Vorlesung aus dem Sommersemester 2013

Transfinite Beweismethoden

PD. Dr. Schuster

6.06.2013

References

1. A. Kertesz, *Einführung in die Transfinite Algebra* (main reference)
2. I. Kaplanski. *Set Theory and Metric Spaces*, AMS 2001
3. G. H. Moore. *Zermelo's Axiom of Choice*, Springer
4. T. Jech. *The Axiom of Choice*, North-Holland
5. H. Rubin, J. E. Rubin. *Equivalents of the Axiom of Choice*, Vol. I + II
6. M. Erne. *Einführung in die Ordnungstheorie*, 1982
7. H. Herrlich. *Axiom of Choice*, Springer, 2006
8. P. Howard, J.E. Rubin. *Consequences of the Axiom of Choice*, AMS, 1998
9. J.L. Bell. *The Axiom of Choice*, College, 2009

History and Motivation

- 1883: Cantor needed a well-order of $\mathbb{R}$, and considered the existence of such order as a "Denkgesetz".
- 1904: Zermelo proves that every set can be well-ordered, (WO). Zermelo used AC.

  $\mathrm{ZF} \vdash \mathrm{AC} \leftrightarrow \mathrm{WO}$
- Peano (1890) in a paper about Diff. Eq. explicitly avoids to use CC by using an algorithmic proof instead.
- $\geq$1904, Zermelo's paper prompted the so-called "Grundlagenkrise"

- 1905: Hamel proved with WO the existence of a basis for $\mathbb{R}$ as a $\mathbb{Q}$-vector space and he used this result to give the general solution of the functional equation $f(x+y) = f(x) + f(y)$ ($f\colon \mathbb{R} \to \mathbb{R}$)
- WO made possible the use of transfinite induction (TI).
- Zorn (1935) put forward Zorn's Lemma (ZL), to make proofs shorter and more algebraic. (Kuratowski already introduced ZL in 1922)
- Teichmüller (1939) and Tukey (1940), Teichmüller-Tukey Principle (TT)
- Of course we know AC, TT, ZL, WO are equivalent.
- Raoult (1988): *Open Induction* (OI), equivalent to ZL and makes proofs even shorter.
- Coquand, Bergen (2004): Dependent choice can be replaced by a combinatorial form of OI.
- AC is problematic from a constructive point of view.

  $\mathrm{AC} + \mathrm{Pow} \vdash \mathrm{EM}$ (Dizconescu, 1970) (EM = Law of excluded middle ($\forall_x (P(x) \vee \neg P(x))$), Pow = Powerset axiom)
- Gödel 1940: $\mathrm{ZF} \nvdash \perp \to \mathrm{ZF} \nvdash \neg\,\mathrm{AC}$
- Cohen 1963: $\mathrm{ZF} \nvdash \perp \to \mathrm{ZF} \nvdash \mathrm{AC}$
- OI is an alternative to AC.
- Hilbert's Programme (HP): Justify the use of ideal objects (e.g. objects constructed by means of ZL or AC) and transfinite methods. Prove with finite methods, that the use of idealistic methods is consistent.
- Revised form of HP (Kreisel and Feferman): Eliminate the use of ideal objects and use only finite and constructive proof methods.
- Successful for a considerable part of commutative algebra (Lombardi, Coquand)

Preliminaries (1).

- *Partial order* $\leq$ (reflexive, transitive, antisymmetric), $(X, \leq)$ is a *poset*.
- A *chain*, or *total order* or *linear order* is a partial order satisfying $x \leq y \vee y \leq x$
- On a poset $(X, \leq)$ we talk about minimal/maximal elements. e.g. x is *minimal* in X $\iff \forall_{y \in X}(y \leq x \to y = x)$ or equiv. $\neg\exists_{y \in X}(y \leq x \wedge y \neq x)$
- $(X, \leq)$ is a chain, x is minimal (maximal), then we say: x is the *least* (*greatest*) element.
- $\leq$ *well-founded*: every non-empty subset has a minimal element.

