3. Elementare Zahlentheorie

Zahlenbereiche

Ziele/Motivation

- nach der axiomatischen Einführung der natürlichen Zahlen ($\mathbb{N}$ und $\mathbb{N}_0$) 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 $\mathbb{Z}$ 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 (Sommersemester) 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 $\mathbb{N}$ und $\subseteq$ auf $\wp(M)$
- Äquivalenzrelation, falls R reflexiv, symmetrisch und transitiv ist.

Beispiel: Äquivalenzrelation

Paritäten

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

$$x \equiv_2 y \quad :\Longleftrightarrow \quad 2 \mid x + y$$

- $x \equiv_2 y \iff x + y$ ist gerade $\iff x, y$ 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 disjunkte Mengen (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. $\dot\bigcup\{Z : Z \in \mathcal{Z}\}$, $A \mathbin{\dot\cup} B, \dots$).

Beispiele

- $\big\{\{n \in \mathbb{N}_0 : n \text{ gerade}\}, \{n \in \mathbb{N}_0 : n \text{ ungerade}\}\big\}$ ist Partition von $\mathbb{N}_0$
- 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 eine Menge $Z \in \mathcal{Z}$ mit $a, b \in Z$ 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. □

Äquivalenzrelationen und Partitionen Teil 2

Satz

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

Beweis: Sei $\sim$ eine Äquivalenzrelation auf A. Zuerst zeigen wir die Existenz einer Partition $\mathcal{Z}$ mit $\sim \,=\, \sim_{\mathcal{Z}}$ und dann die Eindeutigkeit.

- **Definition von $\mathcal{Z}$:** Setze $\mathcal{Z} := \{Z_a \colon a \in A\}$, wobei für jedes $a \in A$
$$Z_a := \{b \in A \colon a \sim b\}\,.$$
- **$\mathcal{Z}$ ist Partition:** Wir zeigen, dass die Mengen Z_a nichtleer und paarweise disjunkt sind und ihre Vereinigung ganz A ergibt.
  - nichtleer und $\bigcup \mathcal{Z} = A$: $\sim$ reflexiv $\Rightarrow a \sim a$ für jedes $a \in A$ $\Rightarrow a \in Z_a$ für jedes $a \in A \Rightarrow Z_a \neq \varnothing$ 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 $Z_a \cap Z_b \neq \varnothing$. ✓

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 $\sim_{\mathcal{Y}}\ =\ \sim\ =\ \sim_{\mathcal{Z}}$ und somit gilt für alle a, $b \in A$

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

  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. $\square$

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
$$[a] = [b] \quad \Longleftrightarrow \quad a \sim b\,.$$
- 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 $f\colon A \to B$ eine Funktion. Für $a, a' \in A$ definiere die Relation $\sim$ durch

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

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

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

$$\begin{tikzcd}
A \arrow[rr, "f"] \arrow[dr, "\kappa"'] & & B \\
& A/{\sim} \arrow[ur, "g"'] &
\end{tikzcd}$$

Beweis

Zu zeigen ist:

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

$\square$

Ganze Zahlen

Idee:

- Die Umkehroperation der Addition, die Subtraktion, kann nicht beliebig innerhalb von $\mathbb{N}_0$ definiert werden. Z. B. $7 - 12$ liegt nicht in $\mathbb{N}_0$.
- Vervollständige $\mathbb{N}_0$ für die Abgeschlossenheit der Subtraktion.
- Definiere die ganze Zahl z als Menge der Paare $(a, b) \in \mathbb{N}_0^2$ mit „$a - b = z$“ (z. B. $(7, 12)$ und $(0, 5)$ sind Repräsentanten von -5).
- Da es aber kein „$-$“ in $\mathbb{N}_0$ gibt, drücken wir diese Beziehung innerhalb von $\mathbb{N}_0$ durch „umstellen“ wie folgt aus

$$„\, a - b = a' - b' \,“ \qquad \Longleftrightarrow \qquad a + b' = a' + b \,.$$

- Damit definieren wir eine Äquivalenzrelation auf $\mathbb{N}_0^2$ deren Äquivalenzklassen den ganzen Zahlen entsprechen.

Ganze Zahlen

formale Definition Idee

Definition ($\mathbb{Z}$)

Durch

$$(a,b) \sim (a',b') \;:\Longleftrightarrow\; a+b' = a'+b \qquad „a-b = a'-b'“$$

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 $\mathbb{Z}$ durch:

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

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

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

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) von $\mathbb{N}_0$
- 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 $x - y := x + (-y)$

$-\colon \mathbb{Z}^2 \to \mathbb{Z}$ mit $(x,y) \mapsto x + (-y)$

Rational Zahlen

Idee:

- vervollständige $\mathbb{Z}$ für die Abgeschlossenheit bezüglich der Division
- Definiere die rationale Zahl q durch ihre Bruchdarstellungen, d. h. das Paar von ganzen Zahlen (a, b) mit $b > 0$ 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

$$„\frac{a}{b} = \frac{a'}{b'}\text{“} \qquad \Longleftrightarrow \qquad a \cdot b' = a' \cdot b\,.$$

- Damit definieren wir eine Äquivalenzrelation auf der Menge

$$\mathbb{Z} \times \mathbb{N}$$

deren Äquivalenzklassen den rationalen Zahlen entsprechen.

Rationale Zahlen

Definition ($\mathbb{Q}$)

Durch

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

wird auf der Menge $\mathbb{Z}\times\mathbb{N}$ eine Äquivalenzrelation definiert.

Wir bezeichnen die Faktormenge $(\mathbb{Z}\times\mathbb{N})/{\approx}$ 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 Ordnung $\leqslant$ aus $\mathbb{Z}$ erweitert man auf ganz $\mathbb{Q}$ durch:

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

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

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

- $+_{\mathbb{Q}}$, $\cdot_{\mathbb{Q}}$ 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) von $\mathbb{Z}$
- 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 $1/q$ bzw. q^{-1}
- allgemein definieren wir dann die Division $x/y := x\cdot(y^{-1})$

Körper

Definition (Körper)

Sei K eine Menge

- mit zwei verschiedenen Elementen $0_K, 1_K \in K$
- und zwei inneren Verknüpfungen $+\colon K \times K \to K$ und $\cdot\colon K \times K \to K$.

