ISSN 2070-0466, p-Adic Numbers, Ultrametric Analysis and Applications, 2017, Vol. 9, No. 4, pp. 257–281. © Pleiades Publishing, Ltd., 2017.

RESEARCH ARTICLES

Polyadic Integer Numbers and Finite (m,n)-Fields*

Steven Duplij**

Mathematisches Institute, Universität Münster, Einsteinstr. 62, D-48149 Münster, Deutschland

Received July 14, 2017

Abstract—The polyadic integer numbers, which form a polyadic ring, are representatives of a fixed congruence class. The basics of polyadic arithmetic are presented: prime polyadic numbers, the polyadic Euler function, polyadic division with a remainder, etc. are introduced. Secondary congruence classes of polyadic integer numbers, which become ordinary residue classes in the "binary limit", and the corresponding finite polyadic rings are defined. Polyadic versions of (prime) finite fields are introduced. These can be zeroless, zeroless and nonunital, or have several units; it is even possible for all of their elements to be units. There exist non-isomorphic finite polyadic fields of the same arity shape and order. None of the above situations is possible in the binary case. It is conjectured that a finite polyadic field should contain a certain canonical prime polyadic field, defined here, as a minimal finite subfield, which can be considered as a polyadic analogue of $GF(p)$.

DOI: 10.1134/S2070046617040021

Key words: *finite field, polyadic ring, (m.n)-field, polyadic integer numbers, Galois field, congruence class.*

1. INTRODUCTION

The theory of finite fields [1] plays a very important role. From one side, it acts as a "gluing particle" connecting algebra, combinatorics and number theory (see, e.g. [2]), and from another it has numerous applications to "reality": in coding theory, cryptography and computer science [3]. Therefore, any generalization or variation of its initial statements can lead to interesting and useful consequences for both of the above. There are two principal peculiarities of finite fields: 1) Uniqueness - they can have only special numbers of elements (the order is any power of a prime integer p^r) and this fully determines them, in that all finite fields of the same order are isomorphic; 2) Existence of their "minimal" (prime) finite subfield of order p, which is isomorphic to the congruence class of integers $\mathbb{Z}/p\mathbb{Z}$. Investigation of the latter is a bridge to the study of all finite fields, since they act as building blocks of the extended (that is, all) finite fields.

We propose a special - polyadic - version of the (prime) finite fields in such a way that, instead of the binary ring of integers $\mathbb{Z}$, we consider a polyadic ring. The concept of the polyadic integer numbers $\mathbb{Z}_{(m,n)}$ as representatives of a fixed congruence class, which form the (m,n)-ring (with m-ary addition and n-ary multiplication), was introduced in [4]. Here we analyze $\mathbb{Z}_{(m,n)}$ in more detail, by developing elements of a polyadic analog of binary arithmetic: polyadic prime numbers, polyadic division with a remainder, the polyadic Euler totient function, etc. ... It is important to stress that the polyadic integer numbers are special variables (we use superscripts for them) which in general have no connection with ordinary integers (despite the similar notation used in computations), because the former satisfy different relations, and coincide with the latter in the binary case only. Next we will define new secondary congruence classes and the corresponding finite (m,n)-rings $\mathbb{Z}_{(m,n)}(q)$ of polyadic integer numbers, which give $\mathbb{Z}/q\mathbb{Z}$ in the "binary limit". The conditions under which these rings become fields are given, and the corresponding "abstract" polyadic fields are defined and classified using their idempotence polyadic order. They have unusual properties, and can be zeroless, zeroless-nonunital or

*The text was submitted by the author in English.

**E-mail: duplijs@math.uni-muenster.de

have several units, and it is even possible for all elements to be units. The subgroup structure of their (cyclic) multiplicative finite n-ary group is analyzed in detail. For some zeroless finite polyadic fields their multiplicative n-ary group is a non-intersecting union of subgroups. It is shown that there exist non-isomorphic finite polyadic fields of the same arity shape and order. None of the above situations is possible in the binary case.

Some general properties of polyadic rings and fields were given in [5–8], but their concrete examples using integers differ considerably from our construction here, and the latter leads to so called nonderived (proper) versions which have not been considered before.

We conjecture that any (m,n)-field with $m>n$ contains as a subfield one of the prime polyadic fields constructed here, which can be considered as a polyadic analog of $GF(p)$.

2. PRELIMINARIES

We use the notations and definitions from [4, 9] (see, also, references therein). We recall (only for self-consistency) some important elements and facts about polyadic rings, which will be needed below.

Informally, a polyadic (m,n)-ring is $\mathcal{R}_{m,n}=\langle R \mid \boldsymbol{\nu}_m, \boldsymbol{\mu}_n\rangle$, where R is a set, equipped with m-ary addition $\boldsymbol{\nu}_m : R^m \to R$ and n-ary multiplication $\boldsymbol{\mu}_n : R^n \to R$ which are connected by the polyadic distributive law, such that $\langle R \mid \boldsymbol{\nu}_m\rangle$ is a commutative m-ary group and $\langle R \mid \boldsymbol{\mu}_n\rangle$ is a semigroup. A *commutative (cancellative) polyadic ring* has a commutative (cancellative) n-ary multiplication $\boldsymbol{\mu}_n$. A polyadic ring is called *derived*, if $\boldsymbol{\nu}_m$ and $\boldsymbol{\mu}_n$ are equivalent to a repetition of the binary addition and multiplication, while $\langle R \mid +\rangle$ and $\langle R \mid \cdot\rangle$ are commutative (binary) group and semigroup respectively. If only one operation $\boldsymbol{\nu}_m$ (or $\boldsymbol{\mu}_n$) has this property, we call such a $\mathcal{R}_{m,n}$ *additively* (or *multiplicatively*) derived (*half-derived*).

In distinction to binary rings, an *n-admissible* "length of word $(\boldsymbol{x})$" should be congruent to $1 \bmod (n-1)$, containing $\ell_\mu(n-1)+1$ elements (ℓ_μ is a "number of multiplications") $\boldsymbol{\mu}_n^{(\ell_\mu)}[\boldsymbol{x}]$ ($\boldsymbol{x}\in R^{\ell_\mu(n-1)+1}$), so called $(\ell_\mu(n-1)+1)$-ads, or *polyads*. An *m-admissible* "quantity of words $(\boldsymbol{y})$" in a polyadic "sum" has to be congruent to $1 \bmod (m-1)$, i.e. consisting of $\ell_\nu(m-1)+1$ summands (ℓ_ν is a "number of additions") $\boldsymbol{\nu}_m^{(\ell_\nu)}[\boldsymbol{y}]$ ($\boldsymbol{y}\in R^{\ell_\nu(m-1)+1}$). Therefore, a straightforward "polyadization" of any binary expression ($m=n=2$) can be introduced as follows: substitute the number of multipliers $\ell_\mu+1\to\ell_\mu(n-1)+1$ and number of summands $\ell_\nu+1\to\ell_\nu(m-1)+1$, respectively.

An example of "trivial polyadization" is the simplest (m,n)-ring derived from the ring of integers $\mathbb{Z}$ as the set of $\ell_\nu(m-1)+1$ "sums" of n-admissible $(\ell_\mu(n-1)+1)$-ads $(\boldsymbol{x})$, where $\boldsymbol{x}\in\mathbb{Z}^{\ell_\mu(n-1)+1}$ [6].

The additive m-ary *polyadic power* and the multiplicative *n-ary polyadic power* are defined by (inside polyadic products we denote repeated entries by $\overbrace{x,\ldots,x}^{k}$ as x^k)

$$x^{\langle\ell_\nu\rangle_{+m}}=\boldsymbol{\nu}_m^{(\ell_\nu)}\left[x^{\ell_\nu(m-1)+1}\right],\quad x^{\langle\ell_\mu\rangle_{\times n}}=\boldsymbol{\mu}_n^{(\ell_\mu)}\left[x^{\ell_\mu(n-1)+1}\right],\ x\in R, \tag{2.1}$$

such that the polyadic powers and ordinary powers differ by one: $x^{\langle\ell_\nu\rangle_{+2}}=x^{\ell_\nu+1}$, $x^{\langle\ell_\mu\rangle_{\times 2}}=x^{\ell_\mu+1}$.

The *polyadic idempotents* in $\mathcal{R}_{m,n}$ satisfy

$$x^{\langle\ell_\nu\rangle_{+m}}=x,\quad x^{\langle\ell_\mu\rangle_{\times n}}=x, \tag{2.2}$$

and are called the *additive ℓ_ν-idempotent* and the *multiplicative ℓ_μ-idempotent*, respectively.

The additive 1-idempotent, the *zero* $z\in R$, is (if it exists) defined by

$$\boldsymbol{\nu}_m[\boldsymbol{x},z]=z,\quad \forall\boldsymbol{x}\in R^{m-1}. \tag{2.3}$$

An element $x\in R$ is called (polyadic) *nilpotent*, if $x^{\langle 1\rangle_{+m}}=z$, and all higher powers of a nilpotent element are nilpotent, as follows from (2.3) and associativity.

The *unit* e of $\mathcal{R}_{m,n}$ is a multiplicative 1-idempotent which is defined (if it exists) as

$$\boldsymbol{\mu}_n\left[e^{n-1},x\right]=x,\quad \forall x\in R, \tag{2.4}$$

where (in case of a noncommutative polyadic ring) x can be on any place. An element $x \in R$ is called a (polyadic) ℓ_μ-*reflection*, if $x^{\langle \ell_\mu \rangle \times n} = e$ (multiplicative analog of a nilpotent element).

Polyadic rings with zero or unit(s) are called additively or multiplicatively *half-derived*, and derived rings have a zero and unit(s) simultaneously. There are polyadic rings which have no unit and no zero, or with several units and no zero, or where all elements are units. But if a zero exists, it is unique. If a polyadic ring contains no unit and no zero, we call it a *zeroless nonunital polyadic ring*. It is obvious that zeroless nonunital rings can contain other idempotents of higher polyadic powers.

So, in polyadic rings (including the zeroless nonunital ones) invertibility can be governed in a way which is not connected with unit and zero elements. For a fixed element $x \in R$ its *additive querelement* $\tilde{x}$ and *multiplicative querelement* $\bar{x}$ are defined by

$$\boldsymbol{\nu}_m \left[x^{m-1}, \tilde{x}\right] = x, \qquad \boldsymbol{\mu}_n \left[x^{n-1}, \bar{x}\right] = x, \tag{2.5}$$

where in the second equation, if the n-ary multiplication $\boldsymbol{\mu}_n$ is noncommutative, $\bar{x}$ can be on any place. Because $\langle R \mid \boldsymbol{\nu}_m \rangle$ is a commutative group, each $x \in R$ has its additive querelement $\tilde{x}$ (and is *querable* or "polyadically invertible"). The n-ary semigroup $\langle R \mid \boldsymbol{\mu}_n \rangle$ can have no multiplicatively querable elements at all. However, if every $x \in R$ has its unique querelement, then $\langle R \mid \boldsymbol{\mu}_n \rangle$ is an n-ary group. Obviously, that n-ary group cannot have nilpotent elements, but can have ℓ_μ-reflections. Denote $R^* = R \setminus \{z\}$, if the zero z exists. If $\langle R^* \mid \boldsymbol{\mu}_n \rangle$ is the n-ary group, then $\mathcal{R}_{m,n}$ is a (m,n)-*division ring*.

Definition 2.1. *A commutative (m,n)-division ring $\mathcal{R}_{m,n}$ is a (m,n)-field $\mathcal{F}_{m,n}$.*

The simplest example of a (m,n)-field derived from $\mathbb{R}$ is the set of $\ell_\nu\,(m-1)+1$ "sums" of admissible $(\ell_\mu\,(n-1)+1)$-ads $(\boldsymbol{x})$, where $\boldsymbol{x} \in \mathbb{R}^{\ell_\mu(n-1)+1}$. Some *nonderived* (m,n)-fields are in

Example 2.2. ***a)*** *The set $i\mathbb{R}$ with $i^2 = -1$ is a $(2,3)$-field with a zero and no unit (operations are made in $\mathbb{C}$), but the multiplicative querelement of ix is $-i/x$ $(x \neq 0)$.*

b) *The set of fractions $\left\{ix/y \mid x, y \in \mathbb{Z}^{odd},\ i^2 = -1\right\}$ is a $(3,3)$-field with no zero and no unit (operations are in $\mathbb{C}$), while the additive and multiplicative querelements of ix/y are $-ix/y$ and $-iy/x$, respectively.*

c) *The set of antidiagonal 2×2 matrices over $\mathbb{R}$ is a $(2,3)$-field with zero $z = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ and two units $e = \pm \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, but the unique querelement of $\begin{pmatrix} 0 & x \\ y & 0 \end{pmatrix}$ is $\begin{pmatrix} 0 & 1/y \\ 1/x & 0 \end{pmatrix}$.*

3. RING OF POLYADIC INTEGER NUMBERS

Recall the notion of the ring of polyadic integer numbers $\mathbb{Z}_{(m,n)}$ which was introduced in [4], where its difference from the (m,n)-ring of integers from [6] was outlined.

Let us consider a congruence class (residue class) of an integer a modulo b

$$[[a]]_b = \{\{a + bk\} \mid k \in \mathbb{Z},\ \ a \in \mathbb{Z}_+,\ b \in \mathbb{N},\ 0 \leq a \leq b-1\}\,. \tag{3.1}$$

We denote a representative element by $x_k = x_k^{[a,b]} = a + bk$, where obviously $\{x_k\}$ is an infinite set.

3.1. External and Internal Operations for Congruence Classes

Informally, there are two ways to equip (3.1) with operations:

1) The "External" way is to define (*binary*) operations between the congruence classes. Let us define on the finite underlying set of b congruence classes $\{[[a]]_b\}$, $a = 0, 1, \ldots, b-1$ the following new binary operations (here, if b is fixed, and we denote the binary class representative by an integer with *one* prime $[[a]]_b \equiv a'$, as well as the corresponding binary operations $+', \cdot'$ between classes)

$$a'_1 +' a'_2 = (a_1 + a_2)', \tag{3.2}$$

$$a'_1 \cdot' a'_2 = (a_1 a_2)'. \tag{3.3}$$

Then, the binary *residue class ring* is defined by

$$\mathbb{Z}/b\mathbb{Z} = \left\{\{a'\} \mid +', \cdot', 0', 1'\right\}. \tag{3.4}$$

In the case of prime $b = p$, the ring $\mathbb{Z}/p\mathbb{Z}$ becomes a *binary* finite field having p elements.

