mathematics

MDPI

Article

On Undecidability of Finite Subsets Theory for Torsion Abelian Groups

Sergey Mikhailovich Dudakov †

Department of Applied Mathematics and Cybernetic, Tver State University, 170100 Tver, Tver Oblast, Russia; sergeydudakov@yandex.ru
† Current address: Zhelyabova, 33, 170100 Tver, Tver Oblast, Russia.

Abstract: Let M be a commutative cancellative monoid with an element of infinite order. The binary operation can be extended to all finite subsets of M by the pointwise definition. So, we can consider the theory of finite subsets of M. Earlier, we have proved the following result: in the theory of finite subsets of M elementary arithmetic can be interpreted. In particular, this theory is undecidable. For example, the free monoid (the sets of all words with concatenation) has this property, the corresponding algebra of finite subsets is the theory of all finite languages with concatenation. Another example is an arbitrary Abelian group that is not a torsion group. But the method of proof significantly used an element of infinite order, hence, it can't be immediately generalized to torsion groups. In this paper we prove the given theorem for Abelian torsion groups that have elements of unbounded order: for such group, the theory of finite subsets allows interpreting the elementary arithmetic.

Keywords: Abelian torsion group; finite subsets theory; undecidability; elementary arithmetic

Citation: Dudakov, S.M. On Undecidability of Finite Subsets Theory for Torsion Abelian Groups. *Mathematics* **2022**, *10*, 533. https://doi.org/10.3390/math10030533

Academic Editors: Alexei Kanel-Belov and Alexei Semenov

Received: 13 December 2021
Accepted: 6 February 2022
Published: 8 February 2022

1. Introduction

Among the central subjects of mathematical logic, there are formal theories investigations. There are theoretical and practical reasons for this interest. For example, such investigations have a value for database query languages. These ideas were proposed by E. F. Codd in [1]. In his papers E. F. Codd introduced the concept of relational databases and query languages. The relational model of a database is a relational finite structure. E. F. Codd proposed to use relational algebra as a query language. Relational algebra is equivalent to the language of first-order logic. To encode database items, various mathematical objects (numbers, words, and so on) are used. Usually, some "natural" operations (or relations) on such objects can be performed. For example, we can perform arithmetical or bitwise operations on natural numbers, concatenation on words, various comparisons, and so on. So, we have a complex structure: a finite relational structure (a database itself) that is embedded into an infinite universe (see [2]). Therefore, a database management system must operate with some logic language on a given universe. But, this possibility can imply the undecidability of many tasks because corresponding problems are undecidable for universes (see, for example [3]). Usually, in such cases, the elementary arithmetic is interpretable as in [4].

Another feature of modern systems is the construction of aggregate types. For example, arrays, maps, or sets (of numbers, words, Boolean values, etc.) can be declared as new data types and can be used in databases. These constructions are finite due to "natural" restrictions of storage capacity. So, we have a structure, which can contain not only atomic objects but aggregates, for example, finite sets of such objects.

The same problem appears in the formal automata theory in the determinization process (see [5]). A finite non-deterministic automaton can be presented by some semigroup (see [6]). So, the deterministic automata corresponds to the semigroup of subsets.

Our investigations began in [7] where algebras of languages are considered. In our papers [8,9] we consider new algebras $\exp \mathfrak{A}$ those are constructed as finite subsets of some source algebra $\mathfrak{A}$. Source algebra operations can be naturally extended to finite subsets, so this is a universal method to construct new structures.

Subsets of algebras, in particular, Abelian groups and commutative semigroups, are actively investigated in algebra and in number theory (for example, see [10] or [11]). Many classic problems can be formulated in the language of subset algebra. For example, the binary Goldbach's conjecture is the claim that $P + P = E$ where P is the set of primes and E is the set of even naturals. Also, the subset sum problem is a classic NP-complete problem (see [12]).

Let us note that this construction of the finite subsets' algebra is not equivalent to the weak monadic second-order logic for the original algebra. The language of the second-order logic allows using first-order variables (see [13]). Hence, the second-order language always includes the first-order language. But in the first-order theory of the finite subset algebra, there is no explicit way to denote first-order objects. This lack is significant because there exist examples, where the first-order theory of the finite subset algebra is algorithmically simpler than the theory of the original algebra. For the weak monadic second-order logic, it is impossible.

The algorithmic properties of finite subsets algebras and their theories are very different. This new theory can be decidable even in the case when the theory of the original algebra is undecidable. And vice versa, for an original structure with decidable theory, the new theory can allow interpreting the elementary arithmetic (see [8]).

The problem for unoids was solved in [14]. In that paper, an infinite set of parameters was found for unoids, and these parameters describe the subsets theory completely.

The typical example of this concept is the formal language theory [5,15]. Words form the free monoid (with concatenation), and every language is a set of words. So, the concatenation of entire languages can be considered as an extension of the word concatenation onto sets of words.

Our previous result, which is proved in [8], is the following. Let $\mathfrak{A}$ be a commutative cancellative monoid with an element of infinite order, then the theory of finite subsets of $\mathfrak{A}$ allows to interpret elementary arithmetic, hence, this theory is undecidable. Examples of such monoids are well-known: numbers with addition or multiplication, polynomials and spaces over a field of characteristic zero, and so on. In particular, every Abelian group that is not a torsion group is such a monoid. So, the natural question appears: does this result hold for the Abelian torsion group?

In this article, we consider Abelian torsion groups with elements of unbounded order. By compactness, every such group is elementary equivalent to some Abelian group with an element of infinite order. But the compactness concept is not applicable here because elementary equivalent source algebras can generate finite subsets algebras that are not elementary equivalent. A corresponding example is given below. Thus, we need to consider Abelian torsion groups themselves.

Example 1. *Let $\mathfrak{C}_i$ be the cyclic additive group of order i. We can suppose that the different groups $\mathfrak{C}_i$ have no common element. Then, the monoid $\mathfrak{A}$ is a union of all $\mathfrak{C}_i$. An operation $+$ in $\mathfrak{A}$ is defined the next way: $x + y = x +_i y$ when $x, y \in \mathfrak{C}_i$, $x + y = 0_1$ otherwise. Here $+_i$ is the operation in $\mathfrak{C}_i$, 0_1 is the neutral element of $\mathfrak{C}_1$.*

Thus, $\exp \mathfrak{A}$ has the following property: for each finite set $X \neq \{0_1\}$ there is $Y \neq \{0_1\}$, $Y \neq \emptyset$ such that $X + Y = Y$. This Y is the union of $\mathfrak{C}_1$ and all $\mathfrak{C}_i$ those intersect with X.

By compactness, there is an elementary equivalent monoid $\mathfrak{A}' \equiv \mathfrak{A}$ that includes the infinite cyclic group $\mathfrak{Z}$. But the given property doesn't hold in $\exp \mathfrak{A}'$ if X has elements from $\mathfrak{Z}$.

In [9] we have shown how to interpret elementary arithmetic in the finite subsets algebra for the multiplicative group of all roots of unity. But that proof can't be applied

to an arbitrary Abelian torsion group because specific properties of the unity roots group are used.

In this paper, we generalize the result from [9] to all Abelian torsion groups with elements of unbounded order. For example, the result holds for any direct sums of unbounded cyclic groups and infinite subgroups of the unity roots group.

2. Basic Definitions and Notation

We consider an arbitrary additively written Abelian torsion group $\mathfrak{G} = (G, +, 0, -)$.

