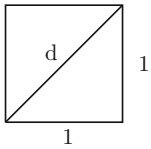
Appendix A
Proofs

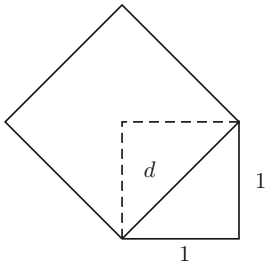
A.1 Irrationality of $\sqrt{2}$

There are many different proofs of irrationality of $\sqrt{2}$. The one that I will present here is due to the American mathematician Stanley Tennenbaum (1927–2005). It is a beautiful proof.

We need some preparation. Consider a unit square pictured below. The length of each side is 1. Let d be the length of the diagonal.

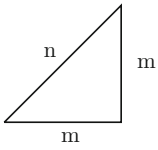


Now consider a d by d square positioned as in the picture below. The dashed lines show a right triangle. The smaller square can be cut into two such triangles, the larger one into four, which shows that the area of the larger square is 2. The larger square is twice larger than the smaller.



R. Kossak, *Mathematical Logic*, Springer Graduate Texts in Philosophy 3,
https://doi.org/10.1007/978-3-319-97298-5

Because the area of the larger square is 2, the length of its side d must be such that $d^2 = 2$. Hence, d is the square root of 2. The picture shows that d is a number between 1 and 2. One can ask if by choosing smaller units of length, one could measure the side of the square with exactly m such units, and the diagonal by exactly n units, where m and n are natural numbers.



If we could find such m and n, it would follow that n^2 is equal to twice m^2, i.e. $2m^2 = n^2$. Then, by dividing both sides by m^2 we would obtain that $2 = (\frac{n}{m})^2$, and that in turn would show that $\sqrt{2} = \frac{n}{m}$, proving that $\sqrt{2}$ is a rational number. Tennenbaum's proof shows that there can be no such m and n. The proof begins now.

Suppose that there is a number m, such that $2m^2$ is a square, i.e. $m^2 + m^2 = n^2$ for some natural number n. Let's see what this m could be.

- Could $m = 1$? No, $1^2 + 1^2 = 2$ is not a square.
- Could $m = 2$? No, $2^2 + 2^2 = 8$ is not a square.
- Could $m = 3$? No, $3^2 + 3^2 = 18$ is not a square.
- Could $m = 4$? No, $4^2 + 4^2 = 32$ is not a square.
- Could $m = 5$? No, $5^2 + 5^2 = 50$, close but not a square.

For $m = 2$ and $m = 5$ we almost succeeded, we missed a square by 1. It is encouraging, but instead of continuing, we will assume that we have found an m that works, and we will examine consequences.

In preparation, let us consider a similar case. It is well know that the sum of squares can be a square. It happens infinitely often. We will illustrate what is going on using pebbles in square boxes. For example, $3^2+4^2 = 5^2$. Fig. A.1, it shows how 9 pebbles and 16 pebbles are first arranged in two square boxes, and then rearranged into five rows with five pebbles in each row in a 5 by 5 square.

Now let rearrange the pebbles differently. In the 5 by 5 square let us place the 9 pebbles to form a square in its upper left corner, and then 16 pebbles to form a square in the lower right corner as in Fig. A.2.

Fig. A.1 $3^2 + 4^2 = 5^2$

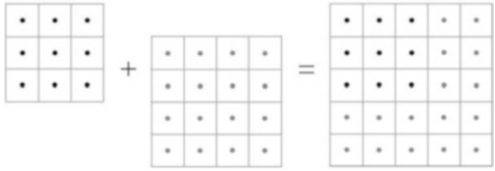


Fig. A.2 Squares rearranged

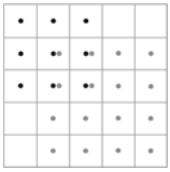


Fig. A.3 $m^2 + m^2 = n^2$

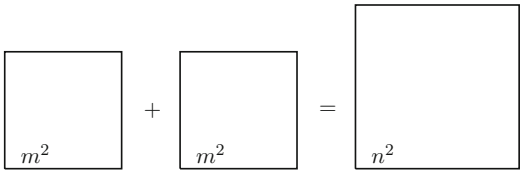
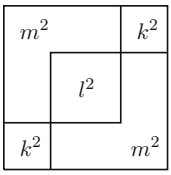


Fig. A.4 Rearranging $m^2 + m^2$



The squares overlap, and the number of doubly occupied slots is equal to the number of empty slots in the other two corners of the big square. It is clear that it is the case by inspecting the picture. For the rest of the proof, keep in mind that when the squares arranged the same fashion as in Fig. A.2, for each doubly occupied slot, there must be one that is left unoccupied.