2) The "Internal" way is to introduce (*polyadic*) operations inside a given class $[[a]]_b$ (with *both* a and b fixed). We introduce the commutative m-ary addition and commutative n-ary multiplication of representatives x_{k_i} of the fixed congruence class by

$$\nu_m [x_{k_1}, x_{k_2}, \ldots, x_{k_m}] = x_{k_1} + x_{k_2} + \ldots + x_{k_m}, \tag{3.5}$$

$$\mu_n [x_{k_1}, x_{k_2}, \ldots, x_{k_n}] = x_{k_1} x_{k_2} \ldots x_{k_n}, \quad x_{k_i} \in [[a]]_b, \; k_i \in \mathbb{Z}. \tag{3.6}$$

In general, the binary sums $x_{k_1} + x_{k_2}$ and products $x_{k_1} x_{k_2}$ are not in $[[a]]_b$.

Proposition 3.1 ([4]). *The polyadic operations ν_m and μ_n become closed in $[[a]]_b$, if the arities (m, n) have the minimal values satisfying*

$$ma \equiv a \,(\mathrm{mod}\, b), \tag{3.7}$$

$$a^n \equiv a \,(\mathrm{mod}\, b). \tag{3.8}$$

Polyadic distributivity is inherited from that of $\mathbb{Z}$, and therefore we have

Definition 3.2 ([4]). *The congruence class $[[a]]_b$ equipped with a structure of nonderived infinite commutative polyadic ring is called a (m, n)-ring of polyadic integer numbers*

$$\mathbb{Z}_{(m,n)} \equiv \mathbb{Z}^{[a,b]}_{(m,n)} = \{[[a]]_b \mid \nu_m, \mu_n\}. \tag{3.9}$$

Obviously, $\mathbb{Z}_{(m,n)}$ (as in the binary case) cannot become a polyadic field with any choice of parameters.

Example 3.3. *In the residue class*

$$[[3]]_4 = \{\ldots -25, -21, -17, -13, -9, -5, -1, 3, 7, 11, 15, 19, 23, 27, 31, 35, 39 \ldots\} \tag{3.10}$$

we can add only $4\ell_\nu + 1$ representatives and multiply $2\ell_\mu + 1$ representatives (ℓ_ν, ℓ_μ are "numbers" of m-ary additions and n-ary multiplications respectively) to retain the same class, e.g., take $\ell_\nu = 2$, $\ell_\mu = 3$ to get $(7 + 11 + 15 + 19 + 23) - 5 - 9 - 13 - 1 = 47 \in [[3]]_4$, $((7 \cdot 3 \cdot 11) \cdot 19 \cdot 15) \cdot 31 \cdot 27 = 55\,103\,895 \in [[3]]_4$. Obviously, we cannot add and multiply arbitrary quantities of numbers in $[[3]]_4$, only the admissible ones. This means that $[[3]]_4$ is the polyadic $(5, 3)$-ring $\mathbb{Z}_{(5,3)} = \mathbb{Z}^{[3,4]}_{(5,3)}$.

Remark 3.4. *After imposing the operations (3.5)–(3.6) the representatives $x^{[a,b]}_k$ become abstract variables (elements of the corresponding (m, n)-ring or polyadic integer numbers) which are not ordinary integers (forming a $(2, 2)$-ring), but have the latter as their "binary limit". So in computations the integral numbers (denoting representatives) should carry their arity shape (m, n) as additional indices. Indeed, the representative, e.g. $3 = 3_{(5,3)} \in \mathbb{Z}^{[3,4]}_{(5,3)}$ is different from*

$3 = 3_{(3,2)} \in \mathbb{Z}^{[1,2]}_{(3,2)}$, *i.e. properly speaking* $3_{(5,3)} \neq 3_{(3,2)}$, *since their operations (multiplication and addition) are different, because they belong to different polyadic rings,* $\mathbb{Z}^{[3,4]}_{(5,3)}$ *and* $\mathbb{Z}^{[1,2]}_{(3,2)}$, *respectively. For conciseness, we omit the indices* (m,n), *if their value is clear from the context.*

Thus, at first sight it seems that one can obtain a polyadic field only in the "external" way, i.e. using the "trivial polyadization" of the binary finite field $\mathbb{Z}/p\mathbb{Z}$ (just a repetition of the binary group operations).This leads to the *derived* polyadic finite fields, which have a very simple structure, in which the admissible binary sums and binary products of the congruence classes are used [6]. However, in the next section we propose a new approach, and thereby construct the *nonderived* finite (m,n)-fields of polyadic integer numbers $\mathbb{Z}_{(m,n)}$.

Remark 3.5. *If* $n = b = p$ *is prime, then* (3.8) *is valid for any* $a \in \mathbb{N}$, *which is another formulation of Fermat's little theorem.*

3.2. Prime Polyadic Integer Numbers

Let us introduce a polyadic analog of prime numbers in $\mathbb{Z}_{(m,n)}$. First we need

Definition 3.6. *A polyadically composite (reducible) number is* $x_k \in \mathbb{Z}_{(m,n)}$, *such that the expansion*

$$x_k = \mu_n^{(\ell)}\left[x_{k_1}, x_{k_2}, , x_{k_{\ell(n-1)+1}}\right], \quad x_{k_i} \in \mathbb{Z}_{(m,n)}, \tag{3.11}$$

is unique, where ℓ *is a number of* n*-ary multiplications, and there exist at least one* $x_{k_i} \neq x_k$ *and* $x_{k_i} \neq e$ *(i.e. is not equal to unit of* $\mathbb{Z}_{(m,n)}$, *if it exists). Denote the set of such numbers* $\{x_{k_i}\} = \mathbb{D}(x_k)$ *which is called the composition set of* x_k.

Definition 3.7. *An irreducible polyadic number is* $x_k \in \mathbb{Z}_{(m,n)}$ *cannot be expressed as any (long) polyadic product* (3.11).

Proposition 3.8. *In the polyadic ring* $\mathbb{Z}^{[a,b]}_{(m,n)}$ *without the unit the elements satisfying*

$$-|a-b|^n < x_k < |a-b|^n \tag{3.12}$$

are irreducible.

Proof. Since $0 \leq a \leq b-1$, the minimal absolute value of an element $x_k \in \mathbb{Z}^{[a,b]}_{(m,n)}$ is $|a-b|$. The minimum of its n-ary product is $|a-b|^n$, and therefore smaller elements cannot be decomposed. □

Example 3.9. *In the* $(6,5)$*-ring* $\mathbb{Z}^{[8,10]}_{(6,5)}$ *all polyadic integer numbers are even, and there is no unit, and so they are binary composite*

$$\mathbb{Z}^{[8,10]}_{(6,5)} = \{\ldots -72, -62, -52, -42, -32, -22, -12, -2, 8, 18, 28, 38, 48, 58, \ldots\} \tag{3.13}$$

Nevertheless, the lowest elements, e.g. $\{-22, -12, 8, 18, 28\}$, *are irreducible, while the smallest (by absolute value) polyadically composite element is* $(-32) = \mu_5\left[(-2)^5\right]$.

Definition 3.10. *A range in which all elements are indecomposable is called a polyadic irreducible gap.*

Remark 3.11. *We do not demand positivity, as in the binary case, because polyadic integer numbers* $\mathbb{Z}^{[a,b]}_{(m,n)}$ (3.9) *are "symmetric" not with respect to* $x = 0$, *but under* $x = x_{k=0} = a$.

The polyadic analog of binary prime numbers plays an intermediate role between composite and irreducible elements.

Definition 3.12. *A polyadic prime number is $x_{k_p} \in \mathbb{Z}_{(m,n)}$, such that it obeys only the unique expansion*

$$x_{k_p} = \mu_n^{(\ell)}\left[x_{k_p}, e^{\ell(n-1)}\right], \tag{3.14}$$

where e a polyadic unit of $\mathbb{Z}_{(m,n)}$ (if exists).

So, the polyadic prime numbers can appear only in those polyadic rings $\mathbb{Z}_{(m,n)}^{[a,b]}$ which contain units. In [4] (**Proposition 6.15**) it was shown that such rings correspond to the *limiting congruence classes* $[[1]]_b$ and $[[b-1]]_b$, and indeed only for them can $a+bk = 1 \bmod b$, and $e^{\ell(n-1)}$ can be a neutral sequence (for $e=1$ always, while for $e=-1$ only when $\ell(n-1)$ is even).

Proposition 3.13. *The prime polyadic numbers can exist only in the limiting polyadic rings $\mathbb{Z}_{(b+1,2)}^{[1,b]}$ and $\mathbb{Z}_{(b+1,3)}^{[b-1,b]}$.*

Proof. The equation $a+bk = 1 \bmod b$ (for $0 \le a \le b-1$) has two solutions: $a=1$ and $a=b-1$ corresponding for two limiting congruence classes $[[1]]_b$ and $[[b-1]]_b$, which correspond to

$$x_k^+ = bk+1, \tag{3.15}$$

$$x_k^- = b(k+1)-1, \quad k \in \mathbb{Z}. \tag{3.16}$$

The parameters-to-arity mapping (3.41) fixes their multiplication arity to $n=2$ and $n=3$ respectively, which gives manifestly

$$\mu_2\left[x_{k_1}^+, x_{k_2}^+\right] = x_k^+, \qquad k = bk_1k_2 + k_1 + k_2, \tag{3.17}$$

$$\mu_3\left[x_{k_1}^-, x_{k_2}^-, x_{k_3}^-\right] = x_k^-, \quad k, k_i \in \mathbb{Z}, \quad i = 1,2,3, \qquad b \in \mathbb{N},$$

$$k = b^2k_1k_2k_3 + (b-1)\left[b\left(k_1k_2 + k_2k_3 + k_1k_3\right) + (b-1)\left(k_1+k_2+k_3\right) + (b-2)\right]. \tag{3.18}$$

Therefore, for $\mathbb{Z}_{(b+1,2)}^{[1,b]}$ we have the unit $e = x_{k=0}^+ = 1$ (which is obvious for the binary multiplication), while in $\mathbb{Z}_{(b+1,3)}^{[b-1,b]}$ the unit is $e = x_{k=-1}^- = -1$ ($b \ge 3$), and the sequence is $\left(e^2\right)$ is evidently neutral. □

Denote the set of ordinary *binary prime numbers* in the interval $1 \le k \le k_{\max}$ by $\mathbb{P}(k_{\max})$, $k_{\max} \in \mathbb{N}$. The set of *prime polyadic numbers* for the polyadic ring $\mathbb{Z}_{(m,n)}^{[a,b]}$ in the interval $x_{-k_{\max}} \le x_k \le x_{k_{\max}}$ is denoted by $\mathbb{P}_{(m,n)}^{[a,b]}(k_{\max})$. Obviously, in the binary limit $\mathbb{P}_{(2,2)}^{[0,1]}(k_{\max}) = \mathbb{P}(k_{\max}) \cup \{-\mathbb{P}(k_{\max})\}$. Nevertheless, prime polyadic numbers can be composite as binary numbers.

Assertion 3.14. The set of prime polyadic numbers in the interval $x_{-k_{\max}} \le x_k \le x_{k_{\max}}$ for $\mathbb{Z}_{(m,n)}^{[a,b]}$ can contain composite binary numbers, i.e.

$$\Delta\mathbb{P}_{(m,n)}^{[a,b]}(k_{\max}) = \mathbb{P}_{(m,n)}^{[a,b]}(k_{\max}) \setminus \left\{\left\{\mathbb{P}\left(x_{k_{\max}}\right) \cup \left\{\mathbb{P}\left(-x_{-k_{\max}}\right)\right\}\right\} \cap [[a]]_b\right\} \ne \varnothing. \tag{3.19}$$

Definition 3.15. ***1)*** *The cardinality of the set of ordinary binary prime numbers $\mathbb{P}(k_{\max})$ is called a prime-counting function and denoted by $\pi(k_{\max}) = |\mathbb{P}(k_{\max})|$.*

2) *The cardinality of the set of prime polyadic numbers $\mathbb{P}_{(m,n)}^{[a,b]}(k_{\max})$ is called a polyadic prime-counting function and denoted by*

$$\pi_{(m,n)}^{[a,b]}(k_{\max}) = \left|\mathbb{P}_{(m,n)}^{[a,b]}(k_{\max})\right|. \tag{3.20}$$

Example 3.16. ***1)*** *Consider* $\mathbb{Z}_{(45,3)}^{[43,44]}$ *and* $k_{\max}=2$*, then*

$$\mathbb{P}_{(45,3)}^{[43,44]}(2)=\{-45,-1,43,87,131\}, \tag{3.21}$$

$$\Delta\mathbb{P}_{(45,3)}^{[43,44]}(2)=\{-45\}, \quad \pi_{(45,3)}^{[43,44]}(2)=5. \tag{3.22}$$

2) *For* $\mathbb{Z}_{(52,3)}^{[50,51]}$ *and* $k_{\max}=5$ *we have*

$$\mathbb{P}_{(52,3)}^{[50,51]}(5)=\{-205,-154,-103,-52,-1,50,101,152,203,254,305\}, \tag{3.23}$$

$$\Delta\mathbb{P}_{(52,3)}^{[50,51]}(5)=\{-205,-154,-52,50,152,203,254,305\}, \ \ \pi_{(52,3)}^{[50,51]}(5)=11. \tag{3.24}$$

Remark 3.17. *This happens because in* $\mathbb{Z}_{(m,n)}^{[a,b]}$ *the role of "building blocks" (prime polyadic numbers) is played by those* x_k *which cannot be presented as a (long) ternary product of other polyadic integer numbers from the same* $\mathbb{Z}_{(m,n)}^{[a,b]}$ *as in* (3.11)*, but which satisfy* (3.14) *only. Nevertheless, such prime polyadic numbers can be composite binary prime numbers.*

In general, for the limiting cases, in which polyadic prime numbers exist, we have

Proposition 3.18. ***1)*** *In* $\mathbb{Z}_{(b+1,2)}^{[1,b]}$ *the "smallest" polyadic integer numbers satisfying*

$$-b<k_p<b+2, \tag{3.25}$$

$$1-b^2<x_{k_p}<(b+1)^2, \tag{3.26}$$

are not decomposable, and therefore such $x_{k_p}\in\mathbb{Z}_{(b+1,2)}^{[1,b]}$ *are all polyadic prime numbers.*

2) *For another limiting case* $\mathbb{Z}_{(b+1,3)}^{[b-1,b]}$ *the polyadic integer numbers satisfying*

$$1-b<k_p<b-1, \tag{3.27}$$

$$-(b-1)^2<x_{k_p}<b^2-1, \tag{3.28}$$

are not ternary decomposable and so all such $x_{k_p}\in\mathbb{Z}_{(b+1,2)}^{[b-1,b]}$ *are polyadic prime numbers.*

Proof. This follows from determining the maximum of the negative values and the minimum of the positive values of the functions x_k^+ and x_k^- in (3.17)–(3.18). □

Definition 3.19. *The range in which all elements are polyadically prime numbers is called the polyadic primes gap, and for the two limiting cases it is given by* (3.26) *and* (3.28)*, respectively.*

For instance, in $\mathbb{Z}_{(52,3)}^{[50,51]}$ for the polyadic primes gap we have $-2500<x_{k_p}<2600$: all such polyadic integer numbers are polyadically prime, but there are many composite binary numbers among them.