An Abelian group is an algebra such that the following equalities is satisfied: $a + (b + c) = (a + b) + c$, $a + b = b + a$, $a + 0 = a$, $a + (-a) = 0$. The notion $a - b$ means $a + (-b)$. The notion na means n-times sum: $a + \cdots + a$ where n is a natural number; or $(-n)(-a)$ for negative n. The order $\operatorname{ord} a$ of $a \in \mathfrak{G}$ is the least positive n (if it exists) such that $na = 0$. In the last case, a has finite order. If all elements of the Abelian group $\mathfrak{G}$ have finite order, then $\mathfrak{G}$ is a torsion group. We consider only torsion groups.

The group operation $+$ induces the corresponding operation on subsets:

$$x + y = \{a + b : a \in x, b \in y\}.$$

In particular, $x + \emptyset = \emptyset$, $x + \{0\} = x$. So, $\{0\}$ is a neutral element. As the source operation, $+$ is commutative and associative, so the induced operation is the same. If sets x and y are finite, then the set $x + y$ is finite also.

Therefore, all finite subsets of G form the commutative monoid (semigroup with a unity) $\exp \mathfrak{G} = (P_f(G), +, \{0\})$. For convenience, later we denote elements of the source group $\mathfrak{G}$ with the initial letters of the alphabet $a, \ldots, h$, and finite subsets with the last letters of the alphabet $u, \ldots, z$. Also, we write $x + a$ and $x - a$ instead of $x + \{a\}$ and $x + \{-a\}$ correspondingly.

A subgroup of the Abelian group $\mathfrak{G}$ is a subset $\mathfrak{H} \subseteq \mathfrak{G}$ that is an Abelian group also with the same operations. If $x \subseteq \mathfrak{G}$, then the subgroup generated by x is the least subgroup $\langle x \rangle$ that includes x. In the Abelian group $\mathfrak{G}$, a coset is a subset of the form $\mathfrak{H} + a$ where $\mathfrak{H} \subseteq \mathfrak{G}$ is a subgroup and $a \in \mathfrak{G}$.

3. Finite Subsets of $\mathfrak{G}$

In this section, we investigate some basic definabilities in the algebra $\exp \mathfrak{G}$ of finite subsets. The main notion introduced here is the kernel of a subset.

The empty set is definable by

$$x = \emptyset \equiv (\forall y) x + y = x.$$

In the following, we consider nonempty sets only.

Lemma 1. *If x contains 0, then $y \subseteq x + y$.*

Proof. If $x = \{0\} \cup x'$, then $y = y + 0 \subseteq (y + 0) \cup (y + x') = y + x$. □

Lemma 2. *Let x be a subgroup of $\mathfrak{G}$. Then, $y + x = x$ if and only if $y \subseteq x$.*

Proof. As x contains 0, so $x + y = x$ implies $y \subseteq x + y = x$ by Lemma 1. The converse is trivial. □

Lemma 3. *In the monoid $\exp \mathfrak{G}$ invertible elements are one-element sets exactly.*

Proof. Evidently, $\{a\} + \{-a\} = \{0\}$. If x contains two elements, then $x + y$ contains at least two elements also, so, $x + y \neq \{0\}$. □

Corollary 1. *One-element sets are definable in $\exp \mathfrak{G}$ with a formula $K_1(x) \equiv (\exists y) x + y = \{0\}$.*

Let the relation $x \approx y$ mean that $x = y + a$ for some $a \in \mathfrak{G}$. This relation is definable:

$$x \approx y \equiv (\exists z)(K_1(z) \wedge x + z = y).$$

The relation $\approx$ is a congruence because $x = x' + a$ and $y = y' + b$ imply $x + y = x' + y' + (a + b)$. Any set $\{a, b, \dots\}$ is congruent to a set of the form $\{0, c, \dots\}$: $\{a, b\} = a + \{0, b - a, \dots, \} \approx \{0, b - a, \dots\}$.

Lemma 4. *The equality $x + x = x$ is true in* $\exp \mathfrak{G}$ *if and only if x is a subgroup of $\mathfrak{G}$. In particular, $x + x = x$ implies $0 \in x$.*

Proof. Let $x + x = x$, a, b are any elements of x, so $a + b \in x + x = x$. Hence, $2a = a + a \in x + x = x$, $3a = 2a + a \in x + x = x$, and so on. Therefore, $na \in x$ for all natural n. In particular, if $n = \operatorname{ord} a$, then $0 = na \in x$ and $-a = (n - 1)a \in x$.

The converse is trivial. □

Lemma 5. *Let x contain 0. Then, there is a natural number n such that $nx = (n + 1)x$.*

Proof. If $x = \{0\}$, then $1x = \{0\} = 2x$.

In the other case, x contains 0 and some non-zero elements $a_1, \dots, a_k$. Let $\operatorname{ord} a_i = l_i$ for $i = 1, \dots, k$. Thus, the set mx contains sums of the form $j_1 a_1 + \dots + j_k a_k$ exactly, where $j_1 + \dots + j_k \leq m$. Each $j_i a_i$ has l_i possible values, so, there are at most $l_1 \dots l_k$ sums of the given kind. Hence, mx has finitely many possible values. By Lemma 1, we have $mx \subseteq mx + x = (m + 1)x$, so, the sequence of sets mx is growing. Therefore, $nx = (n + 1)x$ for some n. □

Corollary 2. *The set $nx = (n + 1)x$ in the previous lemma is the subgroup generated by x.*

Proof. From $nx + x = nx$ we obtain $nx + nx = nx$ by induction. By Lemma 4, the set nx is a subgroup.

If a subgroup z includes x, then z includes mx for all natural m. Hence, $nx \subseteq z$. □

For any set x the notion $\langle x \rangle$ means the subgroup generated by x.

Lemma 6. *The subgroup $\langle x \rangle$ is the least set y such that $x + y = y + y = y$.*

Proof. The equations $x + \langle x \rangle = \langle x \rangle + \langle x \rangle = \langle x \rangle$ follow from the definition of a generated subgroup.

By Lemma 4, the equality $y + y = y$ implies that y is a subgroup. As $0 \in y$, so $x \subseteq x + y = y$. Hence, $\langle x \rangle \subseteq y$, the least of such y is the subgroup $\langle x \rangle$. □

Corollary 3. *The subgroup generated by x is first order definable in* $\exp \mathfrak{G}$.

Proof. The definition is

$$y = \langle x \rangle \equiv y + y = y \wedge y + x = y \wedge (\forall z)(z + z = z \wedge z + x = z \to y + z = z).$$

By Lemmas 4 and 2, the formula $y + z = z$ is equivalent to $y \subseteq z$. □

Definition 1 (Kernel of a set x, $\ker x$)**.** The kernel *of a set x (denote it with* $\ker x$*) is the least subgroup $\mathfrak{H}$ such that x is included in some coset of $\mathfrak{H}$.*

Alternatively stated, $\ker x$ is the least kernel of a homomorphism that maps all the set x to one element.

Corollary 4. $\ker x \subseteq \langle x \rangle$.

Proof. For $\langle x\rangle$ we have $x \subseteq 0 + \langle x\rangle$, so, $\ker x \subseteq \langle x\rangle$ by the definition. □

Lemma 7. *For any set x the kernel* $\ker x$ *exists.*

Proof. Let $a \in x$. Let $\{\mathfrak{H}_i : i \in J\}$ be the family of all subgroups $\mathfrak{H}$ such that $x \subseteq a + \mathfrak{H}$. Hence,

$$x \subseteq \bigcap_i (a + \mathfrak{H}_i) = a + \bigcap_i \mathfrak{H}_i = a + \mathfrak{H}$$

for $\mathfrak{H} = \bigcap_i \mathfrak{H}_i$, this subgroup is the least one, i. e. the kernel $\ker x$. □

Corollary 5. *If $0 \in x$, then* $\ker x = \langle x\rangle$.

