ROCKY MOUNTAIN JOURNAL
OF MATHEMATICS
Volume 52 (2022), No. 4, 1157–1176

AXIOMATIC (AND NON-AXIOMATIC) MATHEMATICS

SAEED SALEHI

Axiomatizing mathematical structures and theories, or *postulating* them as Russell (1919) put it, is a goal of mathematical logic. Some axiomatic systems are mere definitions, such as the axioms of Group Theory; but some are much deeper, such as the axioms of complete ordered fields with which real analysis starts. Groups abound in the mathematical sciences, while by Dedekind's theorem (1888) there exists only one complete ordered field, up to isomorphism. Cayley's theorem (1854) in abstract algebra implies that the axioms of group theory completely axiomatize the class of permutation sets that are closed under composition and inversion.

In this expository article, we survey some old and new results on the first-order axiomatizability of various mathematical structures. As we will see, axiomatizability of some structures are still unsolved questions in mathematics, and several results have been open problems in the past. We will also review identities over addition, multiplication, and exponentiation that hold in the set of positive real numbers; and will have a look at Tarski's high school problem (1969) and its solution.

The method of "postulating" what we want has many advantages;
they are the same as the advantages of theft over honest toil.

– Bertrand Russell (1919, *Introduction to Mathematical Philosophy*)

	$\mathbb{N}$	$\mathbb{Z}$	$\mathbb{Q}$	$\mathbb{R}$	$\mathbb{C}$
$\{<\}$	✓	✓	✓	✓	–
$\{+\}$	✓	✓	✓	✓	✓
$\{<,+\}$	✓	✓	✓	✓	–
$\{+,\times\}$	×	×	×	✓	✓
$\{\times\}$	✓	✓	✓	✓	✓
$\{<,\times\}$	×	×	✓	✓	–
$\mathfrak{exp}$	×	–	–	?	×

Table 1. Axiomatizability.

I warmly appreciate the anonymous referee's most useful comments and suggestions, which greatly improved the presentation and results of the paper. This research was partially supported by IPM grant 98030022.
2020 AMS *Mathematics subject classification:* primary 03B25, 03C10, 03D35, 03F40; secondary 11U05, 12L05.
Keywords and phrases: axiomatic system, first-order logic, identities.
Received by the editors on November 1, 2021, and in revised form on April 10, 2022.

DOI: 10.1216/rmj.2022.52.1157

$\{+\}$	$x+(y+z)=(x+y)+z, \quad x+y=y+x$
$\{\times\}$	$x\cdot(y\cdot z)=(x\cdot y)\cdot z, \quad x\cdot y=y\cdot x, \quad x\cdot 1=x$
$\{+,\times\}$	$x\cdot(y+z)=(x\cdot y)+(x\cdot z)$
$\{\mathfrak{exp}\}$	$(x^y)^z=(x^z)^y, \quad x^1=x, \quad 1^x=1$
$\{\times,\mathfrak{exp}\}$	$x^{(y\cdot z)}=(x^y)^z, \quad (x\cdot y)^z=x^z\cdot y^z$
$\{+,\times,\mathfrak{exp}\}$	$x^{(y+z)}=x^y\cdot x^z, \quad \ldots$

Table 2. Axioms for identities (over $\mathbb{R}^+$).

1. Introduction

A structure consists of a non-empty set D, called domain, together with a language $\mathcal{L}$ that consists of some constant, relation or function symbols which are interpreted over the domain. The abstract definition of a structure $\mathfrak{A}=\langle D;\mathcal{L}\rangle$ from Model Theory is not needed here. In our (first-order) setting, the quantifiers $(\forall,\exists)$ range over the elements of the domain in question (which are taken to be number sets $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$, here). So, subsets of the domain cannot be quantified; thus, the statement "for every nonempty and bounded subset there is a supremum for it" is not first-order, while "every element has an inverse" is so.

One reason for studying mathematical structures and theories in the setting of first-order logic is that despite of the fact that this logic is too weak to represent some fundamental properties (such as *being well-ordered* or *completeness* of ordered sets) it has some other nice properties, such as the *compactness* and *semantic completeness* (proved by Gödel 1930).

On the other hand, second-order logic may seem to be a more expressive framework for studying mathematical theories and structures (in which one can express the properties of *being well-ordered* and *completeness* of ordered sets). But it has its own foundational problems; the same problems that set theory has with *incompleteness* and *truth* (proved by Gödel 1931). In fact, as Quine put it, second-order logic is "set theory in sheep's clothing" (this is actually the title of the fourth section of the fifth chapter of Quine's *Philosophy of Logic*, 1986).

So, we have chosen first-order logic as the framework of our study; though, the study could be undertaken in the framework of second-order logic as well.

In this paper, we survey some old and new results on the first-order axiomatizability of various mathematical structures (see Table 1). Informally speaking, a structure is *axiomatizable* when we have a *theory*, that is a set of sentences called *axioms*, and an algorithm that can recognize whether a given sentence is an axiom or not, in a way that every sentence that is true in the structure is logically derivable from the theory; see Definition 5.7 below for more formal details. The (non-)axiomatizability of many structures in Table 1 are known from almost a century ago; for example, the axiomatizability of the structure $\langle\mathbb{C};+,\times\rangle$ follows from Tarski's theorem (1936), and the non-axiomatizability of $\langle\mathbb{N};+,\times\rangle$ follows from Gödel's theorem (1931). The question of the axiomatizability of e.g. $\langle\mathbb{Q};<,\times\rangle$ seemed to be missing in the literature, which was shown to be axiomatizable in [1] for the first time; Tarski's result implies the axiomatizability of $\langle\mathbb{C};\times\rangle$, but one explicit axiomatization for it was presented in [16] for the first time.

We will also review identities over $+,\times,\mathfrak{exp}$ that hold in the set of positive real numbers (Table 2). The identities on Table 2, except the last row which contains three dots, do completely axiomatize the

identities that hold in the set of positive real numbers ($\mathbb{R}^+$) over the indicated operations. Whether all the identities in the table completely axiomatize the identities in the structure $\langle \mathbb{R}^+; 1, +, \times, \mathfrak{exp} \rangle$ is the well-known *Tarski's high-school problem*, which has an interesting history.

2. Boolean algebras and propositional logic

Arguably, modern logic starts with Boole's *Investigation of the Laws of Thought* (1854); Boole's axiomatic system is called "propositional logic" nowadays. It axiomatizes some basic properties of the conjunction ($\wedge$), disjunction ($\vee$), and negation ($\neg$) connectives. The Boolean expressions (or propositional formulas) are constructed from a fixed infinite set of atoms, say $\{p_0, p_1, p_2, \dots\}$, by means of those connectives. An *evaluation* is a mapping from atoms to $\{\top, \bot\}$ interpreted as truth and falsum; the mapping can be extended to *all* the propositional formulas by the truth-table rules. Two formulas are called (logically) *equivalent* when they have the same value under every evaluation. Let us note that implication ($\rightarrow$) is definable by disjunction and negation as $(a \rightarrow b) \equiv (\neg a) \vee b$, where $\equiv$ denotes equivalence. Boole's axiomatization is in fact nothing but a definition of boolean algebras:

Associativity
$$a \wedge (b \wedge c) \equiv (a \wedge b) \wedge c, \quad a \vee (b \vee c) \equiv (a \vee b) \vee c$$
Commutativity
$$a \wedge b \equiv b \wedge a, \quad a \vee b \equiv b \vee a$$
Distributivity
$$a \wedge (b \vee c) \equiv (a \wedge b) \vee (a \wedge c), \quad a \vee (b \wedge c) \equiv (a \vee b) \wedge (a \vee c)$$
Idempotence
$$a \wedge a \equiv a, \quad a \vee a \equiv a$$
Truth and falsum
$$a \vee (\neg a) \equiv \top, \quad a \wedge \top \equiv a, \quad a \wedge (\neg a) \equiv \bot, \quad a \vee \bot \equiv a$$
de Morgan's laws
$$\neg(a \wedge b) \equiv (\neg a) \vee (\neg b), \quad \neg(a \vee b) \equiv (\neg a) \wedge (\neg b)$$

Many more identities can be deduced (proved) from the above axioms, such as the following:

Example 2.1.

(i) It immediately follows from the axioms that $a \equiv a \wedge \top \equiv a \wedge (p \vee \neg p) \equiv (a \wedge p) \vee (a \wedge \neg p)$.

(ii) The *absorbing properties* of truth and falsum, i.e., $a \vee \top \equiv \top$ and $a \wedge \bot \equiv \bot$ follow from the axioms. We show the former: $a \vee \top \equiv a \vee (a \vee \neg a) \equiv (a \vee a) \vee (\neg a) \equiv a \vee (\neg a) \equiv \top$.

(iii) One can also prove *the absorption laws*: $a \wedge (a \vee b) \equiv a$ and $a \vee (a \wedge b) \equiv a$. Let us show the latter by using (ii) above: $a \vee (a \wedge b) \equiv (a \wedge \top) \vee (a \wedge b) \equiv a \wedge (\top \vee b) \equiv a \wedge (b \vee \top) \equiv a \wedge \top \equiv a$.

(iv) The *double negation law* $\neg\neg a \equiv a$ can be proved as follows: $\neg\neg a \equiv (\neg\neg a) \wedge \top \equiv (\neg\neg a) \wedge (a \vee \neg a) \equiv (\neg\neg a \wedge a) \vee (\neg\neg a \wedge \neg a) \equiv (\neg\neg a \wedge a) \vee (\bot) \equiv (a \wedge \neg\neg a) \vee (a \wedge \neg a) \equiv a \wedge (\neg\neg a \vee \neg a) \equiv a \wedge \top \equiv a$. $\diamond$

We show that *all* the valid laws, according to the truth-table semantics, can be proved from the above axioms; thus we have a complete axiomatic system for Boolean equivalences.

Theorem 2.2 (completeness).
If $a \equiv b$ is valid according to the truth-table semantics, then it is provable from the axioms.

A proof can proceed by normalizing the Boolean terms, or propositional formulas. A (propositional) formula a is said to be in *disjunctive normal form* (DNF) when it is a disjunction of some formulas each of which is a conjunction of some atomic or negated atomic formulas (introduced at the beginning of this section); i.e., $a = \bigvee_i c_i$ where each c_i is $\bigwedge_j \ell_{(i,j)}$ for some atoms or negated-atoms $\ell_{(i,j)}$. Let us recall that, when i ranges over a finite set $\{0, 1, \dots\}$, by $\bigvee_i c_i$ we mean $c_0 \vee c_1 \vee \cdots$, and by $\bigwedge_j d_j$ we mean $d_0 \wedge d_1 \wedge \cdots$. If p is an atom, then (p) and $(\neg p)$ are both DNF; if q is another atom, then the four formulas $(p) \vee (q)$, $(p) \vee (\neg p \wedge q)$, $(p \wedge \neg q) \vee (q)$, and $(p \wedge q) \vee (p \wedge \neg q) \vee (\neg p \wedge q)$ are equivalent DNF's.

Every propositional formula can be seen to be equivalent to a DNF formula, and this can be proved by the above axioms: firstly implication ($\rightarrow$) does not appear in our formulas; and secondly by the double negation law, proved in Example 2.1(iv), and de Morgan's laws, negations ($\neg$) can be pushed as far as possible inside the sub-formulas, so that they appear at most behind atoms. Finally, by distributing all the conjunctions over disjunctions, if any, an equivalent DNF formula is obtained; and this equivalence is provable from the above axioms.

