Fundamenta Informaticae 159 (2018) 279–296
DOI 10.3233/FI-2018-1665
IOS Press

On Axiomatizability of the Multiplicative Theory of Numbers

Saeed Salehi*

Research Institute for Fundamental Sciences (RIFS)*, University of Tabriz*
P.O.Box 51666–16471, Bahman 29th Boulevard, Tabriz, IRAN
School of Mathematics, Institute for Research in Fundamental Sciences (𝕀ℙℳ)
P.O.Box 19395–5746, Niavaran, Tehran, IRAN
salehipour@tabrizu.ac.ir, saeedsalehi@ipm.ir

Abstract. The multiplicative theory of a set of numbers (which could be natural, integer, rational, real or complex numbers) is the first-order theory of the structure of that set with (solely) the multiplication operation (that set is taken to be multiplicative, i.e., closed under multiplication). In this paper we study the multiplicative theories of the complex, real and (positive) rational numbers. These theories (and also the multiplicative theories of natural and integer numbers) are known to be decidable (i.e., there exists an algorithm that decides whether a given sentence is derivable form the theory); here we present explicit axiomatizations for them and show that they are not finitely axiomatizable. For each of these sets (of complex, real and [positive] rational numbers) a language, including the multiplication operation, is introduced in a way that it allows quantifier elimination (for the theory of that set).

Keywords: Decidability; Completeness; Multiplicative Theory; Quantifier Elimination.

1. Introduction

Providing a (complete and computably decidable) axiomatization for mathematical structures is one goal of mathematical logic. This is closely related to the problem of the (computable) decidability

*This research was partially supported by a grant from 𝕀ℙℳ (No. 91030033).
Address for correspondence: Research Institute for Fundamental Sciences RIFS, University of Tabriz, P.O.Box 51666–16471, Bahman 29th Boulevard, Tabriz, IRAN.

Received July 2017; revised December 2017.

of (the theory of) a given mathematical structure, since by the (computable) enumerability of all the formulas (provided that the language of the structure is a computably decidable set), provability of a sentence or its unprovability (which is equivalent to the provability of its negation in complete axiomatizations) can be decided algorithmically in a finite number of steps. Thus by presenting a complete and computably decidable axiomatization for a structure, the computable decidability of the theory of that structure is proved. While the mere knowledge of the decidability of the theory of a structure does not provide us with an explicit axiomatization (for the theory of that structure) and also leaves open the problem of the finite axiomatizability of that structure.

In this paper we study the theories of the sets of complex, real and (positive) rational numbers with the multiplication operation. The multiplicative structure of the complex numbers, i.e., $\langle \mathbb{C}; \times \rangle$, is decidable (and completely and computably axiomatizable) by Tarski's theorem which states that the (additive and multiplicative) theory of the complex numbers ($\langle \mathbb{C}; +, \times \rangle$) is decidable and can be (completely) axiomatized by the theory of *algebraically closed fields of characteristic* 0 (see e.g. [3, Section IV of Chapter 4] or [5, Corollary 2.2.9] or [6, Theorem 21.9]). Here, we axiomatize the theory of this structure directly (without using Tarski's theorem) and show that it cannot be axiomatized by any finite number of sentences. The same holds for the multiplicative theory of the real numbers, $\langle \mathbb{R}; \times \rangle$: it is also decidable (and completely and computably axiomatizable) by Tarski's theorem which states that the (additive and multiplicative) theory of the real numbers ($\langle \mathbb{R}; +, \times \rangle$) is decidable and can be (completely) axiomatized by the theory of *real closed* (*ordered*) *fields* (see e.g. [3, Section V of Chapter 4] or [5, Corollary 3.3.16] or [6, Theorem 21.36]). Again an explicit axiomatization for the theory of this structure is provided here, in which the addition operation is not used.

The decidability of the multiplicative structure of the non-zero rational numbers was announced by A. Mostowski in [7] where he mentions that "the elementary theory of multiplication of rationals different from 0" is the weak power of the additive theory of "all integers (positive and negative)". Here, "the elementary theory" means 'the first-order theory'. The decidability of this theory is claimed to had been proved (beforehand) by W. Szmielew in [13]. We firstly note that the weak power of the additive theory of integers, $\langle \mathbb{Z}; + \rangle$, is the multiplicative theory of the *positive* rational numbers, $\langle \mathbb{Q}^+; \times \rangle$; not the whole (non-zero) rational numbers. Secondly, the multiplicative theory of the positive rational numbers has not been studied in [13] (indeed it appears in none of Szmielew's works). However, Mostowski's results in [7] imply the decidability of the multiplicative theory of the positive rational numbers $\langle \mathbb{Q}^+; \times \rangle$. In the last section of this paper, we give a direct proof of this fact with an explicit axiomatization, and show that the theory of this structure is not finitely axiomatizable. Along the way, for technical reasons, we also study the additive theories of the sets of integer, rational, real and complex numbers, $\langle \mathbb{Z}; + \rangle$, $\langle \mathbb{Q}; + \rangle$, $\langle \mathbb{R}; + \rangle$ and $\langle \mathbb{C}; + \rangle$ (for $\langle \mathbb{N}; + \rangle$ see e.g. [2, Theorem 32A]). The present paper is an extended, much improved and corrected version of the conference paper [11].

1.1. Some preliminaries

Let $\mathbb{P}$ denote the set of all (natural) prime numbers and denote the i^{th} prime number by $\mathfrak{p}_i$ (so we have $\mathfrak{p}_0 = 2, \mathfrak{p}_1 = 3, \mathfrak{p}_2 = 5, \cdots$). Every natural number other than $0, 1$ has a unique factorization into a product of prime numbers (by the fundamental theorem of arithmetic); this holds for every negative integer other than -1 too. Likewise, every rational number other than $-1, 0, 1$ has a unique

factorization into a product of prime numbers in which the exponents could be negative; for example $\frac{175}{84}$ which becomes $\frac{25}{12}$ after simplification can be written as $2^{-2} \cdot 3^{-1} \cdot 5^2$. The symbols $\times$ and $\cdot$ are used interchangeably throughout the paper. For convenience, we make the convention that $0^{-1} = 0$ and we will see that this does not contradict our intuition with the axioms used below. Needless to say x^n symbolizes $x \cdot x \cdot \ldots \cdot x$ ($n-$times) and also $x + x + \cdots + x$ ($n-$times) is abbreviated as $n \centerdot x$. The main tool for the process of quantifier elimination is the following result which can be found in e.g. [2, Theorem 31F] or [3, Theorem 1 in Chapter 4] or [5, Lemma 3.1.5] or [12, Lemma 4.1].

Lemma 1.1. (The Main Lemma of Quantifier Elimination)
A theory (or a structure) admits quantifier elimination if and only if every formula of the form $\exists x(\bigwedge_i \alpha_i)$ is (recursively) equivalent with a quantifier-free formula, where each α_i is either an atomic formula or the negation of an atomic formula.

Proof:
Every formula ψ can be written (equivalently) in the prenex normal form, say

$$\mathsf{Q}_1 x_1 \mathsf{Q}_2 x_2 \cdots \mathsf{Q}_n x_n \theta(x_1, x_2, \cdots, x_n),$$

where Q_i's are quantifiers and θ is quantifier-free. If $\mathsf{Q}_n = \exists$ then let $\theta' = \theta$ and if $\mathsf{Q}_n = \forall$ then let $\theta' = \neg\theta$ (note that in the latter case $\forall x_n \theta \equiv \neg\exists x_n \theta'$). Now, the quantifier-free formula θ' can be written in the disjunctive normal form, say $\bigvee_i \bigwedge_j \alpha_{i,j}$ where each $\alpha_{i,j}$ is a literal (i.e., an atomic or a negated atomic formula). Noting that $\exists x(\bigvee_i \beta_i) \equiv \bigvee_i \exists x \beta_i$ we have

$$\psi \equiv \mathsf{Q}_1 x_1 \mathsf{Q}_2 x_2 \cdots \mathsf{Q}_{n-1} x_{n-1} \square \bigvee_i \exists x_n (\bigwedge_j \alpha_{i,j})$$

where $\square$ is nothing (empty) when $\mathsf{Q}_n = \exists$ and $\square = \neg$ when $\mathsf{Q}_n = \forall$. Now, if $\exists x_n(\bigwedge_j \alpha_{i,j})$ is equivalent with a quantifier-free formula, then ψ is equivalent with a formula with one less quantifier; continuing this way one can show that ψ is equivalent with a formula which has no quantifier. $\square$

2. The multiplicative theory of the complex numbers

For axiomatizing $\langle \mathbb{C}; \times \rangle$ we do not need the addition operation ($+$) and in fact it is not definable from multiplication: the multiplicative automorphism $z \mapsto z^{-1}$ (for $z \neq 0$ and $0 \mapsto 0$) does not preserve the addition operation. Indeed, there exists a nice axiomatization for the multiplicative theory of the complex numbers which will be presented below.

Definition 2.1. (Roots of Unity)
For any natural number $n \geqslant 2$ let $\boldsymbol{\omega}_n = \cos(2\boldsymbol{\pi}/n) + \boldsymbol{i}' \sin(2\boldsymbol{\pi}/n)$. So, all the n^{th} roots of unity are the complex numbers $\{1, \boldsymbol{\omega}_n, \boldsymbol{\omega}_n^2, \cdots, \boldsymbol{\omega}_n^{n-1}\}$. $\circledast$

Let us note that $\boldsymbol{\omega}_2 = -1, \boldsymbol{\omega}_3 = (-1/2) + \boldsymbol{i}'(\sqrt{3}/2)$ and $\boldsymbol{\omega}_4 = \boldsymbol{i}'$.

Theorem 2.2. (Infinite Axiomatizablity of $\langle\mathbb{C};\times\rangle$)
The following theory completely axiomatizes the multiplicative theory of the complex numbers and, moreover, the infinite structure $\langle\mathbb{C};\times,\circ^{-1},\mathbf{0},\mathbf{1},\boldsymbol{\omega}_2,\boldsymbol{\omega}_3,\boldsymbol{\omega}_4,\cdots\rangle$ admits quantifier elimination, and so has a decidable theory.

