0

$- \quad \lambda \quad \boxslash \quad \lambda. \quad \mu \quad O \quad \varepsilon \quad \circlearrowleft \quad \{\}$

Sei $f(x) = x^2$. Dann:

$$\frac{f(x+\varepsilon)-f(x)}{\varepsilon} = \frac{(x+\varepsilon)^2 - x^2}{\varepsilon} = \frac{\cancel{x^2} + 2x\varepsilon + \varepsilon^2 - \cancel{x^2}}{\varepsilon}$$

$$= 2x + \varepsilon = \underline{\underline{2x}}$$

Diese Rechnung wird (nach kleinen Modifikationen) rigoros korrekt — im <u>glatten Topos</u>. Dort rechnen wir mit Zahlen ε mit $\varepsilon^2 = 0$.

Müssen wir uns um das Auswahlaxiom Sorgen machen?
Nein (aber es ist kompliziert).

Metamathematik:

mathematisch präzise über Mathe sprechen
(z.B. die Begriffe „Beweis" und „Wahrheit" definieren)

- Wahre aber unbeweisbare Aussagen
- Aussagen, die beweisenermaßen keine kurzen Beweise haben
- Wie es um die Kontinuumshypothese bestellt? $|\mathbb{N}| <^{?} < |\mathbb{R}|$
  $\rightsquigarrow$ Multiversum der mengentheoretischen Möglichkeiten

$\boxed{\text{LEM: } A \vee (\neg A)}$

Set

0
1
2
$\mathbb{N}$
$\mathbb{R}$
sin
LEM ✓
AC ✓
triv. Topos: $2+2=4$, $2+2=5$

Standardtopos Set

0 1 2 3 …
$\mathbb{N}$ $\mathbb{R}$ sin
$\emptyset$ $\sqrt{2} \notin \mathbb{Q}$ ✓ Auswahlaxiom ✓
$\sqrt{\cdot} : \mathbb{C} \to \mathbb{C}$ unstetig LEM ✓

Gödels L

0 1 2
Set
AC ✓

glatte Topos

0 1 2 3 set „$\varepsilon^2 = 0$"
$\mathbb{N}$ $\mathbb{R}$ AC ✗
$\sqrt{2} \notin \mathbb{Q}$ ✓ LEM ✗

Sh($\mathbb{C}$)

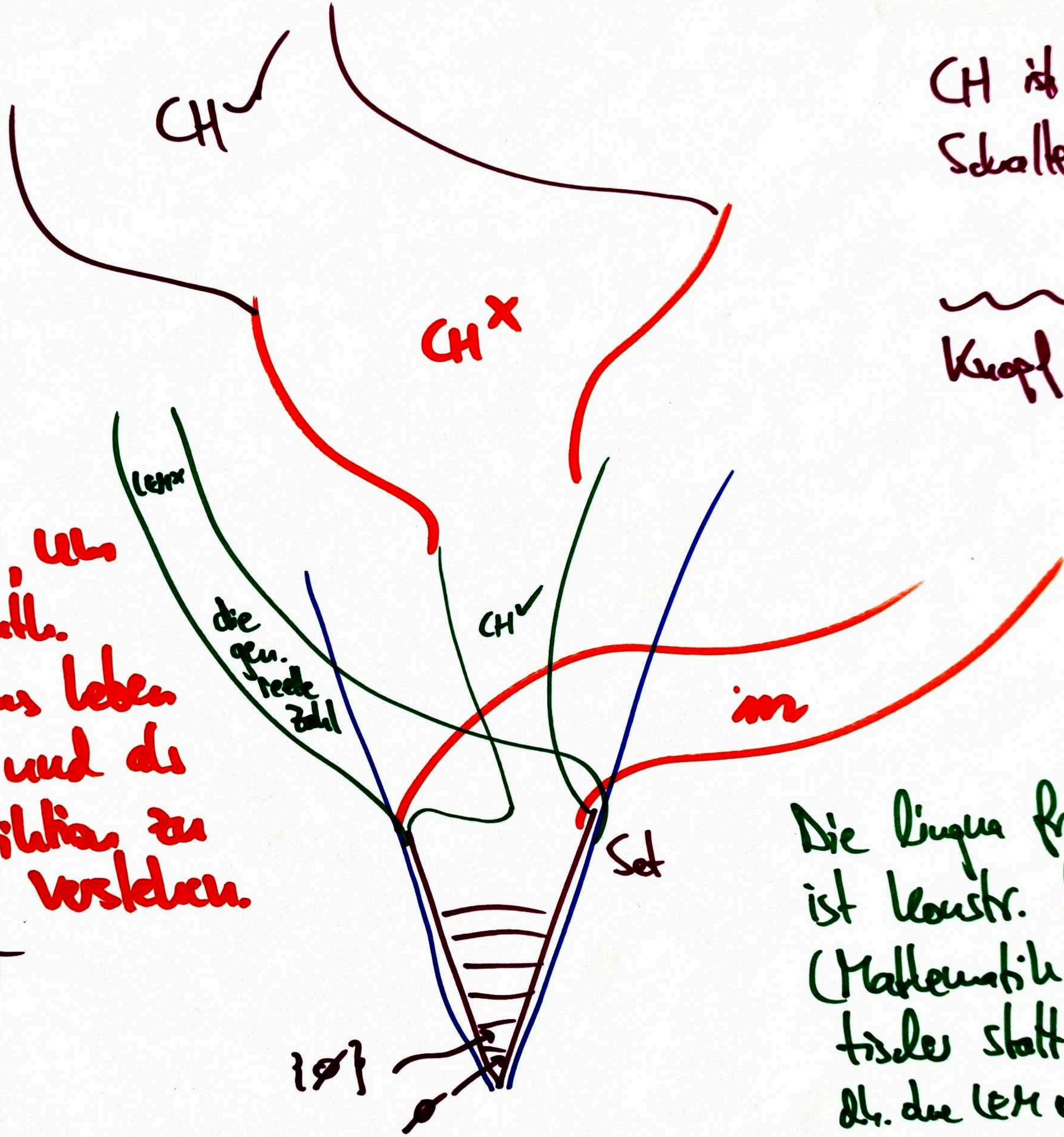
0 1 2
Es gibt eine komplexe Zahl ohne Quadratwurzel
L
AC ✓
AC ✗ LEM ✗

Der effektive Topos Eff

0 1 2 Set AC ✓ glatte Topos
Jede Fkt. $\mathbb{N} \to \mathbb{N}$ ist berechenbar.
AC ✗
LEM ✗

CH ist ein sog. Schalter (engl. switch).

$\sim$ ist ein Knopf (engl. button).



Topostheorie, um gewisse math. Phantome ins Leben zu holen und die wirkliche Fiktion zu verstehen.

$$\int_{-\infty}^{\infty} \frac{1}{x^2+1}\,dx = \pi$$

Die lingua franca aller Topoi ist konstr. Mathematik (Mathematik mit intuitionistischer statt klassischer Logik, d.h. ohne LEM und ohne AC).

③

Ein Körper ist ein Ring mit $1 \neq 0$ und

(a) $\forall x.\ x = 0 \lor x$ ist invertierbar.

(b) $\forall x.\ x \neq 0 \Rightarrow x$ ist invertierbar.

(c) $\forall x.\ x$ nicht inv. $\Rightarrow x = 0.$

(d) Es gibt genau zwei Ideale.

in diesem Sinn ist $\mathbb{R}$ ein Körper (auch ohne LEM und ohne AC)

Prop: Es gibt irrationale Zahlen x, y mit $x^y \in \mathbb{Q}$.

Bew: Es ist $\sqrt{2}^{\sqrt{2}}$ rational oder irrational.

(unkonstruktiv) Im ersten Fall, fertig mit $x = y = \sqrt{2}$.

Im zweiten Fall, fertig mit $x = \sqrt{2}^{\sqrt{2}}$, $y = \sqrt{2}$, denn $x^y = \sqrt{2}^2 = 2$.

Bew: $x = \sqrt{2}$, $y = \underbrace{\log_{\sqrt{2}}(3)}$. Denn $x^y = 3$.

(konstruktiv)

← irrational, denn: Angenommen $\log_{\sqrt{2}} 3 = \frac{a}{b}$ mit $a, b \in \mathbb{N}$ und $b \neq 0$

$$\Rightarrow \quad 3 = (\sqrt{2})^{a/b}$$

$$\Rightarrow \quad 3^b = (\sqrt{2})^a$$

$$\Rightarrow \quad 3^b \cdot 3^b = 2^a$$

↯ zur Eindeutigkeit der Primfaktorzerlegung

Prop: Nach jeder bel. gegebenen natürlichen Zahl n folgt eine Primzahl $p > n$.

Bew: Jeder Primfaktor von $n!+1$ tut's.

(konstruktiv)

Bsp: $n = 4$, $1 \cdot 2 \cdot 3 \cdot 4 + 1 = 25 = \underline{5} \cdot 5$

Prop: Jede Fkt. $f: \mathbb{N} \to \mathbb{N}$ ist gut in dem Sinn, dass $\exists n \in \mathbb{N}: f(n) \leq f(n+1)$.

Bew: Die Fkt. f nimmt ein Minimum an, $f(n)$. Dann sicherlich $f(n) \leq f(n+1)$.

Beh.: A

Bew.: Angenommen nicht.
Dann ....
Also $\lightning$
~~[illegible]~~ A.

Widerspruchsbeweis
(unkonstruktiv)

dieser Beweis zeigt zunächst
nur $\neg\neg A$.
Mit LEM folgt daraus A.

Beh.: $\neg B$.

Bew.: Angenommen doch, d.h.
angenommen B.
Dann ....,
also $\lightning$.

Beweis einer Negation
(konstruktiv)

Def.: $\neg B \equiv (B \Rightarrow \lightning)$

Def.: $\mathrm{LEM} \equiv (A \vee \neg A)$
$\mathrm{DNE} \equiv (\neg\neg A \Rightarrow A)$

Prop.: LEM für alle Aussagen A
$\Longleftrightarrow$ DNE für alle Aussagen A.

Bsp.: $\underbrace{\exists x.\ \text{der Schlüssel liegt an Stelle } x}_{\text{konstruktiv nicht verteidigbar}}$ vs. $\underbrace{\neg\neg\exists x.\ \text{der Schlüssel liegt an Stelle } x}_{\text{konstruktiv verteidigbar}}$

Bem.: Auch konstruktiv gilt $A \Rightarrow \neg\neg A$.

Bsp.: $\neg(\neg A \wedge \neg B) \Rightarrow A \vee B$ lässt sich nicht konstr. verteidigen.

Def.: Eine Menge X ist genau dann *bewohnt*, wenn $\exists x \in X$.

Bem.: X bewohnt $\Rightarrow \neg(X = \emptyset) \Longleftrightarrow \neg\neg\exists x \in X$

Prop.: Jede bewohnte Menge von nat. Zahlen hat ein Minimum.

Prop.: Wenn jede bewohnte Menge von nat. Zahlen ein Minimum enthalten sollte, dann LEM.

Bew.: Sei eine Aussage A gegeben. Zu zg.: $A \vee \neg A$. Wir betrachten $X := \{1\} \cup \{n \in \mathbb{N} \mid n = 0 \wedge A\}$. Nach Vor. ex. ein Minimum $x \in X$. Nach Lemma auf (7) gilt $\underbrace{x = 0}_{\Rightarrow A} \vee \underbrace{x \neq 0}_{\Rightarrow \neg A}$.

Lemma: $\forall x \in \mathbb{N}: x = 0 \vee x \neq 0$.

$\boxed{\forall x \in \mathbb{N}.\ x+1 \neq 0}$ ein Axiom von PA

Beweis: ☺ Beweis durch Induktion über x:

IA $x=0$: ✓ $(A \Rightarrow A \vee B$ ✓$)$

IS $n \to n+1$: Nach Axiom ist $n+1 \neq 0$, also insb. $n+1 = 0 \vee n+1 \neq 0$.

Prop: ☺ Sei X eine beschränkte Menge von nat. Zahlen. Dann:

(a) ~~X enthält~~ Es ist nicht nicht der Fall, dass X ein Min. enthält.

(b) Falls X in $\mathbb{N}$ herauslösbar ist, dann hat X ein Min.

d.h. $\forall x \in \mathbb{N}: x \in X \vee x \notin X$

Bem:
1. Falls jeder endl.-erz. VR eine Basis hat, dann LEM. } für Körper def. (3)(c)
2. Jeder endl.-erz. VR hat nicht nicht eine Basis.

Bem: ~~Es~~ Konstruktiv lässt sich nicht zeigen, dass symm. Matrizen Eigenvektoren haben

$\Uparrow$

Eigenvektoren von symm. Matrizen hängen nicht stetig von den Matrixeinträgen ab

Bem: Konstr. lässt sich zeigen, dass jede symm. Matrix nicht nicht einen EV hat

$\Downarrow$

Eigenvektoren von symm. Matrizen hängen auf einer dichten offenen Teilmenge stetig von den Einträgen ab

8

Thm: (Barr) Wenn man mit LEM A beweisen kann, dann kann man auch ohne LEM $\underbrace{A^{\neg\neg}}$ beweisen

↑ die Doppelnegationsübersetzung von A ($\neg\neg$ einfügen vor jedem $\exists\vee=$)

$\exists x \ldots \rightsquigarrow \neg\neg\exists x\ldots$

$\ldots\vee\ldots \rightsquigarrow \neg\neg(\ldots\vee\ldots)$

$\ldots=\ldots \rightsquigarrow \neg\neg(\ldots=\ldots)$

Fazit: In konstr. Mathematik können wir feinere Unterschiede sehen; sind wir nicht an diesen interessiert, können wir mit der Doppelnegationsübersetzung alle Beweise, die LEM doch verwenden, konstruktiv nachbauen.

$\neg\neg\neg A \Leftrightarrow \neg A$

Bem: $\neg\neg\neg A \Leftrightarrow \neg\neg A$,

Bsp: :)

Beh: Wenn $A \Rightarrow B$, dann $\neg B \Rightarrow \neg A$.

Bew: Angenommen $\neg B$, zu zg: $\neg A$.
Also ang. A, zu zg: $\cancel{X}\ \bot$
Wegen A und $A \Rightarrow B$, folgt B.
Wegen $\neg B$ folgt $\bot$.

Beh: $\neg\neg\neg A \Rightarrow \neg A$.

Bew: Schon gesehen: $A \Rightarrow \neg\neg A$
Nach der Beh folgt
$\neg\neg\neg A \Rightarrow \neg A$.

Grundlagenkrise in der Mathematik (~1900):

Mit gesundem Menschenverstand kann man $1=0$ zeigen

Nämlich so:

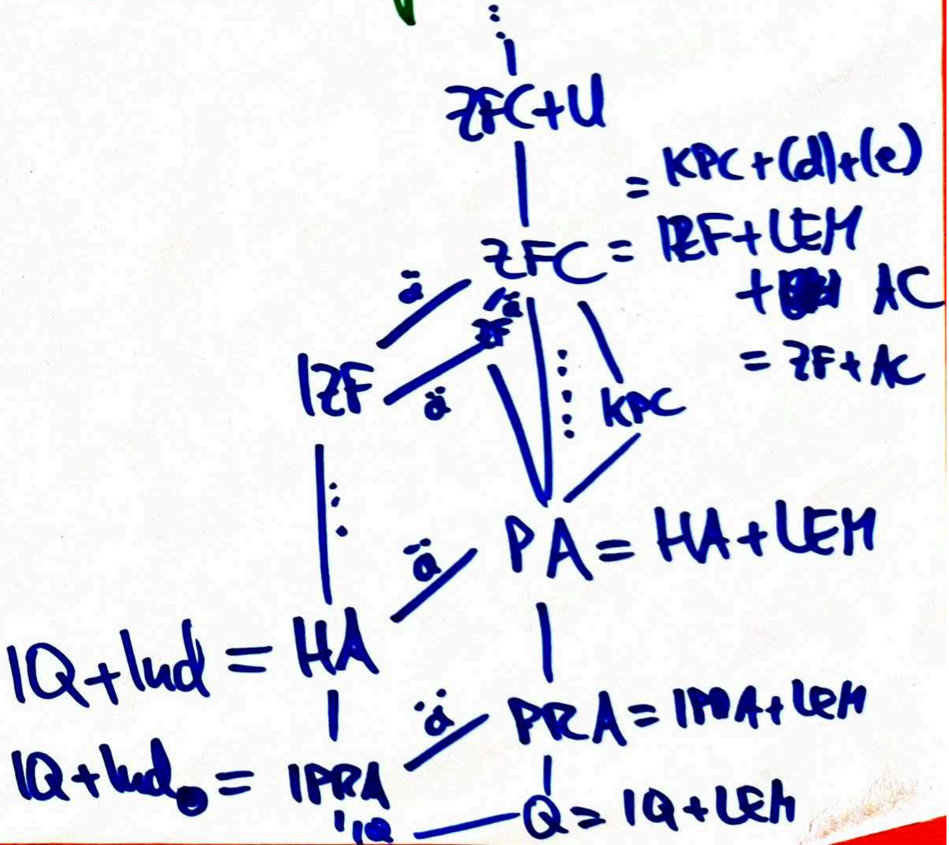
Der gesunde Menschenverstand zeigt, dass es folg. Menge gibt:

X = Menge all derjenigen Mengen K mit der Eig. $K \in K \Rightarrow 1=0$.

Hypothetischer Einschub:
Ang. $X \in X$.
Dann $X \in X \Rightarrow 1=0$.
Folglich $1=0$.

also $X \in X \Rightarrow 1=0$ also $X \in X$ wie dann folgt $1=0$.

(der Beweis ist sogar konstruktiv)



Überwindung der Grundlagenkrise:
Formale Beweise als Goldstandard etablieren.

