3. Elementare Zahlentheorie

Zahlenbereiche

Ziele/Motivation

- nach der axiomatischen Einführung der natürlichen Zahlen ($\mathbb{N}$) mit den Rechenoperationen $+$ und $\cdot$ und der Ordnung $\leqslant$ konstruieren wir daraus die ganzen ($\mathbb{Z}$), die rationalen ($\mathbb{Q}$) und schließlich die reellen Zahlen ($\mathbb{R}$)
- die ganzen Zahlen erlauben zusätzlich die Subtraktion ($-$)
- ganz ähnlich erlauben die rationalen Zahlen $\mathbb{Q}$ die Division ($/$)
- $\mathbb{Z}$ und $\mathbb{Q}$ können als Abschluss/Erweiterung der natürlichen Zahlen bezüglich der Subtraktion und Division angesehen werden
- die reellen Zahlen $\mathbb{R}$ vervollständigen die rationalen Zahlen bezüglich Grenzwerteigenschaften die im Analysis-Teil der Vorlesung (Sommmersemester) relevant werden
- für die Konstruktionen dieser Zahlenbereiche brauchen wir den Begriff der Äquivalenzrelation

Relationen

Definition (Relation)

Eine Relation R auf einer Menge A ist eine Teilmenge der geordneten Paare aus A^2, d. h. $R \subseteq A^2$. Für $(a, b) \in R$ schreibt man auch aRb.

Definition (Eigenschaften von Relationen)

Eine Relation R auf A heißt

- reflexiv: für alle $a \in A$ gilt $(a, a) \in R$.
- symmetrisch: für alle a, $b \in A$ gilt $(a, b) \in R \Longrightarrow (b, a) \in R$.
- antisymmetrisch: für alle a, $b \in A$ gilt $(a, b) \in R \wedge (b, a) \in R \Longrightarrow a = b$.
- transitiv: für alle a, b, $c \in A$ gilt $(a, b) \in R \wedge (b, c) \in R \Longrightarrow (a, c) \in R$.

Definition (Spezielle Relationen)

Eine Relation R auf A ist eine

- Teilordnung (auch Halbordnung, Ordnung, partielle Ordnung genannt), falls R reflexiv, antisymmetrisch und transitiv ist. z. B. $\leqslant$ auf $\mathbb{N}$
- Äquivalenzrelation, falls R reflexiv, symmetrisch und transitiv ist.

Beispiel: Äquivalenzrelation

Paritäten

Wir definieren eine Relation $\equiv_2$ auf $\mathbb{N}_0$ durch

$$x \equiv_2 y \quad :\Longleftrightarrow \quad 2 \,|\, x+y \quad \Longleftrightarrow \quad x+y \text{ ist gerade}.$$

- $x \equiv_2 y$ genau dann, wenn x, y gerade oder beide ungerade

Behauptung: $\equiv_2$ ist eine Äquivalenzrelation auf $\mathbb{N}_0$.

Beweis: Wir überprüfen die drei Eigenschaften einer Äquivalenzrelation:

- Reflexivität: $x + x$ ist gerade für jedes $x \in \mathbb{N}_0$ ✓
- Symmetrie: $x + y = y + x$ für alle x, $y \in \mathbb{N}_0$ ✓
- Transitivität: Falls $x + y$ und $y + z$ gerade sind, dann ist $x + 2y + z$ gerade und, da $2y$ gerade ist, ist auch $x + z$ gerade. D. h. aus $x \equiv_2 y$ und $y \equiv_2 z$ folgt $x \equiv_2 z$ für beliebige x, y, $z \in \mathbb{N}_0$ ✓

Relation $\equiv_2$ ist reflexiv, symmetrisch und transitiv und die Beh. folgt. □

Bemerkung: $\equiv_2$ zerlegt $\mathbb{N}_0$ in zwei Klassen (gerade und ungerade Zahlen) innerhalb denen jeweils alle Paare in Relation stehen.

Partitionen

Definition (Partition)

Ein Partition/Zerlegung einer Menge A ist eine Menge $\mathcal{Z} \subseteq \wp(A)$ von Teilmengen von A, sodass

1. $Z \neq \varnothing$ für alle $Z \in \mathcal{Z}$, — nichtleere Teilmengen
2. $Z \cap Z' = \varnothing$ für alle verschiedenen $Z, Z' \in \mathcal{Z}$ — paarweise disjunkt
3. und $\bigcup \mathcal{Z} := \bigcup \{Z : Z \in \mathcal{Z}\} = A$. — Überdeckung von A

Die Teilmengen aus $\mathcal{Z}$ heißen Partitionsklassen.

