From the Foundational Crisis of Mathematics to Explicit Mathematics

Gerhard Jäger

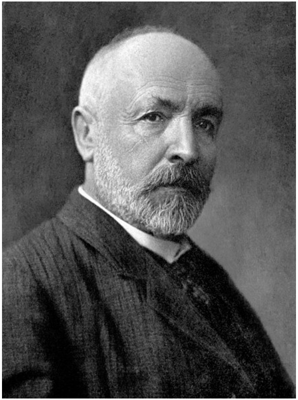
University of Bern

Bernays-Hilbert Summer School
Logic and Computation

Tübingen, July 2019

Part I

The Foundational Crisis of Mathematics



Georg Cantor (1845 – 1918)

How it all started:

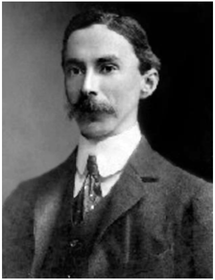
Unter einer "Menge" verstehen wir jede Zusammenfassung M von bestimmten wohlunterschiedenen Objekten m unserer Anschauung oder unseres Denkens (welche die Elemente von M genannt werden) zu einem Ganzen.

A set is a gathering together into a whole of definite, distinct objects of our perception or of our thought – which are called elements of the set.

Russell's paradox

Consider the set $R := \{x : x \notin x\}$

But then $R \in R$ if and only if $R \notin R$, a contradiction!



Bertrand Russell (1872 – 1970)

Russell's scientific oeuvre

- Logic and (foundations of) mathematics, type theory, Principia Mathematica (with A.N. Whitehead)
- One of the founders of Analytical Philosophy ("against Idealism")
- Historian (historical essays)
- Social critic, political activist, pacifist
- Nobel Prize in Literature, 1950 ("in recognition of his varied and significant writings in which he champions humanitarian ideals and freedom of thought")

First reactions to the inconsictency of Cantor's "definition":

- By Russell himself: Several type theories, e.g. ramfied type theory
- Many forms of axiomatic set theories', avoiding Russell's paradox by allowing only restricted forms of comprehension,
  - Zermelo-Fraenkel set theory ZF or ZFC,
  - von Neumann-Bernays-Gödel set theory NBG,
  - Morse-Kelley set theory MK.
- Systems of second or higher-order arithmetic.
- But (at least) two central questions remain:
  - How "safe" are these restriced formalisms?
  - What is a set?

Three traditional ways out of the crisis

- Hilbert's Proof Theory,
- Brouwer's Intuitionism,
- Predicativity à la Russell and Poincaré.

Hilbert's doctrine

Aus dem Paradies, das Cantor uns geschaffen, soll uns niemand vertreiben können. (Nobody should be able to drive us out of Paradise, the Cantor created us.)

David Hilbert (1862 – 1943)

Hilbert's "implicit definition" approach

In analogy to his successful approach to geometry in

Grundlagen der Geometrie (first published 1899)

Hilbert did not consider it necessary give an explicit definition of "set". Instead, he proposed to characterize sets implicitly via their characteristic properties and rules regulating their interplay.

Consequence: Set up an adequate axiomatic framework whose axioms reflect self-evident properties – according to our present working experience – of sets and/or numbers.

However, Hilbert did not claim that (this sort of) self-evidence guarantees consistency.

The program of proof theory (Beweistheorie)

The crucial steps

(1) The eventual aim is a formal system F in which all of mathematics (or at least those parts relevant for us) can be formalized, yielding "decidability" in the following sense: For every menaingful φ,

$$F \vdash \varphi \quad \text{or} \quad F \vdash \neg\varphi.$$

(2) Start off from a basic system F_0 that is justified by finite reasoning (some sort of finite combinatorics).

(3) And then try to develop a sequence of increasing systems

$$F_0, F_1, F_2, \ldots, F_k = F$$

such that F_i establishes the consistency of F_{i+1} *by finite methods*.

What was the ratioanle behind Hilbert's approach?

(1) Formulas and proofs can be coded as finite sequences (of natural numbers).