In the same way we can introduce a polyadic analog of the *Euler (totient) function* which in the binary case counts the number of coprimes to a given natural number. Denote the set of ordinary binary numbers $k>1$ which are *coprime* to $k_{\max}\in\mathbb{N}$ by $\mathbb{S}(k_{\max})$ (named totatives of $k_{\max}$). Then, the cardinality of $\mathbb{S}(k_{\max})$ is defined as Euler function $\varphi(k_{\max})=|\mathbb{S}(k_{\max})|$. Obviously, if $k_{\max}=p$ is prime, then $\varphi(p)=p-1$. The notion of coprime numbers is based on the divisors: the coprime numbers k_1 and k_2 have the greatest common divisor $\gcd(k_1,k_2)=1$. In the polyadic case it is not so straightforward, and we need to start from the basic definitions.

First, we observe that in a (commutative) polyadic ring $\mathcal{R}_{m,n}=\{R\mid\nu_m,\mu_n\}$ the analog of the division operation is usually not defined *uniquely*, which makes it useless for real applications. Indeed, y divides x, where $x,y\in R$, if there exists a sequence $\boldsymbol{z}\in R^{n-1}$ of length $(n-1)$, such that $x=\mu_n[y,\boldsymbol{z}]$. To be consistent with the ordinary integer numbers $\mathbb{Z}$, we demand in the polyadic number ring $\mathbb{Z}_{(m,n)}$: **1)** *Uniqueness* of the result; **2)** i.e. only *one* polyadic number (not a sequence) as the result. This naturally leads to

Definition 3.20. *A polyadic number (quotient) x_{k_2} polyadically divides a polyadic number (dividend) x_{k_1}, if there exists $x_{k_q} := x_{k_1} \div_p x_{k_2}$, called the (unique) result of division, such that*

$$x_{k_1} = \mu_n \left[x_{k_2}, \left(x_{k_q}\right)^{n-1} \right], \qquad x_{k_1}, x_{k_2}, x_{k_q} \in \mathbb{Z}_{(m,n)}. \tag{3.29}$$

Remark 3.21. *For polyadic prime numbers (3.14) the only possibility for the quotient is $x_{k_2} = x_{k_1}$ such that $x_{k_1} = \mu_n \left[x_{k_1}, (e)^{n-1} \right]$ or $x_{k_1} \div_p x_{k_1} = e$, where e is the unit of $\mathbb{Z}_{(m,n)}$.*

Assertion 3.22. Polyadic division is distributive from the left

$$\nu_m \left[x_{k_1}, x_{k_2}, \ldots, x_{k_m} \right] \div_p x_k = \nu_m \left[\left(x_{k_1} \div_p x_k \right), \left(x_{k_2} \div_p x_k \right), \ldots, \left(x_{k_m} \div_p x_k \right) \right], \tag{3.30}$$

but not distributive from the right.

Proof. This follows from the polyadic distributivity in the (m,n)-ring $\mathbb{Z}_{(m,n)}$. □

Example 3.23. ***1)*** *In the polyadic ring $\mathbb{Z}_{(10,4)}^{[4,9]}$ we have uniquely $x_{28} \div_p x_4 = x_4$ or $256 \div_p 4 = 4$.*

2) *For the limiting ring $\mathbb{Z}_{(5,3)}^{[3,4]}$, we find $x_{43} \div_p x_1 = x_{-2}$ or $175 \div_p 7 = -5$.*

In the same way we define a polyadic analog of division with a remainder.

Definition 3.24. *A polyadic division with a remainder is defined, if for a polyadic dividend x_{k_1} and divisor x_{k_2} there exists a polyadic remainder x_{k_r} such that*

$$x_{k_1} = \nu_m \left[\mu_n \left[x_{k_2}, \left(x_{k_q}\right)^{n-1} \right], \left(x_{k_r}\right)^{m-1} \right], \qquad x_{k_1}, x_{k_2}, x_{k_q}, x_{k_r} \in \mathbb{Z}_{(m,n)}, \tag{3.31}$$

which is denoted by $x_{k_r} = x_{k_1} \bmod_p x_{k_2}$, and (3.31) can be presented in the following binary form

$$x_{k_1} = \left(x_{k_2} \boxdot_p x_{k_q} \right) \boxplus_p x_{k_r}. \tag{3.32}$$

The distributivity of these operations is governed by distributivity in the polyadic ring $\mathbb{Z}_{(m,n)}$.

Example 3.25. *In the polyadic ring $\mathbb{Z}_{(6,5)}^{[8,10]}$ we can have different divisions for the same dividend as $38 = ((-22) \boxdot_p (-2)) \boxplus_p 78 = ((-92) \boxdot_p (-2)) \boxplus_p 238$.*

Secondly, because divisibility in the polyadic case is not symmetric with respect to dividend and divisor (3.29), we define polyadically coprime numbers using the definition of compositeness (3.11).

Definition 3.26. *The s polyadic integer numbers $x_{k_1}, \ldots, x_{k_s} \in \mathbb{Z}_{(m,n)}$ are polyadically coprime, if their composition sets do not intersect $\mathbb{D}(x_{k_1}) \cap \mathbb{D}(x_{k_1}) \cap \ldots \cap \mathbb{D}(x_{k_s}) = \varnothing$.*

It is important that this definition does not imply the existence of a unit in $\mathbb{Z}_{(m,n)}$, as opposed to the definition of the polyadic prime numbers (3.14) in which the availability of a unit is crucial.

Assertion 3.27. Polyadically coprime numbers can exist in any polyadic ring $\mathbb{Z}_{(m,n)}$, and *not* only in the limiting cases with unit (see **Proposition 3.13**).

Corollary 3.28. *All elements in the polyadic irreducible gap are polyadically coprime.*

Example 3.29. *In $\mathbb{Z}_{(6,5)}^{[8,10]}$ (3.13) the polyadic integer numbers $(-32) = \mu_5 \left[(-2)^5 \right]$ and $32768 = \mu_5 \left[(8)^5 \right]$ are both composed, but polyadically coprime, because the composition sets $\mathbb{D}(-32) = \{-2\}$ and $\mathbb{D}(32768) = \{8\}$ do not intersect. Alternatively, not polyadically coprime numbers here are, e.g., $(-3072) = \mu_5 \left[(-12), (-2)^2, (8)^2 \right]$ and $(-64512) = \mu_5 \left[-2, (8)^2, 18, 28 \right]$, because $\mathbb{D}(-3072) \cap \mathbb{D}(-64512) = \{-2, 8\} \neq \varnothing$. We cannot multiply these two numbers, because the arity of multiplication is 5.*

Remark 3.30. *For polyadic integer numbers $\mathbb{Z}_{(m,n)}$ we cannot measure the property "to be coprime" in terms of a single element, as in binary case, by their* gcd*, because the n-ary multiplication is only allowed for admissible sequences. Therefore, we need to consider the intersection of the composition sets.*

In the polyadic ring $\mathbb{Z}^{[a,b]}_{(m,n)}$ for a given $k_{\max} \in \mathbb{Z}_+$ we denote by $\mathbb{S}^{[a,b]}_{(m,n)}(k_{\max})$ the set of polyadic prime numbers $x_k \in \mathbb{Z}^{[a,b]}_{(m,n)}$ which are polyadically coprime to $x_{k_{\max}}$ and $x_{-k_{\max}}$ in the open interval $x_{-k_{\max}} < x_k < x_{k_{\max}}$ (we assume that, if two numbers are coprime, then their opposite numbers are also coprime). For the binary limit, obviously, $\mathbb{S}^{[0,1]}_{(2,2)}(k_{\max}) = \mathbb{S}(k_{\max}) \cup \{-\mathbb{S}(k_{\max})\}$.

Definition 3.31. *The cardinality of $\mathbb{S}^{[a,b]}_{(m,n)}(k_{\max})$ is called a polyadic Euler function denoted by*

$$\varphi^{[a,b]}_{(m,n)}(k_{\max}) = \left|\mathbb{S}^{[a,b]}_{(m,n)}(k_{\max})\right|. \tag{3.33}$$

In the binary case $\varphi^{[0,1]}_{(2,2)}(k_{\max}) = 2\varphi(k_{\max})$. Because of *Remark* **3.30**, the computation of the polyadic Euler function requires for each element in the range $x_{-k_{\max}} < x_k < x_{k_{\max}}$ a thorough consideration of composition sets.

Example 3.32. ***1)*** *For the limiting polyadic ring $\mathbb{Z}^{[1,29]}_{(30,2)}$ and $k_{\max} = 10$ we have $x_{-10} = -289$, $x_{10} = 291$ and*

$$\mathbb{S}^{[1,29]}_{(30,2)}(10) = \{-260, -202, -173, -115, -86, -28, 1, 59, 88, 146, 175, 233, 262\}, \tag{3.34}$$

$$\varphi^{[1,29]}_{(30,2)}(10) = 13. \tag{3.35}$$

2) *In another limiting case with ternary multiplication $\mathbb{Z}^{[31,32]}_{(33,3)}$ we get $x_{-5} = -129$, $x_5 = 191$ and*

$$\mathbb{S}^{[31,32]}_{(33,3)}(5) = \{-97, -65, -1, 31, 95, 127\}, \tag{3.36}$$

$$\varphi^{[1,29]}_{(30,2)}(5) = 6. \tag{3.37}$$

3) *In the non-limiting case $\mathbb{Z}^{[7,10]}_{(11,5)}$ and $k_{\max} = 10$ we have $x_{-10} = -93$, $x_{10} = 107$ with*

$$\mathbb{S}^{[7,10]}_{(11,5)}(10) = \{-83, -73, -53, -43, -23, -13, 7, 17, 37, 47, 67, 77, 97\}, \tag{3.38}$$

$$\varphi^{[7,10]}_{(11,5)}(10) = 13. \tag{3.39}$$

4) *For the polyadic Euler function in some other non-limiting cases we have*

$$\varphi^{[27,49]}_{(50,15)}(7) = 6, \quad \varphi^{[17,38]}_{(39,10)}(20) = 21, \quad \varphi^{[16,28]}_{(8,4)}(30) = \varphi^{[46,50]}_{(26,6)}(15) = 0. \tag{3.40}$$

3.3. The Parameters-To-Arity Mapping

Let us consider the connection between congruence classes and arities in more detail.

Remark 3.33. *a) Solutions to* (3.7) *and* (3.8) *do not exist simultaneously for all a and b; b) The pair a, b determines m, n uniquely; c) It can occur that for several different pairs a, b there can be the same arities m, n.*

Therefore, we have

Assertion 3.34. The *parameters-to-arity mapping*

$$\psi : (a,b) \longrightarrow (m,n) \tag{3.41}$$

is a partial surjection.

Here we list the lowest arities which can be obtained with different choices of (a,b).

$$\left.\begin{matrix} m=3 \\ n=2 \end{matrix}\right\} : \left(\begin{matrix} a=1 \\ b=2 \end{matrix}\right), \left(\begin{matrix} a=3 \\ b=6 \end{matrix}\right), \left(\begin{matrix} a=5 \\ b=10 \end{matrix}\right), \left(\begin{matrix} a=7 \\ b=14 \end{matrix}\right), \left(\begin{matrix} a=9 \\ b=18 \end{matrix}\right), \left(\begin{matrix} a=11 \\ b=22 \end{matrix}\right), \left(\begin{matrix} a=13 \\ b=26 \end{matrix}\right), \left(\begin{matrix} a=15 \\ b=30 \end{matrix}\right);$$

$$\left.\begin{matrix} m=4 \\ n=2 \end{matrix}\right\} : \left(\begin{matrix} a=1 \\ b=3 \end{matrix}\right), \left(\begin{matrix} a=4 \\ b=6 \end{matrix}\right), \left(\begin{matrix} a=4 \\ b=12 \end{matrix}\right), \left(\begin{matrix} a=10 \\ b=15 \end{matrix}\right), \left(\begin{matrix} a=7 \\ b=21 \end{matrix}\right), \left(\begin{matrix} a=16 \\ b=24 \end{matrix}\right), \left(\begin{matrix} a=10 \\ b=30 \end{matrix}\right), \left(\begin{matrix} a=22 \\ b=33 \end{matrix}\right);$$

$$\left.\begin{matrix} m=4 \\ n=3 \end{matrix}\right\} : \left(\begin{matrix} a=2 \\ b=3 \end{matrix}\right), \left(\begin{matrix} a=2 \\ b=6 \end{matrix}\right), \left(\begin{matrix} a=8 \\ b=12 \end{matrix}\right), \left(\begin{matrix} a=14 \\ b=21 \end{matrix}\right), \left(\begin{matrix} a=8 \\ b=24 \end{matrix}\right), \left(\begin{matrix} a=20 \\ b=30 \end{matrix}\right), \left(\begin{matrix} a=11 \\ b=33 \end{matrix}\right), \left(\begin{matrix} a=14 \\ b=42 \end{matrix}\right);$$

$$\left.\begin{matrix} m=5 \\ n=2 \end{matrix}\right\} : \left(\begin{matrix} a=1 \\ b=4 \end{matrix}\right), \left(\begin{matrix} a=9 \\ b=12 \end{matrix}\right), \left(\begin{matrix} a=5 \\ b=20 \end{matrix}\right), \left(\begin{matrix} a=21 \\ b=28 \end{matrix}\right), \left(\begin{matrix} a=9 \\ b=36 \end{matrix}\right), \left(\begin{matrix} a=33 \\ b=44 \end{matrix}\right), \left(\begin{matrix} a=13 \\ b=52 \end{matrix}\right), \left(\begin{matrix} a=45 \\ b=60 \end{matrix}\right);$$

$$\left.\begin{matrix} m=5 \\ n=3 \end{matrix}\right\} : \left(\begin{matrix} a=3 \\ b=4 \end{matrix}\right), \left(\begin{matrix} a=3 \\ b=12 \end{matrix}\right), \left(\begin{matrix} a=15 \\ b=20 \end{matrix}\right), \left(\begin{matrix} a=7 \\ b=28 \end{matrix}\right), \left(\begin{matrix} a=27 \\ b=36 \end{matrix}\right), \left(\begin{matrix} a=39 \\ b=52 \end{matrix}\right), \left(\begin{matrix} a=15 \\ b=60 \end{matrix}\right), \left(\begin{matrix} a=51 \\ b=68 \end{matrix}\right).$$

Although it has not been possible to derive a general formula for $\psi(a,b)$, this can be done in some particular cases

Proposition 3.35. ***1)*** *In the limiting cases $(a=1, b-1)$ we have*

$$\psi(1,b) = (b+1,2), \qquad \psi(b-1,b) = (b+1,3). \tag{3.42}$$

2) *If $a \mid b$, then*

$$\psi(a,ad) = \left(d+1, \min_l \log_a (ld+1) + 1\right), \tag{3.43}$$

where l is the smallest integer for which log *takes its minimal integer value.*

3) *If $\gcd(a,b) = d$, then*

$$\psi(a,b) = \psi(a_0 d, b_0 d) = \left(b_0 + 1, \min_l \log_a \left(l\frac{b_0}{a_0} + 1\right) + 1\right), \tag{3.44}$$

with the same l.