$(\mathtt{M}_1)$ $\forall x,y,z\,\big(x\cdot(y\cdot z)=(x\cdot y)\cdot z\big)$
$(\mathtt{M}_2)$ $\forall x\,\big(x\cdot\mathbf{1}=x\big)$
$(\mathtt{M}_3)$ $\forall x\,\big(x\neq\mathbf{0}\longrightarrow x\cdot x^{-1}=\mathbf{1}\big)$
$(\mathtt{M}_4)$ $\forall x,y\,\big(x\cdot y=y\cdot x\big)$
$(\mathtt{M}_5)$ $\forall x\,\big(x\cdot\mathbf{0}=\mathbf{0}=\mathbf{0}^{-1}\big)$
$(\mathtt{M}_{6,n})$ $\bigwedge_{i<j<n}(\boldsymbol{\omega}_n)^i\neq(\boldsymbol{\omega}_n)^j$
$(\mathtt{M}_{7,n})$ $\forall x\,\big(x^n=\mathbf{1}\longleftrightarrow\bigvee_{i<n}x=(\boldsymbol{\omega}_n)^i\big)$
$(\mathtt{M}_{8,n})$ $\forall x\,\exists y\,\big(y^n=x\big)$

Where $n>1$ is a natural number.

Proof:
By $\mathtt{M}_1,\mathtt{M}_2,\mathtt{M}_3$ and $\mathtt{M}_4$ we have $(u\cdot v)^{-1}=u^{-1}\cdot v^{-1}$ for any $u,v\neq\mathbf{0}$; by $\mathtt{M}_5$ this holds even when any of u or v equals to $\mathbf{0}$. So, every term involving x is equal to $x^k\cdot t$ for some x-free term t (i.e., x does not appear in t) and for some $k\in\mathbb{Z}-\{\mathbf{0}\}$. Therefore, every atomic formula involving x is equivalent with $x^k\cdot t=x^m\cdot u$ for some x-free terms t,u and some $\langle k,m\rangle\in\mathbb{N}^2-\{\langle0,0\rangle\}$. If $k\geqslant m>0$ then this atomic formula is equivalent with

$$(x=\mathbf{0})\vee(x\neq\mathbf{0}\wedge t=\mathbf{0}\wedge u=\mathbf{0})\vee(x\neq\mathbf{0}\wedge t\neq\mathbf{0}\wedge x^{k-m}=u\cdot t^{-1}),$$

and if $k\geqslant m=0$ then it is equivalent with

$$(t=\mathbf{0}\wedge u=\mathbf{0})\vee(t\neq\mathbf{0}\wedge x^k=u\cdot t^{-1}).$$

Also, the negated atomic formula $x^k\cdot t\neq x^m\cdot u$, when $k\geqslant m>0$, is equivalent with

$$(x\neq\mathbf{0}\wedge t=\mathbf{0}\wedge u\neq\mathbf{0})\vee(x\neq\mathbf{0}\wedge t\neq\mathbf{0}\wedge x^{k-m}\neq u\cdot t^{-1}),$$

and when $k\geqslant m=0$ is equivalent with

$$(t=\mathbf{0}\wedge u\neq\mathbf{0})\vee(t\neq\mathbf{0}\wedge x^k\neq u\cdot t^{-1}).$$

So, by the Main Lemma (1.1) it suffices to show that every formula of the form

$$\exists x(\bigwedge_{i<\ell}x^{n_i}=t_i\ \wedge\ \bigwedge_{j<k}x^{m_j}\neq s_j)\tag{1}$$

is equivalent with a quantifier-free formula, where t_i's and s_j's are x-free terms and n_i's and m_j's are positive natural numbers. If $\ell=0$ then the formula (1), that is $\exists x(\bigwedge_{j<k}x^{m_j}\neq s_j)$, follows from $\mathtt{M}_{6,n}$ and $\mathtt{M}_{7,n}$ (and so it is equivalent with the quantifier-free formula $\mathbf{0}=\mathbf{0}$): by $\mathtt{M}_{6,n}$'s there are infinitely many elements and by $\mathtt{M}_{7,n}$ (for $n=m_j$) there are at most finitely many x's with $x^{m_j}=s_j$ for each $j<k$. Whence, let us suppose that $\ell>0$. If there are some $i,j<\ell$ such that $n_i<n_j$ then $(x^{n_i}=t_i\wedge x^{n_j}=t_j)\equiv(t_i=\mathbf{0}\wedge x=\mathbf{0}\wedge t_j=\mathbf{0})\vee(t_i\neq\mathbf{0}\wedge x^{n_i}=t_i\wedge x^{n_j-n_i}=t_j\cdot t_i^{-1})$. So, we

can assume that for some $n > 0$ we have $n_i = n$ for all $i < \ell$. Then, for $t = t_0$, the formula (1) is equivalent with the conjunction of the formula $\bigwedge_{i<\ell} t_i = t$ with the following formula

$$\exists x(x^n = t \ \wedge \bigwedge_{j<k} x^{m_j} \neq s_j) \tag{2}$$

whose equivalence with a quantifier-free formula is proved below. Let us note that if $k = 0$ then (2) follows from $\mathtt{M}_{8,n}$ (and so is equivalent with $\mathbf{0} = \mathbf{0}$). Whence, let us suppose that $k > 0$. By $\mathtt{M}_{6,n}$ and $\mathtt{M}_{7,n}$ we have the equivalence $x^m \neq s \longleftrightarrow x^{mn} \neq s^n \vee \bigvee_{0<i<n} x^m = s(\boldsymbol{\omega}_n)^i$ for all complex numbers x, s with $s \neq 0$ and all natural numbers m, n. Thus, $\theta \wedge x^n = t \wedge x^m \neq s$ is equivalent with $\big[s = \mathbf{0} \wedge \theta \wedge x^n = t \wedge x \neq \mathbf{0}\big] \vee \big[s \neq \mathbf{0} \wedge \theta \wedge x^n = t \wedge \big(x^{mn} \neq s^n \vee \bigvee_{0<i<n} x^m = s(\boldsymbol{\omega}_n)^i\big)\big]$. The second disjunct is equivalent with

$$\begin{aligned}
\big[s \neq \mathbf{0} \wedge \theta \wedge x^n = t \wedge \big(x^{mn} \neq s^n \vee \bigvee_{0<i<n} x^m = s(\boldsymbol{\omega}_n)^i\big)\big] \quad &\equiv \\
(s \neq \mathbf{0} \wedge \theta \wedge x^n = t \wedge x^{mn} \neq s^n) \vee \bigvee_{0<i<n} \big(s \neq \mathbf{0} \wedge \theta \wedge x^n = t \wedge x^m = s(\boldsymbol{\omega}_n)^i\big) \quad &\equiv \\
(s \neq \mathbf{0} \wedge \theta \wedge x^n = t \wedge t^m \neq s^n) \vee \bigvee_{0<i<n} \big(s \neq \mathbf{0} \wedge \theta \wedge x^n = t \wedge x^m = s(\boldsymbol{\omega}_n)^i\big).&
\end{aligned}$$

Continuing this way (by eliminating the inequalities —other than $x \neq \mathbf{0}$— one by one) we see that all we need to do is to eliminate the quantifier of the following form of formulas

$$\exists x(\bigwedge_{i<\ell} x^{n_i} = t_i) \quad \text{or} \quad \exists x(x \neq \mathbf{0} \wedge \bigwedge_{i<\ell} x^{n_i} = t_i) \tag{3}$$

where n_i's are positive natural numbers and t_i's are x-free terms (i.e., x does not appear in them). Just like the way we reached at (2) from (1) we can also see that the formulas (3) are equivalent with the conjunctions of an x-free formula with a formula of the form $\exists x(x^n = t)$ or $\exists x(x \neq \mathbf{0} \wedge x^n = t)$ for some positive integer n and some x-free term t. Above we noted that $\exists x(x^n = t)$ follows from $\mathtt{M}_{8,n}$ and so is equivalent with the quantifier-free formula $\mathbf{0} = \mathbf{0}$; thus $\exists x(x \neq \mathbf{0} \wedge x^n = t)$ is equivalent with the quantifier-free formula $t \neq \mathbf{0}$ as well. □

Now we show that the multiplicative theory of the complex numbers is not finitely axiomatizable.

Definition 2.3. (Two Additive Sub-Structures of the Rational Numbers)
Let $m \in \mathbb{N}$ be a positive integer ($m > 0$). Put

$$\mathbb{Z}/m = \{\frac{a}{m} \mid a \in \mathbb{Z}\}, \quad \text{and}$$

$$\mathbb{Q}/m = \{\frac{a}{m^k} \mid a \in \mathbb{Z}, k \in \mathbb{N}\}.$$

These are additive (i.e., closed under addition) subsets of $\mathbb{Q}$. ⊛

Let us note that $\mathbb{Q}/m$ is also closed under the operations $x \mapsto x/d$ for any d which divides m.

Theorem 2.4. (No Finite Axiomatization for $\langle \mathbb{C}; \times \rangle$)
The theory of the structure $\langle \mathbb{C}; \times \rangle$ is not finitely axiomatizable.

Proof:
If the theory is finitely axiomatizable by, say, $B_1, \cdots, B_k$ then the formula $B_1 \wedge \cdots \wedge B_k$ is provable from $\{\mathtt{M}_1, \mathtt{M}_2, \mathtt{M}_3, \mathtt{M}_4, \mathtt{M}_5\} \cup \{\mathtt{M}_{6,n}, \mathtt{M}_{7,n}, \mathtt{M}_{8,n} \mid n > 1\}$ hence just a finite number of the instances of $\mathtt{M}_{8,n}$ are used in the proof. Let N be an arbitrarily large natural number, and put $M = N! = 2 \times \cdots \times N$. Let

$$\mathbb{C}/M = \{\prod_{i<\ell} \mathfrak{p}_i^{r_i} \prod_{j<k} (\boldsymbol{\omega}_j)^{n_j} \mid \ell, k, n_j \in \mathbb{N}, r_i \in \mathbb{Q}/M\}.$$

The set $\mathbb{C}/M$ is a multiplicative subset of $\mathbb{C}$ (is closed under multiplication and inverses) and so satisfies $\mathtt{M}_1, \mathtt{M}_2, \mathtt{M}_3, \mathtt{M}_4, \mathtt{M}_5, \mathtt{M}_{6,n}$ and $\mathtt{M}_{7,n}$ (for all $n \geqslant 2$). Since the set $\mathbb{Q}/M$ is closed under the operations $x \mapsto x/n$ for every $n \in \{1, 2, 3, \cdots, N\}$ then $\mathbb{C}/M$ satisfies $\mathtt{M}_{8,n} : \forall x \exists y (y^n = x)$ for $n = 2, 3, \cdots, N$. But for a large prime number $\mathfrak{p} > M$ the structure $\langle \mathbb{C}/M; \times \rangle$ does not satisfy $\mathtt{M}_{8,\mathfrak{p}} : \forall x \exists y (y^{\mathfrak{p}} = x)$ since by $1/\mathfrak{p} \notin \mathbb{Q}/M$ we have $2^{1/\mathfrak{p}} \notin \mathbb{C}/M$. So, the instances of $\mathtt{M}_{8,n}$ for $n = 2, \cdots, N$ (together with the axioms $\mathtt{M}_1, \mathtt{M}_2, \mathtt{M}_3, \mathtt{M}_4, \mathtt{M}_5, \mathtt{M}_{6,n}$ and $\mathtt{M}_{7,n}$ for all $n > 1$) does not imply the instance of $\mathtt{M}_{8,n}$ for $n = \mathfrak{p}$, where $\mathfrak{p}$ is a prime number greater than $N!$. □

2.1. The additive theory of the complex (and real and rational) numbers

It is interesting to have a look at the additive theory of the complex numbers (i.e., $\langle \mathbb{C}; + \rangle$): its theory is the same as of the additive theory of the real and the rational numbers ($\langle \mathbb{R}; + \rangle$ and $\langle \mathbb{Q}; + \rangle$) and also the multiplicative theory of the positive real numbers ($\langle \mathbb{R}^+; \times \rangle$); cf. [5, Theorem 3.1.9].

