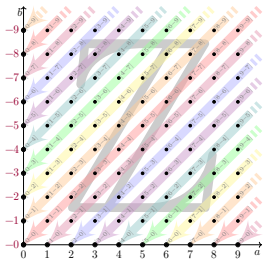
Kapitel B

Aufbau des Zahlensystems

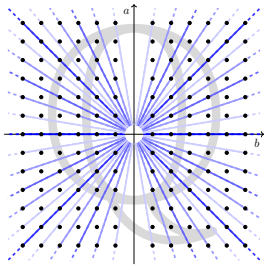
$$\mathbb{N} \hookrightarrow \mathbb{Z} \hookrightarrow \mathbb{Q} \hookrightarrow \mathbb{R} \hookrightarrow \mathbb{C} \hookrightarrow \mathbb{H}$$

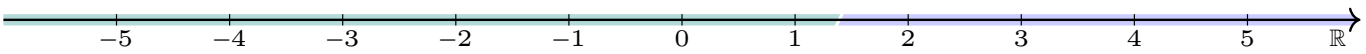
$(\mathbb{N}, 0, s)$: $0 \overset{s}{\mapsto} 1 \overset{s}{\mapsto} 2 \overset{s}{\mapsto} 3 \overset{s}{\mapsto} 4 \overset{s}{\mapsto} 5 \overset{s}{\mapsto} 6 \overset{s}{\mapsto} 7 \overset{s}{\mapsto} 8 \overset{s}{\mapsto} 9 \overset{s}{\mapsto} \dots$



Bitte vergiss alles, was Du auf der Schule gelernt hast; denn Du hast es nicht gelernt. Bitte denke bei allem an das Schulpensum; denn Du hast es doch nicht vergessen.

Edmund Landau (1877–1938)

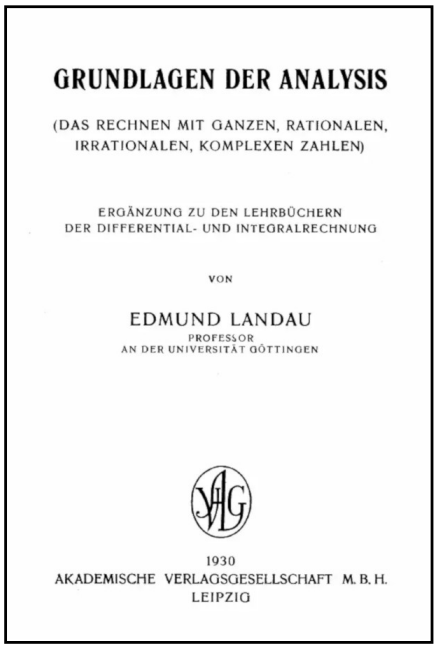


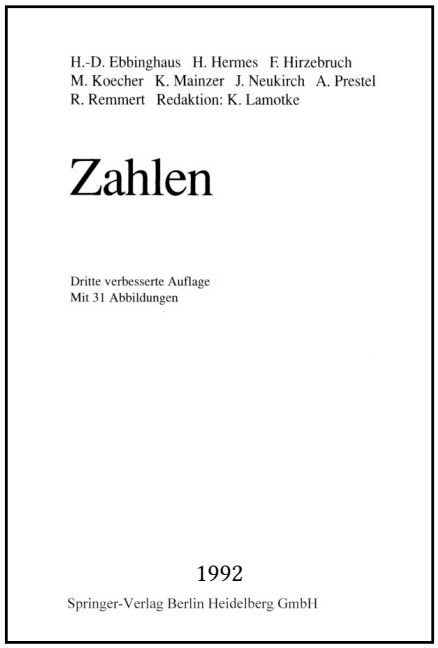


Inhalt dieses Kapitels B

Was sind und was sollen die Zahlen?

Seit Urzeiten nutzen Menschen Zahlen und entwickeln das Rechnen.
Doch was genau sind Zahlen? Und wie entstehen die Rechenregeln?





Bitte vergiss alles, was Du auf der Schule gelernt hast; denn Du hast es nicht gelernt. Bitte denke bei allem an die entsprechenden Stellen des Schulpensums; denn Du hast es doch nicht vergessen. (E. Landau, Vorwort für den Lernenden)

Was sind und was sollen die Zahlen?

Allen ernsthaften Studierenden der Mathematik empfehle ich,
lieber früher als später, den Aufbau des Zahlensystems zu studieren.

Richard Dedekind hat sich in den Jahren 1872–1888 gründlichst mit dem Aufbau der natürlichen Zahlen und ihrer Arithmetik auseinandergesetzt. Als logische Grundlage für sein Unterfangen nutzte er gewinnbringend die damals gerade entstehende Mengenlehre. Diese trägt bis heute!

Auch Edmund Landaus Lehrbuch von 1930 ist ein Klassiker. Hier wurde erstmals der Aufbau des Zahlensystems von den natürlichen Zahlen $\mathbb{N}$ zu den rationalen $\mathbb{Q}$, den reellen $\mathbb{R}$ und schließlich den komplexen Zahlen $\mathbb{C}$ systematisch und präzise ausgeführt. Es ist berühmt für Landaus (von ihm selbst so genannten) „unbarmherzigen Telegrammstil“ und oft zitiert dank seiner beiden prägnanten Vorworte, „Vorwort für den Lernenden“ und „Vorwort für den Kenner“. Auch heute noch erhellend!

Beide Klassiker sind in kommentierten Neuauflagen gut zugänglich. Heutige Studierende finden vielleicht neuere Lehrbücher sympathischer. Ich empfehle das wunderschöne Buch *Zahlen* von Ebbinghaus *et al.*

Aufbau des Zahlensystems $\mathbb{N} \hookrightarrow \mathbb{Z} \hookrightarrow \mathbb{Q} \hookrightarrow \mathbb{R} \hookrightarrow \mathbb{C}$

Die Grundlage aller Mathematik und Anwendung ist das Zahlensystem:

natürliche Zahlen	$\mathbb{N} = \{0, 1, 2, 3, \dots\}$
ganze Zahlen	$\mathbb{Z} = \{a - b \mid a, b \in \mathbb{N}\}$
rationale Zahlen	$\mathbb{Q} = \{z/n \mid z, n \in \mathbb{Z},\ n \neq 0\}$
reelle Zahlen	$\mathbb{R} =$ „$\mathbb{Q}$ und alle Grenzwerte“
komplexe Zahlen	$\mathbb{C} = \{x + \mathrm{i}y \mid x, y \in \mathbb{R}\}$

Wie können Sie diese Zahlbereiche *definieren* und dann *konstruieren*?
ihre Rechenregeln *formulieren* und ihre Eigenschaften *beweisen*? auf einem Computer korrekt *implementieren* bzw. effizient *approximieren*?
Wie können Sie dies selbst *verstehen* und dann anderen *vermitteln*?

Als logisches Fundament und geeignete Sprache nutzen wir die Mengenlehre – für das Zahlensystem wie auch für alles Weitere.
Ich fasse hier in knappen Worten, doch präzise die grundlegenden Rechenregeln zusammen, die Sie im ersten Semester gelernt haben.

Aufbau des Zahlensystems $\mathbb{N} \hookrightarrow \mathbb{Z} \hookrightarrow \mathbb{Q} \hookrightarrow \mathbb{R} \hookrightarrow \mathbb{C}$

Satz B1A: Existenz und Eindeutigkeit von $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$

(0) Die **natürlichen Zahlen** $(\mathbb{N}, +, 0, \cdot, 1)$ sind ein kommutativer Halbring, und $(\mathbb{N}, 0, s : n \mapsto n + 1)$ erfüllt die Dedekind–Peano–Axiome.

(1) Die **ganzen Zahlen** $(\mathbb{Z}, +, 0, \cdot, 1)$ sind ein Integritätsring mit $\mathbb{Z} \supseteq \mathbb{N}$ und entstehen durch Differenzbildung gemäß $\mathbb{Z} = \{a - b \mid a, b \in \mathbb{N}\}$.

(2) Die **rationalen Zahlen** $(\mathbb{Q}, +, 0, \cdot, 1)$ sind ein Körper mit $\mathbb{Q} \supseteq \mathbb{Z}$ und entstehen durch Bruchbildung gemäß $\mathbb{Q} = \{z/n \mid z, n \in \mathbb{Z},\ n \neq 0\}$.

(3) Die **reellen Zahlen** $(\mathbb{R}, +, 0, \cdot, 1)$ sind ein Körper mit $\mathbb{R} \supseteq \mathbb{Q}$ und vollständig geordnet durch $x \leq y \ \Leftrightarrow\ \exists a \in \mathbb{R} : x + a^2 = y$.

(4) Die **komplexen Zahlen** $(\mathbb{C}, +, 0, \cdot, 1)$ sind ein Körper mit $\mathbb{C} \supseteq \mathbb{R}$, wobei $\mathbb{C} = \mathbb{R}[\mathrm{i}] = \{x + \mathrm{i}y \mid x, y \in \mathbb{R}\}$ mit $\mathrm{i} \in \mathbb{C}$ und $\mathrm{i}^2 = -1$.

(5) Die so definierten Objekte $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ existieren: Es gibt Modelle.
Je zwei Modelle sind isomorph, sogar eindeutig isomorph für $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$.

Die komplexen Zahlen $\mathbb{C}$ erlauben über $\mathbb{R}$ genau zwei Automorphismen $\mathrm{id}_{\mathbb{C}}, \mathrm{conj}_{\mathbb{C}} : \mathbb{C} \to \mathbb{C} : x + \mathrm{i}y \mapsto x \pm \mathrm{i}y$, genannt Identität und Konjugation.

Aufbau des Zahlensystems $\mathbb{N} \hookrightarrow \mathbb{Z} \hookrightarrow \mathbb{Q} \hookrightarrow \mathbb{R} \hookrightarrow \mathbb{C}$

Ich wünsche mir, dass Sie den Aufbau des Zahlensystems kennen. Schwache Version: Sie verstehen die obigen Definitionen und können damit arbeiten. Das ist meistens der Fall, und darauf werde ich bauen, wir werden im Folgenden diese Strukturen nutzen. Sie sollen daher verstehen, was diese Definitionen genau sagen, und sich überzeugen, dass sie die vertrauten Zahlbereiche zutreffend beschreiben.

Starke Version: Sie haben den Aufbau Schritt für Schritt durchgeführt, also die zugehörigen Konstruktionen und Beweise detailliert ausgeführt. Das ist meist nicht der Fall. Ich bedaure das, werde es aber hier nicht heilen können. Am Anfang des Studiums kann man diese Konstruktion vermutlich nicht recht würdigen, und später im Studium machen sich die meisten dann andere Sorgen. Das ist unglücklich, aber leider typisch.

Ich begnüge mich daher hier mit einer Erinnerung bzw. einem Appell. Das ist hoffentlich verschmerzlich und folgt dem historischen Vorbild: Mit jedem Zahlbereich wurde lange gerechnet, ehe er begründet wurde. Wenn Sie bereit dazu sind, studieren Sie gründlich – die Grundlagen!

Aufbau des Zahlensystems $\mathbb{N} \hookrightarrow \mathbb{Z} \hookrightarrow \mathbb{Q} \hookrightarrow \mathbb{R} \hookrightarrow \mathbb{C}$

Übung zur Wiederholung: Was bedeuten diese algebraischen Begriffe, kommutativer Halb/Ring, Divisionsring und Körper? Homomorphismen?

Was ist ein geordneter Körper? Was bedeutet hier Vollständigkeit? Welche äquivalenten Formulierungen kennen Sie hierfür?

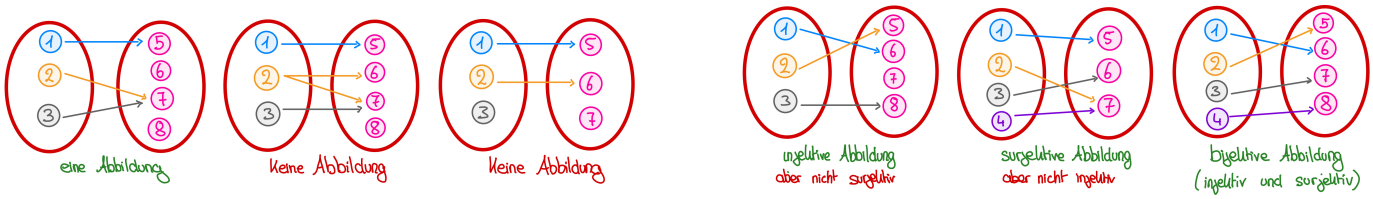
Warum existieren die genannten Objekte? Wie konstruieren Sie diese? Warum sind sie eindeutig? Wie konstruieren Sie die Isomorphismen?

🙂 Der obige zusammenfassende Satz ist eine konzise Erinnerung und definiert eine klare Schnittstelle, auf der wir im Folgenden aufbauen.

```
from __experience__ import numbersystem
from __firstyear__  import numbersystem
from __future__     import numbersystem
```

🙂 Vielleicht überkommt Sie nun doch die mathematische Neugier… Ich empfehle das wunderschöne Buch *Zahlen* von Ebbinghaus *et al.*

Schon der Aufbau des Zahlensystems zeigt uns eindringlich:
Wir benötigen solide Grundlagen in Logik und Mengenlehre!
Diese benötigen wir überall, insbesondere in der Topologie.



This is not to say that the contents of this book are unusually difficult or profound. What is true is that the concepts are very general and very abstract, and that, therefore, they may take some getting used to. […]

The student's task in learning set theory is to steep himself in unfamiliar but essentially shallow generalities till they become so familiar that they can be used with almost no conscious effort.

Paul Halmos (1916–2006), *Naive set theory*

Übung zur Wiederholung: Was genau besagt Russels Antinomie? Warum ist sie eine logische Katastrophe? Wie lösen wir diese ernste Grundlagenkrise durch Rechenregeln / Axiome für die Mengenlehre?

Was ist eine Relation? eine Funktion? Wie erklären Sie ihre Komposition? Was bedeutet injektiv, surjektiv, bijektiv? Wie verhält sich dies zu Links/Rechts/Inversen? Wo benötigen Sie dazu das Auswahlaxiom?

Wie faktorisieren Sie eine Funktion über eine Injektion? eine Surjektion? Was bedeutet eine Funktion ist „wohldefiniert"? Was kann schiefgehen? Was ist also immer zu prüfen, wenn Sie eine Funktion definieren?

Was bedeutet Äquivalenzrelation? Was ist der zugehörige Quotient? Was ist ein Repräsentantensystem? eine wohldefinierte Eigenschaft? Nennen Sie prominente Beispiele, auch aus Schulmathematik und Alltag.

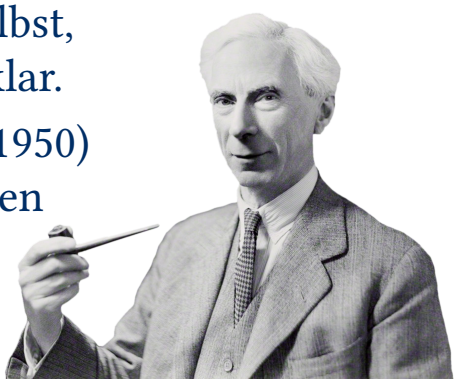
Was ist eine Ordnungsrelation? eine Präordnung? total vs partiell? kleinstes/größtes Element vs minimale/maximale Elemente? Infimum/Supremum? Nennen Sie aussagekräftige Gegen/Beispiele!

Grundlagenkrise: Russels Antinomie (1903)

Für jede Menge x gilt: Entweder enthält x sich selbst, geschrieben $x \in x$, oder nicht, $x \notin x$. So weit, so klar.

Bertrand Russel (1872–1970, Literaturnobelpreis 1950) veröffentlichte 1903 folgende Antinomie der naiven Mengenlehre: Wir untersuchen die Klasse

$$\mathscr{R} = \{ x \mid x \notin x \}.$$



Für jede Menge x gilt $x \in \mathscr{R} \Leftrightarrow x \notin x$. Ist $\mathscr{R}$ eine Menge? Falls ja, so folgt $\mathscr{R} \in \mathscr{R} \Leftrightarrow \mathscr{R} \notin \mathscr{R}$. Logische Katastrophe: Wahr und Falsch sind äquivalent! Falls die Menge $\mathscr{R}$ existiert, so bricht unsere gesamte Logik zusammen.

☹ Nicht alles, was wir formulieren können, ist tatsächlich sinnvoll.
Einzig möglicher Ausweg: Diese Klasse $\mathscr{R}$ ist gar keine Menge!
Die allzu naive Frage „Gilt $\mathscr{R} \in \mathscr{R}$ oder $\mathscr{R} \notin \mathscr{R}$?“ ist damit sinnlos.

🙂 Wir müssen die Konstruktion von Mengen reglementieren!
So restriktiv wie nötig, um Paradoxien wie die obige zu vermeiden.
So expressiv wie möglich, um alles zu formulieren, was wir brauchen.

Die Zermelo–Fraenkel–Axiome: ZF+AC = ZFC

Wir arbeiten in einem Mengenuniversum $(\mathscr{U}, \in, =, \{\}, \bigcup, \mathfrak{P}, \mathfrak{A}_\bullet, \mathfrak{B}_\bullet, \omega, \mathfrak{C})$.
Auf dieser virtuellen Maschine führen wir die gesamte Mathematik aus.

(ZF0) **Fundierung:** In $(\mathscr{U}, \in)$ ist jede Kette $M_0 \ni M_1 \ni M_2 \ni \dots$ endlich.

(ZF1) **Extensionalität:** Für $A, B \in \mathscr{U}$ gilt $A = B$, falls $A \subseteq B$ und $A \supseteq B$.

(ZF2) **Aufzählung:** Zu $a_1, \dots, a_n \in \mathscr{U}$ existiert $\{a_1, \dots, a_n\} \in \mathscr{U}$.

(ZF3) **Vereinigung:** Zu jeder Menge $S \in \mathscr{U}$ existiert $\bigcup S \in \mathscr{U}$.

(ZF4) **Potenz:** Zu jeder Menge $A \in \mathscr{U}$ existiert $\mathfrak{P}(A) \in \mathscr{U}$.

(ZF5) **Aussonderung:** Zu jedem Prädikat $\varphi : \mathscr{U} \to \{0, 1\}$ und jeder Menge $B \in \mathscr{U}$ existiert die Aussonderungsmenge $A = \{ x \in B \mid \varphi(x) \} \in \mathscr{U}$.

(ZF6) **Ersetzung:** Zu jeder Zuordnung $f : \mathscr{U} \to \mathscr{U}$ und jeder Menge $A \in \mathscr{U}$ existiert die Ersetzungsmenge $B = \{ f(x) \mid x \in A \} \in \mathscr{U}$.

(ZF7) **Unendlichkeit:** Es existiert die unendliche Menge $\omega \in \mathscr{U}$ erzeugt durch $\emptyset \in \omega$ und rekursiv $\forall n \in \omega : (n \cup \{n\}) \in \omega$.

(ZF8) **Auswahl:** Die Zuordnung $\mathfrak{C} : \mathscr{U}^* \to \mathscr{U} : a \mapsto x$ erfüllt $x \in a$.

Übung: Explizieren Sie die Definition aller hier verwendeten Begriffe!

Wie vergleichen wir die Größe von Mengen?

Definition B2Q: Mächtigkeit von Mengen

Die Mächtigkeit von Mengen X und Y vergleichen wir wie folgt durch Abbildungen, mit Hilfe von Bijektionen, Injektionen und Surjektionen:

1. Äquipotenz $X \cong Y$ bedeutet, es existiert eine Bijektion $(h, k) : X \cong Y$. Die Mengen X und Y sind gleich groß / gleichmächtig / äquipotent.
2. Die Relation $X \preceq Y$ bedeutet, es existiert eine Injektion $f : X \hookrightarrow Y$. Interpretation: „Die Menge X ist höchstens so groß wie Y."
3. $Y \succeq X$ bedeutet, es existiert eine Surjektion $g : Y \twoheadrightarrow X$ oder $X = \emptyset$. Interpretation: „Die Menge Y ist mindestens so groß wie X."

Gilt $X \cong \{1, \dots, n\}$, so ist X **endlich**, mit Elementezahl $\sharp X = n$.
Gilt $X \cong \mathbb{N}$, so nennen wir die Menge X **abzählbar unendlich**.
Abzählbar bedeutet $X \preceq \mathbb{N}$, das heißt X ist entweder endlich oder abzählbar unendlich; andernfalls ist X **überabzählbar**.

Vor Cantor galten unendliche Mengen als paradox, insbesondere ihre Größenvergleiche. Cantors genial-einfache Definition räumt damit auf.

Wie vergleichen wir die Größe von Mengen?

Beispiel: Im Hörsaal befinden sich weniger Personen (X) als Sitze (Y): Dazu muss ich weder X noch Y zählen, Hinsetzen $X \hookrightarrow Y$ genügt!