Proof. All the statements follow directly from (3.7)–(3.8). □

In our approach, the concrete choice of operations (3.5)–(3.6) inside a conguence class $[[a]]_b$ gives

Assertion 3.36. The number of additions in the polyadic ring $\mathbb{Z}_{(m,n)}^{[a,b]}$ is greater that the number of mutiplications $m > n$ with any choice of (a,b).

Also, not all pairs (a,b) are allowed due to (3.7)–(3.8). We list the *forbidden* (a,b) for $b \leq 20$

$$\begin{aligned} &b=4 : a=2; \\ &b=8 : a=2,4,6; \\ &b=9 : a=3,6; \\ &b=12 : a=2,6,10; \\ &b=16 : a=2,4,6,8,12,14; \\ &b=18 : a=3,6,12,15; \\ &b=20 : a=2,6,10,14,18. \end{aligned} \tag{3.45}$$

The characterization of the fixed congruence class $[[a]]_b$ and the corresponding (m,n)-ring of polyadic integer numbers $\mathbb{Z}_{(m,n)}^{[a,b]}$ can be done in terms of the *shape invariants* $I, J \in \mathbb{Z}_+$ defined uniquely by (TABLE 3 in [4])

$$I = I_m^{[a,b]} = (m-1)\,\frac{a}{b}, \qquad J = J_n^{[a,b]} = \frac{a^n - a}{b}. \tag{3.46}$$

Obviously, in the binary case, when $m = n = 2\,(a = 0, b = 1)$ both shape invariants vanish, $I = J = 0$. Nevertheless, there exist "partially" binary cases, when only $n = 2$ and $m \neq 2$, while J is nonzero, for instance in $\mathbb{Z}_{(6,2)}^{[6,10]}$ we have $I = J = 3$. In Example **3.3** for $\mathbb{Z}_{(5,3)}^{[3,4]}$ we have $I = 3,\ J = 6$. In the limiting cases (3.15)–(3.16) we have, in general, for a fixed b

$$I_{b+1}^{[1,b]} = 1, \quad J_2^{[1,b]} = 0, \tag{3.47}$$

$$I_{b+1}^{[b-1,b]} = b-1, \quad J_3^{[b-1,b]} = (b-1)\,(b-2)\,. \tag{3.48}$$

Thus, one can classify and distinguish the limiting cases of the congruence classes in terms of the invariants and their manifest form (3.47)–(3.48).

4. FINITE POLYADIC RINGS

Now we present a special method of constructing a finite *nonderived* polyadic ring by combining the "external" and "internal" methods. Let us "apply" **1)** to **2)**, such that instead of (3.4), we introduce the finite polyadic ring $\mathbb{Z}_{(m,n)}/c\mathbb{Z}$, where $\mathbb{Z}_{(m,n)}$ is defined in (3.9). However, if we directly consider the "double" class $\{a + bk + cl\}$ and fix a and b, then the factorization by $c\mathbb{Z}$ will not give closed operations for arbitrary c.

Assertion 4.1. If the finite polyadic ring $\mathbb{Z}_{(m,n)}^{[a,b]}/c\mathbb{Z}$ has q elements, then

$$c = bq. \tag{4.1}$$

Proof. It follows from (4.1), that the "double" class remains in $[[a]]_b$. □

Remark 4.2. *The representatives $x_k^{[a,b]} = a + bk$ belong to a (m,n)-ring with the polyadic operations (3.5)–(3.6), while the notions of subtraction, division, modulo and remainder are defined for binary operations. Therefore, we cannot apply the standard binary modular arithmetic to $x_k^{[a,b]}$ directly, but we can define the equivalence relations and corresponding class operations in terms of k.*

4.1. Secondary Congruence Classes

On the set of the "double" classes $\{a + bk + bql\}$, $k, l \in \mathbb{Z}$ and fixed $b \in \mathbb{N}$ and $a = 0, \ldots, b-1$ we define the equivalence relation $\overset{k}{\sim}$ by

$$\{a + bk_1 + bql_1\} \overset{k}{\sim} \{a + bk_2 + bql_2\} \Longrightarrow k_1 - k_2 = ql, \quad l, l_1, l_2 \in \mathbb{Z}. \tag{4.2}$$

Proposition 4.3. *The equivalence relation $\overset{k}{\sim}$ is a congruence.*

Proof. It follows from the *binary* congruency of k's such that $k_1 \equiv k_2 \pmod q$ which is just a rewritten form of the last condition of (4.2). □

So now we can factorize $\mathbb{Z}_{(m,n)}^{[a,b]}$ by the congruence $\overset{k}{\sim}$ and obtain

Definition 4.4. *A secondary (equivalence) class of a polyadic integer* $x_k^{[a,b]} = a + bk \in \mathbb{Z}_{(m,n)}^{[a,b]}$ *"modulo" bq (with q being the number of representatives* $x_k^{[a,b]}$*, for fixed* $b \in \mathbb{N}$ *and* $0 \le a \le b-1$*) is*

$$\left[\left[x_k^{[a,b]}\right]\right]_{bq} = \{\{(a+bk)+bql\} \mid l \in \mathbb{Z},\ q \in \mathbb{N},\ 0 \le k \le q-1\}\,. \tag{4.3}$$

Remark 4.5. *If the binary limit is given by* $a = 0, b = 1$ *and* $\mathbb{Z}_{(2,2)}^{[0,1]} = \mathbb{Z}$*, then the secondary class becomes the ordinary class* (3.1).

If the values of the parameters a, b, q are clear from the context, we denote the secondary class representatives by an integer with *two* primes, as follows $\left[\left[x_k^{[a,b]}\right]\right]_{bq} \equiv x_k'' \equiv x''$.

Example 4.6. ***a)*** *Let* $a = 3, b = 5$*, then for* $q = 4$ *elements we have the secondary classes with* $k = 0, 1, 2, 3$ *(the corresponding binary limits are in brackets)*

$$\left[\left[x_k^{[3,5]}\right]\right]_{20} = 3'', 8'', 13'', 18'' = \begin{cases} 3'' = \{\ldots -17, 3, 23, 43, 63, \ldots\}\,, \\ 8'' = \{\ldots -12, 8, 28, 48, 68, \ldots\}\,, \\ 13'' = \{\ldots -7, 13, 33, 53, 73, \ldots\}\,, \\ 18'' = \{\ldots -2, 18, 38, 58, 78, \ldots\}\,, \end{cases} \tag{4.4}$$

$$\left([[k]]_4 = 0', 1', 2', 3' = \begin{cases} 0' = \{\ldots -4, 0, 4, 8, 12, \ldots\}\,, \\ 1' = \{\ldots -3, 1, 5, 9, 13, \ldots\}\,, \\ 2' = \{\ldots -2, 2, 6, 10, 14, \ldots\}\,, \\ 3' = \{\ldots -1, 3, 7, 11, 15, \ldots\}\,. \end{cases} \right) \tag{4.5}$$

b) *For* $a = 3, b = 6$ *and for* 4 *elements and* $k = 0, 1, 2, 3$

$$\left[\left[x_k^{[3,6]}\right]\right]_{24} = 3'', 9'', 15'', 21'', \qquad \left([[k]]_4 = 0', 1', 2', 3'\right). \tag{4.6}$$

c) *If* $a = 4, b = 5$*, for* 3 *elements and* $k = 0, 1, 2$ *we get*

$$\left[\left[x_k^{[4,5]}\right]\right]_{15} = 4'', 9'', 14'', \qquad \left([[k]]_3 = 0', 1', 2'\right). \tag{4.7}$$

The crucial difference between these sets of classes are: 1) they are described by rings of different arities determined by (3.7) *and* (3.8)*; 2) some of them are fields.*

4.2. Finite Polyadic Rings of Secondary Classes

Now we determine the operations between secondary classes. The most significant difference with the binary class operations (3.2)–(3.3) is the fact that secondary classes obey *nonderived polyadic* operations.

Proposition 4.7. *The set* $\{x_k''\}$ *of q secondary classes* $k = 0, \ldots, q-1$ *(with the fixed* a, b*) can be endowed with the following commutative m-ary addition*

$$x''_{k_{add}} = \nu''_m\left[x''_{k_1}, x''_{k_1}, \ldots, x''_{k_m}\right], \tag{4.8}$$

$$k_{add} \equiv \left((k_1 + k_2 + \ldots + k_m) + I_m^{[a,b]}\right) (\mathrm{mod}\, q) \tag{4.9}$$

and commutative n-ary multiplication

$$x''_{k_{mult}} = \mu''_n\left[x''_{k_1}, x''_{k_1}, \ldots, x''_{k_n}\right], \tag{4.10}$$

$$k_{mult} \equiv \left(a^{n-1}\left(k_1+k_2+\ldots+k_n\right)+a^{n-2}b\left(k_1k_2+k_2k_3+\ldots+k_{n-1}k_n\right)+\ldots \right.$$
$$\left.+b^{n-1}k_1\ldots k_n+J_n^{[a,b]}\right)\left(\mathrm{mod}\, q\right), \tag{4.11}$$

which satisfy the polyadic distributivity, and the shape invariants $I_m^{[a,b]}, J_n^{[a,b]}$ *are defined in* (3.46).

Proof. This follows from the definition of the secondary class (4.3) and manifest form of the "underlying" polyadic operations (3.5)–(3.6), which are commutative and distributive. □

Remark 4.8. *The binary limit is given by* $a=0, b=1$ *and* $m=n=2$, $I_m^{[a,b]}=J_n^{[a,b]}=0$, *such that the secondary class becomes the ordinary congruence class* $x_k''\to k'$, *obeying the standard binary class operations* (3.2)−(3.3), *which in terms of* k *are* $k_{add}\equiv\left(k_1+k_2\right)\left(\mathrm{mod}\, q\right)$, $k_{mult}\equiv\left(k_1k_2\right)\left(\mathrm{mod}\, q\right)$.

Definition 4.9. *The set of secondary classes* (4.3) *equipped with operations* (4.8), (4.10) *is denoted by*

$$\mathbb{Z}_{(m,n)}\left(q\right)\equiv\mathbb{Z}_{(m,n)}^{[a,b]}\left(q\right)=\mathbb{Z}_{(m,n)}^{[a,b]}\diagup\left(bq\right)\mathbb{Z}=\left\{\left\{x_k''\right\}\mid\nu_m'',\mu_n''\right\}, \tag{4.12}$$

and is a finite secondary class (m,n)*-ring of polyadic integer numbers* $\mathbb{Z}_{(m,n)}\equiv\mathbb{Z}_{(m,n)}^{[a,b]}$. *The value* q *(the number of elements) is called its order.*

Informally, $\mathbb{Z}_{(m,n)}=\mathbb{Z}_{(m,n)}\left(\infty\right)$. First, note that the constructed finite (m,n)-rings (4.12) have a much richer structure and exotic properties which do not exist in the binary finite residue class rings (3.4), and, in general, they give many concrete examples for possible different kinds polyadic rings. One of such "non-binary" properties is the availability of several units (for odd multiplicative arity n), and moreover sometimes all ring elements are units (such rings are "automatically" fields, see below).

Example 4.10. ***a)*** *In* $(5,3)$*-ring* $\mathbb{Z}_{(4,3)}^{[3,4]}\left(2\right)$ *with 2 secondary classes both elements are units (we mark units by subscript e)* $e_1=3_e''=3''$, $e_2=7_e''=7''$, *because they are both multiplicative idempotents and satisfy the following ternary multiplication (cf.* (2.4)*)*

$$\mu_3\left[3'',3'',3''\right]=3'',\ \mu_3\left[3'',3'',7''\right]=7'',\ \mu_3\left[3'',7'',7''\right]=3'',\ \mu_3\left[7'',7'',7''\right]=7''. \tag{4.13}$$

b) *In the same way the ring* $\mathbb{Z}_{(7,3)}^{[5,6]}\left(4\right)$ *consists of only 4 units* $e_1=5_e''$, $e_2=11_e''$, $e_3=17_e''$, $e_4=23_e''$, *and no zero.*

c) *Equal arity rings of the same order may be not isomorphic. For instance,* $\mathbb{Z}_{(4,2)}^{[1,3]}\left(2\right)$ *consists of unit* $e=1_e''=1''$ *and zero* $z=4_z''=4''$ *only, satisfying*

$$\mu_2\left[1'',1''\right]=1'',\ \mu_2\left[1'',4''\right]=4'',\ \mu_2\left[4'',4''\right]=4'', \tag{4.14}$$

and therefore $\mathbb{Z}_{(4,2)}^{[1,3]}\left(2\right)$ *is a field, because* $\{1'',4_z''\}\setminus 4_z''$ *is a (trivial) binary group, consisting of one element* $1_e''$. *However,* $\mathbb{Z}_{(4,2)}^{[4,6]}\left(2\right)$ *has the zero* $z=4_z''=4''$, $10''$ *and has no unit, because*

$$\mu_2\left[4'',4''\right]=4'',\ \mu_2\left[4'',10''\right]=4'',\ \mu_2\left[10'',10''\right]=4'', \tag{4.15}$$

so that $\mathbb{Z}_{(4,2)}^{[4,6]}\left(2\right)$ *is not a field, because of the last relation (nilpotency of* $10''$*). Their additive* 4*-ary groups are also not isomorphic (which is easy to show). However,* $\mathbb{Z}_{(4,2)}^{[1,3]}\left(2\right)$ *and* $\mathbb{Z}_{(4,2)}^{[4,6]}\left(2\right)$ *have the same arity and order.*

Recalling **Assertion 3.34**, we conclude more concretely:

Assertion 4.11. For a fixed arity shape (m,n), there can be non-isomorphic secondary class polyadic rings $\mathbb{Z}_{(m,n)}(q)$ of the same order q, which describe different binary residue classes $[[a]]_b$.