(2) Thus, by finite manipulations only, it should be possible to show that proofs of $(0 = 1)$ cannot exist.

A drawback

Gödel's results show that this program cannot work.

Modern proof theory

A new question

Given a fairly weak base theory B – like PRA or PA – and a strong system T. What amount *Inf* of "infinity" has to be added to B such that

$$B + \mathit{Inf} \quad \text{proves the consistency of} \quad T?$$

This leads to

- the notion of *proof-theoretic ordinal* of a formal system and the ordinal analysis of formal theories,
- classification of formal theories according to their proof-theoretic ordinals.

Brouwer's dogma

Mathematics is an essentially languageless mental activity, based on a philosophy of mind and leading to a form of constructive mathematics.

Luitzen Egbertus Jan Brouwer (1881 – 1966)

A non-constructive proof

Theorem

There are irrational numbers a and b such that a^b is rational.

Proof.

We know from school that $\sqrt{2}$ is irrational. Now we distinguish the following two cases:

(i) $\sqrt{2}^{\sqrt{2}}$ is rational. Then simply set $a := b := \sqrt{2}$.

(ii) $\sqrt{2}^{\sqrt{2}}$ is irrational. Then we set $a := \sqrt{2}^{\sqrt{2}}$ and $b := \sqrt{2}$ and observe:

$$a^b = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^{(\sqrt{2}\cdot\sqrt{2})} = \sqrt{2}^2 = 2.$$

This finishes the proof, but this argument does not tell us whether a is $\sqrt{2}$ or $\sqrt{2}^{\sqrt{2}}$. □

Constructive formal systems

Some characteristc properties of constructive systems

- Disjunction property:

$$\mathsf{CS} \ \vdash \ A \vee B \quad \Rightarrow \quad \mathsf{CS} \vdash A \ \text{ or } \ \mathsf{CS} \vdash B.$$

- Existence property:

$$\mathsf{CS} \ \vdash \ \exists x A[x] \quad \Rightarrow \quad \mathsf{CS} \vdash A[t] \ \text{ for some term } \ t.$$

- Constructive systems are based on intuitionistic logic (no “tertium non datur”).

Brouwer-Heyting-Kolmogorov interpretation (BHK) of IL

A proof of

- $\varphi_1 \wedge \varphi_2$ is a pair (π_1, π_2) where π_1 is a proof of φ_1 and π_2 is a proof of φ_2;
- $\varphi_1 \vee \varphi_2$ is a pair (i, π) where i is 0 and π is a proof of φ_1 or i is 1 and π is a proof of φ_2;
- $\varphi_1 \to \varphi_2$ is an operation f that converts any proof π of φ_1 into a proof $f(\pi)$ of φ_2;
- $\forall x \varphi[x]$ is an operation that converts any element a of the universe into a proof $f(a)$ of $\varphi[a]$;
- $\exists x \varphi[x]$ is a pair (a, π) where a is an element of the universe and π a proof of $\varphi[a]$.

The role of contradiction $\bot$

- There is a specific atomic formula $\bot$ that does not have a proof.
- $\neg\varphi$ is defined as $\varphi \rightarrow \bot$.
- Hence a proof of $\neg\varphi$ is an operation that transforms any hypothetical proof of φ into a proof of a contradiction.

Examples

- Consider the formula $\neg(P \wedge \neg P)$, i.e. $(P \wedge (P \rightarrow \bot)) \rightarrow \bot)$.
  A proof of this formula is an operation f that transforms a proof of $(P \wedge (P \rightarrow \bot))$ into a proof of $\bot$. Simply take

$$f((a, b)) \ := \ b(a).$$

- Consider the formula $P \vee \neg P$, i.e. $P \vee (P \rightarrow \bot)$.
  A proof of this formula is a pair (a, b) where

$$a = 0 \text{ and } b \text{ proof of } P \quad \text{or} \quad a = 1 \text{ and } b \text{ proof of } P \rightarrow \bot.$$

  Hence, if neither P nor $P \rightarrow \bot$ are provable, then $P \vee \neg P$ is not provable.

