A Reverse Mathematical Analysis of Hilbert's Nullstellensatz and Basis Theorem

Dhruv Kulshreshtha

May 3, 2024

An honors thesis submitted in partial fulfillment of the
requirements of the degree of Bachelor of Science with Honors

Department of Mathematics, University of Michigan
Ann Arbor, Michigan

Advised by Dr. Andreas Blass and Dr. Jamie Tappenden

Acknowledgements.

I extend my heartfelt appreciation to my advisors, Jamie Tappenden and Andreas Blass, for their unwavering support, invaluable feedback, and continuous encouragement. Their expertise and guidance have been indispensable in shaping my ideas and refining my work, and their anecdotes continue to serve as a source of inspiration. Their dedication to fostering intellectual curiosity has left a lasting impact on me, and I am truly fortunate to have had the opportunity to learn from them.

I would also like to extend my gratitude to Jeremy Avigad, John Baldwin, Matthew Harrison-Trainor, Dave Marker, Colin McLarty, Wilfried Sieg, Karen Smith, and Andrew Snowden for their feedback at various stages of this thesis. Their insights and suggestions have greatly enriched my understanding and helped me navigate through the challenges encountered along the way. I am deeply appreciative of their willingness to share their expertise and take the time to provide valuable input, which has undoubtedly contributed to the quality and depth of this work.

I am eternally grateful to Stephen DeBacker and Sarah Koch, who introduced me to the math community at Michigan through the Math Corps summer camp program, where I learnt the value of mathematics as a means to connect with our students and help them strive to realize their own greatness. I am also deeply indebted to Scott Schneider, whose invaluable mentorship and unwavering dedication towards his students have been instrumental in shaping my academic journey.

Furthermore, I want to extend my deepest gratitude to my friends, whose unwavering support and intellectual stimulation have been invaluable to me. I would especially like to thank Matthew Anderson, Rob Bakal, Hal Berdichesky, Thomas Chen, David Donze, Adam Earnst, Matt Fischer, Cam Haynes, Johnson He, Abby Hess, Kellen Kanarios, Drew Keisling, Horacio Moreno Montanes, Luke Miga, Max Natonson, Whit Thompson, and Jonah Weinbaum. Their presence in my life has not only provided constant encouragement but also served as a source of inspiration and camaraderie that I will forever cherish.

I am also grateful to Hanna Bennett, John Cantu, Ronnie Chen, Paul Kessenich, Jeff Lagarias, Aristotelis Panagiotopoulos, Martin Strauss, and Annie Winkler for their guidance, along with the Departments of Mathematics, Economics, and Philosophy, Society of Undergraduate Math Students, Math Undergraduate Office, Math Scholarships Committee, LSA Honors Program, Office of National Scholarships and Fellowships, Society for the

Advancement of Chicanos/Hispanics and Native Americans in Science, my Math Corps family, and my Math 297 and Math 201 students for their contributions and support throughout my academic journey. Their assistance and encouragement have played a significant role in my growth and development.

Finally, I want to express my heartfelt appreciation to my family for their love, encouragement, and understanding. Their support has been a constant source of strength and motivation, and I am deeply grateful for their unwavering commitment to my well-being and success.

Contents

1 Introduction

The Hilbert Basis Theorem, proven by David Hilbert in his seminal 1890 paper on invariant theory [Hil90], states that a polynomial ring in one variable – and thus, by induction, in finitely many variables – over a Noetherian[1] ring (see Definition 2.3) is itself Noetherian. In addition to its mathematical importance in commutative algebra and algebraic geometry, Hilbert's nonconstructive[2] proof is also of historical significance, representing a broader conscious[3] shift in mathematical thinking from computation to conception.

Before the more famous, long-lasting, and polarizing debate on Zermelo's Axiom of Choice, which Hilbert described as the axiom "most attacked up to the present in the mathematical literature" ([Hil26]; see [Moo82, Introduction]), the Basis Theorem had its very own controversy. Upon learning that Hilbert could prove that any ideal in the polynomial ring was finitely generated, yet could not explicitly write down its generators, Paul Gordan, then at the forefront of invariant theory, exclaimed "Das ist nicht Mathematik. Das ist Theologie," i.e. "This is not mathematics. This is theology." In fairness to Gordan, it is worth noting that he later became a major proponent and developer of Hilbert's ideas.[4]

Hilbert, however, was neither alone nor the first on the "conceptual" side of this debate: Riemann[5], in 1850s Göttingen, inaugurated this broader debate against the purely "computational" approach of mathematical argumentation associated with Kummer, Kronecker and Weierstrass, among other Berlin-mathematicians.[6] The turn of the century also saw several other math-

[1]Note that the Basis Theorem was formulated very differently in Hilbert's original paper. In particular, the now commonly-used terminology of "Noetherian" rings was first introduced by Chevalley in 1943 [Che43], after Noether's landmark 1921 paper [Noe21].

[2]We mean "nonconstructive" in the minimal sense, i.e. proving existence without the means to construct an example.

[3]See, for example, Hilbert's quote in [Hil98, Preface, p.X]: "I have tried to avoid Kummer's elaborate computational machinery so that here too Riemann's principle may be realized and the proofs compelled not by calculations but by thought alone."

[4]As with many thumbnail stories in the history of mathematics, the real situation is more complex and interesting: McLarty accounts for numerous perspectives on the interpretation of this remark, and provides a mathematical description of the nonconstructive content in the Basis Theorem, in [McL12].

[5]A key text for the development of the Riemannian style was his profound PhD thesis on the theory of complex functions [Rie51]. A brief overview of the thesis, setting it in context and charting its significance, is in [Lau99, Chapters 1.2 and 1.3].

[6]Notably, such conceptual argumentation can be traced even further back to Göttingen-

ematicians, such as Cantor and Dedekind – accompanied and supported[7] by Hilbert – drawing inspiration from the Riemannian style of thinking, and, as a result, facing opposition from those on the computational side.[8] Conceptual argumentation of this sort was even taken forward by Hilbert's collaborators and successors, including Emmy Noether – who was trained as a computational invariant theorist under Gordan, but eventually shifted to Hilbert-style methods of mathematical argumentation.

These remarks on the history of this computation/conception debate are relevant, at least spiritually, to this paper; and their relevance will hopefully become more clear to the reader once we begin formally analyzing how nonconstructive certain standard mathematical results are. What it means for a result to be more/less nonconstructive than another is addressed later in the introduction and formalized in Section 3. Furthermore, an explicit example involving the relative nonconstructive content in closely related results about algebraic closures will be given in Section 4.1, and analogous results in the case of real closures will be described in Section 4.4.

For now, we resume our historical discussion with the goal of introducing the second result in the title of this paper. Since a more thorough overview of the computation/conception debate is not directly within the scope of this paper, interested readers may refer to the following more detailed sources: Edwards provides historical context on the broader nineteenth-century shift toward conceptual argumentation in [Edw80]; Beeson also summarizes this shift in [Bee85, Historical Appendix]; Rowe provides a brief historical overview of the Berlin-Göttingen rivalry in [Row00]; Avigad, as mentioned in footnote 8, highlights Dedekind's emphasis on conceptual over algorithmic reasoning, in his development of the theory of ideals, opposing Kronecker's theory, in [Avi06]; and Tappenden provides an overview of Riemann's reorientation to-

mathematicians such as Dirichlet and Gauss (as highlighted in [AM14] and [Fer07]).

[7]Consider Hilbert's description of Cantor's new transfinite arithmetic: "the most astonishing product of mathematical thought, one of the most beautiful realizations of human activity in the domain of the purely intelligible" (see [Boy68, XXV] for details); and his description of [Ded88]: "This essay...is the most important first and profound attempt to ground elementary number theory" (see [Sie13, In.1 (Introduction)] for details).

[8]A particularly interesting rivalry is that between Kronecker and Dedekind, spanning many decades: See for example their attempts at extending Kummer's theory of ideal divisors in [Ded79] and [Kro82]; and the opposing methodologies in their works on the theory of numbers in [Ded88] and [Kro87]. The former is addressed in much detail in [Avi06] and the latter is summarized in [Sie13]. Cantor also faced much opposition from Kronecker on the matter of transfinite numbers – see [Car05] for details.

wards conceptual reasoning in [Tap06], and the contrast between the Riemannian and Weierstrassian approaches to elliptic functions and their generalisations in [Tap23]. Finally, this debate is also addressed in [Sie13], excellently summarized as: "At the heart of the difference between these foundational positions is the freedom of introducing abstract concepts – given by *structural definitions*" [Sie13, In.1 (Introduction)].

In 1893, Hilbert published his second paper on invariant theory [Hil93], in which he proved the Nullstellensatz[9], or zero-locus-theorem, which established a fundamental connection between the more algebraic notion of *ideals* and the more geometric notion of *varieties*. More specifically, ideals (see Definition 2.1) are more algebraic in the sense that they can be seen as generalizing the properties of prime numbers; and varieties (see Definition 2.6) are more geometric in the sense that "they are sets of points in space, generalizing geometric objects like circles, lines, and spheres, that are described by polynomial equations," as described by Karen Smith in an enlightening conversation.

One formulation of the Nullstellensatz goes as follows: Fix a field F, an algebraically closed field extension K of F, and an ideal $I \subseteq F[x_1, \ldots, x_n]$. If $p \in F[x_1, \ldots, x_n]$ vanishes on $\mathbb{V}(I)$ then $p^r \in I$ for some $r \in \mathbb{N}_{>0}$, where $\mathbb{V}(I)$ is the variety determined by I, defined in Definition 2.6. An immediate corollary of the Nullstellensatz is the so-called Weak Nullstellensatz which states that if $I \subseteq F[x_1, \ldots, x_n]$ is a proper ideal, then $\mathbb{V}(I) \neq \varnothing$, i.e. there exists a common zero for all the polynomials in the ideal in every algebraically closed extension of F. This may explain the name of the Nullstellensatz – which can be proven from the Weak Nullstellensatz using the Rabinowitsch trick [Rab30]: a simple, but clever algebraic trick that translates the weak version to the full version by a series of algebraic manipulations, following the introduction of an auxiliary variable. It is worth explicitly noting that since the Rabinowitsch trick boils down to simple algebraic manipulations, this transition is constructive.

Hilbert's first proof of the Nullstellensatz uses the Basis Theorem; however, the Nullstellensatz is seemingly more constructive, at least in its original formulation, than the Basis Theorem. Many authors have even explicitly highlighted the constructive nature of the Nullstellensatz – see, for example, [Arr06] and [Man05] – and the nonconstructive nature of the Basis Theorem

[9]The now commonly-used terminology of "Nullstellensatz" was first introduced by van der Waerden in 1926 [vdW26].