Die Relation $X \preceq Y :\Leftrightarrow \exists f : X \hookrightarrow Y$ ist reflexiv dank $\mathrm{id}_X : X \hookrightarrow X$ und transitiv, denn die Komposition zweiter Injektionen ergibt eine Injektion.

Die Relation $Y \succeq X :\Leftrightarrow (\exists g : Y \twoheadrightarrow X) \vee X = \emptyset$ ist äquivalent zu $X \preceq Y$: Zu jeder Surjektion $g : Y \twoheadrightarrow X$ existiert $f : X \hookrightarrow Y$ mit $g \circ f = \mathrm{id}_X$ (AC). Umgekehrt, zu $f : X \hookrightarrow Y$ existiert $g : Y \twoheadrightarrow X$, oder es gilt $X = \emptyset$.

Strikt kleiner: Wie üblich schreiben wir $X \prec Y$ für $X \preceq Y \wedge Y \not\preceq X$.
Strikt größer: Wie üblich schreiben wir $Y \succ X$ für $Y \succeq X \wedge X \not\succeq Y$.

Die Relation $X \cong Y :\Leftrightarrow \exists (h, k) : X \cong Y$ ist reflexiv dank $(\mathrm{id}, \mathrm{id}) : X \cong X$, symmetrisch dank Vertauschung und transitiv dank Komposition.

Satz von Cantor–Bernstein (B2O): Aus $X \preceq Y$ und $Y \preceq X$ folgt $X \cong Y$, denn aus $f : X \hookrightarrow Y$ und $g : Y \hookrightarrow X$ konstruieren wir $(h, k) : X \cong Y$.

Beispiel: Wie ermitteln zwei Kinder, die noch nicht zählen können, wer mehr Legosteine hat? Vergleichbarkeitssatz B2R von Cantor–Zermelo!

Beispiel: endliche Mengen

Für alle natürlichen Zahlen $m, n \in \mathbb{N}$ gelten die vertrauten Beziehungen:

$$\begin{aligned} \{1,\dots,m\} \cong \{1,\dots,n\} &\quad\Leftrightarrow\quad m = n \\ \{1,\dots,m\} \preceq \{1,\dots,n\} &\quad\Leftrightarrow\quad m \leq n \\ \{1,\dots,m\} \prec \{1,\dots,n\} &\quad\Leftrightarrow\quad m < n \end{aligned}$$

Das klingt plausibel und leuchtet sofort ein, verdient aber einen Beweis. Führen Sie zur Wiederholung das Argument per Induktion sorgsam aus. Das bedeutet, dass die Mächtigkeit *endlicher* Mengen genau das leistet, was wir uns erhoffen, nämlich den üblichen Vergleich nach Elementezahl.

Es gilt $\{1,\dots,n\} \prec \mathbb{N}$. Warum? Zunächst haben wir $\mathrm{inc} : \{1,\dots,n\} \hookrightarrow \mathbb{N}$. Umgekehrt, ist $f : \{1,\dots,n\} \to \mathbb{N}$ eine Funktion, so ist f nicht surjektiv. Auch das klingt plausibel und leuchtet sofort ein, verdient aber dennoch einen Beweis. Hierzu betrachten $m = \sup(f) \in \mathbb{N}$. Für $n = 0$ gilt $m = 0$. Für $n \geq 1$ gilt induktiv $m = \max\{\, f(n),\ \sup(f|_{\{1,\dots,n-1\}}) \,\} \in \mathbb{N}$. Das nachfolgende Element $m + 1$ liegt nicht im Bild von f.

Beispiel: Galileis Paradox (1638)

Aufgabe: Ist die Menge $Q = \{0, 1, 4, 9, 16, 25, \dots\}$ der Quadratzahlen kleiner als die Menge $\mathbb{N} = \{0, 1, 2, 3, 4, 5, \dots\}$ der natürlichen Zahlen? Galilei schloss voreilig, dass Größenvergleiche für unendliche Mengen unsinnig sind. Cantor erkannte, dass dies dennoch möglich ist.

Lösung: (1) Im Sinne der Inklusion haben wir $Q \subsetneq \mathbb{N}$.
Im Poset $(\mathfrak{P}(\mathbb{N}), \subseteq)$ ist demnach Q strikt kleiner als $\mathbb{N}$.

(2) Wir haben die Bijektion $(h, k) : \mathbb{N} \cong Q$ mit $h(x) = x^2$ und $k(y) = \sqrt{y}$.
Im Sinne der Mächtigkeit sind beide Mengen demnach gleich groß!

⚠ Die Formulierungen „größer als“ oder „kleiner als“ oder „gleich groß“ sind daher missverständlich, solange der Kontext nicht präzisiert wird. Das Ergebnis hängt entscheidend davon ab, welche Ordnungsrelation wir dabei zu Grunde legen, wie hier an $\subseteq$ und $\preceq$ eindrücklich zu sehen.

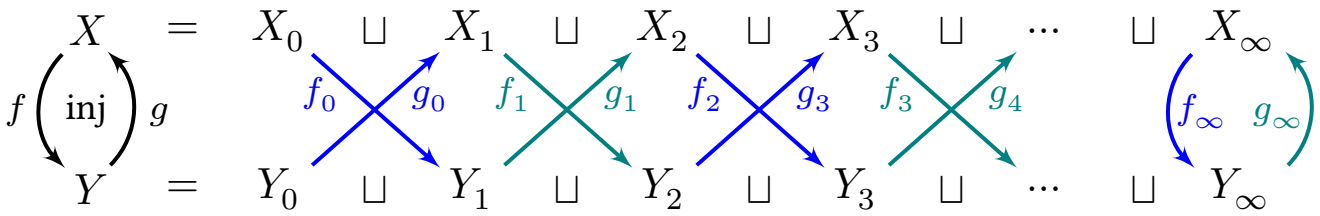
🙂 Um mögliche Missverständnisse zu vermeiden, sagen wir statt *gleich groß* genauer *gleichmächtig* oder *äquipotent* im Sinne der Definition B2Q. Die Mengen $\mathbb{N}$ und Q sind demnach gleichmächtig, sie haben dieselbe **Mächtigkeit**, wir sagen auch: sie haben dieselbe **Kardinalität**.

Der Äquivalenzsatz von Cantor–Bernstein

Satz B2o: Äquivalenzsatz von Cantor–Bernstein

Aus $X \preceq Y$ und $Y \preceq X$ folgt $X \cong Y$. Genauer: Aus Injektionen $f : X \hookrightarrow Y$ und $g : Y \hookrightarrow X$ konstruieren wir explizit eine Bijektion $(h, k) : X \cong Y$.

Jedes Element $x_0 \in X$ hat seine Urbildkette $x_0 \overset{f}{\longleftarrow} y_1 \overset{g}{\longleftarrow} x_2 \overset{f}{\longleftarrow} y_3 \overset{g}{\longleftarrow} \dots$ maximaler Länge $n \in \mathbb{N} \cup \{\infty\}$. Die Elemente der Länge n bilden die Menge $X_n \subseteq X$. Entsprechend definieren wir $Y_n \subseteq Y$. Wir erhalten:



Cantors Reißverschluss: Auf $X = \bigsqcup_n X_n$ und $Y = \bigsqcup_n Y_n$ zerlegen wir f und g jeweils in die Bijektionen $f_n : X_n \xrightarrow{\sim} Y_{n+1}$ und $g_n : Y_n \xrightarrow{\sim} X_{n+1}$. So erhalten wir zueinander inverse Bijektionen $(h, k) : X \cong Y$ vermöge $h = f_0 \sqcup g_0^{-1} \sqcup f_2 \sqcup g_2^{-1} \sqcup \dots \sqcup f_\infty$ und $k = g_0 \sqcup f_0^{-1} \sqcup g_2 \sqcup f_2^{-1} \sqcup \dots \sqcup f_\infty^{-1}$.

☺ Cantors Reißverschluss gelingt konstruktiv, ohne das Auswahlaxiom!

Der Äquivalenzsatz von Cantor–Bernstein

Der Äquivalenzsatz B2o hat eine faszinierend turbulente Geschichte. Er wurde 1887 von Georg Cantor formuliert, aber erst zehn Jahre später 1897 bewiesen. Dies gelang dem damals erst 19-jährigen Studenten Felix Bernstein in Cantors Seminar an der Universität Halle. Zeitgleich und unabhängig veröffentlichte Ernst Schröder einen Beweis, der sich jedoch später als fehlerhaft erwies. Bereits 1887 fand Richard Dedekind einen Beweis, den er aber nicht veröffentlichte. Das genial-einfach-konstruktive Reißverschlussverfahren wurde 1906 von Julius König veröffentlicht.

Satz B2o garantiert, dass wir Mengen nach Mächtigkeit ordnen können. Wir definieren die strikte Ordnung $X \prec Y$ durch $X \preceq Y$ und $Y \not\preceq X$ und entsprechend $X \succ Y$ durch $X \succeq Y$ und $Y \not\succeq X$. Demnach gilt also *höchstens* eine der drei Alternativen $X \prec Y$ oder $X \cong Y$ oder $X \succ Y$.

Der Vergleichbarkeitssatz B2R von Cantor–Zermelo vervollständigt dies durch die Aussage, dass sich je zwei Mengen vergleichen lassen; demnach gilt *genau* eine der drei Alternativen $X \prec Y$ oder $X \cong Y$ oder $X \succ Y$. (Letzteres benötigt das Auswahlaxiom, etwa in Form von Zorns Lemma.)

Der Äquivalenzsatz von Cantor–Bernstein

Beweis: Gegeben sind $f : X \hookrightarrow Y$ und $g : Y \hookrightarrow X$. Die beiden Mengen

$$X_0 := X \setminus g(Y) \quad \text{und} \quad Y_0 := Y \setminus f(X)$$

enthalten alle Elemente ohne Urbild. Per Rekursion enthalten

$$X_{n+1} := g(Y_n) \quad \text{und} \quad Y_{n+1} := f(X_n)$$

alle Elemente mit Urbildfolge der Länge $n+1$. Schließlich enthalten

$$X_\infty := \bigcap\nolimits_{\ell\in\mathbb{N}} (g\circ f)^\ell(X) \quad \text{und} \quad Y_\infty := \bigcap\nolimits_{\ell\in\mathbb{N}} (f\circ g)^\ell(Y)$$

alle Elemente mit unendlicher Urbildfolge. Wir definieren

$$h : X \to Y : x \mapsto \begin{cases} f(x) & \text{für } x \in \bigsqcup_{\ell\in\mathbb{N}} X_{2\ell} \sqcup X_\infty, \\ y & \text{für } x = g(y) \in \bigsqcup_{\ell\in\mathbb{N}} X_{2\ell+1}, \end{cases}$$

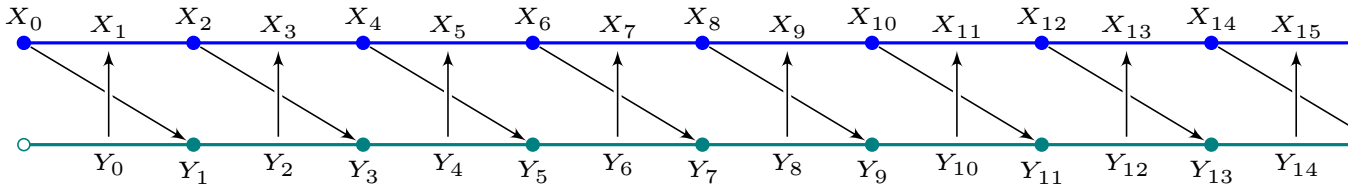
$$k : Y \to X : y \mapsto \begin{cases} x & \text{für } y = f(x) \in \bigsqcup_{\ell\in\mathbb{N}} Y_{2\ell+1} \sqcup Y_\infty, \\ g(y) & \text{für } y \in \bigsqcup_{\ell\in\mathbb{N}} Y_{2\ell}. \end{cases}$$

Damit gilt $k \circ h = \mathrm{id}_X$ und $h \circ k = \mathrm{id}_Y$, wie gewünscht. QED

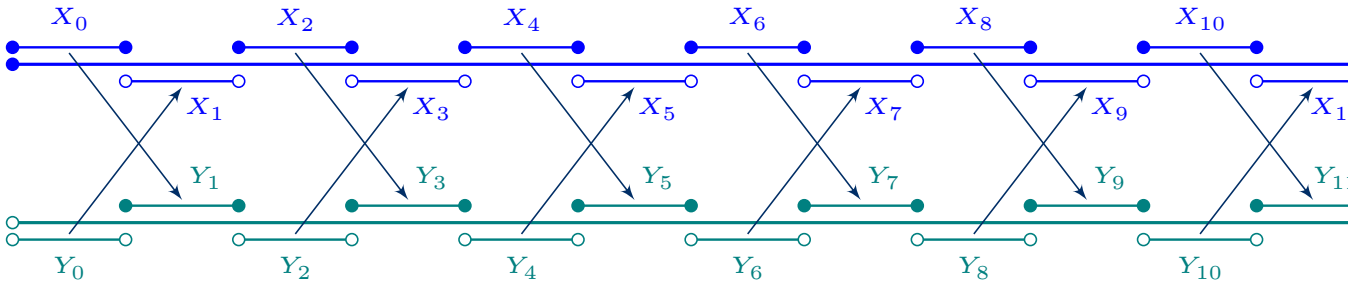
Der Äquivalenzsatz von Cantor–Bernstein

Beispiel: Die Intervalle $X = [0,\infty[$ und $Y =]0,\infty[$ sind gleichmächtig.

Beweis: Wir haben $f : X \hookrightarrow Y : x \mapsto x+1$ und $g = \mathrm{inc} : Y \hookrightarrow X : y \mapsto y$. Cantor–Bernstein konstruiert daraus die Bijektion $(h,k) : X \cong Y$ mit $(h,k) : \mathbb{N} \cong \mathbb{N}_{\geq 1} : x \leftrightarrow x+1$ und $h(x) = k(x) = x$ für $x \notin \mathbb{N}$. Skizze:



Alternative: Wir nutzen $f : x \mapsto x+1$ und $g : y \mapsto y+1$. Skizze:



Beispiel: Die Intervalle $X = [0,3]$ und $Y = [0,2[$ sind gleichmächtig vermöge $f : X \hookrightarrow Y : x \mapsto x/2$ und $g : Y \hookrightarrow X : y \mapsto y$. Siehe Satz B2L.

Mächtigkeit der Primzahlmenge

Aufgabe: Ist die Menge $\mathbb{P} = \{2, 3, 5, 7, 11, 13, \dots\}$ der Primzahlen strikt kleiner als die Menge $\mathbb{N} = \{0, 1, 2, 3, 4, 5, \dots\}$ der natürlichen Zahlen?

Lösung: (1) Im Sinne der Inklusion haben wir $\mathbb{P} \subsetneq \mathbb{N}$.
Im Poset $(\mathfrak{P}(\mathbb{N}), \subseteq)$ ist demnach $\mathbb{P}$ strikt kleiner als $\mathbb{N}$.

(2) Dennoch existiert eine Bijektion $(h, k) : \mathbb{N} \cong \mathbb{P}$.
Im Sinne der Mächtigkeit sind beide Mengen gleich groß!

Ausführliche Konstruktion: Dank Satz ?? ist die Menge $\mathbb{P}$ unendlich.
Ihre Elemente können wir aufsteigend anordnen zu $p_0 < p_1 < p_2 < \dots$.
Dies stiftet die (kanonische, isotone) Bijektion $h : \mathbb{N} \rightarrowtail \mathbb{P} : n \mapsto p_n$.

🙂 Computer-Algebra-Systeme implementieren diese Abbildung $h : \mathbb{N} \rightarrowtail \mathbb{P}$ als eine Funktion, etwa `Prime[n]` oder `ithprime(n)`.

⚠ Die Bijektion $h : \mathbb{N} \rightarrowtail \mathbb{P}$ ist leicht zu *definieren*, aber aufwändig zu *berechnen*. Beispiele: Was ist $h(1000)$? $h(10^6)$? $h(10^9)$? $h(10^{12})$?
Immerhin haben wir explizite und recht genaue Schranken für das Wachstum dieser Funktion $h : \mathbb{N} \to \mathbb{P} \subseteq \mathbb{N}$ (Primzahlsatz).

Mächtigkeit der Primzahlmenge

Woher wissen wir, dass es wirklich *unendlich* viele Primzahlen gibt?
Das ist ein Satz… wir haben einen Beweis… sogar eine Konstruktion:
Zu je gegebenen Primzahlen $p_0, \dots, p_n$ liefert Euklids Konstruktion

$$p_{n+1} := \operatorname{lpf}(p_0 \cdots p_n + 1)$$

eine weitere Primzahl. So erhalten wir eine Injektion $f : \mathbb{N} \hookrightarrow \mathbb{P} : n \mapsto p_n$.
Es gibt jedoch keinen Grund, dass diese Abbildung f zudem surjektiv ist.
Wir haben also nur eine Injektion $f : \mathbb{N} \hookrightarrow \mathbb{P}$, das ist schon viel wert.
Umgekehrt liefert die Inklusion $\mathbb{P} \subseteq \mathbb{N}$ gratis eine Injektion $g : \mathbb{P} \hookrightarrow \mathbb{N}$.

Wäre es nicht schön, wenn wir allgemein aus Injektionen $f : X \hookrightarrow Y$ und $g : Y \hookrightarrow X$ eine Bijektion $(h, k) : X \cong Y$ konstruieren könnten?
Genau das leistet der Äquivalenzsatz B2o von Cantor–Bernstein, ebenso einfach wie elegant, ebenso konstruktiv wie explizit.

Zugegeben, die Bijektion $\mathbb{P} \cong \mathbb{N}$ ist dazu nur ein allzu einfaches Beispiel, das wir leicht auch anders lösen können, ganz konkret wie oben gezeigt.
Doch es illustriert den konstruktiven Nutzen des Äquivalenzsatzes.

Der Vergleichbarkeitssatz von Cantor–Zermelo

Ist die Relation $\preceq$ total? Lassen sich also je zwei Mengen X und Y vergleichen gemäß $X \preceq Y$ oder $Y \preceq X$? Das scheint plausibel, erfordert aber einen Beweis. Für endliche Mengen gelingt dies durch Abzählung, für beliebige unendliche Mengen benötigen wir das Auswahlaxiom!

Satz B2R: Vergleichbarkeitssatz von Cantor–Zermelo

Zu je zwei Mengen X und Y existiert eine Injektion $X \hookrightarrow Y$ oder $Y \hookrightarrow X$.

Beweis: Eine **partielle Bijektion** zwischen X und Y ist eine Bijektion $(h, k) : A \cong B$ zwischen $A \subseteq X$ und $B \subseteq Y$, also $k \circ h = \mathrm{id}_A$ und $h \circ k = \mathrm{id}_B$. Wir definieren $(h, k) \subseteq (h', k')$ durch $A \subseteq A'$ und $B \subseteq B'$ sowie $h(x) = h'(x)$ für alle $x \in A$ und $k(y) = k'(y)$ für alle $y \in B$.

Ist S eine Kette partieller Bijektionen, so ist auch ihre Vereinigung $\bigcup S$ eine partielle Bijektion. Wir können das Lemma von Zorn anwenden: Es existiert eine maximale partielle Bijektion $(h, k) : A \cong B$.

Wäre $A \subsetneq X$ und $B \subsetneq Y$, so könnten wir (h, k) fortsetzen. Also gilt $A = X$ und somit $h : X \hookrightarrow Y$, oder es gilt $B = Y$ und somit $k : Y \hookrightarrow X$. QED

Der Vergleichbarkeitssatz von Cantor–Zermelo

Der Vergleich $X \preceq Y$ von Mengen ist eine Präordnung, da reflexiv und transitiv. Nach dem Äquivalenzsatz von Cantor–Bernstein ist er zudem antisymmetrisch bis auf Bijektion: Aus $X \preceq Y$ und $Y \preceq X$ folgt $X \cong Y$. Wir stellen nun erfreut fest, dass der Vergleich total ist.

Der Vergleichbarkeitssatz B2R von Cantor–Zermelo ist zwar hilfreich, doch notgedrungen nicht-konstruktiv: Er benötigt das Auswahlaxiom, im oben angegebenen Beweis in Form von Zorns Lemma.

Wenn wir also die Mächtigkeit von zwei Mengen vergleichen wollen, so garantiert dieser Satz, dass der Vergleich im Prinzip immer gelingt, gibt uns aber keinen Hinweis, wie dies konkret zu bewerkstelligen sei.

Der Äquivalenzsatz B2O von Cantor–Bernstein hingegen benötigt nicht das Auswahlaxiom: Das oben angegebene Reißverschlussverfahren ist konstruktiv, aus $(f, g) : X \rightleftarrows Y$ konstruieren wir explizit $(h, k) : X \cong Y$.