Part 2

Predicativity:
Russell – Poincaré – Weyl – Schütte – Feferman

The vicious circle principle (VCP)

A definition of an object S is impredicative if it refers to a totality to which S belongs.

A typical example: $S \;=\; \{\, n \in \mathbb{N} : (\forall X \subseteq \mathbb{N})\varphi[X, n] \,\}$

$$? : \quad m \in S \;\rightsquigarrow\; (\forall X \subseteq \mathbb{N})\varphi[X, m] \;\rightsquigarrow\; \varphi[S, m] \;\rightsquigarrow\; m \in S.$$

Russell and Poincaré (around 1901 – 1906), later also Weyl

- VPC is the essential source of inconsistencies.
- The structure of the natural numbers and the principle of induction on the natural numbers (for arbitrary properties) do not require foundational justification; further sets have to be introduced by purely predicative means.

Henri Poincaré (1854 – 1912)

Hermann Weyl (1885 – 1955)

Hermann Weyl: Das Kontinuum (1918)

Subtitle: Kritische Untersuchungen über die Grundlagen der Analysis

Weyl's foundational contributions

- Prior to 1918: Only one publication on the foundations of mathematics,

  Über die Definitionen der mathematischen Grundbegriffe,

  its central aim being to replace the vague idea of "defined property" by a precisely defined notion.

- 1918: *Das Kontinuum*.

- Not much later, Weyl became a convert to Brouwerian intuitionistic constructivism.

1. Independent of the classical versus intuitionistic question, Weyl always (from 1917 on) was critical of the Cantor-style set-theoretic foundations of mahematics:

   The set-theoretical foundations of mathematics are a house built to an essential extent on sand.

2. In *Das Kontinuum*:
   - The natural number system is a basic conception; proof and definition by induction are also basic.
   - All other mathematical concepts (sets and functions) have to be introduced by explicit definitions. There are no completed totalities.
   - Definitions which single out an object from a totality by reference to that totality are not permitted (Russell-Poincaré predicativity).
   - Statements formulated in terms of these notions have a definite truth value (true or false).

Feferman's formal reconstruction in Weyl vindicated: Das Kontinuum 70 years later

- $\mathsf{K}^{(\alpha)}$, basically ACA_0 with some additional syntactic sugar.
- $\mathsf{K}^{(\beta)}$, third-order extension of $\mathsf{K}^{(\alpha)}$.

Explicit function and relation definition.

- For every term $t[\vec{n}]$ there is a constant function symbol F such that $F(\vec{n}) = t[\vec{n}]$.
- For each function constant F there is a relation constant R such that $\forall \vec{n}(R(\vec{n}) \leftrightarrow F(\vec{n}) = 0)$.

Arithmetical comprehensions. For all arithmetical $\varphi[\vec{m}]$ and $\psi[\vec{m}, n]$,

$$\exists R \forall \vec{m}(R(\vec{m}) \leftrightarrow \varphi[\vec{m}]),$$

$$\forall \vec{m} \exists! n \, \psi[\vec{m}, n] \rightarrow \exists F \forall \vec{m}, n(F(\vec{m}) = n \leftrightarrow \psi[\vec{m}, n])$$

Number-valued recursion. For all function constants F and G, representing functions $F : \mathbb{N}^k \to \mathbb{N}$ and $G : \mathbb{N}^{k+2} \to \mathbb{N}$, respectively, there is a function constant $H := Rc_{\mathbb{N}}(F, G)$ representing the function $H : \mathbb{N}^{k+1} \to \mathbb{N}$ such that

$$H(0, \vec{m}) \;=\; F(\vec{m}) \quad \text{and} \quad H(n', \vec{m}) \;=\; G(n, \vec{m}, H(n, \vec{m})).$$

Set-valued recursion. For all function constants F and G, representing functions $F : \mathbb{N}^k \to P(\mathbb{N})$ and $G : \mathbb{N}^{k+1} \times P(\mathbb{N}) \to P(\mathbb{N})$, respectively, there is a function constant $H := Rc(F, G)$ representing the function $H : \mathbb{N}^{k+1} \to P(\mathbb{N})$ such that

$$H(0, \vec{m}) \;=\; F(\vec{m}) \quad \text{and} \quad H(n', \vec{m}) \;=\; G(n, \vec{m}, H(n, \vec{m})).$$

Theorem (Feferman)

$\mathsf{K}^{(\alpha)}$ *is a conservative extension of* PA.