Bemerkung: Disjunkte Vereinigungen werden wir manchmal mit einem Punkt im Vereinigungszeichen anzeigen (z. B. $\dot{\bigcup}\{Z : Z \in \mathcal{Z}\}$, $A \dot{\cup} B$, ...).

Beispiele

- $\{n \in \mathbb{N}_0 : n \text{ gerade}\} \dot{\cup} \{n \in \mathbb{N}_0 : n \text{ ungerade}\}$ partitioniert $\mathbb{N}_0$
- die Menge $\mathcal{Z} = \{Z_k : k \in \mathbb{N}_0\}$ bestehend aus den Mengenfamilien $Z_k = \{A \subseteq \mathbb{N} : A \text{ hat genau } k \text{ Elemente}\}$ partitioniert die Menge der endlichen Teilmengen von $\mathbb{N}$ in unendlich viele Partitionsklassen

Äquivalenzrelationen und Partitionen

Satz

Sei $\mathcal{Z}$ eine Partition der Menge A. Dann definiert

$$x \sim_{\mathcal{Z}} y \quad :\Longleftrightarrow \quad x, y \in Z \text{ für ein } Z \in \mathcal{Z}$$

eine Äquivalenzrelation $\sim_{\mathcal{Z}}$ auf A.

Beweis: Sei $\mathcal{Z}$ eine Partition von A und $\sim_{\mathcal{Z}}$ wie in der Behauptung definiert. Wir zeigen, dass $\sim_{\mathcal{Z}}$ reflexiv, symmetrisch und transitiv ist.

Reflexivität: Sei $a \in A$. Da $A = \dot{\bigcup}\{Z : Z \in \mathcal{Z}\}$ gibt es genau eine Menge $Z \in \mathcal{Z}$ mit $a \in Z$ und somit gilt $a \sim_{\mathcal{Z}} a$.

Symmetrie: Seien $a, b \in A$ mit $a \sim_{\mathcal{Z}} b$. D. h. es gibt $Z \in \mathcal{Z}$ mit $a, b \in \mathcal{Z}$ und somit $b \sim_{\mathcal{Z}} a$.

Transitivität: Seien a, b und $c \in A$ mit $a \sim_{\mathcal{Z}} b$ und $b \sim_{\mathcal{Z}} c$. Nach Definition von $\sim_{\mathcal{Z}}$ gibt es Z und $Z' \in \mathcal{A}$ mit $a, b \in Z$ und $b, c \in Z'$. Also gilt $b \in Z \cap Z'$ und da $\mathcal{Z}$ eine Partition ist (paarweise disjunkte Elemente), folgt $Z = Z'$. Somit enthält Z neben a und b auch c und es folgt $a \sim_{\mathcal{Z}} c$.

Also erfüllt $\sim_{\mathcal{Z}}$ die notwendigen Eigenschaften einer Äquivalenzrelation. □

Satz

Sei $\sim$ eine Äquivalenzrelation auf der Menge A. Dann gibt es genau eine Partition $\mathcal{Z}$ von A mit $\sim = \sim_{\mathcal{Z}}$.

Sei $\sim$ eine Äquivalenzrelation auf A. Zuerst zeigen wir die Existenz einer Partition $\mathcal{Z}$ und dann die Eindeutigkeit.

- **Definition von $\mathcal{Z}$:** Setze $\mathcal{Z} := \{Z_a : a \in A\}$, wobei für jedes $a \in A$
$$Z_a := \{b \in A : a \sim b\}.$$
- **$\mathcal{Z}$ ist Partition:** Wir zeigen, dass die Mengen Z_a nichtleer und paarweise disjunkt sind und ihre Vereinigung ganz A ergibt.
  - **nicht-leer und $\bigcup \mathcal{Z} = A$:** $\sim$ reflexiv $\Rightarrow a \sim a$ für jedes $a \in A$ $\Rightarrow a \in Z_a$ für jedes $a \in A \Rightarrow Z_a \neq \emptyset$ für jedes $a \in A$ und $\bigcup_{a \in A} Z_a = A$
  - **disjunkt:** Angenommen $c \in Z_a \cap Z_b \Rightarrow a \sim c$ und $b \sim c$ und wegen der Symmetrie und Transitivität von $\sim$ folgt $a \sim b$.