A polyadic analog of the characteristic can be introduced, when there exist both a unit and zero in a finite ring. Recall, that if $\mathcal{R}$ is a finite binary ring with unit1 and zero 0, then its characteristic is defined as a smallest integer χ, such that

$$\left(\overbrace{1+1+,\ldots,+1}^{\chi}\right) = \chi \cdot 1 = 0. \tag{4.16}$$

This means that the "number" of unit additions being $\chi - 1$ produces zero. The same is evident for any other element $x \in \mathcal{R}$, because $x = x \cdot 1$.

Definition 4.12. *For the finite polyadic ring $\mathbb{Z}_{(m,n)}(q)$ which contains both the unit e and the zero z, a polyadic characteristic χ_p is defined as a smallest additive polyadic power (2.2) of e which is equal to zero*

$$e^{\langle \chi_p \rangle_{+m}} = z. \tag{4.17}$$

In the binary limit, obviously, $\chi_p = \chi - 1$. A polyadic analog of the middle term in (.11) can be obtained by using the polyadic distributivity and (3.5) as

$$e^{\langle \chi_p \rangle_{+m}} = e^{\langle \chi_p (m-1)+1 \rangle_{\times n}}. \tag{4.18}$$

In TABLE 1 we present the parameters-to-arity mapping $\psi^{[a,b]}_{(m,n)}$ (3.41) together with the polyadic characteristics of those finite secondary class rings $\mathbb{Z}^{[a,b]}_{(m,n)}(q)$ which contain both unit(s) and zero, and which have order less or equal than 10 for $b \leq 6$.

Now we turn to the question of which secondary classes can be described by polyadic finite fields.

5. FINITE POLYADIC FIELDS

Let us consider the structure of the finite secondary class rings $\mathbb{Z}^{[a,b]}_{(m,n)}(q)$ in more detail and determine which of them are polyadic fields.

Proposition 5.1. *A finite polyadic ring $\mathbb{Z}^{[a,b]}_{(m,n)}(q)$ is a secondary class finite (m,n)-field $\mathbb{F}''^{[a,b]}_{(m,n)}(q)$ if all its elements except z (if it exists) are polyadically multiplicative invertible having a unique querelement.*

Proof. In both cases $\{\{x''_k\} \mid \mu''_n\}$ and $\{\{x''_k \setminus z\} \mid \mu''_n\}$ are commutative and cancellative n-ary groups, which follows from the concrete form of multiplication (4.10). Therefore, according to **Definition 2.1**, in such a case $\mathbb{Z}^{[a,b]}_{(m,n)}(q)$ becomes a polyadic field $\mathbb{F}''^{[a,b]}_{(m,n)}(q)$. □

5.1. Abstract Finite Polyadic Fields

In the binary case [1] the residue (congruence) class ring (3.4) with q elements $\mathbb{Z}/q\mathbb{Z}$ is a congruence class (non-extended) field, if its order $q = p$ is a prime number, such that $\mathbb{F}'(p) = \left\{\left\{[[a]]_p\right\} \mid +', \cdot', 0', 1'\right\}$, $a = 0, 1, \ldots, p-1$. Because all non-extended binary fields of a fixed prime order p are isomorphic each other and, in tern, isomorphic to the congruence class field $\mathbb{F}'(p)$, it is natural to study them in a more "abstract" way, i.e. without connection to a specific congruence class structure. This can be achieved by consideration of the one-to-one onto mapping from the congruence class to its representative which preserves the field (ring) structure and provides operations (binary multiplication and addition with ordinary 0 and 1) by modulo p. In other words, the mapping $\Phi_p\left([[a]]_p\right) = a$ is an

Table 1. Polyadic characteristics χ_p for the finite secondary class (m,n)-rings $\mathbb{Z}_{m,n}^{[a,b]}(q)$ of order $2 \le q \le 10$ for $2 \le b \le 6$. The orders q which do not give fields are *slanted*.

$a \setminus b$	2	3	4	5	6
1	$m = \mathbf{3}$ $n = \mathbf{2}$ q=3, $\chi_p = 1$ q=5, $\chi_p = 2$ q=7, $\chi_p = 3$ *q=9*, $\chi_p = 4$	$m = \mathbf{4}$ $n = \mathbf{2}$ q=2, $\chi_p = 1$ *q=4*, $\chi_p = 1$ q=5, $\chi_p = 3$ q=7, $\chi_p = 2$ *q=8*, $\chi_p = 5$ *q=10*, $\chi_p = 3$	$m = \mathbf{5}$ $n = \mathbf{2}$ q=3, $\chi_p = 2$ q=5, $\chi_p = 1$ q=7, $\chi_p = 5$ *q=9*, $\chi_p = 2$	$m = \mathbf{6}$ $n = \mathbf{2}$ q=2, $\chi_p = 1$ q=3, $\chi_p = 1$ *q=4*, $\chi_p = 3$ *q=6*, $\chi_p = 1$ q=7, $\chi_p = 4$ *q=8*, $\chi_p = 3$ *q=9*, $\chi_p = 7$	$m = \mathbf{7}$ $n = \mathbf{2}$ q=5, $\chi_p = 4$ q=7, $\chi_p = 1$
2		$m = \mathbf{4}$ $n = \mathbf{3}$ q=2, $\chi_p = 1$ *q=4*, $\chi_p = 1$ q=5, $\chi_p = 3$ q=7, $\chi_p = 2$ *q=8*, $\chi_p = 5$ *q=10*, $\chi_p = 3$		$m = \mathbf{6}$ $n = \mathbf{5}$ q=2, $\chi_p = 1$ q=3, $\chi_p = 1$ *q=4*, $\chi_p = 3$ *q=6*, $\chi_p = 1$ q=7, $\chi_p = 4$ *q=8*, $\chi_p = 3$ *q=9*, $\chi_p = 7$	$m = \mathbf{4}$ $n = \mathbf{3}$ q=5, $\chi_p = 3$ q=7, $\chi_p = 2$ *q=10*, $\chi_p = 3$
3			$m = \mathbf{5}$ $n = \mathbf{3}$ q=3, $\chi_p = 2$ q=5, $\chi_p = 1$ q=7, $\chi_p = 5$ *q=9*, $\chi_p = 2$	$m = \mathbf{6}$ $n = \mathbf{5}$ q=2, $\chi_p = 1$ q=3, $\chi_p = 1$ *q=4*, $\chi_p = 3$ *q=6*, $\chi_p = 1$ q=7, $\chi_p = 4$ *q=8*, $\chi_p = 3$	$m = \mathbf{3}$ $n = \mathbf{2}$ q=5, $\chi_p = 2$ q=7, $\chi_p = 3$
4				$m = \mathbf{6}$ $n = \mathbf{3}$ q=2, $\chi_p = 1$ q=3, $\chi_p = 1$ *q=4*, $\chi_p = 3$ *q=6*, $\chi_p = 1$ q=7, $\chi_p = 4$ *q=8*, $\chi_p = 3$ *q=9*, $\chi_p = 7$	$m = \mathbf{4}$ $n = \mathbf{2}$ q=5, $\chi_p = 3$ q=7, $\chi_p = 2$ *q=10*, $\chi_p = 3$

isomorphism of binary fields $\Phi_p : \mathbb{F}'(p) \to \mathbb{F}(p)$, where $\mathbb{F}(p) = \{\{a\} \mid +, \cdot, 0, 1\}_{\mathrm{mod}\, p}$ is an "abstract" non-extended (prime) finite field of order p (or *Galois field* $GF(p)$).

In a similar way, we introduce a polyadic analog of the "abstract" binary non-extended (prime) finite fields. Let us consider the set of *polyadic integer numbers* $\{x_k\} \equiv \left\{x_k^{[a,b]}\right\} = \{a + bk\} \in \mathbb{Z}_{(m,n)}^{[a,b]}$, $b \in \mathbb{N}$ and $0 \le a \le b-1$, $0 \le k \le q-1$, $q \in \mathbb{N}$, which obey the operations (3.5)–(3.6). The polyadic version of the prime finite field $\mathbb{F}(p)$ of order p (or Galois field $GF(p)$) is given by

Definition 5.2. *The "abstract" non-extended (prime) finite (m,n)-field of order q is*

$$\mathbb{F}_{(m,n)}(q) \equiv \mathbb{F}_{(m,n)}^{[a,b]}(q) = \{\{a + bk\} \mid \nu_m, \mu_n\}_{\mathrm{mod}\, bq}, \tag{5.1}$$

if $\{\{x_k\} \mid \nu_m\}_{\mathrm{mod}\, bq}$ is an additive m-ary group, and $\{\{x_k\} \mid \mu_n\}_{\mathrm{mod}\, bq}$ (or, when zero z exists, $\{\{x_k \setminus z\} \mid \mu_n\}_{\mathrm{mod}\, bq}$) is a multiplicative n-ary group.

Then we define a one-to-one onto mapping from the secondary congruence class to its representative by $\Phi_q^{[a,b]}\left(\left[\left[x_k^{[a,b]}\right]\right]_{bq}\right) = x_k^{[a,b]}$ and arrive at the following

Proposition 5.3. *The mapping $\Phi_q^{[a,b]} : \mathbb{F}''^{[a,b]}_{(m,n)}(q) \to \mathbb{F}_{(m,n)}^{[a,b]}(q)$ is a polyadic ring homomorphism (being, in fact, an isomorphism) and satisfies (here we use the "prime" notations)*

$$\Phi_q^{[a,b]}\left(\nu_m''\left[x_1'', x_2'', \ldots, x_m''\right]\right) = \nu_m\left[\Phi_q^{[a,b]}(x_1), \Phi_q^{[a,b]}(x_2), \ldots, \Phi_q^{[a,b]}(x_m)\right], \tag{5.2}$$

$$\Phi_q^{[a,b]}\left(\mu_n''\left[x_1'', x_2'', \ldots, x_n''\right]\right) = \mu_n\left[\Phi_q^{[a,b]}(x_1), \Phi_q^{[a,b]}(x_2), \ldots, \Phi_q^{[a,b]}(x_n)\right]. \tag{5.3}$$

Proof. This follows directly from (3.5)–(3.6) and (4.8)–(4.10). Obviously, a mapping defined in this way governs the polyadic distributivity, and therefore $\Phi_q^{[a,b]}$ is a ring homomorphism, or, more exactly, a 1-place heteromorphism for m-ary addition together with n-ary multiplication (see [4]). Because $x_k'' \to x_k$ is one-to-one for any fixed $0 \le k \le q-1$, $\Phi_q^{[a,b]}$ is an isomorphism. □

In TABLE 2 we present the "abstract" non-extended polyadic *finite* fields $\mathbb{F}_{(m,n)}^{[a,b]}(q)$ of lowest arity shape (m,n) and orders q. The forbidden pairs (a,b) for $\mathbb{F}_{(m,n)}^{[a,b]}(q)$ coincide with ones for polyadic rings $\mathbb{Z}_{(m,n)}^{[a,b]}$ listed in (3.45).

5.2. Multiplicative Structure

In the multiplicative structure the following crucial differences between the binary finite fields and $\mathbb{F}_{(m,n)}(q)$ can be outlined.

Remark 5.4. *The order of a non-extended finite polyadic field may not be prime (e.g., $\mathbb{F}_{(3,2)}^{[1,2]}(4)$, $\mathbb{F}_{(5,3)}^{[3,4]}(8)$, $\mathbb{F}_{(4,3)}^{[2,6]}(9)$), and may not even be a power of a prime binary number (e.g. $\mathbb{F}_{(7,3)}^{[5,6]}(6)$, $\mathbb{F}_{(11,5)}^{[3,10]}(10)$), see* TABLE 3.

Remark 5.5. *The polyadic characteristic χ_p of a non-extended finite polyadic field can have values such that $\chi_p + 1$ (corresponding in the binary case to the ordinary characteristic χ) can be nonprime (*TABLE 1*).*

Assertion 5.6. If a secondary class $\left[\left[x_k^{[a,b]}\right]\right]_{bq}$ contains *no zero*, it can be isomorphic to the "abstract" *zeroless* finite polyadic field $\mathbb{F}_{(m,n)}^{[a,b]}(q)$.

Table 2. Content and arities of the secondary class finite polyadic rings $\mathbb{Z}_{(m,n)}^{[a,b]}(q)$ and the corresponding simple finite polyadic (m,n)-fields $\mathbb{F}_{m,n}^{[a,b]}(q)$ of order $2 \le q \le 4$ (framed) for $2 \le b \le 6$. The subscripts e and z mark those secondary classes (two primes are omitted) which play the roles of polyadic unit and polyadic zero respectively. The double frames denote the finite polyadic fields containing both a unit and zero. The last line in a cell (corresponding to a fixed congruence class $[[a]]_b$) gives the allowed orders of finite polyadic fields for $5 \le q \le 10$, and bold numbers mark the orders of such fields which contain both unit(s) and zero.

