J. Wolfart WiSe 2006/07, überarbeitet 2011

Notizen zur Elementarmathematik I

Inhaltsverzeichnis

1 Mengen, Abbildungen, Äquivalenzrelationen

Natürliche Zahlen sind $1, 2, 3, \ldots$, zusammengefasst zur *Menge* $\mathbf{N}$ der *natürlichen Zahlen*. Viele Autoren zählen die 0 dazu, wir werden für die Menge dann $\mathbf{N}_0$ schreiben.
Rolle der natürlichen Zahlen bei der Beschreibung der Welt: Zählen, ordnen, messen, operieren (n Mal eine Handlung ausführen), Codieren (Telefonnummern), Rechnen (Algorithmen ausführen).

Beispiele für Gesetzmäßigkeiten in $\mathbf{N}$: Wenn $a < b$ und $b < c$, dann $a < c$ oder

$$a + b = b + a \quad , \quad a \cdot (b + c) = a \cdot b + a \cdot c \quad , \quad 1 \cdot a = a \, ,$$

jeweils zu verstehen als eine Aussage *für alle natürlichen Zahlen* a, b, c, kurz geschrieben $\forall a \in \mathbf{N}$, $\forall b \in \mathbf{N}$ .... Die mathematischen Kürzel heißen also $\forall$ *für alle*, $\in$ *Element von* oder *gehört zur Menge*.
Wie kommt man zu sochen Gesetzmäßigkeiten?

Erste Möglichkeit: konstruktiv, z.B. indem man natürliche Zahlen als *Mächtigkeit* (Größe, Elementanzahl) endlicher Mengen einführt, vornehmer: *endliche Kardinalzahlen*. Mengen stelle man sich naiv als Zusammenfassung verschiedener (endlich oder unendlich vieler) Elemente vor, z.B.

$$\{a_1, \ldots, a_n\} \quad , \quad \{ \text{ Geraden in der Ebene } \} \quad , \quad \{2, 3, 5, 7, 11, \ldots \text{ prim } \} \, ,$$

wo die Zusammenfassung der Elemente durch geschweifte Klammern { } angedeutet wird. Oft werden diese auch durch zusätzlich nachgestellte Bedingungen eingeschränkt wie z.B. in

$$\{3, 6, 9, 12, \ldots\} = \{n \in \mathbf{N} \mid n \text{ durch } 3 \text{ teilbar } \} \, .$$

Genauso naiv: Eine *Abbildung* einer Menge A in eine Menge B stelle man sich vor als eine Vorschrift $f : A \to B$, welche jedem $a \in A$ ein $b = f(a) \in B$ zuordnet, z.B. die Abbildung $f(x) := x^2$, welche jeder reellen Zahl x ihr Quadrat x^2 zuordnet („:=" bedeutet: die linke Seite ist durch die rechte Seite erklärt) oder

$$f : \mathbf{N} \to \mathbf{N} : n \mapsto f(n) := 2n \, ,$$

welche jede natürlichen Zahl auf die doppelte abbildet. Wie kann man jetzt die Mächtigkeit von Mengen definieren (ohne schon vorher über natürliche Zahlen zu reden)?

Definition 1.1 *Eine Abbildung $f : A \to B$ heißt „injektiv", wenn je zwei verschiedene Elemente von A auf verschiedene Elemente von B abgebildet werden, kurz wenn*

$$f(a_1) \neq f(a_2) \quad \forall a_1 \neq a_2 \in A \, .$$

f heißt „surjektiv", wenn jedes $b \in B$ als Bild unter f vorkommt, kurz

$$\forall b \in B \quad \exists a \in A \quad mit \quad f(a) = b$$

($\exists$ ist das logische Kürzel für „es gibt ein"). f heißt „bijektiv", wenn es zu jedem $b \in B$ „genau ein" $a \in A$ mit $f(a) = b$ gibt.

„Genau ein" ist Mathematikjargon für „eines, aber auch nicht mehr als eines". Im Fall einer bijektiven Abbildung kann man also eine eindeutige *Umkehrabbildung* $B \to A : b \mapsto a$ definieren, wobei $a \in A$ so auszuwählen ist, dass $f(a) = b$ ist.

Satz 1.1 *Die Abbildung $f : A \to B$ ist bijektiv genau dann, wenn sie injektiv und surjektiv ist. Ebenso: Sie ist bijektiv genau dann, wenn eine „Umkehrabbildung" $g : B \to A$ zu f existiert, d.h. mit der Eigenschaft $f(g(b)) = b \,\forall b \in B$ und $g(f(a)) = a \,\forall a \in A$.*

„Genau dann, wenn" (noch kürzer „⇔") ist schon wieder Mathematikjargon, hier für „wenn — aber auch nur dann, wenn" oder für unseren konkreten Fall etwas ausführlicher: „aus *bijektiv* folgt die Existenz einer Umkehrabbildung, und aus der Existenz der Umkehrabbildung folgt, dass f bijektiv ist".
Wenn eine *Bijektion*, d.h. eine bijektive Abbildung zwischen A und B existiert — Richtung egal, s.o. — nennen wir A und B *gleichmächtig*, geschrieben $|A| = |B|$. Anschaulich plausibel: Alle endlichen Mengen mit n Elementen sind gleichmächtig, wenn n eine feste natürliche Zahl ist. Und wenn man natürliche Zahlen noch nicht hat? Dann kann man, indem man alle endlichen gleichmächtigen Mengen miteinander identifiziert, über den so entstehenden Anzahlbegriff die natürlichen Zahlen einführen. Was heißt nun identifizieren?

Definition 1.2 *Für jedes Paar (a, b) von Elementen einer Menge A sei erklärt, ob die „Relation" $a \sim b$ gilt oder nicht. Diese Relation heißt eine „Äquivalenzrelation", wenn*

- *$a \sim a$ für alle $a \in A$ (Reflexivität),*
- *aus $a \sim b$ folgt $b \sim a$ für alle $a, b \in A$ (Symmetrie),*
- *aus $a \sim b$ und $b \sim c$ folgt $a \sim c$ für alle $a, b, c \in A$ (Transitivität).*

Äquivalenzrelationen sind z.B. die Gleichheit (auf beliebigen Mengen), Parallelität auf der Menge aller Geraden der Ebene oder des Raumes (wenn man vereinbart, dass jede Gerade auch zu sich selbst parallel ist), und eben die Gleichmächtigkeit von Mengen; Vorsicht: Die Menge aller Mengen, die man hier zugrundelegen müsste, existiert nicht, man muss also den Definitionsbereich der Relation geeignet einschränken.
Äquivalenzrelationen sind das richtige Instrument, Identifizierungen vorzunehmen; dazu setzen wir die Definition fort.

Definition 1.3 *Auf der Menge A sei die Äquivalenzrelation $\sim$ gegeben. Die Menge aller $b \in A$, welche zu a äquivalent sind, heißt die „Äquivalenzklasse" $[a]$ von a, und das Element a heißt „Repräsentant" von $[a]$.*

Aus dem nächsten Satz wird sogar folgen, dass jedes zu a äquivalente Element $b \sim a$ ebenfalls Repräsentant von $[a]$ ist. Äquivalenzklassen sind *Untermengen* (auch *Teilmengen* genannt, geschrieben $[a] \subseteq A$) von A — ein hoffentlich selbsterklärender Begriff.

Satz 1.2 *Auf der Menge A sei die Äquivalenzrelation $\sim$ gegeben. Zwei Äquivalenzklassen $[a]$ und $[c]$ stimmen entweder überein oder sie sind ,,disjunkt", d.h. haben kein Element gemeinsam.*

Letztere Möglichkeit wird durch $[a] \cap [c] = \emptyset$ ausgedrückt: Links steht der *Durchschnitt* der beiden Mengen, d.h.

$$\{\, b \in A \mid b \in [a] \quad \text{und} \quad b \in [c] \,\}\,,$$

rechts steht das Zeichen für die *leere Menge*, die kein Element enthält. Im Fall, dass $\sim$ die Gleichheit bedeutet, bestehen die Äquivalenzklassen einfach nur aus je einem Element, im Fall der Parallelität von Geraden bestehen die Äquivalenzklassen aus Parallelenscharen, und im Fall, dass $\sim$ durch die Existenz einer Bijektion definiert ist, bestehen Äquivalenzklassen gerade aus allen gleichmächtigen Mengen. Man könnte also 0 als Äquivalenzklasse der leeren Menge, 1 als Äquivalenzklasse aller einelementigen Mengen definieren u.s.w., $\mathbf{N}$ also als die Menge aller Äquivalenzklassen von endlichen Mengen unter der *gleichmächtig*–Äquivalenzrelation. Aber wie erklärt man ,,endlich"? Hier macht man sich die Beobachtung zunutze, dass es für unendliche Mengen A injektive, aber nicht surjektive Abbildungen $f : A \to A$ gibt (z.B. $n \mapsto 2n$ für $A = \mathbf{N}$) und ebenso surjektive, aber nicht injektive Abbildungen von a auf sich. Es ist plausibel, dass dieser Ärger für endliche Mengen nicht auftritt. Naheliegend ist also die sehr merkwürdige

Definition 1.4 *Eine Menge A heißt ,,endlich", wenn jede injektive Abbildung $f : A \to A$ auch surjektiv ist (oder umgekehrt).*

Wie könnte man nun das Rechnen mit natürlichen Zahlen einführen? Wenn wir natürliche Zahlen als Kardinalzahlen $|A|$ endlicher Mengen eingeführt haben, liegt folgende Idee nahe: Für eine zu A disjunkte endliche Menge B (also mit $A \cap B = \emptyset$) definiere man z.B. die Addition durch

$$|A| + |B| := |A \cup B|\,, \quad \text{wenn} \quad A \cup B := \{c \mid c \in A \text{ oder } c \in B\}$$

die *Vereinigungsmenge* der beiden Mengen bezeichnet. Es sei nicht verschwiegen, dass dabei der Teufel in vielen Details liegt: Warum ist das wieder eine endliche Menge? Wie beweist man damit alle bekannten Rechenregeln? Ist die Addition überhaupt *wohldefiniert*, d.h. ändert sich das Ergebnis auch nicht, wenn wir von A und B zu gleichmächtigen Mengen übergehen?

2 Natürliche Zahlen und vollständige Induktion

Nachteil der Einführung natürlicher Zahlen via Kardinalzahlen: Alles basiert auf unbewiesenen Annahmen über Mengen. Solche unbewiesenen Annahmen — *Axiome* — nimmt man

überall in Kauf, man kann höchstens nach Zweckmäßigkeit oder Ökonomie dem einen oder anderen Axiomensystem den Vorzug geben. Für die Einführung von $\mathbf{N}$ besprechen wir hier eine
zweite Möglichkeit: direkt axiomatisch durch das *Axiomensystem von Peano.*

Definition 2.1 $\mathbf{N}$ *ist eine Menge mit einem Element* $1 \in \mathbf{N}$ *und einer ,,Nachfolgerfunktion"* $N : \mathbf{N} \to \mathbf{N}$ *mit folgenden Eigenschaften:*

- *Es gibt keine Zahl* $n \in \mathbf{N}$ *mit Nachfolger* $1 = N(n)$ *.*
- N *ist injektiv.*
- *Das ,,Prinzip der vollständigen Induktion": Jede Teilmenge von* $\mathbf{N}$ *, welche* 1 *enthält und mit jedem* n *auch seinen Nachfolger* $N(n)$ *enthält, ist bereits die gesamte Menge* $\mathbf{N}$ *.*

Anschaulicher: Wenn eine Eigenschaft E auf 1 zutrifft und aus der Gültigkeit von E für $n \in \mathbf{N}$ bereits die Gültigkeit für $N(n)$ folgt, dann ist E für alle natürlichen Zahlen richtig.

Beispiel für eine Folgerung:

Satz 2.1 *Jede natürliche Zahl außer* 1 *ist ein Nachfolger.*

Wie führt man nun Operationen wie ,,+" und ,,·" oder Relationen wie ,,<" auf $\mathbf{N}$ ein? Beispiel einer *rekursiven Definition* ist

- $\forall n \in \mathbf{N}$ sei $n + 1 := N(n)$
- $\forall n, m \in \mathbf{N}$ sei $n + N(m) := N(n + m)$.

Dadurch ist nach Peano die Addition $n + m$ für alle $n, m \in \mathbf{N}$ erklärt. Wenn man soweit ist, kann man analog die Multiplikation festlegen:

- $\forall n \in \mathbf{N}$ sei $n \cdot 1 := n$
- $\forall n, m \in \mathbf{N}$ sei $n \cdot N(m) := n \cdot m + n$.

(mit der Konvention *Punktrechnung vor Strichrechnung*, wie aus der Schule geläufig; ebenso werden wir in Zukunft — soweit das nicht zu Missverständnissen führt — den Multiplikationspunkt ,,·" weglassen.) Beispiel einer Folgerung von sehr vielen, die wir hier übergehen:

Satz 2.2 $\forall n \in \mathbf{N}$ *gilt* $n + 1 = 1 + n$.

Die Definitionen von + und · sind Spezialfälle von Anwendungen des sehr allgemeinen *Rekursionssatzes* von Dedekind:

Satz 2.3 *Sei A eine Menge und seien $\varphi_1, \varphi_2, \varphi_3, \ldots$ Abbildungen $A \to A$. Dann kann man durch Festlegung eines Elements $a \in A$ eindeutig eine Funktion*

$$f : \mathbf{N} \to A$$

durch die Vorschriften $f(1) := a$, $f(N(k)) := \varphi_k(f(k))$ definieren.

Beispiele: — Potenzen $a^1 := a$, $a^{k+1} := a \cdot a^k$,
– Fakultät $1! := 1$, $(k+1)! := k! \cdot (k+1)$,
– Summen $\sum_{n=1}^{1} a_n := a_1$, $\sum_{n=1}^{k+1} a_n := a_{k+1} + \sum_{n=1}^{k} a_n$,
– Produkte $\prod_{n=1}^{1} a_n := a_1$, $\prod_{n=1}^{k+1} a_n := a_{k+1} \cdot \prod_{n=1}^{k} a_n$.

Regel: Überall, wo in der mathematischen Umgangssprache und der Schule Pünktchen ... zu Hilfe genommen werden wie z.B. in $\sum_{n=1}^{k} a_n := a_1 + \ldots + a_k$, steckt in Wirklichkeit der Dedekindsche Rekursionssatz dahinter.
Übrigens erweist es sich in gerade diesen Beispielen als praktisch, $\mathbf{N}_0$ anstelle von $\mathbf{N}$ zu verwenden und die Rekursion mit $k = 0$ anstatt 1 zu beginnen, und zwar mit den ergänzenden Definitionen — auch wenn sie auf den ersten Blick wenig natürlich erscheinen — $a^0 := 1$ (bitte nicht für $a = 0$ verwenden!), $0! := 1$, der *leeren Summe* $\sum_{n=1}^{0} a_n := 0$ und dem *leeren Produkt* $\prod_{n=1}^{0} := 1$.

Unbedingt einüben: vollständige Induktion als Beweisprinzip, hier ein paar Beispiele dafür.

Satz 2.4 *Für alle $n \in \mathbf{N}$ und für $q \neq 1$ gilt*

$$\sum_{i=1}^{n} i \;=\; \frac{n(n+1)}{2}\,, \qquad \sum_{i=1}^{n}(2i-1) \;=\; n^2\,, \qquad \sum_{k=0}^{n} q^k \;=\; \frac{1-q^{n+1}}{1-q}\,.$$

Die letzte Gleichung — die Formel für die *geometrische Summe* — gilt nicht nur für $q \in \mathbf{N}$; wichtig ist nur, dass man multiplizieren und dividieren kann und dass $1 - q \neq 0$ ist. Anwendung: Kapitalansammlung bei Sparplänen bzw. Versicherungen. In Abschnitt 9 und genauer in „Elementarmathematik II" bzw. „Analysis I" lernt man, dass für $-1 < q < 1$ die Potenzen q^k gegen 0 *konvergieren* und dass darum die *unendliche Reihe*, hier genauer die *geometrische* Reihe

$$1 + q + q^2 + q^3 + \ldots \;=\; \sum_{k=0}^{\infty} q^k \;=\; \frac{1}{1-q}$$

einen Sinn erhält und explizit berechnet werden kann. Für uns wird das bereits im Zusammenhang mit recht elementaren Fragen nach periodischen Dezimalbruchentwicklungen

wichtig werden, z.B.

$$1,11111\ldots \;=\; \sum_{k=0}^{\infty}(\frac{1}{10})^k \;=\; \frac{1}{\frac{9}{10}} \;=\; 1+\frac{1}{9}\,.$$

Schließlich sei erwähnt, dass die vollständige Induktion gleichermaßen wichtig für die *Kombinatorik*, die sich mit Anzahlfragen aller Art beschäftigt. Beispiel:

Satz 2.5 *Die Anzahl der möglichen Anordnungen der Menge* $\{1,2,\ldots,n\}$ *ist* $n!$.

