Analysis 1 für Lehramt

WS 2010/11

Harald Woracek

Inhaltsverzeichnis

Prolog: Natürliche Zahlen

Der Begriff der natürlichen Zahl kommt von der unmittelbar einsichtigen Tätigkeit des Zählens. Das Zählen beginnt mit der natürlichen Zahl Eins:

$$1$$

Danach geht man Schritt für Schritt jeweils von einer natürlichen Zahl n zur nächstgrößeren $n \mapsto \hat{n}$. Es ergibt sich eine nie endende Folge:

$$1 \mapsto 2 \mapsto 3 \mapsto 4 \mapsto \ldots \mapsto n \mapsto \hat{n} \mapsto \ldots$$

Die Gesamtheit aller so erhaltenen Zahlen bezeichnen wir mit $\mathbb{N}$, die Menge der *natürlichen Zahlen*. Um auszudrücken das n eine natürliche Zahl sein soll schreiben wir

$$n \in \mathbb{N}.$$

Das Zählen einer Herde von Schafen funktioniert hervorragend, wenn die Tiere alle schön in einer Reihe stehen. Die einfachste Weise eine natürliche Zahl aufzuschreiben, ist es also die entsprechende Anzahl von Strichen (Punkten, Schafen, ...) nebeneinanderzusetzen:

$$1 = |, 2 = ||, 3 = |||, 4 = ||||, \ldots, \hat{n} = n|, \ldots$$

Mit Hilfe dieser Darstellung kann man viele grundlegende Begriffe anschaulich einführen.

Die Summe natürlicher Zahlen: Seien n und m zwei natürliche Zahlen, z.B. gegeben durch eine entsprechende Anzahl von Strichen. Schreibt man n und m hintereinander auf, so erhält man wieder eine Reihe von Strichen, also eine natürliche Zahl. Diese bezeichnet man als die Summe $n + m$ von n und m.

Das Produkt natürlicher Zahlen: Seien n und m zwei natürliche Zahlen, wieder gegeben durch eine entsprechende Anzahl von Strichen. Schreibt man die n representierenden Striche m-mal hintereinander auf, so erhält man wieder ein Strichsymbol, also eine natürliche Zahl. Diese bezeichnet man als das Produkt $n \cdot m$ von n und m.

Die Ordnung natürlicher Zahlen: Seien $n, m \in \mathbb{N}$, z.B. bestehe n aus einer Reihe von weißen Schafen und m aus einer Reihe von schwarzen Schafen. Wir führen das folgende Verfahren durch: Man nehme ein weißes und ein schwarzes Schaf und führe die beiden woanders hin. Diesen Schritt wiederhole man solange wie möglich. Dieses Verfahren findet sicher ein Ende, und zwar wenn entweder keine weißen (aber schon schwarze) Schafe übrig sind, oder wenn überhaupt keine

Schafe mehr da sind, oder wenn keine schwarzen (aber weiße) übrig sind. Es gilt also für zwei natürliche Zahlen n und m stets genau eine (d.h. eine und nur eine) der Beziehungen „n ist kleiner als m“, „n ist gleich m“ bzw. „n ist größer als m“: $n < m$, $n = m$, $n > m$. Man schreibt auch $n \leq m$ für „$n < m$ oder $n = m$“, und analog $n \geq m$ für „$n > m$ oder $n = m$“.

Wir wollen uns für den Anfang mit dieser anschaulichen Einführung zufrieden geben. Mathematisch exakte Definitionen sind im Anhang zusammengestellt, wo wir die natürlichen Zahlen von Grund auf (ausgehend von einigen Axiomen) studieren.

Rechenregeln für natürliche Zahlen.

Für das Rechnen mit natürlichen Zahlen gelten die folgenden Regeln.

Summe und Produkt sind beide assoziativ und kommutativ, d.h.

- $(n + m) + k = n + (m + k)$, $n \cdot (m \cdot k) = (n \cdot m) \cdot k$ (*Assoziativität*).
- $n + m = m + n$, $n \cdot m = m \cdot n$ (*Kommutativität*).

Sie sind verbunden durch das Distributivitätsgesetz von $\cdot$ über $+$, d.h.

- $n \cdot (m + k) = n \cdot m + n \cdot k$ (*Distributivität*).

Es existiert ein neutrales Element für die Multiplikation (nämlich die Zahl 1), d.h.

- Stets gilt $1 \cdot n = n \cdot 1 = n$ (*Neutralität*).

Weiters gelten die *Kürzungsregeln*:

- Ist $n + k = m + k$, so folgt $n = m$.
- Ist $n \cdot k = m \cdot k$, so folgt $n = m$.
- Ist $n + k \leq m + k$ oder $n \cdot k \leq m \cdot k$, so folgt $n \leq m$.

Die Ordnung hat die Eigenschaften

- Stets gilt $n \leq n$ (*Reflexivität*).
- Ist $n \leq m$ und auch $m \leq n$, so folgt $n = m$ (*Antisymmetrie*).
- Ist $n \leq m$ und $m \leq k$, so folgt $n \leq k$ (*Transitivität*).
- Es gilt stets mindestens eine von den beiden Beziehungen $n \leq m$ oder $m \leq n$ (*Totalordnung*).
- Ist M eine Teilmenge von $\mathbb{N}$ die mindestens ein Element enthält, so existiert $m \in M$ mit $m \leq l$, $l \in M$ (*Wohlordnung*).

Sie ist verträglich mit Summe und Produkt gemäß

- Ist $n \leq m$, dann ist stets auch $n + k \leq m + k$ sowie $n \cdot k \leq m \cdot k$.

Wir wollen uns an dieser Stelle damit begnügen die angeführten Rechenregeln zu glauben, bzw. uns einige Regeln anschaulich plausibel zu machen. Eine mathematisch exakte Herleitung aller Regeln ist im Anhang zu finden.

Die Kommutativität von $+$: Sind n und m gegeben durch eine Reihe von Strichen, so ist $n + m$ jenes Strichsymbol, welches man erhält wenn man zuerst n und dann m hintereinander aufschreibt. Nun ist es gleichgültig ob man eine Reihe von Strichen von links nach rechts oder von rechts nach links abzählt. Tut man zweiteres, so erhält man gerade $m + n$.

Die Kommutativität von $\cdot$: Dazu wollen wir uns n vorstellen als Anzahl von vertikal angeordneten Punkten. Schreibt man n dann m-mal hintereinander, so sieht man, daß das Produkt $n \cdot m$ gerade die Anzahl der Punkte des entstandenen Rechtecks ist. Tut man das gleiche mit m und n, also mit vertauschter Reihenfolge, so erhält man gerade das um 90° verdrehte Rechteck. Verdrehen eines Rechtecks ändert aber nichts an der Anzahl der Punkte, also haben wir $n \cdot m = m \cdot n$.

Die Verträglichkeit von $\leq$ mit $+$: Seien n und m representiert durch eine Reihe von weißen bzw. schwarzen Schafen. Sei vorausgesetzt, dass, wenn wir das oben beschriebene Verfahren durchführen, entweder gar keine Schafe oder nur schwarze Schafe übrigbleiben, d.h. dass $n \leq m$ gilt. Die Zahlen $n + k$ und $m + k$ erhält man nun so, dass man zu n bzw. m jeweils k weiße bzw. schwarze Schafe dazustellt. Nun beginnen wir das obige Verfahren durchzuführen. Nach k Schritten bleiben uns von der Herde $n + k$ noch gerade n Stück übrig, und von $m + k$ noch m. Für den $(k+1)$-ten Schritt sind wir also in der gleichen Ausgangslage wie bei dem für n und m durchgeführten Verfahren, und kommen damit auch zum selben Ergebnis, d.h. wir haben $n + k \leq m + k$.

Subtraktion und Division.

Sind n und m natürliche Zahlen mit $n < m$, so existiert genau eine natürliche Zahl l mit $n+l = m$, nämlich jene die von der nach ausführen des obigen Verfahrens übriggebliebene Herde schwarzer Schafe representiert wird. Man bezeichnet diese Zahl als die *Differenz* von m und n, und schreibt

$$l = m - n.$$

Die Operation „$-$“ der Differenzbildung bezeichnet man als *Subtraktion*. Sie ist in folgendem Sinne die Umkehroperation der Addition: Sind a, b, c mit $c = a+b$, so gilt $c - b = a$. Offenbar ist die Differenzbildung im Bereich der natürlichen Zahlen nicht unbeschränkt ausführbar, $m - n$ ist ja nur im Fall $m > n$ definiert. Im Fall $n > m$ existiert auch wirklich keine natürliche Zahl l mit $n + l = m$, weil ja stets $n + l > n > m$ gilt.

Wenn man anstelle der Addition die Multiplikation betrachtet, findet man die gleiche Situation vor. Seien $n, m \in \mathbb{N}$. Soferne eine natürliche Zahl l mit $n = m \cdot l$ existiert, nennt man diese den *Quotienten* von n und m, und schreibt

$$l = n : m.$$

Man spricht auch von der *Division* von n durch m. Ist die Division von n durch m möglich, so sagt man m ist ein *Teiler* von n und schreibt $m \mid n$. Andernfalls schreibt man $m \nmid n$. Wieder ist Division, soferne ausführbar, die Umkehrung

der Multiplikation. Denn sind $n, m, l \in \mathbb{N}$ mit $n = m \cdot l$, so folgt $l = n : m$. Die Situation bezüglich der tatsächlichen Ausführbarkeit einer Division ist aber noch viel schlimmer als bei der Subtraktion, offenbar ist eine Division wirklich nur in den seltensten Fällen tatsächlich ausführbar.

Das Prinzip der vollständigen Induktion.

Will man sich von der Richtigkeit einer Aussage über natürliche Zahlen überzeugen, so steht man vor dem Problem, dass man nicht einfach alle möglichen Werte für die in der Aussage möglicherweise vorkommenden Variablen ausprobieren kann (es gibt ja unendlich viele natürliche Zahlen). Betrachte zum Beispiel die Aussage

> „Für jede natürliche Zahl n sind die beiden Zahlen $n \cdot (n+1)$ und $n \cdot n + n$ gleich."

Durch probieren finden wir

$$\begin{array}{lll}
A(1): & n \cdot (n+1) = 1 \cdot 2 = 2\ , & n \cdot n + n = 1 \cdot 1 + 1 = 1 + 1 = 2 \quad \checkmark \\
A(2): & n \cdot (n+1) = 2 \cdot 3 = 6\ , & n \cdot n + n = 2 \cdot 2 + 2 = 4 + 2 = 6 \quad \checkmark \\
 & \vdots & \\
A(100): & n \cdot (n+1) = 100 \cdot 101 & n \cdot n + n = 100 \cdot 100 + 101 \quad \checkmark \\
 & \quad = 10100\ , & \quad = 10000 + 100 \\
 & & \quad = 10100
\end{array}$$

Wird also wohl hoffentlich immer stimmen. ABER, was ist eigentlich im Fall $A(101)$? oder $A(13259998)$? oder...?!

Mit ein klein wenig Kreativität (in diesem, zugegebenermaßen ziemlich simplen, Beispiel wirklich nur ein ganz klein wenig) findet man heraus, dass man unsere Rechenregeln geschickt kombinieren kann um die oben behauptete Gleichheit zu erhalten:

1. Für jede natürliche Zahl n gilt $n \cdot (n+1) = n \cdot n + n \cdot 1$.
2. Für jede natürliche Zahl n gilt $n \cdot 1 = n$.

Kombiniert also

3. Für jede natürliche Zahl n gilt $n \cdot (n+1) = n \cdot n + n \cdot 1 = n \cdot n + n$.

Eine universelle Methode um Aussagen über natürliche Zahlen zu beweisen, ist das *Prinzip der vollständigen Induktion*. Es besagt:

> *Für jede natürliche Zahl n sei eine Aussage $A(n)$ gegeben. Es gelte*
>
> - Induktionsanfang*: Die Aussage $A(1)$ ist wahr.*
> - Induktionsschritt*: Für jedes $n \in \mathbb{N}$ gilt: Wenn $A(n)$ wahr ist, so ist auch $A(n+1)$ wahr.*
>
> *Dann ist die Aussage $A(n)$ für jede natürliche Zahl n wahr.*

Dieses Prinzip spiegelt genau den schrittweisen Aufbau der natürlichen Zahlen wieder[1]. Man bezeichnet die Voraussetzung die man im Induktionsschritt zur Verfügung hat (hier $A(n)$) als *Induktionsvoraussetzung*.

Wir wollen nun zur Illustration einige Aussagen über natürliche Zahlen herleiten. Zur Abkürzung bezeichnen wir für $k, l \in \mathbb{N}$ die Zahl $\underbrace{k \cdot \ldots \cdot k}_{l \text{ mal}}$ mit k^l, und sprechen von der *n-ten Potenz* der Zahl k.

1 Proposition. *Für jede natürliche Zahl n gilt*

$$2 \cdot (1 + 2 + \ldots + n) = n^2 + n\,.$$

Beweis. Wir benützen vollständige Induktion. Die hier betrachtete Aussage $A(n)$ ist:

„Die beiden Zahlen $2 \cdot (1 + 2 + \ldots + n)$ und $n^2 + n$ sind gleich."

Induktionsanfang: Sei $n = 1$. Es gilt $2 \cdot (1) = 1^2 + 1$, die Aussage $A(1)$ ist also wahr.

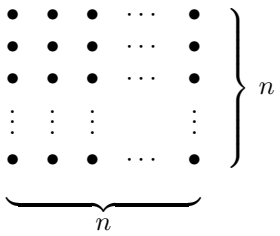
Induktionsschritt: Sei $n \in \mathbb{N}$ gegeben, und sei vorausgesetzt dass $A(n)$ wahr ist. Das heißt wir wissen schon, dass für dieses eine n die Gleichheit $2(1+\ldots+n) = n^2 + n$ gilt (Induktionsvoraussetzung). Dann erhalten wir (RR ... Rechenregel, IV ... Induktionsvoraussetzung)

$$\begin{aligned} 2 \cdot (1 + 2 + \ldots + (n+1)) &\overset{\text{RR}}{=} 2 \cdot ((1 + 2 + \ldots + n) + (n+1)) \overset{\text{RR}}{=} \\ &= 2(1 + \ldots + n) + 2(n+1) \overset{\text{IV}}{=} (n^2 + n) + 2(n+1) \overset{\text{RR}}{=} \\ &= (n^2 + 2n + 1) + (n+1) \overset{\text{RR}}{=} (n+1)^2 + (n+1)\,. \end{aligned}$$

Also ist $A(n+1)$ wahr.

Nach dem Prinzip der vollständigen Induktion ist die betrachtete Aussage $A(n)$ für alle natürlichen Zahlen n wahr. ❑

Beweis (von Proposition 1; #2). Sei $n \in \mathbb{N}$ gegeben. Zeichne ein Quadrat von Punkten mit Seitenlänge n, also insgesamt n^2 Punkte.



Zählt man die Punkte längs der Diagonalen, so erhält man

$$n^2 = 1 + 2 + \ldots + (n-1) + n + (n-1) + \ldots + 2 + 1$$

also $n^2 = 2(1 + 2 + \ldots + (n-1)) + n$ oder $2(1 + 2 + \ldots + n) = n^2 + n$. ❑

[1] Streng logisch betrachtet ist das Induktionsprinzip das einzige Beweismittel welches von Anfang an zur Verfügung steht, vgl. Anhang.

Beweis (von Proposition 1; #3). Sei $n \in \mathbb{N}$ gegeben. Bezeichne mit S die Summe $1 + 2 + \ldots + n$. Dann erhält man für $2 \cdot S$ den Ausdruck

	1	+	2	+	3	+ … +	n		S
+	n	+	$(n-1)$	+	$(n-2)$	+ … +	1		S
=	$(n+1)$	+	$(n+1)$	+	$(n+1)$	+ … +	$(n+1)$		$(n+1)n$

❑

2 Proposition. *Für jede natürliche Zahl n gilt*

$$1 + 2 + 2^2 + \ldots + 2^n = 2^{n+1} - 1$$

Beweis. Wir benützen vollständige Induktion. Die hier betrachtete Aussage $A(n)$ ist:

„Die beiden Zahlen $1 + 2 + 2^2 + \ldots + 2^n$ und $2^{n+1} - 1$ sind gleich."

Induktionsanfang: Sei $n = 1$. Es gilt $(1+2)+1 = (1+1)+2 = 2+2 = 2\cdot(1+1) = 2 \cdot 2$, also ist $1 + 2 = 2 \cdot 2 - 1$. D.h. die Aussage $A(1)$ ist wahr.

Induktionsschritt: Sei $n \in \mathbb{N}$ gegeben, und sei vorausgesetzt dass $A(n)$ wahr ist. Das heißt wir wissen schon, dass für dieses eine n die Gleichheit $1 + 2 + 2^2 + \ldots + 2^n = 2^{n+1} - 1$ gilt (Induktionsvoraussetzung). Es folgt

$$\begin{aligned} 1 + 2 + 2^2 + \ldots + 2^n + 2^{n+1} &\overset{\text{RR}}{=} (1 + 2 + \ldots + 2^n) + 2^{n+1} \overset{\text{IV}}{=} \\ &= (2^{n+1} - 1) + 2^{n+1} \overset{\text{RR}}{=} 2 \cdot 2^{n+1} - 1 \overset{\text{RR}}{=} 2^{n+2} - 1\,. \end{aligned}$$

Also ist $A(n+1)$ wahr.

Nach dem Prinzip der vollständigen Induktion ist die betrachtete Aussage $A(n)$ für alle natürlichen Zahlen n wahr. ❑

Beweis (von Proposition 2; #2). Für beliebige Zahlen x, y und $n \in \mathbb{N}$ gilt nach den Rechenregeln

$$(x - y)(x^n + x^{n-1}y + \ldots + xy^{n-1} + y^n) =$$

$$= \left(x^{n+1} + x^n y + \ldots + x^2 y^{n-1} + xy^n\right) - \left(x^n y + x^{n-1}y^2 + \ldots + xy^n + y^{n+1}\right) =$$

$$= x^{n+1} - y^{n+1}$$

gilt. Speziell für $x = 2$ und $y = 1$ erhält man die gewünschte Gleichheit[2]. ❑

3 Definition. Sei $n \in \mathbb{N}$. Dann heißt n *gerade*, wenn $2|n$. Andernfalls heißt n *ungerade*. //

Offensichtlich ist die Summe zweier gerader Zahlen, sowie das Produkt zweier Zahlen von denen mindestens eine gerade ist, wieder gerade[3].

4 Proposition. *Für jedes $n \in \mathbb{N}$ ist genau eine (d.h. „eine und nur eine") der beiden Zahlen n und $n + 1$ gerade.*

[2] Was ist an diesem Beweis zu bemängeln, und wie kann man diesen Mangel beheben?

[3] Nichts ist offensichtlich! Wie kann man diese Aussagen begründen?

Beweis. Wir benützen vollständige Induktion. Die hier betrachtete Aussage $A(n)$ ist:

„Genau eine der beiden Zahlen n und $n+1$ ist gerade."

Induktionsanfang: Sei $n = 1$. Dann haben wir das Zahlenpaar „$1, 2$" zu betrachten. Die Zahl 2 ist gerade: denn wir können schreiben $2 = 2 \cdot 1$. Es ist nicht ganz so einfach einzusehen, dass die Zahl 1 ungerade ist: Sei m eine gerade Zahl, sodass wir also $m = 2 \cdot l$ schreiben können. Dann gilt

$$m = 2 \cdot l \geq 2 > 1\,,$$

also ist $m \neq 1$.

Induktionsschritt: Sei $n \in \mathbb{N}$ gegeben, und sei vorausgesetzt dass $A(n)$ wahr ist. Das heißt wir wissen schon, dass für dieses eine n genau eine Zahl dieses einen Paares „$n, n+1$" gerade ist (Induktionsvoraussetzung).

Betrachte zuerst den Fall dass n gerade und $n+1$ ungerade ist. Wir schreiben $n = 2 \cdot l$, und erhalten $n + 2 = 2 \cdot (l + 1)$. Also ist $n + 2$ gerade. Wir sehen, dass genau eine Zahl des Paares „$n + 1, n + 2$" gerade ist.

Betrachte nun den Fall, dass n ungerade und $n + 1$ gerade ist. Dann wissen wir schon, dass eine Zahl des Paares „$n + 1, n + 2$" gerade ist, nämlich $n + 1$. Ist $n + 2 = 2 \cdot l$ mit einem $l \in \mathbb{N}$, so muss $l > 1$ sein da ja $n + 2 > 2$ ist. Wir können also die Differenz $l - 1$ bilden, und es folgt $n = 2 \cdot (l - 1)$, d.h. n ist gerade. Da, in dem jetzt betrachteten Fall n ungerade ist, muss $n + 2$ ebenfalls ungerade sein. Also ist $A(n + 1)$ wahr.

Nach dem Prinzip der vollständigen Induktion ist die betrachtete Aussage $A(n)$ für alle natürlichen Zahlen n wahr. ❑

5 Proposition. *Sei $n \in \mathbb{N}$, und seien $n + 1$ natürliche Zahlen gegeben welche alle nicht größer als $2n$ sind. Dann gibt es unter diesen Zahlen eine, welche eine andere der gegebenen Zahlen teilt.*

Beweis. Wir benützen vollständige Induktion. Die hier betrachtete Aussage $A(n)$ ist:

„Für je $n + 1$ verschiedene Zahlen $x_1, \cdots, x_{n+1}$ welche alle nicht größer als $2n$ sind, gibt es Paar (x_i, x_j) mit $x_i \neq x_j$ und $x_i | x_j$."

Induktionsanfang: Sei $n = 1$. Sind zwei verschiedene Zahlen ≤ 2 gegeben, so muss eine von ihnen gleich 1 und die andere gleich 2 sein. Da $1|2$ gilt, sehen wir dass $A(1)$ wahr ist.

Induktionsschritt: Sei $n \in \mathbb{N}$ gegeben, und sei vorausgesetzt dass $A(n)$ wahr ist. Das heißt wir wissen schon, dass für dieses eine n aus je $n + 1$ verschiedenen Zahlen welche nicht größer als $2n$ sind ein Paar ausgewählt werden kann in welchem die eine Zahl die andere teilt (Induktionsvoraussetzung). Seien nun $n + 2$ verschiedene Zahlen $x_1, \ldots, x_{n+2}$, welche alle nicht größer als $2n + 2$ sind, gegeben. O.b.d.A. können wir diese der Grösse nach anordnen, d.h. so nummerieren dass $x_1 < x_2 < \ldots < x_{n+2}$ ist.

Betrachte den Fall dass $x_{n+1} \leq 2n$ ist. Dann sind die Zahlen[4]

$$y_1 := x_1, \ldots, y_{n+1} := x_{n+1}$$

[4]Das Symbol „:=" bedeutet, dass die linke Seite (jene mit dem Doppelpunkt) definiert ist als das was rechts steht.

alle verschieden und nicht größer als $2n$. Die Induktionsvoraussetzung, verwendet mit den Zahlen $y_1, \ldots, y_{n+1}$, liefert uns ein Paar (y_i, y_j) mit $y_i \neq y_j$ und $y_i | y_j$. Das Paar (y_i, y_j) kommt aber auch unter den Zahlen $x_1, \ldots, x_{n+2}$ vor, und haben ein Paar mit der gewünschten Eigenschaft gefunden.

Betrachte den Fall, dass $x_{n+1} > 2n$ ist, und dass die Zahl $n+1$ unter den x_i vorkommt. Wegen $2n < x_{n+1} < x_{n+2} \leq 2n+2$, muss $x_{n+1} = 2n+1$ und $x_{n+2} = 2n+2$ sein. Wir können also das Paar $(n+1, x_{n+2})$ nehmen.

Betrachte schliesslich den Fall, dass $x_{n+1} > 2n$ ist, und die Zahl $n+1$ nicht unter den x_i vorkommt. Betrachte die $n+1$ Zahlen

$$y_1 := x_1, \ldots, y_n := x_n, y_{n+1} := n+1\,.$$

Diese sind alle voneinander verschieden und $\leq 2n$. Die Induktionsvoraussetzung, verwendet mit den Zahlen $y_1, \ldots, y_{n+1}$, liefert uns ein Paar (y_i, y_j) mit $y_i \neq y_j$ und $y_i | y_j$. Jede Zahl die von $n+1$ geteilt wird (ausser $n+1$ selbst) ist mindestens $2n+2$, also kann y_i nicht gleich $n+1$ sein. Wir erhalten nun das gesuchte Paar für die gegebenen Zahlen $x_1, \ldots, x_{n+2}$: Ist $y_j = n+1$, so nehmen wir das Paar $(y_i, 2n+2)$. Ist $y_j \neq n+1$, nehmen wir (y_i, y_j).

Insgesamt sehen wir, dass $A(n+1)$ wahr ist.

Nach dem Prinzip der vollständigen Induktion ist die betrachtete Aussage $A(n)$ für alle natürlichen Zahlen n wahr. ❑

Beweis (von Proposition 5; #2). Seien $n \in \mathbb{N}$ und $n+1$ verschiedene Zahlen $x_1, \cdots, x_{n+1}$, alle nicht größer als $2n$, gegeben. Falls x_i ungerade ist, setze $y_i := x_i$. Ist x_i gerade, so schreibe $x_i = 2^{l_i} y_i$ mit y_i ungerade[5]. Dann sind die $n+1$ Zahlen $y_1, \ldots, y_{n+1}$ alle ungerade und nicht größer als $2n$. Nun gibt es aber nur n verschiedene ungerade Zahlen welche nicht größer als $2n$ sind, also müßen (mindestens) zwei der y's gleich sein[6], d.h. es muss i, j geben mit $i \neq j$ aber $y_i = y_j$.

Ist x_i ungerade oder $l_i \leq l_j$, so gilt $x_i | x_j$. Ist x_j ungerade, oder $l_j \leq l_i$, so gilt $x_j | x_i$. In beiden Fällen haben wir ein Paar mit der gewünschten Eigenschaft gefunden. ❑

Oft ist es praktisch, anstelle der Originalversion, Varianten des Induktionsprinzips zu verwenden. Eine solche wäre zum Beispiel:

6 Satz. *Für jede natürliche Zahl n sei eine Aussage $B(n)$ gegeben. Es gelte*

(*i*) *Die Aussage $B(1)$ ist wahr.*

(*ii*) *Für jedes $n \in \mathbb{N}$ gilt: Wenn alle Aussagen $B(1), \ldots, B(n)$ wahr sind, so ist auch $B(n+1)$ wahr.*

Dann ist die Aussage $B(n)$ für jede natürliche Zahl n wahr.

Beweis. Wir benützen vollständige Induktion. Die hier betrachtete Aussage $A(n)$ ist:

„Alle Aussagen $B(1), \ldots, B(n)$ sind wahr."

[5] Begründe, dass das tatsächlich möglich ist!

[6] Das *Schubfachprinzip*: Teilt man mehr als N Objekte auf N Schubfächer auf, so muss in mindestens einem der Fächer mehr als ein Objekt liegen.

Induktionsanfang: Sei $n = 1$. Dann ist $A(1) = B(1)$, und nach unserer Voraussetzung (i) daher wahr.

Induktionsschritt: Sei $n \in \mathbb{N}$ gegeben, und sei vorausgesetzt dass $A(n)$ wahr ist. Das heißt wir wissen schon, dass für dieses eine n die Aussagen $B(1), \ldots, B(n)$ wahr sind (Induktionsvoraussetzung). Aus unserer Voraussetzung (ii) erhalten wir damit dass $B(n+1)$ wahr ist. Es sind also alle Aussagen $B(1), \ldots, B(n+1)$ wahr, und das ist gerade $A(n+1)$.

Nach dem Prinzip der vollständigen Induktion ist die betrachtete Aussage $A(n)$ für alle natürlichen Zahlen n wahr. Insbesondere ist daher auch $B(n)$ für alle natürlichen Zahlen n wahr. ❑

7 Proposition. *Seien $a_1, a_2, a_3, \ldots$ natürliche Zahlen, und gelte*

$$a_1 = 1, \quad a_{k+1} = a_1 + \ldots + a_k, \ k \in \mathbb{N}\,.$$

Dann gilt $a_k = 2^{k-2}$ für alle $k \geq 3$.

Beweis. Wir benützen vollständige Induktion in der Variante von Satz 6. Die hier betrachtete Aussage $B(n)$ ist:

„Es gilt $a_n = 2^{n-2}$."

Induktionsanfang: Wir berechnen die ersten paar Werte von a_k:

$$\begin{aligned} a_1 &= 1 \\ a_2 &= a_1 = 1 \\ a_3 &= a_2 + a_1 = 1 + 1 = 2 \\ a_4 &= a_3 + a_2 + a_1 = 2 + 1 + 1 = 4 \end{aligned}$$

Insbesondere sehen wir, dass die Aussage $B(1)$ richtig ist.

Induktionsschritt: Sei $n \in \mathbb{N}$ gegeben, und sei vorausgesetzt dass alle Aussagen $B(1), \ldots, B(n)$ wahr sind. Das heißt wir wissen schon, dass $a_k = 2^{k-2}$, $k = 3, \ldots, n+2$, für dieses eine n gilt (Induktionsvoraussetzung). Um $B(n+1)$ zu zeigen, genügt es die Zahl a_{n+3} zu berechnen:

$$\begin{aligned} a_{n+3} = a_{n+2} + a_{n+1} + \ldots + a_2 + a_1 &\overset{\text{IV}}{=} \left(2^n + 2^{n-1} + \ldots + 2 + 1\right) + 1 \overset{\text{Proposition 2}}{=} \\ &= \left(2^{n+1} - 1\right) + 1 = 2^{n+1}\,. \end{aligned}$$

Also gilt $B(n+1)$.

Nach Satz 6 ist die betrachtete Aussage $B(n)$ für alle natürlichen Zahlen n wahr. ❑

Kapitel 1

Einige Grundlagen

1.1 Der Cantorsche Mengenbegriff

1.1.1 Definition. Eine *Menge* ist eine Zusammenfassung von bestimmten, wohlunterschiedenen Objekten unserer Anschauung zu einem Ganzen. Die Objekte heißen *Elemente* der Menge. //

Diese Definition des Begriffes der Menge stammt von Cantor[1]. Sie genügt eigentlich nicht den strengsten logischen Ansprüchen, ist jedoch gut genug um im alltäglichen mathematischen Leben damit Auslangen zu finden[2]. Eine exakte Definition des Mengenbegriffes ist recht kompliziert und würde hier viel zu weit führen.

Wir wollen als erstes darauf eingehen, wie man Mengen üblicherweise aufschreibt. Natürlich kann man sich verbal artikulieren, was ja der Natur des Menschen entspricht. Leider wird das aber oft viel zu kompliziert, und ist manchmal auch Grund für Mißverständnisse.

Ist M eine Menge und x ein Element der Menge, so schreibt man $x \in M$. Ist dagegen x kein Element von M, so schreibt man $x \notin M$. Wir können eine Menge angeben durch Aufzählung ihrer Elemente. Man schreibt zum Beispiel

$$M = \{a, \hat{z}, 17, \text{Strawberry fields forever}, 117, \heartsuit\}$$

für die Menge bestehend aus den Elementen „a“, „$\hat{z}$“, „17“, „Strawberry fields forever“, „117“, „$\heartsuit$“. Die Menge der natürliche Zahlen schreibt man zum Beispiel auf als

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

[1] Georg Cantor. 3.3.1845 St.Petersburg - 6.1.1918 Halle/Saale

[2] Das *Russelsche Paradoxon* (benannt nach Bertrand Russel, 18.5.1872–2.2.1970): Sei $\mathcal{X}$ die Menge aller jener Mengen welche sich selbst nicht als Element enthalten.
Fall 1: Angenommen $\mathcal{X}$ enthält sich selbst als Element. Dann ist (nach Definition von $\mathcal{X}$) $\mathcal{X}$ kein Element von $\mathcal{X}$. Dieser Fall kann also nicht eintreten.
Fall 2: Angenommen $\mathcal{X}$ enthält sich selbst nicht als Element. Dann ist (wieder nach Definition von $\mathcal{X}$) $\mathcal{X}$ ein Element von $\mathcal{X}$. Auch dieser Fall kann also nicht eintreten.
Einer der beiden Fälle muß aber eintreten, da es ja keine anderen Möglichkeiten gibt ?!? Die Lösung des Rätsels ist, dass das Objekt $\mathcal{X}$ gar keine Menge ist, weil es in gewissem Sinne „zu groß“ ist. Die Cantorsche Mengendefinition ist also zu unexakt um immer (z.B. für $\mathcal{X}$) zu funktioneren.

Bei dieser oder ähnlichen Notationen wird stillschweigend vorausgesetzt, daß der Leser die drei Punkte „...“ von sich aus richtig interpretiert. Eine weitere Methode Mengen anzugeben, ist durch Angabe von charakterisierenden Eigenschaften ihrer Elemente. Die Menge der geraden natürlichen Zahlen wäre dann

$$M = \big\{x \in \mathbb{N} : x = 2n \text{ für ein } n \in \mathbb{N}\big\}.$$

Diese Menge würde man in der aufzählenden Schreibweise notieren als $M = \{2, 4, 6, \ldots\}$. Man sieht, daß die Schreibweise mit Angabe von charakterisierenden Eigenschaften wesentlich weniger mißverständlich ist. Ähnlich hat man für jedes $k \in \mathbb{N}$ die Menge

$$M_k = \{x \in \mathbb{N} : k|n\} \tag{1.1.1}$$

aller durch k teilbaren natürlichen Zahlen. Ein etwas komplizierter vorstellbares Objekt ist die Menge

$$M = \{M_k : 17|k\}, \tag{1.1.2}$$

denn die Elemente dieser Menge sind selbst wieder Mengen.

Eine wichtige Rolle spielt auch die sogenannte *leere Menge*: Jene Menge die keine Elemente besitzt. Man schreibt die leere Menge als $\{\}$ oder auch als $\emptyset$.

1.1.2 Definition. Sind A, B Mengen, so sagt man A *ist gleich* B und schreibt $A = B$, wenn A und B die selben Elemente enthalten. Man sagt A ist eine *Teilmenge* von B und schreibt $A \subseteq B$, falls jedes Element von A auch ein Element von B ist. In diesem Fall bezeichnet man auch B als *Obermenge* von A. Schreibweisen wie $A \neq B$, $A \supsetneq B$, o.ä. sind selbsterklärend. //

Hat man zwei oder mehrere Mengen, so kann man diese in verschiedener Weise miteinander verknüpfen.

1.1.3 Definition. Seien M und N Mengen. Dann ist

- $M \cap N := \{x : x \in M \text{ und } x \in N\}$ die *Durchschnittsmenge* von M und N. Das ist also die Menge bestehend aus den Elementen welche in beiden Mengen M und N vorkommen.
- $M \cup N := \{x : x \in M \text{ oder } x \in N\}$ die *Vereinigungsmenge*. Das ist also die Menge mit den Elementen die entweder in M oder in N (oder in beiden) vorkommen.
- $M \times N := \{(x, y) : x \in M, y \in N\}$ das *kartesische Produkt* von M mit N. Das ist also die Menge deren Elemente die geordnete Paare sind deren erste Komponente zu M und deren zweite Komponente zu N gehört.
- $M \setminus N := \{x : x \in M \text{ und } x \notin N\}$ die *Differenzmenge*. Das ist also die Menge aller jener Elemente von M welche nicht zu N gehören.

//

Durchschnitt und Vereinigung einer beliebig großen Familie von Mengen, sowie das kartesische Produkt von endlich vielen Mengen, kann man analog definieren.

1.1.4 Definition. Sei M_i, $i \in I$, eine Familie von Mengen, durchindiziert mit einer Indexmenge I. Dann ist

- $\bigcap_{i\in I} M_i := \{x : \text{Für jedes } i \in I \text{ ist } x \in M_i\}$ der Durchschnitt der Mengenfamilie M_i, $i \in I$.
- $\bigcup_{i\in I} M_i := \{x : \text{Es existiert ein } i \in I \text{ mit } x \in M_i\}$ die Vereinigung der Mengenfamilie M_i, $i \in I$.
- $M_1 \times \ldots \times M_n := \{(x_1, \ldots, x_n) : \text{Für jedes } i = 1, \ldots, n \text{ gilt } x_i \in M_i\}$ das kartesische Produkt der Mengen $M_1, \ldots, M_n$.

//

Man schreibt für das kartesische Produkt von Mengen $M_1, \ldots, M_n$ oft auch $\prod_{i=1}^n M_i$, und kürzt ab $M^n := \underbrace{M \times \ldots \times M}_{n\text{-mal}}$.

Das kartesische Produkt einer beliebig großen Familie von Mengen ist nicht so einfach zu erklären. Man benötigt dazu den Begriff der Funktion, vgl. Definition 1.2.12.

1.1.5 Beispiel.

(*i*) Einfache Beipiele für Durchschnitts- bzw. Vereinigungsbildung wären:

$$\{1,2,3\} \cap \{1,5,7\} = \{1\}, \quad \{a,b,7\} \cap \{3,4,x\} = \emptyset,$$

$$\{2,3,4,5\} \cup \{4,5,6,7\} = \{2,3,4,5,6,7\}, \quad \{a,b,c\} \cup \emptyset = \{a,b,c\}.$$

(*ii*) Seien M_k und M die Mengen aus (1.1.1) bzw. (1.1.2). Beachte, daß sich die Mengen M und

$$\tilde{M} = \bigcup_{k:17|k} M_k$$

wesentlich voneinander unterscheiden. Denn $\tilde{M} = \{17, 34, 51, \ldots\}$, wogegen $M = \{M_{17}, M_{34}, M_{51}, \ldots\}$.

(*iii*) Die Menge $\mathbb{N}\backslash M_2$ ist die Menge der ungeraden natürlichen Zahlen. Weiters ist

$$\{1,2,3,4\} \setminus \{4,5,6,7\} = \{1,2,3\}, \quad \{a,b,c\} \setminus \emptyset = \{a,b,c\}.$$

(*iv*) Das kartesische Produkt $\mathbb{N} \times 2\mathbb{N}$ ist die Menge

$$\mathbb{N} \times 2\mathbb{N} = \big\{(1,2),(1,4),\ldots,(2,2),(2,4),\ldots,(3,2),(3,4),\ldots,\ldots\big\}.$$

//

Ist $N \subseteq M$, so schreibt man für $M \setminus N$ oft auch kurz N^c, das *Komplement* von N in M. Diese abkürzende Schreibweise tritt besonders dann auf, wenn ohnehin aus dem Zusammenhang klar ist, daß alle betrachtenden Mengen, Objekte und sonstigen Dinge, sich in einer „großen Grundmenge“ aufhalten. Befasst man sich z.B. schon seitenlang mit geraden natürlichen Zahlen, so wird man unter $(4\mathbb{N})^c$ die Menge $2\mathbb{N} \setminus 4\mathbb{N}$, also $\{2, 6, 10, 14, \ldots\}$ verstehen. Spielen jedoch sämtliche Überlegungen im Bereich aller natürlichen Zahlen, so wird $(4\mathbb{N})^c$ wohl $\{1, 2, 3, 5, 6, 7, 9, \ldots\}$ bezeichnen. Wie bei vielen anderen (schlampigen) Schreibweisen wird auch hier stillschweigend davon ausgegangen, daß Leser mathematischer Werke typischerweise mitdenken.

Diese Operationen mit Mengen erfüllen diverse Rechenregeln. Einige davon stellen wir nun zusammen.

1.1.6 Proposition (Rechenregeln für Mengen)**.** *Für die oben definierten Operationen mit Mengen gelten die folgenden Rechenregeln:*

(*i*) *Durchschnitt und Vereinigung sind assoziativ und kommutativ. Es gelten die Distributivitätsgesetze*

$$A \cap \bigcup_{i\in I} B_i = \bigcup_{i\in I} (A \cap B_i), \quad A \cup \bigcap_{i\in I} B_i = \bigcap_{i\in I} (A \cup B_i)\,.$$

(*ii*) *Es gilt*

$$A \cap (A \cup B) = A, \quad A \cup (A \cap B) = A\,,$$
$$A \cap A = A \cup A = A\,.$$

(*iii*) *Es gelten die de Morganschen Regeln*[3]

$$\Big(\bigcup_{i\in I} A_i\Big)^c = \bigcap_{i\in I} A_i^c, \quad \Big(\bigcap_{i\in I} A_i\Big)^c = \bigcup_{i\in I} A_i^c\,.$$

Dabei sind alle Komplementbildungen bezüglich einer festen Grundmenge, welche alle auftretenden Mengen umfasst, zu verstehen.

(*iv*) *Es gilt*

$$A \setminus B = A \cap B^c\,.$$

Wieder ist die Komplementbildung bezüglich einer festen Grundmenge zu verstehen, welche die beiden Mengen A, B umfasst.

(*v*) *Es gilt*

$$A \subseteq B \iff A \cap B = A\,.$$

Beweis. Diese Eigenschaften überprüft man unmittelbar durch Einsetzen der jeweiligen Definitionen. Wir wollen exemplarisch einige Punkte nachweisen.

Erste Formel in (*i*)*:* Sei $x \in A \cap \bigcup_{i\in I} B_i$. Dann ist also $x \in A$ und es existiert ein Index $i \in I$ mit $x \in B_i$. Für diesen Index i gilt dann auch $x \in A \cap B_i$, und wir haben $x \in \bigcup_{i\in I}(A \cap B_i)$.

Umgekehrt sei $x \in \bigcup_{i\in I}(A \cap B_i)$. Dann existiert ein Index i mit $x \in A \cap B_i$. Es folgt, dass $x \in A$ und dass, für diesen Index i, auch $x \in B_i$. Insgesamt $x \in A \cap \bigcup_{i\in I} B_i$.

Erste Formel in (*iii*)*:* Sei $x \in \Big(\bigcup_{i\in I} A_i\Big)^c$. Das heißt x gehört nicht zur Vereinigung $\bigcup_{i\in I} A_i$, anders ausgedrückt, es gibt kein $i \in I$ mit $x \in A_i$. Also muss für jedes $i \in I$ der Punkt x zu A_i gehören, und wir sehen $x \in \bigcap_{i\in I} A_i^c$.

Umgekehrt sei $x \in \bigcap_{i\in I} A_i^c$. Dann liegt x in jeder Menge A_i^c, kann daher in keiner Menge A_i sein, und wir erhalten $x \notin \bigcup_{i\in I} A_i$.

Punkt (*v*)*:* Sei vorausgesetzt, dass $A \subseteq B$. Ist $x \in A \cap B$, so ist trivialerweise $x \in A$. Ist $x \in A$, so gilt nach Voraussetzung auch $x \in B$, und daher $x \in A \cap B$. Insgesamt $A \cap B = A$. Umgekehrt sei vorausgesetzt, dass $A \cap B = A$. Sei $x \in A$, dann ist nach Voraussetzung auch $x \in A \cap B$, und damit insbesondere in B. Also haben wir $A \subseteq B$. ❑

[3] Auguste de Morgan. 27.6.1806 Madura (Indien) - 18.3.1871 London

1.1.7 Definition. Sei M eine Menge. Die *Potenzmenge* von M ist die Menge $\{A : A \subseteq M\}$. Das ist also die Menge aller Teilmengen von M. Man schreibt für die Potenzmenge von M oft $\mathcal{P}(M)$. //

1.1.8 Beispiel. Sei $M = \{1, 2, 3\}$. Dann ist die Potenzmenge $\mathcal{P}(M)$ gleich

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

Die Potenzmenge der Menge $\mathbb{N}$ ist schon viel zu groß um sie noch in irgendeiner aufzählenden Weise anschreiben zu können. Sie enthält ja neben Mengen des Typs $\{1, 2, 3\}, \{4, 6, 7, 8, 1004\}$ o.ä. auch noch unendliche Mengen wie zum Beispiel $2\mathbb{N}$ oder $\{n \in \mathbb{N} : n \geq 27\}$ und viele mehr. //

Ist M eine endliche Menge, so ist die Potenzmenge von M ebenfalls endlich. Tatsächlich gilt:

1.1.9 Proposition. *Sei M eine Menge mit n Elementen. Dann hat $\mathcal{P}(M)$ genau 2^n Elemente.*

Beweis. Wir machen Induktion nach der Anzahl der Elemente von M. Hat M nur ein Element, $M = \{x_1\}$, so ist

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

hat also 2^1 Elemente.

Sei nun vorausgesetzt, dass die Potenzmenge jeder Menge mit n Elementen genau 2^n Elemente hat, und sei eine Menge M mit $n + 1$ Elementen gegeben, $M = \{x_1, \ldots, x_n, x_{n+1}\}$. Wir unterteilen die Teilmengen von M in zwei Klassen, nämlich

$$K_1 := \big\{A \subseteq M : x_{n+1} \notin A\big\}, \quad K_1 := \big\{A \subseteq M : x_{n+1} \in A\big\}.$$

Klarerweise gilt $K_1 \cap K_2 = \emptyset$ und $K_1 \cup K_2 = \mathcal{P}(M)$. Die Anzahl der Elemente von $\mathcal{P}(M)$ ist daher gleich der Summe der Anzahlen der Elemente von K_1 und K_2.

Die Menge K_1 ist nichts anderes als $\mathcal{P}(M \setminus \{x_{n+1}\})$, und hat daher 2^n Elemente. Die Klasse K_2 enthält alle Mengen der Gestalt $A' \cup \{x_{n+1}\}$ wobei $A' \in \mathcal{P}(M \setminus \{x_{n+1}\})$, und wird von diesen ausgeschöpft. Sind $A'_1, A'_2 \in \mathcal{P}(M \setminus \{x_{n+1}\})$ verschieden, so sind, da ja weder A'_1 noch A'_2 das Element x_{n+1} enthalten können, auch die Mengen $A'_1 \cup \{x_{n+1}\}$ und $A'_2 \cup \{x_{n+1}\}$ verschieden. Also hat K_2 genauso viele Elemente wie $\mathcal{P}(M \setminus \{x_{n+1}\})$, und das sind 2^n. Insgesamt erhalten wir

$$\#\mathcal{P}(M) = \#K_1 + \#K_2 = 2^n + 2^n = 2^{n+1}.$$

❑

1.2 Relationen und Funktionen

Wir werden im folgenden einige Aussagen- und Prädikatenlogische Schreibweisen verwenden, es aber dabei belassen diese Symbole als Schreibweisen zu ver-

stehen. Nämlich lesen wir

Lese	„$A \wedge B$“	als	„A und B“
Lese	„$A \vee B$“	als	„A oder B“
Lese	„$A \Rightarrow B$“	als	„Wenn A gilt, so gilt auch B“
Lese	„$A \iff B$“	als	„A gilt genau dann, wenn B gilt“
Lese	„$\forall\, i \in I :\ A(i)$“	als	„Für alle $i \in I$ gilt $A(i)$“
Lese	„$\exists\, i \in I :\ A(i)$“	als	„Es existiert ein $i \in I$, sodass $A(i)$ gilt“

Etwas mehr Information zu diesem Thema findet man im Anhang.

1.2.1 Definition. Seien A und B Mengen. Eine Teilmenge R des kartesischen Produktes $A \times B$ heißt *Relation* zwischen A und B. ∥

Ist $x \in A$, $y \in B$ und gilt $(x, y) \in R$, so schreibt man anstelle von $(x, y) \in R$ oft auch xRy.

