

die bestmögliche Zerlegung von $p(x)$.

7. Rationale Funktionen:

Definition.

Sind p, q zwei Polynome, von denen q nicht das Nullpolynom ist, so nennt man

$$f(x) := \frac{p(x)}{q(x)} \quad \text{eine rationale Funktion.}$$

Der Definitionsbereich D_f einer solchen rationalen Funktion f ist die Menge $D_f := \{x \in \mathbb{R} \mid q(x) \neq 0\}$.

Da das Nennerpolynom q einen Grad ≥ 0 haben soll, besitzt es höchstens endlich viele Nullstellen. Eine rationale Funktion ist also fast überall definiert.

Was passiert in einem Punkt x_0 mit $q(x_0) = 0$?

Wir können den Faktor $(x - x_0)$ in der höchstmöglichen Potenz aus $p(x)$ und $q(x)$ herausziehen: Es gibt Zahlen $k \geq 0$ und $l > 0$, sowie Polynome \tilde{p} und \tilde{q} , so daß gilt:

$$p(x) = (x - x_0)^k \cdot \tilde{p}(x) \quad \text{und} \quad q(x) = (x - x_0)^l \cdot \tilde{q}(x),$$

mit $\tilde{p}(x_0) \neq 0$ und $\tilde{q}(x_0) \neq 0$. Dabei ist auch $k = 0$ möglich.

Nun sind zwei Fälle zu unterscheiden:

1. Ist $k \geq l$, so ist

$$f(x) = (x - x_0)^{k-l} \cdot \frac{\tilde{p}(x)}{\tilde{q}(x)},$$

und die rechte Seite der Gleichung ist auch in $x = x_0$ definiert. Man nennt x_0 dann eine *hebbare Unbestimmtheitsstelle* von f . Der „unbestimmte Wert“ $f(x_0) = \frac{0}{0}$ kann in diesem Fall durch eine bestimmte reelle Zahl ersetzt werden.

2. Ist $k < l$, so ist

$$f(x) = \frac{1}{(x - x_0)^{l-k}} \cdot \frac{\tilde{p}(x)}{\tilde{q}(x)}.$$

Hier wird der erste Faktor bei Annäherung an x_0 beliebig groß, während der zweite Faktor einen bestimmten Wert annimmt. Man sagt in dieser Situation: f besitzt in x_0 eine *Polstelle* der Ordnung $l - k$.

8. Grenzwerte und Stetigkeit von Funktionen:

Definition.

Sei $I \subset \mathbb{R}$ ein Intervall, $x_0 \in I$ ein Punkt und f eine (zumindest) auf $I \setminus \{x_0\}$ definierte Funktion.

1. Wir sagen, f *strebt bei Annäherung an x_0 gegen den Wert c* , falls gilt:

Für **jede** Folge (x_n) in $I \setminus \{x_0\}$ mit $\lim_{n \rightarrow \infty} x_n = x_0$ ist $\lim_{n \rightarrow \infty} f(x_n) = c$.

Man schreibt dann: $\lim_{x \rightarrow x_0} f(x) = c$.

Dabei ist auch $c = \pm\infty$ zugelassen!

2. Jetzt sei $I = [a, \infty) = \{x \in \mathbb{R} \mid x \geq a\}$ und f auf ganz I definiert. Wir sagen, f strebt für x gegen Unendlich (asymptotisch) gegen c , falls gilt:

Für jede Folge (x_n) in I mit $\lim_{n \rightarrow \infty} x_n = +\infty$ ist $\lim_{n \rightarrow \infty} f(x_n) = c$.

Man schreibt dann: $\lim_{x \rightarrow +\infty} f(x) = c$.

3. Für Funktionen, die auf $(-\infty, a]$ definiert sind, erklärt man in analoger Weise den Grenzwert $\lim_{x \rightarrow -\infty} f(x)$.

Beispiele :

1. Die Geschichte mit der hebbaren Unbestimmtheitsstelle wird nun klarer:

$$\text{Es ist } \lim_{x \rightarrow -1} \frac{x^2 - 1}{x + 1} = \lim_{x \rightarrow -1} (x - 1) = -2.$$

Die Existenz des Grenzwertes sollte man noch etwas näher erläutern:

Ist (x_n) eine beliebige Folge mit $\lim_{n \rightarrow \infty} x_n = -1$, so ist $\lim_{n \rightarrow \infty} (x_n - 1) = -1 - 1 = -2$.

Weil $f(x) := \frac{x^2 - 1}{x + 1} = x - 1$ ist, ist $f(x_n) = x_n - 1$, und daher $\lim_{x \rightarrow -1} f(x) = -2$.

2. Sei nun $f(x) := \frac{x^2 + 1}{x + 1}$. Diese Funktion ist ebenfalls nicht in $x = -1$ definiert, und sie läßt sich nicht so leicht vereinfachen. Strebt x_n gegen -1 , so strebt $(x_n)^2 + 1$ gegen 2, aber der Nenner $x_n + 1$ gegen 0. Also strebt $f(x_n)$ gegen ∞ ? Halt! Ist $x_n < -1$, so ist $f(x_n) < 0$. Ist dagegen $x_n > -1$, so ist $f(x_n) > 0$. Bei Annäherung „von links“ erhält man daher den Grenzwert $-\infty$ und bei Annäherung „von rechts“ den Grenzwert $+\infty$.

Wir müssen also auch die einseitige Annäherung an eine Stelle untersuchen:

Definition.

Es sei $-\infty \leq a < b \leq +\infty$ und f auf (a, b) definiert. Wir sagen, f besitzt in a die Zahl c als rechtsseitigen Grenzwert, falls gilt:

Für jede Folge (x_n) mit $x_n > a$ und $\lim_{n \rightarrow \infty} x_n = a$ ist $\lim_{n \rightarrow \infty} f(x_n) = c$.

Man schreibt dann:

$$c = \lim_{x \rightarrow a+} f(x) = f(a+).$$

Dabei ist auch $c = \pm\infty$ zugelassen.

Analog wird der linksseitige Grenzwert $\lim_{x \rightarrow b-} f(x) = f(b-)$ mit Hilfe von Folgen (x_n) mit $x_n < b$ und $\lim_{n \rightarrow \infty} x_n = b$ erklärt.

Beispiel :

$$\text{Es ist } \lim_{x \rightarrow 0-} \frac{1}{x} = -\infty \text{ und } \lim_{x \rightarrow 0+} \frac{1}{x} = +\infty.$$

Aus den Grenzwert-Sätzen folgt für Funktionen:

I.5.4 Satz. *Es seien f und g zwei Funktionen auf $I \setminus \{a\}$, wobei I ein Intervall und a ein Punkt aus dem Inneren oder vom Rand des Intervalls ist. Wenn die Grenzwerte $\lim_{x \rightarrow a} f(x) = c$ und $\lim_{x \rightarrow a} g(x) = d$ existieren, dann gilt:*

1. $\lim_{x \rightarrow a} (f(x) \pm g(x)) = c \pm d.$
2. $\lim_{x \rightarrow a} (f(x) \cdot g(x)) = c \cdot d.$
3. *Ist $d \neq 0$, so ist $\lim_{x \rightarrow a} \frac{f(x)}{g(x)} = \frac{c}{d}.$*

Sei $a > 0$, $I := [a, \infty)$ und $f : I \rightarrow \mathbb{R}$ eine Funktion. Dann ist $f(\frac{1}{x})$ für alle $x \in (0, \frac{1}{a}]$ definiert. Offensichtlich gilt:

Wenn $\lim_{x \rightarrow 0^+} f(\frac{1}{x})$ existiert, dann existiert auch $\lim_{x \rightarrow +\infty} f(x)$, und beide Grenzwerte sind gleich.

Entsprechende Überlegungen gelten für die Annäherung an $-\infty$.

Daraus folgt z.B.:

I.5.5 Satz. *Sind p und q zwei Polynome mit $\text{grad}(p) < \text{grad}(q)$, so ist*

$$\lim_{x \rightarrow +\infty} \frac{p(x)}{q(x)} = \lim_{x \rightarrow -\infty} \frac{p(x)}{q(x)} = 0.$$

BEWEIS: Sei

$$p(x) = \sum_{i=0}^m a_i x^i \text{ und } q(x) = \sum_{k=0}^n b_k x^k,$$

mit $m < n$, $a_m \neq 0$ und $b_n \neq 0$. Dann gilt für $f(x) := \frac{p(x)}{q(x)}$:

$$\begin{aligned} f\left(\frac{1}{x}\right) &= \frac{a_m x^{-m} + \dots + a_0}{b_n x^{-n} + \dots + b_0} \\ &= \frac{a_m x^{n-m} + \dots + a_0 x^n}{b_n + b_{n-1} x + \dots + b_0 x^n}. \end{aligned}$$

Also ist $\lim_{x \rightarrow 0^+} f\left(\frac{1}{x}\right) = 0.$ □

Als Folgerung ergibt sich für Polynome p und q mit $\text{grad}(p) > \text{grad}(q)$:

Ist $p(x) = g(x) \cdot q(x) + r(x)$ mit $\text{deg}(r) < \text{deg}(q)$ (Division mit Rest), so ist

$$\lim_{x \rightarrow +\infty} \frac{p(x)}{q(x)} = \lim_{x \rightarrow +\infty} g(x).$$

Definition.

Sei f eine Funktion.

1. Ist $x_0 \in \mathbb{R}$ und $\lim_{x \rightarrow x_0^+} f(x) = \pm\infty$ oder $\lim_{x \rightarrow x_0^-} f(x) = \pm\infty$, so heißt die Gerade $\{(x, y) \mid x = x_0\}$ eine *vertikale Asymptote* von f .
2. Ist g eine weitere Funktion und $\lim_{x \rightarrow \pm\infty} (f(x) - g(x)) = 0$, so heißt der Graph von g eine *asymptotische Kurve* für f . Ist g sogar eine affin-lineare Funktion vom Typ $g(x) = mx + t$, so spricht man auch hier von einer *Asymptoten*.

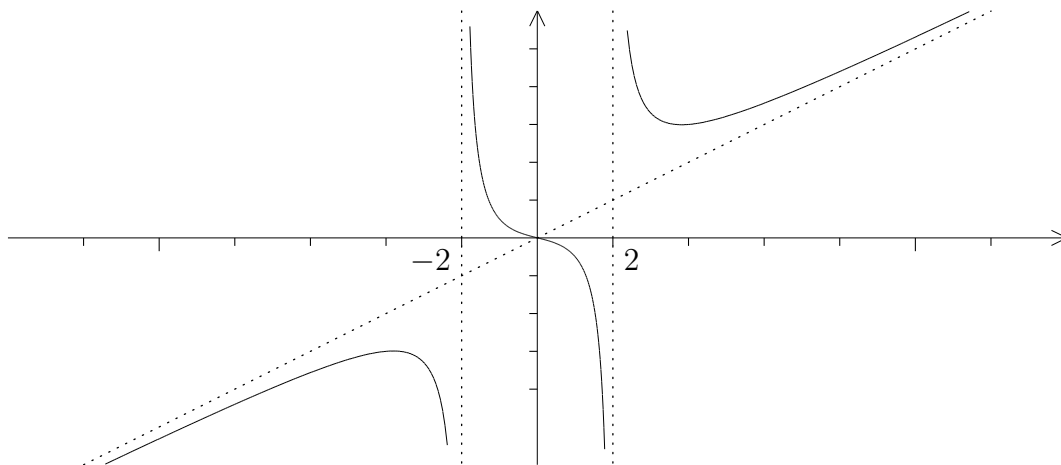
Beispiel:

Sei $f(x) := \frac{x^3 + 2x}{2x^2 - 8}$ für $x \neq \pm 2$. Polynomdivision ergibt:

$$x^3 + 2x = x \cdot (x^2 - 4) + 6x, \quad \text{also}$$

$$f(x) = \frac{x}{2} + \frac{3x}{(x-2)(x+2)}.$$

Die Geraden $\{x = -2\}$ und $\{x = +2\}$ sind offensichtlich vertikale Asymptoten. Die Gerade $\{y = \frac{1}{2}x\}$ ist eine weitere Asymptote, $x = 0$ die einzige Nullstelle. Es ergibt sich dann folgendes Bild:

**Definition.**

Sei $I \subset \mathbb{R}$ ein Intervall, $f : I \rightarrow \mathbb{R}$ eine Funktion und $x_0 \in I$.

f heißt *stetig in x_0* , falls gilt: $\lim_{x \rightarrow x_0} f(x) = f(x_0)$.

f heißt *stetig auf I* , falls f in jedem Punkt $x \in I$ stetig ist.

Nun ist unmittelbar klar:

I.5.6 Satz. Sind f und g beide in x_0 stetig, so sind auch $f \pm g$ und $f \cdot g$ in x_0 stetig.

Da $f(x) := x$ und natürlich auch alle konstanten Funktionen stetig sind, ist jedes Polynom auf ganz \mathbb{R} stetig.

Wir werden weiter unten beweisen, daß rationale Funktionen auf ihrem Definitionsbereich stetig sind. Die rationale Funktion $f(x) := \frac{x^n - 1}{x^m - 1}$ ist in $x = 1$ nicht definiert. Kürzt man durch $x - 1$, so erhält man:

$$f(x) = \frac{1 + x + \cdots + x^{n-1}}{1 + x + \cdots + x^{m-1}} \quad (\text{für } x \neq 1).$$

Also ist offensichtlich $\lim_{x \rightarrow 1} f(x) = \frac{n}{m}$. Die Funktion

$$F(x) := \begin{cases} f(x) & \text{falls } x \neq 1 \\ \frac{n}{m} & \text{falls } x = 1 \end{cases}$$

ist dann stetig, und man sagt, f ist *nach 1 stetig fortsetzbar*.

Betrachten wir schließlich das Beispiel $f(x) := [x]$.

Im Innern der Intervalle $I_n := [n, n + 1]$ ist f konstant und daher stetig. An den Endpunkten $x_n := n$ existieren der linksseitige und der rechtsseitige Grenzwert:

$$\lim_{x \rightarrow n+} f(x) = n = f(n) \quad \text{und} \quad \lim_{x \rightarrow n-} f(x) = n - 1.$$

Also ist f in x_n nicht stetig.

Allgemein gilt:

I.5.7 Satz. *Eine Funktion f ist genau dann in x_0 stetig, wenn $f(x_0+)$ und $f(x_0-)$ beide existieren und gleich sind.*

Definition.

Die Funktion f sei in der Nähe von x_0 definiert. Wenn $f(x_0+)$ und $f(x_0-)$ existieren und *nicht* gleich sind, nennt man x_0 eine *Sprungstelle* von f .

Den Wert $|f(x_0+) - f(x_0-)|$ nennt man die *Sprunghöhe*.

Das folgende Kriterium ist recht nützlich:

I.5.8 Satz. *Sei $f : I := [a, b] \rightarrow \mathbb{R}$ streng monoton wachsend, $J := [f(a), f(b)]$.*

Dann ist $f(I) \subset J$, und f besitzt höchstens Sprungstellen als Unstetigkeitsstellen.

Ist sogar $f(I) = J$, so ist f auf ganz I stetig.

BEWEIS: Mit Hilfe des Satzes von der monotonen Konvergenz kann man folgern, daß überall der linksseitige und der rechtsseitige Grenzwert existiert. Ist $f : I \rightarrow J$ monoton und surjektiv, so kann es aber keine Sprungstellen geben. \square

Wenn einer der einseitigen Grenzwerte (oder gar beide) nicht existieren, dann liegt in x_0 eine kompliziertere Unstetigkeitsstelle vor. Ein Beispiel dafür werden wir später sehen.

Nun folgen weitere wichtige Sätze zur Stetigkeit:

I.5.9 Satz. Die Funktion $f : I \rightarrow \mathbb{R}$ sei in $x_0 \in I$ stetig. Ist $f(x_0) > 0$ (bzw. $f(x_0) < 0$), so gibt es eine ε -Umgebung $U_\varepsilon(x_0)$, so daß $f(x) > 0$ (bzw. $f(x) < 0$) für alle $x \in I \cap U_\varepsilon(x_0)$ ist.

I.5.10 Folgerung. Ist f in x_0 stetig und $f(x_0) \neq 0$, so ist auch $\frac{1}{f}$ in x_0 stetig.

Insbesondere sind rationale Funktionen überall dort stetig, wo sie definiert sind.

I.5.11 Satz. Ist f stetig in x_0 und g stetig in $y_0 := f(x_0)$, so ist die zusammengesetzte Funktion $g \circ f$ stetig in x_0 .

Der Beweis ist sehr einfach.

Besonders wichtig ist der folgende Satz:

I.5.12 Zwischenwertsatz. Sei f auf dem abgeschlossenen Intervall $[a, b]$ stetig, $f(a) \neq f(b)$ und c ein Wert zwischen $f(a)$ und $f(b)$.

Dann gibt es ein $\xi \in [a, b]$ mit $f(\xi) = c$.

BEWEIS: Ist $c = f(a)$ oder $c = f(b)$, so ist nichts zu zeigen.

Es sei also $f(a) < c < f(b)$ (der Fall $f(a) > c > f(b)$ wird ganz analog behandelt). Außerdem sei zur Vereinfachung $c = 0$.

Wir betrachten die Menge $\{x \in [a, b] \mid f(x) < 0\}$. Da $M \neq \emptyset$ ist, existiert $\xi := \sup(M)$, und man kann in $[a, \xi)$ eine monoton wachsende Folge (x_ν) finden, die gegen ξ konvergiert. Wegen der Stetigkeit von f ist $f(\xi) \leq 0$. Wäre aber sogar $f(\xi) < 0$, so wäre $f(x) < 0$ für alle x in einer ε -Umgebung von ξ . Das widerspricht der Definition von ξ . Also ist $f(\xi) = 0$.

□

Als Anwendung untersuchen wir das Verhalten von Polynomen für $x \rightarrow \pm\infty$. Zunächst ist klar:

$$\begin{aligned} \lim_{x \rightarrow +\infty} x^m &= +\infty && (\text{für alle } m \in \mathbb{N}), \\ \lim_{x \rightarrow -\infty} x^m &= \begin{cases} +\infty & \text{falls } m \text{ gerade} \\ -\infty & \text{falls } m \text{ ungerade} \end{cases} \end{aligned}$$

I.5.13 Satz. Sei $f(x) = a_m x^m + \dots + a_1 x + a_0$ ein Polynom vom Grad m . Ist $a_m > 0$, so verhält sich f für $x \rightarrow \pm\infty$ wie x^m . Ist $a_m < 0$, so verhält sich f wie $-x^m$.

BEWEIS: Da $a_m \neq 0$ ist, können wir schreiben:

$$\begin{aligned} f(x) &= a_m x^m \cdot \left(1 + \frac{a_{m-1}}{a_m} \cdot \frac{1}{x} + \dots + \frac{a_0}{a_m} \cdot \frac{1}{x^m} \right) \\ &= a_m x^m \cdot \left(1 + \frac{1}{x} \cdot g\left(\frac{1}{x}\right) \right), \end{aligned}$$

wobei $g(y) := \frac{a_{m-1}}{a_m} + \dots + \frac{a_0}{a_m} \cdot y^{m-1}$ ein Polynom vom Grad $m-1$ ist.

Für $x \rightarrow \pm\infty$ strebt $\frac{1}{x}$ gegen Null. Da g auf ganz \mathbb{R} stetig ist, strebt dann $1 + \frac{1}{x} \cdot g\left(\frac{1}{x}\right)$ gegen 1, also $f(x)$ gegen den gleichen Wert wie $a_m x^m$. Daraus folgt die Behauptung. □

I.5.14 Folgerung. Sei $f(x)$ ein Polynom vom Grad n . Ist n ungerade, so besitzt f wenigstens eine Nullstelle.