Zum *Beweis* mit vollständiger Induktion geht man üblicherweise nach folgendem Schema vor.
Induktionsanfang. Die Aussage stimmt für $n=1$.
Induktionsvoraussetzung oder *Induktionsannahme.* Die Aussage sei für n (oder auch: für alle natürlichen Zahlen $\leq n$) bereits bewiesen.
Induktionsschritt. Daraus wird die Gültigkeit der Aussage für $n+1$ hergeleitet, im konkreten Fall etwa so: Für das letzte Element $n+1$ der Menge stehen $n+1$ verschiedene Plätze der Anordnung zur Verfügung. Zu jeder dieser $n+1$ Möglichkeiten gibt es nach Induktionsannahme $n!$ Möglichkeiten, die verbleibenden n Plätze mit den Elementen $1,2,\ldots,n$ zu besetzen, insgesamt also $n!(n+1)$ mögliche Anordnungen.
Nach den Peano–Axiomen ist damit klar, dass die Aussage für alle natürlichen Zahlen richtig ist; besonders eifrige Formalisten nennen das dann den *Induktionsschluss.*

Definition 2.2 *Für* $k\leq n\in\mathbf{N}_0$ *nennt man die Zahlen*

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

„Binomialkoeffizienten" (der Ausdruck rechts hat nur Sinn für $0<k\leq n$*, man muss dann* $\binom{n}{0}:=1$ *als zusätzliche Konvention einführen).*

Satz 2.6 *Jede Menge aus* n *Elementen hat* $\binom{n}{k}$ *Untermengen aus* k *Elementen.*

Den *Beweis* kann man entweder mittels Satz 2.5 (Induktion über k) oder durch Induktion über n vermöge des folgenden Satzes führen, der auch der Berechnung der Binomialkoeffizienten im *Pascalschen Dreieck* zugrundeliegt.

Satz 2.7 *Für alle* $k\leq n\in\mathbf{N}$ *gilt*

$$\binom{n-1}{k-1}+\binom{n-1}{k} \;=\; \binom{n}{k}\,.$$

Neben Anzahlberechnungen bei endlichen Mengen spielen Binomialkoeffizienten eine große Rolle für die Berechnung von Wahrscheinlichkeiten — die Wahrscheinlichkeit für einen Hauptgewinn im Lotto ist $\binom{49}{6}^{-1}$ also etwa $\frac{1}{14\cdot 10^6}$ — und für die Algebra via *binomischem Lehrsatz*, der nicht nur für $x, y \in \mathbf{N}$, sondern in viel allgemeineren Bereichen gilt:

Satz 2.8

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

3 Ganze Zahlen

sind die Zahlen $\ldots -3, -2, -1, 0, 1, 2, \ldots$, in denen man zu $\mathbf{N}$ noch die 0 und die *negativen* natürlichen Zahlen hinzunimmt (warum wohl?). Wie macht man das mathematisch? Idee: Man betrachtet alle *Differenzen* $a - b$ natürlicher Zahlen und rechnet mit diesen. Zwei Probleme dabei:
– Von Differenzen war noch gar nicht die Rede, was ist das?
– Die gleiche Zahl kann in vielerlei Weise als Differenz geschrieben werden.
Man wird also zunächst einfach von *geordneten Paaren* (a, b) natürlicher Zahlen ausgehen, zusammengefasst zur Menge $\mathbf{N}^2$. *Geordnet* heißt dabei

$$(a, b) = (c, d) \quad :\Longleftrightarrow \quad a = c \quad \text{und} \quad b = d\,.$$

(Entsprechend kann man ebenso geordnete Tripel, ... , geordnete n–Tupel einführen.) Dann wird man Paare, die die gleiche Differenz ergeben, identifizieren müssen, und das macht man wieder einmal durch eine geeignete Äquivalenzrelation, nämlich

$$(a, b) \sim (n, m) \quad :\Longleftrightarrow \quad a + m = b + n\,.$$

Wieder einmal heißen die Doppelpunkte, dass die linke Seite durch die rechte Seite erklärt ist, und natürlich ist zu überprüfen, dass es sich wirklich um eine Äquivalenzrelation handelt! Man beachte, dass zur Definition nur die Addition in $\mathbf{N}$ verwendet wurde, die wir schon kennen. Die Äquivalenzklassen seien mit $[a, b]$ bezeichnet, und diese Äquivalenzklassen sehen wir jetzt als *ganze Zahlen* an und fassen sie zu der Menge $\mathbf{Z}$ zusammen. Natürlich sollten die natürlichen Zahlen darin enthalten sein, was vielleicht nicht mit bloßem Auge zu sehen ist. Dazu genügt es, eine — mit unseren anschaulichen Vorstellungen übereinstimmende — injektive Abbildung $\mathbf{N} \to \mathbf{Z}$ zu finden; hier ist sie:

$$\mathbf{N} \subset \mathbf{Z} \quad \text{vermöge} \quad n \mapsto [n+1, 1]$$

Die Injektivität ist nachzuweisen! Wie führt man jetzt Addition und Multiplikation ein? Geleitet wird man von der Vorstellung, dass die geordneten Paare eigentlich Differenzen bedeuten sollen und dass die Rechenoperationen auf der (eingebetteten) Untermenge $\mathbf{N}$ mit den schon vorher eingeführten Rechenoperationen übereinstimmen sollen, und dass man zur Definition nur Begriffe und Operationen verwenden darf, die man schon hat. Und schließlich sollen die vertrauten Rechengesetze herauskommen.

Satz 3.1 *Auf* $\mathbf{Z}$ *werden durch*

$$[a,b]+[c,d] := [a+c, b+d] \quad \textit{und} \quad [a,b]\cdot[c,d] := [ac+bd, bc+ad]$$

eine Addition und eine Multiplikation definiert, die auf $\mathbf{N}$ *mit der dort gegebenen Addition und Multiplikation übereinstimmen.*

Zum *Beweis* muss man zunächst nachweisen, dass diese Vorschriften *wohldefiniert* sind, d.h. nicht von den gewählten Repräsentanten der Äquivalenzklassen abhängen, dass also z.B.

$$(c,d)\sim(n,m) \quad \Rightarrow \quad (ac+bd, bc+ad)\sim(an+bm, bn+am)$$

gilt, was natürlich aus

$$c+m=d+n \quad \Rightarrow \quad ac+bd+bn+am = bc+ad+an+bm$$

folgt, wenn wir diverse Rechenregeln in $\mathbf{N}$ als bekannt voraussetzen. Dann ist zu zeigen, dass die neuen Operationen nur die alten aus $\mathbf{N}$ fortsetzen, z.B. folgt

$$[n+1,1]\cdot[m+1,1] = [nm+n+m+1, n+1+m+1] = [nm+1,1]$$

aus $(nm+n+m+1, n+m+1)\sim(nm+1,1)$.
Die zentralen Rechenregeln, die man für $\mathbf{Z}$ aus den Rechenregeln für $\mathbf{N}$ herleitet, seien im folgenden Satz zusammengefasst, wobei wir für den Augenblick von der lästigen Äquivalenzklassen–Schreibweise schon einmal abgehen.

Satz 3.2 *Addition und Multiplikation in* $\mathbf{Z}$ *erfüllen die folgenden Rechengesetze. Für alle* $a,b,c\in\mathbf{Z}$ *gelten*

$$\begin{aligned} (a+b)+c &= a+(b+c) \quad \textit{(Assoziativgesetz der Addition)} \\ a+b &= b+a \quad \textit{(Kommutativgesetz der Addition)} \\ \exists 0\in\mathbf{Z} \quad \textit{mit} \quad a+0 &= a \end{aligned}$$

Für alle $a\in\mathbf{Z}$ *gibt es ein eindeutig bestimmtes* $x\in\mathbf{Z}$*, genannt* $x =: -a$*, mit* $a+x=0$.

$$\begin{aligned} (ab)c &= a(bc) \quad \textit{(Assoziativgesetz der Multiplikation)} \\ ab &= ba \quad \textit{(Kommutativgesetz der Multiplikation)} \\ \exists 1\in\mathbf{Z} \quad \textit{mit} \quad a\cdot 1 &= a \\ a(b+c) &= ab+ac \quad \textit{(Distributivgesetz)}. \end{aligned}$$

Wie schon erwähnt, verwenden wir die Konvention „Punktrechnung vor Strichrechnung" und lassen den Multiplikationspunkt weg, wo keine Missverständnisse zu befürchten sind. Aus unserer Konstruktion von $\mathbf{Z}$ folgt die Existenz der 0 als Äquivalenzklasse $[n,n]$ (egal

welches $n \in \mathbf{N}$) und die Existenz des ,,additiven Inversen" $-[n,m]$ als $[m,n]$. Noch eine Konvention: Anstelle von

$$a + (-b) \quad \text{schreibt man} \quad a - b$$

und hat damit beliebige Differenzen eingeführt. Natürlich sind in $\mathbf{Z}$ nicht nur Gleichungen $a + x = 0$ lösbar, sondern beliebige Gleichungen $a + x = c$, und zwar durch $x = c - a$, wie man an Hand der Grundregeln aus Satz 3.2 überprüfen mag. Diese Grundregeln gelten übrigens nicht nur in $\mathbf{Z}$, sondern ebenso in vielen anderen Rechenbereichen wie z.B. für die reellen Zahlen, für Polynome und andere Bereiche, die wir noch kennenlernen werden. Darum führt man für alle diese Rechenbereiche einen gemeinsamen Oberbegriff *(kommutativer) Ring* ein; in dieser Sprache würde Satz 3.2 einfach heißen: $\mathbf{Z}$ *ist ein kommutativer Ring.* Dahinter steckt nicht Lust am Formalismus, sondern Denkökonomie, denn alles was man aus den in Satz 3.2 formulierten *Ringaxiomen* herleiten kann, gilt dann nicht nur in $\mathbf{Z}$, sondern eben auch für sehr viele andere Rechenbereiche. Beispiele für solche Folgerungen aus den Ringaxiomen sind etwa

$$\begin{aligned} 0 \cdot a &= 0 \\ -(-a) &= a \\ (-a)(-b) &= ab \end{aligned}$$

oder der binomische Satz. Zum Abschluss darum zwei künftig sehr wichtige Sachverhalte, die *nicht* aus den Ringaxiomen folgen.

Satz 3.3 $\mathbf{Z} = \mathbf{N} \cup \{0\} \cup -\mathbf{N}$, *und zwar ist das eine disjunkte Vereinigung.*

Satz 3.4 *Wenn* $a, b \in \mathbf{Z}$ *mit* $ab = 0$, *dann ist* $a = 0$ *oder* $b = 0$.

Für die letztgenannte Eigenschaft sagt man auch, $\mathbf{Z}$ sei *nullteilerfrei* und nennt $\mathbf{Z}$ dann einen *Integritätsbereich*. Was in Satz 3.3 mit $-\mathbf{N}$ gemeint ist, sollte klar sein. Die in 3.3 getroffene Einteilung der ganzen Zahlen kann man natürlich auch als Definition nehmen — so geht man meist in der Schule vor —, muss dann aber Addition und Multiplikation über mühsame Fallunterscheidungen vornehmen.

4 Division mit Rest. Stellenwertsysteme

Definition 4.1 $a \in \mathbf{Z}$ *heißt ,,Teiler" von* $b \in \mathbf{Z}$ *und* b *ein ,,Vielfaches" von* a, *geschrieben* $a|b$, *wenn ein* $c \in \mathbf{Z}$ *existiert mit* $ac = b$.

Definition 4.2 *$a \in \mathbf{Z}$ heißt ,,kleiner" als $b \in \mathbf{Z}$, geschrieben $a < b$, wenn $b - a \in \mathbf{N}$ ist. $a \leq b$ ist definiert als ,,$a = b$ oder $a < b$". Entsprechend sind die Relationen $a > b$ und $a \geq b$ definiert. Alle $a > 0$ (also die natürlichen Zahlen) heißen ,,positiv", alle $a < 0$,,negativ".*

Rechenregeln für den Umgang mit Ungleichungen: Für alle ganzen Zahlen a, b, c gilt

$$\begin{aligned} & & a < b & \Leftrightarrow & a + c < b + c \\ & & a < b & \Leftrightarrow & -b < -a \\ a < b & \text{ und } & c > 0 & \Rightarrow & ac < bc \\ a < b & \text{ und } & c < 0 & \Rightarrow & ac > bc\,. \end{aligned}$$

Klar, dass man jetzt auch von einem ,,größten" oder ,,kleinsten" Element einer Menge ganzer Zahlen reden kann (wenn diese denn existieren).

Satz 4.1 *Jede nichtleere Untermenge von $\mathbf{N}$ besitzt ein kleinstes Element.*

Beweis durch vollständige Induktion. Klar, wenn die Menge $M \subseteq \mathbf{N}$ die 1 enthält. Sei nun der Satz bewiesen, wenn M ein $k \leq n$ enthält, und nun enthalte M die Zahl $n + 1$. Entweder ist $n + 1$ kleinstes Element von M oder M enthält ein $k \leq n$, dann ist die Behauptung nach Induktionsvoraussetzung richtig.

Satz 4.2 *Seien $a \in \mathbf{Z}$ und $q \in \mathbf{N}$. Dann gibt es eindeutig bestimmte $b \in \mathbf{Z}$ und $r \in \{0, 1, \ldots, q-1\}$, so dass*

$$a \;=\; qb + r\,.$$

b wird dabei als *Quotient* und r als *Rest* bezeichnet. Aus diesem Satz folgt die Möglichkeit, alle natürlichen Zahlen im *Dezimalsystem* oder allgemeiner in g–adischen *Stellenwertsystemen* zu beschreiben mit $g \in \mathbf{N}$, $g > 1$. Division von a durch ein genügend hohe Potenz g^n, dann den Rest durch g^{n-1} etc. zeigt nämlich

Satz 4.3 *Jedes $a \in \mathbf{N}$ besitzt eine eindeutige Darstellung*

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

mit ,,Ziffern" $b_j \in \{0, 1, \ldots, g-1\}$.

Der Ausdruck rechts ist natürlich *nicht* als Produkt der Ziffern b_j zu lesen! $g = 10$ gibt das vertraute Dezimalsystem, $g = 2$ das in der Informatik benutzte Binärsystem, $g = 60$ das (woher bekannte?) Sechzigersystem, $g = 20$ das möglicherweise von den Kelten benutzte Zwanzigersystem.

5 Teilbarkeit, Kongruenzen und Restklassen

Definition 5.1 *Seien* $a, b, m \in \mathbf{Z}$. *Dann heißen* a *und* b *„kongruent modulo" m, geschrieben*

$$a \equiv b \bmod m \quad \textit{oder} \quad a \equiv b\ (m) \quad ,$$

wenn $m \mid a - b$.

Alternative Formulierungen wären: *wenn ein* $k \in \mathbf{Z}$ *existiert, so dass* $a = b + km$ oder auch *wenn a und b bei Division durch m den gleichen Rest haben.* Kongruenz modulo m ist eine Äquivalenzrelation. Für $m = 0$ stimmt sie einfach mit der Gleichheit überein, und meistens nimmt man $m > 0$ an, weil m und $-m$ die gleiche Äquivalenzrelation ergeben. Die entstehenden Äquivalenzklassen nennt man *Restklassen zum Modul m* und schreibt sie z.B. als $[a]_m$; wenn klar ist, von welchem Modul die Rede ist, lässt man den Index weg. Für $m > 0$ werden die Restklassen genau repräsentiert durch die Divisionsreste $0, 1, \ldots, m-1$, die Menge aller Restklassen $\mathbf{Z}/m\mathbf{Z}$ besitzt dann also m Elemente. Beispiele aus dem täglichen Leben sind die Einteilung der ganzen Zahlen in gerade und ungerade, die Einteilung der Tage in Wochentage, das Zwölftonsystem, das Rechnen mit Uhrzeiten.

Satz 5.1 *Sei* $m \in \mathbf{N}$. *Dann lassen sich auf* $\mathbf{Z}/m\mathbf{Z}$ *eine Addition und eine Multiplikation (repräsentantenweise) definieren durch*

$$[a] + [b] := [a + b] \qquad \textit{und} \qquad [a] \cdot [b] := [ab] \ ,$$

für alle $a, b \in \mathbf{Z}$, *und mit diesen Operationen erfüllt* $\mathbf{Z}/m\mathbf{Z}$ *die Ringaxiome.*

Zunächst muss man wieder einmal die *Wohldefiniertheit* nachweisen, dass also das Ergebnis der Operationen nicht abhängt von der Auswahl der Repräsentanten der Restklasse, obwohl das zunächst so aussieht. Beispiel:

$$[a] = [a'] \ \Rightarrow\ a \equiv a' \bmod m \ \Rightarrow\ a + b \equiv a' + b \bmod m \ \Rightarrow\ [a + b] = [a' + b]$$

Dann sind die Ringaxiome nachzurechnen, also die Rechenregeln aus Satz 3.2. Das ist todlangweilig, es sei aber erwähnt, dass die Rolle der 0 (auch *neutrales Element der Addition* genannt) nun von der *Nullrestklasse* $[0]$ übernommen wird, und die Rolle der 1 (*neutrales Element der Multiplikation*) von der *Einsrestklasse* $[1]$.

Vorsicht: Es gibt hier keine Einteilung in positive und negative Restklassen, und auch die Nullteilerfreiheit ist i.a. nicht gegeben, Beispiel dafür ist $[3]_{24} \cdot [8]_{24} = [24]_{24} = [0]_{24}$. Ein Integritätsbereich entsteht nur dann, wenn m eine Primzahl ist, vgl. nächstes Kapitel. Ähnlich exotisch sind andere Phänomene, dass z.B. die Gleichung $x^2 = 1$ im Ring $\mathbf{Z}/24\mathbf{Z}$ nicht 2, sondern 8 Lösungen hat. Eine schöne Schulanwendung von Restklassen sind die Quersummenregeln für die Teilbarkeit.

Satz 5.2 *Sei die Dezimaldarstellung der Zahl* $a \in \mathbf{N}$ *gegeben als*

$$a \;=\; b_n 10^n + b_{n-1}10^{n-1} + \ldots + b_1 10 + b_0 \;=\; \sum_{j=0}^{n} b_j 10^j \;=\; b_0 b_1 \ldots b_{n-1} b_n \;.$$

Dann ist

- $3 \mid a \quad \Leftrightarrow \quad 3 \mid \sum b_j$
- $9 \mid a \quad \Leftrightarrow \quad 9 \mid \sum b_j$
- $11 \mid a \quad \Leftrightarrow \quad 11 \mid \sum (-1)^j b_j$.

