Elemente der Mathematik

von Peter Koepke

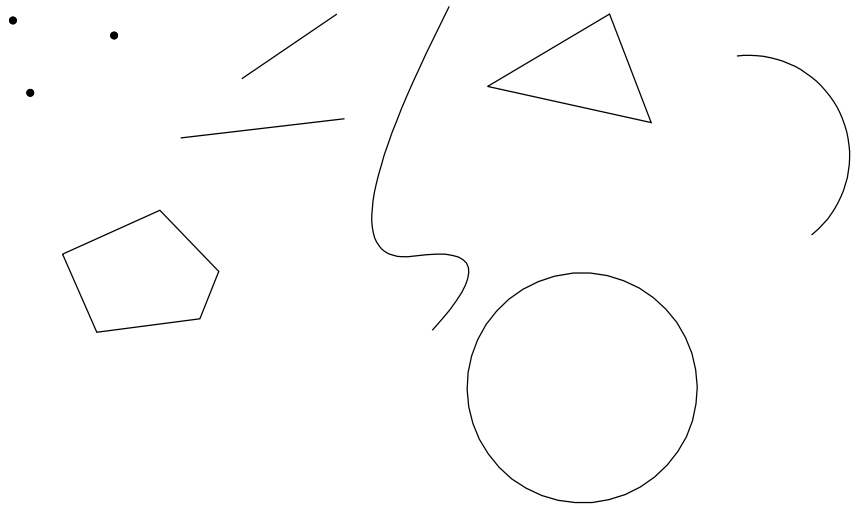
Bonn 2016/17
(unkorrigiertes Vorlesungsskript)

1 Einleitung

Die Vorlesung *Elemente der Mathematik* behandelt die grundlegenden und allgemeinen Gegenst"ande und Begriffe der Mathematik.

Gegenst"ande der Mathematik oder *mathematische Objekte* sind beispielsweise:

- Zahlen: $0, 1, 2, ...,\ -1, -2, ...,\ \frac{3}{5},\ \frac{m}{n},\ \sqrt{2}, e, \pi, ...$
- komplexe Zahlen: $i, 4 + 3\,i$; infinit"are Zahlen: $\infty, \aleph_0, \aleph_1, ...$
- geometrische Figuren:



- Funktionen: x^2, $\sin(x)$, ...
- Mengen von Objekten:
  - $\mathbb{N} = \{0, 1, 2, ...\}$ ist die Menge der nat"urlichen Zahlen
  - $\mathbb{R}$ ist die Menge der reellen Zahlen
- .....

Die Mathematik formuliert und beweist Eigenschaften von Objekten, wie z.B.

- p ist eine Primzahl, 17 ist eine Primzahl, 18 ist keine Primzahl
- zu jeder nat"urlichen Zahl gibt es eine gr"oßere Zahl, die Primzahl ist
- die Winkelsumme in einem Dreieck ist 180 Grad
- $\mathbb{N}$ ist eine Teilmenge von $\mathbb{R}$

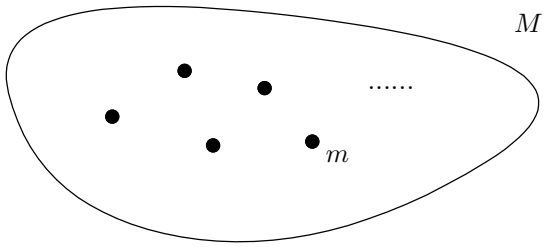
I Wintersemester 2016/2017

2 Informelle Mengenlehre

Der Bereich der mathematischen *Objekte* l"asst sich durch den Begriff der Menge strukturieren. Die Mengenlehre wurde ab 1873 von Georg Cantor "entdeckt". Er charakterisierte Mengen folgendermaßen:

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

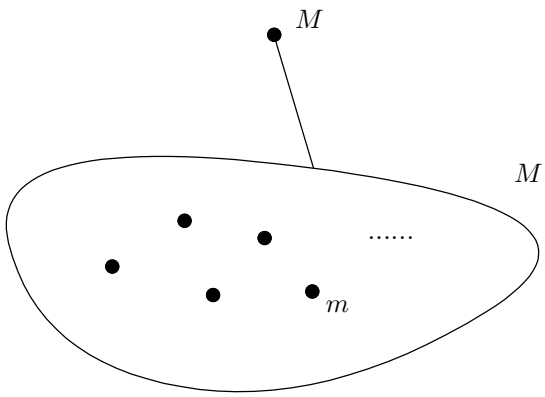
Zusammenfassungen von Objekten werden manchmal graphisch dargestellt:



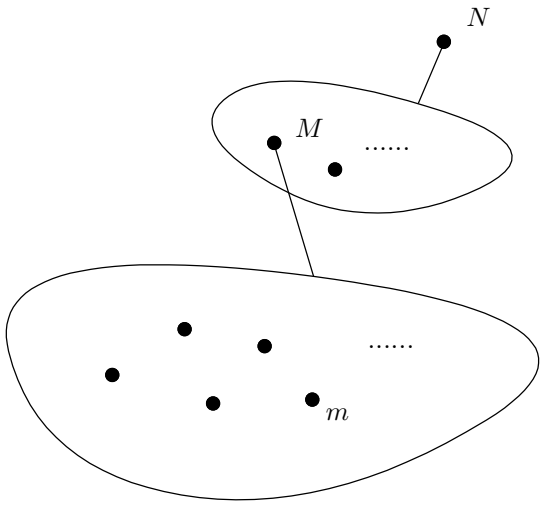
Cantor entwickelte f"ur solche Zusammenfassungen mathematische Begriffe und Gesetze. Felix Hausdorff schrieb 1914 das einflussreiche Buch *Grundz"uge der Mengenlehre*. Er beginnt seine Ausf"uhrungen "ahnlich wie Cantor:

> Eine Menge ist eine Zusammenfassung von Dingen zu einem Ganzen, d.h. zu einem neuen Ding.

Klarer als bei Cantor kommt hier zum Ausdruck, dass eine Zusammenfassung selbst mathematisches Objekt oder "Ding" sein kann. Die Zusammenfassung kann also auch als Punkt in der graphischen Darstellung angesehen werden:



Und das Objekt M kann nun wiederum Element einer Menge N sein:



m ist Element von M, und M ist Element von N. Oder symbolisch: $m \in M \in N$. So ergibt sich eine komplexe Gesamtstruktur, die gen"ugend reichhaltig ist, dass sich alle Gebiete der Mathematik in ihrem Rahmen durchf'uhren lassen.

Hausdorff schrieb in den *Grundz"ugen* hierzu:

> Die Mengenlehre ist das Fundament der gesamten Mathematik.

Wir werden sehen, dass der Mengenbegriff inzwischen “uberall in der Mathematik verwendet wird. Viele Begriffe lassen sich durch Mengen darstellen. Das bedeutet aber nicht, dass die Begriffe der Mathematik Mengen *sind*. Auch wenn man die Zahl 5 durch eine Menge mit genau 5 Elementen darstellen kann, so hat die Zahl 5 dennoch weitere mathematische Aspekte, wie z.B. als L”ange einer Strecke, die besser durch andere Sichtweisen erfasst werden.

Die zentrale Rolle der Mengenlehre in der “New Math” der Schulmathematik der 1970er Jahre war durch die grundlegende und zugleich recht einfach, fast spielerisch erscheinende Theorie motiviert. Inzwischen wird dieser Ansatz aber als didaktisch falsch angesehen und nicht mehr verwendet. “Ubrig geblieben sind mengentheoretische Schreibweisen.

F”ur die Elemente der Mathematik, d.h. f”ur die mathematische Grundlegung und f”ur die Betrachtung von Schulmathematik von einem h”oheren Standpunkt ist die Mengenlehre aber wesentlich. Außerdem bietet uns die Mengenlehre viele Gelegenheiten, mathematisches Beweisen in einem einfachen Bereich kennenzulernen.

3 Mengenlehre

3.1 Elemente und Mengen

Axiom 1. *Wir untersuchen den Bereich der (mathematischen)* Objekte. *Objekte werden durch* Variable $x, y, z, ..., M, N, ..., a, b, c$ *oder durch spezielle* Konstanten *bezeichnet. Zwei Objekte* x, y *sind entweder* gleich*:* $x = y$ *oder* ungleich*:* $x \neq y$.

Typische Konstanten sind die Zahlen $0, 1, 2, ...$.

Axiom 2. *Eine* Zahl *ist ein Objekt.* $0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10$ *sind paarweise verschiedene Zahlen. Paarweise verschieden bedeutet:*

$$\begin{array}{ccccc} 0\neq 1 & 0\neq 2 & 0\neq 3 & 0\neq 4 & ... \\ & 1\neq 2 & 1\neq 3 & 1\neq 4 & ... \\ & & 2\neq 3 & 2\neq 4 & ... \\ & & & 3\neq 4 & ... \\ & & & & \ddots \end{array}$$

Axiom 3. *Eine* Menge *ist ein Objekt.*

Ein Element *einer Menge* M *ist ein Objekt. Wenn* m *Element von* M *ist, so schreiben wir* $m \in M$ *und sagen auch* m *ist in* M *enthalten.*

Wir schreiben $m \notin M$ *wenn* m *nicht in* M *enthalten ist.*

Zusammenfassungen sind dadurch bestimmt, welche Elemente zusammengefasst werden, unabh”angig von ihrer Reihenfolge, oder ob ein Element mehrfach oder nur einfach aufgenommen wird. Die Charakterisierung von Mengen als Zusammenfassungen f”uhrt zu dem folgenden

Axiom 4. (Extensionalit”atsaxiom) Seien M und N Mengen. Wenn jedes Element von M ein Element von N ist, und wenn jedes Element von N ein Element von M ist, dann ist $M = N$.

Mengen sind durch die Angabe ihrer Elemente bestimmt.

Definition 5.

- $\{a, b, c\}$ *ist die Menge der Objekte* a, b *und* c*:* $a \in \{a, b, c\}$, $b \in \{a, b, c\}$, $c \in \{a, b, c\}$, *und wenn* $d \in \{a, b, c\}$ *ist, so ist* $d = a$ *oder* $d = b$ *oder* $c = b$.

– *Allgemeiner ist* $\{a_0, a_1, ..., a_{n-1}\}$ *die Menge der Objekte* $a_0, a_1, ..., a_{n-1}$ *:* $a_0, ..., a_{n-1} \in \{a_0, ..., a_{n-1}\}$*, und wenn* $c \in \{a_0, a_1, ..., a_{n-1}\}$*, so ist* $c = a_0$ *oder* $c = a_1$ *oder ... oder* $c = a_{n-1}$ *.*

Spezialf"alle dieser Definition sind:

– $\{a\}$ *ist die* Einermenge *von* a *.*

– $\{a, b\}$ *ist das* ungeordnete Paar *von* a *und* b *.*

Ein kleiner Beweis erkl"art, wieso dieses Paar als *ungeordnet* bezeichnet wird:

Lemma 6. $\{a, b\} = \{b, a\}$.

Beweis. Sei $c \in \{a, b\}$. Dann ist $c = a$ oder $c = b$. Da $a \in \{b, a\}$ und $b \in \{b, a\}$, ist $c \in \{b, a\}$. Also ist jedes Element von $\{a, b\}$ ein Element von $\{b, a\}$.

Nun sei $c \in \{b, a\}$. Dann ist $c = b$ oder $c = a$. Da $b \in \{a, b\}$ und $a \in \{a, b\}$, ist $c \in \{a, b\}$. Also ist jedes Element von $\{b, a\}$ ein Element von $\{a, b\}$.

Nach dem Extensionalit"atsaxiom ist $\{a, b\} = \{b, a\}$. □

Obwohl die Aussage des Lemmas anschaulich offensichtlich erscheint, muss sie doch aus unseren Axiomen oder *Grundannahmen* bewiesen werden. Es gen"ugt im Prinzip nicht, sich auf einen nat"urlich-sprachlichen Begriff von "Paar" zu berufen oder ein Bild von $\{a, b\}$ zu zeichnen.

Der Beweis des Lemmas benutzt typische Beweisschritte:

1. Es soll das Extensionalit"atsaxiom f"ur die Mengen $M = \{a, b\}$ und $N = \{b, a\}$ benutzt werden. Um $\{a, b\} = \{b, a\}$ zu erhalten, gen"ugt es zu zeigen:

– Jedes Element von $\{a, b\}$ ist ein Element von $\{b, a\}$.

– Jedes Element von $\{b, a\}$ ist ein Element von $\{a, b\}$.

2. Um die *Allaussage* "jedes Element von $\{a, b\}$ ist ein Element von $\{b, a\}$" zu zeigen, wird ein beliebiges Element c von $\{a, b\}$ fixiert und daf"ur $c \in \{b, a\}$ gezeigt. Da $c \in \{a, b\}$ aber beliebig ist, gilt f"ur *jedes* Element von $\{a, b\}$, dass es auch Element von $\{b, a\}$ ist.

Mit denselben einfachen Methoden kann man auch zeigen:

Lemma 7. *Seien* a, b, c *Objekte.*

a) $\{a\} = \{a, a\}$

b) $\{a, b, c\} = \{c, b, a\}$

Beweis. "Ubung □

Definition 8. $\emptyset$ *ist die eindeutig bestimmte Menge, die* kein *Element enth"alt.*

Mengen k"onnen auch durch eine definierende Eigenschaft $A(x)$ bestimmt werden. Wir bezeichnen die Menge aller Objekte x , auf die die Eigenschaft A zutrifft, mit

$$\{x \mid A(x)\}.$$

Lemma 9. *Sei* M *eine Menge. Dann ist* $M = \{x \mid x \in M\}$.

Beweis. Sei $y \in M$. Dann ist $y \in \{x \mid x \in M\}$.

Umgekehrt sei $y \in \{x \mid x \in M\}$. Nach der Definition der Notation $\{x \mid A(x)\}$ ist dann $y \in M$.
Nach dem Extensionalit"atsaxiom ist $M = \{x \mid x \in M\}$. □

Allerdings kann man *nicht* f"ur alle $A(x)$ annehmen, dass die Mengen $\{x \mid A(x)\}$ existiert, weil das zu Widerspr"uchen f"uhren w"urde. Vielmehr werden wir in Definitionen, die $\{x \mid A(x)\}$ benutzen, explizit fordern, dass dies eine Menge ist. Solche Definitionen m"ussen in der Entwicklung der Theorie so verwendet werden, dass die Theorie nicht widerspr"uchlich wird. In mengentheoretischen Axiomensystemen wird geregelt, welche Zusammenfassungen $\{x \mid A(x)\}$ Mengen sind; diese Details "ubersteigen den Rahmen dieser Vorlesung.

Beispiel 10.

a) $\{a_0, ..., a_{n-1}\} = \{x \mid x = a_0 \text{ oder } x = a_1 \text{ oder } ... \text{ oder } x = a_{n-1}\}$;

b) $\emptyset = \{x \mid x \neq x\}$; das Symbol $\neq$ bedeutet dabei "ungleich".

3.2 Teilmengen

Definition 11. *Sei N eine Menge. Eine* Teilmenge *von N ist eine Menge M, so dass jedes Element von M ein Element von N ist. Wir schreiben dann auch $M \subseteq N$. Die Beziehung $\subseteq$ zwischen Mengen wird auch als* Inklusion *bezeichnet.*

Beispiel 12. $\{a, b\} \subseteq \{a, b, c\}$.

Mit der Eigenschaft $\subseteq$ l"asst sich das Extensionalit"atsaxiom umformulieren:

Lemma 13. *Wenn $M \subseteq N$ und $N \subseteq M$, so ist $M = N$.*

Beweis. Sei $M \subseteq N$ und $N \subseteq M$. Nach der Definition der Inklusion ist jedes Element von M ein Element von N und jedes Element von N ein Element von M. Nach dem Extensionalit"atsaxiom ist $M = N$. □

Mengengleichheit wird oft bewiesen, indem die beiden Inklusionen bewiesen werden.

Lemma 14. *Sei M eine Menge. Dann ist $\emptyset \subseteq M$.*

Beweis. Sei $c \in \emptyset$. Nach der Definition von $\emptyset$ ist das ein Widerspruch. Aus einem Widerspruch kann man alles schließen. Insbesondere kann man auf $c \in M$ schließen. Also ist jedes Element von $\emptyset$ ein Element von M. □

Lemma 15. *Sei $M \subseteq \emptyset$. Dann ist $M = \emptyset$.*

Beweis. Nach Lemma 9 ist $\emptyset \subseteq M$. Nach Voraussetzung ist $M \subseteq \emptyset$. Nach Lemma 8 ist $M = \emptyset$. □

$M \subseteq N$ ist eine zweistellige *Relation*, die die Axiome einer *partiellen Ordnung* erf"ullt:

Lemma 16. *Seien M, N, P Mengen*

a) (Reflexivit"at) $M \subseteq M$.

b) (Transitivit"at) $M \subseteq N$ und $N \subseteq P$ impliziert $M \subseteq P$.

c) (Antisymmetrie) $M \subseteq N$ und $N \subseteq M$ impliziert $M = N$.

Bemerkung 17. Der Begriff "Antisymmetrie" bedeutet, dass die Relation "nicht symmetrisch" ist: wenn $M \neq N$ und $M \subseteq N$ dann gilt *nicht* $N \subseteq M$. Denn wenn $N \subseteq M$, dann $M = N$ im Widerspruch zu $M \neq N$.

Beweis. *a)* ist offensichtlich: jedes Element von M ist ein Element von M.

b) Sei $M \subseteq N$ und $N \subseteq P$. Sei $a \in M$. Wegen $M \subseteq N$ ist $a \in N$. Wegen $N \subseteq P$ ist $a \in P$. Also ist jedes Element von M ein Element von P.

c) ist Lemma 8. □

Der Bereich der Mengen mit der Inklusion "ahnelt danach dem Bereich der nat"urlichen Zahlen mit der Ordnungsrelation $\leqslant$.

3.3 Mengenoperationen

Wir definieren "Rechenoperationen" auf Mengen, die der Addition und der Multiplikation auf nat"urlichen Zahlen "ahneln.

Definition 18. *Seien A, B Mengen. Definiere folgende Mengen:*

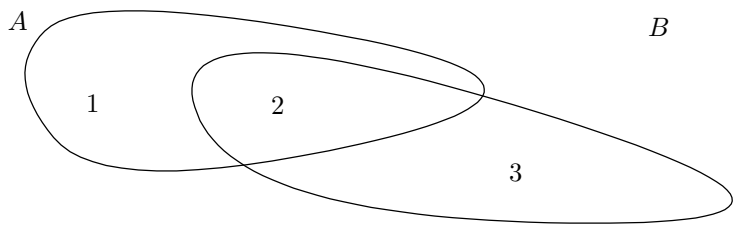
a) $A \cup B = \{x \mid x \in A$ *oder* $x \in B\}$*; $A \cup B$ ist die* Vereinigung *von A und B.*

b) $A \cap B = \{x \mid x \in A$ *und* $x \in B\}$*; $A \cap B$ ist der* Schnitt *von A und B.*

c) $A \setminus B = \{x \mid x \in A$ *und* $x \notin B\}$*; $A \setminus B$ ist die* (Mengen-)Differenz *von A und B.*

d) $A \Delta B = (A \setminus B) \cup (B \setminus A)$*; $A \Delta B$ ist die* symmetrische Differenz *von A und B.*

Diese Operationen lassen sich graphisch anschaulich darstellen.



$A \cup B = 1 + 2 + 3$, $A \cap B = 2$, $A \setminus B = 1$, $A \Delta B = 1, 3$.

Es gelten verschiedene Rechengesetze.

Lemma 19. *Seien A, B, C Mengen. Dann gilt*

a) $(A \cup B) \cup C = A \cup (B \cup C)$ *(*Assoziativit"at *von $\cup$);*

b) $A \cup B = B \cup A$ *(*Kommutativit"at *von* $\cup$*)*

c) $A \cup \emptyset = A$ *(*$\emptyset$ *ist* neutrales Element *von* $\cup$*)*

d) $A \cup A = A$ *(*Idempotenz *von* $\cup$*)*

Diese Gesetze entsprechen den arithmetischen Gesetzen

- $(a+b)+c = a+(b+c)$
- $a+b = b+a$
- $a+0 = a$

Wir beweisen nur das Assoziativgesetz. Die anderen Gleichungen lassen sich sich "ahnlich zeigen.

Beweis. Mengengleichheiten werden m.H. des Extensionalit"atsaxioms gezeigt.

a) **Behauptung:** $(A \cup B) \cup C \subseteq A \cup (B \cup C)$.

Beweis: Sei $x \in (A \cup B) \cup C$. Dann ist $x \in A \cup B$ oder $x \in C$. Dann ist $x \in A$ oder $x \in B$ oder $x \in C$. Dann ist $x \in A$ oder $x \in B \cup C$. Dann ist $x \in A \cup (B \cup C)$. Da $x \in (A \cup B) \cup C$ "beliebig aber fest" war, ist jedes Element von $(A \cup B) \cup C$ ein Element von $A \cup (B \cup C)$. *qed*

Behauptung: $A \cup (B \cup C) \subseteq (A \cup B) \cup C$. Diese Behauptung l"asst sich "genauso" beweisen ("Ubung).

b) **Behauptung:** $A \cup B \subseteq B \cup A$.

Beweis: Sei $x \in A \cup B$. Dann ist $x \in A$ oder $x \in B$. Dann ist $x \in B$ oder $x \in A$. Dann ist $x \in B \cup A$. *qed*

Behauptung: $B \cup A \subseteq A \cup B$. L"asst sich genauso beweisen. □

Lemma 20. *Seien* A, B, C *Mengen. Dann gilt*

a) $(A \cap B) \cap C = A \cap (B \cap C)$ *(*Assoziativit"at *von* $\cap$*);*

b) $A \cap B = B \cap A$ *(*Kommutativit"at *von* $\cap$*)*

c) $A \cap \emptyset = \emptyset$

d) $A \cap A = A$ *(*Idempotenz *von* $\cap$*)*

Diese Gesetze entsprechen den arithmetischen Gesetzen

- $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
- $a \cdot b = b \cdot a$
- $a \cdot 0 = 0$

Das *Distributivgesetz* verbindet Addition und Multiplikation in der Arithmetik:

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

F"ur Vereinigung und Schnitt von Mengen gelten *zwei* Distributivgesetze:

Lemma 21. *Seien* A, B, C *Mengen. Dann gilt*

a) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$*;*

b) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

Beweis. *b*) **Behauptung:** $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$.

Beweis. Sei $x \in A \cup (B \cap C)$. Dann ist $x \in A$, oder $x \in B$ und $x \in C$.

Fall 1. $x \in A$. Dann ist $x \in A \cup B$ und $x \in A \cup C$. Dann ist $x \in (A \cup B) \cap (A \cup C)$.

Fall 2. $x \notin A$. Dann ist $x \in B$ und $x \in C$. Dann ist $x \in A \cup B$ und $x \in A \cup C$. Dann ist $x \in (A \cup B) \cap (A \cup C)$.

In beiden F"allen ist $x \in (A \cup B) \cap (A \cup C)$. *qed*

Behauptung: $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$.

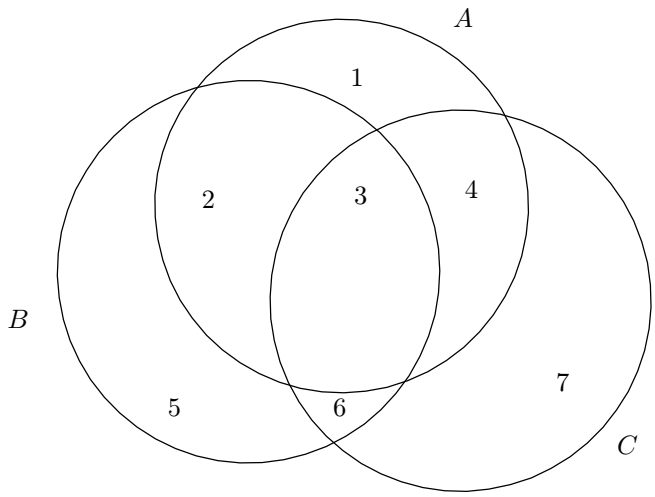
Beweis. Sei $x \in (A \cup B) \cap (A \cup C)$. Dann ist $x \in A \cup B$ und $x \in A \cup C$.

Fall 1. $x \in A$. Dann ist $x \in A$ oder $x \in B \cap C$. Dann ist $x \in A \cup (B \cap C)$.

Fall 2. $x \notin A$. Weil $x \in A \cup B$ ist, ist dann $x \in B$. Weil $x \in A \cup C$ ist, ist $x \in C$. Dann ist $x \in B \cap C$. Dann ist $x \in A \cup (B \cap C)$.

In beiden F"allen ist $x \in A \cup (B \cap C)$. *qed* □

Das Gesetz *a*) entspricht dem Distributivgesetz der Arithmetik, wenn man Vereinigung als Addition und Schnitt als Multiplikation auffasst.



In der Zeichnung ist $A \cap (B \cup C) = A \cap (2+3+4+5+6+7) = 2+3+4$ und $(A \cap B) \cup (A \cap C) = (2+3) \cup (3+4) = 2+3+4$. Man beachte, dass dies *kein* Beweis ist. Insbesondere erfasst die Graphik nicht beliebige Konstellationen der Mengen A, B, C zueinander.

Aufgabe 1. Zeigen Sie, dass das Gesetz *b*) im Bereich der Zahlen falsch ist.

3.4 Inklusion und Mengenoperationen

Im Bereich der (nat"urlichen) Zahlen gibt es Beziehungen zwischen den arithmetischen Operationen $+$ und $\cdot$ und der Ordnungsrelation $\leqslant$. Z.B. folgt aus $m \leqslant m'$ und $n \leqslant n'$, dass $m + n \leqslant m' + n'$. Mengenoperationen und Inklusion stehen auch in verschiedenen Beziehungen.

Lemma 22.

a) $M \subseteq N$ *gdw.* $M \cup N = N$.

b) $M \subseteq N$ *gdw.* $M \cap N = M$.

c) $M \subseteq M'$ *und* $N \subseteq N'$ *impliziert* $M \cup N \subseteq M' \cup N'$.

d) $M \subseteq M'$ *und* $N \subseteq N'$ *impliziert* $M \cap N \subseteq M' \cap N'$.

Beweis. *a)* Sei $M \subseteq N$. F"ur ein Objekt x gilt: wenn $x \in M$ dann $x \in N$.

Angenommen $x \in M$ oder $x \in N$. Dann ist $x \in N$ oder $x \in N$. Somit $x \in N$.

Umgekehrt sei $x \in N$. Dann ist $x \in M$ oder $x \in N$.

Zusammen gilt f'ur alle Objekte x

$$x \in M \text{ oder } x \in N \text{ gdw. } x \in N.$$

Daraus folgt

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

Sei nun $M \cup N = N$. Sei $x \in M$. Dann ist $x \in M \cup N$. Dann ist $x \in N$. Also ist jedes Element von M ein Element von N und $M \subseteq N$.

b) "Ubung.

c) Sei $M \subseteq M'$ und $N \subseteq N'$. Dann ist

$$\begin{aligned}(M \cup N) \cup (M' \cup N') &= (M \cup M') \cup (N \cup N') \\ &= M' \cup N'\end{aligned}$$

Ausf"uhrlicher kann man die formale Rechnung so f'uhren:

$$\begin{aligned}(M \cup N) \cup (M' \cup N') &= ((M \cup N) \cup M') \cup N' \text{ , wegen der Assoziativit"at von } \cup, \\ &= (M \cup (N \cup M')) \cup N' \text{ , wegen der Assoziativit"at von } \cup, \\ &= (M \cup (M' \cup N)) \cup N' \text{ , wegen der Kommutativit"at von } \cup, \\ &= ((M \cup M') \cup N) \cup N' \text{ , wegen der Assoziativit"at von } \cup, \\ &= (M \cup M') \cup (N \cup N') \text{ , wegen der Assoziativit"at von } \cup, \\ &= M' \cup (N \cup N') \text{ , wegen } M \subseteq M', \\ &= M' \cup N' \text{ , wegen } N \subseteq N'.\end{aligned}$$

Wegen *a)* ist dann $M \cup N \subseteq M' \cup N'$.

d) Sei $M \subseteq M'$ und $N \subseteq N'$. Dann ist

$$\begin{aligned}(M \cap N) \cap (M' \cap N') &= (M \cap M') \cap (N \cap N') \\ &= M \cap N\end{aligned}$$

Wegen *a)* ist dann $M \cap N \subseteq M' \cap N'$. □

4 Aussagenlogik

In den bisherigen Beweisen finden wir elementare $\in$-Aussagen der Form $x \in M$, die durch logische Verkn"upfungen wie "und", "oder", "nicht", "wenn ... dann", ... zu komplexeren Aussagen verbunden sind. Beispielsweise lesen wir im Beweis des letzten Lemmas:

... wenn $x \in M$ dann $x \in N$.

Angenommen $x \in M$ oder $x \in N$. Dann ist $x \in N$ oder $x \in N$. Somit $x \in N$.

Umgekehrt sei $x \in N$. Dann ist $x \in M$ oder $x \in N$.

Zusammen ist

$$x \in M \text{ oder } x \in N \text{ gdw. } x \in N.$$

In mathematischen Beweisen wollen wir die Wahrheit von Aussagen zeigen. Dabei ergibt sich die Wahrheit einer komplexen Aussage systematisch aus der Wahrheit oder Falschheit ihrer Teilaussagen.

4.1 Wahrheitswerte

Definition 23. *Wir fixieren die* Wahrheitswerte $\mathbb{F}$ *("falsch") und* $\mathbb{W}$ *("wahr") als zwei verschiedene mathematische Objekte:* $\mathbb{F} \neq \mathbb{W}$. *Auf der Menge* $\{\mathbb{F}, \mathbb{W}\}$ *der Wahrheitswerte vereinbaren wir aussagenlogische Operationen durch "Wahrheitstafeln":*

Das logische oder *ist die Operation* $\vee$ *mit der folgenden Wahrheitstafel:*

$\vee$	$\mathbb{F}$	$\mathbb{W}$
$\mathbb{F}$	$\mathbb{F}$	$\mathbb{W}$
$\mathbb{W}$	$\mathbb{W}$	$\mathbb{W}$

Die Wahrheitstafel ist eine tabellarische oder schematische Schreibweise f"ur die Gleichungen:

$$\mathbb{F} \vee \mathbb{F} = \mathbb{F}, \mathbb{F} \vee \mathbb{W} = \mathbb{W}, \mathbb{W} \vee \mathbb{F} = \mathbb{W}, \mathbb{W} \vee \mathbb{W} = \mathbb{W}.$$

Das logische und *ist die Operation* $\wedge$ *mit der folgenden Wahrheitstafel:*

$\wedge$	$\mathbb{F}$	$\mathbb{W}$
$\mathbb{F}$	$\mathbb{F}$	$\mathbb{F}$
$\mathbb{W}$	$\mathbb{F}$	$\mathbb{W}$

Das logische impliziert *oder* wenn ..., dann *ist die Operation* $\rightarrow$ *mit der folgenden Wahrheitstafel:*

$\rightarrow$	$\mathbb{F}$	$\mathbb{W}$
$\mathbb{F}$	$\mathbb{W}$	$\mathbb{W}$
$\mathbb{W}$	$\mathbb{F}$	$\mathbb{W}$

Hierbei sind die linken Wahrheitswerte als 1. Argument und die rechten als 2. Argument zu verstehen:

$$\mathbb{F} \rightarrow \mathbb{F} = \mathbb{W}, \mathbb{F} \rightarrow \mathbb{W} = \mathbb{W}, \mathbb{W} \rightarrow \mathbb{F} = \mathbb{F}, \mathbb{W} \rightarrow \mathbb{W} = \mathbb{W}.$$

Das logische nicht *ist die Operation* $\neg$ *mit der folgenden Wahrheitstafel:*

$\neg$	
$\mathbb{F}$	$\mathbb{W}$
$\mathbb{W}$	$\mathbb{F}$

D.h. $\neg$ *vertauscht die beiden Wahrheitswerte* $\mathbb{F}$ *und* $\mathbb{W}$.

Definition 24. *Aussagenlogische "Rechenausdr"ucke" sind Terme, die sich mit folgenden Regeln bilden lassen:*

- *die Wahrheitswerte* $\mathbb{F}$ *und* $\mathbb{W}$ *sind aussagenlogische Terme;*
- *die aussagenlogischen Variablen* $X, Y, Z, \ldots$ *sind aussagenlogische Terme, in die beliebige Wahrheitswerte eingesetzt werden k"onnen;*
- *wenn* T, T' *aussagenlogische Terme sind, so auch* $T \vee T'$, $T \wedge T'$, $T \to T'$ *und* $\neg T$.

Beispiele f'ur aussagenlogische Terme sind $X \to Y$, $(X \wedge X) \wedge X$, $\mathbb{W} \to (\mathbb{W} \to \mathbb{F})$, ... Ein Term definiert eine Funktion von Wahrheitswerten, die in die Variablen eingesetzt werden, nach Wahrheitswerten. Da man in jede Variable nur die Argumente $\mathbb{F}$ und $\mathbb{W}$ einsetzen kann, l"asst sich der Werteverlauf eines (kurzen) Terms durch eine Wahrheitstafel darstellen. Die Wahrheitstafel f'ur den Term $(X \wedge (X \to Y)) \to Y$ ergibt sich, indem man f'ur die m"oglichen Werte der Variablen X und Y die Werte der Teilterme $X \to Y$, $X \wedge (X \to Y)$ und $(X \wedge (X \to Y)) \to Y$ nach den obigen Operationstafeln errechnet:

X	Y	$X \to Y$	$X \wedge (X \to Y)$	$(X \wedge (X \to Y)) \to Y$
$\mathbb{F}$	$\mathbb{F}$	$\mathbb{W}$	$\mathbb{F}$	$\mathbb{W}$
$\mathbb{F}$	$\mathbb{W}$	$\mathbb{W}$	$\mathbb{F}$	$\mathbb{W}$
$\mathbb{W}$	$\mathbb{F}$	$\mathbb{F}$	$\mathbb{F}$	$\mathbb{W}$
$\mathbb{W}$	$\mathbb{W}$	$\mathbb{W}$	$\mathbb{W}$	$\mathbb{W}$

Man beachte, dass der Term $(X \wedge (X \to Y)) \to Y$ immer den Wert $\mathbb{W}$ annehmt. Ein Term, der auf diese Weise immer wahr ist, heißt *Tautologie*.

Wie beim Rechnen in Zahlbereichen sind Rechengesetze n"utzlich, mit denen sich Terme umformen lassen. Die Gesetze f'ur $\vee$ und $\wedge$ sind die gleichen wie f'ur die Operationen $\cup$ und $\cap$ auf Mengen.

Lemma 25. *Seien* X, Y, Z *Wahrheitswerte. Dann gilt*

a) $(X \vee Y) \vee Z = X \vee (Y \vee Z)$ *(*Assoziativit"at *von* $\vee$*);*

b) $X \vee Y = Y \vee X$ *(*Kommutativit"at *von* $\vee$*)*

c) $X \vee \mathbb{F} = X$ *(*$\mathbb{F}$ *ist* neutrales Element *von* $\vee$*)*

d) $X \vee X = X$ *(*Idempotenz *von* $\vee$*)*

Beweis. Diese Gesetze lassen sich durch "Uberpr"ufung s"amtlicher M"oglichkeiten zeigen, d.h. durch Wahrheitstafeln. F"ur *a)* haben wir:

X	Y	Z	$X \vee Y$	$Y \vee Z$	$(X \vee Y) \vee Z$	$X \vee (Y \vee Z)$
$\mathbb{F}$	$\mathbb{F}$	$\mathbb{F}$	$\mathbb{F}$	$\mathbb{F}$	$\mathbb{F}$	$\mathbb{F}$
$\mathbb{F}$	$\mathbb{F}$	$\mathbb{W}$	$\mathbb{F}$	$\mathbb{W}$	$\mathbb{W}$	$\mathbb{W}$
$\mathbb{F}$	$\mathbb{W}$	$\mathbb{F}$	$\mathbb{W}$	$\mathbb{W}$	$\mathbb{W}$	$\mathbb{W}$
$\mathbb{F}$	$\mathbb{W}$	$\mathbb{W}$	$\mathbb{W}$	$\mathbb{W}$	$\mathbb{W}$	$\mathbb{W}$
$\mathbb{W}$	$\mathbb{F}$	$\mathbb{F}$	$\mathbb{W}$	$\mathbb{F}$	$\mathbb{W}$	$\mathbb{W}$
$\mathbb{W}$	$\mathbb{F}$	$\mathbb{W}$	$\mathbb{W}$	$\mathbb{W}$	$\mathbb{W}$	$\mathbb{W}$
$\mathbb{W}$	$\mathbb{W}$	$\mathbb{F}$	$\mathbb{W}$	$\mathbb{W}$	$\mathbb{W}$	$\mathbb{W}$
$\mathbb{W}$	$\mathbb{W}$	$\mathbb{W}$	$\mathbb{W}$	$\mathbb{W}$	$\mathbb{W}$	$\mathbb{W}$

Das Assoziativgesetz ergibt sich aus dem Vergleich der beiden rechten Spalten. □

Lemma 26. *Seien X, Y, Z Wahrheitswerte. Dann gilt*

a) $(X \wedge Y) \wedge Z = X \wedge (Y \wedge Z)$ *(*Assoziativit"at *von* $\wedge$*);*

b) $X \wedge Y = Y \wedge X$ *(*Kommutativit"at *von* $\wedge$*)*

c) $X \wedge \mathbb{W} = X$ *(*$\mathbb{W}$ *ist* neutrales Element *von* $\wedge$*)*

d) $X \wedge X = X$ *(*Idempotenz *von* $\wedge$*)*

F"ur $\vee$ und $\wedge$ gelten wiederum zwei Distributivgesetze:

Lemma 27. *Seien X, Y, Z Wahrheitswerte. Dann gilt*

a) $X \wedge (Y \vee Z) = (X \wedge Y) \vee (X \wedge Z)$*;*

b) $X \vee (Y \wedge Z) = (X \vee Y) \wedge (X \vee Z)$*.*

Diese Gesetze erlauben das Umformen von Termen, und sie rechtfertigen auch das "ubliche Weglassen von Klammern. Z.B. k"onnen wir Klammern "ausmultiplizieren".

$$\begin{aligned}(X \vee Y) \wedge (U \vee V) &= ((X \vee Y) \wedge U) \vee ((X \vee Y) \wedge V) \\ &= (U \wedge (X \vee Y)) \vee (V \wedge (X \vee Y)) \\ &= ((U \wedge X) \vee (U \wedge Y)) \vee ((V \wedge X) \vee (V \wedge Y)) \\ &= (U \wedge X) \vee (U \wedge Y) \vee (V \wedge X) \vee (V \wedge Y)\end{aligned}$$

Zusammen mit der Negation $\neg$ ergeben sich weitere wichtige Gesetze:

Lemma 28. *Sein X, Y Wahrheitswerte. Dann gilt*

a) $\neg(\neg X) = X$

b) $\neg(X \vee Y) = (\neg X) \wedge (\neg Y)$

c) $\neg(X \wedge Y) = (\neg X) \vee (\neg Y)$

d) $X \to Y = (\neg X) \vee Y$

e) $X \vee (\neg X) = \mathbb{W}$

b) und c) sind die De Morganschen Gesetze*. e) heißt* tertium non datur*: eine Aussage ist wahr oder falsch, es gibt keine dritten Wahrheitswert.*

Nach *d*) ist eine Implikation wahr, wenn die Pr"amisse falsch ist oder die Konklusion wahr.

Beweis. Wir wollen *c*) aus *a*) und *b*) ableiten:

$$\begin{aligned}\neg(X \wedge Y) &= \neg(\neg(\neg X) \wedge \neg(\neg Y)) \text{ , nach } a) \\ &= \neg(\neg((\neg X) \vee (\neg Y))) \text{ , nach } b) \\ &= (\neg X) \vee (\neg Y) \text{ , nach } a)\end{aligned}$$

□

4.2 Bin"are Arithmetik

Das Rechnen mit Wahrheitswerten "ahnelt dem Rechnen mit Zahlen. Wir k"onnen auf der Menge $\{0, 1\}$ der nat"urlichen Zahlen 0 und 1 Rechenoperationen, die dem Rechnen mit "gerade" und "ungerade" entsprechen, wo z.B. eine Summe von "gerade" und "ungerade" wieder "ungerade" ist:

Definition 29. *Die* bin"are Arithmetik *wird durch folgende Operationen auf* $\{0, 1\}$ *definiert:*

Die bin"are Summe *ist die Operation* $+_2$ *mit der Additionstafel:*

$+_2$	0	1
0	0	1
1	1	0

Die bin"are Multiplikation *ist die Operation* $\times_2$ *mit der Multiplikationstafel:*

$\times_2$	0	1
0	0	0
1	0	1

Man beachte, dass die Tafeln f'ur die Multiplikation und $\wedge$ genau dieselbe Struktur haben:

$\times_2$	0	1
0	0	0
1	0	1

$\wedge$	$\mathbb{F}$	$\mathbb{W}$
$\mathbb{F}$	$\mathbb{F}$	$\mathbb{F}$
$\mathbb{W}$	$\mathbb{F}$	$\mathbb{W}$

Die Tafeln gehen durch Umbennenung der Symbole auseinander hervor. Man sagt dann, dass die Strukturen *isomorph* sind.