Wir sagen K (genauer $(K, +, \cdot)$ bzw. $(K, +, \cdot, 0_K, 1_K)$) ist ein Körper, wenn für alle $a, b, c \in K$ die folgenden Rechengesetze gelten:

(K1) Assoziativgesetze: $a + (b + c) = (a + b) + c$ und $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

(K2) Kommutativgesetze: $a + b = b + a$ und $a \cdot b = b \cdot a$

(K3) Distributivgesetz: $a \cdot (b + c) = a \cdot b + a \cdot c$

(K4) Neutrale Elemente: $a + 0_K = a$ und $1_K \cdot a = a$

(K5) Existenz inverser Elemente:

- es existiert ein $-a \in K$ mit $a + (-a) = 0_K$.
- falls $a \neq 0_K$, dann existiert ein $a^{-1} \in K$ mit $a \cdot a^{-1} = 1_K$.

Bemerkungen

- für 0_K und 1_K schreiben wir meist nur 0 und 1, wenn der Körper klar ist
- $\mathbb{N}_0$ erfüllt (K1) – (K4) mit der üblichen Addition und Multiplikation
- $\mathbb{Z}$ erfüllt (K1) – (K4) und den ersten Teil von (K5)
- $\mathbb{Q}$ erfüllt (K1) – (K5) und ist ein Körper

Beispiele: Körper

- neben $\mathbb{Q}$ sind die bekannten Erweiterungen $\mathbb{R}$ und $\mathbb{C}$ Körper
- weitere wichtige Beispiele sind die endlichen Körper $\mathbb{F}_q$ (auch $GF(q)$) mit q Elementen, wobei $q = p^n$ für eine Primzahl p und $n \in \mathbb{N}$
- der kleinste Körper $\mathbb{F}_2$ hat zwei Elemente 0 und 1 und ist auf der Menge $\{0, 1\}$ mit der Addition und Multiplikation definiert durch

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

  - $-0 = 0, \quad -1 = 1, \quad$ und $\quad 1^{-1} = 1$
  - die anderen Rechengesetze (K1) – (K4) kann man einfach nachprüfen
- $\mathbb{F}_2$ ist der „einzige" Körper mit zwei Elementen, da die Rechengesetze in diesem Fall die Addition und Multiplikation eindeutig bestimmen
  - (K4) und (K2) definieren alle Ergebnisse bis auf $1 + 1$ und $0 \cdot 0$
  - $1 + 1 = 0$ ist erzwungen, da sonst keine -1 existieren würde
  - $0 \cdot 0 = 0$ kann man wie folgt zeigen:

$$0 \cdot 0 \overset{(K4)}{=} 0 \cdot 0 + 0 \overset{(K4)}{=} 0 \cdot 0 + 0 \cdot 1 \overset{(K3)}{=} 0 \cdot (0 + 1) \overset{(K4)}{=} 0 \cdot 1 \overset{(K4)}{=} 0$$

Vollständige Ordnungen

- Neben den Rechenoperationen haben wir auf $\mathbb{N}$, $\mathbb{Z}$ und $\mathbb{Q}$ eine Ordnung $\leqslant$ definiert.
- Dabei ist $\leqslant$ sogar eine Totalordnung (auch lineare, vollständige oder totale Ordnung), d. h. zusätzlich zu den definierenden Ordnungseigenschaften (reflexiv, antisymmetrisch, transitiv) gilt für je zwei Elemente a und b

  $$a \leqslant b \qquad \text{oder} \qquad b \leqslant a\,.$$

  Es sind also **alle** Elemente miteinander vergleichbar (im Gegensatz zur Teilmengenrelation, die nur eine Ordnung aber **keine** Totalordnung ist) und für zwei verschiedene a und b gilt **genau eine** der Beziehungen

  $$a < b \qquad \text{oder} \qquad b < a\,,$$

  wobei $a < b$ durch $a \leqslant b \wedge a \neq b$ definiert ist.
- Darüber hinaus ist es praktisch, wenn die Totalordnung mit den Rechenoperationen „kompatibel“ ist und dies führt zum Begriff des angeordneten Körper.

Angeordnete Körper

Definition (Angeordneter Körper)

Ein Körper K mit einer totalen Ordnung $\leqslant$ auf K heißt angeordnet, falls die folgenden Anordnungsaxiome für alle $a, b, c \in K$ gelten:

(A1) Falls $a \leqslant b$, dann gilt auch $a + c \leqslant b + c$.
(A2) Falls $a \leqslant b$ und $c \geqslant 0$, dann gilt auch $a \cdot c \leqslant b \cdot c$.

Bemerkungen

- $\mathbb{N}_0$, $\mathbb{Z}$ und $\mathbb{Q}$ mit ihrer Ordnung erfüllen die Anordnungsaxiome
- $\mathbb{Q}$ und die Erweiterung $\mathbb{R}$ sind angeordnete Körper
- $\mathbb{C}$ und endliche Körper können nicht angeordnet werden, z. B. für $\mathbb{F}_2$ führt sowohl die Festlegung $0 < 1$ als auch $1 < 0$ wegen $1 + 1 = 0$ zu einem Widerspruch:
$$0 < 1 \quad \xrightarrow{\text{(A1)}} \quad 0 + 1 < 1 + 1 \quad \Longleftrightarrow \quad 1 < 0$$
- (A1) und (A2) implizieren auch $a \cdot c \geqslant b \cdot c$ für $a \leqslant b$ und $c \leqslant 0$, da:
$$a \leqslant b \ \xrightarrow{\text{(A1)}} \ a + \big((-a) + (-b)\big) \leqslant b + \big((-a) + (-b)\big) \ \Longrightarrow \ -b \leqslant -a$$
und Multiplikation mit $-c \geqslant 0$ und Anwendung von (A2) ergibt $b \cdot c \leqslant a \cdot c$.