    Wir zeigen nun $Z_a \subseteq Z_b$: Sei $x \in Z_a$ beliebig $\Rightarrow a \sim x$ und wegen der Symmetrie und Transitivität und $a \sim b$ folgt auch $b \sim x \Rightarrow x \in Z_b$.

    Da $x \in Z_a$ beliebig war, gilt $Z_a \subseteq Z_b$ und die gleiche Argumentation zeigt auch $Z_b \subseteq Z_a$ und somit $Z_a = Z_b$, falls $Z_a \cap Z_b \neq \emptyset$.

Äquivalenzrelationen und Partitionen — Teil 3

Als nächstes zeigen wir $\sim = \sim_{\mathcal{Z}}$ und dann die Eindeutigkeit von $\mathcal{A}$.

$\sim \subseteq \sim_{\mathcal{Z}}$: Sei $a \sim b$, also $(a, b) \in \sim$. Dann gilt $a,\ b \in Z_a$ und aus der Definition von $\sim_{\mathcal{Z}}$ folgt $a \sim_{\mathcal{Z}} b$, also $(a, b) \in \sim_{\mathcal{Z}}$.

$\sim_{\mathcal{Z}} \subseteq \sim$: Sei nun $a \sim_{\mathcal{Z}} b$, also $(a, b) \in \sim_{\mathcal{Z}}$. Dann existiert ein $Z \in \mathcal{Z}$ mit $a,\ b \in Z$. Wegen der Definition von $\mathcal{Z}$ gibt es ein $a' \in Z$ mit $Z = Z_{a'}$.

Da also a, b aus $Z_{a'}$ sind, folgt $a' \sim a$ und $a' \sim b$ und mit Symmetrie und Transitivität von $\sim$ auch $a \sim b$. D. h. $(a, b) \in \sim$ wie gewünscht.

Eindeutigkeit: Sei $\mathcal{Y}$ eine weitere Partition mit $\sim_{\mathcal{Y}} = \sim$. Aus dem bereits Gezeigten folgt also $\sim_{\mathcal{Y}} = \sim = \sim_{\mathcal{A}}$ und somit gilt für alle $a,\ b \in A$

$$a \sim_{\mathcal{Y}} b \quad \Leftrightarrow \quad a \sim b \quad \Leftrightarrow \quad a \sim_{\mathcal{Z}} b\,.$$

Folglich gilt für alle $a \in A$ auch

$$Y_a := \{b \in A\colon a \sim_{\mathcal{Y}} b\} = \{b \in A\colon a \sim b\} = Z_a\,.$$

Somit ist $\{Y_a\colon a \in A\} = \mathcal{Z}$.

Des Weiteren ist Y_a offensichtlich eine Teilmenge der Menge $Y \in \mathcal{Y}$, die a enthält. Aber wegen der Transitivität von $\sim_{\mathcal{Y}}$ gilt tatsächlich $Y_a = Y$. D. h. $\{Y_a\colon a \in A\} = \mathcal{Y}$, also $\mathcal{Y} = \mathcal{Z}$ was den Beweis abschließt. □

Äquivalenzklassen

Definition (Äquivalenzklassen)

Sei $\sim$ eine Äquivalenzrelation auf A.

- Die eindeutig bestimmte Partition $\mathcal{Z}$ aus dem letzten Satz bezeichnet man mit $A/\sim$ und sie heißt Faktormenge/Quotientenmenge.
- Die Elemente von $A/\sim$ heißen Äquivalenzklassen, welche man mit $[a]$ (manchmal auch $\overline{a}$) statt Z_a bezeichnet.
- Die Elemente einer Äquivalenzklasse sind die Repräsentanten dieser Äquivalenzklasse und wir sagen sie sind äquivalent zueinander.
- Äquivalenzklassen sind also paarweise disjunkt.
- Zwei Elemente a und $b \in A$ repräsentieren also die gleiche Äquivalenzklasse genau dann, wenn sie äquivalent sind
$$[a] = [b] \quad \Leftrightarrow \quad a \sim b\,.$$
- Die Funktion $a \mapsto [a]$ heißt kanonische Projektion von A nach $A/\sim$.

Beispiel: Partitioniert man $\mathbb{N}$ in die geraden und ungeraden Zahlen und bezeichnet diese Partition mit $\mathcal{Z}$, so ist $\sim_{\mathcal{Z}}$ die Äquivalenzrelation mit zwei Äquivalenzklassen und zwei Zahlen sind genau denn äquivalent, wenn sie die gleiche Parität haben. Jede ungerade Zahl repräsentiert die Äquivalenzklasse der ungeraden Zahlen usw.