1.2.2 Beispiel.

(*i*) Die *Teilbarkeitsrelation* in $\mathbb{N}$: Sei R die Teilmenge von $\mathbb{N}^2$ definiert durch

$$R := \big\{(x, y) \in \mathbb{N}^2 : x|y\big\}.$$

Elemente von R sind zum Beispiel $(2, 8)$ oder $(1, 5)$. Paare die nicht zu R gehören wären zum Beispiel $(3, 4)$ oder $(2, 5)$.

(*ii*) Die *Ordnungsrelation auf* $\mathbb{N}$: Bezeichne $\leq$ die Relation auf $\mathbb{N}$, die definiert ist als

$$\leq := \big\{(x, y) \in \mathbb{N}^2 : x \leq y\big\}.$$

(*iii*) Die *Gleichheitsrelation* auf einer Menge: Sei M irgendeine Menge, und Δ die Relation

$$\Delta := \big\{(x, y) \in M^2 : x = y\big\}.$$

(*iv*) Die *Elementrelation*: Sei M eine Menge, und bezeichne $\in$ die Relation

$$\in := \big\{(x, y) \in M \times \mathcal{P}(M) : x \in y\big\}$$

Anhand dieser Beispiele wird auch klar warum man oft die Schreibweise xRy der mengentheoretischen Notation $(x, y) \in R$ vorzieht. ∥

Relationen kann man in mannigfaltiger Weise miteinander verknüpfen. Wir wollen hier zwei Operationen anführen: die *Komposition* von Relationen und die *Umkehrrelation* einer Relation. Sind $A \subseteq M \times N$ und $B \subseteq N \times P$, so bezeichnet $B \circ A \subseteq M \times P$ die Relation

$$B \circ A := \big\{(x, z) \in M \times P :\ \exists y \in N : (x, y) \in A, (y, z) \in B\big\}.$$

Die Relation $B \circ A$ heißt die Komposition (oder Hintereinanderausführung, oder Zusammensetzung) der Relationen A und B. Offenbar gilt für Relationen $A \subseteq M \times N, B \subseteq N \times P, C \subseteq P \times Q$ stets

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

$$= \big\{(x, s) \in M \times Q :\ \exists y \in N\, \exists z \in P : (x, y) \in A \wedge (y, z) \in B \wedge (z, s) \in C\big\},$$

d.h. die Komposition von Relationen ist assoziativ. Wieder schreiben wir abkürzend $A^n := \underbrace{A \circ \ldots \circ A}_{n\text{-mal}}$.

Ist $A \subseteq M \times N$ eine Relation, so bezeichnet

$$A^{-1} := \big\{(x, y) \in N \times M : (y, x) \in A\big\}$$

die Umkehrrelation von A (manchmal spricht man auch von der inversen Relation).

Der Begriff der Relation ist sehr allgemein. Relationen mit speziellen zusätzlichen Eigenschaften spielen oft eine bedeutende Rolle. Prominente Beispiele dafür sind die Funktionen, oder die im folgenden Abschnitt behandelten Äquivalenzrelationen bzw. Ordnungsrelationen.

1.2.3 Definition. Seien M und N Mengen. Eine Relation $F \subseteq M \times N$ heißt eine *Funktion* von M nach N, wenn gilt

(i) $\forall x \in M\, \exists y \in N : (x, y) \in F$,

(ii) $\big[(x, y_1) \in F \wedge (x, y_2) \in F\big] \Rightarrow y_1 = y_2$.

//

Die Bedingung (i) besagt, dass jedem x (mindestens) ein Funktionswert y zugeordnet wird, man sagt auch F sei *überall definiert*. Die Bedingung (ii) besagt das jedem $x \in M$ höchstens ein Funktionswert zugeordnet wird. Man sagt auch F sei *wohldefiniert*. Insgesamt hat man also: Eine Funktion von M nach N ist eine (wie auch immer geartete) Vorschrift durch die jedem Element x aus der Menge M in eindeutiger Weise ein Element y aus der Menge N zugeordnet wird. Man bezeichnet y als den *Funktionswert* von F an der Stelle x, und schreibt auch $F(x)$ für jenes Element y mit $(x, y) \in F$. Anstelle des Namens „Funktion“ gebraucht man auch den Namen *Abbildung*. Diese Begriffe bedeuten üblicherweise das Gleiche.

Da für eine Funktion der einem Wert zugeordnete Funktionswert ja eindeutig bestimmt ist, schreibt man eine Funktion F von M nach N auch oft an als

$$F : \left\{ \begin{array}{ccc} M & \to & N \\ x & \mapsto & F(x) \end{array} \right.$$

1.2.4 Beispiel. Die oben besprochene Teilbarkeitsrelation ist keine Funktion. Denn es gilt zwar (i) aus Definition 1.2.3, nicht jedoch (ii). Dagegen ist die Gleichheitsrelation sehr wohl eine Funktion. Man bezeichnet diese auch oft als die *identische Abbildung* auf der Menge M und schreibt dafür id_M. D.h. $\mathrm{id}_M : M \to M$ mit $\mathrm{id}_M(x) = x$.

Sind M, N Mengen und ist $y \in N$, so ist die Relation $M \times \{y\}$ eine Funktion. Man spricht von der *konstanten Funktion* y. //

1.2.5 Bemerkung. In manchem Zusammenhang betrachtet man auch Funktionen die nicht überall definiert sind. Das sind Relationen die nur die Eigenschaft (ii) aus Definition 1.2.3 haben, das es also zu jedem Wert $x \in M$ höchstens einen Funktionswert (d.h. keinen oder genau einen) $y \in N$ gibt. Man muß dann zusätzlich den *Definitionsbereich* der Funktion angeben. Betrachte zum Beispiel die Relation

$$F := \big\{(x, y) \in \mathbb{N}^2 : x = 2y\big\}. \tag{1.2.1}$$

Offenbar ist dieses F eine nur auf der Menge der geraden Zahlen definierte Funktion. //

Den Definitionsbereich (oder *domain*) einer Funktion F von M nach N bezeichnet man auch mit $\operatorname{dom} F$, den *Wertebereich* (oder *range*) von F, das ist die Menge $\{y \in N : \exists x \in M : (x, y) \in F\}$ mit $\operatorname{ran} F$. Ist $y \in N$, und $x \in M$ sodaß $y = F(x)$, so bezeichnet man x als ein *Urbild* von y. Ein Element y kann viele Urbilder haben, kann aber auch kein Urbild haben (nämlich wenn $y \notin \operatorname{ran} F$). Das *vollständige Urbild* einer Teilmenge B von N ist die Menge

$$F^{-}(B) := \big\{x \in M : F(x) \in B\big\}.$$

Für eine Funktion $F : M \to N$ ist also F^{-} eine Funktion von $\mathcal{P}(N)$ nach $\mathcal{P}(M)$.

Die Umkehrrelation einer Funktion muß nicht notwendiger Weise wieder eine Funktion sein. Sie muß nicht einmal eine nicht überall definierte Funktion sein. Betrachte zum Beispiel die konstante Funktion

$$F := \{(x, y) \in \mathbb{N}^2 : y = 1\},$$

von $\mathbb{N}$ nach $\mathbb{N}$. Die Umkehrrelation F^{-1} ist gleich der Menge aller Paare $(1, n)$, $n \in \mathbb{N}$, und kann daher keine (wo auch immer definierte) Funktion sein. Manchmal jedoch ist die Umkehrrelation eine nicht überall definierte Funktion, zum Beispiel ist die Relation F aus (1.2.1) die Umkehrrelation der Funktion

$$G := \{(x, y) \in \mathbb{N}^2 : y = 2x\}.$$

Wir wollen die Beziehungen zwischen Umkehrrelationen und Funktionen näher untersuchen.

1.2.6 Definition. Sei $F : M \to N$ eine Funktion.

(*i*) F heißt *injektiv*, wenn gilt

$$F(x_1) = F(x_2) \;\Rightarrow\; x_1 = x_2,$$

d.h. zu jedem Wert $y \in N$ gibt es höchstens ein Urbild.

(*ii*) F heißt *surjektiv*, wenn gilt

$$\forall y \in N\, \exists x \in M : F(x) = y,$$

oder äquivalent ausgedrückt: $\forall x : F^{-}(\{x\}) \neq \emptyset$. D.h. also, daß jedes Element von N wirklich als Funktionswert von F auftritt, äquivalent ausgedrückt $\operatorname{ran} F = N$.

Weiters bezeichnet man eine Funktion, die sowohl injektiv als auch surjektiv ist als *bijektiv*. //

Eine bijektive Funktion tut also nichts anderes als die Elemente der Menge M so umzubenennen, dass die Menge N entsteht.

1.2.7 Proposition. *Sei F eine Funktion von M nach N.*

(*i*) *Ist F bijektiv, so ist die Umkehrrelation F^{-1} eine Funktion von N nach M.*

(*ii*) *Ist F injektiv, so ist die Umkehrrelation F^{-1} eine (möglicherweise nicht überall definierte) Funktion. Es gilt* $\operatorname{dom} F^{-1} = \operatorname{ran} F$.

Beweis. Offenbar ist (*i*) der Spezialfall surjektiver Funktionen in (*ii*).

Um (*ii*) einzusehen, seien $(y, x_1), (y, x_2) \in F^{-1}$ gegeben. Dann ist $(x_1, y), (x_2, y) \in F$ und wegen der Injektivität von F folgt $x_1 = x_2$. Weiters existiert zu einem $y \in N$ ein Element $x \in M$ mit $y = F(x)$, genau dann wenn $y \in \operatorname{ran} F$. ❑

1.2.8 Bemerkung. Ist F nicht injektiv, so ist die Relation F^{-1} nicht einmal mehr eine nicht überall definierte Funktion. Denn existieren $x_1, x_2 \in M$, $x_1 \neq x_2$, und $y \in N$ mit $(x_1, y), (x_2, y) \in F$, dann ist $(y, x_1), (y, x_2) \in F^{-1}$. Also ist die Eigenschaft (*ii*) von Definition 1.2.3 nicht erfüllt. //

Durch unmittelbares Nachprüfen der Definition erhält man die folgende Aussage[4]:

1.2.9 Proposition. *Seien $F : M \to N$ und $G : N \to P$ Funktionen. Dann ist*

$$G \circ F : M \to P$$

ebenfalls eine Funktion. Es gilt $(G \circ F)(x) = G(F(x))$, $x \in M$. Man bezeichnet $G \circ F$ oft auch als die zusammengesetzte Funktion. ❑

1.2.10 Bemerkung. Sind F und G nicht mehr überall definiert, so muß man bei der Komposition darauf achten, daß die Definitionsbereiche zusammenpassen. Obwohl der Begriff der Komposition von Relationen stets sinnvoll ist, wird oft nur dann von einer zusammengesetzten Funktion $G \circ F$ gesprochen, wenn $\operatorname{dom} G \supseteq \operatorname{ran} F$ gilt. //

1.2.11 Satz. *Eine Funktion $F : M \to N$ ist genau dann bijektiv, wenn es eine Funktion $G : N \to M$ gibt mit*

$$G \circ F = \mathrm{id}_M, \ F \circ G = \mathrm{id}_N .$$

In diesem Fall gilt $G = F^{-1}$.

Beweis. Sei zunächst F bijektiv. Offenbar gilt

$$(F^{-1} \circ F)(x) = x, \ x \in M, \text{ und } (F \circ F^{-1})(y) = y, \ y \in N.$$

Also hat die Funktion F^{-1} alle im Satz geforderten Eigenschaften.

Sei nun die Existenz einer Funktion G mit den genannten Eigenschaften vorausgesetzt. Ist $y \in N$, so setze $x = G(y)$, dann gilt $F(x) = y$. D.h. F ist surjektiv. Ist $F(x_1) = F(x_2)$, so folgt

$$x_1 = G(F(x_1)) = G(F(x_2)) = x_2,$$

also ist F auch injektiv. ❑

Mit Hilfe des Funktionsbegriffs kann man nun auch das kartesische Produkt einer beliebigen Familie von Mengen erklären.

[4] Prüfe nach!

1.2.12 Definition. Sei M_i, $i \in I$, eine Familie von Mengen. Als *kartesisches Produkt* $\prod_{i\in I} M_i$ bezeichnet man die Menge aller Funktionen

$$F : I \to \bigcup_{i\in I} M_i,$$

mit der Eigenschaft $F(i) \in M_i$ für alle $i \in I$. //

Ist eine der Mengen M_i leer, so ist offenbar auch das Produkt $\prod_{i\in I} M_i$ leer. Das, soferne alle Mengen M_i nichtleer sind, auch $\prod_{i\in I} M_i$ nichtleer ist, ist nicht klar. Tatsächlich muß man dies als Axiom fordern, das ist das sogenannte *Auswahlaxiom*:

(Auswahlaxiom) Gegeben eine Indexmenge I und eine Familie von nichtleeren Mengen M_i, $i \in I$, so existiert eine Funktion (*Auswahlfunktion*) $f : I \to \bigcup_{i\in I} M_i$, sodass $f(i) \in M_i$.

Wir werden immer an die Gültigkeit dieses Axioms glauben.

1.2.13 Beispiel.

(*i*) Das kartesische Produkt

$$2^M := \prod_{i\in M} \{0, 1\}$$

ist die Menge aller Funktionen von M in $\{0, 1\}$. Es ist (bis auf Umbenennung) nichts anderes als die Potenzmenge von M: Die Funktion

$$\lambda : \left\{ \begin{array}{ccc} 2^M & \to & \mathcal{P}(M) \\ F & \mapsto & F^-(\{1\}) \end{array} \right.$$

ist bijektiv.

(*ii*) Das kartesische Produkt

$$(2\mathbb{N})^{\mathbb{N}} := \prod_{i\in\mathbb{N}} (2\mathbb{N})$$

ist die Menge aller Abbildungen $F : \mathbb{N} \to (2\mathbb{N})$. Also nichts anderes als die Menge aller Folgen $(c_1, c_2, c_3, \ldots) = (c_n)_{n\in\mathbb{N}}$ deren Folgenglieder gerade natürliche Zahlen sind.

//

1.3 Äquivalenz- und Ordnungsrelationen

1.3.1 Definition. Sei M eine Menge und $R \subseteq M \times M$ eine Relation. R heißt *Äquivalenzrelation* wenn sie die folgenden Eigenschaften besitzt:

(Reflexiv) $\forall x \in M : (x, x) \in R$

(Symmetrisch) $(x, y) \in R \Rightarrow (y, x) \in R$

(Transitiv) $(x, y), (y, z) \in R \Rightarrow (x, z) \in R$

Ist R eine Äquivalenzrelation, so definiert man die *Äquivalenzklasse* eines Elementes x als

$$[x]_R := \big\{y \in M : yRx\big\}.$$

//

1.3.2 Beispiel.

(i) Das wohl grundlegenste Beispiel einer Äquivalenzrelation ist die Gleichheitsrelation Δ. Die Eigenschaften aus Definition 1.3.1 modellieren genau die wesentlichen Eigenschaften des Begriffes der Gleichheit.

(ii) Sei $r \in \mathbb{N}$. Definiere eine Relation auf den natürlichen Zahlen $\mathbb{N}$ durch[5]

$$(x, y) \in \text{ mod } r \ :\Longleftrightarrow\ x = y \text{ oder } x < y \wedge r|(y - x) \text{ oder } y < x \wedge r|(x - y)$$

Für $(x, y) \in \text{ mod } r$ schreibt man auch $x \equiv y \text{ mod } r$.

Diese Relation ist eine Äquivalenzrelation. Sie ist reflexiv, denn nach Definition gilt für jedes $x \in \mathbb{N}$, dass $(x, x) \in \text{ mod } r$. Sie ist auch symmetrisch, denn ist zum Beispiel $x < y$, $(x, y) \in \text{ mod } r$, so folgt $(x', y') := (y, x) \in \text{ mod } r$, denn $y' < x'$ und $r|(x' - y')$.

Um zu sehen dass sie auch transitiv ist, seien $x \equiv y \text{ mod } r$ und $y \equiv z \text{ mod } r$ gegeben. Betrachte zum Beispiel den Fall dass $x < y$ und $y < z$. Dann muss also $r|(y - x)$ und $r(z - y)$ gelten. Es folgt, dass $x < z$ und $r|[(z - y) + (y - x)] = (z - x)$. D.h. wir haben auch $x \equiv z \text{ mod } r$. Die anderen Fälle behandelt man genauso.

//

Äquivalenzrelationen treten überall dort auf, wo man gewisse Elemente einer Menge als gleich betrachten möchte. So wie man in Beispiel 1.3.2, (ii), Zahlen identifiziert, wenn sie sich nur um ein Vielfaches von r unterscheiden. Jene Elemente welche man als gleich betrachtet fasst man zu den Klassen $[x]_R$ zusammen. Dann erhält man, wie wir im nächsten Satz sehen werden, eine Zerlegung der Menge in paarweise disjunkte Klassen.

1.3.3 Definition. Sei M eine Menge. Eine Teilmenge K der Potenzmenge $\mathcal{P}(M)$ heißt *Klasseneinteilung* der Menge M, wenn sie die folgenden Eigenschaften besitzt:

- $\forall\, A \in K :\ A \neq \emptyset$,
- $\bigcup_{A \in K} A = M$,
- $\big[A, B \in K, A \neq B\big] \Rightarrow A \cap B = \emptyset$.

//

[5]Das Symbol „$:\Longleftrightarrow$ “ bedeutet, dass die linke Seite (jene mit dem Doppelpunkt) nach Definition genau dann gilt, wenn die rechte Seite gilt.

1.3.4 Satz. *Sei R eine Äquivalenzrelation auf der Menge M. Dann ist die Menge*

$$K(R) := \big\{[x]_R : x \in M\big\} \subseteq \mathcal{P}(M) \tag{1.3.1}$$

eine Klasseneinteilung von M. Ist umgekehrt K irgendeine Klasseneinteilung von M, so ist

$$R(K) := \big\{(x,y) \in M^2 : \exists A \in K : x,y \in A\big\} \tag{1.3.2}$$

eine Äquivalenzrelation auf M. Die Zuordnungen $R \mapsto K(R)$ und $K \mapsto R(K)$ zwischen den Mengen aller Äquivalenzrelationen auf M bzw. aller Klasseneinteilungen von M sind zueinander invers. D.h. die zur Äquivalenzrelation $R(K)$ gehörige Klasseneinteilung $K(R(K))$ ist wieder K selbst, und die zur Klasseneinteilung $K(R)$ gehörende Äquivalenzrelation $R(K(R))$ ist wieder R selbst.

Beweis. Sei zunächst eine Äquivalenzrelation R gegeben. Betrachte die Menge (1.3.1). Wegen der Reflexivität von R gilt stets $x \in [x]_R$, also ist sicher $[x]_R \neq \emptyset$ und $\bigcup_{A\in K(R)} A = M$. Seien nun $A, B \in K(R)$, $A = [x_1]_R$, $B = [x_2]_R$, und sei $A \cap B \neq \emptyset$. Dann existiert also ein Element $z \in [x_1]_R \cap [x_2]_R$, d.h. $(z,x_1),(z,x_2) \in R$. Wegen der Symmetrie und der Transitivität von R folgt $x_1 R x_2$. Ist nun $y \in [x_1]_R$, d.h. $(y,x_1) \in R$, so folgt wegen der Transitivität auch $(y,x_2) \in R$, d.h. $y \in [x_2]_R$. Wir haben also $[x_1]_R \subseteq [x_2]_R$. Sei andererseits $y \in [x_2]_R$, d.h. $(y,x_2) \in R$. Wegen der Symmetrie gilt $(x_2,x_1) \in R$, und wir schliessen dass $y \in [x_1]_R$. Es folgt, dass auch $[x_2]_R \subseteq [x_1]_R$. Also ist $K(R)$ eine Klasseneinteilung von M.

Sei nun umgekehrt K eine Klasseneinteilung. Die durch (1.3.2) definierte Relation ist reflexiv, denn ist $x \in M$ so existiert $A \in K$ mit $x \in A$. Die Symmetrie ist offensichtlich. Seien nun $x,y,z \in M$, $xR(K)y$, $yR(K)z$. D.h. es existieren $A, B \in K$ mit $x,y \in A$ und $y,z \in B$. Dann ist $y \in A \cap B$, und es folgt $A = B$. Also gilt auch $xR(K)z$.

Sei nun wieder K eine Klasseneinteilung, und betrachte die zur Relation $R(K)$ assoziierte Klasseneinteilung $K(R(K))$. Sei $x \in M$ und $A_0 \in K$ jene Menge der Klasseneinteilung K welche x enthält. Dann gilt

$$y \in [x]_{R(K)} \iff yR(K)x \iff \exists A \in K : x,y \in A \iff y \in A_0$$

d.h. $[x]_{R(K)} = A_0$. Also ist $K(R(K) = K$.

Es bleibt zu zeigen, daß für eine Äquivalenzrelation R stets $R(K(R)) = R$ gilt. Nun ist

$$(x,y) \in R(K(R)) \iff \exists A \in K(R) : x,y \in A \iff y \in [x]_R \iff (x,y) \in R$$

❑

Klasseneinteilungen und Äquivalenzrelationen sind also äquivalente Begriffsbildungen; beide beschreiben das Identifizieren gewisser Elemente einer Menge.

Die zu einer Äquivalenzrelation R assoziierte Klasseneinteilung $K(R)$ ist gerade die Menge der (verschiedenen) Äquivalenzklassen. Diese Menge nennt man *Faktormenge* von M modulo R und schreibt M/R. Die Abbildung $\pi : M \to M/R$, welche jedem Element $x \in M$ die Äquivalenzklasse $[x]_R$ zuordnet heißt *kanonische Projektion*.

Geht man von der Vorstellung aus, daß die Äquivalenzklassen jene Elemente zusammenfassen welche man ohnehin als gleich betrachten möchte, so braucht man um die ganze Menge im Griff zu haben natürlich aus jeder Klasse nur ein einziges Element zu kennen.

1.3.5 Definition. Sei R eine Äquivalenzrelation. Eine Teilmenge $L \subseteq M$ heißt *vollständiges Repräsentantensystem* für R, wenn sie aus jeder Äquivalenzklasse genau ein Element enthält. //

1.3.6 Beispiel. Betrachte wieder die Relationen aus Beispiel 1.3.2.

(i) Sei Δ wieder die Gleichheitsrelation auf einer Menge M. Für ein beliebiges Element $x \in M$ gilt $y \Delta x$ genau dann, wenn $y = x$ ist. Also haben wir $[x]_\Delta = \{x\}$. Die Faktormenge M/Δ kann in natürlicher Weise mit M identifiziert werden, nämlich vermöge der kanonische Projektion. Denn diese operiert als $x \mapsto \{x\}$, und ist daher bijektiv. Ein vollständiges Representantensystem für Δ, ist gegeben durch M selbst.

(ii) Betrachte nun die Äquivalenzrelation $\bmod r$. Ist $x \in \mathbb{N}$, so ist die Äquivalenzklasse $[x]_{\bmod r}$ gegeben als[6]

$$[x]_{\bmod r} = \big\{y \in \mathbb{N} : y \text{ läßt bei Division durch } r \text{ den gleichen Rest wie } x\big\}.$$

Die zugehörige Klasseneinteilung besteht aus den Mengen

$$K_i := \{i, i+r, i+2r, \ldots\},\ i = 1, \ldots, r.$$

Die Menge $\{1, \ldots, r\}$ ist demnach ein Beispiel eines vollständigen Representantensystems für $\bmod r$. Ein anderes Beispiel für ein vollständiges Representantensystem wäre $\{1, 2+3r, \ldots, 5r\}$ o.ä. Die Faktormenge ist gleich

$$\mathbb{N}/\bmod r = \{K_0, K_1, \ldots, K_{r-1}\}.$$

//

1.3.7 Definition. Sei M eine Menge, und $\preceq$ eine Relation auf M, d.h. $\preceq$ ist eine Teilmenge von $M \times M$. Dann heißt $\preceq$ eine *Ordnungsrelation* auf M, wenn sie die folgenden Eigenschaften hat:

(Reflexiv) $\forall x \in M : x \preceq x.$

(Antisymmetrisch) $\big[x \preceq y \wedge y \preceq x\big] \Rightarrow x = y.$

(Transitiv) $\big[x \preceq y \wedge y \preceq z\big] \Rightarrow x \preceq z.$

Man spricht manchmal auch von einer *Halbordnung*.

Eine Halbordnung $(M, \preceq)$ heißt *Totalordnung*, falls je zwei Elemente vergleichbar sind, d.h.

$$x, y \in M \Rightarrow \big[x \preceq y \vee y \preceq x\big].$$

//

1.3.8 Beispiel.

[6] Wir verwenden in diesem Beispiel schon die spätere Proposition 2.4.1.

(*i*) Die Teilbarkeitsrelation auf $\mathbb{N}$ und die Ordnungsrelation auf $\mathbb{N}$ sind Ordnungsrelationen. Erstere ist keine Totalordnung, denn zum Beispiel gilt weder $2|3$ noch $3|2$. Zweitere dagegen ist sehr wohl eine Totalordnung, denn für zwei natürliche Zahlen gilt entweder $x \leq y$ oder $y \leq x$.

(*ii*) Für jede Menge M ist die Gleichheitsrelation eine Ordnungsrelation.

(*iii*) Sei M irgendeine Menge, und betrachte die *Inklusionsrelation* auf der Potenzmenge $\mathcal{P}(M)$, das ist die Relation

$$\subseteq := \big\{(A, B) \in \mathcal{P}(M) \times \mathcal{P}(M) : A \subseteq B\big\}.$$

Diese Relation ist eine Ordnungsrelation.

//

Schliesslich wollen wir noch ein paar Begriffe betreffend Ordnungsrelationen definieren.

1.3.9 Definition. Sei $\preceq$ eine Ordnungsrelation auf der Menge M und sei $L \subseteq M$.

(*i*) Ein Element $y \in M$ heißt *obere Schranke* von L, falls $x \preceq y$ für alle $x \in L$. Es heißt in analoger Weise *untere Schranke* von L, falls $y \preceq x$ für alle $x \in L$.

(*ii*) Ein Element $y \in M$ heißt *Supremum* oder *kleinste obere Schranke*, wenn y eine obere Schranke von L ist, und für jede obere Schranke x von L gilt das $y \preceq x$. Es heißt *Infimum* oder *größte untere Schranke*, wenn y eine untere Schranke von L ist, und für jede untere Schranke x von L gilt $x \preceq y$.

(*iii*) Ein Element $m \in L$ heißt *maximales Element* von L, falls aus $x \in L \wedge m \preceq x$ folgt das $x = m$. Analog heißt m *minimales Element*, wenn aus $x \in L \wedge x \preceq m$ stets $x = m$ folgt.

(*iv*) Ein Element m heißt *größtes Element* von L wenn $m \in L$ und $x \preceq m$ für alle $x \in L$, sowie *kleinstes Element* von L falls $m \in L$ und $m \preceq x$ für alle $x \in L$.

//

1.3.10 Definition. Sei $\preceq$ eine Ordnungsrelation auf der Menge M.

(*i*) Wir sagen $\preceq$ hat die *Supremumseigenschaft*, wenn jede nichtleere und nach oben beschränkte Teilmenge von M ein Supremum besitzt.

(*ii*) Wir sagen $\preceq$ hat die *Imfimumseigenschaft*, wenn jede nichtleere und nach unten beschränkte Teilmenge von M ein Infimum besitzt.

(*iii*) Wir sagen $\preceq$ ist eine Wohlordnung, wenn jede nichtleere Teilmenge von M ein minimales Element besitzt.

//

Kapitel 2

Ganze und rationale Zahlen

Im Bereich der natürlichen Zahlen haben wir die beiden Operationen $+$ und $\cdot$ der Addition und Multiplikation kennengelernt. In manchen Fällen lassen sich diese umkehren, zum Beispiel kann man ja, wenn $n > m$ ist, die Subtraktion $n-m$ durchführen. Divisionen, wie z.B. $12 : 3 = 4$, lassen sich noch viel seltener durchführen. Zum Beispiel ist nicht möglich $3 : 2$ auszurechnen, denn es gibt keine natürliche Zahl x mit $2x = 3$.

Diese Tatsachen nehmen wir zum Anlass unser Zahlensystem erweitern zu wollen.

2.1 Die ganzen Zahlen

Zunächst wollen wir den Mangel beseitigen dass man im allgemeinen nicht subtrahieren kann. Dazu konstruieren wir ein neues „Zahlensystem“ welches die natürlichen Zahlen umfasst und in dem die Subtraktion unbeschränkt durchführbar ist. Um dieses zu erreichen definieren wir einfach die „Differenzen $n - m$“ als neue Zahlen. Dabei haben wir natürlich zu beachten, dass zwei Differenzen $n - m$ und $n' - m'$ auch gleich sein können obwohl n und n' bzw. m und m' verschieden sind, zum Beispiel ist ja $5 - 2 = 7 - 4$.

Sei $\sim \subseteq (\mathbb{N} \times \mathbb{N})^2$ die Relation

$$(x, n) \sim (y, m) \;:\Longleftrightarrow\; x + m = y + n\,.$$

2.1.1 Lemma. *Die Relation $\sim$ ist eine Äquivalenzrelation.*

Beweis. Die Reflexivität und Symmetrie ist klar. Um zu zeigen dass $\sim$ transitiv ist, seien $(x, n) \sim (y, m)$ und $(y, m) \sim (z, k)$ gegeben. Dann gilt $x + m = y + n$ und $y + k = z + m$. Es folgt

$$(x+k)+m = (x+m)+k = (y+n)+k = (y+k)+n = (z+m)+n = (z+n)+m\,,$$

und wegen der Kürzungsregel daher $x + k = z + n$, d.h. $(x, n) \sim (z, k)$. ❑

2.1.2 Definition. Wir bezeichnen die Faktormenge $(\mathbb{N} \times \mathbb{N})/_\sim$ mit $\mathbb{Z}$, und sprechen von dem Ring der *ganzen Zahlen*. //

Wir wollen auf $\mathbb{Z}$ algebraische Operationen „$+$“ und „$\cdot$“, sowie eine Ordnungsrelation „$\leq$“ definieren. Die Vorgangsweise dazu ist zunächst Addition, Multiplikation und Ordnung auf $\mathbb{N} \times \mathbb{N}$ zu definieren, und diese dann mit Hilfe der kanonischen Projektion auf $\mathbb{Z}$ zu übertragen.

Um zu sehen wie wir solche Operationen/Ordnung auf $\mathbb{N} \times \mathbb{N}$ definieren könnten damit auch das herauskommt was herauskommen soll, tun wir einmal so als ob man immer mit Differenzen umgehen dürfte wie man es sich erwartet, und machen ein paar formale Rechnungen:

$$\begin{aligned}
&(x-n)+(y-m) = (x+y)-(n+m)\\
&(x-n)\cdot(y-m) = xy-ny-xm+nm = (xy+nm)-(xm+ny)\\
&x-n \leq y-m \iff x+m \leq y+n
\end{aligned}$$

Diese Rechnungen machen natürlich im allgemeinen keinen Sinn, es ist ja gerade unser Problem dass man nicht immer Differenzen bilden kann, aber sie motivieren die folgende Definition.

2.1.3 Definition. Es seien Abbildungen $+ : (\mathbb{N}\times\mathbb{N})^2 \to \mathbb{N}\times\mathbb{N}$, $\cdot : (\mathbb{N}\times\mathbb{N})^2 \to \mathbb{N}\times\mathbb{N}$ und eine Relation $\leq$ auf $\mathbb{N}\times\mathbb{N}$ definiert als $((x,n),(y,m) \in \mathbb{N}\times\mathbb{N})$

$$\begin{aligned}
(x,n)+(y,m) &:= (x+y, n+m)\\
(x,n)\cdot(y,m) &:= (xy+nm, xm+ny)\\
(x,n) \leq (y,m) &:\iff x+m \leq y+n
\end{aligned}$$

//

2.1.4 Lemma. *Die Operationen „$+$“ und „$\cdot$“ auf $\mathbb{N}\times\mathbb{N}$ sind kommutativ, assoziativ und es gilt das Distributivitätsgesetz von „$\cdot$“ über „$+$“.*

Die Relation $\leq$ auf $\mathbb{N}\times\mathbb{N}$ ist reflexiv und transitiv. Ist $(x,n) \leq (y,m)$ und $(y,m) \leq (x,n)$, so folgt $(x,n) \sim (y,m)$.

Beweis. Seien $(x,n),(y,m) \in \mathbb{N}\times\mathbb{N}$. Dann ist

$$(x,n)+(y,m) = (x+y, n+m) = (y+x, m+n) = (y,m)+(x,n)\,,$$

$$(x,n)\cdot(y,m) = (xy+nm, xm+ny) = (yx+mn, yn+mx) = (y,m)\cdot(x,n)\,.$$

Sei zusätzlich $(z,k) \in \mathbb{N}\times\mathbb{N}$. Dann gilt

$$\big((x,n)+(y,m)\big)+(z,k) = (x+y,n+m)+(z,k) = \big((x+y)+z,(n+m)+k\big) =$$

$$= \big(x+(y+z), n+(m+k)\big) = (x,n)+\big((y,m)+(z,k)\big)\,.$$

Die Gültigkeit der Assoziativität der Multiplikation sowie des Distributivgesetzes rechnet man in genau der gleichen Weise (nur deutlich mühsamer) nach.

Wir kommen zu den Eigenschaften der Relation $\leq$. Die Reflexivität folgt unmittelbar aus der Definition. Sei nun $(x,n) \leq (y,m)$ und $(y,m) \leq (z,k)$. Dann gilt $x+m \leq y+n$ und $y+k \leq z+m$, und wir erhalten

$$(x+k)+m = (x+m)+k \leq (y+n)+k = (y+k)+n \leq (z+m)+n = (z+n)+m\,.$$

Daraus folgt nun das $x+k \leq z+n$, d.h. $(x,n) \leq (z,k)$. Schliesslich sei $(x,n) \leq (y,m)$ und $(y,m) \leq (x,n)$. Dann gilt also $x+m \leq y+n$ und $y+n \leq x+m$, und wir erhalten $x+m = y+n$, d.h. $(x,n) \sim (y,m)$. ❑

Um diese Operationen/Ordnung auf $\mathbb{Z}$ übertragen zu können benötigen wir eine gewisse Verträglichkeit mit der Relation $\sim$.

2.1.5 Lemma. *Seien $(x,n) \sim (x',n')$ und $(y,m) \sim (y',m')$. Dann folgt, dass*

$$\begin{aligned}(x,n)+(y,m) &\sim (x',n')+(y',m')\\ (x,n)\cdot(y,m) &\sim (x',n')\cdot(y',m')\\ (x,n) \le (y,m) &\iff (x',n') \le (y',m)\end{aligned}$$

Beweis. Seien $(x,n) \sim (x',n')$ und $(y,m) \sim (y',m')$ gegeben. Dann gilt

$$(x+y)+(n'+m') = (x+n')+(y+m') = (x'+n)+(y'+m) = (x'+y')+(n+m)\,,$$

und wir sehen das $(x,n)+(y,m) \sim (x',n')+(y',m')$.

Um die Aussage für $\cdot$ zu zeigen, betrachten wir zuerst $(x,n) \sim (x',n')$ und ein (y,m). Dann gilt

$$(xy+nm)+(x'm+n'y) = (x+n')y+(x'+n)m =$$

$$= (x'+n)y+(x+n')m = (x'y+n'm)+(xm+ny)\,,$$

und wir erhalten $(x,n)\cdot(y,m) \sim (x',n')\cdot(y,m)$. Wegen der Kommutativität von $\cdot$ folgt auch dass für (x,n) und $(y,m) \sim (y',m')$ stets $(x,n)\cdot(y,m) \sim (x,n)\cdot(y',m')$ gilt. Insgesamt erhalten wir dass für $(x,n) \sim (x',n')$ und $(y,m) \sim (y',m')$ gilt

$$(x,n)\cdot(y,m) \sim (x',n')\cdot(y,m) \sim (x',n')\cdot(y',m')\,.$$

Die Aussage über $\le$ folgt unmittelbar aus der Definition. ❑

2.1.6 Definition. Seien $a,b \in \mathbb{Z}$ gegeben. Dann definieren wir $a+b$, $a\cdot b$ sowie $a \le b$ wie folgt: Wähle $(x,n),(y,m) \in \mathbb{N}\times\mathbb{N}$ mit $[(x,n)]_\sim = a$ und $[(y,m)]_\sim = b$, und setze

$$\begin{aligned}a+b &:= \big[(x,n)+(y,m)\big]_\sim\\ a\cdot b &:= \big[(x,n)\cdot(y,m)\big]_\sim\\ a \le b &:\iff (x,n) \le (y,m)\end{aligned}$$

Wegen der Verträglichkeitsaussage Lemma 2.1.5 sind durch diese Vorschriften tatsächlich Funktionen $+,\cdot : \mathbb{Z}^2 \to \mathbb{Z}$, und eine Relation $\le$ auf $\mathbb{Z}$ wohldefiniert, denn der Wert der rechten Seiten hängt ja nicht von der Wahl der jeweiligen Representanten (x,n) bzw. (y,m) ab. //

Die wesentlichen Rechenregeln für die Objekte aus $\mathbb{Z}$ sind im folgenden Satz zusammengestellt.

2.1.7 Satz (Rechenregeln für $\mathbb{Z}$)**.** *Für die Operationen/Ordnung auf $\mathbb{Z}$ gelten die folgenden Rechenregeln:*

(*i*) *Die Addition ist assoziativ und kommutativ. Das Element $0 := [(1,1)]_\sim$ ist neutrales Element bezüglich der Addition. Jedes Element besitzt ein additives Inverses.*

(*ii*) *Die Multiplikation ist assoziativ und kommutativ. Das Element* $1 := [(2,1)]_\sim$ *ist neutrales Element bezüglich der Multiplikation. Es gilt die Kürzungsregel*

$$a \cdot c = b \cdot c \Rightarrow a = b, \quad a, b \in \mathbb{Z}, c \in \mathbb{Z} \setminus \{0\}\,.$$

(*iii*) *Es gilt das Distributivitätsgesetz von „·“ über „+“.*

(*iv*) *Die Relation „≤“ ist eine Totalordnung. Sie ist mit den Operationen „+“ und „·“ verträglich:*

$$\begin{aligned} &a \leq b \iff a + c \leq b + c, \quad a, b, c \in \mathbb{Z} \\ &a \leq b \Rightarrow a \cdot c \leq b \cdot c, \quad a, b, c \in \mathbb{Z}, c \geq 0 \\ &a \cdot c \leq b \cdot c \Rightarrow a \leq b, \quad a, b, c \in \mathbb{Z}, c > 0 \end{aligned}$$

(*v*) *Die natürlichen Zahlen sind in* $\mathbb{Z}$ *eingebettet vermöge der injektiven Abbildung*

$$\phi : \left\{ \begin{array}{ccc} \mathbb{N} & \to & \mathbb{Z} \\ x & \mapsto & [(x+1,1)]_\sim \end{array} \right.$$

Diese Abbildung erhält Addition, Multiplikation und Ordnung:

$$\phi(n+m) = \phi(n) + \phi(m),\ \phi(n \cdot m) = \phi(n) \cdot \phi(m),\ n \leq m \Leftrightarrow \phi(n) \leq \phi(m)$$

Beweis. Die Gültigkeit von Assoziativität, Kommutativität sowie Distributivität folgt wegen Lemma 2.1.4.

Sei $a = [(x,n)]_\sim \in \mathbb{Z}$. Dann gilt

$$a + 0 = [(x,n)]_\sim + [(1,1)]_\sim = [(x+1, n+1)]_\sim = [(x,n)]_\sim = a\,,$$

sowie

$$a \cdot 1 = [(x,n)]_\sim \cdot [(2,1)]_\sim = [(2x+n, x+2n)]_\sim = [(x,n)]_\sim = a\,,$$

also ist 0 neutrales Element der Addition und 1 neutrales Element der Multiplikation. Setze $a' := [(n,x)]_\sim$, dann gilt

$$a + a' = [(x,n)]_\sim + [(n,x)]_\sim = [(x+n, n+x)]_\sim = [(1,1)]_\sim = 0\,,$$

also hat a ein additives Inverses, nämlich a'.

Wegen Lemma 2.1.4 ist $\leq$ auf $\mathbb{Z}$ eine Ordnungsrelation. Da stets entweder $x + m \leq y + m$ oder $x + m \geq y + m$ gilt, folgt dass $\leq$ sogar eine Totalordnung ist.

Seien $a, b, c \in \mathbb{Z}$, $a = [(x,n)]_\sim, b = [(y,m)]_\sim, c = [(z,k)]_\sim$. Dann gilt

$$a+c \leq b+c \iff (x+z, n+k) \leq (y+z, m+k) \iff x+z+m+k \leq y+z+n+k$$

$$\iff x + m \leq y + n \iff a \leq b\,.$$

Sei nun angenommen das $a < b$, d.h. das $x + m < y + n$, und das $c \geq 0$, d.h. $z \geq k$. Dann gibt es $t \in \mathbb{N}$ mit $y + n = (x + m) + t$. Wegen $z \geq k$ folgt $tz \geq tk$ und daher auch $(y + n)z = (x + m)z + tz \geq (x + m)z + tk$ und schliesslich

$$(x + m)k + (y + n)z \geq (x + m)z + tk + (x + m)k = (x + m)z + (y + n)k\,.$$

Also haben wir $(xk+nz)+(yz+mk) \geq (xz+nk)+(yk+mz)$, und das heißt gerade $a \cdot c \leq b \cdot c$.

Sei umgekehrt $a \cdot c \leq b \cdot c$, d.h. nach obiger Rechnung $(x+m)k+(y+n)z \geq (x+m)z+(y+n)k$, und $c > 0$, d.h. $z > k$. Angenommen es wäre $a > b$, d.h. $x+m > y+n$. Dann gibt es $t \in \mathbb{N}$ mit $(y+n)+t = x+m$. Damit erhalten wir

$$tk+(y+n)(k+z) \geq tz+(y+n)(z+k)$$

und daraus $tk \geq tz$ und schließlich $k \geq z$, ein Widerspruch. Also gilt $a \leq b$. Die Kürzungsregel für $\cdot$ folgt aus der gerade bewiesenen für $\leq$.

Betrachte die Abbildung ϕ. Angenommen $(x+1,1) \sim (y+1,1)$, dann folgt $x+2 = y+2$, also $x = y$. D.h. ϕ ist injektiv. Es gilt

$$\phi(x)+\phi(y) = [((x+1)+(y+1),1+1)]_\sim = [((x+y)+1,1)]_\sim = \phi(x+y)\,,$$

$$\phi(x)\cdot\phi(y) = \big[((x+1)(y+1)+1,(x+1)+(y+1))\big]_\sim =$$

$$= \big[(xy+x+y+1+1,x+y+1+1)\big]_\sim = [(xy+1,1)]_\sim = \phi(xy)\,,$$

$$\phi(x) \leq \phi(y) \iff (x+1)+1 \leq (y+1)+1 \iff x \leq y\,.$$

❑

Die ganzen Zahlen könnten auch erhalten werden indem man zu den natürlichen Zahlen neue Objekte, nämlich eine „Null“ und „negativen Zahlen“ dazugibt.

2.1.8 Proposition. *Betrachte die Menge*

$$\widetilde{\mathbb{Z}} := \{\ldots,-2,-1,0,1,2,3,\ldots\}\,.$$

Eine Abbildung $\phi : \mathbb{Z} \to \widetilde{\mathbb{Z}}$ ist wohldefiniert durch die Vorschrift

$$[(x,n)]_\sim := \begin{cases} x-n & ,\ x > n \\ 0 & ,\ x = n \\ -(n-x) & ,\ x < n \end{cases}$$

Diese Abbildung ist bijektiv, und erhält Addition, Multiplikation und Ordnung[1].

Beweis. Die Wohldefiniertheit ist klar aus der Definition von $\sim$. Wir zeigen das die Menge $\{(1+k,1),(1,1),(1,1+k)\}$ ein vollständiges Representantensystem für $\sim$ in $\mathbb{N}\times\mathbb{N}$ ist. Dann folgt die Behauptung.

Sei $(x,n) \in \mathbb{N}\times N$. Ist $x > n$, so setze $k := x-n \in \mathbb{N}$. Dann gilt $(x,n) \sim (1+k,1)$. Ist $x = n$, so ist klarerweise $(x,n) \sim (1,1)$ und ist $x < n$, so setze $k := n-x$, dann folgt $(x,n) \sim (1,1+k)$. Die Tatsache dass keine zwei der angegebenen Elemente in der Relation $\sim$ stehen ist klar. ❑

[1] Man könnte zur Definition von $\mathbb{Z}$ also auch die, anschaulich viel vertrautere, Darstellung $\widetilde{\mathbb{Z}}$ heranziehen. Die Definition der Operationen/Ordnung sowie der Beweis der Rechenregeln, wäre dann aber, wegen vieler notwendiger Fallunterscheidungen, recht mühsam. Der hier gewählte Zugang zeigt uns obendrein auch noch ein allgemeines Konzept auf, welches wir gleich wieder anwenden können, nämlich die Verwendung von Äquivalenzrelationen.

2.2 Die rationalen Zahlen

Im Bereich der ganzen Zahlen kann man die Operation des Subtrahierens unbeschränkt ausführen. Auf die Multiplikation trifft dies jedoch noch immer nicht zu. Zum Beispiel gibt es keine Zahl $x \in \mathbb{Z}$ mit $2x = 3$, denn $2x$ durchläuft ja die Werte $..., -4, -2, 0, 2, 4, 6, ...$ Um zu erreichen, dass es Quotienten wie $3 : 2$ gibt, gehen wir analog vor wie bei der Konstruktion von $\mathbb{Z}$: Wir definieren „Quotienten $a : n$“ als neue Zahlen. Wieder haben wir zu beachten, dass zwei Quotienten gleich sein können auch wenn sie verschiedene Zähler und Nenner haben, wie zum Beispiel bei $8 : 4 = 2 : 1$.

Sei $\sim \subseteq (\mathbb{Z} \times \mathbb{N})^2$ die Relation

$$(x, n) \sim (y, m) \ :\Longleftrightarrow \ \ xm = yn\,.$$

2.2.1 Lemma. *Die Relation $\sim$ ist eine Äquivalenzrelation.*

Beweis. Die Reflexivität und Symmetrie ist offensichtlich. Sei nun $(x, n) \sim (y, m)$ und $(y, m) \sim (z, k)$, dann gilt also $xm = yn$ und $yk = zm$. Es folgt

$$(xk)m = (xm)k = (yn)k = (yk)n = (zm)n = (zn)m\,,$$

und wegen der Kürzungsregel in $\mathbb{Z}$ daher $xk = zn$, d.h. $(x, n) \sim (z, k)$. ❑

2.2.2 Definition. Wir bezeichnen die Faktormenge $(\mathbb{Z} \times \mathbb{N})/_\sim$ mit $\mathbb{Q}$, und sprechen vom Körper der *rationalen Zahlen*. //

Um zu sehen wie wir Addition, Multiplikation und Ordnung auf $\mathbb{Z} \times \mathbb{N}$ definieren sollten, machen wir die formalen(!) Rechnungen:

$$\begin{aligned} &\tfrac{x}{n} + \tfrac{y}{m} = \tfrac{xm}{nm} + \tfrac{yn}{mn} = \tfrac{xm+yn}{nm} \\ &\tfrac{x}{n} \cdot \tfrac{y}{m} = \tfrac{xy}{nm} \\ &\tfrac{x}{n} \le \tfrac{y}{m} \iff \tfrac{xm}{nm} \le \tfrac{yn}{nm} \iff xm \le yn \end{aligned}$$

Natürlich machen diese Rechnungen im allgemeinen keinen Sinn, aber sie legen die folgende Definition nahe.