Wir definieren eine aussagenlogische Verkn"upfung, die der Addition entspricht: die *"Aquivalenz* ist definiert als

$$(X \leftrightarrow Y) := (X \to Y) \wedge (Y \to X).$$

Dann ist

X	Y	$X \to Y$	$Y \to Z$	$X \leftrightarrow Y$	$\neg(X \leftrightarrow Y)$
$\mathbb{F}$	$\mathbb{F}$	$\mathbb{W}$	$\mathbb{W}$	$\mathbb{W}$	$\mathbb{F}$
$\mathbb{F}$	$\mathbb{W}$	$\mathbb{W}$	$\mathbb{F}$	$\mathbb{F}$	$\mathbb{W}$
$\mathbb{W}$	$\mathbb{F}$	$\mathbb{F}$	$\mathbb{W}$	$\mathbb{F}$	$\mathbb{W}$
$\mathbb{W}$	$\mathbb{W}$	$\mathbb{W}$	$\mathbb{W}$	$\mathbb{W}$	$\mathbb{F}$

Die Verkn"upfungstafeln f'ur die Addition und f'ur die negierte "Aquivalenz sind isomorph:

$+_2$	0	1
0	0	1
1	1	0

$\neg(X \leftrightarrow Y)$	$\mathbb{F}$	$\mathbb{W}$
$\mathbb{F}$	$\mathbb{F}$	$\mathbb{W}$
$\mathbb{W}$	$\mathbb{W}$	$\mathbb{F}$

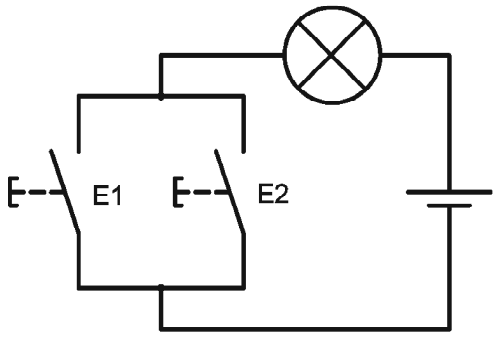
Die negierte "Aquivalenz ist auch das *exklusive Oder*, das dem sprachlichen "entweder ... oder ..." entspricht:

$$\begin{aligned}
\neg(X \leftrightarrow Y) &= \neg((X \to Y) \wedge (Y \to X)) \\
&= (\neg(X \to Y)) \vee (\neg(Y \to X)) \\
&= (\neg((\neg X) \vee Y)) \vee (\neg((\neg Y) \vee X)) \\
&= ((\neg(\neg X)) \wedge (\neg Y)) \vee ((\neg(\neg Y)) \wedge (\neg X)) \\
&= (X \wedge \neg Y) \vee (Y \wedge \neg X)
\end{aligned}$$

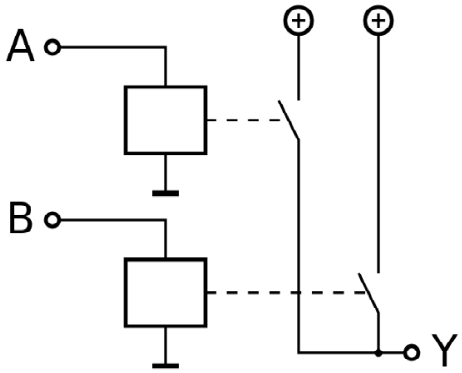
4.3 Digitale Logik und Arithmetik

Die moderne Digitaltechnik beruht auf digitaler Logik und Arithmetik, die sich sehr gut elektrisch implementieren l"asst.

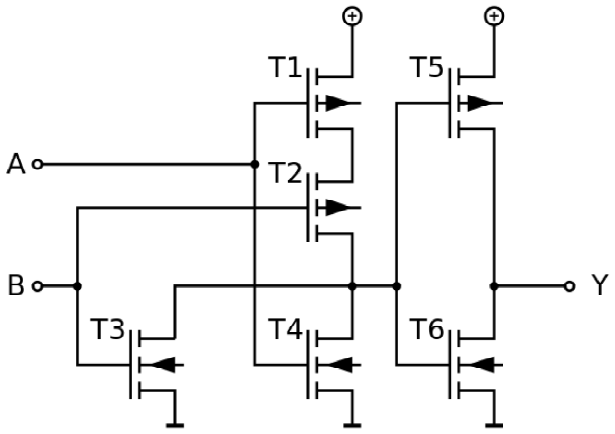
Die Wahrheitswerte $\mathbb{F}$ und $\mathbb{W}$ werden durch Spannung oder Strom "an" bzw. "aus" dargestellt. Mit Schaltern kann man das logische Oder realisieren als:



Und mit Relais:



Und elektronisch mit Transistoren:



Die Addition der einstelligen Bin"arzahlen $m = 0$ und $n = 1$ hat folgende Additionstafel im Dualsystem (Halb-Addierer):

m	n	"Ubertrag	Summe
0	0	0	0
0	1	0	1
1	0	0	1
1	1	1	0

Die Summe l"asst sich mit dem exklusiven Oder realisieren, der "Ubertrag mit einem logischen Und. Wenn man noch einen "Ubertrag u "von rechts" zul"asst, so erh"alt man einen Voll-Addierer:

$m = X$	$n = Y$	$u = Z$	"Ubertrag	Summe
0	0	0	0	0
0	0	1	0	1
0	1	0	0	1
0	1	1	1	0
1	0	0	0	1
1	0	1	1	0
1	1	0	1	0
1	1	1	1	1

Diesen "Ubertrag kann man durch folgenden Term realisieren:

$$(\neg X \wedge Y \wedge Z) \vee (X \wedge \neg Y \wedge Z) \vee (X \wedge Y \wedge \neg Z) \vee (X \wedge Y \wedge Z).$$

Diese Formel kann man in der Arithmetik der Wahrheitswerte umformen, um z.B. eine bessere Implementierung zu finden. Sie ist beispielsweise "aquivalent zu:

$$(X \wedge Y) \vee (X \wedge Z) \vee (Y \wedge Z).$$

Durch Zusammenschalten von Voll-Addierern kann man eine Schaltung zum Addieren von Dualzahlen mit vielen Stellen aufbauen. Wir werden sp"ater auf duale Arithmetik und Arithmetik zu anderen Grundzahlen zur"uckkommen.

4.4 Wahrheitswerte mathematischer Aussagen

Wir sehen "elementare" Ausdr"ucke oder Formeln als gegeben an und stellen daraus komplexe Formeln her, wie wir sie in den mengentheoretischen "Uberlegungen bereits angetroffen haben.

Definition 30. *Aussagenlogische Formeln lassen sich mit folgenden Regeln bilden:*

- *die Wahrheitswerte* $\mathbb{F}$ *und* $\mathbb{W}$ *sind aussagenlogische Formeln;*
- *elementare Ausdr"ucke wie* $x = y$ *oder* $x \in M$ *sind aussagenlogische Formeln*
- *wenn* φ, φ' *aussagenlogische Formeln sind, so auch "*φ *oder* φ'*", "*φ *und* φ'*", "*φ *impliziert* φ'*", und "nicht* φ*".*

Wenn wir voraussetzen, dass jeder elementare Ausdruck (in einer festen Situation) falsch oder wahr ist, so k"onnen wir allen aussagenlogischen Formeln einen Wahrheitswert geben.

Definition 31. *Wir definieren den Wahrheitswert* $\|\varphi\|$ *einer aussagenlogischen Formel* φ *folgendermaßen:*

- $\|\mathbb{F}\| = \mathbb{F}$ *und* $\|\mathbb{W}\| = \mathbb{W}$*;*
- *f"ur einen elementaren Ausdruck* φ *sei* $\|\varphi\| = \mathbb{F}$*, wenn* φ *falsch ist, und* $\|\varphi\| = \mathbb{W}$*, wenn* φ *wahr ist;*
- $\|\varphi \text{ oder } \varphi'\| = \|\varphi\| \vee \|\varphi'\|$
- $\|\varphi \text{ und } \varphi'\| = \|\varphi\| \wedge \|\varphi'\|$

- $\|\varphi \textit{ impliziert } \varphi'\| = \|\varphi\| \to \|\varphi'\|$
- $\|\textit{nicht } \varphi\| = \neg\|\varphi\|$.

Eine aussagenlogische Formel φ heißt wahr*, wenn $\|\varphi\| = \mathbb{W}$ ist.*

Die Wahrheit einer solchen Formel beruht auf Rechengesetzen von Wahrheitswerten und nicht auf weiteren anschaulichen Aspekten. So wird beim "und" von zeitlicher Abfolge abstrahiert, und bei der Implikation sind keine inhaltlichen Zusammenh"ange zwischen 1. und 2. Argument n"otig.

Nach den Regeln f'ur die Implikation "wenn ..., dann" ist die Aussage "wenn $x \in M$, dann $x \in N$" in folgenden Situationen **wahr**:

- $x \in M$, $x \in N$
- $(*)$ $x \notin M$, $x \in N$
- $x \notin M$, $x \notin N$

Sie ist **falsch** in folgender Situation:

- $x \in M$, $x \notin N$

Man beachte die Situation $(*)$: eine Implikation ist auch dann wahr, wenn die linke Seite falsch aber die rechte wahr ist:

- wenn es regnet, ist die Erde nass

Diese Implikation sehen wir gew"ohnlich als wahr an. Sie soll *immer* richtig sein, insbesondere auch unmittelbar nach einem Regen, wenn folgende Situation vorliegt:

- es regnet *nicht*, die Erde ist nass

Und sie soll auch bei sch"onem Wetter gelten, wenn:

- es regnet *nicht*, die Erde ist *nicht* nass

Diese vern"unftige Rechenregel f'ur die Wahrheit einer Implikation erscheint allerdings in gewissen Aussagen nicht nat"urlich:

- wenn $0 = 3$ ist, dann ist $11 = 11$.

Es ist anschaulich nicht klar, wie eine falsche Aussage eine richtige in einem "eigentlichen Sinn" implizieren sollte. Aber darum geht es hier nicht, sondern um eine klar geregelte Zuordnung von Wahrheitswerten.

4.5 Aussagenlogisches Beweisen

In der Mathematik werden wahre mathematische Aussagen identifiziert und ihre Wahrheit bewiesen. Es gibt verschiedene Beweismethoden, von denen wir einige bereits kennengelernt haben. Ein Beweis besteht aus einer Reihe von Beweisschritten, in denen nach gewissen Beweismethoden neue wahre Aussagen aus bereits etablierten wahren Aussagen abgeleitet werden.

4.5.1 Tautologische Beweise

Wenn $...X...Y...Z...$ eine aussagenlogische Tautologie in den Variablen $X, Y, Z, ...$ ist, und wenn man beliebige Aussagen f'ur die Variablen einsetzt, so ergibt sich eine wahre Aussage. Diese Aussage ist dann *tautologisch* bewiesen.

Beispielsweise ist $X \vee \neg X$ eine Tautologie, und damit ist die Aussage "n ist eine Primzahl oder n ist keine Primzahl" wahr, unabh"angig von einer konkreten nat"urlichen Zahl n und unabh"angig davon, ob wir f"ur gegebenes n entscheiden k"onnen, ob es Primzahl ist oder nicht.

4.5.2 Modus ponens

Wenn φ und "φ impliziert ψ" wahr sind, so ist ψ wahr. Denn $\|\varphi \text{ impliziert } \psi\| = \|\varphi\| \to \|\psi\| = \mathbb{W}$ und $\|\varphi\| = \mathbb{W}$ erzwingt, dass $\|\psi\| = \mathbb{W}$.

Beispielsweise sei $\varphi =$ "$x \in M$ und $x \in N$" bereits gezeigt oder angenommen; man kann tautologisch beweisen, dass "$x \in M$ und $x \in N$ impliziert $x \in N$"; dann ist "$x \in N$" auch wahr.

4.5.3 Fallunterscheidung

Wenn "φ impliziert ψ" und "nicht φ impliziert ψ" bewiesen sind, so ist auch ψ bewiesen. Das ergibt sich aus der Tautologie

$$((X \to Y) \wedge (\neg X \to Y)) \to Y.$$

Diese Tautologie ergibt sich aus der Gleichungskette

$$\begin{aligned}
(X \to Y) \wedge (\neg X \to Y) &= (\neg X \vee Y) \wedge (\neg\neg X \vee Y) \\
&= (\neg X \vee Y) \wedge (X \vee Y) \\
&= (\neg X \wedge X) \vee (\neg X \wedge Y) \vee (Y \wedge X) \vee (Y \wedge Y) \\
&= \mathbb{F} \vee (Y \wedge \neg X) \vee (Y \wedge X) \vee Y \\
&= (Y \wedge (\neg X \vee X)) \vee Y \\
&= (Y \wedge \mathbb{W}) \vee Y \\
&= Y \vee Y \\
&= Y
\end{aligned}$$

Im Beweis von $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$ hatten wir angenommen, dass $x \in (A \cup B) \cap (A \cup C)$. Zu zeigen war, dass $x \in A \cup (B \cap C)$.

Das Argument benutzte eine Fallunterscheidung: Unter der Annahme ist $x \in A \cup B$ und $x \in A \cup C$.

Fall 1. $x \in A$. Dann ist $x \in A$ oder $x \in B \cap C$. Dann **gilt die Behauptung** $x \in A \cup (B \cap C)$.

Fall 2. $x \notin A$. Weil $x \in A \cup B$ ist, ist dann $x \in B$. Weil $x \in A \cup C$ ist, ist $x \in C$. Dann ist $x \in B \cap C$. Dann **gilt die Behauptung** $x \in A \cup (B \cap C)$.

In beiden F"allen ist $x \in A \cup (B \cap C)$.

4.5.4 Widerspruchsbeweis

Wenn "nicht φ impliziert $\mathbb{F}$" wahr ist, dann ist φ wahr. Denn

$$\begin{aligned}
\neg X \to \mathbb{F} &= \neg\neg X \vee \mathbb{F} \\
&= \neg\neg X \\
&= X
\end{aligned}$$

Man kann also φ beweisen, indem man $\neg\varphi$ annimmt und dieses zum Widerspruch f"uhrt. Einen solchen Beweis nennt man *Widerspruchsbeweis* oder *indirekten* Beweis.

Ein Musterbeispiel f"ur einen Widerspruchsbeweis ist der Beweis von

Satz 32. *$\sqrt{2}$ ist irrational, d.h. $\sqrt{2}$ ist keine rationale Zahl.*

Beweis. Angenommen, die Behauptung ist falsch: $\sqrt{2}$ ist eine rationale Zahl.

Seien m, n ganze Zahlen mit

(1) $\sqrt{2} = \frac{m}{n}$.

Wir k"onnen außerdem annehmen, dass der Bruch $\frac{m}{n}$ gek"urzt ist.

Aus (1) folgt durch Quadrieren

$$2 = \frac{m^2}{n^2}$$

und

$$2 \cdot n \cdot n = m \cdot m.$$

Die linke Seite der Gleichung ist als Vielfaches von 2 gerade ist. Daher ist die rechte Seite gerade, und m ist eine gerade Zahl. Division beider Seiten der Gleichung durch 2 ergibt

$$n \cdot n = m \cdot \frac{m}{2}.$$

Die rechte Seite dieser Gleichung ist als Vielfaches von m gerade. Daher ist die linke Seite gerade, und n ist eine gerade Zahl.

Die Zahlen m und n sind durch 2 teilbar, und der Bruch $\frac{m}{n}$ ist nicht gek"urzt **Widerspruch**!

Nach dem Prinzip des Widerspruchsbeweises ist die **Behauptung wahr**. □

4.6 Quantorenlogische Formeln

Definition 33. *Quantorenlogische Formeln lassen sich mit folgenden Regeln bilden:*

- *aussagenlogische Formeln sind quantorenlogische Formeln*
- *wenn φ eine quantorenlogische Formel ist, so auch "es gibt ein x, so dass φ", "f"ur alle x gilt φ", wobei x eine Variable ist, die "uber mathematische Objekte l"auft.*

Quantorenlogische Formeln werden auch in symbolischer Notation geschrieben:

- $\exists x \varphi$ statt "es gibt ein x, so dass φ"; solche Formeln heißen *Existenzformeln*;
- $\forall x \varphi$ statt "f"ur alle x gilt φ"; solche Formeln heißen *Allformeln* oder *universelle Formeln*.

Die mengentheoretische Inklusion war mit einer Allformel definiert.

Eine Teilmenge von N ist eine Menge M, so dass jedes Element von M ein Element von N ist. D.h. $M \subseteq N$ gdw. $\forall x(x \in M \to x \in N)$.

Die Negation der Inklusion gilt, wenn es ein $x \in M$ gilt, f'ur das aber $x \notin N$. D.h. $M \not\subseteq N$ gdw. $\exists x(x \in M \wedge x \notin N)$.

4.7 Quantorenlogisches Beweisen

4.7.1 Existenzbeweise

Um $\exists x \varphi(x)$ zu zeigen, zeigt man $\varphi(t)$ f'ur einen Term t. Damit ist ein "Beispiel" f'ur die Eigenschaft gegeben und die Existenz bewiesen.

4.7.2 Universalisierung

Um $\forall x\,\varphi(x)$ zu zeigen, fixiert man ein "beliebiges" x und zeigt $\varphi(x)$. Da x beliebig gew"ahlt/fixiert war, ist $\varphi(x)$ damit f'ur alle Objekte x gezeigt. Also gilt $\forall x\,\varphi(x)$.

Wir hatten diese Beweismethode bei den Beweisen "uber Inklusion und Mengenoperationen oft benutzt. Z.B. hatten wir $M \subseteq N \wedge N \subseteq P \to M \subseteq P$ folgendermaßen gezeigt:

Sei $M \subseteq N \wedge N \subseteq P$. Sei $a \in M$. Wegen $M \subseteq N$ ist $a \in N$. Wegen $N \subseteq P$ ist $a \in P$. Also ist jedes Element von M ein Element von P, d.h. $\forall a\,(a \in M \to a \in P)$. Und, nach Definition der Inklusion, ist $M \subseteq P$.

5 Funktionen

Eine *Funktion* ist ein Objekt.

Der Definitionsbereich einer Funktion f ist eine Menge $\mathrm{def}(f)$.

F"ur $x \in \mathrm{def}(f)$ ist $f(x)$ ein Objekt, das als *Wert* von f an der *Stelle* x bezeichnet wird ("f von x"). Man sagt auch, dass x auf $f(x)$ abgebildet wird und schreibt: $x \mapsto f(x)$.

Das *Bild* der Funktion f ist die Menge $\mathrm{bild}(f) = \{f(x) \mid x \in \mathrm{def}(f)\}$.

F"ur $A \subseteq \mathrm{def}(f)$ ist $f[A] = \{f(x) \mid x \in A\}$ das *Bild* von A unter f.

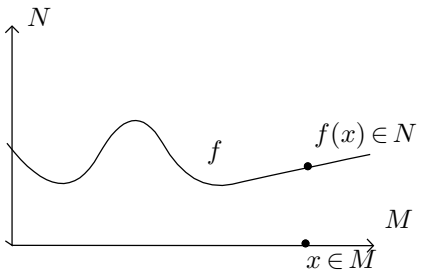
Wir schreiben $f\colon M \to N$ f'ur: f ist eine Funktion mit $\mathrm{def}(f) = M$, N ist eine Menge, und $\mathrm{bild}(f) \subseteq N$ ("f von M nach N").

Der *Raum* aller Funktionen von M nach N ist die Menge

$$N^M = \{f \mid f\colon M \to N\}.$$

Die Exponentialschreibweise ist durch Analogien zur Exponentiation von Zahlen motiviert.

Eine Funktion $f\colon M \to N$ l"asst sich als *Graph* in einer $M \times N$-"Ebene" graphisch darstellen:



"Ahnlich wie eine Menge allein durch ihre Elemente bestimmt ist, so ist eine Funktion durch die Zuordnungen $x \mapsto f(x)$ bestimmt, und wir erhalten ein entsprechendes Extensionalit"atsaxiom:

Extensionalit"atsaxiom f"ur Funktionen. Seien f und g Funktionen. Wenn $\mathrm{def}(f) = \mathrm{def}(g)$ und wenn f'ur jedes $x \in \mathrm{def}(f)$ $f(x) = g(x)$ ist, dann ist $f = g$.

In Analogie zur Definition von Mengen als Zusammenfassung $\{x \mid A(x)\}$ l"asst sich eine Funktion $f\colon M \to N$ durch eine Gleichung

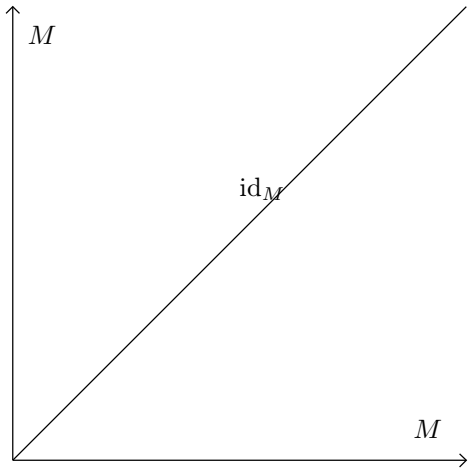
$$f(x) = t(x)$$

definieren, wobei t ein Term unserer Sprache ist, der f'ur jedes $x \in M$ ein Objekt $t(x) \in N$ liefert.

Beispiel 34. Ein einfaches Beispiel einer Funktion ist die *identische* Funktion $\mathrm{id}_M\colon M \to M$ mit

$$\mathrm{id}_M(x) = x.$$

Diese Funktion kann als Diagonale in einer $M \times M$-Ebene dargestellt werden.



Die Definition der Funktionswerte $f(x)$ kann auch Fallunterscheidungen $\varphi_0(x)$, ..., $\varphi_{n-1}(x)$ enthalten: definiere $f\colon M \to N$ mit

$$f(x) = \begin{cases} t_0(x), \text{ wenn } \varphi_0(x) \\ \vdots \\ t_{n-1}(x), \text{ wenn } \varphi_{n-1}(x) \end{cases}$$

Wir werden sehen, dass der Bereich der Funktionen "ahnlich reichhaltig ist wie der Bereich der Mengen.

Definition 35. *F"ur paarweise verschiedene Objekte $a_0, ..., a_{n-1}$ und f"ur beliebige Objekte $b_0, ..., b_{n-1}$ bezeichnet*

$$\begin{pmatrix} a_0 & a_1 & \dots & a_{n-1} \\ b_0 & b_1 & \dots & b_{n-1} \end{pmatrix}$$

die Funktion $f\colon \{a_0, ..., a_{n-1}\} \to \{b_0, ..., b_{n-1}\}$ mit

$$f(x) = \begin{cases} b_0, \text{ wenn } x = a_0 \\ \vdots \\ b_{n-1}, \text{ wenn } x = a_{n-1} \end{cases}$$

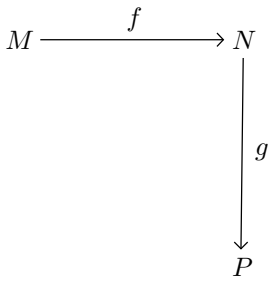
5.1 Kompositionen von Funktionen

Definition 36. *Sei $f\colon M \to N$ und $g\colon N \to P$. Definiere die Funktion $g \circ f\colon M \to P$ durch*

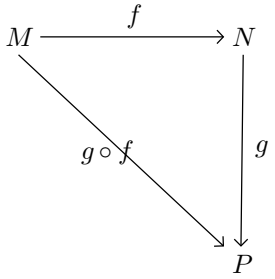
$$(g \circ f)(x) = g(f(x)).$$

$g \circ f$ heißt die Komposition *von g und f. Man sagt daf"ur auch "g nach f", weil erst f und dann g angewendet wird.*

Kompositionen von Funktionen werden oft durch *Diagramme* dargestellt:



Die Funktion $g \circ f$ ist eine Abbildung von M nach N, die wir ebenfalls in das Diagramm eintragen k"onnen.



Dieses Diagramm *kommutiert*, weil die beiden Wege von M nach P - "uber die Menge N bzw. der direkte Weg - dieselbe Zuordnung darstellen.

Das Komponieren von Funktionen hat "Ahnlichkeiten mit der Multiplikation von Zahlen:

Lemma 37. *Seien $f\colon M \to N$, $g\colon N \to P$ und $h\colon P \to Q$. Dann gilt:*

a) $(h \circ g) \circ f = h \circ (g \circ f)$ *(Assoziativit"at von $\circ$);*

b) $f \circ \mathrm{id}_M = f$ *(id_M ist* rechts-neutral *f"ur f);*

c) $\mathrm{id}_N \circ f = f$ *(id_N ist* links-neutral *f"ur f).*

Beweis. *a*) Wir zeigen die Allformel

$$\forall x(x \in M \to ((h \circ g) \circ f)(x) = (h \circ (g \circ f))(x))$$

Fixiere $x \in M$. Dann ist

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

Da $x \in M$ beliebig war, ist die obige Allformel gezeigt.

b+c) Fixiere $x \in M$. Dann ist

$$(f \circ \mathrm{id}_M)(x) = f(\mathrm{id}_M(x)) = f(x)$$

und

$$(\mathrm{id}_N \circ f)(x) = \mathrm{id}_N(f(x)) = f(x). \qquad \square$$

5.2 Surjektive Funktionen

Definition 38. *Eine Funktion $f: M \to N$ ist* surjektiv*, wenn* $\text{bild}(f) = N$.

Lemma 39.

a) Seien $f: M \to N$ und $g: N \to P$ surjektive Funktionen. Dann ist $g \circ f: M \to P$ surjektiv.

b) Seien $f: M \to N$ und $g: N \to P$ Funktionen, und sei $g \circ f: M \to P$ surjektiv. Dann ist g surjektiv.

Beweis. *a)* Sei $z \in P$. Da g surjektiv ist, nimm $y \in N$ mit $g(y) = z$. Da f surjektiv ist, nimm $x \in M$ mit $f(x) = y$. Dann ist $g \circ f(x) = g(f(x)) = g(y) = z$. Also $\exists x \in M\, g \circ f(x) = z$. Da $z \in P$ beliebig ist, ist $\forall z \in P \exists x \in M g \circ f(x) = z$.

b) Sei $z \in P$. Da $g \circ f$ surjektiv ist, nimm $x \in M$ mit $g \circ f(x) = g(f(x)) = z$. $f(x)$ bezeugt die Formel $\exists y \in N g(y) = z$. Da $z \in P$ beliebig ist, ist $\forall z \in P \exists y \in N g(y) = z$. □

5.3 Injektive Funktionen

Definition 40. *Eine Funktion $f: M \to N$ ist* injektiv*, wenn f"ur alle $x, x' \in M$ aus $f(x) = f(x')$ folgt, dass $x = x'$. Als symbolische Formel:*

$$\forall x \in M \forall x' \in M (f(x) = f(x') \to x = x').$$

Lemma 41.

a) Seien $f: M \to N$ und $g: N \to P$ injektive Funktionen. Dann ist $g \circ f: M \to P$ injektiv.

b) Seien $f: M \to N$ und $g: N \to P$ Funktionen, und sei $g \circ f: M \to P$ injektiv. Dann ist f injektiv.

Beweis. *a)* Betrachte $x, x' \in M$ mit $(g \circ f)(x) = (g \circ f)(x')$. Dann ist $g(f(x)) = g(f(x'))$. Da g injektiv ist, ist $f(x) = f(x')$. Da f injektiv ist, ist $x = x'$.

b) Betrachte $x, x' \in M$ mit $f(x) = f(x')$. Dann ist $g \circ f(x) = g \circ f(x')$. Da $g \circ f$ injektiv ist, ist $x = x'$. □

Aufgabe 2. Kann man in Lemma 35 auch folgern, dass g injektiv ist?

Definition 42. *Sei $f: M \to N$ injektiv. Definiere $f^{-1}: \text{bild}(f) \to M$ durch*

$$f^{-1}(y) = x \text{ mit } f(x) = y.$$

Beachte, dass x mit $f(x) = y$ wegen der Injektivit"at von f ein eindeutig bestimmter Term in der Variablen y ist.

Lemma 43. *Sei $f: M \to N$ injektiv mit der Umkehrfunktion $f^{-1}: \text{bild}(f) \to M$*

a) $f^{-1}: \text{bild}(f) \to M$ ist injektiv.

b) $f^{-1}: \text{bild}(f) \to M$ ist surjektiv.

Beweis. *a)* Seien $y, y' \in \text{bild}(f)$ mit $f^{-1}(y) = f^{-1}(y')$. Nach Definition der Umkehrfunktion ist

$$y = f(f^{-1}(y)) = f(f^{-1}(y')) = y'.$$

b) Sei $x \in M$. Sei $y = f(x)$. Dann ist $f^{-1}(y) = x$. □

Beweis. Sei $x \in M$. Dann ist $f^{-1} \circ f(x) = f^{-1}(f(x)) = x$. □

Lemma 44. *Sei $f: M \to N$. Wenn es eine Funktion $g: N' \to M$ gibt mit $\mathrm{bild}(f) \subseteq N'$ und $g \circ f = \mathrm{id}_M$, dann ist f injektiv.*

5.4 Bijektive Funktionen

Definition 45. *Eine Funktion $f: M \to N$ ist* bijektiv*, wenn f surjektiv und injektiv ist.*

Lemma 46. *Die identische Funktion $\mathrm{id}_M: M \to M$ ist bijektiv.*

Lemma 47. *Seien $f: M \to N$ und $g: N \to P$ bijektive Funktionen. Dann ist $g \circ f: M \to P$ bijektiv.*

Lemma 48. *Sei $f: M \to N$ bijektiv. Dann ist die Umkehrabbildung $f^{-1}: M \to N$ bijektiv.*

Beweis. Folgt sofort aus vorangehendem Lemma □

Definition 49. *Die Mengen M, N sind* gleichm"achtig*, wenn es eine Bijektion $f: M \to N$ gibt. Wir schreiben dann $M \sim N$.*

$\sim$ ist eine zweistellige Relation auf Mengen. F"ur Mengen M, N ist $M \sim N$ entweder wahr oder falsch.

Lemma 50. *Die Relation $\sim$ erf"ullt die Axiome einer "Aquivalenzrelation: f"ur alle Mengen M, N, P gilt*

a) $M \sim M$

b) *$M \sim N$ impliziert $N \sim M$*

c) *$M \sim N$ und $N \sim P$ impliziert $M \sim P$*

Beweis. *a*) $\mathrm{id}_M: M \to M$ ist offensichtlich bijektiv.

b) Sei $M \sim N$ mit der Bijektion $f: M \to N$. Dann ist $f^{-1}: N \to M$ bijektiv, und damit $N \sim M$.

c) Seien $M \sim N$ und $N \sim P$ mit den Bijektionen $f: M \to N$ und $g: N \to P$. Dann ist $g \circ f: M \to P$ bijektiv (nach vorigen Lemmas). □

Lemma 51. *Wenn $M \sim \emptyset$, dann ist $M = \emptyset$.*

Beweis. Sei $f: M \to \emptyset$ bijektiv. Angenommen $x \in M$. Dann ist

$$f(x) \in \mathrm{bild}(f) \subseteq \emptyset.$$

Widerspruch. Also besitzt M kein Element, und daher ist $M = \emptyset$. □

Definition 52. *Sei M eine Menge. Die* symmetrische Gruppe *auf M ist die Menge*

$$\mathfrak{S}(M) = \{f \mid f: M \to M \text{ ist bijektiv}\};$$

die Elemente von $\mathfrak{S}(M)$ *heißen* Permutationen *von* M.

Satz 53. *Mit der Komposition* $\circ$ *von Funktionen erf"ullt die symmetrische Gruppe* $\mathfrak{S}(M)$ *die Gruppenaxiome: f"ur* $f, g, h \in \mathfrak{S}(M)$ *gilt*

a) $(f \circ g) \circ h = f \circ (g \circ h)$

b) $f \circ \mathrm{id}_M = \mathrm{id}_M \circ f = f$

c) $f \circ f^{-1} = f^{-1} \circ f = \mathrm{id}_M$

Wir demonstrieren das Rechnen in $\mathfrak{S}(M)$. Sei z.B. $M = \{0, 1, 2\}$. Dann besteht $\mathfrak{S}(M)$ aus 6 Elementen:

$$\mathfrak{S}(M) = \left\{ \begin{pmatrix} 0 & 1 & 2 \\ 0 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 2 \\ 0 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 2 \\ 1 & 0 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 2 \\ 2 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 2 \\ 2 & 1 & 0 \end{pmatrix} \right\}.$$

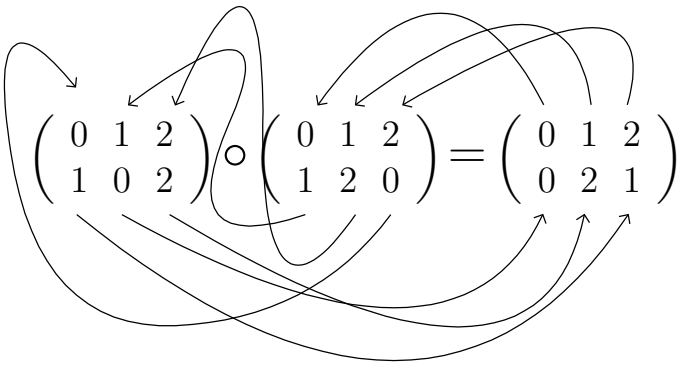
Dabei ist $\begin{pmatrix} 0 & 1 & 2 \\ 0 & 1 & 2 \end{pmatrix} = \mathrm{id}_M$. Die Komposition in dieser Gruppe l"asst sich konkret berechnen. Wir berechnen die Werte einer Komposition auf $\{0, 1, 2\}$ durch:

$$\left(\begin{pmatrix} 0 & 1 & 2 \\ 1 & 0 & 2 \end{pmatrix} \circ \begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \end{pmatrix} \right)(0) = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 0 & 2 \end{pmatrix} \left(\begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \end{pmatrix}(0) \right) = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 0 & 2 \end{pmatrix}(1) = 0$$
$$\left(\begin{pmatrix} 0 & 1 & 2 \\ 1 & 0 & 2 \end{pmatrix} \circ \begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \end{pmatrix} \right)(1) = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 0 & 2 \end{pmatrix} \left(\begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \end{pmatrix}(1) \right) = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 0 & 2 \end{pmatrix}(2) = 2$$
$$\left(\begin{pmatrix} 0 & 1 & 2 \\ 1 & 0 & 2 \end{pmatrix} \circ \begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \end{pmatrix} \right)(2) = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 0 & 2 \end{pmatrix} \left(\begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \end{pmatrix}(2) \right) = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 0 & 2 \end{pmatrix}(0) = 1$$

Also ist

$$\begin{pmatrix} 0 & 1 & 2 \\ 1 & 0 & 2 \end{pmatrix} \circ \begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 2 \\ 0 & 2 & 1 \end{pmatrix}.$$

Diese Berechnung kann man grafisch durch Verfolgen von Pfeilen nachvollziehen:



Also ist

$$\begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \end{pmatrix} \circ \begin{pmatrix} 0 & 1 & 2 \\ 1 & 0 & 2 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 2 \\ 2 & 1 & 0 \end{pmatrix}.$$

Damit ist durch eine Beispielrechnung gezeigt:

Lemma 54. *Die symmetrische Gruppe* $\mathfrak{S}(\{0,1,2\})$ *ist* nicht *kommutativ.*

Aufgabe 3. Geben Sie alle Elemente von $\mathfrak{S}(\emptyset)$, $\mathfrak{S}(\{0\})$, $\mathfrak{S}(\{0,1\})$ und $\mathfrak{S}(\{0,1,2,3\})$ an. Welche dieser Gruppen sind kommutativ?

6 Geordnete Paare

Definition 55. *F"ur alle Objekte* a *und* b *ist* (a,b) *ein Objekt, das das* geordnete Paar *von* a *und* b *genannt wird. Hierf"ur gilt: wenn* $(a,b)=(a',b')$*, dann ist* $a=a'$ *und* $b=b'$*.*

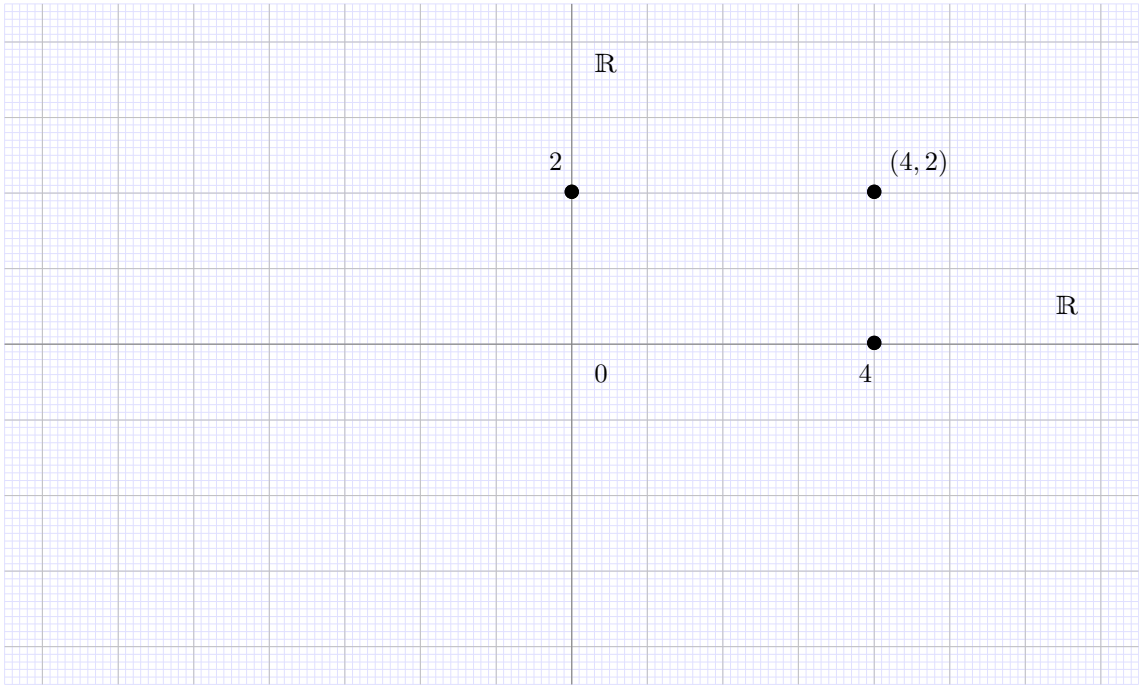
Definition 56. *Das* kartesische Produkt *der Mengen* M *und* N *ist die Menge*

$$M\times N=\{(a,b)\mid a\in M\wedge b\in N\}.$$

Die Notation auf der rechten Seite bedeutet formaler:

$$M\times N=\{x\mid \textit{es gibt } a\in M, b\in N, \textit{ so dass } x=(a,b)\}.$$

Der allgemeine Begriff des kartesischen Produkts entspricht dem bekannten kartesischen Produkt $\mathbb{R}\times\mathbb{R}$, das "ublicherweise auch als *euklidische Ebene* bezeichnet wird. Die Komponenten des Punktes $(4,2)$ werden als seine *kartesischen Koordinaten* bezeichnet.



Wir notieren Rechengesetze f"ur das kartesische Produkt wie die folgenden Distributivgesetze:

Lemma 57. *Seien* M,N,P *Mengen.*

a) $M\times(N\cup P)=(M\times N)\cup(M\times P)$

b) $M\times(N\cap P)=(M\times N)\cap(M\times P)$

Beweis. *a*)

$$\begin{aligned} M \times (N \cup P) &= \{(a,b) \mid a \in M \wedge b \in N \cup P\} \\ &= \{(a,b) \mid a \in M \wedge (b \in N \vee b \in P)\} \\ &= \{(a,b) \mid (a \in M \wedge b \in N) \vee (a \in M \wedge b \in P)\} \\ &= \{(a,b) \mid a \in M \wedge b \in N\} \cup \{(a,b) \mid a \in M \wedge b \in P\} \\ &= (M \times N) \cup (M \times P) \end{aligned}$$

□

Das kartesische Produkt ist *nicht* kommutativ:

Lemma 58. *Es gibt Mengen M und N, so dass $M \times N \neq N \times M$.*

Beweis. $\{0\} \times \{1\} = \{(0,1)\} \neq \{(1,0)\} = \{1\} \times \{0\}$. □

Das kartesische Produkt ist *nicht* assoziativ:

Lemma 59. *Es gibt Mengen M, N, P, so dass $(M \times N) \times P \neq M \times (N \times P)$.*

Beweis.
Fall 1. $0 \neq (0,0)$. Setze $M = N = P = \{0\}$. Dann ist

$$(M \times N) \times P = \{(0,0)\} \times \{0\} = \{((0,0),0)\} \neq \{(0,(0,0))\} = \{0\} \times \{(0,0)\} = N \times (M \times P).$$

Also gibt es in diesem Fall Mengen M, N, P, so dass $(M \times N) \times P \neq M \times (N \times P)$.
Fall 2. $0 = (0,0)$. Dann ist $0 \neq (0,1)$. Setze $M = \{0\}$, $N = \{1\}$, $P = \{0\}$. Dann ist

$$(M \times N) \times P = \{(0,1)\} \times \{0\} = \{((0,1),0)\} \neq \{(0,(1,0))\} = \{0\} \times \{(1,0)\} = N \times (M \times P).$$

Also gibt es in diesem Fall Mengen M, N, P, so dass $(M \times N) \times P \neq M \times (N \times P)$.
Damit gibt es in beiden F"allen Mengen, die die Behauptung erf"ullen. □

Man erh"alt aber eine Art Assoziativit"at und Kommutativit"at, wenn man Mengen, die zueinander bijektiv sind, als "aquivalent auffasst:

Lemma 60. *Seien M, N, P Mengen.*

a) *Es gibt eine bijektive Funktion $f\colon (M \times N) \times P \to M \times (N \times P)$, definiert durch*

$$f(((a,b),c)) = (a,(b,c)).$$

b) *Es gibt eine bijektive Funktion $f\colon M \times N \to N \times M$, definiert durch*

$$f((a,b)) = (b,a).$$

Beweis. *a*) Definiere $f\colon (M \times N) \times P \to M \times (N \times P)$ durch

$$f(((a,b),c)) = (a,(b,c)).$$

(1) f ist injektiv.

Beweis. Seien $x, x' \in (M \times N) \times P$ mit $f(x) = f(x')$. Seien $a, a' \in M$, $b, b' \in N$, $c, c' \in P$, so dass $x = ((a, b), c)$ und $x' = ((a', b'), c')$. Dann ist $(a, (b, c)) = f(x) = f(x') = (a', (b', c'))$. Nach den Grundeigenschaften formaler Paare ist $a = a'$ und $(b, c) = (b', c')$. Und weiter ist $b = b'$ und $c = c'$. Damit ist

$$x = ((a, b), c) = ((a', b'), c') = x'.$$

qed(1)

(2) f ist surjektiv.

Beweis. Sei $y \in M \times (N \times P)$. Seien $a \in M$, $b \in N$, $c \in P$, so dass $y = (a, (b, c))$. Dann ist $x = ((a, b), c) \in (M \times N) \times P$ und

$$f(x) = f(((a, b), c)) = (a, (b, c)) = y.$$

b) Definiere $f: M \times N \to N \times M$ durch

$$f((a, b)) = (b, a).$$

(1) f ist injektiv.