Proof of Theorem 2.2. Assume that all the atoms that appear in a and b belong to the set $\{p_0, \dots, p_k\}$; a and b are provably equivalent to some DNF formulas, such as e.g. $a \equiv \bigvee_i c_i$ and $b \equiv \bigvee_j d_j$ where c_i's and d_j's are conjunctions of some atoms or negated atoms. By Example 2.1(i) we can assume that all the atoms $p_0, \dots, p_k$ appear exactly once in each c_i and d_j.[1] By this assumption, we show that each c_i is equal to some d_j, and vice versa. Thus, a and b are provably equivalent. For a fixed c_i consider the evaluation that maps an atom to $\top$ if it appears positively in c_i, and maps it to $\bot$ if it appears negatively in c_i. Under that evaluation, c_i, and so a, is mapped to $\top$; thus b should be mapped to $\top$ too. So, some d_j should be mapped to $\top$ under that evaluation; and this is possible only when $d_j = c_i$. □

The completeness of propositional logic with respect to the truth-table semantics follows from Theorem 2.2. For example, the validity of the formula $[(p \rightarrow q) \rightarrow p] \rightarrow p$, Peirce's Law (1885), can be proved by first translating $a \rightarrow b$ to $\neg a \vee b$, and then showing the equivalence $\big(\neg[\neg(\neg p \vee q) \vee p] \vee p\big) \equiv \top$ by the above axioms.

We will come back to mathematical *identities* at the end of the paper (Section 7); before that let us study the axiomatizability of some mathematical structures.

3. Axiomatizability and quantifier elimination

We saw in the previous section that propositional logic is axiomatizable in the sense that there exists a set of axioms from which all (logically) valid formulas and only the valid formulas can be derived. This logic is also decidable in the sense that there exists an algorithm, namely truth-tables, for recognizing whether a give propositional formula is logically valid or not. A first-order theory is called *complete* when it either proves or refutes every sentence over its language. A way of proving the completeness of a (first-order) theory is reducing it to propositional logic, which is usually done through the process of quantifier elimination.

Definition 3.1 (effective quantifier elimination, QE).

[1] If some p_k does not appear in some c_i, then we can replace c_i with $(c_i \wedge p_k) \vee (c_i \wedge \neg p_k)$. By the laws of Idempotence and Truth and Falsum every atom can appear at most once in c_i.

A theory T is said to admit *effective quantifier elimination* (QE) when there exists an algorithm that for a given formula $\varphi(\vec{x})$ as input, with the shown free variables, outputs a quantifier-free formula $\theta(\vec{x})$ with exactly the same free variables $(\vec{x})$ such that T proves $\forall\vec{x}[\varphi(\vec{x}) \leftrightarrow \theta(\vec{x})]$. $\diamond$

A quantifier elimination for a theory T requires, for a given formula $\varphi(\vec{x})$, the mere existence of a T-equivalent quantifier-free formula $\theta(\vec{x})$; without requiring θ to be algorithmically obtainable from φ. Quantifier elimination is usually done by the means of the following fundamental lemma, which is proved also in [4, Theorem 31F], [10, Theorem 4.1], and [19, Lemma III.4.1].

Lemma 3.2 (main lemma of quantifier elimination).
A theory T admits QE if and only if there exists an algorithm that for every given formula of the form $\exists x\gamma(x)$, where $\gamma(x)$ is a conjunction of some atoms or negated atoms, outputs a quantifier-free formula θ such that the free variables of θ are all the free variables of $\gamma(x)$ other than x, and the universal closure of $[\exists x\gamma(x) \leftrightarrow \theta]$ is provable in T.

Proof. The "only if" part of the lemma is trivial. For the "if" part, let φ be an arbitrary formula. We show that it is T-equivalent to a quantifier-free formula with the same free variables (as of φ) and that quantifier-free formula can be found algorithmically. Take one of the innermost quantifiers of φ; such as $\forall x\theta(x)$ or $\exists x\theta(x)$ where θ is a quantifier-free formula. In the former case, consider $\neg\exists x\neg\theta(x)$; so without loss of generality, we can assume that the quantifier is existential. We saw that every propositional formula is equivalent to a DNF formula. So, $\exists x\theta(x) \equiv \exists x \bigvee_i \gamma_i(x) \equiv \bigvee_i \exists x\gamma_i(x)$, where each $\gamma_i(x)$ is a conjunction of some atomic or negated atomic formulas. By the assumption, the existing algorithm can find a T-equivalent quantifier-free formula for each $\exists x\gamma_i(x)$; thus that algorithm can find a T-equivalent formula for φ with one less quantifier (than φ). So, by an inductive argument one can show the existence of an algorithm that outputs a quantifier-free formula with the same free variables (as of φ) that is moreover T-equivalent to φ. $\square$

Quantifier elimination is applicable for axiomatizing the complete first-order theory of a structure $\mathfrak{A}$ when we have a candidate theory T in a way that (i) all the axioms of T are true in $\mathfrak{A}$, (ii) T admits QE, and (iii) T either proves or refutes every atomic sentence. Then, T is a complete theory and so it *completely axiomatizes* $\mathfrak{A}$. Thus, T proves every sentence that is true in $\mathfrak{A}$, and refutes every sentence that is not true in $\mathfrak{A}$.

In the following, we will study the structures in Table 1, the number systems $(\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C})$ over the first-order languages that may contain $<$, $+$, $\times$, or $\mathfrak{exp}$.

4. Number systems (order and addition)

Let us first study the order relation ($<$) in number systems. We recall that an *order* is a binary relation that is antisymmetric, transitive, and linear (see the axioms $\mathtt{A}_<$, $\mathtt{T}_<$, $\mathtt{L}_<$ in Theorem 4.1). The order is dense in $\mathbb{Q}$ and $\mathbb{R}$ (see $\mathtt{D}_<$ in Theorem 4.1) and has no endpoints (see $\mathtt{U}_<$ and $\mathtt{B}_<$ in Theorem 4.1). This is all the first-order theory of order can say in $\mathbb{Q}$ and $\mathbb{R}$, since it is a complete theory (first proved by Cantor 1895). However, the structure $\langle\mathbb{Q}; <\rangle$ is very different from the structure $\langle\mathbb{R}; <\rangle$, since the latter is complete (every nonempty and bounded subset has a supremum) while the former is not; also by Cantor's (1874) result, the former is countable but the latter is not.

Theorem 4.1 (an axiomatization for $\langle\mathbb{R}; <\rangle$ and $\langle\mathbb{Q}; <\rangle$).

The (finite) theory of dense linear orders without endpoints (with the following axioms) completely axiomatizes both $\langle \mathbb{R}; < \rangle$ and $\langle \mathbb{Q}; < \rangle$.

($\mathtt{A}_<$) $\forall x, y\, (x < y \to y \not< x)$
($\mathtt{T}_<$) $\forall x, y\, (x < y < z \to x < z)$
($\mathtt{L}_<$) $\forall x, y\, (x < y \vee x = y \vee y < x)$
($\mathtt{D}_<$) $\forall x, y\, (x < y \to \exists w\, [x < w < y])$
($\mathtt{U}_<$) $\forall x \exists u\, (x < u)$
($\mathtt{B}_<$) $\forall x \exists v\, (v < x)$

Proof. Note that the axioms are true in $\langle \mathbb{R}; < \rangle$ and $\langle \mathbb{Q}; < \rangle$; so, it suffices to show that the above theory admits QE. For that we use Lemma 3.2 and show the equivalence of every formula of the form $\exists x \bigwedge_i \gamma_i(x)$ to a quantifier-free formula, where each γ_i is an atom or negated atom. The equivalences $\neg(a < b) \leftrightarrow (a = b) \vee (b < a)$ and $\neg(a = b) \leftrightarrow (a < b) \vee (b < a)$, which are provable in the theory, allow us to neglect negated atomic formulas. Thus, we need to eliminate the quantifier of the formulas of the form $\exists x \big(\bigwedge_i u_i < x \wedge \bigwedge_j x < v_j \wedge \bigwedge_k x = w_k \big)$ only — note that $x = x$ is equivalent to $\top$, and $x < x$ to $\bot$. But that formula is equivalent to $\bigwedge_i u_i < w_0 \wedge \bigwedge_j w_0 < v_j \wedge \bigwedge_k w_0 = w_k$, if the conjunction $\bigwedge_k x = w_k$ is non-empty, and to $\bigwedge_{i,j} u_i < v_j$, if it is empty (non-existent) and none of the other conjunctions are empty; if any of $\bigwedge_i u_i < x$ or $\bigwedge_j x < v_j$ is also empty, then the original formula is equivalent to $\top$. □

The order relation behaves very differently on $\mathbb{Z}$ and $\mathbb{N}$, since here it is a *discrete* order, in the sense that every element has an immediate successor. Let us denote the successor function $x \mapsto (x+1)$ by $\mathfrak{s}$; and let $(x \leqslant y)$ abbreviate $(x < y) \vee (x = y)$. For a proof of the following theorem, first proved by Robinson & Zakon (1960), see e.g. [1, Theorem 2].

Theorem 4.2 (an axiomatization for $\langle \mathbb{Z}; < \rangle$).
The (finitely axiomatized) theory of discrete linear orders without endpoints completely axiomatizes $\langle \mathbb{Z}; <, \mathfrak{s} \rangle$; this theory consists of the axioms $\mathtt{A}_<$, $\mathtt{T}_<$, $\mathtt{L}_<$ (Theorem 4.1) along with

($\mathtt{S}_<$) $\forall x, y\, (x < y \leftrightarrow \mathfrak{s}(x) \leqslant y)$
($\mathtt{P}_<$) $\forall x \exists w\, (\mathfrak{s}(w) = x)$ □

The following, due to Langford (1927), has been proved in e.g. [4, Theorem 32A].

Theorem 4.3 (an axiomatization for $\langle \mathbb{N}; < \rangle$).
The (finitely axiomatizable) theory of discrete linear orders with the least element and without the last element completely axiomatizes $\langle \mathbb{N}; 0, <, \mathfrak{s} \rangle$; this theory consists of the axioms $\mathtt{A}_<$, $\mathtt{T}_<$, $\mathtt{L}_<$ (Theorem 4.1) together with $\mathtt{S}_<$ (Theorem 4.2) and

($\mathtt{Z}_<$) $\forall x\, (0 \leqslant x)$
($\mathtt{P}^0_<$) $\forall x \exists w\, (0 < x \to \mathfrak{s}(w) = x)$ □

Let us note that $\forall x\, [x < \mathfrak{s}(x)]$ is provable from the axiom $\mathtt{S}_<$ (Theorem 4.2); and so one can show that $\forall x, y\, [x < y \leftrightarrow \mathfrak{s}(x) < \mathfrak{s}(y)]$ follows from $\mathtt{S}_<$, $\mathtt{T}_<$ and $\mathtt{L}_<$ (Theorems 4.1,4.2). Therefore, Dedekind–Peano's (1888,1889) axioms $\forall x\, (\mathfrak{s}(x) \neq 0)$ and $\forall x, y\, (\mathfrak{s}(x) = \mathfrak{s}(y) \to x = y)$ are provable from the axiom system $\{\mathtt{A}_<, \mathtt{T}_<, \mathtt{L}_<, \mathtt{S}_<, \mathtt{Z}_<\}$ (Theorems 4.1,4.2,4.3).

4.1. The addition operation. We now study the addition operation $(+)$ in number systems. The most obvious properties of addition are associativity and commutativity (see $\mathtt{A}_+$ and $\mathtt{C}_+$ in Theorem 4.4). Of course, in all of our number systems there is an additive unit element (zero 0), and in all but one (the natural numbers) every element has an additive inverse (the minus element). In $\mathbb{C}, \mathbb{R}$, and $\mathbb{Q}$ addition is torsion-free and divisible (see $\mathtt{T}_+$ and $\mathtt{D}_+$ in Theorem 4.4); it is hard to find any other property of $+$ in $\mathbb{C}, \mathbb{R}, \mathbb{Q}$ that does not follow from the above-mentioned properties.