Beweis für die letzte Regel. Aus

$$10 \equiv -1 \bmod 11 \quad \text{folgt} \quad 10^j \equiv (-1)^j \bmod 11$$

für alle $j = 0, 1, \ldots, n$, und $11 \mid a \;\Leftrightarrow\; a \equiv 0 \bmod 11$ folgt aus der Definition der Kongruenz. Beides ergibt zusammen

$$11 \mid a \quad \Leftrightarrow \quad \sum_{j=0}^{n} b_j 10^j \equiv \sum_{j=0}^{n} b_j (-1)^j \equiv 0 \bmod 11 \quad \Leftrightarrow \quad 11 \mid \sum_{j=0}^{n} b_j (-1)^j \;.$$

6 Euklidischer Algorithmus. Primfaktorzerlegung

Definition 6.1 *Für* $a, b \in \mathbf{Z}$, *nicht beide* $= 0$, *bezeichne* $(a, b) = \mathrm{ggT}(a, b)$ *den ,,größten gemeinsamen Teiler"* $d \in \mathbf{N}$ *von* a *und* b. *Ergänzend definiert man* $(0, 0) := 0$. *Der größte gemeinsame Teiler von mehr als zwei ganzen Zahlen wird entsprechend, z.B. rekursiv über die Anzahl, definiert.*

Die Bestimmung des ggT ist ein Angelpunkt in allen Anwendungen der Zahlentheorie und läuft *nicht* — wie man denken könnte — über die Primfaktorzerlegung von a und b, sondern viel schneller (und mit vielen wichtigen Konsequenzen) über eine fortgesetzte Division mit Rest, genannt der *euklidische Algorithmus*. Klar: Wenn $b = 0$, so ist $(a, b) = \pm a$, genauer: a wenn $a \geq 0$, andernfalls $-a$. Wir verlieren also nichts, wenn wir uns auf den Fall $b \neq 0$ oder sogar $b > 0$ beschränken, im Mathematikjargon gesagt, nehmen wir *ohne Beschränkung der Allgemeinheit* oder *o.B.d.A.* $b > 0$ an.

Satz 6.1 *Seien* $a \in \mathbf{Z}$ *und* $b \in \mathbf{N}$, *o.B.d.A. kein Teiler von* a. *Der größte gemeinsame Teiler von* a *und* b *ist der letzte nichtverschwindende Rest* $d = r_n$ *im folgenden Schema*

von Divisionen.

$$\begin{aligned} a &= q_1 b + r_1 \\ b &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ \vdots &\ \vdots\ \ \vdots \\ r_{n-3} &= q_{n-1} r_{n-2} + r_{n-1} \\ r_{n-2} &= q_n r_{n-1} + r_n \\ r_{n-1} &= q_{n+1} r_n \end{aligned}$$

Wegen $b > r_1 > r_2 > \ldots$ bricht die Folge der Reste nämlich ab, und zwar sogar ziemlich schnell, wie man in Kursen über Zahlentheorie, Angewandte oder Diskrete Mathematik lernen wird. Ferner ist klar, dass für jeden gemeinsamen Teiler von a und b aus der Abfolge der Gleichungen folgt

$$d|a, b \ \Rightarrow\ d|b, r_1 \ \Rightarrow\ d|r_1, r_2 \ \Rightarrow\ \ldots \ \Rightarrow\ d|r_{n-1}, r_{n-2} \ \Rightarrow\ d|r_n\ .$$

Insbesondere folgt daraus $d \leq r_n$, es bleibt also nur zu zeigen, dass auch r_n selbst gemeinsamer Teiler ist. Verfolgt man die Gleichungen umgekehrt von unten nach oben, erhält man

$$r_n|r_{n-1} \ \Rightarrow\ r_n|r_{n-2} \ \Rightarrow\ \ldots \ \Rightarrow\ r_n|b \ \Rightarrow\ r_n|a\ ,$$

r_n ist also auch selbst ein gemeinsamer Teiler.

Satz 6.2 *Unter den gleichen Voraussetzungen liefert der euklidische Algorithmus ganzzahlige Lösungen x, y der ,,diophantischen Gleichung"*

$$d\ =\ xa + yb\ .$$

Zum *Beweis* ist genau wie oben die Kette der Gleichungen von unten nach oben zurückzuverfolgen:

$$d = r_n = r_{n-2} - q_n r_{n-1} = r_{n-2} - q_n\left(r_{n-3} - q_{n-1} r_{n-2}\right) = \left(1 + q_n q_{n-1}\right) r_{n-2} - q_n r_{n-3} = \ldots$$

endet bei einer Darstellung von d als ganzzahliger *Linearkombination* von a und b. Triviale Nebenbemerkung: Wenn $b|a$, lautet die Darstellung natürlich $d = 0a + 1b$.

Definition 6.2 *Wenn der ggT $(a, b) = 1$ ist, heißen a und b ,,teilerfremd". $1 < p \in \mathbf{N}$ heißt ,,Primzahl", wenn p außer 1 und p keine weiteren Teiler besitzt.*

Da jede ganzzahlige Linearkombination $xa+yb$ von a und b durch den ggT von a, b teilbar ist, könnte man den Begriff *teilerfremd* also auch ersetzen durch

$$xa + yb = 1 \qquad \text{ist lösbar in} \quad \mathbf{Z}\ .$$

Multipliziert man die Gleichung mit $c \in \mathbf{Z}$ und setzt $a|bc$ voraus, dann ist nach $xac+ybc = c$ auch die rechte Seite durch a teilbar, also gilt

Satz 6.3 *Seien* $a, b, c \in \mathbf{Z}$ *und* $(a, b) = 1$ *. Aus* $a \mid bc$ *folgt* $a \mid c$ *.*

Man beachte, dass beim Beweis der Satz von der eindeutigen Primfaktorzerlegung keineswegs verwendet wurde. Dieser folgt nämlich erst daraus, indem man den Spezialfall $a = p$ prim betrachtet: Wenn $p|bc$, gilt $p|b$ oder $p|c$. Damit ist nämlich

Satz 6.4 *Jede natürliche Zahl n lässt sich als ein Produkt von Primzahlen schreiben. Dessen Faktoren, die ,,Primfaktoren" von n , sind bis auf die Reihenfolge eindeutig bestimmt.*

leicht zu beweisen. Für die *Existenz* einer Primfaktorzerlegung nehme man an, es gäbe natürliche Zahlen, die sich nicht in Primfaktoren zerlegen lassen, und wende auf die Menge dieser Zahlen Satz 4.1 an (die ,,Suche nach dem kleinsten Verbrecher") und erhält so einen Widerspruch zu der Annahme (wie?). Die *Eindeutigkeit* ist viel schwerer einzusehen und wird auf der Schule darum meist gar nicht zum Thema gemacht. Auch hier kann man wie eben einen *Widerspruchsbeweis* führen, indem man annimmt, es gäbe eine natürliche Zahl mit zwei wesentlich verschiedenen Primfaktorzerlegungen, also

$$p_1 p_2 \cdot \ldots \cdot p_n \;=\; q_1 q_2 \cdot \ldots \cdot q_m \; .$$

Wieder nach Satz 4.1 darf man annehmen, dass diese Zahl kleinstmöglich gewählt ist, dass also keine der Primzahlen p_i unter den Primzahlen q_j vorkommt. Dann investiere man den oben erwähnten Spezialfall von Satz 6.3, um einzusehen, dass z.B. p_1 einen der Faktoren q_j teilen muss. Da diese aber selbst prim sind, muss eben doch eine Gleichheit $p_1 = q_j$ gelten.

Noch ein Widerspruchsbeweis (den Euklid bereits kannte): Angenommen, es gäbe nur endlich viele Primzahlen

$$p_1 = 2 \; , \; p_2 = 3 \; , \; p_3 = 5 \; , \; \ldots \; , \; p_n \; .$$

Dann ist aber $N := p_1 p_2 \cdot \ldots \cdot p_n + 1$ durch keine Primzahl teilbar im Widerspruch zu Satz 6.4, also

Satz 6.5 *Es gibt unendlich viele Primzahlen.*

7 Rationale Zahlen

Definition 7.1 *Sei* $\mathbf{Z}^*$ *die Menge der ganzen Zahlen ohne die* 0 *und* $P := \mathbf{Z} \times \mathbf{Z}^*$ *die Menge der geordneten Paare aus* $\mathbf{Z}$ *und* $\mathbf{Z}^*$ *. Auf P definieren wir eine Äquivalenzrelation durch*

$$(a, b) \sim (m, n) \quad :\Longleftrightarrow \quad an = bm \; ,$$

nennen die Äquivalenzklassen ,,Brüche" oder ,,rationale Zahlen", bezeichnen sie mit $\frac{a}{b}$ *oder* a/b *und fassen die rationalen Zahlen zu der Menge* $\mathbf{Q}$ *zusammen.*

Wir sehen die rationalen Zahlen als eine erneute *Zahlbereichserweiterung* in der Kette

$$\mathbf{N} \subset \mathbf{Z} \subset \mathbf{Q}$$

an vermöge der injektiven Abbildung (*Einbettung*)

$$\mathbf{Z} \to \mathbf{Q} \ : \ z \mapsto \frac{z}{1} \, .$$

„Äquivalenzrelation" und „injektiv" sind natürlich nachzuweisen! Grund für die Erweiterung von Zahlbereichen ist immer, dass man mit den bisherigen Möglichkeiten unzufrieden ist, dass also die bisher verwendeten Zahlen als Modelle für die Realität unzureichend sind oder bestimmte Operationen nicht zulassen. Hier haben wir es damit zu tun, dass z.B. Division mit Rest in $\mathbf{Z}$ für bestimmte Zwecke unzureichend ist und Teilbarkeit eher selten vorkommt. Andererseits möchte man aber die Qualitäten der bisher verwendeten Zahlbereiche behalten, hier also addieren und multiplizieren können, und die neuen Rechenoperationen sollen auf $\mathbf{Z}$ mit den alten übereinstimmen.

Satz 7.1 *Für alle* $\frac{a}{b} \, , \, \frac{c}{d} \in \mathbf{Q}$ *werden durch*

$$\frac{a}{b} + \frac{c}{d} := \frac{ad + bc}{bd} \quad , \quad \frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd}$$

Operationen definiert, die auf $\mathbf{Z}$ *mit den bisher verwendeten übereinstimmen. Sie erfüllen die Ringaxiome, und zwar mit den schon in* $\mathbf{Z}$ *verwendeten Zahlen*

$$0 = \frac{0}{1} \qquad \textit{und} \qquad 1 = \frac{1}{1} \, .$$

Zusätzlich gilt noch die Existenz des „multiplikativen Inversen": Zu jedem $r \in \mathbf{Q}$, $r \neq 0$ *, gibt es eine mit* r^{-1} *oder* $\frac{1}{r}$ *bezeichnete eindeutig bestimmte Lösung* $x \in \mathbf{Q}$ *der Gleichung* $rx = 1$ *.*

Die Ringaxiome zusammen mit der Existenz des multiplikativen Inversen nennt man die *Körperaxiome*, bezeichnet $\mathbf{Q}$ also als *Körper* (engl. „field", in alter Literatur manchmal auch „Rationalitätsbereich"). In diesem Satz ist vieles zu beweisen, aber es ist fast nirgendwo eine Idee erforderlich.

- Addition und Multiplikation sind wohldefiniert
- und setzen die Addition und Multiplikation aus $\mathbf{Z}$ fort.
- Ringaxiome
- und die Existenz des multiplikativen Inversen.

Für den letzten Punkt sollte man anmerken, dass $r = \frac{a}{b}$ genau dann $\neq 0$ ist, wenn a und b beide $\neq 0$ sind; dann ist $\frac{b}{a}$ der richtige Kandidat für r^{-1}.

Der Begriff *Körper* ist wieder eine sehr ökonomische Erfindung: Alles, was man aus ihnen herleiten kann, gilt nicht nur für $\mathbf{Q}$, sondern überall, wo die Körperaxiome gültig sind. Außer den rationalen Zahlen sind das etwa die reellen Zahlen und die rationalen Funktionen, von denen noch die Rede sein wird, aber es gibt auch *endliche Körper*:

Satz 7.2 *Sei p eine Primzahl. Dann ist der Restklassenring $\mathbf{F}_p := \mathbf{Z}/p\mathbf{Z}$ ein Körper.*

Aus Satz 5.1 wissen wir nämlich bereits, dass $\mathbf{F}_p$ ein Ring mit p Elementen ist. Ein Element $r \neq 0$ dieses Rings ist eine Restklasse $[a]_p = [a] \neq [0]$ mit einem Repräsentanten $a \in \mathbf{Z}$, $a \not\equiv 0 \bmod p$, m.a.W. gilt $(a, p) = 1$. Satz 6.2 liefert nun ganzzahlige x, y mit

$$ax + py = 1\,, \quad \text{also} \quad ax \equiv 1 \bmod p\,,$$

also die gewünschte inverse Restklasse $[x] \in \mathbf{F}_p$ zur Restklasse $[a]$.

Auch der Körper $\mathbf{Q}$ ist noch nicht das Ende der Zahlbereichserweiterungen, weil man auch mit rationalen Zahlen noch keineswegs alle mathematischen Bedürfnisse befriedigen kann. Das wird in der Elementargeometrie zu Ende dieser Vorlesung sichtbar werden, aber wir können bereits ein Beispiel vorausschicken.

Satz 7.3 *Die Gleichung $x^2 = 2$ ist in $\mathbf{Q}$ unlösbar, m.a.W. $\sqrt{2}$ ist „irrational".*

Gäbe es nämlich ein $x = \frac{a}{b} \in \mathbf{Q}$ mit $x^2 = 2$, dann dürften wir o.B.d.A. annehmen, dass x in *gekürzter Form* vorliegt, d.h. dass $(a, b) = 1$ ist, a und b also keine gemeinsamen Primteiler besitzen. Wendet man nun Satz 6.4 — eindeutige Primfaktorzerlegung — auf beide Seiten der Gleichung

$$a^2 \;=\; 2\,b^2$$

an, so müssten $2 \mid a$ und b ungerade sein. Links steht aber eine gerade Anzahl von Faktoren $= 2$, rechts nur eine 2, Widerspruch. Klar, dass man diese Idee auf alle $\sqrt{m}$ ausdehnen kann, für die m nicht selbst schon eine Quadratzahl in $\mathbf{Z}$ ist.

8 Ungleichungen, Dezimalbrüche, Beträge

Für den täglichen Gebrauch sind *positive* rationale Zahlen (müssen wir gleich noch definieren) wichtiger als negative ganze Zahlen, erstere werden also auf der Schule eher eingeführt als $-\mathbf{N}$. Man könnte hier genauso vorgehen, bei einem systematischen Aufbau der Mathematik zieht man aber das oben vorgestellte Verfahren vor, weil man uneingeschränkt subtrahieren kann. Ebenso sind für das tägliche Leben Dezimalbrüche wie $17,95$ sicher wichtiger als die gewöhnlichen (oder *gemeinen*) Brüche $\frac{1795}{100} = \frac{359}{20}$, trotzdem zieht man letztere für einen systematischen Aufbau vor, weil Dezimalbrüche für das Rechnen einige sehr lästige Hürden bieten. Davon mehr am Ende von Abschnitt 9.

Definition 8.1 *Die rationale Zahl* $\frac{a}{b}$ *heißt ,,positiv", geschrieben* $\frac{a}{b} > 0$ *, wenn die ganze Zahl* $ab > 0$ *ist. Allgemeiner definieren wir*

$$\frac{a}{b} > \frac{c}{d} \quad :\Longleftrightarrow \quad \frac{a}{b} - \frac{c}{d} > 0 \;\Leftrightarrow\; (ad - bc)bd > 0$$

und entsprechend werden $<, \leq, \geq$ *definiert.*

Wie es vernünftigerweise sein sollte, stimmen alle diese Begriffe auf $\mathbf{Z} \subset \mathbf{Q}$ mit den alten Vereinbarungen über Ungleichungen überein. Rechenregeln für Ungleichungen:

Satz 8.1 *Für alle* $a, b, c \in \mathbf{Q}$ *gelten entweder* $a < b$ *oder* $a = b$ *oder* $a > b$ *,*

$$\begin{aligned}
a < b \quad \textit{und} \quad b < c \;&\Rightarrow\; a < c \\
a < b \;&\Rightarrow\; a + c < b + c\,, \\
a < b \;&\Rightarrow\; ac < bc\,, \quad \textit{wenn} \quad c > 0\,, \\
a < b \;&\Rightarrow\; ac > bc\,, \quad \textit{wenn} \quad c < 0\,, \\
a > 0\,,\; c > 1 \;&\Rightarrow\; a < ac\,, \\
a > 0\,,\; c < 1 \;&\Rightarrow\; a > ac\,, \\
0 < a < b \;&\Leftrightarrow\; 0 < b^{-1} < a^{-1}\,.
\end{aligned}$$

Dass die angegebene Alternative gilt, kann man unmittelbar der Definition entnehmen. Für die anderen Behauptungen braucht man die Definition nur für die ersten drei, da aus diesen alle übrigen folgen. Als Beispiel sei die vierte Behauptung genannt: Aus $c < 0$ folgt mit der zweiten $-c + c = 0 < -c$ also aus $a < b$ und der dritten Aussage $-ac < -bc$, wieder mit der zweiten Aussage daraus

$$0 = ac - ac < ac - bc\,, \text{ somit} \quad bc = bc + 0 < bc + ac - bc = ac\,.$$

Satz 8.2 *Positive rationale Zahlen* $\frac{a}{c}$ *deren Nenner nur aus den Primfaktoren* 2 *und* 5 *zusammengesetzt sind, besitzen eine ,,abbrechende Dezimalbruchentwicklung"*

$$\frac{a}{c} \;=\; b_n b_{n-1} \ldots b_1 b_0, b_{-1} b_{-2} \ldots b_{-k} \;:=\; b_n 10^n + b_{n-1} 10^{n-1} + \ldots + b_1 10 + b_0 + \frac{b_{-1}}{10} + \ldots \frac{b_{-k}}{10^k}$$

mit Ziffern $b_j \in \{0, 1, \ldots, 9\}\,,\; j = -k, -k+1, \ldots, n-1, n\,.$

Wir dürfen nämlich annehmen, dass a, c positiv und teilerfremd sind. Dann ist $c = 2^s \cdot 5^t$, und mit $k \geq s, t$ ist $\frac{a}{c} \cdot 10^k$ eine natürliche Zahl, auf die wir Satz 4.3 anwenden. Anschließend wird wieder durch 10^k dividiert. Klar, dass man einen entsprechenden Satz für alle g–adischen Stellenwertsysteme formulieren kann.