Proof. Let $a = 0$ in the proof of Lemma 7. Thus, $\mathfrak{H} = \bigcap_i \mathfrak{H}_i$ for all subgroups $\mathfrak{H}_i$ such that $x \subseteq \mathfrak{H}_i$. But this intersection is $\langle x\rangle$. □

Lemma 8. *Let $a \in x$, then* $\ker x = \langle x - a\rangle$ *and this subgroup is the least among all subgroups $\langle x - b\rangle$, $b \in \mathfrak{G}$.*

Proof. Evidently, $\ker x = \ker(x - b)$ for all $b \in \mathfrak{G}$ because $x \subseteq a + \mathfrak{H}$ if and only if $x - b \subseteq (a - b) + \mathfrak{H}$ for any subgroup $\mathfrak{H}$. For $a \in x$ we have $0 \in x - a$. By Corollary 5, we obtain $\ker x = \ker(x - a) = \langle x - a\rangle$.

For $b \in \mathfrak{G}$ we have $\ker x = \ker(x - b) \subseteq \langle x - b\rangle$. □

Corollary 6. *If $x \approx y$, then* $\ker x = \ker y$.

Corollary 7. *The kernel of a set is definable in* $\exp \mathfrak{G}$.

Proof. The definition is

$$y = \ker x \equiv (\exists u)\Big(K_1(u) \wedge y = \langle x + u\rangle \wedge (\forall v)(K_1(v) \to \langle x + u\rangle + \langle x + v\rangle = \langle x + v\rangle)\Big).$$

The equality $\langle x + u\rangle + \langle x + v\rangle = \langle x + v\rangle$ is equivalent to $\langle x + u\rangle \subseteq \langle x + v\rangle$ because $0 \in \langle x + v\rangle$. □

Lemma 9. *For all x the equality $\langle x\rangle = \ker x$ is true if and only if $\langle x\rangle = nx$ for almost every natural n.*

Proof. Let $\langle x\rangle = \ker x$, then $\langle x\rangle = \ker x = \langle x - a\rangle$ for all $a \in x$ by Lemma 8. By Corollary 2, we have $\langle x - a\rangle = n(x - a)$ for all but finitely many n due to $0 \in x - a$. From $a \in x$ we can deduce $na \in \langle x\rangle$ for all n, so, for all but finitely many n we have

$$nx = n(a + (x - a)) = na + n(x - a) = na + \langle x - a\rangle = na + \langle x\rangle = \langle x\rangle.$$

Now let $\langle x\rangle = nx$ for all but finitely many n. Let $b \in \mathfrak{G}$, $\operatorname{ord} b = l$. Then, for all but finitely many n multiple of l we obtain $n(x - b) = nx - nb = \langle x\rangle$. Thus, $\langle x\rangle = n(x - b) \subseteq \langle x - b\rangle$. Therefore, $\langle x\rangle$ is the least of all $\langle x - b\rangle$. By Lemma 8, we have $\ker x = \langle x\rangle$. □

Corollary 8. *For any x there is a natural n such that $nx \approx \ker x$.*

Proof. Let $a \in x$, then $x = a + (x - a)$ where $0 \in x - a$. So, for some n we have $nx = na + \langle x - a\rangle = na + \ker(x - a) = na + \ker x \approx x$. □

Lemma 10. $n\{0, a\} \approx \ker\{0, a\}$ *if and only if* $n \geq \operatorname{ord} a - 1$.

Proof. Indeed, we have $\ker\{0,a\} \approx \{0,a,2a,\dots,ma\}$ where $m = \operatorname{ord} a - 1$, and $n\{0,a\} \approx \{0,a,2a,\dots,na\}$. So, the claim is evident. □

Corollary 9. $3\{0,a\} \not\approx \ker\{0,a\}$ *if and only if* $\operatorname{ord} a > 4$.

4. Interpretation of Elementary Arithmetic

Here we define an interpretation of the elementary arithmetic in the algebra $\exp \mathfrak{G}$ of finite subsets.

The positive natural number m we interpret with a pair of sets $x \approx \{0,a\}$ and $X \approx m\{0,a\}$ where $\operatorname{ord} a > 4$ and $m \leq (\operatorname{ord} a - 2)/2$.

In the next sections we define two following relations:

- $P_3(x,X,z)$ that is true if and only if $x \approx \{0,a\}$, $X \approx mx$, and $z \approx \{0,ma\}$ for some positive natural m, $m \leq (\operatorname{ord} a - 2)/2$, and some $a \in \mathfrak{G}$;
- $E(x,X,y,Y)$ that is true if $x \approx \{0,a\}$, $X \approx mx$, $y \approx \{0,b\}$, $Y \approx my$ for some natural m, $m \leq (\operatorname{ord} a - 2)/2$, $m \leq (\operatorname{ord} b - 2)/2$.

Theorem 1. *Elementary arithmetic can be interpreted in the monoid* $\exp \mathfrak{G}$.

Proof. The interpretation area can be defined as

$$I(x,X) \equiv 3x \not\approx \ker x \wedge (\exists z) P_3(x,X,z).$$

The atomic formulas are interpreted the following way:

- each variable x_i is interpreted by a pair (x_i, X_i);
- $x = y$ is interpreted by $E(x,X,y,Y)$;
- $x + y = z$ is interpreted by

$$(\exists x', X', y', Y')(E(x,X,z,X') \wedge E(y,Y,z,Y') \wedge X' + Y' = Z).$$

  This formula says that $x \approx \{0,a\}$, $y \approx \{0,b\}$, $z \approx \{0,c\}$, $X \approx \{0,a,2a,\dots,ma\}$, $Y \approx \{0,b,2b,\dots,nb\}$, $X' \approx \{0,c,2c,\dots,mc\}$, $Y' \approx \{0,c,2c,\dots,nc\}$, and $Z = X' + Y' \approx \{0,c,2c,\dots,(n+m)c\}$.
- $x \cdot y = z$ is interpreted by

$$(\exists X', Y', z', Z')(E(x,X,z,X') \wedge P_3(z,X',z') \wedge E(y,Y,z',Z') \wedge 2Z = Z + Z').$$

  This formula says that $x \approx \{0,a\}$, $y \approx \{0,b\}$, $z \approx \{0,c\}$, $X \approx \{0,a,2a,\dots,ma\}$, $Y \approx \{0,b,2b,\dots,nb\}$, $X' \approx \{0,c,2c,\dots,mc\}$, $z' \approx \{0,mc\}$, $Z' \approx \{0,nc,2nc,\dots,mnc\}$, and $Z \approx \{0,c,2c,\dots,mnc\}$.

The boolean formulas $\phi \wedge \psi$, $\phi \vee \psi$, $\phi \to \psi$, $\neg\phi$ are interpreted as $\Phi \wedge \Psi$, $\Phi \vee \Psi$, $\Phi \to \Psi$, $\neg\Phi$ correspondingly. Here Φ and Ψ are interpretations of ϕ and ψ correspondingly.

The quantified formulas $(\exists x)\phi$ and $(\forall x)\phi$ are interpreted as $(\exists x, X)(I(x,X) \wedge \Phi)$ and $(\forall x, X)(I(x,X) \to \Phi)$ correspondingly. □

Corollary 10. *The theory of* $\exp \mathfrak{G}$ *is undecidable.*

Corollary 11. *Let the Abelian group* $\mathfrak{G}$ *include any infinite subgroup* $\mathfrak{H}$ *of the group of unity roots. Then, the theory of* $\exp \mathfrak{G}$ *allows interpreting the elementary arithmetic and undecidable.*

Proof. If $\mathfrak{G}$ has an element of infinite order, then the result follows from [8]. Otherwise, $\mathfrak{G}$ is a torsion Abelian group and has elements of unbounded order because there are finitely many elements of bounded order in $\mathfrak{H}$. Therefore, the result follows from Theorem 1. □

An immediate generalization of the previous corollary is the following.