– see, for example, [Sim88a], [McL12] and [Ste23]. We formally describe this apparent difference in constructivity using the tools of *reverse mathematics.*

In Section 3, we introduce the research program of reverse mathematics, introduced by Harvey Friedman (see [Fri75]) – and developed by several others – with the goal of determining the minimal set-existence axioms that are needed to prove theorems of non-foundational mathematics (see Section 3.3). Using reverse mathematical techniques, one may argue about theorems of non-foundational mathematics[10] from a more foundational perspective. For example, one may prove that some such result is independent[11] of certain systems of mathematics; and one may even ask whether the minimal axioms that are necessary to prove the Heine-Borel Covering Lemma are also necessary/sufficient to prove the Bolzano-Weierstrass Theorem (see Theorem 3.9), and vice versa.

In particular, in Section 3, we introduce subsystems of second-order arithmetic[12], in increasing order of their relative strengths – which we can then use to formally argue the relative nonconstructive content in the aforementioned kinds of results. However, there are some non-trivial challenges in such an analysis of Hilbert's Nullstellensatz and Basis Theorem.

For example, in the reverse mathematical context, and more broadly, there have been numerous formulations of the Nullstellensatz.[13] In ZFC, these are all provable, hence provably equivalent. However, in weak subsystems of second-order arithmetic, equivalences, or even implications, among these formulations are not so clear.[14]

---

[10] As evidenced by numerous works in topological dynamics, combinatorics, measure theory, commutative algebra, and so on – see, for example [BHS87], [BS86], [BS93],[FH91], [FSS83], [Hir87], [KS89], [Sim88b], and [YS90].

[11] The logic community is not unfamiliar with independence proofs involving set-theoretic statements, like the famous results of Kurt Gödel and Paul Cohen ([Göd38] and [Coh63]; see [Kun80] for accessible proofs). Reverse mathematics, however, provides the machinery to argue the independence of results in, for example, measure theory or commutative algebra.

[12] For now, we will refer to some of these systems without explaining them. Note, however, that we are not presupposing any background knowledge in reverse mathematics from our readers, and will be defining these systems in Section 3.

[13] See, for example, [AM69, Chapter 7], [Eis95, Theorem 4.19], [FSS83, §2], [JL89, Chapter 1], [GCGR19, Theorem 1], [ST04, §1], [Sha13, §2.2], and [SKKT00, §2.3].

[14] In an insightful email conversation, John Baldwin mentioned that a standard formulation of Hilbert's Nullstellensatz is equivalent to the model completeness of ACF (the theory of algebraically closed fields), so it should be low in the (Friedman-Simpson) hierarchy (see Section 3). Furthermore, Matthew Harrison-Trainor mentioned that there could

In Sections 4.2 and 4.3, we describe some formulations of the Nullstellensatz and Basis Theorem, as coded in the reverse mathematics literature, along with where they fit in the Friedman-Simpson hierarchy. More specifically, in [FSS83] and [ST04], Friedman, et al. and Sakamoto and Tanaka show that certain formulations of the Nullstellensatz are provable in the subsystem RCA_0 of second-order arithmetic (see Section 4.2). On the other hand, in [Sim88a], Simpson shows that the Basis Theorem is not provable in RCA_0. Furthermore, it is a consequence of [Sim15, Theorem 2.2] that the Basis Theorem is provable in $\mathsf{RCA}_0 + \Sigma^0_2$-Induction (see Section 3), which provides an upper bound for its nonconstructive content – which, as we will see, comes from what one would expect to be a straightforward inductive argument.

Finally, in Section 4.4, we analyze analogous results to those in Section 4.1, in the context of real closures and formally real fields, and in Section 4.5, we analyze a formulation of the Nullstellensatz in this context.

2 Background: Commutative Algebra

We will presuppose familiarity with the basic definitions of abstract algebra (group, ring, field, etc.) as presented in standard textbooks such as [AM69] and [Eis95]. Henceforth, we use the term *ring* to mean a unital commutative ring, i.e. a ring with a multiplicative identity in which multiplication commutes.

Definition 2.1 (Ideal)**.** Given a ring R, an *ideal* I of R is a nonempty subset of R that satisfies the following

1. If $x \in I$ and $y \in I$, then $x - y \in I$.
2. If $x \in I$ and $a \in R$, then $ax \in I$.

Definition 2.2. Fix a ring R and an ideal $I \subseteq R$. I is said to be

1. *Proper*, if $I \subsetneq R$.

If, furthermore, I is a proper ideal of R, then I is said to be

be a difference of where Hilbert's Nullstellensatz would fit in the hierarchy depending on on whether it is coded using ideals, generators, or just subsets of the field. This remark highlights an important fact to remember: Reverse mathematical results may depend on the manner in which statements are formulated set-theoretically.

2. *Prime*, if for any $x, y \in R$, if $xy \in I$ then $x \in I$ or $y \in I$.

3. *Maximal*, if there is no proper ideal J of R such that $I \subsetneq J$.

Definition 2.3 (Noetherian Ring)**.** A ring R is said to be *Noetherian* if (any of) the following equivalent[15] conditions hold:

1. Every ideal in R is finitely generated.

2. Every non-empty set of ideals in R has a maximal element.

3. The ascending chain condition holds for ideals in R. That is, given ideals I_n in R such that for each n, $I_n \subseteq I_{n+1}$, then there is m such that for each $j \geqslant m$, $I_j = I_{j+1}$.

Theorem 2.4 (Basis Theorem [Hil90])**.** *If R is Noetherian, then so is $R[x]$, i.e. the one-variable polynomial ring over R.*

A standard proof of the Basis Theorem can be found in [Eis95, Theorem 1.2] and [AM69, Theorem 7.5]. The following consequence is the result of a straightforward (over ZFC, for example) inductive argument.[16]

Corollary 2.5. *If R is Noetherian, then so is $R[x_1, \ldots, x_n]$, i.e. the n-variable polynomial ring over R.*

Fix a field F, and an algebraically closed[17] field extension K of F.

Definition 2.6. Given $S \subseteq F[x_1, \ldots, x_n]$, define the *variety* determined by S, denoted $\mathbb{V}(S)$, to be the set of all common zeros of S, i.e.

$$\mathbb{V}(S) = \{\overline{x} \in K^n \mid \forall f \in S \ (f(\overline{x}) = 0)\}.$$

Then Hilbert's Nullstellensatz can be formulated as follows.

[15] These conditions are certainly equivalent over $\mathsf{ZF} + \mathsf{DC}$, where ZF is Zermelo-Fraenkel set theory (see any standard set theory textbook; for example, [End77, Chapter 2]), and DC is the principle of dependent choice (see, for example, [HR98, Form 43]).

[16] We will see in Section 4.3 that over weak subsystems of second-order arithmetic, this argument is not quite as straightforward as one would hope.

[17] Recall that field K is said to be *algebraically closed* if for any non-constant polynomial $h(x) \in K[x]$, there exists $c \in K$ such that $h(c) = 0$.

Theorem 2.7 (Nullstellensatz [Hil93])**.** *Let F and K be as above, and $I \subseteq F[x_1, \ldots, x_n]$ be an ideal. If $p \in F[x_1, \ldots, x_n]$ vanishes on $\mathbb{V}(I)$, i.e. $p(\overline{x}) = 0$ for every $\overline{x} \in \mathbb{V}(I)$, then $p^r \in I$ for some $r \in \mathbb{N}_{>0}$.*[18]

A standard algebraic proof of the Nullstellensatz (formulated slightly differently) can be found in [Eis95, Theorem 4.19]; and a standard model-theoretic proof can be found in [Mar10, Theorem 3.2.11].

An immediate corollary is the so-called Weak Nullstellensatz, which can be formulated as follows.

Corollary 2.8 (Weak Nullstellensatz)**.** *The ideal $I \subseteq F[x_1, \ldots, x_n]$ contains* 1 *if and only if the polynomials in I have no common zeros in K^n.*

An equivalent formulation states that if $I \subseteq F[x_1, \ldots, x_n]$ is a proper ideal, then $\mathbb{V}(I) \neq \varnothing$, i.e. there exists a common zero for all the polynomials in the ideal in every algebraically closed extension of F. As stated previously, the Nullstellensatz can be proven from the Weak Nullstellensatz using the Rabinowitsch trick [Rab30]. As remarked earlier, the Rabinowitsch trick boils down to simple algebraic manipulations; hence, this transition does not increase the non-constructive content.

3 Background: Reverse Mathematics

3.1 Second Order Arithmetic

The axiomatic system Z_2 of Second Order Arithmetic has the language $\mathcal{L}_2$, defined below.

Definition 3.1 ($\mathcal{L}_2$)**.** The language $\mathcal{L}_2$ of second-order arithmetic is a two-sorted language. This means that there are two distinct sorts of variables which are intended to range over two different kinds of objects. Variables of the first sort are known as *number variables*, are denoted by $k, m, n, \ldots$, and are intended to range over the set $\omega = \{0, 1, 2, \ldots\}$ of all natural numbers.[19] Variables of the second sort are known as *set variables*, are denoted by

[18] It is worth explicitly noting that if $I = \langle g_1, \ldots, g_k \rangle$, i.e. the ideal generated by (smallest ideal containing) $g_1, \ldots, g_k$, then $\mathbb{V}(I) = \mathbb{V}(\{g_1, \ldots, g_k\})$.

[19] Here, we use ω, rather than $\mathbb{N}$, to denote the set $\{0, 1, 2, \ldots\}$ of natural numbers because that is the more commonly used notation in logical/set-theoretic contexts. In

$X, Y, Z, \ldots$, and are intended to range over all subsets of ω. $\mathcal{L}_2$ has countably many set and number variables.

Numerical terms, intended to denote natural numbers, are number variables, the constant symbols 0 and 1, and $t_1 + t_2$ and $t_1 \cdot t_2$[20], whenever t_1 and t_2 are numerical terms. Here $+$ and $\cdot$ are binary operation symbols intended to denote addition and multiplication of natural numbers.

Atomic formulas are $t_1 = t_2$, $t_1 < t_2$, and $t_1 \in X$ where t_1 and t_2 are numerical terms and X is any set variable, and are intended to mean that t_1 equals t_2, t_1 is less than t_2, and t_1 is an element of X respectively.

Formulas are built up from atomic formulas by means of propositional connectives $\wedge, \vee, \neg, \rightarrow$ (and, or, not, if...then), and quantifiers $\forall$ and $\exists$ (representing the universal and existential quantifiers). There are, however, two sorts of each quantifier: *numerical quantifiers* (denoted $\forall n, \exists n$ with lower case variables) and *set quantifiers* (denoted $\forall X, \exists X$ with upper case variables).