Klar auch, dass man die Ziffern dieser Entwicklung durch fortgesetzte Division mit Rest erhält wie schon in Abschnitt 4 beschrieben, nur dass jetzt a durch $10^j c$ anstelle von 10^j

dividiert wird und für $j < 0$ stattdessen der Dividend mit 10^{-j} multipliziert wird, bis die Division ohne Rest aufgeht. Man überlege sich, wie das in den auf der Schule verwendeten Algorithmus übersetzt wird!

Natürlich besitzt der Satz 8.2 eine Umkehrung: Wenn $\frac{a}{c}$ eine abbrechende Dezimalbruchentwicklung besitzt, muss $\frac{a}{c} \cdot 10^k \in \mathbf{N}$ sein, bei teilerfremden a, c kann c also nur aus den Primfaktoren von 10 zusammengesetzt sein. Was, wenn diese Voraussetzung nicht erfüllt ist? Unsere Schulerfahrung sagt, dass die fortgesetzte Division dann beliebig weit fortgesetzt werden kann und eine periodische Dezimalbruchentwicklung erzeugt. Warum? Was bedeutet diese? Zu einem tieferen Verständnis sind etliche Vorbereitungen nötig.

Definition 8.2 *Der ,,Betrag"* $|r|$ *der rationalen Zahl* r *ist definiert als*
$|r| := r$ *, wenn* $r \geq 0$ *und* $|r| := -r$ *, wenn* $r < 0$.

Beträge sind vor allem nützlich, um Abstände zwischen Zahlen anzugeben, nämlich in der Form $d(r, s) := |r - s|$, was eine Reihe von Eigenschaften hat, die man vernünftigerweise von Distanzen verlangen sollte: Für alle r, s, t gilt

- $d(r, s) \geq 0$ mit ,, $= 0$ " genau dann, wenn $r = s$,
- $d(r, s) = d(s, r)$
- und die *Dreiecksungleichung* $d(r, t) \leq d(r, s) + d(s, t)$.

All das folgt aus Eigenschaften des Betrages, die man etwa so zusammenstellen kann.

Satz 8.3 *Für alle* $r, s \in \mathbf{Q}$ *gelten*

$$\begin{aligned}
|r| &\geq 0\,, \quad |r| = 0 \quad \textit{nur für} \quad r = 0 \\
|-r| &= |r| \\
|rs| &= |r| \cdot |s| \\
\left|\frac{r}{s}\right| &= \frac{|r|}{|s|}\,, \quad \textit{wenn} \quad s \neq 0 \\
|r+s| &\leq |r| + |s| \\
|r-s| &\leq |r| + |s| \\
\big||r| - |s|\big| &\leq |r| + |s|\,.
\end{aligned}$$

Für das Folgende sollten man sich einige einfache Regeln klarmachen, die daraus folgen:
– Alle x , die von a einen Abstand $< \varepsilon$ haben, erfüllen die Ungleichung $|x-a| = |a-x| < \varepsilon$.
Achtung: Der Buchstabe ε wird in der Analysis immer für eine positive, aber sehr kleine Größe verwendet. Die Menge aller dieser x heißt dann eine *ε–Umgebung* $U_\varepsilon(a)$.
– Wenn x und y in der gleichen ε–Umgebung von a liegen, ist ihr gegenseitiger Abstand $|x - y| < 2\varepsilon$.
– Wenn $x \in U_\varepsilon(a)$ und $y \in U_\varepsilon(b)$, dann liegt $x + y$ in einer 2ε–Umgebung von $a + b$.

9 Konvergenz. Periodische Dezimalbrüche

Definition 9.1 *Eine Folge* $(a_n)_{n\in\mathbf{N}}$ *, also* $a_1, a_2, a_3, \ldots$ *, von (hier zunächst rationalen) Zahlen heißt ,,konvergent" gegen den ,,Limes" oder ,,Grenzwert"* a *, geschrieben*

$$\lim_{n\to\infty} a_n \;=\; a \;,$$

wenn für jedes (noch so kleine) $\varepsilon > 0$ *eine Schranke* $N(\varepsilon)$ *existiert (die i.a. um so größer ausfallen wird, je kleiner man* ε *wählt), so dass*

$$|a_n - a| < \varepsilon \quad \textit{für alle} \quad n \geq N(\varepsilon) \;.$$

Anders gesagt: In jeder noch so kleinen ε*–Umgebung von* a *liegen ,,fast alle" Folgenglieder (Mathejargon für ,,alle bis auf endlich viele" hier also mit der möglichen Ausnahme der* a_n *, für die* $n < N(\varepsilon)$ *).*
Wenn es kein a *gibt, gegen das die Folge konvergiert, heißt die Folge ,,divergent".*

Beispiele. 1. Konstante Folgen, bei denen also $a_n = a$ für ein festes a und alle n ist, sind natürlich gegen a konvergent.
2. $a_n := \frac{1}{n}$ konvergiert gegen 0, weil man jedes noch so kleine $\varepsilon > 0$ mit einem $1/N$ unterbieten kann und darum hat man

$$n \geq N \;\Rightarrow\; |0 - a_n| = \frac{1}{n} \leq \frac{1}{N} < \varepsilon \;.$$

3. Ebenso konvergiert $a_n := (-1)^n/n$ gegen 0.
4. $a_n := (-1)^n$ divergiert, denn bei einer konvergenten Folge müssten die Abstände der Folgenglieder $|a_n - a_m|$ untereinander für hinreichend große $n, m > N$ beliebig klein werden, damit sie in eine gemeinsame ε–Umgebung passen, und das ist hier offensichtlich nicht erfüllt (Light–Version des *Cauchyschen Konvergenzkriteriums*).
5. Aus dem gleichen Grund divergiert die Folge $a_n := b^n$, wenn $b > 1$, denn schon der Abstand zweier benachbarter Folgenglieder wird $a_{n+1} - a_n = (b-1)a_n \geq b - 1$. Durch Induktion erhält man sogar $a_n > n(b-1)$, die Folge wächst also über alle Grenzen.
6. Geht man in Beispiel 5 zu $1/b$ über, so folgt daraus umgekehrt (zunächst für positive $q := 1/b$, dann aber ebenso für die übrigen): Wenn $-1 < q < 1$, dann konvergiert $a_n := q^n$ gegen 0.
Dieses Beispiel ist der Angelpunkt für die Behandlung der *geometrischen Reihe:*

Satz 9.1 *Sei* $-1 < q < 1$ *. Dann ist*

$$1 + q + q^2 + q^3 + \ldots \;=\; \sum_{k=0}^{\infty} q^k \;:=\; \lim_{n\to\infty} \sum_{k=0}^{n} q^k \;=\; \lim_{n\to\infty} \frac{1 - q^{n+1}}{1 - q} \;=\; \frac{1}{1-q} \;.$$

Über das oben gesagte hinaus muss man zum *Beweis* eigentlich nur Satz 2.4, letzte Formel, kennen und über konvergente Folgen $(a_n)_{n\in\mathbf{N}}$ wissen, dass für alle Konstanten b und c gilt

$$\lim_{n\to\infty}(b+a_n) \;=\; b+\lim_{n\to\infty} a_n \quad , \qquad \lim_{n\to\infty} ca_n \;=\; c\lim_{n\to\infty} a_n \; .$$

Mit diesem Satz ist die Bedeutung und die Berechnung des Werts periodischer Dezimalbrüche klar:

$$0,b_1b_2\ldots b_kb_1b_2\ldots b_kb_1b_2\ldots \;:=\; (b_1 10^{k-1}+b_2 10^{k-2}+\ldots+b_k)10^{-k}\sum_{n=0}^{\infty} 10^{-kn} \;=$$

$$=\; (b_1 10^{k-1}+b_2 10^{k-2}+\ldots+b_k)\,\frac{10^{-k}}{1-10^{-k}} \;=\; (b_1 10^{k-1}+b_2 10^{k-2}+\ldots+b_k)\,\frac{1}{10^k-1}$$

Sie stellen also rationale Zahlen dar, deren Nenner (in ungekürzter Form) eine Zahl mit k Ziffern $99\ldots9$ ist. Diese Nenner sind alle teilerfremd zu 10, und umgekehrt gilt:

Satz 9.2 *Sei $d\in\mathbf{N}$ teilerfremd zu 10. Dann gibt es ein $k\in\mathbf{N}$ mit $d \mid 10^k-1$. Somit kann $1/d$ als unendlicher Dezimalbruch mit Periode k geschrieben werden.*

Die Behauptung des Satzes lässt sich in Form der Kongruenz

$$10^k-1\equiv 0 \bmod d \qquad \text{oder} \qquad 10^k\equiv 1 \bmod d$$

schreiben und beruht auf einem Satz der Zahlentheorie und Algebra, der sogar noch mehr sagt: Ein minimal gewähltes k ist Teiler der Anzahl $\varphi(d)$ aller zu d teilerfremden natürlichen Zahlen zwischen 1 und $d-1$. Etwas elementarer kann man folgendermaßen argumentieren: Da es nur endlich viele Restklassen in $\mathbf{Z}/d\mathbf{Z}$ gibt, muss es Exponenten $m<n$ geben, für die $10^m\equiv 10^n \bmod d$ ist. Mit $k:=n-m$ ist also $10^k\cdot 10^m\equiv 10^m \bmod d$, und da 10 und alle Zehnerpotenzen teilerfremd zu d sind, kann man in dieser Kongruenz durch 10^m dividieren und daraus $10^k\equiv 1 \bmod d$ ableiten (ähnlich wie im Beweis von Satz 7.2 löst man die Kongruenz $10^m x\equiv 1 \bmod d$).

Übergang von $1/d$ zu c/d ändert die Ziffernfolge, aber nicht die Periodizität. Damit ist die Natur der Dezimalbruchentwicklungen in den beiden Extremfällen, dass der Nenner d Teiler einer Zehnerpotenz (Satz 8.2) oder teilerfremd zu 10 ist (Satz 9), geklärt. Was passiert in ,,gemischten" Fällen?

Satz 9.3 *Sei $d=d_1d_2\in\mathbf{N}$ mit Faktoren $d_1 \mid 10^m$ und $(d_2,10)=1$. Dann gibt es $x,y\in\mathbf{Z}$ mit*

$$\frac{1}{d} \;=\; \frac{x}{d_1}+\frac{y}{d_2}\;,$$

denn d_1, d_2 sind teilerfremd und darum ist $xd_2 + yd_1 = 1$ ganzzahlig lösbar. Für den Dezimalbruch $1/d$ bzw. allgemeiner c/d heißt das: Die Periodizität ist nach wie vor gegeben, die Periodenlänge hängt nur von dem Faktor d_2 ab, aber es mag eine *Vorperiode* geben, d.h. der Dezimalbruch ist nicht notwendig gleich hinter dem Komma periodisch.

Mit abbrechenden Dezimalbrüchen rechnet es sich leicht, da man einfach nur mit Zehnerpotenzen multiplizieren muss, um die Rechnungen auf das Rechnen mit ganzen Zahlen zurückzuführen. Bei nicht abbrechenden Dezimalbrüchen kämpft man mit zwei misslichen Problemen: Erstens ist die Dezimalbruchdarstellung rationaler Zahlen nicht eindeutig, wie das Beispiel

$$1 \;=\; 1,000\ldots \;=\; 0,9999\ldots$$

zeigt, zweitens steht man vor dem Problem, mit welcher Stelle man die gewohnten Algorithmen, die man aus der Schule für Grundrechenarten kennt, beginnen soll:
$0,7777\ldots \cdot 0,8888\ldots$ rechnet man sicherheitshalber doch besser als $\frac{7}{9} \cdot \frac{8}{9}$. Bei nicht–periodischen unendlichen Dezimalbrüchen fehlt natürlich auch diese Möglichkeit. Warum man auch diese braucht, werden wir gleich sehen.

Zum Schluss dieses Abschnitts sei aber noch angefügt, dass alles, was wir hier für das Dezimalsystem getan haben, entsprechend auf andere g–adische Stellenwertsystem übertragbar ist.

10 Reelle Zahlen. Vollständigkeit

Definition 10.1 *Man nennt ein Folge $(a_n)_{n\in\mathbf{N}}$ von (zunächst einmal) rationalen Zahlen eine „Cauchyfolge", wenn für alle noch so kleinen $\varepsilon > 0$ eine Schranke $N = N(\varepsilon)$ existiert, so dass für alle $n, m \geq N$ gilt*

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

Anschaulich heißt das, dass die Folgenglieder mit wachsendem Index immer dichter liegen. Oben wurde bereits erwähnt, dass alle konvergenten Folgen Cauchyfolgen sind. Ein weiteres Beispiel bilden alle unendlichen Dezimalbrüche, und zwar in folgendem Sinn: Sei $b_k \in \{0, 1, \ldots, 9\}$ eine feste Ziffernfolge mit Indizes $k \in \mathbf{N}$ — wir dürfen auch $k = 0$ und endlich viele negative Indizes zulassen, um Dezimalbrüche mit *Vorkommazahlen* einzuschließen — und die Folge a_n definiert durch die abbrechenden Dezimalbrüche $a_n := \sum_{k\leq n} b_k 10^{-k}$, dann wird diese Folge in der Tat immer dichter, wie man an der Abschätzung

$$|a_n - a_m| \;=\; \sum_{k=m+1}^{n} b_k 10^{-k} \;<\; 10^{-m} \;\leq\; 10^{-N} \quad \text{für alle} \quad n > m \geq N \,.$$

Da wir jedes noch so kleine $\varepsilon > 0$ durch ein solches 10^{-N} unterbieten können, bilden die a_n eine Cauchyfolge. Konvergiert diese Folge? Ja, wenn die Ziffernfolge b_k periodisch

wird, vgl. die Sätze 8.2 und 9.1. Wenn die Ziffernfolge nicht periodisch wird, konvergiert die Folge jedenfalls nicht in unserem bisherigen Zahlbereich $\mathbf{Q}$. Da solche Dezimalbrüche in der ,,Natur" der Geometrie oder Analysis aber vielfältig gebraucht werden, besteht wieder einmal die Notwendigkeit, zu einem größeren Zahlbereich überzugehen, und zwar jetzt zu dem Körper $\mathbf{R}$ der reellen Zahlen. Reelle Zahlen darf man sich wie auf der Schule als die Menge aller $\pm$ Dezimalbrüche vorstellen, abbrechend oder unendlich, periodisch oder nicht–periodisch. Zur Definition eignet sich diese Vorstellung nicht besonders gut, weil (s.o.) mit unendlichen Dezimalbrüchen schlecht zu rechnen ist, und weil offenbar gewisse Identifikationen vorgenommen werden müssen, also wieder eine Klassenbildung bezüglich einer geeigneten Äquivalenzrelation. Wenn man das schon tun muss, kann man auch gleich als Grundmenge alle Cauchyfolgen rationaler Zahlen nehmen und zwei solche Folgen als äquivalent bezeichnen, wenn ihre Differenzfolge gegen 0 konvergiert — man denke etwa an die oben benutzten Folgen abbrechender Dezimalbrüche. Diese kann man dann gliedweise addieren und multiplizieren (in der Tat ein Verfahren, auch für unendliche Dezimalbrüche Rechenoperationen einzuführen, indem man sie durch Folgen abbrechender Dezimalbrüche approximiert), Anordnungen und Beträge einführen und auch wieder Folgen und Konvergenz zu diskutieren. Mühsam, vor allem weil jedesmal auch ,,wohldefiniert" nachgeprüft werden muss!

Es gibt noch andere Möglichkeiten, die reellen Zahlen aus den rationalen zu konstruieren, und diese haben alle ihre Vor– und Nachteile. Insgesamt gilt leider der Erhaltungssatz der mathematischen Schwierigkeit: Es gibt keinen einfachen Weg. Wir begnügen uns, das Endresultat axiomatisch zu beschreiben.

Satz 10.1 *Es gibt einen (im wesentlichen sogar eindeutig bestimmten) Körper* $\mathbf{R}$*, der*

- *(natürlich) Elemente* 0 *und* 1 *sowie Operationen ,,+" und ,,·" besitzt, welche die Körperaxiome erfüllen,*
- *eine Anordnung besitzt, welche verträglich ist mit den Körperoperationen, d.h. die Eigenschaften aus Satz 8.1 erfüllt, in dem insbesondere auch Betrag und Abstand wie in Def. 8.2 eingeführt werden können,*
- *in dem alle Cauchyfolgen konvergieren.*

Die letzte Eigenschaft nennt man *Vollständigkeit.* Dieses Axiomensystem hat — anders als das von Ringen oder Körpern — nicht den denkökonomischen Sinn, viele verschiedene Modelle gleichzeitig zu beschreiben, sondern es dient ähnlich wie das Peano–Axiomensystem der natürlichen Zahlen eher der Klärung der Grundlagen. Einige besondere Eigenschaften der reellen Zahlen (die alle auf $\mathbf{Q}$ nicht zutreffen, ausprobieren!) seien angefügt. *Nach oben beschränkt* heißt eine Menge $U \subset \mathbf{R}$, wenn ein $S \in \mathbf{R}$ existiert mit $x \leq S$ für alle $x \in U$, und S heißt dann *obere Schranke* für U; entsprechend definiert man, was *nach unten beschränkt* bzw. (in beide Richtungen) *beschränkt* sein soll und was ,,beschränkt" für Folgen bedeutet.

