Foundations of Mathematics.

- Does mathematics need foundations? (Not until 1900.)
- *Mathematical approach:* Work towards an axiom system of mathematics with purely mathematical means. (Hilbert's Programme). In its naïve interpretation crushed by Gödel's Incompleteness Theorem.
- *Extra-mathematical approach:* Use external arguments for axioms and rules: pragmatic, philosophical, sociological, (theological ?).
- Foundations of number theory: test case.

Sets are everything (1).

- Different areas of mathematics use different primitive notions: ordered pair, function, natural number, real number, transformation, *etc.*
- Set theory is able to incorporate all of these in one framework:
  - **Ordered Pair.** We define

    $$\langle x, y\rangle := \{\{x\}, \{x, y\}\}.$$

    (Kuratowski pair)
  - **Function.** A set f is called a function if there are sets X and Y such that $f \subseteq X \times Y$ and

    $$\forall x, y, y' \left(\langle x, y\rangle \in f \& \langle x, y'\rangle \in f \to y = y'\right).$$

Sets are everything (2).

- Set theory incorporates basic notions of mathematics:
  - **Natural Numbers.** We call a set X inductive if it contains $\varnothing$ and for each $x \in X$, we have $x \cup \{x\} \in X$. Assume that there is an inductive set. Then define $\mathbb{N}$ to be the intersection of all inductive sets.
  - **Rational Numbers.** We define

$$\mathbb{P} := \{0,1\} \times \mathbb{N} \times \mathbb{N}\backslash\{0\}, \text{ then}$$

$$\langle i,n,m\rangle \sim \langle j,k,\ell\rangle :\iff i = j \ \&\ n \cdot \ell = m \cdot k, \text{ and}$$

$$\mathbb{Q} := \mathbb{P}/\sim.$$

Sets are everything (3).

- Set theory incorporates basic notions of mathematics:
  - **Real Numbers.** Define an order on $\mathbb{Q}$ by

    $$\langle i, n, m \rangle \leq \langle j, k, \ell \rangle :\Longleftrightarrow \; i < j \vee (i = j \;\&\; n \cdot \ell \leq k \cdot m).$$

    A subset X of $\mathbb{Q}$ is called an initial segment if

    $$\forall x, y (x \in X \;\&\; y \leq x \rightarrow y \in X).$$

    Initial segments are linearly ordered by inclusion.
    We define $\mathbb{R}$ to be the set of initial segments of $\mathbb{Q}$.

These definitions implicitly used a lot of set theoretic assumptions.

Sets.

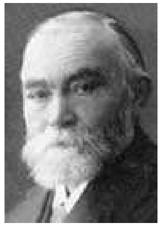
What is a set?

> *Eine Menge ist eine Zusammenfassung bestimmter, wohlunterschiedener Dinge unserer Anschauung oder unseres Denkens zu einem Ganzen.* (Cantor 1895)

The Full Comprehension Scheme. Let X be our universe of discourse (“the universe of sets”) and let Φ be any formula. Then the collection of those x such that $\Phi(x)$ holds is a set:

$$\{x\,;\,\Phi(x)\}.$$

Frege (1).



Gottlob Frege (1848-1925)

Frege's Comprehension Principle. If Φ is any formula, then there is some G such that

$$\forall x(G(x) \leftrightarrow \Phi(x)).$$

The ε operator. In Frege's system, we can assign to "concepts" F (second-order objects) a first-order object εF ("the extension of F").

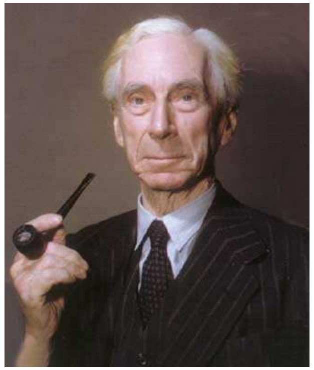
Frege (2).

Basic Law V. If F and G are concepts (second-order objects), then

$$\varepsilon F = \varepsilon G \quad \leftrightarrow \quad \forall x(F(x) \leftrightarrow G(x)).$$

Frege's Foundations of Arithmetic. Let F be an absurd concept ("round square"). Let G be the concept "being equinumerous to εF". We then define $\mathbf{0} := \varepsilon G$.
Suppose $\mathbf{0}$, ... , $\mathbf{n}$ are already defined. Then let H be the concept "being either $\mathbf{0}$ or ... or $\mathbf{n}$" and let $\overline{H}$ be the concept "being equinumerous to εH". Then let $\mathbf{n} + \mathbf{1} := \varepsilon \overline{H}$.

Russell (1).



