Karshi Multidisciplinary International Scientific Journal

www.kmisj.reapress.com

K. Multidiscip. Int. Sci. J. Vol. 2, No. 1 (2025) 17–27.

Paper Type: Original Article

A Theoretical Study on Axiomatizability of First-Order Mathematical Structures

Saeed Salehi[1], **Zahra Sheikhaleslami**[2,*]

[1]Department of Mathematics, University of Tabriz,Bahman 29th Boulevard,51666-16471, Tabriz; Iran, salehipour@tabrizu.ac.ir.
[2]Department of Mathematics, University of Tabriz, Bahman 29th Boulevard, 51666-16471, Tabriz; Iran, zahra.sheikhaleslami@gmail.com.

Citation:

Received: 03 September 2024 Revised: 10 November 2024 Accepted: 24 Februry 2025	Salehi, S., & Sheikhaleslami, Z. (2025). A theoretical study on axiomatizability of first-order mathematical structures. *Karshi multidisciplinary international scientific journal*, 2(1), 17-27

Abstract

Decidability and undecidability are central challenges in mathematical logic, particularly in the axiomatization of first-order structures. This study investigated the axiomatizability of various mathematical structures, emphasizing the roles of completeness, consistency, and compactness. We provide an explicit axiomatization for $\langle \mathbb{Z}; | \rangle$, where $u \mid v$ indicates that u divides v (i.e., $\exists t\,(u \cdot t = v)$), demonstrating its decidability through quantifier elimination. This work extends these findings to $\langle \mathbb{Q}; | \rangle$ and explores the multiplicative theory of integers, $\langle \mathbb{Z}; \times \rangle$, highlighting computable axiomatizations in decidable theories.

Keywords: Axiomatizability, Boolean algebras, Decidability, Incompleteness, Number Structure, First-Order Logic..

1|Introduction

Quantifier elimination is a powerful property that aids in proving decidability,and has numerous applications. In the late 1920s, Tarski led a seminar on logic problems at the University of Warsaw, focusing on developing a method of quantifier elimination. Tarski and his students achieved significant results. One of his students, Mojżesz Presburger, succeeded in developing quantifier elimination procedure for the theory of additive integer numbers (Presburger Arithmetic). The foundational basis for this study lies in the classical results of mathematical

✉ Corresponding Author: zahra.sheikhaleslami@gmail.com
https://doi.org/10.22105/kmisj.v2i1.82

logic and computability theory, notably articulated in the comprehensive text by Boolos, Burgess, and Jeffrey [1]. Foundational algebraic concepts, especially those relevant to universal algebra and logical structures, are drawn from Burris and Sankappanavar's seminal work [2]. The decidability and model-theoretic properties of Boolean algebras are supported by Poizat's developments in model theory [3] and the axiomatizability of the natural lattice as presented by Cégielski [4]. The results regarding complete theories of Boolean algebras and quantifier elimination stem from Ortiz's analysis [5], while logical formalism is further contextualized by Leary and Kristiansen [6]. Philosophical and historical perspectives on logic, as examined by Prawitz and Westerståhl [7], complement the syntactical treatment of formal languages discussed by Dutilh [8]. The general approach to logic formalization aligns with the structure of Enderton's textbook [9]. In formulating a rigorous axiomatization of multiplicative and divisibility structures, this study draws from the algebraic framework introduced by Givant and Halmos [10] and is deeply informed by Salehi's earlier work on axiomatizability of multiplicative theories [11, 12]. The logical number theoretic aspects, particularly related to the structures of $\langle \mathbb{Z}; \times \rangle$ and $\langle \mathbb{Q}; | \rangle$, are situated within the framework developed by Smorynski [13]. Finally, set-theoretic insights and their connections to logic, relevant especially in the context of structural decidability, are considered from the recent work of Habič et al. [14].

A theory or structure in language L admits quantifier elimination if every formula φ in L is equivalent to a quantifier-free formula ψ in L. In this study, we explore the structures of integers, and rational numbers under the divisibility relation. Skolem initially claimed decidability for $\text{Th}(\mathbb{N}; \times, =)$ by employing a quantifier elimination technique [1]. However, Mostowski provided the first proof of decidability, relying on the notion of the weak (direct) powers of a structure, which allowed the reduction of $\text{Th}(\mathbb{N}; \times)$ to $\text{Th}(\mathbb{N}; +)$. Cegielski later axiomatized $\text{Th}(\mathbb{N}; \times)$ [4], and in this paper, we provide an explicit axiomatization for $\text{Th}(\mathbb{Z}; \times)$. The main focus of this study is the exploration of the decidability and axiomatizability of certain first-order mathematical structures, particularly those involving integers, and rational numbers under the divisibility relation. This research extends existing results on $\text{Th}(\mathbb{N}; |)$ [5]to $\text{Th}(\mathbb{Z}; |)$ and investigates the theory of divisibility in rational numbers, $\langle \mathbb{Q}; | \rangle$. This work aims to provide a clear and comprehensive axiomatization of $\langle \mathbb{Q}; | \rangle$, while also contributing to a deeper understanding of divisibility theory in other first-order structures. The results are expected to offer new insights into decidability in mathematical logic, with potential applications. The significance of this research lies in its potential to advance knowledge on the axiomatizability and decidability of first-order structures. By presenting explicit axiomatizations, this study may foster further theoretical developments and practical applications in fields where these structures are fundamental.