The language $\mathcal{L}_1$ for First Order Arithmetic is just $\mathcal{L}_2$ without set quantifiers or set variables. An $\mathcal{L}_2$-formula is said to be *arithmetical* if it contains no set quantifiers, i.e. all the quantifiers appearing are number quantifiers.

Definition 3.2 (Z_2)**.** The axioms of Second Order Arithmetic (Z_2) are as follows:

1. Basic Axioms: For all natural numbers n, m,

    - $m + 1 \neq 0$
    - $m + 1 = n + 1 \rightarrow m = n$
    - $m + 0 = m$
    - $m + (n + 1) = (m + n) + 1$
    - $m \cdot 0 = 0$
    - $m \cdot (n + 1) = (m \cdot n) + m$

---

some cases, when we present algebraic results (such as Theorem 2.7) as they occur "in nature," so to speak, we use $\mathbb{N}$ to denote the set of natural numbers and $\mathbb{N}_{>0}$ to denote the set $\mathbb{N} \setminus \{0\}$. Finally, on some occasions (such as Theorem 3.19 and Lemma 4.15), ω is used (ambiguously) not to signify the set of natural numbers but rather the order type of the set of natural numbers ordered by the usual $<$ relation.

[20]Strictly speaking, these should be $(t_1 + t_2)$ and $(t_1 \cdot t_2)$ to avoid ambiguity in the order of operations, but we take such details for granted.

- $\neg(m < 0)$
- $m < n+1 \leftrightarrow (m < n) \vee (m = n)$

2. Induction Axiom: $\forall X[(0 \in X \wedge \forall n(n \in X \rightarrow n+1 \in X)) \rightarrow \forall n(n \in X)]$

3. Comprehension Scheme: $\exists X \forall n(n \in X \leftrightarrow \varphi(n))$ where $\varphi(n)$ is any $\mathcal{L}_2$-formula in which X doesn't occur freely.

It is a consequence of (2) and (3) that Z_2 implies the full second order induction scheme: For any $\mathcal{L}_2$-formula φ,

$$(\varphi(0) \wedge \forall n(\varphi(n) \rightarrow \varphi(n+1))) \rightarrow \forall n \varphi(n).$$

Definition 3.3 (Models of Z_2)**.** An $\mathcal{L}_2$-structure is an ordered 7-tuple

$$M = \langle |M|, \mathcal{S}_M, +_M, \cdot_M, <_M, 0_M, 1_M \rangle,$$

where $|M|$ is a set which serves as the domain of the number variables, $\mathcal{S}_M$ is a set of subsets of $|M|$ serving as the domain of the set variables, $+_M$ and $\cdot_M$ are binary operations on $|M|$, 0_M and 1_M are distinguished elements of $|M|$, and $<_M$ is a binary relation on $|M|$. We always assume that the sets $|M|$ and $\mathcal{S}_M$ are disjoint and nonempty. Formulas of $\mathcal{L}_2$ are interpreted in M in the obvious way. A *model* of Z_2 is an $\mathcal{L}_2$-structure that satisfies all the axioms in Definition 3.2.

For the purposes of this paper, the domain of numbers $|M|$, and the operations and relations $(+_M, \cdot_M, <_M)$, can be thought of as the usual operations of natural numbers (see ω-models in [Sim09, Chapter VIII]).

3.2 The Arithmetical and Analytical Hierarchies

Given a formula φ, a number variable[21] n is said to be *bound* in φ if every occurrence of n in φ is within the scope of a quantifier of n; and n is said to be *free* if it is not bound.[22] For example, in $\varphi(n) := \forall n(n+n=0)$, n is bound by the quantifier $\forall n$, and in $\psi(n,m) := \exists m(n+m=0)$, n is free.

Let t be a term that does not contain n. We abbreviate $\forall n(n < t \ \rightarrow \varphi)$ as $(\forall n < t)\varphi$ and $\exists n(n < t \ \wedge \varphi)$ as $(\exists n < t)\varphi$. The quantifiers $\forall n < t$ and $\exists n < t$ are called *bounded quantifiers*. A *bounded quantifier formula* is a formula whose quantifiers are all bounded number quantifiers.

[21]The notions of bound and free can all be defined analogously for set variables.
[22]A formula with no free variables is called a *sentence*.

Definition 3.4 (Arithmetical Hierarchy)**.** For $k \in \omega = \{0, 1, 2, \ldots\}$, an $\mathcal{L}_2$-formula φ is said to be Σ^0_k if it is of the form

$$\exists n_1 \forall n_2 \exists n_3 \cdots n_k \ \theta,$$

and an $\mathcal{L}_2$-formula φ is said to be Π^0_k if it is of the form

$$\forall n_1 \exists n_2 \forall n_3 \cdots n_k \ \theta,$$

where $n_1, \ldots, n_k$ are are number variables and θ is a bounded quantifier formula. An $\mathcal{L}_2$-formula is said to be *arithmetical*, if it is Σ^0_k or Π^0_k for some $k \in \omega$.

In both cases, φ consists of k alternating unbounded number quantifiers followed by a formula containing only bounded number quantifiers. In the Σ^0_k case, the first unbounded number quantifier is existential, while in the Π^0_k case it is universal (assuming $k \geqslant 1$). Thus for instance a Π^0_2 formula is of the form $\forall m \exists n \ \theta$, where θ is a bounded quantifier formula. A Σ^0_0 or Π^0_0 formula is the same thing as a bounded quantifier formula.

There is no need to include, in Definition 3.4, additional clauses covering the cases of multiple non-alternating quantifiers, such as $\exists n_1 \forall n_2 \forall n_3 \exists n_4 \ \theta$, since these will always be equivalent to formulas where all the unbounded quantifiers alternate. For example, $\exists n_1 \forall n_2 \forall n_3 \exists n_4 \ \theta$ is equivalent to

$$\exists n_1 \ \forall m \ \forall n_2 {<} m \ \forall n_3 {<} m \ \exists n_4 \ \theta,$$

which can easily be translated to a Σ^0_3 formula using a sequence coding function, as described in [Sho67, Chapter 6].

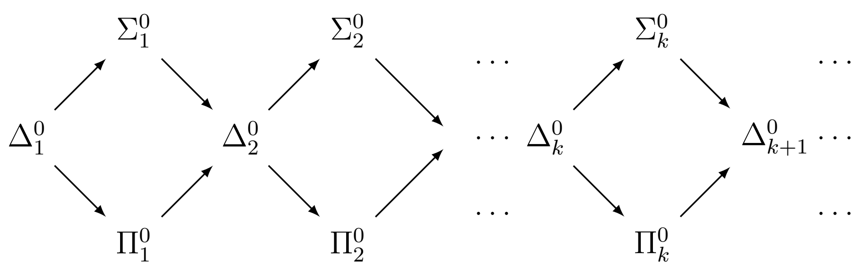
Clearly any Σ^0_k formula is logically equivalent to the negation of a Π^0_k formula, and vice versa. Moreover, up to logical equivalence of formulas, we have $\Sigma^0_k \cup \Pi^0_k \subseteq \Sigma^0_{k+1} \cap \Pi^0_{k+1}$ for each $k \in \omega$. We say an $\mathcal{L}_2$-formula φ is Δ^0_k if it is equivalent to both a Σ^0_k formula and a Π^0_k formula. We make the properties of this hierarchy more explicit as follows.

Proposition 3.5 (See Sections I.7 and IX.1 of [Sim09])**.** *The following hold (up to logical equivalence of formulas):*

1. $\Pi^0_k \subsetneq \Pi^0_{k+1}$ *and* $\Sigma^0_k \subsetneq \Sigma^0_{k+1}$*, for any* $k \in \omega$.
2. $\Delta^0_k \subsetneq \Sigma^0_k, \Pi^0_k$*, for any* $k \geqslant 1$.

3. $\Sigma^0_k \cup \Pi^0_k \subsetneq \Delta^0_{k+1}$*, for any* $k \geqslant 1$*.*

These results (for $k \geqslant 1$) can be summarized using the following figure, where the arrows indicate strict inclusions.



In parallel, the analytical hierarchy, which is the extension of the arithmetical hierarchy with set quantifiers, can be defined similarly. In this case, we quantify over sets of numbers and use arithmetical formulas in place of bounded quantifier formulas. We use 1 as a superscript instead of 0 to explicitly indicate the level of the hierarchy.[23] So for example, $\Delta^1_0 = \Sigma^1_0 = \Pi^1_0$ indicates the class of $\mathcal{L}_2$-formulas with number quantifiers but no set quantifiers. Furthermore, an $\mathcal{L}_2$-formula is Σ^1_1 if it logically equivalent to $\exists X\, \theta$, Π^1_1 if it logically equivalent to $\forall X\, \theta$, Σ^1_2 if it is logically equivalent to $\exists X\, \forall Y\, \theta$, Π^1_2 if it is logically equivalent to $\forall X\, \exists Y\, \theta$, and so on, where $\theta \in \Delta^1_0$.

3.3 Subsystems of Z_2

By a *subsystem* of Z_2, we mean a system of arithmetic with the basic axioms, i.e. 3.2(1), and restrictions of induction or comprehension, i.e. 3.2(2 and 3). For this section, and the rest of this paper, we use [Sim09] as a reference.

We describe the subsystems RCA_0, WKL_0, and ACA_0[24] of Z_2, which differ in their set existence axioms. Furthermore, RCA_0 is weaker than WKL_0 in terms of provability, which again is weaker than ACA_0 in this sense (see [Sim09, I.10.2]). That is,

$$\mathsf{RCA}_0 \vdash \varphi \implies \mathsf{WKL}_0 \vdash \varphi \implies \mathsf{ACA}_0 \vdash \varphi.$$

[23]One can also similarly define higher levels with quantification over sets of sets of numbers, sets of sets of sets of numbers, etc., reflected in the superscripts 2, 3, etc., but an understanding of the first two levels, with superscripts 0 and 1, is sufficient for the purposes of this paper.

[24]These subsystems are three of the “Big Five” subsystems of the Friedman-Simpson hierarchy – as described in [NS23].

Soon we will see that these implications are not reversible, hence RCA_0 is strictly weaker than WKL_0, which again is strictly weaker than ACA_0.

