Skript zur Vorlesung

Elementarmathematik I

Wintersemester 2015/2016

Prof. Dr. Annette Werner

Inhaltsverzeichnis

1 Mengen und Abbildungen

Wir verwenden einen naiven Mengenbegriff. Eine Menge ist für uns eine Zusammenfassung bestimmter, wohlunterschiedener Objekte.

Wenn man das im Rahmen der Mengenlehre formal erfasst, muss man ein bisschen aufpassen, wie das Russell'sche Paradox zeigt. Für die Zwecke dieser Vorlesung reicht jedoch ein naiver Mengenbegriff aus.

Wir interessieren uns vor allem für Zahlbereiche.

Beispiel: $\mathbb{N} = \{1, 2, 3, 4, \ldots\}$ natürliche Zahlen
$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ ganze Zahlen
$\mathbb{Q} = \{\frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0\}$ rationale Zahlen
$\mathbb{R}$ reelle Zahlen

Die geschweiften Klammern { } beschreiben hier den Prozess des Zusammenfassens von Objekten zu einer Menge.

Liegt x in der Menge M, so schreiben wir $x \in M$ und sagen „x ist ein Element von M". Liegt x nicht in M, so schreiben wir $x \notin M$.

Es gibt eine Menge, die kein Element enthält und als leere Menge $\emptyset$ bezeichnet wird.

Ist eine Menge M in einer Menge N enthalten (gilt also für alle $x \in M$ auch $x \in N$), so schreiben wir $M \subset N$ und nennen M eine Teilmenge von N. Zum Beispiel ist $\mathbb{N} \subset \mathbb{Z}$ und $\mathbb{Z} \subset \mathbb{Q}$. Haben zwei Mengen dieselben Elemente, so sind sie gleich. Also gilt $M = N$ genau dann, wenn $M \subset N$ und $N \subset M$ gilt. Man kann Teilmengen konstruieren, indem man alle Elemente in einer Menge zusammenfasst, die eine bestimmte Eigenschaft erfüllen.

Beispiel: $\{a \in \mathbb{Z} : a = 2b \text{ für ein } b \in \mathbb{Z}\}$ die Menge der geraden Zahlen
$\{a \in \mathbb{Z} : |a| \leqq 3\} = \{-3, -2, -1, 0, 1, 2, 3\}$.

Sind M und N zwei Mengen, so definieren wir die Vereinigung

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

und den Schnitt

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

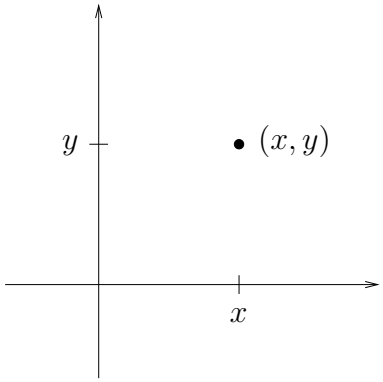
Es seien M und N zwei nicht leere Mengen. Für $x \in M$ und $y \in N$ schreiben wir (x, y) für das geordnete Paar, das x an erster und y an zweiter Stelle enthält. Es gilt $(x, y) = (x', y')$ genau dann, wenn $x = x'$ und $y = y'$ gilt.

Dann ist das kartesische Produkt

$$M \times N = \{(x, y) : x \in M, y \in N\}$$

wieder eine Menge.

Wir kennen dies vom Koordinatensystem für $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$:



Dies kann man auf mehr als zwei Faktoren verallgemeinern. Sind $M_1, \ldots, M_n$ Mengen, so ist

$$M_1 \times \ldots \times M_n = \{(x_1, \ldots, x_n) : x_1 \in M_1, \ldots, x_n \in M_n\}$$

das kartesische Produkt, das aus den geordneten $n-$Tupeln besteht, bei denen der i-te Platz jeweils durch ein Element in der Menge M_i besetzt ist.

Definition 1.1 *Seien M und N Mengen. Eine Abbildung*

$$f : M \to N$$

ist eine Vorschrift, die jedem $x \in M$ ein eindeutig bestimmtes Element $f(x) \in N$ zuordnet.

Für $x \in M$ heißt $f(x)$ das Bild von x unter f. M heißt Definitionsbereich und N heißt Wertemenge der Funktion f.

Beispiel:

i) $f : \mathbb{N} \to \mathbb{N}$ definiert durch $f(x) = x + 1$

ii) $f : \mathbb{Z} \to \mathbb{N} \cup \{0\}$ definiert durch $f(x) = |x| = \begin{cases} x, & \text{falls} \quad x \geqq 0 \\ -x, & \text{falls} \quad x < 0 \end{cases}$

Ist $f : M \to N$ eine Abbildung und $A \subset M$, so definieren wir das Bild von A unter f als die Teilmenge

$$f(A) = \{f(x) : x \in A\} \subset N$$

von N.

Wichtige Eigenschaften von Abbildungen sind die folgenden:

Definition 1.2 *Sei $f : M \to N$ eine Abbildung.*

i) f heißt surjektiv, falls $f(M) = N$ gilt. Das Bild von M unter f ist also N. Mit anderen Worten: Für jedes $y \in N$ existiert ein $x \in M$ mit $f(x) = y$.

ii) f heißt injektiv, wenn aus $x, y \in M$ mit $x \neq y$ folgt $f(x) \neq f(y)$. Mit anderen Worten: Verschiedene Elemente in M haben verschiedene Bilder unter f. Oder auch: Sind zwei Bilder $f(x)$ und $f(x')$ gleich, dann ist $x = x'$.

iii) f heißt bijektiv, wenn f injektiv und surjektiv ist.

Beispiel:

i) $f : \mathbb{N} \to \mathbb{N}, f(x) = x + 1$, ist injektiv, aber nicht surjektiv.

ii) $f : \mathbb{Z} \to \mathbb{Z}, f(x) = x + 1$, ist bijektiv. Für die Surjektivität kommt es also entscheidend auf den angegebenen Wertebereich der Abbildung an.

iii) $f : \mathbb{Z} \to \mathbb{N} \cup \{0\}, f(x) = |x|$, ist surjektiv, aber nicht injektiv.

Hat die Menge M endlich viele Elemente, so nennen wir M eine endliche Menge und schreiben $|M|$ für die Anzahl ihrer Elemente.

Beispiel : $|\{1, 2, 3, 4, 5\}| = 5$
$|\emptyset| = 0.$

Satz 1.3 *Es seien M und N endliche Mengen mit $|M| = |N|$ (das heißt, M und N haben gleich viele Elemente). Dann gilt für eine Abbildung $f : M \to N$:*

i) Ist f injektiv, dann ist f auch surjektiv (und somit bijektiv).

ii) Ist f surjektiv, dann ist f auch injektiv (und somit bijektiv).

Beweis :

i) Ist f injektiv, so folgt $|f(M)| \geqq |M|$, denn zwei verschiedene Elemente aus M werden auf zwei verschiedene Elemente aus N abgebildet. Da $f(M) \subset N$ und somit $|f(M)| \leqq |N|$ gilt, folgt

$$|M| \underset{\text{Vor.}}{=} |N| \geqq |f(M)| \geqq |M|,$$

also steht überall die Gleichheit und es gilt $|N| = |f(M)|$. Daraus folgt $N = f(M)$ (wieso?). Daher ist f surjektiv.

ii) Ist f surjektiv, so gilt $f(M) = N$. Also ist $|f(M)| = |N| \overset{\text{Vor.}}{=} |M|$. Angenommen, x, x' sind zwei verschiedene Elemente aus M. Dann muss $f(x) \neq f(x')$ sein, denn sonst hätte $f(M)$ mindestens ein Element weniger als M. Also ist f injektiv.

□

Achtung: Für unendliche Mengen gilt Satz 1.3 nicht, wie das obige Beispiel $f : \mathbb{N} \to \mathbb{N}, f(x) = x + 1$, zeigt.

Sind $f : M \to N$ und $g : N \to Q$ zwei Abbildungen, so dass der Wertebereich von f mit dem Definitionsbereich von g übereinstimmt, dann können wir die Hintereinanderausführung

$$\begin{aligned} g \circ f : M &\to N \\ x &\mapsto g\big(f(x)\big) \end{aligned}$$

betrachten.

Übungsaufgabe:

i) Ist $g \circ f$ injektiv, so ist f injektiv.

ii) Ist $g \circ f$ surjektiv, so ist g surjektiv.

Beispiel: Für jede Menge M haben wir die identische Abbildung $\mathrm{id}_M : M \to M$, definiert durch $\mathrm{id}_M(x) = x$.

Satz 1.4 *Eine Abbildung $f : M \to N$ ist genau dann bijektiv, wenn es eine Abbildung*

$$g : N \to M$$

gibt, für die gilt

$$g \circ f = id_M \text{ und } f \circ g = id_N.$$

Die Abbildung g ist durch diese Eigenschaften eindeutig bestimmt und wird Umkehrabbildung genannt und mit f^{-1} bezeichnet.

Beweis : „ $\Rightarrow$ “ Angenommen, f ist bijektiv. Dann existiert für jedes $y \in N$ genau ein $x \in M$ mit $f(x) = y$ (wieso ?). Wir setzen $g(y) = x$. Das definiert eine Abbildung $g : N \to M$. Für jedes $y \in N$ gilt $f \circ g(y) = f\big(g(y)\big) = f(x) = y$, also ist $f \circ g = \mathrm{id}_N$. Ist $x \in M$, so sei $y = f(x)$. Dann ist $g(y) = x$, also $g \circ f(x) = x$ und somit $g \circ f = \mathrm{id}_M$.

„ $\Leftarrow$ “ : Angenommen, $g : N \to M$ existiert mit $g \circ f = \mathrm{id}_M$ und $f \circ g = \mathrm{id}_N$. Aus $f(x) = f(x')$ folgt dann

$$x = g\big(f(x)\big) = g\big(f(x')\big) = x'.$$

Daher ist f injektiv.

Für jedes $y \in N$ ist $y = f\big(g(y)\big)$, also liegt y in $f(M)$. Somit ist f auch surjektiv und damit bijektiv.

Die Eindeutigkeit von g sieht man so: Ist $g' : N \to M$ eine weitere Abbildung mit $g' \circ f = \mathrm{id}_M$ und $f \circ g' = \mathrm{id}_N$, so wählen wir für jedes $y \in N$ mit Hilfe der Surjektivität von f ein $x \in M$ mit $f(x) = y$ und erhalten

$$g'(y) = g'\big(f(x)\big) = \mathrm{id}_M(x) = g\big(f(x)\big) = g(y).$$

Also ist $g = g'$. □

2 Die natürlichen Zahlen und das Prinzip der vollständigen Induktion

Die natürlichen Zahlen haben wir im letzten Kapitel einfach naiv als Menge der „Zählzahlen“ $1, 2, 3, \ldots$ eingeführt. Wir wollen diese Menge jetzt axiomatisch beschreiben. Ein Axiom ist ein mathematischer Grundsatz, auf dem man Beweise neuer Aussagen aufbauen kann. Von nichts kommt nichts — mit irgend etwas muss man also anfangen.

Definition 2.1 *(Die Peano-Axiome) Es sei N die Menge mit einem Element 1 und einer Abbildung*

$$\nu : N \to N \quad \textit{(„Nachfolgerfunktion“).}$$

Erfüllen $(N, 1, \nu)$ dann die Axiome

(P 1) es gibt keine Zahl n mit $\nu(n) = 1$ (mit anderen Worten: 1 ist nicht im Bild von ν),

(P 2) *N ist injektiv,*

(P 3) *Jede Teilmenge von N, die 1 enthält und mit jedem n auch den Nachfolger $\nu(n)$ ist bereits die gesamte Menge N,*

so nennen wir N die Menge der natürlichen Zahlen.

Aus den Peano-Axiomen kann man alle Eigenschaften der natürlichen Zahlen nachweisen. So kann man etwa die Addition auf den natürlichen Zahlen wie folgt rekursiv definieren:

1) Für alle $n \in N$ sei $n + 1 := \nu(n)$.

2) Für alle $n, m \in N$ sei $n + \big(\nu(m)\big) = \nu(n + m)$

Dann kann man sich den Spaß machen, aus den Peano-Axiomen die bekannten Rechengesetze für die Addition (etwa die Kommutativität und Assoziativität) herzuleiten. Auch die Multiplikation lässt sich mit den Peano-Axiomen rekursiv definieren.

Das Axiom $(P3)$ heißt auch Axiom der vollständigen Induktion.

Angenommen, wir wollen eine Aussage $A(n)$ für alle natürlichen Zahlen n zeigen. Dann genügt es, zu zeigen:

1) (Induktionsanfang) Die Aussage gilt für $n = 1$. Mit anderen Worten: $A(1)$ ist wahr.

2) (Induktionsschluss) Wenn die Aussage für n gilt, so auch für den Nachfolger $n + 1$. Mit anderen Worten: $A(n) \Rightarrow A(n + 1)$.

Sind 1) und 2) erfüllt, dann erfüllt die Menge

$$\{n \in \mathbb{N} : A(n) \text{ ist wahr}\}$$

nämlich die Bedingung aus dem Axion $(P3)$, also muss sie gleich $\mathbb{N}$ sein. Aber dann gilt die Aussage $A(n)$ für alle n.

Wir demonstrieren dies an einem Beispiel.

Lemma 2.2 *Für alle natürlichen Zahlen n gilt*

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

Beweis : (mit vollständiger Induktion): Hier ist $A(n)$ die Aussage: $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$.

Induktionsanfang: $A(1)$ lautet $1 = \frac{1\cdot(1+1)}{2}$, was trivialerweise richtig ist.

Induktionsschluss: Wir müssen $A(n) \Rightarrow A(n+1)$ zeigen.

Also nehmen wir an, dass $A(n)$ stimmt. Dann gilt $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$.

Wir müssen nun $A(n+1)$ zeigen. Dafür berechnen wir

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

Also stimmt auch $A(n+1)$. □

Ein paar kombinatorische wichtige Anwendungen wollen wir zum Abschluss noch besprechen.

Definition 2.3 *Für jedes $n \in \mathbb{N}$ sei*

$$n! = \prod_{i=1}^{n} i = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n$$

das Produkt aller natürlichen Zahlen von 1 bis n.

Lemma 2.4 *Die Anzahl der bijektiven Abbildungen*

$$\varphi : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$$

ist $n!$.

Eine soche bijektive Abbildung entspricht gerade einer Vertauschung der Reihenfolge der Elemente $(1, 2, 3, \ldots, n)$.

Beweis mit vollständiger Induktion. Es ist $A(n)$ die Aussage:

Die Anzahl der bijektiven Abbildungen

$$\varphi : \{1, \ldots, n\} \to \{1, \ldots, n\} \text{ ist } n!$$

Induktionsanfang: $A(1)$ ist richtig, denn $1 \mapsto 1$ ist die einzige bijektive Abbildung $\{1\} \to \{1\}$.

Induktionsschluss: Wir müssen zeigen $A(n) \Rightarrow A(n+1)$. Also nehmen wir an, $A(n)$ ist richtig. Dann gibt es $n!$ bijektive Abbildungen $\varphi : \{1, \ldots, n\} \to \{1, \ldots, n\}$.

Nun sei $\psi : \{1, 2, \ldots, n+1\} \to \{1, 2, \ldots, n+1\}$ eine bijektive Abbildung. Dann gibt es $(n+1)$ Möglichkeiten für $\varphi(n+1) \in \{1, 2, \ldots, n+1\}$. Wir schränken ψ auf die Teilmenge $\{1, 2, \ldots, n\}$ ein und erhalten eine bijektive Abbildung

$$\varphi_0 : \{1, 2, \ldots, n\} \to \{1, \ldots, n+1\} \backslash \{\varphi(n+1)\}$$

Dabei bedeutet das Zeichen „\“, dass wir das Element $\varphi(n+1)$ aus der Menge $\{1, \ldots, n+1\}$ herausnehmen. Die verbleibende Menge hat n Elemente. Wir können sie also bijektiv auf $\{1, \ldots, n\}$ abbilden. Verknüpfen wir φ_0 mit dieser Bijektion, so erhalten wir eine Bijektion $\varphi : \{1, \ldots, n\} \to \{1, \ldots, n\}$.

Dafür gibt es nach der Induktionsvoraussetzung $A(n)$ gerade $n!$ Möglichkeiten.

Daher gibt es für ψ für jede Wahl von $\varphi(n+1)$ genau $n!$ Möglichkeiten, insgesamt also

$$n!(n+1) = (n+1)!$$

□.

Definition 2.5 *Für natürliche Zahlen k, n mit $k \leqq n$ definieren wir den Binomialkoeffizienten*

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

wobei wir $0! = 1$ setzen. Also ist $\binom{n}{n} = 1$.

Der Binomialkoeffizient spielt eine wichtige Rolle bei der Berechnung von Wahrscheinlichkeiten. So ist $\binom{n}{k}$ die Anzahl aller Möglichkeiten, aus einer Urne mit n nummerierten Kugeln k vorgegebene Zahlen zu ziehen (Lottoprinzip).