Reelle Zahlen

- $\mathbb{Q}$ läßt sich auf der Zahlengeraden darstellen, sodass jede rationale Zahl einem Punkt auf der Zahlengeraden entspricht
- $\mathbb{Q}$ ist dicht in der Zahlengeraden in dem Sinne, dass zwischen je zwei Punkten auf der Zahlengeraden mindestens eine rationale Zahl liegt
- auf der anderen Seite entspricht nicht jeder Punkt auf der Zahlengeraden einer rationalen Zahl, z. B. hatten wir gezeigt, dass $\sqrt{2}$ keine rationale Zahl ist (aber $\sqrt{2}$ entspricht einem Punkt auf der Zahlengeraden)
- man kann $\mathbb{Q}$ so zur Menge $\mathbb{R}$ der reellen Zahlen erweitern, dass jedem Punkt auf der Zahlengeraden eine reelle Zahl entspricht und umgekehrt jede reelle Zahl einem Punkt auf der Zahlengeraden
  - die formale Konstruktion von $\mathbb{R}$ aus $\mathbb{Q}$ überspringen wir hier
  - Standardkonstruktionen basieren auf DEDEKINDschen Schnitten oder auf Äquivalenzklassen von CAUCHY-Folgen $\longrightarrow$ Analysis
  - dabei erweitert man die Addition, die Multiplikation und die totale Ordnung auf $\mathbb{R}$ ($a \leqslant b$, wenn a links von b auf der Zahlengeraden liegt)

$\Rightarrow$ mit der üblichen Addition, Multiplikation und Ordnung ist die Menge der reellen Zahlen $\mathbb{R}$ ein angeordneter Körper

- im Gegensatz zu $\mathbb{Q}$ ist $\mathbb{R}$ auch noch vollständig (siehe Analysis) und bis auf Isomorphie ist $\mathbb{R}$ der einzige vollständige und angeordnete Körper
- die Zahlen in $\mathbb{R} \setminus \mathbb{Q}$ heißen irrationale Zahlen, z. B. $\sqrt{2}$, e, π

$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$?

Streng genommen geht aus den vorangegangenen Definitionen von $\mathbb{Z}$, $\mathbb{Q}$ und $\mathbb{R}$ nicht hervor, dass $\mathbb{N}$ eine Teilmenge von $\mathbb{Z}$ oder $\mathbb{Z}$ eine Teilmenge von $\mathbb{Q}$ ist. Zum Beispiel wurde $\mathbb{Z}$ als die Faktormenge einer Äquivalenzrelation auf $\mathbb{N}_0 \times \mathbb{N}_0$ definiert und diese Faktormenge enthält formal $\mathbb{N}$ nicht!

Auf der anderen Seite, haben wir eine injektive Funktion $n \mapsto [(n, 0)]$ von $\mathbb{N}$ in diese Faktormenge angegeben, für die sich die auf $\mathbb{N}$ definierte Addition und Multiplikation erhält, z. B. für die Addition ergibt sich aus der Definition sofort für alle natürlichen Zahlen ℓ, m und n, dass $\ell + m = n$ genau dann gilt, wenn $[(\ell, 0)] +_{\mathbb{Z}} [(m, 0)] = [(n, 0)]$. Diese Einbettung von $\mathbb{N}$ erlaubt es $\mathbb{N}$ als Teilmenge von $\mathbb{Z}$ zu betrachten und wir werden von nun an $\mathbb{N}$ immer als diese Teilmenge von $\mathbb{Z}$ ansehen.

Genauso kann mit Hilfe der Funktion $z \mapsto [(z, 1)]$ die Menge der ganzen Zahlen in $\mathbb{Q}$ eingebettet werden, welche wiederum durch $q \mapsto [(q)_{n\in\mathbb{N}}]$ als eine Teilmenge von $\mathbb{R}$ aufgefasst werden kann. Von nun an werden wir auf Grund dieser Einbettungen sowohl die rationalen, als auch die ganzen und die natürlichen Zahlen als durch $\leqslant$ vollständig geordnete Teilmengen der reellen Zahlen betrachten und die Addition und Multiplikation einfach mit $+$ und $\cdot$ bezeichnen. Insbesondere gilt also

$$\mathbb{N} \subset \mathbb{N}_0 \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}\,.$$

Mächtigkeiten von Mengen

- Mengen A und B sind gleichmächtig $:\Leftrightarrow$ es gibt Bijektion zwischen A und B
- für $n \in \mathbb{N}_0$ schreiben wir $[n]$ als Kurzform für die Menge $\{1, \ldots, n\}$

Definition

Eine Menge M heißt:

- endlich: falls M gleichmächtig zu $[n]$ für ein $n \in \mathbb{N}_0$, d. h. M hat genau n Elemente (M ist n-elementig, M ist eine n-Menge) und wir schreiben
$$|M| := n\,.$$
- unendlich: falls M **nicht** endlich ist.
- abzählbar: falls M endlich ist **oder** gleichmächtig mit $\mathbb{N}$ ist.
- überabzählbar: falls M **nicht** abzählbar ist.

Bemerkungen

- $M \neq \varnothing$ ist abzählbar genau dann, wenn es eine surjektive Abbildung $f : \mathbb{N} \to M$ gibt und f heißt Aufzählung von M
- $n \mapsto n - 1$ zeigt $\mathbb{N}_0$ ist abzählbar
- $n \mapsto (-1)^n \lfloor n/2 \rfloor$ zeigt $\mathbb{Z}$ ist abzählbar, wobei für $x \in \mathbb{R}$ mit $\lfloor x \rfloor$ die größte ganze Zahl $\leqslant x$ bezeichnet wird

Mächtigkeit von $\mathbb{Q}$

Satz

Die Menge der rationalen Zahlen $\mathbb{Q}$ ist abzählbar.