BEWEIS: O.B.d.A. sei f normiert, d.h. der höchste Koeffizient = 1. Für $x \rightarrow \pm\infty$ verhält sich $f(x)$ wie x^n . Da n ungerade ist, gilt:

$$\lim_{x \rightarrow -\infty} f(x) = -\infty \text{ und } \lim_{x \rightarrow +\infty} f(x) = +\infty.$$

Beschränkt man die stetige Funktion f auf ein Intervall $[a, b]$, wo $a \ll 0$ und $b \gg 0$ ist, so kann man den Zwischenwertsatz benutzen und erhält ein $\xi \in \mathbb{R}$ mit $f(\xi) = 0$. \square

Wichtig ist auch der folgende Satz vom Minimum und Maximum:

I.5.15 Satz von Weierstraß. Die Funktion f sei auf dem abgeschlossenen Intervall $[a, b]$ stetig. Dann nimmt f in gewissen Punkten des Intervalls seinen kleinsten und seinen größten Wert an.

Daß diese Aussage nicht selbstverständlich ist, zeigt folgendes einfache Beispiel: die Funktion $\frac{1}{x}$ ist auf dem offenen Intervall $I = (0, 1)$ stetig, nimmt dort aber keinen größten Wert an.

Den Beweis des Satzes von Weierstraß lassen wir aus.

9. Exponentialfunktion und Logarithmus:

Betrachten wir folgende Tabelle:

n	0	1	2	3	4	5	6	7	8	9	10
2^n	1	2	4	8	16	32	64	128	256	512	1024

Da $x^n \cdot x^m = x^{n+m}$ ist, kann man z.B. $8 \cdot 32$ folgendermaßen berechnen: Es ist

$$8 \cdot 32 = 2^3 \cdot 2^5 = 2^{3+5} = 2^8 = 256.$$

Leider liefert unsere Tabelle nur in wenigen Fällen eine Zurückführung der Multiplikation auf die Addition. Es wäre praktisch, wenn man eine bijektive stetige Funktion $f : [1, \infty) \rightarrow \mathbb{R}_+$ mit $f(2^n) = n$ hätte, für die generell gilt: $f(x \cdot y) = f(x) + f(y)$. Dann wäre

$$x \cdot y = f^{-1}(f(x) + f(y)).$$

Die Mathematiker liefern uns die gewünschte Funktion frei Haus:

I.5.16 Satz.

Zu jeder reellen Zahl $a > 1$ gibt es genau eine streng monoton wachsende und surjektive Funktion $f : \mathbb{R}_+ \rightarrow \mathbb{R}$ mit folgenden Eigenschaften:

1. $f(x \cdot y) = f(x) + f(y)$.
2. $f(1) = 0$.
3. $f(a) = 1$.

Definition.

Die Funktion, deren Existenz der obige Satz sichert, bezeichnet man als *Logarithmus zur Basis a* und schreibt sie in der Form $\boxed{\log_a(x)}$.

Da das Logarithmieren Punkt-Rechnungen in Strich-Rechnungen verwandelt, hat man vor der Einführung des Taschenrechners oder Computers viel mit Logarithmentafeln gearbeitet. Wegen unseres Dezimalsystems benutzten diese Tafeln üblicherweise die Basis 10. Mit $\lg(x)$ bezeichnet man diesen *Zehner-Logarithmus* oder *Briggschen Logarithmus* $\log_{10}(x)$.

$\ln(x) := \log_e(x)$ nennt man den *natürlichen Logarithmus*.

I.5.17 Satz. $\log_a : \mathbb{R}_+ \rightarrow \mathbb{R}$ ist stetig, und es gilt:

1. $\log_a(y^n) = n \cdot \log_a(y)$.
2. $\log_a\left(\frac{u}{v}\right) = \log_a(u) - \log_a(v)$ für $u, v > 0$.

I.5.18 Satz. Sind $a, b \in \mathbb{R}_+$, beide > 1 , so kann man den Logarithmus zur Basis a in den zur Basis b umrechnen: Für $x > 0$ ist

$$\log_b(x) = \frac{\log_a(x)}{\log_a(b)}.$$

Insbesondere gilt:

$$\log_a(b) \cdot \log_b(a) = 1.$$

BEWEIS: Sei $f(x) := \frac{\log_a(x)}{\log_a(b)}$. Dann gilt:

1. $f(x \cdot y) = f(x) + f(y)$.
2. $f(1) = 0$.
3. $f(b) = 1$.

Aber dann muß $f(x) = \log_b(x)$ sein. □

Man kann nun leicht zeigen, daß man $\log_a(x)$ auch für $0 < a < 1$ definieren kann. Aber das ist für uns von geringem Interesse.

Nun bedienen wir uns der Tatsache, daß $\log_a : \mathbb{R}_+ \rightarrow \mathbb{R}$ bijektiv ist.

Definition.

Es sei $a > 1$ eine feste reelle Zahl. Dann wird durch

$$\boxed{\exp_a(x) := (\log_a)^{-1}(x)}$$

eine Funktion auf ganz \mathbb{R} definiert, die *Exponentialfunktion zur Basis a* .

Es folgt:

I.5.19 Satz. Sei $a > 1$.

1. \exp_a ist auf ganz \mathbb{R} stetig und nimmt nur positive Werte an.
2. $\exp_a(x_1 + x_2) = \exp_a(x_1) \cdot \exp_a(x_2)$.
Man nennt das die Funktionalgleichung der Exponentialfunktion.
3. Es ist $\exp_a(0) = 1$ und $\exp_a(1) = a$.
4. \exp_a ist streng monoton wachsend.
5. Ist $n \in \mathbb{N}$, so ist $\exp_a(n) = a^n$ und $\exp_a(\frac{1}{n}) = \sqrt[n]{a}$.
6. Allgemein ist $\exp_a(-x) = (\exp_a(x))^{-1}$.

Die Aussagen folgen alle aus den Eigenschaften des Logarithmus. Z.B. ist

$$\begin{aligned} a &= \exp_a(1) = \exp_a\left(n \cdot \frac{1}{n}\right) \\ &= \exp_a\left(\frac{1}{n} + \dots + \frac{1}{n}\right) \\ &= \exp_a\left(\frac{1}{n}\right)^n. \end{aligned}$$

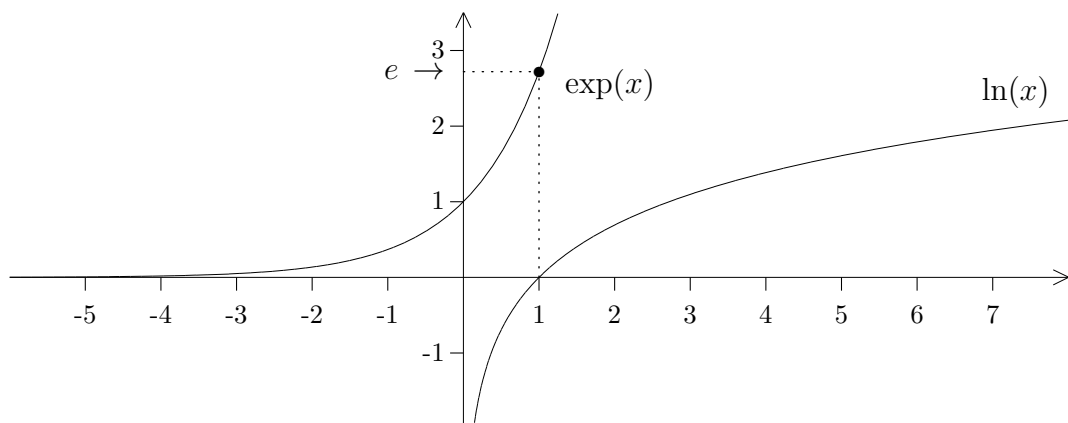
Man schreibt nun auch a^x statt $\exp_a(x)$. Dadurch werden die Formeln noch einprägsamer. Außerdem setzt man

$$\exp(x) := e^x$$

und spricht dabei von der *Exponentialfunktion* schlechthin. Es gilt:

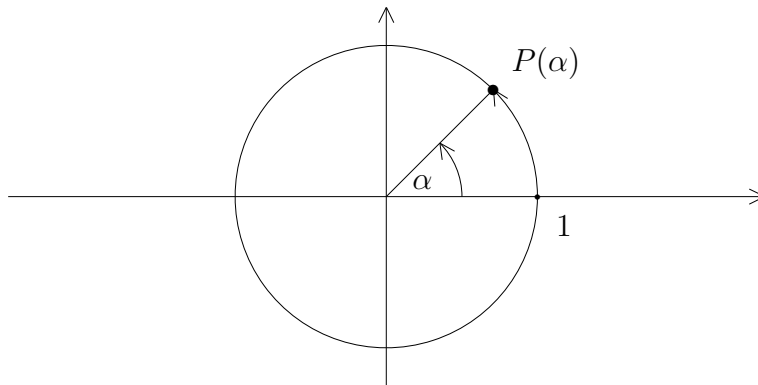
$$a^x = e^{x \ln a}$$

Die Graphen von Exponentialfunktion und Logarithmus haben folgende Gestalt:



10. Winkelfunktionen:

Wir betrachten einen Punkt P im \mathbb{R}^2 , der sich gegen den Uhrzeigersinn auf dem Rand des Einheitskreises bewegt:



Vom Ursprung aus sieht man P unter einem gewissen Winkel α , gemessen von der positiven x -Achse aus. Der Winkel bewegt sich zwischen 0° und 360° . Mit *Arkus von α* (in Zeichen $\text{arc}(\alpha)$) bezeichnet man die Länge des zurückgelegten Bogens. Sie ist proportional zum Winkel.

Bekanntlich bezeichnet π die Länge des halben Einheitskreisbogens. Wegen der Proportionalität zwischen Winkel und Bogenmaß gilt dann:

$$\text{arc}(\alpha) = \frac{\pi}{180} \cdot \alpha.$$

Die Zahl π ist irrational, ja sogar *transzendent*, d.h. sie kann nicht mit Hilfe von Wurzeln aus rationalen Zahlen dargestellt werden. Der Anfang der Dezimalbruchentwicklung von π ist

$$\pi = 3.141592653\dots$$

Die Ziffern 1, 1, 3, 3, 5, 5 liefern übrigens bei geeigneter Anordnung eine erstaunlich gute rationale Näherung von π :

$$\frac{355}{113} = 3.1415929$$

Wir schreiben P in der Form $P(\alpha) = (x(\alpha), y(\alpha))$, wobei α im Bogenmaß gemessen wird. Bewegt sich der Punkt mehrmals um den Kreis, oder bewegt er sich rückwärts, so nimmt er in regelmäßigen Abständen immer wieder die gleiche Position ein.

Definition.

Eine Funktion $f : \mathbb{R} \rightarrow \mathbb{R}$ heißt *periodisch* mit der Periode p , falls $f(x + p) = f(x)$ für alle $x \in \mathbb{R}$ gilt.

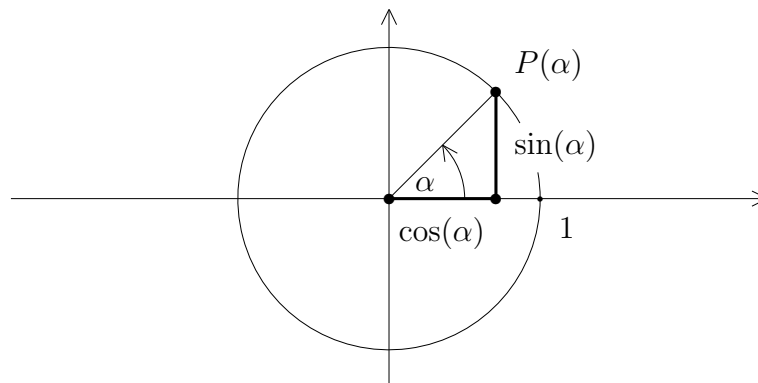
Offensichtlich sind die Komponenten von $P(\alpha)$ periodische Funktionen von α mit der Periode 2π .

Definition.

Die Winkelfunktionen *Sinus* und *Cosinus* werden definiert durch

$$P(\alpha) = (\cos(\alpha), \sin(\alpha)).$$

Wir schreiben allerdings auch dann $\cos(\alpha)$ und $\sin(\alpha)$, wenn mit α der Winkel im Gradmaß gemeint ist, d.h. es ist z.B. $\cos(45^\circ) = \cos\left(\frac{\pi}{4}\right)$.



Von Sinus und Cosinus werden weitere Funktionen abgeleitet, wie

$$\tan(x) := \frac{\sin(x)}{\cos(x)} \quad (\text{Tangens})$$

$$\text{und } \cot(x) := \frac{\cos(x)}{\sin(x)} \quad (\text{Cotangens}).$$

Definition.

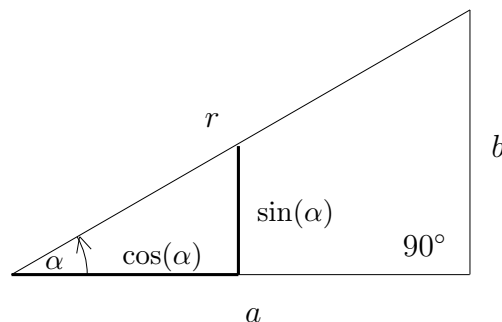
Eine Funktion $f : \mathbb{R} \rightarrow \mathbb{R}$ heißt *gerade*, falls $f(-x) = f(x)$ für alle $x \in \mathbb{R}$ ist. Sie heißt *ungerade*, falls $f(-x) = -f(x)$ für alle $x \in \mathbb{R}$ ist.

Beispiel:

$f(x) := x^2$ ist offensichtlich gerade, während $f(x) := x^3$ ungerade ist.

Da die Punkte $P(\alpha)$ und $P(-\alpha)$ spiegelbildlich zur x -Achse liegen, ist Cosinus eine gerade und Sinus eine ungerade Funktion. Daraus folgt, daß Tangens und Cotangens beides ungerade Funktionen sind.

Eine andere Charakterisierung der Winkelfunktionen stammt aus der Elementargeometrie:



Wir betrachten ein rechtwinkliges Dreieck mit den Katheten a und b und der Hypotenuse r . Der Winkel zwischen a und r sei mit α bezeichnet. Dann nennt man a auch die *Ankathete* zu α und b die *Gegenkathete* zu α , und es gilt – unabhängig von der Größe des Dreiecks – folgende Beziehung:

$$\frac{a}{r} = \frac{\text{Ankathete}}{\text{Hypotenuse}} = \cos(\alpha),$$

$$\frac{b}{r} = \frac{\text{Gegenkathete}}{\text{Hypotenuse}} = \sin(\alpha).$$

Man kann diese Beziehungen benutzen, um einige Werte der Winkelfunktionen zu berechnen:

x	0	$\frac{\pi}{6}$	$\frac{\pi}{4}$	$\frac{\pi}{3}$	$\frac{\pi}{2}$	π
$\cos(x)$	1	$\frac{1}{2}\sqrt{3}$	$\frac{1}{2}\sqrt{2}$	$\frac{1}{2}$	0	-1
$\sin(x)$	0	$\frac{1}{2}$	$\frac{1}{2}\sqrt{2}$	$\frac{1}{2}\sqrt{3}$	1	0
$\tan(x)$	0	$\frac{1}{3}\sqrt{3}$	1	$\sqrt{3}$	∞	0

Um weitere Werte zu ermitteln, braucht man die

I.5.20 Additionstheoreme. Für beliebige Winkel α, β gilt:

$$\begin{aligned}\sin(\alpha + \beta) &= \sin(\alpha)\cos(\beta) + \cos(\alpha)\sin(\beta), \\ \cos(\alpha + \beta) &= \cos(\alpha)\cos(\beta) - \sin(\alpha)\sin(\beta).\end{aligned}$$

Der Beweis kann – zumindest für spitze Winkel – elementargeometrisch geführt werden.

I.5.21 Folgerung. Für beliebige Winkel α gilt:

$$\begin{aligned}\sin(2\alpha) &= 2\sin(\alpha)\cos(\alpha) \\ \cos(2\alpha) &= \cos^2(\alpha) - \sin^2(\alpha).\end{aligned}$$

I.5.22 Folgerung.

- $\sin(\alpha + \frac{\pi}{2}) = \cos(\alpha)$ und $\cos(\alpha + \frac{\pi}{2}) = -\sin(\alpha)$.
- $\sin(\alpha + \pi) = -\sin(\alpha)$ und $\cos(\alpha + \pi) = -\cos(\alpha)$.

Es folgt insbesondere, daß die Graphen von Sinus und Cosinus gleich aussehen, sie sind nur um $\frac{\pi}{2}$ gegeneinander verschoben. Und es folgt, daß Tangens und Cotangens sogar periodisch mit der Periode π sind.

Aus der Definition von Sinus und Cosinus am Einheitskreis ergibt sich außerdem:

I.5.23 Satz. Für alle $x \in \mathbb{R}$ ist $\sin^2(x) + \cos^2(x) = 1$.

I.5.24 Folgerung. Für beliebiges α ist $|\cos(\alpha)| \leq 1$ und $|\sin(\alpha)| \leq 1$.

I.5.25 Satz. Die Funktion $\sin(x)$ ist auf $[0, \frac{\pi}{2}]$ streng monoton wachsend.

Wir verzichten hier auf den BEWEIS, der sehr viel einfacher mit Hilfe der Differentialrechnung geführt werden kann.

Da der Sinus eine ungerade Funktion ist, ist $\sin(x)$ sogar auf $[-\frac{\pi}{2}, +\frac{\pi}{2}]$ streng monoton wachsend. Und da

$$\sin\left(\frac{\pi}{2} + x\right) = \sin\left(\frac{\pi}{2} - x\right)$$

gilt, ist $\sin(x)$ auf $[\frac{\pi}{2}, \frac{3\pi}{2}]$ streng monoton fallend.

I.5.26 Satz. *Es ist*

$$\lim_{x \rightarrow 0} \sin(x) = 0, \quad \lim_{x \rightarrow 0} \cos(x) = 1, \quad \lim_{x \rightarrow 0} \frac{\sin(x)}{x} = 1$$

und

$$\lim_{x \rightarrow 0} \frac{1 - \cos(x)}{x} = 0.$$

Auch dieser BEWEIS kann elementargeometrisch geführt werden.

I.5.27 Folgerung. *Sinus und Cosinus sind auf ganz \mathbb{R} stetig.*

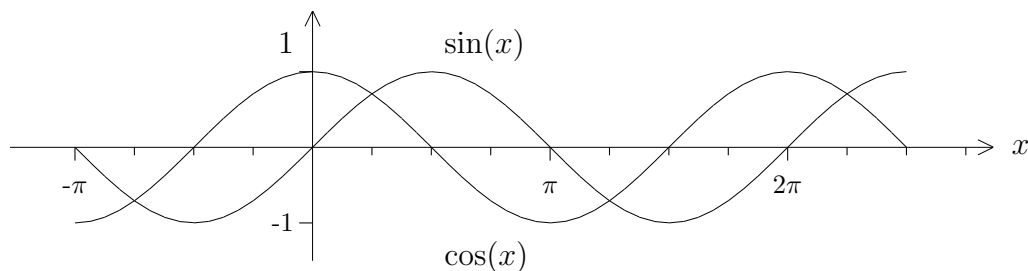
BEWEIS: Auf Grund des gerade bewiesenen Satzes sind $\sin(x)$ und $\cos(x)$ in $x = 0$ stetig. Wir betrachten jetzt nur den Sinus, beim Cosinus geht's analog.