Beweis. Seien $x, x' \in M \times N$ mit $f(x) = f(x')$. Seien $a, a' \in M$, $b, b' \in N$, so dass $x = (a, b)$ und $x' = (a', b')$. Dann ist $(b, a) = f(x) = f(x') = (b', a')$. Nach den Grundeigenschaften formaler Paare ist $b = b'$ und $a = a'$. Damit ist

$$x = (a, b) = (a', b') = x'.$$

qed(1)

(2) f ist surjektiv.

Beweis. Sei $y \in N \times M$. Seien $a \in M$, $b \in N$, so dass $y = (b, a)$. Dann ist $x = (a, b) \in M \times N$ und

$$f(x) = f((a, b)) = (b, a) = y. \qquad \square$$

Definition 61. *Zwei Mengen M, N sind* disjunkt*, wenn $M \cap N = \emptyset$.*

Bei der Definition von Zahlen und ihrer Arithmetik innerhalb der Mengenlehre werden wir oft disjunkte “‘aquivalente” Mengen ben”otigen. Diese kann “uber kartesische Produkte erhalten.

Lemma 62. *Seien M, N Mengen. Dann gibt es Mengen M', N' und bijektive Funktionen f: $M \to M'$, g: $N \to N'$, so dass M', N' disjunkt sind.*

Beweis. Setze $M' = \{0\} \times M$ und $N' = \{1\} \times N$. Definiere $f: M \to M'$ durch $f(x) = (0, x)$.

(2) $f: M \to M'$ ist bijektiv.

Beweis. “Ubung

Definiere $g: N \to N'$ durch $g(x) = (1, x)$. Dann ist g ebenso wie f bijektiv.

(3) $M' \cap N' = \emptyset$.

Beweis. Angenommen $z \in M' \cap N' = (\{0\} \times M) \cap (\{1\} \times N)$. W”ahle $x \in M$ und $y \in N$, so dass $z = (0, x)$ und $z = (1, y)$. Nach den Grundeigenschaften geordneter Paare ist dann $0 = 1$, Widerspruch. Daher besitzt $M' \cap N'$ keine Elemente und ist daher die leere Menge. $\square$

7 Anzahlen und Kardinalit”aten

Zu jeder Menge M ist $|M|$ eine Zahl, die man die *Anzahl* oder die *Kardinalzahl* oder die *Kardinalit”at* von M nennt.

Wir fordern folgendes **Axiome** f'ur Anzahlen: f'ur alle Mengen M und N gilt

- $|M| = |N|$ gdw. es eine Bijektion $f: M \leftrightarrow N$ gibt.
- $|M| \leqslant |N|$ gdw. es eine Injektion $f: M \to N$ gibt.
- die Relation $\leqslant$ auf Anzahlen μ, ν, π ist eine *lineare Ordnung*
  - $\mu \leqslant \mu$ (Reflexivit"at)
  - $\mu \leqslant \nu$ und $\nu \leqslant \pi$ impliziert $\mu \leqslant \pi$ (Transitivit"at)
  - $\mu \leqslant \nu$ und $\nu \leqslant \mu$ impliziert $\mu = \nu$ (Antisymmetrie)
  - $\mu \leqslant \nu$ oder $\nu \leqslant \mu$ (Linearit"at)
- $0 = |\emptyset|$, $1 = |\{0\}|$ und $2 = |\{0,1\}|$

Lemma 63. *F"ur jede Menge x gilt $|\{x\}| = 1$.*

Beweis. Definiere eine Bijektion $f: \{0\} \to \{x\}$ durch $f(0) = x$. Dann ist $|\{x\}| = |\{0\}| = 1$. □

Definition 64. *Seien μ und ν Kardinalzahlen. Dann definiere:*

a) $\mu + \nu = |M \cup N|$, *wobei M und N* disjunkte *Mengen mit $|M| = \mu$ und $|N| = \nu$ sind.*

b) $\mu \cdot \nu = |M \times N|$, *wobei M und N Mengen mit $|M| = \mu$ und $|N| = \nu$ sind.*

c) $\mu^\nu = |M^N|$, *wobei M und N Mengen mit $|M| = \mu$ und $|N| = \nu$ sind.*

Lemma 65. *Die Operationen $+, \cdot,$ und Exponentiation sind wohldefiniert, d.h. wenn M, N, M', N' Mengen mit $|M| = |M'|$ und $|N| = |N'|$ sind, so gilt*

a) $|M \cup N| = |M' \cup N'|$, *wenn M und N disjunkte Mengen sind, und wenn M' und N' disjunkte Mengen sind;*

b) $|M \times N| = |M' \times N'|$;

c) $|M^N| = |M'^{N'}|$.

Beweis. *a)* Seien M, M', N, N' Mengen, wobei $M \cap N = M' \cap N' = \emptyset$ und $|M| = |M'| = \mu$ und $|N| = |N'| = \nu$ ist. Zu zeigen ist, dass $|M \cup N| = |M' \cup N'|$. W"ahle Bijektionen $f: M \to M'$ und g: $N \to N'$. Definiere dann eine Funktion $h: M \cup N \to M' \cup N'$ durch

$$h(x) = \begin{cases} f(x), \text{ falls } x \in M \\ g(x), \text{ falls } x \in N \end{cases}$$

Da M, N disjunkt sind, ist h wohldefiniert.

(1) h ist injektiv.

Beweis. Sei $h(x) = h(x')$.

Fall 1: $h(x) \in M'$. Dann sind $x, x' \in M$ und $f(x) = h(x) = h(x') = f(x)$. Da f injektiv ist, ist $x = x'$.

Fall 2: $h(x) \in N'$. Dann sind $x, x' \in N$ und $g(x) = h(x) = h(x') = g(x)$. Da g injektiv ist, ist $x = x'$.

In beiden F"allen ist $x = x'$. *qed*(1)

(2) h ist surjektiv.

Beweis. Sei $y \in M' \cup N'$.

Fall 1. $y \in M'$. Da $f: M \to M'$ surjektiv ist, w"ahle $x \in M$ mit $f(x) = y$. Dann ist $h(x) = f(x) = y$.

Fall 2. $y \in N'$. Da $g: N \to N'$ surjektiv ist, w"ahle $x \in N$ mit $g(x) = y$. Dann ist $h(x) = g(x) = y$.

In beiden F"allen existiert $x \in M \cup N$ mit $h(x) = y$.

Also ist $h: M \cup N \to M' \cup N'$ bijektiv und $|M \cup N| = |M' \cup N'|$.

b) Seien M, M', N, N' Mengen, mit $|M| = |M'| = \mu$ und $|N| = |N'| = \nu$ ist. Zu zeigen ist, dass $|M \times N| = |M' \times N'|$. W"ahle Bijektionen $f: M \to M'$ und $g: N \to N'$. Definiere dann eine Funktion $h: M \times N \to M' \times N'$ durch

$$h((a,b)) = (f(a), g(b)).$$

(1) h ist injektiv.

Beweis. Seien $a \in M$, $b \in N$ und $h((a,b)) = h((a',b'))$. Dann ist $(f(a), g(b)) = (f(a'), g(b'))$. Nach den Axiomen f'ur geordnete Paare ist $f(a) = f(a')$ und $g(b) = g(b')$. Da f und g injektiv sind, ist $a = a'$ und $b = b'$. Damit ist $(a,b) = (a',b')$. *qed*(1)

(2) h ist surjektiv.

Beweis. Sei $(c,d) \in M' \times N'$. Da $f: M \to M'$ und $g: N \to N'$ surjektiv sind, w"ahle $a \in M$ und $b \in N$, so dass $c = f(a)$ und $d = g(b)$. Dann ist

$$h((a,b)) = (f(a), g(b)) = (c,d). \qquad \square$$

Die Arithmetik mit Kardinalzahlen erf'ullt viele bekannte Gesetze.

Lemma 66. *Seien μ, ν, π Kardinalzahlen. Dann gilt*

a) $(\mu + \nu) + \pi = \mu + (\nu + \pi)$

b) $\mu + \nu = \nu + \mu$

c) $\mu + 0 = \mu$

d) $(\mu \cdot \nu) \cdot \pi = \mu \cdot (\nu \cdot \pi)$

e) $\mu \cdot \nu = \nu \cdot \mu$

f) $\mu \cdot 1 = \mu$

g) $\mu \cdot (\nu + \pi) = (\mu \cdot \nu) + (\mu \cdot \pi)$

Beweis. *b*) Seien M, N disjunkte Mengen mit $|M| = \mu$ und $|N| = \nu$. Dann ist

$$\mu + \nu = |M \cup N| = |N \cup M| = \nu + \mu\,.$$

d) Seien M, N Mengen mit $|M| = \mu$ und $|N| = \nu$. Dann ist $M \times N \sim N \times M$ und

$$\mu \cdot \nu = |M \times N| = |N \times M| = \nu \cdot \mu.$$

Andere: "Ubung. $\square$

Aufgabe 4. Formulieren und beweisen Sie "ahnliche Rechengesetze f'ur die Exponentiation. Was ist μ^0 und 0^μ?

Aufgabe 5. Die Rechenoperationen sind *monoton* bzgl. $\leqslant$: wenn $\mu \leqslant \mu'$ und $\nu \leqslant \nu'$ so ist

a) $\mu + \nu \leqslant \mu' + \nu'$

b) $\mu \cdot \nu \leqslant \mu' \cdot \nu'$

c) wenn $\mu \neq 0$, so ist $\mu^\nu \leqslant (\mu')^{\nu'}$

8 Endliche Mengen

Wir haben eine intuitiven Begriff von Endlichkeit und Unendlichkeit. Die Menge $\{1, 2, 3\}$ ist anschaulich endlich, die Menge $\mathbb{N} = \{0, 1, 2, 3, ...\}$ aller nat"urlichen Zahlen ist anschaulich unendlich. Anschaulich gelten folgende Eigenschaften f'ur endliche Mengen:

1. die leere Menge $\emptyset$ ist endlich;
2. wenn zu einer endlichen Menge x ein weiteres Element y hinzugef'ugt wird, so ist das Resultat $x \cup \{y\}$ endlich;
3. jede endliche Menge entsteht aus der leeren Menge (in endlich vielen Schritten) durch Hinzuf'ugen von einzelnen Elementen.

Die 3. Beobachtung l"asst sich nicht direkt in eine mengentheoretische Definition umsetzen, weil die Endlichkeit einer Menge durch *endlich* viele Schritte beschrieben wird; eine derartige Definition w"urde den Begriff der Endlichkeit durch sich selbst definieren. Man kann aber die 3. Beobachtung durch ein Induktionsaxiom erfassen: wenn man eine Eigenschaft f'ur alle endlichen Mengen beweisen will, so gen"ugt es, dass sich die Eigenschaft entlang der Schritte 1. und 2. vererbt.

Axiom 67. *"x ist* endlich*" ist eine Eigenschaft, die folgende Axiome erf"ullt:*

a) *$\emptyset$ ist endlich;*

b) *wenn M endlich und x ein Objekt ist, so ist die Menge $M \cup \{x\}$ endlich;*

c) *(Induktion) Sei $\varphi(M)$ eine Eigenschaft mit*

1. Induktionsanfang*: $\varphi(\emptyset)$;*

2. Induktionsschritt*: wenn $\varphi(M)$ gilt und x ein Objekt ist, so gilt $\varphi(M \cup \{x\})$.*

Dann gilt $\varphi(M)$ f"ur alle endlichen Mengen M, d.h. f"ur alle Mengen, die endlich sind.

Eine Menge heißt unendlich*, wenn sie nicht endlich ist.*

Dieses Axiom dr"uckt aus, dass die Gesamtheit der endlichen Mengen aus der leeren Menge $\emptyset$ durch den Prozess des "Anh"angens" von einzelnen Elementen "erzeugt" wird. Das Axiom *c*) entspricht der vollst"andigen Induktion f'ur nat"urliche Zahlen. Wir werden sp"ater die vollst"andige Induktion aus *c*) beweisen.

Das folgende Lemma ist anschaulich wahr, bedarf aber eines Beweises m.H. der Axiome der Endlichkeit, weil unsere Theorie keinen anderen Zugriff auf den Begriff "endlich" hat.

Lemma 68. *Die Einermenge $\{x\}$ und die Paarmenge $\{x, y\}$ sind endlich.*

Beweis. Nach *a*) ist $\emptyset$ endlich. Nach *b*) ist $\{x\} = \emptyset \cup \{x\}$ endlich. Nach *b*) ist $\{x, y\} = \{x\} \cup \{y\}$ endlich. □

Lemma 69. *Sei $f\colon M \to N$. Dann ist f"ur endliche Mengen $A \subseteq M$ auch $f[A]$ endlich.*

Beweis. Wir beweisen die Behauptung durch Induktion "uber A. Sei $\varphi(A)$ die Eigenschaft

$$\text{wenn } A \subseteq M, \text{ dann ist } f[A] \text{ endlich.}$$

Es gen"ugt, Induktionsanfang und Induktionsschritt entsprechend dem Endlichkeitsaxiomen zu zeigen.

Induktionsanfang. $\varphi(\emptyset)$.

Beweis. $f[\emptyset] = \emptyset$. Daher ist $f[\emptyset]$ endlich.

Induktionsschritt. Wenn $\varphi(A)$ gilt und x ein Objekt ist, so gilt $\varphi(A \cup \{x\})$.

Beweis. Sei $\varphi(A)$ und sei x ein Objekt. Sei $A \cup \{x\} \subseteq M$. Dann ist $A \subseteq M$ und nach der Induktionsannahme ist $f[A]$ endlich. Weiter ist

$$f[A \cup \{x\}] = f[A] \cup \{f(x)\}$$

endlich. Also gilt $\varphi(A \cup \{x\})$. □

Aus diesem Lemma folgt sofort

Lemma 70. *Wenn M endlich ist, und $M \sim N$, dann ist N endlich.*

Lemma 71. *Sei M endlich und $N \subseteq M$. Dann ist N endlich.*

Beweis. Wenn $N = \emptyset$, dann ist N endlich.

Angenommen $N \neq \emptyset$. W"ahle $a \in N$ und definiere $f: M \to N$ durch

$$f(x) = \begin{cases} x\,, \text{ wenn } x \in N \\ a\,, \text{ wenn } x \notin N \end{cases}$$

Dann ist $f: M \to N$ surjektiv und nach dem obigen Lemma ist $N = f[M]$ endlich. □

Die endlichen Mengen sind unter vielen Operationen abgeschlossen. Z.B.

Lemma 72. *Wenn A und B endlich sind, so auch $A \cup B$.*

Beweis. Fixiere die endliche Menge A. Wir beweisen die Behauptung durch Induktion "uber B mit der Eigenschaft $\varphi(B)$

$$A \cup B \text{ ist endlich.}$$

Induktionsanfang. Sei $B = \emptyset$. Dann ist $A \cup B = A \cup \emptyset = A$ endlich.

Induktionsschritt. Angenommen $A \cup B$ ist endlich und x ist ein Objekt. Dann ist

$$A \cup (B \cup \{x\}) = (A \cup B) \cup \{x\}$$

ebenfalls endlich. □

Lemma 73. *Wenn A und B endlich sind, so auch $A \times B$.*

Beweis. Fixiere die endliche Menge A. Wir beweisen die Behauptung durch Induktion "uber B mit der Eigenschaft $\varphi(B)$:

$$A \times B \text{ ist endlich.}$$

Induktionsanfang. Sei $B = \emptyset$. Dann ist $A \times B = A \times \emptyset = \emptyset$ endlich.

Induktionsschritt. Angenommen $A \times B$ ist endlich und x ist ein Objekt. Dann ist

$$A \times (B \cup \{x\}) = (A \times B) \cup (A \times \{x\}).$$

"Ahnlich einem fr"uheren Argument ist $A \sim A \times \{x\}$ ("Ubung). Damit ist $A \times \{x\}$ endlich. Zusammen ist $A \times (B \cup \{x\})$ als Vereinigung zweier endlicher Mengen endlich. □

Lemma 74. *Wenn A und B endlich sind, so auch A^B.*

Beweis. "Ubung □

Eine echte Teilmenge einer endlichen Menge ist strikt kleiner:

Lemma 75. *Sei $A \subseteq B$, $A \neq B$ und B endlich. Dann ist $A \nsim B$.*

Beweis. Durch Induktion "uber A.

Induktionsanfang. Sei $A = \emptyset$ und $B \neq \emptyset$. Dann ist wegen Lemma 51 $A \nsim B$.

Induktionsschritt. F"ur alle Mengen B mit $A \subseteq B$, $A \neq B$ sei $A \nsim B$. Weiter sei x ein Objekt.

Fall 1. $x \in A$. Dann ist $A \cup \{x\} = A$ und die Eigenschaft vererbt sich trivialerweise auf $A \cup \{x\}$.

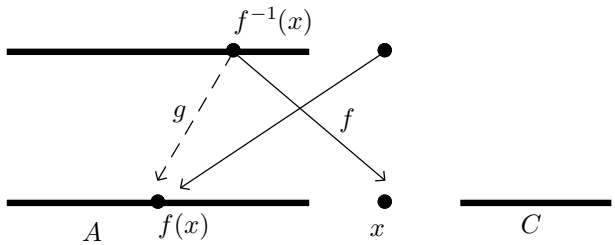
Fall 2. $x \notin A$. Sei $A \cup \{x\} \subseteq B$ mit $A \cup \{x\} \neq B$. Angenommen $A \cup \{x\} \sim B$ mit der Bijektion $f\colon A \cup \{x\} \to B$. Sei $C = B \setminus (A \cup \{x\})$. Die Mengen A, $\{x\}$, C sind paarweise disjunkt. Wir unterscheiden zwei F"alle:

Fall 1. $f(x) \notin A$. Wir schr"anken die Funktion f auf A ein und definieren $\bar{f}\colon A \to B \setminus \{f(x)\}$ durch

$$\bar{f}(u) = f(u).$$

Dann ist $\bar{f}\colon A \to B \setminus \{f(x)\}$ bijektiv (warum?) und $A \sim B \setminus \{f(x)\}$. Weiter ist $A \subseteq B \setminus \{f(x)\}$ und $A \neq B \setminus \{f(x)\}$ (warum?). Das aber widerspricht der Induktionsannahme.

Fall 2. $f(x) \in A$. Bild und Urbild von x liegen ungef"ahr so:



Wir modifizieren die Funktion f, um x aus diesem Bild zu eliminieren, und definieren $g\colon A \to A \cup C$ durch

$$g(u) = \begin{cases} f(u), \text{ falls } u \neq f^{-1}(x) \\ f(x), \text{ falls } u = f^{-1}(x) \end{cases}$$

Dann ist $g\colon A \to A \cup C$ bijektiv (warum?) und $A \sim A \cup C$. Weiter ist $A \subseteq A \cup C$ und $A \neq A \cup C$ (warum?). Das aber widerspricht ebenfalls der Induktionsannahme.

Da beide F"alle zum Widerspruch f"uhren, ist $A \cup \{x\} \nsim B$ wie gew"unscht. □

Damit gilt f"ur endliche Mengen A, B

$$\text{wenn } A \subseteq B \text{ und } A \neq B, \text{ dann ist } |A| < |B|.$$

Dies entspricht der Aristotelischen Maxime, dass ein (echter) Teil kleiner als das Ganze ist. Dieses aber ist im Bereich unendlicher Mengen nicht mehr evident: es gibt genauso viele gerade Zahlen wie nat"urliche Zahlen.

Die Vergleichbarkeit endlicher Kardinalit"aten l"asst sich "ubrigens direkt durch Induktion zeigen:

Lemma 76. *F"ur jede endliche Menge x gilt: wenn z eine endliche Menge ist, so gibt es eine Injektion $f: x \to z$ oder es gibt eine Injektion $g: z \to x$.*

Beweis. Induktion. $x = \emptyset$ klar.

Die Behauptung gelte f"ur x. Sei y Menge. Wir wollen die Behauptung f"ur $x \cup \{y\}$ zeigen. Wenn $y \in x$ ist, so ist $x \cup \{y\} = x$ und die Behauptung gilt nach Induktionsannahme. Sei jetzt also $y \notin x$. Sei z eine endliche Menge. Wenn $z = \emptyset$, so gilt die Behauptung offensichtlich mit der leeren Funktion von $\emptyset$ nach $x \cup \{y\}$. Sei jetzt $z \neq \emptyset$, $v \in z$, $u = z \setminus \{v\}$. Wir wenden jetzt die Induktionsannahme auf x und u an.

Fall 1. Es gibt eine Injektion $f: x \to u$. Definiere $f': x \cup \{y\} \to z = u \cup \{v\}$ durch

$$f'(w) = \begin{cases} f(w), \text{ wenn } w \in x \\ v, \text{ wenn } w = y \end{cases}$$

Fall 2. Es gibt eine Injektion $g: u \to x$. Definiere $g': z = u \cup \{v\} \to x \cup \{y\}$ durch

$$g'(w) = \begin{cases} g(w), \text{ wenn } w \in u \\ y, \text{ wenn } w = v \end{cases}$$

□

9 Nat"urliche Zahlen

Definition 77. *Eine Zahl n ist eine* nat"urliche Zahl, *wenn es eine endliche Menge x mit $n = |x|$ gibt. Es sei $\mathbb{N} = \{|x| \mid x \text{ ist endlich}\}$ die Menge der nat"urlichen Zahlen.*

Die Menge der nat"urlichen Zahlen ist Musterbeispiel einer unendlichen Menge. Sie ist eine unendliche Menge von minimaler Gr"oße.

Definition 78. *Setze $\aleph_0 = |\mathbb{N}|$ ("alef-null"). Eine Menge X heißt* abz"ahlbar unendlich, *wenn $|X| = \aleph_0$.*

Satz 79. *$\aleph_0 + 1 = \aleph_0$, $\aleph_0 + \aleph_0 = \aleph_0$ und $\aleph_0 \cdot \aleph_0 = \aleph_0$.*

Beweis. Durch Angabe geeigneter Bijektionen ("Ubung). □

Bemerkung 80. $\aleph_0$ ist das kleinste Elemente einer Folge $\aleph_0 < \aleph_1 < \aleph_2 < \ldots$ unendlicher Kardinalzahlen. $\aleph_1$, $\aleph_2$, ... sind *"uberabz"ahlbar*. Auch f"ur "uberabz"ahlbare Kardinalzahlen $\aleph_n$ gilt $\aleph_n + \aleph_n = \aleph_n$ und $\aleph_n \cdot \aleph_n = \aleph_n$.

Die Werte der Exponentiation f"ur unendliches $\aleph_n$ sind unbekannt und/oder unbestimmbar: das gilt bereits f"ur den Term $2^{\aleph_0}$.

In Analogie zu der Definition der endlichen Mengen erhalten wir:

Satz 81. (Peano Axiome)

a) $0 \in \mathbb{N}$.

b) *Wenn* $n \in \mathbb{N}$, *so ist* $n+1 \in \mathbb{N}$.

c) *Wenn* $n \in \mathbb{N}$, *so ist* $n+1 \neq 0$.

d) *Wenn* $m, n \in \mathbb{N}$ *und* $m+1 = n+1$, *dann ist* $m = n$.

e) *(*Vollst"andige Induktion*) Sei* $\varphi(x)$ *eine Eigenschaft mit*

1. Induktionsanfang*:* $\varphi(0)$*;*
2. Induktionsschritt*: wenn* $\varphi(n)$ *gilt, so gilt* $\varphi(n+1)$.

Dann gilt $\varphi(n)$ *f"ur alle* $n \in \mathbb{N}$.

Beweis. *a*) $0 = |\emptyset| \in \mathbb{N}$.

b) Sei $n \in \mathbb{N}$. Sei M eine endliche Menge mit $n = |M|$. $1 = |\{x\}|$. Nach Lemma 62 k"onnen wir voraussetzen, dass M und $\{x\}$ disjunkt sind. Dann ist $M \cup \{x\}$ endlich und $n+1 = |M \cup \{x\}| \in \mathbb{N}$.

c) Sei $n+1 = |M \cup \{x\}|$. Dann ist $M \cup \{x\} \neq \emptyset$, $M \cup \{x\} \nsim \emptyset$, und daher $n+1 \neq 0$.

d) Seien $m, n \in \mathbb{N}$ und $m+1 = n+1$. Sei $m+1 = |M \cup \{x\}|$, wobei M und $\{x\}$ disjunkt sind und $m = |M|$. Entsprechend sei $n+1 = |N \cup \{y\}|$, wobei N und $\{y\}$ disjunkt sind und $n = |N|$. Wegen $m+1 = n+1$ w"ahle eine Bijektion $f\colon M \cup \{x\} \to N \cup \{y\}$.

Fall 1. $f(x) = y$. Definiere die Einschr"ankung $f'\colon M \to N$ von f auf M durch

$$f'(u) = u.$$

Dann ist $f'\colon M \to N$ bijektiv und $m = |M| = |N| = n$.

Fall 2. $f(x) \neq y$. Definiere eine Modifikation $f'\colon M \to N$ von f, die die Punkte x und y ausl"asst durch:

$$f'(u) = \begin{cases} f(u), \text{ falls } u \neq f^{-1}(y) \\ f(x), \text{ falls } u = f^{-1}(y) \end{cases}$$

Dann ist $f'\colon M \to N$ bijektiv und $m = |M| = |N| = n$.

e) φ erf"ulle die Annahmen des Induktionsaxioms. Definiere eine Eigenschaft $\psi(x)$ f"ur Mengen x durch

$$\psi(x) \text{ gdw. } x \text{ ist endlich und } \varphi(|x|).$$

Wegen $\varphi(0)$ gilt $\psi(\emptyset)$.

Angenommen $\psi(x)$, und es sei y ein Objekt. Dann ist x endlich und $\varphi(n)$, wobei $n = |x|$.

Fall 1. $y \in x$. Dann ist $x \cup \{y\} = x$ und $\psi(x \cup \{y\})$.

Fall 2. $y \notin x$. Dann ist $|x \cup \{y\}| = |x| + 1 = n+1$. Nach Annahme ist dann $\psi(x \cup \{y\})$.

Also vererbt sich die Eigenschaft ψ in beiden F"allen von x auf $x \cup \{y\}$.

Nach dem Induktionsprinzip gilt dann $\psi(x)$ f"ur *alle* endlichen Mengen x.

F"ur $n \in \mathbb{N}$, $n = |x|$ mit x endlich, gilt dann $\psi(x)$ und daher $\varphi(|x|)$ und $\varphi(n)$. □

Lemma 82. *F"ur jede nat"urliche Zahl* $n \neq 0$ *gibt es ein* $m \in \mathbb{N}$ *mit* $n = m+1$. *Dieses* m *ist nach 81d eindeutig bestimmt; wir nennen es den Vorg"anger von* n *und schreiben* $m = n-1$.

Beweis. Wir beweisen durch vollst"andige Induktion $\forall n \varphi(n)$, wobei $\varphi(n)$ die Eigenschaft ist

$$\text{wenn } n \neq 0, \text{ dann gibt es ein } m \in \mathbb{N} \text{ mit } n = m+1.$$

Induktionsanfang: $\varphi(0)$ gilt, weil in diesem Fall die Pr"amisse $n \neq 0$ der Implikation falsch ist.

Induktionsschritt: Angenommen $\varphi(n)$ gilt. Wir zeigen $\varphi(n+1)$: Offensichtlich ist $n+1 = n+1$, d.h. es gibt eine $m \in \mathbb{N}$ mit $n+1 = m+1$ (n"amlich n). □

10 Darstellungen nat"urlicher Zahlen

Jede nat"urliche Zahl l"asst sich in der Form $0 + 1 + 1 + ... + 1 = (((0 + 1) + 1) + ...) + 1$ darstellen. Diese Form ist aber komplex und unhandlich. Unter Benutzung von Multiplikationen und Exponentiationen lassen sich Zahlen kompakter darstellen und handhaben. Z.B. ist unter Benutzung der Exponentiation: eine Million $= 10^6 = 1000000$. Diese Zahldarstellungen beruhen auf Divisionen ganzer Zahlen mit Rest:

$$428 = 42 \cdot 10 + 8 = (4 \cdot 10 + 2) \cdot 10 + 8 = 4 \cdot 10^2 + 2 \cdot 10 + 8.$$

Hierzu ben"otigen wir

Lemma 83. *Sei b eine nat"urliche Zahl $\geqslant 2$. F"ur jede nat"urliche Zahl $n \in \mathbb{N}$ gibt es eine* Darstellung

$$n = q \cdot b + r \text{ mit } q, r \in \mathbb{N} \text{ und } 0 \leqslant r < b.$$

Diese Darstellung ist eindeutig *bestimmt: wenn*

$$n = q' \cdot b + r' \text{ mit } q', r' \in \mathbb{N} \text{ und } 0 \leqslant r' < b,$$

so ist $q = q'$ und $r = r'$. Wir nennen q den ganzzahligen Quotienten *von n durch b und schreiben $q = \lfloor \frac{n}{b} \rfloor$; r ist der* Rest *der Division von n durch b.*

Beweis. Alle Variablen des Arguments laufen "uber die Menge $\mathbb{N}$. Wir beweisen das Lemma durch vollst"andige Induktion "uber n:

Induktionsanfang: $n = 0$. Dann ist $0 = 0 \cdot b + 0$ eine Darstellung von 0. Sei weiter $0 = q' \cdot b + r'$ mit $0 \leqslant r' < b$ eine Darstellung der 0. Wenn in dem Ausdruck $q' \cdot b + r'$ eine oder beide der Zahlen q' und r' ungleich 0 sind, so ist $q' \cdot b + r' \neq 0$. Also ist $q' = 0$ und $r' = 0$, und die Darstellung ist eindeutig.

Induktionsschritt: Sei $n \in \mathbb{N}$ und sei $n = q \cdot b + r$ mit $0 \leqslant r < b$ die eindeutige Darstellung von n. Dann ist $n + 1 = q \cdot b + r + 1$.

Zur *Existenz* der Darstellung:

Fall 1. $r + 1 < b$. Dann ist $n + 1 = q \cdot b + r + 1$ eine Darstellung von $n + 1$.

Fall 2. $r + 1 = b$. Dann ist $n + 1 = q \cdot b + b = (q + 1) \cdot b + 0$ eine Darstellung von $n + 1$.

Zur *Eindeutigkeit* der Darstellung:

Sei $n + 1 = q \cdot b + r = q' \cdot b + r'$ mit $0 \leqslant r, r' < b$.

Fall 1. $r = r' = 0$.

Dann ist $q \neq 0$ und $q' \neq 0$. Sei $q = q_0 + 1$ und $q' = q'_0 + 1$.

$$\begin{aligned} n + 1 &= (q_0 + 1) \cdot b = q_0 \cdot b + (b - 1) + 1 \\ n + 1 &= (q'_0 + 1) \cdot b = q'_0 \cdot b + (b - 1) + 1 \end{aligned}$$

Daraus folgt

$$\begin{aligned} n &= q_0 \cdot b + (b - 1) \\ n &= q'_0 \cdot b + (b - 1) \end{aligned}$$

Wegen der vorausgesetzten eindeutigen Darstellung f"ur n ist $q_0 = q_0'$ und $q = q'$. Also ist die Darstellung von $n+1$ in diesem Fall eindeutig.

Fall 2. $r = 0$, $r' \neq 0$.

Sei $r' = r_0' + 1$. Wie oben ist $q \neq 0$. Sei $q = q_0 + 1$.

$$\begin{aligned} n+1 &= (q_0+1)\cdot b = q_0 \cdot b + (b-1) + 1 \\ n+1 &= q' \cdot b + r_0' + 1 \end{aligned}$$

Daraus folgt

$$\begin{aligned} n &= q_0 \cdot b + (b-1) \\ n &= q' \cdot b + r_0' \end{aligned}$$

Wegen der vorausgesetzten eindeutigen Darstellung f"ur n ist $b-1 = r_0'$ und $r' = b$, im *Widerspruch* zu $r' < b$. Damit kommt dieser Fall nicht vor. Oder wir k"onnen aus dem Widerspruch beliebig schließen: Auch in diesem Fall ist die Darstellung von $n+1$ eindeutig.

Fall 3. $r \neq 0$, $r' = 0$.

Gegen"uber Fall 2 sind die Rollen von r und r' vertauscht. Wir kommen genau wie dort zu einem Widerspruch.

Fall 4. $r \neq 0$, $r' \neq 0$.

Sei $r = r_0 + 1$ und $r' = r_0' + 1$.

$$\begin{aligned} n+1 &= q \cdot b + r_0 + 1 \\ n+1 &= q' \cdot b + r_0' + 1 \end{aligned}$$

Daraus folgt

$$\begin{aligned} n &= q \cdot b + r_0 \\ n &= q' \cdot b + r_0' \end{aligned}$$

Wegen der vorausgesetzten eindeutigen Darstellung von n ist $q = q'$ und $r_0 = r_0'$. Damit ist $r = r'$, und die Darstellung von $n+1$ ist auch in diesem Fall eindeutig.

Damit ist die Darstellung von $n+1$ in allen F"allen eindeutig. □

Lemma 84. *Sei $b \in \mathbb{N}, b \geqslant 2$ und $k \in \mathbb{N}$. Dann ist*

$$(b-1)\cdot b^k + (b-1)\cdot b^{k-1} + \cdots + (b-1)\cdot b^1 + (b-1) = b^{k+1} - 1.$$

Die Summe kann auch geschrieben werden als

$$\sum_{l=0}^{k} (b-1)\cdot b^l = (b-1)\cdot \sum_{l=0}^{k} b^l.$$

Beweis. Durch vollst"andige Induktion "uber $k \in \mathbb{N}$.

Induktionsanfang: $k = 0$. Dann ist

$$\sum_{l=0}^{k} (b-1)\cdot b^l = (b-1)\cdot b^0 = b-1 = b^{0+1} - 1.$$

Induktionsschritt: Die Gleichung gelte f'ur k (Induktionsvoraussetzung). Dann gilt die Gleichung auch f'ur $k+1$:

$$\begin{aligned}\sum_{l=0}^{k+1}(b-1)\cdot b^l &= (b-1)\cdot b^{k+1}+\sum_{l=0}^{k}(b-1)\cdot b^l\\ &= (b-1)\cdot b^{k+1}+b^{k+1}-1 \text{ (nach Induktionsvoraussetzung)}\\ &= b^{k+2}-b^{k+1}+b^{k+1}-1\\ &= b^{(k+1)+1}-1\end{aligned}$$

□

Der Beweis kann auch elegant durch Ausklammern der Summe gef'uhrt werden:

$$\begin{aligned}&(b-1)\cdot b^l+(b-1)\cdot b^{l-1}+\cdots+(b-1)\cdot b+(b-1)\cdot 1\\ =\ & b^{l+1}-b^l+b^l-b^{l-1}+b^{l-1}-\cdots-b^2+b^2-b+b-1\\ =\ & b^{l+1}-1\end{aligned}$$

Lemma 85. *Sei b eine nat"urliche Zahl $\geqslant 2$. F"ur jede nat"urliche Zahl $n \geqslant 1$ gibt es eine* Darstellung

$$n = z_k\cdot b^k + z_{k-1}\cdot b^{k-1}+\cdots+z_1\cdot b^1+z_0 = \sum_{l=0}^{k} z_l\cdot b^l$$

mit $k\in\mathbb{N}$, $z_0, z_1, ..., z_k \in \{0,1,...,b-1\}$ und $z_k \neq 0$.

*Die Folge $z_k, z_{k-1}, ..., z_1, z_0$ ist eine b-*adische Darstellung *von n ; sie wird einfacher als $z_kz_{k-1}...z_1z_0$ als "Wort" mit den* Ziffern *z_l geschrieben. Wenn man die Basis b hervorheben m"ochte, wird auch $(z_kz_{k-1}...z_1z_0)_b$ geschrieben. Diese Darstellung ist* eindeutig *bestimmt: wenn*

$$n = (y_ly_{l-1}...y_1y_0)_b$$

ebenfalls b-adische Darstellung von n ist, so ist

$$k = l \text{ und } z_k = y_k, z_{k-1} = y_{k-1}, ..., z_1 = y_1, z_0 = y_0\,.$$

Wir schreiben die Gleichheit der Ziffernfolgen in beiden Darstellungen auch als

$$(z_kz_{k-1}...z_1z_0)_b \equiv (y_ly_{l-1}...y_1y_0)_b$$

Im Fall $b=2$ spricht man von der bin"aren *Darstellung von Zahlen und dem* bin"aren Zahlsystem. *Im Fall $b=10$ betrachtet man* Dezimaldarstellungen *und* Dezimalzahlen. *Im Fall $b=16$ spricht man von* hexadezimalen *Darstellungen und* Hexadezimalzahlen.

Beweis. Wir zeigen die Existenz und die Eindeutigkeit der Darstellungen durch zwei vollst"andige Induktionsargumente. Setze $b^* = b-1$; b^* entspricht der 9 in der Dezimaldarstellung, sie hat eine besondere Rolle beim Rechnen "mit "Ubertrag".

Existenz: F"ur $n=0$ ist nichts zu zeigen.

Angenommen, die Behauptung gilt f'ur n. Wir zeigen die Behauptung f'ur $n+1$.

F"ur $1 = 1_b$ eine b-adische Darstellung von $0+1$.

Sei $n>0$ und sei $n=(z_kz_{k-1}...z_1z_0)_b$ eine b-adische Darstellung von n.

Fall 1: $z_0 < b^*$. Dann ist

$$\begin{aligned}n+1 &= (z_kz_{k-1}...z_1z_0)_b+1\\ &= z_k\cdot b^k+z_{k-1}\cdot b^{k-1}+\cdots+z_1\cdot b^1+(z_0+1)\\ &= (z_kz_{k-1}...z_1(z_0+1))_b\end{aligned}$$

eine b-adische Darstellung von $n+1$.

Fall 2: $z_0 = b^*$ und es gibt ein $l \leqslant k$ mit $z_l \neq b^*$. W"ahle $l \leqslant k$ minimal mit dieser Eigenschaft. Dann ist

$$(z_k z_{k-1} ... z_1 z_0)_b = (z_k ... z_l b^* ... b^*)_b$$

$$\begin{aligned} n+1 &= (z_k ... z_l b^* ... b^*)_b + 1 \\ &= z_k \cdot b^k + z_{k-1} \cdot b^{k-1} + \cdots + z_l \cdot b^l + (b^* \cdot b^{l-1} + b^* \cdot b^{l-2} + \cdots + b^* \cdot b + b^*) + 1 \\ &= z_k \cdot b^k + z_{k-1} \cdot b^{k-1} + \cdots + z_l \cdot b^l + (b^l - 1) + 1 \\ &= z_k \cdot b^k + z_{k-1} \cdot b^{k-1} + \cdots + (z_l + 1) \cdot b^l \\ &= (z_k z_{k-1} ... (z_l + 1) 0 ... 0)_b \end{aligned}$$

ist eine b-adische Darstellung von $n+1$.

Fall 3: $z_l = b^*$ f'ur alle $l \leqslant k$. Dann ist

$$(z_k z_{k-1} ... z_1 z_0)_b = (b^* ... b^*)_b$$

mit $k+1$ vielen b^*.

$$\begin{aligned} n+1 &= (b^* ... b^*)_b + 1 \\ &= (b^* \cdot b^k + b^* \cdot b^{k-1} + \cdots + b^* \cdot b + b^*) + 1 \\ &= (b^{k+1} - 1) + 1 \\ &= b^{k+1} \\ &= (10...0)_b \end{aligned}$$

mit $k+1$ vielen 0 ist eine b-adische Darstellung von $n+1$.

Eindeutigkeit:

F"ur $n = 0$ ist nichts zu zeigen.

Angenommen, die Behauptung gilt f'ur n. Wir zeigen die Behauptung f'ur $n+1$.

$n = (z_k z_{k-1} ... z_1 z_0)_b$ ist die eindeutige Darstellung von n. Weiter sei

$$\begin{aligned} 1 &= (y_l y_{l-1} ... y_1 y_0)_b \\ &= y_l \cdot b^l + y_{l-1} \cdot b^{l-1} + \cdots + y_1 \cdot b^1 + y_0 \end{aligned}$$

Damit diese Gleichung gilt, ist es *notwendig*, dass $y_l = y_{l-1} = \cdots = y_1 = 0$ ist. Dann ist $1 = y_0$ und daher

$$(y_l y_{l-1} ... y_1 y_0)_b \equiv (1)_b$$

Damit ist die Darstellung von $1 = 0 + 1$ eindeutig bestimmt.

Sei $n > 0$. Angenommen $n = (z_k z_{k-1} ... z_1 z_0)_b$ ist die eindeutige Darstellung von n. Weiter sei $n+1 = (y_l y_{l-1} ... y_1 y_0)_b$ eine Darstellung von $n+1$. Wir machen eine Fallunterscheidung "ahnlich wie oben:

Fall 1: $y_0 \neq 0$. Dann ist $(y_l y_{l-1} ... y_1 (y_0 - 1))_b$ eine Darstellung von n. Wegen der Eindeutigkeit f'ur n ist

$$(y_l y_{l-1} ... y_1 (y_0 - 1))_b \equiv (z_k z_{k-1} ... z_1 z_0)_b$$

Damit ist $l = k$, $y_l = z_l, ..., y_1 = z_1$, $y_0 - 1 = z_0$ und $y_0 = z_0 + 1$. Also ist die Darstellung von $n+1$ in diesem Fall eindeutig bestimmt.

Fall 2: $y_0 = 0$. Sei $r < l$ maximal mit $y_r = 0$:

$$n+1 = (y_l y_{l-1} ... y_1 y_0)_b \equiv (y_l ... y_{r+1} 0 ... 0)_b$$

Dann ist $y_{r+1} \neq 0$ und

$$\begin{aligned} n &= (y_l ... y_{r+1} 0 ... 0)_b - 1 \\ &= y_l \cdot b^l + \cdots + y_{r+1} \cdot b^{r+1} - 1 \\ &= y_l \cdot b^l + \cdots + (y_{r+1} - 1) \cdot b^{r+1} + (b^{r+1} - 1) \\ &= y_l \cdot b^l + \cdots + (y_{r+1} - 1) \cdot b^{r+1} + b^* \cdot b^r + \cdots + b^* \cdot b^1 + b^* \\ &= (y_l ... (y_{r+1} - 1) b^* ... b^*)_b \end{aligned}$$

Wegen der Eindeutigkeit f'ur n ist

$$(y_l ... (y_{r+1} - 1) b^* ... b^*)_b \equiv (z_k z_{k-1} ... z_1 z_0)_b$$

Damit ist $l = k$, $y_l = z_l, ..., y_{r+2} = z_{r+2}$, $y_{r+1} - 1 = z_{r+1}$, d.h. $y_{r+1} = z_{r+1} + 1$ und $y_r = y_{r-1} = \cdots = y_0 = 0$. Also ist die Darstellung von $n+1$ auch in diesem Fall eindeutig bestimmt. □

Die 0 wird durch die Ziffernfolge "0" dargestellt.