Beweis

Wir geben eine Aufzählung $q_1, q_2, \ldots$ der Menge der rationalen Zahlen > 0 an. Man erhält die Aufzählung, indem man im folgenden Bild bei den Bruch $\frac{1}{1}$ beginnt und den Pfeilen folgt:

$$\begin{tikzcd}
\frac{1}{1} \arrow[r] & \frac{1}{2} \arrow[dl] & \frac{1}{3} \arrow[r] & \frac{1}{4} \arrow[dl] & \frac{1}{5} \arrow[r] & \frac{1}{6} \arrow[dl] & \cdots \\
\frac{2}{1} \arrow[d] & \frac{2}{2} \arrow[ur] & \frac{2}{3} \arrow[dl] & \frac{2}{4} \arrow[ur] & \frac{2}{5} \arrow[dl] & \frac{2}{6} & \cdots \\
\frac{3}{1} \arrow[ur] & \frac{3}{2} \arrow[dl] & \frac{3}{3} \arrow[ur] & \frac{3}{4} \arrow[dl] & \frac{3}{5} & \frac{3}{6} & \cdots \\
\frac{4}{1} \arrow[d] & \frac{4}{2} \arrow[ur] & \frac{4}{3} \arrow[dl] & \frac{4}{4} & \frac{4}{5} & \frac{4}{6} & \cdots \\
\frac{5}{1} \arrow[ur] & \frac{5}{2} & \frac{5}{3} & \frac{5}{4} & \frac{5}{5} & \frac{5}{6} & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots &
\end{tikzcd}$$

Satz

Die Menge der rationalen Zahlen $\mathbb{Q}$ ist abzählbar.

Die Aufzählung lautet also

$$q_1 = \frac{1}{1}, \quad q_2 = \frac{1}{2}, \quad q_3 = \frac{2}{1}, \quad q_4 = \frac{3}{1}, \quad q_5 = \frac{2}{2}, \dots$$

Die Tatsache, dass viele rationale Zahlen hierbei doppelt auftreten, zum Beispiel 1 als $\frac{1}{1}$ und $\frac{2}{2}$ spielt keine Rolle, da eine Aufzählung nicht injektiv sein muss. Es ist aber klar, dass jede rationale Zahl > 0 in dieser Aufzählung irgendwann einmal auftritt.

Mit dieser Aufzählung der rationalen Zahlen > 0 können wir nun aber leicht eine Aufzählung aller rationalen Zahlen angeben:

$$0, q_1, -q_1, q_2, -q_2, \dots$$

leistet das Gewünschte. $\square$

Mächtigkeit von $\mathbb{R}$

Satz (Cantor 1874)

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

Beweis: Wir zeigen, dass schon die Menge der reellen Zahlen, die echt größer als 0 und echt kleiner als 1 sind, überabzählbar ist. Wir führen einen Widerspruchsbeweis. Angenommen, es gibt eine Aufzählung $s_1, s_2, s_3, \ldots$ der reellen Zahlen s mit $0 < s < 1$. Die Zahlen s_n, $n \in \mathbb{N}$ lassen sich als Dezimalzahlen ohne Vorzeichen mit einer 0 vor dem Dezimalpunkt schreiben. Für alle $i, j \in \mathbb{N}$ sei s_{ij} die Ziffer, die in der j-ten Nachkommastelle der Dezimaldarstellung von s_i steht:

$$\begin{array}{ccc} s_1 & = & 0.s_{11}s_{12}s_{13}\ldots \\ s_2 & = & 0.s_{21}s_{22}s_{23}\ldots \\ \vdots & & \vdots \end{array}$$

Nun definieren wir eine weitere reelle Zahl a, die echt zwischen 0 und 1 liegt, die in der Aufzählung aber nicht auftritt. Wir geben die Nachkommastellen $a_1 a_2 a_3 \ldots$ der Zahl a an. Für $i \in \mathbb{N}$ sei

$$a_i := \begin{cases} 4, & \text{falls } s_{ii} \neq 4 \text{ ist und} \\ 5, & \text{sonst.} \end{cases}$$

Es ist klar, dass $a = 0.a_1 a_2 a_3 \ldots$ echt zwischen 0 und 1 liegt. Die Zahl a ist so gewählt, dass es sich an der i-ten Nachkommastelle von s_i unterscheidet. Damit ist a von allen s_i, $i \in \mathbb{N}$ verschieden. $\square$

Teilbarkeit

Definition (Teiler)

Eine ganze Zahl $x \in \mathbb{Z}$ ist ein Teiler von $y \in \mathbb{Z}$, falls ein $d \in \mathbb{Z}$ existiert, sodass

$$y = d \cdot x\,.$$

- Wir sagen auch, y ist ein Vielfaches von x ist und schreiben $x \mid y$.
- Falls x kein Teiler von y ist, dann schreiben wir $x \nmid y$.

Bemerkungen

- jede ganze Zahl $x \in \mathbb{Z}$ teilt also die 0 $\qquad 0 = 0 \cdot x$
- 0 ist nur Teiler von der 0
- es gilt für alle $x, y \in \mathbb{Z}$

$$x \mid y \iff -x \mid y \iff x \mid -y \iff -x \mid -y$$

- Teilbarkeiten in $\mathbb{Z}$ lassen sich also auf Teilbarkeiten in $\mathbb{N}_0$ zurückführen

Teilbarkeitsrelation

Satz

Teilbarkeitsbeziehung $\mid$ definiert eine Relation auf $\mathbb{Z}$ (bzw. auf $\mathbb{N}_0$) mit folgenden Eigenschaften:

- reflexiv, da $x \mid x$
- transitiv, da $x \mid y$ und $y \mid z$ bedeutet, dass es d_1, d_2 mit $y = d_1 \cdot x$ und $z = d_2 \cdot y$ gibt $\implies z = d_2 \cdot y = d_2 \cdot d_1 \cdot x \implies x \mid z$
- antisymmetrisch auf $\mathbb{N}_0$ (aber **nicht** auf $\mathbb{Z}$), da $x \mid y$ und $y \mid x$ bedeutet $y = d_1 \cdot x$ und $x = d_2 \cdot y$ für geeignete d_1 und d_2 $\implies y = d_1 \cdot d_2 \cdot y$ und $x = d_1 \cdot d_2 \cdot x \implies d_1 \cdot d_2 = 1$ oder $y = x = 0$

Des Weiteren gilt:

- $x_1 \mid y_1$ und $x_2 \mid y_2 \implies (x_1 \cdot x_2) \mid (y_1 \cdot y_2)$
- $(x \cdot y_1) \mid (x \cdot y_2)$ und $x \neq 0 \implies y_1 \mid y_2$
- $x \mid y_1$ und $x \mid y_2 \implies x \mid (y_1 \cdot z_1 + y_2 \cdot z_2)$ für alle z_1, z_2.