Now we come back to Tennebaum's proof. Think about what would happen if instead of adding two squares of different sizes, we could add m^2 to m^2 and obtain a bigger square n^2 (Fig. A.3).

The picture will be similar to the one in Fig. A.2, but now since the smaller squares are of the same size, the picture is symmetric, as in Fig. A.4. The region over which the smaller squares overlap must consist of the same number of slots, as the two empty areas. Hence, if l is the length of each side of the square in the middle, and k is the length of each sides of the two smaller squares, then $k^2 + k^2 = l^2$.

Now comes the punch line. If there were a whole number m such that $m^2 + m^2$ is a square then, there would be a smallest such number m. Suppose that m is that smallest number. Then, the argument above shows that there is a smaller natural number k such that $k^2 + k^2 = l^2$, so $k^2 + k^2$ is a square, hence m could not have been the smallest such number, and that is a contradiction and it completes the proof. $\sqrt{2}$ is not rational.

A.2 Cantor's Theorem

In Chap. 5, we saw that the real line $\mathbb{R}$ is made of points that are ideal geometric places determined by the set of *all* Dedekind cuts in the rational numbers. Cantor proved that the collection of all such cuts cannot be obtained in a step-by-step process. In this section we will examine Cantor's argument.

We will show that for every step-by-step construction that at each step generates finitely many points on the real number line, there is always a point that is not generated by the construction. It follows that all of $\mathbb{R}$ cannot be generated step-by-step, or, in other words, that $\mathbb{R}$ is uncountable. We will consider an arbitrary process that in each step generates just one point. This is for notational convenience only, the argument below can be easily adjusted to any other step-by-step construction as long as at each step only a finite number of points in generated. When you read the proof below, it helps to draw pictures.

Let us consider a step-by-step process that generates points on the number line. For $a < b$, the interval $[a, b]$ is the set of all points between a and b, including the endpoints a and b. We will use the process to construct a sequence of intervals $[a_0, b_0]$, $[a_1, b_1]$, $[a_2, b_2]$, ..., each next interval contained in the previous one.

Let p_0, p_1, p_2,... be the sequence of points that our step-by-step process produces one by one. To begin our construction, we take any interval $[a_0, b_0]$ with rational endpoints, and select a rational point q that is different from p_0 and $a_0 < q < b_0$. Since p_0 is different from q, it can only be in one of the intervals $[a_0, q]$ and $[q, b_0]$. If it is not in the first interval, we let $[a_1, b_1]$, be $[a_0, q]$; otherwise we let it be $[q, b_0]$. So p_0 is not in $[a_1, b_1]$. In the second step, we select another rational q, this time different from p_1, such that $a_1 < q < b_1$. We consider intervals $[a_1, q]$ and $[q, b_1]$ and select as $[a_2, b_2]$ the one which does not contain p_1. So $[a_2, b_2]$ contains neither p_0 nor p_1. We continue in this fashion to obtain a nested sequence of nonempty intervals $[a_n, b_n]$ such that for each n, $[a_n, b_n]$ does not contain any of the points $p_0, p_1, \ldots, p_{n-1}$.

Now we add an additional twist to the selection of the points a_n and b_n: we want the distance between them to be smaller than $\frac{1}{n}$. This can be achieved by moving a_n closer to b_n, if a_n and b_n do not satisfy this additional condition already. For such modified sequence of intervals, let $D = \{p : p \in \mathbb{Q} \wedge \exists n\ (p \leq a_n)\}$. Then, D is a Dedekind cut that corresponds to a real number d. Since d belongs to all intervals $[a_n, b_n]$, it must be different from all points p_n, and this finishes the proof.

An interesting feature of this proof is that if the procedure that generates the sequence p_0, p_1, p_2,... is not just "given," but actually is an effective computational procedure, then from the proof we can extract an algorithm to compute the digits in the decimal expansion of the number d. In particular, since there is an effective procedure that lists all real algebraic numbers, we get an algorithm to construct a non-algebraic number.

A.3 Theories of Structures with Finite Domains

In Chap. 11, we noted that structures with finite domains that share the same first-order theories must be isomorphic. This may not be that surprising if one thinks of a structure with a finite number of relations. It seems reasonable that a finite amount of information suffices to describe what those relations on a finite domain look like. The proof that is given below is interesting because it does not attempt to show how a finite structure can be completely described by its first-order properties. It is a proof by contradiction, and it works for an arbitrary number of relations.