10.1 Rechnen mit *b*-adischen Zahlen

Die b-adische Darstellung $n = (z_k z_{k-1} ... z_1 z_0)_b$ f'ur $n > 0$ und $b > 2$ wird durch den folgenden *Algorithmus* (Rechenvorschrift) aus n gewonnen: durch Division mit Rest wird sukzessive definiert:

$$\begin{aligned} n &= n_0 \cdot b + z_0 \text{ mit } 0 \leqslant z_0 < b \text{ und } n_0 \neq 0 \\ n_0 &= n_1 \cdot b + z_1 \text{ mit } 0 \leqslant z_1 < b \text{ und } n_1 \neq 0 \\ n_1 &= n_2 \cdot b + z_2 \text{ mit } 0 \leqslant z_2 < b \text{ und } n_2 \neq 0 \\ &\vdots \\ n_{k-2} &= n_{k-1} \cdot b + z_{k-1} \text{ mit } 0 \leqslant z_{k-1} < b \text{ und } n_{k-1} \neq 0 \\ n_{k-1} &= n_k \cdot b + z_k \text{ mit } 0 \leqslant z_k < b \text{ und } n_k = 0 \end{aligned}$$

Diese Berechnung wird durchgef'uhrt, bis man zu $n_k = 0$ gelangt. Da $n_0 > n_1 > \cdots > n_k$ wird dies nach endlich vielen Schritten erreicht.

Dann ist $(z_k z_{k-1} ... z_1 z_0)_b$ die eindeutig bestimmte b-adische Darstellung von n:

$$\begin{aligned} n &= n_0 \cdot b + z_0 \\ &= (n_1 \cdot b + z_1) \cdot b + z_0 = n_1 \cdot b^2 + z_1 \cdot b + z_0 \\ &= n_2 \cdot b^3 + z_2 \cdot b^2 + z_1 \cdot b + z_0 \\ &\vdots \\ &= n_{k-1} \cdot b^k + z_{k-1} \cdot b^{k-1} + \cdots + z_2 \cdot b^2 + z_1 \cdot b + z_0 \\ &= z_k \cdot b^k + z_{k-1} \cdot b^{k-1} + \cdots + z_2 \cdot b^2 + z_1 \cdot b + z_0 \\ &= (z_k z_{k-1} ... z_1 z_0)_b \end{aligned}$$

Beispiel: Die 7-adische Darstellung von 428:

$$\begin{aligned} 428 &= 61 \cdot 7 + 1 \\ 61 &= 8 \cdot 7 + 5 \\ 8 &= 1 \cdot 7 + 1 \\ 1 &= 0 \cdot 7 + 1 \end{aligned}$$

$$428_{10} = 1151_7 = 1 \cdot 7^3 + 1 \cdot 7^2 + 5 \cdot 7 + 1$$

Statt mit nat"urlichen Zahlen "an sich" rechnet man effektiv mit ihren b-adischen Darstellungen bzw. 7-adischen Darstellungen:

	1	1	5	1
+	2	0	1	6
	0	1	1	0
=	3	2	0	0

Diese Rechnung operiert mit den Ziffern oder "Symbolen" 0, 1, 2, 3, 4, 5, 6 und benutzt eine Additionstafel f"ur die Basis 7:

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	10
2	2	3	4	5	6	10	11
3	3	4	5	6	10	11	12
4	4	5	6	10	11	12	13
5	5	6	10	11	12	13	14
6	6	10	11	12	13	14	15

Der Algorithmus f"ur die "schriftliche Addition" wird durch eine Reihe von Rechenschritten realisiert. Er arbeitet mit *strukturierten, symbolischen Daten* und nicht mit nat"urlichen Zahlen:

Eingabe:

	1	1	5	1
+	2	0	1	6
				0

	1	1	5	1
+	2	0	1	6
			1	0
				0

	1	1	5	1
+	2	0	1	6
		1	1	0
			0	0

	1	1	5	1
+	2	0	1	6
	0	1	1	0
		2	0	0

	1	1	5	1
+	2	0	1	6
0	0	1	1	0
	3	2	0	0

Ergebnis:

	1	1	5	1
+	2	0	1	6
0	0	1	1	0
=	3	2	0	0

In b-adischer Darstellung l"asst sich auch die Summe

				a_k	a_{k-1}	...	a_1	a_0
+		b_l	...	b_k	b_{k-1}	...	b_1	b_0
=	c_{l+1}	c_l	...	c_k	c_{k-1}	...	c_1	c_0

der Zahlen $(a_k a_{k-1}...a_0)_b$ und $(b_l b_{l-1}...b_0)_b$ mit $l \geqslant k$ effizient mit dem Algorithmus der *schriftlichen Addition* berechnen. Dabei m"ussen die "Ubertr"age $u_{l+1}, u_l, ..., u_1, u_0$ bzgl. der Basis b ber"ucksichtigt werden:

				a_k	a_{k-1}	...	a_1	a_0
+		b_l	...	b_k	b_{k-1}	...	b_1	b_0
	u_{l+1}	u_l	...	u_k	u_{k-1}	...	u_1	u_0
=	c_{l+1}	c_l	...	c_k	c_{k-1}	...	c_1	c_0

Dabei ist, wieder unter Benutzung von Division mit Rest,

$$\begin{aligned}
u_0 &= 0 \\
u_1 \cdot b + c_0 &= a_0 + b_0 + u_0 \text{ mit } 0 \leqslant c_0 < b \\
u_2 \cdot b + c_1 &= a_1 + b_1 + u_1 \text{ mit } 0 \leqslant c_1 < b \\
&\vdots \\
u_{k+1} \cdot b + c_k &= a_k + b_k + u_k \text{ mit } 0 \leqslant c_k < b \\
u_{k+2} \cdot b + c_{k+1} &= b_{k+1} + u_{k+1} \text{ mit } 0 \leqslant c_{k+1} < b \\
&\vdots \\
u_{l+1} \cdot b + c_l &= b_l + u_l \text{ mit } 0 \leqslant c_l < b \\
c_{l+1} &= u_{l+1}
\end{aligned}$$

Wenn $c_{l+1} \neq 0$ ist, so ist $(c_{l+1} c_l ... c_0)_b$ die Darstellung der Summe. Ansonsten ist $(c_l c_{l-1} ... c_0)_b$ die Darstellung der Summe.

Noch ein Beispiel mit *schriftlicher Division*.

Wir wollen das Ergebnis 3200_7 durch Rechnen mit der Basis 7 im Zehner-System mit der Basis $10 = 13_7$ darstellen:

```
3 2 0 0 : 1 3 = 2 2 0    R 1 0
2 6
  3 0
  2 6
    1 0
    0 0
    1 0

  2 2 0 : 1 3 = 1 4    R 2
  1 3
    6 0
    5 5
      2

  1 4 : 1 3 = 1    R 1
  1 3
    1

  1 : 1 3 = 0    R 1
  0
  1
```

Also ist

$$3200_7 = 1127_{10}$$

wobei benutzt wird, dass $10_7 = 7_{10}$ ist. Gegenprobe (im Dezimalsystem):

$$3200_7 = 3 \cdot 343 + 2 \cdot 49 = 1029 + 98 = 1127_{10}$$

10.2 Bin"arzahlen

Technisch besonders wichtig ist das 2-adische oder *bin"are* Zahlsystem wegen der Einfachheit der bin"aren Additionstafel

$+_2$	0	1
0	0	1
1	1	10

und der bin"aren Multiplikationstafel

$\times_2$	0	1
0	0	0
1	0	1

Beide lassen sich technisch gut durch digitallogische Schaltungen implementieren.

11 Teilbarkeit

Hatten die Division mit Rest: $n = \lfloor \frac{n}{b} \rfloor \cdot b + r$. Teilbarkeit liegt vor, wenn der Rest $r = 0$.

Definition 86. *Seien $a, d \in \mathbb{N}$. d ist ein* Teiler *von a, oder a ist ein Vielfaches von a , wenn es $x \in \mathbb{N}$ gibt, so dass $a = x \cdot d$. Wir schreiben $d \mid a$ und auch $d \nmid a$ f"ur $\neg(d \mid a)$.*

Man beachte, dass nach dieser Definition $n \mid 0$ f'ur alle $n \in \mathbb{N}$ und $0 \nmid n$ f'ur alle $n \in \mathbb{N} \setminus \{0\}$.

Lemma 87. *Seien $a, b, c \in \mathbb{N}$. Dann gilt*

a) $a \mid b$ *und* $b \mid c$ *impliziert* $a \mid c$.

b) $a \mid b$ *und* $a \mid c$ *impliziert* $a \mid (b + c)$.

c) $(c \cdot a \mid c \cdot b)$ *und* $c \neq 0$ *impliziert* $a \mid b$.

d) $a \mid b$ *und* $b \mid a$ *impliziert* $a = b$.

Die Teilbarkeit erf"ullt die Axiome einer *partiellen Ordnung*:

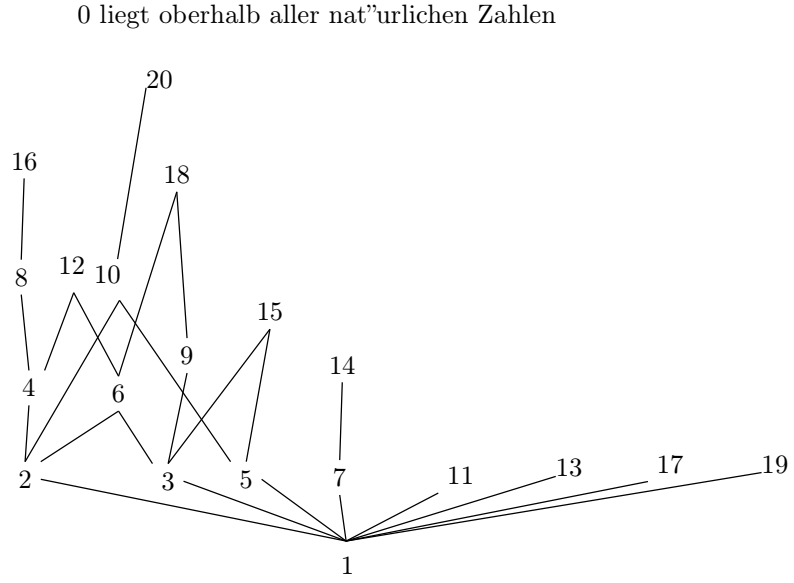
Lemma 88. *Seien $a, b, c \in \mathbb{N}$. Dann gilt*

a) (Reflexivit"at) $a \mid a$.

b) (Transitivit"at) $a \mid b$ *und* $b \mid c$ *impliziert* $a \mid c$.

c) (Antisymmetrie) $a \mid b$ *und* $b \mid a$ *impliziert* $a = b$.

Man beachte, dass | *keine* lineare Ordnung ist, weil die Linearit"at verletzt ist: $2 \nmid 3$ und $3 \nmid 2$. Die Relation auf den Zahlen $0, 1, ..., 20$ kann man folgendermaßen als *Hasse-Diagramm* darstellen:



12 Gr"oßte gemeinsame Teiler und der Euklidische Algorithmus

Definition 89. *Seien $a, b \in \mathbb{N}$ mit $a \neq 0$ oder $b \neq 0$. Dann ist*

$$\mathrm{ggT}(a, b) = \max \{d \in \mathbb{N} \mid d \mid a \wedge d \mid b\}$$

der gr"oßte gemeinsame Teiler *von a und b.*

Lemma 90. *Seien $a, b, c \in \mathbb{N}$ mit $a \neq 0$. Dann*

a) $\mathrm{ggT}(a, b) = \mathrm{ggT}(b, a) \leqslant \max(a, b)$;

b) $\mathrm{ggT}(a, c \cdot a) = a$;

c) $\mathrm{ggT}(a, 0) = \mathrm{ggT}(a, a) = a$;

d) $\mathrm{ggT}(1, b) = 1$.

Beweis. "Ubung. □

Die Division mit Rest erh"alt in gewisser Weise den ggT:

Lemma 91. *Sei $a, b, r \in \mathbb{N}$ mit $a = q \cdot b + r$ und $a \neq 0$. Dann ist*

$$\mathrm{ggT}(a, b) = \mathrm{ggT}(b, r)$$

Beweis. Wir zeigen, dass

$$\{d \in \mathbb{N} \mid d \mid a \wedge d \mid b\} = \{d \in \mathbb{N} \mid d \mid b \wedge d \mid r\}.$$

Wir benutzen das Extensionalit"atsaxiom.

Sei $d \in \{d \in \mathbb{N} \mid d \mid a \wedge d \mid b\}$. Dann gilt $d \mid a \wedge d \mid b$. Da $r = a - q \cdot b$, ist $d \mid r$. Also $d \mid b \wedge d \mid r$ und $d \in \{d \in \mathbb{N} \mid d \mid b \wedge d \mid r\}$.

Umgekehrt sei $d \in \{d \in \mathbb{N} \mid d \mid b \wedge d \mid r\}$. Dann gilt $d \mid b \wedge d \mid r$. Da $a = q \cdot b + r$, ist $d \mid a$. Also $d \mid a \wedge d \mid b$ und $d \in \{d \in \mathbb{N} \mid d \mid a \wedge d \mid b\}$. □

Wenn $a, b, r \in \mathbb{N}$ mit $a > b \geqslant 1$, $a = q \cdot b + r$ und $0 \leqslant r < b$ wie bei der Division mit Rest, so ist $b < a$ und $r < b$. Das bedeutet, dass die Berechnung von $\mathrm{ggT}(a, b) = \mathrm{ggT}(b, r)$ auf kleinere Eingabezahlen reduziert ist.

Dies f"uhrt zum *Euklidischen Algorithmus*:

Seien nat"urliche Zahlen $n_0 \geqslant n_1 > 0$ gegeben. Definiere mit Hilfe der Division mit Rest induktiv bzw. rekursiv:

$$\begin{aligned} n_0 &= q_0 \cdot n_1 + n_2 \text{ mit } 0 \leqslant n_2 < n_1 \\ n_1 &= q_1 \cdot n_2 + n_3 \text{ mit } 0 \leqslant n_3 < n_2 \\ &\vdots \\ n_{k-1} &= q_{k-1} \cdot n_k + 0 \end{aligned}$$

Wenn zum ersten Mal der Rest 0 erreicht wird, stoppt die Berechnung. Dieser Algorithmus berechnet den gr"oßten gemeinsamen Teiler:

Satz 92. *Seien $n_0 \geqslant n_1 > 0$ nat"urliche Zahlen. Dann liefert der Euklidische Algorithmus eine endliche Folge $n_0, \ldots, n_k$ mit*

$$\mathrm{ggT}(n_0, n_1) = n_k.$$

Beweis. *Fall 1*: n_0 ist ein Vielfaches von n_1. Dann ist $n_0 = q_0 \cdot n_1 + 0$. Die Berechnung stoppt sofort mit $n_k = n_1$ und

$$\mathrm{ggT}(n_0, n_1) = \mathrm{ggT}(q \cdot n_1, n_1) = n_1 = n_k.$$

Fall 2: n_0 ist kein Vielfaches von n_1. Dann ist $n_0 > n_1$ und der Euklidische Algorithmus berechnet eine Folge $n_0 > n_1 > n_2 > \ldots > 0$. Eine strikt absteigende Folge von nat"urlichen Zahlen ist endlich. Daher erreicht der Algorithmus schließlich die Gleichung

$$n_{k-1} = q_{k-1} \cdot n_k + 0,$$

womit n_k definiert ist. Nach dem vorangehenden Lemma ist

$$\mathrm{ggT}(n_0, n_1) = \mathrm{ggT}(n_1, n_2) = \ldots = \mathrm{ggT}(n_k, 0) = n_k.$$ □

Beispiel: Seien $n_0 = 53115$ und $n_1 = 2017$. Dann ist

$$\begin{aligned} 53115 &= 26 \cdot 2017 + 673 \\ 2017 &= 2 \cdot 673 + 671 \\ 673 &= 1 \cdot 671 + 2 \\ 671 &= 335 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0 \text{ , STOP} \end{aligned}$$

Damit ist $\mathrm{ggT}(53115, 2017) = 1$. Man nennt die beiden Zahlen dann auch *teilerfremd*: sie haben außer der 1 keinen gemeinsamen Teiler.

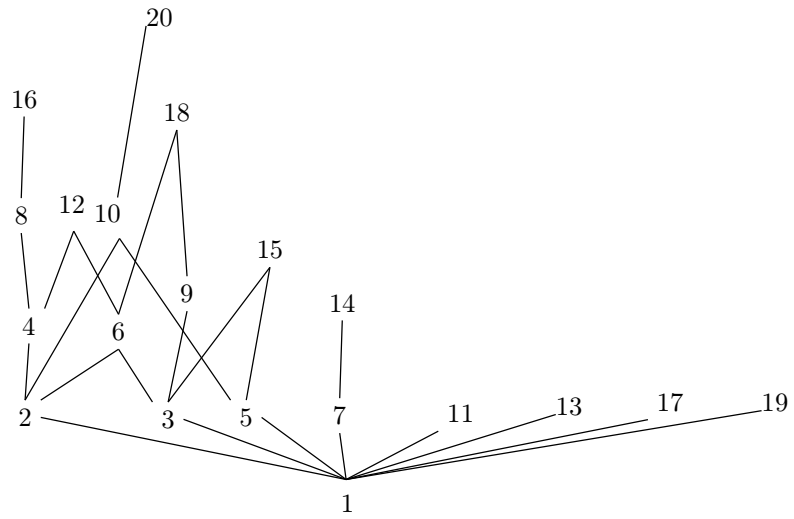
$$\begin{aligned}
53115 &= 26 \cdot 2016 + 699 \\
2016 &= 2 \cdot 699 + 618 \\
699 &= 1 \cdot 618 + 81 \\
618 &= 7 \cdot 81 + 51 \\
81 &= 1 \cdot 51 + 30 \\
51 &= 1 \cdot 30 + 21 \\
30 &= 1 \cdot 21 + 9 \\
21 &= 2 \cdot 9 + 3 \\
9 &= 3 \cdot 3 + 0 \text{ , STOP}
\end{aligned}$$

Also ist $\mathrm{ggT}(53115, 2016) = 3$.

13 Primzahlen

Besonders wichtig f'ur die Teilbarkeitsrelation sind die Zahlen des Hassediagramms, die direkt oberhalb der 1 liegen: $2, 3, 5, 7, 11, 13, 17, 19, \ldots$. Diese Zahlen p haben genau zwei Teiler: 1 und p.

0 liegt oberhalb aller nat"urlichen Zahlen



Definition 93. *Eine nat"urliche Zahl p ist eine* Primzahl *oder* prim*, wenn sie genau zwei Teiler besitzt:*

$$|\{d \in \mathbb{N} \mid d \mid p\}| = 2.$$

D.h., $p \geqslant 2$ und $\{d \in \mathbb{N} \mid d \mid p\} = \{1, p\}$.

Es sei $\mathbb{P}$ die Menge der Primzahlen.

Da jede Zahl $n \geqslant 2$ die zwei Teiler 1 und n besitzt, sind Primzahlen Zahlen mit minimaler Anzahl von Teilern.

Wir beweisen zun"achst eine wichtige Variante der vollst"andigen Induktion.

Satz 94. *(*Allgemeine Induktion*) Sei $\varphi(x)$ eine Eigenschaft, f"ur die gilt:*

Induktivit"at: *wenn $\varphi(n')$ f"ur alle nat"urlichen Zahlen $n' < n$ gilt, so gilt $\varphi(n)$.*

Dann gilt $\varphi(n)$ f"ur alle $n \in \mathbb{N}$.

Beweis. Sei $\varphi(x)$ induktiv. Die Behauptung folgt sofort aus

(1) F"ur alle nat"urlichen Zahlen m und f'ur alle $n < m$ gilt $\varphi(n)$.

Beweis. Durch vollst"andige Induktion "uber m.

Induktionsanfang: $m = 0$. Da es keine nat"urlichen Zahlen $n < 0$ gibt, gilt (1) f'ur 0 trivialerweise.

Induktionsschritt: Angenommen, (1) gilt f'ur m, d.h. $\varphi(n)$ gilt f'ur alle $n < m$. Wegen der Induktivit"at von φ gilt dann auch $\varphi(m)$. Damit gilt $\varphi(n)$ f'ur alle $n < m + 1$ und somit gilt (1) f'ur $m + 1$. □

Das entsprechende (allgemeine) Induktionsschema lautet dann:

Behauptung: F"ur alle nat"urlichen Zahlen n gilt $\varphi(n)$.

Beweis: Durch (allgemeine) Induktion "uber n.

Sei $n \in \mathbb{N}$ und gelte $\varphi(n')$ f'ur alle $n' < n$. ... . Also gilt $\varphi(n)$. □

Lemma 95. *Zu jeder nat"urlichen Zahl $n \geqslant 2$ existiert eine Primzahl p mit $p \mid n$.*

Beweis. Durch Induktion "uber n.

Sei $n \in \mathbb{N}$ und das Lemma gelte f'ur alle $n' < n$. O.B.d.A. sei $n \geqslant 2$..

Fall 1: n ist eine Primzahl. Dann ist die Behauptung mit $p = n$ erf'ullt.

Fall 2: n ist keine Primzahl. Dann gibt es einen Teiler $n' \mid n$ mit $n' \neq 1$ und $n' \neq n$. Damit ist $2 \leqslant n' \leqslant m$. Nach der Induktionsvoraussetzung existiert eine Primzahl p mit $p \mid n'$. Dann ist auch $p \mid n$, und die Behauptung ist erf'ullt. □

Betrachte eine nat"urliche Zahl $n \geqslant 2$. Nach dem Lemma gibt es eine Primzahl p_0 und ein n_0 mit $1 \leqslant n_0 < n$, so dass $n = p_0 \cdot n_0$. Wenn $n_0 \geqslant 2$ ist, gibt es weiter eine Primzahl p_1 und ein n_1 mit $1 \leqslant n_1 < n$, so dass $n = p_0 \cdot p_1 \cdot n_1$. Da es keine unendlich absteigende Folge von nat"urlichen Zahlen gibt, ergeben sich so Folgen $n_0 > n_1 > \cdots > n_k = 1$ und Primzahlen $p_0, p_1, ..., p_k$, so dass

$$n = p_0 \cdot \cdots \cdot p_k .$$

Ein solches Produkt ist eine *Primzahlzerlegung* von n. Wir wollen zeigen, dass eine solche Zerlegung bis auf die Reihenfolge der Faktoren eindeutig ist. Dazu ben"otigen wir passende Begriffe und Notationen f'ur Produkte von endlichen Folgen nat"urlicher Zahlen.

Man beachte, dass es bei Produkten wie $n = 7 \cdot 5 \cdot 5 \cdot 3$ nicht auf die Reihenfolge der Faktoren ankommt. Man kann die Faktoren daher der Gr"oße nach geordnet voraussetzen: $n = 3 \cdot 5 \cdot 5 \cdot 7$. Des weiteren kann man gleiche Faktoren zu Potenzen zusammenziehen: $n = 3 \cdot 5^2 \cdot 7$ oder $n = 3^1 \cdot 5^2 \cdot 7^1$. Schließlich kann man sich vorstellen, die "ubrigen nat"urlichen Zahlen ebenfalls Faktoren mit dem Exponenten 0 sind:

$$n = 0^0 \cdot 1^0 \cdot 2^0 \cdot 3^1 \cdot 4^0 \cdot 5^2 \cdot 6^0 \cdot 7^1 \cdot 8^0 \cdot ...$$

Der Ausdruck auf der rechten Seite ist durch eine Funktion bestimmt, die jeder Zahl i einen Exponenten $e(i) \in \mathbb{N}$ zuordnet.

Definition 96. *F"ur eine Funktion* $e\colon \mathbb{N} \to \mathbb{N}$ *sei*

$$\mathrm{tr}(e) = \{i \in \mathbb{N} \mid e(i) \neq 0\}$$

der Tr"ager *von* π. *Ein* endliches Produkt *nat"urlicher Zahlen ist eine Funktion* $e\colon \mathbb{N} \to \mathbb{N}$, *deren Tr"ager endlich ist. Das endliche Produkt* e *wird auch durch*

$$a_0^{e(a_0)} \cdot a_1^{e(a_1)} \cdots a_{k-1}^{e(a_{k-1})}$$

oder

$$\prod_{i=0}^{k-1} a_i^{e(a_i)}$$

bezeichnet, wobei die a_i *paarweise verschieden sind und* $\{a_0, ..., a_{k-1}\} = \mathrm{tr}(e)$. *Wir sagen, dass eine Zahl* a *in dem Produkt* e vorkommt, *wenn* $a \in \mathrm{tr}(e)$.

Der Wert *des Produkts* $a_0^{e(a_0)} \cdot a_1^{e(a_1)} \cdots a_{k-1}^{e(a_{k-1})}$ *ist die nat"urliche Zahl, die sich durch Auswerten der Potenzierungen und Multiplikationen ergibt. Wenn wir den Wert von* e *mit* $\|e\|$ *bezeichnen, so l"asst sich dieser auch rekursiv (induktiv) definieren:*

$$\begin{aligned} \|e\| &= 1 \text{ , wenn } \mathrm{tr}(e) = \emptyset \\ \left\|a_0^{e(a_0)} \cdot a_1^{e(a_1)} \cdots a_{k-1}^{e(a_{k-1})}\right\| &= \left\|a_0^{e(a_0)} \cdot a_1^{e(a_1)} \cdots a_{k-2}^{e(a_{k-2})}\right\| \cdot a_{k-1}^{e(a_{k-1})} \end{aligned}$$

Man beachte, dass ein Produkt ein formaler Ausdruck wie $2^3 \cdot 3^2$ oder $3^2 \cdot 2^3$ ist. Als Ausdr"ucke sind diese beiden verschieden, aber sie ergeben auf Grund der Gesetze der Arithmetik denselben Wert:

$$\|2^3 \cdot 3^2\| = \|3^2 \cdot 2^3\|.$$

Allerdings ist es "ublich, die Auswertungsstriche fortzulassen, da meistens die Werte im Vordergrund stehen. Wir schreiben dann

$$n = a_0^{e(a_0)} \cdot a_1^{e(a_1)} \cdots a_{k-1}^{e(a_{k-1})}$$

statt

$$n = \left\|a_0^{e(a_0)} \cdot a_1^{e(a_1)} \cdots a_{k-1}^{e(a_{k-1})}\right\|.$$

Satz 97. (Euklid) *Die Menge* $\mathbb{P}$ *der Primzahlen ist unendlich.*

Beweis. Angenommen, die Menge $\mathbb{P}$ sei endlich. Definiere dann das endliche Produkt $e\colon \mathbb{N} \to \mathbb{N}$ aller Primzahlen durch

$$e(q) = \begin{cases} 1 \text{ , wenn } q \in \mathbb{P} \\ 0 \text{ , wenn } q \notin \mathbb{P} \end{cases}$$

Sei

$$n = \|e\| = \left\| \prod_{q \in \mathbb{N}} q^{e(q)} \right\| = \left\| \prod_{p \in \mathbb{P}} p \right\|$$

(der Wert des) Produkt(s) aller Primzahlen. Nach dem vorangehenden Lemma gibt es eine Primzahl p mit $p \mid n + 1$. Da $p \in \mathbb{P}$ ist auch $p \mid n = \|\prod_{p \in \mathbb{P}} p\|$. Das impliziert $p \mid (n + 1 - n) = 1$. Widerspruch. Also ist $\mathbb{P}$ unendlich. $\square$

Andere Beweise des Satzes von Euklid:

1. Aus *Das Buch der Beweise* von M. Aigner und G. M. Ziegler:

Euklids Beweis. F"ur eine beliebige Menge $\{p_1, ..., p_r\}$ von Primzahlen sei $n := p_1 p_2 \cdots p_r + 1$ und p ein Primteiler von n. Wir sehen, dass p von allen p_i verschieden ist, da sonst p sowohl die Zahl n als auch das Produkt $p_1 p_2 \cdots p_r$ teilen w"urde, somit auch die 1, was nicht sein kann. Eine endliche Menge $\{p_1, ..., p_r\}$ kann also niemals die Menge *aller* Primzahlen sein.

2. Eine formale aber lesbare Version dieses Beweises, die von einem automatischen Beweispr"ufer akzeptiert wird:

Satz. The set of prime numbers is infinite.

Beweis. Let A be a finite set of prime numbers. Take a function p and a number r such that p lists A in r steps. ran $p \subseteq \mathbb{N}^+$. $\prod_{i=1}^{r} p_i \neq 0$. Take $n = \prod_{i=1}^{r} p_i + 1$. n is nontrivial. Take a prime divisor q of n (by PrimDiv).

Let us show that q is not an element of A. Assume the contrary. Take i such that ($1 \leq i \leq r$ and $q = p_i$). p_i divides $\prod_{i=1}^{r} p_i$ (by MultProd). Then q divides 1 (by DivMin). Contradiction. qed.

Hence A is not the set of prime numbers. □

3. Der Satz des Euklid im Originaltext aus dem 9. Buch der *Elemente*, Proposition 20 in deutscher "Ubersetzung.

Die Anzahl der Primzahlen ist größer als jede Zahl, die vorgelegt wird.

Wenn A, B, C Primzahlen sind, dann, sage ich, ist die Anzahl der Primzahlen größer als die Anzahl der A, B, C. Denn zu A, B, C sei ED das kleinste gemeinsame Vielfache [wie VII.38.]. Die Summe aus ED und der Einheit DF sei EF.

Es ist dann EF Primzahl oder nicht.

Ist EF Primzahl, dann ist die Anzahl der Primzahlen A, B, C, EF größer als die der A, B, C.

Ist EF keine Primzahl, dann ist EF Vielfache einer Primzahl G [wie VII.34.]. Ich sage, G ist verschieden von A, B, C. Denn wenn nicht, ist, da A, B, C Teiler von ED sind, auch G Teiler von ED. Da G Teiler von EF ist, ist dann G auch Teiler der Einheit DF, was nicht möglich ist. Also ist G verschieden von A, B, C. Da G Primzahl ist, ist die Anzahl der Primzahlen A, B, C, G größer als die der A, B, C, was zu zeigen war.

Definition 98. *Ein endliches Produkt* $e: \mathbb{N} \to \mathbb{N}$ *ist eine* Primfaktorzerlegung *wenn der Tr"ager von* e *nur aus Primzahlen besteht:*

$$\mathrm{tr}(e) \subseteq \mathbb{P}.$$

Eine Primfaktorzerlegung von n *ist eine Primfaktorzerlegung* e *mit*

$$n = \|e\|.$$

Satz 99. *Jede nat"urliche Zahl* $n \geqslant 1$ *besitzt eine Primfaktorzerlegung.*

Beweis. Durch Induktion "uber n. Sei $n \in \mathbb{N}$ und der Satz gelte f'ur $m < n$. F"ur $n = 0$ gilt der Satz trivialerweise. Sei also $n \geqslant 1$.

Fall 1: $n = 1$. Definiere die triviale Primfaktorzerlegung $e: \mathbb{N} \to \mathbb{N}$ durch

$$e(q) = 0.$$

Dann ist $\|e\| = 1$ und e ist eine Primfaktorzerlegung von 1.

Fall 2: $n \geqslant 2$. Nach einem vorangehenden Lemma w"ahle eine Primzahl p mit $p \mid n$. Sei $n = p \cdot m$. Dann ist $1 \leqslant m$ und $m < n$. Nach der Induktionsvoraussetzung w"ahle eine Primfaktorzerlegung $e_0 \colon \mathbb{N} \to \mathbb{N}$ von m. Definiere eine neue Primfaktorzerlegung $e \colon \mathbb{N} \to \mathbb{N}$ durch

$$e(q) = \begin{cases} e_0(q) + 1\,, \text{ falls } q = p \\ e_0(q)\,, \text{ falls } q \neq p \end{cases}$$

Dann ist

$$\|e\| = p \cdot \|e_0\| = p \cdot m = n\,. \qquad \square$$

Lemma 100. *Sei n eine nat"urliche Zahl und sei p ein* Primteiler *von n, d.h. p ist eine Primzahl und $p \mid n$. Dann besitzt n eine Primfaktorzerlegung, in der p vorkommt.*

Beweis. Sei $n = p \cdot m$. Sei $\prod_{i=0}^{k-1} p_i^{e(p_i)}$ eine Primfaktorzerlegung von m. Dann ist

$$p \cdot \prod_{i=0}^{k-1} p_i^{e(p_i)}$$

eine Primfaktorzerlegung von n, in der p vorkommt. $\square$

Satz 101. *Jede nat"urliche Zahl $n \geqslant 1$ besitzt* genau eine *Primfaktorzerlegung.*

Beweis. Durch Induktion "uber n. Sei $n \in \mathbb{N}$ und der Satz gelte f"ur $m < n$. F"ur $n = 0$ gilt der Satz trivialerweise. Sei also $n \geqslant 1$.

Angenommen, n besitze zwei verschiedene Primfaktorzerlegungen

$$n = \prod_{i=0}^{k-1} p_i^{e(p_i)}$$

und

$$n = \prod_{j=0}^{l-1} q_j^{f(q_j)}$$

mit Primzahlen $p_0 < \ldots < p_{k-1}$, $q_0 < \ldots < q_{l-1}$ und Exponenten $e(p_0)$, ..., $e(p_{k-1})$, $f(q_0)$, ..., $f(q_{l-1}) \geqslant 1$. Offensichtlich ist dann $n \geqslant 2$ und n ist keine Primzahl.

(1) Keine Primzahl kommt sowohl in $\prod_{i=0}^{k-1} p_i^{e(p_i)}$ als auch in $\prod_{j=0}^{l-1} q_j^{f(q_j)}$ vor, d.h. $p_i \neq q_j$ f"ur alle $i < k$ und $j < l$.

Beweis. Angenommen $p = p_i = q_j$. Definiere endliche Produkte $e' \colon \mathbb{N} \to \mathbb{N}$ und $f' \colon \mathbb{N} \to \mathbb{N}$ durch

$$e'(q) = \begin{cases} e(q) - 1\,, \text{ falls } q = p_i \\ e(q)\,, \text{ falls } q \neq p_i \end{cases}$$

und

$$f'(q) = \begin{cases} f(q) - 1\,, \text{ falls } q = p_i \\ f(q)\,, \text{ falls } q \neq p_i \end{cases}$$

Dann sind e' und f' zwei verschiedene Primfaktorzerlegungen von n / p_i:

$$n/p = \prod_{i=0}^{k-1} p_i^{e'(p_i)} = \prod_{j=0}^{l-1} q_j^{f'(q_j)}.$$

Das widerspricht der Induktionsvoraussetzung. *qed*(1)

(2) $p_0 \cdot q_0 < n$.

Beweis. Sei o.B.d.A. $p_0 < q_0$. Dann ist

$$p_0 \cdot q_0 < q_0 \cdot q_0 < q_0 \cdot q_1 \leqslant n.$$

qed(2)

Sei $n_0 = n - p_0 \cdot q_0$. Dann ist $1 \leqslant n_0 < n$. Weiter gilt $p_0 \,|\, n_0$ und $q_0 \,|\, n_0$. Nach einem vorangehenden Lemma hat n_0 eine Primfaktorzerlegung, in der p_0 vorkommt und eine Primfaktorzerlegung, in der q_0 vorkommt. Nach Induktionsvoraussetzung ist die Primfaktorzerlegung von n_0 eindeutig, so dass p_0 *und* q_0 in der eindeutigen Primfaktorzerlegung von n_0 vorkommen. Diese sei

$$n_0 = p_0 \cdot q_0 \cdot r_0^{g_0} \cdots r_{m-1}^{g_{m-1}}.$$

Dann ist

$$n = n_0 + p_0 \cdot q_0 = p_0 \cdot q_0 \cdot (r_0^{g_0} \cdots r_{m-1}^{g_{m-1}} + 1).$$

Sei $h \colon \mathbb{N} \to \mathbb{N}$ eine Primfaktorzerlegung von $r_0^{g_0} \cdots r_{m-1}^{g_{m-1}} + 1$. Dann ist

$$n = p_0 \cdot q_0 \cdot \prod_{s \in \mathbb{N}} s^{h(s)}$$

eine weitere Primfaktorzerlegung von n , in der sowohl p_0 als auch q_0 vorkommen. In (1) war aber bewiesen worden, dass in zwei verschiedenen Primfaktorzerlegung von n keine gemeinsamen Primzahlen vorkommen. Widerspruch. □

Lemma 102. *Sei p eine Primzahl mit $p \,|\, a \cdot b$. Dann gilt $p \,|\, a$ oder $p \,|\, b$.*

Beweis. Offensichtlich sind $a, b \geqslant 1$. Seien $e, f \colon \mathbb{N} \to \mathbb{N}$ Primfaktorzerlegungen von a bzw. b:

$$a = \|e\| \text{ und } b = \|f\|.$$

Definiere die "Summe" $g = e + f \colon \mathbb{N} \to \mathbb{N}$ durch $g(q) = e(q) + f(q)$. Dann ist g eine Primfaktorzerlegung von $a \cdot b$:

$$a \cdot b = \|g\|.$$

Weil $p \,|\, a \cdot b$ gibt es eine Primfaktorzerlegung von $a \cdot b$, in der p vorkommt. Weil die Primfaktorzerlegung eindeutig ist, kommt p in g vor, d.h. $g(p) \neq 0$. Da $g(p) = e(p) + f(p)$, ist $e(p) \neq 0$ oder $f(p) \neq 0$. Daraus folgt $p \,|\, a$ oder $p \,|\, b$. □

14 Gruppen

Definition 103. *Eine* Gruppe $\mathfrak{G}$ *besteht aus einer* Tr"agermenge G*, einer* Gruppenoperation $*$: $G \times G \to G$ *und einem* neutralen Element $e \in G$ *so dass f"ur alle $a, b, c \in G$ gilt*

a) $(a * b) * c = a * (b * c)$

b) $a * e = e * a = a$

c) f"ur alle a existiert b mit $a * b = b * a = e$. Man nennt b ein inverses Element *zu a.*

Wir schreiben die Gruppe $\mathfrak{G}$ auch als Tripel ihrer Bestandteile:

$$\mathfrak{G} = (G, *, e).$$

Wenn außerdem noch

d) $a * b = b * a$

gilt, so ist $\mathfrak{G}$ *eine* abelsche *Gruppe.*

Beispiel 104. Wir hatten bereits gesehen: f'ur jede Menge ist die symmetrische Gruppe $\mathfrak{S}(M)$ aller Bijektionen von M mit der Komposition von Funktionen als Gruppenoperation und mit der identischen Abbildung id_M eine Gruppe. Die Gruppe $\mathfrak{S}(\{0,1,2\})$ ist nicht abelsch.

Beispiel 105. Die Menge $\{0,1\}$ mit der bin"aren Summe

$+_2$	0	1
0	0	1
1	1	0

und dem neutralen Element 0 ist eine abelsche Gruppe. Hierzu kann man die Gesetze *a*)-*d*) durch Nachrechnen "uberpr"ufen.

Beispiel 106. Die nat"urlichen Zahlen $\mathbb{N}$ mit der Operation + und der 0 bilden *keine* Gruppe, da das Gesetz *c*) nicht erf'ullt ist: es existiert kein $b \in \mathbb{N}$ mit $1 + b = 0$. Wir werden die nat"urlichen Zahlen bald zu einer Gruppe erweitern.

Das Rechnen in Gruppen hat den Vorteil, dass man "k"urzen" kann:

Lemma 107.

a) *Sei* $a * b = a * c$. *Dann ist* $b = c$.

b) *Sei* $b * a = c * a$. *Dann ist* $b = c$.

Beweis. *a*) Nach *c*) w"ahle ein $d \in G$ mit $d * a = e$. Dann ist

$$b = e * b = (d * a) * b = d * (a * b) = d * (a * c) = (d * a) * c = e * c = c.$$

b) l"asst sich entsprechend beweisen. □

Da die Gruppenoperation assoziativ ist, kann man die Klammern in der obigen Gleichungskette auch weglassen und erh"alt:

$$b = e * b = d * a * b = d * a * c = e * c = c.$$

Lemma 108. *Zu jedem* $a \in G$ *existiert genau ein inverses Element in* G. *Damit l"asst sich die Funktion* $^{-1}\colon G \to G$

$$a^{-1} = \textit{das inverse Element zu } a$$

definieren. Die Funktion $^{-1}\colon G \to G$ *ist bijektiv, d.h.* $^{-1} \in \mathfrak{S}(G)$.

Beweis. Seien b und c inverse Elemente zu a. Dann ist $a * b = e$ und $a * c = e$. Also ist $a * b = a * c$ und nach dem Lemma "uber das K"urzen ist $b = c$. □

Lemma 109.

a) $(a^{-1})^{-1} = a$. *Damit ist* $(^{-1}) \circ (^{-1}) = \mathrm{id}_G$.

b) $(a*b)^{-1} = b^{-1}*a^{-1}$.

Beweis. *a*) Weil $a^{-1}*a = e$.

b) Weil $(a*b)*(b^{-1}*a^{-1}) = a*(b*b^{-1})*a^{-1} = a*e*a^{-1} = a*a^{-1} = e$. □

Lemma 110. *Sei $a \in G$. Definiere eine Funktion $f: G \to G$ durch*

$$f(b) = a*b.$$

Dann ist f bijektiv und $f \in \mathfrak{S}(G)$.

Beweis. (1) f ist surjektiv.

Beweis. Sei $c \in G$. Setze $b = a^{-1}*c$. Dann ist

$$f(b) = a*b = a*(a^{-1}*c) = (a*a^{-1})*c = e*c = c.$$

Also ist $c \in \mathrm{bild}(f)$. *qed*(1)

(2) f ist injektiv.