Proposition 2.5. (Infinite Axiomatizablity of $\langle \mathbb{C}; + \rangle$ and $\langle \mathbb{R}; + \rangle$ and $\langle \mathbb{Q}; + \rangle$)
The following theory completely axiomatizes the additive theory of the complex (and real and rational) numbers and, moreover, the structure $\langle \mathbb{C}; +, -, \mathbf{0} \rangle$ (and $\langle \mathbb{R}; +, -, \mathbf{0} \rangle$ and $\langle \mathbb{Q}; +, -, \mathbf{0} \rangle$) admits quantifier elimination, and so has a decidable theory.

$(\mathtt{A}_1)$ $\forall x, y, z \big(x + (y + z) = (x + y) + z\big)$	$(\mathtt{A}_2)$ $\forall x \big(x + \mathbf{0} = x\big)$
$(\mathtt{A}_3)$ $\forall x \big(x + (-x) = \mathbf{0}\big)$	$(\mathtt{A}_4)$ $\forall x, y \big(x + y = y + x\big)$
$(\mathtt{A}_{5,n})$ $\forall x \big(n \centerdot x = \mathbf{0} \longrightarrow x = \mathbf{0}\big)$	$(\mathtt{A}_6)$ $\exists y \big(y \neq \mathbf{0}\big)$
$(\mathtt{A}_{7,n})$ $\forall x \exists y \big(x = n \centerdot y\big)$	Where $n \geqslant 1$ is a natural number.

Proof:
By $\mathtt{A}_1, \mathtt{A}_2, \mathtt{A}_3$ and $\mathtt{A}_4$ every term involving x is equal to $k \centerdot x + t$ for some x-free term t and $k \in \mathbb{Z} - \{\mathbf{0}\}$. Therefore, every atomic formula involving x is equivalent with $k \centerdot x = t$ for some positive integer k and some x-free term t. Thus, by the Main Lemma (1.1) it suffices to eliminate the quantifier of

$$\exists x (\bigwedge_{i<\ell} n_i \centerdot x = t_i \ \wedge \bigwedge_{j<k} m_j \centerdot x \neq s_j). \tag{4}$$

By $\mathtt{A}_{5,k}$ (and $\mathtt{A}_3$) we have $a = b \longleftrightarrow k \centerdot a = k \centerdot b$, and so we can assume that all n_i's and all m_j's in the formula (4) are equal to each other. Thus we show the equivalence of

$$\exists x (\bigwedge_{i<\ell} q \centerdot x = t_i \ \wedge \bigwedge_{j<k} q \centerdot x \neq s_j) \tag{5}$$

with a quantifier-free formula. By $\mathtt{A}_{7,q}$, (5) is equivalent with the following formula (for $y = q \centerdot x$):

$$\exists y(\bigwedge_{i<\ell} y = t_i \ \wedge \ \bigwedge_{j<k} y \neq s_j). \tag{6}$$

Now, if $\ell > 0$ then (6) is equivalent with the quantifier-free formula $\bigwedge_{i<\ell} t_0 = t_i \wedge \bigwedge_{j<k} t_0 \neq s_j$ and if $\ell = 0$ then (6) i.e., the formula $\exists y(\bigwedge_{j<k} y \neq s_j)$ follows from $\mathtt{A}_6$ (which together with $\mathtt{A}_{5,n}$'s implies that there are infinitely many elements: for $y \neq \mathbf{0}$ we have $k \centerdot y \neq m \centerdot y$ whenever $k \neq m$), and so is equivalent with the quantifier-free formula $\mathbf{0} = \mathbf{0}$. □

Just a little note that this axiomatization of the additive theory of the complex, real and rational numbers cannot be finite:

Proposition 2.6. (No Finite Axiomatization for $\langle \mathbb{C}; + \rangle$ and $\langle \mathbb{R}; + \rangle$ and $\langle \mathbb{Q}; + \rangle$)
The theories of the structures $\langle \mathbb{C}; + \rangle$, $\langle \mathbb{R}; + \rangle$ and $\langle \mathbb{Q}; + \rangle$ are not finitely axiomatizable.

Proof:
It suffices to note that $\mathtt{A}_1, \mathtt{A}_2, \mathtt{A}_3, \mathtt{A}_4, \mathtt{A}_{5,n}, \mathtt{A}_6$, and a finite number of the instances of $\mathtt{A}_{7,n}$ do not imply all the instances of $\mathtt{A}_{7,n}$. For an arbitrary large N let $M = N! = 2 \times \cdots \times N$. Then $\mathbb{Q}/M$ satisfies $\mathtt{A}_1, \mathtt{A}_2, \mathtt{A}_3, \mathtt{A}_4, \mathtt{A}_{5,n}, \mathtt{A}_6$, and also $\mathtt{A}_{7,n} : \forall x \exists y \left(x = n \centerdot y\right)$ for $n \in \{2, \cdots, N\}$, but does not satisfy the instance $\forall x \exists y \left(x = \mathfrak{p} \centerdot y\right)$ of $\mathtt{A}_{7,\mathfrak{p}}$ for a large prime $\mathfrak{p} > M$. □

3. The multiplicative theory of the real numbers

The mapping $x \mapsto 2^x$ is an isomorphism between the additive structure of the real numbers $\langle \mathbb{R}; + \rangle$ and the multiplicative structure of the positive reals $\langle \mathbb{R}^+; \times \rangle$. Indeed the proof of Proposition 2.5 can show the (computable) axiomatizability (and decidability) of the theory of $\langle \mathbb{R}^+; \times \rangle$:

Proposition 3.1. (Axiomatizablity of $\langle \mathbb{R}^+; \times \rangle$—Infinitely)
The following theory completely axiomatizes the structure $\langle \mathbb{R}^+; \times, \circ^{-1}, \mathbf{1} \rangle$ and, moreover, its theory admits quantifier elimination, and so is decidable.

$(\mathtt{M}_1)$ $\forall x, y, z \left(x \cdot (y \cdot z) = (x \cdot y) \cdot z\right)$	$(\mathtt{M}_2)$ $\forall x \left(x \cdot \mathbf{1} = x\right)$
$(\mathtt{M}_3^\circ)$ $\forall x \left(x \cdot x^{-1} = \mathbf{1}\right)$	$(\mathtt{M}_4)$ $\forall x, y \left(x \cdot y = y \cdot x\right)$
$(\mathtt{M}_{7,n}^\circ)$ $\forall x \left(x^n = \mathbf{1} \longrightarrow x = \mathbf{1}\right)$	$(\mathtt{M}_{8,n})$ $\forall x \exists y \left(x = y^n\right)$
$(\mathtt{M}_9)$ $\exists y \left(y \neq \mathbf{1}\right)$	Where $n \geqslant 1$ is a natural number.

However, this theory is not finitely axiomatizable.

Proof:
For $M = N!$ the multiplicative subset of positive real numbers

$$\mathbb{R}^+/M = \{\prod_{i<\ell} \mathfrak{p}_i^{r_i} \mid \ell \in \mathbb{N}, r_i \in \mathbb{Q}/M\}$$

satisfies $\mathtt{M}_1, \mathtt{M}_2, \mathtt{M}_3^\circ, \mathtt{M}_4, \mathtt{M}_{7,n}^\circ, \mathtt{M}_9$ (for all $n \geqslant 1$) and the instances of $\mathtt{M}_{8,n}$ for $n = 1, 2, \cdots, N$ but does not satisfy the instance of $\mathtt{M}_{8,n}$ when n is a prime number greater than M. □

Let us note that $\langle \mathbb{R}^+; \times, \circ^{-1}, \mathbf{1}\rangle$ is an abelian group, and the theory of all abelian groups is decidable (proved by Szmielew for the first time in [14]).

Adding a zero to the elements with the axiom $\forall x \left(x \cdot \mathbf{0} = \mathbf{0} = \mathbf{0}^{-1}\right)$ can completely axiomatize the multiplicative theory of the non-negative real numbers $\langle \mathbb{R}^{\geqslant 0}; \times\rangle$. Since the proof of the following theorem will be essentially repeated in Theorem 3.3, we do not present it.

Proposition 3.2. (Infinite Axiomatizablity of $\langle \mathbb{R}^{\geqslant 0}; \times\rangle$)
The following theory completely axiomatizes the structure $\langle \mathbb{R}^{\geqslant 0}; \times, \circ^{-1}, \mathbf{0}, \mathbf{1}\rangle$ and, moreover, its theory admits quantifier elimination, and so is decidable.

$(\mathtt{M}_1)$ $\forall x, y, z \left(x \cdot (y \cdot z) = (x \cdot y) \cdot z\right)$
$(\mathtt{M}_2)$ $\forall x \left(x \cdot \mathbf{1} = x\right)$
$(\mathtt{M}_3)$ $\forall x \left(x \neq \mathbf{0} \longrightarrow x \cdot x^{-1} = \mathbf{1}\right)$
$(\mathtt{M}_4)$ $\forall x, y \left(x \cdot y = y \cdot x\right)$
$(\mathtt{M}^{\circ}_{7,n})$ $\forall x \left(x^n = \mathbf{1} \longrightarrow x = \mathbf{1}\right)$
$(\mathtt{M}_{8,n})$ $\forall x \exists y \left(x = y^n\right)$
$(\mathtt{M}^{\circ}_9)$ $\exists y \left(y \neq \mathbf{0}, \mathbf{1}\right)$
$(\mathtt{M}_{10})$ $\forall x \left(x \cdot \mathbf{0} = \mathbf{0} = \mathbf{0}^{-1}\right)$
Where $n \geqslant 1$ is a natural number.