Wenn wir also die Gleichmächtigkeit von zwei Mengen zeigen wollen, so genügt es, gegenseitige Injektionen herzustellen. Das ist oft wesentlich einfacher und wird uns in der praktischen Anwendung oft nützen.

Mächtigkeit der ganzen Zahlen $\mathbb{Z}$

Satz B2A: $\mathbb{Z}$ ist abzählbar.

Die Mengen $\mathbb{Z}$ und $\mathbb{N}$ sind gleichmächtig, kurz $\mathbb{Z} \cong \mathbb{N}$.

Beweisidee: Dies gelingt explizit vermöge $(f, g) : \mathbb{N} \cong \mathbb{Z} : a \rightleftarrows b$ mit

$a \in \mathbb{N}$	0	1	2	3	4	5	6	7	8	9	10	...
$b \in \mathbb{Z}$	0	-1	$+1$	-2	$+2$	-3	$+3$	-4	$+4$	-5	$+5$	...

Aufgabe: Formulieren Sie dieses Bijektionspaar explizit.

Lösung: Wir fassen diese Idee in explizite Formeln:

$$f : \mathbb{N} \to \mathbb{Z} : a \mapsto \begin{cases} a/2 & \text{falls } a \in 2\mathbb{N}, \\ -(a+1)/2 & \text{falls } a \in 2\mathbb{N}+1, \end{cases}$$

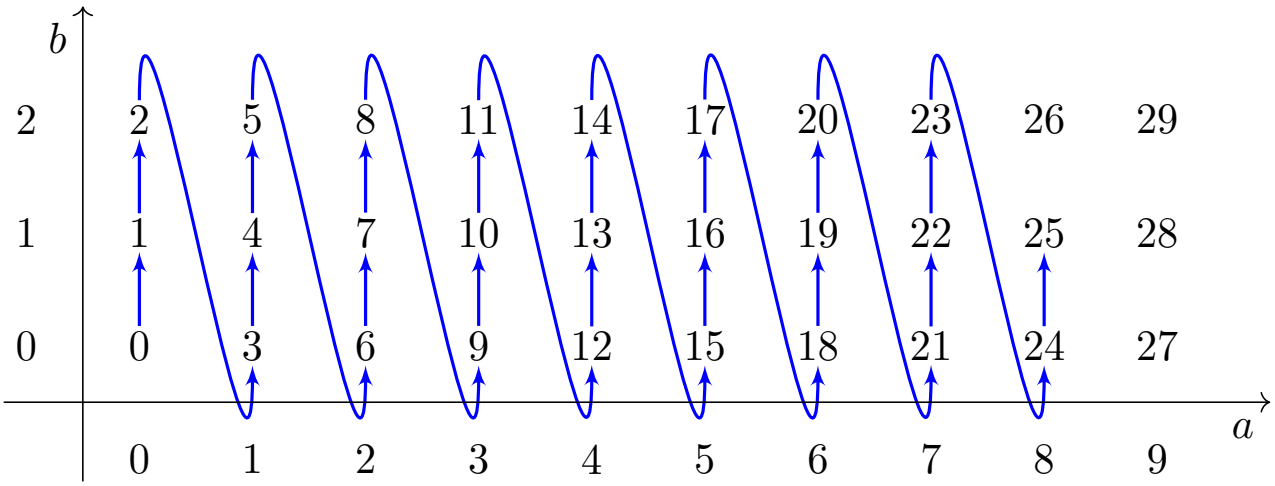
$$g : \mathbb{Z} \to \mathbb{N} : b \mapsto \begin{cases} 2b & \text{falls } b \geq 0, \\ -2b-1 & \text{falls } b < 0. \end{cases}$$

Diese Abbildungen sind wohldefiniert und zueinander invers, es gilt also $g \circ f = \mathrm{id}_{\mathbb{N}}$ und $f \circ g = \mathrm{id}_{\mathbb{Z}}$. Nachrechnen! QED

Mächtigkeit des Produkts $\mathbb{N} \times \{1, \dots, n\}$

Satz B2B: Auch $\mathbb{N} \times \{1, \dots, n\}$ ist abzählbar.

Die Mengen $\mathbb{N} \times \{1, \dots, n\}$ und $\mathbb{N}$ sind gleichmächtig.



Aufgabe: Formulieren Sie dieses Bijektionspaar explizit.

Lösung: Wir nutzen zunächst $\{1, \dots, n\} \cong \{0, \dots, n-1\} : k \rightleftarrows k-1$. Zudem haben wir das Bijektionspaar $(f, g) : \mathbb{N} \times \{0, \dots, n-1\} \cong \mathbb{N}$ mit $f(a, b) = na + b$ und $g(c) = (c \operatorname{quo} n, c \operatorname{rem} n)$. QED

Satz B2c: Grundrechenarten für Mächtigkeiten

Gegeben seien Bijektionen $(\alpha, \alpha') : A \cong A'$ und $(\beta, \beta') : B \cong B'$.
Daraus erhalten wir kanonische Bijektionen für Summe und Produkt:

$$(\alpha \sqcup \beta, \alpha' \sqcup \beta') : A \sqcup B \cong A' \sqcup B',$$
$$(\alpha \times \beta, \alpha' \times \beta') : A \times B \cong A' \times B',$$

Für die Abbildungsmengen erhalten wir die kanonische Bijektion

$$(\varphi, \varphi') : \operatorname{Abb}(A, B) \cong \operatorname{Abb}(A', B')$$

vermöge $\varphi(f) = \beta \circ f \circ \alpha'$ und $\varphi'(f') = \beta' \circ f' \circ \alpha$. Zudem haben wir

$$(\psi, \psi') : (Z^X)^Y \cong Z^{X \times Y} : f \mapsto g$$

vermöge $g(x, y) = f(y)(x)$ für $f : Y \to \operatorname{Abb}(X, Z)$ und $g : X \times Y \to Z$.

Beweis: Diese Abbildungen sind wohldefiniert und zueinander invers:
Alles liegt explizit vor, es genügt sorgsames Nachrechnen! QED

Für die erste Bijektion $A \sqcup B \cong A' \sqcup B'$ setzen wir Disjunktheit voraus, also $A \cap B = A' \cap B' = \emptyset$. Dies können wir immer erzwingen durch

$$(\{1\} \times A) \sqcup (\{2\} \times B) \cong (\{1\} \times A') \sqcup (\{2\} \times B')$$

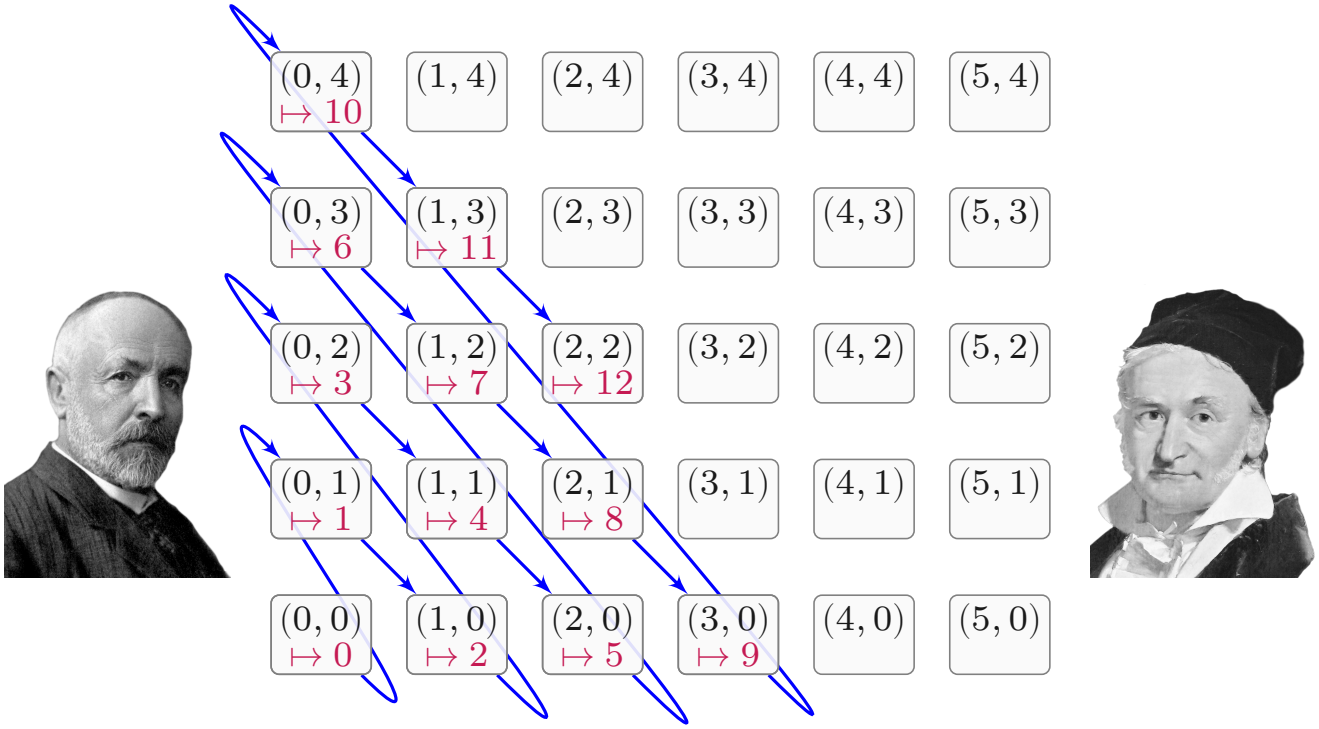
Anschaulich gesagt, wir ersetzen die Menge A durch die Kopie $\{1\} \times A$; zwischen beiden übersetzen wir durch die kanonische Bijektion (ι_2, pr_2). Entsprechend verfahren wir für $\{2\} \times B$ sowie $\{1\} \times A'$ und $\{2\} \times B'$.

Beispiel: Es gilt $(\{1\} \times \mathbb{N}) \sqcup (\{2\} \times \mathbb{N}) = \{1, 2\} \times \mathbb{N} \cong \{0, 1\} \times \mathbb{N} \cong \mathbb{N}$.
Dies ist die Vereinigung von zwei disjunkten Kopien der Menge $\mathbb{N}$,
die Mächtigkeit bleibt dabei gleich, wie oben gesehen (B2B).

Beispiel: Aus $\mathbb{Z} \cong \mathbb{N}$ folgt $\mathbb{Z} \times \mathbb{Z} \cong \mathbb{N} \times \mathbb{N}$ dank B2C.
Wir werden im Folgenden sehen, dass $\mathbb{N}^2 \cong \mathbb{N}$ gilt (??).

Beispiel: Aus $\mathbb{Z} \cong \mathbb{N}$ folgt $\mathbb{Z}^n \cong \mathbb{N}^n$ für alle $n \in \mathbb{N}$ dank B2C.
Wir zeigen im Folgenden $\mathbb{N}^n \cong \mathbb{N}$ für alle $n \in \mathbb{N}_{\geq 1}$ (B2D).

Mächtigkeit des Produkts $\mathbb{N} \times \mathbb{N}$



Es existieren Bijektionen $(f, g) : \mathbb{N}^2 \cong \mathbb{N}$. Sogar verblüffend elegant:

Satz B2A: Cantors erstes Diagonalargument

Die Abbildung $f : \mathbb{N}^2 \to \mathbb{N} : (a, b) \mapsto a + (a + b)(a + b + 1)/2$ ist bijektiv.

Cantors Paarungsfunktion $f : \mathbb{N}^2 \xrightarrow{\sim} \mathbb{N}$

🙂 Es ist höchst erstaunlich, dass uns die Bijektion $f : \mathbb{N}^2 \xrightarrow{\sim} \mathbb{N}$ explizit mit einer so einfachen Funktion gelingt, einem Polynom zweiten Grades!

Aufgabe: Formulieren Sie explizit das Bijektionspaar $(f, g) : \mathbb{N}^2 \cong \mathbb{N}$.

Lösung: Wir übersetzen die obige Skizze in eine Rekursion:

$$g : \mathbb{N} \to \mathbb{N}^2 : \quad g(0) = (0, 0) \text{ und } g(n + 1) = \varphi(g(n)),$$

$$\varphi : \mathbb{N}^2 \to \mathbb{N}^2 : (a, b) \mapsto \begin{cases} (a + 1, b - 1) & \text{falls } b > 0, \\ (0, a + 1) & \text{falls } b = 0. \end{cases}$$

Explizit ausgeschrieben gilt demnach $g : \mathbb{N} \to \mathbb{N}^2 : c \mapsto (a, b)$ mit $s = \max\{ n \in \mathbb{N} \mid n(n + 1)/2 \leq c \}$ und $a = c - s(s + 1)/2$ und $b = s - a$.

Die Umkehrfunktion ist erfreulich einfach (dank dem kleinen Gauß):

$$f : \mathbb{N}^2 \to \mathbb{N} : (a, b) \mapsto a + (a + b)(a + b + 1)/2$$

Diese Abbildungen sind wohldefiniert und zueinander invers, also $g \circ f = \mathrm{id}_{\mathbb{N}^2}$ und $f \circ g = \mathrm{id}_{\mathbb{N}}$. Nachrechnen, per Induktion! QED

Abzählbare Vereinigung abzählbarer Mengen

Die Vereinigung $\bigsqcup_{i\in\mathbb{N}}\{i\}\times\mathbb{N}=\mathbb{N}\times\mathbb{N}$ ist abzählbar dank **??**. Allgemein:

Satz B2B: abzählbare Vereinigung abzählbarer Mengen

Jede abzählbare Vereinigung abzählbarer Mengen ist abzählbar:
Sei I eine abzählbare Indexmenge. Zu jedem Index $i\in I$ sei A_i eine abzählbare Menge. Dann ist auch $A=\bigcup_{i\in I}A_i$ abzählbar.

Beweis: Gegeben seien $f:I\hookrightarrow\mathbb{N}$ und $g_i:A_i\hookrightarrow\mathbb{N}$ für jedes $i\in I$.

$$\begin{array}{ccc} A=\bigcup_{i\in I}A_i & \overset{h}{\dashrightarrow} & \mathbb{N} \\ \mathrm{pr}_2 \uparrow\!\downarrow r & & \uparrow\!\downarrow \mathfrak{K} \\ A'=\bigsqcup_{i\in I}\{i\}\times A_i & \xrightarrow{(i,a)\mapsto(f(i),g_i(a))} & \mathbb{N}\times\mathbb{N} \end{array}$$

Nach Indexwechsel dürfen wir $I\subseteq\mathbb{N}$ annehmen. Eine Rechtsinverse zu $\mathrm{pr}_2:A'\twoheadrightarrow A$ ist $r:a\mapsto(j,a)$ mit $j=\min\{\,i\in I\,|\,a\in A_i\,\}$ dank **??**.
Somit gilt $A\preceq A'\preceq\mathbb{N}\times\mathbb{N}\preceq\mathbb{N}$. Dank Transitivität folgt $A\preceq\mathbb{N}$. QED

Abzählbare Vereinigung abzählbarer Mengen

Korollar B2D: Mächtigkeit von $\mathbb{N}^{(\mathbb{N})}$

(1) Es gilt $\mathbb{N}^n\cong\mathbb{N}$ für jede natürliche Zahl $n\in\mathbb{N}_{\geq 1}$.

(2) Es gilt $\mathbb{N}^{(\mathbb{N})}\cong\mathbb{N}$ für die Menge aller Folgen mit endlichem Träger:

$$\mathbb{N}^{(\mathbb{N})}:=\{\,f:\mathbb{N}\to\mathbb{N}\,\big|\,\sharp\,\mathrm{supp}(f)<\infty\,\}.$$

(3) Hingegen ist die Menge $\mathbb{N}^{\mathbb{N}}=\{\,f:\mathbb{N}\to\mathbb{N}\,\}$ überabzählbar.

Beweis: (1) Induktion über $n\in\mathbb{N}_{\geq 1}$: Für $n=1$ gilt $\mathbb{N}^1\cong\mathbb{N}$.
Für $n\geq 2$ finden wir $\mathbb{N}^n=\mathbb{N}^{n-1}\times\mathbb{N}\cong\mathbb{N}\times\mathbb{N}\cong\mathbb{N}$ dank **??**.

(2) Die Menge $\mathbb{N}^{(\mathbb{N})}$ ist eine abzählbare Vereinigung (**??**) gemäß

$$\mathbb{N}^{(\mathbb{N})}=\bigcup_{n\in\mathbb{N}}\{\,f:\mathbb{N}\to\mathbb{N}\,\big|\,\mathrm{supp}(f)\subseteq\{0,\dots,n\}\,\}.$$

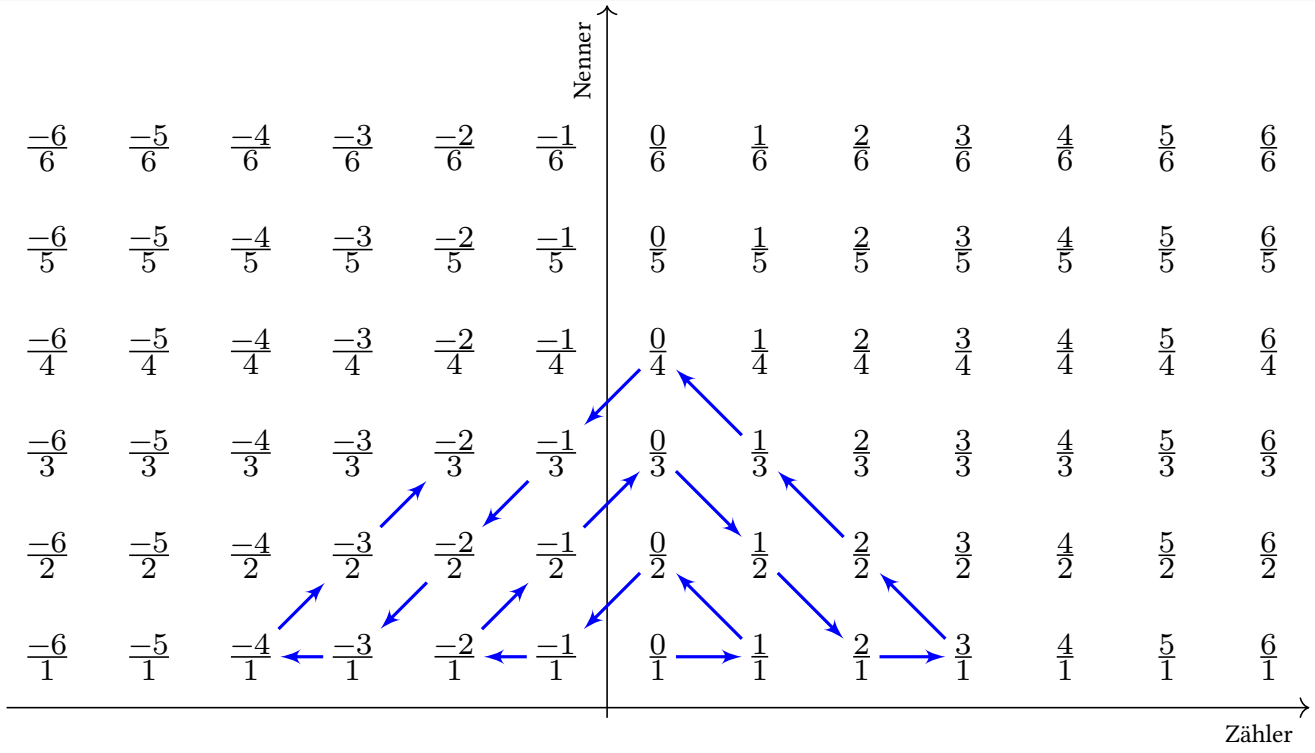
(3) Wir haben $\mathfrak{P}(\mathbb{N})\cong\{0,1\}^{\mathbb{N}}\subseteq\mathbb{N}^{\mathbb{N}}$, und $\mathfrak{P}(\mathbb{N})$ ist überabzählbar; das beweisen wir unten mit Cantors zweitem Diagonalargument B2G.

Beispiel: Der Fundamentalsatz der Arithmetik zeigt $(\mathbb{N}^{(\mathbb{N})},+)\cong(\mathbb{N}_{\geq 1},\cdot)$ vermöge der Zuordnung $(a_0,a_1,a_2,\dots)=a\mapsto n=2^{a_0}\cdot 3^{a_1}\cdot 5^{a_2}\cdots$.

Mächtigkeit der rationalen Zahlen $\mathbb{Q}$

Satz B2E: Mächtigkeit von $\mathbb{Q}$

Die Menge $\mathbb{Q}$ der rationalen Zahlen ist abzählbar unendlich, kurz $\mathbb{Q} \cong \mathbb{N}$.