Größter gemeinsamer Teiler und kleinstes gemeinsames Vielfaches

Definition (ggT und kgV)

Für ganze Zahlen $x, y \in \mathbb{Z}$ ist der größte gemeinsame Teiler ($\mathrm{ggT}(x, y)$) von x und y ist die größte natürliche Zahl $n \in \mathbb{N}$, die sowohl x als auch y teilt, wobei man für $x = y = 0$ üblicherweise $\mathrm{ggT}(0, 0) := 0$ setzt.

Das kleinste gemeinsame Vielfache ($\mathrm{kgV}(x, y)$) von x und y ist die kleinste natürliche Zahl $n > 0$, die sowohl von x als auch von y geteilt wird, wobei man für $x = 0$ oder $y = 0$ üblicherweise $\mathrm{kgV}(x, y) := 0$ setzt.

Beispiele

- $\mathrm{ggT}(18, 45) = 9$ und $\mathrm{kgV}(18, 45) = 90$ und $9 \cdot 90 = 810 = 18 \cdot 45$
- $\mathrm{ggT}(24, 18) = 6$ und $\mathrm{kgV}(24, 18) = 72$ und $6 \cdot 72 = 432 = 24 \cdot 18$
- Allgemein gilt tatsächlich (Beweis folgt später):

$$\mathrm{ggT}(x, y) \cdot \mathrm{kgV}(x, y) = |x \cdot y|,$$

wobei $|z|$ der Absolutbetrag einer ganzen Zahl $z \in \mathbb{Z}$ ist.

Berechnung des ggT

- $\mathrm{ggT}(x, y) = \mathrm{ggT}(|x|, |y|)$ für alle $x, y \in \mathbb{Z} \implies$ o. B. d. A. seien $x, y \in \mathbb{N}_0$

Proposition

Für alle $x, y \in \mathbb{N}_0$ mit $x \geqslant y$ gilt $\mathrm{ggT}(x, y) = \mathrm{ggT}(x - y, y)$.

Beweis

Jeder Teiler von x und y teilt auch $x - y$. Somit gilt auch

$$\mathrm{ggT}(x, y) \mid x - y \quad \text{und} \quad \mathrm{ggT}(x, y) \mid y \implies \mathrm{ggT}(x, y) \leqslant \mathrm{ggT}(x - y, y)\,.$$

Auf der anderen Seite teilt auch jeder Teiler von $x - y$ und y auch $x - y + y = x$ und somit gilt auch

$$\mathrm{ggT}(x - y, y) \mid x \quad \text{und} \quad \mathrm{ggT}(x - y, y) \mid y \implies \mathrm{ggT}(x - y, y) \leqslant \mathrm{ggT}(x, y)\,.$$

Also muss gelten $\mathrm{ggT}(x, y) = \mathrm{ggT}(x - y, y)$ $\square$

- Proposition liefert rekursiven Algorithmus für die Berechnung des ggT

Einfacher EUKLIDischer Algorithmus

Idee

- wende Proposition wiederholt an, bis sich ein Argument auf 0 reduziert

Einfacher rekursiver EUKLIDischer Algorithmus

```
int ggT(int x, int y) {
  if ( x==0 ) return y;
  if ( y==0 ) return x;
  if ( x>=y )
    return ggT(x-y,y);
  else
    return ggT(x,y-x);
}
```

- Algorithmus berechnet den $\mathrm{ggT}(|x|, |y|)$ (Korrektheit):
  - Induktion über $n = |x| + |y|$ mit mehreren Vorgängern
  - Induktionsanfang $x = 0$ oder $y = 0$ klar wegen der Definition des ggT
  - Induktionsschritt für $|x| > 0$ und $|y| > 0$ durch Proposition
- **Problem:** langsamer Algorithmus – Laufzeit $O(|x| + |y|)$ **keine** polynomielle Laufzeit in der Länge der Eingabe $\log|x| + \log|y|$

Warum ist der einfache Algorithmus schlecht?

- Rekursion ist hier unkritisch, keine Mehrfachberechnungen gleicher Teilergebnisse
- wenn x sehr groß und y sehr klein ist, dann wird sehr oft y von x abgezogen
- z. B. $x = 2^{51}$ und $y = 2$ resultiert in $2^{50} \sim 10^{15}$ Subtraktionen für die mein Rechner mehr als **8 Tage** braucht
- für $x = 2^{61}$ und $y = 2$ braucht der Algorithmus dann ~ 1000-mal so lange, obwohl die Eingabe nur 10 Bit länger geworden ist

$\longrightarrow$ exponentielle Laufzeit

Beobachtung

- beim einfachen EUKLIDischen Algorithmus ziehen wir y solange ab, bis $z = x - y < y$ erreicht ist

$\Rightarrow$ Division mit Rest von x und y liefert uns dieses z in einem Schritt

Division mit Rest

Definition und Satz

Für je zwei ganze Zahlen x, $y \in \mathbb{Z}$ mit $y \neq 0$ gibt es eindeutig bestimmte Zahlen $q \in \mathbb{Z}$ und $r \in \mathbb{N}_0$, sodass

$$x = q \cdot y + r \quad \text{und} \quad 0 \leqslant r < |y| \,. \tag{$*$}$$

Die Zahl q heißt Quotient und r heißt Rest der Division.

- div: $\mathbb{Z}^2 \to \mathbb{Z}$ ordnet (x, y) den Quotienten q zu,
- mod: $\mathbb{Z}^2 \to \mathbb{N}_0$ ordnet (x, y) den Rest r zu.