Corollary 12. *Let the Abelian group $\mathfrak{G}$ be not a group of finite exponent (i. e. there is no natural n such that $na = 0$ for all $a \in \mathfrak{G}$). Then, the theory of* $\exp \mathfrak{G}$ *allows interpreting the elementary arithmetic and undecidable.*

5. Multiple Relations

Early, we use the relation P_3 to interpret the multiplication in the algebra $\exp \mathfrak{G}$. Here we establish that this relation P_3 is definable.

In [9] the following claim was proved (Theorem 1):

Lemma 11. *Let $\mathfrak{G}$ be any Abelian torsion group. Then, there is a formula $K_2(x)$ that is true in* $\exp \mathfrak{G}$ *if and only if the set x has exactly two elements.*

Proof. If $\ker x$ contains five or more elements, then the condition can be expressed by the formula

$$(\exists u)\Big(3x = u + x \wedge u \neq 2x \wedge (\forall v)\big(3x = v + x \to v = 2x \vee v = u\big)\Big).$$

Another cases (two, three, or four elements in $\ker x$) are considered separately.

For details see [9]. □

Let us consider the following binary relation P_2:

$$P_2(x, X) \equiv X + \ker x \not\approx X \wedge (\forall u, v)(X = u + v \wedge \neg K_1(v) \to (\exists w)X = u + x + w).$$

Lemma 12. *If $P_2(x, X)$ is true, then $X \approx nx$ for some natural n.*

Proof. If X is invertible, then $X \approx \{0\} = 0x$.

Otherwise, $X = \{0\} + X$ and $K_1(X)$ is false. By the implication, we have $X = \{0\} + x + w_1 = x + w_1$. If w_1 is uninvertible, then the same manner we have $X = x + x + w_2 = 2x + w_2$. So, we obtain $X = nx + w_n$ for all naturals n until w_n is invertible. Then, $X \approx nx$.

Such n must exist because otherwise we have $X \approx \ker x + w_n$ for some n by Corollary 8. Then, $X + \ker x \approx (\ker x + w_n) + \ker x = \ker x + w_n = X$ and $P_2(x, X)$ is false. □

Lemma 13. *If $K_2(x)$ is true, $X \approx mx$, and $X + \ker x \not\approx X$, then the formula $P_2(x, X)$ is true.*

Proof. From $K_2(x)$ we have $x \approx \{0, a\}$ for some a.

Let $X = u + v$ and v have at least two elements. The difference between any two elements of X has the form ia, so, the difference between any two elements of u or any two elements of v have the same form. Hence, $u \subseteq m_1 x + c$ and $v \subseteq m_2 x + d$. Let us select the minimal m_2, then $m_2 > 0$, and we have $u + v \approx u + x + (m_2 - 1)x$. □

Let us define

$$Q(x, y) \equiv (\exists X)(P_2(x, X) \wedge X + x \approx \ker x \wedge y + X = y + X + \ker x).$$

Lemma 14. *Let $x \approx \{0, a\}$ and $K_2(x)$ be true. Then, $Q(x, y)$ is true if and only if $y \approx \{0, ia, \dots\}$ for some $ia \neq 0$.*

Proof. Let $Q(x, y)$ be true. Then, $X \approx mx$ by Lemma 12. From $X + x \approx \ker x$ we have $m \geq \operatorname{ord} a - 2$ and $X \approx \{0, a, 2a, \dots, ma\}$. As $y + X = y + X + \ker x$, so $y + X$ must include $b + \{0, a, 2a, \dots, (m + 1)a\}$. Hence, there are different $c, d \in y$ such that $c + ia = b + ja$ and $d + ka = b + la$. So, $c = b + (j - i)a$, $d = b + (l - k)a$, $j - i \neq l - k$, and $y = c + \{0, (l + i - k - j)a, \dots\}$.

The converse claim is true because $X \approx \{0, a, 2a, \dots, ma\}$, $m = \operatorname{ord} a - 2$, $y + X \approx \{0, a, 2a, \dots, ma, (m + 1 - i)a + ia, \dots\} \approx y + X + \ker x$. □

Lemma 15. *If $Q(x, my)$ is true, $x \approx \{0, a\}$, $y \approx \{0, b\}$, $m < \operatorname{ord} b$, then all elements $ia + jb$ are pairwise different where $i < \operatorname{ord} a$, $j \leq m$.*

Proof. Let $i_1 a + j_1 b = i_2 a + j_2 b$.

If $j_1 = j_2$, then $i_1 a = i_2 a$ and $i_1 = i_2$ due to $i_2, i_1 < \operatorname{ord} a$.

Now let $j_1 > j_2$. If $i_1 = i_2$, then $j_1 b = j_2 b$ and $j_1 = j_2$ due to $j_1, j_2 \leq m < \operatorname{ord} b$. Otherwise, $(j_1 - j_2)b = (i_2 - i_1)a$, $j_1 - j_2 \leq m$, and $i_2 - i_1 \neq 0$. Hence, $my \approx \{0, (i_2 - i_1)a, \dots\}$ that contradicts to $Q(x, my)$ by Lemma 14. □

The relation P_3 is

$$P_3(x, X, z) \equiv K_2(x) \wedge 2X \not\approx \ker x \wedge K_2(z) \\ \wedge (\exists X')(P_2(x, X') \wedge X \approx X' + x \wedge X + X' \approx z + X').$$

Theorem 2. *The formula $P_3(x, X, z)$ is true if and only if $x \approx \{0, a\}$, $X \approx nx$, $z \approx \{0, na\}$ for some $a \in \mathfrak{G}$, $a \neq 0$, and natural $n > 0$, $n \leq (\operatorname{ord} a - 2)/2$.*

Proof. Let $P_3(x, X, z)$ be true. Then, $x \approx \{0, a\}$ for some $a \neq 0$. By Lemma 12, we have $X' \approx n'x$ and $X \approx nx$ for some naturals n' and $n = n' + 1$. If $n > (\operatorname{ord} a - 2)/2$, then $2n \geq 2((\operatorname{ord} a - 2)/2 + 1)$, $2n \geq \operatorname{ord} a - 1$, $2X \approx \{0, a, 2a, \dots, (2n)a\} \approx \ker x$, and we have a contradiction. So, $n \leq (\operatorname{ord} a - 2)/2$. The set $X + X'$ contains exactly $2n$ elements: $X + X' \approx \{0, a, 2a, \dots, (2n - 1)a\}$. So, the set $z + X'$ contains exactly $2n$ elements also. If $z \approx \{0, b\}$, then

$$z + X' \approx \{0, \dots, (n - 1)a, 0 + b, \dots, (n - 1)a + b\}.$$

Hence, $b = na$ or $(n - 1)a + b = -a$. In the first case, we have $z \approx \{0, na\}$. In the second case we have $z \approx \{0, -na\} \approx \{0, na\}$.

Now let $x \approx \{0, a\}$, $X \approx nx$, $z \approx \{0, na\}$ for some $a \in \mathfrak{G}$, $a \neq 0$, and natural $n > 0$, $n \leq (\operatorname{ord} a - 2)/2$. Then, the formulas $K_2(x)$, $2X \not\approx \ker x$, $K_2(z)$ are true. Let $X' = (n - 1)x = \{0, a, \dots, (n - 1)a\} + b$. Thus, $X \approx X' + x$ and $X + X' \approx z + y'$ are true. The formula $P_2(x, X')$ is true by Lemma 13. □

6. The Equivalence Relation

The remaining problem is to define the equality relation for our interpretation of the elementary arithmetic. Thus, our last task is to construct a formula for an equivalence relation $E(x, X, y, Y)$ that is true if and only if $X \approx nx$ and $Y \approx ny$ for some n.