Satz 10.2 *1. Monoton wachsende und nach oben beschränkte Folgen* $a_1 \leq a_2 \leq a_3 \leq \ldots$ *konvergieren.*

2. Jede beschränkte Folge besitzt eine konvergente Teilfolge.

3. Jede nichtleere, nach oben beschränkte Untermenge $U \subset \mathbf{R}$ *besitzt eine kleinste obere Schranke.*

11 Polynome

Definition 11.1 *Ein ,,Polynom" $p(x)$,,über einem Körper K " ist eine formale Summe vom Typ*

$$a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \quad \textit{mit ,,Koeffizienten"} \quad a_j \in K \ , \ j = 0, \ldots, n \ .$$

Wenn $a_n \neq 0$ *, heißt* n *der ,,Grad" des Polynoms, geschrieben* $\deg p(x)$ *.*

Für die Zwecke der Elementarmathematik genügt es dabei, anstelle eines allgemeinen Körpers K den Körper der reellen Zahlen $\mathbf{R}$ zu betrachten und das Polynom als eine Funktion

$$p \ : \ \mathbf{R} \to \mathbf{R} \ : \ x \mapsto p(x)$$

anzusehen, in der x einfach die Rolle der Variablen spielt, für die beliebige Werte eingesetzt werden können, gegebenenfalls in Gleichungen wie $p(x) = 0$ auch die Rolle einer *Unbekannten* übernimmt, deren (reeller?) Wert gesucht wird. Schon diese Doppelrolle zeigt, dass es zweckmäßig ist, Polynome nicht nur als Funktionen aufzufassen. Das wird noch deutlicher, wenn K ein endlicher Körper ist wie z.B. $\mathbf{F}_2$, auf dem die beiden Polynome 1 und x^2+x+1 als Funktionen übereinstimmen. Es ist aber nicht sinnvoll, beide zu identifizieren, da sie auf einem etwas größeren Körper $\mathbf{F}_4 \supset \mathbf{F}_2$, den man in der Algebra konstruiert, keineswegs mehr übereinstimmen. Außerdem wäre die oben gegebene Definition des Grades sinnlos.

Wir bleiben also bei der Betrachtungsweise von Polynomen als formalen Summen (kann man vornehmer formulieren, tun wir aber nicht), auch wenn wir nicht wissen, was x eigentlich bedeuten soll. Wichtig ist aber vor allem, dass man mit x so umgeht, als sei es ein Körper– oder Ringelement, damit beim *Einsetzen* spezieller Körperelement a für x alle Rechnungen, die man vorher mit Polynomen gemacht hat, gültig bleiben oder übernommen werden können. Man definiert also eine *Addition von Polynomen* als

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

$$:= (a_m + b_m)x^m + (a_{m-1} + b_{m-1})x^{m-1} + \ldots + (a_1 + b_1)x + a_0 + b_0 \ ,$$

wenn wir o.B.d.A. $n \leq m$ annehmen, indem wir die eventuell fehlenden Koeffizienten $a_{n+1} = a_{n+2} = \ldots = a_m := 0$ setzen. Wie üblich verkürzen wir die Schreibweise dadurch,

dass wir anstelle der Pünktchen–Summen $\sum_{k=0}^{n} a_k x^k$ schreiben. Die *Multiplikation von Polynomen* wird dann so eingeführt, dass alle Ringaxiome gültig sind, dass $x^k x^j = x^{k+j}$ richtig ist, kurz dass bei Einsetzen die Multiplikation von Körperelementen entsteht.

$$\sum_{k=0}^{n} a_k x^k \cdot \sum_{j=0}^{m} b_j x^j \;:=\; \sum_{s=0}^{n+m} \left(\sum_{k+j=s} a_k b_j \right) x^s \;=\; a_n b_m x^{n+m} + \ldots + (a_0 b_1 + a_1 b_0)x + a_0 b_0$$

Da Körper nullteilerfrei sind, liest man an dieser Definition

$$a_n \,,\, b_m \neq 0 \;\Rightarrow\; a_n b_m \neq 0 \,, \quad \text{also} \quad \deg(p(x)q(x)) = \deg p(x) + \deg q(x)$$

ab. Damit dieses Gesetz uneingeschränkt gültig ist, führt man zweckmäßigerweise die Konvention ein, dass das Nullpolynom $p(x) = 0$ den Grad $-\infty$ besitzt. Dieses ist natürlich das neutrale Element für die Addition, das konstante Polynom 1 das neutrale Element für die Multiplikation, und die offensichtlich gültigen Rechenregeln fassen wir zusammen in der Aussage

Satz 11.1 *Die Polynome mit Koeffizienten im Körper K bilden einen Integritätsbereich $K[x]$. Dieser enthält den Körper K in Form der konstanten Polynome (vom Grad 0 und $-\infty$).*

Genau wie für ganze Zahlen kann man *Teilbarkeit* von Polynomen einführen,

$$p(x) \mid q(x) \quad :\Longleftrightarrow \quad \exists\, t(x) \in K[x] \quad \text{mit} \quad p(x)t(x) = q(x) \,,$$

und genau wie für ganze Zahlen gibt es eine *Division mit Rest:*

Satz 11.2 *Seien $a(x), b(x) \in K[x]$ Polynome mit $b(x) \neq 0$. Dann gibt es eindeutig bestimmte Polynome $q(x), r(x) \in K[x]$ mit $\deg r(x) < \deg b(x)$, so dass*

$$a(x) \;=\; q(x)b(x) + r(x) \,.$$

O.B.d.A. sei dazu $n = \deg a(x) \geq m = \deg b(x) \geq 0$ (im Fall $n < m$ könnte man einfach $q = 0$, $r = a$ wählen) mit

$$a(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 \,, \quad b(x) = b_m x^m + b_{m-1} x^{m-1} + \ldots + b_1 x + b_0 \,.$$

Dann ist $a(x) - \frac{a_n}{b_m} x^{n-m} b(x)$ ein Polynom vom Grad $< n$, wir haben also mit $\frac{a_n}{b_m} x^{n-m}$ das Glied höchsten Grades von $q(x)$ gefunden. Von der verbleibenden Differenz kann man wieder genauso ein Vielfaches von $b(x)$ abziehen und das Verfahren fortsetzen bis die verbleibende Differenz einen Grad $< m$ hat. Die Eindeutigkeit ist leicht zu zeigen.

Teilbarkeit von Polynomen ändert sich nicht, wenn man mit Konstanten $\neq 0$ multipliziert, man kann also den *größten gemeinsamen Teiler* $(a(x), b(x))$ als jenes Polynom $d(x)$

höchsten Grades definieren, welches 1 als führenden Koeffizienten besitzt; Ausnahme: Wir setzen wieder $(0,0) := 0$. *Teilerfremd* heißen zwei Polynome dann, wenn sie nur konstante Polynome als gemeinsam Teiler besitzen, m.a.W. wenn $(a(x), b(x)) = 1$ ist. Da Division mit Rest problemlos funktioniert, ist es wenig überraschend, dass man auch hier den ggT durch den euklidischen Algorithmus bestimmen kann, dass sich also die Sätze 6.1 und 6.2 und die eindeutige Primfaktorzerlegung fast wörtlich übertragen lassen.

Satz 11.3 *Seien $a(x), b(x) \in K[x]$ und $b(x) \neq 0$, o.B.d.A. kein Teiler von a. Der größte gemeinsame Teiler von $a(x)$ und $b(x)$ ist bis auf eine Konstante $\neq 0$ der letzte nichtverschwindende Rest $r_n(x)$ im folgenden Schema von Divisionen.*

$$\begin{aligned} a(x) &= q_1(x)b(x) + r_1(x) \\ b(x) &= q_2(x)r_1(x) + r_2(x) \\ r_1(x) &= q_3(x)r_2(x) + r_3(x) \\ \vdots &\ \vdots\ \ \vdots \\ r_{n-3}(x) &= q_{n-1}(x)r_{n-2}(x) + r_{n-1}(x) \\ r_{n-2}(x) &= q_n(x)r_{n-1}(x) + r_n(x) \\ r_{n-1}(x) &= q_{n+1}r_n(x) \end{aligned}$$

Aus dem euklidischen Algorithmus können Koeffizientenpolynome $p(x), q(x)$ für die Darstellung des ggT

$$d(x) = p(x)a(x) + q(x)b(x)$$

als Linearkombination von a und b bestimmt werden.

Definition 11.2 *„Echte Teiler" eines Polynoms $p(x)$ nennen wir Polynome $q(x)|p(x)$ mit $0 < \deg q < \deg p$ und bezeichnen $q(x) \in K[x]$ als „Primpolynom", wenn $q(x)$ keine echten Teiler besitzt und den führenden Koeffizienten 1 hat.*

Satz 11.4 *Jedes Polynom $q(x) \neq 0$ lässt sich als Produkt von Primpolynomen und einer Konstanten schreiben. Diese sind bis auf die Reihenfolge eindeutig bestimmt.*

Beispiele von Primpolynomen sind alle *linearen* Polynome $x - a$, $a \in K$. Diese sind alle verschieden, es gibt also mindestens ebensoviele Primpolynome wie Elemente in K. Warum steht hier $-a$ statt $+a$? Weil dann a eine sehr einleuchtende Sonderrolle für das Polynom spielt, nämlich als (einzige!) *Nullstelle.* Davon mehr im nächsten Abschnitt.
Genau wie wir in Abschnitt 7 die Erweiterung von $\mathbf{Z}$ zu $\mathbf{Q}$ vorgenommen haben, können wir auch hier den Integritätsbereich $K[x]$ in einen Körper $K(x)$ einbetten, dessen Elemente dann *rationale Funktionen*

$$\frac{p(x)}{q(x)}\,, \quad p(x), q(x) \in K[x]\,, \quad q(x) \neq 0\,,$$

sind, mit denen in naheliegender Weise gerechnet wird. Fasst man sie nicht nur als formale Quotienten von Polynomen, sondern als Abbildungen auf, so muss der Definitionsbereich festgelegt werden. Was für ein Problem tritt dabei auf?

12 Polynome als Polynomfunktionen

Polynome $P(x) \in K[x]$ werden wir vermöge der Einsetzung beliebiger Körperelemente für x als Abbildungen, genannt *Polynomfunktionen*, betrachten. $a \in K$ heißt *Nullstelle* von P, wenn $P(a) = 0$ ist. Division mit Rest durch $x - a$ zeigt die erste Behauptung von

Satz 12.1 *$a \in K$ ist genau dann Nullstelle des Polynoms $P \in K[x]$, wenn $x - a$ Teiler von $P(x)$ ist.*
Wenn die Primfaktorzerlegung des Polynoms

$$P(x) \;=\; r \prod_{i=1}^{m} (x - a_i)^{n_i} \prod q_j$$

ist mit $r \neq 0$, $r \in K$ und Primpolynomen q_j vom Grad > 1, dann sind die $a_i \in K$ genau die Nullstellen von P.

Die zweite Behauptung folgt aus der ersten durch sukzessive Division durch lineare Polynome und Anwendung der eindeutigen Primpolynomzerlegung. Die Exponenten n_i heißen *Vielfachheiten* oder *Multiplizitäten* der Nullstellen a_i. Zählt man die Nullstellen mit ihrer Vielfachheit und berücksichtigt, dass Primpolynome q_j vom Grad > 1 keine Nullstellen in K besitzen, dann sieht man:

Satz 12.2 *Ein Polynom $P \in K[x]$ besitzt höchstens $\deg P$ Nullstellen in K. Diese Schranke wird genau dann erreicht, wenn P in $K[x]$ vollständig in Linearfaktoren zerfällt.*

Letztere Bedingung hängt sehr vom verwendeten Körper ab und ist z.B. immer erfüllt, wenn K der Körper der *komplexen Zahlen* ist (sog. *Fundamentalsatz der Algebra*, entgegen seinem Namen aber eher ein Satz der — komplexen — Funktionentheorie, gehört in die Analysis II). Wir werden uns im folgenden vor allem mit reellen Polynomfunktionen befassen. Wenn nichts anderes gesagt wird, setzen wir also im Folgenden meistens voraus, dass die Koeffizienten alle im Körper $K = \mathbf{R}$ der reellen Zahlen liegen.

Wie erhält man Nullstellen von P explizit? Die Frage ist äquivalent dazu, wie man P in Primfaktoren zerlegt, und offenbar dürfen wir o.B.d.A. annehmen, dass P *normiert* ist, d.h. 1 als führenden Koeffizienten besitzt. Klar: $\deg P = 1 \;\Rightarrow\; P(x) = x - a$ für ein $a \in K$. Für *quadratische Polynome* Q, d.h. $\deg Q = 2$, betrachtet man zweckmäßigerweise zuerst den Spezialfall $Q(x) = x^2 + q$. Für $q \in K = \mathbf{R}$ sind drei Fälle zu unterscheiden.

1. $q > 0$: Da $a^2 \geq 0$ für alle $a \in \mathbf{R}$, ist $Q(a) = a^2 + q > 0$, also hat Q keine Nullstelle in $\mathbf{R}$, Q ist prim.

2. $q = 0$: Hier hat Q eine doppelte Nullstelle in $a = 0$, zerfällt in den doppelten Linearfaktor x.

3. $q < 0$: Hier hat Q zwei Nullstellen, die sich nur um das Vorzeichen unterscheiden, genannt $\pm\sqrt{-q}$, und zerfällt in die beiden Primfaktoren $(x - \sqrt{-q})(x + \sqrt{-q})$.

Die letzte Aussage sieht so vertraut aus, als bräuchte sie keine Begründung, trotzdem zwei Versuche dazu: Erstens kann man ausnutzen, dass $Q(0) < 0$ und andererseits $Q(b) > 0$ ist, sobald b genügend groß ist. Dann weiß man, dass zwischen 0 und b mindestens eine Nullstelle von Q liegen muss, weil Q eine *stetige Funktion* ist und darum der sogenannte *Zwischenwertsatz* anwendbar ist, der besagt, dass dann zwischen 0 und b die Funktion Q alle Werte zwischen $Q(0)$ und $Q(b)$ annimmt. „Stetig" bedeutet, dass für alle konvergenten Folgen $(x_n)_{n\in\mathbf{N}}$ auch die Folge $Q(x_n)$ konvergiert, und zwar mit

$$\lim_{n\to\infty} Q(x_n) \;=\; Q(\lim_{n\to\infty} x_n)\,.$$

(Man mache sich klar, dass der Zwischenwertsatz nicht gilt, wenn man die Funktion auf $K = \mathbf{Q}$ einschränkt!) Zweitens kann man die Existenz von Quadratwurzeln positiver Zahlen als Limes geeigneter Cauchyfolgen zeigen — was uns gleichzeitig ein sehr schnelles Berechnungsverfahren liefert.

Satz 12.3 *Sei $r > 0$ und $x_1 \in \mathbf{R}$ mit $x_1^2 > r$ gewählt. Die Folge (x_n) sei rekursiv definiert durch die Vorschrift*

$$x_{n+1} \;:=\; \frac{1}{2}\left(x_n + \frac{r}{x_n}\right) \quad \textit{für alle} \quad n \in \mathbf{N}\,.$$

Dann konvergiert x_n gegen die positive Quadratwurzel von r.

Beweisidee: Wenn man die Konvergenz der Folge gegen a gezeigt hat, wird aus der Rekursionsgleichung im Limes $a = \frac{1}{2}(a + \frac{r}{a})$ also $a^2 = r$. Zum Beweis der Konvergenz genügt es, zu zeigen, dass es sich um eine Cauchyfolge handelt; dazu empfiehlt es sich, induktiv die Ungleichungen

$$\frac{r}{x_1} < \frac{r}{x_2} < \ldots \quad < \quad \ldots x_3 < x_2 < x_1$$

herzuleiten und zu beweisen, dass die Abstände $x_n - \frac{r}{x_n}$ mit wachsendem n gegen 0 konvergieren.
Startet man mit einer rationalen Zahlen r und x_1, so erhält man dabei eine Folge rationaler Zahlen, aber (Satz 7.3) nicht notwendig einen rationalen Grenzwert.

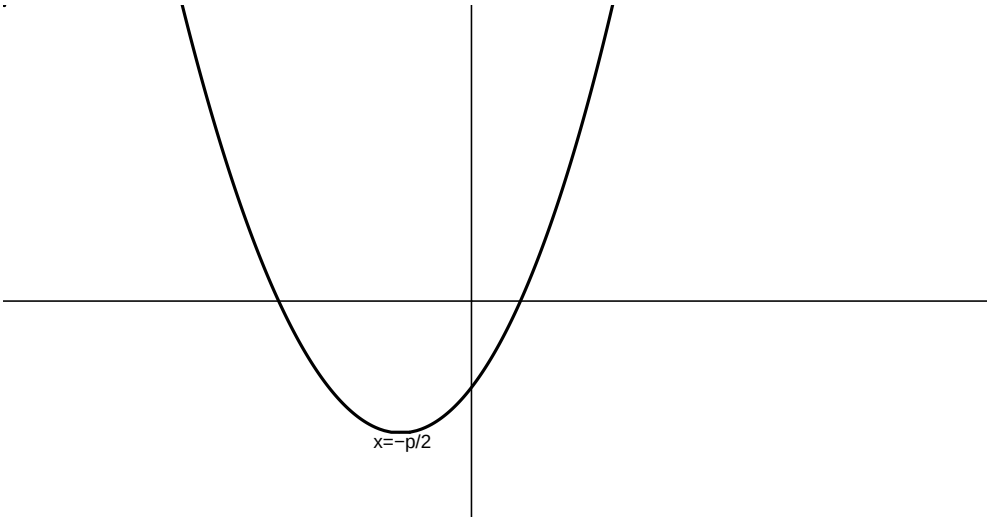
Zurück zu den quadratischen Polynomen, jetzt in immer noch normierter, aber allgemeinerer Form $Q(x) = x^2 + px + q$. Die allgemeine Nullstellengleichung $Q(x) = 0$ lässt sich durch *quadratische Ergänzung* auf den eben diskutierten Spezialfall $p = 0$ zurückführen:

$$x^2 + px + q \;=\; \left(x + \frac{p}{2}\right)^2 + q - \frac{p^2}{4}$$

hat nach dem oben Gesagten die Nullstelle

$$-\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q}\,,$$

wenn der *Radikand* $\frac{p^2}{4} - q \geq 0$ ist.
Geometrische Interpretation: Der *Graph* der Funktion Q, d.h. also die Punktmenge aller $(x, Q(x))$ in der Ebene $\mathbf{R}^2$, ist eine nach oben geöffnete Parabel mit Scheitel bei $x = -\frac{p}{2}$. Die Nullstellen treten bei den Schnitten der Parabel mit der x–Achse $y = 0$ auf, und diese existieren genau dann, wenn der Scheitelpunkt der Parabel (auf oder) unter der x–Achse liegt, also wenn $Q(-\frac{p}{2}) \leq 0$ ist. Das ist gerade dann der Fall, wenn der Radikand ≥ 0 ist.