Beweis. Seien $b, b' \in G$ mit $f(b) = f(b')$. Dann ist $a*b = a*b'$ und nach den K"urzungsregeln ist $b = b'$. □

Satz 111. (Cayley) *Betrachte die Gruppe $\mathfrak{G} = (G, *, e)$. Definiere eine Funktion $\pi: G \to \mathfrak{S}(G)$ durch*

$$(\pi(a))(b) = a*b.$$

Schreibe auch π_a f"ur $\pi(a)$. Dann gilt

a) *π ist injektiv.*

b) $\pi_{a*b} = \pi_a \circ \pi_b$.

c) $\pi_e = \mathrm{id}_G$.

d) $\pi_{a^{-1}} = (\pi_a)^{-1}$.

Beweis. *a*) Seien $a, a' \in G$ mit $\pi_a = \pi_{a'}$. Dann ist

$$a = a*e = \pi_a(e) = \pi_b(e) = b*e = b.$$

b) F"ur alle $c \in G$ gilt

$$\pi_{a*b}(c) = (a*b)*c = a*(b*c) = a*\pi_b(c) = \pi_a(\pi_b(c)) = (\pi_a \circ \pi_b)(c).$$

c) F"ur alle $c \in G$ gilt

$$\pi_e(c) = e*c = c = \mathrm{id}_G(c).$$

d) Weil $\pi_a \in \mathfrak{S}(G)$ ist $(\pi_a)^{-1}$ definiert. F"ur alle $c \in G$ ist $(\pi_a)^{-1}(c)$ das eindeutige b mit $\pi_a(b) = c$. Dieses b erf"ullt $a*b = c$ bzw. $b = a^{-1}*c$ bzw. $b = \pi_{a^{-1}}(c)$. Somit ist $(\pi_a)^{-1}(c) = \pi_{a^{-1}}(c)$ und $\pi_{a^{-1}} = (\pi_a)^{-1}$. □

Nach dem Satz von Cayley l"asst sich jede Gruppe in die symmetrische Gruppe "uber ihrer Tr"agermenge "einbetten". Die Abbildung π ist injektiv und sie bewahrt die Gruppenoperation und das neutrale Element (sowie die Inversenbildung). Dies schreibt man auch als

$$\pi: \mathfrak{G} \to \mathfrak{S}(G)$$

oder

$$\pi\colon (G,*,e)\to(\mathfrak{S}(G),\circ,\mathrm{id}_G)\,.$$

15 Die ganzen Zahlen

Wir wollen die Struktur (ℕ, +, 0) der nat"urlichen Zahlen zur Gruppe (ℤ, +, 0) der *ganzen Zahlen* erweitern. Dabei wollen wir ℤ aus den ℕ konstruieren, um zu demonstrieren, dass das neue Zahlsystem aus dem vorhandenen konstruiert werden kann.

Die Konstruktion kann durch unser Vorwissen "uber die bekannten ganzen Zahlen

$$\ldots,-n,\ldots,-1000,\ldots,-3,-2,-1,0,1,2,3,\ldots,1000,\ldots,n,\ldots$$

motiviert werden. Die negative Zahl -3 ist auf vielfache Weise *Differenz* von nat"urlichen Zahlen:

$$-3=0-3=1-4=2-5=3-6=\ldots$$

Die auftretenden Zahlenpaare $(0,3),(1,4),(2,5),\ldots$ sind in Bezug darauf, die Zahl -3 darzustellen, "aquivalent. Wir arbeiten im Folgenden mit geordneten Paaren nat"urlicher Zahlen, die anschaulich als Differenzen gesehen werden. Zwei "Differenzen" $(a,\,b)$ und $(a',\,b')$, die f"ur $a-b$ und $a'-b'$ stehen sollen, stellen dieselbe Zahl dar oder sind "aquivalent, wenn

$$a+b'=a'+b$$

ist.

Lemma 112. *Sei $Z=\mathbb{N}\times\mathbb{N}$. Definiere eine zweistellige Relation $\sim_Z$ auf Z durch*

$$(a,b)\sim_Z(a',b') \text{ gdw. } a+b'=a'+b.$$

Dann ist $\sim_Z$ eine "Aquivalenzrelation auf Z : f"ur alle $(a,b),(a',b'),(a'',b'')\in Z$ gilt:

a) (Reflexivit"at) $(a,b)\sim_Z(a,b)$

b) (Symmetrie) $(a,b)\sim_Z(a',b')$ impliziert $(a',b')\sim_Z(a,b)$

c) (Transitivit"at) $(a,b)\sim_Z(a',b')$ und $(a',b')\sim_Z(a'',b'')$ impliziert $(a,b)\sim_Z(a'',b'')$.

Beweis. *a)* Da $a+b=a+b$.

b) Sei $(a,b)\sim_Z(a',b')$. Dann ist $a+b'=a'+b$ und $a'+b=a+b'$. Also ist $(a',b')\sim_Z(a,b)$.

c) Sei $(a,b)\sim_Z(a',b')$ und $(a',b')\sim_Z(a'',b'')$. Dann ist $a+b'=a'+b$ und $a'+b''=a''+b'$. Addition der Gleichungen ergibt

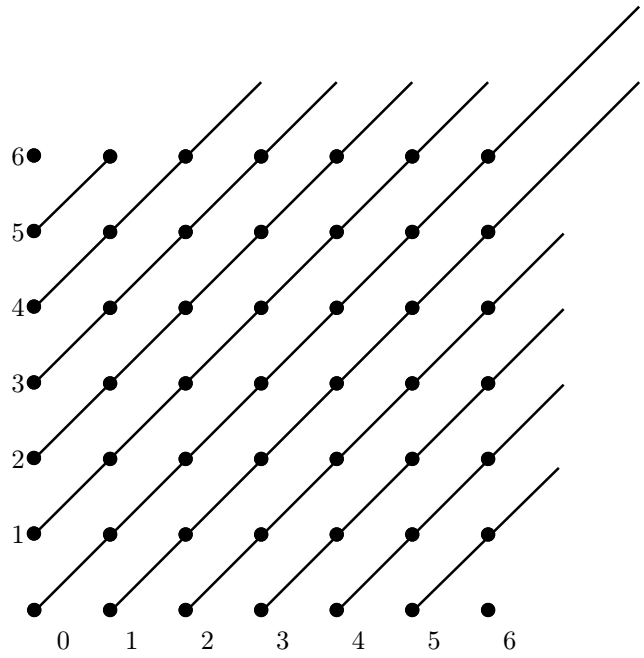
$$a+b'+a'+b''=a'+b+a''+b'.$$

Durch "K"urzung" der auf beiden Seiten vorkommenden Summanden a' und b' und Umordnung ergibt sich

$$a+b''=a''+b,$$

d.h. $(a,b)\sim_Z(a'',b'')$. □

Hier ein Bild von $Z=\mathbb{N}\times\mathbb{N}$; Punkte auf den diagonalen Halbgeraden sind bzgl. $\sim_Z$ zueinander "aquivalent, sie bilden die "Aquivalenzklassen modulo $\sim_Z$.



$Z = \mathbb{N} \times \mathbb{N}$

Lemma 113. *F"ur* $(a,b) \in Z$ *definiere die Menge*

$$\overline{(a,b)} = \{(a',b') \in Z |\, (a',b') \sim_Z (a,b)\}.$$

$\overline{(a,b)}$ *ist die* "Aquivalenzklasse *von* (a,b) *bez"uglich (oder "modulo") der "Aquivalenzrelation* $\sim_Z$*. Dann gilt f"ur* $(a,b),(a',b') \in Z$*:*

a) $(a,b) \in \overline{(a,b)}$.

b) $(a,b) \sim_Z (a',b')$ *gdw.* $\overline{(a,b)} = \overline{(a',b')}$.

c) $(a,b) \nsim_Z (a',b')$ *gdw.* $\overline{(a,b)} \cap \overline{(a',b')} = \emptyset$.

Beweis. *a)* Wegen der Reflexivit"at von $\sim_Z$ ist $(a,b) \sim_Z (a,b)$. Also ist $(a,b) \in \overline{(a,b)}$.

Wir zeigen zun"achst zwei Behauptungen:

(1) $(a,b) \sim_Z (a',b')$ impliziert $\overline{(a,b)} = \overline{(a',b')}$.

Beweis. Sei $(a,b) \sim_Z (a',b')$. Wir zeigen $\overline{(a,b)} = \overline{(a',b')}$ mit Hilfe des Extensionalit"atsaxioms.

Sei $(a'',b'') \in \overline{(a,b)}$. Dann ist $(a'',b'') \sim_Z (a,b)$. Wegen der Transitivit"at von $\sim_Z$ ist $(a'',b'') \sim_Z (a', b')$. Also ist $(a'',b'') \in \overline{(a',b')}$.

Umgekehrt sei $(a'',b'') \in \overline{(a',b')}$. Dann ist $(a'',b'') \sim_Z (a',b')$. Wegen der Symmetrie von $\sim_Z$ ist $(a', b') \sim_Z (a,b)$. Wegen der Transitivit"at von $\sim_Z$ ist $(a'',b'') \sim_Z (a,b)$. Also ist $(a'',b'') \in \overline{(a,b)}$. *qed*(1)

(2) $(a,b) \nsim_Z (a',b')$ impliziert $\overline{(a,b)} \cap \overline{(a',b')} = \emptyset$.

Beweis. Sei $(a,\ b) \nsim_Z (a',\ b')$. Angenommen, es w"are $\overline{(a,b)} \cap \overline{(a',b')} \neq \emptyset$. W"ahle $(a'',\ b'') \in \overline{(a,b)} \cap \overline{(a',b')}$. Dann ist $(a'',b'') \sim_Z (a,b)$ und $(a'',b'') \sim_Z (a',b')$. Wegen der Symmetrie von $\sim_Z$ ist $(a,b) \sim_Z (a'',b'')$. Wegen der Transitivit"at von $\sim_Z$ ist $(a,b) \sim_Z (a',b')$. Widerspruch. *qed*(2)

b) (1) zeigt die "Hin"-Richtung der logischen "Aquivalenz. Umgekehrt sei $\overline{(a,b)} = \overline{(a',b')}$. Dann ist $\overline{(a,b)} \cap \overline{(a',b')} = \overline{(a,b)} \neq \emptyset$. Nach (2) ist damit $(a,b) \sim_Z (a',b')$.

c) (2) zeigt die "Hin"-Richtung der logischen "Aquivalenz. Umgekehrt sei $\overline{(a,b)} \cap \overline{(a',b')} = \emptyset$. Dann ist $\overline{(a,b)} \neq \overline{(a',b')}$. Nach (1) ist damit $(a,b) \nsim_Z (a',b')$. □

Definition 114. *Die Menge der* ganzen Zahlen *sei die Menge aller "Aquivalenzklassen modulo* $\sim_Z$

$$\mathbb{Z} = \{\overline{(a,b)} \mid (a,b) \in Z\}.$$

Definiere die bin"are Operation $+_{\mathbb{Z}}\colon \mathbb{Z}\times\mathbb{Z}\to\mathbb{Z}$ *durch*

$$\overline{(a,b)} +_{\mathbb{Z}} \overline{(a',b')} = \overline{(a+a',b+b')}.$$

Definiere ein neutrales Element

$$0_{\mathbb{Z}} = \overline{(0,0)}.$$

Lemma 115. *Die Operation* $+_{\mathbb{Z}}\colon \mathbb{Z}\times\mathbb{Z}\to\mathbb{Z}$ *ist wohldefiniert.*

Beweis. Seien $\overline{(a,b)} = \overline{(c,d)}$ und $\overline{(a',b')} = \overline{(c',d')}$. Es ist zu zeigen, dass

$$\overline{(a+a',b+b')} = \overline{(c+c',d+d')}.$$

Aus den Annahmen folgt: $a+d=c+b$ und $a'+d'=c'+b'$. Die "Summe" dieser Gleichungen ergibt

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

Sortiert bedeutet das

$$(a+a')+(d+d') = (c+c')+(b+b')$$

und

$$(a+a',b+b') \sim_Z (c+c',d+d').$$ □

Satz 116. $\mathbb{Z}$ *ist eine abelsche Gruppe mit der Gruppenoperation* $+_{\mathbb{Z}}$ *und dem neutralen Element* $0_{\mathbb{Z}}$.

Beweis. Wir "uberpr"ufen die Gruppenaxiome. Seien $\overline{(a,b)}, \overline{(a',b')}, \overline{(a'',b'')} \in \mathbb{Z}$.

Assoziativit"at:

$$\begin{aligned}
(\overline{(a,b)} +_{\mathbb{Z}} \overline{(a',b')}) +_{\mathbb{Z}} \overline{(a'',b'')} &= \overline{(a+a',b+b')} +_{\mathbb{Z}} \overline{(a'',b'')} \\
&= \overline{(a+a'+a'',b+b'+b'')} \\
&= \overline{(a,b)} +_{\mathbb{Z}} \overline{(a'+a'',b'+b'')} \\
&= \overline{(a,b)} +_{\mathbb{Z}} (\overline{(a',b')} +_{\mathbb{Z}} \overline{(a'',b'')})
\end{aligned}$$

Neutralit"at von $0_{\mathbb{Z}} = \overline{(0,0)}$:

$$\overline{(a,b)} +_{\mathbb{Z}} \overline{(0,0)} = \overline{(a,b)} = \overline{(0,0)} +_{\mathbb{Z}} \overline{(a,b)}.$$

Existenz *inverser* Elemente; wir zeigen, dass $\overline{(b,a)}$ invers zu $\overline{(a,b)}$ ist. Weil $(a+b,a+b) \sim_{\mathbb{Z}} (0,0)$ ist

$$\overline{(a,b)} +_{\mathbb{Z}} \overline{(b,a)} = \overline{(a+b,a+b)} = \overline{(0,0)} = \overline{(b,a)} +_{\mathbb{Z}} \overline{(a,b)}.$$

Kommutativit"at:

$$\overline{(a,b)} +_{\mathbb{Z}} \overline{(a',b')} = \overline{(a+a',b+b')} = \overline{(a',b')} +_{\mathbb{Z}} \overline{(a,b)}.$$ □

$\mathbb{Z}$ wurde als Zahlbereich konstruiert, in dem beliebige *Differenzen* bebildet werden k"onnen.

Definition 117. *F"ur $x \in \mathbb{Z}$ bezeichne das inverse Element mit $-x$ (anstelle von x^{-1}); $-x$ ist das* Negative *von x. F"ur $x, y \in \mathbb{Z}$ ist die* Differenz $x - y$ *definiert als $x +_{\mathbb{Z}} (-y)$.*

Satz 118. *Die Struktur $(\mathbb{N}, +, 0)$ l"asst sich durch die Funktion $f: \mathbb{N} \to \mathbb{Z}$,*

$$f(n) = \overline{(n, 0)}$$

"kanonisch" in die Gruppe $(\mathbb{Z}, +_{\mathbb{Z}}, 0_{\mathbb{Z}})$ einbetten. *D.h.:*

a) $f: \mathbb{N} \to \mathbb{Z}$ ist injektiv;

b) f"ur $m, n \in \mathbb{N}$ ist

$$f(m+n) = f(m) +_{\mathbb{Z}} f(n);$$

c) $f(0) = 0_{\mathbb{Z}}$.

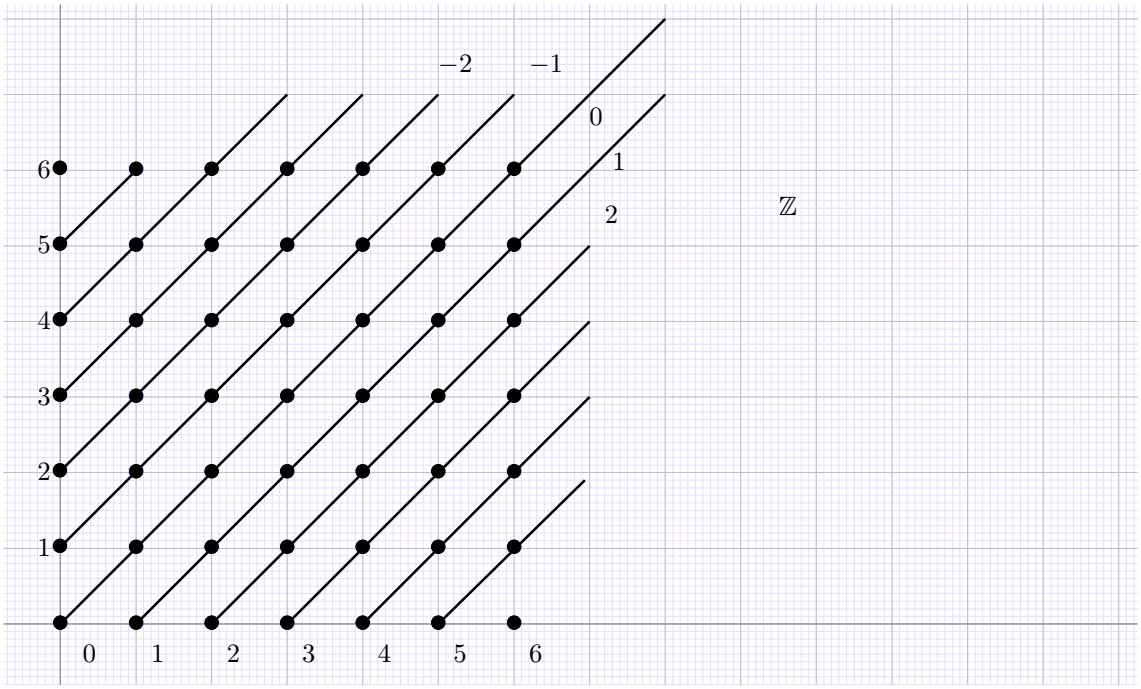
Beweis. *a)* Sei $f(m) = f(n)$. Dann ist $\overline{(m,0)} = \overline{(n,0)}$, $(m,0) \sim_Z (n,0)$ und

$$m = m + 0 = n + 0 = n.$$

b)

$$f(m+n) = \overline{(m+n,0)} = \overline{(m,0)} +_{\mathbb{Z}} \overline{(n,0)} = f(m) +_{\mathbb{Z}} f(n). \qquad \square$$

In der Graphik ist $\mathbb{Z}$ die Menge der diagonalen Halbgeraden. Diese sind von "links oben" nach "rechts unten" der Gr"oße nach geordnet. In der Mitte liegt $0_{\mathbb{Z}} (\equiv 0)$, die Diagonale des Quadranten Z.



Mit Hilfe der kanonischen Einbettung verh"alt sich $(\mathbb{N}, +, 0)$ genauso wie sein Bild $(f[\mathbb{N}], +_{\mathbb{Z}}, 0_{\mathbb{Z}})$ unter f. Wir k"onnen daher eine Identifikation jeder nat"urlichen Zahl $n \in \mathbb{N}$ mit ihrem Bild $f(n)$ vornehmen, womit $\mathbb{N} \subseteq \mathbb{Z}$ ist. Die Operation $+_{\mathbb{Z}}$ auf $\mathbb{Z}$ ist dann eine Erweiterung der Addition auf $\mathbb{N}$, und wir k"onnen vereinfachend auch $+$ f'ur $+_{\mathbb{Z}}$ schreiben. Weiter ist mit dieser Identifikation $0 = 0_{\mathbb{Z}}$. Damit l'asst sich die Struktur der ganzen Zahlen als $(\mathbb{Z}, +, 0)$ schreiben.

Wir wollen jetzt nachweisen, dass die ganzen Zahlen aus den nat"urlichen Zahlen und ihren Negativen bestehen.

Satz 119. *Setze* $-\mathbb{N} = \{-x \mid x \in \mathbb{N}\}$. *Dann ist*

a) $\mathbb{Z} = \mathbb{N} \cup (-\mathbb{N})$

b) $\mathbb{N} \cap (-\mathbb{N}) = \{0\}$

Beweis. *a)* Wir brauchen offensichtlich nur die Inklusion $\subseteq$ zeigen. Sei $x = \overline{(a,b)} \in \mathbb{Z}$.

Fall 1. $a \geqslant b$. Dann gibt es eine nat"urliche Zahl $n \in \mathbb{N}$ mit $b + n = a$. Es gilt $a + 0 = n + b$, $(a, b) \sim_Z (n, 0)$ und $x = \overline{(n,0)} = f(n) \in f[\mathbb{N}]$. Nach der Identifikation von $\mathbb{N}$ und $f[\mathbb{N}]$ ist damit $x \in \mathbb{N}$.

Fall 2. $a < b$. Dann gibt es eine nat"urliche Zahl $n \in \mathbb{N}$ mit $a + n = b$. Es gilt $a + n = 0 + b$, $(a, b) \sim_{\mathbb{Z}} (0, n)$ und $x = \overline{(0,n)} = -\overline{(n,0)} = -f(n) \in -f[\mathbb{N}]$. Nach der Identifikation von $\mathbb{N}$ und $f[\mathbb{N}]$ ist damit $x \in -\mathbb{N}$.

b) Sei $x \in \mathbb{N} \cap (-\mathbb{N})$. Dann gibt es $m, n \in \mathbb{N}$, so dass $x = \overline{(m,0)} = -\overline{(n,0)}$. Dann ist $\overline{(m,0)} = \overline{(0,n)}$, $(m, 0) \sim_Z (0, n)$ und $m + n = 0 + 0 = 0$. Diese Gleichung l"asst sich in $\mathbb{N}$ nur durch $m = n = 0$ l"osen. Damit ist $x = \overline{(0,0)} = 0_{\mathbb{Z}}$ und $x = 0$ nach der Identifikation von 0 und $0_{\mathbb{Z}}$.

Umgekehrt sieht man sofort, dass

$$(0 =)\, 0_{\mathbb{Z}} = \overline{(0,0)} = -\overline{(0,0)} \in f[\mathbb{N}] \cap (-f[\mathbb{N}])(= \mathbb{N} \cap (-\mathbb{N})). \qquad \square$$

II Sommersemester 2017

16 Strukturen

Im ersten Teil der Vorlesung haben wir verschiedene Bereiche mathematischer Objekte kennengelernt, ausgehend von den Bereichen der Mengen und Funktionen. Auf diesen Bereichen existieren Relationen, Operationen und Konstanten mit nat"urlichen und n"utzlichen strukturellen und rechnerischen Eigenschaften:

1. Der Bereich der *Mengen*; darauf Relationen wie: $\in$ Elementbeziehung, $\subseteq$ Teilmenge (reflexiv, transitiv, antisymmetrisch partielle Ordnung); Operationen: $\cup$, $\cap$ Vereinigung, Schnitt (assoziativ, kommutativ, distributiv), $\times$ kartesisches Produkt; Konstante: $\emptyset$ leere Menge.

2. Der Bereich der *Funktionen*; Operation $\circ$ Komposition (assoziativ).

3. Die Menge $\mathbb{N}$ der *nat"urlichen Zahlen*; Relationen: $<, \leqslant$; Operationen: $+, \cdot$; Konstanten: $0, 1$.

4. Die Menge $\mathbb{Z}$ der *ganzen Zahlen*; Relationen: $<, \leqslant$; Operationen: $+, -$; Konstanten: 0.

5. Die *symmetrische Gruppe* $\mathfrak{S}(M)$ auf der Menge M mit der Tr"agermenge $\{f \mid f\colon M \to M$ ist bijektiv$\}$; Operationen: $\circ$ Komposition, $^{-1}$ Inversenbildung; Konstante: id_M.

6. Eine *Gruppe* $\mathfrak{G}$ besteht aus einer Tr"agermenge G, einer Gruppenoperation $*\colon G \times G \to G$ und einem neutralen Element $e \in G$.

Auf allen Bereichen liegt außerdem die Relation = der *Gleichheit* von Elementen vor. Eine Menge ist ein spezieller, "kleiner" Bereich, n"amlich der Bereich ihrer Elemente.

Definition 120. *Ein Bereich $\mathcal{S}$ zusammen mit darauf definierten Relationen, Operationen und Konstanten ist eine* Struktur*, wenn der Bereich $\mathcal{S}$ eine Menge ist, die dann als* Tr"agermenge *von $\mathcal{S}$ bezeichnet wird. Die Tr"agermenge von $\mathcal{S}$ wird oft mit demselben Symbol $\mathcal{S}$ oder mit dem entsprechenden lateinischen Buchstaben S bezeichnet.*

Damit sind die Zahlbereiche $\mathbb{N}$, $\mathbb{Z}$ Strukturen, und auch die symmetrische Gruppe $\mathcal{S}(M)$.

Wir erweitern die Struktur $\mathbb{Z}$ der ganzen Zahlen um eine Multiplikation, die die Multiplikation auf den nat"urlichen Zahlen erweitert. Die ganze Zahl $\overline{(a,b)}$ entspricht anschaulich der Differenz $a-b$. F"ur die Multiplikation von Differenzen ergibt die bekannte "Buchstabenrechnung":

$$(a-b)\cdot(c-d) = a\cdot c - a\cdot d - b\cdot c + b\cdot d = (a\cdot c + b\cdot d) - (a\cdot d + b\cdot c)$$

Dementsprechend definieren wir:

Definition 121. *Definiere die bin"are Operation $\cdot_{\mathbb{Z}}\colon \mathbb{Z}\times\mathbb{Z}\to\mathbb{Z}$ durch*

$$\overline{(a,b)}\cdot_{\mathbb{Z}}\overline{(a',b')} = \overline{(a\cdot a' + b\cdot b', a\cdot b' + b\cdot a')}.$$

Definiere ein neutrales Element

$$1_{\mathbb{Z}} = \overline{(1,0)}.$$

Lemma 122. *Die Operation $\cdot_{\mathbb{Z}}\colon \mathbb{Z}\times\mathbb{Z}\to\mathbb{Z}$ ist wohldefiniert.*

Beweis. "Ubung. □

Nach diesen Definitionen ist $(-1)\cdot_{\mathbb{Z}}(-1) = +1$:

$$(-1)\cdot_{\mathbb{Z}}(-1) = \overline{(0,1)}\cdot_{\mathbb{Z}}\overline{(0,1)} = \overline{(0\cdot 0 + 1\cdot 1, 0\cdot 1 + 1\cdot 0)} = \overline{(1,0)} = 1.$$

Lemma 123. *Die Struktur $(\mathbb{Z},\ \cdot_{\mathbb{Z}},\ 1_{\mathbb{Z}})$ ist assoziativ und kommutativ und besitzt das neutrale Element $1_{\mathbb{Z}}$.*

Beweis. Seien $\overline{(a,b)}, \overline{(a',b')}, \overline{(a'',b'')} \in \mathbb{Z}$.

(Assoziativit"at) Wir berechnen die unterschiedlich geklammerten Produkte

$$\begin{aligned} & (\overline{(a,b)}\cdot_{\mathbb{Z}}\overline{(a',b')})\cdot_{\mathbb{Z}}\overline{(a'',b'')} \\ = \ & \overline{(a\cdot a' + b\cdot b', a\cdot b' + b\cdot a')}\cdot_{\mathbb{Z}}\overline{(a'',b'')} \\ = \ & \overline{(a\cdot a'\cdot a'' + b\cdot b'\cdot a'' + a\cdot b'\cdot b'' + b\cdot a'\cdot b'',\ a\cdot a'\cdot b'' + b\cdot b'\cdot b'' + a\cdot b'\cdot a'' + b\cdot a'\cdot a'')} \end{aligned}$$

und

$$\begin{aligned} & \overline{(a,b)}\cdot_{\mathbb{Z}}(\overline{(a',b')}\cdot_{\mathbb{Z}}\overline{(a'',b'')}) \\ = \ & (a,b)\cdot_{\mathbb{Z}}\overline{(a'\cdot a'' + b'\cdot b'',\ a'\cdot b'' + b'\cdot a'')} \\ = \ & \overline{(a\cdot a'\cdot a'' + a\cdot b'\cdot b'' + b\cdot a'\cdot b'' + b\cdot b'\cdot a'',\ a\cdot a'\cdot b'' + a\cdot b'\cdot a'' + b\cdot a'\cdot a'' + b\cdot b'\cdot b'')} \end{aligned}$$

Die Ausdr"ucke auf den rechten Seiten sind gleich.

(Kommutativit"at)

$$\overline{(a,b)}\cdot_{\mathbb{Z}}\overline{(a',b')} = \overline{(a\cdot a' + b\cdot b', a\cdot b' + b\cdot a')} = \overline{(a'\cdot a + b'\cdot b, a'\cdot b + b'\cdot a)} = \overline{(a',b')}\cdot_{\mathbb{Z}}\overline{(a,b)}.$$

(Neutralit"at)

$$\overline{(a,b)} \cdot_{\mathbb{Z}} \overline{(1,0)} = \overline{(a \cdot 1 + b \cdot 0, a \cdot 0 + b \cdot 1)} = \overline{(a,b)}$$

und

$$\overline{(1,0)} \cdot_{\mathbb{Z}} \overline{(a,b)} = \overline{(1 \cdot a + 0 \cdot b, 1 \cdot b + 0 \cdot a)} = \overline{(a,b)}$$ □

Lemma 124. *Die Struktur* $(\mathbb{Z}, \cdot_{\mathbb{Z}}, 1_{\mathbb{Z}})$ *ist* keine *Gruppe.*

Beweis. Wir zeigen, dass $\overline{(2,0)}$ kein Inverses besitzt ("$\frac{1}{2}$ ist keine ganze Zahl"). Angenommen $\overline{(a,b)}$ w"are invers zu $\overline{(2,0)}$. Dann ist

$$\overline{(1,0)} = \overline{(a,b)} \cdot_{\mathbb{Z}} \overline{(2,0)} = \overline{(a \cdot 2 + b \cdot 0, a \cdot 0 + b \cdot 2)} = \overline{(a \cdot 2, b \cdot 2)}$$

Dann ist $(1,0) \sim_Z (a \cdot 2, b \cdot 2)$ und daher

$$1 + b \cdot 2 = a \cdot 2.$$

Aber die linke Seite der Gleichung ist ungerade, w"ahrend die rechte gerade ist. Widerspruch. □

Man beachte, dass die Struktur des Beweises dem Argument f"ur die Irrationalit"at von $\sqrt{2}$ "ahnelt.

Interessant ist auch das Zusammenspiel der Strukturen $(\mathbb{Z}, +_{\mathbb{Z}}, 0_{\mathbb{Z}})$ und $(\mathbb{Z}, \cdot_{\mathbb{Z}}, 1_{\mathbb{Z}})$ auf $\mathbb{Z}$. Abstrakt wird das durch den Begriff des *Rings* erfasst.

Definition 125. *Eine Struktur* $(R, +, \cdot, 0, 1)$ *ist ein* kommutativer Ring mit Einselement, *wenn die folgenden* Ringaxiome *erf"ullt sind:*

- $(R, +, 0)$ *ist eine abelsche Gruppe (Addition);*
- $(R, \cdot, 1)$ *ist assoziativ, kommutativ mit neutralem Element* 1 *(Multiplikation);*
- *Es gilt das* Distributivgesetz

$$x \cdot (y + z) = x \cdot y + x \cdot z.$$

Die Kommutativit"at eines Rings bezieht sich auf die Kommutativit"at der Multiplikation des Rings. Das Einselement ist das neutrale Element der Multiplication. Wir werden uns in der Vorlesung auf kommutativer Ring mit Einselement beschr"anken und sprechen dann einfacher nur von einem "Ring".

Satz 126. *Die Struktur* $(\mathbb{Z}, +_{\mathbb{Z}}, \cdot_{\mathbb{Z}}, 0_{\mathbb{Z}}, 1_{\mathbb{Z}})$ *ist ein Ring.*

Beweis. Es gen"ugt, das Distributivgesetz zu zeigen. Seien $\overline{(a,b)}, \overline{(a',b')}, \overline{(a'',b'')} \in \mathbb{Z}$. Dann ist

$$\begin{aligned}
& \overline{(a,b)} \cdot_{\mathbb{Z}} (\overline{(a',b')} +_{\mathbb{Z}} \overline{(a'',b'')}) \\
= \; & \overline{(a,b)} \cdot_{\mathbb{Z}} \overline{(a'+a'', b'+b'')} \\
= \; & \overline{(a \cdot a' + a \cdot a'' + b \cdot b' + b \cdot b'', a \cdot b' + a \cdot b'' + b \cdot a' + b \cdot a'')} \\
= \; & \overline{(a \cdot a' + a \cdot a'' + b \cdot b' + b \cdot b'', a \cdot b' + a \cdot b'' + b \cdot a' + b \cdot a'')} \\
= \; & \overline{(a \cdot a' + b \cdot b' + a \cdot a'' + b \cdot b'', a \cdot b' + b \cdot a' + a \cdot b'' + b \cdot a'')} \\
= \; & \overline{(a \cdot a' + b \cdot b', a \cdot b' + b \cdot a')} +_{\mathbb{Z}} \overline{(a \cdot a'' + b \cdot b'', a \cdot b'' + b \cdot a'')} \\
= \; & \overline{(a,b)} \cdot_{\mathbb{Z}} \overline{(a',b')} +_{\mathbb{Z}} \overline{(a,b)} \cdot_{\mathbb{Z}} \overline{(a'',b'')}
\end{aligned}$$

□

In Ringen gelten viele von der "Buchstabenrechnung" bekannte Eigenschaften. Wir verwenden deswegen weitere "ubliche Schreibweisen:

- In einem Ring werden Addition und Multiplikation und die neutralen Elemente meistens einfach durch $+, \cdot, 0, 1$ bezeichnet;
- die Multiplikation bindet st"arker als die Addition, d.h. $x \cdot y + z$ steht f'ur $(x \cdot y) + z$ und nicht f'ur $x \cdot (y + z)$;
- das Multiplikationszeichen wird meistens als Leerstelle geschrieben: $x\,y$ steht f'ur $x \cdot y$;
- x^n steht f'ur $\underbrace{x \cdot \ldots \cdot x}_{n-\text{mal}}$; speziell $x^1 = x$, und man setzt $x^0 = 1$;
- 2 steht f'ur $1 + 1$, 3 steht f'ur $1 + 1 + 1$, usw.
- zu jedem Ringelement x existiert genau ein additives Inverses, das mit $-x$ bezeichnet wird;
- schreibe $x - y$ f'ur $x + (-y)$.

Satz 127. *Sei $(R, +, \cdot, 0, 1)$ ein Ring. Dann gilt darin:*

a) $0 \cdot x = 0$ *;*

b) $(-1) \cdot x = -x$ *;*

c) $-(-1) = 1$*;*

d) $(-1) \cdot (-1) = 1$ *.*

Beweis. *a)* Es gilt $0 \cdot x = (0 + 0) \cdot x = 0 \cdot x + 0 \cdot x$. Durch beidseitige Addition von $-(0 \cdot x)$ ergibt sich

$$0 = -(0 \cdot x) + 0 \cdot x = -(0 \cdot x) + 0 \cdot x + 0 \cdot x = 0 + 0 \cdot x = 0 \cdot x.$$

b) Wir zeigen, dass $(-1) \cdot x$ das eindeutige additive Inverse zu x ist:

$$(-1) \cdot x + x = (-1) \cdot x + 1 \cdot x = ((-1) + 1) \cdot x = 0 \cdot x = 0.$$

c) Das eindeutige additive Inverse zu -1 ist 1.

d) Aus *b)* und *c)* ergibt sich sofort:

$$(-1) \cdot (-1) = -(-1) = 1.$$ □

Das "mysteri"ose" *minus mal minus ist plus* folgt also aus den Rechengesetzen in einem Ring, ohne dass man mit "negativen Schulden" argumentieren muss.

Satz 128. (Binomische Formeln) *Sei $(R, +, \cdot, 0, 1)$ ein Ring. Dann gilt darin:*

a) $(x + y)^2 = x^2 + 2\,x\,y + y^2$*;*

b) $(x - y)^2 = x^2 - 2\,x\,y + y^2$

c) $(x + y)^3 = x^3 + 3\,x^2\,y + 3\,x\,y^2 + y^3$*;*

d) $(x + y)\,(x - y) = x^2 - y^2$.

Beweis. *a)*

$$\begin{aligned}(x+y)^2 &= (x+y)\,(x+y)\\ &= (x+y)\,x+(x+y)\,y\\ &= x\,(x+y)+y\,(x+y)\\ &= x\,x+x\,y+y\,x+y\,y\\ &= x^2+x\,y+x\,y+y^2\\ &= x^2+(x\,y\,1+x\,y\,1)+y^2\\ &= x^2+(x\,y\,(1+1))+y^2\\ &= x^2+x\,y\,2+y^2\\ &= x^2+2\,x\,y+y^2\end{aligned}$$

b − d) "Ubung. □

Wir wollen auch die multiplikative Struktur von $(\mathbb{N},+,\cdot,0,1)$ in die multiplikative Struktur von $(\mathbb{Z},+,\cdot,0,1)$ einbetten.

Definition 129. *Sei $\mathcal{S}$ eine Struktur mit Tr"agermenge S, Relationen $R_0,R_1,\ldots$, Operationen O_0, $O_1,\ldots$ und Konstanten $K_0,K_1,\ldots$. Analog sei $\mathcal{S}'$ eine Struktur mit Tr"agermenge S', Relationen $R'_0,R'_1,\ldots$, Operationen $O'_0,O'_1,\ldots$ und Konstanten $K'_0,K'_1,\ldots$.*

a) *Ein* Homomorphismus *von $\mathcal{S}$ nach $\mathcal{S}'$ ist eine Abbildung $f\colon S\to S'$, so dass f"ur alle $x_0,\ldots,x_{n-1}\in S$ gilt:*

- *$R_i(x_0,\ldots,x_{n-1})$ impliziert $R'_i(f(x_0),\ldots,f(x_{n-1}))$*
- *$f(O_i(x_0,\ldots,x_{n-1}))=O'_i(f(x_0),\ldots,f(x_{n-1}))$*
- *$f(K_i)=K'_i$*

b) *Eine* Einbettung *von $\mathcal{S}$ nach $\mathcal{S}'$ (oder von $\mathcal{S}$ in $\mathcal{S}'$) ist ein Homomorphismus von $\mathcal{S}$ nach $\mathcal{S}'$, der außerdem injektiv ist, und so dass f"ur alle $x_0,\ldots,x_{n-1}\in S$ gilt:*

- *$R_i(x_0,\ldots,x_{n-1})$ genau dann, wenn $R'_i(f(x_0),\ldots,f(x_{n-1}))$*

c) *Ein Isomorphismus von $\mathcal{S}$ nach $\mathcal{S}'$ ist eine Einbettung von $\mathcal{S}$ in $\mathcal{S}'$, die außerdem bijektiv ist.*

Satz 130. *Die Funktion $f\colon\mathbb{N}\to\mathbb{Z}$ mit*

$$f(n)=\overline{(n,0)}$$

ist eine Einbettung der Struktur $(\mathbb{N},+,\cdot,0,1)$ in den Ring $(\mathbb{Z},+_{\mathbb{Z}},\cdot_{\mathbb{Z}},0_{\mathbb{Z}},1_{\mathbb{Z}})$.

Beweis. Wir hatte bereits gezeigt, dass die Funktion f die Addition mit dem Nullelement erh"alt. F"ur die Multiplikation gilt:

$$f(m\cdot n)=\overline{(m\cdot n,0)}=\overline{(m,0)}\cdot_{\mathbb{Z}}\overline{(n,0)}=f(m)\cdot_{\mathbb{Z}}f(n)$$

und

$$f(1)=\overline{(1,0)}=1_{\mathbb{Z}}$$ □

17 Die rationalen Zahlen

In den ganzen Zahlen $\mathbb{Z}$ kann man addieren, subtrahieren und multiplizieren. Dividieren ist hingegen im allgemeinen nicht m"oglich. In $\mathbb{Z}$ existieren keine Zahlen, die dem gew"ohnlichen $\frac{1}{2},\frac{1}{3},\ldots$ entsprechen.

Lemma 131. *Seien $a, b \in \mathbb{Z}$ mit $a \cdot b = 1$. Dann ist entweder $a = b = 1$ oder $a = b = -1$.*

Beweis. Betrachte die Zahl $a = \overline{(a', a'')}$.

Fall 1. $a' < a''$. W"ahle $c \in \mathbb{N}$, so dass $a' + c = a'' = 0 + a''$. Dann ist $(a', a'') \sim_Z (0, c)$ und $a = \overline{(0, c)}$.

Fall 2. $a'' \leqslant a'$. W"ahle $c \in \mathbb{N}$, so dass $a' + 0 = a' = c + a''$. Dann ist $(a', a'') \sim_Z (c, 0)$ und $a = \overline{(c, 0)}$. Wir k"onnen daher annehmen, dass a und b *normierte* Darstellungen der Gestalt $\overline{(0, c)}$ oder $\overline{(c, 0)}$ besitzen.

Fall A. $a = \overline{(c, 0)}$ und $b = \overline{(d, 0)}$. Nach Voraussetzung ist

$$\overline{(c, 0)} \cdot \overline{(d, 0)} = \overline{(c\,d, 0)} = 1 = \overline{(1, 0)}.$$

Daher ist $c\,d + 0 = 1 + 0$ mit nat"urlichen Zahlen c und d. Daraus folgt $c = d = 1$ und

$$a = \overline{(1, 0)} = 1 \text{ und } a = \overline{(1, 0)} = 1.$$

Fall B. $a = \overline{(c, 0)}$ und $b = \overline{(0, d)}$. Nach Voraussetzung ist

$$\overline{(c, 0)} \cdot \overline{(0, d)} = \overline{(0, c\,d)} = 1 = \overline{(1, 0)}.$$

Dann ist $0 + 0 = 1 + c\,d$. Das aber ist ein Widerspruch, da 0 in den nat"urlichen Zahlen kein Nachfolger ist.

Fall C. $a = \overline{(0, c)}$ und $b = \overline{(d, 0)}$ f"uhrt ebenso zum Widerspruch wie Fall B.

Fall D. $a = \overline{(0, c)}$ und $b = \overline{(0, d)}$. Nach Voraussetzung ist

$$\overline{(0, c)} \cdot \overline{(0, d)} = \overline{(c\,d, 0)} = 1 = \overline{(1, 0)}.$$

Daher ist $c\,d + 0 = 1 + 0$ mit nat"urlichen Zahlen c und d. Daraus folgt $c = d = 1$ und

$$a = \overline{(0, 1)} = -1 \text{ und } a = \overline{(0, 1)} = -1. \qquad \square$$

In den ganzen Zahlen haben nur die Zahlen 1 und -1 multiplikative Inverse.