Lemma 16. *Let $3\{0, a\} \not\approx \ker a$, $3\{0, b\} \not\approx \ker b$, and $Q(\{0, a\}, 3\{0, b\})$ be false. Let $x \approx x' = \{0, a, b\}$. Then, there are exactly seven sets u such that $u + x = 3x$.*

Proof. By Corollary 9, we have $\operatorname{ord} a > 4$ and $\operatorname{ord} b > 4$. From falsehood of the formula $Q(\{0, a\}, 3\{0, b\})$ we have all elements $ia + jb$ to be pairwise different for $j \leq 3$ (Lemma 15).

Let $x = x' + c$. From $u + x = 3x$ we have $(u - 2c) + x' = 3x'$. The set $3x'$ consists of all $ia + jb$ for $i + j \leq 3$. From $0 \in x'$ we have $u' = u - 2c \subseteq u' + x' = 3x'$.

If we suppose that u' contains $ia + jb$ where $i + j = 3$, then $u' + x'$ contains $(i + 1)a + jb$. Thus, $(i + 1)a + jb = ka + lb$ for $k + l \leq 3$. If $j = l$, then $(i + 1)a = ka$. As $(i + 1) \leq 4$ and $k \leq 4$, so $i + 1 = k$ that is impossible. If $j < l$, then $(k - i - 1)a + (l - j)b = 0$ that is impossible too. Analogously the case $l < j$ is impossible.

Thus, u' contains $ia + jb$ for $i + j \leq 2$ only, i. e. $u' \subseteq 2x' = \{0, a, b, 2a, 2b, a + b\}$.

Further, $u' \ni 0, 2a, 2b$ because $0, 3a, 3b \in 3x'$ can be obtained only as $0 = 0 + 0$, $3a = 2a + a$, $3b = 2b + b$ correspondingly. To obtain $a + b \in 3x'$ the set u' must contain a, b, or $a + b$.

Thus, $u' = \{0, 2a, 2b\} \cup u''$ for any nonempty $u'' \subseteq \{a, b, a + b\}$. There are exactly seven such u''. □

Lemma 17. *Let $x \approx x' = \{0, a, \dots\}$ for $a \neq 0$. Let there be exactly seven sets u such that $u + x = 3x$. Then, x contains exactly three elements.*

Proof. Let $x = x' + d$. From $u + x = 3x$ we have $(u - 2d) + x' = 3x'$. If x (and x') contains exactly two elements, then there are exactly two such u (see [8], Proposition 4).

Let us denote $u - 2d$ with u'. Let us suppose that x contains four or more elements: $x' = \{0, a, b, c, \dots\}$ for non-zero and pairwise different a, b, c. Then, u' can be $u' = 2x' \setminus u''$ for any $u'' \subseteq \{a, b, c\}$. There exist exactly eight such u'' (and u'). Let us prove $u' + x' = 2x' + x' = 3x'$ for $u' = 2x' \setminus \{a, b, c\}$, then the other possibilities follow. Evidently, we have $u' + x' \subseteq 2x' + x'$, consider the converse inclusion.

- $a + g = g + a$ for $g \notin \{a, b, c\}$;
- $a + a = 2a + 0$ when $2a \notin \{b, c\}$. Let us note that $2a \neq a$;
- $a + a = 0 + c$ when $2a = c$;
- $a + a = 0 + b$ when $2a = b$;
- $a + b = (a + b) + 0$ when $a + b \neq c$. Let us note that $a + b \neq a$ and $a + b \neq b$;
- $a + b = 0 + c$ when $a + b = c$.

The other cases can be considered analogously.

Therefore, if x has four or more elements, then there are at least eight u such that $u + x = 3x$. □

Let us denote

$$K_3(x) \equiv (\exists u_1, \dots, u_7)\Big(\bigwedge_{i=1}^{7} u_i + x = 3x \wedge \bigwedge_{i \neq j} u_i \neq u_j \wedge (\forall u)(u + x = 3x \to \bigvee_{i=1}^{7} u = u_i)\Big).$$

Lemma 18. *Let $K_2(\{0, a\})$ and $K_2(\{0, b\})$ be true, and $Q(\{0, a\}, \{0, b\})$ be false. Then* $\ker\{0, a\} + x \approx \ker\{0, a\} + \{0, b\}$ *if and only if $x \approx x'$ where x' contains at least one element of the form ka, at least one element of the form $ka + b$, and no element of another form.*

Proof. Let $\ker\{0, a\} + x \approx \ker\{0, a\} + \{0, b\}$ be true. Then, $\ker\{0, a\} + x = \ker\{0, a\} + \{0, b\} + c$ for some c. Hence, for any $d \in x$ we have $d = ka + c$ or $d = ka + b + c$. So, $x = x' + c$, and x' contains only elements of the form ka and $ka + b$.

If x' contains only elements of the form ka, then $\ker\{0, a\} + x \approx \ker\{0, a\} \not\approx \ker\{0, a\} + \{0, b\}$. If x' contains only elements of the form $ka + b$, then $\ker\{0, a\} + x' \approx \ker\{0, a\} + b$ and $\ker\{0, a\} + x \approx \ker\{0, a\} \not\approx \ker\{0, a\} + \{0, b\}$.

The converse is trivial. □

Lemma 19. *Let $z \approx \{0, a\}$, $y \approx \{0, b\}$, $Y \approx my$, and the formula $Q(z, Y + y)$ be false. Let x be as in the previous Lemma. Then,* $\ker z + kx \approx \ker x + Y$ *if and only if $k = m$.*

Proof. The set $\ker z + Y$ contains exactly $(m + 1) \operatorname{ord} a$ elements (Lemma 15). The set $\ker z + kx$ contains no more than $(k + 1) \operatorname{ord} a$ elements. So, $k \geq m$.

If $k > m$, then $\ker z + kx$ contains together c and $c + (m + 1)b$ for some c. So, $\ker x + Y$ must contain d and $d + (m + 1)b$ for some d. It is impossible due to falsehood of $Q(z, Y + y)$, thus, $k = m$.

Now let $k = m$, then $\ker z + kx$ consists of $c + ia + jb$ for all i and $j \leq m$, and $\ker z + Y$ consists of $d + ia + jb$ for all i and $j \leq m$. Hence, $\ker z + kx \approx \ker x + Y$. □

Lemma 20. *Let $x \approx \{0, a\}$, $y \approx \{0, b\}$, $\operatorname{ord} a > 4$, $\operatorname{ord} b > 4$, the formulas $K_2(z)$, $K_3(u)$, $K_3(v)$ be true, the formula $Q(x, 4y)$ be false, and* $\ker x + z \approx \ker\{0, a\} + y$, $\ker x + u \approx \ker\{0, a\} + y$, $\ker x + v \approx \ker\{0, a\} + y$. *Then, $x + y + z \approx u + v$ if and only if*

- $z \approx \{a, b\}$ *and* $u \approx \{0, a, b\}$, $v \approx \{a, b, a + b\}$ *(or vice versa), or*
- $z \approx \{0, a + b\}$ *and* $u \approx \{0, a, a + b\}$, $v \approx \{a, b, a + b\}$ *(or vice versa).*

Proof. The converse claim can be verified trivially. So, we must prove the straight one.