Ein formales System besteht aus:
1. einer Signatur (z.B. bei ZFC: $\in$)
2. Schlussregeln (z.B. $A \Rightarrow A \vee B$)
3. Axiomen (z.B. $\forall x.\ x+1 \neq 0$)

Axiome von ZFC:

(a) $\exists x.\ \forall y.\ \neg(y \in x)$ „es gibt eine leere Menge"

(b) $\forall a, b.\ ((\forall x.\ x \in a \Leftrightarrow x \in b) \Rightarrow a = b).$ „Extensionalität" (Mengen sind gleich, wenn sie dieselben Elemente haben)

(c) $\forall x.\ \exists y.\ \forall z.\ (z \in y \Leftrightarrow \exists w.\ (z \in w \wedge w \in x))$ „$\bigcup x$ existiert"

($=$ „$\bigcup x$" $=$ „$\{z \mid \exists w.\ z \in w \in x\}$")

(d) $\forall x.\ \exists y.\ \forall z.\ (z \in y \Leftrightarrow \underbrace{\forall a.\ (a \in z \Rightarrow a \in x)}_{\text{„} z \subseteq x \text{"}})$ „$P(x)$ existiert"

(e) $\forall x.\ \exists y.\ \forall a.\ a \in y \Leftrightarrow (a \in x \wedge P(a))$ ← ein Axiomenschema: je ein Axiom für jede ~~Aussage~~ Formel P (die noch freie Var. enthalten darf) insbes. die Var. a, aber nicht die Var. x, y

($=$ „$\{a \in x \mid P(a)\}$") „Aussonderung" (engl. separation)

(f) $(\forall x.\ ((\forall y.\ (y \in x \Rightarrow P(x))) \Rightarrow P(x)))$
$\Longrightarrow (\forall x.\ P(x))$ „Fundierungsaxiom" „$\in$-Induktion"

⋮

$V_0 := \{\} = \emptyset =: 0$

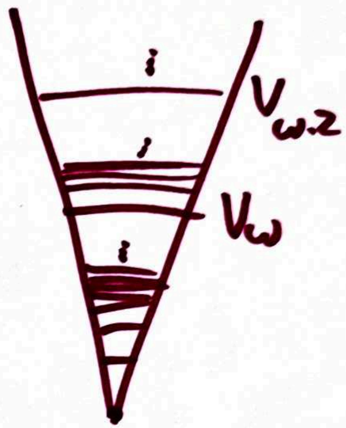
$V_1 := P(V_0) = \{\{\}\} =: 1$

$V_2 := P(V_1) = \{\{\}, \{\{\}\}\} =: 2 = \{0,1\}$

$V_3 := P(V_2) = \{\dots\} \neq 3, \quad 3 := \{0,1,2\}$

$\vdots$

$V_\omega := \bigcup_{n\in\mathbb{N}} V_n$ „die Kumulative Hierarchie"



$V_{\omega+1} := P(V_\omega)$

$V_{\omega+2} := P(V_{\omega+1})$

$\vdots$

Fundiertheits-axiom

$V = \bigcup_\alpha V_\alpha \overset{\text{Fundiertheitsaxiom}}{=}$ die Klasse aller Mengen,

damit ist gemeint: $\forall x. \exists \alpha. x \in V_\alpha$

In Mengenlehre definieren wir +1 wie folgt: (12)

$$n+1 := n \cup \{n\}$$

Bsp: $2+1 = \{0,1\}+1 = \{0, 1, \{0,1\}\} = \{0,1,2\} = 3.$

Signatur von IQ, Q, IPRA, PRA, HA, PA: $0, S, +, \cdot$

S ← Successor (z.B. $S(7)=8$)

Axiome von IQ (= Axiome von Q):

(a) $x+0=x$

(b) $x+S(y) = S(x+y)$

(c) $x \cdot 0 = 0$

(d) $x \cdot S(y) = (x \cdot y) + x$

(e) $\forall x.\ x=0 \vee (\exists y.\ x=S(y))$

(f) ~~...~~ $\forall x.\ S(x) \neq 0$

~~(g) Induktion: $(P(0) \wedge (\forall n.\ P(n) \Rightarrow P(S(n)))) \Rightarrow \forall x.\ P(x)$~~

(h) $\forall x. \forall y. (S(x) = S(y) \Rightarrow x=y)$

Bsp: $1 := S(0)$, $2 := S(1)$.

$$1+1 \overset{\text{Def}}{=} 1+S(0) \overset{(b)}{=} S(1+0) \overset{(a)}{=} S(1) \overset{\text{Def}}{=} 2.$$

Bem: IQ ist <u>nicht</u> mächtig genug, um $\forall x.\ 0+x=x$ zu beweisen

Ind = Induktionsaxiomschema (g) von 12 für bel. Formeln P

Ind_0 = ——— " ——— für sog. Π^1-Aussagen

$\forall \ldots \forall .$ ☺ ← hier keine weiteren $\forall, \exists$

Σ^1-Aussagen: $\exists \ldots \exists .$ ☺

Π^2-Aussagen: $\forall \ldots \forall . \exists \ldots \exists .$ ☺

Σ^2-Aussagen: $\exists \ldots \exists \forall \ldots \forall .$ ☺

Def.: Ein formales System S heißt genau dann <u>inkonsistent</u>, wenn ein S-Beweis von $\bot$ existiert.

Def.: Zwei formale Systeme S, S' sind genau dann <u>äquikonsistent</u>, wenn

$$\mathrm{Incon}(S) \Leftrightarrow \mathrm{Incon}(S').$$

Schlussregeln von intuitionistischer Logik:

$\vdash$ „turnstile"
„bedingt"

(14)

$$\frac{}{A \vdash_{\vec{x}} A} \qquad (\vec{x} = x_1, \dots, x_n)$$

$$\frac{A \vdash_{\vec{x}} B \qquad A \vdash_{\vec{x}} C}{A \vdash_{\vec{x}} B \wedge C}\ \wedge I$$

$$\frac{}{A \vdash_{\vec{x}} \top}\ \top I$$

$$\frac{}{A \wedge B \vdash_{\vec{x}} A}\ \wedge E_1 \qquad \frac{}{A \wedge B \vdash_{\vec{x}} B}\ \wedge E_2$$

$$\frac{}{\bot \vdash_{\vec{x}} A}\ \bot E$$

„ex falsum quodlibet"

$$\frac{}{A \vdash_{\vec{x}} A \vee B}\ \vee I_1$$

$$\frac{}{B \vdash_{\vec{x}} A \vee B}\ \vee I_2$$

$$\frac{A \vdash_{\vec{x}} C \qquad B \vdash_{\vec{x}} C}{A \vee B \vdash_{\vec{x}} C}\ \vee E$$

$$\cancel{\frac{A}{A}}$$

$$\frac{(A \wedge B) \vdash_{\vec{x}} C}{\overline{A \vdash_{\vec{x}} (B \Rightarrow C)}}$$

$$\frac{A \vdash_{\vec{x}} B \qquad B \vdash_{\vec{x}} C}{A \vdash_{\vec{x}} C}\ \mathrm{Cut}$$

$$\frac{A \vdash_{\vec{y},x} B}{\overline{A \vdash_{\vec{y}} (\forall x.\, B)}}\ \text{(in } A \text{ kein } x\text{)}$$

$$\frac{A \vdash_{\vec{y},x} B}{\overline{(\exists x.\, A) \vdash_{\vec{y}} B}}\ \text{(in } B \text{ kein } x\text{)}$$

$$\frac{}{\top \vdash_x x = x}$$

$$\frac{}{(\underbrace{\vec{x} = \vec{y}}_{x_1 = y_1 \wedge x_2 = y_2 \wedge \dots \wedge x_n = y_n} \wedge A) \vdash_{\vec{x},\vec{y}} \underbrace{A[\vec{y}/\vec{x}]}_{\text{dieselbe Formel wie } A,\text{ aber alle } y_i \text{ durch } x_i \text{ ersetzt}}}$$

$$\frac{A \vdash_{\vec{x}} B}{A[\vec{x}/\vec{s}] \vdash_{\vec{y}} B[\vec{x}/\vec{s}]}$$

für Terme $\vec{s}$ im neuen Kontext $\vec{y}$

Zusatzschlussregel von klass. Logik: $\frac{}{\top \vdash A \vee (\neg A)}$ LEM

$\exists + f' + \forall$

mit „$A\Rightarrow\bot$" statt „B"

$$\dfrac{\dfrac{}{A\wedge(A\Rightarrow\bot)\vdash(A\Rightarrow\bot)\wedge A} \qquad \dfrac{\dfrac{}{(A\Rightarrow\bot)\vdash(A\Rightarrow\bot)}}{((A\Rightarrow\bot)\wedge A)\vdash\bot}}{\dfrac{A\wedge(A\Rightarrow\bot)\vdash\bot}{A\vdash\underbrace{\neg\neg A}_{(A\Rightarrow\bot)\Rightarrow\bot}}}$$

$$\dfrac{\dfrac{}{T\wedge(A\wedge B)\vdash A\wedge B}\,{\scriptstyle\wedge E_2} \qquad \dfrac{\dfrac{}{A\wedge B\vdash B}\,{\scriptstyle\wedge E_2} \quad \dfrac{}{A\wedge B\vdash A}\,{\scriptstyle\wedge E_1}}{A\wedge B\vdash B\wedge A}\,{\scriptstyle\wedge I}}{\dfrac{(T\wedge(A\wedge B))\vdash(B\wedge A)}{T\vdash(A\wedge B)\Rightarrow(B\wedge A)}}\,{\scriptstyle Cut}$$

$$\dfrac{\dfrac{}{A\vdash B\vee A}\,{\scriptstyle\vee I_2} \qquad \dfrac{}{B\vdash B\vee A}\,{\scriptstyle\vee I_1}}{A\vee B\vdash B\vee A}\,{\scriptstyle\vee E}$$

$A\wedge(B\wedge C)\vdash(A\wedge B)\wedge C$

$((A\Rightarrow B)\wedge(B\Rightarrow C))\vdash(A\Rightarrow C)$

$((A\wedge B)\Rightarrow C)\vdash(A\Rightarrow(B\Rightarrow C))$

$A\wedge A\vdash A$

$A\wedge(B\vee C)\vdash(A\wedge B)\vee(A\wedge C)$

$(A\Rightarrow B)\vdash(\neg B\Rightarrow\neg A)$

$A\vdash_{\vec{y},x}\exists x.A$

$x=y\vdash_{x,y}y=x$

$\exists x.(A\wedge B)\vdash_{\vec{y}}A\wedge(\exists x.B)$ (wobei kein x in A)

Thm.: (Gödel I) Sei S ein rekursiv axiomatisierbares System, das IQ umfasst. 16
(IPRA) Dann gibt es eine Aussage G mit:
¿ (a) Falls S G beweist, dann ist S inkonsistent.

z.B. IQ, PA, ZFC, $ZFC + \Psi$, ...

(b) Falls S $\neg G$ beweist, ——— " ———.

(IPRA)
Thm.: (Gödel II) Sei S ein rek. ax. System, das IQ umfasst und die HBL-Bedingungen
¡ erfüllt. Dann:
Sollte S seine Konsistenz beweisen, so ist S inkonsistent.

~~Thm.~~ Bsp.: ZFC beweist die Konsistenz von PA.

~~**Bsp.:** ZFC + Con(ZFC) ist konsistent, falls ZFC konsistent ist.~~

Bsp.: $\underbrace{ZFC + Incon(ZFC)}_{\text{ein selbst-hassendes Axiomensystem}}$ ist äquikonsistent zu ZFC.

Def.: $(\neg A) \equiv (A \Rightarrow \bot)$

Angenommen, $ZFC + Incon(ZFC)$ beweist $\bot$.
Dann beweist ZFC, dass $\underbrace{Incon(ZFC) \Rightarrow \bot}_{Con(ZFC)}$.
Mit Gödel II folgt, dass ZFC inkonsistent ist.

Def.: ~~Thm~~ $Prov_S(A)$ $:\Leftrightarrow$ S beweist A $:\Leftrightarrow$ es existiert ein S-Beweis von A.

Thm: (Löb) „Es lohnt sich, an sich zu glauben."
(IPRA) :)

Sei S ein rek. ax. System, das IQ umfasst und die HBL-Bed. erfüllt. Sei A eine Aussage.

Dann gilt:

Falls S $Prov_S(A) \Rightarrow A$ beweist, so beweist S schon A.

Kurz: $Prov_S(Prov_S(A) \Rightarrow A) \Rightarrow Prov_S(A)$.

Bem: Jedes formale System, das die Vor. von Gödel II erfüllt und konsistent ist, misstraut sich.
(ist u.a. agnostisch zur Frage, ob es konsistent ist)

Bsp: ~~Beweis~~ Angenommen, ein System S wie in Löb beweist $\neg Prov_S(A)$.
Dann beweist S $Prov_S(A) \Rightarrow A$. (mit ex falso quod libet) A

aus dieser Annahme folgt insbesondere, dass S $Con(S)$ beweist

Mit Löb folgt, dass S A beweist.
Überrascht nicht, da mit Gödel II S sowieso als inkonsistent entlarvt wird.

Thm: (IPRA) :) Falls PA eine Π^2-Aussage A zeigt, so zeigt auch HA diese.

Def.: Eine Aussage ist genau dann <u>wahr</u>, wenn sie im intendierten Modell stimmt.

Def.: Ein <u>Modell</u> eines formalen Systems S besteht aus

- einer Menge X und
- Funktionen für jedes Funktionssymbol von S sowie Relationen für jedes Relationssymbol von S,

sodass die Axiome von S X-relativiert gelten.

Bsp.: $\mathbb{N}$ ist ein Modell von HA.

← Signatur: $0, S, +, \cdot$

← zusammen mit folg. Funktionen:

$S : \mathbb{N} \to \mathbb{N},\ x \mapsto x+1$

$+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N},\ (x,y) \mapsto x+y$

$\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N},\ (x,y) \mapsto x \cdot y$

$0 \in \mathbb{N}$

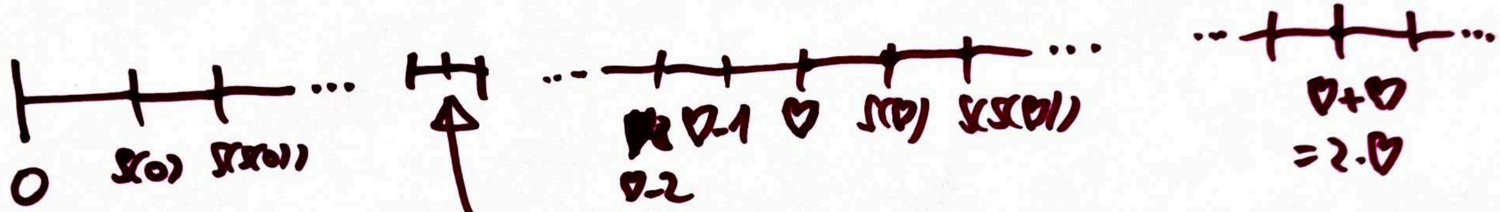
z.B. das Axiom „$\forall x.\ x+0=x$" gilt tatsächlich $\mathbb{N}$-relativiert, denn

$$\forall x \in \mathbb{N}.\ x+0=x. \checkmark$$

Bsp.: Ein Modell von ZFC ist gegeben durch die Gesamtheit aller Mengen (wie sie vielleicht im platonischen Ideenhimmel existieren).

Bsp.: Ein weiteres Modell von HA ist $X := \{2n \mid n \in \mathbb{N}\} = \{0, 2, 4, \ldots\}$ zus. mit $0 \in X$, $S(x) = x+2$, $+$ wie gehabt, $\cdot$ durch gewöhnliche Mult. gefolgt von „$\div 2$".

Bsp.: Sei M ein Modell von HA, das ein Element $\heartsuit \in M$ enthält, welches nicht von der Form $S(S(S(\dots(0))))$ ist.



ein Gödel-Geist

entweder $\frac{\heartsuit}{2}$ oder $\frac{S(\heartsuit)}{2}$ (je nachdem, welche Zahl gerade ist)

$$\frac{\heartsuit}{2} + 1 = \heartsuit \pm n$$
$$\Rightarrow \heartsuit + 2 = 2\heartsuit \pm 2n$$
$$\Rightarrow 2 = \heartsuit \pm 2n$$
$$\Rightarrow \heartsuit = 2 \mp 2n \in \mathbb{N} \ ↯$$

Thm. (Gödels Vollständigkeitssatz)
Jedes konsistente formale System hat ein Modell.

Bem.: Hat ein formales System ein Modell, so ist es konsistent.

Bsp.: Das selbsthassende System $PA + \mathrm{Incon}(PA)$ ist konsistent und hat daher ein Modell,* ein sog. selbsthassendes Modell.
In einem solchen Modell gibt es ein Element $\heartsuit \in M$, sodass M glaubt, dass $\heartsuit$ die Kodierung eines PA-Beweises von $\bot$ ist.
Dieser Beweis hat, wie jeder Beweis, eine gewisse Länge $l \in M$.
Aber l kann nicht von der Form $S(S(\dots(0)))$ sein.

Wie die Liste [10, 30, 5] als einzelne nat. Zahl kodieren?
$$2^{10} \cdot 3^{30} \cdot 5^{5}$$

Bem.: Die Aussage „$\forall x.\ x = \underbrace{S(S(\dots(0)))}_{\text{endlich oft}}$" lässt sich nicht mit den sprachlichen Mitteln von PA ausdrücken.

$x \leq y :\Leftrightarrow \exists z.\ x + z = y$

Bsp.: $X = \{0, 1, 2, \ldots, \heartsuit\}$ ist kein Modell von HA.

zus. mit $0 \in X$, $S : X \to X$, $+ : X \times X \to X$, $\cdot : X \times X \to X$
$\ldots$ $\ldots$

$$\begin{aligned} 0 &\mapsto 1 \\ 1 &\mapsto 2 \\ &\vdots \\ \heartsuit &\mapsto \heartsuit \end{aligned}$$

Def.: „$S \vdash A$" heißt: Es gibt einen S-Beweis der Sequenz $\top \vdash A$.

Prop.: Sei S ein formales System. Sei A eine Formel. Dann gilt:

$$S \vdash A \iff A \text{ gilt in allen Modellen von } S.$$

mit LEM

$$\cancel{\Uparrow} \; \Downarrow$$

A ist wahr

Bew.: „$\Leftarrow$": Angenommen, $\neg(S \vdash A)$.
Dann ist das formale System $S + (\neg A)$ konsistent, denn angenommen $(S + (\neg A)) \vdash \bot$.
Dann $S \vdash \neg\neg A$.
Somit $S \vdash A$ ↯
Nach Gödels Vollständigkeitssatz hat dieses System ein Modell.
In diesem gilt $\neg A$. ↯

Bsp.: (universelle Maschine)

Wir betrachten die folgende Maschine M:

Gehe auf systematische Art und Weise alle PA-Beweise durch.
Sollte dabei ein PA-Beweis einer Behauptung der Form

„Die Maschine M hält nicht mit Ausgabe $\boxed{\underline{n}}$"

auftreten, so halte an mit Ausgabe n.

$\underline{n} := \underbrace{S(S(\dots(0))}_{n \text{ viele } S\text{e}}$

Wenn M anhalten würde, so wäre PA inkonsistent.

Allerdings: Das System $PA_x := PA + \underbrace{\text{„M hält an mit Ausgabe } \underline{x}\text{"}}_{A_x}$ ist, für jedes $x \in \mathbb{N}$, konsistent, denn:

Angenommen $PA_x \vdash \bot$.
Dann $PA \vdash (A_x \Rightarrow \bot)$, d.h. $PA \vdash \neg A_x$, d.h. $PA \vdash$ „M hält an".
Da alle Theoreme von PA auch wahr sind, hält M an.
Folglich ist PA inkonsistent. ↯

Nach Gödels Vollständigkeitssatz gibt es ein Modell X_x von PA_x.
In diesem Modell gilt: „M hält an mit Ausgabe $\underline{x}$."

Lemma: (Diagonallemma) :-)

Sei $A(n)$ eine Formel mit freier Variable n.
Dann gibt es eine Formel B mit:

$$IQ \vdash (B \Leftrightarrow A(\underline{\ulcorner B \urcorner})).$$

$\ulcorner B \urcorner$ ist die Gödelnummer von B

Bew. von Gödel I:

Sei also S ein rek. ax. System, das IQ umfasst.
Mit dem Diagonallemma gibt es eine Aussage G mit

$$S \vdash (G \Leftrightarrow \neg \mathrm{Prov}_S(\underline{\ulcorner G \urcorner})).$$

„Ich bin unbeweisbar (für S)."

Zu zg.: $(S \vdash G) \Rightarrow (S \vdash \bot)$.