For axiomatizing the structures $\langle \mathbb{C}; + \rangle$, $\langle \mathbb{R}; + \rangle$, and $\langle \mathbb{Q}; + \rangle$ we add the constant symbol 0 and the unary function symbol $-$ to the language; needless to say, $n \cdot x$ abbreviates the expression $x + \cdots + x$ (n times) for $n \in \mathbb{N}$.

Theorem 4.4 (an axiomatization for $\langle \mathbb{C}; + \rangle$, $\langle \mathbb{R}; + \rangle$, $\langle \mathbb{Q}; + \rangle$).
The first-order theory of non-trivial, divisible, torsion-free, and commutative groups (with the following infinite set of axioms) completely axiomatizes the structures $\langle \mathbb{Q}; 0, -, + \rangle$, $\langle \mathbb{R}; 0, -, + \rangle$, and $\langle \mathbb{C}; 0, -, + \rangle$.

$(\mathtt{A}_+)$ $\forall x, y, z\ (x + (y + z) = (x + y) + z)$
$(\mathtt{C}_+)$ $\forall x, y\ (x + y = y + x)$
$(\mathtt{U}_+)$ $\forall x\ (x + 0 = x)$
$(\mathtt{I}_+)$ $\forall x\ (x + (-x) = 0)$
$(\mathtt{N}_+)$ $\exists u\ (u \neq 0)$
$(\mathtt{T}_+)$ $\{\forall x\ (n \cdot x = 0 \to x = 0)\}_{n>0}$
$(\mathtt{D}_+)$ $\{\forall x \exists v\ (x = n \cdot v)\}_{n>0}$

Proof. We show that the theory admits QE by using Lemma 3.2. Every atomic formula in the language $\{0, -, +\}$ that contains x can be equivalently written in the form $n \cdot x = t$ for some $n \in \mathbb{N}^+$ and some x–free term t. By $a = b \longleftrightarrow k \cdot a = k \cdot b$, which is provable from the above axioms, it suffices to eliminate the quantifier of $\exists x \big(\mathbb{\bigwedge}_i q \cdot x = t_i \wedge \mathbb{\bigwedge}_j q \cdot x \neq s_j \big)$, which by $\mathtt{D}_+$ (for $n = q$) is equivalent to $\exists y \big(\mathbb{\bigwedge}_i y = t_i \wedge \mathbb{\bigwedge}_j y \neq s_j \big)$. Now, if the conjunct $\mathbb{\bigwedge}_i y = t_i$ is nonempty, then this is equivalent to $\mathbb{\bigwedge}_i t_0 = t_i \wedge \mathbb{\bigwedge}_j t_0 \neq s_j$, and if $\mathbb{\bigwedge}_i y = t_i$ is empty, then it is equivalent to $\top$, since by $\mathtt{N}_+$ there are infinitely many members (for any $u \neq 0$ we have $n \cdot u \neq m \cdot u$ for every $n \neq m$). □

The axiomatization of $\langle \mathbb{Z}; + \rangle$ illustrates a case that one might need to substantially enrich the language of the structure to have QE. As an example, $\exists v\ (x = v + v)$, stating that x is even, is not equivalent to any quantifier-free formula in $\langle \mathbb{Z}; 0, -, + \rangle$.[2] However, if we add the binary relation symbol $\equiv_2$ of congruence modulo 2 to the language, then that formula will be equivalent to $x \equiv_2 0$.

The quantifier elimination of the theory of the structure $\langle \mathbb{Z}; 0, 1, \{\equiv_n\}_{n>1}, -, + \rangle$ can be shown by using a generalized form of the Chinese Remainder Theorem in Number Theory. The Chinese remainder theorem says that a given system of congruence equations $\{x \equiv_{n_i} r_i\}_{i<N}$ has a solution (in $\mathbb{Z}$) if n_i and n_j are coprime for every $i < j < N$. The generalized Chinese remainder theorem says that the system $\{x \equiv_{n_i} r_i\}_{i<N}$ of congruence equations has a solution if and only if for every $i < j < N$ we have $r_i \equiv_{d_{i,j}} r_j$, where $d_{i,j}$ is the greatest common divisor of n_i and n_j. Since such systems either have no solution or have infinitely many solutions, then we can state this more general theorem as follows.

[2] Since the set of even integers is neither finite nor cofinite (i.e., with finite complement), but it can be shown that every set definable in $\langle \mathbb{Z}; 0, -, + \rangle$ by a quantifier-free formula is either finite or cofinite. To see this it suffices to note that the class of finite and cofinite subsets of $\mathbb{Z}$ is closed under complementation, intersection, and union; and every atomic formula with the only free variable x is equivalent in $\langle \mathbb{Z}; 0, -, + \rangle$ to $mx + n = 0$ for some $m, n \in \mathbb{Z}$.

Proposition 4.5 (general Chinese remainder theorem).
If $n_i > 1$ for every $i < N$, then for every $\{r_i\}_{i<N}$ and $\{s_j\}_{j<M}$,

$$\exists x\big(\mathbb{\Lambda}_{i<N} x \equiv_{n_i} r_i \wedge \mathbb{\Lambda}_{j<M} x \neq s_j\big) \Longleftrightarrow \mathbb{\Lambda}_{i<j<N} r_i \equiv_{d_{i,j}} r_j,$$

where $d_{i,j}$ is the greatest common divisor of n_i and n_j. □

For three different proofs of Proposition 4.5, which is a kind of QE by itself, see [16, Propositions 4.5 and 4.1] and [1, Proposition 2] which are due to Ore (1951), Mahler (1958) and Fraenkel (1963), respectively.

We add the congruence relations $\equiv_n$ modulo every natural $n > 1$, along with the constant 1, to the language; let $\bar{i}$ abbreviate $1+\cdots+1$ (i times) for every $i \in \mathbb{N}$.

Theorem 4.6 (an axiomatization for $\langle \mathbb{Z}; + \rangle$).
The theory whose axioms are $\mathtt{A}_+$, $\mathtt{C}_+$, $\mathtt{U}_+$, $\mathtt{I}_+$, and $\mathtt{T}_+$ (Theorem 4.4) with the following axioms completely axiomatizes the structure $\langle \mathbb{Z}; 0, 1, \{\equiv_n\}_{n>1}, -, + \rangle$.

($\mathtt{E}^+$) $\{\forall x, y\,[x \equiv_n y \leftrightarrow \exists u(x = y + n \cdot u)]\}_{n>1}$
($\mathtt{E}_+$) $\big\{\forall x\,\big[\mathbb{V}_{i<n}(x \equiv_n \bar{i})\big]\big\}_{n>1}$
($\mathtt{E}'_+$) $\big\{\mathbb{\Lambda}_{0<i<n}(\bar{i} \not\equiv_n 0)\big\}_{n>1}$

Proof. For showing that the theory admits QE by Lemma 3.2, we note that every atomic formula of x in $\{0, 1, -, +\} \cup \{\equiv_n | \, n > 1\}$ is equivalent to either $m \cdot x = t$ or $m \cdot x \equiv_n t$ for some $m, n \in \mathbb{N}^+$ and some x–free term t. By the provable equivalence $(a \not\equiv_n b) \leftrightarrow \mathbb{V}_{0<i<n}(a \equiv_n b + \bar{i})$ it suffices to show that the formula $(*)$ $\exists x\big(\mathbb{\Lambda}_i q_i \cdot x \equiv_{n_i} r_i \wedge \mathbb{\Lambda}_j q_j \cdot x \neq s_j \wedge \mathbb{\Lambda}_k q_k \cdot x = t_k\big)$ is equivalent to a quantifier-free formula. From the provable equivalences $(a = b) \leftrightarrow (k \cdot a = k \cdot b)$ and $(a \equiv_n b) \leftrightarrow (k \cdot a \equiv_{kn} k \cdot b)$ we can assume that all the q_i's, q_j's and q_k's are equal, to say q. Then, $(*)$ is equivalent to $\exists y\big(y \equiv_q 0 \wedge \mathbb{\Lambda}_i\, y \equiv_{n_i} r_i \wedge \mathbb{\Lambda}_j\, y \neq s_j \wedge \mathbb{\Lambda}_k\, y = t_k\big)$. We can assume that the conjunct $\mathbb{\Lambda}_k\, y = t_k$ is empty (see the proofs of Theorems 4.1 and 4.4); now the result immediately follows from Proposition 4.5 (which is provable from the stated axioms). □

As for $\mathbb{N}$, even $\{0, 1, -, +\} \cup \{\equiv_n | \, n > 1\}$ is not sufficiently rich for QE, since the formula $\exists v(x + v = y)$ is not equivalent in $\langle \mathbb{N}; 0, 1, \{\equiv_n\}_{n>1}, -, + \rangle$ to a quantifier-free formula (it is equivalent to $x \leqslant y$).[3] Here, QE is possible when we add the order relation to the language.

Theorem 4.7 (an axiomatization for $\langle \mathbb{N}; <, + \rangle$).
The theory with the axioms $\mathtt{A}_<$, $\mathtt{T}_<$, $\mathtt{L}_<$ (Theorem 4.1), $\mathtt{S}_<$ (Theorem 4.2), $\mathtt{Z}_<$, $\mathtt{P}^0_<$ (Theorem 4.3), $\mathtt{A}_+$, $\mathtt{C}_+$, $\mathtt{U}_+$ (Theorem 4.4), $\mathtt{E}^+$, $\mathtt{E}_+$ (Theorem 4.6) with the following axioms completely axiomatizes the structure $\langle \mathbb{N}; 0, 1, <, \{\equiv_n\}_{n>1}, + \rangle$.

($\mathtt{M}_+$) $\forall x, y\,(x < y \rightarrow \exists v\,[x + v = y])$
($\mathtt{O}_+$) $\forall x, y, z\,(x < y \rightarrow x + z < y + z)$ □

[3] For a proof, let us call a binary relation $R \subseteq \mathbb{N}^2$ *finite-bounded* when there is a fixed $N \in \mathbb{N}$ such that for every $y \in \mathbb{N}$ the set $\{x \in \mathbb{N} \mid (x, y) \in R\}$ is either infinite or finite with size less than N. The order relation $\leqslant \subseteq \mathbb{N}^2$ is not finite-bounded, but every binary relation definable by a quantifier-free formula in $\langle \mathbb{N}; 0, 1, \{\equiv_n\}_{n>1}, -, + \rangle$ can be shown to be finite-bounded. To see this let us firstly note that the class of finite-bounded binary relations is closed under union. Secondly, every quantifier-free formula with the only free variables x, y is equivalent to $\mathbb{V}_i \mathbb{\Lambda}_j \eta_{i,j}(x, y)$ for some atomic or negated atomic formulas $\eta_{i,j}$. Every atomic formula is equivalent in $\langle \mathbb{N}; 0, 1, \{\equiv_n\}_{n>1}, -, + \rangle$ to either $kx + ly + m \equiv_n 0$ or $kx + ly + m = 0$ for some $k, l, m, n \in \mathbb{Z}$. By $u \not\equiv_n 0 \leftrightarrow \mathbb{V}_{1<i<n} u + \bar{i} \equiv_n 0$ it suffices to consider the negated-atomic formulas of the form $kx + ly + m \neq 0$ only. Therefore, it is enough to see that the binary relation on x, y defined by $\mathbb{\Lambda}_h k_h x + l_h y + m_h \equiv_{n_h} 0 \wedge \mathbb{\Lambda}_i k_i x + l_i y + m_i = 0 \wedge \mathbb{\Lambda}_j k_j x + l_j y + m_j \neq 0$ is finite-bounded; indeed, for a fixed y the set of x's that satisfy this formula is either infinite or finite with size less than 2.