Bertrand Arthur William
3rd Earl Russell (1872-1970)

- Grandson of John 1st Earl Russell (1792-1878); British prime minister (1846-1852 & 1865-1866).
- 1901: Russell discovers Russell's paradox.
- 1910-13: *Principia Mathematica* with Alfred North Whitehead (1861-1947).
- 1916: Dismissed from Trinity College for anti-war protests.
- 1918: Imprisoned for anti-war protests.
- 1940: Fired from City College New York.
- 1950: Nobel Prize for Literature.
- 1957: First Pugwash Conference.

Russell (2).

Frege's Comprehension Principle. Every formula defines a concept.
Basic Law V. If F and G are concepts, then $\varepsilon F = \varepsilon G \leftrightarrow \forall x(F(x) \leftrightarrow G(x))$.

Theorem (Russell). Basic Law V and the Full Comprehension Principle together are inconsistent.

Proof. Let R be the concept "being the extension of a concept which you don't fall under", *i.e.*, the concept described by the formula

$$\Phi(x) \quad :\equiv \quad \exists F(x = \varepsilon F \ \wedge \ \neg F(x)).$$

This concept exists by **Comprehension**. Let $r := \varepsilon R$.
Either $R(r)$ or $\neg R(r)$:

1. If $R(r)$, then there is some F such that $r = \varepsilon F$ and $\neg F(r)$. Thus $\varepsilon F = \varepsilon R$, and by **Basic Law V**, we have that $F(r) \leftrightarrow R(r)$. But then $\neg R(r)$. Contradiction!
2. If $\neg R(r)$, then for all F such that $r = \varepsilon F$ we have $F(r)$. But R is one of these F, so $R(r)$. Contradiction!

q.e.d.

Russell (3).

Theorem (Russell). The Full Comprehension Principle cannot be an axiom of set theory.

Proof. Suppose the Full Comprehension Principle holds, *i.e.*, every formula Φ describes a set $\{x\,;\,\Phi(x)\}$. Take the formula $\Phi(x) :\equiv x \notin x$ and form the set $r := \{x\,;\,x \notin x\}$ ("the Russell class").
Either $r \in r$ or $r \notin r$.

1. If $r \in r$, then $\Phi(r)$, so $r \notin r$. Contradiction!
2. If $r \notin r$, then $\neg\Phi(r)$, so $\neg r \notin r$, *i.e.*, $r \in r$. Contradiction!

q.e.d.

Frege & Russell.

- Russell discovered the paradox in June 1901.
- Russell's Paradox was discovered independently by Zermelo (Letter to Husserl, dated April 16, 1902).

  B. **Rang**, W. **Thomas**, Zermelo's discovery of the "Russell paradox", **Historia Mathematica** 8 (1981), p. 15-22.

- Letter to Frege (June 16, 1902) with the paradox.
- Frege's reply (June 22, 1902):

  > "with the loss of my Rule V, not only the foundations of my arithmetic, but also the sole possible foundations of arithmetic, seem to vanish".

Attempts to resolve the paradoxes.

- **Theory of Types.**
  Russell (1903, “simple theory of types”; 1908, “ramified theory of types”). *Principia Mathematica*.
- **Axiomatization of Set Theory.**
  Zermelo (1908). Skolem/Fraenkel (1922). Von Neumann (1925). “Zermelo-Fraenkel set theory” $\mathbf{ZF}$.
- **Foundations of Mathematics.**
  Hilbert’s 2nd problem: *Consistency proof of arithmetic* (1900). Hilbert’s Programme (1920s).

The Axiomatization of Set Theory (1).

-  **Ernst Zermelo** (1871-1953).

  Zermelo Set Theory (1908) Z^-. Union Axiom, Pairing Axiom, *Aussonderungsaxiom* (Separation), Power Set Axiom, Axiom of Infinity.

  Zermelo Set Theory with Choice ZC^-. Axiom of Choice.

- **Hausdorff** (1908/1914). *Are there any regular limit cardinals?* "weakly inaccessible cardinals".

  > "The least among them has such an exorbitant magnitude that it will hardly be ever come into consideration for the usual purposes of set theory."

The Axiomatization of Set Theory (2).

- **1911-1913.** Paul Mahlo generalizes Hausdorff's questions in terms of fixed point phenomena ($\rightsquigarrow$ Mahlo cardinals).
-  

  Thoralf Skolem (1887-1963) Abraham Fraenkel (1891-1965)

  1922: *Ersetzungsaxiom* (Replacement) $\rightsquigarrow$ ZF^- and ZFC^-.
- **von Neumann** (1929): Axiom of Foundation $\rightsquigarrow$ Z, ZF and ZFC.

