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/S2070046617040033

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: duplij@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 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 \( R_{m,n} = \langle R \mid \nu_m, \mu_n \rangle \), where \( R \) is a set, equipped with \( m \)-ary addition \( \nu_m : R^m \to R \) and \( n \)-ary multiplication \( \mu_n : R^n \to R \) which are connected by the polyadic distributive law, such that \( \langle R \mid \nu_m \rangle \) is a commutative \( m \)-ary group and \( \langle R \mid \mu_n \rangle \) is a semigroup. A commutative (cancellative) polyadic ring has a commutative (cancellative) \( n \)-ary multiplication \( \mu_n \).

A polyadic ring is called derived, if \( \nu_m \) and \( \mu_n \) 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 \( \nu_m \) (or \( \mu_n \)) has this property, we call such a \( R_{m,n} \) additively (or multiplicatively) derived (half-derived).

In distinction to binary rings, an \( n \)-admissible “length of word \((x)\)” should be congruent to 1 mod \((n−1)\), containing \( \ell_m (n−1) + 1 \) elements (\( \ell_m \) is a “number of multiplications”) \( \mu_n^{(\ell_m)} [x] (x \in R^{\ell_m(n−1)+1}) \), so called \((\ell_m (n−1) + 1)\)-ads, or polyads. An \( m \)-admissible “quantity of words \((y)\)” in a polyadic “sum” has to be congruent to 1 mod \((m−1)\), i.e. consisting of \( \ell_m (m−1) + 1 \) summands (\( \ell_m \) is a “number of additions”) \( \nu_m^{(\ell_m)} [y] (y \in R^{\ell_m(m−1)+1}) \). Therefore, a straightforward “polyadization” of any binary expression \((m = n = 2)\) can be introduced as follows: substitute the number of multipliers \( \ell_m + 1 \to \ell_m (n−1) + 1 \) and number of summands \( \ell_m + 1 \to \ell_m (m−1) + 1 \), respectively.

An example of “trivial polyadization” is the simplest \((m, n)\)-ring derived from the ring of integers \( \mathbb{Z} \) as the set of \( \ell_m (n−1) + 1 \) “sums” of \( n \)-admissible \((\ell_m (n−1) + 1)\)-ads \( (x) \), where \( x \in \mathbb{Z}^{\ell_m(n−1)+1} \).

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

\[
\begin{align*}
x^{(\nu_m) + m} &= \nu_m^{(\ell_m)} \left[ x^{\ell_m(m−1)+1} \right], \\
x^{(\mu_n) \times n} &= \mu_n^{(\ell_m)} \left[ x^{\ell_m(n−1)+1} \right], \\
x &\in R,
\end{align*}
\]

(2.1)

such that the polyadic powers and ordinary powers differ by one: \( x^{(\nu_m) + 2} = x^{\ell_m+1}, x^{(\mu_n) \times 2} = x^{\ell_m+1} \).

The \textit{polyadic idempotents} in \( R_{m,n} \) satisfy

\[
x^{(\nu_m) + m} = x, \quad x^{(\mu_n) \times n} = x,
\]

(2.2)

and are called the \textit{additive} \( \nu_i \)-\textit{idempotent} and the \textit{multiplicative} \( \mu_i \)-\textit{idempotent}, respectively.

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

\[
\nu_m [x, z] = z, \quad \forall x \in R^{m−1}.
\]

(2.3)

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

The \textit{unit} \( e \) of \( R_{m,n} \) is a multiplicative 1-idempotent which is defined (if it exists) as

\[
\mu_n [e^{n−1}, x] = x, \quad \forall x \in R,
\]

(2.4)