A proof of Theorem 4.7 can be found in [4, Theorem 32E] where no explicit axiomatization is presented; though, one can see that the proof goes through with our suggested axioms. For a proof of the following theorem (due to Presburger 1929) see e.g. [1, Theorem 5]; other proofs can be found in [10, § 4.III] and [19, §§ III.4.2].

Theorem 4.8 (an axiomatization for $\langle \mathbb{Z}; <, + \rangle$).
The theory with the axioms $\mathtt{A}_<$, $\mathtt{T}_<$, $\mathtt{L}_<$ (Theorem 4.1), $\mathtt{S}_<$ and $\mathtt{P}_<$ (Theorem 4.2), $\mathtt{A}_+$, $\mathtt{C}_+$, $\mathtt{U}_+$, $\mathtt{I}_+$ (Theorem 4.4), $\mathtt{E}_+$ (Theorem 4.6), and $\mathtt{O}_+$ (Theorem 4.7), with $\mathfrak{s}(x)$ set to $x+1$, completely axiomatizes the structure $\langle \mathbb{Z}; 0, 1, <, \{\equiv_n\}_{n>1}, -, + \rangle$. □

The following theorem (stating that the order and addition structure of rational and real numbers can be axiomatized by the theory of non-trivial divisible commutative ordered groups) can be proved by combining the techniques of the proofs of Theorems 4.1 and 4.4 (cf. [1, Theorem 4]).

Theorem 4.9 (axiomatizing $\langle \mathbb{Q}; <, + \rangle$ and $\langle \mathbb{R}; <, + \rangle$).
The theory with the axioms $\mathtt{A}_<$, $\mathtt{T}_<$, $\mathtt{L}_<$ (Theorem 4.1), $\mathtt{A}_+$, $\mathtt{C}_+$, $\mathtt{U}_+$, $\mathtt{I}_+$, $\mathtt{N}_+$, $\mathtt{D}_+$ (Theorem 4.4), and $\mathtt{O}_+$ (Theorem 4.7) completely axiomatizes $\langle \mathbb{Q}; 0, <, -, + \rangle$ and $\langle \mathbb{R}; 0, <, -, + \rangle$. □

Let us note that the axioms $\mathtt{D}_<$, $\mathtt{U}_<$, $\mathtt{B}_<$ (in Theorem 4.1) and $\mathtt{T}_+$ (in Theorem 4.4) are provable from the axiom system presented in Theorem 4.9 just the way that are proved in classical analysis.

5. Number systems (addition and multiplication)

Definition 5.1 (field).
A *field* is a structure over $\{0, 1, +, -, \times, ^{-1}\}$ that satisfies $\mathtt{A}_+$, $\mathtt{C}_+$, $\mathtt{U}_+$, $\mathtt{I}_+$ (Theorem 4.4), and the following axioms:

($\mathtt{Z}_1$) $0 \neq 1$
($\mathtt{A}_\times$) $\forall x, y, z\, (x \cdot (y \cdot z) = (x \cdot y) \cdot z)$
($\mathtt{C}_\times$) $\forall x, y\, (x \cdot y = y \cdot x)$
($\mathtt{U}_\times$) $\forall x\, (x \cdot 1 = x)$
($\mathtt{I}_\times$) $\forall x\, (x \neq 0 \to x \cdot x^{-1} = 1)$
($\mathtt{D}_\times$) $\forall x, y, z\, [x \cdot (y + z) = (x \cdot y) + (x \cdot z)]$

A field has *characteristic zero* if it moreover satisfies

($\mathtt{C}_0$) $\{\overline{n} \neq 0\}_{n>0}$

where, as we recall, $\overline{n}$ abbreviate $1 + \cdots + 1$ (n times). ◇

The field $\langle \mathbb{C}; +, \times \rangle$ is well known to be algebraically closed since it satisfies the Fundamental Theorem of Algebra, i.e., it has a root for every non-trivial polynomial (with coefficients in $\mathbb{C}$). It can be even said that it was created for having all the roots of the polynomials (with real or complex coefficients). This is all one can say about the complex field in the first-order setting, since the theory of algebraically closed fields of characteristic zero is complete, and so it axiomatizes $\langle \mathbb{C}; +, \times \rangle$. The following result was proved by Tarski (1936); see e.g. [10, § 4.IV] for a proof.

Theorem 5.2 (an axiomatization for $\langle \mathbb{C}; +, \times \rangle$).
The theory of algebraically closed fields of characteristic zero, with the axioms $\mathtt{A}_+$, $\mathtt{C}_+$, $\mathtt{U}_+$, $\mathtt{I}_+$, $\mathtt{A}_\times$, $\mathtt{C}_\times$, $\mathtt{U}_\times$, $\mathtt{I}_\times$, $\mathtt{D}_\times$, $\mathtt{C}_0$ (Definition 5.1) along with the following axioms, completely axiomatizes the structure $\langle \mathbb{C}; 0, 1, -, +, \times, ^{-1} \rangle$.

$(\mathtt{FTA}_{\mathbb{C}})$ $\{\forall\langle a_i\rangle_{i<n}\exists x\,(x^n+\sum_{i<n}a_i x^i=0)\}_{n>1}$ □

For super-careful readers, let us note that (i) every non-trivial polynomial can be taken to be a monic by dividing it with the leading (non-zero) coefficient; (ii) the multiplicative inversion $(x\mapsto x^{-1})$ is not really a total function, since it is not defined on zero, but one can make the convention $0^{-1}=0$ without any danger; (iii) and finally, x^i abbreviates the algebraic expression $x\times\cdots\times x$ (i times) of course.

For studying the structure $\langle\mathbb{R};+,\times\rangle$ we first note that the order relation is definable in it: $u\leqslant v\iff\exists x(u+x^2=v)$; and $\langle\mathbb{R};<,+,\times\rangle$ is an ordered field. An ordered field satisfies the order axioms $\mathtt{A}_<$, $\mathtt{T}_<$, $\mathtt{L}_<$ (Theorem 4.1), the axioms of fields (in Definition 5.1), $\mathtt{O}_+$ (Theorem 4.7), and $\mathtt{O}_\times$ (Theorem 5.3 below).

Of course, this is not all one can say about $\langle\mathbb{R};<,+,\times\rangle$. On the other hand, not much can one say about it in the first-order framework; only that every polynomial of even degree can be factorized into some quadratic polynomials (see $\mathtt{FTA}_{\mathbb{R}}$ in Theorem 5.3). This last statement is indeed equivalent to (a real version of) the fundamental theorem of algebra. Here are some examples:

$$x^4+a^4=(x^2+\sqrt{2}\,ax+a^2)(x^2-\sqrt{2}\,ax+a^2)\text{ for }a\in\mathbb{R};\text{[4]}$$

$$x^4-x+\tfrac{3}{4}=\Big(x^2+\sqrt{2\cos 20^\circ}\,x+\cos 20^\circ+\tfrac{1}{2\sqrt{2\cos 20^\circ}}\Big)\Big(x^2-\sqrt{2\cos 20^\circ}\,x+\cos 20^\circ-\tfrac{1}{2\sqrt{2\cos 20^\circ}}\Big);$$

$$x^4+ax^2+a^2=\begin{cases}(x^2+\sqrt{a}\,x+a)(x^2-\sqrt{a}\,x+a) & \text{if } a>0,\\ (x^2+\sqrt{-3a}\,x-a)(x^2-\sqrt{-3a}\,x-a) & \text{if } a<0.\end{cases}$$

Theorem 5.3 (an axiomatization for $\langle\mathbb{R};<,+,\times\rangle$).
Theory of real closed ordered fields which is axiomatized by $\mathtt{A}_<$, $\mathtt{T}_<$, $\mathtt{L}_<$ (Theorem 4.1), the axioms of fields (Definition 5.1), and $\mathtt{O}_+$ (Theorem 4.7) along with the following axioms completely axiomatizes the structure $\langle\mathbb{R};0,1,<,-,+,\times,{}^{-1}\rangle$.

$(\mathtt{O}_\times)$ $\forall x,y,z\,(0<z\wedge x<y\to x\cdot z<y\cdot z)$

$(\mathtt{FTA}_{\mathbb{R}})$ $\{\forall\langle a_i\rangle_{i<2n}\exists\langle b_j,c_j\rangle_{j<n}\forall x\,[(x^{2n}+\sum_{i<2n}a_i x^i)=\prod_{j<n}(x^2+b_j x+c_j)]\}_{n>1}$ □

For a proof of this result of Tarski (1936) see e.g. [17, Appendix], which is a modified version of the proof presented in [10, § 4.V]. Let us note a consequence of $\mathtt{FTA}_{\mathbb{R}}$:

Proposition 5.4 ($\mathtt{FTA}_{\mathbb{R}}\Longrightarrow\mathtt{S}_\times$).
If every quartic monic is equal to the product of two quadratic monics in an ordered field, then every positive element has a square root in that field.

$(\mathtt{S}_\times)$ $\forall x\,(0<x\to\exists u\,[x=u^2])$

Proof. Let $a>0$; by the assumption, $x^4+ax^2+a^2$ is equal to $(x^2+bx+c)(x^2+ux+v)$ for some elements b,c,u,v in the ordered field. So, $u=-b$ and $vc=a^2$; thus (i) $c^2+a^2=c(b^2+a)$ and (ii) $ba^2=bc^2$. If $b=0$, then (i) implies that $c^2-ac+a^2=0$, so $(2c-a)^2+3a^2=0$, a contradiction. Whence, $b\neq 0$; now, (ii) implies that $a^2=c^2$. So, we have either $c=a$ or $c=-a$. If $c=-a$, then by (i) we should have $b^2=-3a<0$, another contradiction. Therefore, $c=a$; and so by (i) we have $b^2=a$. Thus, a has a square root. □

We note that by $\mathtt{S}_\times$ (and the axioms of ordered fields) the high-school equivalence for the existence of the roots of quadratic polynomials can be proved:

[4] As the history goes, Leibniz (1702) mistakenly thought that x^4+a^4 is not equal to a product of quadratics! This identity is due to Bernoulli (1719).

$$\exists x(x^2+bx+c=0)\leftrightarrow\exists x[(2x+b)^2=b^2-4c]\leftrightarrow b^2\geq 4c.$$

It can be easily seen that $\boldsymbol{FTA}_{\mathbb{C}}$ (in Theorem 5.2) is equivalent to the statement that every monic is equal to the product of some linear polynomials:

$$\boldsymbol{FTA}_{\mathbb{C}} \equiv\!\equiv \{\forall\langle a_i\rangle_{i<n}\exists\langle b_j\rangle_{j<n}\forall x\,[(x^n+\textstyle\sum_{i<n}a_ix^i)=\prod_{j<n}(x+b_j)]\}_{n>1},$$

which resembles $\boldsymbol{FTA}_{\mathbb{R}}$ (in Theorem 5.3). Let us note some other consequences of $\boldsymbol{FTA}_{\mathbb{R}}$ (from [17]):

Proposition 5.5 ($\boldsymbol{FTA}_{\mathbb{R}} \Longrightarrow \boldsymbol{RCF}+\boldsymbol{IVT}$).
If every even-degree monic can be factorized into some quadratic monics in an ordered field, then every odd-degree polynomial has a root and the polynomial intermediate value theorem holds.