We first describe PRA, the formal system of primitive recursive arithmetic, which is viewed by many as a plausible explication of "finitistically acceptable reasoning" – see, for example, [Tai81][25] and [Sim88b]. In Section 3.4, we state a conservativity result, due to Harrington, for WKL_0 over PRA, which Simpson argues is a partial realization of *Hilbert's program* for the foundations of mathematics (see [Sim09, Remark IX.3.18]). However, whether or not this is Hilbert's conception is disputed. For example, Sieg argues that Simpson equating finitistic reduction to Hilbert's program is inaccurate; and that Kronecker's name would be more appropriate to attach to said reductionist program [Sie90]. In Section 3.4, we provide some additional context on Hilbert's program, and direct interested readers to more detailed sources.

Definition 3.6 (PRA)**.** The language of PRA is described in [Sim09, Definition IX.3.1]. With reference to Definition 3.1, it contains only number variables, number relations and operations from before, and symbols for each *basic primitive recursive function*: the constant zero function $Z(x) = 0$, the successor function $S(x) = x + 1$, and the projection functions $P_i^k(x_1, \ldots, x_k) = x_i$. It also codes a symbolization of all *primitive recursive functions*, which are built out of the basic functions using the composition and primitive recursion operators.

The *intended model* of PRA consists of the nonnegative integers $\omega = \{0, 1, 2, \ldots\}$, together with the primitive recursive functions, as defined above. The axioms of PRA, defined in [Sim09, Definition IX.3.2], include the usual axioms for equality, zero, the successor and projection functions, composition, and so on, along with the scheme of primitive recursive induction:

Primitive recursive induction

$$(\theta(0) \wedge \forall x\ (\theta(x) \to \theta(\underline{S}(x))) \to \forall x\ \theta(x),$$

where $\theta(x)$ is any quantifier-free formula in the language of PRA with a distinguished free number variable x.

We now describe RCA_0, which is, for all intents and purposes, our base system. More specifically, equivalences such as theorems 3.13 and 3.15 are

[25] "We shall see that there is no question but that [primitive recursive] reasoning is finitist" [Tai81].

considered over RCA_0, and algebraic definitions in, for example, Section 4 are made in RCA_0.

Definition 3.7 (RCA_0)**.** Along with the basic axioms, i.e. 3.2(1), RCA_0 allows for Δ^0_1-comprehension (also called recursive comprehension) and Σ^0_1-induction (equivalently Π^0_1-induction), i.e.

Recursive comprehension

$$\forall x\ (\varphi(x) \leftrightarrow \psi(x)) \rightarrow \exists X\ \forall x\ (x \in X \leftrightarrow \varphi(x)),$$

where φ is Σ^0_1, ψ is Π^0_1, and X is not free in either φ or ψ.

Σ^0_1-*Induction*

$$(\varphi(0) \wedge \forall x\ (\varphi(x) \rightarrow \varphi(x+1))) \rightarrow \forall x\ \varphi(x),$$

where φ is Σ^0_1 (or equivalently Π^0_1).[26]

The acronym RCA stands for Recursive Comprehension axiom, and the subscript 0 indicates that only the restricted induction schema, i.e. Σ^0_1-induction, is being assumed. One may also consider the system RCA, i.e. with the full first-order induction schema, i.e. Σ^0_n-induction. In [FSS83, Introduction], Friedman, et al. motivate why this is not necessary, especially in the algebraic context.

Two quantifier induction, i.e. Σ^0_2-induction or Π^0_2-induction, is not provable in RCA_0, and neither is Σ^0_1-comprehension.

We now list some ordinary mathematical results[27] that are, and aren't, provable in RCA_0. We reserve results in commutative algebra for a deeper analysis in Section 4.

Theorem 3.8 (See Theorem I.8.3 of [Sim09])**.** *The following are provable in* RCA_0.

1. *Baire Category Theorem: Let* $\{U_n : n \in \mathbb{N}\}$ *be a sequence of dense open sets in* $\mathbb{R}^k$*. Then there exists* $x \in \mathbb{R}^k$ *such that* $x \in U_n$ *for all* $n \in \mathbb{N}$.

2. *Intermediate Value Theorem: If* $f(x)$ *is continuous on the unit interval* $[0, 1]$*, and if* $f(0) < 0 < f(1)$*, then there exists* $x \in (0, 1)$ *such that* $f(x) = 0$.

[26] One could analogously define, for example, Σ^0_2-Induction by allowing φ to be Σ^0_2.
[27] Carrying these over to formal arithmetic requires some coding.

3. *Tietze Extension Theorem: Let X be a complete separable metric space. Given a closed set $C \subseteq X$ and a continuous function $f : C \to [-1, 1]$, there exists a continuous function $g : X \to [-1, 1]$ such that $g(x) = f(x)$ for all $x \in C$.*

4. *Weak version of Gödel's Completeness Theorem: Let $X \subseteq \mathsf{Snt}$[28] be consistent and closed under logical consequence. Then there exists a countable model M such that M satisfies φ, for all $\varphi \in X$.*

5. *Soundness Theorem: If $X \subseteq \mathsf{Snt}$ and there exists a countable model M such that M satisfies φ, for all $\varphi \in X$, then X is consistent.*

Theorem 3.9 (Theorems I.9.3 and I.10.3 of [Sim09])**.** *The following are not provable in* RCA_0

1. *The Heine-Borel Covering Lemma: Every covering of the closed interval $[0, 1]$ by a sequence of open intervals has a finite subcovering.*

2. *The Bolzano-Weierstrass Theorem: Every bounded sequence of real numbers, or points in $\mathbb{R}^n$, has a convergent subsequence.*

Both results in Theorem 3.9 are non-constructive, in the sense that they guarantee the existence of certain mathematical objects, without providing an explicit algorithm to find them. In particular, 3.9(1) states the existence of a finite subcovering and 3.9(2) the existence of a convergent subsequence, without giving the machinery to determine what these actually look like or how one could compute them.

It turns out that more can be said about their non-constructive content using the framework of reverse mathematics. More specifically, 3.9(1) is less non-constructive, i.e. more constructive, than 3.9(2), since the former is provably equivalent to WKL_0 (over RCA_0), and the latter is provably equivalent to the strictly stronger ACA_0 (over RCA_0).

[28]Formally, given a countable language $\mathcal{L}$, i.e. a countable set of set of relation, operation, and constant symbols, we identify terms and formulas with their Gödel numbers under a fixed Gödel numbering, which can be constructed by primitive recursion (see [Sim09, Theorem II.3.4]), using $\mathcal{L}$ as a parameter. We can prove in RCA_0 that there exists a set Snt consisting of all Gödel numbers of sentences.

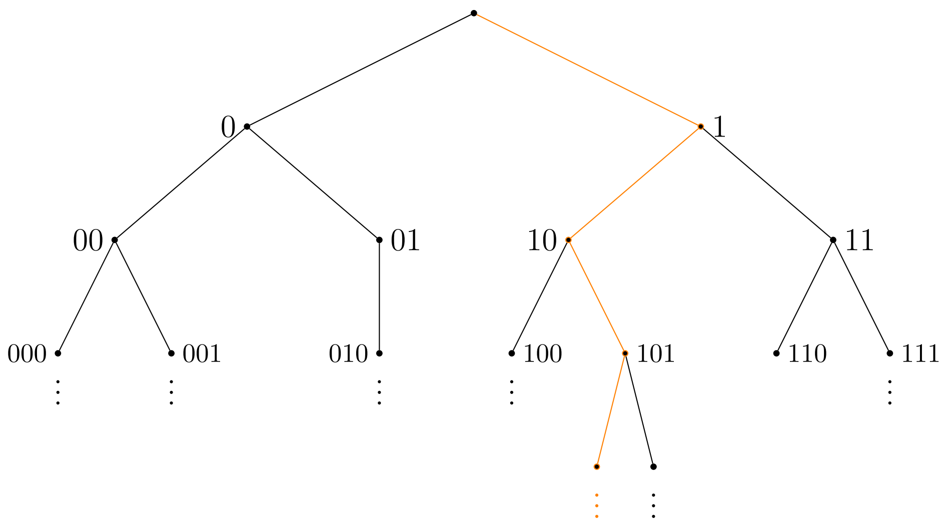


Figure 1: Binary Tree with path

Definition 3.10 (Binary Trees). Let $2^{<\mathbb{N}}$ (where we use the convention $2 = \{0, 1\}$) be the set of all finite sequences of 0's and 1's. A *binary tree* is a set $T \subseteq 2^{<\mathbb{N}}$ such that any initial segment of a sequence in T belongs to T. A *path*[29] through T is a function $f : \mathbb{N} \to 2$ such that for every $k \in \mathbb{N}$, $f[k] = (f(0), f(1), \ldots, f(k-1))$ belongs to T.[30]

Theorem 3.11 (Weak König's Lemma (WKL)). *Every infinite binary tree has a path.*

See Figure 1 for an example of a path (in orange) through a binary tree, as in Theorem 3.11.

Definition 3.12 (WKL_0). WKL_0 is RCA_0 together with WKL.

It is probably no surprise where the WKL acronym comes from. Furthermore, the subscript 0 once again indicates that only the restricted induction schema is being assumed.

[29] By "path," we always mean infinite path.

[30] More generally, we may define a finitely-branching tree as a set $T \subseteq \mathbb{N}^{<\mathbb{N}}$ such that each node has finitely many children and any initial segment of a sequence in T belongs to T. In this case, a path $f : \mathbb{N} \to \mathbb{N}$ is defined analogously.

A lot of ordinary mathematics can be done in WKL_0, as evidenced by the following theorem.[31]

Theorem 3.13. *[See Theorem I.10.3 of [Sim09]] The following are provably pairwise equivalent over* RCA_0*:*

1. WKL_0
2. *The Heine-Borel Covering Lemma: Every covering of the closed interval* $[0, 1]$ *by a (countable) sequence of open intervals has a finite subcovering.*
3. *Every continuous real-valued function on any compact metric space (see [Sim09, Definition III.2.3]) is bounded, has a supremum, and is uniformly continuous.*
4. *Every continuous real-valued function on* $[0, 1]$ *is Riemann integrable.*
5. *Lindenbaum Lemma: Every countable consistent set of sentences extends to a maximal such set.*
6. *Gödel's Completeness Theorem: Every countable consistent set of sentences has a countable model.*
7. *Gödel's Compactness Theorem: Given* $X \subseteq \mathsf{Snt}$ *(see footnote 28), if each finite subset of* X *has a model, then so does* X.
8. *Every countable ring has a prime ideal (see Definition 2.2).*
9. *Brouwer's fixed point theorem: Every continuous function* $f : [0, 1]^n \to [0, 1]^n$ *has a fixed point, i.e. a point* c *such that* $f(c) = c$.

There are still important mathematical results that WKL_0 is not strong enough to prove: for example the Bolzano-Weierstrass Theorem. So we now define ACA_0, which is a stronger (see [Sim09, I.10.2]) subsystem of Z_2 that is strong enough to prove some of these.