Sei $x_0 \in \mathbb{R}$ beliebig, (x_n) eine Folge, die gegen x_0 konvergiert, $h_n := x_n - x_0$. Dann gilt:

$$\sin(x_n) = \sin(x_0 + h_n) = \sin(x_0) \cos(h_n) + \cos(x_0) \sin(h_n),$$

und dieser Ausdruck strebt gegen $\sin(x_0)$. Also ist der Sinus in x_0 stetig. □

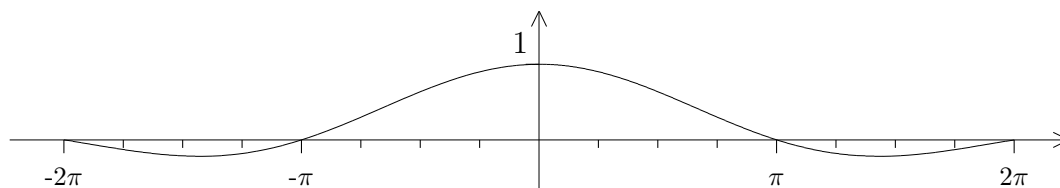
Für die Funktionsgraphen von Sinus und Cosinus ergibt sich nun folgendes Bild:



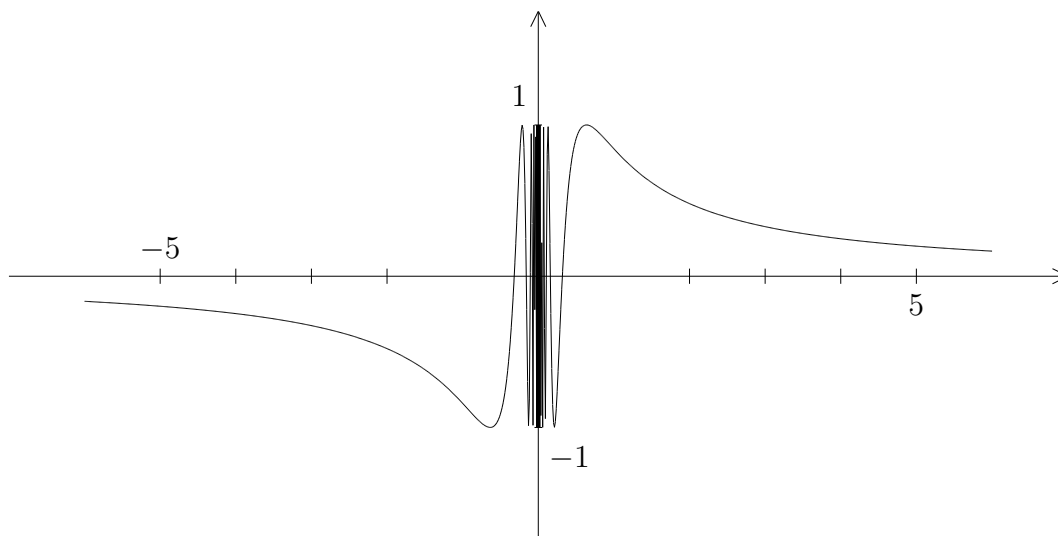
I.5.28 Satz.

Die Funktion $f(x) := \begin{cases} \frac{\sin(x)}{x} & \text{falls } x \neq 0 \\ 1 & \text{falls } x = 0 \end{cases}$ ist überall stetig.

Der BEWEIS ist klar, Der Funktionsgraph dieser Funktion hat folgende Gestalt:



Sehr viel unangenehmer verhält sich die Funktion $f(x) := \sin\left(\frac{1}{x}\right)$:



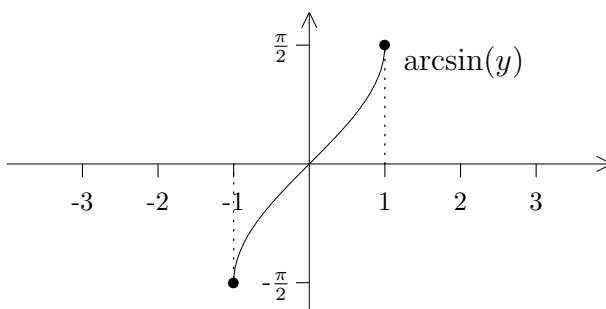
Dies ist ein Beispiel einer Unstetigkeitsstelle, die keine Sprungstelle und keine Polstelle ist.

Als streng monoton wachsende Funktion ist $\sin : [-\frac{\pi}{2}, +\frac{\pi}{2}] \rightarrow [-1, +1]$ bijektiv.

Die Umkehrabbildung

$$\arcsin := \sin^{-1} : [-1, +1] \rightarrow [-\frac{\pi}{2}, +\frac{\pi}{2}]$$

wird als (*Hauptwert des*) *Arcussinus* bezeichnet. Vom „Hauptwert“ spricht man, weil man den Sinus natürlich auf jedem Intervall umkehren kann, wo er streng monoton ist. Das ergibt andere „Zweige“ des Arcussinus.



Der Cosinus ist auf $[0, \pi]$ streng monoton fallend, bildet dieses Intervall also bijektiv auf $[-1, 1]$ ab. Die Umkehrfunktion $\arccos : [-1, 1] \rightarrow [0, \pi]$ ist der Hauptwert des *Arcuscossinus*.

Zwischen 0 und 2π hat der Sinus die Nullstellen 0, π , 2π (wie man sofort am Einheitskreis sieht). Also ist

$$\{x \in \mathbb{R} \mid \sin(x) = 0\} = \{x \in \mathbb{R} \mid \exists n \in \mathbb{Z} \text{ mit } x = n\pi\}$$

die Menge aller Nullstellen des Sinus, und entsprechend ist

$$\{x \in \mathbb{R} \mid \cos(x) = 0\} = \{x \in \mathbb{R} \mid \exists n \in \mathbb{Z} \text{ mit } x = \frac{\pi}{2} + n\pi\}$$

die Menge aller Nullstellen des Cosinus. Außerhalb der letzteren Menge ist der Tangens definiert, und offensichtlich gilt:

$$\lim_{x \rightarrow -\pi/2+} \tan(x) = -\infty \quad \text{und} \quad \lim_{x \rightarrow +\pi/2-} \tan(x) = +\infty.$$

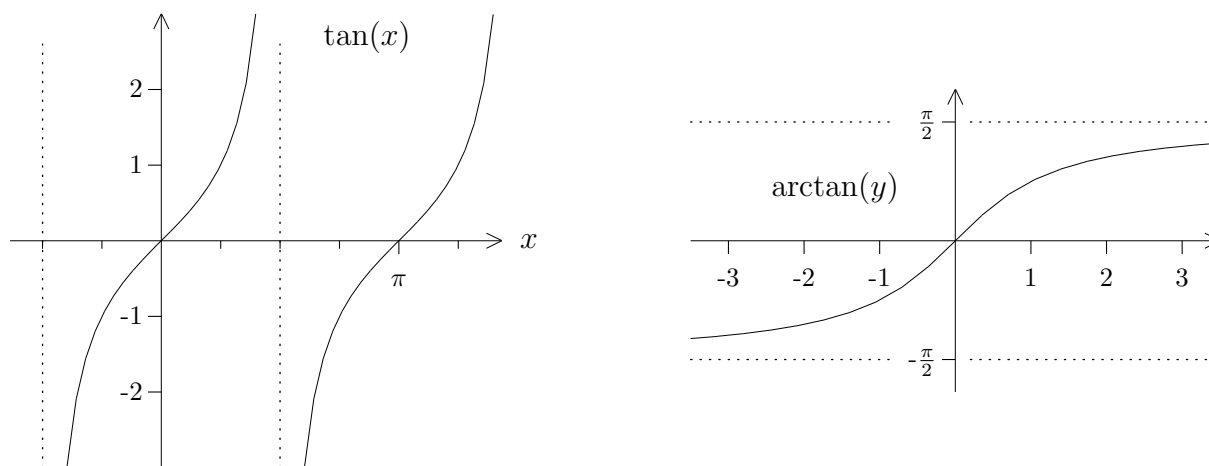
Man kann sich auch überlegen, daß $\tan : (-\frac{\pi}{2}, +\frac{\pi}{2}) \rightarrow \mathbb{R}$ streng monoton wachsend und stetig ist, also bijektiv.

Die Umkehrfunktion

$$\arctan := \tan^{-1} : \mathbb{R} \rightarrow \left(-\frac{\pi}{2}, +\frac{\pi}{2}\right)$$

ist der *Arcustangens*. Man beachte, daß $\pm\frac{\pi}{2}$ nicht als Wert angenommen wird.

Die Graphen von Tangens und Arcustangens sehen folgendermaßen aus:



Schließlich kann man auch den Cotangens auf gewissen Intervallen umkehren und erhält so den Arcuscotangens.

11. Hyperbelfunktionen:

Definition.

Die auf ganz \mathbb{R} definierten Funktionen

$$\sinh(x) := \frac{1}{2}(e^x - e^{-x}) \quad \text{und} \quad \cosh(x) := \frac{1}{2}(e^x + e^{-x})$$

heißen *Sinus hyperbolicus* und *Cosinus hyperbolicus*.

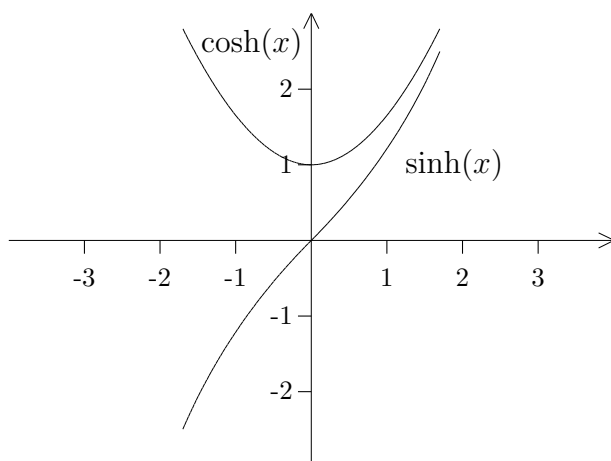
Offensichtlich ist $\cosh(x)$ eine gerade und $\sinh(x)$ eine ungerade Funktion. Weiter gilt:

$$\cosh(0) = 1 \quad \text{und} \quad \lim_{x \rightarrow -\infty} \cosh(x) = \lim_{x \rightarrow +\infty} \cosh(x) = +\infty,$$

sowie

$$\sinh(0) = 0, \quad \lim_{x \rightarrow -\infty} \sinh(x) = -\infty \quad \text{und} \quad \lim_{x \rightarrow +\infty} \sinh(x) = +\infty.$$

Außerdem ist $\sinh(x) < \cosh(x)$ für alle $x \in \mathbb{R}$. Die Graphen sehen also ungefähr folgendermaßen aus:



Es ist

$$\cosh^2(x) - \sinh^2(x) = 1 \quad \text{für alle } x.$$

Deshalb wird durch

$$\varphi(t) := (\cosh(t), \sinh(t))$$

die *Hyperbel* $H := \{(x, y) \in \mathbb{R}^2 \mid x^2 - y^2 = 1\}$ parametrisiert.

Schließlich definiert man noch:

$$\tanh(x) := \frac{\sinh(x)}{\cosh(x)}$$

$$\text{und} \quad \coth(x) := \frac{\cosh(x)}{\sinh(x)}.$$

Über Umkehrfunktionen der Hyperbelfunktionen werden wir an späterer Stelle sprechen.

§6 Vektoren

Unter dem *n-dimensionalen euklidischen Raum* verstehen wir die Menge aller n-Tupel (x_1, \dots, x_n) von reellen Zahlen:

$$\mathbb{R}^n = \{(x_1, \dots, x_n) \mid x_i \in \mathbb{R} \text{ für } i = 1, \dots, n\}.$$

Ein Element des \mathbb{R}^n bezeichnen wir als *Punkt*.

Zu zwei Elementen $\mathbf{x} = (x_1, \dots, x_n) \in \mathbb{R}^n$ und $\mathbf{y} = (y_1, \dots, y_n) \in \mathbb{R}^n$ wird die Summe definiert durch

$$\mathbf{x} + \mathbf{y} := (x_1 + y_1, \dots, x_n + y_n).$$

Zu einem Element $\mathbf{x} = (x_1, \dots, x_n) \in \mathbb{R}^n$ und einer Zahl $\alpha \in \mathbb{R}$ wird das Produkt definiert durch

$$\alpha \cdot \mathbf{x} := (\alpha x_1, \dots, \alpha x_n).$$

Ist $\mathbf{0} = (0, \dots, 0)$ der Nullpunkt und $-(x_1, \dots, x_n) := (-x_1, \dots, -x_n)$, so gelten folgende Rechenregeln:

$$\begin{aligned} V1. \quad \mathbf{x} + (\mathbf{y} + \mathbf{z}) &= (\mathbf{x} + \mathbf{y}) + \mathbf{z}, \\ V2. \quad \mathbf{x} + \mathbf{y} &= \mathbf{y} + \mathbf{x}, \\ V3. \quad \mathbf{x} + \mathbf{0} &= \mathbf{x}, \\ V4. \quad \mathbf{x} + (-\mathbf{x}) &= \mathbf{0}. \end{aligned}$$

$(\mathbb{R}^n, +)$ ist also eine kommutative Gruppe.

Für die Multiplikation gelten folgende Rechenregeln:

$$\begin{aligned} V5. \quad (\alpha + \beta) \cdot \mathbf{x} &= \alpha \cdot \mathbf{x} + \beta \cdot \mathbf{x}, \\ V6. \quad \alpha \cdot (\mathbf{x} + \mathbf{y}) &= \alpha \cdot \mathbf{x} + \alpha \cdot \mathbf{y}, \\ V7. \quad \alpha \cdot (\beta \cdot \mathbf{x}) &= (\alpha\beta) \cdot \mathbf{x}, \\ V8. \quad 1 \cdot \mathbf{x} &= \mathbf{x}. \end{aligned}$$

Definition.

Ein rechteckiges Zahlenschema

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1m} \\ a_{21} & a_{22} & \dots & a_{2m} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nm} \end{pmatrix}$$

wird als (reellwertige) *Matrix* mit *n Zeilen* und *m Spalten* bezeichnet. Die Einträge a_{11}, a_{12}, \dots nennt man die *Koeffizienten* der Matrix.

Die Menge aller solchen $(n \times m)$ -Matrizen wird mit $M_{n,m}(\mathbb{R})$ bezeichnet.

Man kann Matrizen addieren und mit reellen Zahlen multiplizieren:

$$\begin{pmatrix} a_{11} & \dots & a_{1m} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nm} \end{pmatrix} + \begin{pmatrix} b_{11} & \dots & b_{1m} \\ \vdots & & \vdots \\ b_{n1} & \dots & b_{nm} \end{pmatrix} := \begin{pmatrix} a_{11} + b_{11} & \dots & a_{1m} + b_{1m} \\ \vdots & & \vdots \\ a_{n1} + b_{n1} & \dots & a_{nm} + b_{nm} \end{pmatrix},$$

$$\alpha \cdot \begin{pmatrix} a_{11} & \dots & a_{1m} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nm} \end{pmatrix} := \begin{pmatrix} \alpha \cdot a_{11} & \dots & \alpha \cdot a_{1m} \\ \vdots & & \vdots \\ \alpha \cdot a_{n1} & \dots & \alpha \cdot a_{nm} \end{pmatrix}$$

Die „Null-Matrix“ ist gegeben durch

$$\mathbf{0} := \begin{pmatrix} 0 & \dots & 0 \\ \vdots & & \vdots \\ 0 & \dots & 0 \end{pmatrix},$$

und außerdem setzt man

$$- \begin{pmatrix} a_{11} & \dots & a_{1m} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nm} \end{pmatrix} := \begin{pmatrix} -a_{11} & \dots & -a_{1m} \\ \vdots & & \vdots \\ -a_{n1} & \dots & -a_{nm} \end{pmatrix}.$$

Man rechnet nun leicht nach, daß die Regeln V1 – V8 auch in diesem Falle erfüllt sind.

Nun sei M eine beliebige Menge und

$$\mathcal{B}(M, \mathbb{R}) := \{f : M \rightarrow \mathbb{R} \mid \sup\{f(x) : x \in M\} < \infty\}$$

die Menge der beschränkten reellwertigen Funktionen auf M . Zwei Funktionen $f, g \in \mathcal{B}(M, \mathbb{R})$ werden addiert durch

$$(f + g)(x) := f(x) + g(x).$$

Und eine Funktion f wird mit einer reellen Zahl α multipliziert durch

$$(\alpha \cdot f)(x) := \alpha \cdot f(x).$$

Die „Nullfunktion“ ist gegeben durch $0(x) := 0$ für alle $x \in M$. Und mit f liegt auch $-f$ mit $(-f)(x) := -f(x)$ in $\mathcal{B}(M, \mathbb{R})$.

Aus den Rechenregeln für die reellen Zahlen leitet man einfach ab, daß auch für die Elemente von $\mathcal{B}(M, \mathbb{R})$ die Regeln V1 – V8 gelten.

Man kann noch weitere Beispiele für diese Struktur finden:

F sei die Menge aller konvergenten Folgen $(a_n)_{n \in \mathbb{N}}$. Zwei Elemente von F werden in naheliegender Weise addiert:

$$(a_n)_{n \in \mathbb{N}} + (b_n)_{n \in \mathbb{N}} := (a_n + b_n)_{n \in \mathbb{N}}.$$

Die Multiplikation mit $\alpha \in \mathbb{R}$ ist definiert durch

$$\alpha \cdot (a_n)_{n \in \mathbb{N}} := (\alpha \cdot a_n)_{n \in \mathbb{N}}.$$

Die Menge der reellen Polynome

$$p(x) = \sum_{i=0}^n a_i x^i$$

wird mit $\mathbb{R}[x]$ bezeichnet. Wir haben die Addition von Polynomen und die Multiplikation von Polynomen mit reellen Zahlen (also konstanten Polynomen) schon in §5 behandelt. Auch hier sind die Regeln V1 – V8 erfüllt.

Das sollten genug Beispiele sein.

Definition.

Sei K ein Körper (meistens der Körper \mathbb{R}).

Ein K -Vektorraum besteht aus einer (additiv geschriebenen) kommutativen Gruppe V und einer Multiplikation zwischen Elementen von K und Elementen von V , so daß für $x, y \in V$ und $\alpha, \beta \in K$ gilt:

$$\begin{aligned} V5. \quad (\alpha + \beta) \cdot x &= \alpha \cdot x + \beta \cdot x, \\ V6. \quad \alpha \cdot (x + y) &= \alpha \cdot x + \alpha \cdot y, \\ V7. \quad \alpha \cdot (\beta \cdot x) &= (\alpha\beta) \cdot x, \\ V8. \quad 1 \cdot x &= x. \end{aligned}$$

Die Elemente eines Vektorraumes nennt man *Vektoren*.

Ursprünglich verstand man unter einem Vektor einen „Pfeil“ oder eine „gerichtete Größe“. Die Addition erfolgte nach der Parallelogrammregel, die Multiplikation bedeutete eine Streckung. In der modernen linearen Algebra interessiert man sich nur noch für die algebraische Struktur „Vektorraum“. Deshalb kann ein Vektor auch z.B. ein Punkt des \mathbb{R}^n , eine Matrix, eine beschränkte Funktion oder ein Polynom sein.

Bemerkungen :

1. Rechnet man in einem Vektorraum über K (d.h. einem K -Vektorraum), so bezeichnet man die Körperelemente als *Skalare*. Die Skalare werden immer **von links** hermultipliziert!
2. Beim Rechnen in Vektorräumen treten zweierlei Nullen auf. Die Null im Körper K und die Null im Vektorraum V . Es ist

$$0 \cdot x = \mathbf{0} \text{ und } \alpha \cdot \mathbf{0} = \mathbf{0}.$$

I.6.1 Satz. Sei $\alpha \in K$ und $x \in V$. Ist $\alpha \cdot x = \mathbf{0}$, so ist $\alpha = 0$ oder $x = \mathbf{0}$.

BEWEIS: Sei $\alpha \cdot x = \mathbf{0}$. Ist $\alpha = 0$, so ist man fertig. Ist $\alpha \neq 0$, so gibt es in K auch das Inverse α^{-1} , und es gilt:

$$x = 1 \cdot x = (\alpha^{-1}\alpha) \cdot x = \alpha^{-1} \cdot (\alpha \cdot x) = \alpha^{-1} \cdot \mathbf{0} = \mathbf{0}.$$

□

Definition.

Sei V ein K -Vektorraum. Eine Teilmenge $U \subset V$ heißt ein *Untervektorraum* von V , wenn gilt:

1. $0 \in U$.
2. $x, y \in U \implies x + y \in U$.
3. $\alpha \in K, x \in U \implies \alpha \cdot x \in U$.

Ein Untervektorraum ist natürlich selbst wieder ein Vektorraum.