This theory is not finitely axiomatizable. □

The whole set of the real numbers with the multiplication operation, i.e., the structure $\langle \mathbb{R}; \times, \circ^{-1}, \mathbf{0}, \mathbf{1}\rangle$, does not admit quantifier elimination: the formula $\exists x(y = x \cdot x)$ is not equivalent with any quantifier-free formula (in the language $\{\times, \circ^{-1}, \mathbf{0}, \mathbf{1}, -\mathbf{1}\}$). Indeed this formula is equivalent with the quantifier-free formula $y \geqslant 0$, so it is tempting to add order to the language for eliminating the quantifiers. But order is not definable by multiplication in $\mathbb{R}$ since the multiplicative automorphism $x \mapsto 1/x$ (for $x \neq 0$ and $0 \mapsto 0$) does not preserve the order relation (neither does it preserve the addition operation). But if we add the *positivity* property to the language, $\mathcal{P}(y)$ meaning that "y is a positive real number" then the procedure of quantifier elimination can go through (then for example $\exists x(y = x \cdot x)$ is equivalent with the quantifier-free formula $\mathcal{P}(y) \vee y = \mathbf{0}$). Below, $-x$ is a shorthand for $(-1) \cdot x$.

Theorem 3.3. (Infinite Axiomatizablity of $\langle \mathbb{R}; \times\rangle$)
The following theory completely axiomatizes the structure $\langle \mathbb{R}; \times, \circ^{-1}, \mathbf{0}, \mathbf{1}, -\mathbf{1}, \mathcal{P}\rangle$ and, moreover, its theory admits quantifier elimination, and so is decidable.

$(\mathtt{M}_1)$ $\forall x, y, z \left(x \cdot (y \cdot z) = (x \cdot y) \cdot z\right)$
$(\mathtt{M}_2)$ $\forall x \left(x \cdot \mathbf{1} = x\right)$
$(\mathtt{M}_3)$ $\forall x \left(x \neq \mathbf{0} \longrightarrow x \cdot x^{-1} = \mathbf{1}\right)$
$(\mathtt{M}_4)$ $\forall x, y \left(x \cdot y = y \cdot x\right)$
$(\mathtt{M}^{\diamond}_9)$ $\exists y \left(y \neq -\mathbf{1}, \mathbf{0}, \mathbf{1}\right)$
$(\mathtt{M}_{10})$ $\forall x \left(x \cdot \mathbf{0} = \mathbf{0} = \mathbf{0}^{-1}\right)$
$(\mathtt{M}_{11,n})$ $\forall x \left(x^{2n} = \mathbf{1} \longleftrightarrow x = \mathbf{1} \vee x = -\mathbf{1}\right)$
$(\mathtt{M}_{12,n})$ $\forall x \exists y \left(x = y^{2n+1}\right)$
$(\mathtt{M}_{13})$ $\forall x \left(\mathcal{P}(x) \longleftrightarrow \exists y[y \neq \mathbf{0} \wedge x = y^2]\right)$
$(\mathtt{M}_{14})$ $\forall x \left(x \neq \mathbf{0} \longrightarrow [\neg\mathcal{P}(x) \leftrightarrow \mathcal{P}(-x)]\right)$
$(\mathtt{M}_{15})$ $\forall x, y \neq \mathbf{0} \left(\mathcal{P}(x \cdot y) \longleftrightarrow [\mathcal{P}(x) \leftrightarrow \mathcal{P}(y)]\right)$
Where $n \geqslant 1$ is a natural number.

Proof:
Firstly, let us derive $(\mathtt{M}_{16})$ $\neg\mathcal{P}(\mathbf{0}) \wedge \mathcal{P}(\mathbf{1})$ as follows: from $\mathtt{M}_2$, $\mathtt{M}_{10}$ and $\mathtt{M}^{\diamond}_9$ we have $\mathbf{0} \neq \mathbf{1}$ and so $\mathtt{M}_2$ and $\mathtt{M}_{13}$ imply $\mathcal{P}(\mathbf{1})$; also $\mathtt{M}_3$ (together with $\mathbf{0} \neq \mathbf{1}$) implies $\forall x(x^k = \mathbf{0} \longrightarrow x = \mathbf{0})$ whence $\neg\mathcal{P}(\mathbf{0})$ holds

by $\mathtt{M}_{13}$. Then we note that e.g. the sentence $\forall x \left(x^{2k+1} = \mathbf{1} \longrightarrow x = \mathbf{1}\right)$ is derivable from the above axioms, since if $a^{2k+1} = 1$ then by $\mathtt{M}_{16}$ we have $\mathcal{P}(a^{2k+1})$ or equivalently $\mathcal{P}(a^{2k} \cdot a)$. Now by $\mathtt{M}_{13}$ (from which $\mathcal{P}(a^{2k})$ follows) and $\mathtt{M}_{15}$ we have $\mathcal{P}(a)$, and so by $\mathtt{M}_{13}$, $a = b^2$ for some b. Now $\mathtt{M}_{11,2k+1}$ (since $b^{2\cdot(2k+1)} = 1$) implies that either $b = 1$ or $b = -1$ holds; in each case we have $a = b^2 = 1$ (by $\mathtt{M}_{11,1}$). Also, the above axioms imply that there are infinitely many elements, since for any c with $c \neq -1, 0, 1$ (by $\mathtt{M}_9^{\diamond}$) we have $c^k \neq c^m$ whenever $k < m$ (by $\mathtt{M}_{11,m-k}$).
Secondly, the axioms of $\langle \mathbb{R}^+; \times \rangle$ (in Theorem 3.1) are derivable from the above axioms when they are relativized to $\mathcal{P}$. For example, the relativization of $\mathtt{M}_{7,n}^{\circ}$ which is $\forall x\big(\mathcal{P}(x) \longrightarrow [x^n = \mathbf{1} \to x = \mathbf{1}]\big)$ was actually proved above for odd n (and for even n it follows from $\mathtt{M}_{11,n/2}$ noting that $\mathtt{M}_{16}$ and $\mathtt{M}_{14}$ imply that $\neg\mathcal{P}(-\mathbf{1})$ holds). We show the relativization of $\mathtt{M}_{8,n}$ to $\mathcal{P}$: $\forall x \exists y\big(\mathcal{P}(x) \longrightarrow x = y^n\big)$. Write $n = 2^k(2\ell+1)$; we prove this by induction on k. For $k = 0$ it follows from $\mathtt{M}_{12,\ell}$; for the induction step we note that if $(z)^{2^k(2\ell+1)} = x$ then we can assume (by $\mathtt{M}_{14}$ and $(-z)^{2^k(2\ell+1)} = (z)^{2^k(2\ell+1)}$) that $\mathcal{P}(z)$ holds and so the result (the existence of some y with $y^2 = z$ whence $y^{2^{k+1}(2\ell+1)} = z^{2^k(2\ell+1)} = x$) follows immediately from $\mathtt{M}_{13}$.
Finally, the procedure of the quantifier elimination goes as follows. The negations behind $\mathcal{P}$'s can be eliminated by $\mathtt{M}_{14}$ which implies (together with $\mathtt{M}_{16}$) that $\neg\mathcal{P}(x) \equiv (x = \mathbf{0}) \vee \mathcal{P}(-x)$. Also by $\mathtt{M}_{15}$ we have that $\mathcal{P}(u \cdot v) \equiv [\mathcal{P}(u) \wedge \mathcal{P}(v)] \vee [\mathcal{P}(-u) \wedge \mathcal{P}(-v)]$. So, we can assume that $\mathcal{P}(\alpha)$ appears only in the positive form and only when α is either y or $-y$ for a variable y. Now, by Lemma 1.1, it suffices to prove the equivalence of the formulas of the form

$$\exists x(\mathcal{P}(\diamondsuit x) \wedge \bigwedge_{i<\ell} x^{n_i} = t_i \ \wedge \ \bigwedge_{j<k} x^{m_j} \neq s_j)$$

with a quantifier-free formula; where t_i's and s_j's are terms and $\diamondsuit x$ is either x or $-x$. For each variable y which appears in t_i's or s_j's we have $y = \mathbf{0} \vee \mathcal{P}(y) \vee \mathcal{P}(-y)$. The case of $y = 0$ need not be considered, and by changing y to $-y$ if necessary, we can assume that "all the variables are positive", including x. Thus, it suffices to eliminate the quantifier of the formula

$$\exists x(\mathcal{P}(x) \wedge \bigwedge_{\iota<\alpha} \mathcal{P}(y_\iota) \wedge \bigwedge_{i<\ell} x^{n_i} = t_i \ \wedge \ \bigwedge_{j<k} x^{m_j} \neq s_j) \tag{7}$$

where all the variables appearing in t_i's and s_j's are among $\{y_\iota\}_{\iota<\alpha}$. Lastly, we can assume that no minus sign $(-)$ appears in (7) since $-(-u) = u$ and the formulas of the form $v = -w$ can be replaced (are equivalent) with $\mathbf{0} \neq \mathbf{0}$ (since v and w are positive as all their variables are positive). Now the formula (7), when all the variables are positive and no minus sing appears in it, is equivalent with a quantifier-free formula by Proposition 3.1. □

Theorem 3.4. (No Finite Axiomatization for $\langle \mathbb{R}; \times \rangle$)
The theory of the structure $\langle \mathbb{R}; \times \rangle$ is not finitely axiomatizable.