Satz 2.6 *Für alle natürlichen Zahlen $k < n$ gilt*

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

Beweis : Das prüft man leicht nach, indem man die Summe auf einen Hauptnenner bringt:

$$\begin{aligned} \tbinom{n-1}{k-1} + \tbinom{n-1}{k} &= \tfrac{(n-1)!}{(k-1)!(n-k)!} + \tfrac{n-1)!}{(n-1-k)!k!} \\ &= \tfrac{(n-1)!k+(n-1)!(n-k)}{k!(n-k)!} \\ &= \tfrac{n!}{k!(n-k)!} = \tbinom{n}{k}. \end{aligned}$$

□

Diese Formel kann man zu einer sukzessiven Berechnung der Werte $\binom{n}{k}$ im sogenannten Pascal'schen Dreieck verwenden:

$$
\begin{array}{ccccccccccc}
 & & & & & 1 & & & & & \\
 & & & & 1 & & 1 & & & & \\
 & & & 1 & & 2 & & 1 & & & \\
 & & 1 & & 3 & & 3 & & 1 & & \\
 & 1 & & 4 & & 6 & & 4 & & 1 & \\
1 & & 5 & & 10 & & 10 & & 5 & & 1 \\
 & & & & & \ldots & & & & &
\end{array}
$$

Hier stehen in der $n-$ten Reihe die Zahlen $\binom{n}{0}\binom{n}{1}\cdots\binom{n}{n-1}\binom{n}{n}$, wobei wir bei $n = 0$ anfangen und $\binom{0}{0} = 1$ setzen.

Erklären Sie, wie man die Formel aus Satz 2.6 anwenden kann, um sukzessive das Pascal'sche Dreieck zu konstruieren.

Welche Formel steckt hinter der Spiegelsymmetrie des Pascal'schen Dreiecks ?

Zum Abschluss dieses Kapitels wollen wir noch die binomische Formel zeigen:

Satz 2.7 *Für $x, y \in \mathbb{R}$ und $n \in \mathbb{N}$ gilt*

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$$

Beweis : (mit Induktion nach n):

Induktionsanfang: Für $n = 1$ lautet die rechte Seite der Behauptung

$$\binom{1}{0} x^1 y^0 + \binom{1}{1} x^0 y^1 = x + y.$$

Also stimmt die Aussage für $n = 1$.

Induktionsschluss: Angenommen, unsere Behauptung stimmt für n. Dann gilt für alle $x, y \in \mathbb{R}$

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k. \quad (*)$$

Wir untersuchen nun

$$\begin{aligned}(x+y)^{n+1} &= (x+y)^n \cdot (x+y)\\ &\overset{(*)}{=} \Big(\sum_{k=0}^{n} \tbinom{n}{k} x^{n-k}y^k\Big)(x+y)\\ &= \sum_{k=0}^{n} \tbinom{n}{k} x^{n-k+1}y^k + \sum_{k=0}^{n} \tbinom{n}{k} x^{n-k}y^{k+1}\end{aligned}$$

Jetzt ändern wir den Laufindex in der zweiten Summe und setzen $j = k+1$:

$$\sum_{k=0}^{n} \binom{n}{k} x^{n-k}y^{k+1} = \sum_{j=1}^{n+1} \binom{n}{j-1} x^{n+1-j}y^j$$

Dann können wir zusammenfassen:

$$\begin{aligned}(x+y)^{n+1} &= \sum_{k=0}^{n} \tbinom{n}{k} x^{n+1-k}y^k + \sum_{j=1}^{n+1} \tbinom{n}{j-1} x^{n+1-j}y^j\\ &= \tbinom{n}{0} x^{n+1-0}y^0 + \sum_{k=1}^{n} \big[\tbinom{n}{k} + \tbinom{n}{k-1}\big] x^{n+1-k}y^k + \tbinom{n}{n} x^0 y^{n+1}\\ &\overset{2.6}{=} \sum_{k=0}^{n+1} \tbinom{n+1}{k} x^{n+1-k}y^k.\end{aligned}$$

□

Für $n = 2$ ergibt sich die bekannte „erste binomische Formel“:

$$(x+y)^2 = x^2 + 2xy + y^2,$$

die sich auch einfach durch Ausmultiplizieren nachweisen lässt. Der Faktor 2 ist hier der Binomialkoeffizient $\binom{2}{1}$.

Setzt man $z = -y$, so erhält man die „zweite binomische Formel“:

$$\begin{aligned}(x-y)^2 = (x+z)^2 &= x^2 + 2xz + z^2\\ &= x^2 - 2xy + y^2.\end{aligned}$$

3 Stellenwertsysteme

Unser Dezimalsystem beruht darauf, dass wir jede natürliche Zahl als Summe von Vielfachen von Zehnerpotenzen zerlegen. So ist etwa

$$3921 = 1 \cdot 10^0 + 2 \cdot 10^1 + 9 \cdot 10^2 + 3 \cdot 10^3.$$

Dies geht auch mit anderen Basen als 10. Wir brauchen dazu folgende Tatsache:

Satz 3.1 *(Division mit Rest)*
Es sei $q \in \mathbb{N}$. Für jedes $a \in \mathbb{N}$ gibt es eindeutig bestimmte Zahlen $b \in \mathbb{N}$ und $r \in \{0, \ldots, q-1\}$ mit

$$a = qb + r.$$

Hier wird b als Quotient und r als Rest bezeichnet.

Damit können wir für jedes $g \in \mathbb{N}$ mit $g > 1$ die natürlichen Zahlen „$g-$adisch entwickeln“:

Satz 3.2 *Sei $g > 1$ eine natürliche Zahl. Dann lässt sich jedes $a \in \mathbb{N}$ darstellen als*

$$\begin{aligned} a &= b_n g^n + b_{n-1} g^{n-1} + \ldots + b_1 g + b_0 \\ &= \sum_{i=0}^{n} b_i g^i \end{aligned}$$

mit $b_0, \ldots, b_n \in \{0, \ldots, g-1\}$ und $b_n \neq 0$. Diese Darstellung ist eindeutig. Das heißt: Gilt auch

$$a = \sum_{i=0}^{k} b'_i g_i$$

mit $b'_0, \ldots, b'_k \in \{0, \ldots, g-1\}$ und $b'_k \neq 0$, so ist $n = k$ und $b_0 = b'_0, b_1 = b'_1, \ldots, b_n = b'_n$.

Beweis : Da $g > 1$ ist, werden die Potenzen g^m für wachsendes m beliebig groß. Für jedes $a \in \mathbb{N}$ gibt es also ein $m \in \mathbb{N}$ mit $a < g^m$. Wir zeigen die Existenz einer Darstellung der Form $(*)$ für alle $a < g^m$ mit Induktion nach m. Für den Induktionsanfang ist $a < g^1 = q$. Dann können wir $n = 0$ und $b_0 = a$ setzen und erhalten die Behauptung.

Für den Induktionsschluss nehmen wir an, unsere Behauptung gilt für ein $m \in \mathbb{N}$. Wir betrachten eine natürliche Zahl $a < g^{m+1}$. Wir können annehmen, dass $g^m \leqq a$ ist, denn sonst existiert eine Darstellung der Form $(*)$ nach Induktionsvoraussetzung. Wir wenden Satz 3.1 auf $q = g^m$ an und erhalten ein $b \in \mathbb{N}$ und $r \in \{0, \ldots, q^m - 1\}$ mit

$$a = bg^m + r.$$

Da $a \geqq g^m$ ist, muss $b \neq 0$ sein. Aus $a < g^{m+1}$ folgt ferner $b < g$. Wir setzen $n = m, b_n = b$ und wenden auf $r < q^m$ die Induktionsvoraussetzung an. Daraus folgt die Existenz einer Entwicklung

$$a = b_n g^n + b_{n-1} g^{n-1} + \ldots + b_0$$

mit $b_0, \ldots, b_n \in \{0, \ldots, g-1\}$ und $b_n \neq 0$.

Die Eindeutigkeit dieser Darstellung zeigen wir ebenfalls mit Induktion nach m für alle $a < g^m$.

Den Induktionsanfang lassen wir als Übungsaufgabe. Für den Induktionsschluss nehmen wir an, die Darstellung $(*)$ ist eindeutig für alle $a < g^m$ und betrachten ein $a < g^{m+1}$. Es sei

$$a = \sum_{i=0}^{n} b_i g^i = \sum_{j=0}^{k} b'_j g^j$$

mit $b_n \neq 0$ und $b'_k \neq 0$. Aus $0 \leqq b_i \leqq g-1$ und $0 \leqq b'_j \leqq g-1$ folgt mit Hilfe der geometrischen Summenformel

$$g^n \leqq a \leqq \sum_{i=0}^{n} (g-1) g^i = (g-1) \frac{1-g^{n+1}}{1-g} < g^{n+1}$$

und analog

$$g^k \leqq a < g^{k+1}$$

Somit ist $k = n$, und aus der Abschätzung $a < g^{m+1}$ folgt $n \leqq m$. Eine analoge Abschätzung zeigt

$$0 \leqq \sum_{i=0}^{n-1} b_i g^i \leqq \sum_{i=0}^{n-1} (g-1) g^i < g^n$$

sowie $0 \leqq \sum\limits_{i=0}^{n-1} b'_i g^i < g^n$.

Also ist $\sum\limits_{i=0}^{n-1} b_i g^i$ und auch $\sum\limits_{i=0}^{n-1} b'_i g^i$ der Rest bei Division von a durch g^n. Dieser ist eindeutig bestimmt nach Satz 3.1. Also ist

$$\sum_{i=0}^{n-1} b_i g^i = \sum_{i=0}^{n-1} b'_i g^i.$$

Diese Zahl ist $< g^n \leqq g^m$. Nach der Induktionsvoraussetzung gilt also auch

$$b_i = b'_i \text{ für } i = 0, \ldots, n-1.$$

□

Besonders interessant für Anwendungen ist der Fall $g = 2$, indem wir die Binärdarstellung natürlicher Zahlen enthalten. Hier sind alle $b_i \in \{0, 1\}$ und wir schreiben statt

$$a = b_n 2^n + b_{n-1} 2^{n-1} + \ldots + b_1 2 + b_0$$

auch einfach $b_n \dots b_0$ als Folge von „Binärziffern“.

Beispiel: $\begin{aligned} 43 &= 32 + 8 + 2 + 1 \\ &= 2^5 + 0 \cdot 2^4 + 2^3 + 0 \cdot 2^2 + 2 + 1 \end{aligned}$ entspricht den Binärziffern 101011.

In den Übungsaufgaben werden wir weitere Beispiele kennenlernen.

4 Die ganzen Zahlen

Jetzt wollen wir die ganzen Zahlen aus den natürlichen Zahlen konstruieren. Die Idee ist folgende: Wir betrachten Differenzen $a - b$, um negative Zahlen zu konstruieren. Aber was sind Differenzen? Das müssen wir noch definieren. Dazu betrachten wir die Menge $\mathbb{N} \times \mathbb{N}$ geordneter Paare (a, b) von natürlichen Zahlen. Wir wollen jetzt durch das Tupel (a, b) die Zahl $a - b$ definieren. Dazu stoßen wir auf folgende Schwierigkeit: Schon in den natürlichen Zahlen kann

$$a - b = c - d$$

gelten, ohne dass $(a, b) = (c, d)$ ist. (Finden Sie ein Beispiel!) Solche Tupel wollen wir in Zukunft identifizieren. Wir nennen (a, b) und $(c, d) \in \mathbb{N}$ äquivalent und schreiben $(a, b) \sim (c, d)$, falls $a+d = c+b$ gilt. Dies ist eine Aussage, die wir auf den natürlichen Zahlen nachprüfen können. Es gilt (Übungsaufgabe)

i) $(a, b) \sim (a, b)$ für alle $a, b \in \mathbb{N}$.

ii) Ist $(a, b) \sim (c, d)$, so ist auch $(c, d) \sim (a, b)$.

iii) Ist $(a, b) \sim (c, d)$ und $(c, d) \sim (e, f)$, so folgt $(a, b) \sim (e, f)$.

Diese drei Eigenschaften machen eine Äquivalenzrelation aus. Das werden wir jetzt allgemein definieren:

Definition 4.1 *Es sei M eine Menge und $R \subset M \times M$ eine Teilmenge. Wir schreiben $m \sim n$, falls $(m, n) \in R$ ist. Dann heißt R (oder auch $\sim$) eine Äquivalenzrelation auf M, falls folgende drei Bedingungen gelten:*

i) (Reflexivität) Für alle $m \in M$ ist $(m, m) \in R$ (mit anderen Worten: $m \sim m$).

ii) (Symmetrie) Ist $(m, n) \in R$, so folgt $(n, m) \in R$ (mit anderen Worten: Gilt $m \sim n$, so auch $n \sim m$).

iii) (Transitivität) Sind $(m, n) \in R$ *und* $(n, p) \in R$*, so folgt* $(m, p) \in R$*. (mit anderen Worten: gilt* $m \sim n$ *und* $n \sim p$*, so folgt* $m \sim p$*).*

Beispiel: Die eingangs definierte Relation $\{(a, b, c, d) \in \mathbb{N}^4 : a + d = c + b\}$ ist eine Äquivalenzrelation auf $\mathbb{N} \times \mathbb{N}$.

Ist R eine Äquivalenzrelation auf der Menge M, so nennen wir für jedes $m \in M$ die Menge

$$[m] = \{n \in M : n \sim m\}$$

die Äquivalenzklasse von M. Dies ist eine Teilmenge von M.

Lemma 4.2 *Ist* R *eine Äquivalenzrelation auf* M*, so ist für* $m_1, m_2 \in M$ *entweder* $[m_1] = [m_2]$ *oder* $[m_1] \cap [m_2] = \emptyset$*. Äquivalenzklassen sind also entweder gleich oder disjunkt.*

Ferner gilt $[m_1] = [m_2]$ *genau dann, wenn* $m_1 \sim m_2$ $\big($ *also* $(m_1, m_2) \in R\big)$ *gilt.*

Beweis : Wir nehmen an, dass $[m_1] \cap [m_2] \neq \emptyset$ ist. Dann existiert ein $n \in [m_1] \cap [m_2]$. Dieses erfüllt $n \sim m_1$ und $n \sim m_2$. Aus Symmetrie folgt $m_1 \sim n$. Also ist $m_1 \sim n$ und $n \sim m_2$, woraus mit Transitivität $m_1 \sim m_2$ folgt.

Ist nun $k \in [m_1]$ beliebig, so gilt $k \sim m_1$, mit Hilfe der Transitivität also $k \sim m_2$ und somit $k \in [m_2]$. Also ist $[m_1] \subset [m_2]$. Dasselbe Argument zeigt $[m_2] \subset [m_1]$ und damit $[m_1] = [m_2]$. □

Definition 4.3 *Wir definieren die Menge der ganzen Zahlen* $\mathbb{Z}$ *als Menge aller Äquivalenzklassen in* $\mathbb{N} \times \mathbb{N}$ *bezüglich der eingangs definierten Äquivalenzrelation* $\sim$*.*

$$\begin{array}{rcl} \text{Es sei } i : \mathbb{N} & \to & \mathbb{Z} \text{ die Abbildung} \\ n & \mapsto & [(n+1, 1)]. \end{array}$$

Lemma 4.4 *Die Abbildung* i *ist injektiv.*

Beweis : Ist $i(n) = i(m)$, so folgt $[(n + 1, 1)] = [(m + 1, 1)]$ und daher nach Lemma 4.2 $(n + 1, 1) \sim (m + 1, 1)$. Also gilt $n + 2 = m + 2$, woraus $m = n$ folgt. □

Ferner bezeichnen wir die Klasse $[(1, 1)]$ als 0.

Definition 4.5 *Auf $\mathbb{Z}$ definieren wir eine Addition durch*

$$[(a,b)] + [(c,d)] = [(a+c, b+d)]$$

und eine Multiplikation durch

$$[(a,b)] \cdot [(c,d)] = [(ac+bd, bc+ad)]$$

Wir müssen nun prüfen, dass diese Definition sinnvoll ist („wohldefiniert“ ist), das heißt, dass sie nicht von der Wahl von (a,b) abhängt! Dieses Element ist ja durch seine Äquivalenzklasse $[(a,b)]$ nicht eindeutig bestimmt, da jedes Element (a',b') mit $(a,b) \sim (a',b')$ ebenfalls die Äquivalenzklasse $[(a',b')] = [(a,b)]$ liefert. Daher ist zu zeigen:

Gilt $(a,b) \sim (a',b')$ und $(c,d) \sim (c',d')$, so folgt

$$(a+c, b+d) \sim (a'+c', b'+d')$$

und

$$(ac+bd, bc+ad) \sim (a'c'+b'd', b'c'+a'd').$$

Wir zeigen dies hier nur für die Addition, wo (nach Einsetzen der Definition der Äquivalenzrelation $\sim$) aus

$$a + b' = a' + b \text{ und } c + d' = c' + d$$

sofort $a + c + b' + d' = b + d + a' + c'$ folgt.