Beispiele :

1. $\{0\}$ ist immer ein Untervektorraum.
2. Sei $v_0 \in V, v_0 \neq 0$. Dann ist die Menge

$$Kv_0 := \{\lambda \cdot v_0 \mid \lambda \in K\}$$

aller „Vielfachen“ von v_0 ein Untervektorraum von V . Der BEWEIS dafür ist ganz einfach:

- (a) $0 = 0 \cdot v_0$.
- (b) Ist $x = \lambda \cdot v_0$ und $y = \mu \cdot v_0$, so ist $x + y = (\lambda + \mu) \cdot v_0$.
- (c) Es ist $\alpha \cdot (\lambda \cdot v_0) = (\alpha\lambda) \cdot v_0$.

Sind $x_1, \dots, x_k \in V$ und $\alpha_1, \dots, \alpha_k \in K$, so nennt man

$$\sum_{i=1}^k \alpha_i \cdot x_i := \alpha_1 \cdot x_1 + \dots + \alpha_k \cdot x_k$$

eine *Linearkombination* der Vektoren x_1, \dots, x_k . Das Ergebnis ist wieder ein Vektor in V .

Definition.

Seien x_1, \dots, x_n fest gewählte Vektoren in V . Dann setzt man

$$K(x_1, \dots, x_n) := \left\{ \sum_{i=1}^n \alpha_i \cdot x_i \mid \alpha_i \in K \text{ für } i = 1, \dots, n \right\}.$$

I.6.2 Satz.

$U := K(x_1, \dots, x_n)$ ist ein Untervektorraum von V .

BEWEIS: 1) $0 = 0 \cdot x_1 + \dots + 0 \cdot x_n$ liegt in U .

$$2) \quad \sum_{i=1}^n \alpha_i \cdot x_i + \sum_{i=1}^n \beta_i \cdot x_i = \sum_{i=1}^n (\alpha_i + \beta_i) x_i.$$

$$3) \quad \lambda \cdot \sum_{i=1}^n \alpha_i x_i = \sum_{i=1}^n (\lambda \alpha_i) x_i. \quad \square$$

Man nennt diesen Raum den von x_1, \dots, x_n aufgespannten Unterraum und bezeichnet ihn auch mit $\langle x_1, \dots, x_n \rangle$ oder $Kx_1 + \dots + Kx_n$.

Man kann diese Konstruktion noch etwas verallgemeinern:

Sei M eine beliebige Teilmenge des K -Vektorraumes V . Dann nennt man

$$\langle M \rangle := \{x \in V \mid \exists n \in \mathbb{N}_0 \text{ und } x_1, \dots, x_n \in M \text{ mit } x \in \langle x_1, \dots, x_n \rangle\}$$

den von M aufgespannten Untervektorraum.⁷ Er besteht aus allen **endlichen** Linearkombinationen von Elementen aus M .

Ein absonderlicher Spezialfall ist $\langle \emptyset \rangle = \{0\}$.

Definition.

Eine Menge $E \subset V$ heißt *Erzeugendensystem* von V , wenn $\langle E \rangle = V$ ist.

Beispiele:

1. Die sogenannten Einheitsvektoren

$$\mathbf{e}_1 := (1, 0, \dots, 0), \mathbf{e}_2 := (0, 1, 0, \dots, 0), \dots, \mathbf{e}_n := (0, \dots, 0, 1)$$

bilden ein (endliches) Erzeugendensystem von \mathbb{R}^n , denn für einen beliebigen Vektor $\mathbf{x} = (x_1, \dots, x_n) \in \mathbb{R}^n$ gilt:

$$\mathbf{x} = x_1 \cdot \mathbf{e}_1 + \dots + x_n \cdot \mathbf{e}_n.$$

Die Koeffizienten x_1, \dots, x_n sind dabei eindeutig bestimmt.

2. Die „Monome“ $1, x, x^2, x^3, \dots$ bilden ein (unendliches) Erzeugendensystem für den Raum $\mathbb{R}[x]$ der Polynome, denn jedes Polynom ist eine endliche Linearkombination solcher Monome:

$$p(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n.$$

Auch hier ist die Darstellung eindeutig bestimmt!

3. In jedem Vektorraum V ist $\langle V \rangle = V$. Von Eindeutigkeit kann in diesem Falle aber keine Rede sein. Im \mathbb{R}^2 ist z.B.

$$(2, 3) = 2 \cdot (1, 0) + 3 \cdot (0, 1) = 2 \cdot (1, 1) + 1 \cdot (0, 1).$$

4. Im Raum $M_{n,m}(\mathbb{R})$ der $(n \times m)$ -Matrizen sei E_{ij} diejenige Matrix, bei der in der i -ten Zeile an der j -ten Stelle eine 1 und sonst überall Nullen stehen. Dann bilden die $n \cdot m$ Matrizen E_{ij} , $i = 1, \dots, n$, $j = 1, \dots, m$, ein Erzeugendensystem von $M_{n,m}(\mathbb{R})$, denn es gilt:

$$\left(a_{ij} \mid \begin{array}{l} i = 1, \dots, n \\ j = 1, \dots, m \end{array} \right) = \sum_{i,j} a_{ij} E_{ij}.$$

5. Wir sind leider i.a. nicht in der Lage, ein einfaches Erzeugendensystem für den Raum $\mathcal{B}(M, \mathbb{R})$ der beschränkten Funktionen auf einer Menge M anzugeben. Ist $M = \{a_1, \dots, a_n\}$ allerdings eine **endliche** Menge, so können wir wie beim \mathbb{R}^n oder dem Raum $M_{n,m}(\mathbb{R})$ vorgehen. Wir definieren $f_i : M \rightarrow \mathbb{R}$ durch

$$f_i(a_j) := \begin{cases} 1 & \text{falls } i = j, \\ 0 & \text{sonst.} \end{cases}$$

⁷Daß es sich um einen Untervektorraum handelt, zeigt man wie oben.

Ist dann $f \in \mathcal{B}(M, \mathbb{R})$ und $\alpha_i := f(a_i)$, für $i = 1, \dots, n$, so ist

$$f = \alpha_1 \cdot f_1 + \dots + \alpha_n \cdot f_n,$$

denn es ist $(\alpha_1 \cdot f_1 + \dots + \alpha_n \cdot f_n)(a_j) = \alpha_1 \cdot f_1(a_j) + \dots + \alpha_n \cdot f_n(a_j) = \alpha_j = f(a_j)$, d.h. f und $\alpha_1 \cdot f_1 + \dots + \alpha_n \cdot f_n$ stimmen auf jedem der endlich vielen Argumente überein.

Wir haben gesehen, daß die Darstellung eines beliebigen Vektors als Linearkombination von Elementen eines Erzeugendensystems i.a. nicht eindeutig ist, daß sie es aber in Spezialfällen sein kann. Um diesen Sachverhalt zu klären, brauchen wir noch zwei Begriffe.

Definition.

Ein System $B = \{v_1, \dots, v_n\}$ von Vektoren eines K -Vektorraumes V heißt *linear unabhängig*, falls gilt:

$$\sum_{i=1}^n \alpha_i v_i = 0 \implies \alpha_1 = \alpha_2 = \dots = \alpha_n = 0.$$

Ist B außerdem noch ein Erzeugendensystem von V , so nennt man B eine *Basis* von V .

Eine unendliche Menge $B \subset V$ heißt linear unabhängig, wenn jede beliebige endliche Auswahl von Elementen von B linear unabhängig ist. B heißt eine (unendliche) Basis, wenn B linear unabhängig und ein Erzeugendensystem ist.

Ein System von Vektoren x_1, \dots, x_n ist also genau dann linear unabhängig, wenn sich der Nullvektor nur auf triviale Weise als Linearkombination der x_i darstellen läßt.

Beispiele :

1. Ist $x \in V$, $x \neq 0$ und $\alpha \cdot x = 0$ für ein $\alpha \in K$, so muß $\alpha = 0$ sein. Daher ist das System $\{x\}$ für jeden Vektor $x \neq 0$ linear unabhängig.
2. Sei $x \in V$, $x \neq 0$ und $y = \lambda \cdot x$ für ein $\lambda \in K$. Dann ist

$$\lambda \cdot x + (-1) \cdot y = 0, \text{ aber } (\lambda, -1) \neq (0, 0).$$

Also sind x und y nicht linear unabhängig. Man nennt sie *linear abhängig*.

3. Sei $\mathbf{x} = (a, b) \in \mathbb{R}^2$ und $\mathbf{y} = (-b, a) \in \mathbb{R}^2$, $(a, b) \neq (0, 0)$. Wir wollen zeigen, daß $\{\mathbf{x}, \mathbf{y}\}$ linear unabhängig ist.

Sei $\alpha \cdot \mathbf{x} + \beta \cdot \mathbf{y} = \mathbf{0}$. Dann ist

$$\begin{aligned} \alpha \cdot a - \beta \cdot b &= 0 \\ \text{und } \alpha \cdot b + \beta \cdot a &= 0. \end{aligned}$$

Ist $a = 0$, so muß $b \neq 0$ sein, und $\alpha b = \beta b = 0$, also $\alpha = \beta = 0$.

Ist $a \neq 0$, so multiplizieren wir die 1. Gleichung mit α und die 2. mit β . Das ergibt:

$$\begin{aligned} \alpha^2 a - \alpha \beta b &= 0 \\ \text{und } \alpha \beta b + \beta^2 a &= 0, \end{aligned}$$

also $(\alpha^2 + \beta^2) \cdot a = 0$. Das geht nur, wenn $\alpha = \beta = 0$ ist.

4. Die Einheitsvektoren $\mathbf{e}_1, \dots, \mathbf{e}_n \in \mathbb{R}^n$ sind linear unabhängig. Ist nämlich

$$\sum_{i=1}^n \alpha_i \mathbf{e}_i = \mathbf{0},$$

so ist $(\alpha_1, \dots, \alpha_n) = (0, \dots, 0)$, also $\alpha_1 = \alpha_2 = \dots = \alpha_n = 0$. Das bedeutet insbesondere, daß $\{\mathbf{e}_1, \dots, \mathbf{e}_n\}$ eine Basis des \mathbb{R}^n ist.

5. Das unendliche System $\{1, x, x^2, x^3, \dots\} \subset \mathbb{R}[x]$ ist linear unabhängig.

Ist nämlich $p := \sum_{i=0}^n \alpha_i x^i$ eine Linearkombination, die Null ergibt, so ist $p(x) \equiv 0$.

Wäre einer der Koeffizienten $\alpha_i \neq 0$, so wäre $\text{grad}(p) \geq 0$, und p könnte nur endlich viele Nullstellen besitzen. Also muß $\alpha_0 = \alpha_1 = \dots = \alpha_n = 0$ sein.

Da $\{1, x, x^2, x^3, \dots\}$ schon ein Erzeugendensystem von $\mathbb{R}[x]$ bildet, liegt hier sogar eine Basis von $\mathbb{R}[x]$ vor.

I.6.3 Satz. *Eine (endliche) Teilmenge $B = \{v_1, \dots, v_n\}$ eines Vektorraumes V ist genau dann eine Basis von V , wenn sich jedes Element von V eindeutig als Linearkombination der v_i schreiben läßt.*

BEWEIS: a) Sei B eine Basis von V , $x \in V$ beliebig vorgegeben. Da B insbesondere ein Erzeugendensystem ist, läßt sich x als Linearkombination der v_i schreiben. Gibt es zwei Darstellungen

$$x = \sum_{i=1}^n \alpha_i \cdot v_i = \sum_{i=1}^n \beta_i \cdot v_i,$$

so ist

$$0 = \sum_{i=1}^n (\alpha_i - \beta_i) \cdot v_i.$$

Da B linear unabhängig ist, muß $\alpha_i = \beta_i$ sein, für $i = 1, \dots, n$.

b) Ist umgekehrt jedes $x \in V$ eindeutig als Linearkombination der v_i darstellbar, so ist B offensichtlich ein Erzeugendensystem. Und da insbesondere auch der Nullvektor eindeutig darstellbar ist, muß B auch linear unabhängig sein. \square

Häufig steht man vor einer Aufgabe von folgendem Typ:

Sei $U := \{(x_1, x_2, x_3) \in \mathbb{R}^3 \mid x_1 + x_2 + x_3 = 0\}$. Ist U ein Untervektorraum? Wenn ja, bestimme man eine Basis von U .

Die Lösung ist bei diesem einfachen Beispiel nicht schwer. Offensichtlich ist $\mathbf{0} \in U$, und mit $\mathbf{x}, \mathbf{y} \in U$ und $\alpha \in \mathbb{R}$ ist auch $\mathbf{x} + \mathbf{y} \in U$ und $\alpha \cdot \mathbf{x} \in U$. Ist nämlich z.B. $\mathbf{x} = (x_1, x_2, x_3) \in U$, so ist $x_1 + x_2 + x_3 = 0$ und $\alpha \cdot \mathbf{x} = (\alpha x_1, \alpha x_2, \alpha x_3)$, mit $\alpha x_1 + \alpha x_2 + \alpha x_3 = \alpha(x_1 + x_2 + x_3) = 0$, also $\alpha \cdot \mathbf{x} \in U$. Analog behandelt man $\mathbf{x} + \mathbf{y}$.

Nun soll eine Basis von U gesucht werden. Zwischen den Koordinaten eines Vektors $\mathbf{x} \in U$ besteht die Gleichung $x_3 = -x_1 - x_2$. Es liegt nahe, für (x_1, x_2) versuchsweise einmal $(1, 0)$

und einmal $(0, 1)$ zu wählen. Die Komponente x_3 ist dann jeweils schon festgelegt. Das führt zu den beiden Vektoren

$$\mathbf{a}_1 := (1, 0, -1) \quad \text{und} \quad \mathbf{a}_2 := (0, 1, -1).$$

Eine allgemeine Linearkombination dieser beiden Vektoren hat die Gestalt

$$\alpha \cdot \mathbf{a}_1 + \beta \cdot \mathbf{a}_2 = (\alpha, \beta, -\alpha - \beta).$$

Da jedes Element von U diese Gestalt hat, ist $B := \{\mathbf{a}_1, \mathbf{a}_2\}$ ein Erzeugendensystem von U . Und B ist linear unabhängig, denn die obige Linearkombination ergibt genau dann den Nullvektor, wenn $\alpha = \beta = 0$ ist. Also ist B eine Basis.

Daß das geklappt hat, war nicht selbstverständlich. Wir wissen ja noch nicht einmal, ob überhaupt jeder Vektorraum eine Basis besitzt. Mit dieser Fragestellung wollen wir uns jetzt beschäftigen.

Da immer $V = \langle V \rangle$ ist, besitzt jeder Vektorraum ein Erzeugendensystem. Wir nennen ein Erzeugendensystem $E \subset V$ *verkürzbar*, wenn es eine Menge $E' \subsetneq E$ gibt, die auch noch ein Erzeugendensystem von V ist. Es gibt dann sicherlich ein $v \in E \setminus E'$ und Elemente $v_1, \dots, v_n \in E'$, so daß

$$v = \alpha_1 \cdot v_1 + \dots + \alpha_n \cdot v_n$$

ist. Aber dann ist

$$0 = \alpha_1 \cdot v_1 + \dots + \alpha_n \cdot v_n + (-1) \cdot v,$$

also $\{v_1, \dots, v_n, v\}$ und damit erst recht E linear abhängig.

I.6.4 Satz. *Ein Erzeugendensystem ist genau dann verkürzbar, wenn es linear abhängig ist.*

BEWEIS: Die eine Richtung haben wir gerade bewiesen. Ist umgekehrt E linear abhängig, so gibt es Vektoren $v_1, \dots, v_k \in E$ und $\alpha_1, \dots, \alpha_k \in K$ mit

$$\sum_{i=1}^k \alpha_i v_i = 0 \quad \text{und} \quad (\alpha_1, \dots, \alpha_k) \neq (0, \dots, 0).$$

Ist etwa $\alpha_k \neq 0$, so ist

$$v_k = \sum_{i=1}^{k-1} \left(-\frac{\alpha_i}{\alpha_k}\right) v_i.$$

Aber das bedeutet, daß v_k überflüssig ist, E ist verkürzbar. □

Die Strategie bei der Suche nach einer Basis wird daher so aussehen, daß wir mit einem beliebigen Erzeugendensystem beginnen und so lange überflüssige Elemente weglassen, bis das verbliebene System unverkürzbar ist. Dieses System muß dann linear unabhängig sein, also eine Basis.

Leider läßt sich dieses Verfahren bei unendlichen Erzeugendensystemen nicht so ohne weiteres durchführen. Wir setzen daher fortan voraus, daß der betrachtete Vektorraum *endlich erzeugt* ist, also ein endliches Erzeugendensystem besitzt.

I.6.5 Satz. Sei $V \neq \{0\}$ ein endlich erzeugter K -Vektorraum.

Jedes endliche Erzeugendensystem von V enthält eine Basis.

BEWEIS: Sei $E = \{v_1, \dots, v_n\}$ ein Erzeugendensystem des Vektorraumes V . Ist E schon eine Basis, sind wir fertig. Andernfalls ist einer der Vektoren in E von den anderen linear abhängig und läßt sich als Linearkombination der übrigen Vektoren schreiben. Also ist er überflüssig. Nun können wir ihn weglassen und wieder die obigen Überlegungen anstellen. Nach endlich vielen Schritten erhalten wir ein unverkürzbares endliches Erzeugendensystem, in dem keiner der Vektoren mehr von den anderen linear abhängig sein kann. Das muß eine Basis sein. \square

Demnach besitzt jeder endlich erzeugte Vektorraum eine Basis. Die Auswahl der Basis aus einem Erzeugendensystem erfolgt aber arg zufällig, und es ist denkbar, daß nicht einmal die Anzahl der Elemente einer solchen Basis feststeht. Um eine bessere Kontrolle über das Verfahren zu gewinnen, versuchen wir nun, linear unabhängige Systeme zu Basen zu erweitern.

I.6.6 Austausch-Lemma. Sei $B = \{v_1, \dots, v_n\}$ eine Basis von V , $0 \leq k < n$ und $w \in V$ irgendein Vektor, so daß v_1, \dots, v_k, w linear unabhängig sind.

Dann kann man w so gegen ein Element $v_i \in \{v_{k+1}, \dots, v_n\}$ austauschen, daß $B^* := (B \setminus \{v_i\}) \cup \{w\}$ wieder eine Basis ist.

BEWEIS: Es gibt eine Darstellung $w = \sum_{i=1}^n \lambda_i v_i$.

Wäre $\lambda_{k+1} = \dots = \lambda_n = 0$, so wäre w von v_1, \dots, v_k linear abhängig, im Widerspruch zur Voraussetzung. O.B.d.A. sei $\lambda_n \neq 0$. Dann ist

$$v_n = \frac{1}{\lambda_n} \left(w - \sum_{i=1}^{n-1} \lambda_i v_i \right),$$

also $\{v_1, \dots, v_{n-1}, w\}$ ein Erzeugendensystem von V .

Sei nun $\sum_{i=1}^{n-1} \alpha_i v_i + \beta w = 0$. Dann ist

$$\sum_{i=1}^{n-1} (\alpha_i + \beta \lambda_i) v_i + \beta \lambda_n v_n = 0.$$

Daraus folgt:

$$\begin{aligned} \alpha_i + \beta \lambda_i &= 0 \quad \text{für } i = 1, \dots, n-1 \\ \text{und } \beta \lambda_n &= 0. \end{aligned}$$

Wie man sieht, muß $\beta = 0$ und $\alpha_i = 0$ für $i = 1, \dots, n-1$ sein. Also ist $\{v_1, \dots, v_{n-1}, w\}$ linear unabhängig und damit tatsächlich eine Basis. \square

Das Austausch-Lemma ist nur Hilfsmittel für den

I.6.7 Austauschatz. Sei $\{v_1, \dots, v_n\}$ eine Basis von V und $\{w_1, \dots, w_r\}$ ein System linear unabhängiger Vektoren von V .

Dann ist $r \leq n$, und nach geeigneter Numerierung ist $\{w_1, \dots, w_r, v_{r+1}, \dots, v_n\}$ wieder eine Basis von V .