Geht es nun so weiter für kubische Polynome und Polynome noch höheren Grades? Anders gesagt: Kann man für *algebraische Gleichungen* $P(x) = 0$, $P \in \mathbf{R}[x]$, immer explizite Lösungsformeln angeben, die mit den Grundrechenarten und *Wurzelziehen,* d.h. dem Lösen *reiner Gleichungen* vom Typ $x^m = b$ auskommen? In der ersten Hälfte des 16. Jahrhunderts wurde dieses Problem für $\deg P = 3$ und 4 durch die komplizierten ,,Cardanischen" Formeln gelöst, wahrscheinlich die erste große mathematische Erkenntnis seit der großen Zeit der griechischen Mathematik. Ob Cardano selbst oder doch in Wirklichkeit Tartaglia oder Ferrari oder Scipio del Ferro diese Formeln gefunden hatte, bleibe aber hier außer Betracht. Es hat dann bis zum Beginn des 19. Jahrhunderts gedauert, bis durch Arbeiten von Abel und Galois klar wurde, dass algebraische Gleichungen vom Grad > 4 im allgemeinen nicht *auflösbar* sind, d.h. nicht in der beschriebenen Weise mit Hilfe von Wurzeln und Grundrechenarten gelöst werden können. Der Grund dafür hängt mit hochinteressanten Symmetrieeigenschaften der Lösungen zusammen (*Galoistheorie, Gruppentheorie*) und übersteigt ,,Elementar" mathematik bei weitem. Zum Trost: Schon die Cardanischen Formeln sind — heute jedenfalls — von wenig praktischem Nutzen, da man schöne numerische Verfahren zur näherungsweise Lösung von Gleichungen $P(x) = 0$ hat.

Galoistheorie und Gruppentheorie haben ihre Bedeutung für die Mathematik behalten, allerdings nicht für das Lösen von algebraischen Gleichungen. Eine interessante Konsequenz sei aber erwähnt.

Satz 12.4 *Primpolynome in* $\mathbf{R}[x]$ *haben Grad* 1 *oder* 2 *. Jedes reelle Polynom zerfällt also in lineare und quadratische Faktoren.*

Daraus folgt insbesondere

Satz 12.5 *Das Polynom* $P(x) \in \mathbf{R}[x]$ *besitzt jedenfalls dann eine reelle Nullstelle, wenn* $\deg P$ *ungerade ist.*

Einen *Beweis* von Satz 12.5 mit sehr elementaren Methoden kann man so führen. Sei o.B.d.A. P normiert, d.h. von der Bauart

$$P(x) \;=\; x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$$

und n ungerade. Dann wähle man ein sehr großes positives $M > 1$ so, dass $M > |a_{n-1}| + \ldots + |a_1| + |a_0|$ ist. Daraus folgt für $x > M$ mit Hilfe von Dreiecksungleichung und $x^{n-1} > x^{n-2} > \ldots > x > 1$

$$x^n > Mx^{n-1} > x^{n-1}(|a_{n-1}| + \ldots + |a_1| + |a_0|) \geq |a_{n-1}x^{n-1} + \ldots + a_1 x + a_0|\,,$$

dann ist also auf alle Fälle $P(x) > 0$, weil der führende Term x^n überwiegt. Genauso zeigt man, dass für $x < -M$ wegen des ungeraden führenden Exponenten $P(x) < 0$ wird. P nimmt also positive und negative Werte an, nach dem oben schon erwähnten Zwischenwertsatz also auch den Wert 0 .
Diese Überlegung lässt sich zu einem Berechnungsverfahren für Nullstellen beliebiger stetiger Funktionen ausbauen, solange diese positive und negative Werte besitzen: Seien $x_1, x_2 \in \mathbf{R}$ so gefunden, dass $P(x_1) < 0$, $P(x_2) > 0$, und sei $x_3 := \frac{1}{2}(x_1 + x_2)$. Wenn $P(x_3) = 0$, sind wir fertig. Wenn $P(x_3) < 0$, wähle man x_4 als Mittelpunkt des Intervalls zwischen x_3 und x_2 , wenn $P(x_3) > 0$, sei $x_4 := \frac{1}{2}(x_1 + x_3)$ u.s.w. Bei jedem Schritt wird die Intervalllänge halbiert, die Punkte bilden darum eine Cauchyfolge, und jedes der Intervalle enthält laut Zwischenwertsatz eine Nullstelle, und die Konvergenz der so konstruierten Folge x_n gegen eine Nullstelle von P ist leicht zu beweisen.

In der Tat kann man die Konvergenz noch weiter beschleunigen, wenn man nicht einfach nur das arithmetische Mittel von Intervallendpunkten nimmt. Idee: Man lege in dem Punkt $(x_1, P(x_1))$ des Graphen eine Tangente an den Graphen. Diese ist durch ein lineares Polynom gegeben, dessen Nullstelle einfach zu bestimmen ist und die dann als nächste Approximation x_2 dient. Natürlich muss die Tangente existieren, d.h. P muss differenzierbar sein (richtig für alle Polynome) und die Tangente darf nicht etwa die Steigung 0 oder eine allzu flache Steigung haben, sonst existiert x_2 gar nicht oder liegt weitab von der gesuchten Nullstelle. Analysiert man die Idee im Einzelnen, kommt man auf den folgenden Satz (*Newton–Verfahren*, Gegenstand der Numerik bzw. der Elementaren angewandten Mathematik).

Satz 12.6 *Sei P zwischen a und b zweimal differenzierbar, $a < b$, $P(a) < 0$, $P(b) > 0$, x_1 sei ein Startwert zwischen a und b mit $P(x_1)$, $P'(x_1) > 0$, und es sei $P''(x) > 0$ zwischen a und b. Dann ist die rekursiv definierte Folge*

$$x_{n+1} := x_n - \frac{P(x_n)}{P'(x_n)}$$

wohldefiniert und konvergiert gegen eine (eindeutig bestimmte) Nullstelle von P.

Die Berechnung *aller* Nullstellen eines Polynoms P kann man natürlich so vornehmen, dass man zunächst eine Nullstelle a durch Raten oder nach einem der eben genannten Verfahren bestimmt und P dann durch $x - a$ dividiert; der Quotient hat dann einen kleineren Grad und sollte hoffentlich einfacher zu bearbeiten sein.
Man überzeuge sich davon, dass der Algorithmus zur Berechnung der Quadratwurzel in Satz 12.3 nur ein Spezialfall des Newton–Verfahrens ist, angewandt auf $P(x) = x^2 - r$.

13 Rationale Funktionen

Polynomdivision, Primpolynomzerlegung und Nullstellenbestimmung tragen erheblich zum besseren qualitativen Verständnis des Verhaltens rationaler Funktionen bei, was im Folgenden kurz beschrieben werden soll. Nach Konstruktion von $K(x)$ darf man von jeder rationalen Funktion $R(x) = p(x)/q(x) \neq 0$ voraussetzen, dass Zähler– und Nennerpolynom p, q teilerfremd sind, insbesondere dass q nicht das Nullpolynom ist. Wenn $N \subset \mathbf{R}$ die Nullstellenmenge von q bezeichnet, definiert die Einsetzung reeller Zahlen $a \notin N$ eine Abbildung

$$R : \mathbf{R} - N \to \mathbf{R} : a \mapsto \frac{p(a)}{q(a)},$$

welche wieder stetig und beliebig oft differenzierbar ist. Die Punkte aus N nennt man *Singularitäten* oder *Pole* der Funktion R. Um das Verhalten von R qualitativ zu verstehen, tut man gut daran, einige besonders einfache Typen von Funktionen — die sich nachher als Bausteine aller rationalen Funktionen erweisen werden — vorab zu diskutieren, und zwar hinsichtlich ihres Verhaltens in der Nähe von Singularitäten und für sehr große $|x|$.

1. Polynome und ihre Nullstellen kennen wir aus dem letzten Abschnitt. Das Verhalten für $x \to +\infty$ bzw. $x \to -\infty$, also für sehr große und sehr kleine x wird bestimmt durch den Term mit dem höchsten Exponenten.

2. $R(x) = \frac{1}{x-a}$ hat keine Nullstellen, wird für große $|x|$ beliebig klein (kurz: $\lim_{x\to\pm\infty} R(x) = 0$), hat einen Pol in $x = a$, wächst über alle Grenzen, wenn sich x „von oben" gegen a nähert, und fällt unter alle Grenzen, wenn sich x von unten gegen a nähert. Der Graph hat Hyperbelform.

3. Nun sei $Q(x) = x^2 + px + q$ ein quadratisches Polynom ohne Nullstellen, also mit $p^2 < 4q$. Dann hat $R(x) = \frac{1}{Q(x)}$ weder Nullstellen noch Pole, nimmt ein Maximum in $x = -p/2$ an, dem Scheitelpunkt der Parabel $y = Q(x)$, und erfüllt $\lim_{x\to\pm\infty} R(x) = 0$.

4. Mit dem gleichen quadratischen Polynom sei nun $R(x) = \frac{x-a}{Q(x)}$, dann hat R eine Nullstelle in $x = a$, erfüllt aber nach wie vor $\lim_{x\to\pm\infty} R(x) = 0$, denn der quadratische Nenner wächst viel stärker mit $|x|$ als der lineare Zähler. Ein Minimum links von a und ein Maximum rechts von a findet man am besten mit etwas Differentialrechnung.

Diese Aufzählung ist deswegen so wichtig, weil Abschnitt 11 zwei bequeme Zerlegungsmethoden für rationale Funktionen liefert, die erste per Division mit Rest und die zweite per euklidischem Algorithmus. Beide funktionieren für beliebige Koeffizientenkörper K.

Satz 13.1 *Jede rationale Funktion $R \in K(x)$ lässt sich als $R(x) = A(x) + \frac{B(x)}{C(x)}$ schreiben mit Polynomen $A(x), B(x), C(x) \in K[x]$, dabei $C \neq 0$ und $\deg B < \deg C$.*

Satz 13.2 *Seien $F, G \in K[x]$ teilerfremde Polynome $\neq 0$. Dann gibt es Polynome $A, B \in K[x]$ mit*

$$\frac{1}{F(x)G(x)} = \frac{A(x)}{F(x)} + \frac{B(x)}{G(x)}.$$

Fortgesetzte Anwendung dieser beiden Sätze zeigt also, dass man rationale Funktionen in Summen von Polynomen und rationalen Funktionen $B(x)/C(x)^n$ zerlegen kann, bei denen das Nennerpolynom Potenz eines Primpolynoms C ist und der Zähler einen Grad $\deg B < \deg C^n = n \deg C$ besitzt. Da für $K = \mathbf{R}$ Primpolynome linear oder quadratisch ohne reelle Nullstellen sind, haben wir oben eine Liste wesentlicher Bestandteile. Diese *Partialbruchzerlegung* rationaler Funktionen ist u.a. wichtig für das Auffinden von Stammfunktionen in der Integralrechnung.

14 Elementargeometrie in der Ebene

Geometrie ist ein wesentlich komplexeres mathematisches Arbeitsfeld als *Zahlen*, und der Versuch einer systematischeren Begründung von Geometrie wird erst in der Geometrievorlesung unternommen werden. Trotzdem auch hier schon ein erster Einstieg in geometrische Fragestellungen 1. aus dem praktischen Grund, dass ein Kurs über *Didaktik der Geometrie* schon sehr bald kommt und 2. weil die Notwendigkeit, über den Bereich der rationalen Zahlen hinauszugehen, u.a. aus der Geometrie kommt und insofern ein enger Zusammenhang zum Thema *Zahlbereiche* besteht. Einstweilen wählen wir also erst einen eher naiven Zugang zur ebenen Geometrie, ausgehend von der Frage ,,was kann man mit Zirkel und Lineal alles machen"?

1. Man kann zwei verschiedene Punkte P, Q durch eine eindeutig bestimmte Gerade $g =: PQ$ verbinden. Offenbar gehören *Punkte* und *Geraden* also zu den *Grundbegriffen* der Geometrie, ebenso *Inzidenz*, d.h. also „P liegt auf g" bzw. „g geht durch P". Fasst man Geraden als Punktmengen auf, kann man natürlich einfach „$P \in g$" sagen.

2. Man kann durch zwei Punkte $P \neq Q$ eine Einheitsstrecke $\overline{PQ}$ zwischen den Punkten P und Q auf der Geraden PQ festlegen, diese mit Hilfe des Zirkels auf jede andere Gerade und an jeden Punkt übertragen, Beginn des *Messens*: Streckenlängen lassen sich vergleichen und z.B. vervielfachen.

3. Man kann mit dem Zirkel das *Lot* fällen, d.h. zu jeder Geraden g und einem beliebigen Punkt P auf oder außerhalb der Geraden g eine dazu orthogonale Gerade h durch P konstruieren. Neuer Grundbegriff: *Orthogonalität*. Fast die gleiche Konstruktion liefert das *Mittellot* oder die *Mittelsenkrechte* einer Strecke. Die Wiederholung dieser Konstruktion gibt die Möglichkeit, ausgehend von einer Einheitsstrecke Strecken der Längen $n/2^m$ zu konstruieren und zu messen.

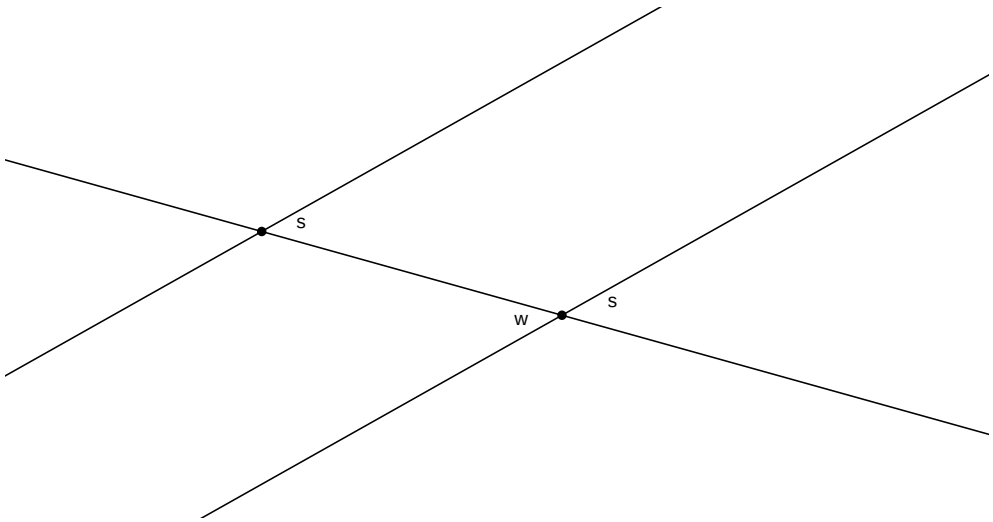
4. Konstruktion der *Winkelhalbierenden*. Ordnet man dem *rechten Winkel* zwischen orthogonalen Geraden den Winkel 90^o bzw. $\pi/2$ zu, dann kann man durch iteriertes Winkelhalbieren und Zusammensetzen von Winkeln eine *Winkelmessung* einführen. Für beliebige Winkel steckt hier natürlich drin, dass man alle Zahlen beliebig gut durch Zahlen vom Typ $\pi n/2^m$ approximieren kann ($n \in \mathbf{Z},\ m \in \mathbf{N}$),

5. Konstruktion von *Parallelen*: Zu jeder Geraden g und jedem Punkt $P \notin g$ kann man mit Zirkel und Lineal (einfacher natürlich mit Lineal und Geodreieck) eine Gerade h konstruieren, die mit P inzidiert und g nicht schneidet, d.h. als Punktmenge $g \cap h = \emptyset$ erfüllt. Dass eine solche Parallele existiert und sogar eindeutig bestimmt ist, sagt das *euklidische Parallelenaxiom*, dessen Gültigkeit alles andere als selbstverständlich ist: Probieren Sie, Geometrie auf der Kugeloberfläche zu entwickeln!

6. Konstruktion von Punkt– und Geraden*spiegelungen*. Man beachte, dass es sich dabei um Bijektionen der Ebene auf sich handelt, welche alle bisher eingeführten geometrischen Sachverhalte und Messgrößen erhalten.