Satz 4.6 *Die Addition und die Multiplikation auf $\mathbb{Z}$ erfüllen folgende Gesetze: Für alle $x, y, z \in \mathbb{Z}$ ist*

i) $(x+y)+z = x+(y+z)$ *(Assoziativgesetz der Addition)*

ii) $x + y = y + x$ *(Kommutativgesetz der Addition)*

iii) Für $0 = [(1,1)]$ *gilt* $x + 0 = x$ *(Neutrales Element der Addition)*

iv) Für jedes $x \in \mathbb{Z}$ gibt es genau ein $y \in \mathbb{Z}$, genannt $-x$, mit $x + y = 0$. (Inverses Element der Addition)

v) $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ *(Assoziativgesetz der Multiplikation)*

vi) $x \cdot y = y \cdot x$ *(Kommmutativgesetz der Multiplikation)*

vii) *Für das Element* $i(1) = [(2,1)]$ *gilt* $i(1)x = x$ *(Neutrales Element der Multiplikation)*

viii) $x(y+z) = xy + xz$ *(Distributivgesetz)*

ix) *Für* $n, m \in \mathbb{N}$ *gilt* $i(n+m) = i(n) + i(m)$

x) *Für* $n, m \in \mathbb{N}$ *gilt* $i(nm) = i(n)i(m)$

Beweis : Das erfolgt durch geduldiges Einsetzen der Definitionen. Wir zeigen hier nur iv) und vii).

iv) Wir definieren für $x = [(a,b)] \in \mathbb{Z}$ das Element y als $[(b,a)]$.

Dann gilt

$$\begin{array}{rcl} x + y & = & [(a,b)] + [(b,a)] \\ & \overset{Def.4.5}{=} & [(a+b, b+a)] \\ & = & [(a+b, a+b)] = [(1,1)] = 0, \end{array}$$

denn die Addition auf $\mathbb{N}$ ist kommutativ.

vii) Ist $x = [(a,b)] \in \mathbb{Z}$, so gilt

$$\begin{array}{rcl} & & i(1)x \\ & = & [(2,1)][(a,b)] \\ & \overset{Def.4.5}{=} & [(2a+b, a+2b)] \\ & = & [(a,b)] = x, \end{array}$$

denn $(2a+b, a+2b) \sim (a,b)$.

□

Wir schreiben für die Multiplikation auch einfach xy statt $x \cdot y$ und für $x + (-y)$ einfach $x - y$. Auch lassen wir die Abbildung i oft weg und schreiben n statt $i(n)$ für $n \in \mathbb{N}$.

Wieso haben wir uns soviel Mühe gemacht mit der Definition von $\mathbb{Z}$ und den Grundrechenarten Addition und Multiplikation? A priori ist nicht klar, wie man ganze Zahlen aus natürlichen Zahlen konstruieren kann. Dass wir aus der Schule daran gewöhnt sind, mit negativen Zahlen zu rechnen, ändert daran nichts. In den Schulbüchern werden die ganzen Zahlen nämlich üblicherweise auch nicht definiert, sondern fallen einfach vom Himmel und werden mit „Schulden“ oder Symmetriebetrachtungen motiviert. Wieso aber ein Rechengesetz der Form $(-1) \cdot (-1) = 1$ gilt,

kann so nicht rigoros begründet werden! In unserer Konstruktion der ganzen Zahlen gilt hingegen:

$$\begin{aligned} -1 &= -[(2,1)] \\ &= [(1,2)], \end{aligned}$$

also ist $(-1)(-1)$ nach der Definition der Multiplikation gerade

$$\begin{aligned} & (-1)\cdot(-1) \\ = \; & [(1,2)][(1,2)] \\ = \; & [(1+4, 2+2)] \\ = \; & [(5,4)] \\ = \; & [(2,1)] \\ = \; & 1. \end{aligned}$$

Dies ist eine rigorose Begründung!

Definition 4.7 *Seien $x, y \in \mathbb{Z}$. x heißt „kleiner als y“$(x < y)$, wenn $y - x \in \mathbb{N}$ gilt, wenn es also ein $n \in \mathbb{N}$ mit*

$$y - x = i(n) = [(n+1, 1)]$$

gibt. x heißt „größer als y“ $(x > y)$, wenn y kleiner als x ist. Wir schreiben $x \geqq y$ (beziehungsweise $x \leqq y$), falls x größer oder gleich (beziehungsweise kleiner oder gleich) y ist.

Dann gelten folgende Regeln:

Lemma 4.8 *Für alle $x, y, z \in \mathbb{Z}$ gilt*

i) $x < y \Rightarrow x + z < y + z$

ii) $x < y \Rightarrow -y < -x$

iii) $a < b$ *und* $c > 0 \Rightarrow ac < bc$

iv) $a < b$ *und* $c < 0 \Rightarrow ac > bc$

Beweis : Übungsaufgabe. □

Jetzt können wir noch zeigen, dass $\mathbb{Z}$ aus den natürlichen Zahlen, der 0 und den negativen natürlichen Zahlen besteht. Dazu sei:

$$\begin{aligned} -\mathbb{N} &= \{-i(n) : n \in \mathbb{N}\} \\ &= \{-[(n+1,1)] = [(1,n+1)] : n \in \mathbb{N}\} \\ &\subset \mathbb{Z}. \end{aligned}$$

Satz 4.9 *Es gilt*

$$\mathbb{Z} = \mathbb{N} \cup \{0\} \cup -\mathbb{N}.$$

Beweis : Sei $x = [(a, b)] \in \mathbb{Z}$. Ist $a = b$, so ist $x = [(1, 1)] = 0$. Ist $a > b$, also $a - b \in \mathbb{N}$ und somit

$$x = [(a - b + 1, 1)] = i(a - b) \in \mathbb{N}.$$

Ist $a < b$, also $b - a \in \mathbb{N}$, so ist

$$x = [(1, b - a + 1)] = -i(b - a) \in -\mathbb{N}.$$

□

Satz 4.10 *Sind $xy \in \mathbb{Z}$ mit $xy = 0$, so folgt $x = 0$ oder $y = 0$. Wir sagen: „$\mathbb{Z}$ ist nullteilerfrei“.*

Beweis : Übungsaufgabe. □

Definition 4.11 *Es seien d und x ganze Zahlen. Wir nennen d Teiler von x, falls es ein $y \in \mathbb{Z}$ gibt mit $dy = x$. Wir schreiben $d|x$, falls d ein Teiler von x ist.*

Wir haben in Satz 3.1 schon die Division mit Rest kennengelernt. Jetzt wollen wir Zahlen identifizieren, die denselben Rest lassen. Genauer definieren wir:

Definition 4.12 *Es seien $a, b \in \mathbb{Z}$ und $m \in \mathbb{N}$. Dann heißen a und b kongruent modulo m (wir schreiben $a \equiv b \mod m$), falls m ein Teiler von $a - b$ ist.*

Also gilt $a \equiv b \mod m$ genau dann, wenn es ein $q \in \mathbb{Z}$ gibt mit $a = qm + b$. Zwei natürliche Zahlen a, b sind also genau dann kongruent modulo $q \in \mathbb{N}$, falls sie bei Division durch q denselben Rest lassen (siehe Satz 3.1).

Beispiel

i) $a \equiv b \mod 1$ für alle $a, b \in \mathbb{Z}$.

ii) $17 \equiv 2 \mod 5$.

iii) $11 \equiv -1 \mod 12$.

Lemma 4.13 *Die Kongruenz modulo m ist eine Äquivalenzrelation.*

Beweis : Übungsaufgabe. □

Lemma 4.14 *Gilt* $a \equiv b \mod m$ *und* $c \equiv d \mod m$, *so folgt*

$$\begin{aligned} a + c &\equiv b + d \mod m \\ \textit{und} \quad a\,c &\equiv b\,d \mod m. \end{aligned}$$

Beweis : Übungsaufgabe. □

Wir wollen jetzt noch die aus der Schule bekannten „Dreier- und Neunerregeln“ für die Diskussion zeigen.

Satz 4.15 *Es sei* $a \in \mathbb{N}$ *die Zahl mit den Ziffern* $a = b_n b_{n-1} \ldots b_1 b_0$ *in Dezimalentwicklung, also*

$$a = b_n \cdot 10^n + b_{n-1} 10^{n-1} + \ldots + b_i 10 + b_0$$

mit $b_0, \ldots, b_n \in \{0, \ldots, 9\}$ *wie in Satz 3.2. Dann ist* $\sum_{i=0}^{n} b_i$ *die sogenannte Quersumme von* a. *Es gilt:*

i) $3|a$ *genau dann, wenn* $3|\sum_{i=0}^{n} b_i$. *(Dreierregel)*

ii) $9|a$ *genau dann, wenn* $9|\sum_{i=0}^{n} b_i$. *(Neunerregel)*

iii) $11|a$ *genau dann, wenn* $11|\sum_{i=0}^{n}(-1)^i b_i$ *(Elferregel)*

Hier ist $\sum_{i=0}^{n}(-1)^i b_i = b_0 - b_1 + b_2 - \ldots \pm b_n$ *die „alternierende Quersumme“.*

Beweis :

i) $3|a$ genau dann, wenn $a \equiv 0 \mod 3$ ist.

Nun ist $10 = 9 + 1 \equiv 1 \mod 3$, also folgt aus Lemma 4.14

$$10^i = \underbrace{10 \cdot \ldots \cdot 10}_{i-\text{mal}} \equiv 1^i = 1 \mod 3$$

und $b_i \cdot 10^i \equiv b_i \mod 3$. Aus demselben Lemma folgt

$$a = \sum_{i=0}^{n} 10^i b_i \equiv \sum_{i=0}^{n} b_i \mod 3.$$

Somit ist $a \equiv 0 \mod 3$ genau dann, wenn $\sum_{i=0}^{n} b_i \equiv 0 \mod 3$.

ii) Das geht analog wie i). Führen Sie das aus!

iii) Es gilt $10 \equiv -1 \mod 11$, woraus mit Lemma 4.14 zunächst

$$10^i \equiv (-1)^i \mod 11,$$

dann

$$b_i 10^i \equiv (-1)^i \mod 11$$

und schließlich

$$a = \sum_{i=0}^{n} b_i 10^i \equiv \sum_{i=0}^{n} (-1)^i b_i \mod 11$$

folgt. Somit ist 11 ein Teiler von a genau dann, wenn $a \equiv 0 \mod 11$. Das ist genau dann der Fall, wenn

$$\sum_{i=0}^{n} (-1)^i b_i \equiv 0 \mod 11$$

ist, wenn also 11 die alternierende Quersumme $\sum_{i=0}^{n} (-1)^i b_i$ teilt.

□

Definition 4.16 *Eine natürliche Zahl $p \geqq 2$ heißt Primzahl, wenn für alle $d \in \mathbb{N}$ gilt:*

$$d|p \Rightarrow d = 1 \text{ oder } d = p.$$

Eine Primzahl ist in den natürlichen Zahlen also nur durch 1 und sich selbst teilbar.

Man kann die Folge aller Primzahlen durch das „Sieb des Eratosthenes“ generieren. Man streicht aus der Folge

$$2, 3, 4, 5, 6, 7, 8, \ldots$$

bis auf 2 alle durch 2 teilbaren Zahlen, bis auf 3 alle durch 3 teilbaren Zahlen, bis auf die nächste Zahl (hier 5) alle Vielfachen usw. Also ergibt sich

$$2, 3, \not{4}, 5, \not{6}, 7, \not{8}, \not{9}, \not{10}, 11, \not{12}, 13, \not{14}, \not{15}, \ldots$$

Am Ende dieses Prozesses bleiben nur die Primzahlen übrig (wieso?).

Der wichtigste Satz der elementaren Zahlentheorie lautet

Satz 4.17 *Jede natürliche Zahl $n \geqq 2$ lässt sich als Produkt von Primzahlen schreiben. Diese Darstellung ist bis auf die Reihenfolge der Faktoren eindeutig.*

Beispiel

$$\begin{aligned} 10 &= 2 \cdot 5 = 5 \cdot 2 \\ 48 &= 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \end{aligned}$$

Satz 4.18 *Es gibt unendlich viele Primzahlen.*

Beweis : Angenommen, es gäbe nur endlich viele Primzahlen. Sei $n \in \mathbb{N}$ ihre Anzahl. Wir nummerieren sie durch als $p_1, p_2, \ldots, p_n$.

Jetzt betrachten wir die Zahl

$$N = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1.$$

Nach Satz 4.17 ist N ein Produkt von Primzahlen, also gibt es ein i mit $p_i | N$.

Da p_i auch ein Teiler des Produkts $p_1 \cdot \ldots \cdot p_n$ ist, folgt

$$p_i | (N - p_1 \cdot \ldots \cdot p_n),$$

also ist p_i ein Teiler von 1. Das ist wegen $p_i \geqq 2$ aber ausgeschlossen. Also ist unsere Annahme falsch und es gibt unendlich viele Primzahlen. □

5 Rationale Zahlen

Jetzt wollen wir die rationalen Zahlen als Menge von Brüchen ganzer Zahlen einführen. Da man Brüche kürzen kann, brauchen wir auch hier wieder eine geeignete Äquivalenzrelation.

Definition 5.1 *Sei $\mathbb{Z}^* = \mathbb{Z} \backslash \{0\}$ die Menge der ganzen Zahlen ohne Null und $P = \mathbb{Z} \times \mathbb{Z}^*$ die Menge aller geordneten Paare (a, b) ganzer Zahlen, wobei die zweite nicht Null ist (also $b \neq 0$). Wir definieren für (a, b) und (c, d) in P :*

$$(a, b) \sim (c, d)$$

genau dann, wenn $ad = cb$ in $\mathbb{Z}$ gilt.

Lemma 5.2 *Das definiert eine Äquivalenzrelation.*

Beweis : Übungsaufgabe. □

Definition 5.3 *Wir definieren $\mathbb{Q}$ (die Menge der rationalen Zahlen) als die Menge der Äquivalenzklassen bezüglich der Relation $\sim$ auf P. Wir schreiben*

$$\frac{a}{b} \textit{ für die Klasse } [(a,b)].$$

Dann gilt $\frac{a}{b} = \frac{c}{d}$, falls $ad = bc$ ist, denn genau dann sind (a, b) und (c, d) äquivalent.

Nun definieren wir eine Abbildung

$$i : \mathbb{Z} \to \mathbb{Q}$$

durch $i(a) = \frac{a}{1}$ für alle $a \in \mathbb{Z}$.

Lemma 5.4 *Die Abbildung i ist injektiv.*

Beweis : Sind $a, b \in \mathbb{Z}$ mit $i(a) = i(b)$, so ist $\frac{a}{1} = \frac{b}{1}$. Das bedeutet $[(a, 1)] = [(b, 1)]$. Nach Lemma 4.2 folgt $(a, 1) \sim (b, 1)$, also $a = b$. □

In Zukunft identifizieren wir immer $\mathbb{Z}$ mit seinem Bild in $\mathbb{Q}$ und lassen die Abbildung i weg.

Satz 5.5 *Für alle $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$ werden durch*

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \textit{ und } \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

eine Addition und eine Multiplikation definiert, die auf der Teilmenge $\mathbb{Z}$ mit der bisher verwendeten Addition und Multiplikation übereinstimmen.

Addition und Multiplikation auf $\mathbb{Q}$ sind kommutativ und assoziativ im Sinne von Satz 4.6 i), ii), v), vi) und erfüllen das Distributivgesetz Satz 4.6 viii). Das Element $0 \in \mathbb{Z}$ ist ein neutrales Element bezüglich der Addition, das heißt, es gilt $x + 0 = x$ für alle $x \in \mathbb{Q}$.

Das Element $1 \in \mathbb{Z}$ ist ein neutrales Element der Multiplikation, das heißt, es gilt $1 \cdot x = x$ für alle $x \in \mathbb{Q}$.

Wie in Satz 4.6 iv) hat jedes $x \in \mathbb{Q}$ ein inverses Element, das wir $-x$ nennen, bezüglich der Addition.

Neu in $\mathbb{Q}$ ist die Tatsache, dass jedes $x \in \mathbb{Q}$ mit $x \neq 0$ auch ein inverses Element bezüglich der Multiplikation besitzt:

Zu x existiert ein $y \in \mathbb{Q}$ mit $xy = 1$. Wir schreiben $x^{-1} = y$ für dieses eindeutig bestimmte Element.

Beweis : Die Addition und die Multiplikation sind auf Vertretern der Äquivalenzklassen definiert. Man muss also zunächst prüfen:

Sind $(a,b) \sim (a',b')$ und $(c,d) \sim (c',d')$, so ist $(ad+bc,bd) \sim (a'd'+b'c',b'd')$ und $(ac,bd) \sim (a'c',b'd')$. Das folgt sofort aus der Definition der Äquivalenzrelation.

Da $\frac{a}{1} + \frac{b}{1} = \frac{ab}{1}$ und $\frac{a}{1} \cdot \frac{b}{1} = \frac{ab}{1}$ direkt aus den Definitionen folgt, setzen diese Operationen die Rechenoperationen auf $\mathbb{Z}$ fort.

Ist $x \in \mathbb{Q}$ mit $x \neq 0$, so gilt $x = \frac{a}{b} = [(a,b)]$ mit $x \neq 0 = [(0,1)]$. Also folgt $(a,b) \not\sim (0,1)$. Daher gilt $a \neq 0$. Somit ist auch $(b,a) \in P$ und wir definieren $y = [(b,a)] = \frac{b}{a} \in \mathbb{Q}$. Da $xy = \frac{a}{b}\frac{b}{a} = 1$ ist, ist y ein inverses Element bezüglich der Multiplikation. Die anderen Behauptungen sind Übungsaufgaben, die leicht sind, wenn man die Definitionen verstanden hat. □

Definition 5.6 *Eine Menge M mit zwei Verknüpfungen*

$$+ : M \times M \to M \text{ und } \cdot : M \times M \to M,$$

für die Assoziativität, Kommutativität und Distributivität im Sinne von Satz 4.6 i), ii), v), vi), viii) gilt und für die neutrale Elemente 0 bezüglich $+$ und 1 bezüglich $\cdot$ sowie inverse Elemente bezüglich $+$ existieren, heißt kommutativer Ring mit 1 (oder einfach nur Ring).