Hier ist zunächst die Beweisidee:

1. Schritt: Wir wenden das Austausch-Lemma auf die Basis $\{v_1, \dots, v_n\}$ und den Vektor $w = w_1 \neq 0$ an, mit $k = 0$. Nach geeigneter Numerierung ist $\{w_1, v_2, \dots, v_n\}$ wieder eine Basis.

2. Schritt: Nun wenden wir das Austausch-Lemma auf die neue Basis und den Vektor $w = w_2$ an. Da $\{w_1, w_2\}$ linear unabhängig ist, ist $k = 1$, und nach geeigneter Numerierung ist $\{w_1, w_2, v_3, \dots, v_n\}$ eine Basis.

So fährt man fort, bis alle w_i ausgetauscht sind. Wäre $r > n$, so wäre schon $\{w_1, \dots, w_n\}$ eine Basis und w_{n+1} von diesen Vektoren linear abhängig. Das kann nicht sein.

Und hier ist nun ein komprimierter

BEWEIS: Wir führen Induktion nach r .

Als **Induktionsanfang** wählen wir $r = 0$. Da ist nichts zu zeigen.

Beim **Induktionsschluß** nehmen wir an, der Satz sei für $r - 1$ schon bewiesen. Dann ist $r \geq 1$, $r - 1 \leq n$ und – nach geeigneter Numerierung – $\{w_1, \dots, w_{r-1}, v_r, \dots, v_n\}$ eine Basis.

Wäre $r - 1 = n$, so wäre $\{w_1, \dots, w_{r-1}\}$ schon eine Basis, und w_r müßte linear abhängig von w_1, \dots, w_{r-1} sein. Das kommt nicht in Frage. Also ist $r - 1 < n$ und damit $r \leq n$. Nach dem Austausch-Lemma kann man w_r gegen eins der Elemente v_r, \dots, v_n austauschen und erhält wieder eine Basis. O.B.d.A. ist v_r das auszutauschende Element. Dann ist $\{w_1, \dots, w_r, v_{r+1}, \dots, v_n\}$ eine Basis. \square

Setzt man alles zusammen, so erhält man den

I.6.8 Basisergänzungssatz.

Sei $E \subset V$ ein endliches Erzeugendensystem von V und $L \subset E$ linear unabhängig. Dann gibt es eine Basis B von V mit $L \subset B \subset E$.

BEWEIS: Es gibt eine Basis $B_0 \subset E$ von V . Nach dem Austauschatz ist $\#L \leq \#B_0$, und man kann L gegen eine Teilmenge $B'_0 \subset B_0$ austauschen, so daß $B := L \cup (B_0 \setminus B'_0)$ wieder eine Basis ist. Nun ist aber $L \subset B \subset E$. \square

Die Anzahl der Elemente eines endlichen Systems von Vektoren von V nennen wir auch die *Länge* des Systems. Sei nun n_e die kleinste auftretende Länge eines Erzeugendensystems und n_u die größte auftretende Länge eines linear unabhängigen Systems in V . Dann gilt für jede Basis B von V :

$$n_e \leq \#(B) \leq n_u.$$

Wir wollen zeigen, daß sogar Gleichheit gilt.

Ist E irgendein Erzeugendensystem und L ein linear unabhängiges System, so ist $\#(L) \leq$

$\#(E)$. Bei festem E gilt das für jedes L , also ist auch $n_u \leq \#(E)$. Und da diese Ungleichung für beliebiges E gilt, ist sogar $n_u \leq n_e$. Damit ist alles gezeigt. \square

Definition.

Ist V ein endlich erzeugter Vektorraum, so nennt man die Zahl $\dim(V)$ der Elemente einer Basis von V die *Dimension* von V .

Ist V nicht endlich erzeugt, so setzt man $\dim(V) := \infty$.

Beispiele :

1. $\dim(\mathbb{R}^n) = n$, denn $\{\mathbf{e}_1, \dots, \mathbf{e}_n\}$ ist eine Basis.
2. $\dim(M_{n,m}(\mathbb{R})) = n \cdot m$, denn die Matrizen E_{ij} bilden eine Basis.
3. $\dim(\mathbb{R}[x]) = \infty$.
4. Ist $\mathbf{v} \in \mathbb{R}^n$, $\mathbf{v} \neq \mathbf{0}$, so ist $\mathbb{R} \cdot \mathbf{v}$ ein 1-dimensionaler \mathbb{R} -Vektorraum, eine sogenannte *Gerade*.
5. Sind $\mathbf{v}_1, \mathbf{v}_2$ zwei linear unabhängige Vektoren des \mathbb{R}^n , so ist $\langle \mathbf{v}_1, \mathbf{v}_2 \rangle = \mathbb{R}(\mathbf{v}_1, \mathbf{v}_2)$ ein 2-dimensionaler \mathbb{R} -Vektorraum, eine *Ebene*.

Die in den Beispielen betrachteten Geraden und Ebenen enthalten immer den Nullpunkt, wie es sich für Untervektorräume gehört. Etwas allgemeiner definiert man:

Definition.

Sei $U \subset \mathbb{R}^n$ ein k -dimensionaler Untervektorraum und $\mathbf{x}_0 \in \mathbb{R}^n$ irgend ein Vektor. Dann nennt man die Menge

$$A = \mathbf{x}_0 + U := \{\mathbf{x} = \mathbf{x}_0 + \mathbf{v} \mid \mathbf{v} \in U\}$$

einen k -dimensionalen *affinen Unterraum* des \mathbb{R}^n .

Im Falle $k = 1$ spricht man von affinen Geraden, im Falle $k = 2$ von affinen Ebenen.

Achtung! Ein affiner Unterraum ist i.a. kein Vektorraum!!!

Etwas ist noch nachzutragen:

I.6.9 Satz. *Jeder Untervektorraum eines endlich erzeugten Vektorraumes ist selbst wieder endlich erzeugt, besitzt also eine Basis.*

BEWEIS: Sei V endlich erzeugt, $U \subset V$ ein Untervektorraum. Jedes linear unabhängige System in U ist auch linear unabhängig in V , muß also $\leq \dim(V)$ Elemente enthalten.

Wir nehmen nun an, U sei nicht endlich erzeugt. v_1, \dots, v_k seien linear unabhängige Elemente. Wäre jeder andere Vektor $w \in U$ von diesen k Vektoren linear abhängig, so wäre $\{v_1, \dots, v_k\}$ bereits ein Erzeugendensystem von U . Da wir das ausgeschlossen haben, muß es wenigstens einen Vektor $v_{k+1} \in U$ geben, so daß auch $\{v_1, \dots, v_k, v_{k+1}\}$

linear unabhängig ist. Dieses Argument kann man so oft wiederholen, bis man mehr als $\dim(V)$ linear unabhängige Vektoren gefunden hat. Widerspruch! \square

Völlig offen ist die Frage geblieben, ob auch unendlich-dimensionale Vektorräume Basen besitzen. Tatsächlich gilt:

I.6.10 Satz. *Jeder Vektorraum besitzt eine Basis.*

Dieser reine Existenzsatz benutzt das sogenannte „Auswahlaxiom“ aus der Mengenlehre. Wir werden ihn hier nicht beweisen.

Wir wollen uns nun noch etwas näher mit der Geometrie des \mathbb{R}^n befassen.

Definition.

Sind $\mathbf{x} = (x_1, \dots, x_n)$, $\mathbf{y} = (y_1, \dots, y_n)$ zwei Vektoren im \mathbb{R}^n , so bezeichnet man die reelle Zahl

$$\mathbf{x} \bullet \mathbf{y} := \sum_{i=1}^n x_i y_i$$

als das (*euklidische*) *Skalarprodukt* von \mathbf{x} und \mathbf{y} .

Für $n = 1$ ist dies das gewöhnliche Produkt reeller Zahlen.

I.6.11 Satz.

1. $\mathbf{x} \bullet \mathbf{y} = \mathbf{y} \bullet \mathbf{x}$.
2. $(\mathbf{x}_1 + \mathbf{x}_2) \bullet \mathbf{y} = \mathbf{x}_1 \bullet \mathbf{y} + \mathbf{x}_2 \bullet \mathbf{y}$.
3. $(\alpha \cdot \mathbf{x}) \bullet \mathbf{y} = \alpha \cdot (\mathbf{x} \bullet \mathbf{y}) = \mathbf{x} \bullet (\alpha \cdot \mathbf{y})$.
4. $\mathbf{x} \bullet \mathbf{x} \geq 0$, und $\mathbf{x} \bullet \mathbf{x} = 0 \iff \mathbf{x} = \mathbf{0}$.

Die BEWEISE sind simpel. Zu Eigenschaft (4): $\mathbf{x} \bullet \mathbf{x} = \sum_{i=1}^n (x_i)^2$ ist offensichtlich ≥ 0 , und $= 0$ genau dann, wenn $x_1 = \dots = x_n = 0$ ist.

Definition.

Die Zahl $\|\mathbf{x}\| := \sqrt{\mathbf{x} \bullet \mathbf{x}} = \sqrt{(x_1)^2 + \dots + (x_n)^2}$ heißt (*euklidische*) *Norm* von \mathbf{x} .

Anschaulich ist die euklidische Norm des Vektors \mathbf{x} seine Länge, also der Abstand des durch \mathbf{x} gegebenen Punktes vom Ursprung.

I.6.12 Satz.

1. *Es ist stets* $\|\mathbf{x}\| \geq 0$, und $\|\mathbf{x}\| = 0 \iff \mathbf{x} = \mathbf{0}$.
2. $\|\alpha \cdot \mathbf{x}\| = |\alpha| \cdot \|\mathbf{x}\|$ für $\alpha \in \mathbb{R}$ und $\mathbf{x} \in \mathbb{R}^n$.
3. *Es gilt die „Scharzsche Ungleichung“:*

$$|\mathbf{x} \bullet \mathbf{y}| \leq \|\mathbf{x}\| \cdot \|\mathbf{y}\|.$$

Gleichheit gilt genau dann, wenn \mathbf{x} und \mathbf{y} linear abhängig sind.

4. Es gilt die „Dreiecks-Ungleichung“:

$$\|\mathbf{x} + \mathbf{y}\| \leq \|\mathbf{x}\| + \|\mathbf{y}\|.$$

BEWEIS: (1) und (2) sind trivial.

(3) Wir setzen $A := \|\mathbf{x}\|^2$, $B := \|\mathbf{y}\|^2$ und $C := \mathbf{x} \bullet \mathbf{y}$. Dann ist zu zeigen: $C^2 \leq AB$.

Ist $B = 0$, so ist $\mathbf{y} = \mathbf{0}$ und beide Seiten verschwinden.

Sei also $B > 0$. Dann verwenden wir einen Trick:

$$\begin{aligned} 0 &\leq \sum_{i=1}^n (Bx_i - Cy_i)^2 \\ &= B^2A - 2BC \cdot C + C^2B \\ &= B^2A - C^2B = B(AB - C^2). \end{aligned}$$

Dann muß $AB - C^2 \geq 0$ sein. Und Gleichheit gilt genau dann, wenn $B\mathbf{x} - C\mathbf{y} = \mathbf{0}$ ist.

(4) Es ist

$$\begin{aligned} \|\mathbf{x} + \mathbf{y}\|^2 &= \sum_{i=1}^n (x_i + y_i)^2 \\ &= \|\mathbf{x}\|^2 + \|\mathbf{y}\|^2 + 2\mathbf{x} \bullet \mathbf{y} \\ &\leq \|\mathbf{x}\|^2 + \|\mathbf{y}\|^2 + 2|\mathbf{x} \bullet \mathbf{y}| \\ &\leq \|\mathbf{x}\|^2 + \|\mathbf{y}\|^2 + 2\|\mathbf{x}\| \cdot \|\mathbf{y}\| \\ &= (\|\mathbf{x}\| + \|\mathbf{y}\|)^2. \end{aligned}$$

□

Definition.

$d(\mathbf{x}, \mathbf{y}) := \|\mathbf{x} - \mathbf{y}\|$ heißt *Abstand* oder *Distanz* von \mathbf{x} und \mathbf{y} .

Speziell ist dann $\|\mathbf{x}\| = d(\mathbf{x}, \mathbf{0})$.

Die Distanz hat folgende Eigenschaften:

I.6.13 Satz.

1. Es ist stets $d(\mathbf{x}, \mathbf{y}) \geq 0$, und $d(\mathbf{x}, \mathbf{y}) = 0 \iff \mathbf{x} = \mathbf{y}$.
2. $d(\mathbf{x}, \mathbf{y}) = d(\mathbf{y}, \mathbf{x})$.
3. Es gilt die Dreiecks-Ungleichung:

$$d(\mathbf{x}, \mathbf{y}) \leq d(\mathbf{x}, \mathbf{z}) + d(\mathbf{z}, \mathbf{y}).$$

BEWEIS: (Nur zu (3)): Es ist

$$\begin{aligned}\|\mathbf{x} - \mathbf{y}\| &= \|(\mathbf{x} - \mathbf{z}) + (\mathbf{z} - \mathbf{y})\| \\ &\leq \|\mathbf{x} - \mathbf{z}\| + \|\mathbf{z} - \mathbf{y}\|.\end{aligned}$$

□

Man kann die Begriffe „Skalarprodukt“, „Norm“ und „Distanz“ verallgemeinern.

Definition.

Sei V ein beliebiger Vektorraum über dem Körper der reellen Zahlen. Ein *Skalarprodukt* auf V ist eine Abbildung, die jedem Paar (v, w) von Vektoren aus V eine reelle Zahl $\langle v, w \rangle$ zuordnet, so daß gilt:

1. $\langle \dots, \dots \rangle$ ist bilinear, d.h.
 - (a) $\langle \alpha \cdot v, w \rangle = \langle v, \alpha \cdot w \rangle = \alpha \cdot \langle v, w \rangle$.
 - (b) $\langle v_1 + v_2, w \rangle = \langle v_1, w \rangle + \langle v_2, w \rangle$ und $\langle v, w_1 + w_2 \rangle = \langle v, w_1 \rangle + \langle v, w_2 \rangle$.
2. $\langle \dots, \dots \rangle$ ist symmetrisch, d.h. $\langle v, w \rangle = \langle w, v \rangle$.
3. $\langle \dots, \dots \rangle$ ist positiv definit, d.h. $\langle v, v \rangle$ ist reell und > 0 für $v \neq 0$.

„bilinear“ heißt „linear in beiden Argumenten“. Wegen der Symmetrie bräuchte man allerdings nur die Linearität im 1. Argument zu fordern.

Durch $\langle (x_1, x_2), (y_1, y_2) \rangle := 2x_1y_1 + 3x_2y_2$ wird z.B. ein Skalarprodukt auf dem \mathbb{R}^2 definiert, das nicht mit dem euklidischen Skalarprodukt übereinstimmt.

Definition.

Sei V ein beliebiger \mathbb{R} -Vektorraum. Eine *Norm* auf V ist eine Abbildung $N : V \rightarrow \mathbb{R}$ mit folgenden Eigenschaften:

1. $N(v) \geq 0$ und $N(v) = 0 \iff v = 0$.
2. $N(\alpha \cdot v) = |\alpha| \cdot N(v)$.
3. $N(v + w) \leq N(v) + N(w)$.

Ist auf V ein Skalarprodukt $\langle \cdot, \cdot \rangle$ gegeben, so erhält man eine Norm auf V durch

$$N(v) := \sqrt{\langle v, v \rangle}.$$

Es gibt aber auch Normen, die nicht von einem Skalarprodukt kommen, z.B. die „Maximums-Norm“ auf dem \mathbb{R}^n :

$$|\mathbf{x}| := \max\{|x_i| : i = 1, \dots, n\}.$$

Auf dem Raum $\mathcal{B}(M, \mathbb{R})$ haben wir die „Supremums-Norm“, mit

$$\|f\| := \sup\{|f(x)| : x \in M\}.$$

Auch sie kommt nicht von einem Skalarprodukt.

Definition.

Sei X eine beliebige Menge. Eine Abbildung $d : X \times X \rightarrow \mathbb{R}$ nennt man eine *Metrik* oder *Distanz* auf X , wenn gilt:

1. $d(x, y) \geq 0$, und $d(x, y) = 0 \iff x = y$.
2. $d(x, y) = d(y, x)$.
3. $d(x, y) \leq d(x, z) + d(z, y)$.

(X, d) nennt man dann einen *metrischen Raum*.

Ist V ein reeller Vektorraum mit einer Norm $N : V \rightarrow \mathbb{R}$, so hat man auf V auch eine Metrik, durch

$$d(v, w) := N(v - w).$$

Es gibt aber auch Metriken, die nicht von einer Norm herrühren. Und der Raum braucht noch nicht mal ein Vektorraum zu sein. Es ist z.B. jedes offene Intervall $I = (a, b) \subset \mathbb{R}$ mit $d(x, y) := |x - y|$ ein metrischer Raum, aber kein Vektorraum.

In einem Vektorraum mit Skalarprodukt kann man auch Winkel einführen. Wir demonstrieren das hier nur im \mathbb{R}^n und nur für das euklidische Skalarprodukt.

Sind $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n \setminus \{\mathbf{0}\}$, so ist $\left| \frac{\mathbf{x} \bullet \mathbf{y}}{\|\mathbf{x}\| \cdot \|\mathbf{y}\|} \right| \leq 1$. (Schwarzsche Ungleichung)

Aber zu jedem $t \in \mathbb{R}$ mit $|t| \leq 1$ gibt es genau ein $\varphi \in [0, \pi]$ mit $\cos(\varphi) = t$.

Definition.

Für Vektoren $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$ mit $\mathbf{x} \neq \mathbf{0}$ und $\mathbf{y} \neq \mathbf{0}$ wird der *Winkel* $\angle(\mathbf{x}, \mathbf{y})$ definiert durch

$$\angle(\mathbf{x}, \mathbf{y}) := \arccos \frac{\mathbf{x} \bullet \mathbf{y}}{\|\mathbf{x}\| \cdot \|\mathbf{y}\|} \in [0, \pi].$$

Ist $\mathbf{y} = \lambda \cdot \mathbf{x}$ mit $\lambda > 0$, so ist $\angle(\mathbf{x}, \mathbf{y}) = 0$. Ist $\mathbf{y} = -\mathbf{x}$, so ist $\angle(\mathbf{x}, \mathbf{y}) = \pi$. Schließlich ist

$$\angle(\mathbf{x}, \mathbf{y}) = \frac{\pi}{2} \iff \mathbf{x} \bullet \mathbf{y} = 0.$$

Definition.

Die Vektoren \mathbf{x} und \mathbf{y} heißen *orthogonal* (oder *senkrecht*) zueinander (in Zeichen: $\mathbf{x} \perp \mathbf{y}$), wenn $\mathbf{x} \bullet \mathbf{y} = 0$ ist.

Man beachte: Ein Skalarprodukt kann verschwinden, obwohl keiner der Faktoren verschwindet. Im \mathbb{R}^2 ist z.B. $(1, 2) \bullet (-2, 1) = 0$.

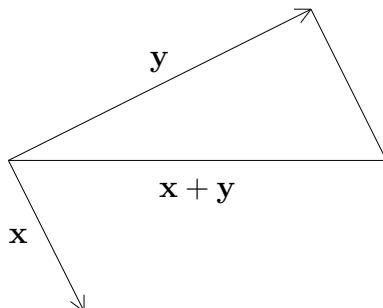
I.6.14 Satz des Pythagoras. *Ist $\mathbf{x} \perp \mathbf{y}$, so ist*

$$\|\mathbf{x} + \mathbf{y}\|^2 = \|\mathbf{x}\|^2 + \|\mathbf{y}\|^2.$$

BEWEIS: Es ist

$$\|\mathbf{x} + \mathbf{y}\|^2 = (\mathbf{x} + \mathbf{y}) \cdot (\mathbf{x} + \mathbf{y}) = \|\mathbf{x}\|^2 + 2\mathbf{x} \cdot \mathbf{y} + \|\mathbf{y}\|^2.$$

Stehen die Vektoren aufeinander senkrecht, so folgt die Behauptung. □



§7 Lineare Abbildungen

Definition.