Angenommen, $S \vdash G$.
Dann auch $S \vdash \neg \mathrm{Prov}_S(\underline{\ulcorner G \urcorner})$.
Da $S \vdash G$, gilt auch: $\underbrace{S \vdash \mathrm{Prov}_S(\underline{\ulcorner G \urcorner})}_{S \vdash „S \vdash G"}$.
Also $S \vdash \bot$.

Zu zg.: $(S \vdash (\neg G)) \Rightarrow (S \vdash \bot)$.

Ang. $S \vdash (\neg G)$. Dann $S \vdash \neg\neg \mathrm{Prov}_S(\underline{\ulcorner G \urcorner})$.
Wenn wir postulieren, dass S nur Wahrheiten beweist, folgt $\neg\neg \mathrm{Prov}_S(\ulcorner G \urcorner)$. ↯ zu $(S \vdash G) \Rightarrow \underline{(S \vdash \bot)}$

ohne diese Zusatz-Vor. geht's mit Rossers Trick

$$\boxed{(S \vdash A) \Rightarrow (IQ \vdash „S \vdash A")}$$

$$\boxed{S \vdash ((A \wedge \neg A) \Rightarrow \bot)}$$

Bew. von Gödel II:

Sei S ein rek. ax. System, das IQ umfasst und die HBL-Bed. erfüllt. Gelte $S \vdash Con(S)$. Z. zg.: $S \vdash \bot$.

Sei G der Gödelsatz aus Gödel I.

Dann gilt: $Con(S) \Rightarrow \neg Prov_S(G)$.

Diese Folgerung kann S nachvollziehen: $S \vdash (Con(S) \Rightarrow \neg Prov_S(G))$.

Somit $S \vdash \neg Prov_S(G)$.

Nach der Konstruktion von G folgt $S \vdash G$.

Mit Gödel I folgt $S \vdash \bot$.

Bew. von Löb:

s. Comic-Beweis

Bsp.: Sei ~~g~~ g Grahams Zahl (oder eine andere große Zahl).
Dann gibt es eine Aussage, die PA beweisen kann, aber nicht in unter ~~g vielen~~ Länge g. (Aber die Aussage selbst ist kurz.)

Denn nach dem Diagonallemma gibt es eine Aussage P mit

$$PA \vdash (P \Leftrightarrow \forall x \leq g : \neg \underbrace{\mathrm{Proof}_{PA}(x, \ulcorner \underline{P} \urcorner)}_{\text{d.h. } x \text{ ist eine Kodierung eines PA-Beweises von } P})$$

(P besagt: „Ich bin nicht unter Länge g beweisbar.")

Beh.: P ist für PA nicht unter Länge g beweisbar.

Bew.: Ang. doch, d.h. es gibt ein $x \leq g$ mit $\mathrm{Proof}_{PA}(x, \ulcorner P \urcorner)$ $\quad \mathrm{Prov}_S(P) \Leftrightarrow \exists x.\ \mathrm{Proof}_S(x, P)$
PA kann diesen Umstand nachvollziehen,
d.h. $PA \vdash \mathrm{Proof}_{PA}(\underline{x}, \ulcorner \underline{P} \urcorner)$.
Auf der anderen Seite $PA \vdash P$, also $PA \vdash \forall y \leq g. \neg \mathrm{Proof}(y, \ulcorner \underline{P} \urcorner)$.
Da $PA \vdash \underline{x} \leq g$, folgt $PA \vdash \bot$. ↯ zur Konsistenz von PA

Auf der anderen Seite gilt $PA \vdash P$ (und daher ist P auch wahr)
Dieses Argument kann formalisiert werden zu einem kurzen PA-Beweis von der Aussage $\mathrm{Con}(PA) \Rightarrow P$.

Bem.: Folgende Systeme zeigen die Konsistenz von PA
(oder auch von HA, denn schon IPRA zeigt die Äquikonsistenz von HA und PA):

- ZFC } durch Angabe eines Modells von PA, nämlich $\mathbb{N}$
- ZF
- IZF } durch Angabe eines Modells von HA, nämlich $\mathbb{N}$
- ~~PA~~ [außer PA ist inkonsistent]
- $\mathrm{IPRA} + \underbrace{\mathrm{TI}_0(\varepsilon_0)}$ } durch finitären Konsistenzbeweis

← transfinite Induktion für Π^1-Aussagen unter $\varepsilon_0 = \omega^{\omega^{\omega^{\cdots}}}$

$= \mathrm{IZF} + \mathrm{LEM} + \mathrm{AC}$

Bem.: ZFC ist für zahlentheoretische Π^2-Aussagen P konservativ über IZF, d.h.:

$$\mathrm{ZFC} \vdash P \quad \Rightarrow \quad \mathrm{IZF} \vdash P.$$

← $\forall \ldots \forall . \exists \ldots \exists . (\%)$ ← ohne $\forall, \exists$

(IPRA)

LEM und AC sind also, wenn es nur um die Etablierung von zahlenth. Π^2-Aussagen geht, nützliche Fiktionen.

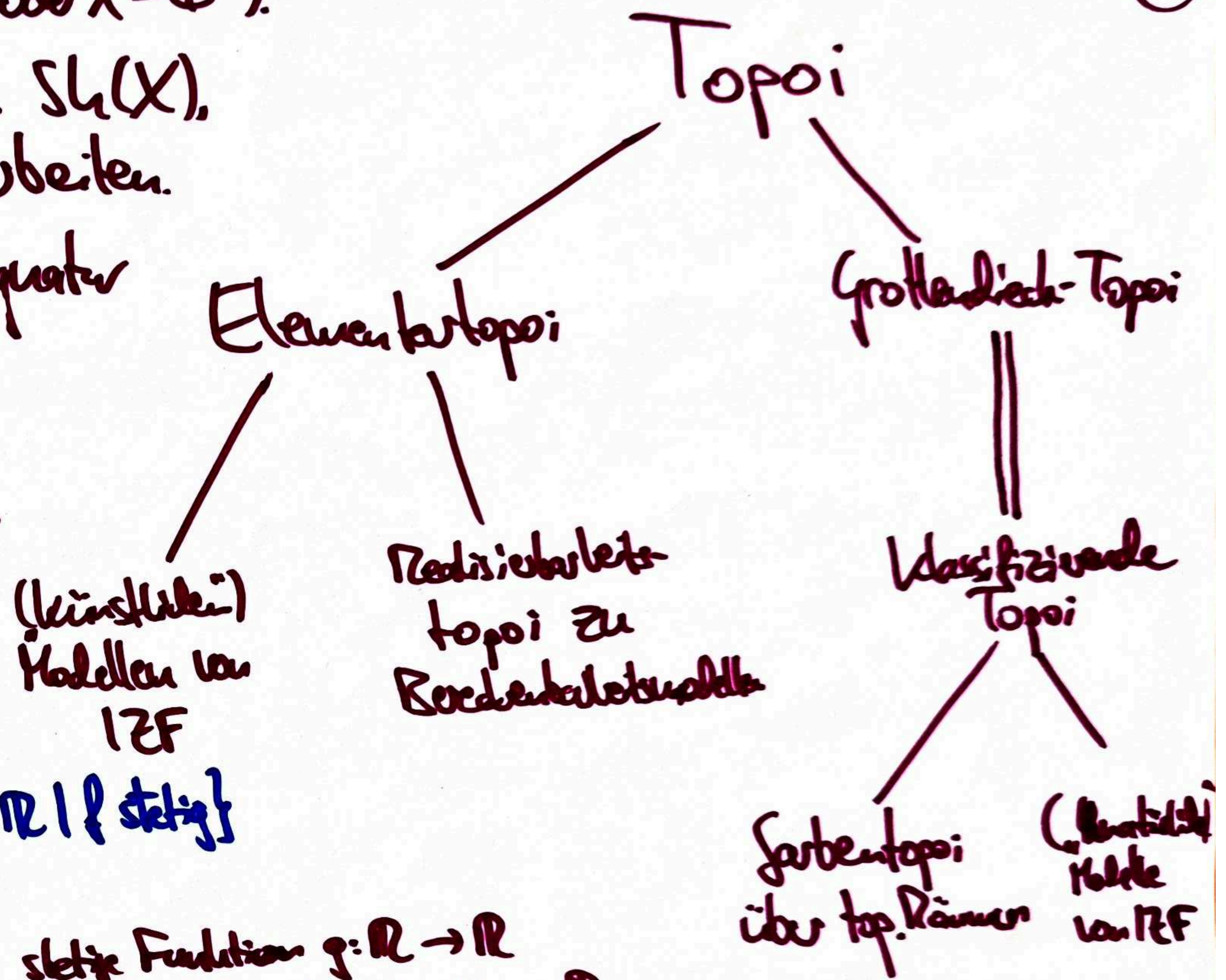
Bem.: Ist ZFC konservativ über PA für zahlenth. Aussagen? Nein! Nicht mal für Π^1-Aussagen:
z.B. $\mathrm{ZFC} \vdash \mathrm{Con}(\mathrm{PA})$, aber $\mathrm{PA} \nvdash \mathrm{Con}(\mathrm{PA})$.

Sei X ein top. Raum (z.B. $X = \mathbb{R}^1$ oder $X = \mathbb{C}^1$).

Dann wollen wir intern im Topos $Sh(X)$, dem Topos der Garben über X arbeiten.

Formeln liegt dabei folgende Signatur zugrunde:

- Sorte $\cancel{\mathbb{R}}$ $\underline{\mathbb{R}}$ der reellen Zahlen
- Sorte $\cancel{\mathbb{N}}$ $\underline{\mathbb{N}}$ der natürlichen Zahlen
- je ein 0-stelliges Funktionssymbol (d.h. je ein Konstantensymbol) für jedes Element von $\underbrace{\Gamma(\underline{\mathbb{R}}, X)}_{=\{f : X \to \mathbb{R} \mid f \text{ stetig}\}}$ und von $\underbrace{\Gamma(\underline{\mathbb{N}}, X)}_{=\{f : X \to \mathbb{N} \mid f \text{ stetig}\}}$
- je ein 1-stelliges Funktionssymbol für jede stetige Funktion $g : \mathbb{R} \to \mathbb{R}$
- je ein 2-stelliges ——— " ——— $h : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$



Was $Sh(X)$ für eine einzelne reelle Zahl hält, ist aus externer Sicht also eine stetige reellwertige Funktion $f : X \to \mathbb{R}$.

$\mathbb{R}$ $\mathbb{N}$ 7 $\sin$

$\boxed{\cancel{\mathbb{R}}\,\underline{\mathbb{R}} \quad \underline{\mathbb{N}} \quad 7 \quad \sin}$ $Sh(X)$

Bem. $Sh(\{\heartsuit\}) \simeq \mathrm{Set}$.

Die externe Interpretation von Formeln von $\mathrm{Sh}(X)$ ergibt sich wie folgt:

$\boxed{\text{Kripke–Joyal-Semantik}}$

- $X \models \top$ gdw. ✓
- $X \models \bot$ gdw. $X = \emptyset$
- $X \models A \wedge B$ gdw. $X \models A$ und $X \models B$
- $X \models A \vee B$ gdw. ~~$X \models A$ oder $X \models B$~~ eine offene Überdeckung $X = \bigcup_{i \in I} U_i$ existiert,
  sodass für alle Indizes $i \in I$ gilt: $U_i \models A|_{U_i}$ oder $U_i \models B|_{U_i}$
- $X \models (A \Rightarrow B)$ gdw. für alle Offenen $U \subseteq X$ gilt: Falls $U \models A|_U$, so $U \models B|_U$
- $X \models \forall s{:}E.\, A(s)$ gdw. für alle Offenen $U \subseteq X$ und alle Elemente $s_0 \in \Gamma(E, U)$ gilt $U \models A|_U(s_0)$.
  ~~für alle Elemente $s_0 \in \Gamma(E, X)$ gilt $X \models A(s_0)$~~
- $X \models \exists s{:}E.\, A(s)$ gdw. ~~ein Element $s_0 \in \Gamma(E, X)$ mit $X \models A(s_0)$ existiert~~
  eine offene Überdeckung $X = \bigcup_{i \in I} U_i$ existiert,
  sodass für alle Indizes $i \in I$ gilt,
  dass ein Element $s_0 \in \Gamma(E, U_i)$ mit $U_i \models A|_{U_i}(s_0)$ existiert.
- $X \models x = y$ gdw. $\underbrace{[\![x]\!]} = \underbrace{[\![y]\!]}$

  Interpretation von den Termen x und y
  (alle vorkommenden Funktionssymbole durch ihre Bedeutung ersetzen)

„Existenz in $\mathrm{Sh}(X)$ ist aus externer Sicht lokale Existenz"

Bsp: [illegible]

$X \models \forall x{:}\mathcal{C}.\ \forall y{:}\mathcal{C}.\ x+y=y+x$

gdw. für alle Offenen $U \subseteq X$ und alle $x_0 \in \Gamma(\mathcal{C}, U)$ gilt: $U \models \forall y{:}\mathcal{C}.\ x_0+y=y+x_0$

gdw. für alle Offenen $V \subseteq U$ und alle $y_0 \in \Gamma(\mathcal{C}, V)$ gilt: $V \models x_0+y_0=y_0+x_0$

Addition von reellen Zahlen

gdw. $x_0|_V + y_0 = y_0 + x_0|_V$

Addition von Funktionen

$$y_0+x_0 : V \longrightarrow \mathbb{R}, \quad p \longmapsto y_0(p)+x_0(p)$$

$$x_0+y_0 : V \longrightarrow \mathbb{R}, \quad p \longmapsto x_0(p)+y_0(p)$$

28 ½

Bsp: Sei $f_0 \in \Gamma(\mathcal{C}, X)$.

$X \models \exists g:\mathcal{C}.\ f_0 \cdot g = 1$

gdw. es eine Überdeckung $X = \bigcup_{i\in I} U_i$ existiert,

sodass für alle $i \in I$ jeweils ein Element $g_0 \in \Gamma(\mathcal{C}, U_i)$

existiert mit $\underbrace{U_i \models f_0|_{U_i} \cdot g_0 = 1.}_{\text{gdw. } f_0|_{U_i} \cdot g_0 = 1}$

(**Bem:** g_0 ist mit dieser Forderung eindt. bestimmt, nämlich $g_0(p) = 1/f_0(p)$.)

gdw. für alle Punkte $p \in X$ gilt: $f_0(p)$ ist in $\mathbb{R}$ invertierbar ($\Leftrightarrow > 0 \vee < 0$)

Bsp: Welche der folgenden Aussagen gelten in $\mathrm{Sh}(X)$?

(a) $\forall x:\mathcal{C}.\ x \text{ inv.} \Rightarrow x \neq 0$

(b) $\forall x:\mathcal{C}.\ x \neq 0 \Rightarrow x \text{ inv.}$

(b') $\forall x:\mathcal{C}.\ \neg(x \text{ inv.}) \Rightarrow x = 0$

(c) $\forall x:\mathcal{C}.\ x = 0 \vee x \text{ inv.}$

(h) $\forall x:\mathcal{C}.\ \neg\neg(x=0) \Rightarrow x = 0$

(i) $\forall x:\mathcal{C}.\ \neg\neg(x \text{ inv.}) \Rightarrow x \text{ inv.}$

$\left.\begin{array}{l}\text{(d) } \exists x:\mathcal{C}.\ e^x = \alpha \\ \text{(e) } \neg\exists x:\mathcal{C}.\ e^x = \alpha \\ \text{(f) } \neg\neg\exists x:\mathcal{C}.\ e^x = \alpha\end{array}\right\}$ im Spezialfall $X = \mathbb{R}$ $\left\{\begin{array}{l}\text{(d') } \exists x:\mathcal{C}.\ e^x = |\alpha| \\ \text{(e') } \neg\exists x:\mathcal{C}.\ e^x = |\alpha| \\ \text{(f') } \neg\neg\exists x:\mathcal{C}.\ e^x = |\alpha|\end{array}\right.$

(g) $\forall x:\mathcal{C}.\ \exists y:\mathcal{C}.\ y^2 = x$

(g') $\forall x:\mathcal{C}.\ \exists y:\mathcal{C}.\ y^2 = |x|$

(j) $\forall x:\mathcal{C}.\ x \geq 0 \vee x < 0$

(k) $\forall x:\mathcal{C}.\ x > 0 \vee x < 1$

Bsp.: Sei $x_0 \in \Gamma(\mathcal{R}, X)$.

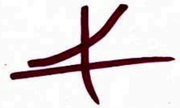
$X \models \underbrace{x_0 \neq 0}_{x_0 = 0 \Rightarrow \bot}$

gdw. für alle Offenen $U \subseteq X$ gilt: Falls $\underbrace{U \models x_0 = 0}_{x_0|_U = 0}$, so $\underbrace{U \models \bot}_{U = \emptyset}$. $\Big\}$ (♡)

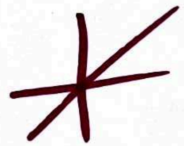
(d.h. $\forall p \in U: x_0(p) = 0$)

Das stimmt z.B. für:

- $X = \mathbb{R}$, ~~x_0~~ $x_0 : X \longrightarrow \mathbb{R}$, $p \longmapsto e^p$



- $X = \mathbb{R}$, $x_0 : X \longrightarrow \mathbb{R}$, $p \longmapsto p$



die generische reelle Zahl α

Bsp.: $X \models \forall x : \mathcal{R}.\ x = 0 \vee x \neq 0$?

$X \models \alpha = 0 \vee \alpha \neq 0$?

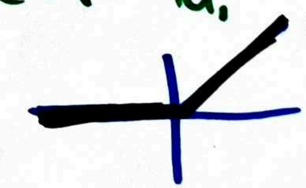
z.B. $X = \mathbb{R}$, $\underbrace{X \models \alpha = 0 \vee \alpha \neq 0}$

gdw. eine offene Überdeckung $X = \bigcup_{i \in I} U_i$ existiert

sodass für alle $i \in I$ gilt:

$\alpha|_{U_i} = 0$ oder (♡) für $\alpha|_{U_i}$

z.B. $X = \mathbb{R}$, $X \models f_0 = 0 \vee f_0 \neq 0$?



f_0

Folgerung: $X \not\models \mathrm{LEM}$.

Bsp.: $X \models \forall x{:}\mathcal{E}.\ (A(x) \Rightarrow B(x))$

gdw. für alle Offenen $U \subseteq X$ und $x_0 \in \Gamma(\mathcal{E}, U)$ gilt, dass
für alle Offenen $V \subseteq U$ gilt, dass
aus $V \models A|_V(x_0|_V)$ folgt, dass $V \models B|_V(x_0|_V)$

gdw. für alle Offenen $W \subseteq X$ und $x_0 \in \Gamma(\mathcal{E}, W)$ gilt, dass
aus $W \models A|_W(x_0)$ folgt, dass $W \models B|_W(x_0)$

Bsp.: $X \models \neg\neg A$
gdw. $[\![A]\!]$:= Wahrheitswert von $A = \bigcup\{U \subseteq X \text{ offen} \mid U \models A\}$ dicht in X liegt
= größte Offene, auf dem A gilt.