- $\leq$ *well-order*: $\leq$ is well-founded linear order.
- WO: every set can be well-ordered.

  Beispiel. (i) $\mathbb{N}$ is well-ordered by $\leq$

  (ii) $\mathbb{Q}^0_+ = [0, +\infty) \cap \mathbb{Q}$. It is linearly ordered, has least element (0), but it is not well-founded. ($s = (\sqrt{2}, +\infty) \cap \mathbb{Q}$).

  (iii) Transfinite Induction (TI) on a poset X. Every progressive subset S of X equals X.
$$\underbrace{\forall_x [\forall_{y<x}(y \in S) \to (x \in S)]}_{S-\text{progressive}} \to \underbrace{\forall_x (x \in S)}_{X=S}$$

  (iv) If $\leq$ is well-founded order, then TI holds on $(X, \leq)$. [If S progressive and $S \neq X$, then $R = X - S$ is non-empty and therefore it has a minimal element x, so that $x \in S$ since S is progressive. $\lightning$.]

  (v) On $\mathbb{N}$, TI rewrites as: $\forall_n [\forall_{m<n}(m \in S) \to n \in S] \to \forall_n (n \in S)$.

Satz (Hamel, 1905)**.** *Any linearly independent subset $S \in V$, when V is a vector space over $\mathbb{K}$ can be extended to a base $S' \supset S$.*

Beweis. Consider a well-order on V, $\langle V_\alpha \mid \alpha \leq \overline{\alpha} \rangle$ ($\overline{\alpha}$ ordinal corresp. to the well-order on V) We can define a (partial) function $f \colon \overline{\alpha} \to V$:

$$f(\alpha) = \text{the least element of } V \text{ that is not a linear combination of } f(\beta) \text{ with } \beta < \alpha \text{ in } S$$

Of course f is not defined, if such an element does not exist.

- f injective
- $f(\overline{\alpha}) \cup S$ is linearly independent. Suppose that a finite linear combination of elements of S and values of f equals 0, and we can assume all coefficients to be non-zero. This combination must induce some element of $f(\overline{\alpha})$, and let α_0 the maximal of the ordinals encountered. Then $f(\alpha_0)$ is a linear combination of S and elements of the form $f(\beta)$ $\beta < \alpha_0$. $\lightning$.

Since $\overline{\alpha}$ has the cardinality of V, f is defined as an initial segment of kind $[0, \alpha)$, with $f(\alpha)$ undefined. This means precisely that every element of V is linear combination of S and $(f(\beta) \colon \beta < \alpha)$ □

In 1821: Cauchy addressed the following functional equation:

$$f(x + y) = f(x) + f(y) \qquad f \colon \mathbb{R} \to \mathbb{R}$$

Cauchy proved that all the continuous solutions are linear, of the form $f(x) = c \cdot x$ for some $c \in \mathbb{R}$. Hamel first proved that $\mathbb{R}$ has a $\mathbb{Q}$-basis.
Suppose $f \colon \mathbb{R} \to \mathbb{R}$ is additive. Then:

- $f(x_1 + \ldots + x_n) = f(x_1) + \ldots + f(x_n)$
- $f(n \cdot x) = n \cdot f(x)$ for all $n \in \mathbb{N}$
- Since $f(0) = f(0+0) = f(0)+f(0) \to f(0) = 0$. Hence if $n \leq 0$, $0 = f(nx+(-n)x) = f(nx) - nf(x)$. So $f(nx) = nf(x)$ for all $n \in \mathbb{Z}$.
- If $q = \frac{m}{n} \in \mathbb{Q}$, then $n \cdot q = m$ so that $n \cdot f(q) = m \cdot f(i)$, so that, posing $c = f(i)$, we have $f(q) = c \cdot q$.