2|The Multiplicative Theory of Integers

The multiplicative theory of integers, denoted $\text{Th}(\mathbb{Z}; \times)$, explores the properties of the structure $\langle \mathbb{Z}; \times \rangle$, where $\mathbb{Z}$ represents the set of all integers and × denotes multiplication. This theory is analogous to the study of the multiplicative theory of natural numbers, $\text{Th}(\mathbb{N}; \times)$, which concerns tht properties of set $\mathbb{N}$ under multiplication. The study of the multiplicative theory of integers, $\text{Th}(\mathbb{Z}; \times)$, is intriguing because of its complexity, reflecting the multiplicative theory of natural numbers, $\text{Th}(\mathbb{N}; \times)$, but with additional intricacies due to the inclusion of negative integers.The structure $\langle \mathbb{Z}; \times \rangle$, is decidable and thus axiomatizable [12,14].

Definition 1. p-adic valuation: The p-adic valuation of u, denoted by V, is defined as follows: [1] For example, if

$$u = p_1^n p_2^m p_3^0 \cdots$$

then

$$V(p_2, u) = p_2^m.$$

Definition 2. A number p is considered prime, denoted by $\mathbf{P}(p)$, if and only if:

$$p \neq 1 \land \forall u \ (u \mid p \to (u = 1 \lor u = p)).$$

Definition 3. A number x is called a p-primary number, denoted by $PR(p, x)$, if and only if:

[1] If $n = \prod_p p^{v(n,p)}$, then we might not explicitly define $v(n, p)$ in the theory. However, we may denote it as $n = \prod_p V(n, p)$, where $V(n, p) = p^{v(n,p)}$. For small v, we have $v(p, a, b) = v(p, a) + v(p, b)$, whereas for large V, we have $V(p, a \cdot b) = V(p, a) \cdot V(p, b)$.

$$\mathbf{P}(p) \wedge \forall q \ ((\mathbf{P}(q) \wedge q \neq p) \to q \nmid x).$$

Corollary 1. ***(Axiomatizability of Th**$(\mathbb{Z}; \times)$**)*** *The following theory completely axiomatizes the structure* $\langle \mathbb{Z}; \times \rangle$.

(1) **Associativity**:

$$\forall u \forall v \forall w, \ (u \cdot (v \cdot w) = (u \cdot v) \cdot w).$$

This axiom states that multiplication is associative, which is a fundamental property of the multiplication operation in the integers.

(2) **Existence of Multiplicative Identity**:

$$\exists u \text{ such that } \forall v, \ (u \cdot v = v \cdot u = v).$$

This axiom asserts the existence of a multiplicative identity (which is 1 for integers) such that multiplying any integer by this identity leaves the integer unchanged.

(3) **Commutativity**:

$$\forall u \forall v, \ (u \cdot v = v \cdot u).$$

This axiom states that multiplication is commutative, meaning the order in which two integers are multiplied does not matter.

(4) **Cancellation Law**:

$$\forall u \forall v \forall w \neq 0, \ (u \cdot w = v \cdot w \to u = v).$$

This axiom indicates that if the product of two pairs of integers with the same multiplier is equal, then the integers themselves must be equal, provided the multiplier is not zero.

(5) **Uniqueness of Multiplicative Inverse**:

$$\forall u, v \neq 0, \ (u \cdot v = 1 \to u = v = 1 \vee u = v = -1).$$

This axiom states that the only integers with a multiplicative inverse (under integer multiplication) are 1 and -1. This axiom is more restrictive, asserting that only 1 and -1 have this property in the context of this axiomatization.

(6) **Unique Roots**:

$$\forall u \forall v, \ (u^n = v^n \to u = v) \quad (n \in \mathbf{N}^*).$$

This axiom ensures that if two integers raised to the same positive integer power are equal, then the integers themselves must be equal. This is crucial for capturing the behavior of integers under exponentiation.

(7) **Division Algorithm**:

$$\forall u \forall n \in \mathbf{N}^*, \ \exists v \exists w, \ (u = n \cdot v + w \wedge w < n \wedge w \neq n).$$

This axiom captures the division algorithm, which states that any integer can be expressed as a quotient and a remainder when divided by a positive integer.

(8) **Unique Factorization**:

$$\forall u, \ \exists v \exists w, \ (u = v^n \cdot w \wedge \forall \acute{v} \forall \acute{w}, \ (u = \acute{v}^n \cdot \acute{w} \to w \mid \acute{w})).$$

This axiom asserts that each integer can be factored uniquely into powers of integers and that these factors are unique up to multiplication by units.

(9) **Existence of Prime Numbers**:

$$\forall u,\ \exists p,\ (P(p) \land p \nmid u).$$

This axiom ensures the existence of prime numbers and that for any integer, there exists a prime that does not divide it.