Mächtigkeit der rationalen Zahlen $\mathbb{Q}$

Es gibt viele Möglichkeiten, eine solche Abzählung auszuführen.
Die Skizze zeigt eine anschauliche, graphische Vorgehensweise.
📖 Eine raffiniert-explizite Abzählung konstruieren N. Calkin, H. Wilf: *Recounting the Rationals.* Amer. Math. Monthly 107 (2000) 360-363.

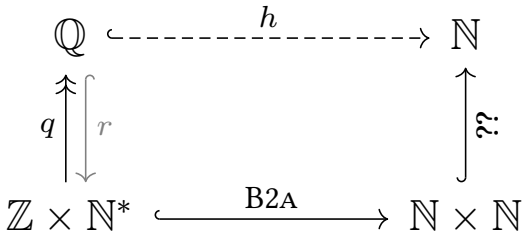
Wir wollen eine Bijektion $\mathbb{N} \rightleftharpoons \mathbb{Q}$ konstruieren. Bei der oben skizzierten Abzählung werden tatsächlich alle rationalen Zahlen durchlaufen, jedoch müssen mehrfache Darstellungen derselben Zahl übergangen werden. Die Grundidee ist anschaulich anhand der Skizze vollkommen klar, doch eine vollständige Präzisierung scheint zunächst schwierig.

Um dies sorgfältig und explizit auszuformulieren, ist es geschickt, unsere bisherigen Konstruktionen gewinnbringend einzusetzen:
Wir haben einerseits $\mathbb{N} \subset \mathbb{Q}$, andererseits ist $\mathbb{Q} = \bigcup_{n \in \mathbb{N}^*} \{ z/n \mid z \in \mathbb{Z} \}$ abzählbare Vereinigung abzählbarer Mengen, also abzählbar dank **??**.
Aus $f : \mathbb{N} \hookrightarrow \mathbb{Q}$ und $g : \mathbb{Q} \hookrightarrow \mathbb{N}$ erhalten wir $(h, k) : \mathbb{Q} \cong \mathbb{N}$ dank Satz B2o.
Damit gelingt eine ebenso präzise wie konkrete Konstruktion.
Wir müssen nur den Mut fassen, alles auszuschreiben!

Mächtigkeit der rationalen Zahlen $\mathbb{Q}$

Beweis: Wir haben einerseits die Inklusion $\mathbb{N} \subset \mathbb{Q}$, also $\mathbb{N} \preceq \mathbb{Q}$.
Die rationalen Zahlen sind also mindestens abzählbar unendlich.

Andererseits haben wir die Surjektion $q : \mathbb{Z} \times \mathbb{N}^* \twoheadrightarrow \mathbb{Q} : (a, b) \mapsto a/b$.



Somit gilt $\mathbb{Q} \preceq \mathbb{Z} \times \mathbb{N}^* \preceq \mathbb{N} \times \mathbb{N} \preceq \mathbb{N}$. Dank Transitivität folgt $\mathbb{Q} \preceq \mathbb{N}$.
Die rationalen Zahlen sind also höchstens abzählbar unendlich.

☺ Dank Cantor–Bernstein B2o gilt $\mathbb{Q} \cong \mathbb{N}$. QED

Bemerkung: Die Quotientenabbildung $q : \mathbb{Z} \times \mathbb{N}^* \twoheadrightarrow \mathbb{Q} : (a, b) \mapsto a/b$ erlaubt eine schöne explizite Rechtsinverse $r : \mathbb{Q} \hookrightarrow \mathbb{Z} \times \mathbb{N}^* : c \mapsto (a, b)$ mit $c = a/b$ und $\operatorname{ggT}(a, b) = 1$: Dies ist die eindeutige Darstellung als vollständig gekürzter Bruch. Wir haben also $(r, q) : \mathbb{Q} \rightleftarrows \mathbb{Z} \times \mathbb{N}^*$.

☺ *Beautiful is better than ugly. Explicit is better than implicit.*

Mächtigkeit der rationalen Zahlen $\mathbb{Q}$

Korollar B2F: Mächtigkeit von $\mathbb{Q}^{(\mathbb{N})}$

(1) Es gilt $\mathbb{Q}^n \cong \mathbb{N}$ für jede natürliche Zahl $n \in \mathbb{N}_{\geq 1}$.

(2) Es gilt $\mathbb{Q}^{(\mathbb{N})} \cong \mathbb{N}$ für die Menge aller Folgen mit endlichem Träger:

$$\mathbb{Q}^{(\mathbb{N})} := \{ f : \mathbb{N} \to \mathbb{Q} \mid \sharp \operatorname{supp}(f) < \infty \}.$$

(3) Hingegen ist die Menge $\mathbb{Q}^{\mathbb{N}} = \{ f : \mathbb{N} \to \mathbb{Q} \}$ überabzählbar.

Aufgabe: Beweisen Sie diese Aussagen als Wiederholung und Übung.

Lösung: Dies beweisen wir wörtlich wie in B2D mit Hilfe von Satz B2C.

(1) Wir führen Induktion über $n \in \mathbb{N}_{\geq 1}$: Für $n = 1$ gilt $\mathbb{Q}^1 \cong \mathbb{N}$ (B2E).
Für $n \geq 2$ finden wir induktiv $\mathbb{Q}^n = \mathbb{Q}^{n-1} \times \mathbb{Q} \cong \mathbb{N} \times \mathbb{N} \cong \mathbb{N}$ (??).

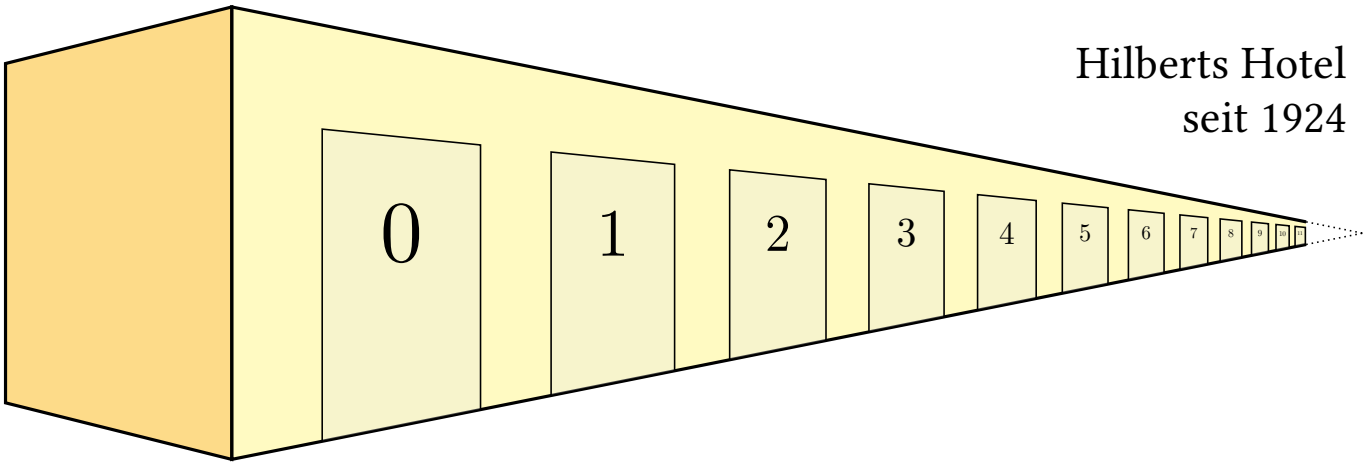
(2) Die Menge $\mathbb{Q}^{(\mathbb{N})}$ ist eine abzählbare Vereinigung (??) gemäß

$$\mathbb{Q}^{(\mathbb{N})} = \bigcup_{n \in \mathbb{N}} \{ f : \mathbb{N} \to \mathbb{Q} \mid \operatorname{supp}(f) \subset \{0, \dots, n\} \}$$

(3) Wir haben $\mathfrak{P}(\mathbb{N}) \cong \{0, 1\}^{\mathbb{N}} \subseteq \mathbb{Q}^{\mathbb{N}}$, und $\mathfrak{P}(\mathbb{N})$ ist überabzählbar;
das beweisen wir unten mit Cantors zweitem Diagonalargument B2G.

Hilberts Hotel

Aus dem Paradies, das Cantor uns geschaffen,
soll uns niemand vertreiben können. (David Hilbert)



Hilberts Hotel hat die Zimmer $0, 1, 2, 3, \ldots$. Alle Zimmer sind belegt.
Ein weiterer Gast kommt noch unter, dank $\mathbb{N} \hookrightarrow \mathbb{N} : n \mapsto n + 1$,
... auch abzählbar viele neue Gäste, dank $\mathbb{N} \hookrightarrow \mathbb{N} : n \mapsto 2n$,
... sogar $\mathbb{N}^2 \hookrightarrow \mathbb{N} : (a, b) \mapsto a + (a + b)(a + b + 1)/2$.

Hilberts Hotel

Wenn in einem **endlichen Hotel** alle Zimmer belegt sind, dann kann kein Gast mehr aufgenommen werden, auch wenn die Managerin die Gäste neu auf die Zimmer verteilt. Es hilft alles nichts! (Invarianz **??**)

Anders in **Hilberts Hotel** mit unendlich vielen Zimmern $0, 1, 2, 3, \ldots$: Sind alle Zimmer belegt, so kann noch ein Gast aufgenommen werden! Der Gast von Zimmer 0 zieht nach 1, der von 1 nach 2, usw.

Ebenso zwei Gäste, oder drei, oder vier... Nun kommt ein Hilbert–Bus mit unendlich vielen neuen Gästen. Die Managerin quartiert die alten Gäste um vermöge der Bijektion $\mathbb{N} \xrightarrow{\sim} 2\mathbb{N} : n \mapsto 2n$. Die neuen Gäste beziehen ihre Zimmer vermöge $\mathbb{N} \xrightarrow{\sim} 2\mathbb{N} + 1 : n \mapsto 2n + 1$. Zusammen erhalten wir so die Bijektion $\{0, 1\} \times \mathbb{N} \xrightarrow{\sim} \mathbb{N} : (i, n) \mapsto 2n + i$ (Satz B2B).

Schließlich kommen unendlich viele Busse, jeder mit unendlich vielen Gästen. Kein Problem, wir haben eine Bijektion $\mathbb{N} \times \mathbb{N} \xrightarrow{\sim} \mathbb{N}$ (Satz **??**).

Übung: Wie verteilen Sie die Zimmer jeweils neu? Schreiben Sie zur Wiederholung alle relevanten Bijektion möglichst schön und explizit aus!

Hilberts Hotel

Hotel Infinity, lyrics © 2000 by Lawrence Mark Lesser

On a dark desert highway — not much scenery
Except this long hotel stretchin' far as I could see.
Neon sign in front read "No Vacancy,"
But it was late and I was tired, so I went inside to plea.

The clerk said, "No problem. Here's what can be done —
We'll move those in a room to the next higher one.
That will free up the first room and that's where you can stay."
I tried understanding that as I heard him say:

[Chorus] "Welcome to the Hotel called Infinity —
Where every room is full (every room is full)
Yet there's room for more.
Yeah, plenty of room at the Hotel called Infinity —
Move 'em down the floor (move 'em down the floor)
To make room for more."

Hilberts Hotel

I'd just gotten settled, I'd finally unpacked
When I saw 8 more cars pull into the back.
I had to move to room 9; others moved up 8 rooms as well.
Never more will I confuse a Hilton with a Hilbert Hotel!

My mind got more twisted when I saw a bus without end
With an infinite number of riders coming up to check in.
"Relax," said the nightman. "Here's what we'll do:
Move to the double of your room number:
that frees the odd-numbered rooms." [Chorus]

Last thing I remember at the end of my stay —
It was time to pay the bill but I had no means to pay.
The man in 19 smiled, "Your bill is on me.
20 pays mine, and so on, so you get yours for free!"

(`larrylesser.com/greatest-lesser-hits`, *Hotel Infinity*)

Mächtigkeit der Potenzmenge

Cantors zweites Diagonalargument: Kann $f : X \to \mathfrak{P}(X)$ surjektiv sein?

$$A := \{ x \in X \mid x \notin f(x) \} \subseteq X.$$

Angenommen, es gäbe ein Element $x \in X$ mit $f(x) = A$.

- Gilt $x \in A$, so folgt $x \notin f(x) = A$, ein Widerspruch.
- Gilt $x \notin A$, so folgt $x \in f(x) = A$, ein Widerspruch.

Wir schließen: Es existiert kein Element $x \in X$ mit $f(x) = A$.

Satz B2G: Cantors zweites Diagonalargument

Zu jeder Menge X ist die Potenzmenge $\mathfrak{P}(X)$ mächtiger, kurz $X \prec \mathfrak{P}(X)$.
Ausführlich gilt $X \preceq \mathfrak{P}(X)$, dank $X \hookrightarrow \mathfrak{P}(X) : x \mapsto \{x\}$, aber $X \not\cong \mathfrak{P}(X)$.

Für endliche Mengen ist das klar, aus $\sharp X = n$ folgt $\mathfrak{P}(X) = 2^n > n$.
Für unendliche Mengen war dies Cantors erschütternde Erkenntnis:
Es gibt verschiedene Unendlichkeiten, insb. überabzählbare Mengen!

Beispiel: Die Potenzmenge $\mathfrak{P}(\mathbb{N}) \cong \{0,1\}^{\mathbb{N}}$ ist überabzählbar.

Mächtigkeit der Potenzmenge

☺ Dieser berühmte Beweis ist genial einfach und einfach genial!
Der Trick heißt traditionell *Cantors zweites Diagonalargument*.
Cantors erstes Diagonalargument beweist $\mathbb{N}^2 \cong \mathbb{N}$, siehe **??**.

Das Argument erinnert uns eindringlich an das Barbier-Paradoxon und die Russelsche Antinomie (B107). Diese logische Katastrophe der allzu naiven Mengenlehre beheben wir durch freiwillige Beschränkung auf die streng reglementierten Mengenkonstruktionen nach Zermelo–Fraenkel und machen seither sehr gute Erfahrungen damit. Hier nun taucht eine Variante dieser Idee erneut auf, als Cantors zweites Diagonalargument.

Im vorliegenden Beweis ist alles kristallklar, alles geht mit rechten Dingen zu: Wir widerlegen die Aussage $A \in \operatorname{Im}(f)$, ganz einfach.
Zudem ist dies ein wunderbares Beispiel für einen Beweis durch Widerspruch zusammen mit einer einfachen Fallunterscheidung.

☺ Ich hoffe, unsere soliden Vorbereitungen zahlen sich hier (und überall) für Sie aus, und Sie genießen die schönen Wow-und-Aha–Erlebnisse.

Illustration zu Cantors Diagonalverfahren

Aufgabe: Illustrieren Sie diesen Beweis im Spezialfall $X = \mathbb{N}$.

Lösung: Gegeben sei eine Folge von Mengen $A_0, A_1, A_2, \ldots \subseteq \mathbb{N}$,
etwa $A_0 = \emptyset$, $A_1 = \{0, 1, 3\}$, $A_2 = \mathbb{N}$, $A_3 = 2\mathbb{N}$, $A_4 = 2\mathbb{N} + 1$, ...
Diese Mengen können wir übersichtlich in einer Tabelle anordnen:

	0	1	2	3	4	5	6	7	8	9	...
A_0	0	0	0	0	0	0	0	0	0	0	...
A_1	1	1	0	1	0	0	0	0	0	0	...
A_2	1	1	1	1	1	1	1	1	1	1	...
A_3	1	0	1	0	1	0	1	0	1	0	...
A_4	0	1	0	1	0	1	0	1	0	1	...
...	...										

Als Tabelle schreiben wir $a_{ij} = 1$, falls $A_i \ni j$, und $a_{ij} = 0$, falls $A_i \not\ni j$.
Entlang der Diagonalen bilden wir die Menge $A = \{ i \in \mathbb{N} \mid a_{ii} = 0 \}$.
Sie kommt nicht in unserer Liste vor, denn $i \in A_i \Leftrightarrow i \notin A$. QED

Illustration zu Cantors Diagonalverfahren

☺ Es gibt keine Abzählung $A_0, A_1, A_2, \ldots$ der Potenzmenge $\mathfrak{P}(\mathbb{N})$.
Jede solche Folge $A_0, A_1, A_2, \ldots \subseteq \mathbb{N}$ lässt immer noch Mengen aus.
Dieses Argument ist, wie gesagt, genial einfach und einfach genial!

Satz B2G optimiert diesen schönen Beweis zu der allgemeinen Aussage $X \prec \mathfrak{P}(X)$, also $X \preceq \mathfrak{P}(X)$ und $X \not\approx \mathfrak{P}(X)$. Der Spezialfall $X = \mathbb{N}$ ist besonders wichtig und anschaulich, daher betone ich diese Illustration.

Dieses Argument nutzen wir später nochmal, geschickt abgewandelt, um zu zeigen, dass die Menge $\mathbb{R}$ der reellen Zahlen überabzählbar ist. Genauer gilt $\mathbb{R} \cong \{0, 1\}^{\mathbb{N}} \cong \mathfrak{P}(\mathbb{N})$, dies erklären wir in Satz B2N.

Bemerkung: Die Menge $\mathbb{N}$ ist unendlich und bereits schwer vorstellbar.
Dank der Dedekind-Peano-Axiome haben wir sie jedoch gut im Griff.

Die Menge $\mathbb{R}$ ist überabzählbar und somit unverstellbar viel größer.
Damit ist nicht Schluss: Die Potenzmenge $\mathfrak{P}(\mathbb{R})$ ist noch riesiger.

Lesen und beweisen und würdigen Sie nochmals Satz B2G.
Cantors Diagonalverfahren ist zurecht berühmt.

Die Menge $\mathbb{R}$ der reellen Zahlen ist überabzählbar.

B233
Erläuterung

Wir wissen, dank Cantors zweitem Diagonalargument B2G, dass es zu jeder Menge X eine strikt mächtigere Menge Y gibt, etwa $Y = \mathfrak{P}(X)$. Dies können wir insbesondere anwenden auf die abzählbar unendliche Menge $\mathbb{N}$: Die Potenzmenge $\mathfrak{P}(\mathbb{N}) \cong \{0,1\}^{\mathbb{N}}$ ist demnach überabzählbar.

Die Mengen $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{N}^n$ hingegen sind abzählbar, gleichmächtig mit $\mathbb{N}$. Das ist anfangs überraschend, denn sie enthalten offensichtlich „mehr“ Elemente als $\mathbb{N}$. Tatsächlich haben wir explizite Bijektionen konstruiert, sie sind erste eindrückliche Beispiele an Sorgfalt und Kunstfertigkeit.

Ein gewaltiger Sprung entsteht bei der Vervollständigung vom Körper $\mathbb{Q}$ der rationalen Zahlen zum Körper $\mathbb{R}$ der reellen Zahlen: Im Gegensatz zur abzählbaren Menge $\mathbb{Q}$ ist die Menge $\mathbb{R}$ überabzählbar! Genauer konstruieren wir in Satz Satz B2N eine Bijektion $\mathbb{R} \cong \{0,1\}^{\mathbb{N}} \cong \mathfrak{P}(\mathbb{N})$.

Die Überabzählbarkeit von $\mathbb{R}$ ist eine überaus erstaunliche Erkenntnis. Wir werden sie auf zwei Arten beweisen: Zunächst als Aufwärmübung die leichtere Aussage, dass die Menge $\mathbb{R}$ überabzählbar ist. Das gelingt direkt als eine raffinierte Variante von Cantors Diagonalverfahren B2G.

Die Menge $\mathbb{R}$ der reellen Zahlen ist überabzählbar.

B234
Erläuterung

Aufgabe: Zeigen Sie, nach Vorbild von Cantors Diagonalverfahren B2G, dass die Menge $\mathbb{R}$ der reellen Zahlen überabzählbar ist.

Beweis-Idee: Vorgelegt sei eine reelle Folge $r_0, r_1, r_2, \ldots \in [0,1]$. Wir schreiben r_k dezimal und konstruieren per Diagonalverfahren eine weitere Zahl $s \in [0,1]$, die noch nicht in dieser Liste vorkommt.

	0	1	2	3	4	5	6	7	8	9	…
r_0	0	0	0	0	0	0	0	0	0	0	…
r_1	9	9	9	9	9	9	9	9	9	9	…
r_2	4	1	4	2	1	3	5	6	2	3	…
r_3	7	3	2	0	5	0	8	0	7	5	…
r_4	1	4	1	5	9	2	6	5	3	5	…
r_5	7	1	8	2	8	1	8	2	8	4	…
…	…										

In unserem Beispiel konstruieren wir $s = 0.549546\ldots$ mit $s \neq r_k$.

Die Menge $\mathbb{R}$ der reellen Zahlen ist überabzählbar.