Proof. Suppose that the polynomial $p(x)$ is of degree m and $p(u)p(v)<0$ holds for some $u<v$. Put

$$q(x)=\frac{1}{p(u)}(1+x^2)^m\,p\Big(u+\frac{v-u}{1+x^2}\Big);$$

then $q(x)=x^{2m}+r(x^2)$ for some polynomial $r(x)$ with degree less than m. So, $q(x)$ can be factorized to say $\prod_{j<m}(x^2+b_jx+c_j)$. Now we have $\prod_{j<m}c_j=q(0)=\frac{p(v)}{p(u)}<0$ and so $c_j<0$ for some j; then we have $b_j^2>4c_j$ and so the quadratic $x^2+b_jx+c_j=0$ has a root, such as t. Now, $w=u+\frac{v-u}{1+t^2}$ is a root of $p(x)=0$ that satisfies $u<w<v$. By a classical real analytic argument, if the intermediate value theorem holds for polynomials in an ordered field, then every odd-degree polynomial has a root in that field. □

So, the fundamental theorem of algebra is really *fundamental* since it can prove some basic theorems in algebra, and it is a kind of fundamental theorem for the mathematical analysis of polynomials as well; see [17] for more details.

So far, we have discussed two applications of number theory and algebra to mathematical logic:

1. the (generalized) Chinese remainder theorem, and

2. the fundamental theorem of algebra.

1. Proposition 4.5 was used in proving that the axiomatic system suggested for the additive structure of integer numbers $\langle\mathbb{Z};+\rangle$ has QE and so it is a complete theory (Theorem 4.6). It is worth noting that Gödel (1931, Lemma 1) also had used the (non-generalized) Chinese remainder theorem in his proof of the first incompleteness theorem for the coding technicalities.
2. The truly *fundamental theorem* of elementary algebra and elementary analysis was used for axiomatizing the additive and multiplicative structures of complex and real numbers, $\langle\mathbb{C};+,\times\rangle$ and $\langle\mathbb{R};+,\times\rangle$, noting that order ($<$) is definable in $\langle\mathbb{R};+,\times\rangle$ (Theorems 5.2 and 5.3).

Now, we present two applications of mathematical logic in other areas of mathematics (especially algebraic geometry):

I. the Tarski–Seidenberg principle, and

II. Hilbert's 17th problem.

I. Theorem 5.3, like many other theorems of QE, is proved by using Lemma 3.2. Let us see how the proof can proceed: first, we note that all the atomic formulas of x over the language $\{0,1,-,+,\times,{}^{-1},<\}$ are equivalent to $p(x)=0$ or $p(x)>0$ for a polynomial p. Second, negation can be eliminated (see

the proof of Theorem 4.1), so QE over this language is equivalent to each statement of "existence of a solution for a system of polynomial equations and inequalities is equivalent to a system of some equations and inequalities between the coefficients of those polynomials". As an example, the sentence $\exists x(ax^2+bx+c=0)$ is known to be equivalent to

$$(a^2>0\wedge b^2\geqslant 4ac)\vee(a=0\wedge b^2>0)\vee(a=0\wedge b=0\wedge c=0).$$

The quoted statement above is called the Tarski–Seidenberg principle in real algebraic geometry (see [2, §1.4]), which is exactly what the translation of Lemma 3.2 would be in the proof of Theorem 5.3 (cf. [12]).

II. Hilbert's celebrated 17th problem (1900) asked (see e.g. [18]): *Given a multivariate polynomial that takes only non-negative values over the reals, can it be represented as a sum of squares of rational functions*? Let us note a couple of examples:

$$x^4-x+\tfrac{3}{4}=\left(x^2-\tfrac{1}{2}\right)^2+\left(x-\tfrac{1}{2}\right)^2+\left(\tfrac{1}{2}\right)^2,$$

$$(x^2+y^2)^2[x^4y^2+x^2y^4+1-3x^2y^2]=(x^2-y^2)^2+[x^2y(x^2+y^2-2)]^2+[xy^2(x^2+y^2-2)]^2+[xy(x^2+y^2-2)]^2.$$

A consequence of the Tarski–Seidenberg principle is the Artin–Lang homomorphism theorem [2, Theorem 4.1.2], which gives a positive answer to the problem; see [2, Theorem 6.1.1]. Let us note that by the fundamental theorem of algebra every non-negative polynomial of one variable can be written as a sum of the squares of some polynomials;[5] but there are non-negative polynomials of two variables that cannot be written as such. One example (see [18]) is Motzkin (1969)'s polynomial $x^4y^2+x^2y^4+1-3x^2y^2$; of course it is the sum of the squares of some *rational* functions (see the second example above).

5.1. Addition and multiplication on natural, integer, and rational numbers. The next structures that we study over the language $\{+,\times\}$ are $\mathbb{Q}$, $\mathbb{Z}$, and $\mathbb{N}$. Here the story becomes dramatically different. To start with, let us note that the axiomatic systems presented for the ordered structures $\langle\mathbb{N};<\rangle$, $\langle\mathbb{Z};<\rangle$, $\langle\mathbb{Q};<\rangle$, and $\langle\mathbb{R};<\rangle$ were all finite (Theorems 4.1,4.2,4.3). Other axiomatic systems were not finite, but were presented in a way that one can recognize whether a given sentence is an axiom of that system or not, in the sense that a properly designed algorithm can recognize them. In the other words, the axiomatic theories for the studied structures were decidable by an algorithm.

To make precise the forthcoming definition, let us make the convention that all our first-order individual variables are $\vartheta,\vartheta',\vartheta'',\vartheta''',\ldots$, made up from ϑ and $'$. Let us fix the following finite set of symbols as an alphabet:

$$\mathcal{A}=\{\neg,\wedge,\vee,\forall,\exists,(,),\vartheta,',0,1,<,=,+,-,\times,\mathfrak{expp}\}.$$

Every formula over the first-order language $\{0,1,<,+,-,\times,\mathfrak{expp}\}$ is a string (i.e., a finite sequence) of the elements of $\mathcal{A}$. There exists an algorithm that decides (outputs `yes` or `no`) if a given such string as input is a well-founded formula or not.

Definition 5.6 (decidability).
A set B of strings of symbols from $\mathcal{A}$ is *decidable* when there exists an algorithm such that for a given string as input outputs `yes` if it belongs to B and outputs `no` otherwise. ◇

Let us note that we have not fixed a rigorous definition for the informal notion of *algorithm* in the above definition; it could be a *recursive function* or a *Turing machine*. By the Church–Turing thesis

[5] The sum of squares for a polynomial may not be unique; for example, $(x^2+2ax+2a^2)^2=(x^2+2ax)^2+(2ax+2a^2)^2$.

(1936) all such formally rigorous and equivalent definitions do define the informal notion of algorithm; so we do not need to fix a formalization. "Axiomatizable" usually means *axiomatizable by a decidable set of axioms*; though more often the decidability of the axiom set is not explicitly mentioned.

Definition 5.7 (axiomatizability).
A theory or a structure is *axiomatizable* when there exists a decidable set of sentences that completely axiomatizes it. ◇

All the theories and structures that we have studied so far are axiomatizable by a decidable set of sentences. Actually, a structure is axiomatizable by a decidable set of sentences if and only if it has a decidable theory; see e.g. [4, Corollary 26I]. For a proof, we note that decidability implies axiomatizability, since one only needs to algorithmically list all the sentences and pick the ones that hold true; thus a decidable set of axioms is obtained. Conversely, if $\mathfrak{A}$ is axiomatizable, then for a given sentence ψ run this algorithm for consecutive n's starting from $n=1$:

> list all the theorems that are proved from the first n axioms in n steps or less
> (if n exceeds the number of axioms, then use all the finitely many axioms);
> if ψ or $\neg\psi$ appears in the list, then output **`yes`** or **`no`** accordingly.

The algorithm will surely terminate (for some n) since the axiomatic system *completely* axiomatizes $\mathfrak{A}$.

Now, the shocking result of Gödel's incompleteness theorem (1931) is that the structure $\langle \mathbb{N}; +, \times \rangle$ is not axiomatizable. As the history goes, Presburger (1929) proved the axiomatizability of $\langle \mathbb{N}; + \rangle$ and Skolem (1930) announced the axiomatizability of $\langle \mathbb{N}; \times \rangle$ (see [19]); so $\langle \mathbb{N}; +, \times \rangle$ was expected to be axiomatizable, that would give evidence for Hilbert's program.

Theorem 5.8 (non-axiomatizability of $\langle \mathbb{N}; +, \times \rangle$).
The full first-order theory of the structure $\langle \mathbb{N}; +, \times \rangle$ is not axiomatizable by any decidable set of sentences. □

Of course, there does exist an undecidable set of sentences that completely axiomatizes $\langle \mathbb{N}; +, \times \rangle$; that is the so-called *true arithmetic*, the set of all the sentences that are true in $\mathbb{N}$.

The non-axiomatizability of $\langle \mathbb{Z}; +, \times \rangle$ is inherited from $\langle \mathbb{N}; +, \times \rangle$ since the set $\mathbb{N}$ is definable in $\langle \mathbb{Z}; +, \times \rangle$ by Lagrange's (1770) four square theorem (see e.g. [19, Theorem II.3.8]). Let $\mathcal{N}(x)$ be the formula $\exists u, v, w, z (u^2+v^2+w^2+z^2=x)$; then for every $m \in \mathbb{Z}$ we have: $m \in \mathbb{N}$ if and only if $\mathcal{N}(m)$ is true in $\mathbb{Z}$. For every formula φ over $\{+, \times\}$, let $\varphi^{\mathcal{N}}$ result from φ by changing every $\forall x\, \Theta$ to $\forall x\, [\mathcal{N}(x) \to \Theta]$ and $\exists x\, \Theta$ to $\exists x\, [\mathcal{N}(x) \wedge \Theta]$; that is *relativizing* all the bounded variables to $\mathcal{N}$. Now, for every sentence ψ over $\{+, \times\}$ we have: ψ is true in $\langle \mathbb{N}; +, \times \rangle$ if and only if $\psi^{\mathcal{N}}$ is true in $\langle \mathbb{Z}; +, \times \rangle$. So, it follows that the structure $\langle \mathbb{Z}; +, \times \rangle$ is not axiomatizable by any decidable set of sentences T, since otherwise $\langle \mathbb{N}; +, \times \rangle$ would be axiomatizable by the decidable set of sentences $T' = \{\psi \mid T \text{ proves } \psi^{\mathcal{N}}\}$.

For another definition of $\mathbb{N}$ in $\langle \mathbb{Z}; +, \times \rangle$ see [15] where it is proved that $\mathbb{Z}$ is definable in $\langle \mathbb{Q}; +, \times \rangle$ as well (see also [14]).