Gilt zusätzlich $1 \neq 0$ und existiert für jedes $x \neq 0$ ein inverses Element bezüglich $\cdot$, so heißt M Körper.

Beispiel: $\mathbb{Z}$ ist ein Ring, $\mathbb{Q}$ ist ein Körper.

Jetzt wollen wir noch die Größer- und Kleiner-Relation von den ganzen Zahlen $\mathbb{Z}$ auf $\mathbb{Q}$ übertragen.

Definition 5.7 *Für rationale Zahlen $\frac{a}{b}$ und $\frac{c}{d}$ gilt $\frac{c}{d} < \frac{a}{b}$ genau dann, wenn $(ad-bc)bd > 0$ ist. Die Relationen $>, \leqq$ und $\geqq$ definieren wir dann analog zu Definition 4.7 mit Hilfe von $<$.*

Die Motivation für diese Definition ist folgende: Ein Bruch $\frac{a}{b}$ soll positiv sein, wenn entweder Zähler und Nenner beide positiv oder beide negativ sind. Das lässt sich einfach als $ab > 0$ ausdrücken.

Die obige Definition heißt nichts anderes als: Das Produkt des Zählers von $\frac{a}{b} - \frac{c}{d}$ mit dem Nenner von $\frac{a}{b} - \frac{c}{d}$ ist positiv (als ganze Zahl).

Lemma 5.8 *i) Auf $\mathbb{Z} \subset \mathbb{Q}$ erhalten wir die bekannten Relationen, wenn wir Definition 5.7 anwenden.*

ii) Für $x, y \in \mathbb{Q}$ gilt entweder $x < y$ oder $x = y$ oder $x > y$.

Für beliebige $x, y, z \in \mathbb{Q}$ gilt

iii) $x < y \Rightarrow x + z < y + z$

iv) $x < y$ *und* $z > 0 \Rightarrow xz < yz$

v) $x < y$ *und* $z < 0 \Rightarrow xz > yz$

vi) $0 < x < y \Rightarrow 0 < y^{-1} < x^{-1}$.

Beweis :

i) folgt sofort aus den Definitionen, wenn wir uns daran erinnern, dass wir eine ganze Zahl a als $[(a, 1)] = \frac{a}{1}$ auffassen.

ii) Angenommen $x = \frac{a}{b}$ und $y = \frac{c}{d}$ sind rationale Zahlen mit $x \neq y$. Dann ist $[(a, b)] \neq [(c, d)]$, also $(a, b) \not\sim (b, d)$, was

$$ad - bc \neq 0$$

bedeutet.

Da b und d ungleich 0 sind, ist auch $bd \neq 0$. Also ist das Produkt

$$(ad - bc)bd \neq 0.$$

Ist es > 0, so ist definitionsgemäß $y < x$, also $x > y$. Ist es < 0, so ist $x < y$.

iii) - vi) Übungsaufgabe.

□

Wir brauchen nun noch den Betrag rationaler Zahlen, den wir wie folgt definieren.

Definition 5.9 *Für $x \in \mathbb{Q}$ definieren wir $|x|$ (den Betrag von x) als*

$$|x| = \begin{cases} x & , \text{ falls } x \geqq 0 \\ -x & , \text{ falls } x < 0. \end{cases}$$

Der Betrag einer rationalen Zahl ist also eine rationale Zahl $\geqq 0$.

Satz 5.10 *Für $x, y \in \mathbb{Q}$ gilt:*

i) $|x| = 0 \Leftrightarrow x = 0$

ii) $|-x| = |x|$

iii) $x \leqq |x|$

iv) $|xy| = |x||y|$

v) $|x \cdot y^{-1}| = |x||y|^{-1}$, *falls* $y \neq 0$

vi) $|x + y| \leqq |x| + |y|$ *(„Dreiecksungleichung“)*

vii) $|x - y| \leqq |x| + |y|$

viii) $\big||x| - |y|\big| \leqq |x| + |y|$.

Beweis :

i) - v) sind leichte Übungsaufgaben, wenn man für iv) und v) Lemma 5.8 benutzt.

vi) Wir nehmen zunächst an, dass $x + y > 0$ ist. Dann folgt mit iii)

$$|x + y| = x + y \leqq |x| + |y|.$$

Im Fall $x + y < 0$ folgt analog

$$|x + y| = -(x + y) = -x + (-y) \leqq |-x| + |-y| \overset{ii)}{=} |x| + |y|$$

vii) folgt aus vi) durch Anwendung auf $(-y)$ statt y.

viii) Ist $|x| > |y|$, so gilt

$$\big||x| - |y|\big| = |x| - |y| \leqq |x| + |y|$$

mit Lemma 5.8 iii).

Ist $|y| > |x|$, so ist $|x| < |y|$ und wir wenden das gerade Gezeigte auf (y, x) statt (x, y) an. Das liefert

$$\big||y| - |x|\big| \leqq |y| + |x| = |x| + |y|.$$

Wegen $\big||y| - |x|\big| \overset{ii)}{=} \big|-(|y| - |x|)\big| = \big||x| - |y|\big|$ folgt die Behauptung.

□

Definition 5.11 *Für zwei Zahlen $x, y \in \mathbb{Q}$ definieren wir ihren Abstand $d(x, y)$ als*

$$d(x, y) = |x - y|.$$

Der Abstand hat die folgenden drei Eigenschaften einer Metrik:

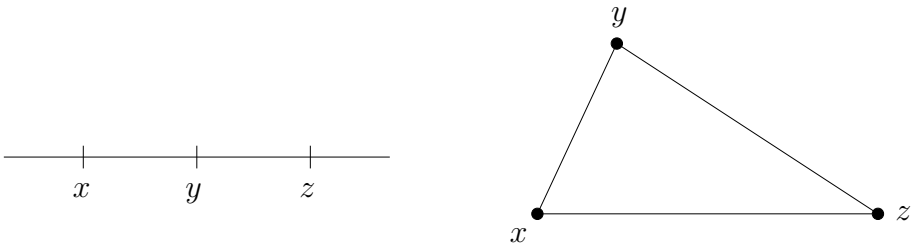
Lemma 5.12 *Für $x, y, z \in \mathbb{Q}$ gilt*

i) $d(x, y) \geqq 0$ *und* $d(x, y) = 0 \Leftrightarrow x = y$

ii) $d(x, y) = d(y, x)$

iii) $d(x, z) \leqq d(x, y) + d(y, z)$ *(„Dreiecksungleichung")*

Wieso heißt iii) Dreiecksungleichung ?



Beweis : Übungsaufgabe. □

Für jedes $x \in \mathbb{Q}$ und $\varepsilon > 0$ sei

$$U_\varepsilon(x) = \{y \in \mathbb{Q} : d(x, y) < \varepsilon\}$$

die „ε-Umgebung von x".

Setzt man die Definitionen ein, so folgt

$$\begin{aligned} U_\varepsilon(x) &= \{y \in \mathbb{Q} : |x - y| < \varepsilon\} \\ &= \{y \in \mathbb{Q} : x - \varepsilon < y < x + \varepsilon\}, \end{aligned}$$

denn $|x - y| < \varepsilon$ ist äquivalent zu

$$-\varepsilon < x - y < \varepsilon.$$

(Überlegen Sie sich das!)

Sind $y, z \in U_\varepsilon(x)$, so folgt aus der Dreiecksungleichung

$$\begin{aligned} d(y, z) &\leqq d(y, x) + d(x, z) \\ &= d(x, y) + d(x, z) \\ &< 2\varepsilon. \end{aligned}$$

6 Konvergenz

Wir wollen jetzt verstehen, wieso periodische Dezimalbrüche rationale Zahlen sind. Dazu brauchen wir den Begriff eines Grenzwertes.

Definition 6.1 *i) Ist für jedes $n \in \mathbb{N}$ eine rationale Zahl $a_n \in \mathbb{Q}$ gegeben, so nennen wir $(a_n)_{n\in\mathbb{N}}$ eine Folge rationaler Zahlen.*

ii) Die rationale Zahl $a \in \mathbb{Q}$ heißt Grenzwert der Folge $(a_n)_{n\in\mathbb{N}}$, falls gilt: Für jedes $\varepsilon > 0$ gibt es ein $N \in \mathbb{N}$, das von ε abhängt, mit $a_n \in U_\varepsilon(a)$ für alle $n \geqq N$. Diese Bedingung bedeutet einfach

$$|a_n - a| < \varepsilon$$

für alle $n \geqq N$.

iii) Ist a Grenzwert der Folge $(a_n)_{n\in\mathbb{N}}$, so sagen wir, $(a_n)_{n\in\mathbb{N}}$ konvergiert gegen a und schreiben

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

Beispiel:

i) Die konstante Folge $(a_n)_{n\in\mathbb{N}}$ mit $a_n = a \in \mathbb{Q}$ für alle $n \in \mathbb{N}$ konvergiert gegen a.

ii) Wir betrachten die Folge $(\frac{1}{n})_{n\geqq\mathbb{N}}$. Für jedes $\varepsilon > 0$ gibt es ein $N \in \mathbb{N}$ mit $\frac{1}{\varepsilon} < N$, also $\frac{1}{N} < \varepsilon$.

Dann gilt für alle $n \geqq N$

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

Also gilt $\lim_{n\to\infty} \frac{1}{n} = 0$.

Lemma 6.2 *Es seien $(a_n)_{n\geqq N}$ und $(b_n)_{n\in\mathbb{N}}$ Folgen in $\mathbb{Q}$ mit $\lim_{n\to\infty} a_n = a$ und $\lim_{n\to\infty} b_n = b$.*

Dann gilt

i) Für jedes c in $\mathbb{Q}$ ist auch die Folge $(ca_n)_{n\geqq 0}$ konvergent, und es gilt $\lim_{n\to\infty} ca_n = ca$.

ii) Die Folge $(a_n + b_n)_{n\in\mathbb{N}}$ konvergiert gegen $a + b$.

iii) Die Folge $(a_n \cdot b_n)_{n\in\mathbb{N}}$ konvergiert gegen ab.

Beweis :

i) Wir wissen, dass es für jedes $\varepsilon > 0$ ein $N \in \mathbb{N}$ gibt mit $|a_n - a| < \varepsilon$ für alle $n \geqq N$. Ist $c = 0$, dann ist die Behauptung klar (Wirklich?). Ist $c \neq 0$, so betrachten wir $\frac{1}{|c|}\varepsilon$. Es gibt ein $N \in \mathbb{N}$ mit

$$|a_n - a| < \frac{1}{|c|}\varepsilon \text{ für alle } n \geqq N.$$

Daraus folgt durch Multiplikation mit $|c|$:

$$|ca_n - ca| < \varepsilon \text{ für alle } n \geqq N.$$

Also folgt $\lim\limits_{n\to\infty} ca_n = ca$.

ii) Es sei $\varepsilon > 0$. Für die Zahl $\frac{\varepsilon}{2} > 0$ finden wir ein $N \in \mathbb{N}$ mit

$$|a_n - a| < \frac{\varepsilon}{2} \text{ für alle } n \geqq N$$

und ein $M \in \mathbb{N}$ mit

$$|b_n - b| < \frac{\varepsilon}{2} \text{ für alle } n \geqq M.$$

Wir wählen $N' = \max\{N, M\}$ als die größere der beiden Zahlen. Dann gilt für alle $n \geqq N'$

$$\begin{aligned} |(a_n + b_n) - (a + b)| &= |(a_n - a) + (b_n - b)| \\ &\leqq |a_n - a| + |b_n - b| \\ &< \tfrac{\varepsilon}{2} + \tfrac{\varepsilon}{2} = \varepsilon, \end{aligned}$$

also gilt $\lim\limits_{n\to\infty} (a_n + b_n) = a + b$.

iii) Übungsaufgabe.

□

Lemma 6.3 *Ist $q \in \mathbb{Q}$ mit $|q| < 1$, so gilt $\lim\limits_{n\to\infty} q^n = 0$.*

Als Hilfsmittel für den Beweis brauchen wir folgenden nützlichen Beobachtungen, die wir in den Übungen zeigen werden.

Lemma 6.4 *(Bernoulli'sche Ungleichung) Für alle $x \in \mathbb{Q}$ mit $x > 0$ und alle $n \geqq 2$ gilt*

$$(1 + x)^n > 1 + nx.$$

Beweis : Das folgt aus Satz 2.7 (Übungsaufgabe.) □

Satz 6.5 *$\mathbb{Q}$ erfüllt das Archimedische Axiom, das heißt, für beliebige $x, y \in \mathbb{Q}$ mit $x > 0$ existiert ein $n \in \mathbb{N}$ mit $nx > y$.*

Beweis : Übungsaufgabe. □

Beweis : (von Lemma 6.3) Wir müssen folgendes zeigen: Für jedes $\varepsilon > 0$ gibt es ein $N \in \mathbb{N}$, so dass

$$|q^n| < \varepsilon$$

für alle $n \geqq N$ gilt.

Es genügt, diese Behauptung für q mit $0 < q < 1$ zu zeigen (wieso?).

Dann ist $\frac{1}{q} > 1$ nach Lemma 5.8, also ist $h = \frac{1}{q} - 1 > 0$. Aus $\frac{1}{q} = 1 + h$ folgt $q = \frac{1}{1+h}$ und somit

$$q^n = \frac{1}{(1+h)^n} < \frac{1}{1+nh} \text{ für } n \geqq 2,$$

denn nach der Bernoulli'schen Ungleichung gilt $(1+h)^n > 1 + nh$.

Für jedes $\varepsilon > 0$ finden wir aber nun ein N mit $1 + nh > \varepsilon$ für alle $n \geqq N$, denn $(nh)_{n\in\mathbb{N}}$ wird beliebig groß nach dem Archimedischen Axiom Satz 6.5. Wir können $N \geqq 2$ annehmen, indem wir N zur Not vergrößern. Dann folgt für alle $n \geqq N$

$$q^n < \frac{1}{1+nh} < \varepsilon.$$

□

Definition 6.6 *Ist $(a_n)_{n\in\mathbb{N}}$ eine Folge rationaler Zahlen, so dass die Folge*

$$\begin{aligned} b_0 &= a_0 \\ b_1 &= a_0 + a_1 \\ b_2 &= a_0 + a_1 + a_2 \\ &\vdots \\ b_n &= \sum_{i=0}^{n} a_i \end{aligned}$$

gegen den Grenzwert b konvergiert, dann sagen wir, die unendliche Reihe $\sum_{n=0}^{\infty} a_n$ konvergiert gegen b und schreiben kurz

$$\sum_{n=0}^{\infty} a_n = b.$$

Also heißt $\sum_{n=0}^{\infty} a_n = b$ einfach $\lim_{N\to\infty} \big(\sum_{n=0}^{N} a_n \big) = b$.

Satz 6.7 *Es sei $q \in \mathbb{Q}$ mit $|q| < 1$. Dann konvergiert die unendliche Reihe $\sum_{n=0}^{\infty} q^n$ und es gilt*

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

Wir nennen $\sum_{n=0}^{\infty} q^n$ auch „geometrische Reihe“.

Beweis : Wir müssen zeigen, dass die Folge der Partialsummen

$$\big(\sum_{n=0}^{N} q^n\big)_{N\in\mathbb{N}} \text{ gegen } \frac{1}{1-q} \text{ konvergiert.}$$

Aus den Übungen wissen wir

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

Da $|q| < 1$ ist, gilt nach Lemma 6.3 $\lim_{N\to\infty} q^N = 0$, also gilt auch $\lim_{N\to\infty} q^{N+1} = 0$ nach Lemma 6.2 i). Aus Lemma 6.2 folgt außerdem

$$\lim_{N\to\infty} \frac{1-q^{N+1}}{1-q} = \frac{1}{1-q}$$

und damit unsere Behauptung. □

Korollar 6.8 *Es sei b eine natürliche Zahl mit den Ziffern $b_1 \dots b_k$ im Dezimalsystem, das heißt, es gilt*

$$b = b_1 10^{k-1} + b_2 10^{k-2} + \dots b_{k-1}10 + b_k.$$

Dann konvergiert die unendliche Reihe

$$10^{-k}b + 10^{-2k}b + 10^{-3k}b + \dots = \sum_{n=1}^{\infty} 10^{-kn}b$$

Beweis : Nach Satz 6.5 konvergiert

$$\sum_{n=0}^{\infty} (10^{-k})^n = \frac{1}{1-10^{-k}}$$

als geometrische Reihe. Also konvergiert nach Lemma 6.2 auch

$$\sum_{n=1}^{\infty} 10^{-kn} = \big(\sum_{n=0}^{\infty} \big(10^{-k}\big)^n\big) - 1,$$

und damit (wieder nach Lemma 6.2) auch die Reihe

$$b\sum_{n=1}^{\infty} 10^{-kn} = \sum_{n=1}^{\infty} 10^{-kn} b.$$

□

Dieses Korollar besagt, dass die Folge der Partialsummen

$$10^{-k}b + 10^{-2k}b + \ldots + 10^{-mk}b$$

für $m \to \infty$ einen Grenzwert in $\mathbb{Q}$ hat. Schreiben wir diese Folge mit Dezimalziffern, so sieht sie so aus:

$$0, \underbrace{b_1 b_2 \ldots b_k}\underbrace{b_1 b_2 \ldots b_k}_{m \text{ mal}} \ldots \underbrace{b_1 b_2 \ldots b_k}$$

Also macht folgende Definition Sinn:

Definition 6.9 *Sind $b_1, \ldots, b_k \in \{0, 1, \ldots, 9\}$ Ziffern, so ist der periodische Dezimalbruch*

$$0, \overline{b_1 b_2 \ldots b_k}$$

definiert als $\sum_{n=1}^{\infty} 10^{-kn}(b_1 10^{k-1} + \ldots + b_{k-1}10 + b_k)$. Dies ist eine rationale Zahl.