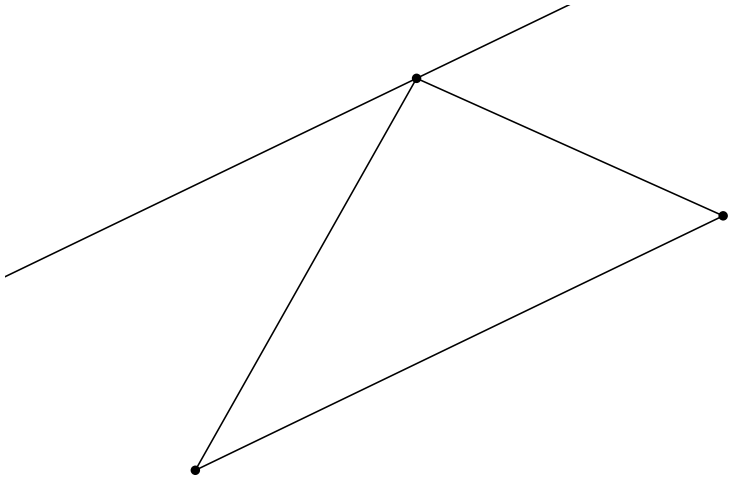
7. Konstruktion von *Translationen* z.B. als Hintereinanderausführung von Spiegelungen an parallelen Geraden und von *Drehungen* z.B. als Hintereinanderausführung von Spiegelungen an sich schneidenden Geraden.

Bei einem mehr systematischen Aufbau der Geometrie spielt die eben genannte *Invarianz* geometrischer Begriffe und Messgrößen eine ganz besondere Rolle. Ihre Bedeutung wird z.B. sichtbar bei der Begründung eines ersten Satzes, den man durch *Parallelverschiebung* längs Geraden (was ist das?) erhält.



Satz 14.1 *Stufenwinkel und Wechselwinkel an Parallelen sind gleich.*

Legt man eine Parallele zur Grundseite eines Dreiecks durch die gegenüberliegende Ecke und addiert die drei so entstehenden Winkel in der Spitze, so ergibt sich



Satz 14.2 *Die Winkelsumme im Dreieck ist* π *.*

Zwei Figuren der Ebene heißen *kongruent*, wenn sie durch eine *Bewegung* der Ebene, d.h. eine Längen– und Winkel–erhaltende Bijektion der Ebene auf sich ineinander übergeführt werden können. Der Name *Kongruenzsätze* für die folgende Zusammenstellung kommt daher, dass die genannten Konstruktionen natürlich nur eindeutig *bis auf Kongruenz* sind,

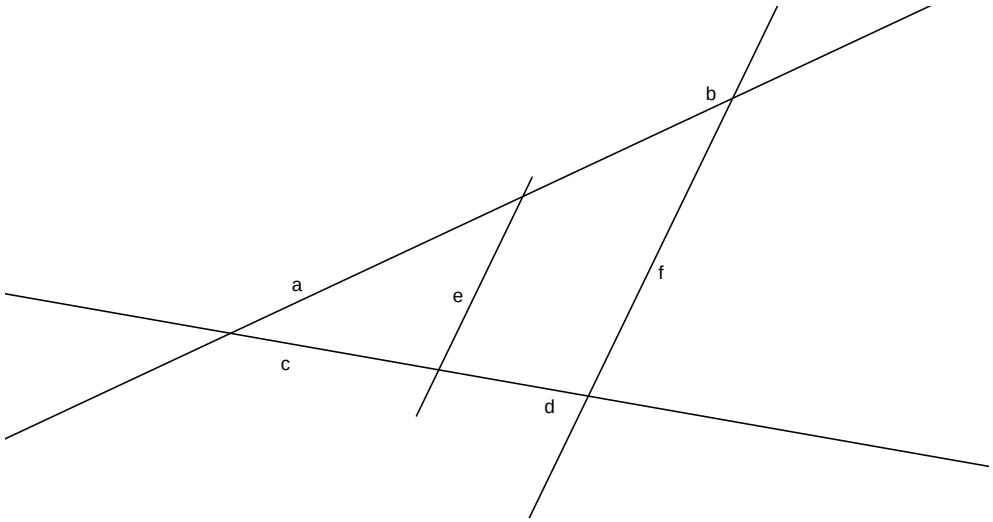
dass man also bestimmte Ausgangsdaten wie einzelne Punkte, Richtungen von Strecken, Orientierung von Winkeln noch frei festlegen kann. Unter *Seite* verstehen wir dabei stillschweigend immer die Seitenlänge (> 0), und *Winkel* sind in diesem Zusammenhang immer > 0 und $< \pi$ (im Rahmen von Analysis oder Elementarmathematik II wird klar, warum die Mathematiker lieber im Bogenmaß als im Gradmaß rechnen).

Satz 14.3 *Dreiecke können eindeutig bis auf Kongruenz konstruiert werden durch die Festlegung von*

- *drei Seiten(längen), wenn die Summe von je zweien größer als die dritte ist (sss),*
- *eine Seite und die beiden angrenzenden Winkel, wenn deren Summe kleiner als π ist (wsw),*
- *zwei Seiten und den eingeschlossenen Winkel (sws),*
- *zwei Seiten und den der größeren Seite gegenüberliegenden Winkel (ssw).*

Dieser Satz ist ein mächtiges Instrument der Elementargeometrie, denn man mag sich überlegen, dass Bewegungen der Ebene bereits durch ihre Wirkung auf ein Dreieck eindeutig bestimmt sind und sich viele ebene Figuren aus Dreiecken zusammensetzen lassen — wenigstens näherungsweise (ausprobieren am Kreis!). Es folgen so z.B. Einsichten über die Natur von Bewegungen oder die Strahlensätze:

Satz 14.4 *Alle ebenen Bewegungen setzen sich aus zwei oder drei Geradenspiegelungen zusammen.*



Satz 14.5 *Gegeben zwei sich schneidende Geraden mit Schnittpunkt P und zwei Parallelen g und h, die P nicht enthalten. Dann gilt für das Verhältnis der Streckenlängen von P bis zu den Schnittpunkten mit g bzw. h (siehe Zeichnung)*

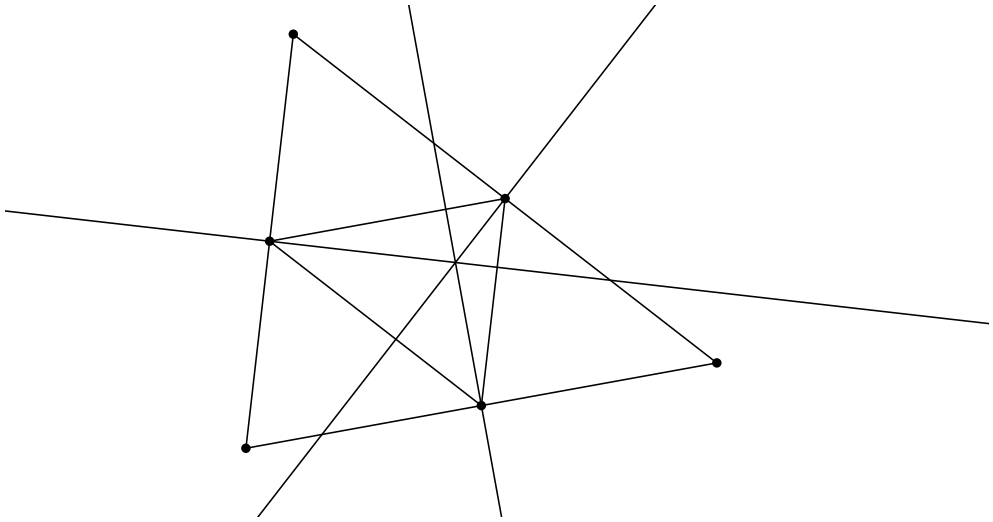
$$a : b = c : d = e : f .$$

Umgekehrt: Wenn $a : b = c : d$, müssen g und h parallel sein.

Damit ist das nötige Instrumentarium beisammen, um die bekannten Sätze über die besonderen Linien im Dreieck zu beweisen. Zur Illustration diene unten eine Zeichnung, welche die Mittelsenkrechten eines größeren Dreiecks als *Höhenlinien* (Lote der Eckpunkte auf die gegenüberliegenden Seiten) des *Mittendreiecks* beschreibt.

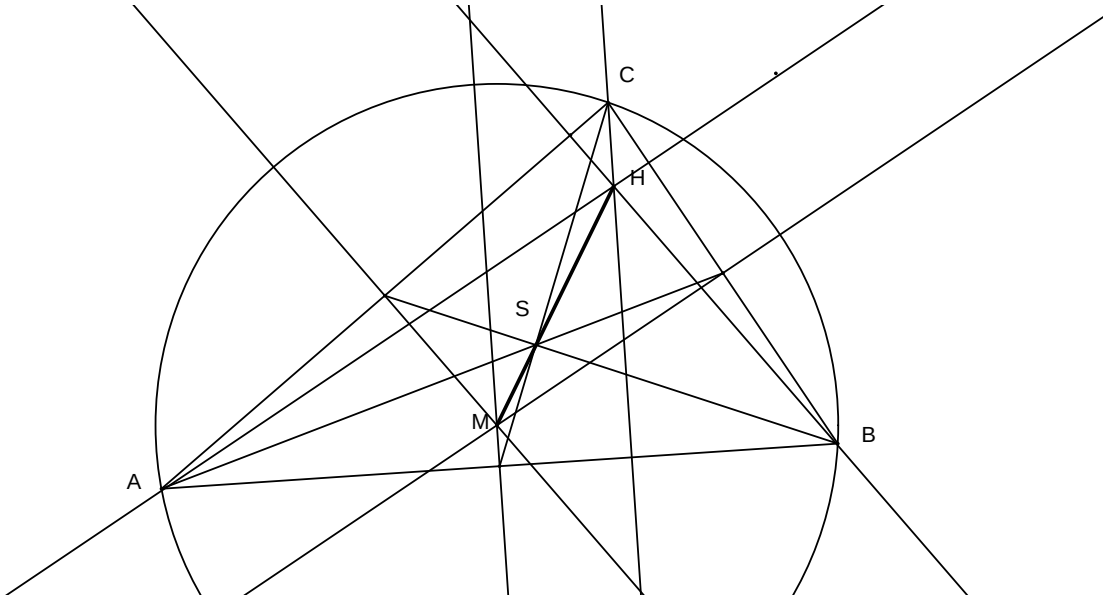
Satz 14.6 *Gegeben ein Dreieck mit Eckpunkten A, B, C. Dann schneiden sich die*

- *Mittelsenkrechten der Seiten in einem Punkt, nämlich dem Umkreismittelpunkt,*
- *Höhenlinien in einem Punkt, dem Höhenschnittpunkt,*
- *,,Seitenhalbierenden" (Verbindungsstrecken zwischen Eckpunkten und gegenüberliegenden Seitenmittelpunkten) in einem Punkt, dem ,,Schwerpunkt" des Dreiecks, der alle Seitenhalbierenden im Verhältnis $2 : 1$ teilt,*
- *Winkelhalbierenden der Innenwinkel in einem Punkt, dem ,,Inkreismittelpunkt" des Dreiecks.*



Zum Abschluss noch ein etwas weniger elementarer Satz von Euler:

Satz 14.7 *In jedem Dreieck liegen der Umkreismittelpunkt M, der Schwerpunkt S und der Höheschnittpunkt H auf einer Geraden, der „Eulerschen Geraden". Die Strecke $\overline{HM}$ wird durch S im Verhältnis $2:1$ geteilt.*

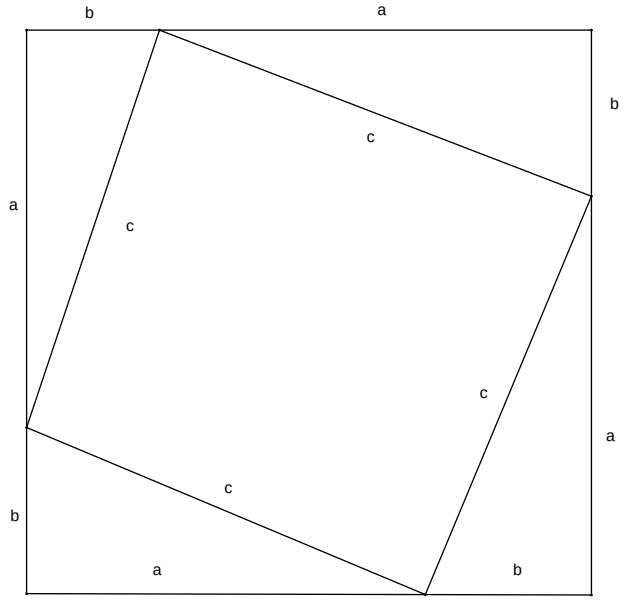


Zum *Beweis* zunächst ein banaler Spezialfall: Wenn $M = S$ ist, stimmen alle Mittelsenkrechten mit den entsprechenden Seitenhalbierenden überein und das Dreieck ist gleichseitig, also gilt sogar $M = S = H$, und dieser Punkt liegt sogar auf vielen Geraden. Sei darum o.B.d.A. $M \neq S$, $e := MS$, und Q sei der Punkt auf e mit $2\overline{MS} = \overline{SQ}$ (hier sind die Streckenlängen gemeint, und S liege zwischen M und Q). Sei M_c der Mittelpunkt von A und B, dann ist nach Satz 14.6 $2\overline{M_cS} = \overline{SC}$, und nach der Umkehrung des Strahlensatzes ist dann die Mittelsenkrechte M_cM parallel zu QC (Achtung: Was passiert im Fall $M_c = M$?), dies muss also die Höhe auf der Seite $c = AB$ sein. Genauso schließt man, dass QA und QB die Höhen auf den beiden anderen Dreieckseiten sind, also ist $Q = H$ der Höhenschnittpunkt.

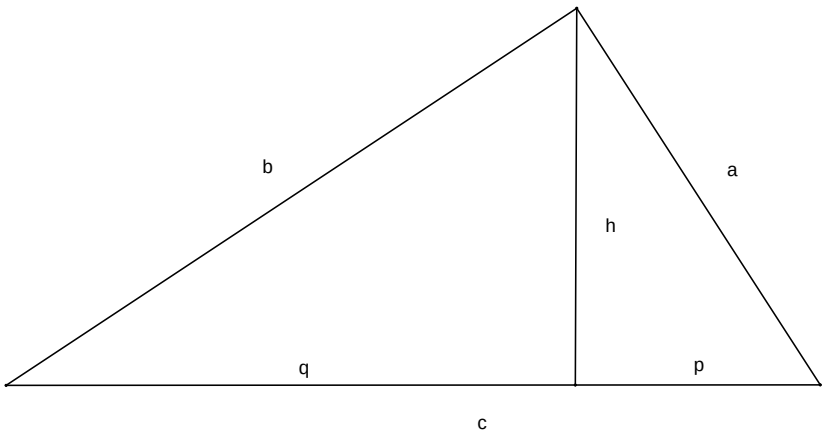
15 Rund um den Satz des Pythagoras

Erinnerung: Dreiecke heißen *rechtwinklig*, wenn zwei Seiten (die *Katheten*, meist mit a, b bezeichnet) senkrecht aufeinander stehen. Die dritte Seite c heißt *Hypotenuse* und wird durch den Höhenfußpunkt in die *Hypotenusenabschnitte* p und q geteilt. Bezeichnet man in der üblichen nachlässigen Notation Seiten und Seitenlängen mit den gleichen Buchstaben und bezeichnet mit h die Länge der Höhenlinie auf der Hypotenuse c, so kann man den Satz des Pythagoras, den *Kathetensatz* und den *Höhensatz* wie folgt formulieren.

Satz 15.1 *Im rechtwinkligen Dreieck gilt* $a^2 + b^2 = c^2$.



Satz 15.2 *Im rechtwinkligen Dreieck gilt* $b^2 = c \cdot q$.



Satz 15.3 *Im rechtwinkligen Dreieck gilt* $h^2 = p \cdot q$.

Einer von einigen möglichen Beweisen des Satzes des Pythagoras (der viel ältere Wurzeln hat und schon den Babyloniern und unabhängig davon den Chinesen bekannt war) ergibt sich aus der Zeichnung oben. Man spricht oft von der *Satzgruppe* des Pythagoras, weil die drei genannten Sätze untereinander logisch äquivalent sind, d.h. aus jedem kann man die beiden anderen herleiten. Dazu muss man nicht sechs Beweise führen, es genügen die folgenden Überlegungen:

15.1 $\Rightarrow$ 15.2 : Anwendung des Pythagoras auf das gesamte sowie auf das rechte und das linke Teildreieck ergibt

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

15.2 $\Rightarrow$ 15.1 durch Anwendung des Satzes auf beide Katheten: $b^2 = cq$ und $a^2 = cp$ $\Rightarrow$ $a^2 + b^2 = c(p+q)$.

15.1, 15.2 $\Rightarrow$ 15.3 folgt aus $h^2 = b^2 - q^2 = (c-q)q$.

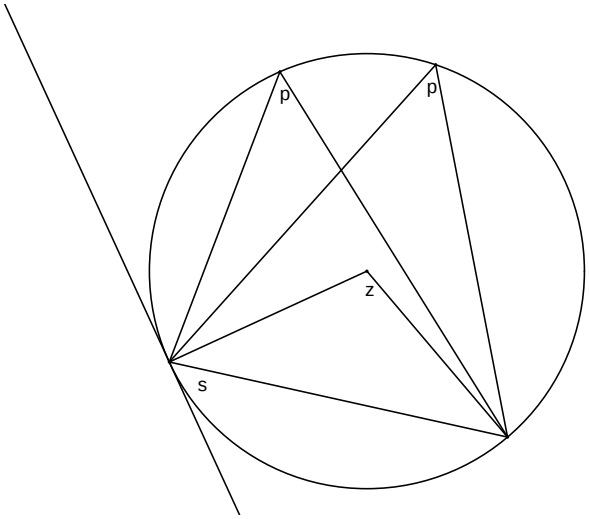
15.3 $\Rightarrow$ 15.1 : Man strecke das rechtwinklige Dreieck um den Faktor $\frac{c}{a}$, dann hat man ein rechtwinkliges Dreieck mit Hypotenuse c^2/a und Katheten cb/a und c , dabei hat die Höhe auf der Hypotenuse die Länge b und der an c anliegende Hypotenusenabschnitt die Länge a . Somit gilt

$$b^2 \;=\; a \cdot (\frac{c^2}{a} - a) \;=\; c^2 - a^2 \; .$$

Direkte Beweise der Sätze 15.2 und 15.3 ohne Verwendung der beiden anderen Sätze ergeben sich z.B. daraus, dass das große Dreieck ähnlich ist zu den beiden Teildreiecken ist. Legt man sie richtig, kann man den Strahlensatz anwenden, um $b : q = c : b$ und $h : q = p : h$ einzusehen.