Remarks:

- Quantification over relations and functions are to be excluded in defining conditions of relations and functions.
- Would Weyl have accepted full induction on $\mathbb{N}$? More restrictive than Russell-Poincaré predicativity.

Feferman's system W

A more flexible framwork for "implementing" Weyl's conceptual ideas.

Arithmetical Comprehension

Let $\mathcal{L}_2$ be the language of second order arithmetic with variables

$$x, y, z, \dots \quad \text{ranging over natural numbers,}$$
$$X, Y, Z, \dots \quad \text{ranging over sets of natural numbers}$$

and constants for all primitve recursive relations and functions. A formula is called *arithmetical* iff it does not quantify ovr sets of natural numbers.

The system ACA_0

- Arithmetical comprehension: For all arithmetical formulas $A[x]$,

$$\exists Y \forall x (x \in Y \leftrightarrow A[x]).$$

- Induction for sets:

$$\forall X (0 \in X \land (\forall y \in X)(y + 1 \in X) \to \forall y (y \in X)).$$

Predicative Hierarchies

Typical predicative definitions

Pick an arbitrary arithmetical formula $A[U, n]$ of second order arithmetic and consider the operation

$$Pow(\mathbb{N}) \ni \; S \;\longmapsto\; \{n \in \mathbb{N} : \mathbb{N} \models A[S, n]\} \;\in Pow(\mathbb{N}).$$

Now we will iterate this operation. To do so, some notation:

- Given a set $S \subseteq \mathbb{N}$ we write

$$m \in (S)_n \;:\Leftrightarrow\; \langle n, m \rangle \in S.$$

- Assume further that $\prec$ is a primitive recursive linear ordering whose field is $\mathbb{N}$ and such that 0 is its least element and $n \oplus 1$ the successor of n in $\prec$.

Now suppose that

$$(S)_0 = X,$$

$$(S)_{n \oplus 1} = \{m \in \mathbb{N} : \mathbb{N} \models A[(S)_n, m]\},$$

$$(S)_\ell = \text{disjoint union of } (S)_n \text{ with } n \prec \ell \text{ if } \ell \text{ limit.}$$

Then we write $\mathcal{H}_A[\prec, X, S]$ and call S an A-hierarchy, starting with X.

Question

For which linear orderings $\prec$ does this definition make sense?

Obvious answer: well-orderings.

But is this really so if one wants to build up sets from below?

Warning: The notion of well-ordering is impredicative!

Let $\prec$ be a (primitive recursive) linear ordering on $\mathbb{N}$ and X a subset of $\mathbb{N}$. $\prec$ is a well-ordering iff every non-empty subset of $\mathbb{N}$ has a least element,

$$WO[\prec] \;:\Leftrightarrow\; (\forall X \subseteq \mathbb{N})(X \neq \varnothing \;\rightarrow\; X \text{ has a } \prec\text{-least element}).$$

In this context also the following notions are used:

$$Prog[\prec, X] \;:\Leftrightarrow\; (\forall m \in \mathbb{N})((\forall n \prec m)(n \in X) \;\rightarrow\; (m \in X)),$$

$$Acc[\prec] \;:=\; \bigcap\{X \subseteq \mathbb{N} : Prog[\prec, X]\}$$

$$= \; \{n \in \mathbb{N} : (\forall X \subset \mathbb{N})(Prog[\prec, X] \;\rightarrow\; n \in X)\}.$$

Then: $\quad WO[\prec] \;\Leftrightarrow\; \mathbb{N} \subseteq Acc[\prec]$.

Central question in connection with such arithmetical hierarchies:

How far are we allowed to iterate?