Mit dieser Definition von periodischen Dezimalbrüchen versteht man auch, wieso $0, \overline{9} = 1$ ist (Übungsaufgabe). Hier wird in Schulbüchern immer gemogelt.

Man kann umgekehrt auch zeigen, dass sich jede rationale Zahl q schreiben lässt als

$$q = m \cdot 10^d + p,$$

wobei $m \in \mathbb{Z}, d \in \mathbb{Z}$ und p ein periodischer Dezimalbruch wie in Definition 6.9 ist.

So gilt etwa $\frac{1}{2} = 5 \cdot 10^{-1} + 0$ oder $13\frac{1}{3} = 13 \cdot 1 + 0, \overline{3}$.

7 Reelle Zahlen

Wir wollen nun die rationalen Zahlen erweitern zu den reellen Zahlen, indem wir Grenzwerte gewisser Folgen hinzunehmen. Dazu betrachten wir zunächst folgendes Beispiel.

Beispiel: Die Folge $\left((-1)^n\right)_{n\in\mathbb{N}}$ hat keinen Grenzwert. Ist nämlich $a \in \mathbb{Q}$ eine rationale Zahl mit

$$|a-1| < 1 =: \varepsilon,$$

so folgt

$$\begin{aligned} 2 = |-1-1| &= |(a-1)-(a+1)| \\ &< 1+|a+1| \end{aligned}$$

nach der Dreiecksungleichung, also muss $|a-(-1)| = |a+1| > 1$ sein. Damit können nicht alle bis auf endlich viele Folgenglieder in $U_1(a)$ liegen.

Das letzte Beispiel motiviert folgendes Lemma:

Lemma 7.1 *Es sei $(a_n)_{n\in\mathbb{N}}$ eine rationale Folge, die gegen $a \in \mathbb{Q}$ konvergiert. Dann gibt es für jedes $\varepsilon > 0$ ein $N \in \mathbb{N}$, so dass für beliebige $n \geqq N$ und $m \geqq N$ gilt*

$$|a_n - a_m| < \varepsilon.$$

Die Folgenglieder einer konvergenten Folge kommen also „beliebig nahe zusammen“.

Beweis : Nach Voraussetzung gilt $\lim\limits_{n\to\infty} a_n = a$. Für jedes $\varepsilon > 0$ gibt es also ein $N \in \mathbb{N}$ mit

$$|a_n - a| < \frac{\varepsilon}{2} \text{ für alle } n \geqq N.$$

(Wieso wir hier $\frac{\varepsilon}{2}$ und nicht ε nehmen, erfährt man erst am Beweisende.)

Nach der Dreiecksungleichung gilt für beliebige $n \geqq N$ und $m \geqq N$

$$\begin{aligned} |a_n - a_m| &= |(a_n - a) + (a - a_m)| \\ &\leqq |a_n - a| + |a - a_m| \\ &= |a - a_n| + |a - a_m| \\ &< \tfrac{\varepsilon}{2} + \tfrac{\varepsilon}{2} = \varepsilon. \end{aligned}$$

□

Definition 7.2 *Eine rationale Folge $(a_n)_{n\geqq N}$ heißt Cauchyfolge, falls es für jedes $\varepsilon > 0$ ein $N \in \mathbb{N}$ gibt, so dass für alle $n \geqq N$ und $m \geqq N$ gilt*

$$|a_n - a_m| < \varepsilon.$$

Lemma 7.1 besagt also, dass jede konvergente Folge in $\mathbb{Q}$ eine Cauchyfolge ist. Wir wollen nun zeigen, dass die Umkehrung in den rationalen Zahlen nicht gilt.

Wir definieren dafür rekursiv eine Folge $(x_k)_{k\in\mathbb{N}}$ in $\mathbb{Q}$, indem wir mit

$$x_1 = 1$$

anfangen, und für gegebenes x_n das nächste Folgenglied als

$$x_{n+1} = \frac{x_n^2 + 2}{2x_n}$$

definieren. Dann ist

$$\left|x_{n+1} - x_n\right| = \left|\frac{x_n^2+2}{2x_n} - \frac{2x_n^2}{2x_n}\right| = \left|\frac{2-x_n^2}{2x_n}\right|.$$

Mit vollständiger Induktion nach n zeigt man

$$\left|\frac{2-x_n^2}{2x_n}\right| \leqq 2^{-n} \text{ (Übungsaufgabe)},$$

also folgt $|x_{n+1} - x_n| \leqq 2^{-n} (*)$.

Sei nun $\varepsilon > 0$. Da die geometrische Reihe $\sum\limits_{n=0}^{\infty} 2^{-n} = \frac{1}{1-\frac{1}{2}} = 2$ konvergiert, gibt es ein $N \in \mathbb{N}$, so dass

$$\left|2 - \sum_{n=0}^{N} 2^{-n}\right| < \varepsilon$$

gilt. Daraus folgt für alle $k \geqq l \geqq N+1$

$$\begin{aligned}
& |x_k - x_l| \\
= \;& |(x_k - x_{k-1}) + (x_{k-1} - x_{k-2}) + \ldots + (x_{l+1} - x_l)| \\
\leqq \;& |x_k - x_{k-1}| + |x_{k-1} - x_{k-2}| + \ldots + |x_{l-1} - x_l| \\
\overset{(*)}{\leqq} \;& 2^{-(k-1)} + 2^{-(k-2)} + \ldots + 2^{-l} \\
\leqq \;& 2 - \sum_{k=0}^{N} 2^{-n} \text{ (alle } 2^{-n} \text{ sind positiv)} \\
< \;& \varepsilon.
\end{aligned}$$

Daher ist $(x_n)_{n\in\mathbb{N}}$ eine Cauchyfolge. Angenommen $(x_n)_{n\in\mathbb{N}}$ konvergiert gegen ein $x \in \mathbb{Q}$. Dann konvergiert auch die Folge $(x_{n+1})_{n\in\mathbb{N}}$ gegen x (Ist Ihnen das klar?).

Also folgt aus Lemma 6.2 und der Tatsache, dass $x_{n+1} = \frac{x_n^2+2}{2x_n}$ ist,

$$x = \frac{x^2+2}{2x},$$

woraus wir $x^2 = 2$ schließen. Diese Gleichung hat aber keine Lösung in den rationalen Zahlen! Dies kann man etwa so einsehen: Angenommen $x = \frac{m}{n} \in \mathbb{Z}$ erfüllt $x^2 = 2$. Wir können nach Kürzen annehmen, dass m und n nicht beide durch 2 teilbar sind. Dann folgt

$$m^2 = 2n^2.$$

Also ist m^2 eine gerade Zahl, damit ist aber auch m gerade, d.h. beide Seiten der Gleichung sind durch 4 teilbar. Das geht nicht, da wir angenommen haben, dass 2 kein Teiler von n ist.

Somit haben wir eine Cauchyfolge $(x_n)_{n\in\mathbb{N}}$ in $\mathbb{Q}$ gefunden, die nicht gegen eine rationale Zahl konvergiert.

Wir wollen jetzt die reellen Zahlen definieren, indem wir zu den rationalen Zahlen alle möglichen Grenzwerte von Cauchyfolgen hinzunehmen.

Definition 7.3 *Zwei Cauchyfolgen $(a_n)_{n\in\mathbb{N}}$ und $(b_n)_{n\in\mathbb{N}}$ in $\mathbb{Q}$ heißen äquivalent und wir schreiben $(a_n)_{n\in\mathbb{N}} \sim (b_n)_{n\in\mathbb{N}}$, falls die Folge $(a_n - b_n)_{n\in\mathbb{N}}$ gegen 0 konvergiert.*

Das definiert eine Äquivalenzrelation (Übungsaufgabe).

Definition 7.4 *Die Menge $\mathbb{R}$ der reellen Zahlen ist definiert als die Menge aller Äquivalenzklassen von Cauchyfolgen in $\mathbb{Q}$.*

Natürlich sollte $\mathbb{Q}$ eine Teilmenge von $\mathbb{R}$ sein. Dazu betrachten wir für jedes $q \in \mathbb{Q}$ die Äquivalenzklasse $i(q)$ der konstanten Folge $a_n = q$ für alle $n \in \mathbb{N}$.

Die Abbildung $i : \mathbb{Q} \to \mathbb{R}$ ist injektiv (Übungsaufgabe).

Jetzt definieren wir eine Addition und eine Multiplikation auf $\mathbb{R}$ durch

$$[(a_n)_{n\in\mathbb{N}}] + [(b_n)_{n\in\mathbb{N}}] = [(a_n + b_n)_{n\in\mathbb{N}}]$$

und

$$[(a_n)_{n\in\mathbb{N}}] \cdot [(b_n)_{n\in\mathbb{N}}] = [(a_n \cdot b_n)_{n\in\mathbb{N}}].$$

Hier muss man wieder nachprüfen, dass diese Definition unabhängig von der Wahl der Vertreter $(a_n)_{n\in\mathbb{N}}$ und $(b_n)_{n\in\mathbb{N}}$ der Äquivalenzklassen $[(a_n)_{n\in\mathbb{N}}]$ und $[(b_n)_{n\in\mathbb{N}}]$ ist.

Außerdem muss man prüfen, dass sowohl $(a_n + b_n)_{n\in\mathbb{N}}$ als auch $(a_n \cdot b_n)_{n\in\mathbb{N}}$ ebenfalls Cauchyfolgen sind (Übungsaufgabe).

Ferner definieren wir für $x = [(a_n)_{n\in\mathbb{N}}]$ und $y = [(b_n)_{n\in\mathbb{N}}]$, dass $x < y$ genau dann gilt, wenn es ein $c \in \mathbb{Q}$ mit $c > 0$ und ein $N \in \mathbb{N}$ gibt, so dass

$$a_n + c \leqq b_n$$

gilt für alle $n \geqq N$.

Es reicht hier nicht, für alle $n \geqq N$ die Ungleichung $a_n < b_n$ zu fordern, wie das Beispiel der Cauchyfolgenklassen $[(\frac{1}{n^2})_{n\in\mathbb{N}}] = [(\frac{1}{n})_{n\in\mathbb{N}})]$ zeigt.

Wir haben in letzten Kapitel bereits gesehen, dass die rekursiv definierte Folge

$$\begin{aligned} x_1 &= 1 \\ x_{n+1} &= \frac{x_n^2+2}{2x_n} = \frac{1}{2}(x_n + \frac{2}{x_n}) \end{aligned}$$

eine Cauchyfolge in $\mathbb{Q}$ ist. Ihre Klasse $x = [(x_n)_{n\in\mathbb{N}}]$ hat die Eigenschaft, dass $x^2 = 2$ gilt, denn man kann leicht nachprüfen, dass $(2-x_n^2)_{n\in\mathbb{N}}$ gegen Null konvergiert. Also ist x eine positive reelle Zahl mit $x^2 = 2$. Wir nennen $x = \sqrt{2}$. Analog definieren wir für jedes $r \in \mathbb{Q}, r > 0$ rekursiv eine Folge durch

$$\begin{aligned} x_1 &\quad \text{beliebig mit } x_1^2 > r \\ x_{n+1} &= \frac{1}{2}(x_n + \frac{r}{x_n}). \end{aligned}$$

Dann ist $(x_n)_{n\in\mathbb{N}}$ eine Cauchyfolge in $\mathbb{Q}$ und die reelle Zahl $x = [(x_n)_{n\in\mathbb{N}}]$ erfüllt $x^2 = r$. Wir schreiben $x = \sqrt{r}$.

Satz 7.5 *i) Die Menge $\mathbb{R}$ zusammen mit der oben definierten Addition und Multiplikation ist ein Körper im Sinne von Definition 5.6.*

ii) Die Aussagen ii) - vi) aus Lemma 5.8 gelten auch für reelle Zahlen.

Beweis :

i) Wir zeigen hier nur die Existenz eines Inversen bezüglich der Multiplikation. Sei also $x = [(a_n)_{n\in\mathbb{N}}]$ eine Äquivalenzklasse von Cauchyfolgen mit $x \neq 0$. Dann konvergiert $(a_n)_{n\in\mathbb{N}}$ nicht gegen 0. Es gibt also ein $\varepsilon > 0$, so dass für unendlich viele k gilt

$$|a_k| \geq 2\varepsilon. \ (*)$$

(Wieso gilt das?) Da $(a_n)_{n\in\mathbb{N}}$ eine Cauchyfolge ist, gibt es ein $N \in \mathbb{N}$, so dass für alle $n, m \geqq N$ gilt

$$|a_n - a_m| < \varepsilon.$$

Unter den unendlich vielen k mit $|a_k| \geq \varepsilon$ finden wir ein $k_0 \geqq N$. Dann gilt für alle $n \geqq N$:

$$|a_n| > \varepsilon,$$

denn aus $|a_n| \leqq \varepsilon$ würde folgen

$$\begin{aligned} |a_{k_0}| &= |(a_{k_0} - a_n) + a_n| \\ &< |a_{k_0} - a_n| + |a_n| < 2\varepsilon \end{aligned}$$

im Widerspruch zu $(*)$.

Also ist insbesondere für jedes $n \geqq N$ das Folgenglied $a_n \neq 0$.

Wir definieren nun eine Folge b_n durch

$$b_n = \begin{cases} 1 & n < N \\ \frac{1}{a_n} & n \geqq N. \end{cases}$$

Da $\left|\frac{1}{a_n} - \frac{1}{a_m}\right| = \left|\frac{a_m - a_n}{a_n a_m}\right| < \frac{|a_m - a_n|}{2\varepsilon}$ gilt für $n, m \geqq N$, kann man leicht nachweisen, dass auch $(b_n)_{n\in\mathbb{N}}$ eine Cauchyfolge ist. Das Produkt $(a_n \cdot b_n)_{n\in\mathbb{N}}$ ist die Folge $a_1, a_2, \ldots, a_{N-1}, 1, 1, 1, \ldots$. Diese ist offenbar äquivalent zur konstanten Folge 1. Also gilt

$$[(a_n)_{n\in\mathbb{N}}] \cdot [(b_n)_{n\in\mathbb{N}}] = 1.$$

Den Rest der Rechengesetze auf den reellen Zahlen lassen wir als Übungsaufgabe.

ii) Wir zeigen nun folgende Aussage aus Lemma 5.8:

Für $x, y \in \mathbb{R}$ gilt entweder $x < y$ oder $x = y$ oder $x > y$.

Den Rest der Aussagen lassen wir als Übungsaufgabe.

Also seien $x = [(a_n)_{n\in\mathbb{N}}]$ und $y = [(b_n)_{n\in\mathbb{N}}]$ zwei Klassen von Cauchyfolgen mit $x \neq y$. Dann konvergiert definitionsgemäß die Folge $(a_n - b_n)_{n\in\mathbb{N}}$ nicht gegen 0. Also gibt es ein $\varepsilon > 0$, so dass für unendlich viele $k \in \mathbb{N}$ gilt

$$|a_k - b_k| > \varepsilon.$$

Da $(a_n)_{n\in\mathbb{N}}$ und $(b_n)_{n\in\mathbb{N}}$ Cauchyfolgen sind, finden wir ein $N \in \mathbb{N}$, so dass für alle $n, m \geqq N$ gilt $|a_n - a_m| < \varepsilon/3$ und $|b_n - b_m| < \varepsilon/3$. Es gibt ferner ein $k_0 \geqq N$ mit

$$|a_{k_0} - b_{k_0}| > \varepsilon.$$

Falls $a_{k_0} > b_{k_0}$ ist, so ist also

$$a_{k_0} > b_{k_0} + \varepsilon.$$

Dann gilt aber auch

$$a_n \geqq b_n + \varepsilon/3$$

für alle $n \geqq N$, denn aus $a_n < b_n + \varepsilon/3$ würde $|a_n - b_n| \leqq \varepsilon/3$, also

$$\begin{aligned} |a_{k_0} - b_{k_0}| &= |(a_{k_0} - a_n) + (a_n - b_n) + (b_n - b_{k_0})| \\ &\leqq |a_{k_0} - a_n| + |a_n - b_n| + |b_n - b_{k_0}| \\ &< \varepsilon/3 + \varepsilon/3 + \varepsilon/3 \\ &= \varepsilon \end{aligned}$$

folgen. Somit ist $[(a_n)_{n\in\mathbb{N}}] > [(b_n)_{n\in\mathbb{N}}]$. Gilt umgekehrt $a_{k_0} < b_{k_0}$, so folgt mit demselben Argument $[(a_n)_{n\in\mathbb{N}}] < [(b_n)_{n\in\mathbb{N}}]$.