Corollary 5.9 (on $\langle \mathbb{Z}; +, \times \rangle$ and $\langle \mathbb{Q}; +, \times \rangle$).
The structures $\langle \mathbb{Z}; +, \times \rangle$ and $\langle \mathbb{Q}; +, \times \rangle$ are not axiomatizable. □

6. Number systems (multiplication and exponentiation)

We saw that by Tarski's result $\langle \mathbb{C}; +, \times \rangle$ is axiomatizable; then its theory is decidable, and so is the theory of $\langle \mathbb{C}; \times \rangle$. Thus, $\langle \mathbb{C}; \times \rangle$ is axiomatizable by a decidable set of sentences; but what is that axiomatic system? This question was answered in [16, Theorem 2.2] by providing an explicit axiomatization for the multiplicative structure of complex numbers:

Theorem 6.1 (an axiomatization for $\langle \mathbb{C}; \times \rangle$).
The (multiplicative) structure $\langle \mathbb{C}; 0, 1, \{\omega_n\}_{n>1}, \times, ^{-1} \rangle$ is axiomatizable by $\mathtt{A}_\times$, $\mathtt{C}_\times$, $\mathtt{U}_\times$, $\mathtt{I}_\times$ (Theorem 5.3) along with the following axioms:

- $(\mathtt{Z}_\times)$ $\forall x\, (x \cdot 0 = 0 = 0^{-1})$
- $(\mathtt{D}^\times)$ $\{\forall x \exists v\, (x = v^n)\}_{n>0}$
- $(\mathtt{R}_\times)$ $\big\{\forall x\, [x^n = 1 \leftrightarrow \mathbb{V}_{i<n} x = (\omega_n)^i]\big\}_{n>1}$
- $(\mathtt{R}^\times)$ $\big\{\mathbb{\Lambda}_{i<j<n} (\omega_n)^i \neq (\omega_n)^j\big\}_{n>1}$

where the constant symbol ω_n is interpreted as $\cos \frac{2\pi}{n} + \boldsymbol{i} \sin \frac{2\pi}{n}$ for every $n > 1$; thus we have $\omega_2 = -1$, $\omega_3 = \frac{1}{2}(-1 + \boldsymbol{i}\sqrt{3})$, $\omega_4 = \boldsymbol{i}$, etc. □

The same question can be asked about the real numbers: we know $\langle \mathbb{R}; \times \rangle$ is decidable by Tarski's result that $\langle \mathbb{R}; +, \times \rangle$ is axiomatizable; but what is an explicit axiomatization for $\langle \mathbb{R}; \times \rangle$? For its answer we need to add the *positivity predicate*, denoted $\mathcal{P}(x)$, to the language. The following result is proved in [16, Theorem 3.3].

Theorem 6.2 (an axiomatization for $\langle \mathbb{R}; \times \rangle$).
The structure $\langle \mathbb{R}; 0, 1, -1, \mathcal{P}, \times, ^{-1} \rangle$ is axiomatizable by $\mathtt{A}_\times$, $\mathtt{C}_\times$, $\mathtt{U}_\times$, $\mathtt{I}_\times$, $\mathtt{Z}_\times$ (Theorem 6.1) along with the following axioms:

- $(\mathtt{N}_\times)$ $\exists u\, (u \neq 0 \wedge u \neq 1 \wedge u \neq -1)$
- $(\mathtt{D}^\times_{\mathrm{o}})$ $\{\forall x \exists v\, (x = v^{2n+1})\}_{n>0}$
- $(\mathtt{R}^{\mathrm{e}}_\times)$ $\{\forall x\, (x^{2n} = 1 \leftrightarrow x = 1 \vee x = -1)\}_{n>1}$
- $(\mathtt{P})$ $\forall x\, (\mathcal{P}(x) \leftrightarrow \exists y \neq 0 [x = y^2])$
- $(\mathtt{P}_\times)$ $\forall x, y \neq 0 (\mathcal{P}(xy) \longleftrightarrow [\mathcal{P}(x) \leftrightarrow \mathcal{P}(y)])$
- $(\mathtt{P}^-_\times)$ $\forall x \neq 0 [\neg \mathcal{P}(x) \leftrightarrow \mathcal{P}([-1]x)]$ □

Let us note that the multiplicative structure of positive real numbers $\langle \mathbb{R}^+; \times \rangle$ is a non-trivial, divisible, torsion-free, and commutative group, since it is isomorphic to $\langle \mathbb{R}; + \rangle$ via the mapping $x \mapsto \ln(x)$.

For axiomatizing the multiplicative structure of rational numbers $\langle \mathbb{Q}; \times \rangle$, we first axiomatize $\langle \mathbb{Q}^+; \times \rangle$ noting that one can obtain an axiomatization for $\langle \mathbb{Q}; \times \rangle$ by adding the constants $0, -1$ and the predicate $\mathcal{P}(x)$ to the language and adding $\mathtt{Z}_\times$, $\mathtt{N}_\times$, $\mathtt{P}$, $\mathtt{P}_\times$, and $\mathtt{P}^-_\times$ (Theorem 6.2) to the axioms. The following is proved in [16, Theorem 4.11]:

Theorem 6.3 (an axiomatization for $\langle \mathbb{Q}^+; \times \rangle$).
The structure $\langle \mathbb{Q}^+; 1, \times, ^{-1} \rangle$ is axiomatizable by $\mathtt{A}_\times$, $\mathtt{C}_\times$, $\mathtt{U}_\times$, $\mathtt{I}_\times$ (Definition 5.1) along with the following axioms:

- $(\mathtt{T}_\times)$ $\{\forall x\, (x^n = 1 \to x = 1)\}_{n>1}$
- $(\mathtt{M}_\times)$ $\big\{\forall \langle x_i \rangle_{i<k} \exists v \forall y \mathbb{\Lambda}_{i<k} (v^n x_i \neq y^{m_i})\big\}_{n,k}$

where $n, k \in \mathbb{N}$, and no $m_i \in \mathbb{N}$ divides n. □

The axioms $\mathtt{M}_\times$ in Theorem 6.3 state that for every sequence $x_0, \ldots, x_{k-1}$ of positive rational numbers and every sequence $m_0, \ldots, m_{k-1}$ of natural numbers none of which divides the natural number n, there exists a positive rational number v such that for every $i < k$ none of $v^n x_i$'s is an m_i-power of a positive rational number. To see that this holds in $\mathbb{Q}^+$ it suffices to take v to be a prime number that does not divide the numerators or denominators of any of x_i's. This does not hold if some m_i divides n since x_i could be an m_i-th power; it does not hold in $\mathbb{R}^+$ either, since every positive real number has an m_i-th root.

Remark 6.4.
The multiplicative structures that we should study next are $\mathbb{Z}$ and $\mathbb{N}$. Here too, as we saw, it suffices to study $\langle \mathbb{N}^+; \times \rangle$ first, and then for $\langle \mathbb{N}; \times \rangle$ we need to add 0 and the axiom $\mathtt{Z}_\times$, and for $\langle \mathbb{Z}; \times \rangle$ we need to add $-1, \mathcal{P}$ and the axioms $\mathtt{P}_\times$ and $\mathtt{P}^-_\times$. Since studying the axioms of $\langle \mathbb{N}^+; \times \rangle$ will not be needed later, and they are too many to be listed in the main body of the paper, and explaining them will take much time and will distract the flow of the paper, we apologetically postpone it to the Appendix. ◇

6.1. Order, multiplication, and exponentiation. Let us move on to the language $\{<, \times\}$ over which $\mathbb{R}$ and $\mathbb{Q}$ are axiomatizable, while $\mathbb{Z}$ and $\mathbb{N}$ are not. The following is proved in [1, Theorem 6].

Theorem 6.5 (an axiomatization for $\langle \mathbb{R}; <, \times \rangle$).
The theory with the axioms $\mathtt{A}_<$, $\mathtt{T}_<$, $\mathtt{L}_<$ (Theorem 4.1), $\mathtt{D}^\times_0$, $\mathtt{O}_\times$ (Theorem 5.3), $\mathtt{S}_\times$ (Proposition 5.4), $\mathtt{A}_\times$, $\mathtt{C}_\times$, $\mathtt{U}_\times$, $\mathtt{I}_\times$, $\mathtt{Z}_\times$ (Theorem 6.1), $\mathtt{R}^{\mathrm{e}}_\times$ (Theorem 6.2) along with the following, completely axiomatizes the structure $\langle \mathbb{R}; 0, 1, -1, <, \times, {}^{-1} \rangle$.

($\mathtt{N}_<$) $\exists u\, (-1 < 0 < 1 < u)$

($\mathtt{O}^-_\times$) $\forall x, y, z\, (z < 0 \wedge x < y \to y \cdot z < x \cdot z)$ □

The axiomatizability of the structure $\langle \mathbb{Q}; <, \times \rangle$ seemed to be missing (or ignored) in the literature. Since $\langle \mathbb{Q}; <, +, \times \rangle$ is not decidable (Corollary 5.9), one could not immediately infer the decidability of $\langle \mathbb{Q}; <, \times \rangle$. Also, $+$ is not definable in $\langle \mathbb{Q}; <, \times \rangle$, this follows from Theorem 6.6 below, and so Corollary 5.9 cannot imply its undecidability. The decidability of $\langle \mathbb{Q}; <, \times \rangle$ was proved, and an explicit axiomatization was provided for it, for the first time in [1, Theorem 7]:

Theorem 6.6 (an axiomatization for $\langle \mathbb{Q}; <, \times \rangle$).
The theory with $\mathtt{A}_<$, $\mathtt{T}_<$, $\mathtt{L}_<$ (Theorem 4.1), $\mathtt{O}_\times$ (Theorem 5.3), $\mathtt{A}_\times$, $\mathtt{C}_\times$, $\mathtt{U}_\times$, $\mathtt{I}_\times$, $\mathtt{Z}_\times$ (Theorem 6.1), $\mathtt{R}^{\mathrm{e}}_\times$ (Theorem 6.2), $\mathtt{M}_\times$ (Theorem 6.3), $\mathtt{N}_<$ (Theorem 6.5), along with the following completely axiomatizes the structure $\langle \mathbb{Q}; 0, 1, -1, <, \times, {}^{-1} \rangle$.

($\mathtt{D}^\times_<$) $\{\forall x, y \exists v\, (0 < x < y \to x < v^n < y)\}_{n>0}$ □

The axioms $\mathtt{D}^\times_<$ in Theorem 6.6 state that $\mathbb{Q}^+$ is dense in the set of its positive radicals.

Theorem 6.7 (non-axiomatizability of $\langle \mathbb{N}; <, \times \rangle$, $\langle \mathbb{Z}; <, \times \rangle$).
The full first-order theory of $\langle \mathbb{N}; <, \times \rangle$ and $\langle \mathbb{Z}; <, \times \rangle$ are not axiomatizable by any decidable set of sentences.

Proof. Firstly, let us note that the successor operation and the constant zero are definable in both of these structures by $v = \mathfrak{s}(u) \Longleftrightarrow u < v \wedge \neg \exists w (u < w < v)$ and $(u = 0) \Longleftrightarrow u \times \mathfrak{s}(u) = u$, respectively. So, the addition operation $(+)$ is definable in the structure $\langle \mathbb{N}; <, \times \rangle$ by Tarski–Robinson's identity [15]: $(u + v = w) \Longleftrightarrow [u = v = w = 0] \vee [w \neq 0 \wedge \mathfrak{s}(wu)\mathfrak{s}(wv) = \mathfrak{s}(w^2 \mathfrak{s}(uv))]$. Thus, by Theorem 5.8, the structure $\langle \mathbb{N}; <, \times \rangle$ is not axiomatizable; neither is $\langle \mathbb{Z}; <, \times \rangle$ since $\mathbb{N}$ is definable in it by the formula $0 \leqslant v$. □

The exponential function is not total in $\mathbb{Z}$ or $\mathbb{Q}$, even when the base is positive: $2^{-1} \notin \mathbb{Z}$ and $2^{\frac{1}{2}} \notin \mathbb{Q}$. As for $\mathbb{N}$ we take $\mathfrak{exp}(x, y) = x^y$ with the convention that $0^0 = 1$; and of course $0^x = 0$ for every $x > 0$. For $\mathbb{R}$ and $\mathbb{C}$ we consider $x \mapsto \boldsymbol{e}^x$ for the Napier–Euler number $\boldsymbol{e}$ in the place of $\mathfrak{exp}(x)$, since if x is negative, then the value of x^y may not exist in $\mathbb{R}$, such as $(-4)^{\frac{1}{4}}$, and even if it exists in $\mathbb{C}$ it may not be unique (for example, $(-4)^{\frac{1}{4}}$ could be $1+\boldsymbol{i}$, $1-\boldsymbol{i}$, $-1+\boldsymbol{i}$, or $-1-\boldsymbol{i}$); indeed, one can take any positive real number (other than 1) for $\boldsymbol{e}$ (noting that for example, $1^{\frac{1}{4}}$ could be 1, -1, $\boldsymbol{i}$, or $-\boldsymbol{i}$). We also add $+$ and $\times$ to the language; so, by *the real exponential field* we mean $\langle \mathbb{R}; +, \times, \boldsymbol{e}^x \rangle$ and by *the complex exponential field* we mean $\langle \mathbb{C}; +, \times, \boldsymbol{e}^x \rangle$.