Obviously, the approach of iterating predicative set formation along well-orderings involves in an essential way the impredicative notion of being a well-ordered relation, even if one restrictes oneself to recursive well-orderings.

The proof-theoretic shift

A step away from the semantic notion of well-ordered relation to predicatively provable well-orderings.

The proof-theoretic shift

Solomon Feferman (1928 – 2016))   Kurt Schütte (1909 – 1998)

Feferman and Schütte: The limit of predicativity

A boot-strap method

(i) We start off from a predicatively accepted ground theory, say ACA_0.

(ii) Then we systematically extend our framework: Whenever we have proved that a primitive recursive linear ordering is a well-ordering, we are allowed to iterate arithmetical comprehension along this well-ordering and to carry through bar induction along this well-ordering.

Originally done by Feferman and Schütte in the context of systems of ramified analysis or/and progressions of theories.

More modern terminology: the theory $AUT(\Pi^0_\infty)$

Recall that for any formula $B[n]$ of second order arithmetic,

$$TI[\prec, B] \;:\Leftrightarrow\; Prog[\prec, B] \to \forall n B[n].$$

$$AUT(\Pi^0_\infty) \;:=\; \mathrm{ACA}_0 + \frac{WO[\prec]}{\forall X \exists Y\, \mathcal{H}_A[\prec, X, Y]} + \frac{WO[\prec]}{TI[\prec, B]},$$

where $\prec$ is a primitive recursive linear ordering, $A[U, n]$ an arithmetical formula, and $B[n]$ an arbitrary formula.

What is the proof-theoretic strength of $AUT(\Pi^0_\infty)$?

Measuring the proof-theoretic strength of a theory

Proof-theoretic ordinal

(1) The ordinal α is *provable in the theory* T iff there exists a primitive-recursive well-ordering $\prec$ of order-type α such that $T \vdash WO[\prec]$.

(2) The *proof-theoretic ordinal of* T is the least ordinal that is not provable in T; it is often denoted by $|T|$.

Every formal theory has a countable proof-theoretic ordinal. The proof-theoretic ordinals provide a linear ordering of formal systems.

The Veblen functions φ_α

Definition

- $H \;:=\; \{\omega^\xi : \xi \in \mathit{On}\}$ the class of *additive principal numbers*;
- $\mathit{Cr}(\alpha) \;:=\; \{\beta \in H : (\forall \xi < \alpha)(\varphi_\xi(\beta) = \beta)\}$;
- $\varphi_\alpha : \mathit{On} \to \mathit{On}$ enumerates the set $\mathit{Cr}(\alpha)$.

Clearly,

$$\varphi_0(\alpha) \;=\; \omega^\alpha,$$

$$\varphi_1(\alpha) \;=\; \varepsilon_\alpha \;\; \text{(fixed points of } \lambda\xi.\omega^\xi\text{)}.$$

Some properties of thes functions

1. $\varphi_{\alpha_1}(\beta_1) < \varphi_{\alpha_2}(\beta_2)$ iff one of the following:
   (i) $\alpha_1 < \alpha_2$ and $\beta_1 < \varphi_{\alpha_2}(\beta_2)$,
   (ii) $\alpha_1 = \alpha_2$ and $\beta_1 < \beta_2$,
   (iii) $\alpha_2 < \alpha_1$ and $\beta_2 < \varphi_{\alpha_1}(\beta_1)$.

2. $\alpha \leq \varphi_\alpha(0)$.

3. $\beta \leq \varphi_\alpha(\beta)$.

Convention: In the following we write $\varphi\alpha\beta$ for $\varphi_\alpha(\beta)$.

Definition

$$\Gamma_0 \ := \ \text{least } \alpha \text{ such that } \alpha = \varphi\alpha 0.$$

General assumption

- In the following we shall use a natural recursive well-ordering $\prec$ of the natural numbers for a segment of the (recursive) ordinals – based on the Veblen functions – which goes beyond Γ_0.
- To each α in the segment we have a number a in the field of $\prec$ whose order-type is α.
- We write $x \prec_a y$ for $x \prec y \wedge y \prec a$.