□

Satz 7.6 *Die Menge $\mathbb{R}$ der reellen Zahlen ist vollständig. Das bedeutet: Jede Cauchyfolge $(a_n)_{n\in\mathbb{N}}$ mit $a_n \in \mathbb{R}$ hat einen Grenzwert in $\mathbb{R}$.*

Diesen Satz können wir hier leider nicht beweisen, dafür muss man mit Folgen von Folgen arbeiten.

Nun sehen wir auch, warum jeder Dezimalbruch

$$0, b_1 b_2 b_3 \ldots$$

mit unendlich vielen Ziffern b_i eine reelle Zahl ist: Die Folge

$$(0, b_1 b_2 \ldots b_n)_{n\in\mathbb{N}}$$

aus $\mathbb{Q}$ ist eine Cauchyfolge. Also ist ihre Klasse eine reelle Zahl. Diese ist gerade der unendliche Dezimalbruch $0, b_1 b_2 b_3 \ldots$.

8 Polynome

Definition 8.1 *Es sei K ein Körper, zum Beispiel $K = \mathbb{R}$. Dann ist ein Polynom über K eine formale Summe der Form*

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

mit $a_0, \ldots, a_n \in K$. Ist $a_n \neq 0$, so heißt $n = \text{grad}\,(p)$ der Grad des Polynoms.

„Formale Summe“ heißt hier, dass wir formal rechnen und nach $X-$Potenzen sortieren, ohne über die Bedeutung von $a \cdot X^n$ nachzudenken.

Wir addieren Polynome daher auch formal: Ist $n \geqq m$, so setzen wir

$$(a_n X^n + a_{n-1}X^{n-1} + \ldots + a_1 X + a_0) + (b_m X^m + b_{m-1}X^{m-1} + \ldots + b_1 X + b_0)$$

$$= (a_n + b_n)X^n + (a_{n-1} + b_{n-1})X^{n-1} + \ldots + (a_1 + b_1)X + (a_0 + b_0),$$

wobei wir $b_{m+1} = \ldots = b_n = 0$ setzen.

Außerdem definieren wir (durch formales Ausmultiplizieren)

$$(a_n X^n + a_{n-1}X^{n-1} + \ldots + a_0)(b_m X^m + b_{m-1}X^{m-1} + \ldots + b_0) = \sum_{k=0}^{n+m} X^k \Big(\sum_{i+j=k} a_i b_j \Big).$$

Beispiel:

i) $(5X^3 + 3X^2 + 1) + (2X^2 + 5X + 4) = 5X^3 + 5X^2 + 5X + 5$

ii) $(3X^2 + 2X + 1)(4X - 2) = 12X^3 + 2X^2 - 2.$

Wir bezeichnen die Menge aller Polynome über K mit $K[X]$. Dann gilt

Satz 8.2 *$K[X]$ zusammen mit der oben definierten Addition und Multiplikation ist ein Ring im Sinne von Definition 5.6. Der Polynomring $K[X]$ enthält den Körper K als Menge der konstanten Polynome.*

Beweis : Übungsaufgabe. □

Genau wie für ganze Zahlen kann man eine Teilbarkeitsbeziehung für Polynome einführen. Sind $p(X)$ und $q(X) \in K[X]$, so sagen wir $p(X)$ teilt $q(X)$ $\big($und schreiben $p(X) \mid q(X)\big)$, falls es ein Polynom $t(X) \in K[X]$ gibt mit

$$p(X)t(X) = q(X).$$

Genau wie bei ganzen Zahlen gibt es eine Division mit Rest:

Satz 8.3 *Es sei $f(X) \in K[X]$ ein Polynom $\neq 0$, das heißt $f(X) = a_n X^n + \ldots + a_0$ mit mindestens einem $a_i \neq 0$.*

Dann gibt es für jedes Polynom $p(X) \in K[X]$ eindeutig bestimmte Polynome $q(X)$ und $r(X)$, so dass grad $r(X) <$ grad $f(X)$ und $p(X) = q(X)f(X) + r(X)$ gilt.

Man kann $q(X)$ und $r(X)$ durch Polynomdivision ermitteln.

Beispiel: Es sei $f(X) = X^2 + 1$ und $p(X) = 2X^5 - 2X + 3$.

Dann rechnen wir

$$\begin{aligned} p(X) &= 2X^3(X^2+1) - 2X^3 - 2X + 3 \\ &= 2X^3(X^2+1) - 2X(X^2+1) + 3 \\ &= (2X^3 - 2X)(X^2+1) + 3. \end{aligned}$$

Hier ist also $r(X) = 3$ und $q(X) = 2X^3 - 2X$.

Bisher waren Polynome für uns formale Summen, jetzt werden wir Polynomfunktionen definieren.

Es sei $c \in K$. Dann definieren wir eine Funktion

$$\lambda_c : K[X] \longrightarrow K$$

durch

$$a_n X^n + \ldots + a_1 X + a_0 \mapsto a_n c^n + \ldots + a_1 c + a_0.$$

Wir setzen also für X die Zahl c ein und rechnen das Ergebnis im Körper K aus.

Lemma 8.4 *Es ist* $\lambda_c\big(p(X) + q(X)\big) = \lambda_c\big(p(X)\big) + \lambda_c\big(q(X)\big)$ *und* $\lambda_c\big(p(X) \cdot q(X)\big) = \lambda_c\big(p(X)\big) \cdot \lambda_c\big(q(X)\big)$.

Beweis : Übungsaufgabe. □

Wir schreiben in Zukunft einfach

$$p(c) := \lambda_c\big(p(X)\big).$$

Definition 8.5 *Eine Zahl $c \in K$ heißt Nullstelle des Polynoms $p(X)$, falls $p(c) = 0$ gilt.*

Satz 8.6 *$c \in K$ ist genau dann eine Nullstelle des Polynoms $p(X) \in K[X]$, wenn gilt*

$$(X - c) \mid p(X).$$

Beweis : Falls $(X - c)|p(X)$ gilt, so folgt $p(X) = (X - c) \cdot t(X)$ für ein $t(X) \in K[X]$. Nach Lemma 8.4 gilt dann $p(c) = (c - c)t(c) = 0$. Also ist c Nullstelle von $p(X)$.

Ist umgekehrt c Nullstelle von $p(X)$, so führen wir eine Division mit Rest von $p(X)$ durch $(X - c)$ durch. Wir finden also Polynome $q(X)$ und $r(X)$ mit grad $\big(r(X)\big) <$

grad $(X - c) = 1$ und $p(X) = (X - c)q(X) + r(X)$. Aus grad $r(X) < 1$ folgt aber, dass $r = a_0$ eine Konstante aus K sein muss. Wegen

$$\begin{aligned} p(c) &= (c - c)q(c) + a_0 \\ &= a_0 \end{aligned}$$

folgt $a_0 = 0$, denn c ist eine Nullstelle von $p(X)$. Also folgt $(X - c) \mid p(X)$. □

Satz 8.7 *Ein Polynom $p(X)$ vom Grad n hat höchstens n verschiedene Nullstellen in K.*

Beweis : Das zeigt man leicht mit Induktion nach n und Satz 8.6. □

Wie berechnen wir die Nullstellen von Polynomen? Das ist nur für sehr kleine Grade einfach.

Ein Polynom vom Grad 1 hat die Form

$$f(X) = a_1X + a_0 \text{ mit } a_1 \neq 0$$

Die einzige Nullstelle ist daher $c = -\frac{a_0}{a_1}$. Ein Polynom vom Grad 2 hat die Form

$$\begin{aligned} f(X) &= a_2X^2 + a_1X + a_0 \text{ mit } a_2 \neq 0 \\ &= a_2\big(X^2 + \tfrac{a_1}{a_2}X + \tfrac{a_0}{a_2}\big) \end{aligned}$$

Offenbar sind die Nullstellen von $f(X)$ dieselben wie die Nullstellen des normierten Polynoms

$$g(X) = X^2 + \frac{a_1}{a_2}X + \frac{a_0}{a_2}.$$

Lemma 8.8 *Setzen wir $p = \frac{a_1}{a_2}$ und $q = \frac{a_0}{a_2}$, so sind die Nullstellen von*

$$g(X) = X^2 + pX + q$$

gerade die reellen Zahlen

$$c_1 = -\frac{p}{2} + \sqrt{\frac{p^2}{4} - q} \text{ und } c_2 = -\frac{p}{2} - \sqrt{\frac{p^2}{4} - q},$$

falls $\frac{p^2}{4} - q \geqq 0$ ist.

Falls $\frac{p^2}{4} - q < 0$ ist, so hat $g(X)$ keine Nullstellen in $\mathbb{R}$ (Beispiel $g(X) = X^2 + 1$).

Beweis : Es gilt (mit quadratischer Ergänzung)

$$g(X) = X^2 + pX + q = \left(X + \frac{p}{2}\right)^2 + \left(q - \frac{p^2}{4}\right)$$

Ist $\frac{p^2}{4} - q < 0$, so ist $q - \frac{p^2}{4} > 0$. Da für alle $c \in \mathbb{R}$ das Quadrat $(c + \frac{p}{2})^2 \geqq 0$ ist, folgt $g(c) > 0$ für alle $c \in \mathbb{R}$. Also kann $g(X)$ keine Nullstelle haben.

Ist $\frac{p^2}{4} - q \geqq 0$, so existiert die reelle Zahl $\sqrt{\frac{p}{2} - q}$. Nun gilt für die reellen Zahlen c_1 und c_2 aus der Behauptung

$$(X - c_1)(X - c_2) = X^2 + pX + q,$$

wie man durch Ausmultiplizieren leicht nachprüft. Also sind c_1 und c_2 Nullstellen von $g(X)$. Ist $c_1 \neq c_2$, dann kann es nach Satz 8.7 keine weiteren Nullstellen von $g(X)$ geben. Ist $c_1 = c_2$, so folgt $\sqrt{\frac{p^2}{4} - q} = 0$, also $q - \frac{p^2}{4} = 0$ und somit $g(X) = (X + \frac{p}{2})^2$. Das hat offenbar nur die Nullstelle $-\frac{p}{2} = c_1 = c_2$. □

9 Konstruktion mit Zirkel und Lineal

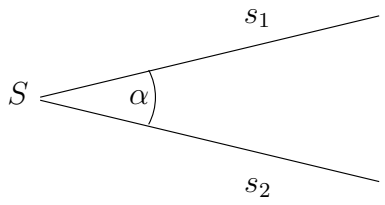
Wir werden nun einige elementare geometrische Konstruktionen wiederholen. Diese gehen auf die Mathematik des antiken Griechenlands zurück. Wegweisend waren hier Euklids „Elemente“ (um 300 v. Chr.), in denen erstmals ein axiomatischer Aufbau der Geometrie unternommen wurde. Euklids Darstellung war noch sehr an die Anschauung gebunden und erst über 2000 Jahre später hat sich ein völlig abstrakter Zugang etabliert. Wegweisend war hier David Hilbert (1862 - 1943): „Man muss jederzeit an Stelle von „Punkten, Geraden, Ebenen“ „Tische, Stühle, Bierseidel“ sagen können.“ In der Geometrie lernen Sie den Begriff eines euklidischen Vektorraums kennen, der Räume mit einer Strecken- und Winkelmessung an die Hand gibt, die Euklids Postulate erfüllen. Wir begnügen uns hier mit einer etwas fundierteren Wiederholung des Schulstoffs.

Wir arbeiten in der Ebene. Diese enthält Punkte und Geraden. Zwei verschiedene Punkte kann man durch eine eindeutig bestimmte Gerade verbinden. Wir untersuchen zunächst Konstruktionen mit Zirkel und Lineal.

Tatsache 9.1 *1) Zwei verschiedene Punkte P und Q definieren eine Strecke $\overline{PQ}$, die auf der eindeutig definierten Geraden durch P und Q liegt. Unser Lineal enthält keine*

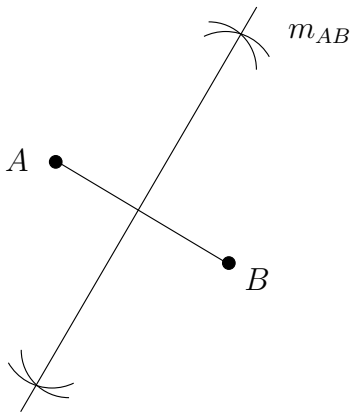
Meßskala, aber mit dem Zirkel können wir zumindest die Länge der Strecke $\overline{PQ}$ auf jede andere Gerade und jeden beliebigen Anfangspunkt übertragen. Auf diese Weise können wir Streckenlängen vervielfachen.

2) *Gegeben sei ein Winkel α mit Scheitelpunkt S und den Schenkeln s_1 und s_2.*



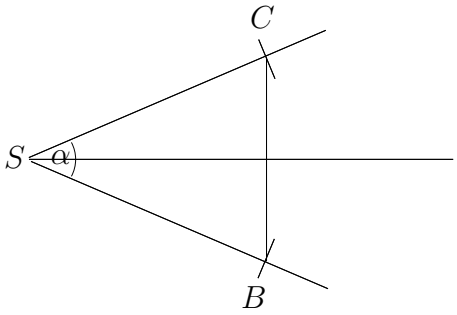
Dann können wir diesen Winkel an jeden anderen Punkt S' so abtragen, dass s_1 auf einer gegebenen Geraden durch S' liegt. Dazu schlagen wir einen Kreis k um S, der s_1 und s_2 in den Punkten A und B schneidet. Denselben Kreis k schlagen wir um S', nennen einen Schnittpunkt mit der Geraden A' und finden B', indem wir mit dem Zirkel die Strecke $\overline{AB}$ in A' so abtragen, dass der Endpunkt auf k liegt.

3) *Zu zwei Punkten A, B können wir die Mittelsenkrechte m_{AB} auf der Strecke $\overline{AB}$ konstruieren, indem wir zwei geeignete Kreise zeichnen (wie?):*



Auf diese Weise können wir Strecken halbieren.

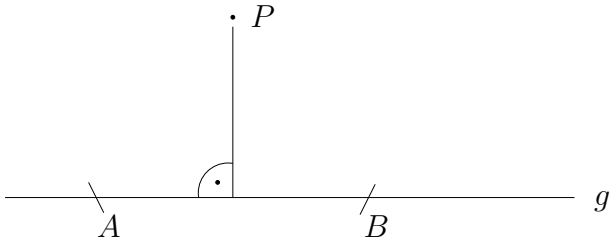
4) *Für einen Winkel α mit Scheitelpunkt S und Schenkeln s_1, s_2 können wir die Winkelhalbierende konstruieren:*



Wir schlagen zunächst einen Kreis um S, der s_1 und s_2 in B und C schneidet. Dann konstruieren wir die Mittelsenkrechte auf der Strecke $\overline{BC}$.

Achtung: Wir haben noch keine Messskala für Strecken und Winkel eingeführt, sondern können diese nur vergleichen, ohne ihre absoluten Werte zu bestimmen.

5) *Mit derselben Konstruktion wie in 3) können wir zu einer gegebenen Gerade g und einem Punkt P, der nicht auf g liegt, das Lot von P auf g fällen,*

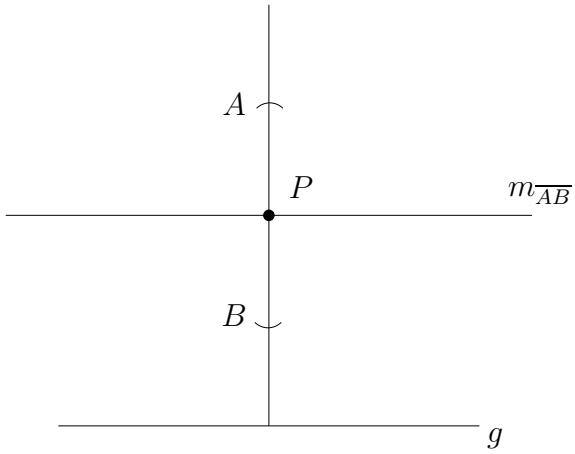


indem wir die Mittelsenkrechte zu $\overline{AB}$ konstruieren, wobei A und B die Schnittpunkte von g mit einem hinreichend großen Kreis um P sind.

Den Winkel, der zwischen A und P gebildet wird, nennen wir rechten Winkel und ordnen ihm die Maßzahl $90°$ (oder $\frac{\pi}{2}$ im Bogenmaß) zu.

6) *Zu jeder Gerade g und jedem Punkt P, der nicht auf g liegt, können wir eine Gerade h durch P konstruieren, die zu g parallel ist, also g nicht schneidet. Dass eine solche Gerade existiert und eindeutig bestimmt ist, folgt aus dem Euklidischen Parallelenaxiom.*

Dazu fällen wir zunächst von P das Lot auf g, schlagen einen Kreis um P, der das Lot in A und B schneidet und konstruieren die Mittelsenkrechte der Strecke $\overline{AB}$.



Aus der antiken Mathematik der Griechen sind drei klassische Konstruktionsprobleme überliefert.