16 Kreise, Winkel und Strecken

Sei ein Kreis und eine Sehne im Kreis fest gegeben. Wählt man einen dritten Punkt auf dem Kreisbogen über der Sehne, so bildet er mit der Sehne ein Dreieck ABC , dessen Winkel p in der Spitze C über der Sehne $\overline{AB}$, der *Peripheriewinkel*, unabhängig von der Wahl von C auf dem Kreisbogen ist; das ist das Hauptresultat des nun folgenden *Peripheriewinkelsatzes*. Die anderen dort vorkommenden Begriffe sind der *Zentriwinkel* z , den die beiden Radien von A und B zum Mittelpunkt M des Kreises einschließen, sowie der *Sehnentangentenwinkel* s , den die Sehne AB und die Kreistangente im Punkt A (oder B) einschließen.



Satz 16.1 *Unabhängig von der Wahl von C auf dem Kreisbogen gilt stets*

$$p = s\ , \quad z = 2p = 2s\ .$$

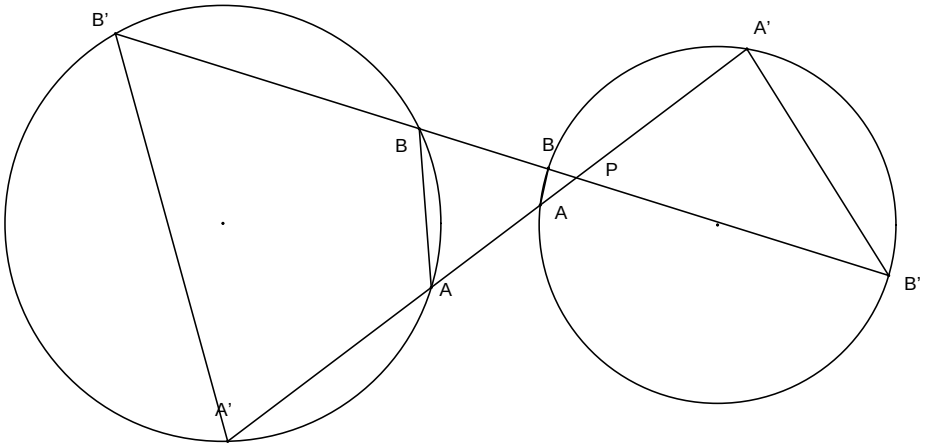
Beweisidee: Alle drei Dreiecke ABM, ACM, BCM sind gleichschenklig, haben also gleiche Winkel an ihrer Basis. Die drei Winkel am Punkt M summieren sich zu 2π, was sich andererseits durch z und p ausdrücken lässt, ausprobieren! Für die Gleichung $z = 2s$ nehme man die Winkel des Dreiecks ABM zu Hilfe, wieder mit Satz 14.2 und der Tatsache, dass $s + \angle MAB = \pi/2$ ist.
Achtung: Was ändert sich an dem Satz, wenn C nicht auf dem Kreisbogen gewählt wird, der auf der gleichen Seite wie M liegt?
Im Grenzfall zwischen den beiden Möglichkeiten ist M gerade der Mittelpunkt von $\overline{AB}$, die Sehne ist ein Durchmesser und der Kreisbogen ein Halbkreis. Da der Zentriwinkel gerade π ist, ergibt sich der *Satz des Thales* „Der Winkel im Halbkreis ist ein Rechter". Da die Umkehrung auch richtig ist, mag man ihn so formulieren:

Satz 16.2 *Das Dreieck ABC hat einen rechten Winkel in C genau dann, wenn $\overline{AB}$ Durchmesser des Umkreises ist.*

Wendet man den Peripheriewinkelsatz auf beide Kreisbögen über und unter der Sehne an, ergibt sich der *Satz vom Sehnenviereck*

Satz 16.3 *Ein Viereck besitzt genau dann einen Umkreis, wenn die gegenüberliegenden Winkel die Winkelsumme π besitzen.*

Weitere Anwendungen des Peripheriewinkelsatzes sind der *Sehnensatz*, der *Sekantensatz* und der *Tangentensatz*.



Satz 16.4 *Gegeben zwei Sehnen durch einen Punkt P im Innern des Kreises mit Endpunkten A, A' bzw. B, B'. Dann gilt für die Streckenlängen*

$$\overline{AP} \cdot \overline{A'P} \;=\; \overline{BP} \cdot \overline{B'P} \;.$$

Satz 16.5 *Das Produkt der beiden Abschnittslängen ist auch dann konstant, wenn P außerhalb des Kreises liegt.*

Satz 16.6

$$\overline{PA} \cdot \overline{PA'} \;=\; \overline{PB}^2 \;,$$

wenn die Gerade PA den Kreis in A und A' schneidet und B der Berührpunkt einer Tangente von P (Punkt außerhalb des Kreises) an den Kreis ist.

Als Beispiel beweisen wir den Sekantensatz. In der Zeichnung berücksichtige man nur die Geraden und den linken Kreis und wende auf das Viereck $A'ABB'$ den Satz vom Sehnenviereck an:

$$\angle ABP = \pi - \angle ABB' = \angle AA'B' \quad \text{und} \quad \angle PAB = \pi - \angle A'AB = \angle A'B'B$$

zeigen, dass die Dreiecke $A'B'P$ und BAP *ähnlich* sind, d.h. die gleichen Winkel besitzen. Aus dem Strahlensatz folgt für die Streckenlängen die Behauptung in der Form

$$\overline{PA} : \overline{PB'} \;=\; \overline{PB} : \overline{PA'} \;.$$

17 Konstruierbarkeit

Zurück zu der Grundsatzfrage aus Abschnitt 14 ,,Was kann man mit Zirkel und Lineal alles machen?". Wir haben eine Reihe von Fundamentalkonstruktionen kennengelernt; dass die Frage aber weit schwerer ist, als es zunächst den Anschein hat, mag man an einer Serie von Problemen sehen, die in der Geometrie der Griechen aufgeworfen wurden und damals nicht beantwortet werden konnten: Kann man mit Zirkel und Lineal

1. aus einem gegebenen Würfel einen Würfel mit doppeltem Rauminhalt konstruieren, d.h. eine Kante um den Faktor $\sqrt[3]{2}$ vergrößern? (sog. ,,Delisches Problem"),
2. einen beliebigen Winkel in drei gleiche Teile teilen,
3. einen zu einem Kreis flächengleiches Quadrat konstruieren (sog. ,,Quadratur des Kreises"),
4. beliebige regelmäßige n–Ecke zeichnen?

Die jeweiligen Antworten sind

1. Nein.
2. Nur in Ausnahmefällen wie z.B. π oder $\pi/2$, aber schon nicht mehr im Fall $\pi/3$.
3. Nein.
4. Nur in Ausnahmefällen, und zwar genau dann, wenn n das Produkt einer Zweierpotenz und paarweise verschiedener Primzahlen der Bauart $2^m + 1$ ist, also für $n = 3, 4, 5, 6, 8, 10, 12, 15, 16, 17, \ldots, 257, \ldots$, nicht aber für $n = 7, 9, 11, 13, 14, \ldots$.

Die Begründungen übersteigen den Rahmen der Elementarmathematik, aber wir wollen sie wenigstens ein Stück weit verfolgen, damit einige der zugrundeliegenden Ideen sichtbar werden. Schon dazu müssen wir etwas vorgreifen und ein paar Fakten aus der Trigonometrie bzw. der analytischen Geometrie einsetzen. Die Fragen kann man jeweils zurückspielen auf die Frage
Gegeben eine Strecke der Länge 1*. Welche Streckenlängen kann man daraus mit Zirkel und Lineal konstruieren?*
Bezeichnet man mit K die so konstruierbaren Streckenlängen, so laufen die oben gestellten Fragen darauf hinaus, ob bzw. für welche reellen α bzw. natürlichen $n > 2$

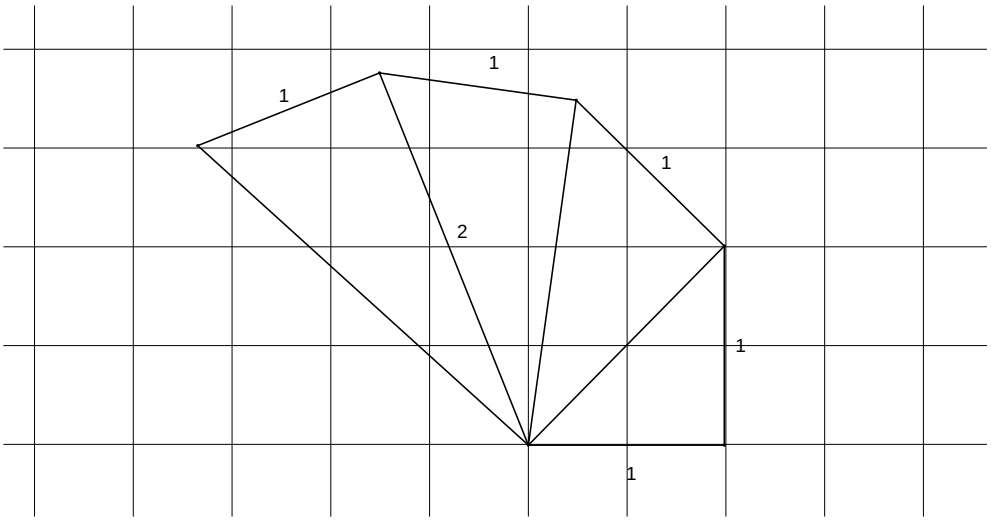
$$\sqrt[3]{2}\,, \quad \sqrt{\pi}\,, \quad \frac{\cos \alpha/3}{\cos \alpha}\,, \quad \cos 2\pi/n \ \in K$$

sind. Wenn man zu K noch 0 sowie alle Zahlen aus $-K$ hinzurechnet, kann man eine zumindest formal einfache Antwort geben:

Satz 17.1 *K ist der kleinste Unterkörper der reellen Zahlen, der mit jedem $r \in K$, $r > 0$, auch seine Quadratwurzel $\sqrt{r}$ enthält.*

Klar dass $K \subset \mathbf{R}$ ist, die 0 und nach Konstruktion auch alle additiven Inversen enthält. Dass man Strecken addieren und subtrahieren kann, ist evident durch Aneinanderanfügen von Strecken auf einer Geraden. Die Möglichkeit von Multiplikation und Division ergibt sich leicht mit Hilfe des Strahlensatzes 14.5 mit Hilfe von Parallelverschiebungen: Man wähle, um z.B. bei gegebenen a und d die Multiplikation $b = ad$ zeichnerisch zu realisieren, $c = 1$ und lese b durch Zeichnen der Parallelen e und f ab. Das Quadratwurzelziehen aus der gegebenen Größe q mache man mit Hilfe des Höhensatzes 15.3: Wähle $p = 1$ und zeichne mit Hilfe des Thaleskreises das rechtwinklige Dreieck aus Satz 15.3, so dass dort $h = \sqrt{q}$ wird.

Wurzeln aus natürlichen Zahlen kann man übrigens sehr hübsch direkt aus dem Satz des Pythagoras konstruieren, indem man mit einem gleichschenklig–rechtwinkligen Dreieck der Kathetenlänge 1 startet, Hypothenuse also von Länge $\sqrt{2}$, diese dann als neue Kathete verwendet, um ein rechtwinkliges Dreieck der Hypothenusenlänge $\sqrt{3}$ daraufzusetzen etc. (s. Zeichnung).



Jetzt fehlt noch die Überlegung, dass bei geometrischen Konstruktionen mit Zirkel und Lineal auch nicht mehr algebraische Operationen mit den gegebenen Daten entstehen können als die Körperoperationen und das Ziehen von Quadratwurzeln. Dazu setzt man Techniken der *analytischen Geometrie* ein; eigentlich genügen dazu Schulkenntnisse, aber man mag das im Geometriekurs des 4. Semesters auffrischen. Angenommen also, man habe in der Ebene mit kartesischen Koordinaten Punkte, Geraden und Kreise konstruiert, deren Koordinaten, Steigungen bzw. Radien alle in dem genannten Körper K liegen. Dann haben alle Abstände zwischen solchen Punkten (x_1, y_1) und (x_2, y_2) die Form $\sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2}$, liegen

also wieder in K . Schnittpunkte solcher Geraden erhält man durch Lösen eines Gleichungssystems

$$y = mx + q \qquad \text{und} \qquad y = ax + b \; .$$

Wenn hier $m, q, a, b \in K$ liegen, dann auch die Koordinaten des Schnittpunkts (wenn er existiert). Das gleiche gilt für die Schnittpunkte einer solchen Gerade mit einem Kreis

$$(x - x_1)^2 + (y - y_1)^2 \; = \; r^2 \; ,$$

wenn die Mittelpunktskoordinaten x_1 und y_1 sowie der Radius r in K liegen, weil man dann quadratische Gleichungen mit Koeffizienten in K zu lösen hat, und nach Abschnitt 12 führt auch diese Aufgabe nicht aus K heraus. Auch beim Schneiden zweier Kreise dieser Art erhält man nur wieder Schnittpunkte mit Koordinaten in K (Übungsaufgabe!), der kleinste Unterkörper von $\mathbf{R}$, in dem Wurzelziehen aus positiven Größen erlaubt ist, ist also die richtige Wahl.

Mit einem nichttrivialen Aufwand an Algebra kann man den fraglichen Körper K etwas näher beschreiben:

Satz 17.2 *Sei K der kleinste reelle Körper, der mit jedem positiven r auch $\sqrt{r}$ enthält. Dann ist jedes $a \in K$ Nullstelle eines eindeutig bestimmten Primpolynoms $P \in \mathbf{Q}[x]$ mit rationalen Koeffizienten; und dessen Grad* $\deg P$ *ist eine Zweierpotenz 2^m .*

Insbesondere besteht K also nur aus *algebraischen Zahlen*, d.h. Nullstellen von Polynomen mit rationalen Koeffizienten. Damit ist bereits klar, dass $\sqrt{\pi} \notin K$, denn π und somit auch $\sqrt{\pi}$ sind *transzendent,* d.h. nicht algebraisch (Lindemann 1882, alle bekannten Beweise sind leider kompliziert). Die Quadratur des Kreises ist also nicht möglich.
Die Unlösbarkeit des Delischen Problems ist mit Satz 17.2 so einzusehen, dass das zu $\sqrt[3]{2}$ gehörige Primpolynom

$$P(x) \; = \; x^3 - 2$$

ist: Es hat nur eine reelle Nullstelle, nämlich $\sqrt[3]{2}$, und könnte darum allenfalls in ein quadratisches Polynom und den Linearfaktor $x - \sqrt[3]{2}$ zerfallen. Dieser liegt aber nicht in $\mathbf{Q}[x]$, weil $\sqrt[3]{2}$ irrational ist, also ist P irreduzibel.
Für die Konstruktion regelmäßiger n–Ecke überlege man sich, dass $\cos \frac{2\pi}{5}$ tatsächlich einer quadratischen Gleichung über $\mathbf{Q}$ genügt — die Konstruktion des regelmäßigen 5–Ecks ist auch seit den Griechen bekannt. $\cos \frac{2\pi}{17}$ ist Nullstelle eines Primpolynoms vom Grad 8 , und Gauss hat eine explizite Konstruktion des regelmäßigen 17–Ecks angegeben. Für $\cos \frac{2\pi}{7}$ ist das Primpolynom kubisch, denn $2 \cos \frac{2\pi}{7}$ ist Nullstelle von

$$P(x) \; = \; x^3 + x^2 - 2x - 1 \; ,$$

und dieses ist irreduzibel (was auch einigen Aufwand an Algebra erfordert), also gibt es keine Konstruktion des regelmäßigen 7–Ecks mit Zirkel und Lineal. Ähnlich ist es mit $\cos \frac{2\pi}{9}$, und damit ist auch klar, dass die Dreiteilung von Winkeln nicht allgemein möglich ist.

Im Zeitalter von CAD sind solche Fragen nach Konstruierbarkeit mit Zirkel und Lineal eher von historischen Interesse. Aber auch früher schon war klar, dass durch eine Erweiterung des Instrumentariums über Zirkel und Lineal hinaus mehr Konstruktionen möglich wurden. Ebenso klar ist, dass man für die genannten Probleme beliebig genaue Näherungslösungen mit Zirkel und Lineal produzieren kann. Von grundsätzlicher Bedeutung ist aber die oben skizzierte Beobachtung, dass Lösbarkeit geometrischer Konstruktionsfragen auf algebraische Probleme zurückgeführt werden kann.

Literatur zur Vorlesung

I. Agricola, Th. Friedrich: Elementargeometrie. Vieweg 2009, EUR 24,90, ISBN 3-528-03221-9

J. Kramer: Zahlen für Einsteiger. Vieweg, EUR 24,90

H. Scheid, W. Schwarz: Elemente der Arithmetik und Algebra, Spektrum, 4. Aufl. 2002, 20,50 EUR ISBN: 3-8274-1386-9

H. Scheid: Elemente der Geometrie, Elsevier/Spektrum, 2006, EUR 22.–, ISBN: 3-8274-1697-3

Index