Wir wollen die Struktur $(\mathbb{Z}, +, \cdot, 0, 1)$ der ganzen Zahlen zur Struktur $(\mathbb{Q}, +, \cdot, 0, 1)$ der *rationalen Zahlen* erweitern. Die Konstruktion wird durch unser Vorwissen "uber die anschaulich bekannten rationalen Zahlen

$$..., -\frac{m}{n}, ..., -\frac{1}{3}, -\frac{1}{2}, -1, 0, 1, \frac{1}{2}, \frac{1}{3}, ..., \frac{m}{n}, ...$$

motiviert. Die rationale Zahl $\frac{2}{5}$ ist auf vielfache Weise *Quotient* von ganzen Zahlen:

$$\frac{2}{5} = \frac{4}{10} = \frac{6}{15} = \frac{-2}{-5} = \frac{-4}{-10} = ...$$

Die auftretenden Zahlenpaare $(2, 5), (4, 10), (6, 15), ...$ sind in Bezug darauf, die Zahl $\frac{2}{5}$ darzustellen, "aquivalent. Wir arbeiten im Folgenden mit geordneten Paaren ganzer Zahlen, die anschaulich als Quotienten oder Br"uche gesehen werden. Zwei Quotienten (a, b) und (a', b'), die f"ur $\frac{a}{b}$ und $\frac{a'}{b'}$ stehen sollen, stellen dieselbe Zahl dar oder sind "aquivalent, wenn

$$a \cdot b' = a' \cdot b$$

ist.

Da wir nicht durch 0 dividieren k"onnen, lassen wir keine Br"uche der Form $\frac{a}{0}$ zu.

Lemma 132. *Sei $Q = \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$. Definiere eine zweistellige Relation $\sim_Q$ auf Q durch*

$$(a,b) \sim_Q (a',b') \text{ gdw. } a \cdot b' = a' \cdot b.$$

Dann ist $\sim_Q$ eine "Aquivalenzrelation auf Q : f"ur alle $(a,b),(a',b'),(a'',b'') \in Q$ gilt:

a) (Reflexivit"at) $(a,b) \sim_Q (a,b)$

b) (Symmetrie) $(a,b) \sim_Q (a',b')$ impliziert $(a',b') \sim_Q (a,b)$

c) (Transitivit"at) $(a,b) \sim_Q (a',b')$ und $(a',b') \sim_Q (a'',b'')$ impliziert $(a,b) \sim_Q (a'',b'')$.

Beweis. *c)* Sei $(a,b) \sim_Q (a',b')$ und $(a',b') \sim_Q (a'',b'')$. Dann ist $a \cdot b' = a' \cdot b$ und $a' \cdot b'' = a'' \cdot b'$.
Fall 1: $a' = 0$. Dann ist $a \cdot b' = 0 \cdot b = 0$. Weil $b' \neq 0$ ist, ist $a = 0$. Ebenso ist $a'' \cdot b' = 0 \cdot b'' = 0$ und $a'' = 0$. Zusammen ist

$$a \cdot b'' = 0 = a'' \cdot b$$

und $(a,b) \sim_Q (a'',b'')$.
Fall 2: $a' \neq 0$. Multiplikation der beiden Gleichungen ergibt

$$a \cdot b' \cdot a' \cdot b'' = a' \cdot b \cdot a'' \cdot b'.$$

Da $a' \neq 0$ ist, l"asst sich die Gleichung durch a' "k"urzen" oder dividieren:

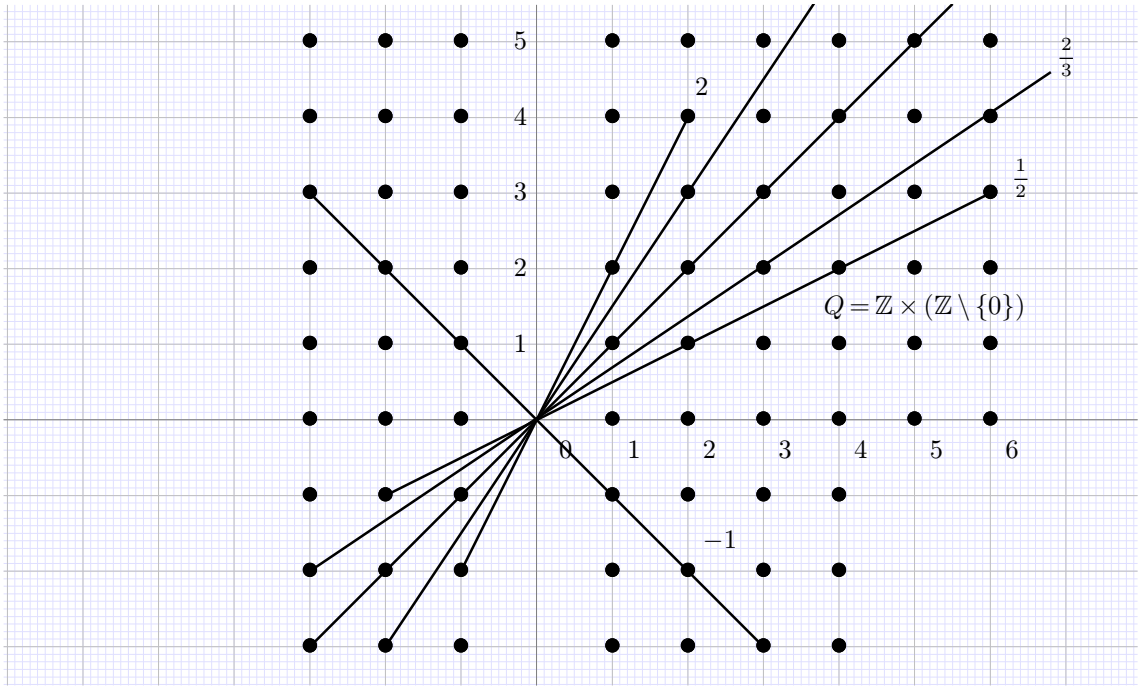
$$a \cdot b' \cdot b'' = b \cdot a'' \cdot b'.$$

Da $b' \neq 0$ ist, kann man weiter durch b' k"urzen:

$$a \cdot b'' = b \cdot a'' = a'' \cdot b.$$

Damit ist auch in diesem Fall $(a,b) \sim_Q (a'',b'')$. □

Hier ein Bild von Q; Punkte auf den Geraden durch den Ursprung sind bzgl. $\sim_Z$ zueinander "aquivalent, sie bilden die "Aquivalenzklassen modulo $\sim_Q$. Man beachte, dass die "Aquivalenzklassen entgegen dem Anschein paarweise disjunkt sind, weil $(0,0) \notin Q$ ist.



Lemma 133. *F"ur* $(a,b)\in Q$ *definiere die Menge*

$$\frac{a}{b}=\{(a',b')\in Q|\,(a',b')\sim_Q(a,b)\}.$$

$\frac{a}{b}$ *ist die* "Aquivalenzklasse *von* (a,b) *bez"uglich (oder "modulo") der "Aquivalenzrelation* $\sim_Q$*. Die "Aquivalenzklasse* $\frac{a}{b}$ *wird als* a (geteilt) durch b *bezeichnet. Derartige "Aquivalenzklassen nennt man auch einen* Bruch.

Dann gilt f"ur $(a,b),(a',b')\in Q$ *:*

a) $(a,b)\in\frac{a}{b}$.

b) $(a,b)\sim_Q(a',b')$ *gdw.* $\frac{a}{b}=\frac{a'}{b'}$.

c) $(a,b)\nsim_Q(a',b')$ *gdw.* $\frac{a}{b}\cap\frac{a'}{b'}=\emptyset$.

Beweis. "Ubung. □

Definition 134. *Die Menge* $\mathbb{Q}$ *der* rationalen Zahlen *ist die Menge aller "Aquivalenzklassen modulo* $\sim_Q$

$$\mathbb{Q}=\left\{\frac{a}{b}\,|\,(a,b)\in Q\right\}.$$

Wir haben die Br"uche abstrakt als "Aquivalenzklassen von Paaren ganzer Zahlen definiert. Das entspricht zun"achst nicht den "ublichen Anschauungen vom Dividieren oder Teilen auf einem Zahlenstrahl oder anderen geometrischen Operationen. Entsprechend den bekannten Regeln des Bruchrechnens erg"anzen wir die Menge $\mathbb{Q}$ zur *Struktur* der rationalen Zahlen.

Definition 135. *Definiere die Addition* $+_{\mathbb{Q}}\colon\mathbb{Q}\times\mathbb{Q}\to\mathbb{Q}$ *durch*

$$\frac{a}{b}+_{\mathbb{Q}}\frac{a'}{b'}=\frac{a\cdot b'+a'\cdot b}{b\cdot b'}.$$

Definiere ein neutrales Element f"ur die Addition durch

$$0_{\mathbb{Z}}=\frac{0}{1}.$$

Definiere die Multiplikation $\cdot_{\mathbb{Q}}\colon\mathbb{Q}\times\mathbb{Q}\to\mathbb{Q}$ *durch*

$$\frac{a}{b}\cdot_{\mathbb{Q}}\frac{a'}{b'}=\frac{a\cdot a'}{b\cdot b'}.$$

Definiere ein neutrales Element f"ur die Multiplikation durch

$$1_{\mathbb{Q}}=\frac{1}{1}.$$

Lemma 136. *Die Struktur* $\mathbb{Q}=(\mathbb{Q},+_{\mathbb{Q}},\cdot_{\mathbb{Q}},0_{\mathbb{Q}},1_{\mathbb{Q}})$ *ist wohldefiniert, d.h. die Operation* $+_{\mathbb{Q}}$ *und* $\cdot_{\mathbb{Q}}$ *sind wohldefiniert. Die Struktur* $\mathbb{Q}$ *ist ein Ring.*

Beweis. "Ubung. □

Wir haben $\mathbb{Q}$ eingef"uhrt, um dividieren zu k"onnen, d.h. um multiplikative Inverse bilden zu k"onnen. Dies ist f"ur alle rationalen Zahlen außer $0_{\mathbb{Q}}$ m"oglich.

Satz 137. $\mathbb{Q}^* = \mathbb{Q} \setminus \{0_\mathbb{Q}\}$ *ist eine abelsche Gruppe mit der Gruppenoperation* $\cdot_\mathbb{Q}$ *und dem neutralen Element* $1_\mathbb{Q}$.

Beweis. Zun"achst ist zu zeigen, dass $\cdot_\mathbb{Q}$ auch eine Operation auf der eingeschr"ankten Menge $\mathbb{Q}^*$ ist, d.h. dass $\mathbb{Q}^*$ gegen"uber $\cdot_\mathbb{Q}$ abgeschlossen ist.

(1) Seien $\frac{a}{b}, \frac{a'}{b'} \in \mathbb{Q}^*$. Dann ist $\frac{a}{b} \cdot_\mathbb{Q} \frac{a'}{b'} \in \mathbb{Q}^*$.

Beweis. Angenommen, $\frac{a}{b} \cdot_\mathbb{Q} \frac{a'}{b'} = 0_\mathbb{Q}$. Dann ist $\frac{a \cdot a'}{b \cdot b'} = \frac{0}{1}$ und $a \cdot a' = a \cdot a' \cdot 1 = 0 \cdot b \cdot b' = 0$. Da $\frac{a}{b}$, $\frac{a'}{b'} \neq \frac{0}{1}$, ist $a, a' \neq 0$. Aber dann ist $a \cdot a' \neq 0$. Widerspruch. *qed*

Wir "uberpr"ufen nun die Gruppenaxiome. Seien $\frac{a}{b}, \frac{a'}{b'}, \frac{a''}{b''} \in \mathbb{Q} \setminus \{0_\mathbb{Q}\}$. Dann gilt:

Assoziativit"at:

$$\left(\frac{a}{b} \cdot_\mathbb{Q} \frac{a'}{b'}\right) \cdot_\mathbb{Q} \frac{a''}{b''} = \frac{a \cdot a'}{b \cdot b'} \cdot_\mathbb{Q} \frac{a''}{b''} = \frac{(a \cdot a') \cdot a''}{(b \cdot b') \cdot b''} = \frac{a \cdot (a' \cdot a'')}{b \cdot (b' \cdot b'')} = \frac{a}{b} \cdot_\mathbb{Q} \frac{a' \cdot a''}{b' \cdot b''} = \frac{a}{b} \cdot_\mathbb{Q} \left(\frac{a'}{b'} \cdot_\mathbb{Q} \frac{a''}{b''}\right).$$

Kommutativit"at:

$$\frac{a}{b} \cdot_\mathbb{Q} \frac{a'}{b'} = \frac{a \cdot a'}{b \cdot b'} = \frac{a' \cdot a}{b' \cdot b} = \frac{a'}{b'} \cdot_\mathbb{Q} \frac{a}{b}.$$

Neutralit"at:

$$\frac{1}{1} \cdot_\mathbb{Q} \frac{a}{b} = \frac{1 \cdot a}{1 \cdot b} = \frac{a}{b}.$$

Existenz *inverser* Elemente: da $\frac{a}{b} \neq 0_\mathbb{Q} = \frac{0}{1}$ ist, gilt $a = a \cdot 1 \neq 0 \cdot b = 0$. Damit ist $(b, a) \in Q$ und $\frac{b}{a} \in \mathbb{Q}$. Wir zeigen, dass $\frac{b}{a}$ invers zu $\frac{a}{b}$ ist:

$$\frac{b}{a} \cdot_\mathbb{Q} \frac{a}{b} = \frac{b \cdot a}{a \cdot b} = \frac{a \cdot b}{a \cdot b} = \frac{1}{1} = 1_\mathbb{Q}. \qquad \square$$

Definiere f"ur $\frac{a}{b}, \frac{a'}{b'}$ den Quotienten

$$\frac{\frac{a}{b}}{\frac{a'}{b'}} = \frac{a\,b'}{a'\,b}$$

Dann ist

$$\frac{\frac{a}{b}}{\frac{a'}{b'}} \frac{a'}{b'} = \frac{a\,b'\,a'}{a'\,b\,b'} = \frac{a}{b}$$

So wie $\mathbb{Z}$ ein Erweiterung von $\mathbb{N}$ war, so l"asst sich $\mathbb{Z}$ in $\mathbb{Q}$ einbetten.

Satz 138. *Der Ring* $(\mathbb{Z}, +, \cdot, 0, 1)$ *l"asst sich durch die Funktion* $f: \mathbb{Z} \to \mathbb{Q}$,

$$f(a) = \frac{a}{1}$$

"kanonisch" in den Ring $(\mathbb{Q}, +_\mathbb{Q}, \cdot_\mathbb{Q}, 0_\mathbb{Q}, 1_\mathbb{Q})$ einbetten.

Beweis. Offensichtlich gilt

(1) $f: \mathbb{Z} \to \mathbb{Q}$ ist injektiv.

Seien $a, a' \in \mathbb{Z}$. Dann ist

$$f(a + a') = \frac{a + a'}{1} = \frac{a}{1} +_\mathbb{Q} \frac{a'}{1} = f(a) +_\mathbb{Q} f(a')$$

und

$$f(a\cdot a')=\frac{a\cdot a'}{1}=\frac{a}{1}\cdot_{\mathbb{Q}}\frac{a'}{1}=f(a)\cdot_{\mathbb{Q}}f(a').$$

Ferner ist $f(0)=\frac{0}{1}=0_{\mathbb{Q}}$ und $f(1)=\frac{1}{1}=1_{\mathbb{Q}}$. □

Also verhalten sich die Elemente $a\in\mathbb{Z}$ innerhalb von $\mathbb{Z}$ genauso wie die entsprechenden Elemente $f(a)$ innerhalb von $\mathbb{Q}$. Wir k"onnen daher jedes $a\in\mathbb{Z}$ mit $f(a)\in\mathbb{Q}$ identifizieren. Damit ist $\mathbb{Z}\subseteq\mathbb{Q}$ und die identische Funktion $\mathrm{id}_{\mathbb{Z}}\colon\mathbb{Z}\to\mathbb{Q}$ ist eine Einbettung von $(\mathbb{Z},+,\cdot,0,1)$ in $(\mathbb{Q},+.\cdot,0,1)$. In diesem Fall sagt man auch, dass $(\mathbb{Z},+,\cdot,0,1)$ eine *Substruktur* von $(\mathbb{Q},+.\cdot,0,1)$ ist, oder dass $(\mathbb{Q},+.\cdot,0,1)$ eine *Erweiterung* von $(\mathbb{Z},+,\cdot,0,1)$ ist.

Das eindeutige additive Inverse von $q\in\mathbb{Q}$ wird mit $-q$ bezeichnet. Schreibe $p-q$ f"ur die Differenz $p+(-q)$.

Das eindeutige multiplikative Inverse von $q\in\mathbb{Q}\setminus\{0\}$ wird mit q^{-1} bezeichnet. Schreibe $\frac{p}{q}$ f"ur den Quotienten $p\cdot(q^{-1})$.

Satz 139. *$\mathbb{Q}=(\mathbb{Q},\leqslant,+,\cdot,0,1)$ ist eine Erweiterung von $\mathbb{Z}=(\mathbb{Z},\leqslant,+,\cdot,0,1)$, die von $\mathbb{Q}$ folgendermaßen erzeugt wird: f"ur jedes $q\in\mathbb{Q}$ gibt es $a\in\mathbb{Z}$ und $b\in\mathbb{Z}\setminus\{0\}$, so dass*

$$q=\frac{a}{b}.$$

Beweis. Nach Konstruktion von $\mathbb{Q}$ gibt es $a\in\mathbb{Z}$ und $b\in\mathbb{Z}\setminus\{0\}$, so dass

$$q=\{(a',b')\in Q|\,(a',b')\sim_Q(a,b)\}.$$

Diese "Aquivalenzklasse hatten wir in der Konstruktion bereits mit $\frac{a}{b}$ bezeichnet. Vor"ubergehend wollen wir sie hier mit $\left[\frac{a}{b}\right]$ bezeichnen. Dann gilt nach Konstruktion von $\mathbb{Q}$ und wegen der Einbettung $\mathbb{Z}\subseteq\mathbb{Q}$:

$$q=\left[\frac{a}{b}\right]=\left[\frac{a}{1}\right]\cdot\left[\frac{1}{b}\right]=\left[\frac{a}{1}\right]\cdot\left(\left[\frac{b}{1}\right]^{-1}\right)=a\cdot(b^{-1})=\frac{a}{b},$$

wobei rechts der neu eingef"uhrte Quotient von a und b steht. □

Definition 140. *Ein* K"orper *ist ein Ring $(K,+,\cdot,0,1)$, bei dem $(K\setminus\{0\},\cdot,1)$ eine abelsche Gruppe ist.*

Satz 141. *$(\mathbb{Q},+.\cdot,0,1)$ ein K"orper.*

Definition 142. *Definiere eine Relation $\leqslant_{\mathbb{Z}}$ auf $\mathbb{Z}$ durch*

$$a-b\leqslant a'-b'\,\text{gdw.}\,a+b'\leqslant a'+b.$$

Dies ist eine lineare Ordnung auf $\mathbb{Z}$.

Definition 143. *Ein* geordneter Ring *ist ein kommutativer Ring mit Einselement und mit einer linearen Ordnung $\leqslant$, so dass f"ur alle $a,b,c\in R$ gilt*

a) $a\leqslant b$ impliziert $a+c\leqslant b+c$;

b) wenn $0\leqslant a$ und $0\leqslant b$, dann ist $0\leqslant a\,b$.

Es gilt dann

Lemma 144. $(\mathbb{Z}, +, \cdot, \leqslant, 0, 1)$ *ist ein geordneter Ring.*

Definition 145. *Definiere Ordnung* $\leqslant_{\mathbb{Q}}$ *auf* $\mathbb{Q}$ *durch*

$$\frac{a}{b} \leqslant_{\mathbb{Q}} \frac{a'}{b'} \text{ gdw. } a\,b' \leqslant a'\,b.$$

Definition 146. *Ein* geordneter K"orper *ist ein geordneter Ring, der außerdem in K"orper ist.*

Lemma 147. $(\mathbb{Q}, +, \cdot, \leqslant, 0, 1)$ *ist ein geordneter K"orper.*

18 Die Unvollst"andigkeit von $\mathbb{Q}$

F"ur geordnete K"orper lassen sich Begriffe aus der Analysis definieren.

Definition 148. *Sei* $K = (K, \leqslant, +, \cdot, 0, 1)$ *ein geordneter K"orper. F"ur* $x \in K$ *definiere den* Absolutbetrag *von* x *als*

$$|x| = \begin{cases} x, \text{ falls } x \geqslant 0 \\ -x, \text{ sonst} \end{cases}$$

Lemma 149. *Der Absolutbetrag in* $K = (K, \leqslant, +, \cdot, 0, 1)$ *erf"ullt die Axiome einer* Norm*:*

a) $|x| = 0$ *gdw.* $x = 0$ *;*

b) (Dreiecksungleichung) $|x + y| \leqslant |x| + |y|$ *;*

c) (Multiplikativit"at) $|x \cdot y| = |x| \cdot |y|$ *.*

Definition 150. *Betrachte eine Funktion* $f\colon \mathbb{Q} \to \mathbb{Q}$ *.* f *heißt* stetig *in* $q \in \mathbb{Q}$*, falls*

$$\forall \varepsilon((\varepsilon \in \mathbb{Q} \wedge \varepsilon > 0) \to \exists \delta((\delta \in \mathbb{Q} \wedge \delta > 0) \wedge \forall x((x \in \mathbb{Q} \wedge |x - q| < \delta) \to |f(x) - f(q)| < \varepsilon))).$$

Da alle Variablen "uber $\mathbb{Q}$ *laufen, notieren wir die Einschr"ankungen auf* $\mathbb{Q}$ *nicht explizit und schreiben stattdessen*

$$\forall \varepsilon(\varepsilon > 0 \to \exists \delta(\delta > 0 \wedge \forall x(|x - q| < \delta \to |f(x) - f(q)| < \varepsilon)))$$

Weiter vereinfachend werden die Forderungen $\varepsilon > 0$ *und* $\delta > 0$ *direkt an die Quantoren geschrieben:*

$$\forall \varepsilon > 0 \exists \delta > 0 \forall x\,(|x - q| < \delta \to |f(x) - f(q)| < \varepsilon).$$

Die Funktion $f\colon \mathbb{Q} \to \mathbb{Q}$ *ist* stetig *(auf* $\mathbb{Q}$*), wenn* f *in jedem* $q \in \mathbb{Q}$ *stetig ist.*

Man kann nun zeigen:

Lemma 151.

a) F"ur $d \in \mathbb{Q}$ *ist die konstante Funktion* $\text{const}_d\colon \mathbb{Q} \to \mathbb{Q}$ *,* $\text{const}_d(x) = d$ *stetig.*

b) *Die identische Funktion* $\mathrm{id}_{\mathbb{Q}}\colon \mathbb{Q}\to\mathbb{Q}$, $\mathrm{id}_{\mathbb{Q}}(x)=x$ *ist stetig.*

c) *Die Quadratfunktion* $\mathrm{sq}\colon \mathbb{Q}\to\mathbb{Q}$, $\mathrm{sq}(x)=x^2$ *ist stetig.*

d) *Die Funktion* $f\colon \mathbb{Q}\to\mathbb{Q}$,

$$f(x)=\begin{cases} x^{-1}, \text{ falls } x\neq 0 \\ a\,, \text{ sonst} \end{cases}$$

mit beliebigem $a\in\mathbb{Q}$ *ist stetig in allen* $q\in\mathbb{Q}\setminus\{0\}$ *und nicht stetig in* $q=0$.

e) *Die Betragsfunktion* $|.|\colon \mathbb{Q}\to\mathbb{Q}$, $x\mapsto|x|$ *ist stetig.*

In der Analysis gilt der *Zwischenwertsatz*:

> Sei f eine stetige Funktion. Sei $a<b$ und $f(a)<f(b)$. F"ur alle s mit $f(a)<s<f(b)$ existiert dann ein x mit $a<x<b$ und
>
> $$f(x)=s\,.$$

Der Zwischenwertsatz gilt *nicht* f"ur stetige Funktionen auf $\mathbb{Q}$:

Lemma 152. *Es gibt eine stetige Funktion* $f\colon \mathbb{Q}\to\mathbb{Q}$ *mit* $f(0)=0$ *und* $f(2)=4$, *aber es gibt kein* x *mit* $0<x<2$ *und* $f(x)=2$.

Beweis. Sei f die Quadratfunktion $f(x)=x^2$. Wegen der Irrationalit"at von $\sqrt{2}$ gibt es kein $x\in\mathbb{Q}$ mit $f(x)=2$. □

Die gew"unschte Zahl $\sqrt{2}$ l"asst sich dennoch durch rationale Zahlen approximieren:

$1<\sqrt{2}<2$, denn $1^2=1<2<4=2^2$

$1,4<\sqrt{2}<1,5$, denn $\left(\frac{14}{10}\right)^2=\frac{196}{100}<2<\frac{225}{100}=\left(\frac{15}{10}\right)^2$

$1,41<\sqrt{2}<1,42$, denn $\left(\frac{141}{100}\right)^2=\frac{19881}{10000}<2<\frac{20164}{10000}=\left(\frac{142}{100}\right)^2$

$1,414<\sqrt{2}<1,415$, denn $\left(\frac{1414}{1000}\right)^2=\frac{1999396}{1000000}<2<\frac{2002225}{1000000}=\left(\frac{1415}{1000}\right)^2$

...

Die Folgen $1, \frac{14}{10}, \frac{141}{100}, \frac{1414}{1000}, \ldots$ und $2, \frac{15}{10}, \frac{142}{100}, \frac{1415}{1000}, \ldots$ scheinen gegen die Zahl $\sqrt{2}$ zu streben. Diese Folgen lassen sich ohne Bezug auf $\sqrt{2}$ definieren. Die linke Folge besteht z.B. aus allen Quotienten der Form

$$\frac{a}{10^n}$$

mit der Eigenschaft $a\in\mathbb{Z}$ und

$$\left(\frac{a}{10^n}\right)^2<2<\left(\frac{a+1}{10^n}\right)^2.$$

Dies legt nahe, die L"ucken der rationalen Zahlen dadurch zu f"ullen, dass man weitere Zahlen mit Hilfe von Folgen rationaler Zahlen definiert.

Definition 153. *Eine* Folge *ist eine Funktion* a *mit Definitionsbereich* $\mathrm{def}(a)=\mathbb{N}$. *Die Folge l"asst sich anschaulich als unendliches Tupel* $(a(0),a(1),\ldots)$ *notieren. Oft schreibt man die Argumente auch als Indizes:* $(a_0,a_1,\ldots)$ *und l"asst auch die Klammern fort:* $a_0,a_1,\ldots$. a *ist eine* Folge rationaler Zahlen*, wenn* $a\colon \mathbb{N}\to\mathbb{Q}$.

Die Folge $1, \frac{14}{10}, \frac{141}{100}, \frac{1414}{1000}, \ldots$ scheint sich bei zunehmenden Indizes immer mehr zusammenzuziehen. Sie "fokussiert auf einen virtuellen Punkt im Unendlichen". Das wird durch die folgende Definition erfasst:

Definition 154. *Eine Folge $a_0, a_1, \ldots$ rationaler Zahlen ist eine* Cauchy-Folge*, wenn*

$$\forall \varepsilon > 0 \exists n_0 \in \mathbb{N} \forall m, n \in \mathbb{N} \, (m \geqslant n_0 \wedge n \geqslant n_0 \to |a_m - a_n| < \varepsilon).$$

Auch hier wird gerne abgek"urzt

$$\forall \varepsilon > 0 \exists n_0 \forall m, n \geqslant n_0 \, |a_m - a_n| < \varepsilon \, .$$

Die Folge $1, \frac{14}{10}, \frac{141}{100}, \frac{1414}{1000}, \ldots$ ist eine Cauchy-Folge. Auch die Folge $2, \frac{15}{10}, \frac{142}{100}, \frac{1415}{1000}, \ldots$ strebt gegen $\sqrt{2}$, weshalb man beide Folgen als "aquivalent ansehen will. Wir sind in der inzwischen vertrauten Situation: zur Konstruktion eines neuen Zahlbereichs wird aus bereits vorhandenen Zahlen eine Menge gebildet. Die neuen Zahlen sind "Aquivalenzklassen einer "Aquivalenzrelation.

Lemma 155. *Sei*

$$R = \{a | \, a \text{ ist eine Cauchy-Folge}\}.$$

Definiere eine zweistellige Relation $\sim_R$ auf R durch

$$a \sim_R b \text{ gdw. } \forall \varepsilon \exists n_0 \forall n \geqslant n_0 \, |a_n - b_n| < \varepsilon \, .$$

Dann ist $\sim_R$ eine "Aquivalenzrelation auf R.

Beweis. "Ubung. □

Definition 156. *F"ur $a \in R$ sei $\tilde{a} = \{b | \, b \sim_R a\}$ die "Aquivalenzklasse von a bezgl. $\sim_R$. Die Menge $\mathbb{R}$ der* reellen Zahlen *ist die Menge aller "Aquivalenzklassen modulo $\sim_R$*

$$\mathbb{R} = \{\tilde{a} \, | \, a \in R\}.$$

Wir erg"anzen $\mathbb{R}$ zum geordneten K"orper der reellen Zahlen, indem wir die rationalen Relationen und Operationen an jedem Index von Cauchy-Folgen durchf"uhren.

Definition 157. *Definiere die Addition $+_{\mathbb{R}} \colon \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ durch*

$$\tilde{a} +_{\mathbb{R}} \tilde{b} = \tilde{c}$$

wobei $c \colon \mathbb{N} \to \mathbb{Q}$ durch $c_n = a_n + b_n$ definiert ist.

Definiere ein neutrales Element $0_{\mathbb{R}} = \tilde{c}$ f"ur die Addition, wobei $c \colon \mathbb{N} \to \mathbb{Q}$ durch $c_n = 0$ definiert ist.

Definiere die Multiplikation $\cdot_{\mathbb{R}} \colon \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ durch

$$\tilde{a} \cdot_{\mathbb{R}} \tilde{b} = \tilde{c}$$

wobei $c \colon \mathbb{N} \to \mathbb{Q}$ durch $c_n = a_n \cdot b_n$ definiert ist.

Definiere ein neutrales Element $1_{\mathbb{R}} = \tilde{d}$ f"ur die Addition, wobei $d \colon \mathbb{N} \to \mathbb{Q}$ durch $d_n = 1$ definiert ist.

Definiere eine zweistellige Relation $\leqslant_{\mathbb{R}}$ auf $\mathbb{R}$ durch

$$\tilde{a} \leqslant_{\mathbb{R}} \tilde{b} \text{ gdw. } \exists n_0 \forall n \geqslant n_0 \, a_n \leqslant b_n \, .$$

Lemma 158. *Die Struktur* $\mathbb{R} = (\mathbb{R}, \leqslant_{\mathbb{R}}, +_{\mathbb{R}}, \cdot_{\mathbb{R}}, 0_{\mathbb{R}}, 1_{\mathbb{R}})$ *ist wohldefiniert.*

Satz 159. *Die Struktur* $\mathbb{R} = (\mathbb{R}, \leqslant_{\mathbb{R}}, +_{\mathbb{R}}, \cdot_{\mathbb{R}}, 0_{\mathbb{R}}, 1_{\mathbb{R}})$ *ist ein geordneter K"orper. Definiere die Abbildung* $f\colon \mathbb{Q} \to \mathbb{R}$ *durch* $f(q) = \tilde{c}$ *, wobei* $c\colon \mathbb{N} \to \mathbb{Q}$ *und* $c_n = q$ *ist. Dann ist* $f\colon \mathbb{Q} \to \mathbb{R}$ *eine Einbettung der Struktur* $\mathbb{Q} = (\mathbb{Q}, \leqslant_{\mathbb{Q}}, +_{\mathbb{Q}}, \cdot_{\mathbb{Q}}, 0_{\mathbb{Q}}, 1_{\mathbb{Q}})$ *in* $\mathbb{R} = (\mathbb{R}, \leqslant_{\mathbb{R}}, +_{\mathbb{R}}, \cdot_{\mathbb{R}}, 0_{\mathbb{R}}, 1_{\mathbb{R}})$.

Beweis. "Ubung. □

Aufgrund dieses Satzes kann man wiederum $q \in \mathbb{Q}$ mit seinem Bild $f(q) \in \mathbb{R}$ identifizieren. Mit dieser Identifizierung ist der geordnete Ring $\mathbb{Q}$ eine Substruktur des geordneten K"orpers $\mathbb{R}$. Außerdem kann man vereinfachend $\mathbb{R} = (\mathbb{R}, \leqslant, +, \cdot, 0, 1)$ anstelle von $\mathbb{R} = (\mathbb{R}, \leqslant_{\mathbb{R}}, +_{\mathbb{R}}, \cdot_{\mathbb{R}}, 0_{\mathbb{R}}, 1_{\mathbb{R}})$ schreiben.

Wir hatten die Konstruktion der reellen Zahlen mit dem Wunsch nach dem Zwischenwertsatz motiviert. Tats"achlich gilt nun:

Satz 160. *Sei* $f\colon \mathbb{R} \to \mathbb{R}$ *eine stetige Funktion. Sei* $a < b$ *und* $f(a) < f(b)$*. F"ur alle* s *mit* $f(a) < s < f(b)$ *existiert dann ein* c *mit* $a < c < b$ *und*

$$f(c) = s\,.$$

Beweis. Es gen"ugt, den Satz f'ur $a = 0$ und $b = 1$ zu zeigen: die Funktion $h\colon \mathbb{R} \to \mathbb{R}$, $h(x) = a + (b-a)\,x$ bildet das Intervall $[0,1]$ ordnungstreu auf $[a,b]$ ab. Die Abbildung $f^* = f \circ h$ ist stetig mit $f^*(0) = (f \circ h)(0) = f(a) < f(b) = (f \circ h)(1) = f^*(1)$. Wenn $0 < d < 1$ mit $f^*(d) = s$, so gilt f'ur $c = h(d)$:

$$a = h(0) < h(d) = c < h(1) = b \text{ und } f(c) = f(h(d)) = f^*(d) = s\,.$$

Wir k"onnen als $a = 0$ und $b = 1$ annehmen.

Definiere eine Folge $c_* = c_0, c_1, \ldots$ durch

$$c_n = \frac{k_n}{2^n},$$

wobei k_n das maximale $k \in \mathbb{N}$ ist, so dass

$$\forall x \left(0 \leqslant x \leqslant \frac{k}{2^n} \to f(x) < s \right).$$

Die Folge ist wohldefiniert.

(1) $c_0, c_1, \ldots$ ist eine Cauchy-Folge.

Beweis. Sei $\varepsilon > 0$. W"ahle $n_0 \in \mathbb{N}$ mit $\frac{1}{2^{n_0}} < \varepsilon$. Seien $m, n \geqslant n_0$. Ohne Einschr"ankung sei $n < m$. Nach Definition der Folge c ist dann

$$\frac{k_n}{2^n} \leqslant \frac{k_m}{2^m} < \frac{k_n + 1}{2^n}.$$

Damit ist

$$|c_m - c_n| = \left| \frac{k_m}{2^m} - \frac{k_n}{2^n} \right| < \frac{1}{2^n} \leqslant \frac{1}{2^{n_0}} < \varepsilon$$

qed(1)

Sei $c = \tilde{c_*} \in \mathbb{R}$. Nach Konstruktion ist $a \leqslant c \leqslant b$.

(2) $f(c) = s$.

Beweis. Angenommen $f(c) \neq s$.

Fall 1. $f(c) > s$. Wegen der Stetigkeit von f gibt es dann ein Intervall der Form $\left[\frac{k}{2^n}, \frac{k+1}{2^n}\right]$, so dass

$$\frac{k}{2^n} < c < \frac{k+1}{2^n} \text{ und } \forall x \in \left[\frac{k}{2^n}, \frac{k+1}{2^n}\right] f(x) > s.$$

Nach Konstruktion gilt dann f'ur $m \geqslant n$ $c_m \leqslant \frac{k}{2^n} < c$. Nach Definition der Ordnung auf $\mathbb{R}$ ist dann

$$c \leqslant \frac{k}{2^n} < c.$$

Widerspruch.

Fall 2. $f(c) < s$. Wegen der Stetigkeit von f gibt es dann ein Intervall der Form $\left[\frac{k}{2^n}, \frac{k+1}{2^n}\right]$, so dass

$$\frac{k}{2^n} < c < \frac{k+1}{2^n} \text{ und } \forall x \in \left[\frac{k}{2^n}, \frac{k+1}{2^n}\right] f(x) < s.$$

Nach Konstruktion gilt dann f'ur $m \geqslant n$ $c_m \notin \left[\frac{k}{2^n}, \frac{k+1}{2^n}\right]$. Nach Definition der Ordnung auf $\mathbb{R}$ ist dann

$$c \leqslant \frac{k}{2^n} \text{ oder } \frac{k+1}{2^n} \leqslant c.$$

Widerspruch.

Beide F"alle f'uhren zum Widerspruch. Also ist $f(c) = s$. *qed*(2).

Offensichtlich ist $0 < c < 1$. □

19 Der Polynomring $K[X]$.

Sei $K = (K, \leqslant, +, \cdot, 0, 1)$ ein fester geordneter K"orper.

Definition 161. *F"ur eine Funktion* $p\colon \mathbb{N} \to K$ *sei*

$$\mathrm{tr}(p) = \{i \in \mathbb{N} \mid p(i) \neq 0\}$$

der Tr"ager *von* π. *Ein* Polynom *"uber* K *ist eine Funktion* $p\colon \mathbb{N} \to K$, *deren Tr"ager endlich ist. Das Polynom* p *wird auch durch*

$$p = p_n X^n + p_{n-1} X^{n-1} + \cdots + p_0$$

oder

$$p = \sum_{i=0}^{n} p_i X^i$$

bezeichnet, wobei $n = \max(\mathrm{tr}(p))$ *ist und* p_i *f"ur* $p(i)$ *steht; wir vereinbaren, dass* $\max(\emptyset) = 0$ *ist. Die Zahlen* p_i *sind die* Koeffizienten *des Polynoms* p, *die Zahl* n *ist der* Grad *des Polynoms* p, *der auch mit* $\mathrm{grad}(p)$ *bezeichnet wird. Das Symbol* X *in diesen Schreibweisen ist die* Variable *oder* Unbestimmte *des Polynoms.*

F"ur $a \in K$ *ist*

$$p(a) = p_n a^n + p_{n-1} a^{n-1} + \cdots + p_0$$

der Wert *von* p *an der Stelle* a. *Wenn* $p(a) = 0$ *ist, so heißt* a *eine* Nullstelle *von* p.

Man kann mit Polynomen “ahnlich wie mit Zahlen rechnen. Das Symbol X wird dabei wie eine “unbestimmte Zahl” im Sinne einer “Bachstabenrechnung” behandelt

Satz 162. *Sei $K[X]$ die Menge aller Polynome “uber K in der Variablen X. $K[X]$ wird zu einem kommutativen Ring mit Einselement erweitert:*

Definiere die Addition $+_{K[X]}\colon K[X]\times K[X]\to K[X]$ durch

$$p +_{K[X]} q = r,$$

wobei das Polynom $r\colon \mathbb{N}\to K$ durch $r_i = p_i + q_i$ definiert ist.

Definiere ein neutrales Element $0_{K[X]} = 0$, wobei alle Koeffizienten des Polynoms auf der rechten Seite $=0$ sind (“verschwinden”).

Definiere die Multiplikation $\cdot_{K[X]}\colon K[X]\times K[X]\to K[X]$ durch

$$p \cdot_{K[X]} q = r,$$

wobei das Polynom $r\colon \mathbb{N}\to K$ durch $r_i = p_0\, q_i + p_1\, q_{i-1} + \cdots + p_i\, q_0$ definiert ist.

Definiere ein neutrales Element $1_{K[X]} = 1$, wobei der 0-te Koeffizient des Polynoms auf der rechten Seite $=0$ ist, w”ahrend alle weitere Koeffizienten verschwinden.

Dann ist

$$K[X] = (K[X], +_{K[X]}, \cdot_{K[X]}, 0_{K[X]}, 1_{K[X]})$$

ein kommutativer Ring mit Einselement.

Beweis. Am kompliziertesten ist der Nachweis der Ringaxiome f”ur die Multiplikation. Wir zeigen nur die Assoziativit”at und Distributivit”at.

Seien $p, q, r \in K[X]$. Sei $n\in\mathbb{N}$. Dann ist

$$\begin{aligned}
((p\cdot_{K[X]} q)\cdot_{K[X]} r)_n &= \sum_{m+k=n} (p\cdot_{K[X]} q)_m \cdot r_k \\
&= \sum_{m+k=n} \left(\sum_{i+j=m} p_i \cdot q_j \right) \cdot r_k \\
&= \sum_{m+k=n} \left(\sum_{i+j=m} p_i \cdot q_j \cdot r_k \right) \\
&= \sum_{i+j+k=n} p_i \cdot q_j \cdot r_k
\end{aligned}$$

und ebenso

$$\begin{aligned}
(p\cdot_{K[X]} (q\cdot_{K[X]} r))_n &= \sum_{i+m=n} p_i \cdot (q\cdot_{K[X]} r)_m \\
&= \sum_{i+m=n} p_i \cdot \left(\sum_{j+k=m} p_j \cdot q_k \right) \\
&= \sum_{i+m=n} \left(\sum_{j+k=m} p_i \cdot q_j \cdot r_k \right) \\
&= \sum_{i+j+k=n} p_i \cdot q_j \cdot r_k
\end{aligned}$$

Also ist

$$(p\cdot_{K[X]} q)\cdot_{K[X]} r = p\cdot_{K[X]} (q\cdot_{K[X]} r).$$

F"ur die Distributivit"at gilt:

$$\begin{aligned}(p \cdot_{K[X]} (q +_{K[X]} r))_n &= \sum_{i+m=n} p_i \cdot (q +_{K[X]} r)_m \\ &= \sum_{i+m=n} p_i \cdot (q_m + r_m) \\ &= \left(\sum_{i+m=n} p_i \cdot q_m\right) + \left(\sum_{i+m=n} p_i \cdot r_m\right) \\ &= (p \cdot_{K[X]} q)_n + (p \cdot_{K[X]} r)_n \\ &= ((p \cdot_{K[X]} q) + (p \cdot_{K[X]} r))_n\end{aligned}$$

Also ist

$$p \cdot_{K[X]} (q +_{K[X]} r) = (p \cdot_{K[X]} q) + (p \cdot_{K[X]} r). \qquad \square$$

Satz 163. *Definiere die Abbildung $f\colon K \to K[X]$ durch $f(a) = a$, wobei der 0-te Koeffizient des Polynoms auf der rechten Seite $=a$ ist, w"ahrend alle weitere Koeffizienten verschwinden. Dann ist f eine Einbettung des Rings $K = (K, \leqslant, +, \cdot, 0, 1)$ in den Ring $K[X] = (K[X], +_{K[X]}, \cdot_{K[X]}, 0_{K[X]}, 1_{K[X]})$.*

Beweis. "Ubung. $\square$

Aufgrund dieses Satzes kann man wiederum $a \in K$ mit seinem Bild $f(a) \in K[X]$ identifizieren. Mit dieser Identifizierung ist $K[X]$ eine Erweiterung von K. Außerdem kann man vereinfachend $K[X] = (K[X], +, \cdot, 0, 1)$ anstelle von $K[X] = (K[X], +_{K[X]}, \cdot_{K[X]}, 0_{K[X]}, 1_{K[X]})$ schreiben.