Theorem A.1 *Let $\mathfrak{A}$ and $\mathfrak{B}$ be structures with finite domains for the same first-order language. If for every first-order sentence φ, φ is true in $\mathfrak{A}$ if and only if it is true in $\mathfrak{B}$, then $\mathfrak{A}$ and $\mathfrak{B}$ are isomorphic.*

Proof Suppose, to the contrary, that $\mathfrak{A}$ and $\mathfrak{B}$ satisfy the assumptions of the theorem, but are not isomorphic. Let A be the domain of $\mathfrak{A}$ and let B be the domain of $\mathfrak{B}$. Let n be the size of A. Since the fact that A has n elements is expressible by a first-order sentence, B must also have n elements.

Because we assumed that $\mathfrak{A}$ and $\mathfrak{B}$ are not isomorphic, none of the functions $f : A \longrightarrow B$ is an isomorphism. There are only finitely many such functions: f_1, f_2, f_3, ..., f_m.[1] Also let $a_1, a_2, \ldots, a_n$ be a list of all elements of A.

Because none of the functions f_i, for $1 \leq i \leq n$ is an isomorphism, for each such i there is a formula $\varphi_i(x_1, x_2, \ldots, x_n)$ such that

$$\varphi_i(a_1, a_2, \ldots, a_n) \text{ holds in } \mathfrak{A},$$

but

$$\varphi_i(f(a_1), f(a_2), \ldots, f(a_n)) \text{ does not hold in } \mathfrak{B}.$$

Now, consider the following sentence φ

$$\exists x_1 \exists x_2 \ldots \exists x_n \, [\varphi_1(x_1, x_2, \ldots, x_n) \wedge \varphi_2(x_1, x_2, \ldots, x_n) \wedge \ldots \wedge \varphi_m(x_1, x_2, \ldots, x_n)].$$

The formulas $\varphi_i(x_1, x_2, \ldots, x_n)$ were chosen so that all the conjuncts in φ hold when interpreted by $a_1, a_2, \ldots, a_n$; hence, φ holds in $\mathfrak{A}$. It remains to show that φ does not hold in $\mathfrak{B}$. If it did, it would have been witnessed by a sequence of elements $b_1, b_2, \ldots, b_n$, but then the function $f : A \longrightarrow B$ defined by $f(a_i) = b_i$, for all i such that $1 \leq i \leq n$ is one of the functions $f_j : A \longrightarrow B$ that we have considered, and it follows that $\varphi_j(b_1, b_2, \ldots, b_n)$ does not hold in $\mathfrak{B}$, contradicting φ.

[1] $m = n^n$, but is not important for the argument.

A.4 Existence of Elementary Extensions

In this section we give a proof of the following theorem that played a big role in Chap. 11.

Theorem A.2 *Every structure with an infinite domain has a proper elementary extension.*

All details of the proof are spelled out in the following four paragraphs. It is a formal mathematical argument, but it is simple. The result is very powerful. In Chap. 11, we saw some of its consequences, and it is used in the next section in a proof of an important theorem in combinatorics. The power of the theorem is not in the simple argument below, it comes from the compactness theorem (Fig. A.5).

Let $\mathfrak{A}$ be a structure with an infinite domain A, and let $\overline{\mathfrak{A}}$ be its expansion obtained by adding names for all elements of the domain. We will add to the language one more constant that is not among the constants naming the elements of A. Let us call it c. We will consider a theory T in this expanded language. T consists of the complete theory of $\overline{\mathfrak{A}}$, $\mathrm{Th}(\overline{\mathfrak{A}})$, and the infinite set of sentences of the form $\neg(c = a)$, one for each element a of A. Notice that $\mathrm{Th}(\overline{\mathfrak{A}})$ includes the types of all finite sequences of the elements of A.

It is easy to see that every finite fragment of T has a model. Indeed, if T' is a finite set of sentences from T, then T' consists of a finite number of sentences $\varphi_1, \varphi_2, \ldots, \varphi_m$ that are true in $\overline{\mathfrak{A}}$, and a finite number of sentences of the form $\neg(c = a_1)$, $\neg(c = a_2), \ldots, \neg(c = a_n)$, for some $a_1, a_2, \ldots, a_n$ in the domain. We will show that T' has a model.

Since A is infinite, there is an element in A that is not among $a_1, a_2, \ldots, a_n$. Let us take such an element and interpret the constant c by it. Then all sentences in T' are true $(\overline{\mathfrak{A}}, c)$. We use here the fact that none of the sentences $\varphi_1, \varphi_2, \ldots, \varphi_m$ mentions c.

