Die Bezeichnung der Kontinuumshypothese kommt von:

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

Beweis: $2 = \{0,1\}$

Betrachte $i: {}^\omega\{0,1\} \longrightarrow \mathbb{R}$, $(x_n)_n \mapsto \sum_{n \geq 0} a_n \cdot 10^{-n-1}$.

injektiv! Also ist $|\mathbb{R}| \geq |{}^\omega\{0,1\}| = 2^\omega$.

Umgekehrt: $p: \mathbb{Z} \times {}^\omega\{0,1\} \longrightarrow \mathbb{R}$, $(m,(a_n)) \mapsto m + \sum_{n \geq 0} a_n 2^{-n-1}$.

surjektiv! Also ist $|\mathbb{R}| \leq |\mathbb{Z} \times {}^\omega\{0,1\}| = \omega \cdot 2^\omega = \max\{\omega, 2^\omega\} = 2^\omega$.

$|\mathbb{Z}| = \omega$.

Also ist $|\mathbb{R}| = 2^\omega$.

qed.

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

(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.

Beweis: (a) $n \mid 0 = a - a \Rightarrow a \equiv a \bmod (n)$. reflexiv.

$a \equiv a' \bmod (n) \Rightarrow n \mid a' - a \Rightarrow n \mid a - a' \Rightarrow a' \equiv a \bmod (n)$. symmetrisch.

$\left\{ \begin{array}{l} a \equiv a' \bmod (n) \\ a' \equiv a'' \bmod (n) \end{array} \right\} \Rightarrow \left| \begin{array}{l} n \mid a' - a \\ \text{und} \\ n \mid a - a' \end{array} \right\} \Rightarrow n \mid a'' - a \Rightarrow a'' \equiv a \bmod (n)$. transitiv.

(b) Nach Vor. ist $n \mid a' - a$ und $n \mid b' - b$.

Damit $n \mid (a' + b') - (a + b) = (a' - a) + (b' - b)$. Also ist $a + b \equiv a' + b' \bmod (n)$.

und $n \mid (a' - a) \cdot b' + a \cdot (b' - b) = a'b' - ab$ d.h. $ab \equiv a'b' \bmod (n)$.

(c) Division mit Rest: $a = q \cdot n + b$.

qed.

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 $[-a]$.

Beweis: Wohldefiniertheit: Zu zeigen: $[a] = [a']$ und $[b] = [b'] \Rightarrow [a+b] = [a'+b']$ und $[ab] = [a'b']$.

Aber dann ist $a \equiv a'$ und $b \equiv b'$ mod (n).
Nach (b) ist also $a+b \equiv a'+b'$ und $ab \equiv a'b'$ mod (n).

Ringaxiome: Assoziativität: $\forall a, b, c \in \mathbb{Z}: \; (ab) \cdot c = a(b \cdot c)$

$$\Rightarrow ([a] \cdot [b]) \cdot [c] = [ab] \cdot [c] = [(ab) \cdot c] = [a(bc)] = [a] \cdot [bc] = [a] \cdot ([b] \cdot [c])$$

Fast analog zeigt man:

$\forall a \in \mathbb{Z}: \; [a] + [-a] = [a + (-a)] = [0]$.

Also existiert ein additives Inverses von $[a]$ und es ist $= [-a]$. qed

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

Ering: R kommut. unitärer Ring mit $x \in R$ invertierbar $\Leftrightarrow \exists y \in R : xy = 1$.
Die Menge $R^\times$ aller invertierbaren Elemente ist eine abelsche Gruppe bzgl. Multiplikation.

Beweis: Sei $[a]$ invertierbar. Also $\exists b \in \mathbb{Z} : [a]\cdot[b] = [1] \Rightarrow n \mid ab - 1 \Rightarrow n$ teilerfremd zu a.
Sei umgekehrt a teilerfremd zu n. Betrachte die Abb. $\varphi : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $[b] \mapsto [a]\cdot[b] = [ab]$.
Damit $\varphi([b]) = 0 \Leftrightarrow [ab] = 0 \Leftrightarrow n \mid ab \Leftrightarrow n \mid b \Leftrightarrow [b] = [0]$. Also ist $\ker(\varphi) = \{[0]\}$.
Also ist φ injektiv. Also ist φ surjektiv. Also exist. $b \in \mathbb{Z}$ mit $[a]\cdot[b] = [1]$. Also ist $[a]$ invertierbar. qed

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

$[3]^2 = [9] = [1]$
$[5]^2 = [25] = [1]$
$[7]^2 = [49] = [1]$.

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

5 und 26 teilerfremd.

Rate: $[5]\cdot[5] = [25] = [-1]$
$\Rightarrow [5]\cdot[-5] = [-25] = [1]$.

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

Ering: Ein kommut. unitärer Ring R ist ein Körper gdw. $1 \neq 0$ ist und $\forall k \in R \setminus \{0\} : k$ invertierbar.

Bem.: $[1] \neq [0] \Leftrightarrow n \nmid 1 - 0 \Leftrightarrow n \neq 1$
$\forall a \in \mathbb{Z} : [a] \neq [0] \Leftrightarrow n \nmid a - 0 = a$.
$[a]$ invertierbar $\Leftrightarrow n$ teilerfremd zu a.

