Lektion 3c: Der Körper der rationalen Zahlen

$\mathbb{N}_0$ erweitern zu $\mathbb{Z}$, Körperaxiome und Körper $\mathbb{Q}$, Abzählbarkeit von $\mathbb{Q}$ und Diagonalargument

Die Ausgangslage

- **Definition:** Eine **algebraische Struktur** ist ein Paar $(M, (f_i)_{i\in\mathbb{N}})$ bestehend aus der Menge M und einer Familie von Verknüpfungen (bzw. Funktionen/Operationen) $(f_i)_{i\in\mathbb{N}}$ mit $f_i : M^n \to M$ und $n \in \mathbb{N}$ für alle i.
  - Die Eigenschaft, dass jeder solche Funktionswert wieder in M liegt, nennt man (algebraische) **Abgeschlossenheit**.

- **Beispiel:** $(\mathbb{N}_0, +, \cdot)$ ist eine solche algebraische Struktur.

- **Frage:** Was kann man in $(\mathbb{N}_0, +, \cdot)$ nicht machen?
  - Inverse Operationen zu $+$ und $\cdot$ (Subtraktion, Division) sind nicht wohldefiniert, da die Abgeschlossenheit verletzt wird!
  - **Z.B.:** $7 - 5 = 2$ weil $2 + 5 = 7$

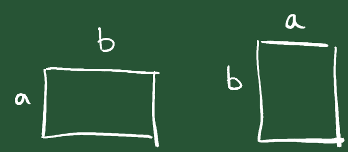
    aber leider gilt $5 - 7 \notin \mathbb{N}$ $\Rightarrow$ Subtrahieren kann dazu führen, dass man die Grundmenge verlässt!

Eine erste Lösung für das Problem

- Um eine (wohldefinierte) inverse Operation zu $+$ zu erhalten, erweitert man die Grundmenge zu $\mathbb{Z}$
- **Saloppe Definition:** $\mathbb{Z} = \mathbb{N}_0 \cup \{-n\colon\ n \in \mathbb{N}\} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$
  - Eine exaktere Konstruktion von $\mathbb{Z}$ erreicht man mit Äquivalenzklassen.
- $(\mathbb{Z}, +, \cdot)$ kann alles, was $(\mathbb{N}_0, +, \cdot)$ kann, aber zusätzlich kann man subtrahieren ☺
  - **Z.B.:** $5 - 7 = -2 \in \mathbb{Z}$ ✓
- Leider kann $\mathbb{Z}$ nicht alles, was man gerne hätte: Die Multiplikation lässt sich nicht zuverlässig rückgängig machen.
  - **Z.B.:** $6 : 2 = 3$ weil $3 \cdot 2 = 6$

    aber leider gilt $2 : 6 \notin \mathbb{Z}$ $\Rightarrow$ Wieder verlässt man möglicherweise die Grundmenge

Die Gretchenfrage der Arithmetik und Algebra



- Was muss in einer Menge mit den Verknüpfungen $+$ und $\cdot$ für die meisten Zwecke möglich sein?

- **Brainstorming:**
  - Man verlässt mit den Verknüpfungen nie die (Grund-) Menge (Grundvoraussetzung für <u>alle</u> algebraischen Strukturen)
  - Flexibilität bei der Reihenfolge der Durchführung/Auswertung („vorteilhaftes Rechnen")
  - Die Verknüpfungen $+$ und $\cdot$ müssen sich miteinander vertragen
  - Man kann neutrale Operationen (identische Abbildung) definieren („do-nothing-Operation") — wird von $\mathbb{N}_0$ erfüllt
  - Die Addition kann rückgängig gemacht werden — wird zusätzlich von $\mathbb{Z}$ erfüllt
  - Man kann die Multiplikation ebenfalls rückgängig machen — hierfür brauchen wir noch eine Lösung

Die Körperaxiome

Farbig markiert sind die Eigenschaften, die von $\mathbb{N}_0$, bzw. von $\mathbb{Z}$ bzw. von $\mathbb{Q}$ erfüllt werden.