Es gibt viele Analogien zwischen dem Polynomring $K[X]$ und dem Ring $\mathbb{Z}$ der ganzen Zahlen. In $K[X]$ gibt Division mit Rest und Teilbarkeit. Wir arbeiten mit einem festen K"orper K.

Lemma 164. *Sei $d \in K[X]$ mit $\operatorname{grad}(d) \geqslant 1$. F"ur jedes $p \in K[X]$ gibt es eindeutig bestimmte Polynome $q, r \in K[X]$ mit*

$$p = q \cdot d + r \text{ mit } \operatorname{grad}(r) < \operatorname{grad}(d).$$

q ist der Quotient *und r der* Rest *der Division von p durch d.*

Beweis. Statt eines Beweises geben wir nur ein Beispiel:

$$\begin{array}{rcrcrcl} (X^3 &+& 2\,X^2 &+& 3\,X &+& 4) : (X^2 + 1) = X + 2 \text{ Rest } 2\,X + 2 \\ \underline{X^3} & & &+& X & & \\ & & 2\,X^2 &+& 2\,X &+& 4 \\ & & \underline{2\,X^2} & & &+& 2 \\ & & & & 2\,X &+& 2 \end{array}$$

Dieses Rechenschema steht f"ur die Gleichung

$$(X^3 + 2\,X^2 + 3\,X + 4) - X \cdot (X^2 + 1) - 2 \cdot (X^2 + 1) = 2\,X + 2$$

bzw.

$$X^3 + 2\,X^2 + 3\,X + 4 = (X + 2) \cdot (X^2 + 1) + (2\,X + 2).$$

Die Division on Polynomen "ahnelt der "schriftlichen" Division von Dezimalzahlen. Offensichtlich kann man so f"ur alle Polynome p, d vorgehen. $\square$

Definition 165. *Das Polynom $d \in K[X]$* teilt *das Polynom $p \in K[X]$, falls es ein Polynom $q \in K[X]$ gibt mit*

$$p = q \cdot d.$$

Wir schreiben dann $q \mid p$.

20 Erweiterung von K"orpern

Wenn $p \in \mathbb{N}$ eine Primzahl ist, so ist $\mathbb{Z}/(p) = \{0, 1, ..., p-1\}$ mit der Addition und Multiplikation "modulo p" ein K"orper. "Ahnlich konstruieren wir einen K"orper $K[X]/p$ f"ur ein Primzahl-"ahnliches Polynom $p \in K[X]$, der den Ausgangsk"orper K erweitert. Weiterhin liefert die Variable X in $K[X]/p$ eine Nullstelle f"ur das Polynom p, w"ahrend p in dem Ausgangsk"orper K keine Nullstelle besitzt.

Definition 166. *Ein Polynom $p \in K[X]$ ist* irreduzibel *in $K[X]$, wenn* $\operatorname{grad}(p) \geqslant 1$, *und f"ur jeden Teiler q von p ist* $\operatorname{grad}(q) = \operatorname{grad}(p)$ *oder* $\operatorname{grad}(q) = 0$.

Irreduzible Polynome in $K[X]$ entsprechen den Primzahlen in $\mathbb{N}$. Im Allgemeinen gibt es viele irreduzible Polynome in $K[X]$. Wir zeigen nur:

Lemma 167. $X^2 + 1 \in \mathbb{R}[X]$ *ist irreduzibel.*

Beweis. Angenommen,

$$X^2 + 1 = q \cdot r$$

mit Polynomen $q = a\,X + b$ und $r = c\,X + d$ aus $\mathbb{R}[X]$ mit $a \neq 0$ und $c \neq 0$. Dann ist

$$X^2 + 1 = (a\,X + b)\,(c\,X + d) = a\,c\,X^2 + (a\,d + b\,c)\,X + b\,d.$$

Weiter ist $c = \frac{1}{a}$ und $d = \frac{1}{b}$ und

$$0 = a\,d + b\,c = \frac{a}{b} + \frac{b}{a} = \frac{a^2 + b^2}{a\,b}.$$

$a^2 + b^2 = 0$ impliziert $a = 0$, $b = 0$, $q = a\,X + b = 0$, und $X^2 + 1 = q \cdot r = 0$. Widerspruch. □

Fixiere ein Polynom $p \in K[X]$ mit $\operatorname{grad}(p) \geqslant 1$. Dabei wird noch nicht Irreduzibilit"at vorausgesetzt.

Lemma 168. *Definiere eine zweistellige Relation $\sim_p$ auf $K[X]$ durch*

$$q \sim_p r \text{ gdw. } p \mid (q - r).$$

Man schreibt auch $q \equiv r \pmod{p}$ f"ur $q \sim_p r$. Dann ist $\sim_p$ eine "Aquivalenzrelation auf $K[X]$. F"ur $q \in K[X]$ sei die Menge

$$\tilde{q} = \{r \in K[X] \mid r \sim_p q\} = \{q + p \cdot s \mid s \in K[X]\} =: q + p \cdot K[X]$$

die "Aquivalenzklasse von q bzgl. $\sim_p$. Weiter sei

$$K[X]/p = \{\tilde{q} \mid q \in K[X]\}$$

die Menge aller "Aquivalenzklassen bzgl. $\sim_p$.

Definiere eine Addition $+_p\colon (K[X]/p)\times(K[X]/p)\to K[X]/p$ *durch*

$$\tilde{q}+_p\tilde{r}=\widetilde{q+r}\,.$$

Definiere ein neutrales Element f"ur die Addition durch

$$0_p=\tilde{0}\,.$$

Definiere eine Multiplikation $\cdot_p\colon (K[X]/p)\times(K[X]/p)\to K[X]/p$ *durch*

$$\tilde{q}\cdot_p\tilde{r}=\widetilde{q\cdot r}\,.$$

Definiere ein neutrales Element f"ur die Multiplikation durch

$$1_p=\tilde{1}\,.$$

Lemma 169. *Die Struktur* $K[X]/p=(K[X]/p,\ +_p,\ \cdot_p,\ 0_p,\ 1_p)$ *ist wohldefiniert, d.h. die Operationen* $+_p$ *und* $\cdot_p$ *sind wohldefiniert. Die Struktur* $K[X]/p=(K[X]/p,+_p,\cdot_p,0_p,1_p)$ *ist ein Ring.*

Beweis. "Ubung. □

Lemma 170. *F"ur jedes* $\tilde{q}\in K[X]/p$ *gibt es ein Polynom* $r\in K[X]$ *mit* $\operatorname{grad}(r)<\operatorname{grad}(p)$ *und*

$$\tilde{q}=\tilde{r}.$$

Damit ist

$$K[X]/p=\{\tilde{r}|\ r\in K[X],\operatorname{grad}(r)<\operatorname{grad}(p)\}.$$

Beweis. r sei der Rest bei der Division von q durch p: $q=s\cdot p+r$. Dann teilt p die Differenz $q-r$ und $\tilde{q}=\tilde{r}$. □

Danach besteht $K[X]/p$ aus den "Aquivalenzklassen der Reste bei der Division durch p und wird auch der *Restklassenring* modulo p bezeichnet.

Lemma 171. *Definiere eine Abbildung* $f\colon K\to K[X]/p$ *durch*

$$f(a)=\tilde{a},$$

wobei a auf der rechten Seite als Polynom in $K[X]$ *zu verstehen ist. Dann ist f eine Einbettung von K in* $K[X]/p$*, und wir k"onnen* $K[X]/p$ *als (Ring-)Erweiterung von K auffassen.*

Wie "ublich, schreiben wir f"ur fixiertes p: $(K[X]/p,+,\cdot,0,1)$ statt $(K[X]/p,+_p,\cdot_p,0_p,1_p)$.

Aus der Irreduzibilit"at von p ergibt sich die st"arkere Eigenschaft:

Satz 172. *Wenn p irreduzibel ist, so ist* $K[X]/p=(K[X]/p,+,\cdot,0,1)$ *ein K"orper.*

Dieser Satz gilt f"ur *alle* irreduziblen Polynome p. Wir beweisen hier nur den Fall, dass das fixierte irreduzible Polynom $p=X^2+1$ ist. Man beachte, dass dann gilt:

$$X\cdot X\sim_p -1,$$

weil die Differenz $X \cdot X - (-1) = X^2 + 1$ durch $X^2 + 1$ teilbar ist. Der "Ubergang zu "Aquivalenzklassen liefert

$$\tilde{X} \cdot_p \tilde{X} = -1_p,$$

und damit gibt es in $K[X]/p$ eine Quadratwurzel aus -1.

Wir benutzen das im folgenden

Beweis. (Spezialfall $p = X^2 + 1$) Wir m"ussen zeigen, dass jedes $\tilde{q} \in K[X]/p$, $\tilde{q} \neq 0$ ein multiplikatives Inverses besitzt. Wir k"onnen annehmen, dass $\text{grad}(q) < 2$ ist: $q = a\,X + b \neq 0$. Betrachte ein weiteres Polynom $c\,X + d \in K[X]$. Dann ist

$$\begin{aligned}(a\,X+b)\,(c\,X+d) &= a\,c\,X^2 + (a\,d+b\,c)\,X + b\,d \\ &\sim_p a\,c\,(-1) + (a\,d+b\,c)\,X + b\,d \\ &\sim_p (a\,d+b\,c)\,X + (b\,d-a\,c)\end{aligned}$$

Wir wollen auf der rechten Seite das Polynom 1 erhalten. Das f"uhrt zu dem Gleichungssystem

$$\begin{aligned}a\,d+b\,c &= 0 \\ b\,d-a\,c &= 1\end{aligned}$$

f"ur die gesuchten Koeffizienten c und d mit den L"osungen

$$c = \frac{-a}{a^2+b^2} \text{ und } d = \frac{b}{a^2+b^2}.$$

Wir erhalten dann:

$$\begin{aligned}(a\,X+b)\,(c\,X+d) &= (a\,X+b)\left(\frac{-a}{a^2+b^2}\,X + \frac{b}{a^2+b^2}\right) \\ &= \frac{-a^2}{a^2+b^2}\,X^2 + \frac{a\,b-b\,a}{a^2+b^2}\,X + \frac{b^2}{a^2+b^2} \\ &\sim_p \frac{-a^2}{a^2+b^2}\,(-1) + \frac{b^2}{a^2+b^2} \\ &= \frac{a^2+b^2}{a^2+b^2} \\ &= 1\end{aligned}$$

□

Wir fixieren ein beliebiges irreduzibles Polynom $p \in K[X]$.

Satz 173. *$\tilde{X}$ ist Nullstelle des Polynoms $p = p_n\,X^n + p_{n-1}\,X^{n-1} + \cdots + p_0 \in K[X]$.*

Beweis. Das Polynom p kann auch als Polynom "uber dem gr"oßeren Koeffizientenk"orper $K[X]/p$ aufgefasst werden:

$$p \in (K[X]/p)[X].$$

Nach den Rechenregeln von $K[X]/p$ gilt:

- $\tilde{X}^i = \widetilde{X^i}$
- $p_i\,\tilde{X}^i = \widetilde{p_i\,X^i}$
- $p_n\,\tilde{X}^n + p_{n-1}\,\tilde{X}^{n-1} + \cdots + p_0 = (p_n\,X^n + p_{n-1}\,X^{n-1} + \cdots + p_0)^{\sim}$

Damit werten wir p an der Stelle $\tilde{X} \in K[X]/p$ aus:

$$\begin{aligned} p(\tilde{X}) &= p_n \tilde{X}^n + p_{n-1} \tilde{X}^{n-1} + \cdots + p_0 \\ &= (p_n X^n + p_{n-1} X^{n-1} + \cdots + p_0)^\sim \\ &= \tilde{p} \\ &= 0_p \end{aligned}$$

□

21 Die komplexen Zahlen

Wir hatten gezeigt, dass das Polynom X^2+1 irreduzibel in $\mathbb{R}[X]$ ist. Der K"orper $\mathbb{R}[X]/X^2+1$ ist eine Erweiterung des K"orpers $\mathbb{R}$, in dem das Polynom X^2+1 die Nullstelle $\tilde{X}$ hat. In $\mathbb{R}[X]/X^2+1$ ist $\tilde{X}$ eine Quadratwurzel von -1. Setze $i = \tilde{X}$; i wird als *imagin"are Einheit* bezeichnet. Damit ist

$$\begin{aligned} \mathbb{R}[X]/X^2+1 &= \{\widetilde{b\,X+a} \,|\, a,b \in \mathbb{R}\} \\ &= \{a + b\,\tilde{X} \,|\, a,b \in \mathbb{R}\} \\ &= \{a + b\,i \,|\, a,b \in \mathbb{R}\}. \end{aligned}$$

Die Rechenoperationen mit ("Aquivalenzklassen von) Polynomen $a+b\,i$ in $\mathbb{R}[X]/X^2+1$ entsprechen dem "Buchstabenrechnen" mit der Regel $i\,i = i^2 = -1$:

$$\begin{aligned} (a+b\,i)+(c+d\,i) &= (a+c)+(b+d)\,i \\ (a+b\,i)\cdot(c+d\,i) &= a\,c + a\,d\,i + b\,c\,i + b\,d\,i^2 = (a\,c - b\,d) + (a\,d + b\,c)\,i \\ \frac{1}{a+b\,i} &= \frac{a-b\,i}{(a+b\,i)\,(a-b\,i)} = \frac{a-b\,i}{a^2+b^2} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}\,i \end{aligned}$$

wobei in der letzten Gleichungskette $a+b\,i \neq 0$ vorausgesetzt ist; dann ist auch $a^2+b^2 \neq 0$.

Bei der Definition der Menge der komplexen Zahlen betonen wir den geometrischen Standpunkt und identifizieren das Polynom $a + b\ i$ mit dem Punkt $(a,\ b) \in \mathbb{R}^2$ des kartesischen Produkts $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$.

Definition 174. $\mathbb{C} = \mathbb{R} \times \mathbb{R}$ *ist die Menge der* komplexen Zahlen. *Das geordnete Paar* $(a,b) \in \mathbb{C}$ *wird auch als* $a+b\,i$ *geschrieben. Definiere die* komplexe Addition $+_{\mathbb{C}} \colon \mathbb{C} \times \mathbb{C} \to \mathbb{C}$ *durch*

$$(a+b\,i) +_{\mathbb{C}} (c+d\,i) = (a+c) + (b+d)\,i.$$

$0_{\mathbb{C}} = 0 + 0\,i$ *ist das neutrale Element der Addition.*

Definiere die komplexe Multiplikation $\cdot_{\mathbb{C}} \colon \mathbb{C} \times \mathbb{C} \to \mathbb{C}$ *durch*

$$(a+b\,i) \cdot_{\mathbb{C}} (c+d\,i) = (a\,c - b\,d) + (a\,d + b\,c)\,i.$$

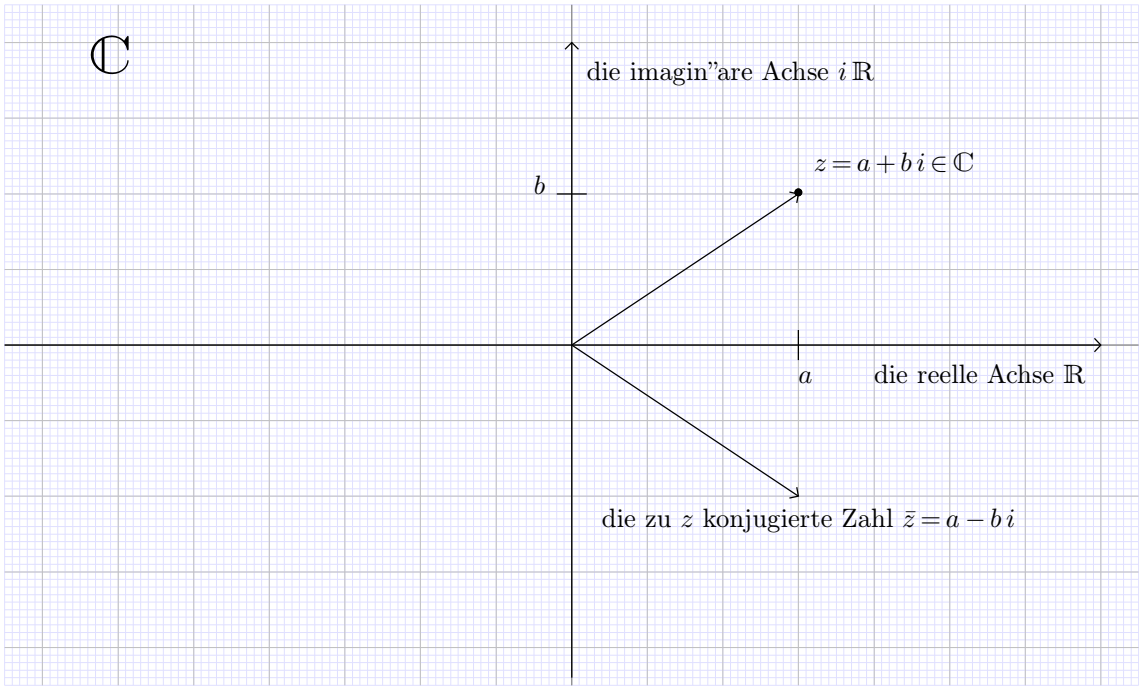
$1_{\mathbb{C}} = 1 + 0\,i$ *ist das neutrale Element der Multiplikation.*

Satz 175. *Die Struktur* $\mathbb{C} = (\mathbb{C},\ +_{\mathbb{C}},\ \cdot_{\mathbb{C}},\ 0_{\mathbb{C}},\ 1_{\mathbb{C}})$ *ist zu dem Restklassenk"orper* $\mathbb{R}[X]/X^2+1$ *isomorph, mittels der Abbildung*

$$(a,b) \mapsto a + b\,i.$$

Damit ist $\mathbb{C}$ *ein K"orper, der den K"orper* $\mathbb{R}$ *der reellen Zahlen* $\mathbb{R}$ *erweitert. Daher k"onnen wir auch einfach* $+, \cdot, 0, 1$ *statt* $+_{\mathbb{C}}, \cdot_{\mathbb{C}}, 0_{\mathbb{C}}, 1_{\mathbb{C}}$ *schreiben.*

Die Struktur der komplexen Zahlen kann als *komplexe Zahlenebene* aufgefasst werden.



Man kann dann komplexe Zahlen unter geometrischen Aspekten betrachten. Z.B. kann man die Menge der komplexen Zahlen an der $\mathbb{R}$-Achse "spiegeln":

Definition 176. *Die* komplexe Konjugation *ist die Abbildung* $f\colon \mathbb{C} \to \mathbb{C}$,

$$f(a + b\,i) = a - b\,i.$$

Wir schreiben auch $\bar{z}$ *anstelle von* $f(z)$.

Satz 177. *Die komplexe Konjugation* f *ist ein Isomorphismus von* $\mathbb{C}$ *nach* $\mathbb{C}$. *Ein Isomorphismus einer Struktur nach dieser Struktur selbst wird auch* Automorphismus *genannt.*

Beweis. Offensichtlich ist $f\colon \mathbb{C} \to \mathbb{C}$ eine bijektive Abbildung. Weiter gilt f'ur $u = a + b\,i$ und $v = c + d\,i$:

$$\begin{aligned} f(u+v) &= f((a+c)+(b+d)\,i) = (a+c)-(b+d)\,i = (a-b\,i)+(c-d\,i) = f(u)+f(v) \\ f(u\cdot v) &= f((a\,c-b\,d)+(a\,d+b\,c)\,i) = (a\,c-b\,d)-(a\,d+b\,c)\,i = (a-b\,i)\cdot(c-d\,i) = f(u)\cdot f(v) \end{aligned}$$

Schließlich ist $f(0) = 0$ und $f(1) = 1$. □

22 Geometrische Interpretation von $\mathbb{C}$

Komplexe Zahlen sind als Punkte der 2-dimensionalen "euklidischen" Ebene $\mathbb{R}^2$ definiert. Die komplexen Rechenoperationen sind dann Operationen auf Punkten von $\mathbb{R}^2$. Man kann $\mathbb{R}^2$ auch als 2-dimensionalen Vektorraum "uber $\mathbb{R}$ auffassen und die komplexen Operationen mit den Vektoroperationen vergleichen.

Lemma 178. *Die komplexe Addition* $+_{\mathbb{C}}\colon \mathbb{C}\times\mathbb{C}\to\mathbb{C}$ *stimmt mit der Vektoraddition* $+_V\colon \mathbb{R}^2\times\mathbb{R}^2\to\mathbb{R}^2$ *des* $\mathbb{R}$*-Vektorraums* $\mathbb{R}^2$ *"uberein.*

Beweis. Seien $u=a+b\,i\in\mathbb{C}$ und $v=c+d\,i\in\mathbb{C}$. Dann ist $u=(a,b)\in\mathbb{R}^2$ und $(c,d)\in\mathbb{R}^2$. Es gilt

$$u+_V v=(a,b)+_V(c,d)=(a+c,b+d)=(a+c)+(b+d)\,i=(a+b\,i)+(b+d\,i)=u+_{\mathbb{C}}v.\qquad\square$$

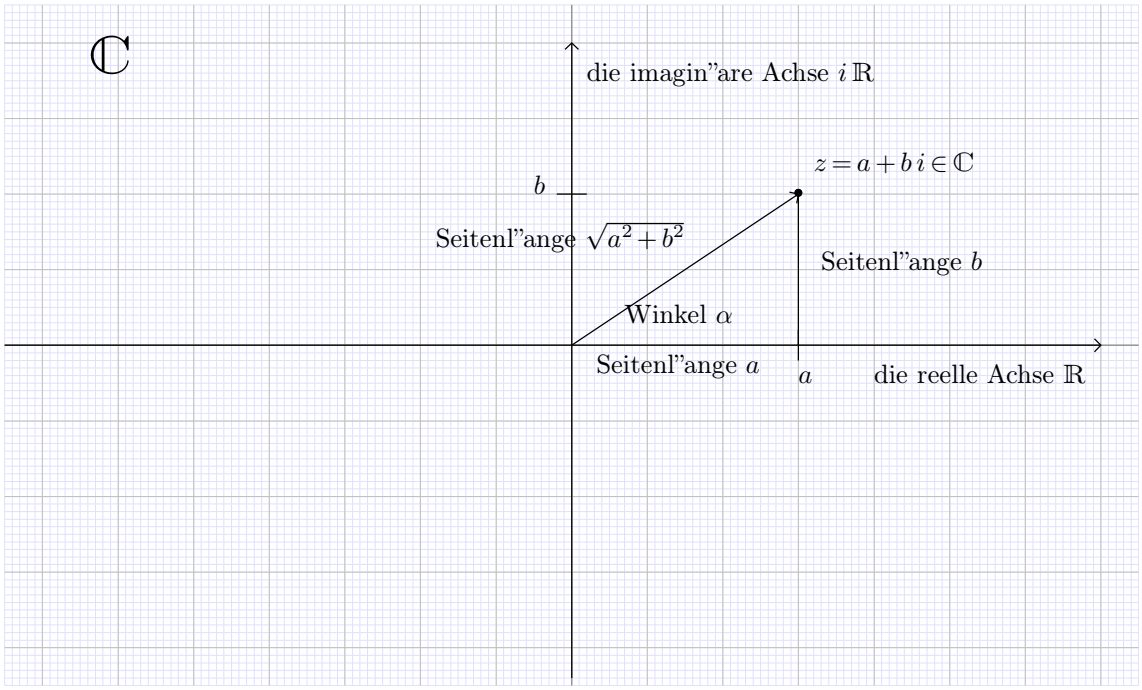
Lemma 179. *Die Einschr"ankung* $\cdot:=\ \cdot_{\mathbb{C}}\restriction(\mathbb{R}\times\mathbb{C})$ *stimmt mit der Skalarmultiplikation* $\cdot_V\colon \mathbb{R}\times\mathbb{R}^2\to\mathbb{R}^2$ *des* $\mathbb{R}$*-Vektorraums* $\mathbb{R}^2$ *"uberein.*

Beweis. Seien $\lambda\in\mathbb{R}$ und $u=a+b\,i\in\mathbb{C}$. Dann ist $u=(a,b)\in\mathbb{R}^2$. Es gilt

$$\lambda\cdot_V u=\lambda\cdot_V(a,b)=(\lambda\,a,\lambda\,b)=(\lambda\,a)+(\lambda\,b)\,i=(\lambda+0\,i)\cdot_{\mathbb{C}}(a+b\,i)=\lambda\cdot_{\mathbb{C}}u.\qquad\square$$

Im folgenden werden wir wir der uneingeschr"ankten komplexen Multiplikationen $\cdot_{\mathbb{C}}$ eine anschauliche, geometrische Deutung geben.

22.1 Polarkoordinaten



Die Zahl $z=a+b\,i\neq 0$ entspricht in der Grafik dem rechtwinkligen Dreieck mit den Eckpunkten $(0,0)$, $(a,0)$ und (a,b). Es sei α der Dreieckswinkel an der Ecke $(0,0)$. Nach den geometrischen Definitionen der trigonometrischen Funktionen Cosinus und Sinus ist

$$\cos\alpha=\frac{a}{\sqrt{a^2+b^2}}\ \text{ und }\ \sin\alpha=\frac{b}{\sqrt{a^2+b^2}}\,.$$

Dann ist

$$z=a+b\,i=\left(\sqrt{a^2+b^2}\cos\alpha\right)+\left(\sqrt{a^2+b^2}\sin\alpha\right)i=\sqrt{a^2+b^2}\,(\cos\alpha+i\sin\alpha).$$

Die komplexe Zahl z ist durch $\sqrt{a^2+b^2}$ und α bestimmt.

Definition 180. *F"ur* $z = a + b\,i \in \mathbb{C}$ *ist*

$$\sqrt{a^2 + b^2}$$

der Betrag *von* z*, der auch mit* $|z|$ *bezeichnet wird. Weiter ist jeder Winkel* α*, der*

$$\cos\alpha = \frac{a}{\sqrt{a^2+b^2}} \text{ und } \sin\alpha = \frac{b}{\sqrt{a^2+b^2}}$$

erf"ullt, ein Argument *von* z*. Man schreibt dann* $\alpha = \arg z$*.*

Die Zahl z *ist durch* $|z|$ *und* $\alpha = \arg z$ *bestimmt:*

$$z = |z|\,(\cos\alpha + i\sin\alpha).$$

Daher kann man z *auch als* $(|z|;\alpha)$ *schreiben, mit* $\alpha = \arg z$*. Man nennt* $(|z|;\alpha)$ *auch* Polarkoordinaten *von* z*; das Paar* $(.;.)$ *mit dem Semikolon bedeutet, dass es sich hier um Polarkoordinaten handelt.*

Wir diskutieren einige spezielle Punkte in der komplexen Ebene:

- spezielle Werte der Cosinus-Funktion: $\cos 0 = 1$, $\cos\frac{\pi}{4} = \frac{1}{2}\sqrt{2}$, $\cos\frac{\pi}{2} = 0$, $\cos\pi = -1$; die Cosinus-Funktion ist *periodisch* mit der Periode $2\,\pi$: $\cos(\alpha + 2\,\pi) = \cos\alpha$; cos ist *symmetrisch* zur y-Achse: $\cos(-\alpha) = \cos\alpha$.
- spezielle Werte der Sinus-Funktion: $\sin 0 = 0$, $\sin\frac{\pi}{4} = \frac{1}{2}\sqrt{2}$, $\sin\frac{\pi}{2} = 1$, $\sin\pi = 0$; die Sinus-Funktion ist *periodisch* mit der Periode $2\,\pi$: $\sin(\alpha + 2\,\pi) = \sin\alpha$; sin ist *punktsymmetrisch* zum Punkt $(0,0)$: $\sin(-\alpha) = -\sin\alpha$.
- $0 = 0\,(\cos\alpha + i\sin\alpha) = (0;\alpha)$ f'ur alle Winkel $\alpha \in \mathbb{R}$.
- $1 = 1\,(\cos 0 + i\sin 0) = (1;0)$.
- $i = 1\,\big(\cos\frac{\pi}{2} + i\sin\frac{\pi}{2}\big) = \big(1;\frac{\pi}{2}\big)$.
- $-1 = 1\,(\cos\pi + i\sin\pi) = (1;\pi)$.
- Wegen der Periodizit"at von sin und cos ist immer $(r;\alpha) = (r;\alpha + 2\,\pi) = (r;\alpha \pm 2\,n\,\pi)$ f'ur alle $n \in \mathbb{N}$.
- Der Einheitskreis in der komplexen Ebene ist die Menge

$$\{(x,y) \in \mathbb{R}^2 \,|\, |(x,y)| = 1\} = \{(x,y) \in \mathbb{R}^2 \,|\, x^2 + y^2 = 1\} = \{(1;\alpha) \,|\, \alpha \in \mathbb{R}\}.$$

In der Analysis haben wir Potenzreihenentwicklungen f'ur die Funktionen $\cos x$ und $\sin x$ kennengelernt:

$$\cos x = 1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \frac{x^6}{6!} \pm \cdots$$

und

$$\sin x = x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} \pm \cdots$$

Wir wollen diese Reihen in Bezug zur Exponentialreihe setzen:

$$e^x = \exp x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \frac{x^4}{4!} + \cdots$$

Dabei nehmen wir an, dass diese Reihen auch f"ur komplexe Argumente definiert sind, absolut konvergieren und sich auf gewohnte Art addieren und multiplizieren lassen. F"ur $x = i\,\alpha$ gilt

$$\begin{aligned} e^{i\alpha} &= 1 + i\,\alpha + \frac{(i\,\alpha)^2}{2!} + \frac{(i\,\alpha)^3}{3!} + \frac{(i\,\alpha)^4}{4!} + \cdots \\ &= 1 + i\,\alpha - \frac{\alpha^2}{2!} - i\,\frac{\alpha^3}{3!} + \frac{\alpha^4}{4!} + i\,\frac{\alpha^5}{5!} - \frac{\alpha^6}{6!} - \ldots \\ &= \left(1 - \frac{\alpha^2}{2!} + \frac{\alpha^4}{4!} - \frac{\alpha^6}{6!} - \ldots\right) + i\left(\alpha - \frac{\alpha^3}{3!} + \frac{\alpha^5}{5!} - \ldots\right) \\ &= \cos\alpha + i\sin\alpha \end{aligned}$$

Wir erhalten damit

$$z = a + b\,i = \sqrt{a^2 + b^2}\,(\cos\alpha + i\sin\alpha) = |z|\,e^{i\alpha}.$$

Die komplexe Exponentialfunktion wird f"ur den Winkelabh"angigkeit der komplexen Zahl z benutzt.

22.2 Komplexe Multiplikation und Additionstheoreme

Wenn wir weiter annehmen, dass die komplexe Exponentialfunktion auch das Gesetz

$$e^x\,e^y = e^{x+y}$$

erf"ullt, so ergibt sich f"ur das komplexe Produkt $u \cdot_{\mathbb{C}} v$ von $u = (r;\alpha)$ und $v = (s;\beta)$:

$$\begin{aligned} (r;\alpha) \cdot_{\mathbb{C}} (s;\beta) &= (r\,e^{i\alpha}) \cdot_{\mathbb{C}} (s\,e^{i\beta}) \\ &= (r\,s)\,e^{i\alpha}\,e^{i\beta} \\ &= r\,s\,e^{i\alpha+i\beta} \\ &= r\,s\,e^{i(\alpha+\beta)} \\ &= (r\,s;\alpha+\beta) \end{aligned}$$

Das Produkt zweier komplexer Zahlen ergibt sich durch

Multiplizieren der Betr"age und durch Addition der Winkel (Argumente).

Bei dem oben besprochenen Produkt $\lambda\,u$ mit $\lambda \in \mathbb{R}$ und $u \in \mathbb{C}$ spielt sich folgendes ab:

Fall 1. $\lambda \geqslant 0$. Dann ist $0 = \arg\lambda$. Damit ist $\arg(\lambda\,u) = \arg u$ und $|\lambda\,u| = \lambda\,|u|$. Also ist $\lambda\,u = \lambda \cdot_{\mathbb{C}} u$ das Skalarprodukt von λ und u.

Fall 2. $\lambda < 0$. Dann ist $\pi = \arg\lambda$. Damit ist $\arg(\lambda\,u) = \pi + \arg u$ und $|\lambda\,u| = (-\lambda)\,|u|$. Der Betrag wird mit $-\lambda$ multipliziert und das Argument um $\pi(=180\,\text{Grad})$ in die Gegenrichtung gedreht. Das aber ist das Skalarprodukt von λ und u.

Aus der Gleichung

$$e^{i\alpha} = \cos\alpha + i\sin\alpha$$

ergeben sich Formeln f"ur $\cos(\alpha+\beta)$ und $\sin(\alpha+\beta)$.

Lemma 181. *Die trigonometrischen Funktionen erf"ullen folgende* Additionstheoreme:

a) $\cos(\alpha+\beta) = \cos(\alpha)\cos(\beta) - \sin(\alpha)\sin(\beta)$;

b) $\sin(\alpha+\beta) = \cos(\alpha)\,\mathrm{sind}(\beta) + \sin(\alpha)\cos(\beta)$.

Beweis.

$$\begin{aligned}\cos(\alpha+\beta)+i\sin(\alpha+\beta) &= e^{i(\alpha+\beta)}\\ &= e^{i\alpha}\,e^{i\beta}\\ &= (\cos\alpha+i\sin\alpha)\,(\cos\beta+i\sin\beta)\\ &= (\cos(\alpha)\cos(\beta)-\sin(\alpha)\sin(\beta))+i\,(\cos(\alpha)\,\mathrm{sind}(\beta)+\sin(\alpha)\cos(\beta))\end{aligned}$$

Da Realteile und Imagin"arteile beider Seiten "ubereinstimmen m"ussen, ergeben sich die Additionsformeln. □

23 Komplexe L"osungen von Polynomgleichungen

23.1 Wurzeln

Mit $\mathbb{R}_0^+$ bezeichnen wir die Menge der nicht-negativen reellen Zahlen:

$$\mathbb{R}_0^+ = \{a\in\mathbb{R}|\, a\geqslant 0\}.$$

Satz 182. *F"ur jede Zahl $a\in\mathbb{R}_0^+$ und jede nat"urliche Zahl $n\geqslant 1$ gibt es eine eindeutig bestimmte Zahl $\sqrt[n]{a}\in\mathbb{R}_0^+$ und $(\sqrt[n]{a})^n = a$. $\sqrt[n]{a}$ heißt die n-te* Wurzel *von a.*

Beweis. Wir betrachten die Funktion $f\colon \mathbb{R}_0^+\to\mathbb{R}_0^+$, $f(x)=x^n$.

(1) f ist streng monoton wachsend: $a,b\in\mathbb{R}_0^+$ und $a<b$ impliziert $f(a)<f(b)$.

Beweisidee. Durch Induktion "uber $m\geqslant 1$ zeige $a^m<b^m$. *qed*(1)

(2) F"ur $b\geqslant 1$ ist $f(b)\geqslant b$.

Beweis. $f(b)=b\,b^{n-1}\geqslant b\,1^{n-1}=b$. *qed*(2)

Es gilt $f(0)=0$ und $f(a+1)\geqslant a+1\geqslant a$. Nach dem Zwischenwertsatz gibt es eine reelle Zahl x mit $0\leqslant x\leqslant a+1$ mit $f(x)=a$. Nach (1) ist x das eindeutig bestimmte $x\in\mathbb{R}_0^+$ mit $f(x)=a$. Damit ist die Existenz von $\sqrt[n]{a}$ gezeigt. □

Definition 183. *$a\in\mathbb{C}$ ist eine n-te* Einheitswurzel*, wenn $a^n=1$.*

Sei $(r;\alpha)$ eine n-te Einheitswurzel in Polarkoordinaten. Dann ist

$$(r;a)^n = (r^n;n\,\alpha) = 1 = (1;0).$$

Dann ist $r^n=1$ und $r=1$ als eindeutig bestimmte nicht-negative reelle n-te Wurzel von 1. Weiter ist $n\,\alpha = k\,2\,\pi$ f"ur ein $k\in\mathbb{Z}$. Dann ist $\alpha=\frac{k}{n}\,2\,\pi$. Man sieht sofort:

Lemma 184. *Sei $n\in\mathbb{N}\setminus\{0\}$. Dann sind die n komplexen Zahlen*

$$1=(1;0),\ \left(1;\frac{1}{n}\,2\,\pi\right),\left(1;\frac{2}{n}\,2\,\pi\right),\ldots,\left(1;\frac{n-1}{n}\,2\,\pi\right)$$

n-te Einheitswurzeln. In Exponentialschreibweise lauten die Zahlen

$$1, e^{i\frac{2\pi}{n}}, e^{i2\frac{2\pi}{n}}, e^{i3\frac{2\pi}{n}},\ldots, e^{i(n-1)\frac{2\pi}{n}}.$$

Mit der Einheitswurzel $\xi=\left(1;\frac{1}{n}\,2\,\pi\right)=e^{i\frac{2\pi}{n}}$ lassen sich diese auch als

$$\xi^0,\xi^1,\ldots,\xi^{n-1}$$

schreiben.

Wir werden sp"ater sehen, dass dies *alle* n-ten Einheitswurzeln sind.

Lemma 185. *Sei* $a = (r;\alpha) \in \mathbb{C}$ *und* $n \in \mathbb{N} \setminus \{0\}$. *Dann ist mit* $z = \left(\sqrt[n]{r}; \frac{\alpha}{n}\right)$

$$z^n = ((\sqrt[n]{r})^n; \alpha) = (r;\alpha) = a.$$

Daher ist z *eine Nullstelle des Polynoms*

$$X^n - a.$$

Mit $\xi = \left(1; \frac{1}{n} 2\pi\right) = e^{i\frac{2\pi}{n}}$ *sind*

$$z, z\xi, z\xi^2, ..., z\xi^{n-1}$$

Nullstellen von $X^n - a$. *F"ur* $a \neq 0$ *sind diese Nullstellen paarweise verschieden.*

23.2 Nullstellen von komplexen Polynomen

Lemma 186. *Sei* $p = p_n X^n + p_{n-1} X^{n-1} + \cdots + p_0 \in \mathbb{C}[X]$ *ein komplexes Polynom, d.h. ein Polynom mit komplexen Koeffizienten, vom Grad* $n \geqslant 1$. *Sei* $a \in \mathbb{C}$ *eine Nullstelle von* p*:* $p(a) = 0$. *Dann wird* p *von* $(X - a)$ *geteilt.*

Beweis. Nach dem Lemma "uber die Polynomdivision mit Rest existieren eindeutig bestimmte Polynome $q, r \in \mathbb{C}[X]$ mit

$$p = q \cdot (X - a) + r \text{ mit } \operatorname{grad}(r) < \operatorname{grad}(X - a) = 1.$$

Dann ist $\operatorname{grad}(r) = 0$ und r ist eine Konstante $r \in \mathbb{C}$.

F"ur $X = a$ gilt dann

$$r = q(a) \cdot (a - a) - p(a) = 0 - 0 = 0.$$

Also ist

$$p = q \cdot (X - a).$$ □

Satz 187. *Sei* $p = p_n X^n + p_{n-1} X^{n-1} + \cdots + p_0 \in \mathbb{C}[X]$ *mit* $\operatorname{grad}(p) \geqslant 1$. *Dann besitzt* p *h"ochstens* n *Nullstellen.*

Beweis. Durch Induktion "uber n.

Induktionsanfang: $n = 1$. Dann ist $p = p_1 X + p_0$. F"ur $a \in \mathbb{C}$ ist

$$p(a) = 0 \leftrightarrow p_1 a + p_0 = 0 \leftrightarrow a = \frac{p_0}{p_1}.$$

Damit hat p genau eine Nullstelle $\frac{p_0}{p_1}$.

Induktionsschritt: Die Behauptung gelte f"ur ein $n \geqslant 1$. Sei $p \in \mathbb{C}[X]$ mit $\operatorname{grad}(p) = n + 1$. Wenn p keine Nullstelle in $\mathbb{C}$ hat, so ist die Behauptung erf"ullt und Induktionsschritt gezeigt. Wir nehmen also an, dass p eine Nullstelle $a \in \mathbb{C}$ hat. Nach XXX gibt es $q \in \mathbb{C}[X]$ mit $\operatorname{grad}(q) = n$ und

$$p = q \cdot (X - a).$$

(1) Wenn $b \in \mathbb{C}$ eine Nullstelle von p ist, so ist $b = a$ oder b ist Nullstelle von q.

Beweis. Sei $p(b)=0$ und $b\neq a$. Dann ist

$$p(b)=q(b)\cdot(b-a) \text{ und } q(b)=\frac{p(b)}{b-a}=\frac{0}{b-a}=0.$$

$qed(1)$

Damit gilt

$$\{b\in\mathbb{C}|\, b \text{ ist Nullstelle von } p\}\subseteq\{a\}\cup\{b\in\mathbb{C}|\, b \text{ ist Nullstelle von } q\}$$

und

$$|\{b\in\mathbb{C}|\, b \text{ ist Nullstelle von } p\}|\subseteq|\{a\}|+|\{b\in\mathbb{C}|\, b \text{ ist Nullstelle von } q\}|\leqslant 1+n$$

Nach dem Prinzip der vollst"andigen Induktion ist das Lemma gezeigt. □

Lemma 188. *Sei $a=(r;\alpha)\in\mathbb{C}$, $a\neq 0$ und $n\in\mathbb{N}\setminus\{0\}$. Setze $z=\left(\sqrt[n]{r};\frac{\alpha}{n}\right)$ und $\xi=\left(1;\frac{1}{n}\,2\,\pi\right)$. Dann sind*

$$z, z\,\xi, z\,\xi^2, ..., z\,\xi^{n-1}$$

s"amtliche Nullstellen von X^n-a, d.h. sie sind s"amtliche n-ten Wurzeln von a.