Lösung: Wegen $\mathbb{N} \subset \mathbb{R}$ ist die Menge $\mathbb{R}$ offensichtlich unendlich.
Wir behaupten, dass bereits das Intervall $[0,1]$ nicht abzählbar ist.

Wir führen einem Widerspruchsbeweis. Angenommen, das Intervall $[0,1]$ wäre abzählbar, das heißt, es gäbe eine Bijektion $\mathbb{N} \cong [0,1] : k \mapsto r_k$.

Wir können jede dieser reellen Zahlen $r_k \in [0,1]$ dezimal darstellen als $r_k = 0.r_{k0}r_{k1}r_{k2}\cdots = \sum_{n=0}^{\infty} r_{kn}10^{-n-1}$ mit Ziffern $r_{kn} \in \mathbb{Z}_{10} = \{0,\dots,9\}$.
Wir betrachten die reelle Zahl s mit den Ziffern $s_n = (r_{nn} + 5) \operatorname{rem} 10$.
Somit gilt $|s - r_k| \geq 4 \cdot 10^{-k-1}$, also insbesondere $s \neq r_k$ für alle $k \in \mathbb{N}$.

Wir erhalten $s \in [0,1]$, aber $s \notin \{\, r_k \mid k \in \mathbb{N} \,\}$. Das ist ein Widerspruch!
Demnach ist das Intervall $[0,1]$ überabzählbar, und somit auch $\mathbb{R}$. QED

🙂 Auch dieser Beweis ist genial einfach und einfach genial!

Diese Aussage und ihren schönen Beweis wollen wir nun optimieren.
Dazu untersuchen wir zunächst die hier benutzte Dezimaldarstellung etwas genauer. Die Basis $B = 10$ ist dabei vollkommen willkürlich; es lohnt sich, gleich eine beliebige Basis $B \in \mathbb{N}_{\geq 2}$ zu betrachten.

Die Menge $\mathbb{R}$ der reellen Zahlen ist überabzählbar.

Wir haben gerade bewiesen, dass die Menge $\mathbb{R}$ überabzählbar ist.
Jedoch gibt es viele überabzählbare Mengen, neben $\mathbb{R}$ kennen wir $\mathfrak{P}(\mathbb{N}) \cong \{0,1\}^{\mathbb{N}}$ sowie $\mathfrak{P}\mathfrak{P}(\mathbb{N})$ und $\mathfrak{P}\mathfrak{P}\mathfrak{P}(\mathbb{N})$ und $\mathfrak{P}\mathfrak{P}\mathfrak{P}\mathfrak{P}(\mathbb{N})$ usw.
Genauer wollen wir eine Bijektion $\mathbb{R} \cong \{0,1\}^{\mathbb{N}} \cong \mathfrak{P}(\mathbb{N})$ konstruieren.

🙂 Auch hierzu bietet uns das Diagonalverfahren hilfreiche Intuition:
Wenn wir reelle Zahlen in der Basis $B = 2$ entwickeln, so erhalten wir beinahe eine Bijektion $[0,1] \cong \{0,1\}^{\mathbb{N}}$. Zusammen mit einer geeigneten Bijektion $\mathbb{R} \cong [0,1]$ erhalten wir so $\mathbb{R} \cong \{0,1\}^{\mathbb{N}} \cong \mathfrak{P}(\mathbb{N})$, wie ersehnt.

⚠ Leider ist die B–adische Entwicklung für manche reellen Zahlen zweideutig, das müssen wir in unserer Konstruktion berücksichtigen.
Die technische Ausführung nutzt daher den Satz von Cantor–Bernstein.
Damit können wir die Mächtigkeit von $\mathbb{R}$ genau bestimmen, wie erhofft.

Das ist nicht nur eine interessante technische Herausforderung, sondern liefert uns zugleich einige interessante Folgerungen wie $\mathbb{R} \cong \mathbb{R}^n \cong \mathbb{R}^{\mathbb{N}}$.
Wir nehmen also mutig einen zweiten Anlauf und untersuchen genauer die B–adische Entwicklung reeller Zahlen und damit deren Mächtigkeit.

Entwicklung reeller Zahlen in Basis B

Sei $B \in \mathbb{N}_{\geq 2}$, etwa binär $B = 2$, ternär $B = 3$ oder dezimal $B = 10$:

$$\pi = 3.14159\,26535\,89793\,23846\,26433\,83279\,\ldots$$
$$0.1 = 0.09999\,99999\,99999\,99999\,99999\,99999\,\ldots$$

Satz B2M: B–adische Entwicklung

Jede Ziffernfolge $a_1, a_2, a_3, \ldots \in \{0, \ldots, B-1\}$ definiert eine reelle Zahl

$$a = \sum_{k=1}^{\infty} a_k B^{-k} = \sup_{n\in\mathbb{N}} \sum_{k=1}^{n} a_k B^{-k} \quad \in \quad [0,1].$$

Umgekehrt lässt sich jede reelle Zahl $a \in [0,1]$ so als eine B–adische Entwicklung schreiben (auf mindestens eine, höchstens zwei Weisen).

$$q : \{0, \ldots, B-1\}^{\mathbb{N}} \twoheadrightarrow [0,1] : (a_{n+1})_{n\in\mathbb{N}} \mapsto a$$

Zu jeder reellen Zahl $a \in]0,1]$ existiert genau eine solche B–adische Entwicklung, bei der unendlich viele Ziffern von 0 verschieden sind.

$$r : [0,1] \hookrightarrow \{0, \ldots, B-1\}^{\mathbb{N}} : a \mapsto (a_{n+1})_{n\in\mathbb{N}}$$

Entwicklung reeller Zahlen in Basis B

Für $s_n = \sum_{k=1}^{n} a_k B^{-k}$ gilt $0 = s_0 \leq s_1 \leq s_2 \leq s_3 \leq \ldots \leq 1$, also existiert der Grenzwert $a = \lim_{n\to\infty} s_n = \sup_{n\in\mathbb{N}} s_n$, denn $(\mathbb{R}, \leq)$ ist vollständig! Die B–adische Reihe definiert so die Abbildung $q : \mathbb{Z}_B^{\mathbb{N}} \twoheadrightarrow [0,1]$.

Umgekehrt konstruieren wir $r : [0,1] \to \mathbb{Z}_B^{\mathbb{N}} : a \mapsto (a_{n+1})_{n\in\mathbb{N}}$ rekursiv: Gegegen sei $a \in]0,1]$ und $(a_1, \ldots, a_n) \in \mathbb{Z}_B^n$ mit $s_n = \sum_{k=1}^{n} a_k B^{-k} < a$. Dazu definieren wir dann $a_{n+1} = \max\{\, z \in \mathbb{Z}_B \mid s_n + zB^{-n-1} < a \,\}$. Im Sonderfall $a = 0$ setzen wir $r(0) = (0, 0, 0, \ldots) \in \mathbb{Z}_B^{\mathbb{N}}$.

Nach Konstruktion ist r rechtsinvers zu q, das bedeutet $q \circ r = \mathrm{id}_{[0,1]}$. Insbesondere ist q somit surjektiv, doch leider nicht injektiv: Zahlen wie $a = 0.1000\ldots = 0.0AAA\ldots$ haben zwei Darstellungen, wobei $A = B - 1$. Das gilt für alle Brüche $a = z/B^n \in [0,1[$ mit Zähler $z \in \{1, \ldots, B^n\}$.

Daher ist eine Bijektion $\mathbb{Z}_B^{\mathbb{N}} \cong [0,1]$ nicht ganz so einfach zu konstruieren. Immerhin erhalten wir eine Bijektion $(q|_X^Y, r|_Y^X) : X \cong Y$ zwischen den echten Teilmengen $X = \{1, \ldots, B-1\}^{\mathbb{N}} \subsetneq \mathbb{Z}_B^{\mathbb{N}}$ und $Y = q(X) \subsetneq [0,1]$. Der folgende Satz fügt alle diese Vorbereitungen sorgsam zusammen.

Mächtigkeit der reellen Zahlen $\mathbb{R}$

Satz B2N: Mächtigkeit von $\mathbb{R}$

(1) Die Menge $\mathbb{R}$ ist überabzählbar, genauer gilt $\mathbb{R} \cong \{0,1\}^{\mathbb{N}} \cong \mathfrak{P}(\mathbb{N})$.
(2) Somit ist $\mathbb{R}$ gleichmächtig zu $\mathbb{R}^d$ für $d \geq 2$ und zu $\mathbb{R}^{\mathbb{N}} = \{ f : \mathbb{N} \to \mathbb{R} \}$.
(3) Strikt mächtiger sind hingegen $\mathfrak{P}(\mathbb{R}) \cong \{0,1\}^{\mathbb{R}} \subset \mathbb{R}^{\mathbb{R}} = \{ f : \mathbb{R} \to \mathbb{R} \}$.

Beweis: (1) Wir konstruieren Injektionen $\mathbb{R} \hookrightarrow \{0,1\}^{\mathbb{N}}$ und $\{0,1\}^{\mathbb{N}} \hookrightarrow \mathbb{R}$. Dank Cantor–Bernstein B2O erhalten wir eine Bijektion $\mathbb{R} \cong \{0,1\}^{\mathbb{N}}$.

Explizit: (1a) Wir haben Bijektionen $f : \mathbb{R} \xrightarrow{\sim}]-1,+1[: x \mapsto x/(1+|x|)$ (A1B) sowie $g :]-1,+1[\xrightarrow{\sim}]0,1[: x \mapsto (x+1)/2$. Die Binärentwicklung stiftet die Injektion $r :]0,1[\hookrightarrow \{0,1\}^{\mathbb{N}}$ dank Satz B2M für $B = 2$.

(1b) Satz B2M für $B = 3$ stiftet eine Injektion $q : \{0,1\}^{\mathbb{N}} \hookrightarrow]0,1] \subset \mathbb{R}$.

(2) Wir haben Bijektionen $\mathbb{N} \cong \mathbb{N} \times \{1,\dots,d\} \cong \mathbb{N} \times \mathbb{N}$. Aus $\mathbb{R} \cong \{0,1\}^{\mathbb{N}}$ folgt $\mathbb{R}^d \cong \{0,1\}^{\mathbb{N}\times\{1,\dots,d\}} \cong \{0,1\}^{\mathbb{N}}$ und $\mathbb{R}^{\mathbb{N}} \cong \{0,1\}^{\mathbb{N}\times\mathbb{N}} \cong \{0,1\}^{\mathbb{N}}$. QED

Übung: Führen Sie die letzten Rechnungen aus mit Hilfe von Satz B2C. Alle Bijektionen sind wunderbar explizit und im Rückblick genial einfach.

Mächtigkeit der reellen Zahlen $\mathbb{R}$

Schon das Ergebnis $\mathbb{N}^2 \cong \mathbb{N}$ ist erstaunlich, ebenso $\mathbb{N}^d \cong \mathbb{N}$ und $\mathbb{N}^{(\mathbb{N})} \cong \mathbb{N}$. Ebenso möchte man vermuten, dass $\mathbb{R}^d$ „wesentlich mehr“ Punkte hat als $\mathbb{R}$, doch ganz im Gegenteil finden Bijektionen $\mathbb{R}^d \cong \mathbb{R}$ und sogar $\mathbb{R}^{\mathbb{N}} \cong \mathbb{R}$.

Dieses Thema wird Sie in Ihrem Studium immer wieder beschäftigen: Natürlich möchten Sie jedem Raum $\mathbb{R}^d$ seine Dimension „$\dim \mathbb{R}^d = d$“ zusprechen. Allein die Mächtigkeit macht jedoch keinen Unterschied! Die Dimension erhält erst durch zusätzliche Struktur ihren Sinn: bezüglich linearer Abbildungen von $\mathbb{R}$–Vektorräumen, oder Diffeomorphismen, oder Homöomorphismen, … Dazu später mehr im Studium.

Cantors **Kontinuumshypothese** (kurz CH) besagt: Aus $\mathbb{N} \subseteq X \subseteq \mathbb{R}$ folgt $X \cong \mathbb{N}$ oder $X \cong \mathbb{R}$. **Verallgemeinert** (GCH): Für jede unendliche Menge A und $A \preceq X \preceq \mathfrak{P}(A)$ gilt $X \cong A$ oder $X \cong \mathfrak{P}(A)$. Das heißt, nach A hat $\mathfrak{P}(A)$ die nächst größere Mächtigkeit, es liegt nichts dazwischen. Dies ist unabhängig von ZFC: Ausgehend von einem ZFC-Universum existieren Modelle, in denen GCH gilt (Kurt Gödel 1940), und ebenso Modelle, in denen GCH nicht gilt (Paul Cohen 1963, Fields-Medaille 1966).

Lässt sich jede reelle Zahl berechnen?

Unendlichkeit kommt in verschiedenen Größen: $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ sind abzählbar, $\mathbb{R}$ ist überabzählbar. Wie lässt sich das anwenden? Gut, dass Sie fragen!

ON COMPUTABLE NUMBERS, WITH AN APPLICATION TO THE ENTSCHEIDUNGSPROBLEM

By A. M. Turing.

[Received 28 May, 1936.—Read 12 November, 1936.]

The "computable" numbers may be described briefly as the real numbers whose expressions as a decimal are calculable by finite means.

📖 A.M. Turing: *On Computable Numbers, with an Application to the Entscheidungsproblem.* Proc. London Math. Soc. 42 (1937) 230–65.

Alan Turing fragte 1936: Können wir jede reelle Zahl $x \in \mathbb{R}$ berechnen? Nein! Es gibt nur abzählbar viele Programme, doch $\mathbb{R}$ ist überabzählbar.

Ausführlich: Wählen Sie eine Programmiersprache. Diese verwendet zu ihrer Codierung ein endliches Alphabet $\mathcal{A}$. Die Menge $\mathcal{A}^* = \bigcup_{n\in\mathbb{N}} \mathcal{A}^n$ ist abzählbar (??), daher gibt es nur abzählbar viele Programme.

Lässt sich jede reelle Zahl berechnen?

Dieses Abzählargument ist heute vollkommen plausibel und naheliegend. Berechenbare Zahlen wurden erstmals 1912 von Emile Borel eingeführt, allerdings noch informell-intuitiv formuliert. Auch als Alan Turing 1936 seinen Artikel schrieb, gab es noch gar keine Computer. Sein epochaler Artikel definiert die Turing–Maschine als universelles Rechenmodell und beweist, dass Hilberts berühmtes Entscheidungsproblem unlösbar ist.

🙂 Damit beginnt die Informatik – noch vor den ersten Computer!

Naiv-anschaulich wollen wir unsere Zahl $x \in \mathbb{R}$ durch ein Programm schrittweise dezimal ausschreiben. Für viele wichtige Zahlen gelingt dies:

$$22/7 = 3.14285\,71428\,57142\,85714\ldots$$
$$\pi = 3.14159\,26535\,89793\,23846\ldots$$
$$\mathrm{e} = 2.71828\,18284\,59045\,23536\ldots$$

Lässt sich jede Folge $f : \mathbb{N} \to \{0,1\}$ oder $g : \mathbb{N} \to \{0,\ldots,9\}$ berechnen? Allgemein stellt sich die Frage ebenso für $h : \mathbb{N} \to \mathbb{K}$ mit $\mathbb{K} = \mathbb{N}, \mathbb{Z}, \mathbb{Q}$. Antwort: Nein! Die Menge $\mathbb{R} \cong \{0,1\}^{\mathbb{N}} \cong \mathfrak{P}(\mathbb{N})$ ist überabzählbar (B2N).

Was genau sind berechenbare reelle Zahlen?

Zur Vereinfachung verstehen wir „berechenbar“ zunächst halbformal als realisierbar in einer typischen Programmiersprache wie Python oder C++ oder äquivalent hierzu abstrakt auf einer Turing–Maschine. Wir müssen diese „mentalen“ Prozesse formalisieren, um Unmöglichkeit zu beweisen. Damit vereinbaren wir berechenbare reelle Zahlen elegant wie folgt:

Definition B2H: berechenbare reelle Zahl

Eine reelle Zahl $a \in \mathbb{R}$ heißt **berechenbar** oder auch **rekursiv**, wenn sie durch eine berechenbare Funktion $f : \mathbb{N} \to \mathbb{Z}$ approximiert wird gemäß

$$\forall n \in \mathbb{N} : \frac{f(n)-1}{2^n} < a < \frac{f(n)+1}{2^n}.$$

Übung: Die berechenbaren Zahlen bilden den Teilkörper $\mathrm{REC} \leq (\mathbb{R}, +, \cdot)$: Sind $a, b \in \mathbb{R}$ berechenbar, so auch $a \pm b$ (leicht) und $a \cdot b$ (interessant) sowie im Falle $b \neq 0$ auch a/b (spannend). Zur Division a/b müssen wir $b \neq 0$ voraussetzen, können es selbst aber nicht effektiv überprüfen:

⚠ Die Gleichheit im Körper $(\mathrm{REC}, +, \cdot)$ ist nicht berechenbar.

Berechenbare Zahlen und das Entscheidungsproblem

⚠ Die Frage „Gilt $a = 0$?“ lässt sich alleine mit einer Approximation f im Allgemeinen nicht effektiv beantworten. Sie ist nur semi-entscheidbar:

Gilt $a = 0$, so gibt uns keine Approximation $f(n) = 0$ eine Garantie; für $n' > n$ könnte $f(n') = 0$ gelten, oder ein $f(n') \neq 0$ auftauchen.

Gilt $a \neq 0$, so existiert $n \in \mathbb{N}$ mit $f(n) \neq 0$, und das beweist $a \neq 0$. Genauer: Aus $f(n) > 0$ folgt $a > 0$. Aus $f(n) < 0$ folgt $a < 0$.

Beispiel: Wir definieren die Zahl $a = \sum_{n=0}^{\infty} a_n 2^{-n}$ durch $a_n = 1$ falls $n \geq 4$ gerade ist und nicht Summe zweier Primzahlen, andernfalls $a_n = 0$. Wir können a beliebig genau approximieren, diese Zahl ist berechenbar im Sinne von B2H. Dennoch wissen wir nicht, ob $a = 0$ oder $a > 0$ gilt. Die Goldbach–Vermutung besagt $a = 0$, und sie ist immer noch offen.

Statt Goldbach können Sie hier Ihre Lieblingsvermutung einsetzen. Das Argument gilt für jede Familie von entscheidbaren Aussagen $A(n)$ und ihre Zusammenfassung zu $\exists n \in \mathbb{N} : A(n)$. Dies ist äquivalent zu $a > 0$ für $a = \sum_{n=0}^{\infty} a_n 2^{-n}$, und ist im Allgemeinen unentscheidbar.

Gibt es transzendente Zahlen?

Ist jede Zahl $\alpha \in \mathbb{R}$ Nullstelle eines rationalen Polynoms $A \in \mathbb{Q}[X]^*$?
Nein! Es gibt nur abzählbar viele rationale Polynome und Nullstellen.

Ausführlich: Erfüllen die Potenzen α^n eine $\mathbb{Q}$–lineare Relation?

$$a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n \overset{?}{=} 0$$

Falls nicht, so heißt α **transzendent**. Falls doch, so heißt α **algebraisch**:
Die Zahl $\alpha \in \mathbb{R}$ ist Nullstelle eines Polynoms $A = \sum_{k=0}^{n} a_k X^k \in \mathbb{Q}[X]^*$.

Beispiele: Jede rationale Zahl $\alpha \in \mathbb{Q}$ ist algebraisch, als Nullstelle des Polynoms $X - \alpha \in \mathbb{Q}[X]^*$. Die reelle Zahl $\alpha = \sqrt{3}$ ist nicht rational, aber immerhin algebraisch, denn α ist Nullstelle von $X^2 - 3 \in \mathbb{Q}[X]^*$.
Ist $7^{2/3}$ algebraisch? Ja, $A = X^3 - 7^2 \in \mathbb{Q}[X]^*$ erfüllt $A(7^{2/3}) = 0$.

Gibt es transzendente Zahlen? Ja, dank Cantors Abzählargument **??**:
Die algebraischen Zahlen $\mathbb{A}$ sind abzählbar, doch $\mathbb{R}$ ist überabzählbar!

Vereinfacht zusammengefasst: Fast alle reellen Zahlen sind transzendent.
Wenn Sie „zufällig“ eine wählen, so ist sie „fast sicher“ transzendent.

Gibt es transzendente Zahlen?

Satz B2ı: Die algebraischen Zahlen sind abzählbar.

Eine reelle Zahl $\alpha \in \mathbb{R}$ heißt **algebraisch** über $\mathbb{Q}$, wenn sie Nullstelle eines rationalen Polynoms $P \in \mathbb{Q}[X]^*$ ist. Andernfalls heißt α **transzendent**.

$$\mathbb{A} := \bigcup_{P \in \mathbb{Q}[X]^*} \{\, \alpha \in \mathbb{R} \mid P(\alpha) = 0 \,\}$$

Die Menge $\mathbb{A} \subseteq \mathbb{R}$ der algebraischen Zahlen ist abzählbar, kurz $\mathbb{A} \cong \mathbb{N}$.
Somit ist das Komplement $\mathbb{T} = \mathbb{R} \setminus \mathbb{A}$ überabzählbar, genauer $\mathbb{T} \cong \mathbb{R}$.