2.2.3 Definition. Es seien Abbildungen $+ : (\mathbb{Z} \times \mathbb{N})^2 \to \mathbb{Z} \times \mathbb{N}$, $\cdot : (\mathbb{Z} \times \mathbb{N})^2 \to \mathbb{Z} \times \mathbb{N}$ und eine Relation $\le$ auf $\mathbb{Z} \times \mathbb{N}$ definiert als $((x, n), (y, m) \in \mathbb{Z} \times \mathbb{N})$

$$\begin{aligned} (x, n) + (y, m) &:= (xm + yn, nm) \\ (x, n) \cdot (y, m) &:= (xy, nm) \\ (x, n) \le (y, m) &:\Longleftrightarrow \ xm \le yn \end{aligned}$$

//

2.2.4 Lemma. *Die Operationen „$+$“ und „$\cdot$“ auf $\mathbb{Z} \times \mathbb{N}$ sind kommutativ, assoziativ und es gilt das Distributivitätsgesetz von „$\cdot$“ über „$+$“.*

Die Relation $\le$ auf $\mathbb{Z} \times \mathbb{N}$ ist reflexiv und transitiv. Ist $(x, n) \le (y, m)$ und $(y, m) \le (x, n)$, so folgt $(x, n) \sim (y, m)$.

Beweis. Die Rechenregeln für Addition und Multiplikation folgen einfach durch einsetzen in die jeweiligen Definitionen.

Wir kommen zu den Eigenschaften von „$\leq$“. Die Reflexivität ist klar. Seien $(x,n) \leq (y,m)$ und $(y,m) \leq (z,k)$. Dann gilt $xm \leq yn, yk \leq zm$. Es folgt

$$(xk)m = (xm)k \leq (yn)k = (yk)n \leq (zm)n = (zn)m\,,$$

und daher $xk \leq zn$, d.h. $(x,n) \leq (z,k)$.

Sei $(x,n) \leq (y,m)$ und $(y,m) \leq (x,n)$, dann gilt also $xm \leq yn$ und $ym \leq xn$. Wir erhalten $xm = yn$, d.h. $(x,n) \sim (y,m)$. ❑

Um diese Operationen/Relation auf $\mathbb{Q}$ übertragen zu können, benötigen wir die folgende Verträglichkeit.

2.2.5 Lemma. *Seien $(x,n) \sim (x',n')$ und $(y,m) \sim (y',m')$. Dann folgt, dass*

$$\begin{aligned}(x,n) + (y,m) &\sim (x',n') + (y',m')\\ (x,n) \cdot (y,m) &\sim (x',n') \cdot (y',m')\\ (x,n) \leq (y,m) &\iff (x',n') \leq (y',m)\end{aligned}$$

Beweis. Seien $(x,n) \sim (x',n')$ und (y,m) gegeben. Dann gilt

$$(xm+yn)n'm = xmn'm + ynn'm =$$

$$= \underbrace{(xn' - x'n)}_{=0} mm + x'nmm + ynn'm = (x'm + yn')nm\,,$$

also $(x,n) + (y,m) \sim (x',n') + (y,m)$. Wegen der Kommutativität folgt auch das für (x,n) und $(y,m) \sim (y',m')$ stets $(x,n)+(y,m) \sim (x,n)+(y',m')$. Setzt man diese beiden Erkenntnisse zusammen, so folgt das für $(x,n) \sim (x',n')$ und $(y,m) \sim (y',m')$ gilt

$$(x,n) + (y,m) \sim (x',n') + (y,m) \sim (x',n') + (y',m')\,.$$

Bei der Multiplikation geht man analog vor. Seien $(x,n) \sim (x',n')$ und (y,m) gegeben. Dann gilt

$$xyn'm = \underbrace{(xn' - x'n)}_{=0} ym + x'nym = x'ynm\,,$$

also $(x,n) \cdot (y,m) \sim (x',n') \cdot (y,m)$. Die gleiche Argumentation wie bei $+$ liefert das gewünschte Ergebnis.

Die Aussage betreffend „$\leq$“ ist klar aus der Definition. ❑

2.2.6 Definition. Seien $a, b \in \mathbb{Q}$ gegeben. Dann definieren wir $a+b$, $a \cdot b$ sowie $a \leq b$ wie folgt: Wähle $(x,n), (y,m) \in \mathbb{Z} \times \mathbb{N}$ mit $[(x,n)]_\sim = a$ und $[(y,m)]_\sim = b$, und setze

$$\begin{aligned}a + b &:= \big[(x,n) + (y,m)\big]_\sim\\ a \cdot b &:= \big[(x,n) \cdot (y,m)\big]_\sim\\ a \leq b &:\iff (x,n) \leq (y,m)\end{aligned}$$

Wegen der Verträglichkeitsaussage Lemma 2.2.5 sind durch diese Vorschriften tatsächlich Funktionen $+, \cdot : \mathbb{Q}^2 \to \mathbb{Q}$, und eine Relation $\leq$ auf $\mathbb{Z}$ wohldefiniert, denn der Wert der rechten Seiten hängt ja nicht von der Wahl der jeweiligen Representanten (x,n) bzw. (y,m) ab. //

Das wir mit rationalen Zahlen so rechnen können wie wir es gewohnt sind, und unser Ziel Quotienten bilden zu können erreicht haben, ist die Aussage des folgenden Satzes.

2.2.7 Satz (Rechenregeln für $\mathbb{Q}$)**.** *Für die Operationen/Ordnung auf $\mathbb{Q}$ gelten die folgenden Rechenregeln:*

(*i*) *Die Addition ist assoziativ und kommutativ. Das Element $0 := [(0,1)]_\sim$ ist neutrales Element bezüglich der Addition. Jedes Element besitzt ein additives Inverses.*

(*ii*) *Die Multiplikation ist assoziativ und kommutativ. Das Element $1 := [(1,1)]_\sim$ ist neutrales Element bezüglich der Multiplikation. Jedes von 0 verschiedene Element besitzt ein multiplikatives Inverses.*

(*iii*) *Es gilt das Distributivitätsgesetz von „$\cdot$“ über „$+$“.*

(*iv*) *Die Relation „$\leq$“ ist eine Totalordnung. Sie ist mit den Operationen „$+$“ und „$\cdot$“ verträglich:*

$$a \leq b \iff a + c \leq b + c, \quad a, b, c \in \mathbb{Q}$$
$$a \leq b \iff a \cdot c \leq b \cdot c, \quad a, b, c \in \mathbb{Q}, c > 0$$

(*v*) *Die ganzen Zahlen sind in $\mathbb{Q}$ eingebettet vermöge der injektiven Abbildung*

$$\phi : \left\{ \begin{array}{ccc} \mathbb{Z} & \to & \mathbb{Q} \\ x & \mapsto & [(x,1)]_\sim \end{array} \right.$$

Diese Abbildung erhält Addition, Multiplikation und Ordnung:

$$\phi(n+m) = \phi(n) + \phi(m),\ \phi(n \cdot m) = \phi(n) \cdot \phi(m),\ n \leq m \Leftrightarrow \phi(n) \leq \phi(m)$$

(*vi*) *Sind $a, b \in \mathbb{Q}$, $a > 0$, so existiert eine Zahl $N \in \mathbb{N}$ mit $Na = \underbrace{a + \ldots + a}_{n\text{-}mal} > b$.*

Beweis. Die Gültigkeit der Rechenregeln Kommutativität, Assoziativität und Distributivität ergibt sich aus den entsprechenden Regeln auf $\mathbb{Z}$ und aus unserer Definition, wie im Beweis von Satz 2.1.7, unmittelbar durch nachrechnen.

Es gilt: Sei $a = [(x,n)]_\sim \in \mathbb{Q}$, dann ist

$$a + 0 = [(x + 0, n \cdot 1)]_\sim = a,\ a \cdot 1 = [(x \cdot 1, n \cdot 1)]_\sim = a\,.$$

Weiters gilt für $b := [(-x,n)]_\sim$, dass

$$a + b = [(xn - xn, nn)]_\sim = [(0, nn)]_\sim = [(0,1)]_\sim = 0\,.$$

Sei nun $a \neq 0$, d.h. $(x,n) \not\sim (0,1)$ oder äquivalent $x \neq 0$. Ist $x \in \mathbb{N}$, so setze $c := [(n,x)]_\sim$, ist $x < 0$, so sei $c := [(-n,-x)]_\sim$. Man sieht $ac = [(xn, nx)]_\sim = 1$, bzw. $ac = [(x(-n), n(-x)]_\sim = 1$.

Seien nun $a = [(x,n)]_\sim, b = [(y,m)]_\sim \in \mathbb{Q}$, $a \leq b$, und sei $c = [(z,k)]_\sim$. Dann folgt

$$(xk + zn)km = xmkk + znkm \leq ynkk + znkm = (yk + zm)kn\,,$$

d.h. $a + c \leq b + c$. Ist zusätzlich $c \geq 0$, d.h. $z \geq 0$, so folgt aus $xm \leq yn$ das auch $xmzk \leq ynzk$, also $ac \leq bc$.

Betrachte nun die Abbildung $\phi : \mathbb{Z} \to \mathbb{Q}$. Diese ist injektiv, denn $(x, 1) \sim (y, 1)$ genau dann wenn $x = y$. Das sie die algebraischen Operationen und die Ordnung erhält rechnet man leicht nach.

Seien $a = [(x, n)]_\sim, b = [(y, m)]_\sim \in \mathbb{Q}$, $a > 0$. Ist $b \leq 0$, wähle $N = 1$. Sei also auch $b > 0$. Es gilt

$$ny \cdot a = \big[(ny, 1) \cdot (x, n)\big]_\sim = [(yx, 1)]_\sim \geq [(y, m)]_\sim = b\,,$$

denn, da $x, y, m \in \mathbb{N}$ sind gilt sicher $mxy \geq y$. Setzt man nun $N := ny + 1$, so erhält man $Na = ny \cdot a + a \geq b + a > b$. ❑

Wir werden im folgenden für die rationale Zahl $[(x, n)]_\sim$ stets das Symbol $\frac{x}{n}$ schreiben. Dieses Symbol drückt tatsächlich die Division von x durch n aus, denn man hat

$$[(x + 1, 1)]_\sim = [(x, n)]_\sim \cdot [(n + 1, 1)]_\sim,$$

also $x = \frac{x}{n} \cdot n$. Wir sehen insbesondere, dass jede rationale Zahl der Quotient von zwei ganzen Zahlen ist (wobei wir $\mathbb{Z}$ vermöge der Einbettung ϕ aus Satz 2.2.7 als Teilmenge von $\mathbb{Q}$ betrachten).

2.3 Körper

Wir wollen die Rechenregeln die wir vom Umgang mit Zahlen gewohnt sind, und die für $\mathbb{Q}$ auch tatsächlich gelten, in den folgenden drei Definitionen zusammenfassen.

2.3.1 Definition. Sei K eine Menge versehen mit zwei algebraischen Operationen „$+$“ und „$\cdot$“. Dann heißt $\langle K, +, \cdot\rangle$ ein *Körper*, wenn die folgenden Gesetze gelten:

(A1) Die Addition ist assoziativ und kommutativ.

(A2) Es existiert ein neutrales Element 0 bezüglich „$+$“.

(A3) Jedes Element besitzt ein additives Inverses.

(M1) Die Multiplikation ist assoziativ und kommutativ.

(M2) Es existiert ein neutrales Element 1 bezüglich „$\cdot$“.

(M3) Jedes von 0 verschiedene Element besitzt ein multiplikatives Inverses.

(D) Es gilt das Distributivitätsgesetz von „$\cdot$“ über „$+$“.

//

2.3.2 Definition. Sei $\langle K, +, \cdot\rangle$ ein Körper und sei „$\leq$“ eine Totalordnung auf K. Dann heißt $\langle K, +, \cdot, \leq\rangle$ ein *angeordneter Körper*, wenn die folgenden Gesetze gelten:

(GK1) Ist $x, y, z \in K$ und $x \leq y$, so folgt $x + z \leq y + z$.

(GK2) Ist $x, y, z \in K$, $x \leq y$ und $z \geq 0$, so folgt $x \cdot z \leq y \cdot z$.

//

2.3.3 Definition. Sei $\langle K, +, \cdot, \leq \rangle$ ein angeordneter Körper. Dann heißt K *archimedisch angeordnet*, wenn gilt: Für alle $x, y \in K$, $x > 0$, existiert $n \in \mathbb{N}$ mit $nx > y$. //

Satz 2.2.7 besagt nun also:

> $\mathbb{Q}$ ist ein archimedisch angeordneter Körper, enthält die ganzen Zahlen, und jedes Element von $\mathbb{Q}$ ist Quotient von zwei ganzen Zahlen.

Wir wollen bemerken das jeder angeordnete Körper $\mathbb{Q}$ enthält, und damit insbesondere auch $\mathbb{Z}$.

2.3.4 Proposition. *Sei K ein angeordneter Körper. Dann gibt es eine injektive Abbildung $\phi : \mathbb{Q} \to K$ welche mit der Addition, Multiplikation und Ordnung erhält.*

Beweis. Wir haben $1 > 0$. Denn wäre $1 < 0$ so würde $1 = 1 \cdot 1 > 1 \cdot 0 = 0$ folgen, ein Widerspruch. Also ist

$$0 < 1 < 1 + 1 < 1 + 1 + 1 < \dots .$$

Es folgt, dass $0 > -1 > -(1+1) > -(1+1+1) > \dots$. Daher ist die Abbildung ϕ die einer ganzen Zahl x das Element

$$\phi(x) := \begin{cases} \underbrace{1 + 1 + \dots + 1}_{x\text{-mal}} & , \ x > 0 \\ -(\underbrace{1 + 1 + \dots + 1}_{-x\text{-mal}}) & , \ x < 0 \\ 0 & , \ x = 0 \end{cases}$$

zuordnet, injektiv. Man rechnet leicht nach, dass sie die Addition und Multiplikation sowie auch die Ordnung erhält.

Da ganz $\mathbb{Q}$ von den Quotienten $\frac{x}{n}$ mit $x \in \mathbb{Z}$, $n \in \mathbb{N}$, ausgeschöpft wird, läßt sie sich durch die Vorschrift

$$\phi\Big(\frac{x}{y}\Big) := \frac{\phi(x)}{\phi(y)}$$

zu einer Abbildung von $\mathbb{Q}$ nach K fortsetzen. Diese ist wohldefiniert, denn ist $\frac{x}{y} = \frac{x'}{y'}$, so folgt $xy' = yx'$, und damit $\phi(x)\phi(y') = \phi(xy') = \phi(yx') = \phi(y)\phi(x')$. Dies wiederum impliziert

$$\frac{\phi(x)}{\phi(y)} = \frac{\phi(x')}{\phi(y')} .$$

Diese Fortsetzung von ϕ erhält ebenfalls die Addition und Multiplikation, denn für je vier Elemente $a, b, c, d \in K$, $b, d \neq 0$, gilt

$$ab^{-1} + cd^{-1} = add^{-1}b^{-1} + cbb^{-1}d^{-1} = (ad + cb)(bd)^{-1} ,$$

$$ab^{-1} \cdot cd^{-1} = (ac)(bd)^{-1} .$$

Es folgt das ϕ injektiv ist, denn wäre $\phi(x) = \phi(y)$ für $x \neq y$, so wäre $\phi(x-y) = 0$ und $x - y \neq 0$. Dann wäre aber

$$1 = \phi(1) = \phi\big((x-y)(x-y)^{-1}\big) = \underbrace{\phi(x-y)}_{=0} \cdot \phi(x-y)^{-1} = 0\,,$$

ein Widerspruch. Sie erhält auch die Ordnung, denn es gilt

$$\frac{x}{n} \leq \frac{y}{m} \iff xm \leq yn \iff \phi(x)\phi(m) \leq \phi(y)\phi(n) \iff \frac{\phi(x)}{\phi(n)} \leq \frac{\phi(y)}{\phi(m)}\,.$$

❑

Schliesslich wollen wir eine oft praktische Formel herleiten, den Binomischen Lehrsatz. Dieser gibt eine Methode den Ausdruck $(a+b)^n$ zu berechnen. Um zu einer Vermutung zu gelangen, wollen wir zuerst ein paar Potenzen $(a+b)^n$ ausrechnen:

$$\begin{aligned}
(a+b)^0 &= 1\\
(a+b)^1 &= a+b\\
(a+b)^2 &= a^2+2ab+b^2\\
(a+b)^3 &= a^3+3a^2b+3ab^2+b^3\\
(a+b)^4 &= a^4+4a^3b+6a^2b^2+4ab^3+b^4
\end{aligned}$$

Die aufgetretenen Koeffizienten, die sogenannten *Binomialkoeffizienten*, kann man in einem dreieckigen Schema anordnen (*Pascalsches Dreieck*[2]).

$$\begin{array}{ccccccccccc}
 & & & & & 1 & & & & & \\
 & & & & 1 & & 1 & & & & \\
 & & & 1 & & 2 & & 1 & & & \\
 & & 1 & & 3 & & 3 & & 1 & & \\
 & 1 & & 4 & & 6 & & 4 & & 1 & \\
 & & & & & \vdots & & & & &
\end{array}$$

Man vermutet(!), daß hier jeder Eintrag gerade die Summe seiner beiden oberen Nachbaren ist. Betrachte das Schema gebildet aus den Quotienten der Einträge mit ihrem linken Nachbaren:

$$\begin{array}{ccccccccccc}
 & & & & & \times & & & & & \\
 & & & & \times & & 1 & & & & \\
 & & & \times & & \frac{2}{1} & & \frac{1}{2} & & & \\
 & & \times & & \frac{3}{1} & & \frac{2}{2} & & \frac{1}{3} & & \\
 & \times & & \frac{4}{1} & & \frac{3}{2} & & \frac{2}{3} & & \frac{1}{4} & \\
 & & & & & \vdots & & & & &
\end{array}$$

Man vermutet(!) auch hier das Bildungsgesetz des Schemas. Also:

$$\text{Koeffizient von } a^{n-k}b^k \text{ in der Entwicklung von } (a+b)^n \overset{\text{Satz 1}}{=} \frac{n}{1} \cdot \frac{n-1}{2} \cdot \ldots \cdot \frac{n-k+1}{k} = \frac{n!}{k!(n-k)!}.$$

[2]Blaise Pascal. 19.6.1623 Cleremont-Ferrand - 19.8.1662 Paris

Dabei haben wir zur Abkürzung $n! := 1 \cdot 2 \cdot \ldots \cdot n$ geschrieben, und $0! := 1$ gesetzt[3].

Wir schreiben im folgenden zur Abkürzung

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

und bezeichnen $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$.

2.3.5 Satz (Binomischer Lehrsatz)**.** *Sei K ein Körper, $a, b \in K$, und $n \in \mathbb{N}_0$. Dann gilt*

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

Beweis. Induktion nach n. Die Fälle $n = 0$ oder $n = 1$ sind unmittelbar einsichtig. Sei die Behauptung richtig für ein $n \in \mathbb{N}$, dann folgt

$$(a+b)^{n+1} = (a+b)^n \cdot (a+b) = \left(\sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k \right) \cdot (a+b) =$$

$$= \sum_{k=0}^{n} \binom{n}{k} a^{n-k+1} b^k + \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^{k+1} =$$

$$= \sum_{k=0}^{n} \binom{n}{k} a^{(n+1)-k} b^k + \sum_{k=1}^{n+1} \binom{n}{k-1} a^{(n+1)-k} b^k =$$

$$= a^{n+1} + \sum_{k=1}^{n} \left[\binom{n}{k} + \binom{n}{k-1} \right] a^{(n+1)-k} b^k + b^{n+1}.$$

Nun gilt

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

und damit folgt die Behauptung. ❑

Wir können am Beispiel des Binomischen Lehrsatzes eine grossen Vorteil unseren axiomatischen Denkweise verdeutlichen: Die Tatsache, dass die Formel aus Satz 2.3.5 für Zahlen a, b gilt, war schon lange Zeit bekannt. Dann hat man analysiert welche Voraussetzungen man eigentlich benötigt um sie herzuleiten. Man sieht, dass man gar nicht mit Zahlen rechnen muss, sondern dass es genügt irgendwelche Objekte zu haben die den entsprechenden Rechenregeln genügen. Dies spiegelt sich in unserer Formulierung darin wieder, dass a, b Elemente eines beliebigen Körpers sein können.

Um einzusehen, dass dies tatsächlich eine interessante Erkenntnis ist, wollen wir ein Beispiel eines Körpers anführen, dessen Elemente keine Zahlen sind.

[3]Man bezeichnet $n!$ als *n-faktoriell*.

2.3.6 Beispiel. Sei K ein Körper. Der *Polynomring* $K[X]$ in einer Variablen über dem Körper K ist definiert als

$$K[X] := \left\{ (a_k)_{k\in\mathbb{N}_0} \in \prod_{k\in\mathbb{N}_0} K : \quad \exists\, N \in \mathbb{N}_0 : a_k = 0, k \geq N \right\}.$$

Ein Element des Polynomringes heißt *Polynom* in einer Variablen mit Koeffizienten in K.

Wir wollen für Polynome eine Addition und eine Multiplikation definieren. Um diese Definition zu motivieren, besinnen wir uns darauf wie man naiv mit ihren Namensgebern umgeht. Dazu schreiben wir ein Polynom $(a_k)_{k\in\mathbb{N}_0}$ an als einen formalen Ausdruck der Gestalt

$$p(X) = a_n X^n + a_{n-1}X^{n-1} + \ldots + a_1 X + a_0 = \sum_k a_k X^k$$

und machen die formalen Rechnungen

$$p(X) + q(X) = \sum_k a_k X^k + \sum_k b_k X^k = \sum_k (a_k + b_k) X^k$$
$$p(X) \cdot q(X) = \Big(\sum_k a_k X^k\Big) \cdot \Big(\sum_k b_k X^k\Big) = \sum_k \Big(\sum_{i+j=k} a_i b_j\Big) X^k$$

Wir werden also definieren: Für $p = (a_k)_{k\in\mathbb{N}_0}, q = (b_k)_{k\in\mathbb{N}_0} \in K[X]$ setze

$$(p+q)(X) := (c_k)_{n\in\mathbb{N}_0} \qquad \text{mit } c_k := a_k + b_k$$
$$(p\cdot q)(X) := (d_k)_{n\in\mathbb{N}_0} \qquad \text{mit } d_k := \sum_{i+j=k} a_i b_j$$

Man kann nachrechnen, dass diese Operationen genau den gleichen Rechenregeln genügen wie wir sie in Satz 2.1.7 für die ganzen Zahlen gezeigt haben.

Führt man nun genau die gleiche Konstruktion durch die uns von den ganzen zu den rationalen Zahlen geführt hat[4], so erhält man einen Körper $K(X)$. Dieser besteht also aus allen Ausdrücken $r(X)$ der Gestalt

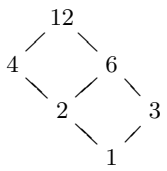
$$r(X) = \frac{p(X)}{q(X)}$$

mit Polynomen p und q, $q \neq 0$. Man spricht von *Körper der rationalen Funktionen* in einer Variablen über K. //

2.4 Teilbarkeitslehre

Wir wollen die Theorie der natürlichen Zahlen noch ein bischen weiterverfolgen. Eine wesentliche Rolle spielt die Teilbarkeitsrelation auf $\mathbb{N}$. Zur Erinnerung: Seien $n, m \in \mathbb{N}$. Wir sagen $n|m$, wenn es eine natürliche Zahl l gibt mit $m = nl$.

Als Beispiel betrachten wir alle Teiler von 12:



[4]Diese Konstruktion nennt man auch Bildung des *Quotientenkörpers*.

Trivialerweise ist jede Zahl n durch 1 und durch sich selbst teilbar, denn

$$n = 1 \cdot n = n \cdot 1.$$

Hat man zwei Zahlen n und m, so haben diese also immer mindestens einen gemeinsamen Teiler (nämlich 1). Es ist eine interessante Tatsache, dass die Menge der gemeinsamen Teiler stets ein (sogar bezüglich der Teilbarkeitsrelation) größtes Element besitzt, vgl. Satz 2.4.2. Dazu zeigen wir zunächst den *Divisionsalgorithmus*.

2.4.1 Proposition (Division mit Rest)**.** *Sind $n, m \in \mathbb{N}$, so gibt es eindeutig bestimmte Zahlen $q, r \in \mathbb{N}_0$ mit $n = q \cdot m + r$ und $0 \leq r < m$.*

Beweis. Es gibt nur endlich viele natürliche Zahlen zwischen 0 und n. Die Zahlen $0, m, 2m, 3m, \ldots$ sind alle verschieden. Also gibt es $q \in \mathbb{N}_0$ mit $qm \leq n < (q+1)m$. Für r wähle man $r = n - qm$, dann hat man eine Darstellung der gewünschten Gestalt gefunden.

Sei $n = q_1 m + r_1 = q_2 m + r_2$, dann folgt $(q_1 - q_2)m = r_2 - r_1$. Nun ist $(q_1 - q_2)m$ einer der Werte $0, \pm m, \pm 2m, \ldots$ wogegen $r_2 - r_1$ einer der Werte $-(m-1), \ldots, 0, \ldots, m-1$ ist. Es folgt $(q_1 - q_2)m = r_2 - r_1 = 0$, also $q_1 = q_2$ und $r_1 = r_2$. ❑

2.4.2 Satz (Satz vom ggT, Euklidischer Algorithmus[5])**.** *Seien $n, m \in \mathbb{N}$. Dann existiert eine eindeutig bestimmte Zahl $d \in \mathbb{N}$ mit den folgenden beiden Eigenschaften:*

(*i*) *Es gilt $d|n$ und $d|m$.*

(*ii*) *Ist t irgendeine natürliche Zahl mit $t|n$ und $t|m$, so gilt $t|d$.*

Es gibt ganze Zahlen a und b mit $d = an + bm$.

Beweis. Wir wenden den Divisionsalgorithmus an, und erhalten schrittweise

$$\begin{array}{rcl} n & = & q_1 m + r_1 \\ m & = & q_2 r_1 + r_2 \\ r_1 & = & q_3 r_2 + r_3 \\ & \vdots & \\ r_{i-3} & = & q_i r_{i-2} + r_{i-1} \\ r_{i-2} & = & q_i r_{i-i} + r_i \\ r_{i-1} & = & q_{i+1} r_i + r_{i+1} \\ & \vdots & \end{array} \tag{2.4.1}$$

Dieses Verfahren kann durchgeführt werden, solange der entstehende Rest r_i verschieden von Null ist. Ist der neu entstandene Rest gleich 0, so bricht das Verfahren ab.

Die Zahlen $m, r_1, r_2 \ldots$ bilden eine absteigende Kette in $\mathbb{N}_0$, d.h. es gilt

$$m > r_1 > r_2 > \ldots$$

[5] Euklid. um 300 v.C.

Würde obiges Verfahren nicht abbrechen, so hätten wir eine unendlich lange absteigende Kette von natürlichen Zahlen gefunden, ein Widerspruch[6]. Daher existiert i, sodass $r_i \neq 0$, $r_{i+1} = 0$.

Die letzte Gleichung aus (2.4.1) hat die Gestalt

$$r_{i-1} = q_{i+1} r_i.$$

Setzt man die Gleichungen der Reihe nach rückwärts ein, so sieht man daß r_i ein Teiler von n und m ist:

$$r_{i-1} = q_{i+1} r_i,\ r_{i-2} = q_i(q_{i+1} r_i) + r_i, \ldots$$

Liest man die Gleichungskette vorwärts, so sieht man daß r_i in der Form $an+bm$ mit gewissen ganzen Zahlen a, b geschrieben werden kann:

$$r_1 = n - q_1 m, r_2 = m - q_2(n - q_1 m), \ldots$$

Die Zahl $d := r_i$ erfüllt nun die Eigenschaften (i) und (ii). Die Gültigkeit von (i) wurde schon oben vermerkt. Sei also t irgendein Teiler von n und m. Dann teilt t auch jede Zahl der Form $an + bm$, insbesondere ist $t|d$.

Wir kommen zum Beweis der Eindeutigkeit. Seien zwei Zahlen d, d' gegeben, die beide die Eigenschaften (i) und (ii) haben. Dann ist $d'|n$, $d'|m$ denn d' erfüllt (i). Damit folgt $d'|d$, denn d erfüllt (ii). Genauso sieht man $d|d'$, und erhält insgesamt $d = d'$. ❑

2.4.3 Definition. Die Zahl d aus Satz 2.4.2 heißt *größter gemeinsamer Teiler* von n und m. Wir schreiben $d = \mathrm{ggT}\{n, m\}$. //

2.4.4 Beispiel. Zum Beispiel wollen wir mit Hilfe des Euklidischen Algorithmus den größten gemeinsamen Teiler von $n = 2124$ und $m = 1764$ bestimmen:

$$2124 = 1 \cdot 1764 + 360,\ 1764 = 4 \cdot 360 + 324,$$

$$360 = 1 \cdot 324 + 36,\ 324 = 9 \cdot 36.$$

Also gilt $\mathrm{ggT}\{2124, 1764\} = 36$. Weiters ist

$$36 = 360 - 1 \cdot 324 = 360 - 1 \cdot (1764 - 4 \cdot 360) = (-1) \cdot 1764 + 5 \cdot 360 =$$

$$= (-1) \cdot 1764 + 5 \cdot (2124 - 1764) = 5 \cdot 2124 + (-6) \cdot 1764.$$

//

Wesentlich für das Folgende ist das nächste Lemma.

2.4.5 Lemma. *Seien $n_1, n_2, m \in \mathbb{N}$ mit $m|n_1 n_2$. Gilt*[7] *$\mathrm{ggT}\{m, n_1\} = 1$, so folgt $m|n_2$.*

Beweis. Es ist $1 = am + bn_1$ für gewisse ganze Zahlen a, b. Also gilt $n_2 = n_2 am + n_2 bn_1$. Da m beide Summanden teilt folgt $m|n_2$. ❑

[6] In einer wohlgeordneten Menge M kann es keine unendlich langen absteigenden Ketten geben: Angenommen es wären $x_n \in M$, $n \in \mathbb{N}$, mit $x_1 > x_2 > x_3 > \ldots$. Die Menge $M' := \{x_n : n \in \mathbb{N}\}$ ist eine nichtleere Teilmenge von M, besitzt also ein kleinstes Element. Es gibt also ein $N \in \mathbb{N}$, sodaß x_N das kleinste Element von M' ist. Ein Widerspruch, da ja $x_{N+1} < x_N$.

[7] Zwei Zahlen deren größter gemeinsamer Teiler gleich 1 ist nennt man auch *relativ prim*.

Die Voraussetzung dass m und n_1 relativ prim sind, kann nicht weggelassen werden. Denn zum Beispiel ist ja $6|(2 \cdot 3)$.

2.4.6 Korollar. *Seien m_1, m_2 Teiler von n. Gilt $\mathrm{ggT}\{m_1, m_2\} = 1$, so folgt $(m_1 m_2)|n$.*

Beweis. Setze $k := \frac{n}{m_2}$, dann ist k eine ganze Zahl, da $m_2|n$. Wir wenden Lemma 2.4.5 an mit $m_1|m_2 k$, und finden $m_1|k$. Also folgt $(m_1 m_2)|n$. ❑

Wir haben schon festgestellt, dass jede Zahl durch 1 und sich selbst geteilt wird. Jene Zahlen die gar keine anderen Teiler besitzen spielen eine besondere Rolle. Sie sind die „multiplikativen Bausteine“ der natürlichen Zahlen, vgl. Satz 2.4.9.

2.4.7 Definition. Eine natürliche Zahl $p \in \mathbb{N}$, $p \neq 1$, heißt *Primzahl*, wenn sie außer 1 und sich selbst keine anderen Teiler besitzt. //

Äquivalent ausgedrückt ist p eine Primzahl, wenn sie nicht als Produkt $p = ab$ mit $a, b < p$ geschrieben werden kann.

2.4.8 Korollar. *Eine Zahl $p \in \mathbb{N}$, $n \neq 1$, ist genau dann Primzahl, wenn sie folgende Eigenschaft hat:*

$$\text{Gilt } p|n_1 n_2, \text{ so folgt } p|n_1 \text{ oder } p|n_2. \tag{2.4.2}$$

Beweis. Habe p die Eigenschaft (2.4.2), sei m ein Teiler von p, und schreibe $p = km$. Dann folgt $p|k$ oder $p|m$. Da jedenfalls $k|p$ und $m|p$, folgt entweder $k = p$ oder $m = p$ (und entsprechend $m = 1$ bzw. $k = 1$).

Habe nun umgekehrt p keine nichttrivialen Teiler und sei $p|n_1 n_2$. Gilt $\mathrm{ggT}\{p, n_1\} \neq 1$, so folgt schon $\mathrm{ggT}\{p, n_1\} = p$, also $p|n_1$. Ist jedoch $\mathrm{ggT}\{p, n_1\} = 1$, so gilt wegen Lemma 2.4.5 die Beziehung $p|n_2$. ❑

Mittels Induktion nach der Anzahl der Faktoren kann man die Eigenschaft (2.4.2) leicht verschärfen: Eine Zahl $p \in \mathbb{N}$, $p \neq 1$, ist genau dann Primzahl, wenn sie die folgende Eigenschaft hat:

$$\text{Gilt } p|n_1 n_2 \cdots n_r, \text{ so existiert ein Index } i \text{ mit } p|n_i.$$

2.4.9 Satz (Satz von der eindeutigen Primfaktorzerlegung)**.** *Jede natürliche Zahl läßt sich, in bis auf die Reihenfolge eindeutiger Weise, als Produkt von Primzahlen darstellen*[8]*.*

Beweis. Wir benützen vollständige Induktion. Die hier betrachtete Aussage $A(n)$ ist:

> „Jede natürliche Zahl k mit $k \leq n$ läßt sich als Produkt von Primzahlen darstellen.“

Induktionsanfang: $n = 1$ ist das leere Produkt von Primzahlen ($n = 2$ ist selbst Primzahl, $n = 3$ ebenfalls, $n = 4$ schreibt sich als $4 = 2 \cdot 2$).

Induktionsschritt: Sei $n \in \mathbb{N}$ gegeben, und sei vorausgesetzt dass $A(n)$ wahr ist. Um $A(n+1)$ zu zeigen, müssen wir nur noch zeigen, dass sich die Zahl $n+1$ als Produkt von Primzahlen darstellen läßt.

[8] Dabei verstehen wir formal das Produkt einer leeren Menge von Primzahlen als 1

Hat $n+1$ außer 1 und sich selbst keinen Teiler, so ist $n+1$ selbst Primzahl, also inbesondere Produkt von Primzahlen. Hat $n+1$ einen Teiler m mit $1 < m < n+1$, so gilt also $n+1 = mk$ mit $m < n+1$ und auch $k < n+1$. Nach Induktionsvoraussetzung sind m und k als Produkt von Primzahlen darstellbar. Damit hat auch deren Produkt $n+1$ diese Eigenschaft.

Nach dem Prinzip der vollständigen Induktion ist die betrachtete Aussage $A(n)$ für alle natürlichen Zahlen n wahr, und die Existenz einer Primfaktorzerlegung damit nachgewiesen.

Für den Beweis der Eindeutigkeit zeigen wir:

> *Seien $n, n' \in \mathbb{N}_0$ und p_i, p_i' Primzahlen. Gilt $\prod_{i=1}^{n} p_i = \prod_{i=1}^{n'} p_i'$, so folgt $n = n'$ und die Primfaktoren p_i und p_i' sind (bis auf Umnummerierung) gleich.*

Um dies einzusehen, machen wir Induktion nach $\min\{n, n'\}$.

Induktionsanfang: Ist eines von n, n' gleich Null, z.B. $n = 0$, so ist $\prod_{i=1}^{n} p_i = 1$. Damit ist auch $\prod_{i=1}^{n'} p_i' = 1$, und da die Faktoren p_i alle größer als 1 sind, muss auch dieses Produkt das leere Produkt sein.

Induktionsschritt: Angenommen es ist $\prod_{i=1}^{n} p_i = \prod_{i=1}^{n'} p_i'$ mit $n, n' > 0$. Wegen $p_1 | \prod_{i=1}^{n'} p_i'$ gilt $p_1 = p_i'$ für ein gewisses i. Nach eventueller Umnummerierung kann man $i = 1$ annehmen. Damit folgt $\prod_{i=2}^{n} p_i = \prod_{i=2}^{n'} p_i'$. Nach Induktionsvoraussetzung ist $n-1 = n'-1$ und es stimmen $p_2, \ldots, p_n$ bis auf Umnummerierung mit $p_2', \ldots, p_{n'}'$ überein. ❑

Der Satz von der eindeutigen Primfaktorzerlegung ist eine wesentliche Eigenschaft der ganzen Zahlen. Er gilt nicht in jedem Zahlensystem!

Man schreibt die Darstellung einer Zahl n als Produkt von Primzahlen oft an, indem man gleiche Primfaktoren zu Potenzen zusammenfaßt:

$$n = \prod_{p \text{ prim}} p^{n(p)},$$

wobei stets $n(p) \geq 0$ ist, und $n(p) > 0$ nur für endlich viele p gilt. Zum Beispiel ist

$$2124 = 2^2 \cdot 3^2 \cdot 59, \quad 1764 = 2^2 \cdot 3^2 \cdot 7^2. \tag{2.4.3}$$

Wir erhalten auch, dass sich jede ganze Zahl sowie jede rationale Zahl in eindeutiger Weise als Produkt von Primzahlen schreiben läßt.

2.4.10 Proposition. *Sei $x \in \mathbb{Q}$, $x \neq 0$. Dann läßt sich x in eindeutiger Weise anschreiben als*

$$x = \epsilon \prod_{p \text{ prim}} p^{x(p)},$$

mit gewissen Zahlen $x(p) \in \mathbb{Z}$ von denen nur endlich viele verschieden von Null sind, und wobei $\epsilon \in \{1, -1\}$.

Dabei gilt $x \in \mathbb{Z}$ genau dann, wenn $x(p) \geq 0$ für alle p.

Beweis. Da $x \neq 0$ ist, können wir $x = \frac{\epsilon n}{m}$ mit $\epsilon \in \{1, -1\}$ und $n, m \in \mathbb{N}$. Dann ist

$$x = \frac{\epsilon \prod_{p \text{ prim}} p^{n(p)}}{\prod_{p \text{ prim}} p^{m(p)}} = \epsilon \prod_{p \text{ prim}} p^{n(p)-m(p)}.$$

Um die Eindeutigkeit einzusehen, seien $\epsilon, \epsilon' \in \{-1, 1\}$ und $x(p), x(p)' \in \mathbb{Z}$ (nur endlich viele verschieden von Null) gegeben mit

$$\epsilon \prod_{p \text{ prim}} p^{x(p)} = \epsilon' \prod_{p \text{ prim}} p^{x(p)'} . \tag{2.4.4}$$

Da das Produkt von Primzahlpotenzen stets positiv ist, folgt dass $\epsilon = \epsilon'$. Schreibe nun $x(p) = x_+(p) - x_-(p)$ mit $x_+(p) := \max\{x(p), 0\}$ und $x_-(p) := \max\{-x(p), 0\}$, und analog $x(p)' = x_+(p)' - x_-(p)'$. Dann besagt (2.4.4)

$$\frac{\prod_{p \text{ prim}} p^{x_+(p)}}{\prod_{p \text{ prim}} p^{x_-(p)}} = \frac{\prod_{p \text{ prim}} p^{x_+(p)'}}{\prod_{p \text{ prim}} p^{x_-(p)'}}$$

und wir erhalten

$$\prod_{p \text{ prim}} p^{x_+(p)} \prod_{p \text{ prim}} p^{x_-(p)'} = \prod_{p \text{ prim}} p^{x_+(p)'} \prod_{p \text{ prim}} p^{x_-(p)}$$

also

$$\prod_{p \text{ prim}} p^{x_+(p)+x_-(p)'} = \prod_{p \text{ prim}} p^{x_+(p)'+x_-(p)}$$

Wegen der Eindeutigkeit der Primfaktorzerlegung einer natürlichen Zahl folgt daraus

$$x_+(p) + x_-(p)' = x_+(p)' + x_-(p)$$

d.h. $x(p) = x_+(p) - x_-(p) = x_+(p)' - x_-(p)' = x(p)'$.

Ist $x \in \mathbb{Z}$, so läßt sich x schreiben als $x = \epsilon \frac{n}{1}$ mit $n \in \mathbb{N}$. Daher existiert eine Primfaktordarstellung von x in der stets $x(p) \geq 0$ ist. Umgekehrt ist, wenn alle $x(p)$ nichtnegativ sind, das Produkt $\epsilon \prod_{p \text{ prim}} p^{x(p)}$ sicher eine ganze Zahl. ❑

Die Teilbarkeitsrelation in $\mathbb{N}$ läßt sich mit Hilfe der Primfaktorzerlegung in sehr einfacher Weise charakterisieren.

2.4.11 Lemma. *Seien $n, m \in \mathbb{N}$, und schreibe*

$$n = \prod_{p \text{ prim}} p^{n(p)} \quad m = \prod_{p \text{ prim}} p^{m(p)}.$$

Dann gilt

$$m|n \iff \forall\, p \text{ prim} : n(p) \leq m(p)$$

Beweis. Sei $m|n$, also $n = km$. Habe k die Darstellung $k = \prod_{p \text{ prim}} p^{k(p)}$. Dann folgt

$$\prod_{p \text{ prim}} p^{n(p)} = n = km = \prod_{p \text{ prim}} p^{k(p)} \cdot \prod_{p \text{ prim}} p^{m(p)} = \prod_{p \text{ prim}} p^{k(p)+m(p)}.$$

Wegen der Eindeutigkeit der Primfaktorzerlegung folgt $n(p) = k(p) + m(p)$, also insbesondere $n(p) \geq m(p)$.

Ist umgekehrt $n(p) \geq m(p)$ für alle p, so definiere $k = \prod_{p \text{ prim}} p^{n(p)-m(p)}$. Dann ist $n = km$, also folgt $m|n$. ❑

2.4.12 Korollar. *Seien $n, m \in \mathbb{N}$ gegeben, und seien $n = \prod_{p \text{ prim}} p^{n(p)}$ und $m = \prod_{p \text{ prim}} p^{m(p)}$ die entsprechenden Primfaktorzerlegungen. Dann gilt*

$$\mathrm{ggT}\{n, m\} = \prod_{p \text{ prim}} p^{\min\{n(p), m(p)\}}.$$

Beweis. Ist $t = \prod_{p \text{ prim}} p^{t(p)}$ ein gemeinsamer Teiler von n und m, so folgt $t(p) \leq n(p)$ und $t(p) \leq m(p)$, also $t(p) \leq \min\{n(p), m(p)\}$. Umgekehrt ist $\prod_{p \text{ prim}} p^{\min\{n(p), m(p)\}}$ sicher ein gemeinsamer Teiler von n und m. ❑

Benützen wir die Primfaktorzerlegungen (2.4.3), so können wir den größten gemeinsamen Teiler von 2124 und 1764 sofort hinschreiben, ohne den Euklidischen Algorithmus auszuführen[9]:

$$\mathrm{ggT}\{2124, 1764\} = 2^2 \cdot 3^2 = 36.$$

Dual zum größten gemeinsamen Teiler definiert man das kleinste gemeinsame Vielfache:

2.4.13 Satz. *Seien $n, m \in \mathbb{N}$. Dann existiert eine eindeutig bestimmte Zahl $v \in \mathbb{N}$ mit den folgenden beiden Eigenschaften:*

(*i*) *Es gilt $n|v$, $m|v$.*

(*ii*) *Ist w irgendeine natürliche Zahl mit $n|w$ und $m|w$, so gilt $v|w$.*

Wir nennen diese Zahl das kleinste gemeinsame Vielfache *von n und m, und schreiben* $\mathrm{kgV}\{m, n\}$.

Sind $n = \prod_{p \text{ prim}} p^{n(p)}$ und $m = \prod_{p \text{ prim}} p^{m(p)}$ die entsprechenden Primfaktorzerlegungen, so gilt

$$\mathrm{kgV}\{n, m\} = \prod_{p \text{ prim}} p^{\max\{n(p), m(p)\}}.$$

Beweis. Definiere $v := \frac{nm}{\mathrm{ggT}\{n,m\}}$. Wegen $\mathrm{ggT}\{n, m\}|n$ erhält man $m|v$. Analog folgt $n|v$, d.h. die Eigenschaft (*i*) ist erfüllt. Um (*ii*) zu zeigen, sei w irgendeine Zahl mit $m, n|w$. Schreibt man $\mathrm{ggT}\{m, n\} = am + bn$ mit gewissen ganzen Zahlen a, b, so ergibt sich

$$\frac{w}{v} = \frac{w}{\frac{nm}{\mathrm{ggT}\{n,m\}}} = \frac{w}{\frac{nm}{am+bn}} = \frac{wam + wbn}{nm}.$$

Da $n|w$ folgt $nm|wam$ und da $m|w$ folgt $mn|wbn$. Insgesamt erhält man also $v|w$. Ist v' eine weitere Zahl mit (*i*) und (*ii*), so folgert man $v'|v$ und $v|v'$, also $v' = v$.

Die Primfaktorzerlegung von $\mathrm{kgV}\{n, m\}$ erhält man wieder unmittelbar aus Lemma 2.4.11. ❑

[9] Man erspart sich dabei allerdings nur scheinbar Arbeit. Tatsächlich ist es wesentlich weniger aufwendig den Euklidischen Algorithmus durchzuführen, als die Primfaktorzerlegung zweier gegebener Zahlen zu finden (was nämlich für sehr große Zahlen praktisch unmöglich ist).

Zum Beispiel erhielten wir $\mathrm{kgV}\{2124, 1764\} = 2^2 \cdot 3^2 \cdot 7^2 \cdot 59 = 104076$.