Gesucht: Ein Tripel $(M, +, \cdot)$, d.h. eine abgeschlossene alg. Struktur, mit $M \supseteq \mathbb{Z}$ und den folgenden Eigenschaften für $x, y, z \in M$:

	Addition $(M, +)$	**Multiplikation** $(M, \cdot)$	**Bemerkungen**
Kommutativität	$f(x,y) = f(y,x)$ $x + y = y + x$	$x \cdot y = y \cdot x$	Reihenfolge vertauschen
Assoziativität	$(x + y) + z = x + (y + z)$	$(x \cdot y) \cdot z = x \cdot (y \cdot z)$	Beliebig Klammern setzen
Neutrale Elemente	$\exists 0 \in M\colon \forall x \in M\colon \; x + 0 = x$	$\exists 1 \in M\colon \forall y \in M\colon \; y \cdot 1 = y$	Dabei gilt: $0 \neq 1$
Inverse Elemente	$\forall x \in M \;\; \exists \xi \in M\colon \; x + \xi = 0$	$\forall y \in M \setminus \{0\} \;\; \exists \eta \in M\colon \; y \cdot \eta = 1$ $0 \cdot z = 0$	„Das Negative“ $\xi =: (-x)$ „Der Kehrwert“ $\eta =: x^{-1}$
Distributivgesetz	$(x + y) \cdot z \; = \; x \cdot z + y \cdot z$		$+$ und $\cdot$ vertragen sich

$(-4) \cdot \left(-\frac{1}{4}\right) = 1 \qquad \frac{2}{3} \cdot \frac{3}{2} = 1$

Ein solches Tripel nennt man **Körper**. Die rationalen Zahlen, also $(\mathbb{Q}, +, \cdot)$, bilden einen, aber nicht den einzigen Körper.

Bemerkungen (1)

- Ein Paar $(M, \circ)$ bestehend aus der Menge M und der Verknüpfung $\circ\colon M \times M \to M$ nennt man…
  - … im Allgemeinen **ein Magma,**
  - … **eine Halbgruppe**, wenn die Assoziativität erfüllt ist,
  - … **ein Monoid**, wenn es zusätzlich ein neutrales Element e gibt (Nullelement bzw. Einselement),
  - … **eine Gruppe**, wenn es zusätzlich für alle $x \in M$ ein Inverses Element bezüglich $\circ$ gibt,
  - … **abelsch** bzw. **kommutativ**, wenn das Kommutativgesetz erfüllt ist.

Niels Henrik Abel
(1802-1829)

- Ein Tripel $(M, \circ, *)$ mit den Verknüpfungen $\circ: M \times M \to M$ und $*: M \times M \to M$ nennt man **Körper**, wenn…
  - … $(M, \circ)$ eine abelsche Gruppe (mit Nullelement 0) ist, und…
  - … $(M \setminus \{0\}, *)$ eine abelsche Gruppe (mit Einselement 1) ist, und…
  - … das Distributivitätsgesetz erfüllt ist.

- Demnach ist $(\mathbb{Q}, +, \cdot)$ ein Körper mit den neutralen Elementen 0 und 1

Wie viele Grundrechenarten gibt es?

- Richtig! Es gibt zwei Grundrechenarten auf $\mathbb{Q}$, nämlich $+$ und $\cdot$
- Für viele Zwecke definiert man man jedoch zwei weitere abgeleitete Operationen, die lediglich eine Abkürzung für die Verknüpfung mit den inversen Elementen sind:
  - Die Subtraktion $x - y$ ist definiert als Addition des Negativen von x: $\quad x - y \coloneqq x + (-y)$
  - Die Division $x : y$ ist für $y \neq 0$ festgelegt als Multiplikation mit dem Kehrwert: $\quad x : y \coloneqq x \cdot \frac{1}{y}$
- **Wichtig:** Aufgrund der Abgeschlossenheit kann es nicht passieren, dass man mit den zwei (vier) Grundrechenarten versehentlich eine Zahl berechnet, die nicht rational ist.
- **Hinweis:** Das Operieren mit den inversen Operationen soll stets als Verknüpfung mit den Inversen verstanden werden! Z.B. $12 : 4 = 12 \cdot \frac{1}{4}$

Bemerkungen (2)

- Die ganzen Zahlen sind in die rationalen Zahlen eingebettet:
  - Man identifiziert eine ganze Zahl $n \in \mathbb{Z}$ mit dem Bruch $\frac{n}{1} \in \mathbb{Q}$
- Die rationalen Zahlen liegen „dicht“ auf dem Zahlenstrahl
  - Das heißt, dass es zu jedem Paar von rationalen Zahlen p und q (mit $p \neq q$) eine rationale Zahl gibt, die zwischen den beiden liegt (z.B. der Mittelpunkt).
- Ein weiteres Paket von Axiomen wird noch benötigt: Die Ordnungsaxiome (im Video zu $\mathbb{R}$)
- Alle Rechenregeln zu $+, -, \cdot, :$ in $\mathbb{Q}$ können aus den Körper- und Ordnungsaxiomen hergeleitet werden!