Beweis: Die Menge aller Polynome vom Grad $< n$ ist abzählbar:

$$\mathbb{Q}[X]_{<n} \underset{\text{Def}}{\cong} \mathbb{Q}^n \underset{\text{B2E}}{\cong} \mathbb{N}^n \underset{\text{B2D}}{\cong} \mathbb{N}$$

Die abzählbare Vereinigung $\mathbb{Q}[X] = \bigcup_{n \in \mathbb{N}} \mathbb{Q}[X]_{<n}$ ist abzählbar (**??**).
Zu jedem Polynom $P \in \mathbb{Q}[X]^*$ ist die Nullstellenmenge in $\mathbb{R}$ endlich.
Somit ist die abzählbare Vereinigung $\mathbb{A} = \bigcup_P P^{-1}(0)$ abzählbar (**??**).
Wir haben also $\mathbb{A} \preceq \mathbb{N}$. Zusammen mit $\mathbb{N} \subseteq \mathbb{A}$ folgt $\mathbb{A} \cong \mathbb{N}$ (B2o). QED

Algebraische vs transzendente Zahlen

Bereits im 18. Jahrhundert entwickelte sich langsam die Vorstellung von Transzendenz und die Vermutung, dass es transzendente Zahlen gibt, so etwa bei Gottfried Wilhelm Leibniz (1646–1716) und Leonhard Euler (1707–1783). Euler formulierte zwar keine klare Definition, war aber überzeugt, dass es solche „schwer fassbaren“ Zahlen geben müsse. Ebenso wie „irrational“ für ‘unvernünftig’ ist auch „transzendent“ für ‘jenseits aller Vernunft’ zunächst ein negativer Begriff des Erstaunens, ja des Erschreckens. Diese Zahlen sind algebraisch nicht zugänglich.

Erste Konstruktionen und Nachweise transzendenter Zahlen gelangen 1844 Joseph Liouville (1809–1882), etwa für die Liouville-Konstante

$$L = \sum_{k=1}^{\infty} 10^{-k!} = 0.11000100000000000000000001000\ldots$$

Georg Cantor bewies 1874 erneut die Existenz transzendenter Zahlen: Überraschenderweise sind sogar fast alle reellen Zahlen transzendent! Im Gegensatz zu Liouville ist Cantors Beweis jedoch nicht konstruktiv; er hilft nicht, einer fest gegebenen Zahl Transzendenz nachzuweisen.

Algebraische vs transzendente Zahlen

⚠ Die Angabe des betrachteten Grundkörpers ist wichtig.
Wenn wir nichts weiter dazusagen, arbeiten wir in $\mathbb{C}$ über $\mathbb{Q}$.

Übung: Jede komplexe Zahl $\alpha \in \mathbb{C}$ ist algebraisch über $\mathbb{R}$, nämlich Nullstelle eines quadratischen Polynoms $P \in \mathbb{R}[X]^*$.

Jeder komplexen Zahl $\alpha \in \mathbb{C}$ ordnen wir ihren Grad über $\mathbb{Q}$ zu:

$$\deg_{\mathbb{Q}} : \mathbb{C} \to \mathbb{N} \cup \{\infty\} : \alpha \mapsto \inf\{\deg P \,|\, P \in \mathbb{Q}[X]^* \wedge P(\alpha) = 0\}$$

Die algebraischen Zahlen sind die von endlichem Grad:

$$\mathbb{A} = \{\alpha \in \mathbb{C} \,|\, \deg_{\mathbb{Q}}(\alpha) < \infty\} = \bigcup_{P \in \mathbb{Q}[X]^*} \{\alpha \in \mathbb{C} \,\big|\, P(\alpha) = 0\}$$

Jede algebraische Zahl hat demnach ein Minimalpolynom:

$$\mu : \mathbb{A} \to \mathbb{Q}[X] : \alpha \mapsto \mu_\alpha \in \mathbb{Q}[X]^1_n,\ n = \deg_{\mathbb{Q}}(\alpha),\ \mu_\alpha(\alpha) = 0$$

Beispiel: Für $\alpha = \pm\sqrt{2}$ gilt $\mu_\alpha = X^2 - 2$. Demnach ist μ nicht injektiv, denn μ_α hat mehrere Nullstellen, die **konjugierten Elemente** zu α.
(Im Beweis von B2ı können wir daher nicht $\mathbb{A} \hookrightarrow \mathbb{Q}[X]$ nutzen.)

Transzendenz von e und π

Cantors grundlegende Elementezählung hat erstaunliche Konsequenzen:

☺ Wenn Sie zufällig gleichverteilt eine reelle Zahl $\alpha \in [0,1]$ wählen, dann ist das Ergebnis mit 100% Wahrscheinlichkeit transzendent.
Das ist Segen und Fluch von elegant-nicht-konstruktiven Beweisen.

☹ Sobald Sie jedoch eine konkrete Zahl $\alpha \in \mathbb{R}$ vorliegen haben, ist es meist extrem schwierig, ihr Transzendenz nachzuweisen.
Hierzu nenne ich zwei berühmte Ergebnisse:

Beispiel: Die Eulersche Zahl e ist transzendent. (C. Hermite, 1873)

$$\mathrm{e} = \exp(1) = \sum_{k=0}^{\infty} \frac{1}{k!} = 1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \frac{1}{4!} + \frac{1}{5!} + \ldots$$

Beispiel: Die Kreiszahl π ist transzendent. (F. Lindemann, 1882)

$$\frac{\pi}{4} = \arctan(1) = \sum_{k=0}^{\infty} \frac{(-1)^k}{2k+1} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \frac{1}{11} + \ldots$$

Allgemein: Ist $\alpha \in \mathbb{C}^*$ algebraisch, so ist $\mathrm{e}^\alpha \in \mathbb{C}$ transzendent.

Transzendenz von e und π

☺ Damit löste Lindemann ein über zweitausend Jahre altes Problem:
Die Quadratur des Kreises allein mit Zirkel und Lineal ist unmöglich!

Bei der Vergeblichkeit der so ausserordentlich zahlreichen Versuche, die Quadratur des Kreises mit Cirkel und Lineal auszuführen, hält man allgemein die Lösung der bezeichneten Aufgabe für unmöglich; es fehlte aber bisher ein Beweis dieser Unmöglichkeit; nur die Irrationalität von π und von π^2 ist festgestellt. Jede mit Cirkel und Lineal ausführbare Construction lässt sich mittelst algebraischer Einkleidung zurückführen auf die Lösung von linearen und quadratischen Gleichungen, also auch auf die Lösung einer Reihe von quadratischen Gleichungen, deren erste rationale Zahlen zu Coefficienten hat, während die Coefficienten jeder folgenden nur solche irrationale Zahlen enthalten, die durch Auflösung der vorhergehenden Gleichungen eingeführt sind. Die Schlussgleichung wird also durch wiederholtes Quadriren übergeführt werden können in eine Gleichung geraden Grades, deren Coefficienten rationale Zahlen sind. Man wird sonach die Unmöglichkeit der Quadratur des Kreises darthun, wenn man nachweist, dass die Zahl π überhaupt nicht Wurzel einer algebraischen Gleichung irgend welchen Grades mit rationalen Coefficienten sein kann. Den dafür nöthigen Beweis zu erbringen, ist im Folgenden versucht worden.

Ferdinand von Lindemann (1852–1939), *Über die Zahl π* (1882)

Transzendenz der eulerschen Zahl $\mathrm{e} = 2.71828\ldots$

Ich beweise als Ausblick hier nur die Transzendenz von e und folge dabei
📖 A. Gelfond: *Transcendental and algebraic numbers.* Dover 1960. 42–44
Hermites Beweis ist eine geniale Kombination aus Analysis und Algebra.

Beweis: Wir zeigen $\mathbb{Q}$–lineare Unabhängigkeit durch Widerspruch.
(0) Bei linearer Abhängigkeit gäbe es $a_0, \ldots, a_n \in \mathbb{Q}$ mit $a_0 \neq 0$ und

$$a_0 + a_1\,\mathrm{e} + a_2\,\mathrm{e}^2 + \cdots + a_n\,\mathrm{e}^n = 0.$$

Wir dürfen und werden im Folgenden $a_0, \ldots, a_n \in \mathbb{Z}$ annehmen, notfalls multiplizieren wir die Gleichung (0) mit einem gemeinsamen Nenner.
(1) Es gilt $\partial_x\,\mathrm{e}^x = \mathrm{e}^x$. Für $f \in \mathscr{C}^1(\mathbb{R},\mathbb{R})$ folgt dank partieller Integration:

$$\mathrm{e}^x \int_{t=0}^{x} \mathrm{e}^{-t}\,f(t)\,\mathrm{d}t = \mathrm{e}^x\,f(0) - f(x) + \mathrm{e}^x \int_{t=0}^{x} \mathrm{e}^{-t}\,f'(t)\,\mathrm{d}t$$

(2) Für $f \in \mathbb{R}[t]_{\leq N}$ und $F := f + f' + \cdots + f^{(N)}$ iterieren wir (1) zu:

$$\mathrm{e}^x \int_{t=0}^{x} \mathrm{e}^{-t}\,f(t)\,\mathrm{d}t = \mathrm{e}^x\,F(0) - F(x)$$

🙂 Das ist Hermites genialer Kunstgriff. Davon profitieren wir.

Transzendenz der eulerschen Zahl $\mathrm{e} = 2.71828\ldots$

(3) Wir summieren (2) für $x = k = 0, \ldots, n$ zu:

$$\textstyle\sum_{k=0}^{n} a_k\,\mathrm{e}^k \int_{t=0}^{k} \mathrm{e}^{-t}\,f(t)\,\mathrm{d}t = F(0)\sum_{k=0}^{n} a_k\,\mathrm{e}^k - \sum_{k=0}^{n} a_k F(k)$$

Sei nun $p > \max\{n, |a_0|\}$ prim und $f(t) = t^{p-1}(t-1)^p \cdots (t-n)^p/(p-1)!$.
(4) Es gilt $F(0) \in \mathbb{Z} \setminus p\mathbb{Z}$, denn wir finden $0 = f(0) = \ldots = f^{(p-2)}(0)$ und $f^{(p-1)}(0) = [(-1)^n n!]^p \in \mathbb{Z} \setminus p\mathbb{Z}$ und schließlich $f^{(i)}(0) \in p\mathbb{Z}$ für $i \geq p$.
(5) Für $k = 1, \ldots, n$ hingegen gilt $F(k) \in p\mathbb{Z}$, denn hier finden wir $0 = f(k) = \ldots = f^{(p-1)}(k)$ und schließlich $f^{(i)}(k) \in p\mathbb{Z}$ für $i \geq p$.
(6) Dank $a_0 \in \mathbb{Z} \setminus p\mathbb{Z}$ liegt $a_0 F(0)$ in $\mathbb{Z} \setminus p\mathbb{Z}$, somit auch $\sum_{k=0}^{n} a_k F(k)$.
(7) Die linke Seite von (3) schätzen wir grob nach oben ab durch:

$$\begin{aligned} \left|\textstyle\sum_{k=1}^{n} a_k\,\mathrm{e}^k \int_{t=0}^{k} \mathrm{e}^{-t}\,f(t)\,\mathrm{d}t\right| &\leq \left[\textstyle\sum_{k=1}^{n} |a_k|\,\mathrm{e}^k\right] \int_{t=0}^{n} |f(t)|\,\mathrm{d}t \\ &\leq \left[\textstyle\sum_{k=1}^{n} |a_k|\,\mathrm{e}^k\right] n^{(n+1)p}/(p-1)! \;=\; a\,b^p/(p-1)! \;\to\; 0 \end{aligned}$$

(8) Damit erreichen wir folgenden Widerspruch für große Primzahlen p:
Die rechte Seite von (3) liegt in $\mathbb{Z} \setminus \{0\}$, die linke jedoch in $]-1, 1[$. QED

Satz B2ȷ: unendliches Komplement

Sei U eine unendliche Menge und $E \subset U$ eine endliche Teilmenge.
Dann ist das Komplement $U \setminus E$ unendlich, genauer gilt $U \setminus E \cong U$.

Aufgabe: Konstruieren Sie explizit eine Bijektion $(g, g') : U \setminus E \cong U$.

Lösung: Das Komplement $U \setminus E$ ist unendlich: Wäre $U \setminus E$ endlich, so auch die Vereinigung $U = (U \setminus E) \cup E$; das ist ein Widerspruch.

Seien $x_0, x_1, \dots, x_{n-1}$ die Elemente der Menge E. Wir setzen diese Nummerierung fort zu einer Injektion $\nu : \mathbb{N} \hookrightarrow U : k \mapsto x_k$ dank **??**.
Sei $F = \nu(\mathbb{N}_{\geq n}) \subseteq U$. Wir haben $(g', g) : E \cup F \cong F : x_k \leftrightarrows x_{n+k}$.
Dies erweitern wir zur ersehnten Bijektion $(g', g) : U \cong U \setminus E$ durch $g'(x) = g(x) = x$ für alle $x \in U \setminus (E \cup F)$.

☺ Die Konstruktion geeigneter Bijektionen ist eine eigene Kunst. Glücklicherweise verfügen Sie über wirksame, allgemeine Werkzeuge. Jedoch erfordert deren Nutzen in weiteren Konstruktionen etwas Übung.

Satz B2ĸ: überabzählbares Komplement

Sei U eine überabzählbare Menge und $A \subset U$ höchstens abzählbar.
Dann ist das Komplement $U \setminus A$ überabzählbar, genauer gilt $U \setminus A \cong U$.

Aufgabe: Konstruieren Sie explizit eine Bijektion $(g, g') : U \setminus A \cong U$.

Lösung: Das Komplement $U \setminus A$ ist überabzählbar: Wäre $U \setminus A$ abzählbar, so auch $U = (U \setminus A) \cup A$ dank **??**; das ist ein Widerspruch.

Demnach existiert eine Injektion $\nu : \mathbb{N} \hookrightarrow U \setminus A$ dank **??**. Sei $B = \nu(\mathbb{N})$.
Die Vereinigung $A \cup B$ ist abzählbar dank **??** und zudem unendlich.
Somit existiert eine Bijektion $(g', g) : A \cup B \cong B$. Wir erweitern diese zu $(g', g) : U \cong U \setminus A$ durch $g'(x) = g(x) = x$ für alle $x \in U \setminus (A \cup B)$.

Beispiele: Die Menge $\mathbb{Q}$ der rationalen Zahlen ist gleichmächtig zu $\mathbb{N}$.
Die Menge $\mathbb{I} = \mathbb{R} \setminus \mathbb{Q}$ der irrationalen Zahlen ist gleichmächtig zu $\mathbb{R}$.

Die Menge $\mathbb{A} \subseteq \mathbb{R}$ der algebraischen Zahlen ist abzählbar, also $\mathbb{A} \cong \mathbb{N}$.
Die transzendenten Zahlen $\mathbb{T} = \mathbb{R} \setminus \mathbb{A}$ sind überabzählbar, $\mathbb{T} \cong \mathbb{R}$. (**??**)

Satz B2ʟ: Mächtigkeit von Intervallen

(1) Jedes rationale Invervall $I \subseteq \mathbb{Q}$ ist entweder leer, $I = \emptyset$, einelementig, $I = \{a\}$, oder abzählbar unendlich, $I \cong \mathbb{Q}$.

(2) Jedes reelle Invervall $I \subseteq \mathbb{R}$ ist entweder leer, $I = \emptyset$, einelementig, $I = \{a\}$, oder überabzählbar, $I \cong \mathbb{R}$.

(3) Allgemein sei $(\mathbb{K}, +, \cdot, \leq)$ ein geordneter Körper. Jedes Intervall $I \subseteq \mathbb{K}$ mit mindestens zwei Elementen ist gleichmächtig zur Menge $\mathbb{K}$.

Beweis: (3) Gegeben seien $a, b \in I$ mit $a < b$. Daraus folgt $[a, b]_{\mathbb{K}} \subseteq I$. Wir haben einerseits die Inklusion $f : I \hookrightarrow \mathbb{K}$. Andererseits haben wir die Bijektion $\mathbb{K} \cong]-1, 1[_{\mathbb{K}}$ aus **??**, somit $g : \mathbb{K} \cong]-1, 1[_{\mathbb{K}} \cong]a, b[_{\mathbb{K}} \hookrightarrow I$. Der Satz von Cantor–Bernstein B2o konstruiert aus den Injektionen $f : I \hookrightarrow \mathbb{K}$ und $g : \mathbb{K} \hookrightarrow I$ die ersehnte Bijektion $(h, k) : I \cong \mathbb{K}$. QED

☺ Diese Konstruktion ist kurz und elegant und wunderbar explizit. Die folgende Aufgabe beleuchtet schöne, konkrete Konstruktionen, die sogar ganz ohne den Satz von Cantor–Bernstein auskommen.

Aufgabe: Konstruieren Sie explizit (möglichst einfache) Bijektionen $(f, f') : [a, b] \cong [0, 1]$, $(g, g') : [0, 1] \cong [0, 1[$ und $(h, h') :]0, 1] \cong]0, 1[$.
(Es gelingt natürlich mit dem allgemeinen Satz via Cantor–Bernstein B2o, die Herausforderung ist hier jedoch eine möglichst simple Konstruktion.)

Lösung: (0) Zunächst gilt $(\tau, \tau) : [a, b] \cong [a, b]$ dank $\tau : x \mapsto b + a - x$, und durch Einschränkung $(\tau, \tau) :]a, b[\cong]a, b[$ und $(\tau, \tau) : [a, b[\cong]a, b]$.

(1) Eine Bijektion $(f, f') : [a, b] \cong [0, 1]$ gelingt affin-linear und isoton mit $f(x) = (x - a)/(b - a)$ und $f'(y) = a + y(b - a)$. Damit gilt $f' \circ f = \mathrm{id}_{[a,b]}$ und $f \circ f' = \mathrm{id}_{[0,1]}$. Durch Einschränkung erhalten wir die Bijektionen $(f, f') : [a, b[\cong [0, 1[$ und $(f, f') :]a, b] \cong]0, 1]$ und $(f, f') :]a, b[\cong]0, 1[$.

(2) In $[0, 1]$ betrachten wir $X := \{ 2^{-n} \mid n \in \mathbb{N} \} = \{1, 1/2, 1/4, \dots\}$ und $Y := X/2 = \{1/2, 1/4, 1/8, \dots\}$. Wir definieren $g : [0, 1] \to [0, 1[$ durch $g(x) = x/2$ für $x \in X$ und $g(x) = x$ sonst, sowie $g' : [0, 1[\to [0, 1]$ durch $g'(y) = 2y$ für $y \in Y$ und $g'(y) = y$ sonst. Damit gilt $g' \circ g = \mathrm{id}_{[0,1]}$ und $g \circ g' = \mathrm{id}_{[0,1[}$. Wörtlich genauso konstruieren wir $(h, h') :]0, 1] \cong]0, 1[$.

Die Ordnung der rationalen Zahlen

Die rationalen Zahlen $(\mathbb{Q}, \leq)$ haben weder Minimum noch Maximum, sie sind abzählbar und außerdem dicht. Letzteres bedeutet: Zu je zwei Punkten $u < v$ in $\mathbb{Q}$ existiert ein Zwischenpunkt $z \in \mathbb{Q}$ mit $u < z < v$. Diese Eigenschaften charakterisieren $(\mathbb{Q}, \leq)$ bis auf Ordnungsisomorpie:

Satz B3A: Ordnung der rationalen Zahlen

Seien $(X, \leq)$ und $(Y, \leq)$ nicht-leere, total geordnete Mengen, ohne Minimum und Maximum, zudem abzählbar und dicht.

(1) Dann existiert ein Ordnungsisomorphismus $(X, \leq) \cong (Y, \leq)$.

Beispiele: Für $X = \mathbb{Z}[\frac{1}{2}] = \{ a/2^n \mid a \in \mathbb{Z},\ n \in \mathbb{N} \}$ gilt $(X, \leq) \cong (\mathbb{Q}, \leq)$.
Es gilt $(]-1, 1[_{\mathbb{Q}}, \leq) \cong (\mathbb{Q}, \leq)$, dies gelingt wunderbar explizit dank A1B.