1) **Deli'sches Problem:**

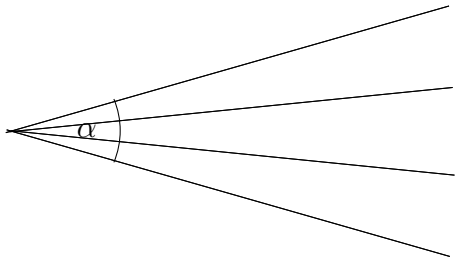
   Im 5. Jahrhundert v. Chr. verlangte das Orakel von Delphi von der Bevölkerung der Insel Delos als Gegenleistung für einen erteilten Ratschlag die Konstruktion eines Würfels, dessen Volumen das Doppelte eines gegebenen Würfels ist. Hat der gegebene Würfel die Kantenlänge s, so hat der gesuchte die Kantenlänge $\sqrt[3]{2}$ s (wieso?). Die Aufgabe läuft also darauf hinaus, das Verhältnis $\sqrt[3]{2}$ der beiden Strecken zueinander mit Zirkel und Lineal zu konstruieren.

2) **Die Quadratur des Kreises:**

   Hier geht es darum, aus einem gegebenen Kreis ein Quadrat mit demselben Flächeninhalt zu konstruieren. Ist r der Radius des Kreises, so ist dieser Flächeninhalt πr^2. Daher ist die Seitenlänge des gesuchten Quadrats $\sqrt{\pi} r$.

3) **Die Dreiteilung eines beliebigen Winkels:**

   Analog zur Winkelhalbierenden sind zwei Halbgeraden gesucht, die einen gegebenen Winkel α in drei gleiche Teile teilen:



Mit Methoden der Algebra kann man heute zeigen, dass die Probleme 1) und 2) unlösbar sind und dass Problem 3) nur für ganz spezielle Winkel funktioniert. Man zeigt zunächst, dass alle mit Zirkel und Lineal aus einer Einheitsstrecke konstruierbaren Streckenlängen einen Körper K bilden. Dann beweist man folgenden Satz.

Satz 9.2 *Jedes $\alpha \in K$ ist Nullstelle eines eindeutig bestimmten Primpolynoms $P(x) \in \mathbb{Q}[X]$, dessen Grad eine Zweierpotenz ist.*

Dabei heißt ein Polynom $P \in \mathbb{Q}[X]$ Primpolynom, falls es sich nicht als Produkt zweier Polynome in $\mathbb{Q}[X]$ mit echt kleinerem Grad schreiben lässt.

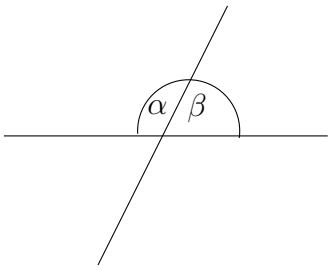
Da $\sqrt{\pi}$ transzendent ist (also nicht Nullstelle irgendeines Polynoms in $\mathbb{Q}[X]$), ist $\sqrt{\pi}$ nicht konstruierbar und damit die Quadratur des Kreises unmöglich. Da $x^3 - 2$ ein Primpolynom in $\mathbb{Q}[X]$ mit Nullstelle $\sqrt[3]{2}$ ist, ist auch das Delische Problem unlösbar, denn der Grad dieses Polynoms ist 3.

Aus der Dreiteilung eines Winkels α folgt die Konstruierbarkeit der Zahl $\cos \alpha/3$ aus der Konstruierbarkeit von $\cos(\alpha)$, das ist aber im allgemeinen nicht der Fall.

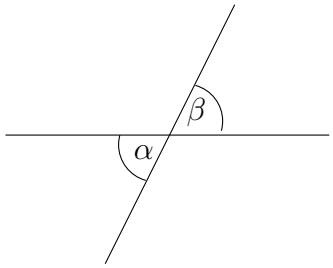
10 Dreiecke

An sich schneidenden Geraden treten Winkelpaare auf, für die wir folgende Bezeichnungen einführen.

Bei zwei Geraden:

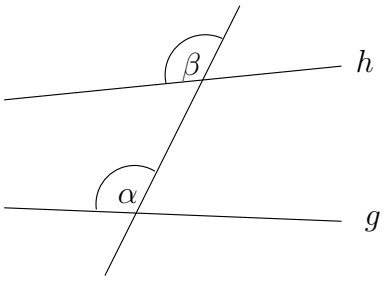


Nebenwinkel

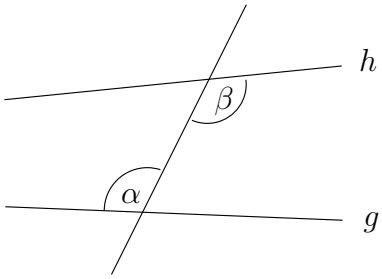


Scheitelwinkel

Bei drei Geraden:



Stufenwinkel



Wechselwinkel

Satz 10.1 *i) Die Summe zweier Nebenwinkel ist 180°.*

ii) Scheitelwinkel sind gleich.

iii) Sind die Geraden g und h parallel, so sind die Stufenwinkel α und β gleich.

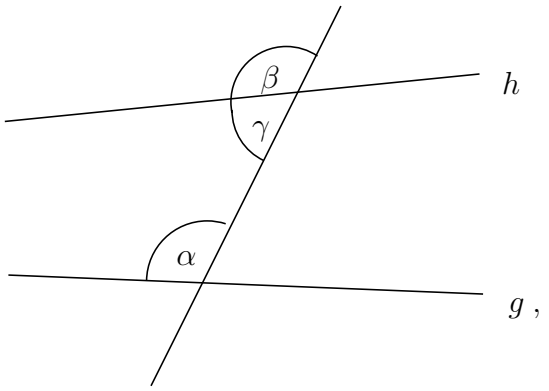
iv) Sind die Geraden g und h parallel, so sind die Wechselwinkel α und β gleich.

Beweis :

i) folgt aus der Definition.

ii) folgt aus i), denn α und β haben einen gemeinsamen Nebenwinkel.

iii) Hier brauchen wir Euklids Postulat V. Es besagt in der Situation



dass sich im Falle $\alpha + \gamma \neq 180°$ die Geraden g und h schneiden.

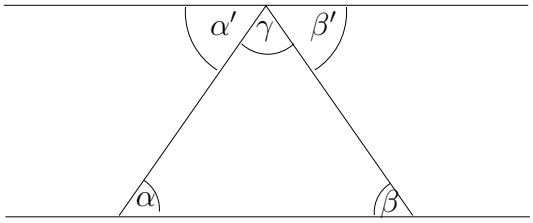
Da der Stufenwinkel β gerade der Nebenwinkel von γ ist, folgt die Behauptung (wie?).

iv) folgt aus i) und iii).

□

Satz 10.2 *Die Winkelsumme im Dreieck ist 180°.*

Beweis :



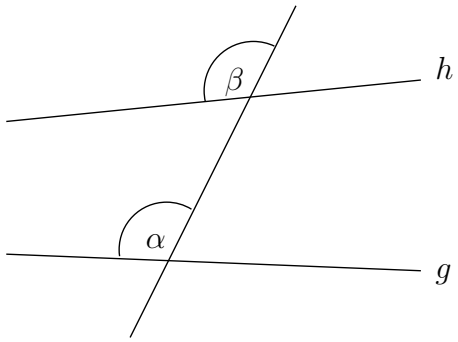
Mit dieser Skizze ist klar, wie die Behauptung aus Satz 10.1 folgt (Übungsaufgabe).
□

Korollar 10.3 *Es gilt die Umkehrung von Satz 10.1 iii) + iv):*

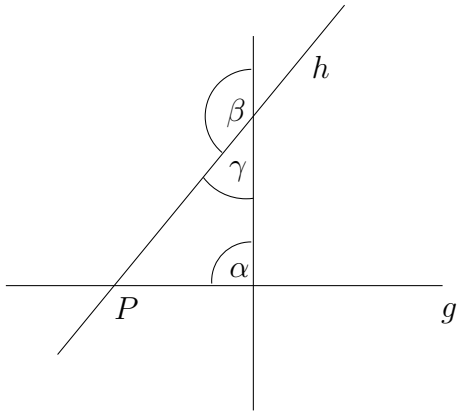
Sind zwei Stufenwinkel gleich, dann sind die anliegenden Geraden g und h parallel.

Sind zwei Wechselwinkel gleich, dann sind die anliegenden Geraden g und h parallel.

Beweis : Gegeben sei folgende Situation:



mit $\alpha = \beta$. Falls g und h nicht parallel sind, so schneiden sie sich in einem Punkt P. Ohne Einschränkung liegt dieser auf derselben Seite wie α und β, sonst ersetzen wir α und β durch ihre Nebenwinkel.



Dann erhalten wir

$$\begin{aligned} \alpha + \gamma &= \alpha + (180^\circ - \beta) \\ &= 180^\circ \text{ (wegen } \alpha = \beta) \end{aligned}$$

im Widerspruch zu Satz 10.2. □

Definition 10.4 *Zwei Dreiecke heißen kongruent, wenn sie durch eine längen- und winkeltreue Abbildung der Ebene ineinander überführt werden.*

(Solche Abbildungen kann man mit etwas mehr Arbeit genauer bestimmen.)

Satz 10.5 *Dreiecke sind bis auf Kongruenz eindeutig festgelegt durch*

- *drei Seitenlängen, wenn die Summe von je zweien größer ist als die dritte* (sss).
- *eine Seite und die beiden anliegenden Winkel, wenn deren Summe* $< \pi$ *ist* (wsw).

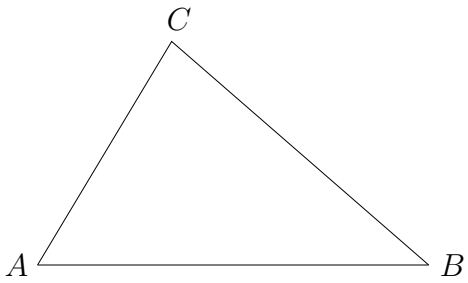
- *zwei Seiten und den eingeschlossenen Winkel* (sws).
- *zwei Seiten und den der größeren Seite gegenüberliegenden Winkel* (ssw).

Insbesondere folgt aus Satz 10.5, dass alle Seitenlängen und alle Winkel in zwei Dreiecken übereinstimmen, wenn dies für eine Konfiguration der Form $(sss), (wsw), (sws)$ oder (ssw) gilt.

Wir schreiben ab sofort $|AB|$ für die Länge der Strecke $\overline{AB}$. Die Bedingung für die (sss)-Kongruenz ergibt sich aus der sogenannten Dreiecksungleichung: Sind A, B, C Punkte in der Ebene, dann gilt

$$|AB| \leqq |AC| + |BC|,$$

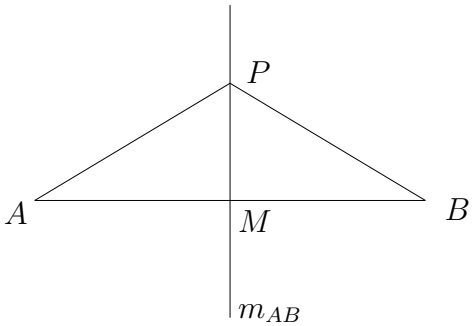
wobei sogar $|AB| < |AC| + |BC|$ gilt, falls C nicht auf der Strecke $\overline{AB}$ liegt.



Anschaulich gesprochen: Es ist ein Umweg, wenn man, um von A nach B zu kommen, über C geht.

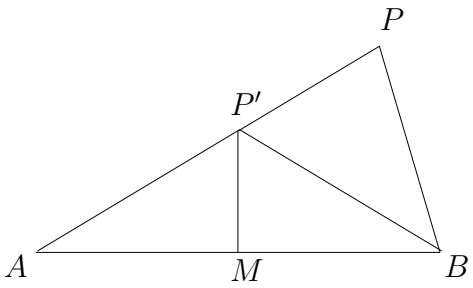
Satz 10.6 *Gegeben sei eine Strecke $\overline{AB}$. Ein Punkt P liegt genau dann auf der Mittelsenkrechten m_{AB}, wenn die Strecken $\overline{PA}$ und $\overline{PB}$ gleich lang sind, das heißt, wenn $|PA| = |PB|$ gilt.*

Beweis : Liegt P auf m_{AB}, so erhalten wir zwei Dreiecke:



Die beiden Dreiecke sind $(sws)-$kongruent, also ist die Seite $\overline{PA}$ genauso lang wie die Seite $\overline{PB}$.

Liegt P nicht auf m_{AB}, so ist ohne Einschränkung $P \neq A$ und $P \neq B$. Betrachten wir die Geraden g durch A und P und f durch B und P, so schneidet mindestens eine von ihnen m_{AB}, denn sie sind nicht parallel. Wir betrachten die Situation, in der g die Mittelsenkrechte m_{AB} in einem Punkt P' schneidet:



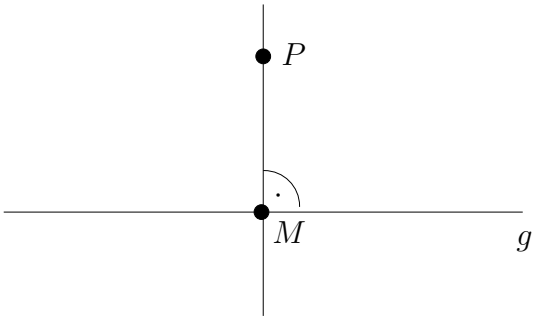
Nach Voraussetzung ist $P' \neq P$.

Da nach dem oben gezeigten $\overline{P'A}$ und $\overline{P'B}$ gleich lang sind, folgt

$$\begin{aligned} |PA| - |PB| &= |PP'| + |P'A| - |PB| \\ &= |PP'| + |P'B| - |PB| \\ &> 0 \text{ nach der Dreiecksungleichung.} \end{aligned}$$

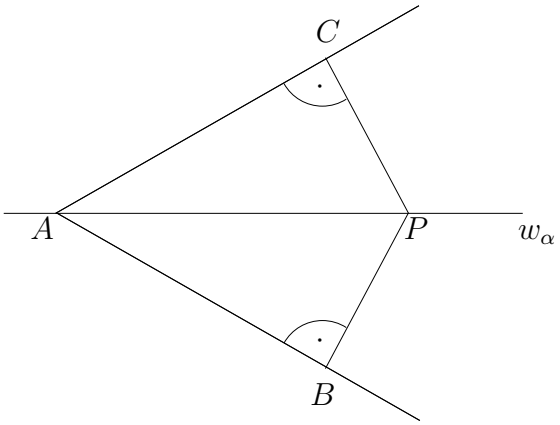
□

Definition 10.7 *Es sei g eine Gerade und P ein Punkt. Wir definieren den Abstand von P zu g als die Länge der Strecke $\overline{PM}$, wobei $M \in g$ der Fußpunkt des Lotes von P auf g ist:*

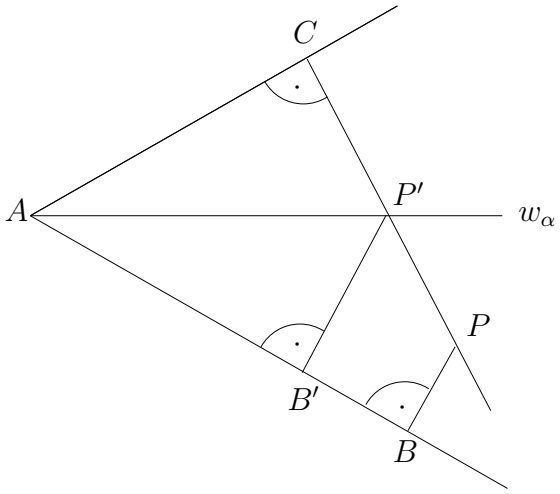


Satz 10.8 *Es sei P ein Punkt in dem Gebiet, das von den Schenkeln eines Winkels $\alpha < 180°$ begrenzt wird. Dann liegt P genau dann auf der Winkelhalbierenden w_α, wenn P von den beiden Schenkeln den gleichen Abstand hat.*

Beweis : Liegt P auf w_α, so sind die beiden Dreiecke in folgender Zeichnung $(wsw)-$kongruent:



Also sind die Strecken $\overline{PB}$ und $\overline{PC}$ gleich lang. Liegt P nicht auf w_α, dann haben wir ohne Einschränkung eine Situation wie in folgender Skizze mit P' auf w_α:

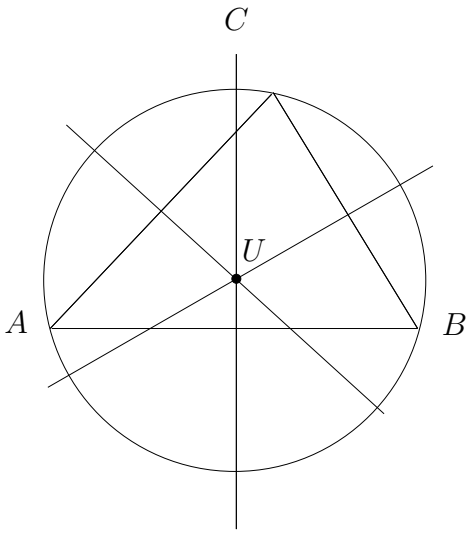


Nach dem oben gezeigten gilt $|P'C| = |P'B'|$. Also folgt

$$\begin{aligned} |PC| - |PB| &= |PP'| + |P'C| - |PB| \\ &= |PP'| + |P'B'| - |PB| \\ &\geq |PB'| - |PB| > 0 \end{aligned}$$

nach der Dreiecksungleichung. □

Satz 10.9 *Die drei Mittelsenkrechten der Seiten in einem Dreieck schneiden sich in einem Punkt U. Dies ist der Mittelpunkt des sogenannten Umkreises des Dreiecks, der alle drei Ecken des Dreiecks schneidet.*