Denn: $X \models (A \Rightarrow \bot) \Rightarrow \bot$
gdw. für alle Offenen $U \subseteq X$: falls $\underbrace{U \models (A \Rightarrow \bot)}$, so $U = \emptyset$
gdw. für alle Offenen $W \subseteq U$: falls $\underbrace{W \models A}$, so $W = \emptyset$
gdw. $W \subseteq [\![A]\!]$

gdw. für alle Offenen $U \subseteq X$: falls $U \cap [\![A]\!] = \emptyset$, so $U = \emptyset$
gdw. $[\![A]\!] \subseteq X$ dicht

Def.: $M \subseteq X$ <u>dicht</u>
$:\Longleftrightarrow \forall$ Offenen $V \subseteq X$:
$M \cap V = \emptyset \Rightarrow V = \emptyset$

Bsp.: $\{x \in \mathbb{R} \mid x < 0 \vee x > 0\} \subseteq \mathbb{R}$ dicht.

Auflösung der Fragenliste von (28): (33)

(a) ✓

(b) X Gegenbsp. α

(b') ✓ (liegt an Stetigkeit der Elemente von $\Gamma(\mathcal{C}, U)$)

(c) X Gegenbsp. α

(d) X (d') X

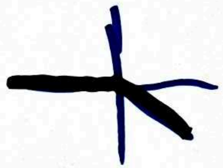
(e) X (e') X

(f) X (f') ✓ $[\![\exists x{:}\mathbb{R}.\ e^x = |x|]\!] = \{p \in \mathbb{R} \mid \overbrace{p<0 \vee p>0}^{\Leftrightarrow:\ p \# 0}\}$

(g) X Gegenbsp. konst. Fkt. -1 (g') ✓ $(y(p) := \sqrt{x(p)})$

(h) ✓ ~~dichte~~ stetige reellwertige Fkt., die auf einer dichten offenen Teilmenge Null sind, sind schon konstant Null

(i) X Gegenbsp. α

(j) X Gegenbsp. 

(k) ✓

$\forall x.\neg A(x)$

$\neg\exists x.\ A(x)$

$\exists x.\neg A(x)$

$\neg\forall x.\ A(x)$

$X \models f_0 \overset{>}{\geq} 0$

gdw. für alle $p \in X$ gilt:

$f_0(p) \underset{>}{\geq} 0$

Thm: AC $\Rightarrow$ LEM. (Satz von Diaconescu, ...)

Def: AC: Für jede Menge X von bewohnten Mengen existiert eine Funktion f, sodass $\forall M \in X:\ f(M) \in M$.

eine Auswahlfunktion für X

Bsp: Eine Auswahlfkt. für X = Menge der Städte ist $f: M \mapsto$ die jüngste Person in M.

Bsp: Sei $X = \{M_1, \ldots, M_n\}$ eine endliche Menge an bewohnten Mengen.

$M_i \neq M_j$ für $i \neq j$

Da M_1 bewohnt, ex. ein Element $x_1 \in M_1$.

$\vdots$

Da M_n bewohnt, ex. ein Element $x_n \in M_n$.

Damit haben wir folg. Auswahlfkt.: $\cancel{i \mapsto x_i}$. $M_i \mapsto x_i$

Bew. Thm: Sei P eine Aussage, zu zeigen: $P \vee (\neg P)$.

Setze $X := \{A, B\}$, wobei
$$A = \{x \in \{0,1\} \mid x = 0 \vee P\}$$ bewohnt durch 0
$$B = \{x \in \{0,1\} \mid x = 1 \vee P\} \subseteq \{0,1\}.$$ bewohnt durch 1

Nach Vor. gibt es eine Auswahlfkt. f: $f(A) \in A$, $f(B) \in B$

Es ist $f(A) = 0 \vee \underbrace{f(A) = 1}_{\Rightarrow 1 \in A \Rightarrow 1 = 0 \vee P \Rightarrow P}$

Es ist $\underbrace{f(B) = 0}_{\Rightarrow P} \vee \underbrace{f(B) = 1}_{\Rightarrow \neg P}$.

(denn falls P, so $A = B$, also $f(A) = f(B)$)

Def: CC: Für jede abzählbare Menge $X = \{M_0, M_1, M_2, \dots\}$ von bewohnten Mengen

countable choice

existiert eine Funktion f mit Definitionsmenge $\mathbb{N}$, sodass $f(n) \in M_n$ für alle $n \in \mathbb{N}$

DC: Sei A eine Menge und $R \subseteq A \times A$ eine Relation.

dependent choice

Gelte $\forall x \in A.\ \exists y \in A: \ (x,y) \in R$. ← d.h. R ist total!

Dann gibt es für jedes Element $x_0 \in A$ eine Funktion $f: \mathbb{N} \to A$ mit $f(0) = x_0$ und $\forall n \in \mathbb{N}: (f(n), f(n+1)) \in R$.

Prop. ~~Bem.~~ $AC \Rightarrow DC \Rightarrow CC$.

Bew.: Gelte AC. Zu zg. DC.

Sei A eine Menge, R eine totale Relation auf A und $x_0 \in A$.

Zu jeder endlichen Liste $[x_0, x_1, \dots, x_n]$ mit $\forall i < n: (x_i, x_{i+1}) \in R$ und $n \in \mathbb{N}$ definieren wir folgende Menge $M_{[x_0,\dots,x_n]} := \{[x_0,\dots,x_n,y] \mid y \in A, (x_n, y) \in R\}$

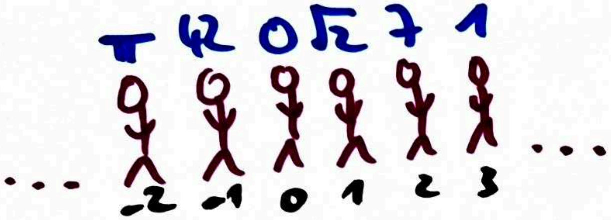
Da R total ist, sind diese Mengen bewohnt.

Nach AC existiert eine Auswahlfunktion g für diese Menge von Mengen.

Dann definieren wir $f: \mathbb{N} \to A$ wie folgt:

$$0 \longmapsto x_0, \quad n+1 \longmapsto \text{letztes Element der Liste } g(M_{[f(0),\dots,f(n)]}).$$

Bsp.:



Menge der Mathematiker:innen. in der Skizze $M = \mathbb{Z}$

Eine <u>Konfiguration</u> ist eine Funktion $f: M \longrightarrow \mathbb{R}$.

Zwei Konfigurationen f, f' heißen <u>äquivalent</u> genau dann, wenn $\{p \in M \mid f(p) \neq f'(p)\}$ endlich ist.

Mit AC existiert eine Abbildung g, die jeder Äquivalenzklasse einen Repräsentanten zuordnet.

Wenn jede Person p als Vermutung für ihre reelle Zahl g(Äquivalenzklasse der sichtbaren Konfiguration)(p), so werden nur endlich viele Personen irren.

Bem: AC entstand durch Extrapolation einer leicht nachweisbaren Tatsache über endliche Mengen ins Unendliche.
Es gibt auch andere solche Prinzipien, wie etwa AD (axiom of determinacy), die teilweise AC widersprechen.
(**Bem:** AD $\Rightarrow$ jede Teilmenge von $\mathbb{R}^n$ ist Lebesgue-messbar $\Longrightarrow \neg$ Banach–Tarski)
Daher ist $ZF + (CC + DC) + AD$ ein schöner Kontext für klassische Analysis.

Bem: AC $\Leftrightarrow$ (Zorn $\wedge$ LEM).

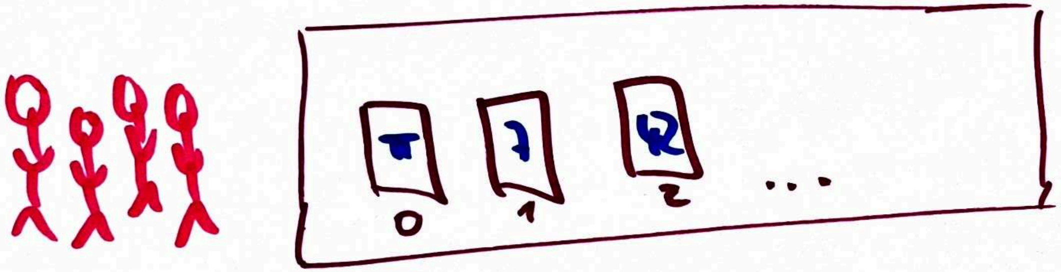
Bem: Gilt Zorn in der Metatheorie, so gilt Zorn auch in allen $Sh(X)$, für bel. top. Räume X.

Bem: (Mindestens) Mit LEM folgt: AC $\Leftrightarrow$ jeder Vektorraum hat eine Basis.

Bem.: Für konkrete Resultate (zahlentheoretische Π^2-Aussagen) ist AC irrelevant, da für solche ZFC über IZF konservativ ist. (und auch LEM)

Bem.: Auch abstrakte Resultate lassen sich mit der „Sprache der punktfreien Topologie" oft so umformulieren, dass sie nicht mehr AC und LEM voraussetzen. Steht AC zur Verfügung, so lassen sich diese Umformulierungen noch länger prokrastinieren.

Bsp.:



Rätsel von David Wärn und Christian Sattler kommuniziert

Agenda:
- Metatheorem über interne Sprache
- Spracherweiterung
- Anwendungen
- Gegenbsp. zu AC und andere Beispiele

(35)

Prop.: (a) Ist $U \subseteq X$ ein Offenes und gilt $X \models A$, so auch $U \models A|_U$. „Monotonie"

(b) Ist $X = \bigcup_{i \in I} U_i$ eine offene Überdeckung und gilt $U_i \models A|_{U_i}$ für alle $i \in I$, so folgt $X \models A$. „Lokalität"

Thm.: Gilt $X \models A$ und zeigt intuitionistische Logik $A \vdash B$, so gilt auch $X \models B$. „Soundness"

Es ist dieses Theorem, welches uns ermöglicht, innerhalb von Topoi mathematisch zu argumentieren

Aus interner Sicht sind $\mathbb{R}$ und $\underline{\mathbb{N}}$ Beispiele für Mengen.

Aus externer Sicht sind $\mathbb{R}$ und $\underline{\mathbb{N}}$ Beispiele für Garben auf X.

Def.: Eine Garbe $\mathcal{E}$ auf X besteht aus

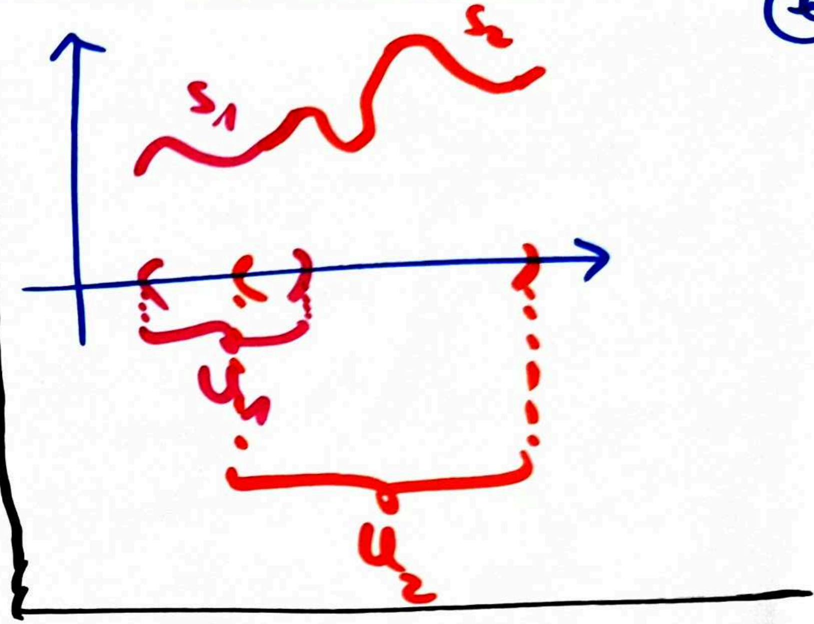
- je einer Menge $\Gamma(\mathcal{E}, U)$ für jedes Offene $U \subseteq X$
- je einer Abbildung $\Gamma(\mathcal{E}, U) \longrightarrow \Gamma(\mathcal{E}, V)$, $s \mapsto s|^U_V$ für $V \overset{\text{off}}{\subseteq} U \overset{\text{off}}{\subseteq} X$,

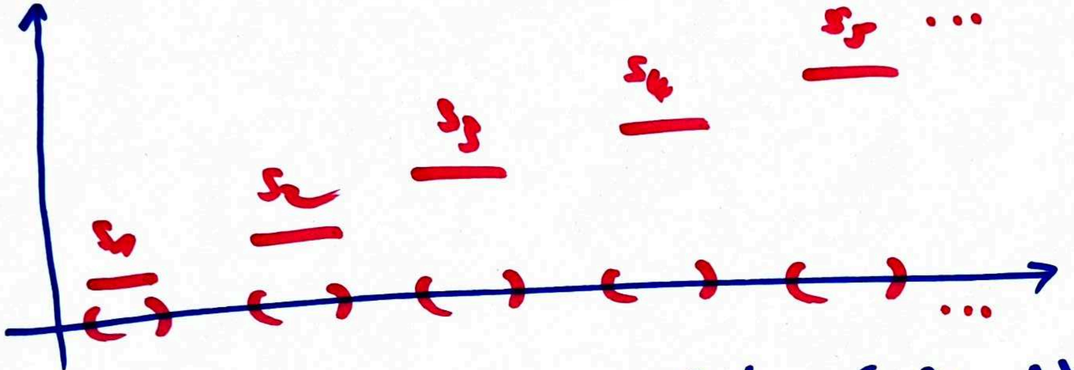
sodass

- $s|^U_U = s$, $\quad (s|^U_V)|^V_W = s|^U_W$ für $W \overset{\text{off}}{\subseteq} V \overset{\text{off}}{\subseteq} U \overset{\text{off}}{\subseteq} X$ „Prägarbenaxiome"
- ist $U = \bigcup_{i \in I} U_i$ eine offene Überdeckung und ist $(s_i)_{i \in I}$ eine Familie von Elementen $s_i \in \Gamma(\mathcal{E}, U_i)$ mit $s_j|^{U_j}_{U_j \cap U_k} = s_k|^{U_k}_{U_j \cap U_k}$ für alle $j, k \in I$, „Verklebeaxiom"

so existiert genau ein Element $s \in \Gamma(\mathcal{E}, U)$ mit $s|^U_{U_i} = s_i$ für alle $i \in I$.

Bsp.: Sei $\Gamma(\mathcal{B}, U) = \{f: U \to \mathbb{R} \mid f \text{ beschränkt}\}$ und $\cdot|^U_V$ wie bei $\mathcal{C}$ (also gewöhnliches Einschränken von Fkt.).
Es ist $\mathcal{B}$ eine Prägarbe, aber keine Garbe.





Def.: Ein <u>Morphismus</u> $\eta: \mathcal{E} \to \mathcal{F}$ <u>von Garben</u> $\mathcal{E}, \mathcal{F}$ auf X besteht aus

- je einer Abbildung $\eta_U: \Gamma(\mathcal{E}, U) \to \Gamma(\mathcal{F}, U)$ für alle Offenen $U \subseteq X$

sodass

- für alle $V \overset{\text{off}}{\subseteq} U \overset{\text{off}}{\subseteq} X$ gilt: $(\eta_U(s))|^U_V = \eta_V(s|^U_V)$ für alle $s \in \Gamma(\mathcal{E}, U)$.

Bsp.: Sei $\mathcal{D}$ die Garbe der stetig differenzierbaren Funktionen auf $X = \mathbb{R}^1$.
Dann ist folg. Familie von Abb. ein Morphismus $\mathcal{D} \to \mathcal{C}$:

$$\eta_U: \Gamma(\mathcal{D}, U) \to \Gamma(\mathcal{C}, U), \quad s \mapsto s' \text{ (Ableitung von } s)$$

Bsp.: Sei „$(f_x)_{x\in X}$ eine stetige Familie stetiger Funktionen" gegeben,

d.h. sei: $f: X \times \mathbb{R} \longrightarrow \mathbb{R}$ stetig.

$$(x,a) \longmapsto f_x(a)$$

(z.B. $X = [-1,1]$, $f_x(a) = \sin(a) + e^{x\cdot a} - x^2$)

~~(z.B. $X = [-1,1]$, $f_x(a) = \begin{cases} \sin(a), & \text{falls } x \leq 0 \\ e^a, & \text{falls } x > 0 \end{cases}$)~~

Dann können wir wie folgt einen Garbenmorphismus $\eta: \mathcal{C} \to \mathcal{C}$ definieren:

$$\eta_U : \underbrace{\Gamma(\mathcal{C},U)}_{=\{s:U\to\mathbb{R} \,\mid\, s \text{ stetig}\}} \longrightarrow \Gamma(\mathcal{C},U)$$

$$s \longmapsto \underbrace{(x \mapsto f_x(s(x)))}_{=\eta_U(s)}$$

Damit können wir die Signatur erweitern:

- je eine Sorte für jede Garbe $\mathcal{E}$ auf X
- je ein 1-ärisches Funktionssymbol für jeden Garbenmorphismus $\mathcal{E} \to \mathcal{F}$
- je ein 2-ärisches Funktionssymbol für jeden Garbenmorphismus $\mathcal{E} \times \mathcal{F} \to \mathcal{G}$
- je ein 0-ärisches Funktionssymbol für jedes Element in $\Gamma(\mathcal{E}, X)$

⋮

Bsp.: Intern haben wir das Funktionssymbol exp zur Verfügung. Es steht für denjenigen Garbenmorphismus, den wir aus dem obigen Bsp. erhalten, wenn wir $f_x(a) = e^a$ setzen.

Bsp.: Sei M eine beliebige Menge.
Dann gibt es die Garbe $\underline{M}$ mit $\Gamma(\underline{M}, U) = \{ f : U \to M \mid f \text{ stetig} \}$.
($\cdot|^U_V$ durch Einschränkung.)

mit diskreter Topologie

$\Leftrightarrow$ f lokal konstant

Bem.: $\underline{M}$ ist eine (winzige) Untergarbe von $\mathcal{C}$.

Ist $A(s)$ eine Formel über X mit freier Variable $s : \mathcal{E}$, so können wir zur Signatur die Sorte $\mathcal{E}'$

$$\{ s : \mathcal{E} \mid A(s) \}$$

hinzufügen. Die Interpretation dieser Sorte ist folgende Untergarbe von $\mathcal{E}$:

$$\Gamma(\mathcal{E}', U) = \{ s_0 \in \Gamma(\mathcal{E}, U) \mid U \models A(s_0|_U) \}.$$

Bsp.: Die Interpretation des internen Ausdrucks „$\{ s : \mathcal{C} \mid s > 0 \}$" ist die Garbe der überall positiven stetigen reellwertigen Funktionen.

Def.: $X \models \bigwedge_{a \in M} A(a)$ genau dann, wenn für alle $a_0 \in M$ gilt: $X \models A(a_0)$

M bel. Menge

$X \models \bigvee_{a \in M} A(a)$ genau dann, wenn eine offene Überdeckung $X = \bigcup_{i \in I} U_i$ existiert, sodass für jedes $i \in I$ ein $a_0 \in M$ mit $U_i \models A|_{U_i}(a_0)$ existiert.

Prop.: $X \models \bigwedge_{a \in M} A(a)$ genau dann, wenn $X \models \forall a : \underline{M}.\ A(a)$.