2.4.14 Bemerkung. Betrachte die halbgeordnete Menge $\langle \mathbb{N}, | \rangle$. Dann ist $\mathrm{ggT}\{m, n\}$ das Infimum der beiden Elemente m und n, und $\mathrm{kgV}\{m, n\}$ deren Supremum. ///

Es stellt sich die Frage wie man Primzahlen bestimmen kann. Zuerst wollen wir bemerken:

2.4.15 Satz (Euklid)**.** *Es gibt unendliche viele Primzahlen.*

Beweis. Angenommen es gäbe nur endlich viele Primzahlen $p_1, \ldots, p_r$. Betrachte die Zahl $n = p_1 \cdot \ldots \cdot p_r + 1$. Dann existiert eine Primzahl p welche n teilt. Da $p_1, \ldots, p_r$ alle Primzahlen sind, gilt $p = p_i$ für ein gewisses i. Wegen $p|n$ und $p|p_1 \cdot \ldots \cdot p_r$ folgt auch $p|1$, ein Widerspruch. ❑

Zur Bestimmung aller Primzahlen welche kleiner als eine gewisse Zahl n sind kann man wie folgt vorgehen (*Sieb des Eratosthenes*[10]): Man schreibt alle natürlichen Zahlen bis n auf und streicht 1. Die erste Zahl die stehen bleibt, nämlich 2, ist eine Primzahl. Alle anderen Vielfachen von 2 streicht man. Die nächste Zahl die stehenbleibt, nämlich die 3, ist Primzahl. Alle weiteren Vielfachen von 3 streicht man. Dieses Verfahren setzt man fort bis man bei der ersten Zahl angelangt ist, deren Quadrat größer ist als n.

Zum Beispiel bestimmen wir alle Primzahlen $p \leq 57$:

$$\not{1}\ 2\ 3\ \not{4}\ 5\ \not{6}\ 7\ \not{8}\ \not{9}\ \not{10}\ 11\ \not{12}\ 13\ \not{14}\ \not{15}\ \not{16}\ 17\ \not{18}\ 19\ \not{20}$$

$$\not{21}\ \not{22}\ 23\ \not{24}\ \not{25}\ \not{26}\ \not{27}\ \not{28}\ 29\ \not{30}\ 31\ \not{32}\ \not{33}\ \not{34}\ \not{35}\ \not{36}\ 37\ \not{38}\ \not{39}\ \not{40}$$

$$41\ \not{42}\ 43\ \not{44}\ \not{45}\ \not{46}\ 47\ \not{48}\ \not{49}\ \not{50}\ \not{51}\ \not{52}\ 53\ \not{54}\ \not{55}\ \not{56}\ \not{57}$$

Gestrichen wurden alle Vielfachen von 2,3,5 und 7 ($8^2 = 64 > 57$). Alle Primzahlen ≤ 57 sind also

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53.$$

Wegen ihrer weiten Verbreitung im alltäglichen Gebrauch[11], wollen wir noch eine Möglichkeit angeben natürliche Zahlen darzustellen.

2.4.16 Proposition (Zifferndarstellung zur Basis b)**.** *Sei $b \in \mathbb{N}$, $b > 1$, gegeben, und bezeichne*

$$\mathcal{Z} := \left\{ (z_l)_{l \in \mathbb{N}_0} \in \prod_{l \in \mathbb{N}_0} \{0, \ldots, b-1\} : \quad \exists\, N \in \mathbb{N}_0 : x_l = 0, l \geq N \right\}.$$

Dann ist die Abbildung

$$\zeta_b : \left\{ \begin{array}{rcl} \mathcal{Z} & \to & \mathbb{N}_0 \\ (z_l)_{l \in \mathbb{N}_0} & \mapsto & \sum_{l \in \mathbb{N}_0} z_l b^l \end{array} \right.$$

bijektiv.

[10] Eratosthenes von Kyrene. $\sim$ 284 v.C. Kyrene (Shahhat, Lybien) - $\sim$ 200 v.C. Alexandria
[11] Wie zum Beispiel stillschweigend auch in den vorangegangenen Zeilen...

Beweis. Als allererstes müssen wir bemerken, dass, auf Grund der Definition von $\mathcal{Z}$, in der Summe auf der rechten Seite der Definition von ζ_b immer nur endlich viele von Null verschiedene Summanden auftreten. Die Definition ist also sinnvoll.

Um zu sehen, dass ζ_b surjektiv ist, verwenden wir Induktion. Klarerweise gilt

$$0 = \sum_{l\in\mathbb{N}_0} 0\cdot b^l = \zeta_b\big((0,0,0,\ldots)\big)\,.$$

Sei vorausgesetzt dass alle Zahlen $\le n$ im Bild von ζ_b liegen. Betrachte zuerst den Fall $b \nmid n+1$. Schreibe $n = \zeta_b\big((z_0,z_1,z_2,\ldots)\big) = \sum_{l\in\mathbb{N}_0} z_l b^l$, dann muss $z_0 \neq b-1$ sein. Also folgt

$$n+1 = (z_0+1) + \sum_{l\in\mathbb{N}} z_l b^l = \zeta_b\big((z_0+1,z_1,z_2,\ldots)\big)\,.$$

Im Fall $b \mid n+1$ schreibe $\frac{n+1}{b} = \zeta_b\big((z_0,z_1,z_2,\ldots)\big) = \sum_{l\in\mathbb{N}_0} z_l b^l$. Dann folgt

$$n+1 = b\Big(\sum_{l\in\mathbb{N}_0} z_l b^l\Big) = \sum_{l\in\mathbb{N}_0} z_l b^{l+1} = \zeta_b\big((0,z_0,z_1,z_2,\ldots)\big)\,.$$

Wir kommen zur Injektivität. Seien $(z_l)_{l\in\mathbb{N}_0}, (z'_l)_{l\in\mathbb{N}_0} \in \mathcal{Z}$ gegeben, und gelte $\zeta_b\big((z_l)_{l\in\mathbb{N}_0}\big) = \zeta_b\big((z'_l)_{l\in\mathbb{N}_0}\big)$, d.h.

$$\sum_{l\in\mathbb{N}_0} z_l b^l = \sum_{l\in\mathbb{N}_0} z'_l b^l.$$

Betrachte die Menge aller Zahlen $l\in\mathbb{N}_0$ sodaß $z_l - z'_l \neq 0$. Ist diese Menge leer, so haben wir $(z_l)_{l\in\mathbb{N}_0} = (z'_l)_{l\in\mathbb{N}_0}$. Angenommen sie wäre nichtleer. Dann besitzt sie ein kleinstes Element l_0. Nun gilt $\sum_{l\in\mathbb{N}_0}(z_l - z'_l)b^l = 0$, und es folgt

$$b^{l_0+1}\Big|\sum_{l\in\mathbb{N}_0}(z_l-z'_l)b^l = (z_{l_0}-z'_{l_0})b^{l_0} + \sum_{l\ge l_0+1}(z_l-z'_l)b^l\,.$$

Jeder Summand der letzten Summe wird sicher von b^{l_0+1} geteilt, also muss auch $(z_{l_0}-z'_{l_0})b^{l_0}$ durch b^{l_0+1} geteilt werden, und damit $b|(z_{l_0}-z'_{l_0})$. Da $z_{l_0}-z'_{l_0} \in \{-(b-1),\ldots,-1,0,1,\ldots,b-1\}$, folgt $z_{l_0}-z'_{l_0}=0$, ein Widerspruch. ❑

Man schreibt zur Abkürzung auch

$$\zeta_b\big((z_l)_{l\in\mathbb{N}_0}\big) =: z_{l_{\max}} z_{l_{\max}-1}\ldots z_1 z_0\,,$$

wobei $l_{\max} := \max\{l\in\mathbb{N}_0 : z_l \neq 0\}$. Damit dies Sinn macht, muss natürlich aus dem Zusammenhang klar sein welchen Wert b hat.

Kapitel 3

Die reellen Zahlen

3.1 Nicht-rationale Grössen

Die Mathematik früher Zeit hat sich ausführlich mit geometrischen Objekten beschäftigt, und man hat lange die Philosophie vertreten dass sich jedes Objekt in dieser Welt durch natürlichen Zahlen beschreiben läßt. Die Entdeckung von sogenannten inkommensurablen (nicht gemeinsam meßbaren) Größen hat diese Anschauung jedoch wiederlegt. Wir wollen nun zwei Beispiele solcher geometrischen Größen geben. Zuerst müssen wir dazu den Begriff der Inkommensurabilität etwas exakter formulieren.

Das Messen einer Strecke a funktioniert zum Beispiel so, daß man eine bestimmte Maßeinheit e hintereinanderlegt bis man a ausgeschöpft hat. Diese Methode ist natürlich nur dann zielführend, wenn die Strecke a ein ganzzahliges Vielfaches der Maßeinheit e ist, $a = m \cdot e$ mit $m \in \mathbb{N}$.

3.1.1 Definition. Zwei Strecken a_1 und a_2 heißen *kommensurabel* (gemeinsam messbar), wenn es eine Maßeinheit e gibt, sodaß sich sowohl a_1 als auch a_2 mit Hilfe von e messen lassen. In diesem Fall ist dann $a_1 = m_1 e$, $a_2 = m_2 e$. Das Verhältnis $a_1 : a_2$ ist also gleich $m_1 : m_2$, dem Verhältnis zweier ganzer Zahlen. Sind die Strecken a_1, a_2 nicht kommensurabel, so heißen sie *inkommensurabel*. //

Um zu zwei gegebenen Strecken a_1, a_2 eine gemeinsame Maßeinheit zu bestimmen, geht man wie folgt vor (*Verfahren der Wechselwegnahme*): Man trägt die kleinere Strecke (o.B.d.A. a_2) so oft wie möglich auf der größeren ab, den Rest bezeichne man mit a_3, sodaß also $a_3 < a_2$. Diesen Schritt iteriert man solange wie möglich. In Formeln:

$$a_1 = n_1 a_2 + a_3 \text{ mit } a_3 < a_2.$$

Mit a_2 und a_3 verfährt man genauso:

$$a_2 = n_2 a_3 + a_4 \text{ mit } a_4 < a_3.$$

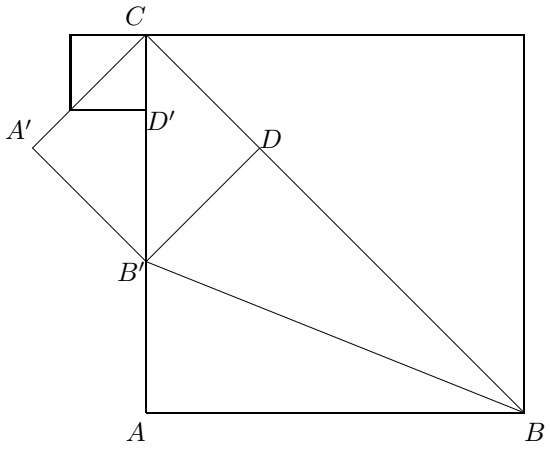
Und so weiter, solange der neu entstehende Rest verschieden von Null ist.

Bricht dieses Verfahren in einem Schritt ab, d.h. ist $a_{i+1} = 0$ für ein gewisses i, so hat man mit a_i ein gemeinsames Maß für die Strecken a_1 und a_2 gefunden.

Haben umgekehrt a_1 und a_2 ein gemeinsames Maß, ist also $a_1 = m_1 e$ und $a_2 = m_2 e$ mit einer gewissen Strecke e, so beschreibt dieses Vefahren genau den Euklidischen Algorithmus zur Bestimmung des größten gemeinsamen Teilers $\mathrm{ggT}\{m_1, m_2\}$, es bricht also ab.

3.1.2. *Schlußfolgerung:* *Zwei Strecken sind genau dann kommensurabel, wenn das Verfahren der Wechselwegnahme abbricht, was wiederum genau dann der Fall ist, wenn sie ein rationales Verhältnis haben.*

3.1.3 Beispiel. Wir betrachten Seite und Diagonale eines Quadrates und führen das Verfahren der Wechselwegnahme durch.



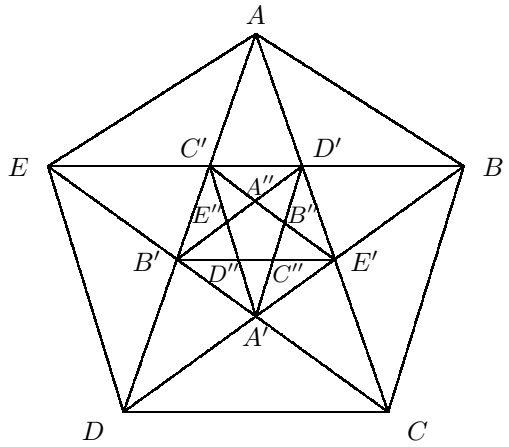
Auf der Diagonalen BC trägt man die Seite AB ab und erhält den Punkt D. In D zeichnet man die Senkrechte auf die Diagonale und schneidet sie mit der Seite AC um den Punkt B' zu erhalten. Ein solcher Schnittpunkt existiert, da wegen der Dreiecksungleichung sicher $AB < BC < 2AB$. Nun gilt $\angle CB'D = \angle CBA$ also auch gleich $\angle ACB$. Das Dreieck $\bigtriangleup(B'DC)$ ist also gleichschenkelig und rechtwinkelig, man kann es daher zu einem Quadrat vervollständigen. Die Seite diesses Quadrates ist der Diagonalrest CD. Die Dreiecke $\bigtriangleup(ABB')$ und $\bigtriangleup(BDB')$ sind kongruent, denn sie haben zwei Seiten und den der größeren Seite gegenüberliegender Winkel gemeinsam. Es folgt also $AB' = CD$.

Mit dem kleineren Quadrat verfährt man genauso. Und so weiter. Dieses Verfahren kann nie abbrechen, da Diagonale und Seite eines Quadrates stets verschieden lang sind; man erhält bloss immer kleinere Quadrate.

Wir schliessen, dass das Seite und Diagonale eines Quadrates inkommensurabel sind, und ihr Verhältnis daher keine rationale Zahl ist. //

3.1.4 Beispiel (Hippasos[1]). Betrachten wir nun ein regelmäßiges Fünfeck $ABCDE$:

[1] Hippasos von Metapont. um 450 v.C.



Die Diagonalen erzeugen in der Mitte ein kleineres regelmäßiges Fünfeck $A'B'C'D'E'$. Je eine Seite und eine Diagonale am regelmäßigen Fünfeck sind aus Symetriegründen parallel. Die Dreiecke AED und $BE'C$ haben daher parallele Seiten, sind also ähnlich. Es folgt

$$AD : AE = BC : BE'.$$

Es ist $AE = DE'$, da AE und BD bzw. DE und AC parallel sind. Damit folgt

$$BE' = BD - AE,$$

und obiges Verhältnis besagt also

$$\text{Diagonale} : \text{Seite} = \text{Seite} : (\text{Diagonale - Seite}).$$

Beachte insbesondere, daß $BD - AE < BC$ folgt.

Bezeichne a_1 die Diagonale, a_2 die Seite, a_3 ihre Differenz, so ist also

$$a_1 = 1 \cdot a_2 + a_3,\ a_3 < a_2$$

Setze $a_4 = a_2 - a_3$, dann ist

$$a_4 = BC - (BD - BC) = 2 \cdot BC - BD = (BA' + DE') - BD = A'E',$$

also ist a_4 die Seite des Fünfecks $A'B'C'D'E'$. Die Dreiecke $\bigtriangleup(BE'C)$ und $\bigtriangleup(BE'C')$ sind Spiegelbilder voneinander. Denn $BC = BC'$ und wegen

$$\angle BE'C = \pi - \angle E'BC - \angle C'BE' = \pi - 2\angle E'BC,$$

wobei das letzte Gleichheitszeichen gilt da $\bigtriangleup(CE'B)$ gleichschenkelig ist, folgt $\angle BCE' = \angle BC'E'$. Also ist $BE' = C'E'$ und daher $a_3 = E'C'$. Es folgt $a_4 < a_3$, d.h.

$$a_2 = 1 \cdot a_3 + a_4,\ a_4 < a_3.$$

Da a_3 und a_4 Diagonale bzw. Seite der kleineren Fünfecks sind können wir das gleiche Argument wiederholen und erhalten

$$a_3 = 1 \cdot a_4 + a_5,\ a_5 < a_4$$

$$a_4 = 1 \cdot a_5 + a_6,\ a_6 < a_5$$

$$a_5 = 1 \cdot a_6 + a_7,\ a_7 < a_6$$

.....

Dieses Verfahren bricht nie ab, denn man erhält einfach immer kleinere Fünfecke. Seite und Diagonale eines Fünfecks sind aber stets voneinander verschieden.

Das oben beschriebene Verfahren ist genau das Verfahren der Wechselwegnahme für Diagonale und Seite des Fünfecks. Die Diagonale und Seite eines regelmäßigen Fünfecks haben also kein rationales Verhältnis. //

Diese beiden Beispiele beruhen auf der gleichen allgemeinen Feststellung, nämlich, dass man im Körper $\mathbb{Q}$ nicht immer Wurzelziehen kann. Man kann nämlich zeigen, dass, wenn x und y das Verhältnis von Diagonale und Seite eines Quadrates bzw. eines regelmäßigen Fünfecks bezeichnen, die Beziehungen

$$x^2 = 2, \quad (2y-1)^2 = 5$$

gelten.

3.1.5 Definition. Sei K ein Körper, $n \in \mathbb{N}$, und $x \in K$. Eine Zahl $y \in K$ heißt eine *n-te Wurzel* von x, wenn $y^n = x$ gilt. Im Fall $n = 2$ spricht man auch von einer *Quadratwurzel*. //

3.1.6 Proposition. *Sei $n \in \mathbb{N}$ und sei $k \in \mathbb{N}$ so daß k nicht n-te Potenz einer natürlichen Zahl ist. Dann ist k auch nicht n-te Potenz einer rationalen Zahl.*

Beweis. Wir zeigen zunächst: Seien $a, b \in \mathbb{N}$ mit $b^n | a^n$, dann gilt auch $b|a$. Seien $a = \prod p_i^{r_i}$, $b = \prod q_i^{s_i}$ die Primfaktorzerlegungen von a und b. Wegen $b^n | a^n$ muß $r_i n \geq s_i n$ sein. Also ist auch $r_i \geq s_i$, und damit $b|a$.

Sei nun $x \in \mathbb{Q}$, $x = \frac{a}{b}$ mit $x^n = k \in \mathbb{N}$, d.h. $\frac{a^n}{b^n} = k$. Dann ist $b^n | a^n$, und es folgt $b|a$, d.h. $x \in \mathbb{N}$. ❑

Diese Aussage zeigt uns, dass es im Körper $\mathbb{Q}$ sehr viele Zahlen gibt die keine Quadratwurzel haben. Denn die Quadrate natürlicher Zahlen sind ja nur $1 = 1^2, 4 = 2^2, 9 = 3^2, 16 = 4^2, \ldots$.

Um geometrischen Größen wie den oben diskutierten (aber auch vielen anderen, z.B. der Länge des Umfang eines Kreises mit Radiu 1) Maßzahlen zuordnen zu können, und sie damit einer algorithmischen Behandlung zugänglich zu machen, ist es also notwendig eine weitere Erweiterung des betrachteten Zahlbereiches vorzunehmen.

3.2 Die reellen Zahlen

Wir wollen nun jene Eigenschaft herausfiltern, deren Absenz im Körper $\mathbb{Q}$ für die im letzten Abschnitt festgestellten Phänomene verantwortlich ist.

3.2.1 Definition. Sei $\langle K, +, \cdot, \leq \rangle$ ein angeordneter Körper. Dann heißt K *vollständig angeordnet*, wenn „$\leq$“ die Supremumseigenschaft hat. //

Die Supremumseigenschaft besagt, dass jede nichtleere nach oben beschränkte Menge ein Supremum hat. Da in einem angeordneten Körper $x \leq y$ genau dann gilt wenn $-y \leq -x$, ist dieses äquivalent dazu, dass jede nichtleere nach unten beschränkte Menge ein Infimum besitzt.

Wir werden zeigen, dass es im wesentlichen genau einen vollständig angeordneten Körper gibt, vgl. Satz 3.2.4, und diesen werden wir dann den Körper der reellen Zahlen nennen. Vorher wollen wir uns aber überlegen was man mit der Supremumseigenschaft alles machen kann. Wir wollen in Erinnerung rufen, dass jeder angeordnete Körper die rationalen Zahlen $\mathbb{Q}$ als Teilkörper enthält, vgl. Proposition 2.3.4.

3.2.2 Proposition. *Sei $\langle K, +, \cdot, \leq \rangle$ ein vollständig angeordneter Körper. Dann gilt:*

(*i*) *K ist archimedisch angeordnet.*

(*ii*) *Ist $x, y \in K$, $x < y$, dann existiert $p \in \mathbb{Q}$ mit $x < p < y$.*

Die Aussage (ii) nennt man auch die Dichteeigenschaft *von $\mathbb{Q}$ in K.*

Beweis. Angenommen die Aussage (i) wäre falsch. Dann gibt es $x, y \in K, x > 0$, mit $nx \leq y$ für alle $n \in \mathbb{N}$. Also ist die nichtleere Menge $A := \{nx : n \in \mathbb{N}\}$ nach oben beschränkt, und daher existiert $\alpha := \sup A$. Da $x > 0$ ist, ist $\alpha - x < \alpha$ und daher keine obere Schranke von A. D.h. es gibt eine Zahl $m \in \mathbb{N}$ sodass $\alpha - x < mx$. Es folgt $\alpha < (m+1)x$, ein Widerspruch. Also ist die Aussage (i) richtig.

Wir kommen zum Beweis von (ii). Seien $x, y \in K$ mit $x < y$ gegeben. Dann ist $y - x > 0$. Wendet man (i) an mit $(y - x)$ und 1, so folgt dass es eine Zahl $n \in \mathbb{N}$ gibt mit $n(y - x) > 1$. Wendet man (i) an mit 1 und nx bzw. $-nx$, so erhält man natürliche Zahlen m_1, m_2 mit $m_1 \cdot 1 > nx$ sowie $m_2 \cdot 1 > -nx$. Also ist $-m_2 < nx < m_1$. Da es nur endlich viele ganze Zahlen m zwischen $-m_2$ und m_1 gibt, muss für eine von ihnen gelten $m - 1 \leq nx < m$. Kombiniert man diese Ungleichung mit $n(y - x) > 1$, so folgt

$$nx < m \leq nx + 1 < ny\,,$$

und damit $x < \frac{m}{n} < y$. ❑

3.2.3 Proposition. *Sei K ein vollständig angeordneter Körper, sei $x \in K$, $x > 0$, und sei $n \in \mathbb{N}$. Dann existiert genau eine Zahl $y \in K$, $y > 0$, sodass $y^n = x$.*

Beweis. Wir zeigen zuerst die Eindeutigkeit. Seien $y_1, y_2 > 0$ und sei z.B. $y_1 < y_2$. Dann folgt auch $y_1^n < y_2^n$ und daher können nicht beide der Gleichung $y^n = x$ genügen.

Wir kommen zum Beweis der Existenz. Sei $E := \{t \in K : t > 0, t^n < x\}$. Betrachte $t_0 := \frac{x}{1+x}$. Dann ist $0 < t_0 < 1$ und daher $t_0^n < t_0$. Weiters ist $t_0 < x$, insgesamt sehen wir das $t_0^n < x$. Also ist $E \neq \emptyset$. Setze $t_0 := 1 + x$, dann ist $t_0 > 1$, also auch $t_0^n > t_0$. Weiters ist $t_0 > x$. Ist nun $t \geq t_0$, so erhalten wir $t^n \geq t_0^n > x$, d.h. $t \notin E$. Also ist E nach oben beschränkt, z.B. ist ja t_0 eine obere Schranke.

Da K vollständig angeordnet ist, existiert $y := \sup E$. Wegen $0 < \frac{x}{1+x} \in E$ ist sicher $y > 0$. Wir zeigen im folgenden dass $y^n = x$ ist, und zwar indem wir die beiden anderen Möglichkeiten $y^n < x$ und $y^n > x$ ausschliessen.

Dazu machen wir die folgende Bemerkung. Für beliebige Elemente $a, b \in K$ gilt

$$b^n - a^n = (b-a)(b^{n-1} + b^{n-2}a + \ldots + ba^{n-2} + a^{n-1})\,.$$

Also erhalten wir für $0 < a < b$ die Abschätzung

$$b^n - a^n < (b-a)nb^{n-1}\,.$$

Sei nun angenommen $y^n < x$. Wähle $h \in \mathbb{Q}$ mit $0 < h < 1$ und

$$h < \frac{x - y^n}{n(y+1)^{n-1}}\,.$$

Dies ist möglich denn $x - y^n > 0$ und wegen der Dichteeigenschaft von $\mathbb{Q}$. Setze in obiger Abschätzung $a = y$ und $b = y + h$. Dann folgt

$$(y+h)^n - y^n < hn(y+h)^{n-1} < hn(y+1)^{n-1} < x - y^n\,.$$

Also ist $(y+h)^n < x$ und daher $y + h \in E$. Ein Widerspruch, denn y ist eine obere Schranke von E.

Sei nun angenommen $y^n > x$. Setze

$$k := \frac{y^n - x}{ny^{n-1}}\,.$$

Dann ist $0 < k < y$. Ist $t \geq y - k$, so folgt wieder unter Verwendung obiger Abschätzung, diesmal mit $b = y, a = (y-k)$

$$y^n - t^n \leq y^n - (y-k)^n < kny^{n-1} = y^n - x\,.$$

Also ist $t^n > x$ und daher $t \notin E$. Wir sehen das $y - k$ eine obere Schranke von E ist, ein Widerspruch denn y ist die kleinste obere Schranke von E. ❑

Die nach obiger Proposition eindeutig bestimmte Zahl $y > 0$, die ja eine n-te Wurzel von x ist, schreibt man auch als $\sqrt[n]{x}$.

Die Existenz von Wurzeln in einem vollständig angeordneten Körper ermöglicht uns eine in gewissem Sinne allgemeinere Potenzfunktion zu definieren. Bisher hatten wir die Potenzfunktion für natürliche Zahlen als Exponenten betrachtet:

$$\left\{\begin{array}{rcl} K \times \mathbb{N} & \to & K \\ (x,y) & \mapsto & x^y := \underbrace{x \cdot \ldots \cdot x}_{y\text{-mal}} \end{array}\right.$$

Nun definieren wir ($K^+ := \{x \in K : x > 0\}$, $\mathbb{Q}^+ := \{x \in \mathbb{Q} : x > 0\}$)

$$\left\{\begin{array}{rcl} K^+ \times \mathbb{Q}^+ & \to & K^+ \\ (x, \frac{p}{n}) & \mapsto & x^{\frac{p}{n}} := \underbrace{\sqrt[n]{x} \cdot \ldots \cdot \sqrt[n]{x}}_{p\text{-mal}} \end{array}\right. \tag{3.2.1}$$

Obwohl man hier die gleiche Symbolik verwendet, nämlich x^y, ist aufgrund der verschiedenen Definitionsbereiche ($K \times \mathbb{N}$ bzw. $K^+ \times \mathbb{Q}^+$) Vorsicht geboten.

Man kann die Funktion (3.2.1) einfach zu einer Funktion $K^+ \times \mathbb{Q} \to K^+$ fortsetzen, nämlich indem man

$$x^0 := 1, \quad x \in K^+$$
$$x^{-\frac{p}{n}} := \frac{1}{x^{\frac{p}{n}}}, \quad x \in K^+, \frac{p}{n} \in \mathbb{Q}^+$$

setzt. Mit diesen Definitionen kann man die folgenden Rechenregeln zeigen: Für $x, x_1, x_2 \in K^+$ und $y, y_1, y_2 \in \mathbb{Q}$ gilt

$$(x_1 x_2)^y = x_1^y x_2^y, \quad x^{y_1} x^{y_2} = x^{y_1+y_2}, \quad \left(x^{y_1}\right)^{y_2} = x^{y_1 y_2}\,.$$

Wir wollen nun aber zum Hauptergebnis dieses Abschnittes kommen. Um diese, anspruchsvolle, Konstruktion zu motivieren denken wir uns eine Gerade gezeichnet, gemeinsam mit einer Einheitsstrecke. Auf dieser Geraden denken wir uns die rationalen Zahlen durch fortgesetztes auftragen und unterteilen der Einheitsstrecke aufgetragen. Obwohl es -anschaulich- beliebig nahe an jedem Punkt eine rationale Zahl gibt, gibt es nach dem im letzten Abschnitt Gesagten Punkte welche nicht rational sind, zum Beispiel die Länge der Diagonale eines regelmäßigen Fünfecks mit Seitenlänge 1.

Unsere Konstruktion beruht auf der folgenden Bemerkung, die R.Dedekind[2] gemacht hat:

> „Zerfallen alle Punkte der Geraden in zwei Klassen von der Art, daß jeder Punkt der ersten Klasse links von jedem Punkt der zweiten Klasse liegt, so existiert ein und nur ein Punkt, welcher diese Einteilung aller Punkte in zwei Klassen, diese Zerschneidung der Geraden in zwei Stücke, hervorbringt."

Man kann also einen Punkt P der Geraden identifizieren mit der Menge aller Punkte die links von ihm liegen. Da man nun aber mit den rationalen Punkten beliebig nahe an den Punkt P herankommt, genügt es alle rationalen (!) Punkte die links von P liegen zu kennen um P selbst eindeutig zu rekonstruieren.

3.2.4 Satz. *Es gibt einen vollständig angeordneten Körper. Dieser ist bis auf Isomorphie eindeutig bestimmt.*

Beweis. Der Beweis dieses Satzes ist relativ lang und wird in mehreren Schritten geführt, von denen wir auch nicht alle im Detail ausführen werden.

Schritt 1: Eine Teilmenge α von $\mathbb{Q}$ heißt ein *Dedekindscher Schnitt*, wenn sie die folgenden drei Eigenschaften besitzt:

(DS1) $\alpha \neq \emptyset$, $\alpha \neq \mathbb{Q}$.

(DS2) Ist $p \in \alpha$ und $q \in \mathbb{Q}$ mit $q < p$, dann ist auch $q \in \alpha$.

(DS3) Ist $p \in \alpha$, so existiert $r \in \alpha$ mit $r > p$.

Die Menge aller Dedekindschen Schnitte bezeichnen wir mit K.

Dieser Begriff modelliert die Anschauung der Menge aller (rationalen) Punkte die „links von dem Punkt (der Geraden) liegen".

Die Eigenschaft (DS3) besagt das α kein größtes Element hat. Aus der Eigenschaft (DS2) erhält man unmittelbar die folgenden beiden Aussagen:

(i) Ist $p \in \alpha$ und $q \notin \alpha$, dann ist $p < q$.

(ii) Ist $r \notin \alpha$ und $s > r$, so ist $s \notin \alpha$.

[2]Richard Dedekind. 6.10.1831 Braunschweig - 12.2.1916 Braunschweig

Schritt 2: Wir definieren eine Relation „$\leq$“ auf K durch

$$\alpha \leq \beta \ :\Longleftrightarrow \ \ \alpha \subseteq \beta,\ \alpha, \beta \in K\,.$$

Diese Relation ist offenbar eine Ordnungsrelation. Wir zeigen das sie sogar eine Totalordnung ist. Seien $\alpha, \beta \in K$ und sei angenommen das $\alpha \not\leq \beta$, d.h. $\alpha \not\subseteq \beta$. Dann existiert also $p \in \alpha$ mit $p \notin \beta$. Es folgt das für alle $q > p$ gilt $q \notin \beta$ und das für alle $q < p$ gilt $q \in \alpha$. Ist also $q \in \beta$, so muss $q < p$ sein und daher zu α gehören. D.h. es gilt $\beta \leq \alpha$.

Schritt 3: In diesem Schritt zeigen wir das K mit der Ordnung $\leq$ die Supremumseigenschaft besitzt. Sei $A \subseteq K$ eine nichtleere und nach oben beschränkte Teilmenge von K. Setze

$$\gamma := \bigcup_{\alpha \in K} \alpha\,.$$

Wir zeigen das $\gamma \in K$. Da A nichtleer ist, existiert $\alpha_0 \in A$. Nun ist α_0 nichtleer und $\alpha_0 \subseteq \gamma$, also ist auch $\gamma \neq \emptyset$. Da A nach oben beschränkt ist, existiert $\beta \in K$ mit $\alpha \subseteq \beta$ für alle $\alpha \in A$. Daher ist auch $\gamma \subseteq \beta$. Da $\beta \neq \mathbb{Q}$, ist auch $\gamma \neq \mathbb{Q}$. Also erfüllt γ die Eigenschaft (DS1). Ist $p \in \gamma$, so existiert $\alpha \in A$ mit $p \in \alpha$. Also gehört jedes $q < p$ auch zu α und damit zu γ. Weiters existiert $r \in \alpha$ mit $r > p$. Dieses r gehört ebenfalls zu γ. Wir sehen das γ die Eigenschaften (DS2) und (DS3) hat.

Wir zeigen das $\gamma = \sup A$. Die Tatsache das $\alpha \leq \gamma$ für alle $\alpha \in A$ ist klar. Ist $\beta \in K$ mit $\beta \geq \alpha$, $\alpha \in A$, d.h. $\beta \supseteq \alpha$, $\alpha \in A$, so folgt da γ die Vereinigung aller $\alpha \in A$ ist, das $\beta \supseteq \gamma$.

Schritt 4: Wir definieren eine Addition auf K. Für $\alpha, \beta \in K$ setze

$$\alpha + \beta := \big\{r + s :\ r \in \alpha, s \in \beta\big\}\,.$$

Weiters setze $0^* := \{p \in \mathbb{Q} :\ p < 0\}$.

Als erstes zeigen wir das tatsächlich $\alpha + \beta \in K$. Da $\alpha \neq \emptyset$ und $\beta \neq \emptyset$, folgt das auch $\alpha + \beta \neq \emptyset$. Wähle $r' \notin \alpha$ und $s' \notin \beta$, dann ist $r' > r$, $r \in \alpha$, und $s' > s$, $s \in \beta$. Also erhalten wir $r' + s' > r + s$, $r \in \alpha, s \in \beta$. Damit kann $r' + s'$ nicht zu $\alpha + \beta$ gehören. Wir sehen das $\alpha + \beta$ die Eigenschaft (DS1) besitzt. Sei nun $p \in \alpha + \beta$ gegeben, und schreibe $p = r + s$ mit gewissen $r \in \alpha$, $s \in \beta$. Ist $q < p$, so ist $q - s < r$ und daher $q - s \in \alpha$. Also ist $q = (q - s) + s \in \alpha + \beta$, und wir sehen das (DS2) gilt. Wähle $t \in \alpha$ mit $t > r$, dann folgt $t + s > p$ und $t + s \in \alpha + \beta$, also gilt auch (DS3).

Die Addition ist kommutativ, denn es gilt

$$\alpha + \beta = \{r + s :\ r \in \alpha, s \in \beta\} = \{s + r :\ r \in \alpha, s \in \beta\} = \beta + \alpha\,.$$

Sie ist assoziativ, denn

$$\alpha + (\beta + \gamma) = \big\{r + u :\ r \in \alpha, u \in (\beta + \gamma)\big\} =$$

$$= \big\{r + (s + t) :\ r \in \alpha, s \in \beta, t \in \gamma\big\} = \big\{(r + s) + t :\ r \in \alpha, s \in \beta, t \in \gamma\big\} =$$

$$= \big\{v + t :\ v \in (\alpha + \beta), t \in \gamma\big\} = (\alpha + \beta) + \gamma\,.$$

Wir zeigen das 0^* neutrales Element bezüglich der Addition ist. Ist $r \in \alpha$ und $s \in 0^*$, so ist $r + s < r$, also $r + s \in \alpha$. D.h. $\alpha + 0^* \leq \alpha$. Sei umgekehrt $p \in \alpha$. Wähle $r \in \alpha$, $r > p$. Dann gilt $p = r + (p - r) \in \alpha + 0^*$.

Es bleibt zu zeigen das jedes Element von K ein additives Inverses besitzt. Sei also $\alpha \in K$ gegeben. Setze

$$\beta := \left\{p \in \mathbb{Q} : \exists\, r > 0 : -p - r \notin \alpha\right\}.$$

Als erstes zeigen wir das $\beta \in K$. Sei $s \notin \alpha$ und setze $p := -s - 1$, dann ist $-p - 1 = s \notin \alpha$, also $p \in \beta$, d.h. $\beta \neq \emptyset$. Ist $q \in \alpha$, so ist $-q \notin \beta$ und damit $\beta \neq \mathbb{Q}$. Es gilt also (DS1). Sei nun $p \in \beta$ gegeben. Wähle $r > 0$ sodass $-p-r \notin \alpha$. Ist $q < p$, so gilt $-q - r > -p - r$ und daher $-q - r \notin \alpha$, d.h. $q \in \beta$. Es gilt also (DS2). Setze $t := p + \frac{r}{2}$. Dann ist $t > p$ und $-t - \frac{r}{2} = -p - r \notin \alpha$, d.h. $t \in \beta$. Also gilt (DS3).

Ist $r \in \alpha$ und $s \in \beta$, so ist $-s \notin \alpha$ und daher $r < -s$. Daher ist $r + s < 0$, d.h. $r + s \in 0^*$. Wir sehen das $\alpha + \beta \leq 0^*$.

Umgekehrt sei $v \in 0^*$. Setze $w := -\frac{v}{2}$, dann ist $w > 0$. Sei $q \notin \alpha$, dann gibt es, da $\mathbb{Q}$ archimedisch angeordnet ist, $n_1 \in \mathbb{N}$ mit $n_1 w > q$ und daher $n_1 w \notin \alpha$. Sei $q \in \alpha$, dann gibt es $n_2 \in \mathbb{N}$ mit $n_2 w > -q$, und daher mit $-n_2 w \in \alpha$. Es existiert also $n \in \mathbb{Z}$ mit $nw \in \alpha$ aber $(n+1)w \notin \alpha$. Setze $p := -(n+2)w$. Dann ist $p \in \beta$, denn $-p - w \notin \alpha$. Wir haben also

$$v = nw + p \in \alpha + \beta\,.$$

Schritt 5: Die Addition ist mit der Ordnung verträglich. Denn ist $\alpha \leq \beta$, d.h. $\alpha \subseteq \beta$, und ist $\gamma \in K$, so folgt $\alpha + \gamma \subseteq \beta + \gamma$.

Schritt 6: Wir definieren eine Multiplikation auf K. Seien zunächst $\alpha, \beta > 0$. Dann setze

$$\alpha \cdot \beta := \left\{p \in \mathbb{Q} : \exists r \in \alpha, s \in \beta, r, s > 0 : p \leq rs\right\}.$$

Man zeigt genauso wie in Schritt 4, dass $\alpha \cdot \beta$ tatsächlich ein Element von K ist, dass die Multiplikation kommutativ und assoziativ ist, und dass das Distributivgesetz gilt.

Weiters definieren wir

$$1^* := \{p \in \mathbb{Q} : p < 1\}\,.$$

Wieder sieht man analog wie in den vorherigen Beweisschritten dass 1^* neutrales Element bezüglich der Multiplikation ist und dass jedes Element $\alpha > 0$ ein multiplikatives Inverses $\beta > 0$ besitzt.

Um nun die Multiplikation auch für Elemente $\alpha < 0$ zu definieren, setze

$$\alpha \cdot \beta := \begin{cases} (-\alpha) \cdot (-\beta) & ,\ \alpha < 0^*, \beta < 0^* \\ (-\alpha) \cdot \beta & ,\ \alpha < 0^*, \beta > 0^* \\ \alpha \cdot (-\beta) & ,\ \alpha > 0^*, \beta < 0^* \end{cases}$$

Der Beweis der Rechengesetze folgt aus den bereits bekannten Regeln für die Multiplikation von positiven Zahlen durch Fallunterscheidungen.

Schritt 8: Wir zeigen das jeder vollständig angeordnete Körper L isomorph zu dem oben konstruierten Körper K ist. Beachte, dass L und K als angeordnete Körper den Körper der rationalen Zahlen enthalten. Definiere

$$\phi : \left\{ \begin{array}{ccc} L & \to & K \\ x & \mapsto & \{p \in \mathbb{Q} : p < x\} \end{array} \right. \quad , \quad \psi : \left\{ \begin{array}{ccc} K & \to & L \\ \alpha & \mapsto & \sup \alpha \end{array} \right.$$

Die Abbildung ϕ ist wohldefiniert, denn $\{p \in \mathbb{Q} : p < x\}$ ist ein Dedekindscher Schnitt. Auch ist ψ ist wohldefiniert, denn α ist eine nichtleere und beschränkte Teilmenge von $\mathbb{Q} \subseteq L$ und besitzt daher in L ein Supremum.

Man zeigt mit genau den gleichen Argumentationsweisen wie in den vorherigen Beweisschritten, dass ϕ und ψ zueinander inverse Bijektionen sind, welche mit Addition, Multiplikation und Ordnung verträglich sind. Also sind L und K als angeordnete Körper isomorph. ❑

Wir wollen festhalten, dass die Einbettung von $\mathbb{Q}$ in den oben konstruierten Körper K, die nach Proposition 2.3.4 existiert, explizit gegeben ist durch

$$q \mapsto \{p \in \mathbb{Q} : p < q\},\ q \in \mathbb{Q}\,.$$

3.2.5 Definition. Die *reellen Zahlen* $\mathbb{R}$ sind der (nach dem letzten Satz in eindeutiger Weise existierende) vollständig angeordnete Körper. //

3.3 Algebraische Gleichungen

Wir betrachten wieder Polynome über einem Körper K. Ist $p(X) = \sum a_n X^n \in K[X]$, $p \neq 0$, so definiert man den *Grad* von p als

$$\operatorname{grad} p := \max\{n \in \mathbb{N} \cup \{0\} : a_n \neq 0\}\,.$$

Man setzt oft formal $\operatorname{grad} 0 := -\infty$. Der Grad des Polynoms $p(X)$ ist also die höchste Potenz von X die in $p(X)$ tatsächlich vorkommt. Ist $\operatorname{grad} p = n$, so nennt man den Koeffizienten a_n auch den *Führungskoeffizienten* von p.

Für den Grad von Polynomen gelten die folgenden beiden Rechenregel welche sich unmittelbar aus der Definition von $+$ und $\cdot$ ergeben:

$$\operatorname{grad}(p+q) \leq \max\{\operatorname{grad} p, \operatorname{grad} q\}\,,$$

$$\operatorname{grad}(p \cdot q) = \operatorname{grad} p + \operatorname{grad} q,\ p, q \neq 0\,.$$

Der Körper K ist in $K[X]$ eingebettet indem man einer Zahl $a \in K$ das konstante Polynom $p_a(X) = a$ zuordnet. Diese Einbettung ist offenbar sowohl mit der Addition als auch mit der Multiplikation verträglich.

Ähnlich wie bei den natürlichen Zahlen gibt es auch in $K[X]$ einen *Divisionsalgorithmus*.

3.3.1 Proposition (Division mit Rest)**.** *Sind $p, q \in K[X]$, $q \neq 0$, so gibt es eindeutig bestimmte Polynome $s, r \in K[X]$ mit $p = sq + r$ und* $\operatorname{grad} r < \operatorname{grad} q$.

Beweis. Um die Existenz von s und r zu zeigen führen wir Induktion nach $\operatorname{grad} p$ durch.

Sei $\operatorname{grad} p = 0$, d.h. $p(X) = a_0$ mit $a_0 \in K \setminus \{0\}$. Falls $\operatorname{grad} q = 0$ ist, $q = c_0 \in K \setminus \{0\}$, dann setze $s := \frac{a_0}{c_0}$, $r := 0$. Andernfalls setze $s := 0$ und $r := p$.

Sei nun angenommen dass jedes Polynom p dessen Grad kleiner als N ist in der angegebenen Weise faktorisiert werden kann, und sei $p(X) = \sum_{n=0}^{N} a_n X^n$ ein Polynom vom Grad N. Ist $\operatorname{grad} q > \operatorname{grad} p$, so setze $s := 0$ und $r := p$.

Das ist eine Zerlegung der gewünschten Gestalt. Sei $\operatorname{grad} q \leq \operatorname{grad} p$, $q(X) = \sum_{n=0}^{M} b_n X^n$ mit $M = \operatorname{grad} q$. Betrachte

$$p_1(X) := p(X) - \frac{a_N}{b_M} X^{N-M} q(X)\,,$$

dann ist $\operatorname{grad} p_1 < \operatorname{grad} p = N$. Daher existiert nach Induktionsvoraussetzung s_1, r_1, $\operatorname{grad} r_1 < \operatorname{grad} q$, mit $p_1 = s_1 q + r_1$. Es folgt

$$p(X) = \big(s_1(X) + \frac{a_N}{b_M} X^{N-M}\big) q(X) + r_1(X)\,,$$

und das ist eine Zerlegung der gewünschten Gestalt.

Wir kommen zum Beweis der Eindeutigkeit. Angenommen wir haben $p = s_1 q + r_1 = s_2 q + r_2$ mit $\operatorname{grad} r_1, \operatorname{grad} r_2 < \operatorname{grad} q$. Dann folgt also

$$(s_1 - s_2)q = r_2 - r_1\,.$$

Ist $s_1 \neq s_2$, so haben wir $\operatorname{grad}((s_1 - s_2)q) = \operatorname{grad}(s_1 - s_2) + \operatorname{grad} q \geq \operatorname{grad} q$. Andererseits ist aber $\operatorname{grad}(r_1 - r_2) \leq \max\{\operatorname{grad} r_1, \operatorname{grad} r_2\} < \operatorname{grad} q$. Ein Widerspruch. Es folgt $s_1 = s_2$, und damit auch $r_1 = r_2$. ❑

Mit jedem Polynom in $K[X]$ kann man eine Funktion auf K assoziieren.

3.3.2 Definition. Sei K ein Körper, und $p \in K[X]$, $p(X) = \sum\limits_k a_k X^k$. Dann definieren wir die von p auf K induzierte *Polynomfunktion* als

$$F_p : \left\{ \begin{array}{ccc} K & \to & K \\ b & \mapsto & \sum\limits_{k=0}^{\operatorname{grad} p} a_k b^k \end{array} \right.$$

//

Man schreibt oft zur Abkürzung auch $p(b)$ anstelle von $F_p(b)$. Das ist recht anschaulich, denn man erhält ja $F_p(b)$ gerade in dem man in $p(X)$ die Variable X durch das Körperelement b ersetzt und die enstehende (endliche) Summe in K ausrechnet. Es kann jedoch auch zur Verwirrung Anlass geben, denn im allgemeinen muß man ein Polynom p von der Polynomfunktion Funktion F_p wohl unterscheiden. Z.B. kann es vorkommen das $p \neq 0$ ist, aber $F_p(b) = 0$ für alle $b \in K$. In den Fällen die bei uns normalerweise auftreten, $K = \mathbb{Q}, \mathbb{R}$ oder $\mathbb{C}$, kann man zeigen dass diese Unterscheidung nicht nötig ist[3].

Ist $p \in K[X]$, so kann man sich fragen welche Werte die Funktion $x \mapsto p(x)$, $x \in K$, annimmt. Speziell kann man sich nach ihren *Nullstellen* fragen, d.h. an welchen Stellen sie den Wert 0 annimmt. Man sucht also nach den Lösungen $x \in K$ einer Gleichung der Gestalt

$$p(x) = \sum_{k=0}^{N} a_k x^k = 0\,.$$

Eine solche Gleichung nennt man auch *algebraische Gleichung*. Im allgemeinen weiss man nicht ob eine solche Gleichung überhaupt Lösungen besitzt oder nicht.

[3]Genauer gesagt, es gilt: Für die angeführten Körper ist die Abbildung

$$\Phi : \left\{ \begin{array}{ccc} K[X] & \to & \{f : f \text{ Funktion von } K \text{ nach } K\} \\ p & \mapsto & F_p \end{array} \right.$$

injektiv.