$a \setminus b$	2	3	4	5	6
1	$m = \mathbf{3}$ $n = \mathbf{2}$ $1_e,3$ $1_e,3_z,5$ $1_e,3,5,7$ q=**5**,**7**,8	$m = \mathbf{4}$ $n = \mathbf{2}$ $1_e,4_z$ $1_e,4,7$ $1_e,4_z,7,10$ q=**5**,**7**,9	$m = \mathbf{5}$ $n = \mathbf{2}$ $1_e,5$ $1_e,5,9_z$ $1_e,5,9,13$ q=**5**,**7**,8	$m = \mathbf{6}$ $n = \mathbf{2}$ $1_e,6_z$ $1_e,6_z,11$ $1_e,6,11,16_z$ q=5,**7**	$m = \mathbf{7}$ $n = \mathbf{2}$ $1_e,7$ $1_e,7,13$ $1_e,7,13,19$ q=**5**,6,**7**,8,9
2		$m = \mathbf{4}$ $n = \mathbf{3}$ $2_z,5_e$ $2,5,8_e$ $2,5_e,8_z,11_e$ q=**5**,**7**,9		$m = \mathbf{6}$ $n = \mathbf{5}$ $2_z,7_e$ $2_e,7,12_z$ $2,7_e,12_z,17_e$ q=5,**7**	$m = \mathbf{4}$ $n = \mathbf{3}$ $2,8_z$ $2,8_e,14$ $2,8_z,14,20$ q=**5**,**7**,9
3			$m = \mathbf{5}$ $n = \mathbf{3}$ $3_e,7_e$ $3_z,7_e,11_e$ $3,7_e,11,15_e$ q=**5**,6,**7**,8	$m = \mathbf{6}$ $n = \mathbf{5}$ $3_e,8_z$ $3_z,8_e,13_e$ $3_e,8_z,13_e,18$ q=5,**7**	$m = \mathbf{3}$ $n = \mathbf{2}$ $3,9_e$ $3,9_z,15$ $3,9_e,15,21$ q=**5**,**7**,8
4				$m = \mathbf{6}$ $n = \mathbf{3}$ $4_z,9_e$ $4_e,9_z,14_e$ $4_z,9_e,14,19_e$ q=5,**7**	$m = \mathbf{4}$ $n = \mathbf{2}$ $4_z,10$ $4,10_e,16$ $4,10,16_z,22$ q=**5**,**7**,9
5					$m = \mathbf{7}$ $n = \mathbf{3}$ $5_e,11_e$ $5,11,17_e$ $5_e,11_e,17_e,23_e$ q=**5**,6,**7**,8,9

Zeroless fields are marked by one frame in TABLE 2. There exist finite polyadic fields with *more than one* unit, and also *all* elements can be units. Such cases are marked in TABLE 3 by subscripts which indicate the number of units.

Denote the Abelian finite multiplicative n-ary group of $\mathbb{F}^{[a,b]}_{(m,n)}(q)$ by $\mathcal{G}^{[a,b]}_{n}(q)$.

Example 5.7. ***1)*** *The finite* $(6,3)$*-field* $\mathbb{F}^{[4,5]}_{(6,3)}(3)$ *of order* 3 *has two units* $\{4,14\} \equiv \{4_e, 14_e\}$ *and zero* $9 \equiv 9_z$*, and its multiplicative* 3*-ary group* $\mathcal{G}^{[4,5]}_{3}(2)$ *is*

$$\mu_3[4,4,4] = 4,\ \mu_3[4,4,14] = 14,\ \mu_3[4,14,14] = 4,\ \mu_3[14,14,14] = 14.$$

2) *In* $\mathbb{F}^{[5,6]}_{(7,3)}(4)$ *of order* 4 *all the elements* $\{5,11,17,23\} \equiv \{5_e, 11_e, 17_e, 23_e\}$ *are units (see* (2.4)*), because for its* 3*-ary group* $\mathcal{G}^{[5,6]}_{3}(4)$ *we have*

$$\begin{gathered}\mu_3[5,5,5] = 5, \mu_3[11,11,11] = 11, \mu_3[17,17,17] = 17, \mu_3[23,23,23] = 23,\\ \mu_3[5,5,11] = 11,\ \mu_3[5,5,17] = 17,\ \mu_3[5,5,23] = 23,\\ \mu_3[11,11,5] = 5,\ \mu_3[11,11,17] = 17,\ \mu_3[11,11,23] = 23,\\ \mu_3[17,17,5] = 5,\ \mu_3[17,17,11] = 11,\ \mu_3[17,17,23] = 23,\\ \mu_3[23,23,5] = 5,\ \mu_3[23,23,11] = 11,\ \mu_3[23,23,17] = 17.\end{gathered}$$

In general, n-ary groups may contain no units (and multiplicative idempotents) at all, and invertibility is controlled in another way, by querelements: each element of any n-ary group should be (uniquely) "quereable" (2.5). In case of (m,n)-fields both m-ary additive group and n-ary multiplicative group $\mathcal{G}^{[a,b]}_{n}(q)$ can be of this kind. By analogy with zeroless-nonunital rings we have

Definition 5.8. *A polyadic field* $\mathbb{F}_{(m,n)}$ *is called zeroless-nonunital, if it contains no zero and no unit.*

Assertion 5.9. The zeroless-nonunital polyadic fields are totally (additively and multiplicatively) non-derived.

Proposition 5.10. ***1)*** *If* $\gcd(bq) \neq 1$*, then* $\mathbb{F}^{[a,b]}_{(m,n)}(q)$ *is zeroless.* ***2)*** *The zero can exist only, if* $\gcd(bq) = 1$ *and the field order* $q = p$ *is prime.*

Proof. It follows directly from the definition of the polyadic zero (2.3) and (4.9). □

Let us consider examples of zeroless-nonunital finite fields of polyadic integer numbers $\mathbb{F}^{[a,b]}_{(m,n)}(q)$.

Example 5.11. ***1)*** *The zeroless-nonunital polyadic finite fields having lowest* $|a+b|$ *are, e.g.,* $\mathbb{F}^{[3,8]}_{(9,3)}(2)$, $\mathbb{F}^{[3,8]}_{(9,3)}(4)$, $\mathbb{F}^{[5,8]}_{(9,3)}(4)$, $\mathbb{F}^{[5,8]}_{(9,3)}(8)$, *also* $\mathbb{F}^{[4,9]}_{(10,4)}(3)$, $\mathbb{F}^{[4,9]}_{(10,4)}(9)$, *and* $\mathbb{F}^{[7,9]}_{(10,4)}(3)$, $\mathbb{F}^{[7,9]}_{(10,4)}(9)$.

2) *The multiplication of the zeroless-nonunital* $(9,3)$*-field* $\mathbb{F}^{[5,8]}_{(9,3)}(2)$ *is*

$$\mu_3[5,5,5] = 13,\ \mu_3[5,5,13] = 5,\ \mu_3[5,13,13] = 13,\ \mu_3[13,13,13] = 5.$$

Using (2.2) *we find the (unique) multiplicative querelements* $\bar{5} = 13$*,* $\overline{13} = 5$*. The addition of* $\mathbb{F}^{[5,8]}_{(9,3)}(2)$ *is*

$$\begin{gathered}\nu_9\left[5^9\right] = 13,\ \nu_9\left[5^8,13\right] = 5,\ \nu_9\left[5^7,13^2\right] = 13,\ \nu_9\left[5^6,13^3\right] = 5,\ \nu_9\left[5^5,13^4\right] = 13,\\ \nu_9\left[5^4,13^5\right] = 5,\ \nu_9\left[5^3,13^6\right] = 13,\ \nu_9\left[5^2,13^7\right] = 5,\ \nu_9\left[5,13^8\right] = 13, \nu_9\left[13^9\right] = 5.\end{gathered}$$

The additive (unique) querelements are $\tilde{5} = 13$*,* $\widetilde{13} = 5$*. So all elements are additively and multiplicatively querable (polyadically invertible), and therefore* ν_9 *is* 9*-ary additive group operation and* μ_3 *is* 3*-ary multiplicative group operation, as it should be for a field. Because it contains no unit and no zero,* $\mathbb{F}^{[5,8]}_{(9,3)}(2)$ *is actually a zeroless-nonunital finite* $(9,3)$*-field of order* 2.

Other zeroless-nonunital finite polyadic fields are marked by frames in TABLE 3.

Remark 5.12. *The absence of zero does not guarantee that a* (m,n)*-ring* $\mathcal{R}^{[a,b]}_{(m,n)}(q)$ *is a field. For that, both* $\langle [[a]]_b \mid \nu_m\rangle$ *and* $\langle [[a]]_b \mid \mu_n\rangle$ *have to be polyadic groups.*

Example 5.13. *The* $(4,3)$*-ring* $\mathcal{R}^{[2,3]}_{(4,3)}(6)$ *is zeroless, and* $\langle [[3]]_4 \mid \nu_4\rangle$ *is its* 4*-ary additive group (each element has a unique additive querelement). Despite each element of* $\langle [[2]]_3 \mid \mu_3\rangle$ *having a querelement, it is not a multiplicative* 3*-ary group, because for the two elements* 2 *and* 14 *we have nonunique querelements*

$$\mu_3[2,2,5]=2,\ \mu_3[2,2,14]=2,\ \mu_3[14,14,2]=14,\ \mu_3[14,14,11]=14. \tag{5.4}$$

The conditions on the congruence classes $[[a]]_b$ and the invariants I,J (3.46), which give the same arity structure are given in [4]. Note, that there exist polyadic fields of the same arities (m,n) and the same order q which are not isomorphic (in contrast with what is possible in the binary case).

Example 5.14. *The polyadic* $(9,3)$*-fields corresponding to the congruence classes* $[[5]]_8$ *and* $[[7]]_8$ *are not isomorphic for orders* $q=2,4,8$ *(see* TABLE 3*). Despite both being zeroless, the first* $\mathbb{F}^{[5,8]}_{(9,3)}(q)$ *are nonunital, while the second* $\mathbb{F}^{[7,8]}_{(9,3)}(q)$ *has two units, which makes an isomorphism impossible.*

Recall [1], that in a (non-extended, prime) finite binary field $\mathbb{F}(p)$, the *order of an element* $x\in\mathbb{F}(p)$ is defined as a smallest integer λ such that $x^\lambda=1$. Obviously, the set of fixed order elements forms a cyclic subgroup $\mathcal{G}_\lambda$ of the multiplicative binary group of $\mathbb{F}(p)$, and $\lambda\mid(p-1)$. If $\lambda=p-1$, such an element is called a *primitive (root)*, it generates all elements, and these exist in any finite binary field. Moreover, any element of $\mathbb{F}(p)$ is idempotent $x^p=x$, while all its nonzero elements satisfy $x^{p-1}=1$ (Fermat's little theorem). A non-extended (prime) finite field is fully determined by its order p (up to isomorphism), and, moreover, any $\mathbb{F}(p)$ is isomorphic to $\mathbb{Z}/p\mathbb{Z}$.

In the polyadic case, the situation is more complicated. Because the related secondary class structure (5.1) contains parameters in addition to the number of elements q, the order of (non-extended) polyadic fields may not be prime, or nor even a power of a prime integer (e.g. $\mathbb{F}^{[5,6]}_{(7,3)}(6)$ or $\mathbb{F}^{[3,10]}_{(11,5)}(10)$). Also, as was shown above, finite polyadic fields can be zeroless, nonunital and have many (or even all) units (see TABLE 3). Therefore, we cannot use units in the definition of the element order. Instead, we propose an alternative:

Definition 5.15. *If an element of the finite polyadic field* $x\in\mathbb{F}_{(m,n)}(q)$ *satisfies*

$$x^{\langle\lambda_p\rangle_{\times n}}=x, \tag{5.5}$$

then the smallest such λ_p *is called the idempotence polyadic order and denoted* $\operatorname{ord}x=\lambda_p$.

Obviously, $\lambda_p=\lambda$ (see (2.1)).

Definition 5.16. *The idempotence polyadic order* $\lambda_p^{[a,b]}$ *of a finite polyadic field* $\mathbb{F}^{[a,b]}_{(m,n)}(q)$ *is the maximum* λ_p *of all its elements, and we call such field* $\lambda_p^{[a,b]}$*-idempotent and denote* $\operatorname{ord}\mathbb{F}^{[a,b]}_{(m,n)}(q)=\lambda_p^{[a,b]}$.

In TABLE 3 we present the idempotence polyadic order $\lambda_p^{[a,b]}$ for the (allowed) finite polyadic fields $\mathbb{F}^{[a,b]}_{(m,n)}(q)$ (5.1) with $2\le b\le 10$ and order $q\le 10$.

Definition 5.17. *Denote by q_* the number of nonzero distinct elements in $\mathbb{F}_{(m,n)}(q)$*

$$q_* = \begin{cases} q-1, & \text{if } \exists z \in \mathbb{F}_{(m,n)}(q) \\ q, & \text{if } \nexists z \in \mathbb{F}_{(m,n)}(q), \end{cases} \tag{5.6}$$

which is called a reduced (field) order.

The second choice of (5.6) in the binary case is absent, because any commutative binary group (as the additive group of a field) contains a zero (the identity of this group), and therefore any binary field has a zero, which does not always hold for the m-ary additive group of $\mathbb{F}_{(m,n)}$ (see *Example* **5.11**).

Theorem 5.18. *If a finite polyadic field $\mathbb{F}_{(m,n)}(q)$ has an order q, such that $q_* = q_*^{adm} = \ell(n-1)+1$ is n-admissible, then (for $n \geq 3$ and one unit):*

1) *A sequence of the length $q_*(n-1)$ built from any fixed element $y \in \mathbb{F}_{(m,n)}(q)$ is neutral*

$$\mu_n^{(q_*)}\left[x, y^{q_*(n-1)}\right] = x, \quad \forall x \in \mathbb{F}_{(m,n)}(q). \tag{5.7}$$

2) *Any element y satisfies the polyadic idempotency condition*

$$y^{\langle q_* \rangle_{\times n}} = y, \quad \forall y \in \mathbb{F}_{(m,n)}(q). \tag{5.8}$$

Proof. **1)** Take a long n-ary product of the q_* distinct nonzero elements $x_0 = \mu_n^{(\ell)}\left[x_1, x_2, \ldots, x_{q_*}\right]$, such that q_* can take only multiplicatively n-admissible values q_*^{adm}, where $\ell \in \mathbb{N}$ is a "number" of n-ary multiplications. Then polyadically multiply each x_i by a fixed element $y \in \mathbb{F}_{(m,n)}(q)$ such that all q_* elements $\mu_n\left[x_i, y^{n-1}\right]$ will be distinct as well. Therefore, their product should be the same x_0. Using commutativity and associativity, we obtain

$$\begin{aligned} x_0 &= \mu_n^{(\ell)}\left[x_1, x_2, \ldots, x_{q_*}\right] = \mu_n^{(\ell)}\left[\mu_n\left[x_1, y^{n-1}\right], \mu_n\left[x_2, y^{n-1}\right], \ldots, \mu_n\left[x_{q_*}, y^{n-1}\right]\right] \\ &= \mu_n^{(q_*)}\left[\mu_n^{(\ell)}\left[x_1, x_2, \ldots, x_{q_*}\right], y^{q_*(n-1)}\right] = \mu_n^{(q_*)}\left[x_0, y^{q_*(n-1)}\right]. \end{aligned} \tag{5.9}$$

2) Insert into the formula obtained above $x_0 = y$, then use (2.2) to get (5.8). □

Finite polyadic fields $\mathbb{F}_{(m,n)}^{[a,b]}(q)$ having n-admissible reduced order $q_* = q_*^{adm} = \ell(n-1)+1$ ($\ell \in \mathbb{N}$) (underlined in TABLE 3) are closest to the binary finite fields $\mathbb{F}(p)$ in their general properties: they are half-derived, while if they contain a zero, they are fully derived. If $q_* \neq q_*^{adm}$, then $\mathbb{F}_{(m,n)}^{[a,b]}(q)$ can be nonunital or contain more than one unit (subscripts in TABLE 3).