Proof:
For $M = (2N + 1)!$ the following set of real numbers

$$\mathbb{R}/M = \{0\} \cup \{(-1)^\iota \prod_{i<\ell} \mathfrak{p}_i^{r_i} \mid \iota \in \{0, 1\}, \ell \in \mathbb{N}, r_i \in \mathbb{Q}/M\}$$

with the multiplication operation and the positivity property satisfies the axioms

$$\mathtt{M}_1, \mathtt{M}_2, \mathtt{M}_3, \mathtt{M}_4, \mathtt{M}_9^{\diamond}, \mathtt{M}_{10}, \mathtt{M}_{11,n}, \mathtt{M}_{13}, \mathtt{M}_{14}, \mathtt{M}_{15} \text{ (for any } n \geqslant 1)$$

and the instances of $\mathtt{M}_{12,n}$ for $n = 1, 2, \cdots, N$, but does not satisfy the instance of $\mathtt{M}_{12,n}$ when $2n+1$ is a prime number greater than M. □

4. The multiplicative theory of the (positive) rational numbers

It will be highly fruitful if we have a look at the theory of $\langle \mathbb{Z}; + \rangle$ before axiomatizing $\langle \mathbb{Q}^+; \times \rangle$. Let us note that the structure $\langle \mathbb{Q}^+; \times, \circ^{-1}, \mathbf{1} \rangle$ is an abelian group and $\langle \mathbb{Q}^+; \times, \circ^{-1}, \mathbf{1}, < \rangle$ is a regularly dense ordered abelian group (in the terminology of [10]). The theory of all regularly dense ordered abelian groups is proved to be decidable in [10].

4.1. The additive theory of the integer numbers

The theory of the structure $\langle \mathbb{Z}; + \rangle$ does not admit quantifier-elimination since for example the formula $\exists x(a + n \centerdot x = b)$ is not equivalent with a quantifier-free formula (even in the language $\{+, -, \mathbf{0}, \mathbf{1}\}$), where $n \centerdot u = u + \cdots + u$ [n–times]. However, adding the congruence relations $\{\equiv_n\}_{n>1}$ (modulo standard natural numbers) to the language enables us to prove quantifier-elimination. By definition $a \equiv_n b$ holds when $a - b$ is divisible by (is a multiple of) n. For that we use the following version of the generalized Chinese remainder theorem (which is a form of quantifier-elimination).

Proposition 4.1. (Generalized Chinese Remainder [4])
For integers $m_0, m_1, \cdots, m_k \geqslant 2$ and $r_0, r_1, \cdots, r_k$ we have

$$\exists x \Big(\bigwedge_{0 \leqslant i \leqslant k} x \equiv_{m_i} r_i \Big) \quad \Longleftrightarrow \quad \bigwedge_{0 \leqslant i < j \leqslant k} r_i \equiv_{d_{i,j}} r_j$$

where $d_{i,j}$ is the greatest common divisor of m_i and m_j (for each $i < j$).

Proof:
The 'only if' ($\Longrightarrow$) direction is trivial; for the other direction let p be any prime which divides the product $m_0 \cdot m_1 \cdot \ldots \cdot m_k$, and let $\alpha(i)$ be the greatest number u such that p^u divides m_i. Fix an $\ell_p \in \{0, 1, \cdots, k\}$ (which depends on p) such that $\alpha(\ell_p)$ is the maximum of $\alpha(0), \alpha(1), \cdots, \alpha(k)$. The set of such prime p's is finite. By the (non-generalized) Chinese Remainder Theorem (see e.g. [12, Chapter I, Section 6]) there exists some integer x such that

$$\bigwedge_{p \in \mathbb{P}} x \equiv_{p^{\alpha(\ell_p)}} r_{\ell_p}.$$

We show that $x \equiv_{m_i} r_i$ holds for any i. Fix an i; it suffices to show that $x \equiv_{p^{\alpha(i)}} r_i$ holds for any prime p (in the above mentioned finite set). By the definition of ℓ_p we have $\alpha(\ell_p) \geqslant \alpha(i)$, so by the assumption $r_{\ell_p} \equiv_{d_{i,\ell_p}} r_i$ we have $r_{\ell_p} \equiv_{p^{\alpha(i)}} r_i$. Thus $x \equiv_{p^{\alpha(\ell_p)}} r_{\ell_p}$ implies $x \equiv_{p^{\alpha(i)}} r_i$. □

Corollary 4.2. (An Infinite Version of the Chinese Remainder Theorem)
For integers $m_0, m_1, \cdots, m_k \geqslant 2$, and $r_0, r_1, \cdots, r_k, n_0, n_1, \cdots, n_\ell$ we have

$$\exists x \big(\bigwedge_{0 \leqslant i \leqslant k} x \equiv_{m_i} r_i \ \wedge \bigwedge_{0 \leqslant \iota \leqslant \ell} x \neq n_\iota \big) \quad \Longleftrightarrow \quad \bigwedge_{0 \leqslant i < j \leqslant k} r_i \equiv_{d_{i,j}} r_j$$

where $d_{i,j}$ denotes the greatest common divisor of m_i and m_j.

Proof:
If the right-hand-side holds then by Proposition 4.1 there exists some x_0 such that $\bigwedge_{0 \leqslant i \leqslant k} x_0 \equiv_{m_i} r_i$. To make sure that x_0 could be taken to be different from all n_ι's, it suffices to note that for any arbitrarily large L the number $x = m_0 \cdot m_1 \cdot \ldots \cdot m_k \cdot L + x_0$ too satisfies $\bigwedge_{0 \leqslant i \leqslant k} x \equiv_{m_i} r_i$. □

Proposition 4.3. (Infinite Axiomatizablity of $\langle \mathbb{Z}; + \rangle$)
The following theory completely axiomatizes the additive theory of the integer numbers and, moreover, the structure $\langle \mathbb{Z}; +, -, \mathbf{0}, \mathbf{1}, \{\equiv_n\}_{n>1} \rangle$ admits quantifier elimination.

$(\mathtt{A}_1)$ $\forall x, y, z \big(x + (y + z) = (x + y) + z \big)$	$(\mathtt{A}_2)$ $\forall x \big(x + \mathbf{0} = x \big)$
$(\mathtt{A}_3)$ $\forall x \big(x + (-x) = \mathbf{0} \big)$	$(\mathtt{A}_4)$ $\forall x, y \big(x + y = y + x \big)$
$(\mathtt{A}_{5,n})$ $\forall x \big(n \centerdot x = \mathbf{0} \longrightarrow x = \mathbf{0} \big)$	$(\mathtt{A}_6^\circ)$ $\mathbf{1} \neq \mathbf{0}$
$(\mathtt{A}_{7,n}^\circ)$ $\forall x \exists! y \big(\bigvee_{i<n} x = n \centerdot y + \bar{i} \big)$	Where $\bar{i} = \mathbf{1} + \cdots + \mathbf{1}$ (for $i-$times)

and $n > 1$ is a natural number.

Proof:
Let us first note that $\mathtt{A}_{7,n}^\circ$ is equivalent with $\forall x \big(\underline{\bigvee}_{i<n} x \equiv_n \bar{i} \big)$, where $\underline{\vee}$ is the exclusive disjunction; whence $\underline{\bigvee}_i \psi_i \iff \bigvee_i \psi_i \ \wedge \ \bigwedge_{i \neq j} \neg(\psi_i \wedge \psi_j)$. So, the negation signs behind the congruences can be eliminated by the equivalences $(t \not\equiv_n u) \iff \bigvee_{0<i<n} (t \equiv_n u + \bar{i}\,)$. By the Main Lemma (1.1) it suffices to eliminate the quantifier of the formula

$$\exists x (\bigwedge_{\iota < \alpha} p_\iota \centerdot x \equiv_{q_\iota} r_\iota \ \wedge \ \bigwedge_{i<\ell} n_i \centerdot x = t_i \ \wedge \ \bigwedge_{j<k} m_j \centerdot x \neq s_j). \tag{8}$$

By $\mathtt{A}_5$ (and $\mathtt{A}_3$) we have $a = b \longleftrightarrow n \centerdot a = n \centerdot b$, and so $a \equiv_m b \longleftrightarrow n \centerdot a \equiv_{mn} n \centerdot b$; whence we can assume that all p_ι's, n_i's and m_j's in (8) are equal to each other. Thus we show the equivalence of

$$\exists x (\bigwedge_{\iota < \alpha} h \centerdot x \equiv_{q_\iota} r_\iota \ \wedge \ \bigwedge_{i<\ell} h \centerdot x = t_i \ \wedge \ \bigwedge_{j<k} h \centerdot x \neq s_j)$$

with a quantifier-free formula. But this is equivalent with the following formula (for $y = h \centerdot x$):

$$\exists y \big(y \equiv_h \mathbf{0} \ \wedge \ \bigwedge_{\iota < \alpha} y \equiv_{q_\iota} r_\iota \ \wedge \ \bigwedge_{i<\ell} y = t_i \ \wedge \ \bigwedge_{j<k} y \neq s_j \big). \tag{9}$$

Now, if $\ell > 0$ then (9) is equivalent with the quantifier-free formula

$$t_0 \equiv_h \mathbf{0} \ \wedge \ \bigwedge_{\iota < \alpha} t_0 \equiv_{q_\iota} r_\iota \ \wedge \ \bigwedge_{i<\ell} t_0 = t_i \ \wedge \ \bigwedge_{j<k} t_0 \neq s_j$$

and if $\ell = 0$ then (9) is of the form

$$\exists y\big(\bigwedge_{i<\ell} y \equiv_{m_i} r_i \ \wedge \bigwedge_{j<k} y \neq s_j\big)$$

which is equivalent with a quantifier-free formula by Corollary 4.2. □

Again this axiomatization of the additive theory of the integer numbers cannot be finite:

Proposition 4.4. (No Finite Axiomatization for $\langle\mathbb{Z};+\rangle$)
The theory of the structures $\langle\mathbb{Z};+\rangle$ is not finitely axiomatizable.