3.3.3 Beispiel.

- Sei $p(X) = X^2 - 1 \in \mathbb{Q}[X]$. Die Gleichung $x^2 - 1 = 0$ hat in $\mathbb{Q}$ die beiden Lösungen $x = 1$ und $x = -1$, wie man durch Einsetzen sieht. Nun gilt für jedes $x \in \mathbb{Q}$, dass $x^2 - 1 = (x-1)(x+1)$, und daher kann es keine anderen Lösungen geben.
- Sei $p(X) = X^2 + 1 \in \mathbb{R}[X]$. Die Gleichung $x^2 + 1 = 0$ hat in $\mathbb{R}$ keine Lösung. Denn für jedes $x \in \mathbb{R}$ gilt $x^2 \geq 0$, und daher $x^2 + 1 \geq 1 > 0$.
- Sei $p(X) = X^3 + X \in \mathbb{R}[X]$. Die Gleichung $x^3 + x = 0$ hat in $\mathbb{R}$ eine Lösung, nämlich $x = 0$. Andere Lösungen kann es nicht geben, denn es gilt $p(x) = x(x^2 + 1)$.
- Sei $p(X) = X^3 \in \mathbb{R}[X]$. Die Gleichung $x^3 = 0$ hat in $\mathbb{R}$ ebenfalls genau eine Lösung, nämlich $x = 0$.
- Sei $p(X) = X^2 - 2 \in \mathbb{R}[X]$. Nach Proposition 3.2.3 hat die Gleichung $x^2 - 2 = 0$ eine Lösung in $\mathbb{R}$, nämlich $\sqrt{2}$. Durch Einsetzen folgt dass auch $-\sqrt{2}$ eine Lösung ist. Diese beiden Lösungen sind verschieden, denn $\sqrt{2} \neq 0$. Nun gilt für jedes $x \in \mathbb{R}$, dass $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$, und daher kann es keine anderen Lösungen geben.
- Sei $p(X) = X^2 - 2 \in \mathbb{Q}[X]$. Nach Proposition 3.1.6 hat die Gleichung $x^2 - 2 = 0$ keine Lösung in $\mathbb{Q}$.

Wir wollen festhalten, dass die Existenz und Anzahl von Lösungen einer algebraischen Gleichung überhaupt nicht von vornherein klar ist, und sogar davon abhängen kann welcher Körper zugrundegelegt wird. //

Aus dem Divisionsalgorithmus, vgl. Proposition 3.3.1, erhalten wir eine obere Schranke für die Anzahl der Nullstellen eines Polynoms.

3.3.4 Korollar. *Sei $p \in K[X]$, $p \neq 0$, dann hat p höchstens* $\operatorname{grad} p$ *viele Nullstellen.*

Beweis. Sei $x_0 \in K$ eine Nullstelle eines Polynomes $p \in K[X]$ mit $\operatorname{grad} p > 0$. Wir dividieren p mit Rest durch $(X - x_0)$. Dann erhalten wir $p(X) = s(X)(X - x_0) + r(X)$ mit $\operatorname{grad} r = 0$, d.h. r konstant. Setzt man in dieser Zerlegung speziell für X den Wert x_0 ein, so folgt

$$0 = p(x_0) = s(x_0) \underbrace{(x_0 - x_0)}_{=0} + r\,,$$

also $r = 0$. Damit haben wir $p(X) = s(X)(X - x_0)$ mit einem gewissen Polynom $s \in K[X]$. Offenbar muss dabei $\operatorname{grad} s = \operatorname{grad} p - 1$ gelten.

Um nun die Behauptung des Korollars zu zeigen, verwenden wir Induktion nach $\operatorname{grad} p$. Ist $\operatorname{grad} p = 0$, so ist also p konstant. Wegen $p \neq 0$ gibt es keine Nullstellen. Sei angenommen die Behauptung ist richtig für alle Polynome mit Grad kleiner als N und sei $p \in K[X]$ mit $\operatorname{grad} p = N$ gegeben. Hat p keine Nullstelle, so sind wir fertig. Ist x_0 eine Nullstelle von p, so können wir nach dem obigen $p(X) = s(X)(X - x_0)$ schreiben und dabei ist $\operatorname{grad} s < N$. Jede Nullstelle von p muss entweder eine Nullstelle von s oder gleich x_0 sein. Nach Induktionsvoraussetzung hat s höchstens $N - 1$ Nullstellen, insgesamt hat also p höchstens N Nullstellen. ❑

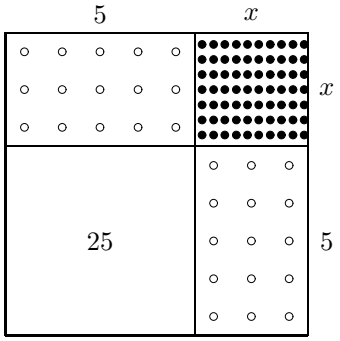
Wir wollen jedoch anmerken, dass jedes *lineares nichtkonstantes Polynom* in $K[X]$, das ist ein Polynom vom Grad 1, genau eine Nullstelle hat. Denn ist $p(X) = a_1X + a_0$ mit $a_1 \neq 0$, so ist

$$p(x) = 0 \iff x = -\frac{a_0}{a_1}\,.$$

Polynome mit reellen Koeffizienten; quadratische Gleichungen.

Für Polynome mit reellen Koeffizienten wollen wir die Frage nach der Existenz von Nullstellen etwas näher betrachten. Beginnen wir mit Polynomen p vom Grad 2, d.h. betrachten wir *quadratische Gleichungen*.

3.3.5 Beispiel. Betrachten wir die Gleichung $x^2+10x = 39$. Zeichne die folgende Skizze:



Die gepunkteten Flächen gemeinsam ergeben genau die linke Seite unserer Gleichung: Das dunkle Quadrat steht für x^2. Wegen $5 = \frac{10}{2}$ stehen die beiden Rechtecke für $2 \cdot 5x = 10x$. Wir vervollständigen diese Figur zu einem Quadrat. Die Fläche, die zu diesem Zwecke ergänzt werden muß ist $5 \cdot 5 = 25$. Die Fläche der Gesamtfigur ist $(5 + x)^2$. Wir erhalten also

$$(5 + x)^2 = (x^2 + 10x) + 25 = 39 + 25 = 64.$$

Also ist $5 + x = 8$ oder $x = 3$.

Entfernt man sich von der geometrischen Anschauung, so kann $5 + x$ auch den Wert -8 annehmen, denn auch $(-8)^2 = 64$. Also ist auch $x = -13$ eine Lösung. //

Hat man eine Gleichung $x^2 + px + q = 0$ zu lösen, geht man analog vor: Man ergänzt die linke Seite auf ein vollständiges Quadrat. Wegen der Formel

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

muß man zu diesem Zwecke $\frac{p^2}{4} - q$ addieren. Es ergibt sich

$$0 + (\frac{p^2}{4} - q) = (x^2 + px + q) + (\frac{p^2}{4} - q) = x^2 + px + \frac{p^2}{4} = (x + \frac{p}{2})^2.$$

Die gesuchte Lösung x ist also eine reelle Zahl mit

$$(x + \frac{p}{2})^2 = \frac{p^2}{4} - q.$$

Es können drei Fälle auftreten:

(i) $\frac{p^2}{4} - q > 0.$

(ii) $\frac{p^2}{4} - q = 0.$

(iii) $\frac{p^2}{4} - q < 0.$

Im Fall (i) existieren zwei Lösungen x_1 und x_2, nämlich

$$x_1 = -\frac{p}{2} + \sqrt{\frac{p^2}{4} - q},\ x_2 = -\frac{p}{2} - \sqrt{\frac{p^2}{4} - q}.$$

Im zweiten Fall existiert eine Lösung $x = -\frac{p}{2}$. Wogegen im letzten Fall keine Lösung existiert, da das Quadrat einer reellen Zahl stets ≥ 0 ist.

Hat man nun die quadratische Gleichung in der Form $a_2x^2 + a_1x + a_0 = 0$ gegeben, so erhält man (durch Division durch a_2) die Lösungen

$$x_{1,2} = -\frac{a_1}{2a_2} \pm \sqrt{\frac{a_1^2}{4a_2^2} - \frac{a_0}{a_2}} = \frac{-a_1 \pm \sqrt{a_1^2 - 4a_0a_2}}{2a_2}.$$

Polynome mit reellen Koeffizienten; kubische Gleichungen.

Kommen wir als nächstes zu Polynomen vom Grad 3, also zu *kubischen Gleichungen*.

Betrachte eine Gleichung der Gestalt

$$x^3 + px + q = 0. \tag{3.3.1}$$

Die Beschränkung auf diese spezielle Gestalt einer kubischen Gleichung ist keine Einschränkung der Allgemeinheit. Denn ist eine Gleichung $a_3x^3 + a_2x^2 + a_1x + a_0 = 0$ gegeben, $a_3 \neq 0$, so setze $y := x + \frac{a_2}{3a_3}$. Setzt man dieses in die gegebene Gleichung ein, und dividiert durch a_3, so erhält man eine Gleichung der Gestalt (3.3.1) für y. Kann man diese lösen, so erhält man natürlich auch eine Lösung x der Ausgangsgleichung.

Um die Gleichung (3.3.1) zu lösen versuchen wir den Ansatz $x = u + v$ mit noch näher zu bestimmenden Größen u und v. Man erhält

$$0 = (u+v)^3 + p(u+v) + q = (u^3 + 3u^2v + 3uv^2 + v^3) + p(u+v) + q =$$

$$= (u^3 + v^3) + (3uv + p)(u+v) + q.$$

Um diese Gleichung möglichst einfach zu machen, verlangen wir

$$3uv + p = 0$$

d.h. $v = -\frac{p}{3u}$. Setzt man das in die Gleichungen ein, so ergibt sich

$$u^3 - \frac{p^3}{27u^3} + q = 0$$

oder

$$(u^3)^2 + qu^3 + (-\frac{p^3}{27}) = 0.$$

Das ist eine quadratische Gleichung für u^3 die, falls

$$\frac{q^2}{4} + \frac{p^3}{27} \geq 0$$

zwei (bzw. eine) reelle Lösungen hat. Nämlich

$$u^3_{1,2} = -\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}.$$

Für v ergibt sich

$$v^3_{1,2} = -\frac{p^3}{27(-\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}})} = -\frac{p^3(-\frac{q}{2} \mp \sqrt{\frac{q^2}{4} + \frac{p^3}{27}})}{27(-\frac{p^3}{27})}$$

Wegen der Beziehung $3uv + p = 0$, sieht man, daß man das Vorzeichen der Wurzel bei $u^3_{1,2}$ und $v^3_{1,2}$ unterschiedlich wählen muß. Für x ergibt sich somit

$$x = u + v = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$$

3.3.6 Beispiel. Als Beispiel betrachten wir die Gleichung

$$x^3 - 5x + 2 = 0.$$

Man errät eine Lösung: $x = 2$. Durchdividieren ergibt

$$x^2 + 2x - 1 = 0,$$

und diese Gleichung hat die Lösungen $-1 \pm \sqrt{2}$. Man erhält also für x genau die drei Werte

$$x_1 = 2,\ x_2 = -1 + \sqrt{2},\ x_3 = -1 - \sqrt{2}.$$

Die oben hergeleitete Formel versagt jedoch, da

$$\frac{2^2}{4} + \frac{(-5)^3}{27} = 1 - \frac{125}{27} < 0.$$

Und doch muß $u + v$ einer der drei obigen Werte sein ?!? //

3.3.7 Bemerkung. Gleichungen höheren Grades kann man nicht mehr so einfach behandeln. Für Gleichungen vierten Grades kann man noch allgemeine Lösungsformeln von ähnlicher (nur noch komplizierterer) Gestalt (mit $+, \cdot$ und Wurzeln) angeben. Für Gleichungen höheren Grades ist das im allgemeinen nicht möglich. Diese expliziten Lösungsformeln für Gleichungen vom Grad 3 und 4 nennt man auch *Cardanosche Formeln*[4]. //

[4]Geronimo Cardano. 24.9.1501 Pavia - 21.9.1576 Rom

3.4 Die komplexen Zahlen

Sei K ein Körper und $p \in K[X]$. Ist $a_1 \in K$ eine Nullstelle von p, so kann man, wie wir in Korollar 3.3.4 gesehen haben, den Linearfaktor $(X - a_1)$ abspalten und erhält $p(X) = q(X)(X - a_1)$ mit einem Polynom $q \in K[X]$ dessen Grad um 1 kleiner ist als der von p. Iteriert man diese Vorgangsweise solange das neu entstandene Polynom eine Nullstelle in K hat, erhält man eine Darstellung

$$p(X) = q(X) \prod_{i=1}^{m} (X - a_i)$$

mit einem Polynom $q \in K[X]$ welches keine Nullstellen in K hat. Dabei gilt $\operatorname{grad} q = \operatorname{grad} p - m$.

Natürlich ist es eine besonders schöne Situation, wenn q konstant ist, d.h. wenn man p als Produkt von Linearfaktoren schreiben kann.

3.4.1 Definition. Ein Körper K heißt *algebraisch abgeschlossen*, wenn sich jedes Polynom aus $K[X]$ als Produkt von Linearfaktoren aus $K[X]$ schreiben läßt. ∥

Wie wir in Beispiel 3.3.3 gesehen haben ist der Körper $\mathbb{R}$ nicht algebraisch abgeschlossen, denn das Polynom $X^2 + 1 \in \mathbb{R}[X]$ hat in $\mathbb{R}$ keine Nullstellen[5].

Wir wollen nun eine algebraisch abgeschlossenen Körper konstruieren der $\mathbb{R}$ umfasst. Dazu müssen wir zumindest erzwingen, dass das Polynom $X^2 + 1$ eine Nullstelle (im neuen Körper) hat. Um die unten gegebenen Definitionen zu motivieren, wollen wir wieder auf unsere Anschauung zurückgreifen. Eine Nullstelle von $X^2 + 1 = 0$ ist so etwas wie eine „Quadratwurzel aus -1“. Da der gesuchte Körper die reellen Zahlen umfassen soll, muss er alle Ausdrücke der Gestalt

$$a + b\sqrt{-1}, \quad a, b \in \mathbb{R}$$

enthalten (wahrscheinlich noch viel mehr, aber diese ganz sicher). Um zu erraten wie man mit solchen Zahlen operiert, machen wir die formalen Rechnungen:

$$\begin{aligned}
&(a + b\sqrt{-1}) + (c + d\sqrt{-1}) = (a + c) + (b + d)\sqrt{-1} \\
&(a + b\sqrt{-1})\cdot(c + d\sqrt{-1}) = \\
&\qquad = a\cdot c + a \cdot d\sqrt{-1} + b\sqrt{-1} \cdot c + b \underbrace{\sqrt{-1} \cdot d\sqrt{-1}}_{=-1} = \\
&\qquad = (ac - bd) + (ad + bc)\sqrt{-1}
\end{aligned}$$

Diese Motivation führt zu der folgenden Definition.

3.4.2 Definition. Die Menge der *komplexen Zahlen* $\mathbb{C}$ ist definiert als die Menge der Paare reeller Zahlen, d.h.

$$\mathbb{C} := \mathbb{R} \times \mathbb{R}\,.$$

[5] Die Menge der Nullstellen in K eines Produktes von Linearfaktoren $p(X) = \prod_{i=1}^{m}(X - a_i)$, $a_i \in K$, ist gleich $\{a_1, \ldots, a_m\}$. Insbesondere existieren Nullstellen in K.

Für zwei komplexe Zahlen (a, b) und (c, d) definieren wir eine Addition und eine Multiplikation als

$$(a, b) + (c, d) := (a + c, b + d)$$
$$(a, b) \cdot (c, d) := (ac - bd, bc + ad)$$

//

Wir haben in $\mathbb{C}$ eigentlich nur eine Minimalversion von dem was man wahrscheinlich braucht um einen $\mathbb{R}$ umfassenden Körper zu konstruieren zu $\mathbb{R}$ dazugetan (man erinnere sich an unsere Motivation). Interessanterweise stellt sich heraus, dass trotzdem $\mathbb{C}$ schon ein Körper ist. Dies könnte man „zu Fuß“ nachrechnen; das ist aber mühsam, und es gibt eine deutlich schnellere (dafür etwas trickreiche) Beweisvariante, die sich auf die Matrizenrechnung aus der Linearen Algebra stützt.

3.4.3 Satz. *Die komplexen Zahlen $\langle \mathbb{C}, +, \cdot \rangle$ sind ein Körper.*

Beweis. Wir betrachten die Abbildung

$$\phi : \begin{cases} \mathbb{C} & \to & \mathbb{R}^{2\times 2} \\ (a, b) & \mapsto & \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \end{cases}$$

Diese ist injektiv und es gilt, wie man unmittelbar nachrechnet, für je zwei komplexe Zahlen z_1 und z_2

$$\phi(z_1 + z_2) = \phi(z_1) + \phi(z_2), \quad \phi(z_1 \cdot z_2) = \phi(z_1) \cdot \phi(z_2)\,.$$

Daher sind die Rechengesetze welche in $\mathbb{R}^{2\times 2}$ gelten, nämlich Assoziativgesetze, Kommutativgesetze, sowie das Distributivgesetz auch in $\mathbb{C}$ richtig.

Die Existenz neutraler Elemente in $\mathbb{C}$ folgt, da die Nullmatrix und die Einheitsmatrix im Bild von ϕ liegen. Explizit ist $(0, 0)$ neutrales Element für „$+$“, und $(1, 0)$ neutrales Element für „$\cdot$“. Die Existenz eines additiven Inversen folgt, da das Bild von ϕ mit einer Matrix A auch die Matrix $-A$ enthält. Explizit ist $-(a, b) = (-a, -b)$.

Es bleibt zu zeigen, dass jede von Null verschiedene komplexe Zahl ein multiplikatives Inverses besitzt. Sei also $(a, b) \in \mathbb{C} \setminus \{0\}$ gegeben. Dann ist also $a \neq 0$ oder $b \neq 0$, und wir sehen das

$$\det \phi\big((a, b)\big) = a^2 + b^2 > 0\,.$$

Daher ist die Matrix $\phi\big((a, b)\big)$ invertierbar, und

$$\phi\big((a, b)\big)^{-1} = \frac{1}{a^2 + b^2} \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \phi\Big(\Big(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2}\Big)\Big)\,.$$

Also ist haben wir ein multiplikatives Inverses von (a, b) gefunden, explizit ist

$$\frac{1}{(a, b)} = \Big(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2}\Big).$$

❑

Noch interessanter ist dass, obwohl wir in $\mathbb{C}$ eigentlich nur eine Minimalversion von dem was man wahrscheinlich braucht um einen algebraische abgeschlossenen Körper zu erhalten zu $\mathbb{R}$ dazugetan haben (nämlich eine einzige Nullstelle von einem einzigen Polynom), der Körper $\mathbb{C}$ schon algebraisch abgeschlossen ist. Dies ist die Aussage des sogenannten *Fundamentalsatzes der Algebra*. Wir können diesen Satz mit unseren jetzigen Mitteln nicht beweisen, werden aber später (Analysis 2) darauf zurückkommen.

Im folgenden werden wir immer eine abkürzende Schreibweise verwenden um komplexe Zahlen anzuschreiben, nämlich schreiben wir „$a + ib$“ für die komplexe Zahl (a, b). Diese Notation hat historische Wurzeln, das formale Symbol i bezeichnet man als die *imaginäre Einheit*. Tatsächlich rechnet man mit i so wie man es sich aus unserer Motivation erwartet, denn es gilt

$$i^2 = (0 + 1i)^2 = -1\,,$$

d.h. i ist im Körper $\mathbb{C}$ eine Quadratwurzel aus -1.

Nach dem (noch nicht bewiesenen) Fundamentalsatz der Algebra, haben durch die Erweiterung von $\mathbb{R}$ zu $\mathbb{C}$ gewonnen, dass sich jedes Polynom als Produkt von Linearfaktoren schreiben läßt. Wir haben allerdings auch eine wesentliche Eigenschaft von $\mathbb{R}$ verloren, nämlich dass $\mathbb{R}$ ein (sogar vollständig) angeordneter Körper ist.

3.4.4 Proposition. *Sei K ein angeordneter Körper, und sei $a \in K$, $a > 0$. Dann hat das Polynom $X^2 + a$ keine Nullstelle in K.*

Insbesondere gibt keine Ordnungsrelation auf $\mathbb{C}$, sodass $\mathbb{C}$ mit dieser zu einem angeordneten Körper wird.

Beweis. Sei $x \in K$. Ist $0 \leq x$, so folgt dass auch $0 = 0 \cdot x \leq x \cdot x = x^2$. Ist $x \leq 0$, so folgt $0 = x - x \leq 0 - x = -x$, und nach dem eben bewiesenen $0 \leq (-x) \cdot (-x) = x^2$. Also sind Quadrate in K stets positiv, $x^2 \geq 0$ für alle $x \in K$. Wir erhalten $x^2 + a \geq a > 0$, $x \in K$, und daher hat $X^2 + a$ keine Nullstelle in K.

In $\mathbb{C}$ gilt $i^2 = -1 < 0$, also kann $\mathbb{C}$ niemals ein angeordneter Körper sein. ❑

Schliesslich wollen wir einige elementare Eigenschaften zusammenstellen. Dazu definieren wir

$$\mathrm{Re}(a + ib) := a,\ \mathrm{Im}(a + ib) := b, \quad |z| := \sqrt{(\mathrm{Re}\, z)^2 + (\mathrm{Im}\, z)^2}\,,$$

und sprechen vom *Realteil*, *Imaginärteil*, und *Betrag* der komplexen Zahl $a + ib$. Das Wurzelsymbol in dieser Definition bezeichnet dabei die, nach Proposition 3.2.3 in eindeutiger Weise existierende, nichtnegative reelle Quadratwurzel.

3.4.5 Lemma. *Es gilt:*

(*i*) *Die Abbildung*

$$\psi : \left\{ \begin{array}{ccc} \mathbb{R} & \to & \mathbb{C} \\ x & \mapsto & x + 0 \cdot i \end{array} \right.$$

ist injektiv und mit der Addition und Multiplikation verträglich.

(*ii*) *$\mathbb{C}$ ist ein $\mathbb{R}$-Vektorraum mit Dimension 2.*

(*iii*) *Für je zwei komplexe Zahlen z, w gilt $|z \cdot w| = |z| \cdot |w|$.*

Beweis. Die Injektivität von ψ ist klar, die Verträglichkeit mit den algebraischen Operationen folgt leicht:

$$(a + 0 \cdot i) + (b + 0 \cdot i) = (a + b) + 0 \cdot i, \quad (a + 0 \cdot i) \cdot (b + 0 \cdot i) = (ab) + 0 \cdot i\,.$$

Die Vektorraumgesetze folgen unmittelbar aus den Körperaxiomen, da ψ mit Addition und Multiplikation verträglich ist. Nun ist $\{1, i\}$ eine Basis von $\mathbb{C}$ über $\mathbb{R}$, also haben wir Dimension 2.

Um die Multiplikativität des Betrages einzusehen, erinnern wir uns an den Beweis von Satz 3.4.3. Die dort benützte Abbildung $\phi : \mathbb{C} \to \mathbb{R}^{2\times 2}$ war mit der Multiplikation verträglich. Nun gilt

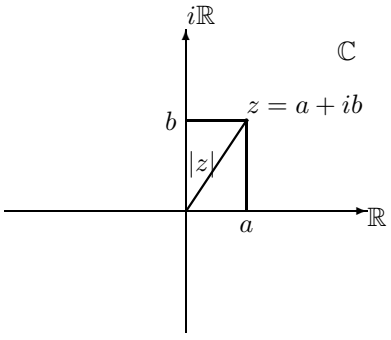
$$|z|^2 = (\operatorname{Re} z)^2 + (\operatorname{Im} z)^2 = \det \phi(z).$$

Wir erhalten

$$|zw|^2 = \det \phi(zw) = \det \big[\phi(z)\phi(w)\big] = \det \phi(z) \cdot \det \phi(w) = |z|^2 \cdot |w|^2\,.$$

Da die nichtnegative reelle Quadratwurzel einer nichnegativen reellen Zahl nach Proposition 3.2.3 ja eindeutig ist, folgt $|zw| = |z| \cdot |w|$. ❑

Offenbar kann man sich den Körper $\mathbb{C}$ der komplexen Zahl als Ebene veranschaulichen, man spricht auch von der *Gaußschen Zahlenebene*[6]. Die reellen Zahlen, die ja bis auf Umbenennung vermöge der Abbildung ψ in $\mathbb{C}$ enthalten sind, erscheinen in dieser Veranschaulichung als die x-Achse. Die *rein imaginären Zahlen*, das sind die komplexen Zahlen der Gestalt bi, $b \in \mathbb{R}$, als die y-Achse. Dementsprechend spricht man in der Gaußschen Zahlenebene von der x-Achse als der *reellen Achse*, und von der y-Achse als der *imaginären Achse*. Der Real- bzw. Imaginärteil einer komplexen Zahl erscheint als die x- bzw. y-Koordinate des entsprechenden Punktes, und ihr Betrag als der Abstand vom Nullpunkt.



[6]Carl-Friedrich Gauß. 30.4.1777 Braunschweig - 23.2.1855 Göttingen

Kapitel 4

Der Konvergenzbegriff

Haben wir eine Folge $x_1, x_2, x_3, \ldots$ von Punkten eines gewissen Raumes X und des weiteren ein Element $x \in X$, so werden wir sagen:

> Die Punkte x_i konvergieren gegen x, wenn für alle hinreichend großen Indizes i das Element x_i beliebig nahe an x herankommt.

Um diesem anschaulichen Begriff Sinn zu geben, müssen wir klären was es heißt das x_i beliebig „nahe“ an x ist.

4.1 Metrische Räume

Um zu sagen wann ein Punkt x „nahe“ bei einem anderen Punkt y liegt, müssen wir also in irgendeiner Weise den Abstand von x zu y messen können.

Betrachten wir zum Beispiel die Menge X aller Punkte der Ebene. Dann ist es naheliegend als Abstand zwischen x und y die Länge $l_{x,y}$ der Strecke die die beiden Punkte verbindet zu nehmen.

Man sieht das die folgenden Regeln gelten: Stets ist $l_{x,y} \geq 0$ denn Längen sind immer positiv. Dabei gilt „=“ genau dann, wenn $x = y$, denn eine Strecke hat dann und nur dann Länge 0 wenn Anfangs- und Endpunkt gleich sind. Es ist stets $l_{x,y} = l_{y,x}$, denn vertauscht man Anfangs- und Endpunkt so bleibt die Länge der Strecke erhalten. Schwieriger einzusehen, aber anschaulich doch klar, ist die Gültigkeit der Dreiecksungleichung: In jedem Dreieck ist die Länge einer Seite höchstens so groß wie die Summe der Längen der anderen Seiten. D.h. für je drei Punkte (die Eckpunkte des Dreiecks) gilt $l_{x,z} \leq l_{x,y} + l_{y,z}$.

Es sind nun genau diese drei Eigenschaften die es ausmachen dass „die Länge der Verbindungsstrecke“ ein vernünftiger Begriff für den Abstand zweier Punkte ist.

4.1.1 Definition. Sei X eine Menge, $d : X \times X \to \mathbb{R}$ eine Funktion. Dann heißt d eine *Metrik* auf X, und $\langle X, d\rangle$ ein *metrischer Raum*, wenn gilt

(M1) Für alle $x, y \in X$ ist $d(x, y) \geq 0$. Es gilt $d(x, y) = 0$ genau dann, wenn $x = y$.

(M2) Für alle $x, y \in X$ gilt $d(x, y) = d(y, x)$.

(M3) Sind $x, y, z \in X$, so gilt die *Dreiecksungleichung*:

$$d(x,z) \leq d(x,y) + d(y,z)\,.$$

//

In dem Beispiel von dem wir oben ausgegangen sind, ist $X := \mathbb{R}^2$ und

$$d(x,y) := \sqrt{(x_1-y_1)^2 + (x_2-y_2)^2}, \quad x = (x_1,x_2), y = (y_1,y_2) \in X\,.$$

Man kann allgemeiner eine analoge Formel verwenden um eine Metrik auf $X := \mathbb{R}^n$ zu definieren, nämlich[1]

$$d(x,y) := \Big(\sum_{j=1}^{n}(x_j-y_j)^2\Big)^{\frac{1}{2}}, \quad x = (x_1,\ldots,x_n), y = (y_1,\ldots,y_n) \in \mathbb{R}^n\,.$$

Man spricht von der *euklidischen Metrik* des $\mathbb{R}^n$. Die Gültigkeit von (M1) und (M2) ist aus der Definition offensichtlich, die Dreiecksungleichung dagegen ist schwieriger einzusehen:

4.1.2 Lemma. *Seien $n \in \mathbb{N}$, $a_1,\ldots,a_n,b_1,\ldots,b_n \in \mathbb{R}$. Dann gilt (*Schwarzsche Ungleichung[2]*)*

$$\left(\sum_{i=1}^{n} a_i b_i\right)^2 \;\leq\; \left(\sum_{i=1}^{n} a_i^2\right) \cdot \left(\sum_{i=1}^{n} b_i^2\right),$$

*und (*Minkowskische Ungleichung[3]*)*

$$\left(\sum_{i=1}^{n}(a_i+b_i)^2\right)^{\frac{1}{2}} \;\leq\; \left(\sum_{i=1}^{n} a_i^2\right)^{\frac{1}{2}} + \left(\sum_{i=1}^{n} b_i^2\right)^{\frac{1}{2}}.$$

Beweis. Wir verwenden die Bezeichnungen $\vec{a} := (a_1,\ldots,a_n)$, $\vec{b} := (b_1,\ldots,b_n)$ und

$$(\vec{a},\vec{b}) := \sum_{i=1}^{n} a_i b_i.$$

Für reelle Zahlen t_1, t_2 ist

$$t_1\vec{a} + t_2\vec{b} := (t_1a_1 + t_2b_1, \ldots, t_1a_n + t_2b_n)\,,$$

und offenbar gilt

$$(t_1\vec{a} + t_2\vec{b}, \vec{c}) = t_1(\vec{a},\vec{c}) + t_2(\vec{b},\vec{c})\,.$$

Wegen $(\vec{a},\vec{b}) = (\vec{b},\vec{a})$ ist $(.,.)$ auch in der hinteren Komponente linear (vgl. den Begriff des Skalarproduktes auf einem Vektorraum in der Linearen Algebra).

Um die Schwarzsche Ungleichung zu zeigen, gehen wir von der trivialen Bemerkung aus, daß für jedes n-Tupel $\vec{x} = (x_1,\ldots,x_n)$ gilt

$$(\vec{x},\vec{x}) = \sum_{i=1}^{n} x_i^2 \geq 0.$$

[1] Wir bezeichnen hier die eindeutige nichtnegative Quadratwurzel einer nichtnegativen reellen Zahl x mit $x^{\frac{1}{2}}$.

[2] Hermann Amandus Schwarz. 25.1.1843 Hermsdorf (Sobiecin, Polen) - 30.11.1921 Berlin

[3] Hermann Minkowski. 22.6.1864 Alexoten (bei Kaunas, UdSSR) - 12.1.1909 Göttingen

Es ist also für alle $t \in \mathbb{R}$

$$0 \leq (\vec{a} + t\vec{b}, \vec{a} + t\vec{b}) = (\vec{a}, \vec{a}) + 2t(\vec{a}, \vec{b}) + t^2(\vec{b}, \vec{b}),$$

d.h. die quadratische Gleichung $(\vec{b}, \vec{b})x^2 + 2(\vec{a}, \vec{b})x + (\vec{a}, \vec{a}) = 0$ hat nie zwei verschiedene Lösungen. Also gilt

$$(\vec{a}, \vec{b})^2 - (\vec{a}, \vec{a})(\vec{b}, \vec{b}) \leq 0.$$

Ausgeschrieben ergibt das die Schwarzsche Ungleichung.

Die Minkowskische Ungleichung folgt nun unmittelbar. Seien zunächst $a_i, b_i \geq 0$, dann gilt

$$\sum_{i=1}^{n}(a_i + b_i)^2 = \sum_{i=1}^{n} a_i(a_i + b_i) + \sum_{i=1}^{n} b_i(a_i + b_i) \leq$$

$$\leq \left(\sum_{i=1}^{n} a_i^2\right)^{\frac{1}{2}} \left(\sum_{i=1}^{n}(a_i + b_i)^2\right)^{\frac{1}{2}} + \left(\sum_{i=1}^{n} b_i^2\right)^{\frac{1}{2}} \left(\sum_{i=1}^{n}(a_i + b_i)^2\right)^{\frac{1}{2}} =$$

$$= \left[\left(\sum_{i=1}^{n} a_i^2\right)^{\frac{1}{2}} + \left(\sum_{i=1}^{n} b_i^2\right)^{\frac{1}{2}}\right] \left(\sum_{i=1}^{n}(a_i + b_i)^2\right)^{\frac{1}{2}}.$$

Für a_i, b_i beliebig gilt

$$\left(\sum_{i=1}^{n}(a_i + b_i)^2\right)^{\frac{1}{2}} \leq \left(\sum_{i=1}^{n}(|a_i| + |b_i|)^2\right)^{\frac{1}{2}} \leq \left(\sum_{i=1}^{n}|a_i|^2\right)^{\frac{1}{2}} + \left(\sum_{i=1}^{n}|b_i|^2\right)^{\frac{1}{2}} =$$

$$= \left(\sum_{i=1}^{n} a_i^2\right)^{\frac{1}{2}} + \left(\sum_{i=1}^{n} b_i^2\right)^{\frac{1}{2}}.$$

❑

Wann immer wir von $\mathbb{R}^n$ als metrischen Raum sprechen ohne die Metrik auf die wir uns beziehen näher zu spezifizieren, meinen wir $\mathbb{R}^n$ versehen mit der euklidischen Metrik.

4.1.3 Beispiel. Sei $X := \mathbb{C}$, und setze $d(z, w) := |z - w|$. Dann ist d eine Metrik auf $\mathbb{C}$. Um dies einzusehen, betrachten wir $\mathbb{C}$ als Gaußsche Zahlenebene. D.h. wir identifizieren $\mathbb{C}$ mit $\mathbb{R}^2$ vermöge der bijektiven Abbildung

$$\lambda : \left\{ \begin{array}{ccc} \mathbb{C} & \to & \mathbb{R}^2 \\ z & \mapsto & (\operatorname{Re} z, \operatorname{Im} z) \end{array} \right.$$

Bezeichne d_2 die euklidische Metrik am $\mathbb{R}^2$. Es gilt

$$d(z, w) = d(z - w, 0) = \sqrt{(\operatorname{Re}(z - w))^2 + (\operatorname{Im}(z - w))^2} =$$

$$= \sqrt{(\operatorname{Re} z - \operatorname{Re} w)^2 + (\operatorname{Im} z - \operatorname{Im} w)^2} = d_2\big((\operatorname{Re} z, \operatorname{Im} z), (\operatorname{Re} w, \operatorname{Im} w)\big) =$$

$$= d_2(\lambda(z), \lambda(w)).$$

Also können wir die Gültigkeit der Axiome (M1)–(M3) von d_2 auf d übertragen: Offenbar ist $d(z-w) \geq 0$. Ist $d(z,w) = 0$, so folgt $\lambda(z) = \lambda(w)$, und da λ injektiv ist auch $z = w$. Die Symmetrie $d(z,w) = d(w,z)$ ist wieder klar, die Dreiecksungleichung folgt ebenfalls leicht, denn

$$d(z,w) = d_2(\lambda(z),\lambda(w)) \leq d_2(\lambda(z),\lambda(u)) + d_2(\lambda(u),\lambda(w)) = d(z,u) + d(u,w)\,.$$

Angesichts dieser Tatsache, dass man d vermöge λ mit d_2 identifizieren kann, bezeichnet man d auch als *euklidische Metrik* auf $\mathbb{C}$. Wann immer wir von $\mathbb{C}$ als metrischen Raum sprechen ohne die Metrik auf die wir uns beziehen näher zu spezifizieren, meinen wir $\mathbb{C}$ versehen mit der euklidischen Metrik.

Die Tatsache, dass eine Metrik der Dreiecksungleichung genügt spiegelt sich in diesem Beispiel in der *Dreiecksungleichung für den Betrag* wieder. Es gilt nämlich stets

$$|z+w| \leq |z| + |w|\,,$$

denn

$$|z+w| = |z-(-w)| = d(z,-w) \leq d(z,0) + d(0,-w) = |z| + |w|\,.$$

Wir erhalten daraus auch die *Dreiecksungleichung nach unten*:

$$\big||x| - |y|\big| \leq |x+y|\,. \tag{4.1.1}$$

Um dieses einzusehen, bemerke

$$|x| = |(x+y)+(-y)| \leq |x+y| + |y|,$$

also $|x| - |y| \leq |x+y|$. Analog folgt

$$|y| \leq |x+y| + |x|,$$

also auch $|y| - |x| \leq |x+y|$. Insgesamt erhält man (4.1.1). ∥

Die gleiche Situation wie in dem obigen Beispiel hat man auch für $X = \mathbb{R}$ anstelle von $\mathbb{C}$. Denn es gilt ja $|x| = (x^2)^{\frac{1}{2}}$, $x \in \mathbb{R}$, also ist die euklidische Metrik d_2 am $\mathbb{R}^1$ gerade gegeben als

$$d_2(x,y) = |x-y|, \quad x,y \in \mathbb{R}\,.$$

Metriken treten in verschiedensten Zusammenhängen auf.

4.1.4 Beispiel.

(*i*) Sei noch einmal $X := \mathbb{R}^2$ und setze

$$d_1(x,y) := |x_1 - y_1| + |x_2 - y_2|, \quad x = (x_1,x_2), y = (y_1,y_2) \in \mathbb{R}^2\,.$$

Dann ist d_1 eine Metrik: Die Gültigkeit von (M1) und (M2) ist wieder aus der Definition offensichtlich. Um die Dreiecksungleichung einzusehen, seien $x,y,z \in \mathbb{R}$ gegeben. Dann folgt, mit Hilfe der Dreiecksungleichung für den Betrag,

$$d_1(x,z) = |x_1-z_1|+|x_2-z_2| \leq \big(|x_1-y_1|+|y_1-z_1|\big)+\big(|x_2-y_2|+|y_2-z_2|\big) =$$

$$= \big(|x_1-y_1|+|x_2-y_2|\big) + \big(|y_1-z_1|+|y_2-z_2|\big) = d_1(x,y) + d_1(y,z)\,.$$

Diese Metrik ist offenbar nicht gleich der euklidischen Metrik, denn zum Beispiel ist $d_1((0,0),(2,1)) = 3$ aber $d((0,0),(2,1)) = \sqrt{5}$.

Anschaulich interpretiert bezeichnet man d_1 manchmal als *New York-Metrik*. Denn stellt man sich in der Ebene einen Stadtplan mit lauter rechtwinkeligen Strassen vor, dann misst $d_1(x,y)$ gerade die Länge des Fußweges von der Kreuzung x zur Kreuzung y.

Ganz analog definiert man eine Metrik am $\mathbb{R}^n$:

$$d_1(x,y) = \sum_{j=1}^{n} |x_j - y_j|, \quad x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n) \in \mathbb{R}^n \,.$$

Der Nachweis von (M1)-(M3) geht genauso wie im oben betrachteten Fall $n = 2$.

(*ii*) Betrachte die ganzen Zahlen $X := \mathbb{Z}$ und halte eine Primzahl p fest. Setze

$$d_{(p)}(x,y) := \begin{cases} \frac{1}{p^{n(p)}} & , \; x \neq y, x - y = \pm \prod_{q \text{ prim}} q^{n(q)} \\ 0 & , \; x = y \end{cases}$$

Dann ist $d_{(p)}$ eine Metrik auf $\mathbb{Z}$, die *p-adische Metrik*. Denn (M1) ist nach Definition erfüllt, (M2) ist ebenfalls richtig denn vertauscht man x und y, so ändert sich bei der Differenz $x - y$ nur das Vorzeichen, nicht jedoch die Primfaktoren und ihre Potenzen. Die Dreiecksungleichung ist wieder schwieriger einzusehen. Wir zeigen, dass in diesem Fall sogar die stärkere Ungleichung

$$d_{(p)}(x,z) \leq \max\left\{d_{(p)}(x,y), d_{(p)}(y,z)\right\}, \quad x,y,z \in \mathbb{Z}\,,$$

gilt. Diese Ungleichung impliziert tatsächlich sofort die Dreiecksungleichung, denn für je zwei Zahlen $a, b \geq 0$ ist stets $\max\{a,b\} \leq a + b$.

Schreibe

$$x - z = \pm \prod_{q \text{ prim}} q^{n_1(q)}, \; x - y = \pm \prod_{q \text{ prim}} q^{n_2(q)}, \; y - z = \pm \prod_{q \text{ prim}} q^{n_3(q)}\,,$$

sodaß also

$$d_{(p)}(x,z) = \frac{1}{p^{n_1(p)}}, \; d_{(p)}(x,y) = \frac{1}{p^{n_2(p)}}, \; d_{(p)}(y,z) = \frac{1}{p^{n_3(p)}}\,.$$

Betrachte den Fall dass $d_{(p)}(x,y) \geq d_{(p)}(y,z)$, d.h. dass $n_2(p) \leq n_3(p)$. Dann gilt also $\max\{d_{(p)}(x,y), d_{(p)}(y,z)\} = d_{(p)}(x,y)$. Wegen $n_2(p) \leq n_3(p)$ ist

$$p^{n_2(p)} | (y - z)\,,$$

und daher auch $p^{n_2(p)} | [(x-y)+(y-z)] = x - z$. Es folgt das $n_2(p) \leq n_1(p)$, d.h. das $d_{(p)}(x,y) \geq d_{(p)}(x,z)$.

Der Fall $d_{(p)}(x,y) \leq d_{(p)}(y,z)$ wird genauso behandelt.

(*iii*) Auf $\mathbb{Z}$ haben wir natürlich auch die euklidische Metrik $d(x,y) = |x - y|$, denn $\mathbb{Z}$ ist ja eine Teilmenge von $\mathbb{C}$. Diese ist verschieden von der Metrik $d_{(p)}$, denn zum Beispiel ist ja $d_{(p)}(0,p) = \frac{1}{p}$, wogegen $d(0,p) = p$.

(*iv*) Sei X eine nichtleere Menge, und $B(X,\mathbb{R})$ die Menge aller beschränkten Funktionen von X nach $\mathbb{R}$, d.h. die Menge aller jener Funktionen $f : X \to \mathbb{R}$, für die gilt dass die Menge $\{|f(x)| : x \in X\}$ beschränkt ist. Auf $B(X,\mathbb{R})$ definieren wir eine Metrik (die *Supremumsmetrik*) als

$$d_\infty(f,g) := \sup\{|f(x) - g(x)| : x \in X\}.$$

Die Tatsache, dass d_∞ die Axiome (M1) und (M2) erfüllt ist klar. Zum Nachweis der Dreiecksungleichung seien $f, g, h \in B(X,\mathbb{R})$ gegeben. Dann gilt, für jedes $x \in X$,

$$|f(x) - h(x)| \le |f(x) - g(x)| + |g(x) - h(x)| \le d_\infty(f,g) + d_\infty(g,h).$$

Also ist $d_\infty(f,g)+d_\infty(g,h)$ eine obere Schranke der Menge $\{|f(x)-g(x)| : x \in X\}$. Da $d_\infty(f,h)$ die kleinste obere Schranke dieser Menge ist, folgt $d_\infty(f,h) \le d_\infty(f,g) + d_\infty(g,h)$.

(*v*) Sei X die Menge aller Adressen in Wien, und sei $d(x,y)$ die minimale Zeitspanne (in Minuten) die man benötigt um mit öffentlichen Verkehrsmitteln von x nach y zu kommen. Die Axiome (M1) und (M2) sind offensichtlich erfüllt, ebenso die Dreiecksungleichung (M3), denn Umwege dauern länger.

Betrachtet man Wien auf dem Stadtplan, also als Teilmenge des $\mathbb{R}^2$, so hat man natürlich auch die euklidische Metrik d_2, d.h. die Distanz zwischen x und y gemessen in der Luftlinie (in Kilometer). Diese Metriken sind wesentlich verschieden, denn zum Beispiel ist (www.vor.at bzw. Messung am Stadtplan)

$$\begin{aligned} &d(\text{Breitenseer Straße 10, Kardinal-Nagl-Platz 8}) = 22\\ &d(\text{Breitenseer Straße 10, Spohrstraße 1}) = 33\\ &d_2(\text{Breitenseer Straße 10, Kardinal-Nagl-Platz 8}) = 6,7\\ &d_2(\text{Breitenseer Straße 10, Spohrstraße 1}) = 3,3 \end{aligned}$$

Man sieht, dass es Punkte x, y, z gibt mit $d(x,y) < d(x,z)$ aber $d_2(x,y) > d_2(x,z)$.

//

4.2 Definition des Grenzwertes

Wir wollen nun eine exakte Definition des am Anfang dieses Kapitels anschaulich formulierten Konvergenzbegriffes geben.

4.2.1 Definition. Sei $\langle X, d\rangle$ ein metrischer Raum, $(x_i)_{i\in\mathbb{N}}$ eine Folge von Elementen $x_i \in X$, und $x \in X$. Dann heißt $(x_i)_{i\in\mathbb{N}}$ *konvergent gegen* x, wenn gilt

$$\forall \epsilon \in \mathbb{R}, \epsilon > 0\ \exists N \in \mathbb{N} :\ d(x_i, x) < \epsilon \text{ für alle } i \ge N.$$

In diesem Fall schreibt man $\lim_{i\to\infty} x_i = x$.

Ist $(x_i)_{i\in\mathbb{N}}$ eine Folge in X, und gibt es ein Element $x \in X$ sodaß $\lim_{i\to\infty} x_i = x$, so sagt man die Folge $(x_i)_{i\in\mathbb{N}}$ ist in X *konvergent*. Ist eine Folge nicht konvergent, so sagt man auch sie sei *divergent*. //

Man verwendet auch andere Schreibweisen für $\lim_{i\to\infty} x_i = x$, wie zum Beispiel $(x_i)_{i\in\mathbb{N}} \to x$, oder $x_i \to x$, $i \to \infty$, oder nur $x_i \to x$.

4.2.2 Beispiel.

(*i*) Sei $\langle X, d\rangle$ ein beliebiger metrischer Raum, und sei $x \in X$. Betrachte die konstante Folge $x_1 = x_2 = x_3 = \ldots = x$. Dann gilt $\lim_{i\to\infty} x_i = x$.

Um dies einzusehen sei $\epsilon \in \mathbb{R}$, $\epsilon > 0$, gegeben. Wir müssen eine Zahl $N \in \mathbb{N}$ finden sodaß $d(x_i, x) < \epsilon$ für alle $i \geq N$. Wähle $N := 1$, dann gilt für jedes $i \geq N$

$$d(x_i, x) = d(x, x) = 0 < \epsilon\,.$$

Dieses Beispiel ist natürlich in gewissem Sinne trivial, denn die Folgenglieder x_i sind ja schon alle gleich dem Grenzwert x, kommen also natürlich beliebig nahe.

(*ii*) Sei $X = \mathbb{R}$, dann gilt $\lim_{n\to\infty} \frac{1}{n} = 0$.