Assertion 5.19. The finite fields $\mathbb{F}_{(m,n)}^{[a,b]}(q)$ of n-admissible reduced order $q_* = q_*^{adm}$ cannot have more than one unit and cannot be zeroless-nonunital.

Assertion 5.20. If $q_* \neq q_*^{adm}$, and $\mathbb{F}_{(m,n)}^{[a,b]}(q)$ is unital zeroless, then the reduced order q_* is the product of the idempotence polyadic field order $\lambda_p^{[a,b]} = \operatorname{ord}\mathbb{F}_{(m,n)}^{[a,b]}(q)$ and the number of units κ_e (if $a \nmid b$ and $n \geq 3$)

$$q_* = \lambda_p^{[a,b]}\kappa_e. \tag{5.10}$$

Let us consider the structure of the multiplicative group $\mathcal{G}_n^{[a,b]}(q_*)$ of $\mathbb{F}_{(m,n)}^{[a,b]}(q)$ in more detail. Some properties of commutative cyclic n-ary groups were considered for particular relations between orders and arity. Here we have: 1) more parameters and different relations between these, the arity and order; 2) the (m,n)-field under consideration, which leads to additional restrictions. In such a way exotic polyadic groups and fields arise which have unusual properties that have not been studied before.

Table 3. Idempotence polyadic orders $\lambda_p^{[a,b]}$ for (allowed) finite polyadic fields $\mathbb{F}_{(m,n)}^{[a,b]}(q)$, with $2 \le b \le 10$ and field orders $2 \le q \le 10$. If q_* is n-admissible, they are underlined. The zeroless-nonunital cases are framed. Subscripts correspond to the number of units $\kappa_e \ge 2$, while nonframed entries have exactly one unit.

$[[a]]_b$		*Arities*	*Finite polyadic field order q*								
b	a	(m,n)	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*
2	1	$(3,2)$	2	**2**	2	**4**	∅	**6**	4	∅	∅
3	1	$(4,2)$	**1**	3	∅	**4**	∅	**6**	∅	9	∅
	2	$(4,3)$	**1**	$\underline{3}$	∅	$\mathbf{2}_{2e}$	∅	$\mathbf{3}_{2e}$	∅	$\underline{9}$	∅
4	1	$(5,2)$	2	**2**	4	**4**	∅	**6**	8	∅	∅
	3	$(5,3)$	1_{2e}	$\mathbf{1}_{2e}$	2_{2e}	$\mathbf{2}_{2e}$	∅	$\mathbf{3}_{2e}$	4_{2e}	∅	∅
5	1	$(6,2)$	**1**	**2**	∅	5	∅	**6**	∅	∅	∅
	2	$(6,5)$	**1**	$\mathbf{1}_{2e}$	∅	$\underline{5}$	∅	$\mathbf{3}_{2e}$	∅	∅	∅
	3	$(6,5)$	**1**	$\mathbf{1}_{2e}$	∅	$\underline{5}$	∅	$\mathbf{3}_{2e}$	∅	∅	∅
	4	$(6,3)$	**1**	$\mathbf{1}_{2e}$	∅	$\underline{5}$	∅	$\mathbf{3}_{2e}$	∅	∅	∅
6	1	$(7,2)$	2	3	2	**4**	6	**6**	4	9	∅
	2	$(4,3)$	∅	$\underline{3}$	∅	$\mathbf{2}_{2e}$	∅	$\mathbf{3}_{2e}$	∅	$\underline{9}$	∅
	3	$(3,2)$	2	∅	2	**4**	∅	**6**	4	∅	∅
	4	$(4,2)$	∅	3	∅	**4**	∅	**6**	∅	9	∅
	5	$(7,3)$	1_{2e}	$\underline{3}$	1_{4e}	$\mathbf{2}_{2e}$	3_{2e}	$\mathbf{3}_{2e}$	2	$\underline{9}$	∅
7	1	$(8,2)$	**1**	**2**	∅	**4**	∅	7	∅	∅	∅
	2	$(8,4)$	**1**	**2**	∅	$\underline{4}$	∅	$\underline{7}$	∅	∅	∅
	3	$(8,7)$	**1**	$\mathbf{1}_{2e}$	∅	$\mathbf{2}_{2e}$	∅	$\underline{7}$	∅	∅	∅
	4	$(8,4)$	**1**	**2**	∅	$\underline{4}$	∅	$\underline{7}$	∅	∅	∅
	5	$(8,7)$	**1**	$\mathbf{1}_{2e}$	∅	$\mathbf{2}_{2e}$	∅	$\underline{7}$	∅	∅	∅
	6	$(8,3)$	**1**	$\mathbf{1}_{2e}$	∅	$\mathbf{2}_{2e}$	∅	$\underline{7}$	∅	∅	∅
8	1	$(9,2)$	2	**2**	4	**4**	∅	**6**	8	∅	∅
	3	$(9,3)$	$\boxed{2}$	$\mathbf{1}_{2e}$	$\boxed{4}$	$\mathbf{2}_{2e}$	∅	$\mathbf{3}_{2e}$	$\boxed{8}$	∅	∅
	5	$(9,3)$	$\boxed{2}$	$\mathbf{1}_{2e}$	$\boxed{4}$	$\mathbf{2}_{2e}$	∅	$\mathbf{3}_{2e}$	$\boxed{8}$	∅	∅
	7	$(9,3)$	1_{2e}	$\mathbf{1}_{2e}$	2_{2e}	$\mathbf{2}_{2e}$	∅	$\mathbf{3}_{2e}$	4_{2e}	∅	∅
9	1	$(10,2)$	**1**	3	∅	**4**	∅	**6**	∅	9	∅
	2	$(10,7)$	**1**	$\boxed{3}$	∅	$\mathbf{2}_{2e}$	∅	$\mathbf{1}_{6e}$	∅	$\boxed{9}$	∅
	4	$(10,4)$	**1**	$\boxed{3}$	∅	$\underline{4}$	∅	$\mathbf{2}_{3e}$	∅	$\boxed{9}$	∅
	5	$(10,7)$	**1**	$\boxed{3}$	∅	$\mathbf{2}_{2e}$	∅	$\mathbf{1}_{6e}$	∅	$\boxed{9}$	∅
	7	$(10,4)$	**1**	$\boxed{3}$	∅	$\underline{4}$	∅	$\mathbf{2}_{3e}$	∅	$\boxed{9}$	∅

Definition 5.21. *An element* $x_{prim} \in \mathcal{G}_n^{[a,b]}(q_*)$ *is called* n*-ary primitive, if its idempotence order is*

$$\lambda_p = \operatorname{ord} x_{prim} = q_*. \tag{5.11}$$

Then, all λ_p polyadic powers $x_{prim}^{\langle 1\rangle_{\times n}}, x_{prim}^{\langle 2\rangle_{\times n}}, \dots, x_{prim}^{\langle q_*\rangle_{\times n}} \equiv x_{prim}$ generate other distinct elements, and so $\mathcal{G}_n^{[a,b]}(q_*)$ is a finite cyclic n-ary group generated by x_{prim}, i.e. $\mathcal{G}_n^{[a,b]}(q_*) = \left\langle \left\{ x_{prim}^{\langle i\rangle_{\times n}} \right\} \mid \mu_n \right\rangle$. We denote a number primitive elements in $\mathbb{F}_{(m,n)}^{[a,b]}(q)$ by κ_{prim}.

Assertion 5.22. For zeroless $\mathbb{F}_{(m,n)}^{[a,b]}(q)$ and prime order $q = p$, we have $\lambda_p^{[a,b]} = q$, and $\mathcal{G}_n^{[a,b]}(q)$ is indecomposable ($n \geq 3$).

Example 5.23. *The smallest* 3*-admissible zeroless polyadic field is* $\mathbb{F}_{(4,3)}^{[2,3]}(3)$ *with the unit* $e = 8$ *and two* 3*-ary primitive elements* $2, 5$ *having* 3*-idempotence order* $\operatorname{ord} 2 = \operatorname{ord} 5 = 3$*, so* $\kappa_{prim} = 2$ *, because*

$$2^{\langle 1\rangle_{\times 3}} = 8,\ 2^{\langle 2\rangle_{\times 3}} = 5,\ 2^{\langle 3\rangle_{\times 3}} = 2, \quad 5^{\langle 1\rangle_{\times 3}} = 8,\ 5^{\langle 2\rangle_{\times 3}} = 2,\ 5^{\langle 3\rangle_{\times 3}} = 5, \tag{5.12}$$

and therefore $\mathcal{G}_3^{[2,3]}(3)$ *is a cyclic indecomposable* 3*-ary group.*

Assertion 5.24. If $\mathbb{F}_{(m,n)}^{[a,b]}(q)$ is zeroless-nonunital, then every element is n-ary primitive, $\kappa_{prim} = q$, also $\lambda_p^{[a,b]} = q$ (the order q can be not prime), and $\mathcal{G}_n^{[a,b]}(q)$ is a indecomposable commutative cyclic n-ary group without identity ($n \geq 3$).

Example 5.25. *The* $(10,7)$*-field* $\mathbb{F}_{(10,7)}^{[5,9]}(9)$ *is zeroless-nonunital, each element (has* $\lambda_p = 9$*) is primitive and generates the whole field, and therefore* $\kappa_{prim} = 9$*, thus the* 7*-ary multiplicative group* $\mathcal{G}_7^{[5,9]}(9)$ *is indecomposable and without identity.*

The structure of $\mathcal{G}_n^{[a,b]}(q_*)$ can be extremely nontrivial and may have no analogs in the binary case.

Assertion 5.26. If there exists more than one unit, then:

1) If $\mathcal{G}_n^{[a,b]}(q_*)$ can be decomposed on its n-ary subroups, the number of units κ_e coincides with the number of its *cyclic* n-ary subgroups $\mathcal{G}_n^{[a,b]}(q_*) = \mathcal{G}_1 \cup \mathcal{G}_2 \dots \cup \mathcal{G}_{k_e}$ which *do not* intersect $\mathcal{G}_i \cap \mathcal{G}_j = \varnothing, i, j = i = 1, \dots, \kappa_e, i \neq j$.

2) If a zero exists, then each $\mathcal{G}_i$ has its own unit e_i, $i = 1, \dots, \kappa_e$.

3) In the zeroless case $\mathcal{G}_n^{[a,b]}(q) = \mathcal{G}_1 \cup \mathcal{G}_2 \dots \cup \mathcal{G}_{k_e} \cup E(\mathcal{G})$, where $E(\mathcal{G}) = \{e_i\}$ is the split-off subgroup of units.

Example 5.27. ***1)*** *In the* $(9,3)$*-field* $\mathbb{F}_{(9,3)}^{[5,8]}(7)$ *there is a single zero* $z = 21 \equiv 21_z$ *and two units* $e_1 = 13 \equiv 13_e$*,* $e_2 = 29 \equiv 29_e$*, and so its multiplicative* 3*-ary group* $\mathcal{G}_3^{[5,8]}(6) = \{5, 13, 29, 37, 45, 53\}$ *consists of two nonintersecting (which is not possible in the binary case)* 3*-ary cyclic subgroups* $\mathcal{G}_1 = \{5, 13_e, 45\}$ *and* $\mathcal{G}_2 = \{29_e, 37, 53\}$ *(for both* $\lambda_p = 3$*)*

$$\mathcal{G}_1 = \left\{ 5^{\langle 1\rangle_{\times 3}} = 13_e, 5^{\langle 2\rangle_{\times 3}} = 45, 5^{\langle 3\rangle_{\times 3}} = 5 \right\},\ \bar{5} = 45, \overline{45} = 5,$$

$$\mathcal{G}_2 = \left\{ 37^{\langle 1\rangle_{\times 3}} = 29_e, 37^{\langle 2\rangle_{\times 3}} = 53, 37^{\langle 3\rangle_{\times 3}} = 37 \right\},\ \overline{37} = 53, \overline{53} = 37.$$

All nonunital elements in $\mathcal{G}_3^{[5,8]}(6)$ *are (polyadic)* 1*-reflections, because* $5^{\langle 1\rangle_{\times 3}} = 45^{\langle 1\rangle_{\times 3}} = 13_e$ *and* $37^{\langle 1\rangle_{\times 3}} = 53^{\langle 1\rangle_{\times 3}} = 29_e$*, and so the subgroup of units* $E(\mathcal{G}) = \{13_e, 29_e\}$ *is unsplit* $E(\mathcal{G}) \cap \mathcal{G}_{1,2} \neq \varnothing$.

2) *For the zeroless* $\mathbb{F}_{(9,3)}^{[7,8]}(8)$*, its multiplicative* 3*-group* $\mathcal{G}_3^{[5,8]}(6) = \{7, 15, 23, 31, 39, 47, 55, 63\}$ *has two units* $e_1 = 31 \equiv 31_e$*,* $e_2 = 63 \equiv 63_e$*, and it splits into two nonintersecting nonunital cyclic* 3*-subgroups (*$\lambda_p = 4$ *and* $\lambda_p = 2$*) and the subgroup of units*

$$\mathcal{G}_1 = \left\{7^{\langle 1\rangle_{\times 3}} = 23, 7^{\langle 2\rangle_{\times 3}} = 39, 7^{\langle 3\rangle_{\times 3}} = 55, 7^{\langle 4\rangle_{\times 3}} = 4\right\},\ \bar{7} = 55, \overline{55} = 7, \overline{23} = 39, \overline{39} = 23,$$

$$\mathcal{G}_2 = \left\{15^{\langle 1\rangle_{\times 3}} = 47, 15^{\langle 2\rangle_{\times 3}} = 15\right\},\quad \overline{15} = 47, \overline{47} = 15,$$

$$E(\mathcal{G}) = \{31_e, 63_e\}.$$

There are no ℓ_μ*-reflections, and so* $E(\mathcal{G})$ *splits out* $E(\mathcal{G}) \cap \mathcal{G}_{1,2} = \varnothing$.