$\bigvee$ $\qquad\qquad$ $\exists$

Bsp.: In $Sh(X)$ für $X = \mathbb{R}^1$ gibt es ein Gegenbeispiel zu CC.
Zu $n \in \mathbb{N}_{\geq 1}$ definieren wir dazu intern folgende Menge (aus ext. Sicht also eine Garbe):

$$M_n := \{a : \underline{\mathbb{N}} \mid a = 0 \wedge |\alpha| < 1/n\} \cup \{a : \underline{\mathbb{N}} \mid a = 1 \wedge |\alpha| > \tfrac{1}{2n}\}$$

die generische reelle Zahl

Aus interner Sicht sind diese M_n alle bewohnt, denn:

$$\exists a : \underline{\mathbb{N}}.\ a \in M_n$$
$$\Leftrightarrow \exists a : \underline{\mathbb{N}}.\ (a = 0 \wedge |\alpha| < 1/n) \vee (a = 1 \wedge |\alpha| > 1/2n)$$
$$\Leftrightarrow |\alpha| < 1/n \vee |\alpha| > 1/2n$$

Aus externer Sicht haben wir so Garben definiert (Untergarben $\underline{\mathbb{N}}$).
Für Offene $U \subseteq \mathbb{R}^1$ ~~mit $0 \in U$ gilt dabei~~ der Form $(-\varepsilon, \varepsilon)$ gilt dabei:

$$\Gamma(M_n, U) = \emptyset, \quad \text{wenn } n \text{ hinreichend groß ist.}$$

$X \models AC$ würde besagen, dass lokal eine Auswahlfunktion existiert.
Aber auf Offenen, die den Ursprung enthalten, ist das nicht möglich, da es für hinreichend großes n den Garben M_n an Schnitten mangelt.

Fazit: $X \not\models AC$.

Mehr noch: $X \models \neg AC$.

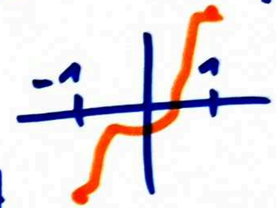
(Garbenmorphismen $\underline{M} \to \mathcal{E}$ stehen in natürlicher Bijektion zu ~~Elementen von~~ Funktionen $M \to \Gamma(\mathcal{E}, X)$.)

Bsp: Für $X = \mathbb{R}^1$ gilt $X \models \neg\, \mathrm{IVT}$.

$\forall f : \mathbb{R} \to \mathbb{R}$ stetig.
$f(-1) < 0 \wedge f(1) > 0 \Rightarrow \exists a : \mathbb{R}.\ f(a) = 0$

Auf der anderen Seite gilt, für alle X:

$X \models \mathrm{IVT}_{\mathrm{sms}}$ ← IVT für streng monoton steigende Fkt.

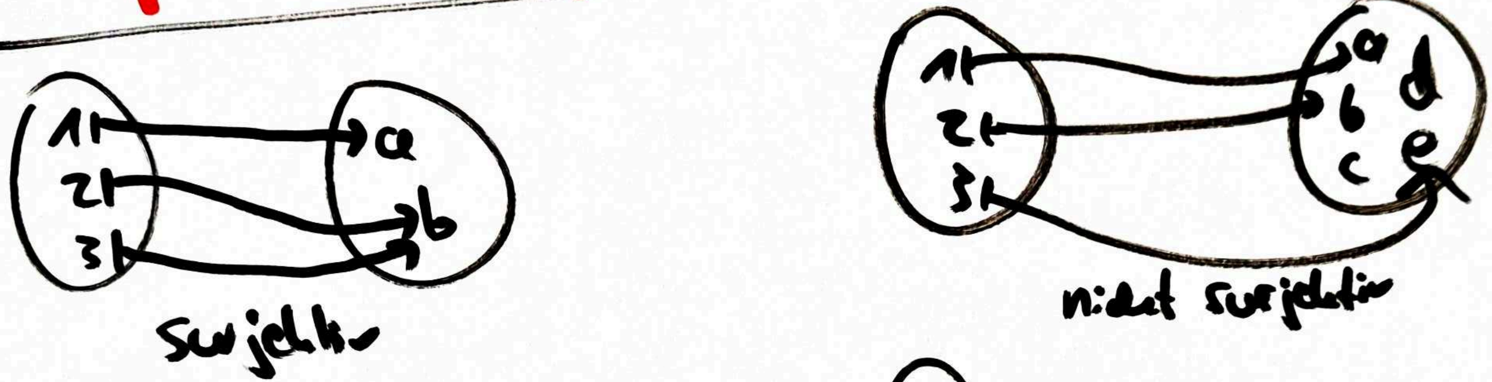


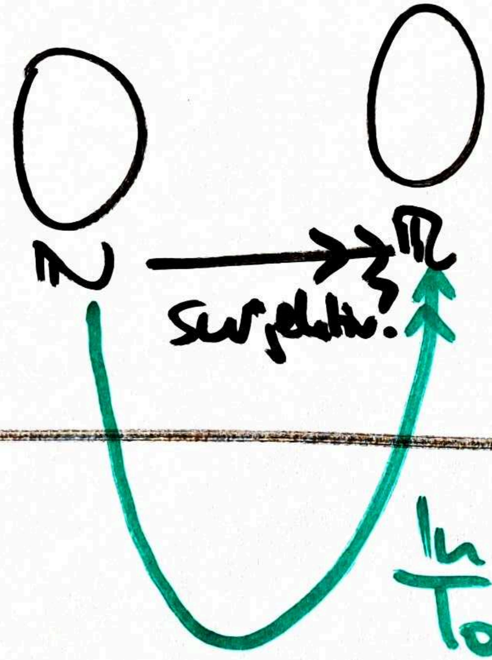
d.h. $a < b \Rightarrow f(a) < f(b)$

Daraus folgt eine nicht ganz uninteressante Beobachtung:

Sei $(f_x)_{x \in X}$ eine stetige Familie stetiger sms Fkt.
Gelte $f_x(-1) < 0$ und $f_x(1) > 0$ für alle $x \in X$.
Dann gibt es nicht nur für jedes $x \in X$ eine Nullstelle a_x von f_x, sondern zusätzlich ist die Abb. $X \to \mathbb{R},\ x \mapsto a_x$ stetig.

Garbentopoi über allgemeinen Siten als top. Räumen — Topoi nach Maß





Im Standardtopos Set gibt es <u>keine</u> Surjektion $\mathbb{N} \twoheadrightarrow \mathbb{R}$.

In einem maßgeschneiderten Topos gibt es eine solche Surjektion.

Mengen nach Maß:
$\underline{\{1, 2, 3\}} \cup \{♡, \#\}$

Ringe nach Maß

wie Körper, aber multiplikative Inverse dürfen fehlen

z.B. $\mathbb{Z}$, $\mathbb{Z}[X]$, $\mathbb{Q}$, $\mathbb{Q}[X,Y]$, $\mathbb{Z}/(7)$, ...

- Ring A, Element $s \in A \rightsquigarrow A/(s)$

dieselbe Menge wie A, aber mit neuen Identifizierungen:

$x \sim y :\Longleftrightarrow \exists u \in A: x - y = us$

Hier ist s wie gewünscht zu Null gemacht

$s \sim 0$, denn $s - 0 = 1 \cdot s$

- Ring A, Element $s \in A \rightsquigarrow A[s^{-1}] \cong A[X]/(sX-1)$

Hier ist s wie gewünscht invertierbar gemacht

Def.: Eine <u>forcing notion</u> L besteht aus

vorgestellt als Approximation an ein hypothetisches „generisches Objekt"

- einer Menge L von forcing conditions,
- einer Relation $\leq$ auf L, welche reflexiv und transitiv ist sowie
- für jedes Element $\sigma \in L$ eine Menge $\mathrm{Cov}(\sigma)$ von Überdeckungen von σ

gewisse Mengen von Elementen, die $\leq \sigma$ sind

sodass folgende Stabilitätsbedingung erfüllt ist:

$$\forall \sigma \in L\ \forall R \in \mathrm{Cov}(\sigma)\ \forall \tau \in L, \tau \leq \sigma:\ \exists S \in \mathrm{Cov}(\tau).\ \underbrace{S \subseteq \downarrow R}$$

d.h. $\forall \nu \in S.\ \exists \nu' \in R.\ \nu \leq \nu'$

Bsp.: Jeder top. Raum X gibt Anlass zu einer forcing notion:

$L :=$ Menge der Offenen von X

$\leq \ := \ \subseteq$

$\mathrm{Cov}(U) := \{ M \mid U = \bigcup M \}$

Menge von Offenen von X

Dann gilt $\underbrace{\mathrm{Set}[L]} \simeq \mathrm{Sh}(X)$.

der Topos, der gemäß der Anleitung L gebaut wird

Bsp.: Sei τ eine beliebige benannte Menge (z.B. $\tau = \mathbb{R}$).
Wir suchen eine forcing notion L, sodass Set[L] eine Surjektion $\underline{\mathbb{N}} \twoheadrightarrow \underline{\tau}$ enthält.

(Obacht: Set[L] hat möglicherweise „sein eigenes τ", das davon unbeeinflusst ist. z.B. $\underline{\tau} \neq \tau$.)

Idee: Wir sammeln endliche Approximationen an eine solche Surjektion auf:

$$f : \mathbb{N} \rightharpoonup \tau$$
$$0 \mapsto \pi$$
$$1 \mapsto e$$
$$2 \mapsto 42$$

eine partielle Abbildung

als Liste geschrieben: $[\pi, e, 42]$

$$3 \mapsto 0$$

eine „etwas surjektivere" Approximation

$$4 \mapsto 0$$

eine „etwas mehr definierte" Approx

$L :=$ Menge der endlichen Listen von Elementen von τ.

$\tau \leq \sigma \;:\Longleftrightarrow\; \sigma$ ist ein Präfix von $\tau \Leftrightarrow \tau = \sigma \mathbin{++} \sigma'$ für eine Liste σ'

„τ ist eine bessere Approx. als σ"

„τ ist eine Verfeinerung von σ"

Bsp.: $[\pi, e, 42, 0] \leq [\pi, e, 42]$.

$$\mathrm{Cov}(\sigma) := \{\, \{\sigma \mathbin{++} [a] \mid a \in \tau\} \,\} \cup \{\, \{\sigma \mathbin{++} \tau \mid \tau \text{ so, dass } a \in \sigma \mathbin{++} \tau\} \mid a \in \tau \,\}.$$

Auch ohne LEM folgt:
- $\forall M.\ \neg \exists\, M \twoheadrightarrow P(M)$
- $\forall M.\ \neg \exists\, M \twoheadrightarrow 2^M$

Aber ohne LEM kann es sein, dass
- $\mathbb{R} \cong P(\mathbb{N})$ scheitert.

Bsp: Forcing notion, um LEM zu erzwingen:

$$L := \{\heartsuit\}$$

$$\heartsuit \leq \heartsuit$$

$$\mathrm{Cov}(\heartsuit) = \{ M \mid \neg\neg(M \text{ bewohnt}) \}$$

$\in P(\{\heartsuit\})$

z.B., falls wir die ganze Zeit über in $\mathrm{Sh}(\mathbb{R}^1)$ gearbeitet haben sollten, dann ist folgende Menge M eine Überdeckung von $\heartsuit$:

$$\{ \heartsuit \mid \alpha \# 0 \}$$

$\rightsquigarrow$ Dann $\mathrm{Set}[L] \models \mathrm{LEM}$.

Teilmenge mit
- $0 \in \mathfrak{p}$
- $x, y \in \mathfrak{p} \Rightarrow x + y \in \mathfrak{p}$
- $x \in \mathfrak{p}, a \in A \Rightarrow ax \in \mathfrak{p}$

Ideal $\mathfrak{p} \subseteq A$ mit
- $1 \notin \mathfrak{p}$ (d.h. $1 \in \mathfrak{p} \Rightarrow \bot$)
- $xy \in \mathfrak{p} \Rightarrow (x \in \mathfrak{p} \vee y \in \mathfrak{p})$

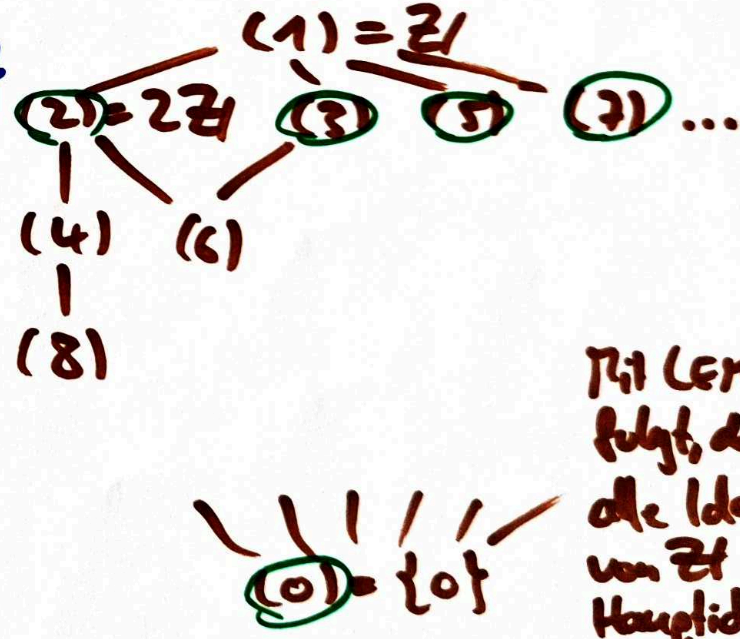
Bsp: Forcing notion, um ein Primideal eines gegebenen Rings A zu erzwingen:

$L :=$ Menge der endlich erzeugten Ideale von A

$$\mathfrak{a} \leq \mathfrak{b} :\Longleftrightarrow \mathfrak{a} \supseteq \mathfrak{b}$$

$$\mathrm{Cov}(\mathfrak{a}) := \{ \{\mathfrak{a} + (x), \mathfrak{a} + (y)\} \mid x, y \in A, xy \in \mathfrak{a} \} \cup \{ \emptyset \mid 1 \in \mathfrak{a} \}$$

Idealkarte von $\mathbb{Z}$:



Mit LEM folgt, dass alle Ideale von $\mathbb{Z}$ Hauptideale sind.

Def.: Ein Filter F einer forcing notion L ist eine Teilmenge $F \subseteq L$ mit:

(a) F ist abgeschlossen unter Vergröberung: $\tau \leq \sigma,\ \tau \in F \Rightarrow \sigma \in F$

(b) F ist $\searrow$-gerichtet: $\alpha, \beta \in F \Rightarrow \exists \sigma \leq \alpha, \beta\colon \sigma \in F$, F bewohnt

(c) F spaltet Überdeckungen: $\sigma \in F,\ R \in \mathrm{Cov}(\sigma) \Rightarrow \underline{F \between R}$

d.h. $\exists \tau\colon \tau \in F \cap R$

Bsp.: Sei X ein top. Raum und L die zugehörige forcing notion von (45).
Dann gibt jeder Punkt $x_0 \in X$ Anlass zu einem Filter von L:

$$F := \{ U \overset{\text{off}}{\subseteq} X \mid x_0 \in U \}$$

Ist X nüchtern, so stehen über diese Beziehung die Punkte von X in kanonischer Bijektion zu den Filtern von L.

Bsp.: Sei A ein Ring und L die forcing notion von (45).
Sei $\mathfrak{p} \subseteq A$ ein Primideal. Dann gibt es den folgenden Filter:

$$F := \{ \mathfrak{a} \in L \mid \mathfrak{a} \subseteq \mathfrak{p} \}$$

Ist umgekehrt F ein Filter, so ist $\bigcup F$ ein Primideal.
Dies gibt eine Bijektion zwischen den Primidealen von A und Filtern von L.

Bsp.: Sei X eine bewohnte Menge und L die forcing notion zum Erzwingen einer Surjektion $\mathbb{N} \twoheadrightarrow X$ von (44).
Sei $f\colon \mathbb{N} \twoheadrightarrow X$ eine Surjektion. Dann können wir folg. Filter F konstruieren:

$$F := \{ [x_0, \ldots, x_{n-1}] \mid \underline{f(0) = x_0, \ldots, f(n-1) = x_{n-1}} \}.$$

Das gibt eine Bijektion

d.h. $[x_0, \ldots, x_{n-1}]$ ist mit f kompatibel!

Motto: Sinn und Zweck einer forcing notion ist es, Bastelvorlage für einen Topos zu sein, in dem es einen generischen Filter gibt.

Sei L eine forcing notion.

Def.: Ein Prädikat P auf L heißt genau dann monoton, wenn:

$$\tau \leq \sigma,\ P\sigma \Rightarrow P\tau.$$

d.h. $P \subseteq L$ und notationelle Vereinbarung: $\sigma \in P :\Leftrightarrow P\sigma$

(alternativ: Abb. $P : L \to \Omega$)

Ω = Menge der Wahrheitswerte $= \mathcal{P}(\{\heartsuit\}) = \{\emptyset, \{\heartsuit\}, \ldots ? \}$

$\emptyset$: false, $\{\heartsuit\}$: true

Bsp.: Sei τ eine bewohnte Menge und L die forcing notion „Surjektion $\mathbb{N} \twoheadrightarrow \tau$" von (44). Seien $a_0, b_0 \in \tau$.

- $P_1\sigma :\Longleftrightarrow a_0 \in \sigma$
- $P_2\sigma :\Longleftrightarrow a_0 \notin \sigma$ ← nicht monoton
- $P_3\sigma :\Longleftrightarrow [a_0, b_0]$ ~~ist eine~~ ist eine Teilliste von σ
- $P_4\sigma :\Longleftrightarrow$ Summe aller Einträge von σ ist $\geq \pi$ (im Fall $\tau = \mathbb{R}$)
- $P_5\sigma :\Longleftrightarrow \sigma$ enthält mind. eine Wiederholung

Def.: Sei $\sigma \in L$. Sei P ein ~~Präd~~ monotones Prädikat auf L.

Dann: $\forall \tau \leq \sigma.\ P\tau :\Longleftrightarrow \underbrace{P \mid \sigma}$ „P bars σ"

„Unabhängig davon, wie genau sich σ weiter entwickelt, schlussendlich zu feineren Approximationen τ, wird $P\tau$ gelten."

$\neg(P \wedge (\neg P))$ ✓

$\neg(\neg\neg P \wedge \neg P)$ ✓

Def: Genau dann $P|\sigma$, wenn es einen bezeugenden Baum gibt, der nur gemäß der folgenden Konstruktionsregeln aufgebaut ist:

„induktive Def."

$$\frac{P\sigma}{P|\sigma}$$

„Wenn P schon jetzt gilt, dann erst recht schlussendlich."

$$\cancel{\frac{P|\tau \text{ für ein } \tau\in\sigma}{P|\sigma}}$$

$$\frac{P|\tau \text{ für alle } \tau\in R}{P|\sigma}\ R\in Cov(\sigma)$$

Bsp: $P_1|[\,]$ vermöge:

$$\dfrac{\dfrac{P_1\tau}{P_1|\tau} \text{ für alle } \tau \text{ mit } a_0\in\tau}{P_1|[\,]}$$

Prop: Ist P ein monotones Prädikat auf L, so ist auch $P|\cdot$ ein monotones Prädikat, d.h.

$$\tau\preceq\sigma,\ P|\sigma \Rightarrow P|\tau.$$

(Hier geht die Stabilitätsbed. ein!)