Um dies einzusehen sei $\epsilon \in \mathbb{R}$, $\epsilon > 0$, gegeben. Wir müssen eine Zahl $N \in \mathbb{N}$ finden sodaß $|\frac{1}{n} - 0| = \frac{1}{n} < \epsilon$ gilt wenn nur $n \geq N$. Dazu benützen wir die Dichteeigenschaft von $\mathbb{Q}$ in $\mathbb{R}$: Wähle $\frac{p}{q} \in \mathbb{Q}$ mit $0 < \frac{p}{q} < \epsilon$. Setzt man $N := q$, dann gilt für alle $n \in \mathbb{N}$ mit $n \geq N$

$$\frac{1}{n} \leq \frac{1}{N} = \frac{1}{q} \leq \frac{p}{q} < \epsilon\,.$$

(*iii*) Aus der Dreiecksungleichung nach unten erhalten wir die folgende Aussage: Ist $(z_n)_{n\in\mathbb{N}}$ eine Folge komplexer Zahlen, und gilt $z_n \to z$, so ist auch $|z_n| \to |z|$. Um dies einzusehen sei $\epsilon > 0$ gegeben. Wähle $N \in \mathbb{N}$ sodass $|z_n - z| < \epsilon$ für $n \geq N$. Für solche n ist dann auch

$$\big||z_n| - |z|\big| \leq |z_n - z| < \epsilon.$$

(*iv*) Es gibt viele Folgen die nicht konvergieren. Zum Beispiel betrachte die Folge $(x_n)_{n\in\mathbb{N}}$ in $\mathbb{C}$ mit $x_n := i^n$. Das ist also die Folge

$$(x_n)_{n\in\mathbb{N}} : \quad i, -1, -i, 1, i, -1, -i, \ldots$$

Angenommen es wäre $x_n \to x$ für ein gewisses $x \in \mathbb{C}$. Wähle $N \in \mathbb{N}$, sodaß $|x_n - x| < \frac{1}{2}$, $n \geq N$. Ist $n \geq N$ ein Vielfaches von 4, so folgt das $x_n = 1$, und daher $|x - 1| < \frac{1}{2}$. Ist $n \geq N$ jedoch gerade aber nicht durch 4 teilbar, so ist $x_n = -1$, und daher $|x + 1| < \frac{1}{2}$. Wir erhalten $2 = |1 - (-1)| \leq |1 - x| + |x - (-1)| < 1$, ein Widerspruch.

//

4.2.3 Bemerkung. Ändert man in einer Folge $x_1, x_2, \ldots$ endlich viele Folgenglieder ab, d.h. betrachtet man an ihrer Stelle eine Folge der Gestalt

$$y_1, \ldots, y_N, x_{N+1}, x_{N+2}, \ldots$$

so ist die abgeänderte Folge genau dann konvergent, wenn es die ursprüngliche ist. Weiters stimmen in diesem Fall die Grenzwerte der beiden Folgen überein.

Genauso gilt: Streicht man endlich viele Folgenglieder aus einer heraus, so ist die abgeänderte Folge genau dann konvergent, wenn es die ursprüngliche ist, und in diesem Fall stimmen die Grenzwerte der beiden Folgen überein. //

Wie wir gesehen haben muß eine Folge keinen Grenzwert haben. Wenn sie jedoch einen hat, so ist dieser eindeutig bestimmt.

4.2.4 Satz. *Sei $\langle X, d\rangle$ ein metrischer Raum und sei $(x_i)_{i\in\mathbb{N}}$ eine Folge von Elementen von X. Dann hat die Folge $(x_i)_{i\in\mathbb{N}}$ höchstens einen Grenzwert.*

Beweis. Es gelte $x_i \to x$ und $x_i \to y$ und sei angenommen das $x \neq y$, sodaß also $d(x,y) > 0$. Wähle $N_1 \in \mathbb{N}$ sodaß $d(x_i, x) < \frac{d(x,y)}{3}$, $i \geq N_1$, und $N_2 \in \mathbb{N}$ sodaß $d(x_i, y) < \frac{d(x,y)}{3}$, $i \geq N_2$. Dann folgt für $N := \max\{N_1, N_2\}$

$$d(x,y) \leq d(x, x_N) + d(x_N, y) < \frac{d(x,y)}{3} + \frac{d(x,y)}{3} = \frac{2d(x,y)}{3} < d(x,y)\,,$$

ein Widerspruch. ❑

4.2.5 Beispiel.

(*i*) Sei $q \in \mathbb{R}$, $0 < q < 1$, und betrachte die Folge $(q^n)_{n\in\mathbb{N}}$. Dann gilt $\lim_{n\to\infty} q^n = 0$.

Wir verwenden zum Beweis die *Bernoullische Ungleichung*[4]: Diese besagt, dass

$$(1+x)^n \geq 1 + nx,\ x > -1, n \in \mathbb{N}\,.$$

Das sieht man mittels vollständiger Induktion ein: Ist $n = 1$, so besagt sie $1 + x \geq 1 + x$, was offenbar stimmt. Angenommen sie sei nun für ein $n \in \mathbb{N}$ richtig. Dann folgt, da $x > -1$ ist,

$$(1+x)^{n+1} = (1+x)^n(1+x) \geq (1+nx)(1+x) =$$

$$= 1 + (n+1)x + nx^2 \geq 1 + (n+1)x\,.$$

Setzt man in der Bernoullischen Ungleichung $x = \frac{1}{q} - 1$, dann erhält man

$$\big(\frac{1}{q}\big)^n \geq 1 + n(\frac{1}{q} - 1)\,.$$

Da die Ordnung archimedisch ist und $\frac{1}{q} - 1 > 0$, gibt es zu jedem gegebenen $\epsilon > 0$ eine Zahl $N \in \mathbb{N}$ mit $N(\frac{1}{q} - 1) \geq \frac{1}{\epsilon} - 1$ und damit auch $(\frac{1}{q})^N \geq \frac{1}{\epsilon}$, also $q^N \leq \epsilon$. Es folgt dass $q^n < q^N \leq \epsilon$ für alle $n \geq N + 1$.

(*ii*) Sei $z \in \mathbb{C}$. Wir betrachten die Folge $(S_n)_{n\in\mathbb{N}}$ die definiert ist durch

$$S_n := \sum_{k=0}^{n} z^k.$$

Das ist die sogenannte *geometrische Reihe*. Ist $|z| < 1$, so ist diese Folge konvergent und zwar gilt

$$\lim_{n\to\infty} S_n = \frac{1}{1-z}\,.$$

[4]Bernoulli: Schweizer Gelehrtenfamilie. Niklaus B. 1623-1708 (Ratherr in Basel), Jakob I B. 1657-1705, Niklaus B. 1662-1716 (Maler), Johann I B. 1667-1748, Niklaus I B. 1687-1759, Niklaus II B. 1695-1726, Daniel B. 1700-1782, Johann II B. 1710-1790, Johann III B. 1744-1807, Jakob II B. 1759-1789

Um dies einzusehen, erinnern wir uns, dass

$$1^n - z^n = (1-z)(1 + z + \ldots + z^{n-1}),$$

und daher

$$S_{n-1} = \frac{1}{1-z} - \frac{z^n}{1-z}.$$

Sei nun $\epsilon > 0$ gegeben. Wähle $N \in \mathbb{N}$ mit $|z|^n < \epsilon$, $n \geq N$, dann folgt

$$\left|S_{n-1} - \frac{1}{1-z}\right| \leq \frac{|z|^n}{|1-z|} < \frac{\epsilon}{1-|z|}, \quad n \geq N.$$

Also konvergiert S_n gegen $\frac{1}{1-z}$.

Beachte das wir hier eigentlich eine Ungleichung der Form „$d(x_i, x) <$ Konstante mal ϵ“ erhalten haben, streng genommen also nicht das was in der Definition gefordert wurde. Startet man jedoch anstelle von ϵ mit der, ebenfalls positiven, Zahl $(1-|z|)\epsilon$, so erhält man Ende der Ungleichungskette nur ϵ.

//

Die Tatsache ob eine Folge von Punkten eines Raumes X konvergiert oder nicht, kann (muß aber nicht) von der gerade betrachteten Metrik abhängen.

4.2.6 Beispiel.

(*i*) Betrachte die ganzen Zahlen $\mathbb{Z}$, und sei eine Primzahl p festgehalten. Wir wollen überlegen, dass die Folge $(p^n)_{n\in\mathbb{N}}$ bezüglich der Metrik $d_{(p)}$ gegen 0 konvergiert, bezüglich der euklidischen Metrik d jedoch divergiert.

Sei $\epsilon > 0$ gegeben. Wähle $N \in \mathbb{N}$ mit $\frac{1}{p^N} < \epsilon$, dann gilt für alle $n \geq N$

$$d_{(p)}(p^n, 0) = \frac{1}{p^n} \leq \frac{1}{p^N} < \epsilon.$$

Sei nun angenommen es existiere $x \in \mathbb{Z}$ sodaß $p^n \to x$ bezüglich der euklidischen Metrik d. Wähle $N \in \mathbb{N}$ sodaß $d(p^n, x) < 1$, $n \geq N$. Dann folgt

$$p^n = d(p^n, 0) \leq d(p^n, x) + d(x, 0) < 1 + |x|, \quad n \geq N.$$

Das ist ein Widerspruch, denn da die Ordnung auf $\mathbb{Z}$ archimedisch ist, gibt es $n \in \mathbb{N}$, $n \geq N$, mit $n \cdot 1 > 1 + |x|$ und daher auch

$$p^n \geq 1 + n(p-1) \geq n \cdot 1 \geq 1 + |x|.$$

Tatsächlich sind in $\langle \mathbb{Z}, d\rangle$ nur die ab einem Index konstanten Folgen konvergent. Denn sei $x_i \to x$. Wähle $N \in \mathbb{N}$ mit $|x_i - x| < \frac{1}{2}$, $i \geq N$. Dann folgt $x_i = x$, $i \geq N$, denn zwei verschiedene ganze Zahlen haben sicher einen Abstand von mindestens 1.

(*ii*) Sei $(x_i)_{i\in\mathbb{N}}$ eine Folge von Elementen des $\mathbb{R}^n$. Wir wollen zeigen, dass diese Folge genau dann bezüglich der Metrik d_1 konvergiert, wenn sie bezüglich der euklidischen Metrik konvergiert, und dass in diesem Fall die jeweiligen Grenzwerte übereinstimmen.

Um dies einzusehen, bedienen wir uns der Ungleichungen

$$\max_{k=1,\dots,n}\left\{|x_k|\right\} \le \Big(\sum_{k=1}^{n}|x_k|^2\Big)^{\frac{1}{2}} \le \sum_{k=1}^{n}|x_k| \le n\cdot\max_{k=1,\dots,n}\left\{|x_k|\right\}. \quad (4.2.1)$$

Dabei sieht man das zweite „$\le$“ durch quadrieren, das erste und dritte ist klar. Diese Ungleichungen besagen nun, dass

$$d_2(x,y) \le d_1(x,y) \text{ und } d_1(x,y) \le n d_2(x,y)\,.$$

Sei nun $x_i \to x$ bezüglich d_1. Um zu zeigen, dass $x_i \to x$ bezüglich d_2 sei $\epsilon > 0$ gegeben. Wähle $N \in \mathbb{N}$ sodass $d_1(x_i, x) < \epsilon$ für $i \ge N$. Dann folgt dass auch $d_2(x_i, x) < \epsilon$ für solche i.

Umgekehrt, sei vorausgesetzt dass $x_i \to x$ bezüglich d_2, und sei $\epsilon > 0$ gegeben. Wähle $N \in \mathbb{N}$ sodass $d_2(x_i, x) < \frac{1}{n}\epsilon$ für $i \ge N$. Dann folgt dass $d_1(x_i, x) \le n d_2(x_i, x) < \epsilon$ für solche i.

//

Aus der Ungleichungskette (4.2.1) zieht man noch eine nützliche Folgerung, nämlich

4.2.7 Proposition. *Sei $(x_i)_{i\in\mathbb{N}}$ eine Folge von Punkten $x_i = (x_{i,1}, \dots, x_{i,n}) \in \mathbb{R}^n$, und sei $y = (y_1, \dots, y_n) \in \mathbb{R}^n$. Dann gilt $\lim_{i\to\infty} x_i = y$ genau dann, wenn*

$$\lim_{i\to\infty} x_{i,k} = y_k, \quad k = 1, \dots, n\,. \quad (4.2.2)$$

Beweis. Sei angenommen dass $x_i \to y$, und sei $k \in \{1, \dots, n\}$ und $\epsilon > 0$ gegeben. Wähle $N \in \mathbb{N}$ mit $d_2(x_i, x) < \epsilon$ für $i \ge N$. Dann folgt

$$|x_{i,k} - y_k| \le \Big(\sum_{l=1}^{n}|x_{i,l} - y_l|^2\Big)^{\frac{1}{2}} = d_2(x_i, y) < \epsilon, \quad i \ge N\,,$$

also $x_{i,k} \to y_k$ in $\mathbb{R}$.

Sei umgekehrt (4.2.2) vorausgesetzt und $\epsilon > 0$ gegeben. Wähle $N_1, \dots, N_n$ aus (4.2.2) und setze $N := \max\{N_1, \dots, N_n\}$. Dann gilt für $i \ge N$ wegen der entsprechenden Ungleichung aus (4.2.1)

$$d_2(x_i, y) \le n \max_{k=1,\dots,n}\{|x_{i,k} - y_k|\} < n\cdot\epsilon\,,$$

also gilt $x_i \to y$ bezüglich d_2. Beachte: Wieder haben wir eine Abschätzung „Konstante mal ϵ“ erhalten. Startet man mit $\frac{\epsilon}{n}$ anstelle von ϵ, so erhält man am Ende der Ungleichung nur ϵ. ❑

4.2.8 Korollar. *Sei $(z_i)_{i\in\mathbb{N}}$ eine Folge komplexer Zahlen und $z \in \mathbb{C}$. Dann gilt $\lim_{i\to\infty} z_i = z$ genau dann, wenn*

$$\lim_{i\to\infty}\mathrm{Re}(z_i) = \mathrm{Re}\,z \text{ und } \lim_{i\to\infty}\mathrm{Im}(z_i) = \mathrm{Im}\,z\,.$$

Beweis. Das ist gerade die Aussage von Proposition 4.2.7 für $n = 2$. ❑

Ein manchmal nützlicher Begriff ist der der Teilfolge einer gegebenen Folge.

4.2.9 Definition. Sei $(x_i)_{i\in\mathbb{N}}$ eine Folge. Ist $k : \mathbb{N} \to \mathbb{N}$ eine Funktion mit der Eigenschaft $k(n) < k(n+1)$, $n \in \mathbb{N}$, so heißt die Folge $(y_i)_{i\in\mathbb{N}}$ mit $y_i := x_{k(i)}$ eine *Teilfolge* von $(x_i)_{i\in\mathbb{N}}$. //

Zum Beispiel betrachte die Folge $x_n := \frac{1}{n}$. Dann wäre also die Folge $y_n := \frac{1}{3n+2}$ eine Teilfolge, die Funktion k wäre in diesem Beispiel gerade $k(n) := 3n+2$. Natürlich ist eine Folge selbst stets auch eine Teilfolge von sich, wähle nämlich $k(n) := n$.

Die Konvergenz einer Folge steht nun in Zusammenhang mit der Konvergenz von Teilfolgen.

4.2.10 Satz. *Sei $(x_n)_{n\in\mathbb{N}}$ eine Folge von Punkten eines metrischen Raumes $\langle X, d\rangle$ und sei $x \in X$. Dann gilt*

(i) Ist $\lim_{n\to\infty} x_n = x$ und $(x_{k(n)})_{n\in\mathbb{N}}$ eine Teilfolge von $(x_n)_{n\in\mathbb{N}}$, so ist auch $\lim_{n\to\infty} x_{k(n)} = x$.

(ii) Es gilt $\lim_{n\to\infty} x_n = x$ genau dann, wenn jede Teilfolge $(x_{k(n)})_{n\in\mathbb{N}}$ von $(x_n)_{n\in\mathbb{N}}$ eine Teilfolge $(x_{k(l(n))})_{n\in\mathbb{N}}$ hat, welche gegen x konvergiert.

Beweis. Um (i) einzusehen, sei angenommen daß $x_n \to x$, und sei $(x_{k(n)})_{n\in\mathbb{N}}$ eine Teilfolge. Zu $\epsilon > 0$ wähle $N \in \mathbb{N}$ sodaß $d(x_n, x) < \epsilon$ für alle $n \geq N$. Wegen $k(n) \geq n$, gilt dann erst recht $d(x_{k(n)}, x) < \epsilon$, $n \geq N$. Also haben wir $x_{k(n)} \to x$.

Wir haben damit auch eine Implikation von (ii) gezeigt, denn ist $x_n \to x$ so ist für jede Teilfolge $(x_{k(n)})_{n\in\mathbb{N}}$ diese Folge selbst eine Teilfolge von sich. Nach (i) konvergiert sie gegen x.

Für die Umkehrung in (ii) sei nun angenommen, daß jede Teilfolge von $(x_n)_{n\in\mathbb{N}}$ eine gegen den Wert x konvergente Teilfolge enthält. Angenommen es wäre nicht $x_n \to x$. Dann existierte also $\epsilon > 0$, sodaß es für jedes $N \in \mathbb{N}$ ein $n \geq N$ gibt mit $d(x_n, x) \geq \epsilon$. Wir konstruieren eine Teilfolge von $(x_n)_{n\in\mathbb{N}}$ rekursiv wie folgt: Es gibt ein $k(1)$ mit $d(x_{k(1)}, x) \geq \epsilon$. Zu $N = k(1) + 1$ gibt es nach dem oben Gesagten ein $k(2) \geq N$ mit $d(x_{k(2)}, x) \geq \epsilon$. Zu $N = k(2)+1$ gibt es, wieder nach dem oben Gesagten ein $k(3)$ mit $k(3) \geq N$ und $d(x_{k(3)}, x) \geq \epsilon$. Verfährt man induktiv so weiter, so erhält man eine Teilfolge $y_n := x_{k(n)}$, für welche gilt

$$d(y_n, x) \geq \epsilon, \quad n \in \mathbb{N}.$$

Sie kann also keine gegen x konvergente Teilfolge enthalten, ein Widerspruch. ❑

4.3 Vollständigkeit

Hat man eine Folge gegeben und möchte sie auf Konvergenz untersuchen, so besteht das Problem, dass man zuerst einmal den Grenzwert erraten muß, bevor man die Konvergenzbedingung nachweisen kann. Um diese Schwierigkeit umgehen zu versuchen, benützt man die Beobachtung, daß bei einer konvergenten Folge der Grenzwert x durch ein hinreichend spätes Folgenglied x_m ersetzen werden kann ohne die Aussage das x_n nahe ist wesentlich zu stören.

4.3.1 Proposition. *Die Folge $(x_n)_{n\in\mathbb{N}}$ sei konvergent. Dann gilt*

$$\forall \epsilon > 0\, \exists N \in \mathbb{N} : d(x_n, x_m) < \epsilon \text{ für alle } n, m \geq N.$$

Beweis. Sei $\epsilon > 0$ gegeben. Aus der Definition der Konvergenz weiß man daß eine Zahl $N \in \mathbb{N}$ existiert mit der Eigenschaft daß $d(x_n, x) < \frac{\epsilon}{2}$, $n \geq N$. Hier bezeichnet x den Grenzwert der Folge $(x_n)_{n\in\mathbb{N}}$ der zwar nach Voraussetzung existiert, über den sonst aber nichts bekannt zu sein braucht. Dann gilt nach der Dreiecksungleichung für $n, m \geq N$

$$d(x_n, x_m) \leq d(x_n, x) + d(x, x_m) < \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon.$$

❑

4.3.2 Definition. Sei $\langle X, d\rangle$ ein metrischer Raum, und sei $(x_n)_{n\in\mathbb{N}}$ eine Folge von Elementen von X. Diese Folge heißt eine *Cauchy-Folge*[5] falls gilt

$$\forall \epsilon > 0\, \exists N \in \mathbb{N} : d(x_n, x_m) < \epsilon \text{ für alle } n, m \geq N.$$

//

Wir haben in Proposition 4.3.1 gezeigt, daß jede konvergente Folge eine Cauchy-Folge ist. Würde nun jede Cauchy-Folge konvergieren, so könnten wir die Konvergenz einer Folge nachweisen ohne ihren Grenzwert explizit kennen zu müssen. Leider ist dies bei vielen metrischen Räumen nicht der Fall.

4.3.3 Definition. Ein metrischer Raum $\langle X, d\rangle$ heißt *vollständig*, wenn jede Cauchy-Folge von Elementen aus X in X einen Grenzwert besitzt. //

Die herausragende Bedeutung der reellen Zahlen begründet sich unter anderem auch auf der Tatsache, dass $\mathbb{R}$ vollständig ist. Diese spiegelt genau die definierende Eigenschaft von $\mathbb{R}$, nämlich vollständig angeordnet zu sein, wieder.

Dies einzusehen bedarf noch etwas Vorbereitung.

4.3.4 Definition. Sei $\langle X, d\rangle$ ein metrischer Raum, und sei $Y \subseteq X$. Dann heißt Y *beschränkt*, wenn es eine Zahl $M > 0$ und einen Punkt $x_0 \in X$ gibt, sodaß

$$d(y, x_0) \leq M, \quad y \in Y\,.$$

//

Die Menge Y ist also beschränkt, wenn sie ganz in einem gewissen Kreis (Mittelpunkt x_0, Radius M) liegt.

Beachte, dass man hat: Y ist beschränkt genau dann, wenn es zu jedem Punkt $x \in X$ eine Zahl $M_x > 0$ gibt mit $d(y, x) \leq M_x$, $y \in Y$. Denn, ist $x \in X$ gegeben, so setze $M_x := M + d(x, x_0)$. Dann gilt für jedes $y \in Y$

$$d(y, x) \leq d(y, x_0) + d(x_0, x) \leq M + d(x, x_0) = M_x\,.$$

4.3.5 Lemma. *Sei $(x_n)_{n\in\mathbb{N}}$ eine Cauchy-Folge, dann ist $\{x_n : n \in \mathbb{N}\}$ beschränkt. Die Umkehrung gilt nicht (ausser der Raum X besteht aus nur einem Element).*

Beweis. Wähle $N \in \mathbb{N}$ mit $d(x_n, x_m) < 1$ für $n, m \geq N$. Setzt man

$$M := 1 + \max\{d(x_1, x_N), \ldots, d(x_{N-1}, x_N)\}\,,$$

so erhält man das $d(x_n, x_N) \leq M$ für jedes $n \in \mathbb{N}$ gilt.

Um zu sehen dass die Umkehrung im allgemeinen nicht richtig sein kann, wähle $x, y \in X$, $x \neq y$, und betrachte die Folge $x, y, x, y, x, y, x, \ldots$. Diese ist beschränkt aber nicht Cauchy-Folge. ❑

[5] Augustin Louis Cauchy. 21.8.1789 Paris - 22.5.1857 Sceaux (bei Paris)

4.3.6 Definition. Eine Folge $(x_n)_{n\in\mathbb{N}}$ heißt *monoton* wenn entweder

$$x_1 \leq x_2 \leq x_3 \leq \dots \text{ (monoton wachsend)}$$

oder

$$x_1 \geq x_2 \geq x_3 \geq \dots \text{ (monoton fallend)}$$

gilt. //

4.3.7 Satz. *Sei $(x_n)_{n\in\mathbb{N}}$ eine monotone und beschränkte Folge reeller Zahlen. Dann ist $(x_n)_{n\in\mathbb{N}}$ in $\mathbb{R}$ konvergent.*

Beweis. Betrachte zuerst den Fall, dass die Folge $(x_n)_{n\in\mathbb{N}}$ monoton wachsend ist. Da sie beschränkt ist, ist die nichtleere Menge $\{x_n : n \in \mathbb{N}\}$ nach oben beschränkt. Nun gilt die Supremumseigenschaft, also existiert $x := \sup\{x_n : n \in \mathbb{N}\}$. Wir zeigen, daß $\lim_{n\to\infty} x_n = x$ gilt. Sei $\epsilon > 0$ gegeben. Da $x - \epsilon < x$ gilt, kann $x - \epsilon$ keine obere Schranke der Menge $\{x_n : n \in \mathbb{N}\}$ sein. Es gibt also ein $N \in \mathbb{N}$ mit $x_N > x - \epsilon$. Da die Folge $(x_n)_{n\in\mathbb{N}}$ monoton wächst, folgt $x_n \geq x_N > x - \epsilon$ für alle $n \geq N$. Da stets $x \geq x_n$ gilt, erhält man für $n \geq N$

$$0 \leq x - x_n < \epsilon,$$

und damit auch $|x_n - x| < \epsilon$.

Ist die Folge $(x_n)_{n\in\mathbb{N}}$ monoton fallend, so setze $x := \inf\{x_n : n \in \mathbb{N}\}$ und schließe analog. ❑

Die Bedingung „monoton und beschränkt“ ist hinreichend für Konvergenz, aber nicht notwendig; betrachte zum Beispiel die Folge $\left(\frac{(-1)^n}{n}\right)_{n\in\mathbb{N}}$. Dagegen ist die Bedingung „beschränkt“ notwendig für Konvergenz, aber nicht hinreichend; betrachte die Folge $((-1)^n)_{n\in\mathbb{N}}$.

Wir benützen Satz 4.3.7 nun um zu zeigen das $\mathbb{R}$ vollständig ist.

4.3.8 Satz (Cauchysches Konvergenzkriterium)**.** *Sei $(x_n)_{n\in\mathbb{N}}$ eine Cauchy-Folge reeller Zahlen. Dann existiert eine reelle Zahl x, sodaß $(x_n)_{n\in\mathbb{N}}$ gegen x konvergiert.*

Beweis. Der Beweis stützt sich auf die folgenden beiden Aussagen.

Schritt 1: Wir zeigen, dass jede Folge $(a_n)_{n\in\mathbb{N}}$ eine monotone Teilfolge $(a_{n(k)})_{k\in\mathbb{N}}$ besitzt.

Wir sagen die Folge $(a_n)_{n\in\mathbb{N}}$ besitzt beim Index k eine Spitze, falls $a_k \geq a_n$ für alle $n \geq k$. Wenn es unendlich viele Spitzen gibt, bilden sie eine monoton fallende Teilfolge. Gibt es keine oder nur endlich viele Spitzen so kann man einen Index k finden, ab dem keine Spitzen mehr auftreten. Setze $n_0 = k + 1$. Da n_0 keine Spitze ist existiert $n_1 > n_0$ mit $a_{n_1} > a_{n_0}$. Wieder kann n_1 keine Spitze sein, und daher muß n_2 existieren mit $a_{n_2} > a_{n_1}$. Verfährt man induktiv so weiter, erhält man eine monoton wachsende Teilfolge.

Schritt 2: Wir zeigen: Besitzt eine Cauchy-Folge $(x_n)_{n\in\mathbb{N}}$ eine konvergente Teilfolge, so ist sie konvergent.

Sei $(x_n)_{n\in\mathbb{N}}$ eine Cauchy-Folge und $(x_{n(k)})_{k\in\mathbb{N}}$ eine konvergente Teilfolge, $\lim_{k\to\infty} x_{n(k)} = x$. Sei $\epsilon > 0$ gegeben. Wähle N_1 so groß, daß $|x_n - x_m| < \epsilon$

für $n, m \geq N_1$. Wähle N_2 so groß, daß $|x_{n(k)} - x| < \epsilon$ für $k \geq N_2$. Sei $N := \max\{N_1, N_2\}$, dann gilt für $n \geq N$

$$|x_n - x| = |(x_n - x_{n(N)}) + (x_{n(N)} - x)| \leq |x_n - x_{n(N)}| + |x_{n(N)} - x| < \epsilon + \epsilon = 2\epsilon.$$

Beachte hier, dass $n(N) \geq N$.

Beweis des Satzes: Wir setzen diese beiden Aussagen nun mit Satz 4.3.7 zusammen. Sei $(x_n)_{n\in\mathbb{N}}$ eine Cauchy-Folge. Dann ist $(x_n)_{n\in\mathbb{N}}$ beschränkt. Wähle nach Schritt 1 eine monotone Teilfolge, dann ist diese natürlich ebenfalls beschränkt. Nach Satz 4.3.7 ist diese Teilfolge konvergent. Wegen Schritt 2 ist daher auch die Folge $(x_n)_{n\in\mathbb{N}}$ selbst konvergent. ❑

4.3.9 Korollar. *Der Raum $\mathbb{R}^n$ ist vollständig. Insbesondere sind auch die komplexen Zahlen $\mathbb{C}$ vollständig.*

Beweis. Wir bemerken, dass eine Folge $(x_i)_{i\in\mathbb{N}}$ von Punkten $x_i = (x_{i,1}, \ldots, x_{i,n})$ des $\mathbb{R}^n$ genau dann eine Cauchy-Folge ist, wenn für jedes $k \in \{1, \ldots, n\}$ die Folge $(x_{i,k})_{i\in\mathbb{N}}$ reeller Zahlen eine Cauchy-Folge ist. Dieses folgt mit Hilfe von (4.2.1), denn einerseits ist

$$|x_{i,k} - x_{j,k}| \leq d_2(x_i, x_j)\,,$$

und andererseits ist

$$d_2(x_i, x_j) \leq n \cdot \max_{k=1,\ldots,n} |x_{i,k} - x_{j,k}|\,.$$

Zum Beweis des Korollares sei nun $(x_i)_{i\in\mathbb{N}}$ eine Cauchy-Folge im $\mathbb{R}^n$. Dann ist für jedes $k = 1, \ldots, n$ die Folge $(x_{i,k})_{i\in\mathbb{N}}$ eine Cauchy-Folge in $\mathbb{R}$. Daher existieren $y_1, \ldots, y_n \in \mathbb{R}$ mit $x_{i_k} \to y_k$, $i \to \infty$. Nach Proposition 4.2.7 folgt $x_i \to (y_1, \ldots, y_n)$. ❑

4.4 Rechenregeln für Grenzwerte

Hat man auf einem metrischen Raum auch algebraische Operationen, so kann man sich fragen ob diese mit Grenzwerten verträglich sind. Betrachten wir zum Beispiel den Raum $\mathbb{R}^n$. Dann haben wir die Operationen der Addition

$$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n)$$

und der skalaren Multiplikation ($\lambda \in \mathbb{R}$)

$$\lambda \cdot (x_1, \ldots, x_n) = (\lambda x_1, \ldots, \lambda x_n)\,.$$

4.4.1 Proposition. *Es gilt:*

(*i*) *Seien $(x_i)_{i\in\mathbb{N}}$ und $(y_i)_{i\in\mathbb{N}}$ zwei Folgen im $\mathbb{R}^n$. Ist $\lim_{i\to\infty} x_i = x$ und $\lim_{i\to\infty} y_i = y$, so folgt dass $\lim_{i\to\infty}(x_i + y_i) = x + y$.*

(*ii*) *Sei $(x_i)_{i\in\mathbb{N}}$ eine Folge im $\mathbb{R}^n$ und $\lambda \in \mathbb{R}$. Ist $\lim_{i\to\infty} x_i = x$, so folgt dass $\lim_{i\to\infty}(\lambda \cdot x_i) = \lambda \cdot x$.*

Beweis. Der Beweis begründet sich auf der Festellung, dass für $x, y \in \mathbb{R}^n$ stets

$$d_2(x,y) = \Big(\sum_{k=1}^{n}(x_k - y_k)^2\Big)^{\frac{1}{2}} = d_2(x-y,0)$$

gilt, und dass für $x, y \in \mathbb{R}^n$, $\lambda \in \mathbb{R}$,

$$d_2(\lambda\cdot x, \lambda\cdot x) = \Big(\sum_{k=1}^{n}(\lambda x_k - \lambda y_k)^2\Big)^{\frac{1}{2}} =$$

$$= \Big(\sum_{k=1}^{n}\lambda^2(x_k - y_k)^2\Big)^{\frac{1}{2}} = \Big(\lambda^2\sum_{k=1}^{n}(x_k - y_k)^2\Big)^{\frac{1}{2}} = |\lambda| d_2(x,y)\,.$$

Um nun (i) einzusehen, sei $\epsilon > 0$ gegeben. Wähle $N_1, N_2 \in \mathbb{N}$ mit $d_2(x_i, x) < \epsilon$ für $i \geq N_1$ und $d_2(y_i, y) < \epsilon$ für $i \geq N_2$. Setze $N := \max\{N_1, N_2\}$, dann folgt für $i \geq N$

$$d_2(x_i + y_i, x + y) = d_2([x_i + y_i] - [x + y], 0) = d_2([x_i - x] - [y - y_i], 0) =$$

$$= d_2(x_i - x, y - y_i) \leq d_2(x_i - x, 0) + d_2(0, y - y_i) = d_2(x_i, x) + d_2(y_i, y) < 2\epsilon\,.$$

Um (ii) zu beweisen, wähle $N \in \mathbb{N}$ mit $d_2(x_i, x) < \epsilon$ für $i \geq N$. Dann folgt

$$d_2(\lambda x_i, \lambda x) = |\lambda| d_2(x_i, x) < |\lambda|\epsilon\,.$$

❑

Im Fall des $\mathbb{R}^n$ für $n = 1$ oder $n = 2$, d.h. betrachten wir reelle bzw. komplexe Zahlen, so haben wir eine weitere algebraische Operation, nämlich die der Multiplikation und die Inversenbildung.

4.4.2 Proposition. *Es gilt:*

- (i) *Seien* $(x_n)_{n\in\mathbb{N}}$ *und* $(y_n)_{n\in\mathbb{N}}$ *zwei Folgen im* $\mathbb{R}$ *oder* $\mathbb{C}$. *Ist* $\lim_{n\to\infty} x_n = x$ *und* $\lim_{n\to\infty} y_n = y$, *so folgt dass* $\lim_{n\to\infty}(x_n \cdot y_n) = x \cdot y$.
- (ii) *Sei* $(x_n)_{n\in\mathbb{N}}$ *eine Folge in* $\mathbb{R}$ *oder* $\mathbb{C}$. *Ist* $\lim_{n\to\infty} x_n = x$ *und* $x \neq 0$, *so ist* x_n *für hinreichend große Indizes verschieden von Null, und es gilt* $\lim_{n\to\infty} \frac{1}{x_n} = \frac{1}{x}$.

Beweis. Seien Folgen $(x_n)_{n\in\mathbb{N}}$ und $(y_n)_{n\in\mathbb{N}}$ reeller oder komplexer Zahlen gegeben mit $x_n \to x$ und $y_n \to y$. Weiters sei $\epsilon > 0$ gegeben. Wähle $C > 0$ sodass $|y_n| \leq C$, $n \in \mathbb{N}$. Eine solche Zahl existiert da konvergente Folgen insbesondere beschränkt sind. Es folgt

$$|x_n y_n - xy| = |(x_n - x)y_n + x(y_n - y)| \leq |x_n - x|\cdot|y_n| + |x|\cdot|y_n - y|$$

$$< \epsilon|y_n| + |x|\epsilon \leq (C + |x|)\epsilon.$$

Wir haben also eine Abschätzung der Gestalt Konstante (!) mal Epsilon gefunden und es folgt daher, daß $x_n y_n \to xy$.

Sei nun $x_n \to x$ und $x \neq 0$. Dann gilt auch $|x_n| \to |x|$, und daher ist für hinreichend große Werte von n sicher $|x_n| \geq \frac{|x|}{2}$. Es folgt die Abschätzung

$$\left|\frac{1}{x_n} - \frac{1}{x}\right| = \frac{|x - x_n|}{|x|\cdot|x_n|} \leq |x - x_n|\cdot\frac{2}{|x|^2}$$

und damit wird die Differenz $\frac{1}{x_n} - \frac{1}{x}$ für große n beliebig klein. ❑

Betrachten wir nun reelle Zahlen. Dort haben wir, neben den bereits diskutierten algebraischen Operationen, auch noch die Ordnungsrelation „$\leq$“. Auch diese ist mit Grenzwerten verträglich.

4.4.3 Proposition. *Seien $(x_n)_{n\in\mathbb{N}}$ und $(y_n)_{n\in\mathbb{N}}$ zwei Folgen reeller Zahlen, und gelte $x_n \leq y_n$ für alle $n \in \mathbb{N}$. Ist $\lim_{n\to\infty} x_n = x$ und $\lim_{n\to\infty} y_n = y$, so folgt dass auch $x \leq y$.*

Beweis. Wir nehmen indirekt an, daß $x > y$ ist. Wähle $\epsilon > 0$ mit $\epsilon < \frac{(x-y)}{3}$. Dann existiert N so groß, daß $|x_n - x| < \epsilon$ und $|y_n - y| < \epsilon$ für $n \geq N$. Für solche n gilt dann

$$x_n = (x_n - x) + (x - y) + (y - y_n) + y_n \geq y_n + \big[(x - y) - |x_n - x| - |y - y_n|\big] >$$

$$> y_n + \frac{x - y}{3} > y_n$$

ein Widerspruch. ❑

Als nächstes wollen wir eine oft praktische Methode angeben, mit Hilfe derer man auf die Konvergenz einer Folge reeller Zahlen schliessen kann.

4.4.4 Satz (Einzwick-Satz)**.** *Seien $(x_n)_{n\in\mathbb{N}}$, $(y_n)_{n\in\mathbb{N}}$ und $(a_n)_{n\in\mathbb{N}}$ Folgen mit $x_n \leq a_n \leq y_n$ für alle $n \in \mathbb{N}$. Gilt*

$$\lim_{n\to\infty} x_n = \lim_{n\to\infty} y_n,$$

so existiert auch der Grenzwert $\lim_{n\to\infty} a_n$ und ist gleich dem gemeinsamen Grenzwert von $(x_n)_{n\in\mathbb{N}}$ und $(y_n)_{n\in\mathbb{N}}$.

Beweis. Setze $a := \lim_{n\to\infty} x_n$. Zu $\epsilon > 0$ wähle $N \in \mathbb{N}$ mit $|x_n - a|, |y_n - a| < \epsilon$ für $n \geq N$. Für solche n folgt

$$-\epsilon < x_n - a \leq a_n - a \leq y_n - a < \epsilon,$$

d.h. $|a_n - a| < \epsilon$. ❑

4.4.5 Beispiel.

(*i*) Die Folge $x_n = \sqrt[n]{n}$ konvergiert gegen 1. Setze $a_n := x_n - 1$, dann ist $a_n \geq 0$ und $(1 + a_n)^n = n$. Nach dem Binomischen Lehrsatz gilt

$$n = (1 + a_n)^n = \sum_{k=0}^{n} \binom{n}{k} 1^k a_n^{n-k} \geq 1 + \frac{n(n-1)}{2} a_n^2.$$

Damit folgt $0 \leq a_n^2 \leq \frac{2(n-1)}{n(n-1)} = \frac{2}{n} \to 0$, also $a - N^2 \to 0$.

Daraus folgt das auch $a_n \to 0$: Wäre nicht $a_n \to 0$, so existierte ein $\epsilon > 0$ und eine Teilfolge $a_{k(n)}$ mit $a_{k(n)} \geq \epsilon$, $n \in \mathbb{N}$. Daher wäre $a_{k(n)}^2 \geq \epsilon^2$, $n \in \mathbb{N}$, ein Widerspruch. Wir schliessen das tatsächlich $a_n \to 0$ und damit $x_n \to 1$.

(*ii*) Ist $q > 0$ fest, so gilt $\lim_{n\to\infty} \sqrt[n]{q} = 1$. Betrachte den Fall $q > 1$. Dann gilt stets $\sqrt[n]{q} \geq 1$. Für n hinreichend groß gilt $\sqrt[n]{q} \leq \sqrt[n]{n}$. Also folgt $\sqrt[n]{q} \to 1$. Der Fall $q = 1$ ist klar. Im Fall $0 < q < 1$ betrachte $\frac{1}{\sqrt[n]{q}}$.

//

Kapitel 5

Unendliche Reihen

5.1 Der Begriff der Reihe

Wir sind schon einmal einer Folge $(S_n)_{n\in\mathbb{N}}$ begegnet die von der speziellen Gestalt $S_n = \sum_{k=0}^{n} a_k$ mit gewissen Zahlen a_k war. Das war die geometrische Reihe $S_n = 1+z+\ldots+z^n$ mit $|z| < 1$. Wir haben gezeigt, dass diese Folge konvergiert und zwar zum Grenzwert $\frac{1}{1-z}$. Das heißt also dass, für große Werte von n die Summe $\sum_{n=0}^{n} z^n$ dem Wert $\frac{1}{1-z}$ beliebig nahe kommt. Es ist also naheliegend zu schreiben

$$\frac{1}{1-z} = \sum_{n=0}^{\infty} z^n \,.$$

5.1.1 Definition. Sei $(a_k)_{k\in\mathbb{N}}$ eine Folge komplexer Zahlen. Bezeichne mit S_n, $n \in \mathbb{N}$, die endliche Summe

$$S_n := a_1 + a_2 + \ldots + a_n.$$

Die Folge $(S_n)_{n\in\mathbb{N}}$ heißt dann die *unendliche Reihe* mit den Summanden a_k.

Hat die Folge $(S_n)_{n\in\mathbb{N}}$ einen Grenzwert, so sagen wir die Reihe sei *konvergent*. In diesem Fall nennen wir ihren Grenzwert die *Summe der unendlichen Reihe* und benützen die Schreibweise

$$\lim_{n\to\infty} S_n =: \sum_{k=1}^{\infty} a_k \,.$$

Falls der Grenzwert $\lim\limits_{n\to\infty} S_n$ nicht existiert heißt die Reihe *divergent*. Die Folgenglieder S_n einer Reihe bezeichnet man auch als *Partialsummen*, die Zahlen a_k als *Summanden*. ∥

5.1.2 Bemerkung.

(*i*) Der Begriff einer Reihe macht offenbar nicht nur für Folgen $(a_k)_{k\in\mathbb{N}}$ komplexer Zahlen Sinn, sondern z.B. auch wenn $a_k \in \mathbb{R}^n$ ist. Tatsächlich müssen wir, damit obige Definition sinnvoll ist, nur wissen was es heißt zwei Elemente zu addieren und was es heißt dass eine Folge konvergiert.

(*ii*) Ändert man endlich viele Summanden einer Reihe ab, so ändert das nichts am Konvergenzverhalten der Reihe. Die tatsächliche Summe verändert sich natürlich schon.

(*iii*) Um die Notation zu vereinfachen benützt man die Schreibweise $\sum_{k=1}^{\infty} a_k$ auch für die Reihe $(S_n)_{n\in\mathbb{N}}$ selbst, und sagt dann $\sum_{k=1}^{\infty} a_k$ sei konvergent oder divergent.

//

5.1.3 Beispiel. Betrachte zum Beispiel die Reihe $\sum_{k=1}^{\infty} \frac{1}{k(k+1)}$. Wegen $\frac{1}{k(k+1)} = \frac{1}{k} - \frac{1}{k+1}$ gilt (*Teleskopreihe*)

$$S_n := \sum_{k=1}^{n} \frac{1}{k(k+1)} = \sum_{k=1}^{n} \left(\frac{1}{k} - \frac{1}{k+1} \right) = 1 - \frac{1}{n+1}.$$

Daher ist $\lim_{n\to\infty} S_n = 1$, d.h. die Reihe $\sum_{k=1}^{\infty} \frac{1}{k(k+1)}$ konvergiert und ihre Summe ist 1.

Läßt man die ersten drei Terme weg, d.h. ersetzt sie durch 0, so gilt für die entsprechenden Partialsummen S'_n stets $(n \geq 3)$

$$S'_n = S_n - \frac{1}{1\cdot 2} - \frac{1}{2\cdot 3} - \frac{1}{3\cdot 4} = \left(1 - \frac{1}{n+1}\right) - \frac{3}{4} \to \frac{1}{4}.$$

D.h. die Reihe $\sum_{k=4}^{\infty} \frac{1}{k(k+1)}$ ist ebenfalls konvergent. Ihre Summe ist $\frac{1}{4}$. //

Auf Grund der Definition einer unendlichen Reihe als Limes ihrer Partialsummen können wir Aussagen über Folgen sofort auf Reihen übertragen.

5.1.4 Korollar. *Es gilt*

(*i*) *Das* Cauchysche Konvergenzkriterium *: Die Reihe $\sum_{k=1}^{\infty} a_k$ ist genau dann konvergent, wenn gilt*

$$\forall \epsilon > 0\, \exists N \in \mathbb{N} : \left| \sum_{k=m+1}^{n} a_k \right| < \epsilon, \quad n > m \geq N.$$

(*ii*) Rechenregeln für Reihen*: Sind $\sum_{k=1}^{\infty} a_k$ und $\sum_{k=1}^{\infty} b_k$ konvergent, so ist auch $\sum_{k=1}^{\infty}(a_k + b_k)$ konvergent. Es gilt*

$$\sum_{k=1}^{\infty}(a_k + b_k) = \left(\sum_{k=1}^{\infty} a_k\right) + \left(\sum_{k=1}^{\infty} b_k\right).$$

Ist $\sum_{k=1}^{\infty} a_k$ konvergent und λ eine feste (reelle oder komplexe) Zahl, so ist auch $\sum_{k=1}^{\infty}(\lambda a_k)$ konvergent. Es gilt

$$\sum_{k=1}^{\infty}(\lambda a_k) = \lambda \cdot \sum_{k=1}^{\infty} a_k.$$

Beweis.
(*i*) Für die Partialsummen $S_n = \sum_{k=1}^{n} a_k$ gilt

$$S_n - S_m = \sum_{k=m+1}^{n} a_k.$$

(*ii*) Für die entsprechenden Partialsummen $S_n = \sum_{k=1}^{n} a_k$, $T_n = \sum_{k=1}^{n} b_k$ und $U_n = \sum_{k=1}^{n}(a_k + b_k)$ gilt

$$S_n + T_n = U_n.$$

Weiters gilt für $V_n = \sum_{k=1}^{n}(\lambda a_k)$ stets $V_n = \lambda S_n$. ❑

5.1.5 Bemerkung. Beim letzten Beweis haben wir die Rechengesetze wie Kommutativität, Distributivität u.ä. die für endliche Summen gelten benützt. Das Verhalten dieser Rechenregeln bei unendlichen Reihen ist wesentlich komplizierter, vgl. u.a. Beispiel 5.3.1. //

Will man mit Hilfe des Cauchyschen Konvergenzkriterium eine Reihe auf Konvergenz überprüfen, so muß man den Ausdruck

$$\left| \sum_{k=m+1}^{n} a_k \right|$$

abschätzen. Verwendet man die Dreiecksungleichung, so erhält man

$$\left| \sum_{k=m+1}^{n} a_k \right| \leq \sum_{k=m+1}^{n} | a_k | = \left| \sum_{k=m+1}^{n} |a_k| \right|. \tag{5.1.1}$$

Kennt man also eine hinreichend gute Abschätzung für den entsprechenden Ausdruck der Reihe $\sum_{k=1}^{\infty} |a_k|$, so ist man fertig.