Beweis

- Existenz: Eine der $|y| \geqslant 1$ hintereinander liegenden ganzen Zahlen
$$x - 0\,, \; x - 1\,, \; \ldots\,, \; x - (|y| - 1)$$
ist ein Vielfaches von y.
$\Longrightarrow$ es gibt $r \in \{0, 1, \ldots, |y| - 1\}$ und $q \in \mathbb{Z}$ mit $x - r = q \cdot y$. ✓
- Eindeutigkeit: Falls $qy + r = x = q'y + r'$ wie in $(*)$, dann gilt
$$0 = (q - q')y + (r - r') \text{ mit } |r - r'| < |y|.$$
$\Longrightarrow$ $y \mid (r - r')$, da $y \mid 0$ und $y \mid (q - q')y$
$\Longrightarrow$ wegen $|r - r'| < |y|$ folgt dann $r = r'$
$\Longrightarrow$ $qy = q'y$ und wegen $y \neq 0$ folgt $q = q'$ ✓ $\square$

Verbesserter EUKLIDischer Algorithmus

- Ersetze Subtraktionen durch Division mit Rest
- Proposition 2: $\mathrm{ggT}(x, y) = \mathrm{ggT}(\mathrm{mod}(x, y), y)$

  $\longrightarrow$ Beweis wie bei der Proposition zuvor

Verbesserter rekursiver EUKLIDischer Algorithmus

```
int ggT(int x, int y) {
  if ( x==0 ) return y;
  if ( y==0 ) return x;
  if ( x>=y )
    return ggT(x%y,y); /* x%y = mod(x,y) */
  else
    return ggT(x,y%x);
}
```

- Korrektheit: Algorithmus berechnet den $\mathrm{ggT}(|x|, |y|)$,

  $\longrightarrow$ Induktionsbeweis wie zuvor mit Proposition 2
- mod ist etwas teurer (Laufzeit) als Subtraktion, aber der verbesserte EUKLIDische Algorithmus hat polynomielle Laufzeit in der Länge der Eingabe $\log|x| + \log|y|$

Kongruenzen

Definition

Ganze Zahlen x, $y \in \mathbb{Z}$ sind kongruent modulo m für eine natürliche Zahl $m \in \mathbb{N}$, falls

$$\operatorname{mod}(x, m) = \operatorname{mod}(y, m)\,,$$

d. h. x und y haben denselben Rest bei Division durch m. In diesem Fall sagen wir auch, x ist kongruent zu y modulo m und schreiben

$$x \equiv y \pmod{m}\,.$$

Bemerkungen

- $x \equiv y \pmod{m} \iff m \mid x - y$
- Kongruenz modulo m definiert Äquivalenzrelation auf $\mathbb{Z}$:
  - Reflexivität $\checkmark$
  - Symmetrie $\checkmark$
  - Transitivität: $m \mid x - y$ und $m \mid y - z \Rightarrow m \mid x - y + y - z$ $\checkmark$

Restklassen

Definition (Restklassen)

Für jede natürliche Zahl $m \in \mathbb{N}$ und jede ganze Zahl $x \in \mathbb{Z}$ heißt die Äquivalenzklasse

$$[x]_m := \{y \in \mathbb{Z} \colon x \equiv y \pmod{m}\}$$

die Restklasse von x modulo m.

Folgerungen

- für jedes $m \in \mathbb{N}$ gibt es genau m verschiedene Restklassen modulo m

$$[0]_m\,,\ [1]_m\,,\ \ldots\,,\ [m-1]_m\,.$$

- die Restklassen bilden eine Partition von $\mathbb{Z}$, d. h. sie sind paarweise disjunkt und

$$\mathbb{Z} = [0]_m \mathbin{\dot\cup} \ldots \mathbin{\dot\cup} [m-1]_m$$

- Menge der Restklassen (Faktormenge der Äquivalenzrelation kongruent modulo m)

$$\mathbb{Z}/m\mathbb{Z} := \big\{[0]_m\,,\ [1]_m\,,\ \ldots\,,\ [m-1]_m\big\}$$

Modulare Arithmetik

- mit Restklassen kann man gut rechnen
- $x_1 \equiv y_1 \pmod{m}$ und $x_2 \equiv y_2 \pmod{m} \Rightarrow (x_1 + x_2) \equiv (y_1 + y_2) \pmod{m}$

$\Rightarrow$ $[z]_m + [z']_m := [z + z']_m$ ist wohldefinierte Addition auf $\mathbb{Z}/m\mathbb{Z}$

  - Addition auf $\mathbb{Z}/m\mathbb{Z}$ ist assoziativ und kommutativ
  - $[0]_m$ ist neutrales Element der Addition auf $\mathbb{Z}/m\mathbb{Z}$
  - Subtraktion kann durch $[z]_m - [z']_m := [z - z']_m$ definiert werden
  - $[-z]_m$ ist invers zu $[z]_m$, d. h. $-[z]_m = [-z]_m$
  - für $\ell \in \{0, \ldots, m-1\}$ gilt $-[\ell]_m = [-\ell]_m = [m - \ell]_m$

- $x_1 \equiv y_1 \pmod{m}$ und $x_2 \equiv y_2 \pmod{m} \Rightarrow (x_1 \cdot x_2) \equiv (y_1 \cdot y_2) \pmod{m}$

$\Rightarrow$ $[z]_m \cdot [z']_m := [z \cdot z']_m$ ist wohldefinierte Multiplikation auf $\mathbb{Z}/m\mathbb{Z}$

  - Multiplikation auf $\mathbb{Z}/m\mathbb{Z}$ ist assoziativ und kommutativ
  - $[1]_m$ ist neutrales Element der Multiplikation auf $\mathbb{Z}/m\mathbb{Z}$
  - im Allgemeinen gibt es keine inversen Elemente für die Multiplikation:

$$[2]_4 \cdot [0]_4 = [0]_4\,, \qquad [2]_4 \cdot [1]_4 = [2]_4\,,$$
$$[2]_4 \cdot [2]_4 = [4]_4 = [0]_4\,, \qquad [2]_4 \cdot [3]_4 = [6]_4 = [2]_4$$

  $\Rightarrow [2]_4$ hat kein multiplikativ Inverses in $\mathbb{Z}/4\mathbb{Z}$

  - Addition und Multiplikation erfüllen das Distributivgesetz

Für jedes $m \in \mathbb{N}$ heißt $\mathbb{Z}/m\mathbb{Z}$ mit Verknüpfungen $+$ und $\cdot$ Restklassenring modulo m.

- $\mathbb{Z}/1\mathbb{Z} = \{[0]_1\} = \{\mathbb{Z}\}$ ist trivial (Nullring), aber $\mathbb{Z}/2\mathbb{Z} = \mathbb{F}_2$ ist sogar ein Körper

Gaussklammer

Definition

Sei $\xi \in \mathbb{R}$ eine reelle Zahl. Dann bezeichnet

- $\lceil \xi \rceil$ die kleinste ganze Zahl $z \in \mathbb{Z}$ mit $z \geqslant \xi$.
- $\lfloor \xi \rfloor$ die größte ganze Zahl $z \in \mathbb{Z}$ mit $z \leqslant \xi$.