Proof:
Let $\mathfrak{p}$ be an arbitrarily large prime. Trivially, $\mathbb{Z}/\mathfrak{p}$ satisfies $\mathtt{A}_1, \mathtt{A}_2, \mathtt{A}_3, \mathtt{A}_4, \mathtt{A}_{5,n}$ and $\mathtt{A}_6^\circ$ (for each $n > 1$). However, $\mathbb{Z}/\mathfrak{p}$ does not satisfy $\mathtt{A}_{7,n}^\circ$ when $n = k\mathfrak{p}$ is a multiple of $\mathfrak{p}$: if there were some $y \in \mathbb{Z}/\mathfrak{p}$ and $i < k\mathfrak{p}$ such that $1/\mathfrak{p} = k\mathfrak{p} \centerdot y + i$ then $y = b/\mathfrak{p}$ for some $b \in \mathbb{Z}$, and so $1/\mathfrak{p} = kb + i \in \mathbb{Z}$; a contradiction! But, $\mathbb{Z}/\mathfrak{p}$ satisfies $\mathtt{A}_{7,n}^\circ$ when $n < \mathfrak{p}$: since n is relatively prime to $\mathfrak{p}$ then by Bézout's Lemma there are some a, b such that $an + b\mathfrak{p} = 1$. Fix an element $x = z/\mathfrak{p} \in \mathbb{Z}/\mathfrak{p}$ for some $z \in \mathbb{Z}$. By the Division Algorithm there are some q, i such that $bz = nq + i$ and $0 \leqslant i < n$. Now, for $y = (az+\mathfrak{p}q)/\mathfrak{p} \in \mathbb{Z}/\mathfrak{p}$ we have $n\centerdot y+i = (naz)/\mathfrak{p}+(n\mathfrak{p}q)/\mathfrak{p}+i = z(an/\mathfrak{p})+bz = z(an+b\mathfrak{p})/\mathfrak{p} = x$. It can be seen that this y (and also i) is unique for x. Since if $x = n\centerdot y' + j$ for some $y' = \beta/\mathfrak{p}$ ($\beta \in \mathbb{Z}$) and $0 \leqslant j < n$ then for $\alpha = az + \mathfrak{p}q$ we have $\mathfrak{p}(j - i) = n(\alpha - \beta)$ and so by $(n, \mathfrak{p}) = 1$ the number n should divide $j - i$; thus $j = i$ (because of $0 \leqslant i, j < n$) whence $\alpha = \beta$ which implies that $y' = y$. So, no finite number of the instances of $\mathtt{A}_{7,n}^\circ$ (together with $\mathtt{A}_1, \mathtt{A}_2, \mathtt{A}_3, \mathtt{A}_4, \mathtt{A}_{5,n}$ and $\mathtt{A}_6^\circ$) can imply all the instances of $\mathtt{A}_{7,n}^\circ$. □

4.2. The multiplicative theory of the positive rational numbers

We need a version of the Generalized Chinese Remainder Theorem which has more information than Proposition 4.1 and Corollary 4.2.

Proposition 4.5. (General Chinese Remainder [8])
The system $\{x \equiv_{m_i} r_i\}_{i<\ell}$ of congruence equations has a solution in $\mathbb{Z}$ if and only if for every $i \neq j$, $r_i \equiv_{d_{i,j}} r_j$ where $d_{i,j}$ is the greatest common divisor of m_i and m_j. Moreover, if m is the least common multiple of m_i's then the solution x_0 (if exists) is a linear combination of $r_i(m/m_i)$'s and is unique modulo m; so all the solutions will be of the form $L\cdot m + x_0$ for some (arbitrary) $L \in \mathbb{Z}$.

Proof:
Suppose $\bigwedge_{i\neq j} r_i \equiv_{d_{i,j}} r_j$; we will show the existence of an integer x_0 which satisfies $\bigwedge_{i<\ell} x_0 \equiv_{m_i} r_i$. Then of course every number $x = L \cdot m + x_0$ satisfies the system of equations $\bigwedge_{i<\ell} x \equiv_{m_i} r_i$ as well, and every solution y of the equations $\bigwedge_{i<\ell} y \equiv_{m_i} r_i$ satisfies $\bigwedge_{i<\ell} x_0 \equiv_{m_i} y$, and so $x_0 \equiv_m y$, therefore $y = L \cdot m + x_0$ for some $L \in \mathbb{N}$. Since the greatest common divisor of the numbers $\{m/m_i\}_{i<\ell}$ is 1, by generalized Bézout's identity, there are $\{c_i\}_{i<\ell}$ such that the identity $\sum_{i<\ell} c_i \cdot (m/m_i) = 1$ holds. Let $e_{i,j}$ denote the least common multiplier of m_i and m_j. For any

$i \neq j$ the number $d_{i,j}$ divides $r_i - r_j$ and the number $e_{i,j}$ divides m; so there are $p_{i,j}$ and $q_{i,j}$ such that $r_i - r_j = p_{i,j} \cdot d_{i,j}$ and $m = q_{i,j} \cdot e_{i,j}$. By $d_{i,j} \cdot e_{i,j} = m_i \cdot m_j$ we have $(r_i - r_j)m/m_i = p_{i,j} \cdot d_{i,j} \cdot q_{i,j} \cdot e_{i,j}/m_i = p_{i,j} \cdot q_{i,j} \cdot m_j$. Put $x_0 = \sum_{i<\ell} r_i \cdot c_i \cdot (m/m_i)$. Then

$$\begin{aligned} x_0 &= r_j c_j m/m_j + \textstyle\sum_{i\neq j} r_i \cdot c_i \cdot (m/m_i) \\ &= r_j c_j m/m_j + \textstyle\sum_{i\neq j} (r_i - r_j) \cdot c_i \cdot (m/m_i) + \sum_{i\neq j} r_j \cdot c_i \cdot (m/m_i) \\ &= r_j \cdot \textstyle\sum_i c_i \cdot (m/m_i) + \sum_{i\neq j} (r_i - r_j) \cdot c_i \cdot (m/m_i) \\ &= r_j + \textstyle\sum_{i\neq j} c_i \cdot (r_i - r_j) \cdot (m/m_i) \\ &= r_j + \textstyle\sum_{i\neq j} c_i \cdot p_{i,j} \cdot q_{i,j} \cdot m_j \\ &= r_j + m_j \cdot \textstyle\sum_{i\neq j} c_i \cdot p_{i,j} \cdot q_{i,j}, \end{aligned}$$

which implies the desired conclusion $x_0 \equiv_{m_j} r_j$ (for every $j < \ell$). □

The language $\{\times\}$ does not allow quantifier elimination for $\langle \mathbb{Q}^+; \times \rangle$, since e.g. the formula $\exists x(y = x^2)$ is not equivalent with a quantifier–free formula. So, we introduce the following:

Definition 4.6. (The Property of Having the $\mathbf{n^{th}}$ Root)
For any $n \geqslant 2$ let $\Re_n$ be the property of "being the n^{th} power of a rational number". In the other words $\Re_n(x) \equiv \exists y[\in \mathbb{Q}](x = y^n)$. ⊛

Lemma 4.7. (The First Quantifier Elimination for $\Re$)
The system of relations $\{\Re_{n_i}(u_i \cdot x)\}_{i<\ell}$ has a solution in $\mathbb{Q}^+$ if and only if $\Re_{d_{i,j}}(u_i \cdot u_j^{-1})$ holds for every $i \neq j$, where $d_{i,j}$ is the greatest common divisor of n_i and n_j. Moreover, if $\bigwedge_{i\neq j} \Re_{d_{i,j}}(u_i \cdot u_j^{-1})$ holds then for n the least common multiplier of $\{n_i\}_{i<\ell}$ and for some fixed $\{c_i\}_{i<\ell} \subseteq \mathbb{Z}$ which satisfy the equality $\sum_{i<\ell} c_i(n/n_i) = 1$, all of the solutions are of the form $w^n \prod_{i<\ell}(u_i)^{-c_i \cdot n/n_i}$ for some (arbitrary) $w \in \mathbb{Q}^+$.

Proof:
Clearly, if $\Re_{n_i}(u_i x)$ and $\Re_{n_j}(u_j x)$ hold then $\Re_{d_{i,j}}(u_i x)$ and $\Re_{d_{i,j}}(u_j^{-1} x^{-1})$, and so $\Re_{d_{i,j}}(u_i u_j^{-1})$ holds. Conversely, suppose that $\bigwedge_{i\neq j} \Re_{d_{i,j}}(u_i u_j^{-1})$ holds. Since the greatest common divisor of n/n_i's is 1 there are some $\{c_i\}_{i<\ell}$ such that $\sum_{i<\ell} c_i(n/n_i) = 1$. We show that $x_0 = \prod_{i<\ell}(u_i)^{-c_i n/n_i}$ satisfies $\bigwedge_{i<\ell} \Re_{n_i}(u_i x_0)$. For a fix prime p, assume the exponents of p in the unique factorizations of $\{u_i\}_{i<\ell}$ are respectively $\{\alpha_i\}_{i<\ell}$. Then the exponent of p in the unique factorization of x_0 will be $\alpha = \sum_{i<\ell} -c_i \alpha_i (n/n_i)$. Also, by the assumption $\bigwedge_{i\neq j} \Re_{d_{i,j}}(u_i u_j^{-1})$ we have $\bigwedge_{i\neq j} \alpha_i \equiv_{d_{i,j}} \alpha_j$. So, by the proof of the General Chinese Remainder Theorem (Proposition 4.5), $\bigwedge_i \alpha \equiv_{n_i} -\alpha_i$. This means that the exponent of (every prime) in the unique factorization of $u_i x_0$ is a multiple of n_i, whence $\Re_{n_i}(u_i x_0)$ holds (for each $i < \ell$). Now assume for $y \in \mathbb{Q}^+$ the relation $\bigwedge_i \Re_{n_i}(u_i y)$ holds. Then for any prime p, if the exponent of p in the unique factorization of y is β, we have $\bigwedge_i \beta \equiv_{n_i} -\alpha_i$. Whence, by the proof of Proposition 4.5 we have $\beta \equiv_n \alpha$, and so $y = w^n x_0$ for some $w \in \mathbb{Q}^+$. □

Let us note that Lemma 4.7 is a kind of quantifier elimination:

$$\exists x \big[\bigwedge_i \Re_{n_i}(x u_i) \big] \iff \bigwedge_{i\neq j} \Re_{d_{i,j}}(u_i u_j^{-1});$$

so is the next lemma in which we show that

$$\exists x\big[\bigwedge_{j}\Re_{n_j}(xu_j)\wedge\bigwedge_{k}\neg\Re_{m_k}(xv_k)\big]\iff\bigwedge_{i\neq j}\Re_{d_{i,j}}(u_iu_j^{-1})\wedge\bigwedge_{k:\,m_k|n}\neg\Re_{m_k}(av_k),$$

where $d_{i,j}$ is the greatest common divisor of n_i and n_j, n is the least common multiplier of $\{n_i\}$'s and $a=\prod_{i<\ell}(u_i)^{-c_in/n_i}$ in which $\sum_{i<\ell}c_in/n_i=1$.

Lemma 4.8. (The Second Quantifier Elimination for $\Re$)
The system of relations $\{\Re_{n_j}(xu_j)\}_{j<\ell},\{\neg\Re_{m_k}(xv_k)\}_{k<l}$ has a solution (for x) in $\mathbb{Q}^+$ if and only if for any $i\neq j$ we have $\Re_{d_{i,j}}(u_iu_j^{-1})$ and for any k such that m_k divides n we have $\neg\Re_{m_k}(av_k)$ where $d_{i,j}$ is the greatest common divisor of n_i and n_j, n is the least common multiplier of all the $\{n_i\}$'s, $a=\prod_{i<\ell}(u_i)^{-c_in/n_i}$ and $\sum_{i<\ell}c_in/n_i=1$.