If f is continuous, then $f(x) = c \cdot x$ for all $x \in \mathbb{R}$. (Cauchy's Result). If x is real, $y = \frac{m}{n} \cdot x$, then $f(n \cdot y) = f(m \cdot x) \rightsquigarrow f(y) = \frac{m}{n} f(x)$. Hence f is $\mathbb{Q}$-linear. If we have a basis of $\mathbb{R}$ over $\mathbb{Q}$, say B, then each h is determined by its values on B.

Satz. *If $f\colon \mathbb{R} \to \mathbb{R}$ is a non-continuous solution f of the Cauchy equation, then it's graph $G(f) = \{(x, f(x))\colon x \in \mathbb{R}\}$ is dense in $\mathbb{R}^2$*

Beweis. Let $(x, y) \in \mathbb{R}^2$ and U is a neighborhood of (x, y). Since f is a non-$\mathbb{R}$-linear solution, there exist $a, b \neq 0$ in $\mathbb{R}$, such that $\alpha = \frac{f(a)}{a}$ and $\beta = \frac{f(b)}{b}$ are different. This means $u = (a, f(a)), v = (b, f(b))$ are independent, and therefore are a basis of $\mathbb{R}$. There exist $p, q \in \mathbb{R}$ sucht that $(x, y) = pu + qv$. Since $\overline{\mathbb{Q}^2} = \mathbb{R}^2$, we can find $\overline{p}, \overline{q} \in \mathbb{Q}$ such that $\overline{p}u + \overline{q}u \in U$. Therefore $\overline{p}u + \overline{p}v = (\overline{p}a + \overline{q}b, \overline{p}f(a) + \overline{q}f(b)) = (\overline{p}a + \overline{q}b, f(\overline{p}a + \overline{q}b)) \in U \cap G(f)$ $\square$

Preliminaries (2): Zorn's Lemma. Let $(X, \leq)$ be a poset, $S \subseteq X$, $x \in X$.

- x an *upper bound* of S: $\forall_{s \in S}(s \leq x)$.
- x *least upper bound* or *supremum* of S: $\forall_{u \in X}[\forall_{s \in S}(s \leq u) \leftrightarrow x \leq u]$, that is:
  (i) x is an upper bound of S. ($x = u$, $\leftarrow$).
  (ii) if $u \in X$ upper bound of S, then $x \leq u$ ($\to$).
- *Common form of Zorn's Lemma*: If $X \neq \emptyset$ and every chain $C \subseteq X$ with $C \neq \emptyset$ has an upper bound, then X has a maximal element.
- We could chop $X \neq \emptyset$ together with $X \neq \emptyset$, [$\emptyset$is chain], or we can keep $X \neq \emptyset$ and every chain $C \subseteq X$, $C \neq \emptyset$ has a supremum.
- All of this can be reversed: Let $(X, \leq)$ be a poset. $D \subseteq X$ is called *directed*: $\forall_{x,y \in D} \exists_{z \in D}(x \in z \wedge y \leq z)$.
- Every chain is a directed subset.
- A maximal element of a directed subset is also its greatest element.
- X *directed complete*: every directed subset $D \subseteq X$, with $D \neq \emptyset$, D has a supremum in X, we write the supremum as $\bigvee D$.
- *dcpo*: directed complete partial order.

- V Vectorspace, S Subspace. $V, S = \{W : W \leq V\}$ is a dcpo with $\leq$ as partial order with V as V. Exercise!
- A subset of a dcpo X is *closed* if $\bigvee D \in S$ for all $D \subseteq S$ non-empty directed subset.
- S is closed subset of the dcpo $(\mathbb{P}, \subseteq)$
- Here follow two equivalent formulations of Zorn's Lemma:
  - Every dcpo $X \neq 0$ has a maximal element
  - If X is a dcpo, then every closed subset $S \subseteq X$ with $S \neq 0$ has a maximal element.

13.06.2013

Definition. Sei $(x, \leq)$ partielle Ordnung, $D \subseteq X$ *gerichtet*, wenn jede endliche Teilmenge von D eine obere Schrankeun D hat. Dies ist gleichbedeutend mit $D \neq \emptyset$ und erfüllt die alte Definition, d.h. $\forall_{x,y \in D} \exists_{z \in D} (x \leq z \wedge y \leq x)$.

