Die Bezeichnung der Kontinuumshypothese kommt von:

Satz: Es gilt $|\mathbb{R}| = 2^{\omega}$.

Modul-Arithmetik

Referenz: [Halbeisen-Skript: Kapitel 10]

Im folgenden fixieren wir eine ganze Zahl $n \geqslant 1$.

Definition: Für $a, a' \in \mathbb{Z}$ schreiben wir $a \equiv a' \bmod (n)$ und sagen „*a ist kongruent zu a' modulo n*“, falls $a' - a$ ein Vielfaches von n ist.

Proposition: (a) Dies ist eine Äquivalenzrelation auf $\mathbb{Z}$.

(b) Gilt $\left\{ \begin{array}{l} a \equiv a' \bmod (n) \ \text{ und} \\ b \equiv b' \bmod (n) \end{array} \right\}$, so gilt auch $\left\{ \begin{array}{l} a + b \equiv a' + b' \bmod (n) \ \text{ und} \\ a \cdot b \equiv a' \cdot b' \bmod (n) \end{array} \right\}$.

(c) Für jedes $a \in \mathbb{Z}$ existiert ein eindeutiges $b \in \mathbb{Z}$ mit $0 \leqslant b < n$ und $a \equiv b$ modulo (n). Also ist $\{0, 1, \ldots, n-1\}$ ein Repräsentantensystem für die Äquivalenzrelation.

Man könnte die Menge $Rep := \{0, 1, \ldots, n-1\}$ mit einer Ringstruktur versehen, indem man zu je zwei Elementen $a, b \in Rep$ die eindeutigen Elemente $a \oplus b$ und $a \odot b$ von Rep assoziiert mit $a + b \equiv a \oplus b \bmod (n)$ und $a \cdot b \equiv a \odot b \bmod (n)$. In der Praxis geht man anders vor:

Proposition-Definition: Bezeichne die Äquivalenzklasse eines Elements $a \in \mathbb{Z}$ mit $[a]$. Dann existiert eine eindeutige Struktur eines kommutativen unitären Rings auf der Menge

$$\mathbb{Z}/n\mathbb{Z} \;:=\; \{[a] : a \in \mathbb{Z}\}$$

mit dem Nullelement $[0]$ und dem Einselement $[1]$, so dass für alle $[a], [b] \in \mathbb{Z}/n\mathbb{Z}$ gilt:

$$[a] + [b] = [a + b] \qquad \text{und} \qquad [a] \cdot [b] = [a \cdot b].$$

Weiter ist das additive Inverse jedes Elements $[a]$ gleich $[-a]$.

Proposition: Ein Element $[a] \in \mathbb{Z}/n\mathbb{Z}$ ist genau dann invertierbar, wenn a teilerfremd zu n ist.

Beispiel: Die invertierbaren Elemente von $\mathbb{Z}/8\mathbb{Z}$ sind $[1], [3], [5], [7]$ mit $[3]^2 = [5]^2 = [7]^2 = [1]$.

Beispiel: Das Element $[5]$ von $\mathbb{Z}/26\mathbb{Z}$ ist invertierbar mit dem Inversen $[-5] = [21]$.

Proposition: Der Ring $\mathbb{Z}/n\mathbb{Z}$ ist ein Körper genau dann, wenn n eine Primzahl ist.

Definition: Für jede Primzahl schreiben wir kürzer $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$.

Proposition-Definition: Für jeden endlichen Körper k gilt:

(a) Es existiert eine eindeutige Primzahl p, so dass k einen zu $\mathbb{F}_p$ isomorphen Unterkörper enthält.

(b) Diese Primzahl heisst die *Charakteristik von* k.

(c) Die Kardinalität von k ist gleich p^n für eine natürliche Zahl $n \geqslant 1$.

Satz: Für jede Primpotenz p^n existiert ein endlicher Körper k mit $|k| = p^n$, und je zwei solche sind isomorph.

(Beweis eventuell später)

Proposition-Definition: Sei p eine Primzahl. Sei R ein kommutativer unitärer Ring mit der Eigenschaft $p \cdot 1_R = 0$. Dann ist die Abbildung

$$\varphi\colon R \to R, \quad a \mapsto a^p$$

ein Ringhomomorphismus, das heisst, für alle $a, b \in R$ gilt

$$\begin{aligned} \varphi(a+b) &= \varphi(a) + \varphi(b) \\ \varphi(a \cdot b) &= \varphi(a) \cdot \varphi(b) \\ \varphi(1) &= 1 \end{aligned}$$

Dieser Homomorphismus heisst *p-Frobenius* und wird bezeichnet mit Frob_p.

Proposition: Für jeden endlichen Körper k der Charakteristik p ist $\mathrm{Frob}_p \colon k \to k$ ein Automorphismus und auf dem Unterkörper $\mathbb{F}_p$ die Identität.

Folge: *(Kleiner Satz von Fermat)* Für jede Primzahl p und jede ganze Zahl a gilt $a^p \equiv a \bmod (p)$.

Proposition: *(Satz von Wilson)* Für jede Primzahl p gilt $(p-1)! \equiv -1 \bmod (p)$.