Gegenbeispiele: Die geordneten Mengen $([0, 1]_{\mathbb{Q}}, \leq)$ und $([0, 1[_{\mathbb{Q}}, \leq)$ und $(]0, 1]_{\mathbb{Q}}, \leq)$ sind abzählbar und dicht, haben aber Minimum oder Maximum; daher sind sie nicht isomorph zu $(]0, 1[_{\mathbb{Q}}, \leq) \cong (\mathbb{Q}, \leq)$.
Es gilt $(\mathbb{Z}, \leq) \ncong (\mathbb{Q}, \leq)$, denn die Ordnung $(\mathbb{Z}, \leq)$ ist nicht dicht.
Es gilt $(\mathbb{R}, \leq) \ncong (\mathbb{Q}, \leq)$, denn die Menge $\mathbb{R}$ ist nicht abzählbar.

Die Ordnung der rationalen Zahlen

Beweis: Wir konstruieren eine ordnungstreue Bijektion $f : X \xrightarrow{\sim} Y$ nach der „Zick-Zack-Methode“ von Cantor (1895) und Hausdorff (1914).

Vorgelegt seien Abzählungen $\mathbb{N} \xrightarrow{\sim} X : k \mapsto a_k$ und $\mathbb{N} \xrightarrow{\sim} Y : k \mapsto b_k$. Rekursiv konstruieren wir $\emptyset = X_0 \subset X_1 \subset X_2 \subset \dots$ mit $X = \bigcup_{n \in \mathbb{N}} X_n$ und $\emptyset = Y_0 \subset Y_1 \subset Y_2 \subset \dots$ mit $Y = \bigcup_{n \in \mathbb{N}} Y_n$ und darauf ordnungstreue Bijektionen $f_n : X_n \to Y_n$ mit $f_{n+1}|_{X_n}^{Y_n} = f_n$. Der Anfang $n = 0$ ist trivial.

Sei $n \geq 0$ und $f_n : X_n \xrightarrow{\sim} Y_n$ bereits konstruiert. Für n gerade sei $i \in \mathbb{N}$ minimal mit $a_i \notin X_n$. Sei $j \in \mathbb{N}$ minimal mit $b_j \notin Y_n$, sodass $a_i \mapsto b_j$ die Bijektion $f_n : X_n \xrightarrow{\sim} Y_n$ monoton fortsetzt. Solch ein b_j existiert, da $f_n(X_n) = Y_n$ endlich ist und $Y \supset Y_n$ dicht ohne Extrema. Wir setzen $X_{n+1} := X_n \cup \{a_i\}$ und $Y_{n+1} := Y_n \cup \{b_j\}$ und $f_{n+1} = f_n \cup \{(a_i, b_j)\}$.

Hausdorffs Kniff: Für n ungerade tauschen wir die Rollen von X und Y. Das geschickte Hin-und-Her garantiert $X = \bigcup_{n \in \mathbb{N}} X_n$ und $Y = \bigcup_{n \in \mathbb{N}} Y_n$. Die Isomorphismen $f_n : X_n \xrightarrow{\sim} Y_n$ erfüllen $f_{n+1}|_{X_n}^{Y_n} = f_n$ für alle $n \in \mathbb{N}$, vereinigen sich also zum Isomorphismus $f = \bigcup_{n \in \mathbb{N}} f_n : X \to Y$. QED

Die Ordnung der rationalen Zahlen

Diese genial-einfache Konstruktion zeigt noch etwas mehr:

Satz B3: Ordnung der rationalen Zahlen

(2) Jeder Ordnungsisomorphismus $g : (A, \leq) \xrightarrow{\sim} (B, \leq)$ zwischen endlichen Teilmengen $A \subset X$ und $B \subset Y$ lässt sich fortsetzen zu einem Ordnungsisomorphismus $f : (X, \leq) \xrightarrow{\sim} (Y, \leq)$.

(3) Dazu genügt, dass $A \cap [u, v]$ endlich ist für alle $u, v \in X$, ebenso B in Y.

Beweis: Wir beginnen die obige Konstruktion mit $f_n = g : A \xrightarrow{\sim} B$. Die Ausführung empfehle ich als Übung zur Wiederholung.

⚠ Für beliebige Teilmengen A und B gilt diese Fortsetzbarkeit nicht!

Gegenbeispiel: Zu $A = \mathbb{N} \subset \mathbb{Q}$ und $B = \{1 - 2^{-n} \mid n \in \mathbb{N}\} \subset \mathbb{Q}$ ist $g : A \xrightarrow{\sim} B : n \mapsto 1 - 2^{-n}$ ein Ordnungsisomorphismus. Er lässt sich nicht fortsetzen zu $f : (\mathbb{Q}, \leq) \xrightarrow{\sim} (\mathbb{Q}, \leq)$: Angenommen, wir hätten $f : (\mathbb{Q}, \leq) \xrightarrow{\sim} (\mathbb{Q}, \leq)$ mit $f|_A^B = g$. Zu $y = 1 > 1 - 2^{-n}$ gehört dann $x = f^{-1}(y) \in \mathbb{Q}$ mit $x > n$ für alle $n \in \mathbb{N}$, und das ist unmöglich.

Die Ordnung der rationalen Zahlen

Cantor bewies dieses Ergebnis bereits 1884. Sein Artikel zur *Theorie der Ordnungstypen* wurde von der Zeitschrift Acta Mathematica zunächst zur Publikation angenommen, doch der Herausgeber Mittag–Leffler war persönlich von dem Thema nicht überzeugt und bat Cantor, den Artikel zurückzuziehen. So erschien der Satz erst 1895, elf Jahre später.

Aufgabe: Cantor bewies den Satz noch nicht mit der Zick-Zack-Methode, sondern mit der einseitigen Variante. Gelingt die Konstruktion dennoch?

Lösung: Ja! In Cantors Konstruktion gilt weiterhin $X = \bigcup_{n \in \mathbb{N}} X_n$. Wir müssen nur $Y = \bigcup_{n \in \mathbb{N}} Y_n$ zeigen, also die Surjektivität von f. Angenommen, es gäbe ein $b_j \in Y \setminus \bigcup_{n \in \mathbb{N}} Y_n$. Wir wählen j minimal. Sei $n \geq 0$ minimal, sodass $\{b_0, \dots, b_{j-1}\} \subseteq Y_n = \{f(a_0), \dots, f(a_{n-1})\}$. Sei $i \geq n$ minimal, sodass a_i genauso zu $a_0, \dots, a_{n-1}$ liegt wie b_j zu $f(a_0), \dots, f(a_{n-1})$. In Cantors Konstruktion gilt dann $f_i : a_i \mapsto b_j$. Das widerspricht unserer Annahme. Also ist f surjektiv.

☺ Hausdorffs eleganter Zick-Zack-Kniff vereinfacht das Argument, und verleiht dem verblüffenden Satz einen ebenso genialen Beweis.

Isomorphiespiele: Samson gegen Delila

Isomorphiespiele: Samson gegen Delila

Wir spielen auf zwei totalen Ordnungen, hier ein konkretes Beispiel:

$$X = \{0 < 1 < 2 < 3 < 4 < 5 < 6 < 7\}$$
$$Y = \{0 < 1 < 2 < 3 < 4 < 5 < 6 < 7 < 8 < 9\}$$

In Runde $n = 1, 2, 3, \ldots$ ziehen die Spieler Elemente $(a_n, b_n) \in X \times Y$:
(0) Verfügbar sind $X_n = X \setminus \{a_1, \ldots, a_{n-1}\}$ und $Y_n = Y \setminus \{b_1, \ldots, b_{n-1}\}$.
(1) Samson (*spoiler*) wählt ein Element, entweder $a_n \in X_n$ oder $b_n \in Y_n$.
(2) Delila (*duplicator*) wählt komplementär dazu $b_n \in Y_n$ oder $a_n \in X_n$.

Dabei muss stets Monotonie gelten, also $a_i < a_j \Leftrightarrow b_i < b_j$ für alle i, j.
Anschaulich verbinden wir alle Paare (a_i, b_i) ohne Überkreuzungen.

Samson bekommt anfangs $5€$ und zahlt $1€$ an Delila für jede Antwort.
Samson will einen Unterschied zwischen $(X, \leq)$ und $(Y, \leq)$ aufdecken.
Delila will dies verhindern oder zumindest möglichst lange verzögern.

Im Casino spielen zwei Teams, Links und Rechts. Um die unglückliche Asymmetrie aufzuheben, spielt Team Links auf der linken Tafel Samson und auf der rechten Tafel Delila, Team Rechts entsprechend umgekehrt.

Isomorphiespiele: Samson gegen Delila

Erfolgreiche Strategien ähneln einer binären Suche: Teile und herrsche! Sie wollen eine nachweislich optimale Strategie? Hier ist die Challenge:

Satz B3A: Isomorphiespiel zwischen endlichen Totalordnungen

Zu $k := |X| < |Y| < \infty$ sei $\nu(k)$ die kleinste Zahl n, für die Samson eine Strategie hat, mit der er spätestens in Runde $n+1$ gewinnt. Dann gilt

$$\nu(k) = \lfloor \log_2(k+1) \rfloor.$$

Aufgabe: Wie findet man dieses schöne Ergebnis? Bestimmen Sie $\nu(k)$ für kleine Werte $k = 0, 1, 2, 3, 4, \dots$. Daraus entsteht eine Vermutung!

Lösung: Kleine Werte können Sie leicht austüfteln. Dabei entsteht die folgende Tabelle, dazu eine allgemeine Vermutung und Beweisidee.

$k =$	0	1	2	3	4	5	6	7	…	14	15	…	30	31	…
$\nu(k) =$	0	1	1	2	2	2	2	3	…	3	4	…	4	5	…

Die Werte entstehen aus $\lambda(0) = 0$ rekursiv durch $\lambda(k+1) = \lambda(\lfloor k/2 \rfloor) + 1$. Inkremente entstehen nur bei $1, 3, 7, 15, \dots$, also gilt $\lambda(k) = \lfloor \log_2(k+1) \rfloor$.

Isomorphiespiele: Samson gegen Delila

Beweis: Wir beweisen (1) $\nu(k) \leq \lambda(k)$ und (2) $\nu(k) \geq \lambda(k)$ per Induktion über $k \in \mathbb{N}$. Für $k = 0$ gilt $\nu(0) = 0 = \lambda(0)$. Im Folgenden sei also $k \geq 1$.

(1) Samson halbiert $Y = Y_{<b} \sqcup \{b\} \sqcup Y_{>b}$ mit $|Y_{>b}| - |Y_{<b}| \in \{0, 1\}$. Nach Delilas Zug $X = X_{<a} \sqcup \{a\} \sqcup X_{>a}$ gilt $|X_{<a}| \neq |Y_{<b}|$ oder $|X_{>a}| \neq |Y_{>b}|$. Daraus wählt Samson (X', Y') mit $|X'|$ minimal. Damit erreicht Samson $|X'| \leq \lfloor (k-1)/2 \rfloor$ und spielt weiter auf (X', Y'). Per Induktion folgt:

$$\nu(k) \;\leq\; 1 + \nu(\lfloor (k-1)/2 \rfloor) \;\leq\; 1 + \lambda(\lfloor (k-1)/2 \rfloor) \;=\; \lambda(k)$$

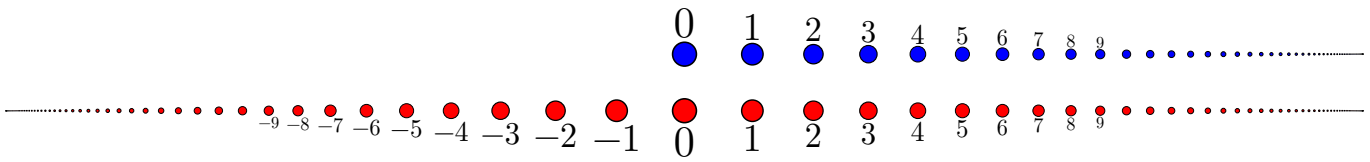
(2) Egal wie Samson zieht, entweder $a \in X$ oder $b \in Y$, Delila kann stets so parieren, dass jedes der beiden Intervallpaare (X', Y') links und rechts $\lfloor (k-1)/2 \rfloor \leq |X'| < |Y'|$ oder $|X'| = |Y'|$ erfüllt. Per Induktion folgt:

$$\nu(k) \;\geq\; 1 + \nu(\lfloor (k-1)/2 \rfloor) \;\geq\; 1 + \lambda(\lfloor (k-1)/2 \rfloor) \;=\; \lambda(k)$$

Das beweist den Satz durch Konstruktion optimaler Strategien. QED

Ganz praktisch können Sie diese Strategien direkt erproben: Spielen! Sowohl (1) als auch (2) erfordern einige Fallunterscheidungen: Übung!

Isomorphiespiele: Samson gegen Delila



Wir spielen $(\mathbb{N}, \leq)$ gegen $(\mathbb{Z}, \leq)$. Samsons Gewinnstrategie als Formel:

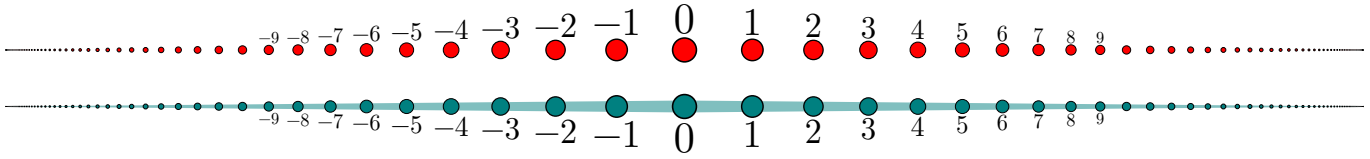
$$\exists a_1 \in \mathbb{N} \ \forall a_2 \in \mathbb{N} : a_1 \leq a_2$$
$$\forall b_1 \in \mathbb{Z} \ \exists b_2 \in \mathbb{Z} \ : b_1 > b_2$$

Die erste Aussage ist wahr für $(\mathbb{N}, \leq)$. Die zweite Aussage negiert die erste und ist wahr für $(\mathbb{Z}, \leq)$; wir ersetzen $\mathbb{N}$ durch $\mathbb{Z}$ und a_n durch b_n. Diese Formel unterscheidet also beide Strukturen! Das übersetzt Samson in seine Gewinnstrategie, indem er jeweils die Existenzquantoren spielt.

Ausführlich: Samson wählt das kleinste Element $a_1 = 0$ in $(\mathbb{N}, \leq)$. Delila antwortet mit irgendeinem Element b_1 in $(\mathbb{Z}, \leq)$. Samson wählt dazu nun b_2 in $(\mathbb{Z}, \leq)$ mit $b_2 < b_1$. Daraufhin muss Delila aufgeben.

☺ Die Anzahl der Runden entspricht der Anzahl der Variablen.

Isomorphiespiele: Samson gegen Delila



Wir spielen $(\mathbb{Z}, \leq)$ gegen $(\mathbb{Q}, \leq)$. Samsons Gewinnstrategie als Formel:

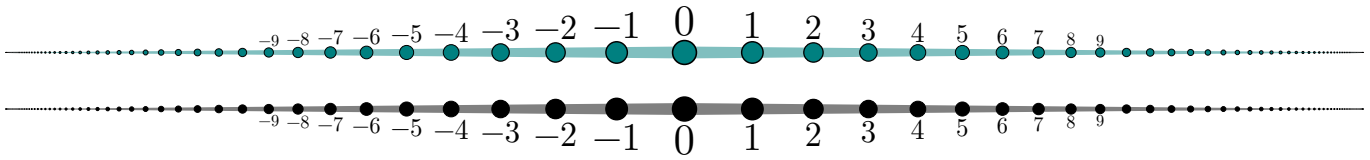
$$\exists a_1 \in \mathbb{Z} \ \exists a_2 \in \mathbb{Z} \ \forall a_3 \in \mathbb{Z} : [\, a_1 < a_2 \wedge (a_1 \geq a_3 \vee a_3 \geq a_2) \,]$$
$$\forall b_1 \in \mathbb{Q} \ \forall b_2 \in \mathbb{Q} \ \exists b_3 \in \mathbb{Q} : [\, b_1 \geq b_2 \vee (b_1 < b_3 \wedge b_3 < b_2) \,]$$

Die zweite Aussage ist wahr für $(\mathbb{Q}, \leq)$; sie besagt, die Ordnung ist dicht. Die erste Aussage negiert die zweite und ist wahr für $(\mathbb{Z}, \leq)$, da nicht dicht. Diese Formel unterscheidet also beide Strukturen! Das übersetzt Samson in seine Gewinnstrategie, indem er die Existenzquantoren spielt.

Ausführlich: Samson wählt zwei Elemente a_1 und $a_2 = a_1 + 1$ in $(\mathbb{Z}, \leq)$. Delila antwortet mit Elementen b_1 und b_2 in $(\mathbb{Q}, \leq)$ mit $b_1 < b_2$. Samson wählt b_3 in $(\mathbb{Q}, \leq)$ mit $b_1 < b_3 < b_3$. Daraufhin muss Delila aufgeben.

☺ Die Anzahl der Runden entspricht der Anzahl der Variablen.

Isomorphiespiele: Samson gegen Delila



Wir spielen $(\mathbb{Q}, \leq)$ gegen $(\mathbb{R}, \leq)$. Hier kommt das Spiel nie zum Ende!

Die geordneten Mengen $(\mathbb{Q}, \leq)$ und $(\mathbb{R}, \leq)$ sind nicht isomorph, schon die zugrundeliegenden Mengen $\mathbb{Q}$ und $\mathbb{R}$ erlauben keine Bijektion: Die rationalen Zahlen $\mathbb{Q}$ sind abzählbar, die reellen Zahlen $\mathbb{R}$ überabzählbar.

Dennoch führt das Isomorphiespiel (in nur endlicher Zeit) zu keiner Entscheidung: Weder Samson noch Delila kann einen Gewinn erzwingen, da dem jeweils anderen immer noch weitere Zugmöglichkeiten bleiben.

Gleichbedeutend: Diese beiden Ordnungen sind **elementar äquivalent**, jede Aussage der Logik erster Stufe (endlich viele Quantoren je über eine Elementvariable) hat für $(\mathbb{Q}, \leq)$ und $(\mathbb{R}, \leq)$ denselben Wahrheitswert.

☺ Es gibt nicht-isomorphe Modelle, die elementar äquivalent sind!

Isomorphiespiele: Samson gegen Delila

Wir erklären die **n–Äquivalenz** $(X, \leq) \equiv_n (Y, \leq)$ zweier Ordnungen dadurch, dass Delila immer mindestens n Runden überstehen kann.

Dem gegenüber steht der **Quantorenrang** $\mathrm{qr}(\varphi)$ einer Formel $\varphi \in \mathrm{FO}(\leq)$ als die Schachtelungstiefe der Quantoren: Ist φ atomar, also von der Form $(x \leq y)$, so gilt $\mathrm{qr}(\varphi) := 0$. Rekursiv definieren wir $\mathrm{qr}(\neg\varphi) := \mathrm{qr}(\varphi)$ und $\mathrm{qr}(\varphi \vee \psi) = \mathrm{qr}(\varphi \wedge \psi) := \max\{\mathrm{qr}(\varphi), \mathrm{qr}(\psi)\}$ für alle Junktoren sowie $\mathrm{qr}(\forall x : \varphi) = \mathrm{qr}(\exists x : \varphi) := \mathrm{qr}(\varphi) + 1$ für die Quantoren. Wir schreiben $\mathrm{FO}_n(\leq)$ für die Menge aller Formeln von Quantorenrang höchstens n.

Satz B3в: Korrespondenzsatz von Ehrenfeucht–Fraïssé

Genau dann gilt n–Äquivalenz $(X, \leq) \equiv_n (Y, \leq)$, wenn jede Formel $\varphi \in \mathrm{FO}_n(\leq)$, vom Quantorenrang $\leq n$, auf beiden Modellen denselben Wahrheitswert ergibt, formal geschrieben $((X, \leq) \vDash \varphi) \Leftrightarrow ((Y, \leq) \vDash \varphi)$.

Der Beweis gelingt per Induktion über n. Dies wird hier nicht ausgeführt.
📖 N. Immermann: *Descriptive Complexity.* Springer 1999, Thm. 6.10.
L. Libkin: *Elements of Finite Model Theory.* Springer 2012, Thm. 3.9.