The Axiomatization of Set Theory (3).

- **Zermelo** (1930): ZFC doesn't solve Hausdorff's question (independently proved by Sierpiński and Tarski).
- **Question.** Does ZF prove AC?

Cardinals & Ordinals (1).

Cardinality. Two sets A and B are called equinumerous if there is a bijection $\pi : A \to B$. Equinumerosity is an equivalence relation. The cardinality of A is its equinumerosity equivalence class.

Ordinals. A linear order $\langle X, \leq \rangle$ is called a well-order if there is no infinite strictly descending chain, *i.e.*, a sequence

$$x_0 > x_1 > x_2 > ...$$

Examples. Finite linear orders, $\langle \mathbb{N}, \leq \rangle$.

Nonexamples. $\langle \mathbb{Z}, \leq \rangle$, $\langle \mathbb{Q}, \leq \rangle$, $\langle \mathbb{R}, \leq \rangle$.

Cardinals and Ordinals (2).

Important: If $\langle X, \leq \rangle$ is not a wellorder, that does not mean that the set X cannot be wellordered.

$$\begin{array}{cccccccc} & -1 & -2 & -3 & -4 & -5 & \ldots \\ & 0 & 1 & 2 & 3 & 4 & \ldots \\ \rightsquigarrow & 0 & -1 & 1 & -2 & 2 & \ldots \end{array}$$

$$z \sqsubseteq z^* :\leftrightarrow |z| < |z^*| \ \vee \ (|z| = |z^*| \,\&\, z \leq z^*)$$

There is an isomorphism between $\langle \mathbb{N}, \leq \rangle$ and $\langle \mathbb{Z}, \sqsubseteq \rangle$. The order $\langle \mathbb{Z}, \sqsubseteq \rangle$ is a wellorder, thus $\mathbb{Z}$ is wellorderable.
If $\mathbf{L}$ and $\mathbf{L}^*$ are wellorders then either $\mathbf{L}$ is orderisomorphic to an initial segment of $\mathbf{L}^*$ or vice versa.

Cardinals and Ordinals (3).

If $\mathbf{L}$ and $\mathbf{L}^*$ are wellorders then either $\mathbf{L}$ is orderisomorphic to an initial segment of $\mathbf{L}^*$ or vice versa.

The class of wellorders is wellordered by

$$\mathbf{L} \preccurlyeq \mathbf{L}^* \leftrightarrow \mathbf{L} \text{ is orderisomorphic to an initial segment of } \mathbf{L}^*.$$

Ordinals are the equivalence classes of orderisomorphism. We let Ord be the class of all ordinals.

Operations on ordinals (1).

If $\mathbf{L} = \langle L, \leq \rangle$ and $\mathbf{M} = \langle M, \sqsubseteq \rangle$ are linear orders, we can define their sum and product:

$\mathbf{L} \oplus \mathbf{M} := \langle L \dot{\cup} M, \preceq \rangle$ where $x \preceq y$ if

- $x \in L$ and $y \in M$, or
- $x, y \in L$ and $x \leq y$, or
- $x, y \in M$ and $x \sqsubseteq y$.

$\mathbf{L} \otimes \mathbf{M} := \langle L \times M, \preceq \rangle$ where $\langle x, y \rangle \preceq \langle x^*, y^* \rangle$ if

- $y \sqsubset y^*$, or
- $y = y^*$ and $x \leq x^*$.

Operations on ordinals (2).

Fact. $\mathbb{N} \oplus \mathbb{N}$ is isomorphic to $\mathbb{N} \otimes \mathbf{2}$.

Exercise. These operations are not commutative: there are linear orders such that $\mathbf{L} \oplus \mathbf{M}$ is not isomorphic to $\mathbf{M} \oplus \mathbf{L}$ and similarly for $\otimes$. (Exercise 38.)

Observation. If $\mathbf{L}$ and $\mathbf{M}$ are wellorders, then so are $\mathbf{L} \oplus \mathbf{M}$ and $\mathbf{L} \otimes \mathbf{M}$.

The Axiom of Choice (1).

The Axiom of Choice (AC). For every function f defined on some set X with the property that $f(x) \neq \varnothing$ for all x, there is a choice function F defined on X, such that

for all $x \in X$, we have $F(x) \in f(x)$.

- Implicitly used in Cantor's work.
- Isolated by Peano (1890) in Peano's Theorem on the existence of solutions of ordinary differential equations.
- **1904.** Zermelo's wellordering theorem.

The Axiom of Choice (2).

Question. Are all sets wellorderable?

Theorem (Zermelo's Wellordering Theorem). If AC holds, then all sets are wellorderable.