Beispiele

FOIL
First Inner Outer Last

$(a+b)\cdot(c+d)$

1) Beweise mithilfe der Körperaxiome die Rechenregel für das Produkt zweier Binome (d.h. $(a+b)\cdot(c+d)$).

$$(a+b)\cdot(c+d) \overset{\text{Distr.}}{=} a\cdot(c+d) + b\cdot(c+d) \overset{\text{Komm}\,\cdot}{=} (c+d)\cdot a + (c+d)\cdot b \;\ldots$$

$$\ldots \overset{\text{Distr.}}{=} (c\cdot a + d\cdot a) + (c\cdot b + d\cdot b) \overset{+\text{Ass.}}{=} c\cdot a + d\cdot a + c\cdot b + d\cdot b$$

$$\overset{\cdot\,\text{Komm.}}{=} a\cdot c + b\cdot c + a\cdot d + b\cdot d$$

2) Definiere die Multiplikation zweier rationaler Zahlen und leite daraus die Division von Brüchen her.

Weitere wichtige Körper

- In der Analysis wird insbesondere $\mathbb{R}$ und $\mathbb{C}$ untersucht, die mit $+$ und $\cdot$ jeweils einen Körper bilden
- Die (endlichen) Restklassenkörper zur Menge $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ für $p \in \mathbb{P}$ in der Algebra und Zahlentheorie
- Die weiteren endlichen Körper $\mathbb{F}_{p^k}$ mit p^k Elementen (für $p \in \mathbb{P}$ und $k \in \mathbb{N}$)

Abzählbarkeit von $\mathbb{Q}$

- Obwohl es nicht intuitiv klingt: Die Menge $\mathbb{Q}$ ist abzählbar, also gleichmächtig zu $\mathbb{N}_0$.
- Beweis durch das CANTORSCHE Diagonalargument:
  - Liste alle nichtnegativen Brüche nach folgendem Tabellenschema auf:
    - Entlang einer Zeile nimmt der Zähler immer um 1 zu
    - Entlang der Spalten wird der Nenner immer um 1 mehr
  - Mit der blauen Linie können wir dann diagonal alle diese Brüche auffädeln
    - Man nummeriere entlang der blauen Linie alle vorkommenden Brüche aufsteigend
    - Erreicht man einen bereits vorhandenen Bruch, dann streicht man ihn weg
  - Eine Nummerierung dieser Brüche entspricht einer Bijektion von $\mathbb{N}$ nach $\mathbb{Q}_0^+$
  - Um eine Bijektion von $\mathbb{N}$ nach ganz $\mathbb{Q}$ zu erhalten, schummelt man einfach die negativen Brüche (abwechselnd zu den positiven) in die Liste (orange)
  - Damit ist eine solche Bijektion gefunden und ganz $\mathbb{Q}$ somit abzählbar. ■

$$
\begin{array}{cccccc}
\frac{0}{1} & \frac{1}{1} & \frac{2}{1} & \frac{3}{1} & \frac{4}{1} & \cdots \\[6pt]
 & \frac{1}{2} & \cancel{\frac{2}{2}} & \frac{3}{2} & \cancel{\frac{4}{2}} & \cdots \\[6pt]
 & \frac{1}{3} & \frac{2}{3} & \cancel{\frac{3}{3}} & \frac{4}{3} & \cdots \\[6pt]
 & \frac{1}{4} & \cancel{\frac{2}{4}} & \frac{3}{4} & \frac{4}{4} & \cdots \\[6pt]
 & \frac{1}{5} & \frac{2}{5} & \frac{3}{5} & \frac{4}{5} & \cdots \\[6pt]
 & \vdots & \vdots & \vdots & \vdots & \ddots
\end{array}
$$