Es seien V und W zwei (gleiche oder verschiedene) K -Vektorräume.

Eine Abbildung $F : V \rightarrow W$ heißt K -linear (oder kurz *linear*, wenn klar ist, um welchen Körper es sich handelt), falls für alle $u, v \in V$ und $\alpha \in K$ gilt:

1. $f(u + v) = f(u) + f(v)$.
2. $f(\alpha \cdot v) = \alpha \cdot f(v)$.

Bemerkung : Ist f linear, so ist auf jeden Fall $f(0) = 0$.

BEWEIS dafür: Es ist $f(0) = f(0 + 0) = f(0) + f(0)$. Subtrahiert man nun auf beiden Seiten der Gleichung $f(0)$, so erhält man $0 = f(0)$.

Beispiele :

1. Sei $f : \mathbb{R} \rightarrow \mathbb{R}$ eine lineare Funktion, also eine proportionale Zuordnung $x \mapsto mx$, mit einem Proportionalitätsfaktor $m \neq 0$. Dann gilt:

$$(a) \quad f(x + y) = m(x + y) = mx + my = f(x) + f(y).$$

$$(b) \quad f(\alpha \cdot x) = m(\alpha x) = (m\alpha)x = (\alpha m)x = \alpha \cdot (mx) = \alpha \cdot f(x).$$

Also ist eine lineare Funktion auch eine lineare Abbildung zwischen Vektorräumen.

Ist f affin-linear, also $f(x) = mx + t$, und ist $t \neq 0$, so ist f nicht linear, denn es ist z.B. $f(2 \cdot x) = m \cdot (2x) + t = 2 \cdot (mx) + 2t - t = 2 \cdot f(x) - t$.

2. Die Funktion $g : x \mapsto x^2$ ist nicht linear, denn es ist

$$g(x + y) = (x + y)^2 = x^2 + y^2 + 2xy = g(x) + g(y) + 2xy.$$

3. Die Verallgemeinerung des Begriffs der linearen Funktion auf den Fall mehrerer Veränderlicher sieht folgendermaßen aus:

$$f : \mathbb{R}^n \rightarrow \mathbb{R} \text{ mit } f(x_1, \dots, x_n) := m_1 x_1 + \dots + m_n x_n.$$

Wir können das etwas kürzer schreiben. Setzen wir $\mathbf{m} := (m_1, \dots, m_n)$, so ist

$$f(\mathbf{x}) = \mathbf{m} \bullet \mathbf{x}.$$

Dadurch wird auch die Analogie zum 1-dimensionalen Fall deutlicher, und der Linearitätsbeweis ist ganz einfach:

$$(a) \quad f(\mathbf{x} + \mathbf{y}) = \mathbf{m} \bullet (\mathbf{x} + \mathbf{y}) = \mathbf{m} \bullet \mathbf{x} + \mathbf{m} \bullet \mathbf{y} = f(\mathbf{x}) + f(\mathbf{y}).$$

$$(b) \quad f(\alpha \cdot \mathbf{x}) = \mathbf{m} \bullet (\alpha \cdot \mathbf{x}) = \alpha \cdot (\mathbf{m} \bullet \mathbf{x}) = \alpha \cdot f(\mathbf{x}).$$

Definition.

Sei V ein beliebiger K -Vektorraum. Eine lineare Abbildung $f : V \rightarrow K$ nennt man eine *Linearform* auf V .

Beispiele :

1. Die Abbildung $\mathbf{x} \mapsto \mathbf{m} \bullet \mathbf{x}$ ist eine Linearform auf dem \mathbb{R}^n .
2. Sei $V := \mathcal{B}(M, \mathbb{R})$. Für jedes Element $x \in M$ wird die „Auswertungsfunktion“ e_x durch

$$e_x(f) := f(x)$$

definiert. Das ist eine Linearform $e_x : V \rightarrow \mathbb{R}$:

$$(a) \quad e_x(f + g) = (f + g)(x) = f(x) + g(x) = e_x(f) + e_x(g).$$

$$(b) \quad e_x(\alpha \cdot f) = (\alpha \cdot f)(x) = \alpha \cdot f(x) = \alpha \cdot e_x(f).$$

3. Sei $V = M_{n,n}(\mathbb{R})$ der Raum der $(n \times n)$ -Matrizen. Für eine Matrix $A \in M_{n,n}(\mathbb{R})$ wird die *Spur* von A definiert durch

$$A = \left(a_{ij} \mid \begin{array}{l} i = 1, \dots, n \\ j = 1, \dots, n \end{array} \right) \mapsto \text{Spur}(A) := \sum_{i=1}^n a_{ii}. \quad (\text{Summe der Diagonalelemente})$$

Dann ist $\text{Spur} : M_{n,n}(\mathbb{R}) \rightarrow \mathbb{R}$ eine Linearform.

I.7.1 Satz. *Ist $f : \mathbb{R}^n \rightarrow \mathbb{R}$ eine Linearform, so gibt es einen (eindeutig bestimmten) Vektor $\mathbf{m} \in \mathbb{R}^n$, so daß $f(\mathbf{x}) = \mathbf{m} \bullet \mathbf{x}$ ist.*

BEWEIS: $\{\mathbf{e}_1, \dots, \mathbf{e}_n\}$ sei die Standardbasis des \mathbb{R}^n . Ist f eine Linearform auf dem \mathbb{R}^n , so setzen wir $m_i := f(\mathbf{e}_i)$ für $i = 1, \dots, n$, und $\mathbf{m} := (m_1, \dots, m_n)$.

Für einen beliebigen Vektor $\mathbf{x} \in \mathbb{R}^n$ haben wir die Darstellung

$$\mathbf{x} = x_1 \cdot \mathbf{e}_1 + \dots + x_n \cdot \mathbf{e}_n.$$

Also ist

$$\begin{aligned} f(\mathbf{x}) &= f(x_1 \cdot \mathbf{e}_1 + \dots + x_n \cdot \mathbf{e}_n) \\ &= x_1 \cdot f(\mathbf{e}_1) + \dots + x_n \cdot f(\mathbf{e}_n) \\ &= x_1 \cdot m_1 + \dots + x_n \cdot m_n \\ &= \mathbf{m} \bullet \mathbf{x}. \end{aligned}$$

Gibt es nun zwei Vektoren \mathbf{m} und \mathbf{m}^* , so daß

$$f(\mathbf{x}) = \mathbf{m} \bullet \mathbf{x} = \mathbf{m}^* \bullet \mathbf{x} \quad \text{für alle } \mathbf{x} \text{ ist,}$$

so gilt für die Komponenten:

$$m_i = \mathbf{m} \bullet \mathbf{e}_i = \mathbf{m}^* \bullet \mathbf{e}_i = m_i^*, \quad \text{für } i = 1, \dots, n.$$

□

I.7.2 Satz. Sind $f : V \rightarrow W$ und $g : W \rightarrow L$ lineare Abbildungen zwischen K -Vektorräumen, so ist auch $g \circ f : V \rightarrow L$ eine K -lineare Abbildung.

Den simplen BEWEIS überlasse ich dem Leser.

Ist K ein beliebiger Körper, so bildet $K^n := K \times \dots \times K$ einen K -Vektorraum (mit komponentenweiser Addition und skalarer Multiplikation). Auch hier gibt es Einheitsvektoren $\mathbf{e}_1, \dots, \mathbf{e}_n$, und die Einheitsvektoren bilden eine Basis.

Für jedes i definiert die „Projektion“ $\text{pr}_i : K^n \rightarrow K$ mit $\text{pr}_i(x_1, \dots, x_n) := x_i$ eine Linearform auf K^n . Ist nun $f : K^n \rightarrow K^k$ eine lineare Abbildung, so setzt man $f_i := \text{pr}_i \circ f$. Dann ist f_i für jedes i eine Linearform, und man kann schreiben:

$$f = (f_1, \dots, f_k).$$

I.7.3 Folgerung. Eine Abbildung $f : \mathbb{R}^n \rightarrow \mathbb{R}^k$ ist genau dann linear, wenn es Vektoren $\mathbf{a}_1, \dots, \mathbf{a}_k \in \mathbb{R}^n$ gibt, so daß für jedes $\mathbf{x} \in \mathbb{R}^n$ gilt:

$$f(\mathbf{x}) = (\mathbf{a}_1 \bullet \mathbf{x}, \dots, \mathbf{a}_k \bullet \mathbf{x}).$$

Die Vektoren $\mathbf{a}_1, \dots, \mathbf{a}_k$ sind dabei eindeutig bestimmt.

Definition.

Sei $f : V \rightarrow W$ eine lineare Abbildung zwischen K -Vektorräumen. Dann heißt

$$\begin{array}{ll} \text{Im}(f) & := \{w \in W \mid \exists v \in V \text{ mit } f(v) = w\} \quad \text{das Bild von } f \\ \text{und } \text{Ker}(f) & := \{v \in V \mid f(v) = 0\} \quad \text{der Kern von } f. \end{array}$$

I.7.4 Satz. Ist $f : V \rightarrow W$ linear, so sind $\text{Im}(f) \subset W$ und $\text{Ker}(f) \subset V$ jeweils Untervektorräume.

BEWEIS: Für jede lineare Abbildung gilt: $f(0) = 0$. Also liegt die Null sowohl in $\text{Im}(f)$ als auch in $\text{Ker}(f)$.

1) Sind $u, v \in \text{Ker}(f)$, so ist $f(u+v) = f(u) + f(v) = 0 + 0 = 0$ und $f(\alpha \cdot v) = \alpha \cdot f(v) = \alpha \cdot 0 = 0$. Also liegen auch $u+v$ und $\alpha \cdot v$ in $\text{Ker}(f)$.

2) Sind $w_1, w_2 \in \text{Im}(f)$, so gibt es Elemente $v_1, v_2 \in V$ mit $f(v_1) = w_1$ und $f(v_2) = w_2$. Dann ist $w_1 + w_2 = f(v_1) + f(v_2) = f(v_1 + v_2) \in \text{Im}(f)$ und $\alpha \cdot w_1 = \alpha \cdot f(v_1) = f(\alpha \cdot v_1) \in \text{Im}(f)$. \square

I.7.5 Satz. Sei $f : V \rightarrow W$ linear.

1. f ist genau dann surjektiv, wenn $\text{Im}(f) = W$ ist.
2. f ist genau dann injektiv, wenn $\text{Ker}(f) = \{0\}$ ist.

BEWEIS: 1) ist trivial.

2) a) Sei f injektiv. Ist $v \in \text{Ker}(f)$, so ist $f(v) = 0 = f(0)$, also $v = 0$.

b) Sei umgekehrt $\text{Ker}(f) = \{0\}$. Ist $f(v_1) = f(v_2)$, so ist $f(v_1 - v_2) = 0$, also $v_1 - v_2 \in \text{Ker}(f)$, d.h. $v_1 - v_2 = 0$ und damit $v_1 = v_2$. \square

Beispiele :

1. $f : \mathbb{R}^2 \rightarrow \mathbb{R}$ mit $f(x_1, x_2) := x_1 - x_2 = (1, -1) \bullet (x_1, x_2)$ ist eine Linearform. Da $f(x, 0) = x$ ist, ist f surjektiv, also $\text{Im}(f) = \mathbb{R}$.

Weiter ist $\text{Ker}(f) = \{(x_1, x_2) \mid x_1 - x_2 = 0\} = \{(x, x) \mid x \in \mathbb{R}\}$. Da dies nicht der Nullraum ist, ist f auch nicht injektiv. Tatsächlich ist z.B. $f(3, 2) = f(5, 4)$.

2. Auch $e_x : \mathcal{B}(M, \mathbb{R}) \rightarrow \mathbb{R}$ mit $e_x(f) := f(x)$ ist eine Linearform. Es ist $\text{Im}(e_x) = \mathbb{R}$, denn die konstanten Funktionen liefern schon alle reellen Zahlen als Werte.

Es ist $\text{Ker}(e_x) = \{f \in \mathcal{B}(M, \mathbb{R}) \mid f(x) = 0\}$ die Menge all derjenigen Funktionen, die in x eine Nullstelle besitzen.

3. Sei $f : \mathbb{R}^2 \rightarrow \mathbb{R}^3$ definiert durch

$$f(x_1, x_2) := (x_1 - x_2, x_1 + x_2, 3x_1 + 2x_2).$$

Nun gilt:

$$(x_1, x_2) \in \text{Ker}(f) \iff x_1 - x_2 = 0, x_1 + x_2 = 0 \text{ und } 3x_1 + 2x_2 = 0.$$

Aber das ist genau dann der Fall, wenn $x_1 = x_2 = 0$ ist. Also ist $\text{Ker}(f) = \{0\}$ und f injektiv.

Nun wollen wir das Bild bestimmen. Offensichtlich liegen die Vektoren

$$\mathbf{a}_1 := f(1, 0) = (1, 1, 3) \text{ und } \mathbf{a}_2 := f(0, 1) = (-1, 1, 2)$$

in $\text{Im}(f)$, und sie sind linear unabhängig:

Ist nämlich $\lambda \cdot \mathbf{a}_1 + \mu \cdot \mathbf{a}_2 = \mathbf{0}$, so ist $f(\lambda, \mu) = f(\lambda \cdot (1, 0) + \mu \cdot (0, 1)) = \lambda \cdot f(1, 0) + \mu \cdot f(0, 1) = \mathbf{0}$, also $(\lambda, \mu) \in \text{Ker}(f)$, d.h. $\lambda = \mu = 0$.

Ist nun \mathbf{w} ein beliebiges Element von $\text{Im}(f)$, so gibt es ein $\mathbf{v} = (v_1, v_2) \in \mathbb{R}^2$ mit $\mathbf{w} = f(\mathbf{v}) = f(v_1 \cdot (1, 0) + v_2 \cdot (0, 1)) = v_1 \cdot \mathbf{a}_1 + v_2 \cdot \mathbf{a}_2$.

Also ist $\text{Im}(f) = \langle \mathbf{a}_1, \mathbf{a}_2 \rangle$, und $\{\mathbf{a}_1, \mathbf{a}_2\}$ sogar eine Basis von $\text{Im}(f)$. Insbesondere ist f nicht surjektiv.

Die Ideen aus dem letzten Beispiel lassen sich verallgemeinern.

I.7.6 Satz. Sei $f : \mathbb{R}^n \rightarrow \mathbb{R}^m$ linear. Dann gibt es eine Basis $\{\mathbf{a}_1, \dots, \mathbf{a}_n\}$ des \mathbb{R}^n und ein k mit $0 \leq k \leq n$, so daß gilt:

1. $\{\mathbf{a}_1, \dots, \mathbf{a}_k\}$ ist eine Basis von $\text{Ker}(f)$.
2. $\{f(\mathbf{a}_{k+1}), \dots, f(\mathbf{a}_n)\}$ ist eine Basis von $\text{Im}(f)$.

BEWEIS: Als Untervektorraum des \mathbb{R}^n besitzt $\text{Ker}(f)$ eine Basis $B = \{\mathbf{a}_1, \dots, \mathbf{a}_k\}$. Da B auch im \mathbb{R}^n linear unabhängig ist, kann man B nach dem Austauschsatz gegen Elemente der Standardbasis austauschen, d.h., es gibt Vektoren $\mathbf{a}_{k+1}, \dots, \mathbf{a}_n \in \{\mathbf{e}_1, \dots, \mathbf{e}_n\}$, so daß $\{\mathbf{a}_1, \dots, \mathbf{a}_k, \mathbf{a}_{k+1}, \dots, \mathbf{a}_n\}$ eine Basis des \mathbb{R}^n ist.

Ist $\mathbf{y} = f(\mathbf{x}) \in \text{Im}(f)$, so gibt es eine Darstellung $\mathbf{x} = \sum_{i=1}^n \alpha_i \mathbf{a}_i$. Da $f(\mathbf{a}_i) = \mathbf{0}$ für $i = 1, \dots, k$ ist, folgt:

$$\mathbf{y} = \sum_{i=k+1}^n \alpha_i f(\mathbf{a}_i).$$

Also ist $\{f(\mathbf{a}_{k+1}), \dots, f(\mathbf{a}_n)\}$ ein Erzeugendensystem von $\text{Im}(f)$.

Sei nun $\sum_{i=k+1}^n \lambda_i f(\mathbf{a}_i) = \mathbf{0}$. Dann ist

$$f\left(\sum_{i=k+1}^n \lambda_i \mathbf{a}_i\right) = \mathbf{0}, \text{ also } \sum_{i=k+1}^n \lambda_i \mathbf{a}_i \in \text{Ker}(f).$$

Aber dann gibt es Koeffizienten $\lambda_1, \dots, \lambda_k$, so daß gilt:

$$\sum_{i=k+1}^n \lambda_i \mathbf{a}_i = \sum_{i=1}^k \lambda_i \mathbf{a}_i, \text{ also } \sum_{i=1}^k \lambda_i \mathbf{a}_i + \sum_{i=k+1}^n (-\lambda_i) \mathbf{a}_i = \mathbf{0}.$$

Das ist nur möglich, wenn alle λ_i verschwinden. Also ist $\{f(\mathbf{a}_{k+1}), \dots, f(\mathbf{a}_n)\}$ sogar eine Basis von $\text{Im}(f)$. \square

I.7.7 Folgerung 1 (Dimensions-Formel). Sei $f : \mathbb{R}^n \rightarrow \mathbb{R}^m$ linear. Dann gilt:

$$\dim(\text{Ker}(f)) + \dim(\text{Im}(f)) = n.$$

I.7.8 Folgerung 2. Sei $f : \mathbb{R}^n \rightarrow \mathbb{R}^m$ linear und injektiv, $\{\mathbf{a}_1, \dots, \mathbf{a}_n\}$ eine Basis des \mathbb{R}^n .

Dann ist $\{f(\mathbf{a}_1), \dots, f(\mathbf{a}_n)\}$ eine Basis von $\text{Im}(f)$.

I.7.9 Folgerung 3. Sei f eine lineare Abbildung des \mathbb{R}^n auf sich. Dann sind folgende Aussagen äquivalent:

1. f ist injektiv.
2. f ist surjektiv.
3. f ist bijektiv.

BEWEIS: Soll die Äquivalenz mehrerer Aussagen gezeigt werden, so tut man dies üblicherweise mit Hilfe eines „Zirkel-Schlusses“:

$$(1) \implies (2) \implies (3) \implies (1)$$

Darin sind alle gewünschten Äquivalenzen enthalten.

(1) \implies (2) : Ist f injektiv, so ist $\dim(\text{Ker}(f)) = 0$, also $\dim(\text{Im}(f)) = n$, also $\text{Im}(f) = \mathbb{R}^n$ und f surjektiv.

(2) \implies (3) : Ist f surjektiv, so ist $\dim(\text{Im}(f)) = n$, also $\text{Ker}(f) = \{0\}$ und f damit injektiv, also sogar bijektiv.

(3) \implies (1) : Trivial! □

Definition.

Eine bijektive lineare Abbildung $f : V \rightarrow W$ nennt man einen *Isomorphismus*. Die Räume V und W heißen dann *isomorph* (in Zeichen $V \cong W$).

I.7.10 Satz. Ist $f : V \rightarrow W$ ein Isomorphismus, so ist auch $f^{-1} : W \rightarrow V$ linear.

BEWEIS: Seien $\mathbf{w}_1, \mathbf{w}_2 \in W$, $\alpha \in K$. Dann gilt:

$$\exists \mathbf{v}_1, \mathbf{v}_2 \in V \text{ mit } f(\mathbf{v}_1) = \mathbf{w}_1 \text{ und } f(\mathbf{v}_2) = \mathbf{w}_2.$$

Also ist

$$\begin{aligned} f^{-1}(\mathbf{w}_1 + \mathbf{w}_2) &= f^{-1}(f(\mathbf{v}_1) + f(\mathbf{v}_2)) \\ &= f^{-1}(f(\mathbf{v}_1 + \mathbf{v}_2)) \\ &= \mathbf{v}_1 + \mathbf{v}_2 \\ &= f^{-1}(\mathbf{w}_1) + f^{-1}(\mathbf{w}_2), \end{aligned}$$

und

$$\begin{aligned} f^{-1}(\alpha \cdot \mathbf{w}_1) &= f^{-1}(\alpha \cdot f(\mathbf{v}_1)) \\ &= f^{-1}(f(\alpha \cdot \mathbf{v}_1)) \\ &= \alpha \cdot \mathbf{v}_1 \\ &= \alpha \cdot f^{-1}(\mathbf{w}_1). \end{aligned}$$

□

Wir wollen jetzt den Zusammenhang zwischen linearen Abbildungen und Matrizen herstellen.