Lemma ((Kuratowski-)Zorn (ZL))**.** *Jeder dcpo $X \neq 0$ hat ein maximales Element. Äquivalent: Ist X ein dcpo und $S \subseteq X$ abgeschlossen, $S \neq 0$, so hat S ein max. Element*

Definition. Nun sei S eine Menge; $X = \mathbb{P}(S)$ mit $\subseteq$; $F, G \subseteq X$. F heißt *von endlichem Charakter*, wenn für alle $T \subseteq S$ gilt: $T \in F \iff \forall T_0 \subseteq T (T_0 \text{ endlich } \rightarrow T_0 \in F)$. G *von coendlichem Charakter*, wenn für alle $T \subseteq S$ gilt: $T \in G \subseteq \exists_{T_0 \subseteq T} (T_0 \text{ endlich } \wedge T_0 \in G)$. Falls $X = F \dot\cup G$, so gilt: F von endlichem Charakter $\iff$ G von coendlichem Charakter.

Lemma ((Teichmüller-)Tukey (TuL))**.** *Ist S eine Menge, und $F \subseteq \mathbb{P}(S)$, so gilt: $F \neq \emptyset \wedge F$ von endlichem Charakter $\rightarrow$ F hat maximales Element.*

Definition. Wieder sei X dcpo. $F \subseteq X$ *abgeschlossen*, wenn für jedes gerichtete $D \subseteq X$ gilt: $\underbrace{D \subseteq F}_{\forall_{x \in X}(x \in D \rightarrow x \in F)} \rightarrow \bigvee D \in F$. G *offen*, wenn für jedes gerichtete $D \subseteq X$ gilt: $\bigvee D \in G \rightarrow \underbrace{\exists_{x \in X}(x \in D \wedge x \in G)}_{D \cap G \neq 0}$ $(X = F \dot\cup G \rightarrow F \text{ abg. } \iff G \text{ offen})$

Lemma. *Es sei $X = \mathbb{P}(S)$, $F, G \subseteq X$.*

(a) F von endlichem Charakter $\rightarrow$ F abgeschlossen.

(b) G von coendlichem Charakter $\rightarrow$ G offen.

Beweis. nur (a). Es sei $D \subseteq X$ gerichtet mit $D \subseteq F$. Zu Zeigen: $\bigcup D \in F$. Es sei $T = \bigcup D$ und $T_0 \subseteq T$, T_0 endl. Dazu gibt es endl. $D_0 \subseteq D$ mit $T_0 \subseteq \bigcup D_0$. Da D gerichtet ist, hat D_0 eine obere Schranke $R \in D$. Dann $T_0 \subseteq R \in F$, also $T_0 \in F$, da T_0 endl. und F von endl. Charakter. $\square$

Definition. Sei X wieder ein dcpo, $G \subseteq X$. G progressiv, wenn $\forall_{x \in X} [\forall_{y > x} (y \in G) \rightarrow x \in G$

Definition (Offene Induktion (OI))**.** Ist X ein dcpo und $G \subseteq X$ offen, so gilt: G progressiv $\to G = X$, d.h.

$$\forall_x[\forall_{y>x}(y \in G) \to x \in G] \to \forall_{x \in X}(x \in G)$$

OI ist TI für offene $G \subseteq X$ mit X dcpo.