(10) **Prime Divisibility**:

$$\forall p \forall u \forall v,\ ((P(p,u) \land P(p,v)) \to u \mid v \lor v \mid u).$$

This axiom states that if a prime number divides two integers, then one of those integers must divide the other.

(11) **Prime Factorization**:

$$\forall u \forall p,\ (P(p) \to \exists v,\ (u = V(p,v))).$$

This axiom asserts the unique factorization of integers into prime factors.

(12) **Equality of Prime Factor Representations**:

$$u = v \leftrightarrow \forall p,\ (P(p) \to \exists v,\ (V(p,u) = V(p,v))).$$

This axiom states that two integers are equal if and only if their prime factorizations are identical.

(13) **Multiplication of Prime Factor Representations**:

$$\forall u \forall v \forall p,\ (P(p) \to V(p, u \cdot v) = V(p,u) \cdot V(p,v)).$$

This axiom ensures that the prime factor representation of a product is the product of the prime factor representations.

(14) **Divisibility in Terms of Prime Factors**:

$$\forall u \forall v,\ (\forall p,\ (P(p) \to V(p,u) \mid V(p,v)) \to u \mid v)\,.$$

This axiom relates the divisibility of integers to the divisibility of their prime factors.

(15) **Existence of Prime Factors for Multiples**:

$$\forall u \forall v,\ \exists w,\ \forall p,\ (P(p) \to (p \mid u \to V(p,w) = V(p,v)) \land (p \nmid u \to V(p,w) = 1))\,.$$

This axiom ensures the existence of a suitable integer w given u and v such that certain conditions involving prime factors are met.

(16) **Prime Factor Behavior for Non-divisors**:

$$\forall u\, \exists v\, \forall p\ (P(p) \to (p \nmid u \to V(p,v) = 1) \land (p \mid u \to V(p,v) = p \cdot V(p,u)))\,.$$

This axiom describes the behavior of prime factors for integers that are not divisible by a given prime.

(17) **Behavior of Prime Factors for Products**:

$$\begin{gathered}\forall u \forall v\, \exists w\, \forall p \Big((P(p) \to (p \mid u \cdot v \land V(p,u) \equiv_n V(p,v)) \to V(p,w) = p) \land \\ \land\, (p \nmid u \cdot v \lor V(p,u) \not\equiv_n V(p,v) \to V(p,w) = 1) \Big), \quad (n \in \mathbb{N}).\end{gathered}$$

This axiom ensures that every integer has an additive inverse, capturing the structure of integers under addition and subtraction.

3|The Divisibility Theory of Integers

In this section, we focus on axiomatizing the divisibility theory of integers and demonstrating its decidability. The divisibility relation, denoted as $u \mid v$, is the standard notation where u divides v, defined as:

$$u \mid v \leftrightarrow \exists w \in \mathbf{Z},; u \cdot w = v.$$

We recommend using this symbol consistently throughout our discussion. The structure $\langle \mathbb{Z}^+, | \rangle$ is decidable and axiomatizable, where $\mathbb{Z}^+$ denotes the positive integers. The theory of divisibility in $\mathbb{Z}$ can be defined in terms of divisibility in $\mathbb{N}$, specifically:

$$z = -z' \iff z \neq z' \text{ and } z \mid z' \text{ and } z' \mid z.$$

Now, we proceed to axiomatize the divisibility theory of integers [2,12]. The following axioms completely axiomatizes the structure $\langle \mathbb{Z}; | \rangle$:

- $[D_1] \forall u\, (u \mid u)$: Every integer divides itself.
- $[D_2] \forall u, v\, (u \mid v \wedge v \mid u \rightarrow u = v)$: If an integer u divides v and v divides u, then u and v are equal.
- $[D_3] \forall u, v, w\, (u \mid v \wedge v \mid w \rightarrow u \mid w)$: If u divides v and v divides w, then u divides w.
- $[D_4] \forall u, v\, \exists z\, (z \mid u, v \wedge \forall t\, (t \mid u, v \rightarrow t \mid z)\, ;\, z = u \sqcap v)$: For any integers u and v, there exists an integer z (denoted as $u \sqcap v$) that is a common divisor of u and v, and any common divisor of u and v divides z.
- $[D_5] \forall u, v\, \exists w\, (u, v \mid w \wedge \forall t\, (u, v \mid t \rightarrow w \mid t)\, ;\, w = u \sqcup v)$: For any integers u and v, there exists an integer w (denoted as $u \sqcup v$) that is a common multiple of u and v, and w divides any common multiple of u and v.
- $[D_6] \forall u\, (1 \mid u)$: 1 divides every integer.
- $[D_7] \forall u, v\, [\forall w\, (SI(w) \rightarrow [w \mid u \rightarrow w \mid v]) \rightarrow u \mid v]$: If for all strongly irreducible elements w, w divides u implies w divides v, then u divides v.
- $[D_8] \forall u, v, w\, (SI^*(u) \wedge SI^*(v) \wedge SI^*(w) \wedge [(u, v \mid w) \vee (w \mid u, v)] \rightarrow u \mid v \vee v \mid u)$: If u, v, and w are strongly irreducible, and either u and v together divide w or w divides both u and v, then either u divides v or v divides u.
- $[D_9] \forall u, a\, ([SI^*(a) \wedge a \mid u] \rightarrow \exists b\, (SI(b) \wedge a \mid b \mid u \wedge \forall c\, (SI(c) \wedge c \mid u, a) \rightarrow c \mid b))$: If a is strongly irreducible and divides u, then there exists a b such that a divides b, b divides u, and any strongly irreducible c that divides both u and a also divides b.
- $[D_{10}] \forall u\, (u \neq 0 \rightarrow \exists a\, (\mathbf{P}(a) \wedge a \mid u))$: For any non-zero u, there exists a prime a that divides u.
- $[D_{11}] \forall u\, (u \neq 0 \rightarrow \exists a\, (\mathbf{P}(a) \wedge a \nmid u))$: For any non-zero u, there exists a prime a that does not divide u.
- $[D_{12}] \forall u\, \exists s\, \forall a\, (\mathbf{P}(a) \rightarrow [(V(a, u) \neq 0 \rightarrow V(a, s) \neq a) \wedge (V(a, u) = 0 \rightarrow V(a, s) = 0)])$, where $s = \mathbf{SUPP}(u)$: For any u, there exists s (denoted as $\mathbf{SUPP}(u)$) such that for any prime a, if $V(a, u) \neq 0$, then $V(a, s) \neq a$, and if $V(a, u) = 0$, then $V(a, s) = 0$.
- $[D_{13}] \forall u, v\, \exists w\, \forall a\, (\mathbf{P}(a) \rightarrow [(a \nmid u \rightarrow V(a, w) = V(a, v)) \wedge (a \mid u \rightarrow V(a, w) = 0)])$, where $w = \bar{\mathbf{T}}(u, v)$: For any u and v, there exists w (denoted as $\bar{\mathbf{T}}(u, v)$) such that for any prime a, if a does not divide u, then $V(a, w) = V(a, v)$, and if a divides u, then $V(a, w) = 0$.
- $[D_{14}] \forall a, u\, (SI(a, u) \rightarrow \exists v\, (SI(a, v) \wedge u \mid v \wedge v \neq u \wedge \forall w\, ((SI(a, w) \wedge u \mid w) \rightarrow w \mid v)))$, where $v = \mathbf{S}_a(u)$: If a and u are strongly irreducible, then there exists v (denoted as $\mathbf{S}_a(u)$) such that u divides v, v is not equal to u, and any w that is strongly irreducible with a and u, and u divides w, then w divides v.
- $[D_{15_1}] \forall a, u\, (SI(a, u) \wedge u \neq 0 \rightarrow \exists v\, (SI(a, v) \wedge \mathbf{S}_a(v) = u))$: If a and u are strongly irreducible and $u \neq 0$, then there exists v such that v is strongly irreducible with a and $\mathbf{S}_a(v) = u$.
- $[D_{15_2}] \forall u\, \exists v\, \forall a\, (\mathbf{P}(a) \rightarrow [(a \nmid u \rightarrow V(a, v) = 0) \wedge (a \mid u \rightarrow V(a, v) = \mathbf{S}_a V(a, u))])$, where $v = \mathbf{I}(u)$: For any u, there exists v (denoted as $\mathbf{I}(u)$) such that for any prime a, if a does not divide u, then $V(a, v) = 0$, and if a divides u, then $V(a, v) = \mathbf{S}_a V(a, u)$.

- $[D_{16}]\forall u, v\, \exists w\, \forall a\, (\mathbf{P}(a) \to [V(a,w) = 0 \vee (a \mid w \wedge V(a,w) = a \leftrightarrow (a \mid u \vee a \mid v) \wedge V(a,u) \mid V(a,v))])$: For any u and v, there exists w such that for any prime a, $V(a,w) = 0$ or a divides w and $V(a,w) = a$ if and only if a divides u or a divides v, and $V(a,u)$ divides $V(a,v)$.

4|Atomless Boolean Algebra

This section focuses on atomless Boolean algebra. Boolean algebra was first introduced by Boole in 1854, but it was Alfred Tarski who established the decidability of the theory of Boolean algebra. The following formulas are in this section focusing on atomless Boolean algebra.

Lemma 1. *Let $\mathcal{L} = \langle 0, 1, \wedge, \vee, \neg \rangle$ be the language of Boolean algebras. The equivalence*

$$(1)\ \exists u\ (ru = 0 \wedge s\bar{u} = 0 \wedge \bigwedge_{i=1}^{m} a_i u \neq 0 \wedge \bigwedge_{j=1}^{n} b_j \bar{u} \neq 0)$$

holds with

$$(2)\ (rs = 0 \wedge \exists v\ (\bigwedge_{i=1}^{m} a_i \bar{r} v \neq 0 \wedge \bigwedge_{j=1}^{n} b_j \bar{s} \bar{v} \neq 0).$$

Proof: For the proof from (1) to (2): Assume there exists u such that

$$ru = 0 \wedge s\bar{u} = 0 \wedge \bigwedge_{i=1}^{m} a_i u \neq 0 \wedge \bigwedge_{j=1}^{n} b_j \bar{u} \neq 0.$$