From ord $b > 4$ and falsehood of $Q(x, 4y)$ we obtain that $b, 2b, 3b, 4b$ are not equal ia for any i (Lemma 15).

By Lemma 18, we have $z \approx \{0, \alpha a + b\}$, $u \approx \{0, \delta a + b, \zeta a + kb\}$, $v \approx \{0, \beta a + b, \gamma a + mb\}$, for some integers $\alpha, \beta, \gamma, \delta, \zeta$ and $k, m \in \{0, 1\}$. So, we have the equality

$$\{0, a\} + \{0, b\} + \{0, \alpha a + b\} = c + \{0, \delta a + b, \zeta a + kb\} + \{0, \beta a + b, \gamma a + mb\} \quad (1)$$

for some c. The left set in (1) consists of elements of the form ia, $ia + b$, and $ia + 2b$. The right set in (1) contains c, so $c = \theta a$, $c = \theta a + b$, or $c = \theta a + 2b$ for some integer θ. For $c = \theta a + b$ or $c = \theta a + 2b$ the right set contains $ia + 3b$ or $ia + 4b$ correspondingly. It is impossible because $ia + 3b$ and $ia + 4b$ don't belong to the left set. Thus, $c = \theta a$.

Further, let us show $m + k = 1$, i. e. one of them is 0 and another is 1. If we expand (1), then we obtain

$$\begin{aligned}\{0, a, b, a + b, \alpha a + b, (\alpha + 1)a + b, \alpha a + 2b, (\alpha + 1)a + 2b\}\\ = \{\theta a, (\delta + \theta)a + b, (\zeta + \theta)a + kb, (\beta + \theta)a + b, (\gamma + \theta)a + mb, (\delta + \beta + \theta)a + 2b,\\ (\zeta + \beta + \theta)a + (k + 1)b, (\delta + \gamma + \theta)a + (m + 1)b, (\zeta + \gamma + \theta)a + (k + m)b\}. \quad (2)\end{aligned}$$

For $m = k = 1$ the right set in (2) can't contain 0 and a together from the left set.

For $m = k = 0$ the right set in (2) contains θa, $(\zeta + \theta)a$, $(\gamma + \theta)a$, and $(\zeta + \gamma + \theta)a$. These elements can be equal to only a or 0 in the left set. As u and v contain three elements, ζ and γ can't be equal to zero. Thus, $\zeta = \gamma = \pm 1$ and $2a = 0$. It contradicts to ord $a > 4$.

Now we can suppose $k = 0$, $m = 1$. Hence, the equality (2) becomes

$$\begin{aligned}\{0, a, b, a + b, \alpha a + b, (\alpha + 1)a + b, \alpha a + 2b, (\alpha + 1)a + 2b\}\\ = \{\theta a, (\delta + \theta)a + b, (\zeta + \theta)a, (\beta + \theta)a + b, (\gamma + \theta)a + b, (\delta + \beta + \theta)a + 2b,\\ (\zeta + \beta + \theta)a + b, (\delta + \gamma + \theta)a + 2b, (\zeta + \gamma + \theta)a + b\}.\end{aligned}$$

It is clear that θa and $(\zeta + \theta)a$ must be equal 0 and a only, hence, $\theta = 0$, $\zeta = 1$ or $\theta = 1$, $\zeta = -1$. In the second case, we have

$$\{0, a\} + \{0, b\} + \{0, \alpha a + b\} = a + \{0, \delta a + b, -a\} + \{0, \beta a + b, \gamma a + b\}$$

and

$$\{0, a\} + \{0, b\} + \{0, \alpha a + b\} = \{0, (\delta + 1)a + b, a\} + \{0, \beta a + b, \gamma a + b\}$$

that is the first case.

Thus, we can consider only the equality

$$\begin{aligned}\{0, a, b, a + b, \alpha a + b, (\alpha + 1)a + b, \alpha a + 2b, (\alpha + 1)a + 2b\}\\ = \{0, \delta a + b, a, \beta a + b, \gamma a + b, (\delta + \beta)a + 2b,\\ (\beta + 1)a + b, (\delta + \gamma)a + 2b, (\gamma + 1)a + b\}. \quad (3)\end{aligned}$$

The elements $\alpha a + 2b$ and $(\alpha + 1)a + 2b$ from the left set in (3) must be equal to $(\delta + \beta)a + 2b$ and $(\delta + \gamma)a + 2b$ from the right set. It follows that $\gamma = \beta \pm 1$. So, we can assume that $\gamma = \beta + 1$ and $\alpha = \delta + \beta$. Hence, we obtain

$$\begin{aligned}\{0, a, b, a + b, (\delta + \beta)a + b, (\delta + \beta + 1)a + b, (\delta + \beta)a + 2b, (\delta + \beta + 1)a + 2b\}\\ = \{0, \delta a + b, a, \beta a + b, (\beta + 1)a + b, (\delta + \beta)a + 2b,\\ (\beta + 1)a + b, (\delta + \beta + 1)a + 2b, (\beta + 2)a + b\}. \quad (4)\end{aligned}$$

Now we can consider all possibilities for $\delta a + b$ from the right set in (4). It must be equal to 0, a, $(\delta + \beta)a + 2b$, or $(\delta + \beta + 1)a + 2b$ from the left set in (4). Thus, we have the next four possibilities.

1. $\delta a + b = b$, $\delta = 0$, and we have

$$\begin{aligned}\{0, a, b, a + b, \beta a + b, (\beta + 1)a + b, \beta a + 2b, (\beta + 1)a + 2b\}\\ = \{0, b, a, \beta a + b, (\beta + 1)a + b, \beta a + 2b,\\ (\beta + 1)a + b, (\beta + 1)a + 2b, (\beta + 2)a + b\}.\end{aligned}$$

Then, $(\beta + 2)a + b$ can be equal to b or $a + b$ only. In the first case, we have $\beta = -2$ and

$$\begin{aligned}\{0, a, b, a + b, -2a + b, -a + b, -2a + 2b, -a + 2b\}\\ = \{0, b, a, -2a + b, -a + b, -2a + 2b, -a + b, -a + 2b, b\}.\end{aligned}$$

That is impossible because $a + b$ from the left set is not in the right one. Thus, $(\beta + 2)a + b = a + b$, $\beta = -1$, $\alpha = -1$, $\gamma = 0$, and we have

$$\{0, a\} + \{0, b\} + \{0, -a + b\} = \{0, b, a\} + \{0, -a + b, b\}$$

or

$$\{0, a\} + \{0, b\} + \{a, b\} = \{0, b, a\} + \{a, b, a + b\}.$$

2. $\delta a + b = a + b$, $\delta = 1$, and we have

$$\begin{aligned}\{0, a, b, a + b, (\beta + 1)a + b, (\beta + 2)a + b, (\beta + 1)a + 2b, (\beta + 2)a + 2b\}\\ = \{0, a + b, a, \beta a + b, (\beta + 1)a + b, (\beta + 1)a + 2b,\\ (\beta + 1)a + b, (\beta + 2)a + 2b, (\beta + 2)a + b\}.\end{aligned}$$

So, $\beta a + b$ can be equal to b or $a + b$ only. It means that $\beta = 0$ or $\beta = 1$. In the second case, we obtain

$$\begin{aligned}\{0, a, b, a + b, 2a + b, 3a + b, 2a + 2b, 3a + 2b\}\\ = \{0, a + b, a, a + b, 2a + b, 2a + 2b, 2a + b, 3a + 2b, 3a + b\}.\end{aligned}$$

That is impossible because b from the left set is not in the right one. Hence, $\beta = 0$, $\alpha = 1$, $\gamma = 1$, and we have

$$\{0, a\} + \{0, b\} + \{0, a + b\} = \{0, a + b, a\} + \{0, b, a + b\}.$$

3. $\delta a + b = (\delta + \beta)a + b$, $\delta = \delta + \beta$, so $\beta = 0$. We have

$$\begin{aligned}\{0, a, b, a + b, \delta a + b, (\delta + 1)a + b, \delta a + 2b, (\delta + 1)a + 2b\}\\ = \{0, \delta a + b, a, b, a + b, \delta a + 2b, a + b, (\delta + 1)a + 2b, 2a + b\}.\end{aligned}$$

Then, $2a + b$ can be equal $\delta a + b$ or $(\delta + 1)a + b$ only. We have $\delta = 2$ or $\delta = 1$. In the first case, we have

$$\begin{aligned}\{0, a, b, a + b, 2a + b, 3a + b, 2a + 2b, 3a + 2b\}\\ = \{0, 2a + b, a, b, a + b, 2a + 2b, a + b, 3a + 2b, 2a + b\}.\end{aligned}$$

This is impossible because $3a + b$ from the left set not in the right set. Thus, $\delta = 1$ and we have the case 2.