Beobachtung

Für alle $z \in \mathbb{Z}$ und $n \in \mathbb{N}$ gilt

$$\operatorname{div}(z, n) = \left\lfloor \frac{z}{n} \right\rfloor \quad \text{und} \quad \operatorname{mod}(z, n) = z - n \cdot \left\lfloor \frac{z}{n} \right\rfloor .$$

Primzahlen

Definition (Primzahlen)

Eine natürliche Zahl $p \geqslant 2$ heißt Primzahl, falls 1 und p die einzigen Teiler von p in $\mathbb{N}$ sind.

- Menge der Primzahlen $\{2, 3, 5, 7, 11, 13, \ldots, 2011, 2017, 2027, \ldots\}$
- 1 und n heißen auch die trivialen (natürlichen) Teiler von $n \in \mathbb{N}$
- 1, -1, z und $-z$ sind die trivialen (ganzen) Teiler von $z \in \mathbb{Z}$

Definition (teilerfremd)

Zwei ganze Zahlen heißen teilerfremd (auch relativ prim), falls die 1 der einzige gemeinsame Teiler in $\mathbb{N}$ ist. Es gilt also

$$x, y \in \mathbb{Z} \quad \text{sind teilerfremd} \quad \iff \quad \mathrm{ggT}(x, y) = 1$$

- Teilerfremdheit ist **nicht** reflexiv, **nicht** transitiv, aber symmetrisch
- Für teilerfremde $z \in \mathbb{Z}$ und $m \in \mathbb{N}$ gilt:
  $(z \cdot x) \equiv (z \cdot y) \pmod{m} \implies x \equiv y \pmod{m}$ für alle x, $y \in \mathbb{Z}$.

Falls $p \in \mathbb{N}$ eine Primzahl ist, dann ist $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ ein Körper.

Primfaktorzerlegung

Satz (Hauptsatz der elementaren Zahlentheorie)

Für jede natürliche Zahl $n \in \mathbb{N}$ gibt es

- ein $k \in \mathbb{N}_0$,
- paarweise verschiedene Primzahlen $p_1, \ldots, p_k$
- und natürliche Zahlen $\alpha_1, \ldots, \alpha_k \in \mathbb{N}$,

sodass

$$n = \prod_{i=1}^{k} p_i^{\alpha_i} .$$

Diese Produktdarstellung von n heißt Primfaktorzerlegung und ist bis auf die Reihenfolge der Faktoren eindeutig.

Bemerkungen

- für $n = 1$ ist $k = 0$ und der Satz folgt, da das leere Produkt 1 ist
- für $n \geqslant 2$ ist immer $k \geqslant 1$
- Sicherheit vieler Verschlüsselungsverfahren beruht auf der Annahme, dass für gegebenes n die Primfaktorzerlegung **nicht** effizient berechenbar ist
  $\longrightarrow$ theoretisch effizient berechenbar mit Quantencomputern
  $\longrightarrow$ Entscheidungsproblem liegt in **NP** $\cap$ **coNP**

Existenz der Primfaktorzerlegung

Beweis (Widerspruch)
Sei n die kleinste natürliche Zahl, für die es keine Primfaktorzerlegung gibt.

- $n \neq 1$, da das leere Produkt eine Primfaktorzerlegung der 1 ist
- n ist keine Primzahl, da sonst $n = p^\alpha$ mit $p = n$ und $\alpha = 1$ eine Primfaktorzerlegung von n ist

$\Rightarrow$ n hat von 1 und n verschiedene Teiler

$\Rightarrow$ es gibt $x, y \in \mathbb{N}$ mit

$$1 < x < n, \qquad 1 < y < n \qquad \text{und} \qquad n = xy$$

Da n die kleinste Zahl ohne Primfaktorzerlegung ist, gibt es Primfaktorzerlegungen von x und y, d. h. für geeignete $k, \ell \in \mathbb{N}$, Primzahlen $p_1, \dots, p_k$, $q_1, \dots, q_\ell$ und $\alpha_1, \dots, \alpha_k, \beta_1, \dots, \beta_\ell \in \mathbb{N}$ gilt:

$$x = \prod_{i=1}^{k} p_i^{\alpha_i} \qquad \text{und} \qquad y = \prod_{j=1}^{\ell} q_j^{\beta_j} .$$

Somit ist $n = xy = \prod_{i=1}^k p_i^{\alpha_i} \prod_{j=1}^\ell q_j^{\beta_j}$ und ggf. durch das Zusammenfassen von Faktoren (falls $p_i = q_j$), erhalten wir eine Primfaktorzerlegung von n. $\lightning$

Lemma von BÉZOUT

- Beweis der Eindeutigkeit beruht auf dem Lemma von EUKLID, welches eine Konsequenz des Lemmas von BÉZOUT ist

Lemma (BÉZOUT)

Für alle ganzen Zahlen $x, y \in \mathbb{Z}$ gibt es ganze Zahlen $s, t \in \mathbb{Z}$, sodass

$$\mathrm{ggT}(x, y) = sx + ty\,.$$

- Der $\mathrm{ggT}(x, y)$ kann als Linearkombination von x und y dargestellt werden.
- Für teilerfremde $x, y \in \mathbb{Z}$ gibt es somit $s, t \in \mathbb{Z}$ mit $sx + ty = 1$.