By the compactness theorem, T has a model. Let us call it $\mathfrak{B}$. All constants naming the elements of A, are interpreted as elements of the domain of $\mathfrak{B}$, and those interpretations are related to each other in $\mathfrak{B}$ exactly as they were in $\mathfrak{A}$, because all the information about those relations is included in T. Hence, $\mathfrak{B}$ contains an isomorphic copy of $\mathfrak{A}$, and in this sense it is an extension of $\mathfrak{A}$. Moreover, since T

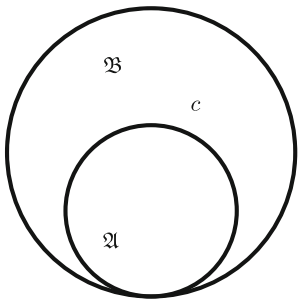


Fig. A.5 $\mathfrak{B}$ is a proper elementary extension of $\mathfrak{A}$ with a new element c

contains types of all finite sequences from A, $\mathfrak{B}$ is an elementary extension of $\mathfrak{A}$. Finally, because the constant c must be interpreted as an element outside the domain of $\mathfrak{A}$, $\mathfrak{B}$ is a proper extension. Its domain has at least one new element.

A.5 Ramsey's Theorem

If an infinite set is cut into a finite number of pieces, then at least one of those pieces must be infinite. How do we know that? This is a basic intuition concerning infinity. We cannot build an infinite set by putting together a finite number of finite sets. If each of the pieces is finite, then so is their union. This section is devoted to a proof of a similar, but harder to prove result. We need some definitions first.

For a set X, $[X]^2$ is the set of all unordered pairs of elements of X. For example, if $X = \{a, b\}$, then $[X]^2$ consists of only one pair $\{a, b\}$.

For a subset A of $[X]^2$, a subset H of X is *A-homogeneous* if either for all distinct a, and b in H, $\{a, b\}$ is in A, or for all distinct a and b in H, $\{a, b\}$ is not in A.

Theorem A.3 (Infinite Ramsey's Theorem for pairs) *Let X be a countably infinite set. For every subset A of $[X]^2$, there exists an infinite subset H of X that is A-homogeneous.*

Ramsey's theorem can be also formulated in term of graphs. Think of the infinite graph whose set of vertices is X, such that there is an edge between any two vertices. Suppose that each edge $\{a, b\}$ is colored either red or blue. Ramsey's theorem says that no matter how the coloring is done, there always will be an infinite set of vertices H such that either all edges $\{a, b\}$, with a and b in H are red, or all such edges are blue.

In another interpretation, think of A as the set of pairs of elements having a certain property. Ramsey's theorem says that for every property of pairs of elements, every infinite set has an infinite subset such that either all pairs from that subset have that property, or none of them have. We can identify each edge with the unordered pair of vertices it connects. This interpretation justifies the inclusion of the theorem in this book, as in this form the theorem is a stepping stone toward constructions of elementary extensions with non-trivial symmetries. The reason to include the proof below is that it illustrates the use of elementary extensions.

The usual proof of Ramsey's theorem is not hard, but is not elementary either. The proof given below is a little simpler than the one that is usually given in textbooks. The simplification is due to the use of Theorem A.2 from the previous section.

A set X is countably infinite if its elements can be enumerated using natural numbers. Thus, to prove the theorem we can assume that X is the set of natural

numbers $\mathbb{N}$.[2] The theorem is about sets of unordered pairs of natural numbers, but it will be convenient to represent them as the ordered pairs (m, n), where m is less than n.[3] With these conventions in mind we can now begin the proof .

Let a subset A of $[\mathbb{N}]^2$ be given. We will consider the structure $\mathfrak{N} = (\mathbb{N}, <, A)$ and its proper elementary extension $\mathfrak{N}^* = (\mathbb{N}^*, <^*, A^*)$. Notice that A and A^* are binary relations. Let c be an element of $\mathbb{N}^*$ that is not in $\mathbb{N}$. Because the extension is elementary, for every natural number n, $n <^* c$.[4]

Now we will define a sequence of natural numbers. Let $x_0 = 0$, and suppose that the sequence $x_0, x_1, \ldots, x_n$ has been defined so that $x_0 < x_1 < \cdots < x_n$, and for all $i < j \leq n$

$$(x_i, x_j) \in A \Longleftrightarrow (x_i, c) \in A^*$$

Our task now is to define x_{n+1}. The formula below says that there is an element v of $\mathbb{N}^*$ that behaves with respect $x_0, x_1, \ldots, x_n$ exactly as c does. It is obviously true in $\mathfrak{N}^*$, since c is such an element. To make the statement a bit shorter, we will use symbols ϵ_i, for each $i \leq n$, with the interpretation: if $(x_i, c) \in A^*$, then $\epsilon_i = \in$, otherwise $\epsilon_i = \notin$.

$$\exists v[x_n <^* v \wedge (x_0, v)\epsilon_0 A^* \wedge (x_1, v)\epsilon_1 A^* \cdots \wedge (x_n, v)\epsilon_n A^*]. \qquad (*)$$

Now comes the crucial part of the argument. Since $\mathfrak{N}^*$ is an elementary extension of $\mathfrak{N}$, there must be an element in $\mathbb{N}$ that has the property expressed by $(*)$ when A^* and $<^*$ are replaced with A and $<$, respectively. We define x_{n+1} to be a least such element.