Prop: Sei F ein Filter von L. Sei $\sigma\in F$. Dann:

$$P|\sigma \Rightarrow \exists\tau\preceq\sigma.\ \tau\in F\wedge P\tau.$$

Bem: Folgendes Prinzip ist als „Bar-Induktionsprinzip" bekannt und eine Konsequenz von LEM und DC:

für einige wichtige forcing notions

Falls $\exists\tau\preceq\sigma.\ \tau\in F\wedge P\tau$ für alle ~~monotonen Prädikate~~ Filter F von L, so $P|\sigma$.

Wir nutzen folgende Signatur:

- für jede Menge M eine Sorte $\underline{M}$
- für jede Abb. $M \to N$ ein Funktionssymbol $\underline{M} \to \underline{N}$
- für jede Abb. $M \times N \to Z$ ein Funktionssymbol $\underline{M} \times \underline{N} \to \underline{Z}$

  $\vdots$
- für jedes Prädikat $P \subseteq M$ ein 1-stelliges Relationssymbol $\underline{P} \subseteq \underline{M}$
- für jede Relation $R \subseteq M \times M'$ ein 2-stelliges Relationssymbol $\underline{R} \subseteq \underline{M} \times \underline{M'}$

  $\vdots$
- ein 1-stelliges Relationssymbol $\mathfrak{G} \subseteq \underline{L}$

für jedes Element $s \in M$ ein nullstelliges Funktionssymbol $\underline{s}$ der Sorte $\underline{M}$ ($[\![\underline{s}]\!] = s$)

Def.: $\sigma \models \top$ gdw. ✓

$\sigma \models \bot$ gdw. $\nabla \tau \leq \sigma.\ \bot$ (d.h. $P \mid \sigma$ für P mit $P\tau \Leftrightarrow \bot$)

$\sigma \models A \wedge B$ gdw. $\sigma \models A$ und $\sigma \models B$

$\sigma \models A \vee B$ gdw. $\nabla \tau \leq \sigma.\ (\tau \models A$ oder $\tau \models B)$

$\sigma \models (A \Rightarrow B)$ gdw. für alle $\tau \leq \sigma$ gilt: Falls $\tau \models A$, dann $\tau \models B$.

$\sigma \models \forall s{:}\underline{M}.\ A(s)$ gdw. für alle $\tau \leq \sigma$ und $s_0 \in M$ gilt: $\tau \models A(\underline{s_0})$

$\sigma \models \exists s{:}\underline{M}.\ A(s)$ gdw. $\nabla \tau \leq \sigma.$ (es ex. ein $s_0 \in M$ mit $\tau \models A(\underline{s_0})$)

$\sigma \models x = y$ gdw. $\nabla \tau \leq \sigma.\ [\![x]\!] = [\![y]\!]$

$\sigma \models \underline{P}x$ gdw. $\nabla \tau \leq \sigma.\ P[\![x]\!]$

$\sigma \models \underbrace{\mathfrak{G}\,\delta}_{\text{„}\delta \text{ liegt im generischen Filter“}}$ gdw. $\cancel{\sigma \leq [\![\delta]\!]}$ $\nabla \tau \leq \sigma.\ \tau \leq [\![\delta]\!]$

(insb. gilt: $\sigma \models \mathfrak{G}(\underline{\sigma})$)

Def.: $\mathrm{Set}[L] \models A$ gdw. für alle $\sigma \in L$ gilt, dass $\sigma \models A$.

Bsp.: Sei τ eine bewohnte Menge und L die forcing notion „Surjektion $\mathbb{N} \twoheadrightarrow \tau$" von (44).

Dann:

$$\mathrm{Set}[L] \models \forall a : \underline{\tau}.\ \underbrace{\exists \delta : \underline{L}.\ a \in \delta \wedge G\delta}_{\text{„die gen. Surjektion trifft a"}}$$

gdw. ~~f.a. $\sigma \in L$ gilt:~~

f.a. $\tau \leq \sigma$ und $a_0 \in \tau$ gilt: $\underbrace{\tau \models \exists \delta : \underline{L}.\ a \in \delta}$

d.h. $\nabla \nu \in \tau.$ (es ex. $\delta \in L$ mit $\nu \models \underbrace{\underline{a_0} \in \underline{\delta}}$)

d.h. $\nabla \mu \leq \nu.\ a_0 \in \delta$

Bsp.: Für die gen. Surjektion f gilt:

$$\forall a, b : \underline{\tau}.\ \neg\neg \exists n : \underline{\mathbb{N}}.\ f(n) = a \wedge f(n+1) = b.$$

Bsp.: Sei A ein Ring. Sei L die forcing notion, um ein Primideal von A zu erzwingen (45). Dann gibt es in $\mathrm{Set}[L]$ den generischen Filter von L, G. Aus Sicht von $\mathrm{Set}[L]$ ist G also eine gewisse Menge von Elementen von $\underline{L}$. Das <u>generische Primideal</u> erhalten wir aus G durch folgende Definition:

$$a \in \mathfrak{p} :\Longleftrightarrow \exists b : \underline{L}.\ a \in b \wedge Gb$$

Nebenbei bemerkt: Wieso ist G wirklich ein Filter, aus Sicht von $\mathrm{Set}[L]$?

z.B. wieso gilt: $\mathrm{Set}[L] \models \forall \sigma : \underline{L}.\ \forall \tau : \underline{L}.\ G\sigma \wedge G\tau \Rightarrow \exists \nu : \underline{L}.\ \nu \leq \sigma \wedge \nu \leq \tau \wedge G\nu$

— das kocht sich herunter zu:

Falls $\nabla \tau \leq \sigma.\ P\tau$ und $\nabla \tau \leq \sigma.\ Q\tau$,

so auch $\nabla \tau \leq \sigma.\ (P\tau \wedge Q\tau)$.

Außerdem: Falls $\emptyset \in \mathrm{Cov}(\sigma)$, so gilt $\nabla \tau \leq \sigma.\ P\tau$ für <u>alle</u> monotonen Prädikate P.

Bsp.: Sei c eine bewohnte Menge und L die forcing notion „Surjektion $\mathbb{N} \twoheadrightarrow c$". In $Set[L]$ können wir dann mit Hilfe von G die <u>generische Surjektion</u> konstruieren:

$$\gamma(n) = x \;:\Longleftrightarrow\; \exists \sigma : \underline{L}.\ G\sigma \wedge \sigma[\underline{n}] = \underline{x}$$

(dabei $n : \underline{\mathbb{N}},\ x : \underline{c}$)

Def.: Ist σ eine endl. Liste, $n \in \mathbb{N}$, a ein Element, so bedeutet „$\sigma[n] = a$", dass in σ a an n-ter Stelle vorkommt.

Prop.: Sei A ein Ring. Dann gilt für das gen. Primideal folgendes:

$$(a \models \underline{x} \in \mathfrak{P}) \iff \underbrace{(\nabla b \le a.\ x \in b)}.$$

↑ später werden wir sehen, dass das genau dann der Fall ist, wenn $x \in \sqrt{a}$, d.h. wenn $\exists n \in \mathbb{N}: x^n \in a$

Thm. (Krull) Sei A ein Ring. Sei $x \in A$. Dann: $x \in \mathfrak{p}$ für alle PI $\mathfrak{p} \subseteq A$ $\Rightarrow$ x nilpotent (d.h. $x^n = 0$ f.e. $n \in \mathbb{N}$)

? (BPIT)

Bew.: $a \models \underline{x} \in \mathfrak{P}$

gdw. $a \models \exists b : \underline{L}.\ \underline{x} \in b \wedge G b$

gdw. $\nabla c \le a.$ (es ex. $b \in L$ mit $c \models (\underline{x} \in \underline{b} \wedge G\underline{b})$)

gdw. $\nabla c \le a.$ (es ex. $b \in L$ mit $\nabla d \le c.\ x \in b$ und $\nabla d \le c.\ \underbrace{d \le b}_{b \le d}$)

$\underbrace{\qquad\qquad\qquad\qquad\qquad\qquad}$

gdw. $\nabla d \le c.\ (x \in b$ und $b \le d)$

gdw. $\nabla c \le a.\ \nabla d \le c.\ x \in d$

gdw. $\nabla e \le a.\ x \in e.$

Ähnlich können wir zeigen, in Bezug auf die gen. Surj.:

$$(\sigma \models \gamma(\underline{n}) = \underline{x}) \iff \underbrace{(\nabla \tau \le \sigma.\ \tau[n] = x)}.$$

$\iff \sigma[n] = x$ falls LEM und c mind. zwei versch. Elemente enth.

Oder auch schon falls nur ein Element $y \in c$ mit $x \neq y$ existiert

Konstr. Rettung: Wenn $x \in \mathfrak{P}$, dann ist x nilpotent.

Rep.: Sei X eine (bzw.) Menge. In welchem Topos finden wir eine <u>generische Teilmenge</u> von X? (52)

Dazu folgende forcing notion:

$$L := \text{Menge der endlichen Teilmengen von } X$$

$$A \leq B \;:\Longleftrightarrow\; B \subseteq A.$$

$$\mathrm{Cov}(A) := \emptyset$$

In $\mathrm{Set}[L]$ können wir aus dem gen. Filter G die gen. Teilmenge M von $\underline{X}$ machen:

$$x \in M \;:\Longleftrightarrow\; \exists A : \underline{L}.\ x \in A \wedge G A$$

Dann gilt für jede Stufe $A \in L$ und jedes Element $x \in X$:

$$A \Vdash \underline{x} \in M \quad \text{gdw.} \quad \nabla B \leq A.\ x \in B \quad \text{gdw.} \quad x \in A$$

Überraschenderweise gilt:

$$\mathrm{Set}[L] \models \forall x_1, \dots, x_n : \underline{X}.\ x_1, \dots, x_n \in M \Rightarrow \neg\neg \exists y : \underline{X}.\ y \in M \wedge y \neq x_1 \wedge \dots \wedge y \neq x_n$$

„M ist anonym unendlich"

Spezialfall $n=0$:

$$\mathrm{Set}[L] \models \neg\neg(M \text{ bewohnt})$$

$$\mathrm{Set}[L] \models \neg\neg(\exists x : \underline{X}.\ x \in M)$$

gdw. für alle $A \in L$: $A \Vdash \neg\neg(\exists x : \underline{X}.\ x \in M)$

gdw. für alle $A \in L$: für alle $B \leq A$: es ist nicht der Fall, dass $B \Vdash \neg(\exists x : \underline{X}.\ x \in M)$

$B \Vdash \bot$ gdw. $\nabla C \leq B.\ ↯$ gdw. $↯$

gdw. f.a. $A \in L$ und $B \leq A$ es nicht der Fall ist, dass f.a. $C \leq B$ es nicht der Fall ist, dass ein $x_0 \in X$ ex. mit $\underbrace{C \Vdash \underline{x_0} \in M}_{\text{d.h. } x_0 \in C}$

gdw. $\underbrace{\forall A \in L\, \forall B \leq A}_{\forall B \in L}.\ \neg \forall C \leq B\ \underbrace{\neg \exists x_0 \in X.\ x_0 \in C}_{C = \emptyset}$

Prop.: $(\nabla \tau \leq \sigma.\ \nabla \upsilon \leq \tau.\ P\upsilon) \Leftrightarrow \nabla \tau \leq \sigma.\ P\tau$

Prop.: $((\nabla \tau \leq \sigma.\ P\tau) \wedge (\nabla \tau \leq \sigma.\ Q\tau)) \Leftrightarrow \nabla \tau \leq \sigma.\ (P\tau \wedge Q\tau)$

Prop.: $(\forall \tau \in L.\ P\tau \Rightarrow Q\tau) \Longrightarrow ((\nabla \tau \leq \sigma.\ P\tau) \Rightarrow (\nabla \tau \leq \sigma.\ Q\tau))$

Prop.: $\tau \leq \sigma,\ \sigma \models A \Rightarrow \tau \models A$ „Monotonie"

Prop.: $(\nabla \tau \leq \sigma.\ (\tau \models A)) \Rightarrow \sigma \models A$ „Lokalität"

Thm.: Wenn $\sigma \models A$ und intuitionistisch $A \vdash B$, dann $\sigma \models B$.
(Genauer: Wenn int. $A(x_1, \ldots, x_n) \vdash_{x_1 : \underline{M}_1, \ldots, x_n : \underline{M}_n} B(x_1, \ldots, x_n)$,
dann $\sigma \models \forall x_1 : \underline{M}_1.\ \ldots\ \forall x_n : \underline{M}_n.\ A(x_1, \ldots, x_n) \Rightarrow B(x_1, \ldots, x_n))$

Prop.: Seien alle Überdeckungen bewohnt. Dann:
(a) $\neg(\sigma \models \bot)$ für alle $\sigma \in L$
(b) für alle $\sigma \in L$: $\sigma \models \neg\neg A$ gdw. $\forall \tau \leq \sigma.\ \neg\neg \exists \upsilon \leq \tau.\ \upsilon \models A$
(c) $(\sigma \models A) \Leftrightarrow A$, falls in A ∇ nicht vorkommt

Beob.: $\mathrm{Set}[L] \models \forall x : \underline{A}.\ (x \notin \mathfrak{p}$
$\Rightarrow \mathfrak{p} + (x) = (1))$.
Ein Wunder!

Prop.: $\mathfrak{a} \models \neg(1 \in \mathfrak{p})$
$\mathfrak{a} \models \forall x, y : \underline{A}.\ x, y \in \mathfrak{p} \Rightarrow x \pm y \in \mathfrak{p}$
$\mathfrak{a} \models \forall x, y : \underline{A}.\ x \cdot y \in \mathfrak{p} \Rightarrow (x \in \mathfrak{p} \vee y \in \mathfrak{p})$

Thm.: $\mathfrak{a} \models \underline{x} \in \mathfrak{p}$ gdw. $x \in \sqrt{\mathfrak{a}}$ (d.h. $\exists n \in \mathbb{N} : x^n \in \mathfrak{a}$) $\leftarrow$ algebraisch gehaltvoll

Prop.: In dem Topos, der die generische Injektion $\underline{2} \to \underline{1}$ enthält, gilt $\bot$.
$\underline{2} = \{0, 1\}$, $\underline{1} = \{0\}$

Def.: Eine Ultra-Surjektion $f : \mathbb{N} \twoheadrightarrow \tau$ ist eine Abb. mit $\forall a \in \mathbb{N}\ \exists b \in \mathbb{N} : b \geq a \wedge f(b) = x$, $\forall x \in \tau$

Aufg.: Baue einen Topos, der die generische Ultra-Surjektion $\mathbb{N} \twoheadrightarrow \tau$ enthält.

Einschub: Reverse Mathematik

Z_2 – Arithm. 2. Ordn.

Big Five:

Π^1_1-CA = ATR$_0$ + „Π^1_1-Komprehension" ← Kann Cantor-Bendixson*

|

ATR$_0$

|

ACA$_0$ = WKL$_0$ + „arithmetische Komprehension" ← Kann Bolzano-Weierstraß*

$\{x \in \mathbb{N} \mid \ldots\}$ ← bel. arithmet. Aussagen (d.h. ohne Quant. über Mengen)

ACA$_0$ ← konservativ über PA für Aussagen 1. Ordnung

← Kann Heine-Borel*

|

WKL$_0$

|

RCA$_0$ = PA − Ind + Induktionsaxiom für Mengen + „rekursive Komprehension"

$\{x \in \mathbb{N} \mid \ldots\}$ ← hier dürfen nur solche Bed. stehen, die durch eine TM entscheidbar sind

Induktionsaxiom für Mengen: $\forall$ Menge X. $(0 \in X \wedge (\forall n \in \mathbb{N}.\ n \in X \Rightarrow n+1 \in X)) \Rightarrow (\forall n \in \mathbb{N}.\ n \in X)$

* verkappte abzählbare Variante

Die Big Five werden geprägt durch:

- Theoreme in der Kombinatorik
- unverkappte Theoreme in der sonstigen Mathematik [siehe Sam Sanders]

Induktionsprinzip für $P \mid \sigma$:

Um $\forall \sigma. ((P \mid \sigma) \Rightarrow Q\sigma)$ zu beweisen, genügt es nachzuweisen, dass:

1. $\forall \sigma. (P\sigma \Rightarrow Q\sigma)$ „Induktionsanfang"
2. $\forall \sigma. \forall R \in Cov(\sigma). ((\forall \tau \in R. Q\tau) \Rightarrow Q\sigma)$ „Induktionsschritt"

<u>Bsp:</u> <u>Zg:</u> $\forall \sigma.\ \cancel{P \models S}\ S \mid \sigma \Longrightarrow P \mid \sigma$

wobei $S\tau :\Longleftrightarrow P \mid \tau$

<u>Bew:</u> Laut Induktionsprinzip müssen wir zeigen:

1. $\forall \sigma. (S\sigma \Rightarrow P \mid \sigma)$
2. $\forall \sigma. \forall R \in Cov(\sigma). ((\forall \tau \in R. P \mid \tau) \Rightarrow P \mid \sigma)$

<u>Zu 1.:</u> ✓ nach Def. von S

<u>Zu 2.:</u> ✓ wg. Schlussregel

Bew. des Soundness-Theorems:

z.B. können wir $\overline{A \vdash_{\vec{x}} A}$ nachbauen: $\sigma \models \forall \vec{x}. (A(\vec{x}) \Rightarrow A(\vec{x}))$ ✓

z.B. können wir $\overline{A \wedge B \vdash_{\vec{x}} A}$ nachbauen: $\sigma \models \forall \vec{x}. ((A(\vec{x}) \wedge B(\vec{x})) \Rightarrow A(\vec{x}))$ ✓

z.B. können wir $\dfrac{A \vdash_{\vec{x}} C \qquad B \vdash_{\vec{x}} C}{A \vee B \vdash_{\vec{x}} C}$ nachbauen:

Gelte $\sigma \models \forall \vec{x}. (A(\vec{x}) \Rightarrow C(\vec{x}))$ $\boxed{1}$ und gelte $\sigma \models \forall \vec{x}. (B(\vec{x}) \Rightarrow C(\vec{x}))$ $\boxed{2}$.

Zu zg.: $\sigma \models \forall \vec{x}. ((A(\vec{x}) \vee B(\vec{x})) \Rightarrow C(\vec{x}))$.

Schlussendlich kommen wir auf folg. Beh.

$$\tau \models A(\vec{x}_0) \vee B(\vec{x}_0) \xRightarrow{\text{Lokalität}} \tau \models C(\vec{x}_0) \quad ✓$$

gdw. $\nabla \nu \leq \tau. \, (\nu \models A(\vec{x}_0) \xRightarrow{\text{wg. } \boxed{1}} \nu \models C(\vec{x}_0)$

oder $\nu \models B(\vec{x}_0)) \xRightarrow{\text{wg. } \boxed{2}} \nu \models C(\vec{x}_0)$

$\Rightarrow \nu \models C(\vec{x}_0)$

usw. für die weiteren Schlussregeln ;)

instruktiv!

Bei Realisierbarkeitstopoi bauen wir Topoi aus Modellen für Berechenbarkeit, wie z.B. Turingmaschinen, Superturingmaschinen oder dem λ-Kalkül.