Theorem 6.8 (non-axiomatizability of $\langle \mathbb{N}; \mathfrak{exp} \rangle$).
The first-order theory of $\langle \mathbb{N}; \mathfrak{exp} \rangle$ is not axiomatizable.

Proof. Since one can define $\times$ and $+$ in $\langle \mathbb{N}; \mathfrak{exp} \rangle$ (see [4, Exercise 1, page 223]) by $(u \times v = w) \iff \forall x\, [x^w = (x^u)^v]$ and $(u + v = w) \iff \forall x\, [x^w = (x^u) \times (x^v)]$. So, the result follows from Theorem 5.8. □

Theorem 6.9 (non-axiomatizability of $\langle \mathbb{C}; +, \times, \boldsymbol{e}^x \rangle$).
The complex exponential field is not axiomatizable.

Proof. Indeed, the formula $\forall x, y\, (\boldsymbol{e}^{xy} = -x^2 = 1 \to \boldsymbol{e}^{xy \cdot v} = 1)$ defines $\mathbb{Z}$ in $\langle \mathbb{C}; +, \times, \boldsymbol{e}^x \rangle$, see e.g. [12], since $\forall x\, (x^2 = -1 \leftrightarrow x = \pm \boldsymbol{i})$ holds in $\mathbb{C}$, and for every y we have $\boldsymbol{e}^{\pm iy} = 1$ if and only if $y = k\boldsymbol{\pi}$ for some $k \in \mathbb{Z}$. The result follows from Corollary 5.9. □

One of the most exciting questions in axiomatizability theory is the question of the axiomatizability of $\langle \mathbb{R}; +, \times, \boldsymbol{e}^x \rangle$, the real exponential field (due to Tarski 1951) which is still open. An interesting instance of interaction between seemingly different areas of mathematics (number theory and logic) is the result of Macintyre and Wilkie [11] which states that $\langle \mathbb{R}; +, \times, \boldsymbol{e}^x \rangle$ *is axiomatizable if and only if the weak Schanuel conjecture is true*. So, if a theoretical computer scientist or a mathematical logician shows that $\langle \mathbb{R}; +, \times, \boldsymbol{e}^x \rangle$ is (non-)axiomatizable, then the weak Schanuel conjecture is solved in the field of computational number theory, and if a number theorist solves that problem, then we know whether $\langle \mathbb{R}; +, \times, \boldsymbol{e}^x \rangle$ is axiomatizable or not. If the conjecture is true, then we have an axiomatization for $\langle \mathbb{R}; +, \times, \boldsymbol{e}^x \rangle$ which is "quite complicated and ugly" according to Marker [12].

7. Identities (over $+, \times, \mathfrak{exp}$ in $\mathbb{R}^+$)

First-order sentences can be restricted in at least two ways: one can consider the sentences of the form (a) $\exists \vec{x}\, \eta(\vec{x})$ where $\eta(\vec{x})$ is an equation (between two terms on $\vec{x}$ and possibly some other parameters); or (b) $\forall \vec{x}\, \eta(\vec{x})$ where $\eta(\vec{x})$ is as above.

The formula in (a) is a statement that a *diophantine equation* is solvable; these formulas are closely related to Hilbert's 10th problem (1900). Since they are discussed elsewhere (see e.g. [14]), here we discuss the formulas in (b), which are called *identities*.

For a proof of the parts (i) and (ii) of the following theorem see e.g. [8]; and for a proof of part (iii), which is due to Martin [13], see e.g. [9, Corollary 3.7].

Theorem 7.1 (identities with a single operation).
(i) The identities of $\langle \mathbb{R}^+; + \rangle$ are axiomatized by
($\mathbb{A}_+$) $x + (y + z) = (x + y) + z$

($\mathtt{C}_+$) $x+y=y+x$

(ii) The identities of $\langle \mathbb{R}^+; 1, \times\rangle$ are axiomatized by

($\mathtt{A}_\times$) $x\cdot(y\cdot z)=(x\cdot y)\cdot z$

($\mathtt{C}_\times$) $x\cdot y=y\cdot x$

($\mathtt{U}_\times$) $x\cdot 1=x$

(iii) The identities of $\langle \mathbb{R}^+; 1, \mathfrak{exp}\rangle$ are axiomatized by

($\mathtt{C}_\wedge$) $(x^y)^z=(x^z)^y$

($\mathtt{Z}_\wedge$) $1^x=1$

($\mathtt{U}_\wedge$) $x^1=x$ □

Let us note that $0\notin\mathbb{R}^+$ and so the identity ($\mathtt{U}_+$) $x+0=x$ is not expressible here; and since we do not have $-$ in our language, the identity ($\mathtt{I}_+$) $x+(-x)=0$ is not expressible either. The part (I) of the following theorem appears in [8]; for the part (II), which appeared in [13] first, see e.g. [9, Corollary 3.9].

Theorem 7.2 (identities with two operations).

(I) The identities of $\langle \mathbb{R}^+; 1, +, \times\rangle$ are axiomatized by $\mathtt{A}_+$, $\mathtt{C}_+$, $\mathtt{A}_\times$, $\mathtt{C}_\times$, $\mathtt{U}_\times$ (Theorem 7.1) along with the following identity:

($\mathtt{D}_\times$) $x\cdot(y+z)=(x\cdot y)+(x\cdot z)$

(II) The identities of $\langle \mathbb{R}^+; 1, \times, \mathfrak{exp}\rangle$ are axiomatized by $\mathtt{A}_\times$, $\mathtt{C}_\times$, $\mathtt{U}_\times$, $\mathtt{Z}_\wedge$, $\mathtt{U}_\wedge$ (Theorem 7.1) along with the following identities:

($\mathtt{D}^\times_\wedge$) $x^{(y\cdot z)}=(x^y)^z$

($\mathtt{D}^\wedge_\times$) $(x\cdot y)^z=x^z\cdot y^z$ □

Let us note that the axiom $\mathtt{C}_\wedge$ (Theorem 7.1.iii) is provable from $\mathtt{C}_\times$ (Theorem 7.1.ii) and $\mathtt{D}^\times_\wedge$ (Theorem 7.2.II).

The axioms in Theorem 7.2.I (for $\{+,\times\}$) suffice for proving many of the high-school identities, such as

- the binomial identity: $(x+y)^n=\sum_{i\leqslant n}\binom{n}{i}x^i y^{n-i}$ for $n\in\mathbb{N}$, and
- $(x+y+1)^n=\sum_{(i+j\leqslant n)}\binom{n}{i+j}\binom{i+j}{i}x^i y^j$ for $n\in\mathbb{N}$,

and the more difficult one:

($\mathtt{W}^\alpha_\beta$): $(P^\alpha+Q^\alpha)^\beta(R^\beta+S^\beta)^\alpha=(P^\beta+Q^\beta)^\alpha(R^\alpha+S^\alpha)^\beta$ for $\alpha,\beta\in\mathbb{N}$,

where $P(x)=x+1$, $Q(x)=x^2+x+1$, $R(x)=x^3+1$, and $S(x)=x^4+x^2+1$ are polynomials on the variable x.

We show that the identities of Table 2 derive Wilkie's (1981) identity $\mathtt{W}^\alpha_\beta$ when at least one of α or β is a natural number (and the other one could be a variable). So, let us assume that $\alpha\in\mathbb{N}$; we note that $PS=QR=x^5+x^4+x^3+x^2+x+1$. We have:

$(P^\alpha+Q^\alpha)^\beta(R^\beta+S^\beta)^\alpha=(P^\alpha+Q^\alpha)^\beta\sum_{i\leqslant\alpha}\binom{\alpha}{i}R^{\beta i}S^{\beta(\alpha-i)}=$

$\sum_{i\leqslant\alpha}\binom{\alpha}{i}[(P^\alpha+Q^\alpha)R^iS^{\alpha-i}]^\beta=$

$\sum_{i\leqslant\alpha}\binom{\alpha}{i}\big([(PR)^i(PS)^{\alpha-i}]+[(QR)^i(QS)^{\alpha-i}]\big)^\beta=$

$$\sum_{i\leqslant\alpha}\binom{\alpha}{i}\big([(PR)^i(QR)^{\alpha-i}]+[(PS)^i(QS)^{\alpha-i}]\big)^\beta=$$
$$\sum_{i\leqslant\alpha}\binom{\alpha}{i}\big(R^\alpha[P^iQ^{\alpha-i}]+S^\alpha[P^iQ^{\alpha-i}]\big)^\beta=$$
$$\sum_{i\leqslant\alpha}\binom{\alpha}{i}\big([R^\alpha+S^\alpha][P^iQ^{\alpha-i}]\big)^\beta=$$
$$(R^\alpha+S^\alpha)^\beta\sum_{i\leqslant\alpha}\binom{\alpha}{i}(P^\beta)^i(Q^\beta)^{\alpha-i}=(P^\beta+Q^\beta)^\alpha(R^\alpha+S^\alpha)^\beta.$$

Indeed, Wilkie's identity $\mathtt{W}^\alpha_\beta$ is true even when both α,β are variables: since for $T(x)=x^2-x+1$ we have $R=PT$ and $S=QT$, thus $T^{\alpha\beta}$ can be factored out from both sides of $\mathtt{W}^\alpha_\beta$. Note that the positive-valued polynomial T is not expressible in the language $\{1,+,\times,\mathfrak{exp}\}$.

Tarski's high-school problem asked whether the identities of Table 2 could axiomatize all the identities of the positive cone of the real exponential field, i.e., the structure $\langle\mathbb{R}^+;1,+,\times,\mathfrak{exp}\rangle$. It was posed first by Doner & Tarski (1969) and was popularized in 1977 by Henkin [8] as a then open problem. Wilkie [20] showed in 1981 that $\mathtt{W}^\alpha_\beta$ is not derivable from Tarski's high-school identities when both α and β are variables (see also [5]).

Wilkie [20] also proved that the identities of $\langle\mathbb{R}^+;1,+,\times,\mathfrak{exp}\rangle$ are axiomatizable by a decidable set of identities, and Gurevič [6] showed that it is not axiomatizable by any finite set of identities. However, Tarski's conjecture holds true for a wide range of identities.