Beweis (wie Proposition vor dem EUKLIDischen Algorithmus)

- o. B. d. A. $x, y \in \mathbb{N}_0$ (Warum?) und $x \geqslant y$ (Warum?)
- Induktion nach x mit mehreren Vorgängern
- Induktionsanfang: $x = 0$, klar da dann $y = 0$ und $\mathrm{ggT}(0, 0) = 0$
- Induktionsschritt:

$$\mathrm{ggT}(x, y) \overset{\text{Prop.}}{=} \mathrm{ggT}(x - y, y) \overset{\text{I. A.}}{=} s'(x - y) + t'y = s'x + (t' - s')y$$

und die Aussage folgt mit $s = s'$ und $t = t' - s'$ $\square$

Erweiterter EUKLIDischer Algorithmus

rekursive Berechnung von $\mathrm{ggT}(x, y)$, s und t mit $\mathrm{ggT}(x, y) = sx + ty$

```
int erwEuklid(int x, int y, int *s,  int *t) {
  if ( x==0 ){ *s=0; *t=1; return y; }
  if ( y==0 ){ *s=1; *t=0; return x; }
  int ggT, sp, tp;                  /* Zwischenergebnisse speichern */
  if ( x>y ){
    ggT = erwEuklid(x%y, y, &sp, &tp);       /* % = mod,  / = div  */
    *s = sp; *t = tp - sp*(x/y);             /* s und t verrechnen */
    return ggT;
  }
  else{
    ggT = erwEuklid(x, y%x, &sp, &tp);
    *s = sp - tp*(y/x); *t = tp;             /* s und t verrechnen */
    return ggT;
  }
}
```

Korrektheit folgt induktiv mit $x = q \cdot y + r$ für $q = \mathrm{div}(x, y)$ und $r = \mathrm{mod}(x, y)$ durch:

$$\mathrm{ggT}(x, y) = \mathrm{ggT}(r, y) = s'r + t'y$$

und wegen $r = x - q \cdot y$ folgt $\mathrm{ggT}(x, y) = s'x + (t' - s' \cdot q)y$.

Lemma von Euklid

Lemma (Euklid)

Für alle ganzen Zahlen $x, y \in \mathbb{Z}$ und jede natürliche Zahl $n \in \mathbb{N}$ gilt

$$n \mid xy \quad \text{und} \quad \mathrm{ggT}(x, n) = 1 \qquad \Longrightarrow \qquad n \mid y\,.$$

Insbesondere teilt also jede Primzahl p einen Faktor x oder y, falls p Teiler des Produkts xy ist.

Beweis

Wegen Bézouts Lemma (für x und n) gibt es $s, t \in \mathbb{Z}$ mit

$$sx + tn = \mathrm{ggT}(x, n) = 1 \qquad \Longrightarrow \qquad sxy + tny = y\,.$$

Da $n \mid xy$ gibt es ein $d \in \mathbb{Z}$ mit $xy = dn$ und damit erhalten wir

$$y = s \cdot dn + tny = (sd + ty)n\,.$$

Somit ist y ein Vielfaches von n. $\square$

Eindeutigkeit der Primfaktorzerlegung

Beweis (Widerspruch)
Sei n die kleinste natürliche Zahl, für die es mindestens zwei Primfaktorzerlegungen gibt.

- $n \neq 1$, da die 1 ausschließlich durch das leere Produkt als Produkt dargestellt werden kann
- n ist keine Primzahl, da wir sonst eine Primzahl als Produkt von Primzahlen schreiben könnten
- beide Primfaktorzerlegungen können keinen gemeinsamen Primfaktor p haben, da sonst n/p eine kleinere Zahl mit meheren Primfaktorzerlegungen wäre

$\Rightarrow$ es gibt unterschiedliche Primzahlen p und q und $x, y \in \mathbb{N}$ mit

$$1 < x < n\,, \qquad 1 < y < n\,, \qquad x \neq y \qquad \text{und} \qquad px = n = qy$$

Insbesondere haben wir

$$p \mid qy \qquad \text{und} \qquad \mathrm{ggT}(p, q) = 1\,.$$

Nach dem Lemma von EUKLID ist p also ein Teiler von y, aber dies widerspricht der obigen Beobachtung, dass wegen der minimalen Wahl von n keine Primzahl in beiden Primfaktozerlegungen vorkommt. $\lightning$

Wieviele Primzahlen gibt es?

Satz (Euklid 300v. Chr.)

Es gibt unendlich viele Primzahlen.

Beweis (Widerspruch)

Angenommen es gibt nur endlich viele Primzahlen $p_1, \ldots, p_k$.

- **Beobachtung:** N und $N+1$ haben keinen gemeinsamen Teiler $\geqslant 2$, da jeder Teiler auch $N+1-N=1$ teilt
- betrachte das Produkt $N = p_1 \cdot \ldots \cdot p_k$

$\Rightarrow$ N und $N+1$ haben keine gemeinsamen Primfaktoren

$\Rightarrow$ alle Primzahlen aus der Primfaktorzerlegung von $N+1$ sind verschieden von $p_1, \ldots, p_k$

- wegen $N+1>1$ gibt es auch mindestens einen Primfaktor q von $N+1$

Es gibt also eine weitere Primzahl q verschieden von $p_1, \ldots, p_k$. $\lightning$

ggT und kgV und Primfaktoren

Satz

Für alle ganzen Zahlen x und $y \in \mathbb{Z}$ gilt

$$\operatorname{ggT}(x,y) \cdot \operatorname{kgV}(x,y) = |x \cdot y|\,.$$

Beweis

- o. B. d. A. $x,\ y \in \mathbb{N}_0$ (Warum?)
- falls $x = 0$ oder $y = 0$, dann $\operatorname{kgV}(x,y) = 0$ und die Formel folgt
- seien $p_1, \ldots, p_\ell$ alle gemeinsamen Primfaktoren von x und y und

$$x = \prod_{i=1}^{\ell} p_i^{\alpha_i} \cdot \prod_{i=\ell+1}^{k} p_i^{\alpha_i} \quad \text{und} \quad y = \prod_{i=1}^{\ell} p_i^{\beta_i} \cdot \prod_{i=\ell+1}^{m} q_i^{\beta_i}$$

die Primfaktorzerlegungen von x und y

Damit folgt

$$\operatorname{ggT}(x,y) = \prod_{i=1}^{\ell} p_i^{\min(\alpha_i,\beta_i)}$$

$$\operatorname{kgV}(x,y) = \prod_{i=1}^{\ell} p_i^{\max(\alpha_i,\beta_i)} \cdot \prod_{i=\ell+1}^{k} p_i^{\alpha_i} \cdot \prod_{i=\ell+1}^{m} q_i^{\beta_i}\,.$$

Da $\min(\alpha_i,\beta_i) + \max(\alpha_i,\beta_i) = \alpha_i + \beta_i$ folgt die Aussage. □