4. $\delta a + b = (\delta + \beta + 1)a + b$, $\delta = \delta + \beta + 1$, and $\beta = -1$. We obtain

$$\{0, a, b, a + b, (\delta - 1)a + b, \delta a + b, (\delta - 1)a + 2b, \delta a + 2b\}$$
$$= \{0, \delta a + b, a, -a + b, b, (\delta - 1)a + 2b, b, \delta a + 2b, a + b\}.$$

In this case, $-a + b$ can be $(\delta - 1)a + b$ or $\delta a + b$ only, i. e. $\delta = 0$ or $\delta = -1$. The last implies

$$\{0, a, b, a + b, -2a + b, -a + b, -2a + 2b, -a + 2b\}$$
$$= \{0, -a + b, a, -a + b, b, -2a + 2b, b, -a + 2b, a + b\},$$

that is impossible: $-2a + b$ is in the left set but is not in the right one. So, $\delta = 0$ and we have the case 1. □

Lemma 21. *Let* $3m < \operatorname{ord} a$, $3m < \operatorname{ord} b$, $m \geq 2$, $Q(\{0, a\}, 3m\{0, b\})$ *be false, and* $x \approx \{0, a', b'\}$ *where* $a' = \pm a$ *and* $b' = \pm b$. *Then,* $P_2(x, mx)$ *is true.*

Proof. Falsehood of $Q(\{0, a\}, 3m\{0, b\})$ means that $jb \neq ia$ for $0 < j \leq 3m$ (Lemma 15). Hence, $\pm jb \neq ia$ also, and $jb' \neq ia'$.

Let $x = c + \{0, a', b'\}$. Then, the set mx consists of $mc + ia' + jb'$ where $i + j \leq m$. Evidently, $mx + x \not\approx \ker x$ because $mx + x$ can't contain g and $g + (m + 2)b'$ together: $m + 2 \leq m + m \leq 3m - 2 < \operatorname{ord} a - 1$.

Let $u + v = mx$ and $d \in u$. Then, $(u - d) + (v - mc + d) = m\{0, a, b\}$. As $0 \in u - d$, so $v_1 = v - mc + d \subseteq m\{0, a', b'\}$, hence, $u_1 = u - d \subseteq m\{0, a', b', -a', -b'\}$.

If u_1 contains no elements of the form $-ia' \pm jb'$, $i > 0$, then $u_2 = u_1$ and $v_2 = v_1$. Otherwise, let us select $-i_1a' \pm jb' \in u'$ with maximal i_1. Then, v_1 can't contain $ia' + kb'$ with $i < i_1$. Assume $u_2 = u_1 + i_1a'$ and $v_2 = v_1 - i_1a'$.

If u_2 contains no elements of the form $ia' - jb'$, $j > 0$, then $u_3 = u_2$ and $v_3 = v_2$. Otherwise, let us select $ia' - j_2b' \in u_2$ with maximal j_2. Then, v_2 can't contain $ka' + jb'$ with $j < j_2$. Assume $u_3 = u_2 + j_2b'$ and $v_3 = v_2 - j_2b$.

Then, $v_3 \subseteq m\{0, a', b'\}$, $u_3 \subseteq 2m\{0, a', b'\}$, and $u_3 + v_3 = u_1 + v_1 = m\{0, a', b'\}$.

Let us select $i_0a' + j_0b' \in v_3$ with maximal $i_0 + j_0$. If $i_0 + j_0 = 0$, then v_3 and v are invertible. Otherwise, $i_0 + j_0 \geq 1$ and $v_3 \subseteq (i_0 + j_0)\{0, a', b'\}$. In this case, u_3 can't contain $ia' + jb'$ with $i + j > m - i_0 - j_0$, i. e. $u_3 \subseteq (m - i_0 - j_0)\{0, a', b'\}$. Then

$$m\{0, a', b'\} = u_3 + v_3 \subseteq u_3 + (i_0 + j_0)\{0, a', b'\}$$
$$\subseteq (m - i_0 - j_0)\{0, a', b'\} + (i_0 + j_0)\{0, a', b'\} = m\{0, a', b'\}.$$

Thus, $u_3 + (i_0 + j_0)\{0, a', b'\} = m\{0, a', b'\}$ and we have $u + x + (i_0 + j_0 - 1)x \approx mx$. □

Lemma 22. *Let the formulas* $I(x, X)$ *and* $I(y, Y)$ *be true, and* $Q(x, 4Y)$ *be false. Then,* $n = m$ *if and only if all the following formulas are true for some* z, Z, u, U, v, V:

1. $K_2(z)$, $K_3(u)$, $K_3(v)$;
2. $P_2(z, Z)$;
3. $P_2(u, U)$, $P_2(v, V)$;
4. $\ker x + Z \approx \ker x + Y$, $\ker x + U \approx \ker x + Y$, $\ker x + V \approx \ker x + Y$;
5. $x + y + z \approx u + v$;
6. $X + Y + Z \approx U + V$.

Proof. Let $n = m$. Assume $z = \{0, a + b\}$, $Z = mz$, $u = \{0, a, a + b\} \approx \{0, -a, b\}$, $U = mu$, $v = \{0, b, a + b\} \approx \{0, a, -b\}$, $V = mu$. Then, $K_2(z)$ is true by Lemma 11; $K_3(u)$ and $K_3(v)$ are true by Lemma 16; $P_2(z, Z)$ is true by Lemma 13; $P_2(u, U)$ and $P_2(v, V)$ are true by Lemma 21; $\ker x + Z \approx \ker x + Y$, $\ker x + U \approx \ker x + Y$, and $\ker x + V \approx \ker x + Y$ are true by Lemma 18; $x + y + z \approx u + v$ and $X + Y + Z \approx U + V$ are true by Lemma 20.

Now let all the formulas 1–6 be true. Then, from 1 we have z has two elements (Lemma 11), u and v have three elements (Lemma 17). By Lemma 20, from 5 we have

- $z \approx \{a, b\}$, $u \approx \{0, a, b\}$, $v \approx \{a, b, a+b\} \approx \{0, -a, -b\}$ or
- $z \approx \{0, a+b\} \approx \{-a, b\}$, $u \approx \{0, a, a+b\} \approx \{0, -a, b\}$, $v \approx \{0, b, a+b\} \approx \{0, a, -b\}$.