Beweis. $z, z\,\xi, z\,\xi^2, ..., z\,\xi^{n-1}$ sind n paarweise verschiedene Nullstellen von X^n-a. Mehr kann es nach dem Satz nicht geben. □

23.3 Quadratische Gleichungen

Sei $p_2\,X^2+p_1\,X+p_0\in\mathbb{C}[X]$ mit $\text{grad}(p)=2$ (d.h. $p_2\neq 0$). Wir bestimmen Nullstellen $z\in\mathbb{C}$ durch *logisch* "aquivalente Umformungen der Gleichung $p_2\,z^2+p_1\,z+p_0=0$.

$$\begin{aligned}
& p_2\,z^2+p_1\,z+p_0=0\\
\leftrightarrow\ & z^2+\frac{p_1}{p_2}\,z+\frac{p_0}{p_2}=0\\
\leftrightarrow\ & z^2+p\,z+q=0\\
\leftrightarrow\ & z^2+2\,\frac{p}{2}\,z+\left(\frac{p}{2}\right)^2-\left(\frac{p}{2}\right)^2+q=0\\
\leftrightarrow\ & \left(z+\frac{p}{2}\right)^2=\left(\frac{p}{2}\right)^2-q
\end{aligned}$$

Dabei haben wir im Hinblick auf die "p-q-Formel" $p=\frac{p_1}{p_2}$ und $q=\frac{p_0}{p_2}$ gesetzt.

Die letzte Zeile besagt, dass $z+\frac{p}{2}$ *Quadratwurzel* (= 2. Wurzel) von $\left(\frac{p}{2}\right)^2-q$ ist. Es gibt genau 2 Quadratwurzeln von $\left(\frac{p}{2}\right)^2-q$, die sich um den Faktor $\xi=\left(1;\frac{1}{2}\,2\,\pi\right)=(1;\pi)=-1$ unterscheiden. Wir bezeichnen diese Wurzeln mit

$$+\sqrt{\left(\frac{p}{2}\right)^2-q} \quad \text{und} \quad -\sqrt{\left(\frac{p}{2}\right)^2-q}$$

Damit l"asst sich die Kette von "Aquivalenzen fortsetzen:

$$\begin{aligned}
\leftrightarrow\ & z+\frac{p}{2}=+\sqrt{\left(\frac{p}{2}\right)^2-q} \quad \text{oder} \quad z+\frac{p}{2}=-\sqrt{\left(\frac{p}{2}\right)^2-q}\\
\leftrightarrow\ & z=-\frac{p}{2}+\sqrt{\left(\frac{p}{2}\right)^2-q} \quad \text{oder} \quad z=-\frac{p}{2}-\sqrt{\left(\frac{p}{2}\right)^2-q}\\
\leftrightarrow\ & z=-\frac{p}{2}\pm\sqrt{\left(\frac{p}{2}\right)^2-q}\,.
\end{aligned}$$

Satz 189. *Die Nullstellenmenge des Polynoms* $X^2+p\,X+q\in\mathbb{C}[X]$ *ist*

$$\left\{-\frac{p}{2}+\sqrt{\left(\frac{p}{2}\right)^2-q},-\frac{p}{2}-\sqrt{\left(\frac{p}{2}\right)^2-q}\right\}.$$

Diese Menge heißt auch L"osungsmenge *der quadratischen Gleichung* $X^2+p\,X+q=0$. *Die Gleichung hat genau dann genau eine L"osung, wenn* $\left(\frac{p}{2}\right)^2-q=0$ *ist. Das ist "aquivalent zu* $p^2-4\,q=0$. *Der Term* $p^2-4\,q$ *ist die* Diskriminante *der quadratischen Gleichung.*

23.4 Gleichungen 3. Grades (kubische Gleichungen)

Gesucht ist die Nullstellenmenge eines Polynoms

$$X^3+a\,X^2+b\,X+c\in\mathbb{C}[X]$$

Lemma 190. $z\in\mathbb{C}$ *ist Nullstelle von* $X^3+a\,X^2+b\,X+c$ *gdw.* $z+\frac{a}{3}$ *Nullstelle des Polynoms*

$$X^3+\left(3\left(\frac{a}{3}\right)^2-\frac{2}{3}\,a^2+b\right)X+\left(-\left(\frac{a}{3}\right)^3+a\left(\frac{a}{3}\right)^2-b\,\frac{a}{3}+a\right)\in\mathbb{C}[X]$$

ist.

Beweis. F"ur alle $z\in\mathbb{C}$ gelten die "Aquivalenzen:

$$\begin{aligned}
&z^3+a\,z^2+b\,z+a=0\\
\leftrightarrow\ &\left(\left(z+\frac{a}{3}\right)-\frac{a}{3}\right)^3+a\left(\left(z+\frac{a}{3}\right)-\frac{a}{3}\right)^2+b\left(\left(z+\frac{a}{3}\right)-\frac{a}{3}\right)+a=0\\
\leftrightarrow\ &\left(z+\frac{a}{3}\right)^3-3\left(z+\frac{a}{3}\right)^2\frac{a}{3}+3\left(z+\frac{a}{3}\right)\left(\frac{a}{3}\right)^2-\left(\frac{a}{3}\right)^3+a\left(z+\frac{a}{3}\right)^2-2\,a\left(z+\frac{a}{3}\right)\frac{a}{3}+a\left(\frac{a}{3}\right)^2+\\
&b\left(z+\frac{a}{3}\right)-b\,\frac{a}{3}+a=0\\
\leftrightarrow\ &\left(z+\frac{a}{3}\right)^3+3\left(z+\frac{a}{3}\right)\left(\frac{a}{3}\right)^2-\left(\frac{a}{3}\right)^3-2\,a\left(z+\frac{a}{3}\right)\frac{a}{3}+a\left(\frac{a}{3}\right)^2+b\left(z+\frac{a}{3}\right)-b\,\frac{a}{3}+a=0\\
\leftrightarrow\ &\left(z+\frac{a}{3}\right)^3+\left(3\left(\frac{a}{3}\right)^2-\frac{2}{3}\,a^2+b\right)\left(z+\frac{a}{3}\right)+\left(-\left(\frac{a}{3}\right)^3+a\left(\frac{a}{3}\right)^2-b\,\frac{a}{3}+a\right)=0
\end{aligned}$$

□

Um die Nullstellen eines Polynoms $X^3+a\,X^2+b\,X+c$ zu bestimmen, gen"ugt es also, die L"osungen einer Gleichung der Form

$$(*)\qquad\qquad X^3+p\,X+q=0$$

zu bestimmen.

Wir wollen die Nullstellen z von $X^3+p\,X+q$ als Summen $z=x+y$, $x,y\in\mathbb{C}$ gewinnen. Es gilt

$$(x+y)^3-3\,x\,y\,(x+y)-x^3-y^3=0$$

Es gilt:

(1) Wenn $-3\,x\,y=p$ und $-x^3-y^3=q$ ist, so ist $x+y$ eine L"osung von $(*)$.

F"ur derartige Zahlen x^3 und y^3 gilt

$$x^3\,y^3=-\left(\frac{p}{3}\right)^3\quad\text{und}\quad x^3+y^3=-q.$$

Satz 191. (Satz von Vieta) *Seien $u, v \in \mathbb{C}$ mit $u + v = c$ und $u\,v = d$. Dann ist $\{u, v\}$ die L"osungsmenge der quadratischen Gleichung*

$$X^2 - c\,X + d = 0.$$

Beweis. Nach der p-q-Formel sind die L"osungen:

$$z = -\frac{-u-v}{2} \pm \sqrt{\Big(\frac{-u-v}{2}\Big)^2 - u\,v} = \frac{u+v}{2} \pm \sqrt{\frac{u^2+2\,u\,v+v^2-4\,u\,v}{4}} = \frac{u+v}{2} \pm \sqrt{\frac{u^2-2\,u\,v+v^2}{4}} =$$

$$\frac{u+v}{2} \pm \sqrt{\frac{(u-v)^2}{4}} = \frac{u+v}{2} \pm \frac{u-v}{2} = u \text{ bzw. } v. \qquad \square$$

Damit sind x^3 und y^3 wie in (1) L"osungen der quadratischen Gleichung

$$X^2 + q\,X - \Big(\frac{p}{3}\Big)^3 = 0.$$

Nach der p-q-Formel hat diese Gleichung die L"osungen

$$x^3 = -\frac{q}{2} + \sqrt{\Big(\frac{q}{2}\Big)^2 + \Big(\frac{p}{3}\Big)^3} \quad \text{und} \quad y^3 = -\frac{q}{2} - \sqrt{\Big(\frac{q}{2}\Big)^2 + \Big(\frac{p}{3}\Big)^3}$$

Die Gleichungen haben die L"osungen

$$x_0 = \sqrt[3]{-\frac{q}{2} + \sqrt{\Big(\frac{q}{2}\Big)^2 + \Big(\frac{p}{3}\Big)^3}}\ , \text{ sowie } x_1 = x_0\,e^{\frac{2\pi i}{3}} \text{ und } x_2 = x_0\,e^{\frac{4\pi i}{3}},$$

bzw.

$$y_0 = \sqrt[3]{-\frac{q}{2} - \sqrt{\Big(\frac{q}{2}\Big)^2 + \Big(\frac{p}{3}\Big)^3}}\ , \text{ sowie } y_1 = y_0\,e^{\frac{2\pi i}{3}} \text{ und } y_2 = y_0\,e^{\frac{4\pi i}{3}}.$$

Dann ist

$$\begin{aligned} x_0\,y_0 &= \sqrt[3]{\left(-\frac{q}{2} + \sqrt{\Big(\frac{q}{2}\Big)^2 + \Big(\frac{p}{3}\Big)^3}\right)\left(-\frac{q}{2} - \sqrt{\Big(\frac{q}{2}\Big)^2 + \Big(\frac{p}{3}\Big)^3}\right)} \\ &= \sqrt[3]{\frac{q^2}{4} - \Big(\frac{q}{2}\Big)^2 - \Big(\frac{p}{3}\Big)^3} \\ &= \sqrt[3]{-\Big(\frac{p}{3}\Big)^3} = -\frac{p}{3} \end{aligned}$$

"Ahnlich ergibt sich $x_1\,y_2 = -\frac{p}{3}$ und $x_2\,y_1 = -\frac{p}{3}$. Damit sind

$$\begin{aligned} z_0 = x_0 + y_0 &= \sqrt[3]{-\frac{q}{2} + \sqrt{\Big(\frac{q}{2}\Big)^2 + \Big(\frac{p}{3}\Big)^3}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\Big(\frac{q}{2}\Big)^2 + \Big(\frac{p}{3}\Big)^3}} \\ z_1 = x_1 + y_2 &= e^{\frac{2\pi i}{3}}\sqrt[3]{-\frac{q}{2} + \sqrt{\Big(\frac{q}{2}\Big)^2 + \Big(\frac{p}{3}\Big)^3}} + e^{\frac{4\pi i}{3}}\sqrt[3]{-\frac{q}{2} - \sqrt{\Big(\frac{q}{2}\Big)^2 + \Big(\frac{p}{3}\Big)^3}} \\ z_2 = x_2 + y_1 &= e^{\frac{4\pi i}{3}}\sqrt[3]{-\frac{q}{2} + \sqrt{\Big(\frac{q}{2}\Big)^2 + \Big(\frac{p}{3}\Big)^3}} + e^{\frac{2\pi i}{3}}\sqrt[3]{-\frac{q}{2} - \sqrt{\Big(\frac{q}{2}\Big)^2 + \Big(\frac{p}{3}\Big)^3}} \end{aligned}$$

L”osungen von $(*)$.

23.5 Historische Bemerkungen

Quadratische Gleichungen $p_2\,z^2 + p_1\,z + p_0 = 0$ wurden bereits im Altertum gel”ost. Ein Blick auf die p-q-Formel

$$z = -\frac{p}{2} \pm \sqrt{\left(\frac{p}{2}\right)^2 - q}$$

zeigt, dass die Bestimmung von L”osungen kompliziert wird, wenn man in eingeschr”ankten Zahlbereichen arbeitet. Wenn keine negativen und keine komplexen Zahlen zur Verf”ugung stehen, existieren manche Zwischenschritte und L”osungen nicht, so dass die L”osungsmengen “uber gewisse Fallunterscheidungen von den Anfangsdaten abh”angen. So unterscheidet Al-Chwarizmi, aus dessen Namen der Begriff *Algorithmus* abgeleitet ist, ungefähr 825 n.Chr. sechs Typen quadratischer Gleichungen, deren (positive reelle) L”osungen auf unterschiedlichen Wegen bestimmt werden.

Kubische Gleichungen

Im fr”uhen 16. Jahrhundert fand der italienische Mathematiker *Scipione del Ferro* eine von ihm gehaltene Methode, um kubische Gleichungen der Form $x^3 + m\,x = n$ zu l”osen. Wir hatten oben gesehen, dass alle kubische Gleichungen auf diese Form gebracht werden k”onnen. Kurz vor seinem Tod gab er das Geheimnis an seinen Studenten *Antonio Fiori* weiter.

Niccolò Fontana Tartaglia

Um 1530 gab es einen ber”uhmten Wettstreit zwischen Fiori und Niccolo Tartaglia. Tartaglia musste Probleme der Form $x^3 + m\,x = n$ l”osen, w”ahrend Fiori Probleme der Form $x^3 + m\,x^2 = n$ erhielt. Tartaglia war auch im Besitz einer Methode f”ur Gleichungen der Form $x^3 + m\,x = n$ w”ahrend die Form $x^3 + m\,x^2 = n$ wesentlich schwerer ist. So gewann Tartaglia den Wettkampf.

Sp”ater wurde Tartaglia von *Girolamo Cardano* “uberredet, ihm seine L”osung preiszugeben. Es wurde vereinbart, dass Cardano das Geheimnis nicht ver”offentlichen durfte, oder nur, wenn Tartaglia vorher selbst genug Zeit f”ur eine Ver”offentlichung erhielte. Cardano erfuhr jedoch von Ferros fr”ueheren Arbeiten und ver”offentlichte diese in seinem Buch *Ars Magna*. Tartaglia sah das als einen Bruch der Vereinbarung. Er forderte Cardano zu einem Wettstreit heraus, den ein Sch”uler Cardanos, Lodovico Ferrari, annahm. Der Sch”uler besiegte Tartaglia, der daraufhin sein Ansehen und sein Einkommen verlor.

Cardano bemerkte, dass in der Methode von Tartaglia Quadratwurzeln aus negativen Zahlen gezogen wurden. Er schrieb dar”uber in der Ars Magna. Rafael Bombelli stellte weitere Untersuchungen hierzu an. Cardano und Bombelli werden h”aufig als die Entdecker der komplexen Zahlen angesehen.

Biquadratische Gleichungen

Die erste geschlossene Lösung der quartischen Gleichung fand der italienische Mathematiker Lodovico Ferrari (1522–1565). Diese Lösung veröffentlichte sein Lehrer Gerolamo Cardano 1545 in dem Werk *Ars magna de Regulis Algebraicis*.

23.6 Nullstellen von Gleichungen h"oheren Grades

Satz 192. *Sei $p = p_n X^n + p_{n-1} X^{n-1} + \cdots + p_0 \in \mathbb{R}[X]$ ein reelles Polynom vom Grad n, wobei n eine* ungerade *nat"urliche Zahl ist. Dann besitzt p eine reelle Nullstelle.*

Beweis. Ohne Beschr"ankung der Allgemeinheit kann man annehmen, dass $p_n = 1$ ist ("Ubung). Setze

$$M = \max\{|p_{n-1}|, ..., |p_0|\} \text{ und } A = M + 2$$

Dann ist

$$\begin{aligned} p(A) &= A^n + p_{n-1} A^{n-1} + \cdots + p_0 \\ &\geqslant A^n - M A^{n-1} - M A^{n-2} - \cdots - M \\ &= A^n - M \frac{A^n - 1}{A - 1} \\ &= \frac{A^{n+1} - A^n - M A^n + M}{A - 1} \\ &> \frac{A^{n+1} - (M+1) A^n}{A - 1} \\ &= \frac{(M+2)A^n - (M+1) A^n}{A - 1} \\ &> 0 \end{aligned}$$

und

$$\begin{aligned} p(-A) &= (-A)^n + p_{n-1} (-A)^{n-1} + \cdots + p_0 \\ &\leqslant -A^n + M A^{n-1} + M A^{n-2} + \cdots + M \\ &< 0 \end{aligned}$$

Da die Polynomfunktion $x \mapsto p(x)$ stetig ist, l"asst sich der Zwischenwertsatz anwenden: es gibt ein $z \in \mathbb{R}$, $-A < z < A$, so dass $p(z) = 0$ ist □

Damit hat ein reelles Polynom 5. Grades eine reelle Nullstelle. Nach den Erfahrungen mit Polynomen 2., 3. und 4. Grades w"urde man eine allgemeine L"osungsformel erwarten, die aus mit Hilfe der Wurzelfunktionen $\sqrt{u}, \sqrt[3]{u}, \sqrt[4]{u}$ und $\sqrt[5]{u}$ und anderen Rechenoperationen gebildet ist. Man nennt die Wurzelfunktionen auch *Radikale* (nach *radix* = Wurzel).

Definition 193. *Ein Radikalen-Ausdruck ist ein Term, der sich auf folgende Weise bilden l"asst:*

- *die Terme p_0, p_1, p_2, ... sind Radikalen-Ausdr"ucke (Variable f"ur Koeffizienten von Polynomen);*
- *jede rationale Zahl ist ein Radikalen-Ausdruck (rationale Konstanten);*
- *wenn t_0, t_1 Radikalen-Ausdr"ucke sind, so sind auch $t_0 + t_1$, $-t_0$, $t_0 \cdot t_1$, $\frac{t_0}{t_1}$ Radikalen-Ausdr"ucke (rationale Funktionen);*
- *wenn t ein Radikalen-Ausdruck ist und $n \in \mathbb{N} \setminus \{0, 1\}$, so ist $\sqrt[n]{t}$ ein Radikalen-Ausdruck (Wurzeln).*

Definition 194. *Eine komplexe Polynomgleichung*

$$p(x) = p_n x^n + p_{n-1} x^{n-1} + \cdots + p_0 = 0$$

hat eine L"osung durch Radikale*, wenn es einen Radikalen-Ausdruck t in den Koeffizienten des Polynoms gibt, der eine Nullstelle von p ist.*

Unter dem L"osen von Polynomgleichungen verstand man lange Zeit die Suche nach L"osungen durch Radikale. Ideal w"aren Radikalen-Ausdr"ucke, die f'ur alle Polynome festen Grades (alle) Nullstellen liefern. Diese existieren f'ur Gleichungen 2., 3. und 4. Grades. F"ur den Grad 5 ging die Suche nicht voran. Schließlich wurde die Unm"oglichkeit eines allgemeinen L"osungsterms gezeigt:

Satz 195. (Satz von Abel und Ruffini) *Es gibt eine Polynomgleichung 5. Grades, die keine L"osung durch Radikale besitzt.*

Ein *Beweis* des Satzes kann mit den Mitteln dieser Vorlesung nicht erbracht werden. "Ublicherweise wird der Satz in der *"Einf"uhrung in die Algebra* bewiesen. Eine vage Vorstellung kann man anhand unserer Radikalterme f'ur die Gleichungen 2. und 3. Grades geben.

Beim L"osungs-Term

$$z_0 \;=\; \sqrt[3]{-\frac{q}{2}+\sqrt{\left(\frac{q}{2}\right)^2+\left(\frac{p}{3}\right)^3}}+\sqrt[3]{-\frac{q}{2}-\sqrt{\left(\frac{q}{2}\right)^2+\left(\frac{p}{3}\right)^3}}$$

konnten f'ur die linke 3. Wurzeln alle 3 Wurzeln benutzt werden. Diese Vertauschungsm"oglichkeiten haben zur Folge, dass die drei L"osungen ebenfalls auf systematische Art vertauscht werden. Die L"osungsmengen besitzen gewisse Symmetrie(-Gruppen), die durch die Symmetrieen von 2. und 3. Wurzeln erzeugt werden.

Andererseits lassen sich Gleichungen 5. Grades angeben, deren Symmetriegruppen isomorph zu $\mathfrak{S}_5 = \mathfrak{S}(\{0,1,2,3,4\})$ ist. Man kann aber zeigen, dass sich $\mathfrak{S}_5$ nicht durch "Wurzelsymmetrien" erzeugen l"asst.

Diese Ideen werden in der *Galois-Theorie* systematisch erfasst. Diese Theorie stellt einen engen Zusammenhang zwischen K"orpererweiterungen der Gestalt

$$K[X]/p$$

und endlichen Gruppen her.

23.7 Der Fundamentalsatz der Algebra

Satz 196. (Gauß) *Sei* $p = p_n X^n + p_{n-1} X^{n-1} + \cdots + p_0 \in \mathbb{C}[X]$ *ein Polynom vom Grad* $n \geqslant 1$. *Dann besitzt* p *eine komplexe Nullstelle.*

Dieser Satzes kann in verschiedenen mathematischen Theorien bewiesen werden, aber vollst"andige Beweise gehen "uber die M"oglichkeiten dieser Vorlesung hinaus. Es gibt "analytische" Beweise, die vor allem Methoden der Analysis benutzen, und "algebraische" Beweise, die auf dem "Rechnen" in Strukturen beruhen. Wir haben analytische Methoden benutzt, um zu zeigen, dass reelle Polynome von *ungeradem* Grad Nullstellen besitzen, und wir haben algebraische Methoden benutzt, um Nullstellen f'ur Polynome 2. und 3. Grades zu finden. Carl-Friedrich Gauß hat einen Beweis des Fundamentalsatzes gegeben, in dem diese Methoden kombiniert werden.

Wir wollen ein anschauliches Argument f'ur den Fundamentalsatz geben:

Sei $r \in \mathbb{R}$, $r \geqslant 0$. Die Funktion $K_r\colon [0, 2\pi] \to \mathbb{C}$, $K_r(\alpha) = r\, e^{i\alpha}$ hat den Kreis mit Mittelpunkt 0 und Radius r als Bildmenge:

$$\mathrm{bild}(K_r) = \{z \in \mathbb{C} \mid |z| = r\}.$$

Dabei lassen wir auch den "uneigentlichen" Kreis mit Radius 0 zu. Wir untersuchen, wie dieser Kreis vom Polynom p abgebildet wird. Wie sieht die Abbildung

$$p \circ K_r\colon [0, 2\pi] \to \mathbb{C}$$

aus? Offensichtlich ist das Bild eine "Schleife" in $\mathbb{C}$: das Bild ist eine zusammenh"angende Kurve, deren Endpunkt gleich dem Anfangspunkt ist:

$$p \circ K_r(0) = p \circ K_r(2\,\pi).$$

Falls p von der einfachen Gestalt $p = p_n\,X^n$ ist, so ist

$$p \circ K_r(\alpha) = p(r\,e^{i\alpha}) = p_n\,(r\,e^{i\alpha})^n = (p_n\,r^n)\,e^{i\alpha n}.$$

Das Bild dieser Abbildung ist der Kreis mit Mittelpunkt 0 und Radius $p_n\,r^n$. Dieser Kreis wird von der Abbildung $p \circ K_r$ n-mal durchlaufen.

F"ur ein allgemeines Polynom $p = p_n\,X^n + p_{n-1}\,X^{n-1} + \cdots + p_0 \in \mathbb{C}[X]$ und einen gen"ugend großen Radius r_* bestimmt der Term $p_n\,X^n$ das Verhalten der Schleife $p \circ K_{r_*}$. Die Schleife verl"auft im Wesentlichen wie $p_n\,X^n$, die "ubrigen Glieder $p_{n-1}\,X^{n-1} + \cdots + p_0$ bewirken verh"altnism"aßig kleine Abweichungen. So l"auft die Schleife $p \circ K_{r_*}$ ebenso wie $p_n\,(r_*\,e^{i\alpha})^n$ n-mal um den Nullpunkt.

Wir wollen nun argumentieren, dass das Polynom $p = p_n\,X^n + p_{n-1}\,X^{n-1} + \cdots + p_0$ eine Nullstelle in $\mathbb{C}$ besitzt. Wir arbeiten mit einem Widerspruchsbeweis: Angenommen es sei $p(z) \neq 0$ f"ur alle $z \in \mathbb{C}$.

F"ur den Radius $r = 0$ ist $p \circ K_r$ eine konstante Schleife, die aus einem einzigen Punkt $\neq 0$ besteht. Diese Schleife l"auft daher 0-mal um den Nullpunkt.

F"ur jede reelle Zahl $r \geqslant 0$ ist $p \circ K_r$ eine Schleife, die 0 nicht als Bildpunkt besitzt. F"ur jedes r l"asst sich daher eine *Windungszahl* $w(r) \in \mathbb{N}$ definieren, die besagt, dass $p \circ K_r$ $w(r)$-mal um den Nullpunkt l"auft.

Man kann zeigen, dass die Funktion

$$w\colon \mathbb{R}_0^+ \to \mathbb{N}$$

stetig ist. Es ist $w(0) = 0$ und $w(r_*) = n \geqslant 1$. Aber eine stetige Funktion von $\mathbb{R}_0^+$ nach $\mathbb{N}$ muss konstant sein. Widerspruch.

24 Geraden und Kreise in der komplexen Ebene

Die Menge der komplexen Zahlen ist die Menge der Punkte der zweidimensionalen (Zeichen-) Ebene. Wir identifizieren den Punkt $(x, y) \in \mathbb{R}^2$ mit der komplexen Zahl $z = x + i\,y$.

Aus der Linearen Algebra ist bekannt: Geraden im $\mathbb{R}^2$ sind genau die Mengen

$$\text{I:} \qquad G = \{(x, y) \in \mathbb{R}^2 |\; a\,x + b\,y = c\}$$

mit $a, b, c \in \mathbb{R}$ und $(a, b) \neq (0, 0)$. Mit $d = a - i\,b$ l"asst sich die Bedingung $a\,x + b\,y = c$ als Bedingung f"ur z innerhalb der komplexen Arithmetik umformen:

$$\begin{aligned}
& a\,x + b\,y = c \\
\leftrightarrow\ & a\,x + a\,i\,y - i\,b\,x + b\,y + a\,x - a\,i\,y + i\,b\,x + b\,y = 2\,c \\
\leftrightarrow\ & (a - i\,b)\,(x + i\,y) + (a + i\,b)\,(x - i\,y) = 2\,c \\
\leftrightarrow\ & d\,z + \bar{d}\,\bar{z} = 2\,c
\end{aligned}$$

Damit ist

$$\text{II:} \qquad G = \{z \in \mathbb{C} |\; d\,z + \bar{d}\,\bar{z} = 2\,c\}.$$

Umgekehrt l"asst sich jede Zahl $d \in \mathbb{C} \setminus \{0\}$ als $d = a - i\,b$ mit $(a, b) \neq (0, 0)$ darstellen. Damit sind die Darstellungen I und II "aquivalent, und wir haben bewiesen:

Lemma 197. *Die Geraden in der komplexen Ebene $\mathbb{C}$ sind genau die Mengen*

$$G = \{z \in \mathbb{C} |\, f z + \bar{f}\bar{z} + g = 0\}$$

mit $f \in \mathbb{C} \setminus \{0\}$ und $g \in \mathbb{R}$.

Aus der Linearen Algebra ist weiterhin bekannt: Kreise im $\mathbb{R}^2$ sind genau die Mengen

$$\text{I:} \qquad K = \{(x,y) \in \mathbb{R}^2 |\, \|(x,y) - (a,b)\| = r\}$$

wobei (a,b) der Mittelpunkt und $r > 0$ der Radius des Kreises ist. Mit $d = a + i\,b$ l"asst sich die Bedingung $\|(x,y) - (a,b)\| = r$ als Bedingung f"ur z innerhalb der komplexen Arithmetik umformen:

$$\begin{aligned}
& \|(x,y) - (a,b)\| = r \\
\leftrightarrow\ & (x-a)^2 + (y-b)^2 = r^2 \\
\leftrightarrow\ & ((x-a) + i\,(y-b))\,((x-a) - i\,(y-b)) = r^2 \\
\leftrightarrow\ & (z-d)\,(\bar{z} - \bar{d}) = r^2 \\
\leftrightarrow\ & z\bar{z} - \bar{d}\,z - d\,\bar{z} + d\,\bar{d} = r^2 \\
\leftrightarrow\ & z\bar{z} - \bar{d}\,z - d\,\bar{z} + d\,\bar{d} - r^2 = 0 \\
\leftrightarrow\ & z\bar{z} + f z + \bar{f}\bar{z} + g = 0
\end{aligned}$$

mit $f = -\bar{d}$ und $g = d\,\bar{d} - r^2 \in \mathbb{R}$. Es ist dann auch $f\,\bar{f} = d\,\bar{d} > d\,\bar{d} - r^2 = g$.

Wenn umgekehrt $f \in \mathbb{C}$ und $g \in \mathbb{R}$ mit $f\,\bar{f} > g$ gegeben sind, so gelten die obigen "Aquivalenzen mit dem Kreismittelpunkt $(a,b) = -\bar{f}$ und dem Radius $r = \sqrt{f\,\bar{f} - g} > 0$. Also gilt

Lemma 198. *Die Kreise (mit positivem Radius) in der komplexen Ebene $\mathbb{C}$ sind genau die Mengen*

$$K = \{z \in \mathbb{C} |\, z\bar{z} + f z + \bar{f}\bar{z} + g = 0\}$$

mit $f \in \mathbb{C}$, $g \in \mathbb{R}$ und $f\,\bar{f} > g$.

Wir k"onnen beide Lemmata zusammenfassen:

Satz 199. *Die Geraden und Kreise in der komplexen Ebene $\mathbb{C}$ sind genau die Mengen*

$$K = \{z \in \mathbb{C} |\, e\,z\bar{z} + f z + \bar{f}\bar{z} + g = 0\}$$

mit $e, g \in \mathbb{R}$, $f \in \mathbb{C}$ und $f\,\bar{f} > e\,g$.

Beweis. Die Geradendarstellungen von Lemma 197 lassen sich mit $e = 0$ in die hier betrachtete Form "uberf"uhren. Die Kreisdarstellungen entsprechend mit $e = 1$.

Umgekehrt sei $K = \{z \in \mathbb{C} |\, e\,z\bar{z} + f z + \bar{f}\bar{z} + g = 0\}$ mit $e, g \in \mathbb{R}$, $f \in \mathbb{C}$ und $f\,\bar{f} > e\,g$.

Fall 1. $e = 0$. Dann ist $f\,\bar{f} > e\,g = 0$ und $f \neq 0$. Damit liegt nach Lemma 197 eine Gerade vor.

Fall 2. $e \neq 0$. Dann kann man die Bedingung durch e dividieren und

$$K = \left\{ z \in \mathbb{C} |\, z\bar{z} + \frac{f}{e} z + \frac{\bar{f}}{e}\bar{z} + \frac{g}{e} = 0 \right\}$$

mit $\frac{f}{e} \in \mathbb{C}$, $\frac{g}{e} \in \mathbb{R}$ und

$$\frac{f}{e}\,\frac{\bar{f}}{e} > \frac{e\,g}{e\,e} = \frac{g}{e}.$$

Damit liegt ein Kreis vor. □

Angesichts dieses Satzes kann man Geraden auch als spezielle Kreise ansehen, deren Radius und Mittelpunkt im Unendlichen liegt. Die Menge der *verallgemeinerten Kreise* sei die Menge aller Geraden in $\mathbb{C}$ zusammen mit der Menge aller Kreise von positivem Radius.

25 Die Riemannsche Zahlenkugel

Wir betrachten Transformationen von $\mathbb{C}$, insbesondere bijektive Abbildungen, die Geraden und Kreise erhalten.

F"ur $a \in \mathbb{C} \setminus \{0\}$ ist die komplexe Multiplikation $t: \mathbb{C} \to \mathbb{C}$, $t(z) = a\,z$ eine lineare Abbildung, die aus einer *Streckung* mit dem Faktor $|a|$ und einer *Drehung* um $\arg(a)$ besteht. Diese Transformation bildet verallgemeinerte Kreise auf verallgemeinerte Kreise ab.

F"ur $b \in \mathbb{C}$ besteht die Abbildung $t': \mathbb{C} \to \mathbb{C}$, $t'(z) = a\,z + b$ zus"atzlich aus einer *Verschiebung* oder *Translation* um den Vektor b. Auch t' bildet verallgemeinerte Kreise auf verallgemeinerte Kreise ab.

Bei den Argumenten zum Fundamentalsatz der Algebra hatten wir gesehen, dass Polynomabbildungen $z \to p(z)$ Kreise nicht erhalten, wenn $\operatorname{grad}(p) \geqslant 2$ ist.

25.1 Die komplexe Inversion

Definition 200. *Die Abbildung* $I: \mathbb{C} \setminus \{0\} \to \mathbb{C}$, $I(z) = \frac{1}{z}$ *heißt* Inversion.

Lemma 201. *Die Inversion bildet verallgemeinerte Kreise, die den Nullpunkt nicht enthalten, auf verallgemeinerte Kreise ab.*

Beweis. Sei

$$K = \{z \in \mathbb{C} \mid e\,z\,\bar{z} + f\,z + \bar{f}\,\bar{z} + g = 0\}$$

ein verallgemeinerter Kreis mit $e, g \in \mathbb{R}$, $f \in \mathbb{C}$ und $f\,\bar{f} > e\,g$. Außerdem sei $z \notin K$, was "aquivalent zu $g \neq 0$ ist. Dann ist

$$\begin{aligned} I[K] &= \left\{\frac{1}{z} \mid e\,z\,\bar{z} + f\,z + \bar{f}\,\bar{z} + g = 0\right\} \\ &= \left\{\frac{1}{z} \mid e + \frac{f}{\bar{z}} + \frac{\bar{f}}{z} + \frac{g}{z\,\bar{z}} = 0\right\}, \text{ da } z \neq 0 \text{ sein muss;} \\ &= \left\{\frac{1}{z} \mid g\,\frac{1}{z}\overline{\left(\frac{1}{z}\right)} + \bar{f}\,\frac{1}{z} + f\overline{\left(\frac{1}{z}\right)} + e = 0\right\} \end{aligned}$$

mit $g, e \in \mathbb{R}$, $\bar{f} \in \mathbb{C}$ und $\bar{f}\,f > g\,e$. Der Term $\frac{1}{z}$ durchl"auft $\mathbb{C} \setminus \{0\}$ genau dann wenn z $\mathbb{C} \setminus \{0\}$ durchl"auft. Also ist

$$I[K] = \{w \mid g\,w\,\bar{w} + \bar{f}\,w + f\bar{w} + e = 0\}$$

ein verallgemeinerter Kreis, der 0 nicht enth"alt. □

25.2 Die Riemannsche Zahlenkugel

Der Punkt 0 spielt eine besondere Rolle bei der Inversion I. Ein verallgemeinerter Kreis, der 0 enth"alt, kann an der Stelle 0 nicht durch I abgebildet werden, da der Term $\frac{1}{0}$ nicht definiert ist. Sei

$$K = \{z \in \mathbb{C} \mid e\,z\,\bar{z} + f\,z + \bar{f}\,\bar{z} + g = 0\}$$

ein verallgemeinerter Kreis mit $e, g \in \mathbb{R}$, $f \in \mathbb{C}$ und $f\bar{f} > e\,g$, der 0 enth"alt: $0 \in K$. Daraus folgt $g = 0$, $f\bar{f} > 0$ und $f \neq 0$. Die Inversion von $K \setminus \{0\}$ ist nach dem Argument des vorangehenden Beweises

$$I[K \setminus \{0\}] = \{w \,|\, 0\,w\,\bar{w} + \bar{f}\,w + f\bar{w} + e = 0\} = \{w \,|\, \bar{f}\,w + f\bar{w} + e = 0\},$$

also eine Gerade. Umgekehrt ist die Inversion einer Gerade ein Kreis durch 0, aus der der Punkt 0 herausgenommen ist.

Wir wollen eine Erweiterung des Zahlbereichs $\mathbb{C}$ vornehmen, so dass die Inversion der 0 erkl"art ist. Dies wird durch Hinzuf"ugen eines *unendlich fernen Punktes* ∞ erreicht.

Definition 202. *Sei ∞ ("Unendlich") ein neues Symbol. Die Riemannsche Zahlenkugel $\hat{\mathbb{C}}$ ist definiert als*

$$\hat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}.$$

Die arithmetischen Operationen von $\mathbb{C}$ werden auf $\hat{\mathbb{C}}$ durch folgende Definitionen erweitert:

- *f"ur $z \in \mathbb{C}$ ist $z \pm \infty = \infty \pm z = \infty$;*
- *f"ur $z \in \mathbb{C} \setminus \{0\}$ ist $z \cdot \infty = \infty \cdot z = \infty$, $\frac{z}{\infty} = 0$ und $\frac{z}{0} = \infty$.*
- *Die Ausdr"ucke $\infty \pm \infty$, $0 \cdot \infty$ und $\frac{\infty}{\infty}$ sind* nicht *definiert.*

Damit k"onnen wir die Inversion auf die Riemannsche Zahlenkugel erweitern:

Definition 203. *Die Abbildung $I\colon \hat{\mathbb{C}} \to \hat{\mathbb{C}}$, $I(z) = \frac{1}{z}$ heißt* Inversion.

Wir vereinbaren außerdem, dass jede Gerade in $\hat{\mathbb{C}}$ den Punkt ∞ enth"alt.

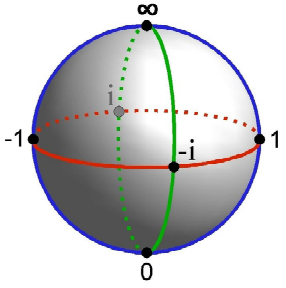
Lemma 204. *Die Inversion ist eine Bijektion der Riemannschen Zahlenkugel: $I\colon \hat{\mathbb{C}} \leftrightarrow \hat{\mathbb{C}}$. Die Inversion ist eine* Involution, *d.h. $I \circ I = \mathrm{id}_{\hat{\mathbb{C}}}$.*

Beweis. "Ubung. □

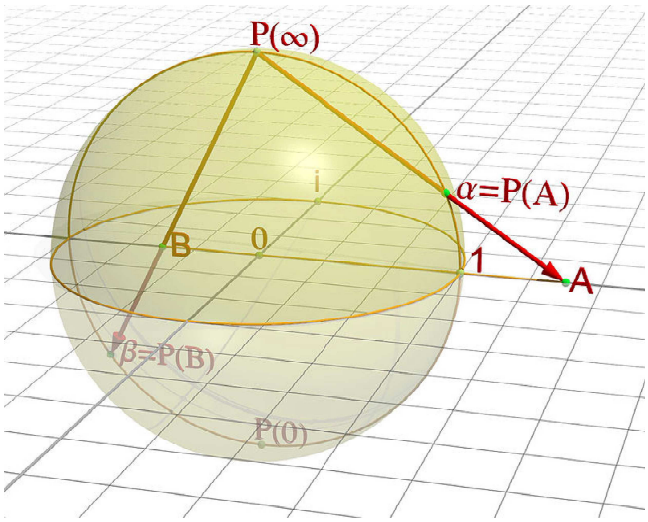
Lemma 205. *Die Inversion bildet verallgemeinerte Kreise auf verallgemeinerte Kreise ab. Geraden werden auf Kreise abgebildet, die die 0 enthalten, und umgekehrt.*

Beweis. "Ubung. □

Der Begriff Zahlen*kugel* l"asst sich durch eine Bijektion zwischen $\hat{\mathbb{C}}$ und einer Kugeloberfl"ache erkl"aren: $\hat{\mathbb{C}}$ entsteht, wenn man die komplexe Ebene um eine (unendlich) große Kugel nach oben zusammengezogen denkt. Das verbleibende Loch wird durch die neue Zahl ∞ gef"ullt.



Die *stereographische Projektion* vom "Nordpol" $P(\infty)$ auf die "Aquatorialebene ist eine Bijektion zwischen der Kugeloberfl"ache ohne Nordpol und $\mathbb{C}$. Wenn man $P(\infty)$ nach ∞ abbildet, erh"alt man eine Bijektion zwischen der gesamten Kugeloberfl"ache und $\hat{\mathbb{C}}$.



(Von Jean-Christophe BENOIST - Eigenes Werk. Merci à Friedrich A. Lohmüller pour sa bibliothèque POV., CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=2199313)

Anmerkung 206. Wir haben das Zahlsystem $\mathbb{C}$ durch Hinzuf'ugen einer neuen Zahl ∞ zum Zahlsystem $\hat{\mathbb{C}}$ erweitert. Diese Erweiterung war dadurch motiviert, die Inversion bijektiv zu machen. Allerdings verliert der Zahlbereich durch das Element ∞ wichtige algebraische Eigenschaften: ∞ hat kein multiplikatives Inverses, wir k"onnen nicht $0 \cdot \infty = 1$ setzen und dann wie in einem K"orper weiter rechnen.

Es ist sinnvoll, die Zahl ∞ als *Unendlich* zu bezeichnen, etwa weil $\frac{1}{0} = \infty$ ist, oder weil man sich ∞ als den unendlich weit entfernten "Fluchtpunkt" auf jeder Gerade vorstellen kann.

Wir hatten bereits andere Unendlichkeiten behandelt: die Menge $\mathbb{N}$ der nat"urlichen Zahlen ist unendlich, ihre Anzahl (oder Kardinalit"at) war durch das Unendlichkeitssymbol $\aleph_0$ bezeichnet worden:

$$\aleph_0 = |\mathbb{N}| .$$

Man beachte, dass es Beziehungen zwischen den verschiedenen Unendlichkeiten geben kann, aber dass man sie trotzdem nicht gleichsetzen darf:

$$\aleph_0 \neq \infty$$