[31]Due to model-theoretic extension principles such as the Upwards Löwenheim-Skolem Theorem, the restriction to countable structures, e.g. countable rings, is not an actual limitation to the generality of these results. However, such machinery is outside the scope of subsystems of Z_2.

Definition 3.14 (ACA_0)**.** ACA_0 is RCA_0 together with arithmetical comprehension, i.e.

Arithmetical comprehension

$$\exists X\ \forall x\ (x \in X \leftrightarrow \varphi(x)),$$

where φ is Σ^0_n (or equivalently Π^0_n), for some n, and X does not occur freely in φ.

The acronym ACA stands for Arithmetical Comprehension axiom, and the subscript 0 serves the same purpose as before.

The following theorem motivates the relative strength of ACA_0 as compared to WKL_0. More specifically, since the following results are equivalent to ACA_0, they are not provable in WKL_0.

Theorem 3.15 (See Theorem I.9.3 of [Sim09])**.** *The following are provably pairwise equivalent over* RCA_0*:*

1. ACA_0
2. *Bolzano-Weierstrass Theorem: Every bounded sequence of real numbers, or points in* $\mathbb{R}^n$*, has a convergent subsequence.*
3. *Every Cauchy sequence of real numbers is convergent.*
4. *Every bounded sequence of real numbers has a least upper bound.*
5. *Monotone convergence theorem: Every bounded monotone sequence of real numbers is convergent.*
6. *Every sequence of points in a compact metric space has a convergent subsequence.*
7. *Every countable ring has a maximal ideal (see Definition 2.2).*
8. *Every countable vector space over any countable field has a basis.*
9. *Every countable field (of characteristic 0) has a transcendence basis.*
10. *Every countable Abelian group has a unique (up to isomorphism) divisible closure.*

11. König's Lemma: Every infinite, finitely branching tree has a path.

In theorems 3.13 and 3.15, we intentionally omit results pertaining to algebraic/real closures of fields. These will be covered in later sections, particularly 4.1 and 4.4.

3.4 Conservativity results and Hilbert's program

In subsequent sections, we study results involving the provability of algebraic results in certain subsystems of Z_2, particularly RCA_0 and ACA_0. One may ask why authors have seemingly avoided studying some of these results in WKL_0. As it turns out, WKL_0 is conservative over RCA_0 for the kinds of sentences that these results can be formulated in (see Theorem 3.16). Furthermore, we also study a conservativity result of WKL_0 over PRA[32], and its connection (or lack thereof) to Hilbert's program.

The following theorem may be expressed by saying that WKL_0 is conservative over RCA_0 for Π^1_1 sentences.

Theorem 3.16 (Friedman; see Corollary IX.2.6 of [Sim09]). *If φ is a Π^1_1 sentence and WKL_0 proves φ, then RCA_0 also proves φ.*

Similarly, the following theorem may be expressed by saying that WKL_0 is conservative over PRA for Π^0_2 sentences.

Theorem 3.17 (Harrington; see Theorem IX.3.16 of [Sim09]). *If φ is a Π^0_2 sentence and WKL_0 proves φ, then PRA also proves φ.*[33]

In [Sim88b], Simpson argues that Theorem 3.17 represents a partial realization of *Hilbert's program* (by which he means *finitistic reductionism*) for the foundations of mathematics.[34] The goal of finitistic reductionism, in this regard, was to show that non-finitistic set-theoretical mathematics can be reduced to PRA, by means of conservation results (for Π^0_1 sentences).

---

[32]Note that although the proof of Theorem 3.17 in [Sim09] uses model-theoretic techniques, Sieg [Sie85] gives a primitive recursive proof transformation which, given a proof of a Π^0_2 φ in WKL_0, generates a proof of φ in PRA. Hence, this result is provable within a finitary system and thus allows the reduction to go through.

[33]A proof of Theorem 3.17, and its extension to a strengthening WKL_0^+ of WKL_0, is outlined in [Day19, Sections 5 and 6].

[34]As stated before, although Hilbert did not explicitly spell out a precise definition of *finitism*, many (see, for example, [Sim88b] and [Tai81]) agree that the formal system of PRA (see Definition 3.6) captures the essence of this notion.

Of the many proof-theoretic advances of the early twentieth-century, one that is arguably the most significant[35] – as well as the most relevant to the realization (or, in this case, the lack thereof) of finitistic reductionism – is Gödel's publication of his incompleteness theorems [Göd31, Theorems VI and XI][36]. A consequence of these incompleteness theorems is that a complete realization of Hilbert's program is impossible.

However, it is still worth trying to understand what parts of Hilbert's program are salvageable, i.e. what sorts of infinitistic mathematics can, in fact, be reduced to finitism. Simpson (see [Sim09, Remark IX.3.18]) reformulates this question, in the language of subsystems of Z_2 as: Which interesting subsystems of Z_2 are conservative over PRA for Π^0_1 sentences? In this regard Theorem 3.17 provides a partial answer to his question, and, in turn, a partial realization of Hilbert's program. This, however, relies on the assumption that finitistic reductionism is, in fact, Hilbert's conception – which is disputed (refer to discussion in 3.3).

Since it is not directly within the scope of (but still relevant to) this paper, we pause our discussion on Hilbert's program and Gödel's incompleteness theorems here, and refer interested readers to more detailed sources: Sieg provides a much more informative description of Hilbert's program(s) in [Sie13, Section II]; Eastaugh provides a much more complete overview of the partial realization story in [Eas15, Section 4.5]; Davis lists and discusses undecidability results including (and following) Gödel's incompleteness theorems in [Dav65]; and Prince provides an easy-to-follow annotated version of Gödel's 1931 paper in [Pri22].

[35] One may recall von Neumann's remark on the occasion of the presentation of the Albert Einstein Award to Gödel in 1951: "Kurt Gödel's achievement in modern logic is singular and monumental – indeed, it is more than a monument; it is a landmark which will remain visible far in space and time."

[36] Roughly, Gödel's First Incompleteness Theorem [Göd31, Theorem VI] is the assertion that any consistent formal system F within which a certain amount of elementary arithmetic can be carried out is incomplete. That is, there are statements of the language of F which can neither be proved nor disproved in F. Furthermore, Gödel's Second Incompleteness Theorem [Göd31, Theorem XI] is the assertion that for any consistent system F within which a certain amount of elementary arithmetic can be carried out, the consistency of F cannot be proved in F itself.

3.5 Provable Ordinals

In this section we introduce notion of *provable ordinals* for subsystems of Z_2, and define $\mathrm{ord}(T_0)$ for a subsystem T_0 of Z_2. These form the basis of Gentzen-style proof theory (see [Sim09, Section IX.5]), which has been used to obtain various independence results in subsystems of Z_2 (see [Sim09, Remark IX.5.11]). In particular, it is used in showing that Hilbert's Basis Theorem is not provable in subsystems of Z_2 that are weaker (refer Section 3.3) than ACA_0, as in 4.17.

Definition 3.18. Let T_0 be a subsystem of Z_2 which includes RCA_0. A *provable ordinal* of T_0 is a countable ordinal α such that, for some primitive recursive well-ordering $W \subseteq \mathbb{N}$, $|W| = \alpha$ and T_0 proves $\mathrm{WO}(W)$, i.e. that, via a pairing function (see [Sim09, §II.2]), W codes a well-ordering of length α. The supremum of the provable ordinals of T_0 is denoted $\mathrm{ord}(T_0)$.

We now state the provable ordinals of the systems we are concerned with.

Theorem 3.19 (See Theorems IX.5.4 and IX.5.7 of [Sim09])**.** *We have*

$$\mathrm{ord}(\mathsf{RCA}_0) = \mathrm{ord}(\mathsf{WKL}_0) = \omega^\omega,$$

and

$$\mathrm{ord}(\mathsf{ACA}_0) = \varepsilon_0 := \sup(\omega, \omega^\omega, \omega^{\omega^\omega}, \ldots).$$

4 Reverse Mathematical analysis

We first discuss results involving algebraic closures, as an excellent example highlighting the relative strengths of RCA_0, WKL_0, and ACA_0 – see Theorems 4.6, 4.7, and 4.9. We then analyse Hilbert's Nullstellensatz (Section 4.2) and Basis Theorem (Section 4.3) from a reverse mathematical perspective, drawing from results in [FSS83], [ST04], [Sim88a], and [Sim15]. Finally, we state some analogous results in the context of real closed fields (Sections 4.4 and 4.5).

4.1 Algebraic Closure

Unless specified otherwise, the following definitions are made in RCA_0 and the results are stated over RCA_0 as well.

We first define the notion of a countable field in RCA_0 (refer [Sim09, Section II.9]. The more general definition of a countable structure in RCA_0 can be found in [FSS83, Section 2].

Definition 4.1. A *countable field* F consists of a set $|F| \subseteq \mathbb{N}$, together with binary operations $+_F, \cdot_F$, a unary operation $-_F$, and distinguished elements $0_F, 1_F$ such that the system $\langle |F|, +_F, -_F, \cdot_F, 0_F, 1_F \rangle$ obeys the usual field axioms.

Definition 4.2 (See §2 of [FSS83])**.** RCA_0 proves that for any countable field F and any $m \in \mathbb{N}$, there exists a countable commutative ring $F[x_1, \dots, x_m]$ consisting of 0 along with all (Gödel numbers of) expressions of the form

$$f(x_1, \dots, x_m) = \sum_{i_1 + \cdots i_m \leqslant n} a_{i_1 \dots i_m} x_1^{i_1} \cdots x_m^{i_m},$$

where $(i_1, \dots, i_m) \in \mathbb{N}^m$, $m \in \mathbb{N}$, $a_{i_1 \dots i_m} \in K$, and $a_{i_1 \dots i_m} \neq 0$ for at least one $(i_1, \dots, i_m) \in \mathbb{N}^m$ with $i_1 + \cdots + i_m = n$. This is the *ring of polynomials in m commuting indeterminates $x_1, \dots, x_m$ over F.*

Definition 4.3. A countable field F is said to be *algebraically closed* if for all nonconstant polynomials $f(x) \in F[x]$, there exists $a \in F$ such that $f(a) = 0$.[37]

Definition 4.4. Let F be a countable field. An *algebraic closure* of F consists of an algebraically closed countable field K, together with a monomorphism $h : F \to K$ such that for all $b \in K$, there exists a nonconstant polynomial $f(x) \in F[x]$ such that $h(f)(b) = 0$.

The following results emphasize the relative strengths of RCA_0, WKL_0, and ACA_0, in this context of algebraic closures of countable fields. More specifically, RCA_0 only proves the existence of algebraic closures; WKL_0 goes one step further, proving the uniqueness of algebraic closures; and ACA_0 proves the existence of *strong algebraic closures*.