<u>Schreibweise:</u> $e \cdot n \downarrow$:⟺ die e-te Turingmaschine hält bei Eingabe von n an.
In diesem Fall steht $e \cdot n$ für das Berechnungsergebnis.

Bsp: Es gibt eine Zahl $p \in \mathbb{N}$ mit: $\forall n \in \mathbb{N}.\ p \cdot n \downarrow$ und $\forall n \in \mathbb{N}: (p \cdot n = 1 \Leftrightarrow n \text{ prim})$

Bsp: Es gibt Zahlen $\pi_1, \pi_2 \in \mathbb{N}$ mit folg. Eigenschaft:
Die π_i-te Maschine interpretiert ihre Eingabe als Paar und extrahiert die i-te Komponente.

Der <u>effektive Topos</u> ist derjenige Realisierbarkeitstopos, der aus Turingmaschinen gebaut wird: Eff.

Beispiele:

① „Nach jeder Zahl kommt eine Primzahl." $(\forall n \in \mathbb{N}\ \exists p \in \mathbb{N}.\ p > n \wedge p \text{ prim})$
Set ✓ Eff ✓

② „Jede Zahl ist prim oder nicht prim."
Set ✓ (wg. LEM) Eff ✓

③ „Jede Fkt. $f: \mathbb{N} \to \mathbb{N}$ hat eine Nullstelle oder nicht."
Set ✓ (wg. LEM) Eff ✗ (Das hieße: Es gibt eine TM, die eine TM, die eine Fkt. $f: \mathbb{N} \to \mathbb{N}$ berechnet, einliest, und entweder eine Nullstelle von f oder einen Nullstellenabwesenheitsnachweis ausgibt.)
Eff(STM) ✓

④ „Jede Fkt $f: \mathbb{N} \to \mathbb{N}$ ist berechenbar durch eine TM."
Set ✗ Eff ✓ (trivialerweise) Eff(STM) ✗
Eff(λC) ✗

Eine Aussage gilt in Eff genau dann, wenn sie einen computable witness (berechenbaren Zeugen) besitzt — was das genau bedeutet, erklärt die

Kleene-Semantik:

Def.: $Eff \models A$ gdw. $\exists e \in \mathbb{N}: e \models A$, wobei:

$e \models \top$ gdw. ✓

$e \models \bot$ gdw. ↯

$e \models x = y$ gdw. $[\![x]\!] = [\![y]\!]$

$e \models A \wedge B$ gdw. $\pi_1 \cdot e\downarrow$ und $\pi_2 \cdot e\downarrow$ und $\pi_1 \cdot e \models A$ und $\pi_2 \cdot e \models B$

$e \models (A \Rightarrow B)$ gdw. f.a. $r \in \mathbb{N}$ mit $r \models A$ gilt, dass $e \cdot r\downarrow$ mit $e \cdot r \models B$

$e \models A \vee B$ gdw. $\pi_1 \cdot e\downarrow$ und $\pi_2 \cdot e\downarrow$ und $(\pi_1 \cdot e = 0 \Rightarrow \pi_2 \cdot e \models A)$ und $(\pi_1 \cdot e \neq 0 \Rightarrow \pi_2 \cdot e \models B)$

$e \models \forall n{:}\mathbb{N}.\ A(n)$ gdw. f.a. $n_0 \in \mathbb{N}$ gilt: $e \cdot n_0\downarrow$ und $e \cdot n_0 \models A(n_0)$

$e \models \exists n{:}\mathbb{N}.\ A(n)$ gdw. $\pi_1 \cdot e\downarrow$ und $\pi_2 \cdot e\downarrow$ und $\pi_2 \cdot e \models A(\underline{\pi_1 \cdot e})$

$e \models \forall f{:}\mathbb{N}\to\mathbb{N}.\ A(f)$ gdw. für alle $f_0: \mathbb{N} \to \mathbb{N}$ und $r \in \mathbb{N}$, die f_0 berechnen, gilt: $e \cdot r\downarrow$ und $e \cdot r \models A(\underline{f_0})$

$e \models \exists f{:}\mathbb{N}\to\mathbb{N}.\ A(f)$ gdw. $\pi_1 \cdot e\downarrow$ und $\pi_2 \cdot e\downarrow$ und $\pi_1 \cdot e$ berechnet eine Fkt. f_0 und $\pi_2 \cdot e \models A(\underline{f_0})$

⑤ „A gdw. $Eff \models A$“ (für arithmet. Aussagen)
Set ✗ Eff ✓

⑥ „DC“
Set ✓ (dank DC) Eff ✓ (auch, wenn DC in der Metaebene nicht zur Verfügung steht)

6' „CC“ Set ✓ (dank CC) Eff ✓ (auch ohne CC in der Metaebene)

$\forall x{:}\mathbb{N}.\ \exists y{:}\mathbb{N}.\ A(x,y) \Rightarrow \exists f{:}\mathbb{N}\to\mathbb{N}.\ \forall x{:}\mathbb{N}.\ A(x, f(x))$

⑦ „AC“
Set ✓ (dank AC)
Eff ✗

⑧ „MP“
Set ✓ (dank MP, was aus LEM folgt)
Eff ✓ (dank MP)

6'' „$\forall x{:}\mathbb{N}\to\mathbb{N}.\ \exists y{:}\mathbb{N}.\ A(x,y) \Rightarrow \exists f{:}\mathbb{N}^{\mathbb{N}}\to\mathbb{N}.\ \forall x{:}\mathbb{N}\to\mathbb{N}.\ A(x, f(x))$“
Set ✓ (lang to) Eff ✗ Eff(STM) ✓

$$\forall f{:}\mathbb{N}\to\mathbb{N}.\ \neg\neg\exists n.\ f(n) = 0 \Rightarrow \exists n.\ f(n) = 0$$

⑨ „HA hat bis auf Isomorphie exakt ein Modell“
Set ✗ Eff ✓

⑩ „Jede Fkt. $\mathbb{R} \to \mathbb{R}$ ist stetig.“
Set ✗ Eff ✓ Eff(STM) ✗

Thm: Wenn HA eine Aussage A zeigt, so gilt $\mathrm{Eff} \models A$. „Soundness"

Genauer gilt:

$$\mathrm{IPRA} \vdash \left(\forall A\colon (\mathrm{HA} \vdash A) \Rightarrow \exists e.\ \cancel{e \Vdash A}\ \mathrm{HA} \vdash (e \Vdash A)\right)$$

hier darf nicht stehen: „$e \Vdash A$"

Man kann also auf maschinelle Art und Weise aus HA-Beweisen Programme machen (berechenbare Zeugen für die bewiesenen Aussagen).

Prop: $e \Vdash \neg A$ gdw. $\forall r \in \mathbb{N}\colon (r \Vdash A) \Rightarrow \bot$ gdw. $\neg \exists r\colon r \Vdash A$.

Insb.: $\mathrm{Eff} \models \neg A$ gdw. $\neg\, \mathrm{Eff} \models A$.

Bem: Berechenbare Zeugen von negierten Aussagen sind niemals informativ.

Prop: $e \Vdash \neg\neg A$ gdw. $\neg\neg \exists r.\ r \Vdash A$.

Bem: Berechenbare Zeugen von Aussagen der Form $\neg\neg A$ beinhalten nur das Versprechen, dass im platonischen Ideenhimmel ein berechenbarer Zeuge für A ex., ohne einen Hinweis zu geben, wie dieser gefunden werden könnte.

Bsp: $\mathrm{Eff} \models \forall n\colon \mathbb{N}.\ \neg\neg(n \text{ prim}) \Rightarrow n \text{ prim}$.

Bem: Eff enthält kein Modell von PA, denn jedes Modell von PA wäre auch ein Modell von HA, aber das (bis auf Isomorphie) eindeutige Modell $\mathbb{N}$ von HA erfüllt nicht LEM.

Dennoch glaubt Eff, dass PA konsistent ist, denn in Eff wirkt der IPRA-Beweis der Äquikonsistenz von HA und PA; und HA ist aus Sicht von Eff aufgrund der Existenz eines Modells sicherlich konsistent

Was aus Sicht von Eff eine reelle Zahl ist, ist aus externer Sicht eine Turingmaschine, die eine nat. Zahl n als Eingabe einliest und eine rationale Zahl q_n als Ausgabe zurückgibt. Dabei muss gelten:

$$|q_n - q_m| \leq 2^{-n} + 2^{-m} \quad \text{für alle } n, m \in \mathbb{N}.$$

(Also darf q_n vom Grenzwert um höchstens 2^{-n} abweichen.)

Zwei solche Maschinen geben dieselbe reelle Zahl, wenn

$$|q_n - \tilde{q}_m| \leq 2^{-n} + 2^{-m} \quad \text{für alle } n, m \in \mathbb{N}.$$

Bsp: In Eff gibt es $\pi, \tau, e, \sqrt{2}, \sqrt{\pi^\pi}, \ldots$

Die Chaitinsche Haltekonstante Ω gibt es in Eff dagegen nicht.

Auszüge aus dem Beweis des Soundness-Theorems:

Wir müssen nachprüfen, dass die Kleene-Semantik alle logischen Schlussregeln und die Axiome von HA mitmacht.

z.B. $\dfrac{}{A \vdash_{\vec{x}} A} \rightsquigarrow \mathrm{Eff} \models \forall \vec{x}.\, (A(\vec{x}) \Rightarrow A(\vec{x}))$ ✓

$\dfrac{}{A \wedge B \vdash_{\vec{x}} A} \rightsquigarrow \mathrm{Eff} \models \forall \vec{x}.\, ((A(\vec{x}) \wedge B(\vec{x})) \Rightarrow A(\vec{x}))$ ✓ mit π_1

$(A(0) \wedge \forall n.\, A(n) \Rightarrow A(n+1))) \Rightarrow (\forall n.\, A(n))$ ✓ mittels Rekursion/loop

Hier ist ein berechenbarer Zeuge für LEM:

```
def oracle(A):
    # Aufgabe: Paar (0, x) zurückgeben, wobei x ein ber. Zeuge für A ist,
    #     oder Paar (1, y) zurückgeben, wobei y ein ber. Zeuge für ¬A ist.
    return (1, lambda x: outer_return (0, x))
                     ← ein hypoth. Zeuge für A
```

Eff $\models \neg$LEM,
aber Eff' $\models$ LEM, wenn Eff' gebaut wird mit einem Berechnungsmodell, das backtracking/continuations unterstützt

Ist eng damit verwandt, dass intuitionistische Logik zeigt:

$$\neg\neg(A \vee \neg A)$$

"CPS-Übersetzung in der Informatik = $\neg\neg$-Übersetzung in der Logik"

Forschungsprogramm von Olivia Caramello & Friends:

$$Sh(\mathcal{C}, J) \simeq Sh(\tilde{\mathcal{C}}, \tilde{J})$$

$(\mathcal{C}, J)$ Situs $\qquad\qquad$ $(\tilde{\mathcal{C}}, \tilde{J})$ Situs

Topoi als Brücken zw. unverwandt scheinenden Siten

Theorem von Ax-Grothendieck:

Sei $f: \mathbb{C}^n \longrightarrow \mathbb{C}^n$ eine Polynomfunktion.

Dann gilt: Ist f injektiv, so ist f surjektiv.

$\mathbb{C} \quad \cdots \quad S \quad \cdots \quad \mathbb{F}_p$

Bew.: (1) Die Beh. ist trivial für Polynomfkt. $\mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n$, wobei $\mathbb{F}_q$ ein endl. Körper mit q Elementen ist.

(2) Die Beh. folgt für Polynomfkt. $\overline{\mathbb{F}_p}^n \longrightarrow \overline{\mathbb{F}_p}^n$, wobei $\overline{\mathbb{F}_p}$ ein algebraischer Abschluss von $\mathbb{F}_p$ ist. $(\overline{\mathbb{F}_p} = \bigcup \mathbb{F}_{p^n})$

(3) ~~Die~~ Das formale System S „algebraisch abgeschlossener Körper der Charakteristik 0" ist vollständig: Für jede Aussage A gilt $S \vdash A$ oder $S \vdash \neg A$.

Axiome: $1+1 \neq 0$

$1+1+1 \neq 0$

$1+1+1+1 \neq 0$

$\vdots$

Insb.: $\underbrace{S \vdash \text{Beh.}}_{\Rightarrow \text{Beh.}}$ oder $S \vdash \neg\text{Beh.}$

$\Rightarrow \neg$Beh. für ~~alle~~ $\overline{\mathbb{F}_p}^n \to \overline{\mathbb{F}_p}^n$ für p hinreichend groß (größer als das größte Char-Axiom, das im Beweis verwendet wurde) ↯

Gilt $\mathrm{Eff} \models \forall f : \mathbb{N} \to \mathbb{N}.\ \exists a : \mathbb{N}.\ \forall b : \mathbb{N}.\ f(a) \leq f(b)$? ✗

Hier ist ein backtracking verwendender berechenbarer Zeuge:

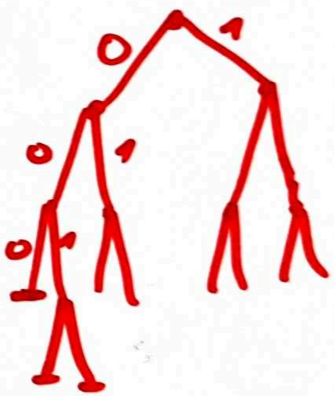
```
def minimum(f):
    # Ausgabe: Paar (a, h),   wobei a ∈ N
    #   und h eine Fkt. ist, die ein b ∈ N
    #   als Argument nimmt und einen
    #   Zeugen von f(a) ≤ f(b) zurückgibt
    def go(n):
        return (n, lambda b:
            if f(n) ≤ f(b) then ✓
                      else outer_return(go(b)))

    go(0)
```

In Eff gibt es einen binären Baum den sog. Kleene-Baum K mit folg. Eig.:

(a) Jede endliche 0/1-Folge ist ein Pfad in K oder nicht.

(b) Für jede nat. Zahl n gilt: Es gibt einen Pfad in K der Länge $\geq n$.

(c) Für jede unendliche 0/1-Folge $\gamma : \mathbb{N} \to \{0,1\}$ gilt:
Es gibt ein n, sodass der Pfad $[\gamma(0), \dots, \gamma(n)]$ nicht zu K gehört.



„Es gibt keinen unendlichen Pfad in K"

Eine Konsequenz aus der Existenz von K:

Es gibt stetige Fkt. $[0,1] \to \mathbb{R}$, die kein Maximum annehmen.

Für $2^{\mathbb{N}} = \{ \gamma : \mathbb{N} \to \{0,1\} \}$ statt $[0,1]$ geht das Gegenbeispiel so:

$$f : 2^{\mathbb{N}} \longrightarrow \mathbb{N}$$

$\gamma \longmapsto$ erstes $n \in \mathbb{N}$, sodass $[\gamma(0), \dots, \gamma(n-1)]$ kein Pfad von K ist

Die top. Räume $[0,1]$ und $2^{\mathbb{N}}$ sind in Eff also nicht kompakt ¡

Abhilfe: ~~top. Räume~~ Örtlichkeiten (locales)

- sind eine Verallg. von (nüchternen) top. Räumen
- als Örtl. sind $[0,1]$, $2^{\mathbb{N}}$ und viele weitere Räume ganz ohne LEM und AC kompakt
- Satz von Tychonoff für Örtl. ist ohne LEM und AC nachweisbar (für top. Räume äqu. zu AC (folgt LEM))
- Produkt von parakompakten Örtl. ist wieder parakompakt (anders als für top. Räume)
- Schnitt von dichten Teilmengen ist wieder dicht
- Örtl. können nichttrivial sein, auch wenn sie keine Punkte haben ($\mathbb{Q} \cap (\mathbb{R} \setminus \mathbb{Q})$) ✓
- Banach–Tarski funktioniert nicht für Örtl. ✓

- in der Welt der Örtl. gibt es ein cooles Fraktal X ohne Entsprechung in der Welt der top. Räume, nämlich die Örtlichkeit der Super-Surjektionen $\mathbb{N} \to \mathbb{R}$:

$$X = \dot{\bigcup_{s \in \mathbb{R}}} (\text{die Unterörtl. der Super-Surjektionen } f \text{ mit } f(0) = s)$$

Def.: Ein <u>Grothendieck-Topos</u> ist eine Kategorie, die äquivalent ist zur Kategorie der Garben über einem Situs $(\mathcal{C}, J)$.

vermöge eines volltreuen und wesentlich surjektiven Funktor

Bsp.: $Sh(X)$ **Bsp.:** Set

Bsp: $Set[L]$

Def: Ein <u>Situs</u> ~~ist~~ besteht aus
- einer Kategorie $\mathcal{C}$ (die klein sollte)
- einer Bedeckung: der Angabe einer Menge von Überdeckungen für jedes Objekt U von $\mathcal{C}$

gewisse Mengen von Morphismen mit Ziel U

sodass ein Stabilitätsaxiom gilt. (siehe nLab, <u>site</u>)

Bsp: Jede forcing notion L gibt Anlass zu einem Situs:

Obj. von $\mathcal{C}$: die Elemente von L

Mor. von $\mathcal{C}$: $\mathrm{Hom}_{\mathcal{C}}(\tau,\sigma) := \cancel{\begin{cases}\{\heartsuit\}, & \text{falls } \tau\le\sigma \\ \emptyset, & \text{sonst}\end{cases}} = \{\heartsuit \mid \tau \le \sigma\}$

Bedeckung: zu jedem $R \in \mathrm{Cov}(\sigma)$ die Überdeckung $\{\tau \to \sigma \mid \tau \in R\}$

Bsp: Der ~~große~~ gros Zariski-~~Topos~~ Site eines Rings A ist:

Obj.: endl. präs. A-Algebren (z.B. A, $A[X]$, $A[X,Y]/(X^2-Y^3)$, ...)

Mor.: $\mathrm{Hom}(B,C) := \{\varphi : C \to B \mid \varphi\ A\text{-Algebrenhomo}\}$

Bedeckung: Für jede Zerlegung der Eins, $1 = f_1 + \dots + f_n \in B$, ist $\{B[f_1^{-1}] \to B, \dots, B[f_n^{-1}] \to B\}$ eine Überdeckung von B.

Feferman-Mengenlehre ZFC/\$:
- Sprache ist die von ZFC + Konstantensymbol \$
- ZFC-Axiome
- Für jede Aussage A, die sich nicht auf \$ bezieht: $A \Leftrightarrow A^{\$}$
- ZFC/\$ ist konservativ über ZFC

Vorgestellt als Menge aller kl. Mengen (\$ selbst ist eine gr. Menge)

Der gros Zariski-Topos von A ist dann die Kat. der Garben über diesem Situs. (66)
Schreibweise: Zar(A).

Zar(A) enthält die generische lokale A-Algebra $\mathcal{O}$:

d.h. ~~es ex. genau ein max. Ideal~~
d.h. $1 \neq 0$ und
$x+y$ inv. $\Rightarrow$ x inv. $\vee$ y inv.