Wäre $n = n_1 n_2$ mit $n_1, n_2 > 1$
wäre $n \nmid n_1 \Rightarrow [n_1] \neq [0]$
aber n_1 nicht teilerfremd zu $n \Rightarrow [n_1]$ nicht invertierbar.

qed

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 $n \geqslant 1$.

Beweis: (a) $\varphi: \mathbb{Z} \to k$, $a \mapsto a \cdot 1_k = \begin{cases} 1+\dots+1 & \text{ist } a \text{ Terme falls } a \geq 1 \\ 0 & \text{falls } a = 0 \\ -1-\dots-1 & \text{ist } -a \text{ Terme falls } a \leq -1 \end{cases}$.

k endlich $\Rightarrow$ nicht injektiv.
Seien $0 \leq a < b$ minimal mit $\varphi(a) = \varphi(b)$. Dann ist $\varphi(b-a) = \varphi(b) - \varphi(a) = 0$.
Minimalität $\Rightarrow a = 0$ und $\varphi(0), \varphi(1), \dots, \varphi(b-1)$ paarweise verschieden.
$\Rightarrow \mathbb{Z}/b\mathbb{Z} \to k$, $[a] \mapsto a \cdot 1_k$. Wohldef. da $[a] = [a'] \Rightarrow a' = a + mb$ für ein $m \in \mathbb{Z}$
$\Rightarrow \varphi(a') = \varphi(a) + \varphi(m) \cdot \varphi(b) = \varphi(a)$, ($\varphi(b) = 0$)
Injektiv: für jedes $[a] \neq [0]$ in $\mathbb{Z}/b\mathbb{Z}$ ist $k \to k$, $x \mapsto [a] \cdot x$ injektiv $\Rightarrow$ Surjektiv. $\Rightarrow \mathbb{Z}/b\mathbb{Z}$ Körper $\Rightarrow b$ Primzahl.
(c) $\mathbb{F}_p \subset k$, $\Rightarrow k$ ist Vektorraum über $\mathbb{F}_p$ mit $n := \dim_{\mathbb{F}_p}(k) < \infty$. $\Rightarrow |k| = |\mathbb{F}_p^n| = p^n$. qed

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

(Beweis eventuell später)

$1+1+\ldots+1=0$ (p Terme)

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

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

$(a+b)^p = a^p + b^p$.

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

Beweis: $\varphi(1) = 1^p = 1$.

$\varphi(a \cdot b) = (ab)^p = a^p b^p = \varphi(a) \cdot \varphi(b)$

$$\varphi(a+b) = (a+b)^p = \sum_{k=0}^{p} \binom{p}{k} \cdot a^{p-k} \cdot b^k = a^p + b^p.$$

gilt in jedem kommutativen unitären Ring.

$$\binom{p}{k} = \begin{cases} 1 & \text{falls } k = 0 \text{ oder } p. \\ \frac{p!}{k!(p-k)!} \equiv 0 \text{ und (*) für } 0 < k < p. & \end{cases}$$

da p im Zähler aber nicht im Nenner vorkommt.

$$\Rightarrow \binom{p}{k} \cdot 1_R = \begin{cases} 1_R & \text{falls } k = 0, p \\ 0 & \text{falls } 0 < k < p. \end{cases}$$

Qed.

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.

Beweis. $\mathrm{Frob}_k(a) = a^p = 0 \Leftrightarrow a = 0$. Also ist $\ker(\mathrm{Frob}_p) = \{0\} \Rightarrow \mathrm{Frob}_p$ injektiv.
$\Rightarrow$ bijektiv. $\Rightarrow$ Automorphismus.
$\mathrm{Frob}_p(1) = 1^p = 1$
$\forall n$: $\mathrm{Frob}_p(n+1) = \mathrm{Frob}_p(n) + \mathrm{Frob}_p(1) = \mathrm{Frob}_p(n) + 1$
} Induktion über $n \Rightarrow \mathrm{Frob}_p(n \cdot 1_k) = n \cdot 1_k$.
$\Rightarrow \mathrm{Frob}_p|_{\mathbb{F}_p} = \mathrm{id}$.
qed.

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

$\mathbb{F}_p$: $\forall a \in \mathbb{Z}$: $[a]^p = [a] \Rightarrow a^p \equiv a \ (p)$.

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

Beweis. Betrachte das Polynom $f(X) := X^p - X$. Grad p.
$\Rightarrow \forall\ \bar{a} \in \mathbb{F}_p$: $f(\bar{a}) = \bar{a}^p - \bar{a} = 0$.
$\Rightarrow f(X) = \prod_{\bar{a} \in \mathbb{F}_p} (X - \bar{a})$ in $\mathbb{F}_p[X]$.
$X^p - X$
$\Rightarrow X^{p-1} - 1 = \prod_{0 \neq \bar{a} \in \mathbb{F}_p} (X - \bar{a}) = \prod_{\xi=1}^{p-1} (X - \bar{\xi})$

Koeffizientenvergleich:
$\Rightarrow -1 = \prod_{\xi=1}^{p-1} (-\bar{\xi})$ in $\mathbb{F}_p$.
$= (-1)^{p-1} \cdot (p-1)!$ in $\mathbb{F}_p$
$\Rightarrow (p-1)! = (-\bar{1})^p = -\bar{1}$ in $\mathbb{F}_p$
$\Rightarrow (p-1)! \equiv -1 \bmod (p)$.
qed.