5.1.6 Definition. Sei $(a_k)_{k\in\mathbb{N}}$ eine Folge komplexer Zahlen. Die Reihe $\sum_{k=1}^{\infty} a_k$ heißt *absolut konvergent*, wenn die Reihe der Beträge $\sum_{k=1}^{\infty} |a_k|$ konvergiert. //

Wegen der Beziehung (5.1.1) ist eine absolut konvergente Reihe auch konvergent. Die Umkehrung gilt jedoch im allgemeinen nicht, vgl. Beispiel 5.2.2 und Beispiel 5.3.1.

5.2 Konvergenzkriterien

Aus dem Cauchyschen Konvergenzkriterium erhält man unmittelbar eine einfache notwendige Bedingung für die Konvergenz einer Reihe.

5.2.1 Proposition. *Sei $(a_k)_{k\in\mathbb{N}}$ eine Folge komplexer Zahlen. Ist die Reihe $\sum_{k=1}^{\infty} a_k$ konvergent, dann ist*

$$\lim_{k\to\infty} a_k = 0.$$

Beweis. Sei $\epsilon > 0$ gegeben. Dann existiert $N \in \mathbb{N}$, so daß für $N \leq m < n$ gilt $|\sum_{k=m+1}^{n} a_k| < \epsilon$. Insbesondere gilt für $n > N$ (wähle $m := n-1$) stets $|a_n| < \epsilon$. ❑

5.2.2 Beispiel. Sei $\alpha \in \mathbb{Q}$. Betrachte die Reihe

$$I_\alpha := \sum_{k=1}^{\infty} \frac{1}{k^\alpha}. \tag{5.2.1}$$

Wir sehen, dass diese Reihe für $\alpha \leq 0$ divergiert, denn in diesem Fall bilden die Summanden keine Nullfolge.

Für $\alpha > 0$ gilt $\lim_{k\to\infty} \frac{1}{k^\alpha} = 0$, die Reihe I_α muss aber trotzdem nicht konvergieren.

Betrachte dazu zum Beispiel die *harmonischen Reihe* $I_1 = \sum_{k=1}^{\infty} \frac{1}{k}$. Die Folge der Partialsummen

$$S_n = \sum_{k=1}^{n} \frac{1}{k}$$

ist monoton wachsend da alle Summanden positiv sind. Für die Existenz des Limes ist also notwendig und hinreichend, daß diese Folge beschränkt ist. Nun gilt jedoch

$$S_{2^l} = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8} + \frac{1}{9} + \ldots + \frac{1}{2^l} \geq$$

$$1 + \frac{1}{2} + \underbrace{\frac{1}{4} + \frac{1}{4}}_{=\frac{1}{2}} + \underbrace{\frac{1}{8} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8}}_{=\frac{1}{2}} + \frac{1}{16} + \ldots + \frac{1}{2^l} \geq 1 + l \cdot \frac{1}{2},$$

d.h. S_{2^l} kann für $l \to \infty$ nicht beschränkt bleiben. //

Bei diesem Beispiel ist eigentlich nur eingegangen, daß man eine gewisse Teilfolge der Folge der Partialsummen nach unten abschätzen kann mit einer Folge die nicht beschränkt bleibt. Dies wurde dadurch erreicht, daß man die Glieder der gegebenen Summe einzeln nach unten abgeschätzt hat. Diese Idee, die auch in der anderen Richtung funktioniert, führt uns auf die folgenden hinreichenden Bedingungen für Konvergenz bzw. Divergenz von Reihen mit nichtnegativen Summanden.

5.2.3 Satz. *Seien $(a_k)_{k\in\mathbb{N}}$ und $(b_k)_{k\in\mathbb{N}}$ Folgen nichtnegativer reeller Zahlen. Dann gilt*

(*i*) Minorantenkriterium*: Ist $\sum_{k=1}^{\infty} b_k$ divergent und $a_k \geq b_k$, $k \in \mathbb{N}$, so ist auch $\sum_{k=1}^{\infty} a_k$ divergent.*

(*ii*) Majorantenkriterium*: Ist $\sum_{k=1}^{\infty} b_k$ konvergent und $a_k \leq b_k$, $k \in \mathbb{N}$, so ist auch $\sum_{k=1}^{\infty} a_k$ konvergent.*

Beweis. Bezeichne mit S_n bzw. T_n die Partialsummen der Reihen $\sum_{k=1}^{\infty} a_k$ bzw. $\sum_{k=1}^{\infty} b_k$. Da die Summanden a_k und b_k alle nichtnegativ sind, sind die Folgen $(S_n)_{n\in\mathbb{N}}$ und $(T_n)_{n\in\mathbb{N}}$ monoton wachsend. Nun ist eine monoton wachsende Folge genau dann konvergent, wenn sie nach oben beschränkt ist.

Gilt $a_k \geq b_k$ für alle $k \in \mathbb{N}$, so folgt $S_n \geq T_n$, $n \in \mathbb{N}$. Also impliziert die Unbeschränktheit von $(T_n)_{n\in\mathbb{N}}$, dass auch $(S_n)_{n\in\mathbb{N}}$ nicht beschränkt ist. Das zeigt das Minorantenkriterium.

Gilt $a_k \leq b_k$ für alle $k \in \mathbb{N}$, so folgt $S_n \leq T_n$, $n \in \mathbb{N}$. Also impliziert die Beschränktheit von $(T_n)_{n\in\mathbb{N}}$, dass auch $(S_n)_{n\in\mathbb{N}}$ beschränkt ist. Das zeigt das Majorantenkriterium. ❑

Das Majoranten bzw. Minorantenkriterium wird oft in der folgenden Form angewendet:

5.2.4 Korollar. *Seien $(a_k)_{k\in\mathbb{N}}$ und $(b_k)_{k\in\mathbb{N}}$ Folgen positiver reeller Zahlen. Gibt es reelle Zahlen $c, C > 0$, sodass*

$$c \leq \frac{a_k}{b_k} \leq C, \quad k \in \mathbb{N},$$

dann sind die Reihen $\sum_{k=1}^{\infty} a_k$ und $\sum_{k=1}^{\infty} b_k$ entweder beide konvergent oder beide divergent.

Beweis. Sei $\sum_{k=1}^{\infty} b_k$ konvergent. Nach unserer Voraussetzung gilt $a_k \leq Cb_k$, $k \in \mathbb{N}$, also ist nach dem Majorantenkriterium $\sum_{k=1}^{\infty} a_k$ konvergent.

Umgekehrt sei $\sum_{k=1}^{\infty} b_k$ divergent. Wegen $cb_k \leq a_k$ und dem Minorantenkriterium ist dann auch $\sum_{k=1}^{\infty} a_k$ divergent. ❑

Die Voraussetzung dieses Korollars ist insbesondere dann erfüllt wenn der Grenzwert $\lim_{k\to\infty} \frac{a_k}{b_k}$ existiert und positiv ist.

5.2.5 Beispiel. Durch Vergleich mit der harmonischen Reihe ist nach dem Minorantenkriterium die Reihe $I_\alpha = \sum_{k=1}^{\infty} \frac{1}{k^\alpha}$ auch für alle $\alpha \in \mathbb{Q}$, $\alpha \leq 1$, divergent. //

Wir wollen das Majorantenkriterium nun ausnützen um durch Vergleich mit der geometrischen Reihe zwei hinreichende Bedingungen für absolute Konvergenz bzw. Divergenz einer Reihe zu erhalten.

5.2.6 Satz. *Sei $(a_k)_{k\in\mathbb{N}}$ eine Folge komplexer Zahlen. Dann gilt:*

(*i*) Wurzelkriterium*: Es existiere eine Zahl q, $0 < q < 1$, und ein Index $k_0 \in \mathbb{N}$, sodaß*

$$\sqrt[k]{|a_k|} \leq q, \quad k \geq k_0\,. \tag{5.2.2}$$

Dann ist die Reihe $\sum_{k=1}^{\infty} a_k$ absolut konvergent.

Gibt es eine Teilfolge $(a_{k(l)})_{l\in\mathbb{N}}$ von $(a_k)_{k\in\mathbb{N}}$ mit $\sqrt[k]{|a_{k(l)}|} \geq 1$, so ist die Reihe $\sum_{k=1}^{\infty} a_k$ divergent.

(*ii*) Quotientenkriterium*: Sei vorausgesetzt dass stets $a_k \neq 0$. Es existiere eine Zahl q, $0 < q < 1$, und ein Index $k_0 \in \mathbb{N}$, sodaß*

$$\frac{|a_{k+1}|}{|a_k|} \leq q, \quad k \geq k_0\,. \tag{5.2.3}$$

Dann ist die Reihe $\sum_{k=1}^{\infty} a_k$ absolut konvergent.

Gibt es einen Index $k_0 \in \mathbb{N}$ mit $\frac{|a_{k+1}|}{|a_k|} \geq 1$, $k \geq k_0$, so ist die Reihe $\sum_{k=1}^{\infty} a_k$ divergent.

Beweis.
Wurzelkriterium: Ist $\sqrt[k]{|a_k|} \leq q < 1$, $k \geq k_0$, so gilt $|a_k| \leq q^k$ für diese k. Da die Reihe $\sum_{k=k_0}^{\infty} q^k$ konvergiert, zeigt das Majorantenkriterium dass $\sum_{k=k_0}^{\infty} |a_k|$, und damit auch $\sum_{k=1}^{\infty} |a_k|$ konvergiert.

Ist dagegen $\sqrt[k]{|a_k|} \geq 1$ für unendlich viele Indizes k, kann $(a_k)_{k\in\mathbb{N}}$ keine Nullfolge sein, und daher ist die Reihe divergent.

Quotientenkriterium: Es existiere $q < 1$, sodaß für hinreichend große $k \in \mathbb{N}$, d.h. für alle $k \geq k_0$ mit einem geeigneten k_0, gilt

$$|a_{k+1}| \leq q a_k\,.$$

Dann ist also

$$|a_l| \leq q^l \frac{|a_{k_0}|}{q^{k_0}}, \quad l \geq k_0\,,$$

und wir erhalten $\sqrt[l]{|a_l|} \leq q \cdot \sqrt[l]{\frac{|a_{k_0}|}{q^{k_0}}}$. Da der zweite Faktor mit $l \to \infty$ gegen 1 strebt, finden wir eine Zahl $\hat{q} < 1$ und einen Index k_1 sodass für $k \geq k_1$ stets

$\sqrt[k]{|a_k|} \le \hat{q}$ gilt. Also können wir das Wurzelkriterium anwenden, und sehen dass $\sum_{k=1}^{\infty} a_k$ absolut konvergiert.

Ist $\frac{|a_{k+1}|}{|a_k|} \ge 1$, so kann $(a_k)_{k\in\mathbb{N}}$ keine Nullfolge sein, da sie ab einem Index monoton wächst. ❑

Diese Bedingungen werden oft in der folgenden Form angewandt:

5.2.7 Korollar. *Sei $(a_k)_{k\in\mathbb{N}}$ eine Folge komplexer Zahlen. Ist*

$$\lim_{k\to\infty} \frac{|a_{k+1}|}{|a_k|} < 1 \text{ bzw. } \lim_{k\to\infty} \sqrt[k]{|a_k|} < 1\,,$$

so ist die Reihe $\sum_{k=1}^{\infty} a_k$ absolut konvergent. Ist einer dieser Limiten dagegen > 1, so ist die Reihe divergent.

Beweis. Ist $\lim_{k\to\infty} \frac{|a_{k+1}|}{|a_k|} < 1$, so setze $\epsilon := 1 - \lim_{k\to\infty} \frac{|a_{k+1}|}{|a_k|}$ und wähle k_0, sodaß für $k \ge k_0$ gilt $|\frac{|a_{k+1}|}{|a_k|} - \lim_{k\to\infty} \frac{|a_{k+1}|}{|a_k|}| < \frac{\epsilon}{2}$. Dann ist

$$\frac{|a_{k+1}|}{|a_k|} < 1 - \frac{\epsilon}{2} =: q < 1, \quad k \ge k_0\,.$$

In den anderen Fällen geht man genauso vor. ❑

5.2.8 Beispiel.

(*i*) Betrachte die Reihe $\sum_{n=0}^{\infty} \frac{1}{n!}$. Diese Reihe ist konvergent, denn es gilt

$$\frac{\frac{1}{(n+1)!}}{\frac{1}{n!}} = \frac{1\cdot 2\cdot \ldots \cdot n}{1\cdot 2\cdot \ldots \cdot n\cdot (n+1)} = \frac{1}{n} \to 0\,.$$

(*ii*) Bezeichne mit $\tau(n)$ die Anzahl der Teiler der natürlichen Zahl n. Wir betrachte die Reihe $\sum_{n=1}^{\infty} \tau(n)x^n$ wobei $x > 0$ ist. Wegen $\tau(n) \le n$ gilt

$$\sqrt[n]{\tau(n)x^n} = x\cdot \sqrt[n]{\tau(n)} \le x\cdot \sqrt[n]{n} \to x\,.$$

Ist also $x < 1$, so ist die Reihe konvergent. Für $x \ge 1$ ist sie sicher divergent, denn dann bilden die Summanden keine Nullfolge.

Wir haben im Beweis von Satz 5.2.6 gesehen dass das Quotientenkriterium schwächer als das Wurzelkriterium ist[1]. Das eben betrachtete Beispiel ist nun eines wo das Wurzelkriterium zum Ziel führt, das Quotientenkriterium aber versagt. Denn: Sei $n > 2$ eine Primzahl. Dann gilt $\tau(n) = 2$. Weiters ist n sicher ungerade, und damit kann $n+1$ keine Primzahl sein, also gilt $\tau(n+1) \ge 3$. Wir erhalten damit

$$\frac{\tau(n+1)x^{n+1}}{\tau(n)x^n} \ge \frac{3}{2}\cdot x\,.$$

[1]Das heißt dass die Voraussetzung (5.2.3) des Quotientenkriteriums stets jene des Wurzelkriteriums, das ist (5.2.2), impliziert. Führt für eine gegebene Reihe das Quotientenkriterium zum Ziel (=Konvergenzbeweis), dann muß es das Wurzelkriterium erst recht tun. Der Grund warum man das Quotientenkrietrium überhaupt formuliert, ist dass die Bedingung (5.2.3) oft recht einfach zu überprüfen ist.

Im Fall $x \geq \frac{2}{3}$ ist dieser Quotient ≥ 1. Da es unendlich viele Primzahlen gibt, können wir also das Quotientenkriterium nicht anwenden.

Wir sehen, dass für $\frac{2}{3} \leq x < 1$ das Wurzelkriterium die Konvergenz der Reihe zeigt, das Quotientenkriterium jedoch nicht anwendbar ist.

(*iii*) In vielen Situationen können Wurzel- oder Quotientenkriterium nicht angewendet werden. So zum Beispiel immer dann, wenn $\lim_{k\to\infty} \sqrt[k]{|a_k|} = 1$ ist. Dass in diesem Fall tatsächlich keine Aussage gemacht werden kann, sieht man am Beipiel der Reihe I_α aus (5.2.1). Es ist in diesem Beispiel stets

$$\sqrt[k]{a_k} = (\sqrt[k]{k})^\alpha \to 1\,.$$

Wir wissen aus Beispiel 5.2.5, dass für $\alpha \leq 1$ die Reihe (5.2.1) divergiert. Dagegen kann man zeigen, dass sie für $\alpha > 1$ konvergiert, vgl. Beispiel 5.2.13

//

Der folgende Satz gibt uns eine hinreichende Bedingung für Konvergenz (aber nicht notwendigerweise absolute Konvergenz).

5.2.9 Satz (Dirichletsches[2]Kriterium)**.** *Sei $(a_n)_{n\in\mathbb{N}}$ eine monoton fallende Nullfolge reeller Zahlen, und sei $(b_n)_{n\in\mathbb{N}}$ eine Folge komplexer Zahlen, sodaß für eine gewisse Zahl $M > 0$ gilt*

$$\Big|\sum_{n=1}^{N} b_n\Big| \leq M, \quad N \in \mathbb{N}.$$

Dann ist die Reihe $\sum_{n=1}^{\infty} a_n b_n$ konvergent.

Wir zeigen zunächst eine Hilfsaussage.

5.2.10 Lemma. *Sei $(\alpha_k)_{k\in\mathbb{N}}$ eine monotone Folge reeller Zahlen, $(\beta_k)_{k\in\mathbb{N}}$ eine Folge komplexer Zahlen, und $L > 0$. Gilt*

$$\Big|\sum_{k=1}^{m} \beta_k\Big| \leq L, \quad m \in \mathbb{N}\,,$$

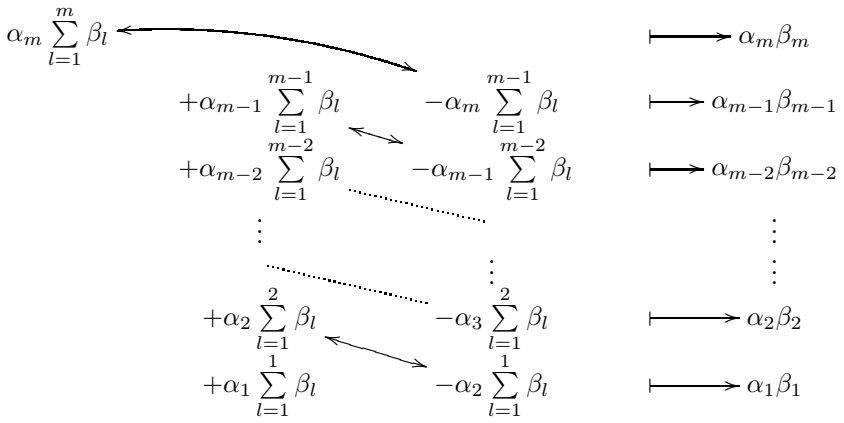
so folgt

$$\Big|\sum_{k=1}^{m} \alpha_k\beta_k\Big| \leq L\big(|\alpha_1| + 2|\alpha_m|\big), \quad m \in \mathbb{N}\,.$$

Beweis. Wir schreiben die Summe $\sum_{k=1}^{m} \alpha_k\beta_k$ in trickreicher Weise um (*Abelsche partielle Summation*):

$$\sum_{k=1}^{m} \alpha_k\beta_k = \alpha_m \sum_{l=1}^{m} \beta_l + \sum_{k=1}^{m-1} \Big[(\alpha_k - \alpha_{k+1}) \sum_{l=1}^{k} \beta_l\Big]$$

[2]Johann Peter Gustav Lejeune Dirichlet. 13.2.1805 Düren (bei Aachen) - 5.5.1859 Göttingen



Es folgt

$$\Big|\sum_{k=1}^{m}\alpha_k\beta_k\Big| \le |\alpha_m|\cdot L + \sum_{k=1}^{m-1}|\alpha_k-\alpha_{k+1}|\cdot L\,.$$

Da alle Zahlen $(\alpha_k-\alpha_{k+1})$ das gleiche Vorzeichen haben, gilt

$$\sum_{k=1}^{m-1}|\alpha_k-\alpha_{k+1}| = \Big|\sum_{k=1}^{m-1}(\alpha_k-\alpha_{k+1})\Big| \le |\alpha_1|+|\alpha_m|\,.$$

Das zeigt die gewünschte Abschätzung. ❑

Beweis (von Satz 5.2.9). Wähle $N\in\mathbb{N}$ mit $|a_n|<\epsilon$, $n\ge N$. Wir wenden das obige Lemma an mit

$$\alpha_k := a_{N+k},\quad \beta_k := b_{N+k},\qquad L := 2M\,.$$

Die Voraussetzung des Lemmas ist erfüllt, den $(m\in\mathbb{N})$

$$\Big|\sum_{k=1}^{m}\beta_k\Big| = \Big|\sum_{n=N+1}^{N+m}b_n\Big| \le \Big|\sum_{n=1}^{N+m}b_n-\sum_{n=1}^{N}b_n\Big| \le 2M\,.$$

Wir erhalten, dass

$$\Big|\sum_{n=N+1}^{N+m}a_nb_n\Big| = \Big|\sum_{k=1}^{m}\alpha_k\beta_k\Big| \le L\big(|\alpha_1|+2|\alpha_m|\big) = 2M\big(|a_{N+1}|+2|a_{N+m}|\big) < 2M\cdot 3\epsilon$$

Nach dem Cauchyschen Kriterium ist die Reihe $\sum_{k=1}^{\infty}a_kb_k$ konvergent. ❑

5.2.11 Korollar (Abelsches[3]Kriterium)**.** *Sei die Reihe $\sum_{n=1}^{\infty}b_n$ konvergent und sei $(a_n)_{n\in\mathbb{N}}$ eine monotone und beschränkte Folge. Dann ist die Reihe $\sum_{n=1}^{\infty}a_nb_n$ konvergent.*

Beweis. Die Folge $(a_n)_{n\in\mathbb{N}}$ ist konvergent, $a_n\to a$. Es gilt

$$\sum_{n=1}^{N}a_nb_n = \sum_{n=1}^{N}(a_n-a)b_n + a\sum_{n=1}^{N}b_n.$$

[3]Niels Henrik Abel. 5.8.1802 Finnö (Norwegen) - 6.4.1829 Froland (Norwegen)

Für $N \to \infty$ existiert für jeden der beiden Summanden auf der rechten Seite der Grenzwert, denn die Reihe $\sum_{n=1}^{\infty}(a_n - a)b_n$ konvergiert nach dem Dirichletschen Kriterium und die Reihe $\sum_{n=1}^{\infty} b_n$ nach Voraussetzung. ❑

5.2.12 Korollar (Leibnitz[4]Kriterium)**.** *Sei $\sum_{n=1}^{\infty}(-1)^n a_n$ eine alternierende Reihe, d.h. $a_n \geq 0$, $n \in \mathbb{N}$. Ist $(a_k)_{k\in\mathbb{N}}$ monoton fallend und gilt $\lim_{n\to\infty} a_n = 0$, so folgt dass die Reihe $\sum_{n=1}^{\infty}(-1)^n a_n$ konvergiert.*

Beweis. Setze im Dirichletschen Kriterium $b_n = (-1)^n$ ❑

5.2.13 Beispiel. Wir können nun zeigen, dass die Reihe I_α aus (5.2.1) für jedes $\alpha \in \mathbb{Q}$, $\alpha > 1$ konvergiert.

Wähle $m \in \mathbb{N}$ mit $\frac{m+1}{m} \leq \alpha$. Nach dem Majorantenkriterium genügt es die Behauptung für den Exponenten $\frac{m+1}{m}$ zu zeigen.

Betrachte die Reihe $\sum_{k=1}^{\infty}(-1)^{k+1}\frac{1}{k^{\frac{1}{m}}}$. Diese ist nach dem Leibnitz Kriterium konvergent. Nun ist

$$\frac{1}{(2k-1)^{\frac{1}{m}}} - \frac{1}{(2k)^{\frac{1}{m}}} = \frac{(2k)^{\frac{1}{m}} - (2k-1)^{\frac{1}{m}}}{(2k-1)^{\frac{1}{m}}(2k)^{\frac{1}{m}}} = \frac{1}{(2k-1)^{\frac{1}{m}}(2k)^{\frac{1}{m}}}\cdot$$

$$\cdot\frac{(2k)-(2k-1)}{(2k)^{\frac{m-1}{m}} + (2k)^{\frac{m-2}{m}}(2k-1)^{\frac{1}{m}} + \ldots + (2k)^{\frac{1}{m}}(2k-1)^{\frac{m-2}{m}} + (2k-1)^{\frac{m-1}{m}}} \geq$$

$$\geq \frac{1}{(2k)^{\frac{2}{m}}m(2k)^{\frac{m-1}{m}}} = \frac{1}{m2^{\frac{m+1}{m}}}\cdot\frac{1}{k^{\frac{m+1}{m}}}$$

Es folgt nach dem Majorantenkriterium, daß auch die Reihe $\sum_{k=1}^{\infty}\frac{1}{k^{\frac{m+1}{m}}}$ konvergent ist. //

5.3 Das Rechnen mit Reihen

Wir werden im Folgenden sehen, dass absolute Konvergenz gewährleistet dass man mit der Reihe genauso umgehen kann wie wenn sie eine endlich Summe wäre.

Zuerst beschäftigen wir uns mit der Kommutativität der Addition. Ist $\sum_{k=1}^{N} a_k$ eine endliche Summe, so können wir die Summanden beliebig umordnen ohne das sich die Summe verändert. Anders ausgedrückt, ist σ eine *Permutation* von $\{1,\ldots,N\}$, d.h. eine Bijektion von $\{1,\ldots,N\}$ auf sich, dann gilt $\sum_{k=1}^{N} a_k = \sum_{k=1}^{N} a_{\sigma(k)}$.

5.3.1 Beispiel. Betrachte die *alternierende harmonische Reihe*

$$S = 1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \frac{1}{5} - \frac{1}{6} \pm \ldots.$$

Diese ist nach Leibnitz konvergent.

Ordnen wir die Summanden in einer anderen Reihenfolge an, z.B. als

$$\underbrace{1-\frac{1}{2}}_{=\frac{1}{2}} - \frac{1}{4} + \underbrace{\frac{1}{3}-\frac{1}{6}}_{=\frac{1}{6}} - \frac{1}{8} + \underbrace{\frac{1}{5}-\frac{1}{10}}_{=\frac{1}{10}} - \frac{1}{12} + \underbrace{\frac{1}{7}-\frac{1}{14}}_{=\frac{1}{14}} - \frac{1}{16} + \ldots =$$

[4]Gottfried Wilhelm Leibnitz. 1.7.1646 Leipzig - 14.11.1716 Hannover

$$= \frac{1}{2} - \frac{1}{4} + \frac{1}{6} - \frac{1}{8} + \frac{1}{10} - \frac{1}{12} + \frac{1}{14} - \frac{1}{16} + \ldots = \frac{1}{2}\big(1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \frac{1}{5} - \frac{1}{6} \pm \ldots\big),$$

so erhalten wir gerade $\frac{S}{2}$.

Die Summe einer Reihe kann also von der Reihenfolge der Summanden abhängen. Tatsächlich kann man eine konvergente aber nicht absolut konvergente Reihe stets so umordnen, dass jede beliebige Summe, oder gar eine divergente Reihe, herauskommt. //

5.3.2 Definition. Sei $\sum_{k=1}^{\infty} a_k$ gegeben. Unter einer *Umordnung* dieser Reihe verstehen wir eine Reihe $\sum_{k=1}^{\infty} b_k$ mit $b_k = a_{\sigma(k)}$ wo σ eine Bijektion von $\mathbb{N}$ auf sich ist. //

5.3.3 Satz. *Sei $(a_k)_{k\in\mathbb{N}}$ eine Folge komplexer Zahlen, und sei die Reihe $\sum_{k=1}^{\infty} a_k$ absolut konvergent. Dann ist auch jede Umordnung $\sum_{k=1}^{\infty} a_{\sigma(k)}$ absolut konvergent und hat die gleiche Summe.*

Beweis. Zuerst eine vorbereitende Bemerkung. Sei $\sigma^{-1} : \mathbb{N} \to \mathbb{N}$ die inverse Abbildung von σ. Für $N \in \mathbb{N}$ definieren wir

$$L^+(N) := \max_{k\le N} \sigma(k), \quad L^-(N) := \max_{k\le N} \sigma^{-1}(k)\,.$$

Dann gilt

$$\{\sigma(1), \ldots, \sigma(N)\} \subseteq \{1, \ldots, L^+(N)\}$$
$$\{1, \ldots, N\} \subseteq \{\sigma(1), \ldots, \sigma(L^-(N))\}$$

Sei nun $\epsilon > 0$ gegeben, und wähle $N \in \mathbb{N}$ mit

$$\sum_{k=m+1}^{m'} |a_k| < \epsilon, \quad m' > m \ge N\,.$$

Sei $n \ge L^-(N)$, dann gilt

$$\sum_{k=1}^{n} a_k - \sum_{k=1}^{n} a_{\sigma(k)} = \sum_{k=N+1}^{n} a_k + \Big(\sum_{k=1}^{N} a_k - \sum_{k=1}^{n} a_{\sigma(k)}\Big) = \sum_{k=N+1}^{n} a_k - \sum_{\substack{k\in\{1,\ldots,n\}\\ \sigma(k)\notin\{1,\ldots,N\}}} a_{\sigma(k)}$$

und wir erhalten

$$\Big|\sum_{k=1}^{n} a_k - \sum_{k=1}^{n} a_{\sigma(k)}\Big| \le \sum_{k=N+1}^{n} |a_k| + \sum_{\substack{k\in\{1,\ldots,n\}\\ \sigma(k)\notin\{1,\ldots,N\}}} |a_{\sigma(k)}| \le \sum_{k=N+1}^{n} |a_k| + \sum_{k=N+1}^{L^+(n)} |a_k| < 2\epsilon$$

Es gilt also

$$\lim_{m\to\infty} \Big(\sum_{k=1}^{n} a_k - \sum_{k=1}^{n} a_{\sigma(k)}\Big) = 0\,,$$

und wir sehen, dass die umgeordnete Reihe $\sum_{k=1}^{\infty} a_{\sigma(k)}$ konvergiert und zwar zur gleichen Summe wie $\sum_{k=1}^{\infty} a_k$.

Wendet man die obige Überlegung an auf die Reihe $\sum_{k=1}^{\infty} |a_k|$ und die entsprechende Umordnung $\sum_{k=1}^{\infty} |a_{\sigma(k)}|$, so folgt daß $\sum_{k=1}^{\infty} |a_{\sigma(k)}|$ konvergiert, d.h. $\sum_{k=1}^{\infty} a_{\sigma(k)}$ ist absolut konvergent. ❑

Als nächstes wollen wir uns mit dem Distributivgesetz befassen. Für zwei endliche Summen gilt ja

$$\left(\sum_{i=1}^{N} a_i\right) \cdot \left(\sum_{j=1}^{M} b_j\right) = \sum_{i=1}^{N} \sum_{j=1}^{M} a_i b_j \,.$$

Um das Produkt zu berechnen, muß man also alle Einzelprodukte aufsummieren. Möchte man nun das Produkt von zwei Reihen ausrechnen,

$$\left(\sum_{i=1}^{\infty} a_i\right) \cdot \left(\sum_{j=1}^{\infty} b_j\right) = ?,$$

so muß man alle Einzelprodukte $a_i b_j$, $i, j = 1, 2, 3, \ldots$, aufsummieren:

$$\begin{array}{ccccccc} a_1b_1 & + & a_1b_2 & + & a_1b_3 & + & \ldots \\ + & & + & & + & & \\ a_2b_1 & + & a_2b_2 & + & a_2b_3 & + & \ldots \\ + & & + & & + & & \\ a_3b_1 & + & a_3b_2 & + & a_3b_3 & + & \ldots \\ + & & + & & + & & \\ \vdots & & \vdots & & \vdots & & \end{array}$$

Wie wir wissen, ist es eine heikle Aufgabe in welcher Reihenfolge man dieses tut.

Wir betrachten also eine *Doppelreihe*: Seien Zahlen a_{ij}, $i, j \in \mathbb{N}$, gegeben

$$\begin{array}{cccc} a_{11} & a_{12} & a_{13} & \ldots \\ a_{21} & a_{22} & a_{23} & \ldots \\ a_{31} & a_{32} & a_{33} & \ldots \\ \vdots & \vdots & \vdots & \ddots \end{array}$$

Verschiedene Möglichkeiten um alle a_{ij} aufzusummieren wären zum Beispiel zuerst die Zeilen aufzusummieren, $s_i = \sum_{j=1}^{\infty} a_{ij}$, und dann die Spalten:

$$S_1 = \sum_{i=1}^{\infty} \left(\sum_{j=1}^{\infty} a_{ij}\right)$$

oder zuerst die Spalten, $v_j = \sum_{i=1}^{\infty} a_{ij}$, und dann die Zeilen

$$S_2 = \sum_{j=1}^{\infty} \left(\sum_{i=1}^{\infty} a_{ij}\right)$$

oder man summiert längs der Diagonalen

$$S_3 = \sum_{k=2}^{\infty} \left(\sum_{i+j=k} a_{ij}\right)$$

oder überhaupt auf irgend eine andere Weise.

5.3.4 Definition. Eine Reihe $\sum_{k=1}^{\infty} b_k$ heißt eine *lineare Anordnung* der Doppelreihe $\sum_{i,j=1}^{\infty} a_{ij}$, falls $b_k = a_{\sigma(k)}$ mit einer Bijektion $\sigma : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$. //

Von den drei oben genannten Summationsmethoden ist nur die Summation längs der Diagonalen eine lineare Anordnung.

5.3.5 Beispiel. Betrachte man

$$\begin{array}{ccccccccccc}
1 & - & 1 & + & 0 & + & 0 & + & \dots & = & 0 \\
+ & & + & & + & & + & & & & \\
0 & + & 1 & - & 1 & + & 0 & + & \dots & = & 0 \\
+ & & + & & + & & + & & & & \\
0 & + & 0 & + & 1 & - & 1 & + & \dots & = & 0 \\
+ & & + & & + & & + & & & & \\
0 & + & 0 & + & 0 & + & 1 & - & \dots & = & 0 \\
+ & & + & & + & & + & & & & \\
\vdots & & \vdots & & \vdots & & \vdots & & & & \vdots \\
= & & = & & = & & = & & & & = \\
1 & + & 0 & + & 0 & + & 0 & + & \dots & = & 1 \setminus 0
\end{array}$$

d.h. $\sum_{i=1}^{\infty} \left(\sum_{j=1}^{\infty} a_{ij} \right) = 0$, $\sum_{j=1}^{\infty} \left(\sum_{i=1}^{\infty} a_{ij} \right) = 1$. Summiert man längs der Diagonalen, so erhält man

$$1 - 1 + 1 - 1 + 1 - 1 \pm \dots,$$

diese Summe ist also nicht einmal konvergent. //

5.3.6 Satz. *Seien komplexe Zahlen a_{ij}, $i, j \in \mathbb{N}$, gegeben. Es existiere eine Konstante $C > 0$, sodaß*

$$\sum_{i=1}^{M} \sum_{j=1}^{M} |a_{ij}| \leq C, \quad M \in \mathbb{N}\,.$$

Dann ist jede lineare Anordnung von $\sum_{i,j=1}^{\infty} a_{ij}$ absolut konvergent und und alle haben die gleiche Summe S. Weiters gilt

$$S = \sum_{i=1}^{\infty} \left(\sum_{j=1}^{\infty} a_{ij} \right) = \sum_{j=1}^{\infty} \left(\sum_{i=1}^{\infty} a_{ij} \right)$$

wobei alle auftretenden Reihen absolut konvergieren.

Beweis. Sei $\sum_{k=1}^{\infty} b_k$ eine lineare Anordnung von $\sum_{i,j=1}^{\infty} a_{ij}$. Da $\left(\sum_{k=1}^{N} |b_k| \right)_{N \in \mathbb{N}}$ eine monoton wachsende Folge ist, und nach unserer Voraussetzung durch C nach oben beschränkt ist, ist sie konvergent. D.h. $\sum_{k=1}^{\infty} b_k$ ist absolut konvergent. Da je zwei lineare Anordnungen Umordnungen voneinander sind, folgt die erste Behauptung.

Das gleiche Argument zeigt, daß alle Reihen $\sum_{i=1}^{\infty} a_{ij}$, $j \in \mathbb{N}$, und $\sum_{j=1}^{\infty} a_{ij}$, $i \in \mathbb{N}$, absolut konvergent sind.

Sei $\epsilon > 0$ gegeben. Wähle eine lineare Anordnung $\sum_{k=1}^{\infty} b_k$ der betrachteten Doppelreihe, und $N \in \mathbb{N}$ mit

$$\sum_{k=m+1}^{n} |b_k| < \epsilon, \quad n > m \geq N\,.$$

Wähle $U, V \in \mathbb{N}$ mit

$$\{b_1, \ldots, b_N\} \subseteq \{a_{ij} : \ i = 1, \ldots, U, \, j = 1, \ldots, V\} .$$

Für $u \geq U$ und $v \geq V$ wähle $L(u, v) \geq N$ mit

$$\{a_{ij} : \ i = 1, \ldots, u, \, j = 1, \ldots, v\} \subseteq \{b_k : k = 1, \ldots, L(u, v)\} .$$

Dann gilt

$$\left| \sum_{i=1}^{u} \sum_{j=1}^{v} a_{ij} - \sum_{k=1}^{l} b_k \right| \leq \sum_{k=N+1}^{l} |b_k| < \epsilon, \quad l \geq L(u, v), \, v \geq V, \, u \geq U .$$

Wir gehen in dieser Beziehung, für festgehaltenes u und v, zum Grenzwert $l \to \infty$ über. Es folgt

$$\left| \sum_{i=1}^{u} \sum_{j=1}^{v} a_{ij} - \sum_{k=1}^{\infty} b_k \right| \leq \epsilon, \quad v \geq V, \, u \geq U .$$

In dieser Beziehung gehen wir, für festgehaltenes u, zum Grenzwert $v \to \infty$ über, und erhalten

$$\left| \sum_{i=1}^{u} \left(\sum_{j=1}^{\infty} a_{ij} \right) - \sum_{k=1}^{\infty} b_k \right| \leq \epsilon, \quad u \geq U .$$

Beachte bei dieser Argumentation, daß wir wissen das alle auftretenden Limiten existieren.

Wir haben also gezeigt, dass der Grenzwert $\lim_{u\to\infty} \sum_{i=1}^{u} \left(\sum_{j=1}^{\infty} a_{ij} \right)$ existiert und gleich S ist, d.h. $\sum_{i=1}^{\infty} \left(\sum_{j=1}^{\infty} a_{ij} \right) = S$. Vertauscht man in der obigen Argumentation die Rollen von u und v, so erhält man $\sum_{j=1}^{\infty} \left(\sum_{i=1}^{\infty} a_{ij} \right) = S$.

Die absolute Konvergenz der auftretenden Reihen folgt, da die Voraussetzung des Satzes nur vom Betrag $|a_{ij}|$ abhängt, und wir daher die gezeigte Aussage auch auf $|a_{ij}|$, $i, j \in \mathbb{N}$, anwenden können. ❑

5.3.7 Bemerkung. Im zweiten Teil des obigen Beweises haben wir eigentlich gezeigt, daß zwei Grenzübergänge vertauschbar sind:

$$\lim_{u\to\infty} \lim_{v\to\infty} \sum_{i=1}^{u} \sum_{j=1}^{v} a_{ij} = \lim_{v\to\infty} \lim_{u\to\infty} \sum_{i=1}^{u} \sum_{j=1}^{v} a_{ij}$$

//

5.3.8 Korollar. *Seien die beiden Reihen $\sum_{i=0}^{\infty} a_i$ und $\sum_{j=0}^{\infty} b_j$ absolut konvergent. Dann ist jede lineare Anordnung der Doppelreihe $\sum_{i,j=1}^{\infty} a_i b_j$ absolut konvergent und alle haben die gleiche Summe S, nämlich*

$$S = \left(\sum_{i=0}^{\infty} a_i \right) \cdot \left(\sum_{j=0}^{\infty} b_j \right) .$$

Beweis. Sei $\sum_{i=1}^{\infty} |a_i| = C$, $\sum_{j=1}^{\infty} |b_j| = D$, dann folgt

$$\sum_{i=1}^{N}\sum_{j=1}^{M} |a_i b_j| = \Big(\sum_{i=1}^{N} |a_i|\Big) \cdot \Big(\sum_{j=1}^{M} |b_j|\Big) \leq C \cdot D\,,$$

also sind nach Satz 5.3.6 alle linearen Anordnungen sowie die iterierten Reihen absolut konvergent und haben die gleiche Summe S.

Die iterierten Reihen kann man aber leicht berechnen:

$$S = \lim_{N\to\infty} \lim_{M\to\infty} \sum_{i=1}^{N}\sum_{j=1}^{M} a_i b_j = \lim_{N\to\infty} \lim_{M\to\infty} \Big[\Big(\sum_{i=1}^{N} a_i\Big) \cdot \Big(\sum_{j=1}^{M} b_j\Big)\Big] =$$

$$= \lim_{N\to\infty} \Big[\Big(\sum_{i=1}^{N} a_i\Big) \cdot \Big(\sum_{j=1}^{\infty} b_j\Big)\Big] = \Big(\sum_{i=1}^{\infty} a_i\Big) \cdot \Big(\sum_{j=1}^{\infty} b_j\Big)\,.$$

❑

Anhang A

Symbole und Operationen der Logik

Auf der ersten mit mathematischen Inhalten befassten Seite des dtv-Atlas zur Mathematik findet sich der folgenden Text:

Die Mathematik ist wie jede Wissenschaft darauf angewiesen, ihre Ergebnisse mündlich und schriftlich zu formulieren. Wegen der Vielfalt der Sprachen und der Gefahr von Mißverständnissen beim Gebrauch der Umgangssprache ist man in der Mathematik mehr und mehr dazu übergegangen, die Aussagen in einer künstlichen, formalisierten Sprache wiederzugeben, die nur noch die logisch bedeutsamen Elemente der Umgangssprache enthält. Es beginnt damit, daß man selbst den Begriff der *Aussage* zu präzisieren hat. Im allgemeinen fordert man, daß die Aussagen in die Klasse der wahren und die Klasse der falschen Aussagen eingeteilt werden können (*Prinzip der Zweiwertigkeit*). Eine Aussage ist dann jedes schrift-sprachliche Gebilde, dem entweder der *Wahrheitswert* des Wahren W oder der des Falschen F zukommt. Dabei spielt es keine Rolle, auf welche Weise der Wahrheitswert festgestellt wird. Bei bis heute nicht bewiesenen Vermutungen in der Mathematik etwa steht der Wahrheitswert gar nicht fest, doch darf bei der üblichen Auffassung angenommen werden, daß sie entweder wahr oder falsch sind.

Obwohl manche der hier genannten Punkte auch oft in Zweifel gezogen werden (z.B. Zweiwertigkeit, Beliebigkeit der Beweismethode, o.ä.), scheint dieser Text ein recht brauchbares Bild zu vermitteln.

Ist A eine Aussage, so schreiben wir $w(A)$ für den Wahrheitswert von A. Beispiele für Aussagen (mathematischer oder auch nichtmathematischer Natur) wären z.B.

A_1	Die Rose ist eine Pflanze	$w(A_1) = W$
A_2	2+4=6	$w(A_2) = W$
A_3	Der Affe ist ein Fisch	$w(A_3) = F$
A_4	Alle Nullstellen der Riemannschen Zetafunktion liegen auf der Geraden $\operatorname{Re} z = \frac{1}{2}$	$w(A_4) =$ unbekannt
A_5	4 ist eine Primzahl	$w(A_5) = F$

Es gibt auch schrift-sprachliche Gebilde die keine Aussage liefern, z.B. „Die Zahl 5 ist größer“.

Man kann nun Aussagen in mannigfaltiger Weise miteinander Verknüpfen.

Manche dieser Operationen treten so häufig auf, daß sie einen eigenen Namen bekommen.

1.0.9 Definition. Seien A und B Aussagen. Dann verstehen wir unter

- $\neg A$ die Aussage „*nicht* A“, welche genau dann wahr ist, wenn A falsch ist.
- $A \vee B$ die Aussage „A *oder* B“, welche genau dann wahr ist, wenn A wahr ist oder B wahr ist (oder beide).
- $A \wedge B$ die Aussage „A *und* B“, welche genau dann wahr ist, wenn sowohl A als auch B wahr sind.
- $A \Rightarrow B$ die Aussage „*wenn* A*, dann* B“. Diese Aussage ist genau dann wahr, wenn B immer dann wahr ist wenn A wahr ist. D.h. der Fall, daß zwar A wahr ist, B jedoch falsch darf nicht auftreten.
- $A \iff B$, die Aussage „A *genau dann, wenn* B“. Diese Aussage ist genau dann wahr, wenn A und B entweder gemeinsam wahr oder gemeinsam falsch sind.

//

1.0.10 Beispiel. Mit den oben angeführten Beispielen von Aussagen $A_1, \ldots, A_5$ lassen sich in einfacher Weise einige Verknüpfungen anschreiben. Zum Beispiel sind $A_1 \wedge A_2$, $A_1 \vee A_3$, $\neg A_5$ wahre Aussagen, jedoch $A_1 \wedge A_3$, $A_3 \vee A_5$ falsch. Wahr ist $A_2 \Rightarrow A_1$, falsch ist $A_2 \Rightarrow A_3$. Offenbar wahr sind $A_1 \iff A_2$ sowie $A_3 \iff A_5$. Falsch wäre jedoch $A_1 \iff A_3$.

Die Natur der Implikation „$\Rightarrow$“ ist anschaulich nicht so klar wie die von $\vee$ oder $\wedge$. Man beachte zum Beispiel, daß die Aussagen $A_3 \Rightarrow A_2$, $A_3 \Rightarrow A_4$, $A_3 \Rightarrow A_5$ sämtliche wahr sind. Weiters wahr ist $A_4 \Rightarrow A_1$, der Wahrheitswert von $A_4 \Rightarrow A_3$ ist jedoch unbekannt. //

Die benannten zweistelligen logischen Verknüpfungen von Aussagen sind nicht voneinander unabhängig. Zum Beispiel besagt $A \Rightarrow B$ nichts anderes als $\neg A \vee B$, in Formeln also

$$(A \Rightarrow B) \iff (\neg A \vee B), \tag{A.0.1}$$

oder es besagt $A \iff B$ nichts anderes als $(A \Rightarrow B) \wedge (B \Rightarrow A)$. Man kann sogar sämtliche denkbaren Verknüpfungen aus einer einzigen zweistelligen Verknüpfung ableiten, z.B. aus dem sogenannten *Sheffer-Strich* $A|B$. Diese Aussage ist genau dann wahr, wenn nicht zugleich A und B wahr sind. D.h.

$$A|B \iff \neg(A \wedge B).$$

Man kann alle Verknüpfungen mit Hilfe dieses Strichsymbols schreiben, z.B. gilt $(\neg A) \iff (A|A)$ oder $(A \Rightarrow B) \iff (A|(B|B))$. Eine weitere logische Verknüpfung, die aus der Informatik wohlbekannt ist, ist das „*nor*“: $(A \text{ nor } B) \iff \neg(A \vee B)$. Wesentliche Eigenschaft dieser Verknüpfung ist, daß man aus ihr ebenfalls alle anderen Verknüpfungen ableiten kann.

Einen Ausdruck in dem -Aussagen representierende- Variablen, sowie logische Verknüpfungen vorkommen nennt man *Aussageform*. Eine Aussageform kann, je nach Belegung der Variablen mit wahren oder falschen Aussagen den

Wahrheitswert wahr oder falsch annehmen. Eine interessante Rolle spielen jene Aussageformen, welche stets (d.h. egal welche Aussagen man für die Variablen einsetzt) wahr sind. Solche sind von besonderem Interesse für die Mathematik, da sie logische Schlußweisen representieren aus denen sich ein mathematischer Beweis aufbaut. Einige Beispiele solcher *allgemeingültigen Aussageformen* stellen wir in der folgenden Proposition zusammen. Den Beweis führt man durch Belegen der Aussagevariablen mit sämtlichen denkbaren Kombinationen aus wahr oder falsch.