Die Menge $L(\mathbb{R}^n, \mathbb{R}^k)$ der linearen Abbildungen von \mathbb{R}^n nach \mathbb{R}^k ist selbst wieder ein Vektorraum. Die Verknüpfungen erklärt man analog zu denen auf dem Raum der reellwertigen (beschränkten) Funktionen.⁸

$$\begin{aligned} (f + g)(\mathbf{x}) &:= f(\mathbf{x}) + g(\mathbf{x}) \\ \text{und } (\alpha \cdot f)(\mathbf{x}) &:= \alpha \cdot (f(\mathbf{x})). \end{aligned}$$

⁸Natürlich sind die linearen Abbildungen i.a. nicht beschränkt. Aber wir hatten im Falle des Raumes $\mathcal{B}(M, \mathbb{R})$ die Beschränktheit der Funktionen auch nicht bei der Einführung der Vektorraumstruktur, sondern erst später bei der Einführung einer Norm gebraucht.

Allerdings muß man noch nachprüfen, daß die neu gebildeten Abbildungen $f + g$ und $\alpha \cdot f$ wieder linear sind. Aber das sind zwei einfache Rechnungen, die wir hier nicht ausführen.

Ist nun eine Matrix $A \in M_{k,n}(\mathbb{R})$ gegeben, so kann man die k Zeilen von A (mit jeweils n Einträgen) als Vektoren $\mathbf{a}_1, \dots, \mathbf{a}_k$ auffassen und eine lineare Abbildung $f_A : \mathbb{R}^n \rightarrow \mathbb{R}^k$ definieren, durch

$$f_A(\mathbf{x}) := (\mathbf{a}_1 \bullet \mathbf{x}, \dots, \mathbf{a}_k \bullet \mathbf{x}).$$

Somit wird jeder Matrix $A \in M_{k,n}(\mathbb{R})$ auf eindeutige Weise eine lineare Abbildung $f_A : \mathbb{R}^n \rightarrow \mathbb{R}^k$ zugeordnet. Das ergibt eine Abbildung Φ von $M_{k,n}(\mathbb{R})$ nach $L(\mathbb{R}^n, \mathbb{R}^k)$. Und diese Abbildung ist bijektiv, denn wir können sofort die Umkehrabbildung angeben:

Ist $f \in L(\mathbb{R}^n, \mathbb{R}^k)$ beliebig vorgegeben, so sind durch die Linearformen $f_i := \text{pr}_i \circ f : \mathbb{R}^n \rightarrow \mathbb{R}$ auf eindeutige Weise Vektoren \mathbf{a}_i mit $f_i(\mathbf{x}) = \mathbf{a}_i \bullet \mathbf{x}$ festgelegt, für $i = 1, \dots, k$. Faßt man diese k Vektoren zu einer Matrix $M(f) \in M_{k,n}(\mathbb{R})$ zusammen, so ist $f_{M(f)} = f$ und $M(f_A) = A$, also durch $f \mapsto M(f)$ die Umkehrabbildung Φ^{-1} gegeben.

Man kann übrigens diese Beziehung zwischen Matrizen und linearen Abbildungen auf Vektorräume vom Typ K^n und sogar auf beliebige endlich-dimensionale Vektorräume übertragen. Allerdings muß man dabei den Gebrauch des Skalarproduktes umgehen. Das werden wir an späterer Stelle tun.

Wir wollen nun zeigen, daß die Abbildung $\Phi : M_{k,n}(\mathbb{R}) \rightarrow L(\mathbb{R}^n, \mathbb{R}^k)$ mit $\Phi(A) := f_A$ sogar linear ist:

Wird A aus den Zeilen $\mathbf{a}_1, \dots, \mathbf{a}_k$ und B aus den Zeilen $\mathbf{b}_1, \dots, \mathbf{b}_k$ gebildet, so wird $A + B$ aus den Zeilen $\mathbf{a}_1 + \mathbf{b}_1, \dots, \mathbf{a}_k + \mathbf{b}_k$ und $\alpha \cdot A$ aus den Zeilen $\alpha \cdot \mathbf{a}_1, \dots, \alpha \cdot \mathbf{a}_k$ gebildet. Daraus folgt:

$$\begin{aligned} f_{A+B}(\mathbf{x}) &= ((\mathbf{a}_1 + \mathbf{b}_1) \bullet \mathbf{x}, \dots, (\mathbf{a}_k + \mathbf{b}_k) \bullet \mathbf{x}) \\ &= (\mathbf{a}_1 \bullet \mathbf{x} + \mathbf{b}_1 \bullet \mathbf{x}, \dots, \mathbf{a}_k \bullet \mathbf{x} + \mathbf{b}_k \bullet \mathbf{x}) \\ &= (\mathbf{a}_1 \bullet \mathbf{x}, \dots, \mathbf{a}_k \bullet \mathbf{x}) + (\mathbf{b}_1 \bullet \mathbf{x}, \dots, \mathbf{b}_k \bullet \mathbf{x}) \\ &= f_A(\mathbf{x}) + f_B(\mathbf{x}) = (f_A + f_B)(\mathbf{x}). \end{aligned}$$

Also ist $\Phi(A + B) = \Phi(A) + \Phi(B)$.

Genauso sieht man:

$$\begin{aligned} f_{\alpha \cdot A}(\mathbf{x}) &= ((\alpha \cdot \mathbf{a}_1) \bullet \mathbf{x}, \dots, (\alpha \cdot \mathbf{a}_k) \bullet \mathbf{x}) \\ &= \alpha \cdot (\mathbf{a}_1 \bullet \mathbf{x}, \dots, \mathbf{a}_k \bullet \mathbf{x}) \\ &= \alpha \cdot f_A(\mathbf{x}) \\ &= (\alpha \cdot f_A)(\mathbf{x}). \end{aligned}$$

Also ist auch $\Phi(\alpha \cdot A) = \alpha \cdot \Phi(A)$.

Damit ist Φ sogar ein Isomorphismus von \mathbb{R} -Vektorräumen. Zwischen Matrizen und linearen Abbildungen besteht – was die Struktur als Vektorraum angeht – kein wesentlicher Unterschied.

Als nächstes ordnen wir auch jedem Vektor $\mathbf{x} \in \mathbb{R}^n$ eine Matrix $M(\mathbf{x}) \in M_{n,1}(\mathbb{R})$ zu,

nämlich die Spalte

$$M((x_1, \dots, x_n)) := \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}.$$

Ist $\mathbf{x} \in \mathbb{R}^n$ und $f \in L(\mathbb{R}^n, \mathbb{R}^k)$, so definiert man das Matrizenprodukt $M(f) \circ M(\mathbf{x}) \in M_{k,1}(\mathbb{R})$ durch

$$\boxed{M(f) \circ M(\mathbf{x}) := M(f(\mathbf{x}))}.$$

Dann folgt:

$$\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{k1} & \cdots & a_{kn} \end{pmatrix} \circ \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} a_{11}x_1 + \cdots + a_{1n}x_n \\ \vdots \\ a_{k1}x_1 + \cdots + a_{kn}x_n \end{pmatrix}.$$

Zur Bezeichnung von Spaltenvektoren benutzen wir an Stelle des Symbols $M(\mathbf{x})$ gelegentlich auch das Symbol \vec{x} . Ist $A \in M_{k,n}(\mathbb{R})$, so sind z.B. die n Spaltenvektoren

$$A \circ \vec{e}_i = M(f_A(\mathbf{e}_i)) \in \mathbb{R}^k$$

gerade die n Spalten der Matrix A .

Wir können jetzt auch ein Produkt für beliebige Matrizen einführen:

Definition.

Ist $A \in M_{m,n}(\mathbb{R})$ und $B \in M_{n,l}(\mathbb{R})$, so ist $A \circ B \in M_{m,l}(\mathbb{R})$ definiert durch

$$\boxed{A \circ B := M(f_A \circ f_B)}.$$

In Worten: Das Produkt der Matrizen A und B ist die Matrix, die zur Verknüpfung der linearen Abbildungen f_A und f_B gehört.

Aus der Definition ergibt sich, daß das Matrizenprodukt nur in gewissen Fällen gebildet werden kann. Man kann $A \circ B$ genau dann bilden, wenn der Definitionsbereich von f_A mit dem Wertebereich von f_B übereinstimmt. Bei Abbildungen $f_A : \mathbb{R}^n \rightarrow \mathbb{R}^m$ und $f_B : \mathbb{R}^l \rightarrow \mathbb{R}^n$ ist die Bedingung erfüllt, dann ist $f_{A \circ B} = f_A \circ f_B : \mathbb{R}^l \rightarrow \mathbb{R}^m$ definiert.

Wir wollen nun untersuchen, wie man die Koeffizienten c_{ik} von $A \circ B$ aus den Koeffizienten a_{ij} von A und b_{jk} von B berechnen kann. Es ist

$$\begin{aligned} (A \circ B) \circ M(\mathbf{e}_k) &= M(f_A \circ f_B) \circ M(\mathbf{e}_k) \\ &= M((f_A \circ f_B)(\mathbf{e}_k)) \\ &= M(f_A(f_B(\mathbf{e}_k))) \\ &= A \circ (B \circ M(\mathbf{e}_k)) \\ &= \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} \circ \begin{pmatrix} b_{1k} \\ \vdots \\ b_{nk} \end{pmatrix} = \begin{pmatrix} a_{11}b_{1k} + \cdots + a_{1n}b_{nk} \\ \vdots \\ a_{m1}b_{1k} + \cdots + a_{mn}b_{nk} \end{pmatrix}. \end{aligned}$$

Also ist

$$c_{ik} = \sum_{j=1}^n a_{ij}b_{jk}.$$

Das bedeutet:

Das Element in der i -ten Zeile und k -ten Spalte von $A \circ B$ erhält man, indem man die i -te Zeile von A auf die k -te Spalte von B legt, die dann übereinander liegenden Elemente multipliziert und schließlich alle Produkte aufsummiert.

$$\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ \boxed{a_{i1} \quad \cdots \quad a_{in}} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} \circ \begin{pmatrix} b_{11} & \cdots & \boxed{b_{1k}} & \cdots & b_{1l} \\ \vdots & & \vdots & & \vdots \\ b_{n1} & \cdots & \boxed{b_{nk}} & \cdots & b_{nl} \end{pmatrix} = \begin{pmatrix} \vdots & & & & \\ \cdots & \boxed{\sum_{j=1}^n a_{ij} b_{jk}} & \cdots & & \\ \vdots & & & & \end{pmatrix} \leftarrow i$$

$\uparrow k$

Auch hier sieht man, daß die Anzahl der Spalten von A mit der Anzahl der Zeilen von B übereinstimmen muß.

Es folgen nun einige Rechenregeln für das Matrizenprodukt:

I.7.11 Satz.

Seien $A, A' \in M_{n,m}(\mathbb{R})$, $B, B' \in M_{m,l}(\mathbb{R})$ und $C \in M_{l,r}(\mathbb{R})$. Dann gilt:

1. $A \circ (B \circ C) = (A \circ B) \circ C$.
2. $A \circ (B + B') = A \circ B + A \circ B'$.
3. $(A + A') \circ B = A \circ B + A' \circ B$.
4. $\alpha \cdot (A \circ B) = (\alpha A) \circ B = A \circ (\alpha B)$ für $\alpha \in \mathbb{R}$.

Der BEWEIS erfolgt durch Nachrechnen, die Aussagen ergeben sich leicht aus den entsprechenden Eigenschaften der zugehörigen linearen Abbildungen.

Achtung!! Im allgemeinen ist $A \circ B \neq B \circ A$!!!

Hier ist ein einfaches Beispiel:

$$\begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 0 \\ 2 & 2 \end{pmatrix} = \begin{pmatrix} 1 \cdot 1 + 1 \cdot 2 & 1 \cdot 0 + 1 \cdot 2 \\ 0 \cdot 1 + 2 \cdot 2 & 0 \cdot 0 + 2 \cdot 2 \end{pmatrix} = \begin{pmatrix} 3 & 2 \\ 4 & 4 \end{pmatrix},$$

aber

$$\begin{pmatrix} 1 & 0 \\ 2 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 1 \cdot 1 + 0 \cdot 0 & 1 \cdot 1 + 0 \cdot 2 \\ 2 \cdot 1 + 2 \cdot 0 & 2 \cdot 1 + 2 \cdot 2 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 2 & 6 \end{pmatrix}.$$

Es gibt noch mehr seltsame Effekte: z.B. kann ein Matrizenprodukt die Null ergeben, auch wenn keiner der beiden Faktoren Null ist:

$$\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \circ \begin{pmatrix} 0 & 0 \\ 2 & 3 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Das bedeutet, daß man bei Matrizengleichungen i.a. nicht kürzen kann: Wenn $X \circ A = X \circ B$ ist, mit $X \neq 0$, so muß keineswegs $A = B$ gelten!

§8 Komplexe Zahlen

Die Gleichung $x^2 + 1 = 0$ hat in \mathbb{R} keine Lösung. Nun hatte aber z.B. auch die Gleichung $x^2 - 2 = 0$ in \mathbb{Q} keine Lösung, und dieses Problem konnte dadurch beseitigt werden, daß man die Lösung in dem größeren Zahlenbereich \mathbb{R} gefunden hat.

Also stellt sich die Frage: Gibt es einen größeren Zahlenbereich als \mathbb{R} , in dem vielleicht die Gleichung $x^2 + 1 = 0$ lösbar ist? Oder genauer: Gibt es einen Körper K mit folgenden Eigenschaften:

1. $\mathbb{R} \subset K$.
2. Die algebraischen Verknüpfungen $+$ und \cdot und ihre Gesetzmäßigkeiten werden von \mathbb{R} auf K fortgesetzt.
3. Es gibt ein Element $\mathbf{j} \in K$ mit $\mathbf{j}^2 = -1$.

Auf den ersten Blick erscheint das ziemlich unsinnig. Aber nimmt man die Existenz von K trotzdem einmal an, so erhält man (für $a, b, c, d \in \mathbb{R}$) folgende Regeln:

$$\begin{aligned} (a + b\mathbf{j}) + (c + d\mathbf{j}) &= (a + c) + (b + d)\mathbf{j}, \\ \text{und } (a + b\mathbf{j}) \cdot (c + d\mathbf{j}) &= (ac - bd) + (ad + bc)\mathbf{j}. \end{aligned}$$

Was sagt uns das? Wenn es den gewünschten Körper K gibt, und wenn jedes Element von K in der Form $a + b\mathbf{j}$ mit $a, b \in \mathbb{R}$ dargestellt werden kann, so wissen wir schon, wie wir zwei Elemente von K addieren und multiplizieren müssen. Aber dann sieht es so aus, als müßten wir die Elemente von K in einem 2-dimensionalen Vektorraum suchen, also in einer Ebene. Und auch dafür hat schon jemand eine Erklärung gefunden: Wenn die Multiplikation mit -1 (in \mathbb{R}) eine Drehung um 180° bedeutet und wenn $\mathbf{j}^2 = -1$ ist, so sollte die Multiplikation mit \mathbf{j} eine Drehung um 90° bedeuten. Das zwingt uns aus der Zahlengerade hinaus in die Ebene.

Jetzt haben wir genug Motivation für die folgende

Definition.

Unter der Menge der *komplexen Zahlen* versteht man die Ebene \mathbb{R}^2 , auf der neben der vektoriellen Addition zusätzlich eine Multiplikation gegeben ist:

$$(a, b) \cdot (c, d) := (ac - bd, ad + bc).$$

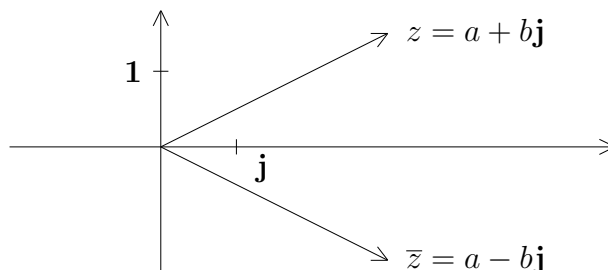
Das Element $(1, 0)$ wird mit $\mathbf{1}$ bezeichnet, das Element $(0, 1)$ mit \mathbf{j} .

Die Menge der komplexen Zahlen wird auch mit dem Symbol \mathbb{C} bezeichnet. Jedes Element $z \in \mathbb{C}$ kann auf eindeutige Weise in der Form $z = a + b\mathbf{j}$ geschrieben werden, mit $a, b \in \mathbb{R}$. Man nennt dann $\operatorname{Re}(z) := a$ den *Realteil* und $\operatorname{Im}(z) := b$ den *Imaginärteil* von z .

Die reellen Zahlen bilden eine Teilmenge der komplexen Zahlen (nämlich genau diejenigen komplexen Zahlen, deren Imaginärteil $= 0$ ist). Wir wissen aus der Vektorrechnung schon, daß $(\mathbb{C}, +, 0)$ eine kommutative Gruppe ist. Die 1 ist sicher ein neutrales Element für die

Multiplikation. Assoziativität und Kommutativität der Multiplikation kann man – mit genügend Geduld – nachrechnen, genauso das Distributivgesetz. Nun müssen wir noch das Reziproke zu einer komplexen Zahl $z \neq 0$ finden. Eine direkte Herleitung ist etwas mühsam, deshalb verwenden wir einen einfachen Trick:

Ist $z = a + b\mathbf{j} \in \mathbb{C}$, so nennt man $\bar{z} := a - b\mathbf{j}$ die zu z *konjugierte komplexe Zahl*.



Es gilt:

$$1. \quad \overline{z + w} = \bar{z} + \bar{w}.$$

$$\begin{aligned} \overline{(a + b\mathbf{j}) + (c + d\mathbf{j})} &= \overline{(a + c) + (b + d)\mathbf{j}} = (a + c) - (b + d)\mathbf{j} \\ &= (a - b\mathbf{j}) + (c - d\mathbf{j}) = \overline{a + b\mathbf{j}} + \overline{c + d\mathbf{j}}. \end{aligned}$$

$$2. \quad \overline{z \cdot w} = \bar{z} \cdot \bar{w}.$$

$$\begin{aligned} \overline{(a + b\mathbf{j}) \cdot (c + d\mathbf{j})} &= \overline{(ac - bd) + (ad + bc)\mathbf{j}} = (ac - bd) - (ad + bc)\mathbf{j} \\ \text{und} \\ \overline{(a + b\mathbf{j})} \cdot \overline{(c + d\mathbf{j})} &= (a - b\mathbf{j}) \cdot (c - d\mathbf{j}) = (ac - bd) - (ad + bc)\mathbf{j}. \end{aligned}$$

$$3. \quad \bar{\bar{z}} = z.$$

$$4. \quad \text{Ist } z = a + b\mathbf{j}, \text{ so ist } z \cdot \bar{z} = (a + b\mathbf{j}) \cdot (a - b\mathbf{j}) = a^2 + b^2 \geq 0.$$

Ist $z \neq 0$, so ist sogar $z \cdot \bar{z} > 0$.

5. Realteil und Imaginärteil einer komplexen Zahl sind gegeben durch

$$\operatorname{Re}(z) = \frac{1}{2}(z + \bar{z}) \quad \text{und} \quad \operatorname{Im}(z) = \frac{1}{2\mathbf{j}}(z - \bar{z}).$$

Die reelle Zahl $|z| := +\sqrt{z\bar{z}} \geq 0$ nennt man den *Betrag* der komplexen Zahl z . Ist $z = a + b\mathbf{j}$, so ist

$$|z| = \sqrt{a^2 + b^2} = \|(a, b)\|$$

die euklidische Norm und besitzt deshalb auch die gleichen Eigenschaften.