Lemma 4.5 (Lemma II.9.3 of [Sim09])**.** *The following are provable in* RCA_0*:*

[37] By $f(a)$, we mean taking the alternative notation $\sum_{i=0}^{n} a_i x^i$ for the polynomial $f(x)$, and plugging in a in place of x.

1. ACF, *i.e. the first-order theory of algebraically closed fields, admits quantifier elimination: For any formula* φ *there exists a quantifier-free formula* ψ*, containing no new free variables (see 3.2), such that* $\mathsf{ACF} \vdash (\varphi \leftrightarrow \psi)$.[38]

2. *For any quantifier-free formula* φ*, if* $\mathsf{ACF} \vdash \varphi$*, then* $\mathsf{AF} \vdash \varphi$*, where* AF *is the theory of fields.*

Simpson notes that these well-known results in Lemma 4.5 have purely syntactical proofs[39] which can be transcribed in RCA_0. Friedman, Simpson, and Smith then use Lemma 4.5 to prove the following result.

Theorem 4.6 (Theorem 2.5 of [FSS83])**.** RCA_0 *proves that every countable field has an algebraic closure.*[40]

Theorem 4.6 is a powerful result that provides the machinery needed to prove some formulations of Hilbert's Nullstellensatz in RCA_0, which we discuss in detail in Section 4.2. We now discuss two strengthenings of Theorem 4.6, which are no longer provable in RCA_0.

The following theorem states that, over RCA_0, WKL is equivalent to the existence of unique algebraic closures. Since WKL is itself not provable in RCA_0, it follows that RCA_0 does not prove the uniqueness of algebraic closures.

Theorem 4.7 (Theorem 3.3 of [FSS83])**.** *The following assertions are equivalent over* RCA_0*:*

1. *Weak König's Lemma*

2. *Every countable field has a unique (up to isomorphism) algebraic closure.*

Simpson defines the notion of a strong algebraic closure as follows (see [Sim09, Section III.3]).

[38]The symbol $\vdash$ is read as "proves;" and we write $T \vdash \varphi$ if there is a *proof* of φ from T. One may refer to [Mar10, §2] for a rigorous definition of *proof*. However, for this discussion, it would suffice to have an intuitive understanding of the notion of a *proof*.

[39]Simpson's proof relies on Tarski's syntactical quantifier elimination methods – presented in, for example, [KK00].

[40]A different proof of this theorem can also be found in [Sim09, Theorem II.9.4].

Definition 4.8. Let F be a countable field. A *strong algebraic closure* of F is an algebraic closure $h : F \to K$ (see Definition 4.4) with the further property that h is an isomorphism of F onto a subfield of K.

Theorem 4.9 (Theorem III.3.2 of [Sim09])**.** *The following assertions are pairwise equivalent over* RCA_0*:*

1. ACA_0
2. *Every countable field has a strong algebraic closure.*
3. *Every countable field is isomorphic to a subfield of a countable algebraically closed field.*

4.2 Hilbert's Nullstellensatz

As stated before, there have been numerous formulations of the Nullstellensatz (see footnote 13), many of which are hard to compare in subsystems of Z_2. In this section we discuss some formulations, as coded in the literature, in the reverse mathematical context.

Friedman, Simpson, and Smith describe two formulations of the Nullstellensatz in [FSS83, Section 2], which we label HN_1 and HN_2: Let F be a countable field and $f_1, \dots, f_m \in F[x_1, \dots, x_n]$.

HN_1. $f_1, \dots, f_m$ have a common root in some extension of F if and only if $f_1, \dots, f_m$ have a common root in an algebraic extension of F.

HN_2. $f_1, \dots, f_m$ have a common root in some extension of F if and only if $1 \notin (f_1, \dots, f_m)$.[41]

Theorem 4.10 (Section 2 of [FSS83])**.** RCA_0 *proves* HN_1*.*

This follows from Lemma 4.5, i.e. RCA_0 proving quantifier-elimination for ACF, and Theorem 4.6, i.e. RCA_0 proving the existence of algebraic closures for countable fields.

Theorem 4.11 (Section 2 of [FSS83])**.** RCA_0 *proves* HN_2*.*

[41]Note that HN_2 is very closely related to what was stated as the Weak Nullstellensatz in Corollary 2.8.

Although this version is customarily reduced to HN_1 by extending the ideal generated by $f_1, \ldots, f_m$ to a prime or maximal ideal, the general results on the existence of prime or maximal ideals require more than RCA_0 (see Theorems 3.13 and 3.15). The proof of HN_2 in RCA_0 relies on a method of elimination, satisfied by Kronecker's Elimination, which is explained in more detail in [FSS83] and [Ste23].

Corollary 4.12 (Section 2 of [FSS83]). RCA_0 *proves that* g *vanishes on* $\mathbb{V}(f_1, \ldots, f_m)$ *if and only if there exists* $r \geqslant 1$ *such that* $g^r \in \langle f_1, \ldots, f_m \rangle$.[42]

It is a consequence of Corollary 4.12, by elimination, that RCA_0 proves the existence of the set of all such g's, i.e. the radical ideal[43] generated by $f_1, \ldots, f_m$.

Sakamoto and Tanaka introduce what they call Hilbert's Nullstellensatz for complex numbers in [ST04, Section 1], which we label HN_3:

HN_3 For any $n, m \in \mathbb{N}$, if $p_1, \ldots, p_m \in \mathbb{C}[x_1, \ldots, x_n]$ have no common zeros, then $1 \in \langle p_1, \ldots, p_m \rangle$.[44]

Theorem 4.13 (Theorem 8 of [ST04]). HN_3 *is provable in* RCA_0.

4.3 Hilbert's Basis Theorem

Simpson codes the Basis Theorem in terms of what he calls Hilbertian rings, defined in this section. In standard set theory, like ZFC, it is provable that a ring R is Hilbertian if and only if every ideal in R is finitely generated, i.e. R is Noetherian (see Definition 2.3). On the other hand, in the reverse-mathematical context, although this equivalence holds over stronger base theories like ACA_0 [Sim88a, Remark 2.2], it does not necessarily hold over weaker theories. In particular, over RCA_0, the notion of Hilbertian is somewhat stronger than every ideal being finitely generated (see [Sim88a, Remark 2.2]). Thus, over RCA_0, the Basis Theorem coded in terms of Hilbertian rings implies the version coded in terms of every ideal being finitely generated.

[42] Note that Corollary 4.12 is the special case of what was stated as Hilbert's Nullstellensatz in Theorem 2.7, when $I = \langle f_1, \ldots, f_m \rangle$, i.e. the ideal generated by $f_1, \ldots, f_m$, whose existence is provable in RCA_0 (see [FSS83, Lemma 2.10]).

[43] More generally, given an ideal I of a ring R, the radical ideal generated by I is $\mathrm{rad}(I) := \{a \in R \mid \exists n(a^n \in I)\}$.

[44] Note that HN_3 is the special case of the backwards direction of the Weak Nullstellensatz in Corollary 2.8, when $I = \langle p_1, \ldots, p_m \rangle$.

Definition 4.14. Within RCA_0, let R be a countable commutative ring. We say that R is *Hilbertian* if for every sequence $(r_i)_{i\in\mathbb{N}}$ of elements of R, there exists $k \in \mathbb{N}$ such that for all $j \in \mathbb{N}$, there exist $s_0, \ldots, s_k \in R$ such that $r_j = \sum_{i\leqslant k} s_i r_i$.

Simpson then gives two, provably equivalent over RCA_0, formulations of the Basis Theorem (see [Sim88a]), which we label HB_1 and HB_2.

HB_1. For all $m \in \mathbb{N}$ and all countable fields K, the commutative ring $K[x_1, \ldots, x_m]$ is Hilbertian.

HB_2. For each $m \in \mathbb{N}$, there exists a countable field K such that the commutative ring $K[x_1, \ldots, x_m]$ is Hilbertian.

For the remainder of this section, we list results that narrow where the Basis Theorem fits in the Friedman-Simpson Hierarchy.

Recall from Theorem 3.19 that $\mathrm{ord}(\mathsf{RCA}_0) = \omega^\omega$. That is, RCA_0 can prove that any ordinal $\alpha < \omega^\omega$ is well-ordered, and cannot do so for ω^ω. The following result asserts that RCA_0 does not prove $\mathrm{WO}(\omega^\omega)$.

Lemma 4.15 (Proposition 2.6(2) of [Sim88a])**.** $\mathsf{RCA}_0 \nvdash \mathrm{WO}(\omega^\omega)$. *That is, there is no primitive recursive well-ordering W of order-type ω^ω, such that* $\mathsf{RCA}_0 \vdash \mathrm{WO}(W)$.

Lemma 4.16 (Theorem 2.7 of [Sim88a])**.** *The following assertions are pairwise equivalent over* RCA_0

1. HB_1

2. HB_2

3. $\mathrm{WO}(\omega^\omega)$

In this regard, ω^ω is a measure of what Simpson calls the "intrinsic logical strength" of the Basis Theorem (see [Sim88a, Section 1]).[45]

Since HB_1 and HB_2 are provably equivalent over RCA_0, we will henceforth refer to them as HB.

[45]In [KY16], Kreuzer and Yokoyama show that many principles of first-order arithmetic, previously only known to lie strictly between Σ^0_1-Induction and Σ^0_2-Induction, are equivalent to $\mathrm{WO}(\omega^\omega)$. Hence, these have the same "intrinsic logical strength" as the Basis Theorem. They argue that, in some sense, $\mathrm{WO}(\omega^\omega)$ should be considered a *natural* first-order principle between Σ^0_1-Induction and Σ^0_2-Induction, and should have its own place (see [KY16, Figure 3]) in the Paris-Kirby Hierarchy (as defined in [HP98]).

Theorem 4.17. RCA_0 *does not prove* HB*.*

This is a direct consequence of the two preceding lemmas, i.e. Lemma 4.15 and Lemma 4.16: Since $\mathsf{RCA}_0 \nvdash \mathrm{WO}(\omega^\omega)$ and $\mathsf{RCA}_0 \vdash (\mathrm{WO}(\omega^\omega) \leftrightarrow \mathsf{HB})$, we may conclude that $\mathsf{RCA}_0 \nvdash \mathsf{HB}$.