Now imagine that the whole infinite sequence of the $x_0, x_1, x_2, \ldots$ has been constructed. Let $B = \{x_n : n \in \mathbb{N}\}$. The construction guarantees that for all x and y in B, if $x < y$, then (x, y) is in A if and only if $(x, c) \in A^*$. Let $H = \{x \in B : (x, c) \in A^*\}$ if this set is infinite, otherwise let $H = \{x \in B : (x, c) \notin A^*\}$. Then, H has the required property: either for all x in H the pair (x, c) is in A^*, and then for all x and y in H, such that $x < y$, (x, y) is in A; or for all x in H, (x, c) is not in A^*, hence for all x and y in H, such that $x < y$, (x, y) is not in A. This finishes the proof.

[2] If $X = \{x_0, x_1, x_2 \ldots\}$ is an enumeration of X, then Ramsey's Theorem for X is a straightforward consequence of Ramsey's Theorem for the set of indices $\{0, 1, 2 \ldots\}$.

[3] Since $\{m, n\} = \{n, m\}$ we can identify each unordered pair with the ordered pair in which $m < n$.

[4] An argument showing this is given in Sect. 12.1.

A.5.1 A Stronger Version of Ramsey's Theorem

The use of an elementary extension and the "infinite" element c in it made the proof of Ramsey's theorem a bit more streamlined than the usual combinatorial proof, but it comes at a price. The proof shows that there must exist a set H with the required properties, but it not telling us much more about this set. That is because we do not have sufficient information about A^* and the "infinte" element c that are used to define the homogeneous set H. The definition of H given in the proof is not a first-order definition in $(\mathbb{N}, <, A)$. It is a set-theoretic definition that refers to the inductively defined infinite sequence $x_0, x_1, x_2, \ldots$. The proof tells us that an infinite homogeneous set exists for any set of pairs A, but we don't know how complex H is in comparison to A. However, there is another similar proof that provides more information.

In Theorem A.3, let us assume in addition that the set A is first-order definable in $(\mathbb{N}, +, \cdot)$. For such an A, we can show that there is a homogeneous set H that is also first-order definable in $(\mathbb{N}, +, \cdot)$. To prove that, instead of an elementary extension $(\mathbb{N}^*, <^*, A^*)$, we can use an elementary extension of the richer structure $(\mathbb{N}^*, +^*, \cdot^*)$. It is not necessary to include A, and $<$ explicitly, since $<$ definable and we assume that A is definable as well. To reach the stronger conclusion, we can now use a stronger version of Theorem A.2. The arithmetic structure $(\mathbb{N}, +, \cdot)$ not only has a proper elementary extension, as any other structure with infinite domain has. It also has a *conservative* elementary extension, i.e. an extension $(\mathbb{N}^*, +^*, \cdot^*)$ such that for each set X^* that is parametrically definable in $(\mathbb{N}^*, +^*, \cdot^*)$, the intersection of X^* with $\mathbb{N}$ is definable in $(\mathbb{N}, +, \cdot)$.[5] If we use such a conservative extension, then one can show[6] that the set H, that we defied in the proof is extended to a set H^* that is defined in $(\mathbb{N}^*, +^*, \cdot^*)$ using the parameter c, so that H is the intersection of H^* with $\mathbb{N}$. It follows that H is definable in $(\mathbb{N}, +, \cdot)$.

[5] In $(\mathbb{N}, +, \cdot)$ all natural numbers are definable, hence every parametrically definable set is also definable without parameters.

[6] This part of the argument is routine, but a bit technical so we skip it.