Wie macht man Funktionen injektiv?

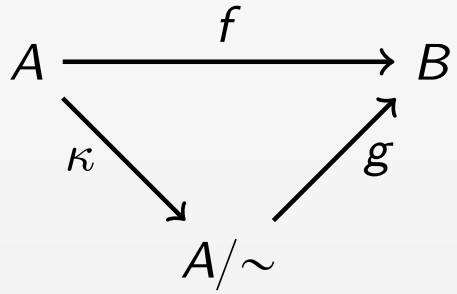
Satz

Sei $f : A \to B$ eine Funktion. Für $a, a' \in A$ definiere die Relation $\sim$ durch

$$a \sim a' \quad :\Leftrightarrow \quad f(a) = f(a') .$$

Dann ist $\sim$ eine Äquivalenzrelation und $[a] \mapsto f(a)$ eine injektive Funktion $g : A/\sim \to B$.

Sei κ die kanonische Projektion von $\sim$. Dann besagt der Satz, es gibt inj. g mit $f = g \circ \kappa$



Beweis

Zu zeigen ist:

1. $\sim$ ist eine Äquivalenzrelation, ✓
2. g ist wohldefiniert, d. h. $g([a])$ ist unabhängig vom gewählten Repräsentanten! ✓
3. g ist injektiv. ✓

□

Ganze Zahlen

Idee:

- Die Umkehroperation der Addition, die Subtraktion, kann nicht beliebig innerhalb von $\mathbb{N}$ definiert werden. Z. B. $7 - 12$ liegt nicht in $\mathbb{N}$.
- Erweitere $\mathbb{N}$, um Abgeschlossenheit bezüglich der Subtraktion zu erhalten.
- Definiere die ganze Zahl z als Menge der Paare von natürlichen Zahlen (a, b) mit „$a - b = z$“ (z. B. $(7, 12)$ und $(0, 5)$ sind Repräsentanten von -5).
- Da es aber kein „$-$“ in $\mathbb{N}$ gibt, drücken wir diese Beziehung innerhalb von $\mathbb{N}$ durch „umstellen“ wie folgt aus

$$\text{„}a - b = a' - b'\text{“} \quad \Leftrightarrow \quad a + b' = a' + b\,.$$

- Damit definieren wir eine Äquivalenzrelation auf $\mathbb{N}^2$ deren Äquivalenzklassen den ganzen Zahlen entsprechen.

Ganze Zahlen

formale Definition Idee

Definition ($\mathbb{Z}$)

Durch

$$(a,b) \sim (a',b') :\Leftrightarrow a + b' = a' + b \qquad \text{„}a - b = a' - b'\text{“}$$

wird auf $\mathbb{N}_0^2$ eine Äquivalenzrelation definiert.

Wir bezeichnen die Faktormenge $\mathbb{N}_0^2/\sim$ mit $\mathbb{Z}$ und nennen ihre Elemente die ganzen Zahlen. Ganze Zahlen der Form $[(n,0)]$ bezeichnen wir kürzer durch die natürliche Zahl n und ganze Zahlen der Form $[(0,n)]$ als $-n$.

Die Operationen $+$ und $\cdot$ und die Ordnung $\leqslant$ von $\mathbb{N}$ erweitert man auf ganz $\mathbb{Z}$

$$[(a,b)] +_{\mathbb{Z}} [(a',b')] :\Leftrightarrow [(a+a', b+b')] \qquad \text{„}(a-b)+(a'-b') = (a+a')-(b+b')\text{“}$$

$$[(a,b)] \cdot_{\mathbb{Z}} [(a',b')] :\Leftrightarrow [(a\cdot a' + b\cdot b', a\cdot b' + b\cdot a')] \qquad \text{„}(a-b)\cdot(a'-b') = (a\cdot a' + b\cdot b') - (a\cdot b' + b\cdot a')\text{“}$$

$$[(a,b)] \leqslant_{\mathbb{Z}} [(a',b')] :\Leftrightarrow a + b' \leqslant a' + b \qquad \text{„}(a-b) \leqslant (a'-b')\text{“}$$

Bemerkungen:

- $+_{\mathbb{Z}}$, $\cdot_{\mathbb{Z}}$ und $\leqslant_{\mathbb{Z}}$ sind wohldefiniert und wir schreiben einfach $+$, $\cdot$ und $\leqslant$
- $\mathbb{Z}$ "erbt" die Rechengesetze (Kommutativität, Assoziativität, Distributivität) aus $\mathbb{N}$
- für jedes $z \in \mathbb{Z}$ gibt es genau ein $z' \in \mathbb{Z}$ mit $z + z' = 0$ $\qquad [(a,b)] + [(b,a)] \sim [(0,0)]$
- z' bezeichnen wir mit $-z$
- allgemein definieren wir dann die Subtraktion $x - y := x + (-y)$
  $-: \mathbb{Z}^2 \to \mathbb{Z}$ mit $(x,y) \mapsto x + (-y)$

Rationale Zahlen

Idee:

- Vervollständige $\mathbb{Z}$, um Abgeschlossenheit bezüglich der Division zu erhalten.
- Definiere die rationale Zahl q durch ihre Bruchdarstellungen, d. h. das Paar von ganzen Zahlen (a, b) mit $b \neq 0$ soll die rationale Zahl $q = a/b$ repräsentieren und verschiedene Bruchdarstellungen der Selben Zahl q werden gleich (äquivalent) gesetzt.
- Ähnlich wie bei der Darstellung von „$-$“, stellen wir um

$$\text{„}\frac{a}{b} = \frac{a'}{b'}\text{“} \qquad \Leftrightarrow \qquad a \cdot_{\mathbb{Z}} b' = a' \cdot_{\mathbb{Z}} b\,.$$

- Damit definieren wir eine Äquivalenzrelation auf $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ deren Äquivalenzklassen den rationalen Zahlen entsprechen.

Rationale Zahlen

Definition ($\mathbb{Q}$)

Durch

$$(a,b) \approx (a',b') \;:\Leftrightarrow\; a \cdot b' \;=\; a' \cdot b \qquad „\frac{a}{b} = \frac{a'}{b'}“$$

wird auf $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ eine Äquivalenzrelation definiert.

Wir bezeichnen die Faktormenge $(\mathbb{Z} \times (\mathbb{Z} \setminus \{0\}))/\approx$ mit $\mathbb{Q}$ und nennen ihre Elemente die rationalen Zahlen. Rationale Zahlen der Form $[(z,1)]$ bezeichnen wir kürzer durch die ganze Zahl z und rationale Zahlen der Form $[(1,z)]$ als $1/z$ bzw. z^{-1}.

Die Operationen $+$ und $\cdot$ und die vollständige Ordnung $\leqslant$ aus $\mathbb{Z}$ erweitert man auf ganz $\mathbb{Q}$

$$[(a,b)] +_{\mathbb{Q}} [(a',b')] \;:\Leftrightarrow\; [(a \cdot b' + a' \cdot b\,,\; b \cdot b')] \qquad „\frac{a}{b} + \frac{a'}{b'} = \frac{a \cdot b' + a' \cdot b}{b \cdot b'}“$$

$$[(a,b)] \cdot_{\mathbb{Q}} [(a',b')] \;:\Leftrightarrow\; [(a \cdot a'\,,\; b \cdot b')] \qquad „\frac{a}{b} \cdot \frac{a'}{b'} = \frac{a \cdot a'}{b \cdot b'}“$$

$$[(a,b)] \leqslant_{\mathbb{Q}} [(a',b')] \;:\Leftrightarrow\; a \cdot b' \leqslant a' \cdot b \qquad „\frac{a}{b} \leqslant \frac{a'}{b'}“$$

- $+_{\mathbb{Q}}$, $\cdot_{\mathbb{Q}}$ und $\leqslant_{\mathbb{Q}}$ sind wohldefiniert und wir schreiben einfach $+$, $\cdot$ und $\leqslant$
- wir definieren die Subtraktion analog wie in $\mathbb{Z}$, d. h. für $q = [(a,b)]$ setze $-q = [(-a,b)]$
- $\mathbb{Q}$ “erbt” die Rechengesetze (Kommutativität, Assoziativität, Distributivität) aus $\mathbb{Z}$
- für jedes $q \in \mathbb{Q} \setminus \{0\}$ gibt es genau ein $q' \in \mathbb{Q}$ mit $q \cdot q' = 1$ $\quad [(a,b)] \cdot [(b,a)] \approx [(1,1)]$
- q' bezeichnen wir mit q^{-1}
- allgemein definieren wir dann die Division $x/y := x \cdot (y^{-1})$