Furthermore, Simpson showed in [Sim15] that $\mathsf{RCA}_0 + \Sigma^0_2$-Induction was enough to prove $\mathrm{WO}(\omega^\omega)$:

Lemma 4.18 (Theorem 2.2 of [Sim15])**.** $\mathrm{WO}(\omega^\omega)$ *is provable in* $\mathsf{RCA}_0 + \Sigma^0_2$*-Induction.*

Recall that Σ^0_2-Induction (see footnote 26) is not provable in RCA_0 (see [Sim09, Chapter II]). Thus, $\mathsf{RCA}_0 + \Sigma^0_2$-Induction is strictly stronger in terms of provability than RCA_0.

Theorem 4.19. HB *is provable in* $\mathsf{RCA}_0 + \Sigma^0_2$*-Induction.*

This is a direct consequence of Lemmas 4.16 and 4.18: Since $\mathsf{RCA}_0 \vdash (\mathrm{WO}(\omega^\omega) \leftrightarrow \mathsf{HB})$ and $\mathsf{RCA}_0 + \Sigma^0_2$-Induction $\vdash \mathrm{WO}(\omega^\omega)$, we may conclude that $\mathsf{RCA}_0 + \Sigma^0_2$-Induction $\vdash \mathsf{HB}$.

Simpson also shows that the provability result in Lemma 4.18 is not reversible, i.e. $\mathsf{RCA}_0 + \mathrm{WO}(\omega^\omega)$ does not prove Σ^0_2-Induction [Sim15, Section 4]. In fact, even assuming additional machinery, namely the Σ^0_2-Bounding Principle (see [Sim15, Definition 2.1]), does not suffice [Sim15, Corollary 4.3]. This reinforces Kreuzner and Yokoyama's argument (see footnote 45) that $\mathrm{WO}(\omega^\omega)$ should be considered a natural first-order principle between Σ^0_1-Induction and Σ^0_2-Induction.

It is worth making explicit that for a fixed $m \in \mathbb{N}$, RCA_0 proves $\mathrm{WO}(\omega^m)$ (see [Sim88a, Proposition 2.6(1)]). As a consequence, RCA_0 proves the following

$\mathsf{HB}(m)$. For all countable fields K, the commutative ring $K[x_1, \ldots, x_m]$ is Hilbertian.

In particular, $\mathsf{HB}(1)$ is what was stated as Theorem 2.4. Hence, if, by "Hilbert's Basis Theorem" one means $\mathsf{HB}(1)$, then Hilbert's Basis Theorem is, indeed, provable in RCA_0.

Moreover, the nonconstructive content in HB truly comes from what was referred to as a "straightforward inductive argument" in Section 2. More explicitly:

Theorem 4.20 (See Proposition 2.6(3) of [Sim88a]). RCA_0 *proves that*

$$\mathsf{HB} \leftrightarrow \forall m\ \mathsf{HB}(m).$$

In conclusion, although some formulations of the Nullstellensatz are provable in RCA_0 (see Theorems 4.10, 4.11, 4.13), it follows from Simpson's results (Theorems 4.17 and 4.19) that the Basis theorem, for arbitrary $m \in \mathbb{N}$, needs strictly more machinery. In this sense, the Basis theorem is strictly more nonconstructive than the Nullstellensatz.

4.4 Real closures and formally real fields

In this section, we analyze analogous results to those in Section 4.1, in the context of real closures and formally real fields.[46] As before, unless specified otherwise, the following definitions are made in RCA_0 and the results are stated over RCA_0 as well.

Definition 4.21. A *countable ordered field* consists of a countable field F together with a binary relation $< \subseteq |F|^2$ such that $(F, <)$ obeys the usual ordered field axioms, for example, $\forall x \forall y (x < y \vee x = y \vee y < x)$ and $(x < y \leftrightarrow x + z < y + z)$.

Definition 4.22. A countable ordered field is said to be *real closed* if it has the intermediate value property for polynomials, i.e. for all $g \in F[x]$ and $a, b \in F$, if $g(a) < 0 < g(b)$ then there is $c \in F$, between a and b, such that $g(c) = 0$.

Definition 4.23. A *real closure* of a countable ordered field F consists of a countable real closed ordered field L together with a monomorphism $h : F \to L$ such that for each $b \in L$ there exists a nonconstant $g(x) \in F[x]$ such that $h(g)(b) = 0$.

Theorem 4.24 (Theorems 2.12 and 2.18 of [FSS83]). *The following is provable in* RCA_0*: Every countable ordered field F has a real closure. Furthermore, the real closure is unique in the sense that, if $h_1 : F \to L_1$ and $h_2 : F \to L_2$ are two real closures of F, then there exists a unique isomorphism $h : L_1 \to L_2$ such that $h(h_1(a)) = h_2(a)$ for all $a \in F$.*

[46] These structures are studied model-theoretically in [JL89] and [Mar10].

It is worth noting that RCA_0 was not strong enough to prove the uniqueness of algebraic closures (see Section 4.1).

Definition 4.25. A countable field F is said to be *formally real* if -1 is not a sum of squares in F – or, equivalently, if F does not contain a sequence of elements $\langle c_0, \ldots, c_n \rangle$, with at least one $c_i \neq 0$ and $n \in \mathbb{N}$, such that $\sum_{i=0}^{n} c_i^2 = 0$.

Definition 4.26. A countable field F is said to be *orderable* if there exists a binary relation relation $<$ on F, under which $(F, <)$ is an ordered field.

The following theorem can be thought of as the real-closed analog of Theorem 4.7:

Theorem 4.27 (Theorem 3.5 of [FSS83])**.** *The following assertions are equivalent over* RCA_0*:*

1. *Weak König's Lemma*

2. *Every countable formally real field is orderable.*

The proof of Theorem 4.27 is the content of [FSS83, Theorem 3.5] (or [Sim09, Theorem IV.4.5]).

Corollary 4.28. *The following assertions are equivalent over* RCA_0*:*

1. *Weak König's Lemma*

2. *Every countable formally real field has a real closure.*

This is an immediate consequence of Theorem 4.24.

Definition 4.29. Let F be a countable field. A *strong real closure* of F is a real closure $h : F \to L$ (see Definition 4.23) with the further property that h is an isomorphism of F onto a subfield of L.

The following theorem can be thought of as the real-closed analog of Theorem 4.9.

Theorem 4.30 (Theorem III.3.2 of [Sim09])**.** *The following assertions are pairwise equivalent over* RCA_0*:*

1. ACA_0

2. *Every countable ordered field has a strong real closure.*
3. *Every countable formally real field has a strong real closure.*
4. *Every countable ordered field is isomorphic to a subfield of a countable real closed ordered field.*
5. *Every countable formally real field is isomorphic to a subfield of a countable real closed ordered field.*

4.5 Real Nullstellensatz

In the spirit of real closed analogs, one may wonder if there is a real version of the Nullstellensatz. Recall that the field of real numbers is not algebraically closed; this poses a nontrivial challenge.

For an algebraically closed field K, Hilbert's Nullstellensatz establishes a one-to-one (order-reversing) correspondence between the posets of radical ideals (see footnote 43) in $K[x_1, \ldots, x_n]$ and affine varieties (Definition 2.6 should suffice for this discussion) in K^n. This correspondence fails over $\mathbb{R}$. For instance, the ideal $I = \langle x^2+1 \rangle$ is a radical ideal in $\mathbb{R}[x]$, since $\mathbb{R}[x]/I \cong \mathbb{C}$ is a field. The real variety $\mathbb{V}(I) = \varnothing$ coincides with the variety $\mathbb{V}(\langle 1 \rangle)$ determined by the ideal $\langle 1 \rangle$ in $R[x]$. Thus, two different radical ideals define the same variety in $\mathbb{R}^n$, and Hilbert's Nullstellensatz fails.

There is, however, a somewhat analogous statement in the case of real closed fields (see [Mar10, §3.4]).

RN Let F be a real closed field, and I be a prime ideal in $F[x_1, \ldots, x_n]$. Then $\mathbb{V}_F(I)$ is nonempty if and only if whenever $p_1, \ldots, p_m \in F[x_1, \ldots, x_n]$ and $\sum p_i^2 \in I$, then for each i, $p_i \in I$.

A proof of this Real Nullstellensatz (over ZFC) can be found in [Dic85]. Sakamoto and Tanaka state that it would be an interesting question to decide whether the Real Nullstellensatz is provable in RCA_0; however, it is unclear how this result would even be coded in RCA_0 [ST04, §4].

References

[AM69] Michael F. Atiyah and Ian G. MacDonald. *Introduction to Commutative Algebra.* Addison-Wesley-Longman, 1969.

[AM14] Jeremy Avigad and Rebecca Morris. The concept of "character" in Dirichlet's theorem on primes in an arithmetic progression. *Archive for History of Exact Sciences*, 68:265–326, 2014.

[Arr06] Enrique Arrondo. Another Elementary Proof of the Nullstellensatz. *The American Mathematical Monthly*, 113(2):169–171, 2006.

[Avi06] Jeremy Avigad. Methodology and Metaphysics in the Development of Dedekind's Theory of Ideals. In José Ferreirós and Jeremy Gray, editors, *The Architecture of Modern Mathematics*, pages 159–186. Oxford University Press, 2006.

[Bee85] Michael J. Beeson. *Foundations of Constructive Mathematics*, volume 6 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge.* Springer, Berlin, Heidelberg, 1985.

[BHS87] Andreas R. Blass, Jeffrey L. Hirst, and Stephen G. Simpson. Logical analysis of some theorems of combinatorics and topological dynamics. In Stephen G. Simpson, editor, *Logic and Combinatorics*, volume 65 of *Contemporary Mathematics*, pages 125–156. American Mathematical Society, 1987.

[Boy68] Carl B. Boyer. *A History of Mathematics.* New York, London, Sydney: John Wiley & Sons, Inc, 1968.

[BS86] Douglas K. Brown and Stephen G. Simpson. Which set existence axioms are needed to prove the separable Hahn-Banach theorem? *Annals of Pure and Applied Logic*, 31:123–144, 1986.

[BS93] Douglas K. Brown and Stephen G. Simpson. The Baire Category Theorem in Weak Subsystems of Second-Order Arithmetic. *The Journal of Symbolic Logic*, pages 557–578, 1993.

[Car05] Patrick Hatfield Carey. Beyond Infinity: Georg Cantor and Leopold Kronecker's Dispute over Transfinite Numbers. *Senior Honors Thesis, Boston College*, 2005.

[Che43] Claude Chevalley. On the Theory of Local Rings. *Annals of Mathematics*, 44(4):690–708, 1943.

[Coh63] Paul J. Cohen. The Independence of the Continuum Hypothesis. *Proceedings of the National Academy of Sciences USA*, 50(6):1143–1148, 1963.