Then, we have:

$$ru = 0 \wedge rs\bar{u} = 0 \Rightarrow rs(u + \bar{u}) = 0 \Rightarrow rs(1) = 0 \Rightarrow rs = 0.$$

And,

$$a_i x \neq 0 \Rightarrow a_i x(r + \bar{r}) \neq 0 \Rightarrow a_i ur + a_i u\bar{r} \neq 0 \Rightarrow a_i u\bar{r} \neq 0,$$

which is equivalent to the following formula:

$$\Rightarrow \exists u(\bigwedge_{i=1}^{m} a_i \bar{r} u \neq 0 \wedge \bigwedge_{j=1}^{n} b_j \bar{s} \bar{u} \neq 0).$$

For the other direction, let $rs = 0$. There exists v such that

$$\bigwedge_{i=1}^{m} a_i \bar{r} v \neq 0 \wedge \bigwedge_{j=1}^{n} b_j \bar{s} \bar{v} \neq 0.$$

Let us put

$$u = \bar{r}(s + v),$$
$$\bar{u} = r + \bar{s}\bar{v} = (r + \bar{s})(r + \bar{v}) = \bar{s}(r + \bar{v}).$$

Then,

$$a_i u = a_i \bar{r}(s + v) = a_i \bar{r} s + a_i \bar{r} v \supseteq a_i \bar{r} v \neq 0,$$
$$b_j \bar{u} = b_j \bar{s}(r + \bar{v}) = b_j \bar{s} r + b_j \bar{s} \bar{v} \supseteq b_j \bar{s} \bar{v} \neq 0.$$

In this way, we establish the following equivalence:

$$\bigwedge_{i=1}^{m} a_i u \neq 0 \wedge \bigwedge_{j=1}^{n} b_j \bar{u} \neq 0,$$

which implies the desired conclusion. □

Corollary 2. *The theory of atomless Boolean algebras in the language $\mathcal{L} = \{0, 1, \wedge, \vee, \neg, =\}$ admits quantifier elimination and is therefore decidable.*

- $[B_1]$ $u \wedge v = v \wedge u, \quad u \vee v = v \vee u.$
- $[B_2]$ $u \wedge (v \wedge w) = (u \wedge v) \wedge w, \quad u \vee (v \vee w) = (u \vee v) \vee w.$

- $[B_3]$ $(u \wedge v) \vee v = v, \quad (u \vee v) \wedge v = v.$
- $[B_4]$ $u \wedge (v \vee w) = (u \wedge v) \vee (u \wedge w), \quad u \vee (v \wedge w) = (u \vee v) \wedge (u \vee w).$
- $[B_5]$ $u \wedge \overline{u} = 0, \quad u \vee \overline{u} = 1.$
- $[B_6]$ $\neg At(u)(At(u)$ is $u \neq 0 \wedge \neg \exists v(v \neq 0 \wedge u \wedge v = v)) \Rightarrow 0 \neq 1.$

Proof: By using B_1, B_2, B_3, B_4, B_5, each term on x is equal to $x \cdot r + \overline{x} \cdot s$. Thus, every atomic formula involving x is equal to $x \cdot r + \overline{x} \cdot s = 0$. As a consequence, by using quantifier elimination (Lemma 4.4), it is sufficient to eliminate quantifiers of the following formulas:

$$\exists x(rx = 0 \wedge s\bar{x} = 0 \wedge \bigwedge_{i=1}^{m} u_i x \neq 0 \wedge \bigwedge_{j=1}^{n} v_j \bar{x} \neq 0). \tag{1}$$

Thus, by Lemma (4.4) we show

$$\equiv rs = 0 \wedge \exists y(\bigwedge_{i=1}^{m} u_i \bar{r} y \neq 0 \wedge \bigwedge_{j=1}^{n} v_j \bar{s} \bar{y} \neq 0). \tag{2}$$

It suffices to eliminate the quantifier of the formula:

$$\exists y(\bigwedge_{i=1}^{m} a_i y \neq 0 \wedge \bigwedge_{j=1}^{n} b_j \bar{y} \neq 0). \tag{3}$$

This is equivalent to the following formula:

$$\equiv \bigwedge_{i=1}^{m} a_i \neq 0 \wedge \bigwedge_{j=1}^{n} b_j \neq 0, \tag{4}$$

which implies the desired conclusion.