In any case, from 2 and 3 we obtain $Z \approx k_z z$, $U \approx k_u u$, $V \approx k_v v$ by Lemma 12. By Lemma 18, from 4 we have $k_z = k_u = k_v = m$. Thus, from 6 we have

$$n\{0, a\} + m\{0, b\} + m\{a, b\} \approx m\{0, a, b\} + m\{a, b, a+b\}$$

or

$$n\{0, a\} + m\{0, b\} + m\{0, a+b\} \approx m\{0, a, a+b\} + m\{0, b, a+b\}.$$

If we suppose $n > m$, then the left sets have g and $g + (n+m)a$ (or $g + (n+m)a + mb$) for some g, but the right sets can't have them together because all $ia + jb$ are pairwise different for $i \leq 2n$, $j \leq 3m$ (Lemma 15).

Now let us suppose $n < m$, then the right sets have g and $g + ia + 2mb$ (or $g + (i + m)a + 2mb$) for some g and $i \leq m$. By Lemma 15, we have $2mb \neq ia$ for all $i \neq 0$. The left sets can have only elements of the form h and $h + ia + 2mb$ (or $h + (i+m)a + 2mb$) for some h and $i \leq n$. Hence, $\{0, \dots, na\} = \{0, \dots, ma\}$ that means $n + 1 \geq \operatorname{ord} a$. It contradicts to $2X \not\approx \ker x$ (the formula $I(x, X)$ includes $P_3(x, X, \dots)$).

Therefore, $n = m$. □

Let us construct formulas E' and E:

$$\begin{aligned} E'(x, X, y, Y) \equiv I(x, X) \wedge I(y, Y) \wedge \neg Q(x, 4Y) \\ \wedge (\exists z, Z, u, U, v, V)(K_2(z) \wedge K_3(u) \wedge K_3(v) \wedge P_2(z, Z) \wedge P_2(u, U) \wedge P_2(v, V) \\ \wedge \ker x + Z = \ker x + Y \wedge \ker x + U = \ker x + Y \wedge \ker x + V = \ker x + Y \\ \wedge x + y + z = u + v \wedge X + Y + Z = U + V); \end{aligned}$$

$$E(x, X, w, W) \equiv (\exists y, Y)(K_2(y) \wedge I(y, Y) \wedge E'(x, X, y, Y) \wedge E(w, W, y, Y)).$$

Theorem 3. *Let $I(x, X)$ and $I(w, W)$ be true. Then, $E(x, X, w, W)$ is true if and only if $X \approx nx$ and $W \approx nw$ for some n.*

Proof. From $I(x, X)$ and $I(w, W)$ we have $X \approx n_1 x$ and $W \approx n_2 w$.

Let $E(x, X, w, W)$ be true. Let us fix y and Y, so $Y \approx ny$. Then, $E'(x, X, y, Y)$ and $E'(w, W, y, Y)$ are true. By Lemma 22, we have $n_1 = n$ and $n_2 = n$, so $n_1 = n_2$.

Now let $X \approx nx$ and $W \approx nw$ where $x \approx \{0, a\}$ and $w \approx \{0, b\}$. Then, $n \leq (\operatorname{ord} a - 2)/2$ and $n \leq (\operatorname{ord} b - 2)/2$. Let us select $y = \{0, c\}$ such that $\operatorname{ord} c > (4 \operatorname{ord} a)^2$ and $\operatorname{ord} c > (4 \operatorname{ord} b)^2$, $Y = ny$. So, we have the formula $I(y, Y)$ to be true and the formula $Q(x, 4Y)$ to be false. Thus, $E'(x, X, y, Y)$ and $E'(w, W, y, Y)$ are true by Lemma 22. □

7. Conclusions

We have established that for any Abelian group of infinite exponent the algebra of finite subsets allows us to interpret elementary arithmetic. The natural question is

- Let $\mathfrak{G}$ be an infinite Abelian group of the finite exponent. Can elementary arithmetic be interpreted in the algebra of finite subsets of $\mathfrak{G}$.

Another problem is generalizing this result to non-Abelian groups. For groups with an element of infinite order, this can be done easily. Indeed, let a be an element of a group. Then, the center of the centralizer of a is an Abelian group containing all a^n. This can be expressed in $\exp \mathfrak{G}$:

$$C(x, y) \equiv K_1(x) \wedge xy = yx; \quad Z(x, y) \equiv C(x, y) \wedge (\forall z)(C(x, z) \to yz = zy).$$

Thus, the formula $Z(\{0, a\}, y)$ is true for all $y \subseteq \{0, a\}^n$. Now we can use results from [8].

But such a method can't be used for torsion groups because proofs of claims in Section 6 significantly use commutativity. Hence, the next question is

- Let $\mathfrak{G}$ be an infinite torsion group. Can elementary arithmetic be interpreted in the algebra of finite subsets of $\mathfrak{G}$.

Funding: This research is funded by Russian Foundation for Fundamental Investigations (RFFI), grant number 20-01-00435.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The author declares no conflict of interest.

References

1. Codd, E.F. A relational model for large shared data banks. *Commun. ACM* **1970**, *13*, 377–387.
2. Kanellakis, P.C.; Kuper, G.M.; Revesz, P.Z. Constraint Query Languages. *J. Comput. Syst. Sci.* **1995**, *51*, 26–52.
3. Kanel'-Belov, A.Y.; Chilikov, A.A. On the Algorithmic Undecidability of the Embeddability Problem for Algebraic Varieties over a Field of Characteristic Zero. *Math Notes* **2019**, *106*, 299–302.
4. Poonen, B.; Shlapentokh, A. Diophantine definability of infinite discrete nonarchimedean sets and Diophantine models over large subrings of number field. *J. Reine Angew. Math.* **2005**, *588*, 27–47.
5. Hopcroft, J.E.; Motwani, R.; Ullman, J.D. *Introduction to Automata Theory, Languages, and Computation*, 3rd ed.; Pearson Education Limited: Harlow, UK, 2013.
6. Brough, T.; Cain, A.J. Automaton semigroup constructions. *Semigroup Forum* **90**, *3*, 763–774.
7. Dudakov, S.M.; Karlov, B.N. On Decidability of Theories of Regular Languages. *Theory Comput. Syst.* **2021**, *65*, 462–478.
8. Dudakov, S.M. On Undecidability of Subset Theory for Some Monoids. *J. Phys. Conf. Ser.* **2021**, *1902*, 012060.
9. Dudakov, S.M. On theory of finite subsets monoid for one torsion Abelian group. *Vestn. TVGU. Seriya Prikl. Mat. [Her. Tver State Univ. Ser. Appl. Math.]* **2021**, *2*, 39–55. (In Russian)
10. Balandraud, E.; Girard, B.; Griffiths, S.; Hamidoune, Y. Subset sums in abelian groups. *Eur. J. Comb.* **2013**, *34*, 1269–1286.
11. Kosters, M. The subset sum problem for finite abelian groups. *J. Comb. Theory Ser. A* **2013**, *120*, 527–530.
12. Cormen, T.H.; Leiserson, C.E.; Rivest, R.L.; Stein, C. *Introduction to Algorithms*, 3rd ed.; The MIT Press: Cambridge, CA, USA, 2009.
13. Boolos, G.S.; Burgess, J.P.; Jeffrey, R.C. *Computability and Logic*, 5th ed.; Cambridge University Press: New York, NY, USA, 2007.
14. Karlov, B.N. On elementary equivalence of some unoids and unoids of their subsets. *Vestn. TVGU. Seriya Prikl. Mat. [Her. Tver State Univ. Ser. Appl. Math.]* **2021**, *3*, 18–32. (In Russian)
15. Place, T.; Zeitoun, M. Separating Regular Languages with First-Order Logic. *Log. Methods Comput. Sci.* **2016**, *12*. Available online: https://doi.org/10.2168/LMCS-12(1:5)2016 (accessed on 6 February 2022).