[Dav65] Martin Davis. *The Undecidable: Basic Papers on Undecidable Propositions, Unsolvable Problems and Computable Functions.* Hewlett, NY, USA: Dover Publication, 1965.

[Day19] Gabriel Day. Some Conservativity Results in Reverse Mathematics of Interest to Hilbert's Program. *University of Chicago REU*, 2019.

[Ded79] Richard Dedekind. Über die Theorie der ganzen algebraischen Zahlen, 1879. Supplement X to Dirichlet's *Vorlesungen über Zahlentheorie*. Friedrich Vieweg und Sohn, Braunschweig, 1863.

[Ded88] Richard Dedekind. Was sind und was sollen die Zahlen? *Vieweg, Braunschweig*, 1888.

[Dic85] M. A. Dickmann. Applications of Model Theory to Real Algebraic Geometry. In Carlos A. Di Prisco, editor, *Methods in Mathematical Logic*, volume 1130 of *Lecture Notes in Mathematics*. Springer, Berlin, Heidelberg, 1985.

[Eas15] Benedict Eastaugh. Reverse Mathematics: A Philosophical Account. *PhD thesis, University of Bristol*, 2015.

[Edw80] Harold M. Edwards. The Genesis of Ideal Theory. *Archive for History of Exact Sciences*, 23(4):321–378, 1980.

[Eis95] David Eisenbud. *Commutative Algebra with a View Toward Algebraic Geometry.* Springer New York, 1995.

[End77] Herbert B. Enderton. *Elements of Set Theory.* Academic Press Inc., 1977.

[Fer07] José Ferreirós. ‘O $\Theta\varepsilon\grave{o}\varsigma$’ A$\rho\iota\theta\mu\eta\tau\acute{\iota}\zeta\varepsilon\iota$: The Rise of Pure Mathematics as Arithmetic with Gauss. In *The Shaping of Arithmetic after C. F. Gauss's Disquisitiones Arithmeticae*, pages 234–268. Springer, Berlin, 2007.

[FH91] Harvey M. Friedman and Jeffrey L. Hirst. Reverse mathematics and homeomorphic embeddings. *Annals of Pure and Applied Logic*, 54:229–253, 1991.

[Fri75] Harvey M. Friedman. Some systems of second order arithmetic and their use. *Proceedings of the 1974 International Congress of Mathematicians*, 1:235–242, 1975.

[FSS83] Harvey M. Friedman, Stephen G. Simpson, and Rick L. Smith. Countable algebra and set existence axioms. *Annals of Pure and Applied Logic*, 25:141–181, 1983.

[GCGR19] Edisson Gallego, Juan D. Vélez C., and Danny A. J. Gómez-Ramírez. A general version of the Nullstellensatz for arbitrary fields. *Open Mathematics*, 17(1):556–558, 2019.

[Göd31] Kurt Gödel. Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I. *Monatshefte für Mathematik und Physik*, 38:173–198, 1931.

[Göd38] Kurt Gödel. The Consistency of the Axiom of Choice and of the Generalized Continuum-Hypothesis. *Proceedings of the National Academy of Sciences of the United States of America*, 24:556–557, 1938.

[Hil90] David Hilbert. Über die Theorie der algebraischen Formen. *Mathematische Annalen*, 36(4):473–574, 1890.

[Hil93] David Hilbert. Über die vollen Invariantensysteme. *Mathematische Annalen*, 42(3):313–373, 1893.

[Hil26] David Hilbert. Über das Unendliche. *Mathematische Annalen*, 95:161–190, 1926.

[Hil98] David Hilbert. *Theory of Algebraic Number Fields.* Springer Berlin, 1998. Translated by Ian T. Adamson. (Originally published as *Die Theorie der algebraischen Zahlkörper*, Springer Fachmedien Wiesbaden, 1897).

[Hir87] Jeffrey L. Hirst. Combinatorics in Subsystems of Second Order Arithmetic. *PhD thesis, Pennsylvania State University*, 1987.

[HP98] Petr Hájek and Pavel Pudlák. *Metamathematics of First-Order Arithmetic.* Perspectives in Mathematical Logic. Springer-Verlag, Berlin, 1998.

[HR98] Paul Howard and Jean E. Rubin. *Consequences of the Axiom of Choice.* Mathematical Surveys and Monographs, Vol. 59. American Mathematical Society, 1998.

[JL89] Christian U. Jensen and Helmut Lenzing. *Model Theoretic Algebra: With particular emphasis on Fields, Rings, Modules.* Algebra, Logic and Applications Series Volume 2. Routledge, 1989.

[KK00] Georg Kreisel and Jean-Louis Krivine. *Elements of Mathematical Logic*, volume 48 of *Studies in Logic and the Foundation of Mathematics.* Elsevier Science, 2000. Translated Alan Slomson. (Originally published as *Éléments de Logique Mathématique*, Dunod, Paris, 1967).

[Kro82] Leopold Kronecker. Grundzüge einer arithmetischen Theorie der algebraischen Grössen. *Journal für reine und angewandte Mathematik*, 92:1–122, 1882.

[Kro87] Leopold Kronecker. Über den Zahlbegriff. *Philosophische Aufsätze, Eduard Zeller zu seinem fünfzigjährigen Doctorjubiläum gewidmet*, page 261–274, 1887.

[KS89] Kostas Katzikiriakou and Stephen G. Simpson. Countable valued fields in weak subsystems of second-order arithmetic. *Annals of Pure and Applied Logic*, 41:27–32, 1989.

[Kun80] Kenneth Kunen. *Set Theory: An Introduction to Independence Proofs.* North-Holland, 1980.

[KY16] Alexander P. Kreuzer and Keita Yokoyama. On principles between Σ_1- and Σ_2-induction and monotone enumerations. *Journal of Mathematical Logic*, 64(1):1650004, 2016. https://arxiv.org/abs/1306.1936.

[Lau99] Detlef Laugwitz. *Bernhard Riemann: 1826 - 1866 Turning Points in the Conception of Mathematics*. Birkhäuser, Boston, 1999. Translated by Abe Shenitzer.

[Man05] Marco Manetti. Nullstellensatz for everybody. *Unpublished*, 2005. Translated by Jon Rokne. (Originally published as *Nullstellensatz per tutti* in 2004).

[Mar10] David Marker. *Model Theory: An Introduction*. Springer New York, 2010.

[McL12] Colin McLarty. Hilbert on Theology and its Discontents: The Origin Myth of Modern Mathematics. In Apostolos Doxiadis and Barry Mazur, editors, *Circles Disturbed: The Interplay of Mathematics and Narrative*, pages 105–129. Princeton University Press, 2012.

[Moo82] Gregory H. Moore. *Zermelo's Axiom of Choice*. Studies in the History of Mathematics and Physical Sciences. Springer New York, 1982.

[Noe21] Emmy Noether. Idealtheorie in Ringbereichen. *Mathematische Annalen*, 83:24–66, 1921.

[NS23] Dag Normann and Sam Sanders. The Biggest Five of Reverse Mathematics. *Journal of Mathematical Logic*, 2023.

[Pri22] Hal Prince. *The Annotated Gödel: A Reader's Guide to His Classic Paper on Logic and Incompleteness*. Homebred Press, 2022.

[Rab30] J. L. Rabinowitsch. Zum Hilbertschen Nullstellensatz. *Mathematische Annalen*, 102(1):520, 1930.

[Rie51] Bernhard Riemann. Grundlagen für eine allgemeine Theorie der Functionen einer veränderlichen complexen Grösse, 1851. Inauguraldissertation, Göttingen.

[Row00] David E. Rowe. Episodes in the Berlin-Göttingen Rivalry, 1870-1930. *The Mathematical Intelligencer*, 22:60–69, 2000.

[Sha13] Igor R. Shafarevich. *Basic Algebraic Geometry 1*. Springer Berlin, Heidelberg, 2013.

[Sho67] Joseph R. Shoenfield. *Mathematical Logic*. Addison-Wesley Publishing Company, 1967.

[Sie85] Wilfried Sieg. Fragments of Arithmetic. *Annals of Pure and Applied Logic*, 28:30–71, 1985.

[Sie90] Wilfried Sieg. Review of Simpson [1985]. *The Journal of Symbolic Logic*, 55(2), 1990.

[Sie13] Wilfried Sieg. *Hilbert's Programs and Beyond*. Oxford University Press, 2013.

[Sim88a] Stephen G. Simpson. Ordinal Numbers and the Hilbert Basis Theorem. *The Journal of Symbolic Logic*, 53(3), 1988.

[Sim88b] Stephen G. Simpson. Partial Realizations of Hilbert's Program. *The Journal of Symbolic Logic*, 53(2):349–363, 1988.

[Sim09] Stephen G. Simpson. *Subsystems of Second Order Arithmetic*. Perspectives in Logic. Cambridge University Press, second edition, 2009. First edition published as *Subsystems of Second Order Arithmetic*. Perspectives in Mathematical Logic. Springer, 1999.

[Sim15] Stephen G. Simpson. Comparing $\mathrm{WO}(\omega^\omega)$ with Σ^0_2 induction. https://arxiv.org/abs/1508.02655, 2015.

[SKKT00] Karen E. Smith, Lauri Kahanpää, Pekka Kekäläinen, and William Traves. *An Invitation to Algebraic Geometry*. Springer New York, NY, 2000.

[ST04] Nobuyuki Sakamoto and Kazuyuki Tanaka. The strong soundness theorem for real closed fields and Hilbert's Nullstellensatz in second order arithmetic. *Arch. Math. Logic*, 43:337–349, 2004.

[Ste23] Jan Stevens. Early proofs of Hilbert's Nullstellensatz. https://arxiv.org/abs/2309.14024, 2023.

[Tai81] W. W. Tait. Finitism. *Journal of Philosophy*, 78(9):524–546, 1981.

[Tap06] Jamie Tappenden. The Riemannian Background to Frege's Philosophy. In José Ferreirós and Jeremy Gray, editors, *The Architecture of Modern Mathematics: Essays in History and Philosophy*, pages 107–150. Oxford University Press, 2006.

[Tap23] Jamie Tappenden. History of Mathematics Illuminates Philosophy of Mathematics: Riemann, Weierstrass and Mathematical Understanding. In Karine Chemla, José Ferreirós, et al., editors, *The Richness of the History of Mathematics*, pages 617–649. Springer, 2023.

[vdW26] Bartel L. van der Waerden. Ein algebraisches Kriterium für die Lösbarkeit eines Systems homogener Gleichungen. *Proceedings Amsterdam*, 29:142–149, 1926.

[YS90] Xiaokang Yu and Stephen G. Simpson. Measure theory and weak König's lemma. *Archive for Mathematical Logic*, 30:171–180, 1990.