Definition (Tukey-Induktion (TuI))**.** Ist S Menge, $G \subseteq \mathbb{P}(S)$, so gilt: G von coendl. Charakter $\wedge$ G progressiv $\to G = \mathbb{P}(S)$

Satz. *(a)* ZL $\iff$ OI

(b) TuL $\iff$ TuI

Beweis. Nur (a). X dcpo, $X = F \dot\cup G$, dann: $F = \emptyset \iff G = X$, F abgeschlossen $\iff$ G offen; F hat kein max. El. $\iff$ G progressiv.
ZL für X auch als: $S \subseteq X$ abgeschlossen, hat kein maximales Element $\to S = \emptyset$. OI für X: $G \subseteq X$ offen, progressiv $\to G = X$. □

Allgemeine Abhängigkeit

Definition. Es sei S eine Menge, sowie $\lhd \subseteq S \times \mathbb{P}(S)$. Stets seien $a, b, c \in S$ und $U, V, W \in S$. $\lhd$ *Überdeckung(srelation)*, wenn gelten:

- *Reflexivität*: $a \in U \to a \lhd U$
- *Transitivität*: $a \lhd U \wedge U \lhd V \to a \lhd V$

Wobei $U \lhd V$ steht für $\forall_{b \in U}(b \lhd V)$.

Bemerkung. *Eine Überdeckungsrelation ist das gleiche wie ein* Abschlußoperator $U \mapsto U^{\lhd}$ *auf* $\mathbb{P}(S)$*, mit den folgenden Axiomen:*

- Reflexivität*:* $U \subseteq U^{\lhd}$
- Transitivität*:* $U \subseteq V^{\lhd} \to U^{\lhd} \subseteq V^{\lhd}$

Korrespondenz $\lhd \leftrightsquigarrow \_^{\lhd}$*: Zu* $\lhd$ *definiere* $U^{\lhd} = \{a \in S : a \lhd U\}$*.* $a \lhd U \leftrightsquigarrow a \in U^{\lhd}$*.*
Alternatives Axiomensystem:

- *Reflexivität: wie oben.*
- *Monotonie:* $U \subseteq V \to U^{\lhd} \subseteq V^{\lhd}$
- *Idempotenz:* $U^{\lhd\lhd} \subseteq U^{\lhd}$*. (mit Refl. sogar =)*

[R+T → M; T→I; M+I→T]

Definition. Eine Überdeckungsrelation $\lhd$ heißt

- *unitär* oder *Schottsch*, wenn aus $a \lhd U$ folgt: $\exists_{b \in U}(a \lhd \{b\})$.
- *finitär* oder *Stonesch*, wenn aus $a \lhd U$ folgt: $\exists_{U_0 \subseteq U}(U_0 \text{ endlich} \wedge a \lhd U_0)$.

Eine finitäre Überdeckungsrelation $\lhd$ heißt *Abhängigkeitsrelation*, wenn $\lhd$ die *Abhängigkeitseigenschaft* hat, d.h. wenn für alle $a, b \in S$, $U \subseteq S$ gilt:

$$a \lhd U \cup \{b\} \to a \lhd U \vee b \lhd U \cup \{a\}$$

Ein $U \subseteq S$ heißt *($\lhd$-)abhängig*, wenn $\exists_{b \in U}(b \lhd U - \{b\})$.
U heißt *($\lhd$-)unabhängig*, wenn $\forall_{b \in U}(b \lhd U - \{b\}$.

Bemerkung. *U abhängig $\to U \neq \emptyset$; $\emptyset$ unabhängig.*

Beispiel. (a) S Menge; $a \lhd U \equiv a \in U$, d.h. $U^{\lhd} = U$; Dann $\lhd$ unitär und jedes $U \subseteq S$ ist unabhängig.

(b) S Vektorraum; $U^{\lhd} = (U)$ der von U erzeugte Untervektorraum. $\lhd$ unitär; "(un)abhängig" ist "linear (un)abhängig" (!)

(c) $R \subseteq S$ komm. Ringe; für $U \subseteq S$ sei $R[U]$ die *Ringadjunktion* von U an R in S, d.h.

$$R[U] = \bigcup_{n \geq 0} \{f(u_1, \ldots, u_n) \colon f \in R[X_1, \ldots, X_n]; u_1, \ldots, u_n \in U\}$$

$U^{\lhd} = \overline{R[U]}^S$ ganzer Abschluß von $R[U]$ in S, d.h. $a \lhd U \iff a^n = r_1 a^{n-1} + \ldots + r_{n-1}^a + r_n$ für geeignete $n \geq 1$; $r_1, \ldots, r_n \in R[U]$.