Appendix B
Hilbert's Program

The general study of mathematical structures by means of formal logic is relatively new. The applications of logic that I described in his book were not the original motivation behind the developments in mathematical logic that led to first-order logic and related formal systems, but they turned out to be a very useful byproduct. Mathematicians study numbers and geometric figures, and come up with patterns and regularities. They deal with *proofs*, irrefutable arguments showing that such and such fact is true. What are those proofs based on? They are based on a *theory* that starts with basic, undeniable observations concerning numbers and geometric figures and then proceeds piling up results derived from previously established ones by logical deductions. That is a description of the kind of mathematics we learn about at school. Some mathematics nowadays is still like that, but most of it is not. While still rooted in classical numerical, geometric, and algebraic problems, modern mathematics, has evolved into an extremely diverse body of knowledge. The current official classification identifies 98 general mathematical subjects, each of which splits into a large number of more specialized subcategories. The names of the subjects will say very little to nonspecialists, and it is becoming harder and harder to have a clear picture of what all this is about. However, there is one distinctive feature that is present explicitly in most subjects, and that is an open and unrestricted use of arguments involving infinity. How does one *use* infinity? If you have studied calculus, you have seen examples of uses of infinity on almost every page the textbook. In fact, the whole idea of calculus is built on reasoning about infinite processes. But we do not need to refer to calculus to see the presence of infinity in mathematics.

Since $\sqrt{2}$ is not rational, it cannot be represented as a finite decimal, and, as shown in Sect. 5.5, it cannot be represented as an infinite repeating decimal. It is represented by an infinite non-repeating sequence of digits. Once we start thinking about it, all kinds of questions arise. In what sense do we say that $\sqrt{2}$ *is* an infinite sequence? How can we know anything about that entire sequence? How is one infinite sequence added to another sequence; how are such sequences multiplied?

R. Kossak, *Mathematical Logic*, Springer Graduate Texts in Philosophy 3,
https://doi.org/10.1007/978-3-319-97298-5

Mathematics provides very good answers, but working with infinite objects requires substantively more than just basic numerical and geometric intuitions. Where do our intuitions concerning infinity come from? All mathematical entities are abstract, but if we only talk about those that are finite (and not too large), we can still rely on our direct insight. We can argue about finite mathematical objects as we would about ordinary "real life" entities, and the results are usually precise and correct. It is not so when it comes to infinity. The history of mathematics is full of episodes showing how cavalier approaches to infinity lead to paradoxes and contradictions.

In the 1870s, Georg Cantor proved that the points filling a square can be put into a one-to-one correspondence with the points of one of its sides. In this sense, the *number* of points of the square is the same as the *number* of points of its side. In Cantor's time, the result was considered counterintuitive, as "clearly" two-dimensional objects (squares) are larger than one-dimensional ones (line segments).

Cantor's result is just a first step into the exploration of the vast world of infinite sets. Infinitistic methods proved useful in establishing mathematical results, but they were also a subject of criticism and concerns about their validity. In response to criticism, Hilbert proposed a program to prove once and for all that infinity, and set theory that deals with it, have a proper place in mathematics. Here is an outline of his program:

1. Define a system based on a formal language in which all mathematical statements can be expressed, and in which proofs of theorems can be carried out according to well-defined, strict rules of proof.
2. Show that the system is *complete*, i.e. all true mathematical statements can be proved in the formalism.
3. Show that the system is *consistent*, i.e. it is not possible to derive a statement and its negation. The proof of consistency should be carried out using finitistic means without appeal to the notion of actual infinity.
4. Show that the system is *conservative*, i.e. if a statement about concrete objects of mathematics, such as natural numbers or geometric figures, has a proof involving infinitistic methods, then it also has an elementary proof in which those methods are not used.
5. Show that the system is *decidable* by finding an algorithm for deciding the truth or falsity of any mathematical statement.

All elements of Hilbert's program had a tremendous impact on the development of the foundations of mathematics. Our main concern in this book was its first, initial stage—designing a system in which all of mathematics can be formalized. It is the part of the program that has been successfully completed in the first half of the twentieth century. At the beginning, a major candidate for the formal system to encompass all mathematics was the theory of types developed by Alfred North Whitehead and Bertrand Russell in *Principia Mathematica*. The elaborate system of Whitehead and Russell was later replaced by a combination of first-order logic, developed earlier by Gottlob Frege, and axiomatic set theory. The story of Hilbert's remaining desiderates is complex and interesting. First-order logic turned out to be complete, as was shown by Kurt Gödel in 1929; but in the following year

Gödel proved his celebrated incompleteness theorems which in effect caused the collapse of Hilbert's program. Gödel showed that for any consistent formal system that is strong enough there are statements about natural numbers that are true, but unprovable in the system. Hilbert's program collapsed, but it inspired a great body of research in foundations of mathematics, including all methods we discussed in this book. Of particular interest is the consistency problem.