We prove the theory of atomless Boolean algebra admits quantifier elimination. As for atomless Boolean algebras, its decidability follows from the decidability of the entire principle of Boolean algebras (TBA) demonstrated via Tarski and Ershov. It follows from the fact that any sentence A is true on all atomless Boolean algebras if and only if the theory of Boolean algebras proves the sentence “all elements are atomless" $\Rightarrow A$. □

5|The Divisibility Theory of Rational Numbers

The rational numbers $\mathbb{Q}$ can be seen as an extension of the integers $\mathbb{Z}$ by including ratios of integers. The theory of the structure $\langle \mathbb{Q}^+; | \rangle$ is decidable. The divisibility relation (but for 0 divides z, which is true if and only if $z = 0$); the theory $\langle \mathbb{Q}^+; | \rangle$ is hence interdefinable with the theory of an infinite set $Th(\mathbb{Q}; 0)$ in the language that just contains = and one constant 0. The axiomatization of the elementary $Th(\mathbb{Q}; |)$ such that ($u|v$ is the standard notation for "u divides v"):

(1) $\exists u \left(\forall v(v|u) \wedge \forall v(v \neq u \rightarrow \forall w(w|v \leftrightarrow w \neq u))\right).$

(2) $\exists v_0, ..., v_n \quad (1 \leq n).$

Here, axiom 1 asserts that there exists zero (an element with the desired divisibility properties), and axiom 2 asserts the existence of infinitely many distinct elements. It is trivial to show that (1). This list of axioms gives a countably categorical theory, and (2). All the axioms hold in $(\mathbb{Q}; |)$. Hence, it is indeed an axiomatization of $Th(\mathbb{Q}; |)$.

The $Th(\mathbb{Q}; |)$ such that $p \mid q \leftrightarrow \exists m \in \mathbf{N}^+(p \cdot m = q)$ is axiomatizable. This structure falls under the category of algebraic structures.

D_1 $\forall u \, (u \mid u)$.
Every element divides itself.

D_2 $\forall u, v\,(u \mid v \wedge v \mid u \to u = v)$.
If two elements divide each other, they are equal.

D_3 $\forall u, v, w\,(u \mid v \wedge v \mid w \to u \mid w)$.
Divisibility is transitive.

D_4 $\forall u, v\,\exists z\,(z \mid u, v \wedge \forall t\,[t \mid u, v \to t \mid z])$, $z = u \sqcap v$.
There exists a greatest common divisor for any two elements.

D_5 $\forall u, v\,\exists w\,(u, v \mid w \wedge \forall t\,[u, v \mid t \to w \mid t])$, $w = u \sqcup v$.
There exists a least common multiple for any two elements.

D_6 $\forall u\,(1 \mid u)$.
The element 1 divides every element.

D_7 $\forall u, v\,[\forall w\,(SI(w) \to [w \mid u \to w \mid v]) \to u \mid v]$.
If for all simple elements w, w divides u implies w divides v, then u divides v.

D_8 $\forall u, v, w\,(SI^*(u) \wedge SI^*(v) \wedge SI^*(w) \wedge [(u, v \mid w) \vee (w \mid u, v)] \to u \mid v \vee v \mid u)$.
For any three simple elements, if they pairwise divide or are divided by a third element, then one divides the other.

D_9 $\forall u, a\,([SI^*(a) \wedge a \mid u] \to \exists b\, SI(b) \wedge a \mid b \mid u \wedge \forall c\,(SI(c) \wedge c \mid u, a) \to c \mid b)$.
For any u and simple element a dividing u, there exists a simple element b such that $a \mid b \mid u$ and any simple element c dividing both u and a divides b.

D_{10} $\forall u\,(u \neq 0 \to \exists a\,(\mathbf{P}(\mathbf{a}) \wedge a \mid u))$.
Every nonzero element has a prime divisor.

D_{11} $\forall u\,(u \neq 0 \to \exists a\,(\mathbf{P}(\mathbf{a}) \wedge a \not| u))$.
Every nonzero element has a prime that does not divide it.

D_{12} $\forall u\,\exists s\,\forall a\,(\mathbf{P}(\mathbf{a}) \to (V(a, u) \neq 0 \to V(a, s) \neq a) \wedge (V(a, u) = 0 \to V(a, s) = 0)))$.
For every element u, there exists a unique element s, denoted $\mathbf{SUPP}(u)$, such that for every prime a, $V(a, u) \neq 0$ implies $V(a, s) \neq a$ and $V(a, u) = 0$ implies $V(a, s) = 0$.

D_{13} $\forall u, v\,\exists w\,\forall a\,(\mathbf{P}(\mathbf{a}) \to ((a \not| u \to V(a, w) = V(a, v)) \wedge (a \mid u \to V(a, w) = 0)))$.
For every u and v, there exists a unique w, denoted $\bar{\mathbf{T}}(u, v)$, such that for every prime a, $a \not| u$ implies $V(a, w) = V(a, v)$ and $a \mid u$ implies $V(a, w) = 0$.

D_{14} $\forall a, u\,(SI(a, u) \to \exists v\,(SI(a, v) \wedge u \mid v \wedge v \neq u \wedge \forall w\,(SI(a, w) \wedge u \mid w) \to v \mid w)))$.
For any simple element a and any element u such that $SI(a, u)$, there exists a unique element v, denoted $\mathbf{S}_a(u)$, such that $SI(a, v)$, $u \mid v$, $v \neq u$, and for all w, $SI(a, w) \wedge u \mid w$ implies $v \mid w$.