Proof:
Suppose that $x\in\mathbb{Q}^+$ satisfies the system $\{\Re_{n_j}(xu_j)\}_{j<\ell},\{\neg\Re_{m_k}(xv_k)\}_{k<l}$. Then by Lemma 4.7, $\bigwedge_{i\neq j}\Re_{d_{i,j}}(u_iu_j^{-1})$ holds, and moreover x is of the form w^na for some $w\in\mathbb{Q}^+$. We show that $\bigwedge_{k:\,m_k|n}\neg\Re_{m_k}(av_k)$ holds too. Suppose $m_k\mid n$. Then $v_kx=v_kw^na$, and so by $\Re_{m_k}(w^n)$ and $\neg\Re_{m_k}(v_kx)$ we have that $\neg\Re_{m_k}(av_k)$. Conversely, suppose that

$$\bigwedge_{i\neq j}\Re_{d_{i,j}}(u_iu_j^{-1})\wedge\bigwedge_{k:\,m_k|n}\neg\Re_{m_k}(av_k).$$

Then by Lemma 4.7 for any $w\in\mathbb{Q}^+$ the number $x=aw^n$ satisfies $\bigwedge_{j<\ell}\Re_{n_j}(xu_j)$. We choose a suitable w for which $x=aw^n$ also satisfies $\bigwedge_{k<l}\neg\Re_{m_k}(xv_k)$. Choose $\mathfrak{p}$ be a (sufficiently large) prime number which does not appear in the (unique) factorization of any of $\{u_j\}_{j<\ell}$ or $\{v_k\}_{k<l}$. Now we show that $x=a\mathfrak{p}^n$ satisfies $\bigwedge_{k<l}\neg\Re_{m_k}(xv_k)$:

(i) If m_k divides n then $\neg\Re_{m_k}(av_k)$ and $\Re_{m_k}(\mathfrak{p}^n)$; whence $\neg\Re_{m_k}(xv_k)$.

(ii) If m_k does not divide n, then $\neg\Re_{m_k}(\mathfrak{p}^n)$ and so $\neg\Re_{m_k}(xv_k)$, because the prime number $\mathfrak{p}$ does not appear in the unique factorization of a or v_k (if we had $\Re_{m_k}(xv_k)\equiv\Re_{m_k}(a\mathfrak{p}^nv_k)$ then we must have had $\Re_{m_k}(\mathfrak{p}^n)$ or $m_k\mid n$, a contradiction). □

Corollary 4.9. (The Third Quantifier Elimination for $\Re$)
For any finite sequences $\{t_\iota\}_\iota,\{u_j\}_j,\{v_k\}_k\subseteq\mathbb{Q}^+$ we have

$$\exists x\in\mathbb{Q}^+\big[\bigwedge_{\iota}x\neq t_\iota\wedge\bigwedge_{j}\Re_{n_j}(xu_j)\wedge\bigwedge_{k}\neg\Re_{m_k}(xv_k)\big]\iff\bigwedge_{i\neq j}\Re_{d_{i,j}}(u_iu_j^{-1})\wedge\bigwedge_{k:\,m_k|n}\neg\Re_{m_k}(av_k),$$

where $d_{i,j}$ is the greatest common divisor of n_i and n_j, n is the least common multiplier of $\{n_i\}$'s and $a=\prod_i(u_i)^{-c_in/n_i}$ in which $\sum_ic_in/n_i=1$.

Proof:
It suffices to note that in the proof of Lemma 4.8 there are infinitely many prime numbers which do not appear in the factorization of any of $\{u_j\}_j$ or $\{v_k\}_k$. □

Now, we have all the necessary tools for proving our desired quantifier elimination theorem.

Theorem 4.10. (The Quantifier Elimination of $\langle \mathbb{Q}^+; \times, \mathbf{1}, \circ^{-1}, \{\Re_n\}_{n\geqslant 2}\rangle$)
The theory of the structure $\langle \mathbb{Q}^+; \times, \mathbf{1}, \circ^{-1}, \Re_2, \Re_3, \cdots \rangle$ admits quantifier elimination.

Proof:
By Lemma 1.1 it suffices to eliminate the quantifier of the formula

$$\exists x \big[\bigwedge_h x^{\alpha_h} = s_h \wedge \bigwedge_i x^{\beta_i} \neq t_i \wedge \bigwedge_j \Re_{n_j}(u_j \cdot x^{\gamma_j}) \wedge \bigwedge_k \neg \Re_{m_k}(v_k \cdot x^{\delta_k}) \big].$$

By the equivalences $a = b \leftrightarrow a^\eta = b^\eta$ and $\Re_\ell(a) \leftrightarrow \Re_{\ell\eta}(a^\eta)$ we can assume that all the exponents α_h's, β_i's, γ_j's and δ_k's are equal, to say q. So, we are to eliminate the quantifier of

$$\exists x \big[\bigwedge_h x^q = s_h \wedge \bigwedge_i x^q \neq t_i \wedge \bigwedge_j \Re_{n_j}(u_j \cdot x^q) \wedge \bigwedge_k \neg \Re_{m_k}(v_k \cdot x^q) \big]$$

which is equivalent (for $y = x^q$) with the formula

$$\exists y \big[\Re_q(y) \wedge \bigwedge_h y = s_h \wedge \bigwedge_i y \neq t_i \wedge \bigwedge_j \Re_{n_j}(u_j y) \wedge \bigwedge_k \neg \Re_{m_k}(v_k y) \big].$$

Thus, it suffices to prove the equivalence of the formulas of the form

$$\exists x \big[\bigwedge_h x = s_h \wedge \bigwedge_i x \neq t_i \wedge \bigwedge_j \Re_{n_j}(u_j x) \wedge \bigwedge_k \neg \Re_{m_k}(v_k x) \big] \tag{10}$$

with a quantifier-free formula. If the conjunction $\bigwedge_h x = s_h$ is nonempty then the formula (10) is equivalent with the quantifier-free formula

$$\bigwedge_h s_0 = s_h \wedge \bigwedge_i s_0 \neq t_i \wedge \bigwedge_j \Re_{n_j}(u_j s_0) \wedge \bigwedge_k \neg \Re_{m_k}(v_k s_0)$$

and otherwise the formula (10) is actually

$$\exists x \big[\bigwedge_i x \neq t_i \wedge \bigwedge_j \Re_{n_j}(u_j x) \wedge \bigwedge_k \neg \Re_{m_k}(v_k x) \big]$$

which is equivalent with a quantifier-free formula by Corollary 4.9. □

By a close inspection of the proof of Theorem 4.10 (and its prerequisites Proposition 4.5, Lemmas 4.7,4.8 and Corollary 4.9) we can give an explicit complete axiomatization for the multiplicative theory of the positive rational numbers.

Theorem 4.11. (Infinite Axiomatizability of $\langle \mathbb{Q}^+; \times \rangle$)
The following theory completely axiomatizes the structure $\langle \mathbb{Q}^+; \times, \mathbf{1}, \circ^{-1} \rangle$.

$(\mathtt{M}_1)$ $\forall x, y, z \left(x \cdot (y \cdot z) = (x \cdot y) \cdot z\right)$	$(\mathtt{M}_2)$ $\forall x \left(x \cdot \mathbf{1} = x\right)$
$(\mathtt{M}_3^\circ)$ $\forall x \left(x \cdot x^{-1} = \mathbf{1}\right)$	$(\mathtt{M}_4)$ $\forall x, y \left(x \cdot y = y \cdot x\right)$
$(\mathtt{M}_{7,n}^\circ)$ $\forall x \left(x^n = \mathbf{1} \longrightarrow x = \mathbf{1}\right)$	$(\mathtt{M}_{16,n})$ $\forall v_1, \ldots, v_\ell \exists x \forall z \bigwedge_{k=1}^{\ell} \left(x^n \cdot v_k \neq z^{m_k}\right)$
Where $n \geqslant 1$ is a natural number, and	none of m_k's divide n (i.e., $m_1 \nmid n, \cdots, m_\ell \nmid n$).

Proof:
Firstly, we note that the axiom $\mathtt{M}_{16,n}$ is equivalent with $\forall v_1,\dots,v_\ell \exists x \bigwedge_{k=1}^{\ell} \neg\Re_{m_k}(x^n v_k)$, when no m_k divides n (for $k=1,\cdots,\ell$). Secondly, this axiom implies the existence of infinitely many such x's. Since for fixed $v_1,\cdots,v_\ell$ there is some x such that $\bigwedge_{k=1}^{\ell} \neg\Re_{m_k}(x^n v_k)$. Now, fix a prime $\mathfrak{p} > n$. Then for $v_1,\cdots,v_\ell, x^{\mathfrak{p}-n}$ and the sequence $m_1,\cdots,m_k,\mathfrak{p}$ (none of which divides n) by this axiom there exists some y such that $\bigwedge_{k=1}^{\ell} \neg\Re_{m_k}(y^n v_k) \wedge \neg\Re_{\mathfrak{p}}(y^n x^{\mathfrak{p}-n})$. Then $y = x$ implies $\neg\Re_{\mathfrak{p}}(x^n x^{\mathfrak{p}-n})$ or $\neg\Re_{\mathfrak{p}}(x^{\mathfrak{p}})$ a contradiction; so $y \neq x$. Continuing this way, by induction, if there are $x_1,\cdots,x_m$ such that $\bigwedge_{i\neq j} x_i \neq x_j$ and $\bigwedge_{i=1}^{m}\bigwedge_{k=1}^{\ell} \neg\Re_{m_k}(x_i^n v_k)$ then by this axiom for the sequence $v_1,\cdots,v_\ell, x_1^{\mathfrak{p}-n},\cdots,x_m^{\mathfrak{p}-n}$ and the numbers $m_1,\cdots,m_\ell,\mathfrak{p},\cdots,\mathfrak{p}$ (none of which divides n) there exists some y such that $\bigwedge_{k=1}^{\ell} \neg\Re_{m_k}(y^n v_k) \wedge \bigwedge_{i=1}^{m} \neg\Re_{\mathfrak{p}}(y^n x_i^{\mathfrak{p}-n})$. Again it can be seen that y cannot be equal to any of x_i's (for $i=1,\cdots,m$) and so could be taken as x_{m+1}. Thus, the axiom $\mathtt{M}_{16,n}$ implies that for any sequence $\{v_k\}_{k=1}^{\ell}$ of positive rationals and any sequence $\{m_k\}_{k=1}^{\ell}$ of integers none of which divides n there are infinitely many positive rationals x such that for all $k=1,\cdots,\ell$, $x^n v_k$ is not an m_k's power of any rational number. To see that $\mathtt{M}_{16,n}$ is true (in the set of positive rationals) take x to be a prime number that does not appear in the (unique) factorizations of any of v_k's (for $k=1,\cdots,\ell$); cf. the proof of Lemma 4.8. So, the axiomatization is sound. To see that it is also complete, we observe that the proofs of Theorem 4.10, Lemmas 4.7,4.8 and Corollary 4.9 can go through by using these axioms only, noting that in the proof of Corollary 4.9 and Lemma 4.8 we need the existence of infinitely many x's such that $\neg\Re_{m_k}(x^n \cdot a v_k)$ holds when m_k does not divide n (when m_k divides n then any x satisfies $\neg\Re_{m_k}(x^n \cdot a v_k)$ by the assumption $\neg\Re_{m_k}(a v_k)$), and this is exactly what the axiom $\mathtt{M}_{16,n}$ provides us. □

Theorem 4.12. (No Finite Axiomatization for $\langle\mathbb{Q}^+;\times\rangle$)
The theory of the structures $\langle\mathbb{Q}^+;\times\rangle$ is not finitely axiomatizable.