If all elements are units $E(\mathcal{G}) = \mathcal{G}_n^{[a,b]}(q)$, then, obviously, this group is 1-idempotent, and $\lambda_p = 1$.

Assertion 5.28. If $\mathbb{F}_{(m,n)}^{[a,b]}(q)$ is zeroless-nonunital, then there no n-ary cyclic subgroups in $\mathcal{G}_n^{[a,b]}(q)$.

The subfield structure of $\mathbb{F}_{(m,n)}^{[a,b]}(q)$ can coincide with the corresponding subgroup structure of the multiplicative n-ary group $\mathcal{G}_n^{[a,b]}(q_*)$, only if its additive m-ary group has the same subgroup structure. However, additive m-ary groups of all polyadic fields $\mathbb{F}_{(m,n)}^{[a,b]}(q)$ have the same structure: they are cyclic and have no proper m-ary subgroups, each element generates all other elements, i.e. it is a primitive root. Therefore, we arrive at

Theorem 5.29. *The polyadic field* $\mathbb{F}_{(m,n)}^{[a,b]}(q)$*, being isomorphic to the* (m,n)*-field of polyadic integer numbers* $\mathbb{Z}_{(m,n)}^{[a,b]}(q)$*, has no any proper subfield.*

In this sense, $\mathbb{F}_{(m,n)}^{[a,b]}(q)$ can be named a *prime polyadic field*.

6. CONCLUDING REMARKS

Recall that any binary finite field has an order which is a power of a prime number $q = p^r$ (its characteristic), and all such fields are isomorphic and contain a prime subfield $GF(p)$ of order p which is isomorphic to the congruence (residue) class field $\mathbb{Z}/p\mathbb{Z}$ [1].

Conjecture 6.1. *A finite* (m,n)*-field (with* $m > n$*) should contain a minimal subfield which is isomorphic to one of the prime polyadic fields constructed above, and therefore* $\mathbb{F}_{(m,n)}^{[a,b]}(q)$ *can be interpreted as a polyadic analog of* $GF(p)$.

This conjecture opens the promising possibility that the presented unusual properties of the polyadic finite fields (which do not exist in binary fields) could have non-standard applications (e.g. in number theory, cryptography and coding theory) and could lead to a specific polyadic version of the Galois theory.

ACKNOWLEDGEMENTS

The author would like to express his sincere thankfulness to Joachim Cuntz, Christopher Deninger, Mike Hewitt, Maurice Kibler, Grigorij Kurinnoj, Daniel Lenz, Jim Stasheff, Alexander Voronov, and Wend Werner for fruitful discussions.

APPENDIX. MULTIPLICATIVE PROPERTIES OF EXOTIC FINITE POLYADIC FIELDS

Here we list concrete examples of finite polyadic fields which have properties that are not possible in the binary case (see TABLE 3). Only the multiplication of fields will be shown, because their additive part is huge (many pages) for higher arities, and does not carry so much distinctive information.

1) The first exotic finite polyadic field which has a number of elements which is not a prime number, or prime power (as it should be for a finite binary field) is $\mathbb{F}^{[5,6]}_{(7,3)}(6)$, which consists of 6 elements $\{5,11,17,23,29,35\}$, $q=6$, It is zeroless and contains two units $\{17,35\}\equiv\{17_e,35_e\}$, $\kappa_e=2$, and each element has the idempotence polyadic order $\lambda_p=3$, i.e. $\mu_3\left[x^7\right]=x,\ \forall x\in\mathbb{F}^{[5,6]}_{(7,3)}(6)$. The multiplication is

$$\begin{gathered}
\mu_3[5,5,5]=17,\mu_3[5,5,11]=23,\mu_3[5,5,17]=29,\mu_3[5,5,23]=35,\mu_3[5,5,29]=5,\\
\mu_3[5,5,35]=11,\mu_3[5,11,11]=29,\mu_3[5,11,17]=35,\mu_3[5,11,23]=5,\mu_3[5,11,29]=11,\\
\mu_3[5,11,35]=17,\mu_3[5,17,17]=5,\mu_3[5,17,23]=11,\mu_3[5,17,29]=17,\mu_3[5,17,35]=23,\\
\mu_3[5,23,23]=17,\mu_3[5,23,29]=23,\mu_3[5,23,35]=29,\mu_3[5,29,29]=29,\mu_3[5,29,35]=35,\\
\mu_3[5,35,35]=5,\mu_3[11,11,11]=35,\mu_3[11,11,17]=5,\mu_3[11,11,23]=11,\mu_3[11,11,29]=17,\\
\mu_3[11,11,35]=23,\mu_3[11,11,17]=5,\mu_3[11,17,17]=11,\mu_3[11,17,23]=17,\mu_3[11,17,29]=23,\\
\mu_3[11,17,35]=29,\mu_3[11,17,23]=17,\mu_3[11,17,29]=23,\mu_3[11,17,35]=29,\mu_3[11,23,23]=23,\\
\mu_3[11,23,29]=29,\mu_3[11,23,23]=23,\mu_3[11,23,35]=35,\mu_3[11,29,29]=35,\mu_3[11,29,35]=5,\\
\mu_3[11,35,35]=11,\mu_3[17,17,17]=17,\mu_3[17,17,23]=23,\mu_3[17,17,29]=29,\mu_3[17,17,35]=35,\\
\mu_3[17,23,23]=29,\mu_3[17,23,29]=35,\mu_3[17,29,29]=5,\mu_3[17,29,35]=11,\mu_3[17,35,35]=17,\\
\mu_3[23,23,23]=35,\mu_3[23,23,29]=5,\mu_3[23,23,35]=11,\mu_3[23,29,29]=11,\mu_3[23,29,35]=17,\\
\mu_3[23,35,35]=23,\mu_3[29,29,29]=17,\mu_3[29,29,35]=23,\mu_3[29,35,35]=29,\mu_3[35,35,35]=35.
\end{gathered}$$

The multiplicative querelements are $\bar{5}=29,\overline{29}=5,\overline{11}=23,\overline{23}=11$. Because

$$5^{\langle1\rangle_{\times3}}=17_e,\ 5^{\langle2\rangle_{\times3}}=29,\ 5^{\langle3\rangle_{\times3}}=5,\ 29^{\langle1\rangle_{\times3}}=17_e,\ 29^{\langle2\rangle_{\times3}}=5,\ 29^{\langle3\rangle_{\times3}}=29, \tag{A.1}$$

$$11^{\langle1\rangle_{\times3}}=35_e,\ 11^{\langle2\rangle_{\times3}}=23,\ 11^{\langle3\rangle_{\times3}}=11,\ 23^{\langle1\rangle_{\times3}}=35_e,\ 23^{\langle2\rangle_{\times3}}=11,\ 23^{\langle3\rangle_{\times3}}=23, \tag{A.2}$$

the multiplicative 3-ary group $\mathcal{G}^{[5,6]}_{(7,3)}(6)$ consists of two *nonintersecting* cyclic 3-ary subgroups

$$\mathcal{G}^{[5,6]}_{(7,3)}(6)=\mathcal{G}_1\cup\mathcal{G}_2,\quad \mathcal{G}_1\cap\mathcal{G}_2=\varnothing, \tag{A.3}$$

$$\mathcal{G}_1=\{5,17_e,29\}, \tag{A.4}$$

$$\mathcal{G}_2=\{11,23,35_e\}, \tag{A.5}$$

which is impossible for binary subgroups, as these always intersect in the identity of the binary group.

2) The finite polyadic field $\mathbb{F}^{[5,6]}_{(7,3)}(4)=\{\{5,11,17,23\}\mid\nu_7,\mu_3\}$ which has the same arity shape as above, but with order 4, has the exotic property that *all elements* are units, which follows from its multiplication

$$\begin{gathered}
\mu_3[5,5,5]=5,\mu_3[5,5,11]=11,\mu_3[5,5,17]=17,\mu_3[5,5,23]=23,\mu_3[5,11,11]=5,\\
\mu_3[5,11,17]=23,\mu_3[5,11,23]=17,\mu_3[5,17,17]=5,\mu_3[5,17,23]=11,\mu_3[5,23,23]=5,\\
\mu_3[11,11,11]=11,\mu_3[11,11,17]=17,\mu_3[11,11,23]=23,\mu_3[11,17,17]=11,\mu_3[11,17,23]=5,\\
\mu_3[11,23,23]=11,\mu_3[17,17,17]=17,\mu_3[17,17,23]=23,\mu_3[17,23,23]=17,\mu_3[23,23,23]=23.
\end{gathered}$$

3) Next we show by construction, that (as opposed to the case of binary finite fields) there exist *non-isomorphic* finite polyadic fields of the same order and arity shape. Indeed, consider these two $(9,3)$-fields of order 2, that are $\mathbb{F}^{[3,8]}_{(9,3)}(2)$ and $\mathbb{F}^{[7,8]}_{(9,3)}(2)$. The first is zeroless-nonunital, while the second is zeroless with two units, i.e. all elements are units. The multiplication of $\mathbb{F}^{[3,8]}_{(9,3)}(2)$ is

$$\mu_3[3,3,3]=11,\ \mu_3[3,3,11]=3,\ \mu_3[3,11,11]=11,\ \mu_3[11,11,11]=3,$$

having the multiplicative querelements $\bar{3}=11, \overline{11}=3$. For $\mathbb{F}^{[7,8]}_{(9,3)}(2)$ we get the 3-group of units

$$\mu_3[7,7,7]=7,\ \mu_3[7,7,15]=15,\ \mu_3[7,15,15]=7,\ \mu_3[15,15,15]=15.$$

They have different idempotence polyadic orders $\operatorname{ord}\mathbb{F}^{[3,8]}_{(9,3)}(2)=2$ and $\operatorname{ord}\mathbb{F}^{[7,8]}_{(9,3)}(2)=1$. Despite their additive m-ary groups being isomorphic, it follows from the above multiplicative structure, that it is not possible to construct an isomorphism between the fields themselves.

4) The smallest exotic finite polyadic field with more than one unit is $\mathbb{F}^{[2,3]}_{(4,3)}(5)=\{\{2,5,8,11,14\}\mid\nu_4,\mu_3\}$ of order 5 with two units $\{11,14\}\equiv\{11_e,14_e\}$ and the zero $5\equiv 5_z$. The presence of zero allows us to define the polyadic characteristic (4.17) which is 3 (see TABLE 1), because the 3rd additive power of all elements is equal to zero

$$2^{\langle 3\rangle_{+4}}=8^{\langle 3\rangle_{+4}}=11_e^{\langle 3\rangle_{+4}}=14_e^{\langle 3\rangle_{+4}}=5_z. \tag{A.6}$$

The additive querelements are

$$\tilde{2}=11_e,\ \ \tilde{8}=14_e,\ \ \widetilde{11}_e=8,\ \ \widetilde{14}_e=2. \tag{A.7}$$

The idempotence polyadic order is $\operatorname{ord}\mathbb{F}^{[2,3]}_{(4,3)}(5)=2$, because for nonunit and nonzero elements

$$2^{\langle 2\rangle_{\times 3}}=2,\ \ 8^{\langle 2\rangle_{\times 3}}=8, \tag{A.8}$$

and their multiplicative querelements are $\bar{2}=8$, $\bar{8}=2$. The multiplication is given by the cyclic 3-ary group $\mathcal{G}^{[2,3]}_3(4)=\{\{2,8,11,14\}\mid\mu_3\}$ as:

$$\begin{gathered}\mu_3[2,2,2]=8,\mu_3[2,2,8]=2,\mu_3[2,2,11]=14,\mu_3[2,2,14]=11,\mu_3[2,8,8]=8,\\ \mu_3[2,8,11]=11,\mu_3[2,8,14]=14,\mu_3[2,11,11]=2,\mu_3[2,11,14]=8,\mu_3[2,14,14]=2,\\ \mu_3[8,8,8]=2,\mu_3[8,8,11]=14,\mu_3[8,8,14]=11,\mu_3[8,11,11]=8,\mu_3[8,11,14]=2,\\ \mu_3[8,14,14]=8,\mu_3[11,11,11]=11,\mu_3[11,11,14]=14,\mu_3[11,14,14]=11,\mu_3[14,14,14]=14.\end{gathered}$$

We observe that, despite having two units, the cyclic 3-ary group $\mathcal{G}^{[2,3]}_3(4)$ has no decomposition into nonintersecting cyclic 3-ary subgroups, as in (A.3). One of the reasons is that the polyadic field $\mathbb{F}^{[5,6]}_{(7,3)}(6)$ is zeroless, while $\mathbb{F}^{[2,3]}_{(4,3)}(5)$ has a zero (see **Assertion 5.26**).

REFERENCES

1. R. Lidl and H. Niederreiter, *Finite Fields* (Cambridge Univ. Press, Cambridge, 1997).
2. G. L. Mullen and D. Panario, *Handbook of Finite Fields* (CRC Press, Boca Raton, 2013).
3. A. J. Menezes, P. C. van Oorschot and S. A. Vanstone, *Handbook of Applied Cryptography* (CRC Press, Boca Raton, 1997).
4. S. Duplij, "Arity shape of polyadic algebraic structures," preprint Math. Inst., Muenster, 43 pp., arXiv: math.RA/1703.10132 (2017).
5. G. Crombez, "On (n,m)-rings," Abh. Math. Semin. Univ. Hamb. **37**, 180 (1972).
6. J. J. Leeson and A. T. Butson, "On the general theory of (m,n) rings," Algebra Univers. **11**, 42 (1980).
7. A. Pop and M. S. Pop, "Some embeddings theorems for $(n,2)$-rings," Bul. Ştiinţ. Univ. Baia Mare, Ser. B, Fasc. Mat.-Inform. **18**, 311 (2002).
8. S. Duplij and W. Werner, "Structure of unital 3-fields," preprint Math. Inst., Muenster, 17 pp., arXiv: math.RA/1505.04393 (2015).
9. S. Duplij, "Polyadic systems, representations and quantum groups," J. Kharkov National Univ., ser. Nuclei, Particles and Fields **1017**, 28 (2012). Extended version in arXiv: math.RT/1308.4060.