Ist nun $z \neq 0$, so ist $z\bar{z} = |z|^2 > 0$, und es gilt:

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

Also ist

$$z^{-1} = \frac{\bar{z}}{|z|^2}, \quad \text{für } z \neq 0.$$

Also ist \mathbb{C} ein Körper. Allerdings kann \mathbb{C} nicht wie \mathbb{R} angeordnet werden, denn wenn es eine Anordnung auf \mathbb{C} gäbe, dann müßte $1 \cdot 1 = 1$ und $\mathbf{j} \cdot \mathbf{j} = -1$ positiv sein, also auch $0 = 1 + (-1)$. Aber das widerspricht den Regeln einer Anordnung.

Definition.

Sei $I \subset \mathbb{R}$ ein Intervall. Eine Abbildung $f : I \rightarrow \mathbb{C}$ wird auch als *komplexwertige Funktion* bezeichnet.

Sie kann immer in der Form $f = g + \mathbf{j}h$ in Realteil und Imaginärteil zerlegt werden. g und h sind dabei gewöhnliche reelle Funktionen. Man nennt dann f z.B. stetig, wenn g und h es sind.

Ein wichtiges Beispiel einer solchen komplexwertigen Funktion wollen wir sogleich einführen:

Ist $z = a + \mathbf{j}b$ eine komplexe Zahl mit $|z| = 1$, so ist $a^2 + b^2 = 1$ und es gibt eine eindeutig bestimmte Zahl $t \in [0, 2\pi)$ mit

$$\cos(t) = a \text{ und } \sin(t) = b.$$

Für beliebige komplexe Zahlen $z \neq 0$ erhält man dementsprechend eine Darstellung

$$z = |z| \cdot (\cos t + \mathbf{j} \sin t).$$

Das ist die sogenannte „Polarkoordinaten-Darstellung“ von z . Die Zahl $\arg(z) := t$ nennt man das *Argument* von z . Erlaubt man, daß t beliebig in \mathbb{R} gewählt wird, so ist das Argument nur bis auf 2π eindeutig bestimmt. Für $z = 0$ kann man überhaupt keinen Winkel ermitteln, deswegen haben wir diesen Fall ausgeschlossen.

Nun folgt eine auf den ersten Blick befremdliche Definition:

Definition.

Für $t \in \mathbb{R}$ sei $e^{\mathbf{j}t} := \cos(t) + \mathbf{j} \sin(t)$.

Die Rechtfertigung liefert der folgende Satz:

I.8.1 Satz.

1. $e^{\mathbf{j} \cdot 0} = 1$.
2. $e^{\mathbf{j}(t+s)} = e^{\mathbf{j}t} \cdot e^{\mathbf{j}s}$.

BEWEIS: 1) $\cos(0) = 1$ und $\sin(0) = 0$.

2) Mit dem Additionstheorem erhält man:

$$\begin{aligned} \cos(t+s) + \mathbf{j} \sin(t+s) &= \\ &= \cos(t) \cos(s) - \sin(t) \sin(s) + \mathbf{j} [\sin(t) \cos(s) + \cos(t) \sin(s)] \\ &= [\cos(t) + \mathbf{j} \sin(t)] \cdot [\cos(s) + \mathbf{j} \sin(s)]. \end{aligned}$$

□

Bemerkung : Die Beziehung

$$e^{\mathbf{j}t} = \cos(t) + \mathbf{j} \sin(t)$$

wird als *Eulersche Formel* bezeichnet.

Das Rechnen mit Winkelfunktionen wird auf diese Weise stark vereinfacht. Z.B. gilt:

I.8.2 Moivre'sche Formel.

$$(\cos t + \mathbf{j} \sin t)^n = \cos(nt) + \mathbf{j} \sin(nt).$$

BEWEIS:

$$(e^{\mathbf{j}t})^n = e^{\mathbf{j}nt}.$$

□

Interessant ist auch die folgende „Weltformel“:

$$e^{\mathbf{j}\pi} + 1 = 0.$$

Sie verbindet die wichtigsten Konstanten der Mathematik miteinander: 0, 1, \mathbf{j} , π und e . Der Beweis ist simpel: Es ist $\cos(\pi) = -1$ und $\sin(\pi) = 0$.

Nun versuchen wir, Wurzeln aus komplexen Zahlen zu ziehen.

I.8.3 Satz. Die Gleichung $z^n = 1$ hat in \mathbb{C} genau n Lösungen, nämlich

$$\zeta_{k,n} := e^{\frac{k}{n} \cdot 2\pi \mathbf{j}}, \quad k = 0, 1, \dots, n-1.$$

BEWEIS: Die Punkte $\zeta_{k,n} = \cos(k \cdot \frac{2\pi}{n}) + \mathbf{j} \sin(k \cdot \frac{2\pi}{n})$, $k = 0, 1, \dots, n-1$, liegen auf den Ecken eines (dem Einheitskreis einbeschriebenen) regelmäßigen n -Ecks. Insbesondere sind sie alle verschieden.

Da $e^{k \cdot 2\pi \mathbf{j}} = \cos(k \cdot 2\pi) + \mathbf{j} \sin(k \cdot 2\pi) = 1$ ist, ist

$$(\zeta_{k,n})^n = e^{k \cdot 2\pi \mathbf{j}} = 1 \text{ für } k = 0, 1, \dots, n-1.$$

Sei umgekehrt $w \in \mathbb{C}$ irgendeine Lösung der Gleichung $z^n = 1$. Dann ist $|w|^n = |w^n| = 1$, also $|w| = 1$, also $w = e^{\mathbf{j}t}$ für ein geeignetes $t \in [0, 2\pi)$. Da außerdem $e^{\mathbf{j}tn} = w^n = 1$ ist, muß gelten:

$$\cos(tn) = 1 \text{ und } \sin(tn) = 0.$$

Das ist nur möglich, wenn $tn \in \{2\pi k \mid k \in \mathbb{Z}\}$ ist. Da $t \in [0, 2\pi)$ liegt, kommen für tn nur die Werte $0, 2\pi, 4\pi, \dots, (n-1)2\pi$ in Frage. Also muß t von der Form $t = \frac{k}{n} \cdot 2\pi$ sein. □

Definition.

Die Zahlen $\zeta_{k,n} := e^{\frac{k}{n} \cdot 2\pi \mathbf{j}}$, $k = 0, 1, \dots, n-1$, heißen die n -ten Einheitswurzeln.

Man braucht übrigens zu jedem n jeweils nur die erste Einheitswurzel zu kennen, denn es ist ja $\zeta_{k,n} = (\zeta_{1,n})^k$.

Beispiel :

Sei $n = 3$. Es ist $\frac{2\pi}{3} = \text{arc}(120^\circ)$,

$$\cos(120^\circ) = -\frac{1}{2} \quad \text{und} \quad \sin(120^\circ) = \frac{1}{2}\sqrt{3}.$$

Daraus folgt:

$$\zeta_{0,3} = 1, \quad \zeta_{1,3} = -\frac{1}{2} + \frac{\mathbf{j}}{2}\sqrt{3} \quad \text{und} \quad \zeta_{2,3} = (\zeta_{1,3})^2 = -\frac{1}{2} - \frac{\mathbf{j}}{2}\sqrt{3}.$$

I.8.4 Satz. *In \mathbb{C} besitzt jede Zahl $z \neq 0$ genau n n -te Wurzeln.*

BEWEIS: Sei $z = re^{\mathbf{j}t}$, mit $r = |z|$ und einem geeigneten $t \in [0, 2\pi)$. Dann setzen wir

$$z_k := \sqrt[n]{r} \cdot e^{\frac{\mathbf{j}t}{n}} \cdot \zeta_{k,n}, \quad k = 0, 1, \dots, n-1.$$

Offensichtlich sind dies n verschiedene komplexe Zahlen z_k mit $z_k^n = z$.

Ist andererseits w irgendeine Lösung der Gleichung $w^n = z$, so ist $w^n = z_0^n$, also

$$(wz_0^{-1})^n = 1.$$

Das bedeutet, daß es eine n -te Einheitswurzel $\zeta_{k,n}$ gibt, so daß $w = z_0 \cdot \zeta_{k,n}$ ist. \square

Man kann also in \mathbb{C} nie von *der* n -ten Wurzel einer Zahl z sprechen, es gibt stets n verschiedene. Das gilt auch im Falle $n = 2$! Das Symbol \sqrt{z} ist also zweideutig. In \mathbb{R} haben wir dagegen die positive Lösung der Gleichung $x^2 = a$ als *die* Wurzel aus a definiert.

Der obige Satz enthält eine wichtige Aussage über komplexe Polynome.⁹

Das Polynom $z^n - w$ besitzt (für jedes $w \in \mathbb{C}$) eine Nullstelle.

Im Reellen ist das falsch, z.B. hat $x^2 + 1$ keine Nullstelle in \mathbb{R} . Das zeigt die Bedeutung des folgenden Satzes:

I.8.5 Fundamentalsatz der Algebra.

Jedes nicht konstante komplexe Polynom hat in \mathbb{C} wenigstens eine Nullstelle.

Wir verzichten hier auf den nicht ganz einfachen Beweis.

Durch fortgesetzte Polynomdivision erhält man nun:

I.8.6 Satz. *Jedes nicht konstante komplexe Polynom läßt sich in Linearfaktoren zerlegen.*

Es gibt eine interessante Anwendung auf reelle Polynome:

⁹Ein komplexes Polynom ist eine Zuordnung $z \mapsto p(z) = a_n z^n + a_{n-1} z^{n-1} + \dots + a_1 z + a_0$, also eine Funktion, die *komplexe Argumente* zuläßt. Genauer werden wir solche Funktionen erst im 3. Semester behandeln.

I.8.7 Satz.

Es sei $p(z) = \sum_{i=0}^n a_i z^i$ ein Polynom mit **reellen** Koeffizienten. Dann gilt:

1. Ist $\alpha \in \mathbb{C}$ und $p(\alpha) = 0$, so ist auch $p(\bar{\alpha}) = 0$.
2. Die Anzahl der nicht-reellen Nullstellen von p ist gerade.
3. Ist n ungerade, so besitzt p mindestens eine reelle Nullstelle.
4. Besitzt p keine reelle Nullstelle, so ist $p(z)$ Produkt von Potenzen von quadratischen reellen Polynomen.

BEWEIS: Ist $\alpha \in \mathbb{C}$, so ist $\alpha = \bar{\alpha} \iff \alpha \in \mathbb{R}$.

1) Da alle a_i reell sind, ist

$$p(\bar{\alpha}) = \overline{p(\alpha)} = 0.$$

2) Ist $\alpha \notin \mathbb{R}$, so ist $\bar{\alpha} \neq \alpha$. Also kann man die nicht-reellen Nullstellen in Paaren zusammenfassen.

3) Es gibt $n = 2m + 1$ komplexe Nullstellen. Wegen (2) muß mindestens eine davon reell sein.

4) Sei $\alpha = a + b\mathbf{j}$ eine nicht-reelle Nullstelle. Dann enthält $p(z)$ den Faktor

$$(z - \alpha)(z - \bar{\alpha}) = (z - a - b\mathbf{j})(z - a + b\mathbf{j}) = (z - a)^2 - (b\mathbf{j})^2 = z^2 - 2az + (a^2 + b^2),$$

und der ist ein quadratisches Polynom mit reellen Koeffizienten. Fortgesetzte Polynomdivision ergibt die Behauptung. \square

Zum Schluß ein paar historische Anmerkungen:

In der Renaissance (etwa ab 1400) begann sich die Wissenschaft langsam von den christlichen Überlieferungen zu lösen. Nach der Eroberung Konstantinopels durch die Türken im Jahre 1453 kamen viele Gelehrte nach Italien und setzten dort neue Entwicklungen in Gang. Die Universität von Bologna entwickelte sich zu einem Zentrum der Mathematik.

Die Araber hatten bis dahin die Algebra als neue Disziplin weit vorangetrieben. Bei der Lösung der allgemeinen kubischen Gleichung

$$x^3 + ax^2 + bx + c = 0$$

waren sie jedoch erfolglos geblieben. Diesem Problem widmete man sich nun mit großem Eifer, und um 1500 fand Scipione dal Ferro eine rechnerische Lösung der Gleichung $y^3 + ay = b$ für $a, b > 0$. Er veröffentlichte seine Ergebnisse keineswegs, das war damals nicht üblich. Unter dem Siegel der Verschwiegenheit teilte er die Lösungsmethode seinem Schwiegersohn und Amtsnachfolger Nave und dem Rechenmeister Antonio Maria Fiore mit. Letzterer war wohl eher ein kleiner Geist. Voller Stolz über sein neues Wissen forderte er öffentlich den Rechenmeister Niccolo von Brescia, genannt *Tartaglia* (der „Stotterer“), zum Wettstreit auf. Jeder sollte 30 Aufgaben bei einem Notar hinterlegen,

50 Tage Zeit waren zur Lösung vorgesehen. Doch zu Fiores Überraschung löste Tartaglia sämtliche Aufgaben in wenigen Stunden. Und da dieser – wie er später behauptete – kurz vor dem Wettstreit, in der Nacht vom 12. zum 13. Februar 1535, herausbekommen hatte, wie man Gleichungen vom Typ $y^3 = ay + b$ oder $y^3 + b = ay$ lösen kann, stellte er seinerseits Aufgaben, von denen Fiore keine einzige bewältigen konnte.

Als der Ausgang des Wettstreites bekannt geworden war, bedrängte Girolamo Cardano, einer der erfahrensten Algebraiker seiner Zeit, den Rechenmeister Tartaglia, er möge ihm doch das Geheimnis verraten. Nach langem Zögern gab Tartaglia schließlich nach, ließ sich unter Eid Verschwiegenheit zusichern und verriet Cardano seine Formeln, wenn auch in dunklen Versen versteckt.

Zusammen mit seinem Schüler Ludovico Ferrari kam Cardano zu der Ansicht, daß Tartaglias Methoden mit denen dal Ferros übereinstimmten, und daß der Rechenmeister seine Ergebnisse deshalb nicht auf redlichem Wege erworben habe. Er fühlte sich nicht mehr an die Schweigepflicht gebunden und veröffentlichte 1545 in seinem großen Werk „Ars magna“ unter anderem auch die Methode zur Auflösung kubischer Gleichungen. Obwohl er Tartaglia als Urheber benannte, war dieser hell empört und bezichtigte Cardano des Eidbruches.

Ferrari nahm an Stelle seines Meisters den Fehdehandschuh auf, und es kam zu einem öffentlichen Briefwechsel zwischen Tartaglia und Ferrari, in dem sich beide übel beschimpften. Nach längerem Zögern nahm Tartaglia die Einladung zu einem öffentlichen Disput in Mailand im August 1548 an. Cardano war dabei nicht zugegen, jedoch zahlreiche Freunde Ferraris. Der Vormittag verging mit Streitigkeiten über die Auswahl der Kampfrichter, polemischen Vorwürfen und weitschweifigen Reden, dann nahte die Mittagsstunde, die Menge zerstreute sich und Tartaglia reiste eilends wieder ab. Wahrscheinlich hatte er sein Lösungsverfahren tatsächlich aus Aufzeichnungen von dal Ferro entnommen.

Bei dem Versuch, möglichst viele verschiedene Formen kubischer Gleichungen zu lösen, stieß Cardano erstmals auf den sogenannten „casus irreducibilis“, der z.B. bei der Gleichung $y^3 - 6y + 4 = 0$ auftritt. Die Cardanischen Formeln liefern in diesem Falle als Lösung den fiktiven Wert

$$y = \sqrt[3]{-2 + 2\sqrt{-1}} + \sqrt[3]{-2 - \sqrt{-1}}.$$

Cardano war hier mit seinem Latein am Ende.

Erst Rafael Bombelli (1526 - 1572) führte die Überlegungen weiter, indem er systematisch mit Wurzeln aus negativen Zahlen rechnete. Dabei stellte er fest:

$$(1 + \sqrt{-1})^3 = -2 + 2\sqrt{-1} \text{ und } (1 - \sqrt{-1})^3 = -2 - 2\sqrt{-1}.$$

Setzt man dies in die Lösung ein, so erhält man:

$$x = (1 + \sqrt{-1}) + (1 - \sqrt{-1}) = 2,$$

und das ist tatsächlich eine Lösung der Ausgangsgleichung.

Trotz dieses Erfolges blieben den Mathematikern die Wurzeln aus negativen Zahlen noch lange suspekt. Descartes bezeichnete sie 1637 als *imaginäre (also eingebildete) Zahlen*.

Euler führte 1777 das Symbol $i := \sqrt{-1}$ ein, das noch heute gebräuchlich ist.¹⁰ Aber erst Gauß führte 1831 den Begriff „komplexe Zahl“ für einen Ausdruck der Form $z = a + bi$ mit reellen Zahlen a und b ein und schaffte es, die neuen Zahlen hoffähig zu machen.

1835 beschrieb der irische Mathematiker Sir William Rowan Hamilton die komplexen Zahlen als Paare von reellen Zahlen. Und er kam auch auf die Idee, nun nach einer Multiplikationsregel für Zahlentripel (a, b, c) zu suchen.

13 Jahre lang suchte er vergeblich, aber vergeblich nach dieser Multiplikation. Dann kam ihm der entscheidende Gedanke: Statt mit drei reellen Komponenten versuchte er es mit vier. Die Einheiten nannte er e , i , j und k . Er hatte schon früh festgestellt, daß er bei seinen „hyperkomplexen“ Zahlen auf das Kommutativgesetz verzichten mußte und setzte

$$ij = -ji =: k.$$

Mit dem Sprung in die 4. Dimension hatte er Erfolg. Die neuen Zahlen nannte er „**Quaternionen**“. Er war selbst so begeistert von seiner Entdeckung, daß er sein Leben fortan der Erforschung der Quaternionen widmete.

Und 1877 bewies Frobenius:

\mathbb{C} und \mathbb{H} sind die einzigen assoziativen Zahlbereichserweiterungen von \mathbb{R} .

¹⁰außer bei den Elektrotechnikern, die lieber das Symbol \mathbf{j} benutzen, weil mit i die *Stromstärke* bezeichnet wird.

Literaturverzeichnis:

Logik, Mengenlehre, Axiomatik der reellen Zahlen, Abbildungen, elementare Funktionen und komplexe Zahlen:

K. Fritzsche: *Mathematik für Einsteiger*, Vor- und Brückenkurs zum Studienbeginn, Spektrum-Verlag, 1995.

Vektorräume und lineare Abbildungen:

K. Jänich: *Lineare Algebra*, Springer-Verlag, (1. Auflage 1979)

G. Fischer: *Lineare Algebra*, Vieweg, (10. Auflage 1995)

Differenzierbare Funktionen:

S.L. Salas / E. Hille: *Calculus*, Spektrum-Verlag, 1994,
sehr ausführlich, gut zum Nacharbeiten geeignet.

K. Endl / W. Luh: *Analysis I*, AULA-Verlag, (1. Auflage 1972),

H. Heuser: *Lehrbuch der Analysis, Teil 1*, Teubner-Verlag, 1979,

K. Königsberger: *Analysis 1*, Springer (3. Auflage 1995, anspruchsvoll, aber sehr gut)

S. Lang: *Analysis I*, Springer-Verlag (in Englisch),

Apostol: *Calculus 1*, John Wiley (in Englisch).

Sonstige Literatur (Ingenieur-Mathematik):

Meyberg/Vachenauer (2 Bd., Springer),

Ansorge/Oberle (2 Bd., Akademie-Verlag),

Burg/Haf/Wille (5 Bd., Teubner),

Papula (3 Bd., Vieweg), teilweise mathematisch bedenklich,

Fetzer/Fränkell (Springer),

Furlau („Das gelbe Rechenbuch“, Formelsammlung und durchgerechnete Aufgaben,
3 Bd., Verlag Martina Furlau, Dortmund).