Proof:
For any finite number we provide a model for the axioms $\mathtt{M}_1,\mathtt{M}_2,\mathtt{M}_3^{\circ},\mathtt{M}_4,\mathtt{M}_{16,n}$ and that finite number of the instances of $\mathtt{M}_{7,n}^{\circ}$ in which some other instances of $\mathtt{M}_{7,n}^{\circ}$ fails. Let $\mathfrak{p}$ be a sufficiently large prime, and consider $\{r\cdot\boldsymbol{\omega}_{\mathfrak{p}}^k \mid k\in\mathbb{N}, r\in\mathbb{Q}^+\}$ (together with the multiplication operation). This is a multiplicative subset of the complex numbers whose every member has a unique factorization as $\boldsymbol{\omega}_{\mathfrak{p}}^k\prod_i \mathfrak{p}_i^{n_i}$ for $0\leqslant k<\mathfrak{p}$ and $n_i\in\mathbb{Z}$. It is straightforward to see that this structure satisfies $\mathtt{M}_1,\mathtt{M}_2,\mathtt{M}_3^{\circ},\mathtt{M}_4$ and the instances of $\mathtt{M}_{7,n}^{\circ}$ for $n<\mathfrak{p}$ but not $\forall x\left(x^{\mathfrak{p}}=\mathbf{1}\longrightarrow x=\mathbf{1}\right)$ since $(\boldsymbol{\omega}_{\mathfrak{p}})^{\mathfrak{p}}=1$ but $\boldsymbol{\omega}_{\mathfrak{p}}\neq 1$. It also satisfies $\mathtt{M}_{16,n}$ since for any given $v_1,\cdots,v_\ell$ it suffices to take x to be a (sufficiently large) prime that does not appear in the unique factorizations of v_k's. □

5. Conclusions

The theory of the multiplication of the non-negative rational numbers $\langle\mathbb{Q}^{\geqslant 0};\times\rangle$ could also be completely axiomatized by adding the axiom $\forall x\left(x\cdot\mathbf{0}=\mathbf{0}=\mathbf{0}^{-1}\right)$ to the axioms of $\langle\mathbb{Q}^+;\times\rangle$ (and relativizing the axioms $\mathtt{M}_3^{\circ}$ and $\mathtt{M}_{16}$ to non-zero elements) just like Proposition 3.2 (with a proof in lines of that of Theorem 3.3). Also by adding the positivity property ($\mathcal{P}(x)\equiv x>0$) to the language we could completely axiomatize the multiplicative theory of the rational numbers $\langle\mathbb{Q};\times\rangle$ (just like

Theorem 3.3). Indeed, the theory of the structures $\langle \mathbb{Q}; \times, \circ^{-1}, \mathbf{0}, \mathbf{1}, -\mathbf{1}, \mathcal{P} \rangle$ admits quantifier elimination but unfortunately $\mathcal{P}$ is not definable in $\langle \mathbb{Q}; \times, \circ^{-1}, \mathbf{0}, \mathbf{1}, -\mathbf{1} \rangle$. To see this, consider the function from $\mathbb{Q}$ into itself that maps $-1, 0, 1$ to themselves, and maps each rational number r whose unique factorization is $(-1)^\iota \prod_{j\in\mathbb{N}} \mathfrak{p}_j^{n_j}$ (where cofinitely many of the integers n_j's are zero) to $(-1)^{n_0} r$. This function is bijective and preserves the multiplication operation but does not preserve the positivity property, since $\frac{2}{3}$ which is positive is mapped to $-\frac{2}{3}$ which is not positive. We leave open the problem of finding a $\langle \mathbb{Q}; \times \rangle-$definable language $\mathcal{L}$ such that $\langle \mathbb{Q}; \mathcal{L} \rangle$ admits quantifier elimination. Overall, the theory of the structure $\langle \mathbb{Q}; \times \rangle$ is decidable while the theory of the structure $\langle \mathbb{Q}; +, \times \rangle$ is not (proved by Robinson [9]); let us note that the decidability of the theories of $\langle \mathbb{R}; \times \rangle$ and $\langle \mathbb{C}; \times \rangle$ were inherited from the decidability of the theories of $\langle \mathbb{R}; +, \times \rangle$ and $\langle \mathbb{C}; +, \times \rangle$ by Tarski's results. Interestingly, the axioms of $\langle \mathbb{R}; \times \rangle$ in Theorem 3.3 are the laws of signs (positivity and negativity) and multiplication in the high school, and the axioms of $\langle \mathbb{C}; \times \rangle$ in Theorem 2.2 are the laws learned in the freshmen calculus lessons. As for the integers, a complete axiomatization, by the method of quantifier elimination, was given for $\langle \mathbb{N}^+; \times \rangle$ in [1] (see also [12]). This result can be extended to the theory of the structure $\langle \mathbb{N}; \times \rangle$ (cf. [6, Exercise 23.17]). Also, the theory of the structure $\langle \mathbb{Z}; \times \rangle$ can be proved to be decidable by the methods of [1] by providing an explicit (and complete and decidable) axiomatization with the method of quantifier elimination (in a suitable $\{\times\}$-definable language).

All of the new and old results of the paper are summarized in the following table, in which (only) the structures $\langle \mathbb{N}; +, \times \rangle$, $\langle \mathbb{Z}; +, \times \rangle$ and $\langle \mathbb{Q}; +, \times \rangle$ are undecidable (while the rest of the structures, $\langle \mathbb{N}; + \rangle$, $\langle \mathbb{Z}; + \rangle$, $\langle \mathbb{Q}; + \rangle$, $\langle \mathbb{R}; + \rangle$, $\langle \mathbb{C}; + \rangle$, $\langle \mathbb{N}; \times \rangle$, $\langle \mathbb{Z}; \times \rangle$, $\langle \mathbb{Q}; \times \rangle$, $\langle \mathbb{R}; \times \rangle$, $\langle \mathbb{C}; \times \rangle$, $\langle \mathbb{R}; +, \times \rangle$ and $\langle \mathbb{C}; +, \times \rangle$, are decidable and thus axiomatizable by recursively enumerable sets of sentences).

	$\mathbb{N}$	$\mathbb{Z}$	$\mathbb{Q}$	$\mathbb{R}$	$\mathbb{C}$
$\{+\}$	[2, Th. 32E]	Prop. 4.3	Prop. 2.5	Prop. 2.5	Prop. 2.5
$\{\times\}$	[1]	[1] (& § 5)	Th. 4.10 (& § 5)	Th. 3.3	Th. 2.2
$\{+, \times\}$	[2, Cor. 35A]	[6, Th. 16.7]	[9]	[6, Th. 21.36]	[6, Th. 21.9]

References

[1] Cégielski P. "*Théorie Élémentaire de la Multiplication des Entiers Naturels*", in: C. Berline, K. McAloon, J.-P. Ressayre (eds.) **Model Theory and Arithmetic**, Comptes Rendus d'une Action Thématique Programmée du C.N.R.S. sur la Théorie des Modèles et l'Arithmétique, Paris, France, 1979/80, Lecture Notes in Mathematics 890, Springer 1981 pp. 44–89. ISBN: 9783540111597, doi:10.1007/BFb0095657.

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

[3] Kreisel G, and Krivine JL. *Elements of Mathematical Logic: Model Theory*, North–Holland 1971. ISBN: 9780720422658.

[4] Mahler K. *On the Chinese Remainder Theorem*, Mathematische Nachrichten 1958;18:120-122. doi:10.1002/mana.19580180112.

[5] Marker D. *Model Theory: An Introduction*, Springer 2002. ISBN: 9781441931573.

[6] Monk JD. *Mathematical Logic*, Springer 1976. ISBN: 9780387901701.

[7] Mostowski A. *On Direct Products of Theories*, The Journal of Symbolic Logic 1952;17(1):1–31. doi: 10.2307/2267454.

[8] Ore O. *The General Chinese Remainder Theorem*, The American Mathematical Monthly 1951;59(6):365–370. doi:10.2307/2306804.

[9] Robinson J. *Definability and Decision Problems in Arithmetic*, The Journal of Symbolic Logic 1949; 14(2):98–114. doi:10.2307/2266510.

[10] Robinson A, and Zakon E. *Elementary Properties of Ordered Abelian Groups*, Transactions of the American Mathematical Society 1960;96:222–236. doi:10.2307/1993461.

[11] Salehi S. "*Axiomatizing Mathematical Theories: Multiplication*", in: A. Kamali-Nejad (ed.) Proceedings of Frontiers in Mathematical Sciences, Sharif University of Technology. Tehran, Iran 2012, pp. 165–176. URL `https://arxiv.org/pdf/1612.06525.pdf`.

[12] Smoryński C. *Logical Number Theory I: An Introduction*. Springer 1991. ISBN: 9783540522362.

[13] Szmielew W. "*Decision Problem in Group Theory*", in: E.W. Beth, H.J. Pos, J.H.A. Hollak (eds.) Proceedings of the Tenth International Congress of Philosophy, Vol. 2. North-Holland, Amsterdam 1949 pp. 763–766. doi:10.5840/wcp1019492212.

[14] Szmielew W. *Elementary Properties of Abelian Groups*, Fundamenta Mathematicæ 1955;41:203–271. doi:10.4064/fm-41-2-203-271.