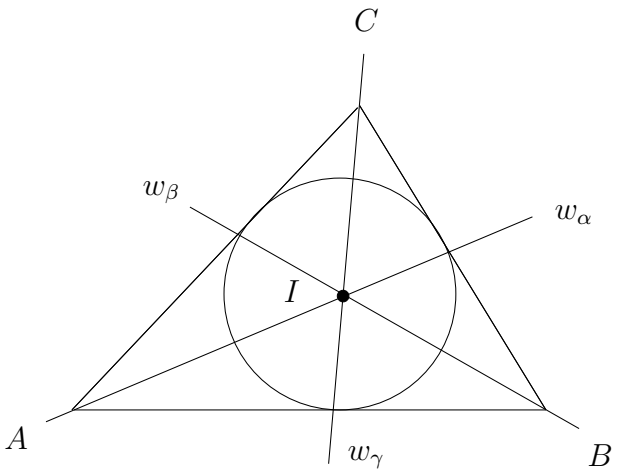


Beweis : Es seien A, B, C die Eckpunkte des Dreiecks. Wir betrachten die Mittelsenkrechten m_{AB} und m_{CA}. Diese sind nicht parallel, da A, B und C nicht auf einer

Geraden liegen. Also schneiden sich m_{AB} und m_{CA} in einem Punkt U. Nach Satz 10.6 gilt $|UA| = |UB|$ und $|UC| = |UA|$, woraus $|UB| = |UC|$ und damit wieder nach Satz 10.6 (in der anderen Richtung) $U \in m_{BC}$ folgt. Also schneiden sich tatsächlich alle drei Mittelsenkrechten im Punkt U. Da $|UA| = |UB| = |UC|$ ist, geht der Kreis um U mit Radius $|UA|$ durch alle drei Ecken des Dreiecks. □

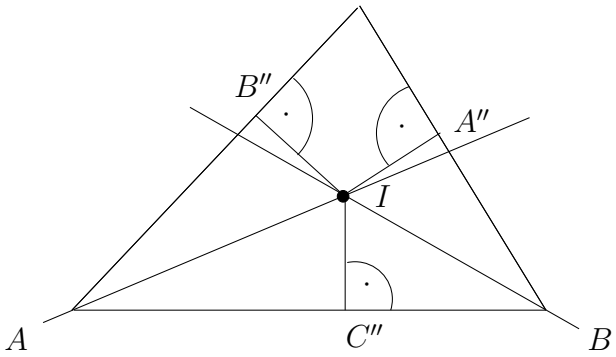
Achtung: Der Umkreismittelpunkt U muss nicht im Inneren des Dreiecks liegen. Dies ist nur für sogenannte spitzwinklige Dreiecks der Fall, in denen kein Winkel $\geqq 90°$ ist (Übungsaufgabe).

Satz 10.10 *Die drei Winkelhalbierenden in einem Dreieck schneiden sich in einem Punkt I. Dieser ist der Mittelpunkt des Inkreises des Dreiecks, der alle drei Seiten in genau einem Punkt berührt.*



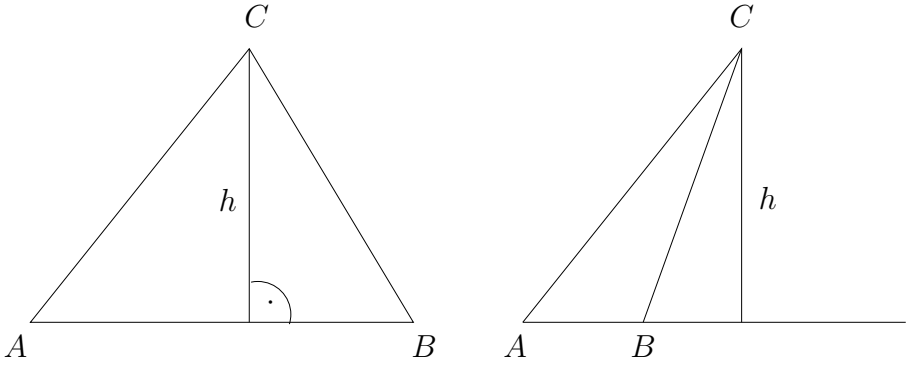
Beweis : Es seien α, β, γ die Winkel in den Ecken A, B, C des Dreiecks. Die Winkelhalbierenden w_α und w_β sind nicht parallel (Übungsaufgabe), also schneiden sie sich in einem Punkt I.

Es seien A'', B'' und C'' die Lotfußpunkte der drei Lote von I auf den Dreiecksseiten:



Dann folgt aus Satz 10.8 die Gleichung $|IB''| = |IC''|$, denn I liegt auf w_α, sowie $|IA''| = |IC''|$, denn I liegt auf w_β. Also ist auch $|IA''| = |IB''|$ und damit nach Satz 10.8 $I \in w_\gamma$. Also schneiden sich die drei Winkelhalbierenden in dem Punkt I. Schlagen wir um den Punkt I einen Kreis mit Radius $|IA''| = |IB''| = |IC''|$, so trifft dieser das Dreieck genau in A'', B'' und C''. □

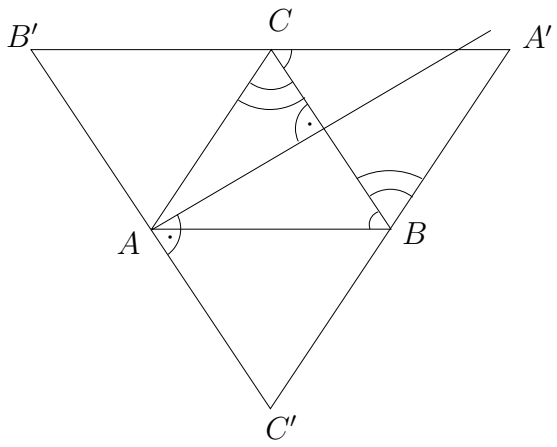
Definition 10.11 *In einem Dreieck heißt jedes der drei Lote von einem Eckpunkt zur Gerade durch die gegenüberliegende Seite eine Höhe des Dreiecks.*



Eine Höhe kann auch außerhalb des Dreiecks liegen.

Satz 10.12 *Die drei zur Gerade verlängerten Höhen in einem Dreieck schneiden sich in einem Punkt.*

Beweis : Wir konstruieren zu einem gegebenen Dreieck mit den Ecken A, B, C ein Dreieck mit den Ecken A', B', C', indem wir jeweils die Parallelen der Seiten durch den gegenüberliegenden Eckpunkt betrachten.



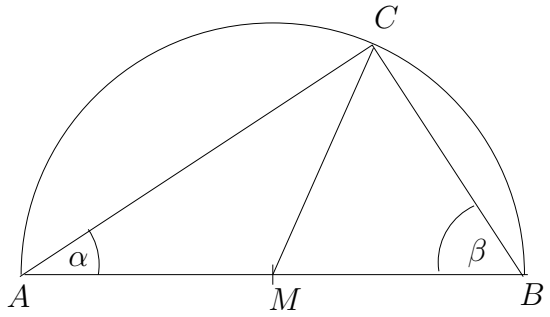
Dann ist das Dreieck ABC nach Satz 10.1 (wsw) kongruent zum Dreieck $A'BC$. Analog ist das Dreieck ABC kongruent zum Dreieck $B'AC$ und zum Dreieck ABC'. Also folgt $|B'C| = |AB| = |CA'|$. Somit ist C der Seitenmittelpunkt von $\overline{B'A'}$. Analog sind A und B die Seitenmittelpunkte der Strecken $\overline{B'C'}$ beziehungsweise $\overline{C'A'}$.

Daher liegen die Ecken des Ausgangsdreiecks ABC auf den Mittelsenkrechten des Dreiecks $A'B'C'$, und die Behauptung folgt aus Satz 10.9. □

Wir wollen jetzt noch einige bestimmte Sätze über rechtwinklige Dreiecke zeigen.

Satz 10.13 *(Satz des Thales) Liegt die Ecke C eines Dreiecks auf dem Halbkreis über der Strecke $\overline{AB}$, dann hat das Dreieck ABC in der Ecke C einen $90°-$Winkel.*

Beweis :



Nach Voraussetzung liegt C auf dem Kreis um den Seitenmittelpunkt M mit Radius $|MA| = |MB|$. Also gilt $|MC| = |MA| = |MB|$. Das Dreieck AMC ist also gleichschenklig, das heißt, es hat zwei gleich lange Seiten. Aus dem $(sws)-$Kongruenzsatz folgt, dass die Winkel dieses Dreiecks in den Ecken A und C gleich sind. Analog sind auch die Winkel des Dreiecks CMB in den Ecken C und B gleich.

Ist α der Winkel des Dreiecks ABC in A und β der Winkel in B, so ist der Winkel des Dreiecks ABC in C somit $\alpha + \beta$. Da die Winkelsumme im Dreieck $180°$ ist, folgt

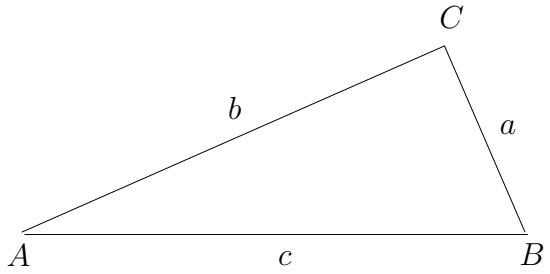
$$\begin{aligned} & \alpha + \beta + (\alpha + \beta) = 180°, \\ \text{also} \quad & \alpha + \beta = 90°. \end{aligned}$$

□

Wir wollen jetzt noch den berühmten Satz des Pythagoras behandeln. Wir nennen ein Dreieck rechtwinklig, falls einer seiner Winkel $90°$ beträgt. Die Seite, die diesem Winkel gegenüberliegt, heißt Hypothenuse, die beiden anderen Seiten heißen Katheten. Dann gilt

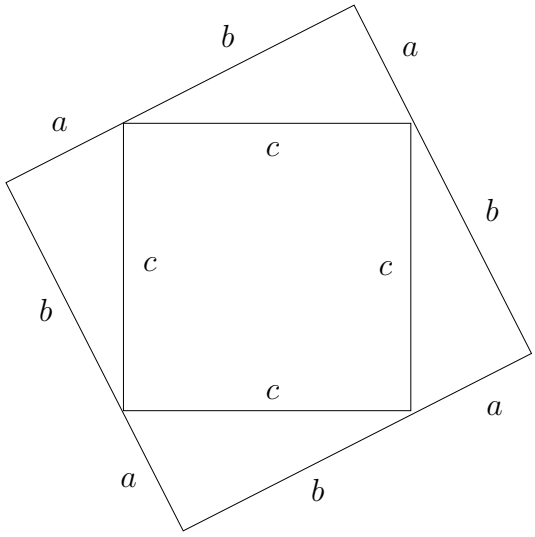
Satz 10.14 *(Satz des Pythagoras)*

In einem rechtwinkligen Dreieck ist das Quadrat der Hypothenusenlänge gleich der Summe der Quadrate der beiden Kathetenlängen.



In diesem Bild sind c die Hypothenusenlänge und a und b die Kathetenlängen, also gilt $c^2 = a^2 + b^2$.

Beweis : Wir betrachten in der Situation der Zeichnung ein Quadrat der Seitenlänge c und errichten über jeder Seite das gegebene Dreieck:

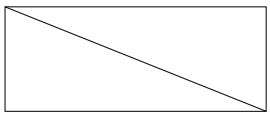


Da die Winkelsumme im Dreieck $180°$ beträgt, erhalten wir so ein Quadrat der Seitenlänge $a + b$. (Begründen Sie das!)

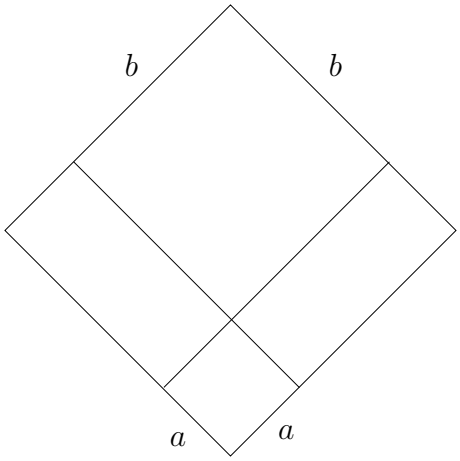
Setzen wir die Flächen zusammen, so ergibt sich

$$(a + b)^2 = c^2 + 4\frac{ab}{2},$$

denn der Flächeninhalt eines rechtwinkligen Dreiecks ist offenbar der halbe Flächeninhalt des von den Katheten aufgespannten Rechtecks

 .

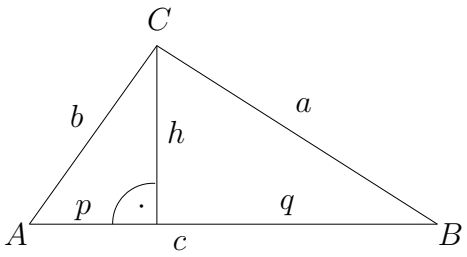
Nun können wir das Quadrat der Seitenlänge $a + b$ aber auch wie folgt unterteilen:



Also gilt auch $(a+b)^2 = a^2 + b^2 + 2ab$ (dazu hätten wir auch eine binomische Formel bemühen können).

Aus den beiden Ausdrücken für $(a+b)^2$ folgt $c^2 = a^2 + b^2$. □

Wir betrachten wieder ein rechtwinkliges Dreieck mit den Ecken ABC und der Höhe h auf die Hypothenuse:



Der Fußpunkt der Höhe teilt die Hypothenuse in zwei Abschnitte der Länge p und q. (Wieso liegt die Höhe h in dieser Situation im Dreieck ?)

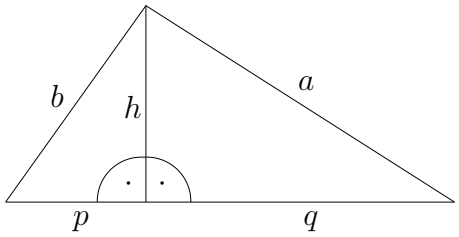
Dann gilt

Satz 10.15 *(Höhensatz)*
In einem rechtwinkligen Dreieck ist der Flächeninhalt des Quadrats über der Höhe auf die Hypothenuse gleich dem Flächeninhalt des Rechtecks aus den beiden Hypothenusenabschnitten.

Mit den Bezeichnungen aus obiger Skizze gilt also

$$h^2 = pq.$$

Beweis : Da die Höhe senkrecht auf der Hypothenuse steht, unterteilt sie das Ausgangsdreieck in zwei rechtwinklige Dreiecke. Auf beide wenden wir nun den Satz des Pythagoras an.



Also gilt $b^2 = h^2 + p^2$ und $a^2 = h^2 + q^2$. Wir addieren beide Formeln, verwenden den Satz des Pythagoras im großen Dreieck und erhalten

$$\begin{aligned} c^2 &= a^2 + b^2 \\ &= h^2 + q^2 + h^2 + p^2. \end{aligned}$$

Nun setzen wir $c = p + q$ ein. Das liefert

$$\begin{aligned} p^2 + 2pq + q^2 &= (p+q)^2 \\ &= c^2 \\ &= h^2 + q^2 + h^2 + p^2. \end{aligned}$$

Daraus folgt sofort $2pq = 2h^2$, also die gewünschte Relation

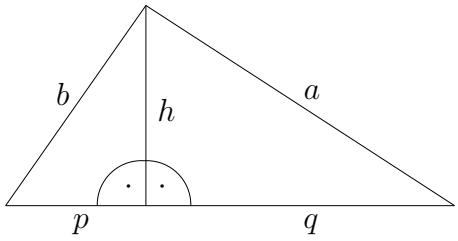
$$h^2 = pq.$$

□

Satz 10.16 *(Kathetensatz)*
In einem rechtwinkligen Dreieck ist der Flächeninhalt des Quadrates über einer Kathete gleich dem Flächeninhalt des Rechtecks aus der Hypothenuse und dem der Kathete anliegenden Hypothenusenabschnitt. Mit den Bezeichnungen aus unserer Skizze gilt also

$$a^2 = cq \text{ und } b^2 = cp.$$

Beweis : Wir wenden den Satz des Pythagoras auf das kleine Dreieck an, das als Hypothenuse eine der Katheten hat:



Betrachten wir die Kathete a, so erhalten wir

$$a^2 = h^2 + q^2.$$

Nach dem Höhensatz Satz 10.15 gilt

$$h^2 = pq,$$

das setzen wir ein und erhalten

$$\begin{aligned} a^2 &= h^2 + q^2 \\ &= pq + q^2 \\ &= q(p+q) \\ &= qc, \end{aligned}$$

wie behauptet.

Die Relation $b^2 = cp$ zeigt man analog. □