Let us say that a term t over $\{1,+,\times,\mathfrak{exp}\}$ is of level 1 when for every sub-term u^v of t either u is a variable or u contains no variable; for example, $x^y+(1+1)^z$. A term t is of level 2 when for every sub-term u^v of t we have that u is of level 1; for example $p(x)^u+q(x)^v$ is of level 2 when p,q are polynomials of the variable x, and u,v are variables. Let us note that the term $(P(x)^\alpha+Q(x)^\alpha)^\beta$, which appears in $\mathtt{W}^\alpha_\beta$, is not of level 2 in general. The following theorem is proved in [7, Proposition 4.4.5]:

Theorem 7.3 (Tarski's conjecture for terms of level 2).
If $(r=s)$ is a valid identity of the structure $\langle\mathbb{R}^+;1,+,\times,\mathfrak{exp}\rangle$ where r and s are terms of level 2, then $(r=s)$ can be proved from the identities of Table 2. □

So, Wilkie's result [20] (Theorem 7.4 below) is a boundary result, since some terms in $\mathtt{W}^\alpha_\beta$ are of level 3 (which are the terms with the property that for every sub-term u^v of them, u is a term of level 2).

Theorem 7.4 (Tarski's conjecture, *not* for higher levels).
The identity $\mathtt{W}^\alpha_\beta$ holds in $\langle\mathbb{R}^+;1,+,\times,\mathfrak{exp}\rangle$ but is not provable from the identities of Table 2 when x,α,β are all variables. □

An axiomatization for the multiplication of positive natural numbers

An axiomatization for $\langle\mathbb{N}^+;1,\times\rangle$ was presented in [3], whose proofs are available only in French; an English exposition of the axioms without any proofs appears in [19, § III.5]. We need the following notation for presenting the axioms:

$y\sqsubseteq x\Longleftrightarrow\exists w(y\cdot w=x)$,
$\mathscr{P}(x)\Longleftrightarrow x\neq1\wedge\forall y\,(y\sqsubseteq x\to y=1\vee y=x)$,
$\mathscr{R}(x,y)\Longleftrightarrow\mathscr{P}(x)\wedge x\sqsubseteq y\wedge\forall z\,(\mathscr{P}(z)\wedge z\neq x\to z\not\sqsubseteq y)$, and
$\mathscr{V}(x,y,z)\Longleftrightarrow\mathscr{R}(x,z)\wedge z\sqsubseteq y\wedge\forall w\,(\mathscr{R}(x,w)\wedge w\sqsubseteq y\to w\sqsubseteq z)$;`if x[y; o.w. just P(x)&z=1.`
which state, respectively, that "y divides x", "x is a prime", "y is a power of the prime x", and "z is the largest power of the prime x that divides y". Here are Cégielski's axioms [3]:

$(\mathtt{A}_\times)$ $\forall x,y,z\,(x\cdot(y\cdot z)=(x\cdot y)\cdot z)$

$(\mathtt{C}_\times)$ $\forall x,y\,(x\cdot y=y\cdot x)$

$(\mathtt{U}_\times)$ $\forall x\,(x\cdot 1=x)$

$(\mathtt{C}^\times)$ $\forall x,y,z\,(x\cdot y=x\cdot z\to y=z)$

$(\mathtt{U}^\times)$ $\forall x,y\,(x\cdot y=1\to x=y=1)$

$(\mathtt{D}^\times)$ $\{\forall x,y\,(x^n=y^n\to x=y)\}_{n>1}$

$(\mathtt{E}_\times)$ $\{\forall x\exists u,v\,(x=u^n v\wedge\forall y,z[x=y^n z\to v\sqsubseteq z])\}_{n>1}$

$(\mathtt{P}^\times)$ $\forall x\exists v\,(\mathscr{P}(v)\wedge v\not\sqsubseteq x)$

$(\mathtt{R}_\times)$ $\forall u,x,y\,(\mathscr{R}(u,x)\wedge\mathscr{R}(u,y)\to x\sqsubseteq y\vee y\sqsubseteq x)$

$(\mathtt{V}_\exists)$ $\forall u,x\,[\mathscr{P}(u)\to\exists v\mathscr{V}(u,x,v)]$

$(\mathtt{V}_\sqsubseteq)$ $\forall x,y\,(\forall u,v,w[\mathscr{P}(u)\wedge\mathscr{V}(u,x,v)\wedge\mathscr{V}(u,y,w)\to v\sqsubseteq w]\longrightarrow x\sqsubseteq y)$

$(\mathtt{T}_\times)$ $\forall x,y\exists z\forall u\,(\mathscr{P}(u)\longrightarrow[u\not\sqsubseteq x\to\mathscr{V}(u,z,1)]\wedge[u\sqsubseteq x\to\forall v\{\mathscr{V}(u,z,v)\leftrightarrow\mathscr{V}(u,y,v)\}])$

$(\mathtt{V}_\times)$ $\forall x,y\,(\forall u,v,w[\mathscr{P}(u)\wedge\mathscr{V}(u,x,v)\wedge\mathscr{V}(u,y,w)\to\mathscr{V}(u,x\cdot y,v\cdot w)])$

$(\mathtt{S}^\times)$ $\{\forall x,y\exists z\forall u\,(\mathscr{P}(u)\longrightarrow[u\sqsubseteq x\cdot y\wedge\exists v,w\{\mathscr{V}(u,x,v)\wedge\mathscr{V}(u,y,w^n v)\}\to\mathscr{V}(u,z,u)]\wedge$
$[\neg(u\sqsubseteq x\cdot y\wedge\exists v,w\{\mathscr{V}(u,x,v)\wedge\mathscr{V}(u,y,w^n v)\})\to\mathscr{V}(u,z,1)])\}_{n>0}$

By $\mathtt{A}_\times$, $\mathtt{U}_\times$, $\mathtt{C}^\times$, and $\mathtt{U}^\times$ the relation $\sqsubseteq$ is antisymmetric: if $a\sqsubseteq b\sqsubseteq a$, then $a=b$. For every prime u and every x there exists some v, by $\mathtt{V}_\exists$, such that $\mathscr{V}(u,x,v)$. That v is unique by $\mathtt{R}_\times$; so let us denote it by $\mathcal{V}(u,x)$. So, if u ranges over the primes, then $x=\prod_{u\sqsubseteq x}\mathcal{V}(u,x)$. Thus, $\mathtt{V}_\times$ is equivalent to $\mathcal{V}(u,xy)=\mathcal{V}(u,x)\mathcal{V}(u,y)$; and the number z in $\mathtt{T}_\times$ is $\prod_{u\sqsubseteq x}\mathcal{V}(u,y)$. The axiom $\mathtt{S}^\times$ states the existence of $\prod_{[u\sqsubseteq xy,\mathcal{V}(u,x)\sqsubseteq_n\mathcal{V}(u,y)]}u$, where $a\sqsubseteq_n b$ is by definition $\exists w(aw^n=b)$. Finally, we note that the following sentences are provable from the axioms:

$(\mathtt{V}_=)$ $\forall x,y\,(\forall u[\mathscr{P}(u)\to\mathcal{V}(u,x)=\mathcal{V}(u,y)]\longrightarrow x=y)$

$(\mathtt{I}_\times)$ $\forall x\exists w\forall u\,(\mathscr{P}(u)\to[u\not\sqsubseteq x\to\mathcal{V}(u,w)=1]\wedge[u\sqsubseteq x\to\mathcal{V}(u,w)=u\mathcal{V}(u,x)])$

$(\mathtt{P}^\times_\exists)$ $\forall x\,(x\neq 1\to\exists u[\mathscr{P}(u)\wedge u\sqsubseteq x])$

In fact, $\mathtt{V}_=$ follows from $\mathtt{V}_\sqsubseteq$, and $\mathtt{I}_\times$ follows from $\mathtt{S}^\times$ by putting $w=xz$ where z is stated to exist by $\mathtt{S}^\times$ for $x=y,n=1$. Indeed, $\mathtt{V}_=$ is the axiom $A11$ in [3] (V_2 in [19]), and $\mathtt{I}_\times$ is the axiom $A15$ in [3] (I in [19]) which, as we saw, are redundant. For $\mathtt{P}^\times_\exists$ we note that if no prime divides $\alpha\neq 1$, then $\mathcal{V}(u,\alpha)=1$ for every prime u; so by $\mathtt{V}_\sqsubseteq$ we have $\alpha\sqsubseteq y$ for every y, and this contradicts $\mathtt{P}^\times$ (by which also the infinitude of primes can be proved).

References

[1] Z. Assadi and S. Salehi, "On decidability and axiomatizability of some ordered structures", *Soft Comput.* **23**:11 (2019), 3615–3626.

[2] J. Bochnak, M. Coste, and M.-F. Roy, *Real algebraic geometry*, Ergebnisse der Math. (3) **36**, Springer-Verlag, Berlin, 1998.

[3] P. Cegielski, "Théorie élémentaire de la multiplication des entiers naturels", pp. 44–89 in *Model theory and arithmetic* (Paris, 1979–1980), Lecture Notes in Math. **890**, Springer, 1981.

[4] H. B. Enderton, *A mathematical introduction to logic*, 2nd ed., Academic Press, 2001.

[5] R. Gurevič, "Equational theory of positive numbers with exponentiation", *Proc. Amer. Math. Soc.* **94**:1 (1985), 135–141.

[6] R. Gurevič, "Equational theory of positive numbers with exponentiation is not finitely axiomatizable", *Ann. Pure Appl. Logic* **49**:1 (1990), 1–30.

[7] R. H. Gurevič, "Detecting algebraic (in)dependence of explicitly presented functions (some applications of Nevanlinna theory to mathematical logic)", *Trans. Amer. Math. Soc.* **336**:1 (1993), 1–67.

[8] L. Henkin, "The logic of equality", *Amer. Math. Monthly* **84**:8 (1977), 597–612.

[9] C. W. Henson and L. A. Rubel, "Some applications of Nevanlinna theory to mathematical logic: identities of exponential functions", *Trans. Amer. Math. Soc.* **282**:1 (1984), 1–32. Corrigendum at **294**:1 (1986), 381.

[10] G. Kreisel and J.-L. Krivine, *Elements of mathematical logic. Model theory*, North-Holland, Amsterdam, 1967.

[11] A. Macintyre and A. J. Wilkie, "On the decidability of the real exponential field", pp. 441–467 in *Kreiseliana*: *about and around Georg Kreisel*, edited by P. Odifreddi, A K Peters, Wellesley, MA, 1996.

[12] D. Marker, "Model theory and exponentiation", *Notices Amer. Math. Soc.* **43**:7 (1996), 753–759.

[13] C. F. Martin, "Axiomatic bases for equational theories of natural numbers (abstract)", *Notices Amer. Math. Soc.* **19**:7 (1972), 778–779.

[14] B. Poonen, "Undecidability in number theory", *Notices Amer. Math. Soc.* **55**:3 (2008), 344–350.

[15] J. Robinson, "Definability and decision problems in arithmetic", *J. Symbolic Logic* **14** (1949), 98–114.

[16] S. Salehi, "On axiomatizability of the multiplicative theory of numbers", *Fund. Inform.* **159**:3 (2018), 279–296.

[17] S. Salehi and M. Zarza, "First-order continuous induction and a logical study of real closed fields", *Bull. Iranian Math. Soc.* **46**:1 (2020), 225–243.

[18] K. Schmüdgen, "Around Hilbert's 17th problem", *Doc. Math.* Extra volume: Optimization stories (2012), 433–438.

[19] C. Smoryński, *Logical number theory, I: An introduction*, Springer, Berlin, 1991.

[20] A. J. Wilkie, "On exponentiation: a solution to Tarski's high school algebra problem", preprint. Reprinted in *Connections between model theory and algebraic and analytic geometry*, *Quaderni di Matematica* (Seconda Univ. Napoli), **6**, (2000), pp. 107–129,.

Saeed Salehi: root@saeedsalehi.ir
Department of Mathematics, Statistics, and Computer Science, University of Tabriz, P.O.Box 51666-16471, Tabriz, Iran
and
School of Mathematics, Institute for Research in Fundamental Sciences, P.O.Box 19395-5746, Tehran, Iran