Definitionof an auxiliary theory

$$\Pi^0_\infty\text{-CA}_{<\alpha} \;:=\; \mathsf{ACA}_0 + WO[\prec_a] + \forall X \exists Y \mathcal{H}_A[\prec_a, X, Y],$$

where a is of order type smaller that α and $A[X, n]$ arithmetical.

Main Lemma

For all α and all b of order-type less than $\varphi\alpha 0$,

$$\Pi^0_\infty\text{-CA}_{<\alpha} \;\vdash\; WO[\prec_b].$$

Theorem (Lower bound)

$$\Gamma_0 \;\leq\; |AUT(\Pi^0_\infty)|.$$

Proof.

Consider the sequence $\alpha_0 := \omega$, $\alpha_1 := \varphi 10$, and and $\alpha_{n+1} := \varphi\alpha_n 0$ for $n \geq 1$. Then we have

$$\sup(\alpha_n : n \in \mathbb{N}) = \Gamma_0 \quad \text{and} \quad \Pi^0_\infty\text{-CA}_{<\alpha_n} \;\vdash\; WO[< \alpha_{n+1}],$$

yielding our assertion. □

Theorem (Upper bound)

Proof.

By cut elimination. □

Corollary

The proof-theoretic ordinal of $AUT(\Pi^0_\infty)$ *is the ordinal* Γ_0*, and* $L_{\Gamma_0} \cap Pow(\mathbb{N})$ *is its least standard model.*

Reverse Mathematics (Friedman, Simpson, et al.)

Five central subsystems of second order arithmetic – The Big Five

$$\mathsf{RCA}_0 \ - \ \mathsf{WKL}_0 \ - \ \mathsf{ACA}_0 \ - \ \mathsf{ATR}_0 \ - \ \Pi^1_1\text{-}\mathsf{CA}_0$$

The principle (ATR) of arithmetical transfinite recursion

$$\forall R(WO[R] \ \rightarrow \ \exists X \, \mathcal{H}_A[R, X]),$$

where $A[X, n]$ is an arbitrary arithmetical formula which may contain additional parameters.

$$\mathsf{ATR}_0 \ := \ \mathsf{ACA}_0 + (\mathsf{ATR})$$

Predicative reducibility of ATR_0

Theorem (Friedman, McAloon, Simpson, J)

1. *The proof-theoretic ordinal of* ATR_0 *is the ordinal* Γ_0.
2. ATR_0 *does not have a minimum* ω*-model or* β*-model, but HYP is the intersection of all* ω*-models of* ATR_0.
3. Γ_{ε_0} *is the proof-theoretic ordinal of*

$$\mathrm{ATR} \;:=\; \mathrm{ATR}_0 + \textit{induction on } \mathbb{N} \textit{ for all } \mathcal{L}_2 \textit{ formulas}$$

First consequences:

(1) $AUT(\Pi^0_\infty)$ and ATR_0 are proof-theoretically equivalent but conceptually very different.

(2) And is there a big conceptual difference between ATR_0 and ATR?

Equivalences

Fixed points of positive arithmetical clauses (AFP)

$$\exists X \forall n (n \in X \;\leftrightarrow\; A[X^+, n]),$$

where $A[X^+, n]$ is an arbitrary X-positive arithmetical formula which may contain additional parameters.

Comparability of well-orderings (CWO)

$$\forall X, Y\, (WO[X] \wedge WO[Y] \;\rightarrow\; (|X| \leq |Y| \vee |Y| \leq |X|))$$

Π^1_1 reduction (Π^1_1-Red)

$$\forall n (A[n] \rightarrow B[n]) \;\rightarrow\; \exists X (\{n : A[n]\} \subseteq X \subseteq \{n : B[n]\}),$$

where $A[n]$ and $B[n]$ are arbitrary Σ^1_1 and Π^1_1 formulas, respectively.

Theorem (Avigad, Friedman, Simpson)

(ATR), (AFP), (CWO), *and* (Π^1_1-Red) *are pairwise equivalent over* ACA_0.