If we argue informally, it is not unusual to come up with contradictory statements. A good example is Cantor's theorem stating that there is a one-to-one correspondence between the points of a square and the points of one of its sides. When Cantor proved his result, it was believed to be false, and in fact it was later proved to be false by L.E.J. Brouwer. How is that possible? How can one have proofs of two contradictory statements? The secret is that when nineteenth century mathematicians talked about one-to-one correspondences, they meant not arbitrary correspondences, but the continuous ones. Brouwer proved that there cannot be a continuous one-to-one correspondence between the points of a square and the points of its side, confirming the good intuition of the mathematicians who had thought that to be the case. Cantor's one-to-one correspondence was (and had to be) discontinuous. Contradictions in informal reasoning can arise from imprecise understanding of terms used. Once differences in terminology are clarified, contradictions should disappear. There is no guarantee that this will always happen, but at least this is how it has worked in practice so far.

In formal systems all terms are precisely defined upfront, and so are the rules of arguments (proofs). There is no room for ambiguity. There are many proof systems, but their common feature is that the rules of proof are mechanical. How do we design such systems, and how can we prove that inconsistencies will not be found in them? It was Hilbert's profound insight that formal statements and formal proofs are finite combinatorial objects and that one can argue about them mathematically. If there is no contradiction in a system (which we believe to be the case for the commonly used systems of mathematics today), this itself is an example of a mathematical statement that can be turned into a theorem once a proof is supplied. Hilbert believed that this could be done. His belief was shattered by Gödel's second incompleteness theorem which states that if a system is strong enough its consistency cannot be proved within the system. Formalized mathematics cannot prove its own consistency!

It was only a brief sketch, for a full account I strongly recommend Craig Smoryński's excellent book [32].

While Hilbert's program turned out untenable, its impact can not be overstated. Formalization of mathematics was crucial for the development of computer science and computer technology. We can talk to machines and they talk to us. We have a formal language to communicate. This is a success story, but in this book we have examined a different, and perhaps somewhat unexpected aspect of formalization. One could ask: Is there any point in learning a formal language if one is not interested in formalizing mathematical arguments or in talking to a machine? The answer is "yes," for several reasons. One is that formal methods play an important role in building and analyzing mathematical structures, and if you are interested in structures in general, those are good examples to consider. Secondly, when

expressed in a formal language, properties of structures become, as Hilbert wanted, mathematical objects. Each has its own internal structure. They can be classified according to various levels of complexity. They can be manipulated revealing meanings that may not be that transparent in an informal approach. Finally, the properties of elements of structures that are expressible by first-order formulas have a certain *geometric structure*. This geometry brings a kind of geometric thinking that can be applied in situations that do not seem to have much to do with traditionally understood geometry. Such geometrization has been effective in several areas of modern mathematics. For an account of these developments, see David Marker's entry on Logic and Model Theory in [23].

Bibliography

1. Badiou, A. (2010). *Being and event*. London/New York: Continuum.
2. Bagaria, J. Set theory. In E. N. Zalta (Ed.), *The Stanford encyclopedia of philosophy* (Winter 2017 ed.). https://plato.stanford.edu/archives/win2017/entries/set-theory/
3. Baldwin, J. T. (2017). *Model theory and the philosophy of mathematical practice: Formalization without foundationalism*. Cambridge: Cambridge University Press.
4. Button, T., & Walsh, S. (2018). *Philosophy and model theory* (With a historical appendix by Wilfrid Hodges). Oxford: Oxford University Press.
5. Beth, E. W. (1970). *Aspects of modern logic*. Dordecht/Holland: D. Reidel Publishing Company.
6. Borovik, A. (2014). English orthography as a metaphor for everything that goes wrong in mathematics education. *Selected Passages from Correspondence with Friends, 2*(2), 9–16.
7. DeLillo, D. (2016). *Zero K*. New York: Scribner.
8. Hacking, I. (2014) *Why is there philosophy of mathematics at all?* Cambridge: Cambridge University Press.
9. Hallett, M. Zermelo's axiomatization of set theory. In E. N. Zalta (Ed.), *The Stanford encyclopedia of philosophy* (Winter 2016 ed.). https://plato.stanford.edu/archives/win2016/entries/zermelo-set-theory/
10. Hardy, G. H. (1929). Mathematical proof. *Mind. A Quarterly Review of Psychology and Philosophy, 38*(149), 1–25.
11. Hilbert, D. (1926). Uber das Unendliche. *Mathematische Annalen, 95*, 161–190.
12. Dews, P. Review of *Being and Event* by Alain Badiou. *Notre Dame Phiosophical Reviews*. https://ndpr.nd.edu/news/being-and-event/
13. Hodges, W. Tarski's truth definitions. In E. N. Zalta (Ed.), *The Stanford encyclopedia of philosophy* (Fall 2014 ed.). http://plato.stanford.edu/archives/fall2014/entries/tarski-truth/
14. Hodges, W. Model theory. In E. N. Zalta (Ed.), *The Stanford encyclopedia of philosophy* (Fall 2013 ed.). https://plato.stanford.edu/archives/fall2013/entries/model-theory/
15. Hodges, W., & Scanlon, T. First-order model theory. In E. N. Zalta (Ed.), *The Stanford encyclopedia of philosophy* (Spring 2018 ed.). https://plato.stanford.edu/archives/spr2018/entries/modeltheory-fo/
16. Husserl, E. (2003). *Philosophy of arithmetic. Psychological and logical investigations—With supplementary texts from 1887–1901* (Edmund Husserl Collected Works, Vol. X, D. Willard, Trans.). Dordrecht/Boston: Kluwer Academic Publishers.
17. Grzegorczyk, A. (2013). *Outline of mathematical logic: Fundamental results and notions explained with all details*. New York: Springer.