D_{15_1} $\forall a, u\,(SI(a, u) \wedge u \neq 0) \to \exists v\,(SI(a, v) \wedge \mathbf{S}_a(v) = u)$.
For any simple element a and any nonzero element u such that $SI(a, u)$, there exists a unique element v, denoted $\mathbf{P}_a(u)$, such that $SI(a, v)$ and $\mathbf{S}_a(v) = u$.

D_{15_2} $\forall u\,\exists v\,\forall a\,(\mathbf{P}(\mathbf{a}) \to ((a \not| u \to V(a, v) = 0) \wedge (a \mid u \to V(a, v) = \mathbf{S}_a V(a, u))))$.
For every element u, there exists a unique element v, denoted $\mathbf{I}(u)$, such that for every prime a, $a \not| u$ implies $V(a, v) = 0$ and $a \mid u$ implies $V(a, v) = \mathbf{S}_a V(a, u)$.

D_{16} $\forall u\,\forall v\,\exists w\,\forall a\,(\mathbf{P}(\mathbf{a}) \to (V(a, w) = 0 \vee a \wedge V(a, w) = a \leftrightarrow (a \mid u \vee a \mid v) \wedge V(a, u) \mid V(a, v)))$.
For every u and v, there exists a unique w such that for every prime a, $V(a, w) = 0$ or a and $V(a, w) = a$ if and only if $(a \mid u \vee a \mid v)$ and $V(a, u) \mid V(a, v)$.

D_{17} $\forall u\,\forall v\,\exists w\,\forall a\,(\mathbf{P}(\mathbf{a}) \to (V(a, w) = 0 \vee a \wedge V(a, w) = a \leftrightarrow (a \mid u \vee a \mid v) \wedge V(a, u) \mid V(a, v)))$.
For every u and v, there exists a unique w such that for every prime a, $V(a, w) = 0$ or a and $V(a, w) = a$ if and only if $(a \mid u \vee a \mid v)$ and $V(a, u) \mid V(a, v)$.

D_{18} $u \sqcap v = v \sqcap u \qquad u \sqcup v = v \sqcup u$.
The operations $\sqcap$ and $\sqcup$ are commutative.

D_{19}

$$u \sqcap (v \sqcap w) = (u \sqcap v) \sqcap w$$
$$u \sqcup (v \sqcup w) = (u \sqcup v) \sqcup w.$$

The operations $\sqcap$ and $\sqcup$ are associative.

D_{20}

$$(u \sqcap v) \sqcup v = v$$
$$(u \sqcup v) \sqcap v = v.$$

The operations $\sqcap$ and $\sqcup$ are idempotent.

D_{21}

$$u \sqcap (u \sqcup v) = u$$
$$u \sqcup (u \sqcap v) = u.$$

Absorption laws for $\sqcap$ and $\sqcup$.

D_{22}

$$u \sqcap (v \sqcup w) = (u \sqcap v) \sqcup (u \sqcap w)$$
$$u \sqcup (v \sqcap w) = (u \sqcup v) \sqcap (u \sqcup w.)$$

Distributive laws for $\sqcap$ and $\sqcup$.

D_{23}

$$u \sqcap u^{-1} = 1$$
$$u \sqcup u^{-1} = u$$

This axiom states that each element u has an inverse u^{-1} such that $u \sqcap u^{-1} = 1$ (where 1 is the identity element for $\sqcap$) and $u \sqcup u^{-1} = u$ (where u remains unchanged under $\sqcup$).

D_{24}

$$\neg P(a)$$

This axiom states that a specific predicate $P(a)$ is not true for element a.

D_{25}

$$\forall u, v, w \ (u \cdot (v \cdot w) = (u \cdot v) \cdot w)$$

This is the associativity of multiplication. It states that the way in which elements are grouped in multiplication does not affect the result.

D_{26}

$$\forall u, v \ (0 < u < v \to \exists w \ (u^{2n} < w < v^{2n}), \ n \geq 1.)$$

This axiom ensures that for any u and v such that $0 < u < v$, there exists an element w between u^{2n} and v^{2n} for some $n \geq 1$. This is related to the density of elements in the structure.

D_{27}

$$\forall \xi_1, \ldots, \xi_l \ \exists u \ \forall w \ \bigwedge_{k=1}^{l} (u^n \cdot \xi_k \neq w^{m_k})$$

This axiom states that for any set of elements $\xi_1, \ldots, \xi_l$, there exists an element u such that for all elements w, the products $u^n \cdot \xi_k$ are not equal to w^{m_k} for any $k = 1, \ldots, l$. This relates to the existence of certain elements with specific properties in the structure.