Satz B3c: Grundregeln zur Termumformung, Dedekind 1888

(0) In den natürlichen Zahlen $(\mathbb{N}, +, 0, \cdot, 1, \hat{})$ gilt für alle $x, y, z \in \mathbb{N}$:

(A1)	$x + y = y + x$	(M1)	$x \cdot y = y \cdot x$
(A2)	$(x + y) + z = x + (y + z)$	(M2)	$(x \cdot y) \cdot z = x \cdot (y \cdot z)$
(A3)	$x + 0 = x$	(M3)	$x \cdot 1 = x$
(D0)	$x \cdot 0 = 0$	(D1)	$x \cdot (y + z) = (x \cdot y) + (x \cdot z)$
(P0)	$x^0 = 1$	(P1)	$x^{y+z} = x^y \cdot x^z$
(P2)	$x^1 = x$	(P3)	$x^{y \cdot z} = (x^y)^z$
(P4)	$1^x = 1$	(P5)	$(x \cdot y)^z = x^z \cdot y^z$
(P6)	$0^x = 0$ für $x \neq 0$		

Dies sind die 15 Grundregeln, die wir aus der Schule kennen und lieben und alltäglich in jeder Rechnung einsetzen, etwa zur Zifferndarstellung. Wie üblich kürzen wir $x \cdot y$ ab zu xy, sparen Klammern gemäß Potenz-vor-Punkt-vor-Strich und nutzen $2 = 1 + 1$, $3 = 2 + 1$, $4 = 3 + 1$, $5 = 4 + 1$, ...

Beispiel: Es gelten weitere nützliche Identitäten, für alle $x, y \in \mathbb{N}$ etwa:

$$x + (y \cdot x) = x \cdot (y + 1)$$
$$(x + y)^2 = x^2 + 2xy + y^2$$

Übung: Müssen wir diese Identitäten als weitere Axiome hinzufügen? Nein, wir können sie aus den obigen Grundregeln ableiten! Allgemein:

Satz B3c: polynomiale Identitäten

(1) Gilt $f(x_1, \dots, x_n) = g(x_1, \dots, x_n)$ für zwei Formeln f und g über $(\mathbb{N}, +, 0, \cdot, 1)$ und alle $x_1, \dots, x_n \in \mathbb{N}$, so können wir diese Gleichheit bereits aus den ersten acht Grundregeln (A123, M123, D01) ableiten.

Beweisskizze: Beide Seiten der Gleichung sind Polynome in $x_1, \dots, x_n$. Ausmultiplizieren und Monomesammeln bringt sie in Standardform. Für diese genügt es, die Koeffizienten zu vergleichen. (Warum?) QED

☺ Der Kalkül der obigen Grundregeln ist in diesem Sinne *vollständig* und jede Identität im Halbring $(\mathbb{N}, +, 0, \cdot, 1)$ ist algorithmisch *entscheidbar*.

Die Saga der *high school identities*

Der Logiker Alfred Tarski (1901–1983) vermutete in den 1960er Jahren die Vollständigkeit auch für $(\mathbb{N}, +, 0, \cdot, 1, \hat{})$, mit Potenzierung, konnte dies aber nicht beweisen. Diese Frage wurde berühmt als *Tarski's high school algebra problem:* Lässt sich jede Identität in $(\mathbb{N}, +, 0, \cdot, 1, \hat{})$ aus den 15 Grundregeln ableiten? Diese harmlos anmutende Frage beschäftigte viele prominente Logiker und erwies sich als überraschend schwierig.

Alex Wilkie zeigte 1981, dass Tarskis Vermutung falsch ist. Das war eine große Überraschung, und der Beweis ist erfreulich konkret und leicht:

Satz B3c: Wilkie 1981

(2) In $(\mathbb{N}, +, 0, \cdot, 1, \hat{})$ gilt für alle $x, y \in \mathbb{N}$ die folgende Identität $W(x, y)$:

$$\begin{aligned} &((1+x)^y + (1+x+x^2)^y)^x \cdot ((1+x^3)^x + (1+x^2+x^4)^x)^y \\ = \; &((1+x)^x + (1+x+x^2)^x)^y \cdot ((1+x^3)^y + (1+x^2+x^4)^y)^x \end{aligned}$$

(3) Sie lässt sich jedoch nicht aus Dedekinds 15 Grundregeln (0) ableiten.

Aufgabe: Beweisen Sie zunächst die Gültigkeit von Wilkies Identität (2).

Die Saga der *high school identities*

Lösung: (2) Zu $x \in \mathbb{N}$ haben wir $\bar{x} := 1 - x + x^2 \in \mathbb{N}_{\geq 1}$ und damit

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

Das ist der entscheidende Trick, ab hier genügen Dedekinds Grundregeln. Genauer: Für $x = 0$ setzen wir $\bar{x} = 1$, für $x = v + 1$ setzen wir $\bar{x} = 1 + vx$. Dank (1) folgt die obige Faktorisierung für alle $x \in \mathbb{N}$. (Nachrechnen!) Beide Seiten von Wilkies Identität $W(x, y)$ sind demnach gleich

$$((1+x)^y + (1+x+x^2)^y)^x \cdot \bar{x}^{xy} \cdot ((1+x)^x + (1+x+x^2)^x)^y.$$

Können wir dies allein aus den Grundregeln ableiten? Wilkies zeigte, dass dies unmöglich ist. Wie können wir dies beweisen? Wenn Sie zeigen wollen, dass etwas *möglich* ist, dann ist meist der beste Beweis, es zu tun! Wenn Sie zeigen wollen, dass etwas *nicht möglich* ist, dann genügt nicht, es nicht zu tun… oder erfolglos zu versuchen und frustriert aufzugeben. Die Unmöglichkeit beweisen wir, indem wir ein Hindernis benennen!

Die Saga der *high school identities*

📖 S.N. Burris, K.A. Yeats: *The saga of the high school identities.* Algebra Universalis 52 (2004) 325–342. Zum Beweis der Unmöglichkeit (3) zitiere ich ihr verblüffendes Argument durch ein 13elementiges Gegenmodell:

$+$	0	1	2	3	4	a	b	c	d	e	f	g	h
0	0	1	2	3	4	a	b	c	d	e	f	g	h
1	1	2	3	4	4	2	3	d	3	3	3	3	4
2	2	3	4	4	4	3	4	3	4	4	4	4	4
3	3	4	4	4	4	4	4	4	4	4	4	4	4
4	4	4	4	4	4	4	4	4	4	4	4	4	4
a	a	2	3	4	4	b	4	b	3	h	3	3	4
b	b	3	4	4	4	4	4	4	4	4	4	4	4
c	c	d	3	4	4	b	4	b	3	3	3	3	4
d	d	3	4	4	4	3	4	3	4	4	4	4	4
e	e	3	4	4	4	h	4	3	4	4	3	h	4
f	f	3	4	4	4	3	4	3	4	3	4	3	4
g	g	3	4	4	4	3	4	3	4	h	3	4	4
h	h	4	4	4	4	4	4	4	4	4	4	4	4

$\cdot$	0	1	2	3	4	a	b	c	d	e	f	g	h
0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	a	b	c	d	e	f	g	h
2	0	2	4	4	4	b	4	b	4	4	4	4	4
3	0	3	4	4	4	4	4	4	4	4	4	4	4
4	0	4	4	4	4	4	4	4	4	4	4	4	4
a	0	a	b	4	4	c	b	c	b	h	4	4	4
b	0	b	4	4	4	b	4	b	4	4	4	4	4
c	0	c	b	4	4	c	b	c	b	4	4	4	4
d	0	d	4	4	4	b	4	b	4	4	4	4	4
e	0	e	4	4	4	h	4	4	4	4	4	h	4
f	0	f	4	4	4	4	4	4	4	4	4	4	4
g	0	g	4	4	4	4	4	4	h	4	4	4	4
h	0	h	4	4	4	4	4	4	4	4	4	4	4

$\hat{}$	0	1	2	3	4	a	b	c	d	e	f	g	h
0	1	0	0	0	0	0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	1	2	4	4	4	4	4	4	4	f	4	4	4
3	1	3	4	4	4	e	4	4	4	g	4	e	h
4	1	4	4	4	4	4	4	4	4	4	4	4	4
a	1	a	c	c	c	c	c	c	c	c	c	c	c
b	1	b	4	4	4	4	4	4	4	4	4	4	4
c	1	c	c	c	c	c	c	c	c	c	c	c	c
d	1	d	4	4	4	f	4	4	4	4	4	4	4
e	1	e	4	4	4	4	4	4	4	h	4	4	4
f	1	f	4	4	4	4	4	4	4	4	4	4	4
g	1	g	4	4	4	h	4	4	4	4	4	h	4
h	1	h	4	4	4	4	4	4	4	4	4	4	4

Satz B3c: Burris–Yeats 2004

(4) Dieses Modell $(X, +, 0, \cdot, 1, \hat{})$ auf der Menge $X = \{0, 1, 2, 3, 4, a, \dots, h\}$ erfüllt Dedekinds 15 Grundregeln, aber nicht Wilkies Identität $W(a, e)$.

Die Saga der *high school identities*

Übung: Schreiben Sie ein Python-Programm, das für $(X, +, 0, \cdot, 1, \hat{})$ alle 15 Grundregeln nachprüft und alle Ausnahmen für $W(x, y)$ findet.

Lösung: Die Elemente der Menge X codieren wir durch $0, 1, \dots, 12$ und hinterlegen die obigen Tabellen als drei Arrays `add`, `mul`, `exp`.

```
print('Axioms', all([ add[x][y] == add[y][x]                              #A1
                and add[add[x][y]][z] == add[x][add[y][z]]                 #A2
                and add[x][0] == x                                        #A3
                and mul[x][y] == mul[y][x]                                #M1
                and mul[mul[x][y]][z] == mul[x][mul[y][z]]                #M2
                and mul[x][1] == x                                        #M3
                and mul[x][0] == 0                                        #D0
                and mul[x][add[y][z]] == add[mul[x][y]][mul[x][z]]        #D1
                and exp[x][0] == 1                                        #P0
                and exp[x][add[y][z]] == mul[exp[x][y]][exp[x][z]]        #P1
                and exp[x][1] == x                                        #P2
                and exp[x][mul[y][z]] == exp[exp[x][y]][z]                #P3
                and exp[1][x] == 1                                        #P4
                and exp[mul[x][y]][z] == mul[exp[x][z]][exp[y][z]]        #P5
                and (exp[0][x] == 0 or x == 0)                            #P6
    for x in range(0,13) for y in range(0,13) for z in range(0,13) ]))
```

Die Saga der *high school identities*

Im Nachhinein ist das genial einfach. Doch wie kommt man darauf? Das ist Teil einer langen Saga: Wilkies ursprünglicher Beweis (1981) war rein syntaktisch. Gurevič fand 1985 ein Gegenmodell mit 60 Elementen, später ein kleineres mit 34. Burris reduzierte dies 1988 auf 29 Elemente, 1990 auf 17, zusammen mit Yeats 2001 schließlich auf 13; ihre Methode verband monatelange Computersuche mit sachkundiger Optimierung.

Burris und Yeats vermuten, dass sie damit das Minimum gefunden haben, also keine noch kleineren Gegenmodelle existieren. Eine erschöpfende Computersuche könnte hier Klarheit schaffen, ist aber aufwändig und soweit ich weiß bisher noch nicht vollständig durchgeführt worden.

Vermutlich empfinden Sie den Beweis als kurz und einfach, doch das obige Gegenmodell als „künstlich“ und wenig erhellend. Völlig zu Recht! Seine Konstruktion durch „brute force“ bleibt leider noch unbefriedigend.

Bisher scheint kein „natürliches“ oder erhellendes Gegenmodell bekannt. Noch lehrreicher als ein möglichst kleines, aber obskures Gegenmodell wäre ein elegantes Gegenmodell, gut verständlich und aussagekräftig.

Die Saga der *high school identities*

Was passiert, wenn wir zu Dedekinds Grundregeln noch Wilkies Identität hinzufügen? Sind die Umformungsregeln damit vollständig? Nein! Gurevič konstruierte für jedes ungerade n eine Identität $W_n(x,y)$:

$$(A^x + B^x)^y \cdot (C^y + D^y)^x = (A^y + B^y)^x \cdot (C^x + D^x)^y,$$

wobei $A = 1 + x$ und $B = 1 + x + x^2 + \ldots + x^{n-1}$ sowie $C = 1 + x^n$ und $D = 1 + x^2 + x^4 + \cdots + x^{2n-2}$. Für $n = 3$ ist dies die Identität von Wilkie. Die gesamte Familie dieser Identitäten gilt in $(\mathbb{N}, +, 0, \cdot, 1, \hat{})$, sie kann jedoch aus keiner endlichen Menge von Axiomen abgeleitet werden.

R. Gurevič: *Equational theory of positive numbers with exponentiation is not finitely axiomatizable.* Ann. Pure and Applied Logic 49 (1990) 1–30

Warum erzähle ich das? Es lehrt uns, die sorgsame Konstruktion von $(\mathbb{N}, +, 0, \cdot, 1, \hat{})$ zu würdigen, und zeigt, dass selbst Grundlagen wie die *„high school identities“* zu interessanten und kniffligen Forschungsfragen führen, sobald wir nur genau hinsehen. Die hier illustrierten Techniken durch Beweis und Gegenbeispiel verhelfen Ihnen überall zur Klarheit.

Matrixkalkül: komplexe Zahlen als 2×2–Matrizen

Satz B3D: die komplexen Zahlen $\mathbb{C}$ als Matrizen über $\mathbb{R}$

Im Matrixring $(\mathbb{R}^{2\times2}, +, 0_{2\times2}, \cdot, 1_{2\times2})$ betrachten wir die Teilmenge

$$C := \left\{ z = \left[\begin{smallmatrix} x & -y \\ y & x \end{smallmatrix}\right] \,\middle|\, x, y \in \mathbb{R} \right\}.$$

Sie bildet einen Teilring. Das bedeutet, sie enthält $0_{2\times2}$ und $1_{2\times2}$ und ist abgeschlossen unter Matrixaddition, Negation und Multiplikation:

$$\left[\begin{smallmatrix} x & -y \\ y & x \end{smallmatrix}\right] \cdot \left[\begin{smallmatrix} u & -v \\ v & u \end{smallmatrix}\right] = \left[\begin{smallmatrix} xu-yv & -(yu+xv) \\ yu+xv & xu-yv \end{smallmatrix}\right]$$

Jedes Element $z \neq 0$ in $(C, \cdot)$ ist invertierbar, denn $\det(z) = x^2 + y^2 > 0$:

$$\left[\begin{smallmatrix} x & -y \\ y & x \end{smallmatrix}\right]^{-1} = \frac{1}{x^2+y^2} \left[\begin{smallmatrix} x & y \\ -y & x \end{smallmatrix}\right]$$

Somit ist $(C, +, \cdot)$ ein Divisionsring. Er ist zudem sogar kommutativ:

$$\left[\begin{smallmatrix} u & -v \\ v & u \end{smallmatrix}\right] \cdot \left[\begin{smallmatrix} x & -y \\ y & x \end{smallmatrix}\right] = \left[\begin{smallmatrix} ux-vy & -(uy+vx) \\ uy+vx & ux-vy \end{smallmatrix}\right]$$

Somit ist C ein Körper. Er ist isomorph zu den komplexen Zahlen:

$$(\mathbb{C}, +, \cdot) \cong (C, +, \cdot) : x + \mathrm{i}y \leftrightarrows \left[\begin{smallmatrix} x & -y \\ y & x \end{smallmatrix}\right]$$

Matrixkalkül: komplexe Zahlen als 2×2–Matrizen

Wir betrachten hier nicht die gesamte Menge $\mathbb{R}^{2\times2}$ aller reellen 2×2–Matrizen, sondern nur eine spezielle Teilmenge $C \subset \mathbb{R}^{2\times2}$.

Diese ist abgeschlossen unter Addition, Negation und Multiplikation: Für je zwei Matrizen $z, w \in C$ gilt $z + w \in C$, $-w \in C$ und $z \cdot w \in C$. Zudem gilt $0_{2\times2} \in C$ und $1_{2\times2} \in C$. Wir nennen dies einen **Teilring**.

☺ Allein daraus folgt bereits, dass $(C, +, 0_{2\times2}, \cdot, 1_{2\times2})$ ein Ring ist.

Übung: Wiederholen Sie die acht Ringaxiome und prüfen Sie jedes einzelne hier nach. Sie werden sehen, dass es *trivialerweise* erfüllt ist.

Struktur $(C, +, \cdot)$	$(C, +)$				$(C, +, \cdot)$		$(C, \cdot)$			
Eigenschaft	Ass	Ntr	Inv	Com	DL	DR	Ass	Ntr	Inv*	Com
erben als Teilring	✓	✓	✓	✓	✓	✓	✓	✓	–	–
extra nachrechnen									✓	✓

Trivial bedeutet, es folgt ohne weiteres Zutun sofort aus der Definition. Erst nachdem Sie sich selbst einmal diese notwendige doch lehrreiche Mühe gemacht haben, sind Sie berechtigt auszurufen: „Das ist trivial!“

Matrixkalkül: Quaternionen als 2×2–Matrizen

Satz B3E: die Quaternionen $\mathbb{H}$ als Matrizen über $\mathbb{C}$

Im Matrixring $(\mathbb{C}^{2\times2}, +, 0_{2\times2}, \cdot, 1_{2\times2})$ betrachten wir die Teilmenge

$$H := \{ q = \left[\begin{smallmatrix} z & -w \\ \overline{w} & \overline{z} \end{smallmatrix}\right] \,|\, z, w \in \mathbb{C} \}.$$

Sie bildet einen Teilring. Das bedeutet, sie enthält $0_{2\times2}$ und $1_{2\times2}$ und ist abgeschlossen unter Matrixaddition, Negation und Multiplikation:

$$\left[\begin{smallmatrix} z_1 & -w_1 \\ \overline{w_1} & \overline{z_1} \end{smallmatrix}\right] \cdot \left[\begin{smallmatrix} z_2 & -w_2 \\ \overline{w_2} & \overline{z_2} \end{smallmatrix}\right] = \left[\begin{smallmatrix} z_1 z_2 - w_1 \overline{w_2} & -z_1 w_2 - w_1 \overline{z_2} \\ \overline{w_1} z_2 + \overline{z_1} w_2 & -\overline{w_1} w_2 + \overline{z_1} z_2 \end{smallmatrix}\right]$$

Jedes Element $q \neq 0$ in $(H, \cdot)$ ist invertierbar, $\det(q) = |z|^2 + |w|^2 > 0$:

$$\left[\begin{smallmatrix} z & -w \\ \overline{w} & \overline{z} \end{smallmatrix}\right]^{-1} = \frac{1}{z\overline{z} + w\overline{w}} \left[\begin{smallmatrix} \overline{z} & w \\ -\overline{w} & z \end{smallmatrix}\right]$$

Somit ist $(H, +, \cdot)$ ein Divisionsring. Er ist jedoch nicht kommutativ:

$$E = \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right],\ I = \left[\begin{smallmatrix} \mathrm{i} & 0 \\ 0 & -\mathrm{i} \end{smallmatrix}\right],\ J = \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right],\ K = \left[\begin{smallmatrix} 0 & -\mathrm{i} \\ -\mathrm{i} & 0 \end{smallmatrix}\right] \quad \Rightarrow$$

$\cdot$	I	J	K
I	$-E$	K	$-J$
J	$-K$	$-E$	I
K	J	$-I$	$-E$

Dieser Divisionsring ist isomorph zu Hamiltons Quaternionen:

$$(\mathbb{H}, +, \cdot) \cong (H, +, \cdot) : \alpha + \beta\mathrm{i} + \gamma\mathrm{j} + \delta\mathrm{k} \leftrightarrows \alpha E + \beta I + \gamma J + \delta K.$$

Matrixkalkül: Quaternionen als 2×2–Matrizen

Die Teilmenge $H \subset \mathbb{C}^{2\times2}$ ist ein Teilring: Es gilt $0_{2\times2} \in H$ und $1_{2\times2} \in H$.
Für je zwei Matrizen $z, w \in H$ gilt $z + w \in H$, $-w \in H$ und $z \cdot w \in H$.

☺ Allein daraus folgt bereits, dass $(H, +, 0_{2\times2}, \cdot, 1_{2\times2})$ ein Ring ist.

Struktur $(H, +, \cdot)$	$(H, +)$				$(H, +, \cdot)$		$(H, \cdot)$			
Eigenschaft	Ass	Ntr	Inv	Com	DL	DR	Ass	Ntr	Inv*	Com
erben als Teilring	✓	✓	✓	✓	✓	✓	✓	✓	–	–
extra nachrechnen									✓	–

☺ Unsere sorgsame Vorbereitung zum Matrixkalkül zahlt sich hier aus!
Die Ringaxiome haben wir für $(\mathbb{K}^{n\times n}, +, \cdot)$ allgemein nachgewiesen.
Das können wir immer wieder wunderbar nutzen, so auch hier.

☺ Ohne weitere Mühe sehen wir sofort, dass H ein Schiefkörper ist.
Das ist eine explizite, doch sparsame Konstruktion der Quaternionen.
Die direkte, naive Konstruktion ist möglich, aber eher mühsamer.

Aufgabe: Lassen sich so auch die Oktaven in $\mathbb{H}^{2\times2}$ darstellen? **Lösung:**
Nein, die Multiplikation in $\mathbb{H}^{2\times2}$ ist assoziativ, die Oktaven jedoch nicht.