R. Kossak, *Mathematical Logic*, Springer Graduate Texts in Philosophy 3,
https://doi.org/10.1007/978-3-319-97298-5

18. Kline, M. (1972). *Mathematical thought from ancient to modern times*. New York: Oxford University Press.
19. Knight, J. F., Pillay, A., & Steinhorn, C. (1986). Definable sets in ordered structures. II. *Transactions of the American Mathematical Society, 295*(2), 593–605.
20. Mancosu, P. (2012). *The adventure of reason. Interplay between philosophy of mathematics and mathematical logic: 1900–1940*. Oxford: Oxford University Press.
21. Mancosu, P. (2016). *Abstraction and infinity*. Oxford: Oxford University Press.
22. Marker, D. (2002). *Model theory: An introduction* (Graduate texts in mathematics, Vol. 217). New York: Springer.
23. Marker, D. (2008). Logic and model theory. In T. Gowers, J. Barrow-Green, & I. Leader (Eds.), *Princeton companion to mathematics*. Princeton: Princeton University Press.
24. Mostowski, A. (1969). *Constructible sets with applications*. Amsterdam: North Holland Publishing Company/Warszawa: Państwowe Wydawnictwo Naukowe.
25. Manin, Y. (2009). *A course in mathematical logic for mathematicians* (Graduate texts in mathematics, Vol. 53, 2nd ed., with Collboration by Boris Zilber). New York: Springer.
26. Mostowski, A. (1967). *Thirty years of foundational studies: Lectures on the development of mathematical logic and the study of the foundations of mathematics in 1930–1964* (Acta Philosophica Fennica, Vol. 17). Helsinki: Akateeminen Kirjakauppa.
27. Mostowski, A. (1979). *Foundational studies: Selected works*. North-Holland: Elsevier.
28. Peterzil, Y., & Starchenko S. (1996) Geometry, calculus and Zil'ber's conjecture. *Bulletin of Symbolic Logic, 2*(1), 72–83.
29. Reid, C. (1996). *Julia, a life in mathematics* (With Contributions by Lisl Gaal, Martin Davis and Yuri Matijasevich). Washington, DC: Mathematical Association of America.
30. Reid, C. (1996). *Hilbert*. New York: Springer.
31. Singh, S. (1997). *Fermat's last theorem*. London: Fourth Estate.
32. Smoryński, C. (2012) *Adventures in formalism*. London: College Publications.
33. Stillwell, J. (2018). *Reverse mathematics. Proofs from the inside out*. Princeton: Princeton University Press.
34. Tarski, A. (1933). The concept of truth in the languages of the deductive sciences (Polish). *Prace Towarzystwa Naukowego Warszawskiego, Wydział III Nauk Matematyczno-Fizycznych, 34*, Warsaw; expanded English translation in Tarski, A. (1983). *Logic, semantics, metamathematics, papers from 1923 to 1938*. Edited by John Corcoran. Indianapolis: Hackett Publishing Company.
35. Tarski, A. (1948). *A decision method for elementary algebra and geometry.* Santa Monica: RAND Corporation.
36. Van den Dries, L. (1998). *Tame topology and o-minimal structures*. New York: Cambridge University Press.
37. Wagon, S. (1985). *The Banach-Tarski paradox*. Cambridge: Cambridge University Press.
38. Wittgenstein, L. (1976). *Wittgenstein's lectures on the foundations of mathematics, Cambridge, 1939* (Edited by Cora Diamond). Chicago: The University of Chicago Press.
39. Zalamea, F. (2012). *Synthetic philosophy of contemporary mathematics*. Falmouth: Urbanomic/New York: Sequence Press.

Index

R. Kossak, *Mathematical Logic*, Springer Graduate Texts in Philosophy 3,
https://doi.org/10.1007/978-3-319-97298-5