6|Decidability for the Theory of Rational Numbers

Consider the theory of the rational numbers $(\mathbb{Q}^+; |)$, where $|$ denotes divisibility:

$$p \mid q \leftrightarrow \exists m(p \cdot m = q)$$

For example, $\frac{5}{3}$ divides $\frac{7}{3}$ by the definition above (since $\frac{5}{3} \times \frac{7}{5} = \frac{7}{3}$). The structure $(\mathbb{Q}^+; |)$, where $|$ is the divisibility relation, is decidable. Notably, we have:

$$p \mid q \leftrightarrow \exists m(p \cdot m = q)$$

in $\mathbb{Q}$ (rational numbers) is equivalent to:

$$p = 0 \to q = 0,$$

Thus, all formulations in the language $|$ can be translated into the same formulations of the language of the signature, which includes a single constant 0. Quantifier elimination for this language is known, and $0 = 0$. It follows that:

$$Th(\mathbb{Q}^+; |)$$

is decidable. However, $p \mid q \leftrightarrow \exists m \in \mathbf{N}^+(p \cdot m = q)$ is not equivalent to $p \mid q \leftrightarrow \exists m(p \cdot m = q)$. Therefore, decidability for the theory of rational numbers $(\mathbb{Q}^+; |)$, where:

$$p \mid q \leftrightarrow \exists m \in \mathbf{N}^+(p \cdot m = q)$$

is false.

7|Proof of Decidability

We now present a proof that the divisibility theory of rational numbers $(\mathbb{Q}; |)$ is decidable.

Proposition 1. *The theory of rational numbers $(\mathbb{Q}; |)$, where divisibility is defined as $p \mid q \Leftrightarrow \exists m(p \cdot m = q)$, is decidable.*

Proof: Let φ be any formula in the divisibility theory of rational numbers, we perform the following:

(1) We express φ in terms of prime factor decompositions of the rational numbers involved. Since every rational number has a unique factorization, the divisibility relations can be reduced to checking conditions on these factorizations.

(2) Apply quantifier elimination as outlined in the algorithm. This ensures that any existential quantifier (representing the existence of a divisor) is removed, leading to an equivalent quantifier-free formula.

(3) By known results from model theory, the quantifier-free fragment of the theory of $(\mathbb{Q}; |)$ is decidable. Thus, for any input formula φ, we can determine whether φ is true or false in $(\mathbb{Q}; |)$.

Therefore, the theory of $(\mathbb{Q}; |)$ is decidable, as any formula can be reduced to a quantifier-free form which can be algorithmically checked for truth. □

8|Conclusion

In this paper, we provided explicit axiomatizations for the structures $\langle \mathbb{Z}; | \rangle$, $\langle \mathbb{Z}; \times \rangle$, and $\langle \mathbb{Q}; | \rangle$, showing the intricate relationship between decidability, axiomatizability, and quantifier elimination. The results extend previous work on the divisibility theory of integers and rational numbers, contributing to the broader understanding of first-order structures in mathematical logic.

This study lays the groundwork for future investigations. In particular, we intend to explore the axiomatizability and decidability of structures arising in fractal geometry. Such work aims to understand whether logical frameworks developed for algebraic structures can be extended to more complex and self-similar mathematical systems.

Acknowledgments

The authors would like to express their sincere gratitude to the editors and anonymous reviewers for their invaluable comments and constructive feedback, which significantly contributed to the enhancement of this paper. In particular, we are deeply thankful to Dr. Davron Aslonqulovich Juraev for his insightful guidance and editorial support throughout the development of this work.

References

[1] Boolos, G.S., Burgess, John P. and Jeffrey, Richard C. (2007). *Computability and Logic*, Cambridge University Press. 5th ed., ISBN: 9780521701464.

[2] Burris, S.N., & Sankappanavar, H.P. (1981). *Course in Universal Algebra*. Springer-Verlag, ISBN 3-540-90578-2.

[3] Poizat, B. (2000). *A Course in Model Theory*, Springer.

[4] Cégielski, P. (1989). The elementary theory of the natural lattice is finitely axiomatizable. *Notre Dame Journal of Formal Logic*, 30(1), 138–150. https://doi.org/10.1305/ndjfl/1093635001.

[5] Ortiz, C.T. (2018). *Complete Theories of Boolean Algebras*. Departament de Matemàtiques Informàtica, June 27.

[6] Leary, Ch.C. & Kristiansen, L. (2019). *A Friendly Introduction to Mathematical Logic*, Milne Library.

[7] Prawitz D., & Westerståhl, D. (1994). *Logic and Philosophy of Science in Uppsala*, Springer Science and Business Media, Tir 8, 1392 AP-Philosophy.

[8] Dutilh, N.C. (2012). *Formal Languages in Logic*, ISBN: 9781107020917.

[9] Enderton, H.B. (2001). *A Mathematical Introduction to Logic*, Academic Press (2nd ed.), ISBN: 9780122384523.

[10] Givant S. & Halmos, P. (2009). *Introduction to Boolean Algebras*, Undergraduate Texts in Mathematics. Springer.

[11] Salehi, S. (2018). On axiomatizability of the multiplicative theory of numbers, *Fundamenta Informaticae*, 159(3), 279–296.

[12] Salehi, S. (2012). *Axiomatizing Mathematical Theories :Multiplication*, in:A.Kamali-Nejad (ed). Proceedings of Frontiers in Mathematical Sciences, Sharif University of Technology. Tehran, Iran, (2012) 165–176.

[13] Smorynski, C. (1991). *Logical Number Theory I*. Springer-Verlag.

[14] Habič, M.E., Hamkins, J.D., Klausner, L.D., Verner, J. & Williams, K.J. (2019). *Set-theoretic blockchains*, Archive for Mathematical Logic.