1.0.11 Proposition. *Die folgenden Aussageformen sind unabhängig von der Belegung der Variablen mit wahren oder falschen Aussagen wahr:*

(*i*) $A \vee \neg A$ *(*Satz vom ausgeschlossenen Dritten*)*

(*ii*) $\neg(A \wedge \neg A)$ *(*Satz vom Widerspruch*)*

(*iii*) $\neg\neg A \iff A$ *(*Satz von der doppelten Verneinung*)*

(*iv*) $(A \wedge B) \Rightarrow A$, $A \Rightarrow (A \vee B)$

(*v*) $(A \iff B) \Rightarrow (A \Rightarrow B)$

(*vi*) $\neg(A \wedge B) \iff (\neg A) \vee (\neg B)$, $\neg(A \vee B) \iff (\neg A) \wedge (\neg B)$ *(*Sätze von deMorgan[1]*)*

(*vii*) $(A \Rightarrow B) \iff (\neg A \vee B)$

(*viii*) $(A \Rightarrow B) \iff (\neg B \Rightarrow \neg A)$ *(*Kontrapositionssatz*)*

(*ix*) $((A \Rightarrow B) \wedge A) \Rightarrow B$ *(*modus ponens*)*

(*x*) $((A \Rightarrow B) \wedge \neg B) \Rightarrow \neg A$ *(*modus tollens*)*

(*xi*) $((A \Rightarrow B) \wedge (B \Rightarrow C)) \Rightarrow (A \Rightarrow C)$ *(*modus barbara*)*

(*xii*) $(A \wedge (B \vee C)) \iff ((A \wedge B) \vee (A \wedge C))$, $(A \vee (B \wedge C)) \iff ((A \vee B) \wedge (A \vee C))$ *(*Distributivsätze*)*

Beweis. Wir werden exemplarisch einige dieser Punkte zeigen. Betrachte zum Beispiel die erste deMorgansche Regel: Für die Aussageform $\neg(A \wedge B)$ ergibt sich

$$\neg(A \wedge B): \quad \begin{array}{c|cc} B \backslash A & W & F \\ \hline W & F & W \\ F & W & W \end{array}$$

Für $\neg A \vee \neg B$ erhält man

$$\neg A \vee \neg B: \quad \begin{array}{c|cc} B \backslash A & W & F \\ \hline W & F & W \\ F & W & W \end{array}$$

Man sieht dass, egal welche Wahrheitswerte A und B haben, die beiden Aussageformen $\neg(A \wedge B)$ und $\neg A \vee \neg B$ gemeinsam wahr oder falsch sind.

[1] Auguste de Morgan. 27.6.1806 Madura (Indien) - 18.3.1871 London

Für Beweisführungen bedeutsam ist der modus ponens:

$A \Rightarrow B$:

B \ A	W	F
W	W	W
F	F	W

$(A \Rightarrow B) \wedge A$:

B \ A	W	F
W	W	F
F	F	F

$\big((A \Rightarrow B) \wedge A\big) \Rightarrow B$:

B \ A	W	F
W	W	W
F	W	W

❑

Es gibt auch viele komplexere allgemeingültige Aussageformen. Das eine solche Aussageform allgemeingültig ist, kann man natürlich immer durch belegen der involvierten Variablen mit allen möglichen Wahrheitswerten zeigen, oft kann man sich aber diese Arbeit ersparen und die Allgemeingültigkeit durch anwenden der bereits bekannten Regeln herleiten.

1.0.12 Proposition. *Die folgenden Aussageformen sind unabhängig von der Belegung der Variablen mit wahren oder falschen Aussagen wahr:*

(i) $\big(A \Rightarrow (B \wedge C)\big) \Rightarrow (A \Rightarrow B)$, $\big((A \vee B) \Rightarrow C\big) \Rightarrow (A \Rightarrow C)$

(ii) $\big(((A \wedge \neg B) \Rightarrow C) \wedge \neg C\big) \Rightarrow (A \Rightarrow B)$

Beweis. Wir zeigen exemplarisch den Punkt (ii). Es gilt

(1)	(modus tollens)	$\big(((A \wedge \neg B) \Rightarrow C) \wedge \neg C\big) \Rightarrow \neg(A \wedge \neg B)$
(2)	(deMorgan)	$\neg(A \wedge \neg B) \iff (\neg A \vee B)$
(3)	(v)	$\neg(A \wedge \neg B) \Rightarrow (\neg A \vee B)$
(4)	(A.0.1)	$\neg A \vee B \iff (A \Rightarrow B)$
(5)	(v)	$\neg A \vee B \Rightarrow (A \Rightarrow B)$
(6)	2-mal (modus barbara)	$\big(((A \wedge \neg B) \Rightarrow C) \wedge \neg C\big) \Rightarrow (A \Rightarrow B)$

❑

1.0.13 Bemerkung. Prinzip des direkten Beweises: Um eine Implikation $A \Rightarrow B$ zu beweisen, zeigt man eine Reihe von Implikationen $A \Rightarrow C_1$, $C_1 \Rightarrow C_2$, …, $C_n \Rightarrow B$, und wendet den modus barbara an. //

Betrachtet man mathematische (oder auch irgendwelche anderen) Aussagen, so stößt man auch auf Redewendungen wie „für alle Dinge gilt... “, oder „es gibt ein Ding für das...“. Um solche Aussagen ebenfalls formal zu erfassen und um mit ihnen, auch wenn sie in komplexeren Zusammenhang auftreten, logisch korrekt umgehen zu können, führt man sogenannte *Quantoren* ein. Den *Allquantor* $\forall$ und den *Existenzquantor* $\exists$. Diese Bezeichnungen sind in gewissem Maße wohl selbsterklärend. Ist zum Beispiel $A(n)$ die Aussage über natürliche Zahlen „n ist eine Primzahl“, so bedeutet

$$\exists n : A(n) \wedge (4 < n < 10)$$

nichts anderes als „es existiert eine Primzahl n die größer als 4 aber kleiner 10 ist. Offensichtlich ist diese Aussage wahr. Weiters bedeutet zum Beispiel

$$\forall n \in \mathbb{N} : 3 | (2n + 1)$$

die Aussage „für jede natürliche Zahl n, ist 3 ein Teiler von $2n + 1$“. Eine offensichtlich falsche Aussage. Im allgemeinen werden natürlich auch mehrere Quantoren gemeinsam in einer Formel auftreten. Zum Beispiel bedeutet

$$\forall n \in \mathbb{N}\ \exists m \in \mathbb{N} : (5|m) \wedge (m \geq n)$$

nichts anderes als die (offenbar wahre) Aussage „für jede natürliche Zahl n existiert eine natürliche Zahl m, welche durch 5 teilbar ist und größer oder gleich n ist“.

Genauso wie bei den Verknüpfungen der Aussagenlogik, sind auch hier jene Formeln von besonderer Bedeutung, die stets, also unabhängig von der Belegung gewisser Variablen mit gewissen Wahrheitswerten, wahr sind. Der Beweis solcher Sätze der Prädikatenlogik ist jedoch nicht mehr so einfach wie bei jenen der Aussagenlogik, da Quantoren ja im allgemeinen Aussagen über unendliche Mengen darstellen können. Solche kann man nicht mehr durch Einsetzen aller möglichen Varianten auf Richtigkeit testen.

1.0.14 Proposition. *Die folgenden Formeln der Prädikatenlogik sind allgemeingültig.*

(i) Verneinungssätze*:*

$$\neg(\forall x : A(x)) \iff \exists x : (\neg A(x)),\ \neg(\exists x : A(x)) \iff \forall x : (\neg A(x)).$$

(ii) Vertauschbarkeitssätze*:*

$$\forall x\ \forall y : A(x,y) \iff \forall y\ \forall x : A(x,y),$$
$$\exists x\ \exists y : A(x,y) \iff \exists y\ \exists x : A(x,y),$$
$$\exists x\ \forall y : A(x,y) \Rightarrow \forall y\ \exists x : A(x,y).$$

(iii) $(\forall x : A(x)) \Rightarrow A(x)$, $A(x) \Rightarrow (\exists x : A(x))$.

Man beachte das die Formel

$$\forall y\ \exists x : A(x,y) \Rightarrow \exists x\ \forall y : A(x,y)$$

nicht allgemeingültig ist.

1.0.15 Beispiel. Betrachte zum Beispiel die Aussage

$$\forall n \in \mathbb{N}\, \exists m \in \mathbb{N} :\ 2|(n+m)$$

d.h. „Für jede natürliche Zahl n existiert eine natürliche Zahl m, sodass $n + m$ gerade ist“. Diese Aussage ist offensichtlich wahr, für m kann man 1 oder 2 wählen, je nachdem ob n ungerade oder gerade ist. Betrachtet man jedoch die Aussage

$$\exists m \in \mathbb{N}\, \forall n \in \mathbb{N} :\ 2|(n+m)$$

so hat man eine falsche Aussage. Denn: Ist m gerade, so ist für $n = 1$ die Zahl $m + n$ ungerade, ist dagegen m ungerade, so ist für $n = 2$ die Zahl $m + n$ ungerade.

Der wesentliche Unterschied zwischen $\forall y\, \exists x : A(x,y)$ und $\exists x\, \forall y : A(x,y)$ ist: Im ersten Fall existiert zwar zu jedem y ein x, dieses darf jedoch von y abhängen. Dagegen muß im zweiten Fall ein x existieren welches für alle y funktioniert, d.h. für jedes y ein und das selbe x. //

Eine weitere Schreibweise sei, ob ihrer häufigen Verwendung, noch erwähnt: Der Ausdruck

$$\exists | x : A(x)$$

fasst die beiden Aussagen $\exists x : A(x)$ und $A(y) \Rightarrow y = x$ zusammen. Er besagt also: „Es existiert genau ein x sodass $A(x)$ wahr ist“.

Wir wollen zur Illustration nun die Aussage von Proposition 1 und ihren Beweis analysieren. Dazu müssen wir uns zuerst einmal klar machen, welche Ansprüche wir an Formulierung und Beweis eines mathematischen Satzes stellen. In der Formulierung eines Satzes müssen zumindest die folgenden Dinge klar herausgestellt sein:

(1) Was sind die Dinge die wir betrachten, bzw. in welcher Situation befinden wir uns.

(2) Was sind die Voraussetzungen von denen wir ausgehen.

(3) Was ist die Schlussfolgerung die wir ziehen.

Ein Beweis eines Satzes ist dann eine Herleitung der Wahrheit der gewünschten Schlussfolgerung unter Annahme der Wahrheit der Voraussetzungen und mit Hilfe logischer Schlussregeln. Meistens wird ein Beweis geführt indem man herleitet, dass die Aussageform „(Voraussetzungen)⇒(Konklusion)“ wahr ist. Denn dann kann man mit Hilfe des modus ponens von der Wahrheit der Voraussetzungen auf die Wahrheit der Konklusion schliessen.

Kommen wir jetzt wirklich zu Proposition 1.

(1) Was sind die Dinge die wir betrachten? Natürliche Zahlen.

(2) Was sind unsere Voraussetzungen? Nicht klar.

(3) Was ist unsere Schlussfolgerung? Für jede natürliche Zahl n sind die beiden Zahlen $2(1 + \ldots + n)$ und $n^2 + n$ gleich.

Wollen wir nun den ersten Beweis von Proposition 1 betrachten, dann wird sich wohl hoffentlich auch herausstellen welche Voraussetzungen wir benötigen. Bezeichne die Aussage „Die beiden Zahlen $2(1 + \ldots + n)$ und $n^2 + n$ sind gleich“ mit $A(n)$. Dann ist unsere Schlussfolgerung also $\forall n \in \mathbb{N} : A(n)$.

Schritt 1, Induktionsanfang „$A(1)$“:

$$\begin{aligned} 2 \cdot 1 &\overset{RR}{=} 2 \\ 1 \cdot 1 + 1 &\overset{RR}{=} 1 + 1 \overset{def}{=} 2 \end{aligned}$$

Hier haben wir die Rechenregel benützt dass 1 ist neutrales Element der Multiplikation ist, sowie die Definition der Zahl 2 als Nachfolger von 1, $2 = S(1)$, und die Definition von $1 + 1$ nämlich $1 + 1 = +_1(1) = S(1)$. Wir haben gezeigt: Wenn alle diese Regeln gelten, so ist $A(1)$ wahr.

Schritt 2, Induktionsschritt „$\forall n \in \mathbb{N} : A(n) \Rightarrow A(n + 1)$“:

$$2\big(1 + 2 + \ldots + n + (n + 1)\big) \overset{RR}{=} 2\big((1 + 2 + \ldots + n) + (n + 1)\big) \overset{RR}{=}$$

$$\overset{RR}{=} 2(1 + 2 + \ldots + n) + 2(n + 1) \overset{IV}{=} (n^2 + n) + 2(n + 1) \overset{def}{=}$$

$$\stackrel{def}{=} (n^2+n)+(1+1)(n+1) \stackrel{RR}{=} (n^2+n)+(n+1)+(n+1) \stackrel{RR}{=}$$

$$\stackrel{RR}{=} (n^2+n+n+1)+(n+1) \stackrel{RR}{=} (n+1)^2+(n+1)$$

Hier haben wir benützt: Assoziativgesetz, Distributivgesetz, die Induktionsvoraussetzung, und die Definition von 2 als Nachfolger von 1. Wir haben gezeigt: Wenn alle diese Regeln gelten, so ist $\forall n \in \mathbb{N} : A(n) \Rightarrow A(n+1)$ wahr.

Schritt 3, Prinzip der vollständigen Induktion: Dieses besagt, dass $A(1) \wedge (\forall n \in \mathbb{N} : A(n) \Rightarrow A(n+1)) \Rightarrow \forall n \in \mathbb{N} : A(n)$.

Schritt 4, Anwendung des modus ponens: Setzt man nun voraus, dass alle benützten Rechenregeln und das Prinzip der vollständigen Induktion gelten, so schliessen wir mit Hilfe des modus ponens wegen Schritt 1 auf die Wahrheit von $A(1)$, wegen Schritt 2 auf die Wahrheit von $\forall n \in \mathbb{N} : A(n) \Rightarrow A(n+1)$, und wegen Schritt 3 auf die Wahrheit von $\forall n : A(n)$.

Anhang B

Axiomatischer Aufbau der natürlichen Zahlen

Um mit Hilfe logischer Schlüsse irgendwelche Aussagen herzuleiten, müssen wir von irgendwelchen Grundaussagen ausgehen. Denn unsere Beweise sind ja immer Implikationen „(Voraussetzungen)⇒(Konklusion)“, und um mit Hilfe des modus ponens auf die Wahrheit der Konklusion zu schliessen benötigen wir die Wahrheit der Voraussetzungen. Solche Grundaussagen, auf deren Wahrheit man sich einigt, nennt man auch *Axiome*. Natürlich wird man versuchen möglichst wenige Axiome zu fordern, denn schliesslich wollen wir nicht mehr als unbedingt nötig einfach glauben.

2.0.16 Definition. Die *natürlichen Zahlen* sind eine Menge $\mathbb{N}$, in der ein Element $1 \in \mathbb{N}$ ausgezeichnet ist und auf der eine Funktion $S : \mathbb{N} \to \mathbb{N}$ definiert ist, so daß gilt

(S1) S ist injektiv.

(S2) $1 \notin S(\mathbb{N})$.

(S3) Ist $M \subseteq \mathbb{N}$, $1 \in M$ und $S(M) \subseteq M$, so ist $M = \mathbb{N}$.

(S1)–(S3) sind auch bekannt als die *Peano*[1] *Axiome* für $\mathbb{N}$. //

Man beachte, dass wir hier eigentlich gar nicht gesagt was „natürliche Zahlen“ nun wirklich sind, sondern vielmehr festgelegt haben welche Eigenschaften etwas haben muss, damit es den Namen „natürliche Zahlen“ verdient.

Bevor man sich mit einem durch eine solche, axiomatische, Definition gegebenen Objekt zu beschäftigen beginnt, stellt man sich natürlich ein paar Fragen: Existiert so ein Objekt überhaupt? Wie viele solche Objekte gibt es? Modelliert diese Definition tatsächlich was wir modellieren wollen?

Die erste Frage werden wir nicht behandeln, das würde hier zu weit führen. Wir wollen uns damit begnügen, wegen der Tatsache das der Akt des Zählens in unserem Leben ständig auftritt, an die Existenz von „natürlichen Zahlen“ zu glauben. Bezüglich der zweiten Frage werden wir in Korollar 2.0.21 sehen, dass das Objekt $\mathbb{N}$ durch die Axiome (S1)–(S3) im wesentlichen eindeutig bestimmt ist.

[1] Guiseppe Peano. 27.8.1858 Spinetta bei Cueno - 20.4.1939 Turin

Die dritte Frage wollen gleich diskutieren: Die Funktion S entspricht gerade der Nachfolgerabbildung $n \mapsto \hat{n}$. Die Axiome (S1) und (S2) besagen also das zwei Zahlen gleich sein müssen wenn sie den gleichen Nachfolger haben, bzw. dass die Zahl 1 nicht der Nachfolger irgendeiner Zahl ist.

Das dritte Axiom ist genau das Prinzip der vollständigen Induktion. (S3) besagt, in Worten formuliert: Haben wir irgendeine Teilmenge M der natürlichen Zahlen, die die erste natürliche Zahl 1 enthält und mit jeder Zahl welche sie enthält auch deren Nachfolger, so muß diese Teilmenge schon alle natürlichen Zahlen enthalten.

Haben wir eine Aussage $A(n)$, $n \in \mathbb{N}$, gegeben, so nehmen wir für die in (S3) auftretende Teilmenge M die Menge aller jener natürlichen Zahlen für die $A(n)$ wahr ist. Dann besagt (S3) also gerade: Ist $A(1)$ wahr, und gilt stets, dass aus der Gültigkeit von $A(n)$ auch die Gültigkeit von $A(n+1)$ folgt, dann gilt $A(n)$ für alle n. Wir sehen das (S3) das Prinzip der vollständigen Induktion impliziert. Ist umgekehrt eine Teilmenge M gegeben, und wendet man das Prinzip der vollständigen Induktion an auf die Aussage

$$A(n) := \text{„}n \text{ gehört zu } M\text{“},$$

so erhält man (S3). Also impliziert auch umgekehrt das Prinzip der vollständigen Induktion (S3).

Man erkennt nun auch die herausragende Bedeutung des Prinzips der vollständigen Induktion: Es ist das einzige Beweismittel welches wir von Anfang an für natürliche Zahlen zur Verfügung haben.

Nun können wir daran gehen aus den Axiomen (S1)–(S3) die Theorie der natürlichen Zahlen aufzubauen, z.B. die Operationen + und $\cdot$ und alle Rechenregeln ausschliesslich mit Hilfe von (S1)–(S3) zu definieren und zu beweisen.

2.0.17 Satz (Rekursionssatz)**.** *Sei A eine Menge, $a \in A$, $g : A \to A$. Dann existiert genau eine Abbildung $\phi : \mathbb{N} \to A$ mit $\phi(1) = a$ und $\phi \circ S = g \circ \phi$.*

Beweis. Betrachte alle Teilmengen $H \subseteq \mathbb{N} \times A$ mit den Eigenschaften

(i) $(1, a) \in H$

(ii) Ist $(n, b) \in H$, so gilt auch $(S(n), g(b)) \in H$.

Solche Teilmengen existieren, z.B. hat $\mathbb{N} \times A$ die Eigenschaften (i) und (ii). Sei ϕ der Durchschnitt aller solchen Teilmengen. Klarerweise hat ϕ auch die Eigenschaften (i) und (ii), ist also die kleinste Teilmenge von $\mathbb{N} \times A$ mit diesen Eigenschaften.

Wir behaupten dass ϕ eine Funktion ist, d.h. dass gilt: Zu jedem $n \in \mathbb{N}$ existiert genau ein $b \in A$ sodass $(n, b) \in \phi$. Um dieses einzusehen verwenden wir Induktion nach n.

Induktionsanfang: Es ist $(1, a) \in \phi$. Wäre noch $(1, c) \in \phi$ mit $c \neq a$, so betrachte $D := \phi \setminus \{(1, c)\}$. Wegen $c \neq a$ ist $(1, a) \in D$, also hat D die Eigenschaft (i). Ist $(n, b) \in D$, so ist auch $(n, b) \in \phi$, und daher auch $(S(n), g(b)) \in \phi$. Wegen (S2) ist $S(n) \neq 1$, also sicher $(S(n), g(b)) \neq (1, c)$. Es folgt $(S(n), g(b)) \in \phi \setminus \{(1, c)\} = D$, und wir sehen, dass D auch die Eigenschaft (ii) hat.

Ein Widerspruch dazu, daß ϕ kleinstmöglich ist.

Induktionsschritt: Sei vorausgesetzt, dass es genau ein $b \in A$ mit $(n, b) \in \phi$ gibt. Wir müssen zeigen, dass es auch genau ein $\tilde{b} \in A$ gibt mit $(S(n), \tilde{b}) \in \phi$. Setze

$\tilde{b} := g(b)$, dann ist, wegen (ii), $(S(n), \tilde{b}) \in \phi$. Wäre noch $(S(n), c) \in \phi$ mit $c \neq \tilde{b}$, so betrachte wieder $D := \phi \setminus \{(S(n), c)\}$. Wegen (S2) ist $S(n) \neq 1$, also sicher $(S(n), c) \neq (1, a)$. Daher ist $(1, a) \in \phi \setminus \{(S(n), c)\} = D$. Ist ein Element $(n', b') \in D$, so folgt jedenfalls $(S(n'), g(b')) \in \phi$. Ist $n' \neq n$, so ist wegen (S1) auch $S(n') \neq S(n)$, und wir folgern $(S(n'), g(b')) \in D$. Ist $n' = n$, so muß nach der Induktionsvoraussetzung $b' = b$ sein, und daher ist $g(b') = g(b) = \tilde{b}$. Wegen $c \neq \tilde{b}$ folgt auch in diesem Fall $(S(n'), g(b')) \in D$. Wieder haben wir einen Widerspruch dazu erhalten, dass ϕ die kleinste Teilmenge mit den Eigenschaften (i) und (ii) ist.

Es ist also ϕ eine Funktion $\phi : \mathbb{N} \to A$. Die Eigenschaft (i) bedeutet $\phi(1) = a$. Wegen (ii) ist stets $(S(n), g(\phi(n)) \in \phi$, also $\phi(S(n)) = g(\phi(n))$.

Die Eindeutigkeit von ϕ folgt einfach mit Induktion. Dazu sei $\tilde{\phi}$ eine weitere Abbildung von $\mathbb{N}$ nach A mit der Eigenschaft $\tilde{\phi} \circ S = g \circ \tilde{\phi}$.
Induktionsanfang: $\phi(1) = a = \tilde{\phi}(1)$.
Induktionsschritt: Nach Induktionsvoraussetzung gilt $\phi(n) = \tilde{\phi}(n)$ also folgt

$$\tilde{\phi}(S(n)) = g(\tilde{\phi}(n)) = g(\phi(n)) = \phi(S(n)).$$

❑

2.0.18 Bemerkung. Satz 2.0.17 rechtfertigt rekursive Definitionen (wie zum Beispiel in den Übungsaufgaben schon vorgekommen). Eine Funktion $\varphi : \mathbb{N} \to \mathbb{N}$ ist nämlich durch die Vorgabe von $\varphi(1)$ und eine Vorschrift die $\varphi(S(n))$ durch $\varphi(n)$ ausdrückt eindeutig festgelegt (Eindeutigkeitsaussage von Satz 2.0.17). Weiters existiert zu jeder beliebigen Vorgabe dieser Daten auch eine Funktion mit den geforderten Eigenschaften (Existenzaussage von Satz 2.0.17). //

2.0.19 Bemerkung. Wir haben in diesem Beweis eine oft gebräuchliche Methode verwendet, nämlich das *Prinzip des indirekten Beweises*. Um eine Implikation $A \Rightarrow B$ zu zeigen, bedient man sich der allgemeingültigen Aussageform aus Proposition 1.0.12, (ii), das ist

$$\big(((A \wedge \neg B) \Rightarrow C) \wedge \neg C\big) \Rightarrow (A \Rightarrow B) \tag{B.0.1}$$

Betrachten wir den Induktionsanfang im Beweis des Rekursionssatzes. Dieser hat so funktioniert: „Wäre $(1, c) \in \phi$ mit $c \neq a$, so folgt ... dass es eine kleinere Menge als ϕ gibt mit (i) und (ii). Widerspruch!“. Man betrachtet hier die folgenden Aussagen:

A: Voraussetzungen des Satzes
B: Ist $(1, c) \in \phi$, so ist $c = a$
C: Es gibt eine kleinere Menge als ϕ mit (i) und (ii)

Dann ist

$\neg B$: Es gibt $c \neq a$ mit $(1, c) \in \phi$
$\neg C$: ϕ ist die kleinste Menge mit (i) und (ii)

Wie im Anschluss an die Definition von ϕ festgestellt wurde, ist die Aussage $\neg C$ wahr. In der Argumentation im Induktionsanfang haben wir gezeigt, dass $(A \wedge \neg B) \Rightarrow C)$ wahr ist. Also hat die Aussage auf der linken Seite von (B.0.1) den Wahrheitswert „wahr“. Wegen des modus ponens und der Wahrheit von (B.0.1), muß auch $(A \Rightarrow B)$ den Wahrheitswert „wahr“ haben. //

2.0.20 Bemerkung. Indirekte Beweise sind manchmal unbeliebt. Sie sind auch oft vom logischen Standpunkt komplizierter als notwendig, aber doch irgendwie anschaulich und praktisch. Den oben analysierten Induktionsanfang könnte man auch wie folgt formulieren: Sei $(1, c) \in \phi$. Betrachte $D := \phi \setminus \{(1, c)\}$. Ist $(n, b) \in D$, so ist auch $(n, b) \in \phi$, und daher auch $(S(n), g(b)) \in \phi$. Wegen (S2) ist $S(n) \neq 1$, also sicher $(S(n), g(b)) \neq (1, c)$. Es folgt $(S(n), g(b)) \in D$, und wir sehen dass D die Eigenschaft (ii) hat. Nun gilt $D \subsetneq \phi$, also kann D nicht beide, (i) und (ii), erfüllen. Also kann D nicht (i) erfüllen, d.h. $(1, a) \notin D$. Nun ist $(1, a) \in \phi$, und $\phi = D \cup \{(1, c)\}$, also folgt $(1, a) = (1, c)$, insbesondere $c = a$.

Zur Analyse dieses Beweises, betrachte die folgenden Aussagen: A und B wie oben,

E_1: $D \subseteq \mathbb{N} \times A$ erfüllt (i)
E_2: $D \subseteq \mathbb{N} \times A$ erfüllt (ii)
F: $D \supseteq \phi$

Es gilt dann $E_1 \wedge E_2 \Rightarrow F$. Nach dem Kontrapositionssatz und den de Morganschen Regeln also auch $\neg F \Rightarrow (\neg E_1 \vee \neg E_2)$. Nach Definition von D ist $\neg F$ wahr. Also muß auch $\neg E_1 \vee \neg E_2$ wahr sein. Nun haben wir gezeigt, dass E_2 wahr ist, also $\neg E_2$ falsch. Damit muss $\neg E_1$ wahr sein (denn die Aussageform $(X \vee Y) \wedge \neg Y \Rightarrow X$ ist allgemeingültig). Wir schliessen dass $(1, a) \notin D$. Nun gilt $(1, a) \in \phi = D \cup \{(1, c)\}$, d.h. $(1, a) \in D \vee (1, a) \in \{(1, c)\}$ ist wahr. Wieder schliessen wir dass $(1, a) \in \{(1, c)\}$ wahr ist.

Wir haben hier auch das *Prinzip des Beweises durch Kontraposition* verwendet: Um eine Implikation $A \Rightarrow B$ zu zeigen, zeigt man $\neg B \Rightarrow \neg A$. Der Unterschied zum indirekten Beweis liegt darin, dass man beim Beweis durch Kontraposition als Voraussetzung nur $\neg B$ hat, wogegen man beim indirekten Beweis $\neg B$ und A beide als Voraussetzungen verwenden kann. //

2.0.21 Korollar (Eindeutigkeitssatz)**.** *Seien $\mathbb{N}$ und $\mathbb{N}'$ Mengen mit ausgezeichneten Elementen $1 \in \mathbb{N}$ und $1' \in \mathbb{N}'$ und Abbildungen $S : \mathbb{N} \to \mathbb{N}$, $S' : \mathbb{N}' \to \mathbb{N}'$, so daß für beide die Axiome (S1), (S2) und (S3) gelten. Dann gibt es eine bijektive Abbildung $\varphi : \mathbb{N} \to \mathbb{N}'$ mit $\varphi(1) = 1'$ und $S' \circ \varphi = \varphi \circ S$.*

Beweis. Wendet man den Rekursionssatz an auf $A = \mathbb{N}'$, $a = 1'$, und $g = S'$, so folgt daß eine Abbildung $\varphi : \mathbb{N} \to \mathbb{N}'$ existiert mit $\varphi(1) = 1'$ und $S' \circ \varphi = \varphi \circ S$. Durch Vertauschung der Rollen von $\mathbb{N}$ und $\mathbb{N}'$ erhält man eine Abbildung $\psi : \mathbb{N}' \to \mathbb{N}$ mit $\psi(1') = 1$ und $S \circ \psi = \psi \circ S'$.

Betrachte die Abbildung $\Phi = \psi \circ \varphi : \mathbb{N} \to \mathbb{N}$. Es gilt $\Phi(1) = 1$ und

$$S \circ \Phi = (S \circ \psi) \circ \varphi = \psi \circ (S' \circ \varphi) = (\psi \circ \varphi) \circ S = \Phi \circ S$$

Die identische Abbildung $\mathrm{id}_{\mathbb{N}}$ hat die selben Eigenschaften, also folgt nach der Eindeutigkeitsaussage des Rekursionssatzes $\Phi = \mathrm{id}_{\mathbb{N}}$. Analog zeigt man $\varphi \circ \psi = \mathrm{id}_{\mathbb{N}'}$, also ist φ bijektiv und es gilt $\varphi^{-1} = \psi$. ❑

Wir kommen nun zur Diskussion der algebraischen Operation der Addition und Multiplikation, sowie der Ordnungsrelation auf $\mathbb{N}$. Ziel ist es alle jene Begriffe und Eigenschaften die wir im Prolog, motiviert aus unserer Anschauung, als plausibel erkannt haben, zu definieren und beweisen. D.h. also, sie alleine aus den Axiomen (S1)–(S3) mittels logischer Schlüsse herzuleiten. Dabei dürfen wir den Rekursionssatz und den Eindeutigkeitssatz zu Hilfe nehmen, denn dieser wurde ja bereits aus (S1)–(S3) hergeleitet.

2.0.22 Definition. Wir definieren für jedes $m \in \mathbb{N}$ Abbildungen $+_m : \mathbb{N} \to \mathbb{N}$ und $\cdot_m : \mathbb{N} \to \mathbb{N}$ rekursiv:

$$+_m(1) := S(m) \text{ und } +_m(S(n)) = S(+_m(n)),$$

$$\cdot_m(1) := m \text{ und } \cdot_m(S(n)) = +_m(\cdot_m(n)).$$

Weiters definieren wir eine Relation $\leq$ auf $\mathbb{N}$ durch

$$n \leq m :\iff (n = m) \text{ oder } (\exists t \in \mathbb{N} : +_t(n) = m).$$

//

Sind $m, n \in \mathbb{N}$, so schreibt man auch

$$+_m(n) =: m + n, \ \cdot_m(n) =: m \cdot n,$$

und spricht von der *Addition* bzw. *Multiplikation*.

2.0.23 Satz. *Die Addition im Bereich $\mathbb{N}$ der natürlichen Zahlen erfüllt die Gesetze*

- *Für alle $a, b, c \in \mathbb{N}$ gilt $(a + b) + c = a + (b + c)$ (*Assoziativität*)*
- *Für alle $a, b \in \mathbb{N}$ gilt $a + b = b + a$ (*Kommutativität*)*

sowie die Kürzungsregel

- *Sind $n, m, k \in \mathbb{N}$ und gilt $m + k = n + k$, so folgt $m = n$.*

Die Multiplikation ist ebenfalls assoziativ, kommutativ und erfüllt die Kürzungsregel. Zusätzlich gilt noch

- *Für jedes $a \in \mathbb{N}$ ist $a \cdot 1 = 1 \cdot a = a$. (*Existenz des neutralen Elementes*)*

Die Addition hängt mit der Multiplikation zusammen über das Distributivitätsgesetz

- *Für $a, b, c \in \mathbb{N}$ gilt stets $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$.*

Die Relation $\leq$ ist eine Wohlordnung und ist mit den Operationen $+$ und $\cdot$ verträglich:

- *Ist $a, b, c \in \mathbb{N}$ und gilt $a \leq b$, so folgt $a + c \leq b + c$*
- *Ist $a, b, c \in \mathbb{N}$ und gilt $a \leq b$, so folgt $a \cdot c \leq b \cdot c$*

Es gilt weiters

- *Ist umgekehrt $n, m, l \in \mathbb{N}$ mit $n + l \leq m + l$ oder $n \cdot l \leq m \cdot l$, so folgt $n \leq m$.*

Beweis. Wir zeigen exemplarisch einige dieser Eigenschaften. Die anderen folgert man in ganz analoger Weise.

Assoziativität von $+$: Seien $k, m \in \mathbb{N}$ fest gewählt, wir führen Induktion nach n durch.
Induktionsanfang: $(k + m) + 1 = +_{k+m}(1) = +_{+_k(m)}(1) = S(+_k(m)) =$

$+_k(S(m)) = +_k(+_m(1)) = k + (m+1)$
Induktionsschritt: Nach Induktionsvoraussetzung gilt $(k+m)+n = k+(m+n)$, d.h. $+_{k+m}(n) = +_k(+_m(n))$. Es folgt

$$(k+m) + S(n) = +_{k+m}(S(n)) = S(+_{k+m}(n)) \overset{IV}{=} S(+_k(+_m(n))) =$$

$$= +_k(S(+_m(n))) = +_k(+_m(S(n))) = k + (m + S(n)).$$

Kommutativität von +: Wir zeigen $\forall m \in \mathbb{N} \forall n \in \mathbb{N} : m + n = n + m$ mittels Induktion nach m.
Induktionsanfang ($m = 1$): Wir müssen zeigen dass

$$\forall n \in \mathbb{N} : 1 + n = n + 1 \tag{B.0.2}$$

mittels Induktion nach n. Der Fall $n = 1$ ist klar, denn $1 + 1 = 1 + 1$. Für den Induktionsschritt $n \to S(n)$ gehen wir aus von der Induktionsvoraussetzung $1 + n = n + 1$, d.h. $+_1(n) = +_n(1)$. Daraus folgt

$$S(n) + 1 = +_{S(n)}(1) = S(S(n)) = S(+_n(1)) \overset{IV}{=} S(+_1(n)) =$$

$$= +_1(S(n)) = 1 + S(n).$$

Induktionsschritt ($m \to S(m)$): Wir zeigen, daß die Gültigkeit der Aussage

$$\forall n \in \mathbb{N} : m + n = n + m \tag{B.0.3}$$

die Gültigkeit von

$$\forall n \in \mathbb{N} : S(m) + n = n + S(m) \tag{B.0.4}$$

impliziert. Um (B.0.4) zu beweisen, führen wir Induktion nach n durch. Betrachte also zuerst den Fall $n = 1$. Nach der bereits bewiesenen Aussage (B.0.2), gilt $S(m) + 1 = 1 + S(m)$. Der Induktionsschritt $n \to S(n)$ hat nun als Induktionsvoraussetzung $S(m) + n = n + S(m)$ und wir erhalten

$$S(m) + S(n) = +_{S(m)}(S(n)) = S(+_{S(m)}(n)) \overset{IV(n)}{=} S(+_n(S(m))) =$$
$$= S(S(+_n(m))) \overset{IV(m)}{=} S(S(+_m(n))) =$$
$$= S(+_m(S(n))) \overset{IV(m)}{=} S(+_{S(n)}(m)) = +_{S(n)}(S(m)) = S(n) + S(m).$$

Kürzungsregel für +: Wir zeigen

$$\forall k \in \mathbb{N} \forall m, n \in \mathbb{N} : \big(m + k = n + k \Rightarrow m = n\big)$$

Dazu verwenden wir Induktion nach k.
Induktionsanfang: Sei $m + 1 = n + 1$, d.h. $S(m) = S(n)$. Da S injektiv ist, folgt $m = n$.
Induktionsschritt: Sei $m + (k + 1) = n + (k + 1)$. Dann ist auch $(m + k) + 1 = (n + k) + 1$, und nach dem Induktionsanfang folgt $m + k = n + k$. Nun impliziert die Induktionsvoraussetzung $m = n$.

Antisymmetrie von ≤: Angenommen $n \leq m$ und $m \leq n$. Gilt in einer der beiden

Relationen das Gleichheitszeichen, so sind wir fertig. Sei angenommen, dass für gewisse $t_1, t_2 \in \mathbb{N}$ gilt $n + t_1 = m$ und $m + t_2 = n$. Dann folgt

$$n + (t_1 + t_2) = (n + t_1) + t_2 = m + t_2 = n\,,$$

also auch $(t_1 + t_2 + 1) + n = 1 + n$. Nach der Kürzungsregel folgt $t_1 + t_2 + 1 = 1$, d.h. $S(t_1 + t_2) = 1$. Ein Widerspruch zu (S2).

Verträglichkeit von $\leq$ mit $+$: Sei $n \leq m$ und $k \in \mathbb{N}$. Gilt in $n \leq m$ das Gleichheitszeichen, so folgt klarerweise auch $n + k = m + k$ also insbesondere $n + k \leq m + k$. Sei also $t \in \mathbb{N}$ mit $n + t = m$. Dann ist

$$m + k = (n + t) + k = n + (t + k) = n + (k + t) = (n + k) + t.$$

Also folgt ebenfalls $n + k \leq m + k$. ❑

Anhang C

Das Lemma von Zorn

Das Lemma von Zorn ist ein fundamentales Hilfsmittel aus der Mengenlehre. Es ist äquivalent zum Auswahlaxiom und zum Wohlordnungssatz und war von daher vor allem in der ersten Hälfte des 20. Jahrhunderts umstritten. Mittlerweile sind die Mathematiker entspannter, auch wenn ein möglicher Verzicht auf das Auswahlaxiom immer noch in manchen Situationen explizit hervorgehoben wird.

3.0.24 Definition. Sei $(M, \leq)$ eine halbgeordnete Menge. Wenn für jede total geordnete Teilmenge von M eine obere Schranke existiert, dann heißt M *induktiv geordnet*. Wenn sogar jeweils eine kleinste obere Schranke existiert, dann heißt M strikt induktiv geordnet. //

Folgendes Lemma ist der zentrale Hilfsatz zum Beweis des Lemma von Zorn.

3.0.25 Lemma. *Es sei $(M, \leq)$ eine nichtleere halbgeordnete Menge mit einem kleinsten Element o, sodass M strikt induktiv ist. Schließlich sei $F : M \to M$ eine Abbildung mit der Eigenschaft (Monotonie)*

$$m \leq F(m),\ m \in M.$$

Dann gibt es ein $m \in M$ mit $F(m) = m$.

Beweis. Wie nennen eine Teilmenge S von M zulässig, wenn die folgenden drei Bedingungen gelten: $o \in S$, $F(S) \subseteq S$, und für jede total geordnete Teilmenge $T \subseteq S$ liegt auch die kleinste obere Schranke $\sup T$ in S. Zum Beispiel ist M selbst zulässig.

Nun sei S_0 der Durchschnitt aller zulässigen Teilmengen von M. Da in jeder zulässigen Teilmenge auch o liegt, enthält der Durchschnitt zumindest das Element o . Außerdem gelten auch die beiden anderen Bedingungen für Zulässigkeit. Also ist S_0 selbst zulässig und damit die kleinste aller zulässigen Teilmengen von M.

Wenn wir nun zeigen können, dass S_0 total geordnet ist, dann folgt daraus für die kleinste obere Schranke $\sup S_0$ einerseits, dass $\sup S_0$ das größte Element von S_0 ist. Andererseits gilt aber wegen der Zulässigkeit $F(\sup S_0) \leq \sup S_0$. Wir bekommen insgesamt

$$\sup S_0 \leq F(\sup S_0) \leq \sup S_0,$$

und damit die gewünschte Gleichheit. Noch zu zeigen ist also die Behauptung, dass S_0 total geordnet ist.

Für den Beweis nennen wir $e \in S_0$ ein extremales Element, wenn für alle $s \in S_0$ mit $s \leq e, s \neq e$ $(s < e)$ gilt, dass $F(s) \leq e$. Zum Beispiel ist o extremal. Für ein extremales e setzen wir

$$S_e := \{s \in S_0 : s \leq e \vee F(e) \leq s\}.$$

Dann ist für jedes extremale e die Menge S_e zulässig:

- o liegt in S_e.
- Für jedes Element $s \in S_e$ folgt aus $s < e$ schon $F(s) \leq e$, aus $s = e$ folgt $F(s) = F(e)$, und aus $s \not\leq e$ folgt $F(e) \leq s \leq F(s)$. Also gilt insgesamt $F(S_e) \subseteq S_e$.
- Es sei T eine total geordnete Teilmenge von S_e. Wenn dann für alle $t \leq \sup T$ die Ungleichung $t \leq e$ gilt, dann gilt auch $\sup T \leq e$. Wenn es aber mindestens ein t gibt, sodass $t \not\leq e$ gilt, dann ist $F(e) \leq t \leq F(t) \leq \sup T$. Wir sehen also in beiden Fällen, dass $\sup T \in S_e$.

Da aber S_0 die kleinste zulässige Teilmenge von M ist, muss also für alle extremalen e gelten:

$$S_e = S_0.$$

Nun müssen wir noch zeigen, dass jedes $e \in S_0$ extremal ist. Dann folgt nämlich für $s \in S_0$, dass $s \in S_e$ bzw.

$$s \leq e \vee e \leq F(e) \leq s,$$

also die Tatsache, dass S_0 total geordnet ist.

Um zu beweisen, dass jedes $e \in S_0$ extremal ist, betrachten wir

$$E := \{e \in S_0 : e \text{ ist extremal}\}.$$

Wir weisen nach, dass E zulässig und damit gleich S_0 ist.

- $o \in E$ ist klar.
- Wir müssen zeigen, dass mit e auch $F(e)$ in E liegt. Ist $s \in S_0 = S_e$ und $s < F(e)$, so müssen wir $F(s) \leq F(e)$ folgern. Da $s \in S_e$, gilt $s \leq e$ oder $F(e) \leq s$, wobei wir letzteres wegen unserer Voraussetzung ausschließen können. Aus $s \leq e$ folgt aber wegen $e \in E$, dass $F(s) \leq F(e)$.
- Nun sei noch $T \subseteq E$ total geordnet. Zu zeigen ist, dass $\sup T \in E$. Sei dazu $s \in S_0, s < \sup T$. Wenn für jedes $t \in T$ die Relation $F(t) \leq s$ gelten würde, dann wäre wegen $t \leq F(t)$ auch $\sup T \leq s$. Das ist ein Widerspruch. Also gibt es ein extremales $e \in T$ mit $F(e) \not\leq s$, und da $S_0 = S_e$ gilt, folgt daraus zwangsweise $s \leq e$. Ist $s \neq e$, so folgt wegen $e \in E$, dass $F(s) \leq e \leq \sup T$. Da $\sup T \in S_0 = S_e$, $s < \sup T$ folgt aus $s = e$, dass $F(s) = F(e) \leq \sup T$. Damit folgt insgesamt, dass $\sup T$ extremal ist.

❑

Nun können wir das Lemma von Zorn aus dem Auswahlaxiom herleiten.

3.0.26 Satz. *Es sei $(M, \leq)$ eine nichtleere induktiv geordnete Menge. Dann besitzt M ein maximales Element.*

Beweis. Wir behandeln zuerst den Fall einer strikt induktiv geordneten Menge.

Sei $x \in M$ fest. Ist m maximales Element von $\{y \in M : x \leq y\}$, so ist m auch maximales Element von M. Also dürfen wir uns auf den Fall beschränken, dass M ein kleinstes Element enthält. Wir nehmen an, es gebe kein maximales Element. Dann finden wir für jedes $m \in M$ ein größeres Element $F(m)$ und definieren damit eine Funktion $F : M \to M$, für die gilt:

$$\forall m \in M : m < F(m).$$

Man beachte, dass man für die Existenz einer solchen Funktion F das Auswahlaxiom verwendet. In der Tat ist F eine Auswahlfunktion der Familie $(A_m)_{m \in M}$, wobei $A_m = \{x \in M : m \leq x,\ m \neq x\}$.

Da M strikt induktiv geordnet ist, folgt aus Lemma 3.0.25, dass $F(m) = m$ für ein $m \in M$, und und wir haben einen Widerspruch gefunden.

Nun sei M induktiv geordnet, und sei $\mathcal{H}$ die Menge aller total geordneten Teilmengen von M. Dann ist $\mathcal{H}$ bezüglich der Inklusion eine Halbordnung, und zwar eine strikt induktive, denn ist $\mathcal{T} \subseteq \mathcal{H}$ totalgeordnet (bzgl. $\subseteq$), so auch $\cup\mathcal{T}$ (bzgl. $\leq$), und diese Teilmenge von M ist auch die kleinste obere Schranke von $\mathcal{T}$ (bzgl. $\subseteq$).

Also besitzt $\mathcal{H}$ nach dem ersten Beweisteil ein maximales Element T. Es sei O eine obere Schranke von T. Dann muss O zu T gehören, da $T \cup \{O\}$ eine total geordnete Menge ist, die T umfasst, aber T ist schon maximal.

Dieses Element O ist dann ein maximales Element von M, denn für jedes $m \in M$ folgt aus $O \leq m$, dass m eine obere Schranke von T ist, und somit ebenfalls zu T gehören muss. Insbesondere folgt $m \leq O$ und damit $m = O$. ❑

Literaturverzeichnis

[EL] K.Endl,W.Luh: *Analysis I-III,* Aula Verlag, Wiesbaden 1986.

[F] G.M.Fichtenholz: *Differential- und Integralrechnung I-III,* Deutscher Verlag der Wissenschaften, Berlin 1964.

[GO] B.Gelbaum,J.Olmsted: *Counterexamples in Analysis,* Holden-Day Inc., SanFrancisco 1964.

[GL] H.Grauert, I.Lieb: *Differential- und Integralrechnung I-III,* Springer Verlag, Heidelberg 1967.

[H] H.Heuser: *Lehrbuch der Analysis 1,2,* Teubner Verlag, Stuttgart 1989.

[L] S.Lang: *A first course in calculus,* Springer Verlag, Heidelberg 1986.

[R] W.Rudin: *Principles of Mathematical Analysis,* McGraw-Hill, New York 1953, third edition 1976.

Diese Liste könnte beliebig verlängert werden. Zu den Grundlagen der Analysis gibt es sehr viele Bücher, und viele von diesen sind auch (inhaltlich und didaktisch) gut geschrieben. Letzlich ist es jedem Leser selbst überlassen, ein Buch kritisch zu beurteilen, und für gut/schlecht bzw. sympathisch/unangenehm zu befinden. Mein persönliches Ranking in obiger Liste ist:

Platz 1: [R]
Platz 2: [F],[H] (haben komplett unterschiedlichen Präsentationsstil)
Platz 3: [L]

Index