$\Gamma(\mathcal{O}, B) := B.$

Bsp: Besonders wichtig ist $\mathrm{Zar}(\mathbb{Z})$.
Dieser Topos enthält den generischen lokalen Ring $\mathcal{O}$. Dabei gilt:

kohärente Formeln: $\cancel{\forall}\ \cancel{\Rightarrow}$

~~Eine kohärente Sequenz φ~~
Für jede kohärente Sequenz $\sigma \equiv (A \vdash_{\vec{x}} B)$ in der Sprache der Ringe gilt:
dass folg. Aussagen äquivalent sind:

1. σ gilt für $\mathcal{O}$.
2. σ ist aus den Axiomen für einen lokalen Ring mit oder ohne LEM beweisbar.
3. σ gilt für alle lok. Ringe in allen Grothendieck-Topoi (insb. in Set)

Für nicht-kohärente Sequenzen gibt es aber Unterschiede zw. $\mathcal{O}$ und anderen lok. Ringen.
z.B. $\mathrm{Zar}(\mathbb{Z}) \models \forall s{:}\mathcal{O}.\ s \neq 0 \Rightarrow s$ inv.

Für Nachweise von koh. Sequenzen für lokale Ringe dürfen wir daher oBdA das Körperaxiom voraussetzen.

Def.: Ein <u>Elementartopos</u> ist eine Kategorie, die
- endliche Limiten hat,
- kartesisch abgeschlossen ist und
- über einen Unterobjektklassifizierer Ω verfügt.

(potenziell irreführend, da wichtige Eig. unerwähnt bleiben wie die Existenz endlicher Kolimiten)

Bsp.: Set (sofern wir Potenzmengen wie üblich zur Verfügung haben)
- $1 = \{\heartsuit\}$, $X \times Y$, $X \times_Z Y$
- $\mathrm{Hom}(X,Y)$ wieder eine Menge
- $\Omega = P(\{\heartsuit\}) =$ Menge der Wahrheitswerte $\overset{\text{LEM}}{=} \{\underset{\text{false}}{\emptyset}, \underset{\text{true}}{\{\heartsuit\}}\}$

  — Teilmengen $U \subseteq X$ stehen in natürlicher Bijektion zu Abb. $X \xrightarrow{\chi_U} \Omega$

$$(U \subseteq X) \longmapsto \chi_U \text{ mit } \chi_U(x) := \text{Wahrheitswert, dass } x \in U = \{\heartsuit \mid x \in U\}$$

$$(\chi^{-1}[\{\heartsuit\}] \subseteq X) \longleftarrow\!\shortmid\ \chi$$

(Ist Set ein Elementartopos, so ist auch jeder Grothendieck-Topos ein Elementartopos.)

Bsp.: Eff ist die „Setoid-Hülle" über folgender Kat. Asm der Assemblies ($\approx$ „Kat. der Datentypen")
(welche selbst noch kein Elementartopos ist):

Objekte: Paar $(X, \Vdash)$, wobei: X eine Menge ist und $(\Vdash) \subseteq X \times \mathbb{N}$ mit $\forall x \in X\, \exists n \in \mathbb{N}.\ x \Vdash n$

Morphismen: $\mathrm{Hom}((X,\Vdash),(X',\Vdash')) := \{f : X \to X' \mid \exists e.\ \forall x \in X\, \forall n \in \mathbb{N}.\ x \Vdash n \Rightarrow (e \cdot n \downarrow \wedge f(x) \Vdash' e \cdot n)\}$

„n ist eine Kodierung von x"

z.B. $(\mathbb{N}, \Vdash)$ mit $n \Vdash m :\Longleftrightarrow n = m$

$$\begin{tikzcd}
& & Q \arrow[dl, dashed, "!"'] \arrow[dll, bend right, "\varphi_1"'] \arrow[d, bend left, "\varphi_2"] \\
X & X \times Y \arrow[l, "\pi_1"'] \arrow[r, "\pi_2"] & Y
\end{tikzcd}$$

Bsp: Ist M ein Modell von IZF, so ist die Kat. der M-Mengen und M-Abb. ein Elementartopos.

$(a,b) := \{\{a\},\{a,b\}\}$
Kuratowski-Paare

Zum Körper mit einem Element: $\mathbb{F}_1$, $\mathbb{F}_{un}$

Wie viele k-dim. Untervektorräume hat ein n-dim. Vektorraum über $\mathbb{F}_q$?

$$\begin{bmatrix} n \\ k \end{bmatrix}_q := \frac{[n]!_q}{[k]!_q\,[n-k]!_q}, \quad \text{wobei } [a]!_q := [1]_q \cdot [2]_q \cdot \ldots \cdot [a]_q,$$

$$\text{und wobei } [a]_q = 1 + q + q^2 + \ldots + q^{a-1} \overset{q=1}{=} a$$

(„q-Analogon der Zahl a")

Setzen wir ohne Rechtfertigung $q := 1$, so erhalten wir

$$\begin{bmatrix} n \\ k \end{bmatrix}_1 = \binom{n}{k}.$$

So entsteht folg. Gedanke: n-dim. Vektorräume über $\mathbb{F}_1$ sollten dasselbe sein wie n-elementige Mengen, und k-dim. Untervektorräume dasselbe wie k-elementige Teilmengen. (besser punktiert)

Hoffnung: Riemannsche Vermutung mit $\mathbb{F}_1$ lösen — $\mathrm{Spec}(\mathbb{Z})$ als Kurve über $\mathbb{F}_1$ behandeln und Delignes 1974er-Beweis der Weil-Vermutung geeignet anpassen.

Ein Kandidat für eine Def. des „étalen Topos von $\mathbb{F}_1$" ist folgende (Connes, Caterina Consani):
Topos der Prägarben auf $\mathbb{N}^\times$ = Kat. der Funktoren $(\mathbb{N}^\times)^{op} \to \mathrm{Set}$
mit wichtigstem Objekt $\cancel{(\mathbb{Z}, +, \cdot)}$ $(\mathbb{Z}, \max, +)$

Es gibt einen Begriff von „Abb. zwischen Topoi", nämlich geometrischer Morphismus:

Ein geom. Mor. $\mathcal{E} \to \mathcal{F}$ ist ein geom. Funktor $\mathcal{F} \to \mathcal{E}$.

Bsp.: Jede stetige Abb. $X \to Y$ zw. top. Räumen induziert einen geom. Mor. $Sh(X) \to Sh(Y)$.

Def.: Ein Punkt eines Topos $\mathcal{E}$ ist ein geom. Mor. $\underbrace{Sh(\{\heartsuit\})}_{\simeq Set} \to \mathcal{E}$.

Bsp.: Für nüchterne top. Räume X gibt es eine kanon. Bijektion zwischen den Punkten von X und den topostheor. Punkten von $Sh(X)$.

Bem.:
$$\begin{tikzcd}
\mathrm{SoberTop} \arrow[r, hook] \arrow[d] & \mathrm{Loc} \arrow[r, hook] \arrow[d, hook] & \mathrm{Sit} \arrow[r, hook] & \mathrm{Topoi} \\
\mathrm{Top} & \mathrm{ForcNots} \arrow[ur, hook] & &
\end{tikzcd}$$
volltreue Einbettungen.

Für Topoi können auch folg. Begriffe definiert werden: Offenes, Untertopos, Überdeckung, Kompaktheit, ...

Bsp.: Die Punkte von $Set[L]$ stehen in kanon. Bij. zu den Filtern von L; und jede forcing condition gibt Anlass zu einem Offenen von $Set[L]$.

Der Ring $\mathbb{R}[X_1,\dots,X_n]$ ist doch der Ring der (regulären) Fkt. auf dem Raum $\mathbb{R}^n$. Können wir die Elemente eines bel. Rings A auch als (reg.) Fkt. auf einem gewissen Raum auffassen? Ja! Dieser Raum ist $Spec(A)$, „Spektrum von A". Als forcing notion ist dieser Raum geschwind konstruiert:

$L := A$

$f \le g \;:\Leftrightarrow\; (f) \subseteq \sqrt{(g)} \Leftrightarrow \exists n \in \mathbb{N}, h \in A: f^n = gh$ (eine forcing cond. f stellen wir uns als ~~das Offene der~~ die Antiverschwindungsmenge von f vor)

$Cov(f) := \{\{f_1,\dots,f_n\} \mid \sqrt{(f)} = \sqrt{(f_1,\dots,f_n)}\}$

Die Strukturgarbe ist $\mathcal{O}$ mit $\Gamma(\mathcal{O}, f) := A[f^{-1}]$. „$\{p \mid f(p) \text{ inv.}\}$" $\longrightarrow$

Def.: $\Box A \;:\Longleftrightarrow\;$ A gilt in allen Grothendieck-Topoi

$\Diamond A \;:\Longleftrightarrow\;$ A gilt in mind. einem positiven Gr.-Topos. — stärkere Fassung von „nicht trivial"

$\Diamond\!\!\!\cdot\;\, A \;:\Longleftrightarrow\;$ A gilt in mind. einem positiv overten Gr.-Topos.

Bsp.: Sei A ein Ring und $x \in A$.

Mit AC kann man zeigen: $(\forall$ Primideale $\mathfrak{p}$ von $A.\ x \in \mathfrak{p}) \Rightarrow x$ nilpotent. (Krull)

Ohne AC und ohne LEM so: $(\Box(\forall$ ——— " ——— $)) \Rightarrow x$ nilpotent.

Bsp.: Sei A ein nichttrivialer Ring.

Mit AC kann man zeigen: A hat ein maximales Ideal

Ohne AC und ohne LEM kann man zeigen: $\Diamond\!\!\!\cdot\;\,(\underbrace{\text{——— " ———}}_{\text{keine Aussage 1. Ordnung}})$.

Sprechweise:

$\Box$ „überall"

$\Diamond$ „irgendwo" $\longleftarrow$ für alle kohärenten Sequenzen σ gilt: $(\Diamond\sigma) \Rightarrow \sigma$.

$\Diamond\!\!\!\cdot\;\,$ „in der Nähe" $\longleftarrow$ für alle Aussagen 1. Ordnung A gilt: $(\Diamond\!\!\!\cdot\;\, A) \Rightarrow A$.

Bsp.: Ist X eine bel. (vielleicht überabzählbare) bewohnte Menge, so gilt $\Diamond\!\!\!\cdot\;\,(\exists \mathbb{N} \twoheadrightarrow X)$, d.h. $\Diamond\!\!\!\cdot\;\,(X$ abzählbar). Es gilt sogar: $\Diamond\!\!\!\cdot\;\,\Box(X$ abzählbar)

Bsp.: $\Box\Diamond$LEM, $\Box\Diamond\!\!\!\cdot\;\,(\neg$LEM)

Mit $\Box$, $\Diamond$, $\Diamond\!\!\!\cdot\;\,$ können wir auf kurze und knappe Art und Weise das topostheor. Multiversum bereisen ~~[illegible]~~ (aufwärts).

Klassische Mechanik:

- Phasenraum Σ, die Punkte von Σ sind die möglichen $\overset{\text{reinen}}{\downarrow}$ Zustände des Systems
  (z.B. für ein freies Teilchen im $\mathbb{R}^3$: $\Sigma = \mathbb{R}^3 \times \mathbb{R}^3 = \{(x, y, z, v_x, v_y, v_z)\}$)
- Reine Zustände = Punkte von Σ $\hat{=}$ C^*-Algebrenhomomorphismen $A \to \mathbb{C}$,
  wobei $A := C(\Sigma, \mathbb{C})$
  $=$ C^*-Algebra der stetigen komplexwertigen Funktionen auf Σ

$$(p \in \Sigma) \longmapsto \begin{pmatrix} A \longrightarrow \mathbb{C} \\ f \longmapsto f(p) \end{pmatrix}$$

- gemischte Zustände = Wahrscheinlichkeitsmaße μ auf Σ $\hat{=}$ lin. Abb. $\varphi : A \to \mathbb{C}$
  mit $\varphi(1) = 1$
  und $\varphi(a^* a) \geq 0$
- Observable = stetige Fkt. $\Sigma \to \mathbb{R}$ $\hat{=}$ selbstadj. Elemente in A
- Erwartungswert einer Observablen a
  in einem (gemischten) Zustand φ = $\varphi(a)$

$$\mu \longmapsto \begin{pmatrix} A \longrightarrow \mathbb{C} \\ f \longmapsto \int_\Sigma f(x)\, d\mu(x) \end{pmatrix}$$

Zwischen Σ und A kann mit Gelfand-Naimark-Korrespondenz umgerechnet werden:

$$(\text{kompakte Hausdorffräume})^{op} \simeq (\text{komm. } C^*\text{-Algebren})$$

$$X \longmapsto C(X, \mathbb{C}) = \{f : X \to \mathbb{C} \mid f \text{ stetig}\}$$

$$\operatorname{Spec}(A) \longleftarrow A$$

Quantenmechanik:

- Ausgangspunkt zur Beschreibung eines quantenmech. Systems: eine nichtkomm. C^*-Algebra. (z.B. ist H ein Hilbertraum-Beschreibung des Systems, so $A := L(H,H)$)
  (z.B. für freies Teilchen im $\mathbb{R}^3$: $H = H^1(\mathbb{R}^3)$) $L^2(\mathbb{R}^3)$

  Nicht umrechenbar in einen Phasenraum. ☹

- Ein reiner Zustand ist eine Abb. $A \xrightarrow{\varphi} \mathbb{C}$, die ein C^*-Algebrenhomo ist.
- Ein gemischter Zustand ist eine Abb. $A \xrightarrow{\varphi} \mathbb{C}$ mit $\varphi(1) = 1$, $\varphi(a^*a) \geq 0$ und φ linear.

$\varphi(a+b) = \varphi(a) + \varphi(b)$ für alle $a, b \in A$

Elemente addieren, die nicht miteinander kommutieren?! $ab \neq ba$

- Ein reiner Zustand ist eine Abb. $A \xrightarrow{\varphi} \mathbb{C}$, die auf jeder komm. Unter-C^*-Algebra $B \subseteq A$ ein C^*-Algebrenhomo ist

  $\forall B \subseteq A$ komm. Unter-C^*-Algebra:
  $\forall a, b \in B$: $\varphi(a+b) = \varphi(a) + \varphi(b)$

- Ein gemischter Zustand ist eine Abb. $A \xrightarrow{\varphi} \mathbb{C}$ mit $\varphi(1) = 1$, $\varphi(a^*a) \geq 0$ und $\varphi|_B$ linear für alle komm. Unter-C^*-Algebren $B \subseteq A$.

Def.: Der <u>Bohr-Topos</u> Bohr(A) von A entsteht aus folg. forcing notion:

$L :=$ Menge der komm. Unter-C^*-Algebren.

$B \leq B' \;:\Longleftrightarrow\; B \supseteq B'$

$\mathrm{Cov}(B) = \emptyset$

Die nichtkomm. C^*-Algebra A hat in Bohr(A) ein Spiegelbild $\mathcal{O}$:

$\Gamma(\mathcal{O}, B) := B.$

Dann gilt: $\mathrm{Bohr}(A) \models$ ($\mathcal{O}$ ist eine <u>komm.</u> C^*-Algebra)

Innerhalb von Bohr(A) hat das qm. System dann also sogar einen Phasenraum, nämlich $\mathrm{Spec}(\mathcal{O})$ (als Örtlichkeit).

Innerhalb von Bohr(A) erscheint das qm System also wie ein System der klass. Mechanik.

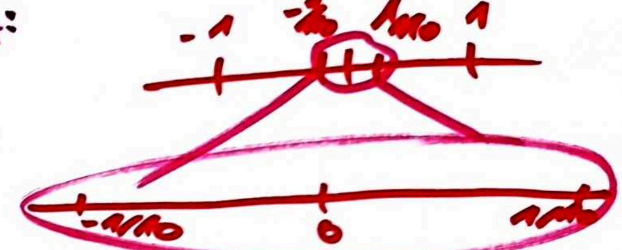
Synthetische Differentialgeometrie

Axiom: (Mikroaffinität)

$\Delta = \{ \varepsilon \in R \mid \varepsilon^2 = 0 \}$ „infinitesimale Monade um 0"

Sei $f : \Delta \to R$ eine bel. Abb.
Dann gibt es eindeutig bestimmte Zahlen $a, b \in R$ mit:

$$\forall \varepsilon \in \Delta : \; f(\varepsilon) = a + b\varepsilon.$$



Bem.: $a = f(0)$.

Prop.: $\neg(\Delta = \{0\})$.

Bew.: Sonst Widerspruch zur Eindeutigkeit von b.

R ist ein Körper im Sinne von $x \neq 0 \Rightarrow x$ inv.

Prop.: $\neg \exists \varepsilon \in \Delta.\ \varepsilon \neq 0$

Bew.: Ang. doch. Dann also gibt es $\varepsilon \in \Delta$ mit $\varepsilon \neq 0$.
Also ε inv. Somit $1 = 1^2 = (\varepsilon \varepsilon^{-1}) \cdot (\varepsilon \cdot \varepsilon^{-1}) = \varepsilon^2 \cdot (\varepsilon^{-1})^2 = 0$ ↯

Kor.: $\neg$LEM.

~~Def.~~ / ~~Sei~~

Prop.: (Mikrokürzbarkeit) Gelte $x\varepsilon = y\varepsilon$ für alle $\varepsilon \in \Delta$. Dann $x = y$.

Bew.: wg. Eindeutig im Mikroaffinitätsaxiom.

Def.: Sei $f : R \to R$ eine bel. Abb. Sei $x_0 \in R$. Dann ist $f'(x_0) \in R$ die eindt. best. Zahl mit folg. Eigenschaft:

$$f(x_0 + \varepsilon) = f(x_0) + \varepsilon f'(x_0) \quad \text{für alle } \varepsilon \in \Delta.$$

(dazu Mikroaffinität anwenden auf $h : \Delta \to R,\ \varepsilon \mapsto f(x_0 + \varepsilon)$)

Bsp: Sei $f(x) = x^2$.

Dann: $f(x+\varepsilon) = (x+\varepsilon)^2 = x^2 + \underbrace{2x}_{= f'(x)}\varepsilon + \cancel{\varepsilon^2}$.

Bsp: $(g \circ f)(x+\varepsilon)$

$$= g(f(x+\varepsilon)) = g(f(x) + \underbrace{\varepsilon f'(x)}_{\substack{=:\delta \\ (\delta^2 = 0)}}) = g(f(x)) + \varepsilon \underline{\underline{f'(x)\, g'(f(x))}}$$

Es gibt den sog. glatten Topos $\mathcal{E}$. In ihm gibt es einen Ring R, der aus Sicht von $\mathcal{E}$, das Mikroaffinitätsaxiom erfüllt.

Außerdem gibt es einen volltreuen Funktor $\mathrm{Man} \overset{\dot{-}}{\hookrightarrow} \mathcal{E}$.

$$\mathbb{R}^1 \longmapsto R$$

(Warnung: $R \neq \mathbb{C}$.)

Thm: Sei $f, g: \mathbb{R} \to \mathbb{R}$ eine glatte Abb. Dann:

$f' = g$ gdw. $\mathcal{E} \models (\underline{f}' = g)$

übliches differenzieren

gemäß interner Def. differenzieren

Bew: Es gibt eine glatte Fkt. h mit $f(x+y) = f(x) + y\, g(x) + y^2 h(x,y)$.

$\Rightarrow \mathcal{E} \models \forall \varepsilon : \Delta.\ f(x+\varepsilon) = f(x) + \varepsilon g(x) + \underbrace{\varepsilon^2 h(x,\varepsilon)}_{=0}$. $\Rightarrow \mathcal{E} \models f'(x) = g(x)$