Dann: $\lhd$ finitäre Überdeckungsrelation. R, S Körper, $R(U)$ statt $R[U] \to \lhd$ Abhängigkeitsrelation und "$\lhd$-(un)abhängigkeit" ist "algebraisch (un)abhängig". Siehe B.L. van der Warden, (Moderne) Algebra I, §64.

Definition. Nun sei $\lhd$ wieder eine allgemeine Abhängigkeitsrelation. *U erzeugt S*, wenn $S \lhd U$, d.h. $\forall_{b \in S}(b \lhd U)$. *$U$ Basis*, wenn U unabhängig, und U erzeugt S.
In den Beispielen (b) und (c) ist eine Basis eine Vektorraumbasis bzw. eine Tanszendenzbasis. U ist *maximal unabhängig* genau dann, wenn jedes $V \subseteq S$ mit $V \supsetneq U$ abhängig ist (*), sowie U unabhängig ist.

Lemma. *U maximal unabhängig $\iff$ U Basis*

Beweis. "$\Rightarrow$" (gilt i.a. nicht für $\lhd$ nur Überdeckungsrelation): Zeige: (*) $\wedge$ $S \not\lhd U \to U$ abhängig. Nehme $b \in S$ mit $b \not\lhd U$. Speziell $b \notin U$, d.h. $U \subsetneq U \cup \{b\}$. Nach (*) ist $U \cup \{b\}$ abhängig, d.h. es gibt $a \in U \cup \{b\}$ mit $a \lhd (U \cup \{b\}) - \{a\}$. Sofort folgt $a \neq b$ $[a = b \to b \lhd U \ \lightning]$. Also $a \lhd (U - \{a\}) \cup \{b\}$. Nach Abhängigkeitseigenschaft ist dann $a \lhd U - \{a\}$, damit U abhängig, da ja $a \in U$ wegen $a \neq b$, oder $b \lhd (U - \{a\}) \cup \{a\}$, d.h. $b \lhd U$. $\lightning$.
"$\Leftarrow$": Nur zu Zeigen: (*). Ist $V \supsetneq U$, etwa $b \in V - U$, so ist $U - \{b\} = U$ und $b \lhd U$, also $b \lhd U - \{b\}$ und damit $b \lhd V - \{b\}$, also V abhängig. $\square$

Satz. *Zu jedem unabhängigen $U \subseteq S$ gibt es eine Basis W mit $W \supseteq U$.*

Beweis mit ZL. Verwende obiges Lemma. Es sei $G = E \cap F$, wobei $E = \{V \subseteq S \colon V \supseteq U\}$ und $F = \{V \subseteq S \colon V \text{unabhängig}\}$ ein maximales Element W von G ist die gewünschte Basis. Zu Zeigen: $G \neq \emptyset$ und G dcpo. Nun ist $U \in G$. Ist $D \subseteq G$ gerichtet, so ist $\bigcup D \in E$, da $D \neq \emptyset$, sowie $\bigcup D \in F$, da F abgeschlossen, da F von endl. Charakter (Lemma oben). □

Typische Anwendung V Vektorraum, $x \in V$. Dann gilt: $\forall_{\varphi in V^*}(\varphi(x) = 0) \to x = 0$.

Indirekter Beweis, mit ZL. Wäre $x \neq 0$, so wäre $U = \{x\}$ unabhängig, also gäbe es (Satz) eine Basis W von V mit $W \supseteq U$; d.h. $x \in W$ Definiere $\varphi \in V*$ durch $\varphi(x) = 1$ und $\varphi \restriction W - \{x\} = 0$. Dann $\varphi(x) \neq 0.\lightning$. □

stephan.kulla@campus.lmu.de sswunk@googlemail.com