



UDC 519.872:519.217

PACS 07.05.Tp, 02.60.Pn, 02.70.Bf

DOI: 10.22363/2658-4670-2021-29-4-387-398

On involutive division on monoids

Oleg K. Kroytor¹, Mikhail D. Malykh^{1,2}

¹ Peoples' Friendship University of Russia (RUDN University)
6, Miklukho-Maklaya St., Moscow, 117198, Russian Federation

² Meshcheryakov Laboratory of Information Technologies
Joint Institute for Nuclear Research, Dubna, Russia
6, Joliot-Curie St., Dubna, Moscow Region, 141980, Russian Federation

(received: September 1, 2021; accepted: September 22, 2021)

We consider an arbitrary monoid M , on which an involutive division is introduced, and the set of all its finite subsets $\text{Set } M$. Division is considered as a mapping $d : \text{Set } M \times M$, whose image $d(U, m)$ is the set of divisors of m in U . The properties of division and involutive division are defined axiomatically. Involutive division was introduced in accordance with the definition of involutive monomial division, introduced by V. P. Gerdt and Yu. A. Blinkov. New notation is proposed that provides brief but explicit allowance for the dependence of division on the $\text{Set } M$ element. The theory of involutive completion (closures) of sets is presented for arbitrary monoids, necessary and sufficient conditions for completeness (closedness) — for monoids generated by a finite set X . The analogy between this theory and the theory of completely continuous operators is emphasized. In the last section, we discuss the possibility of solving the problem of replenishing a given set by successively expanding the original domain and its connection with the axioms used in the definition of division. All results are illustrated with examples of Thomas monomial division.

Key words and phrases: involutive monomial division, Gröbner basis

1. Introduction

The creation of the technique of involutive bases as an alternative to the classical Gröbner bases and its application to the study of ideals in polynomial and differential rings is undoubtedly one of the most important contributions made by V. P. Gerdt and his disciples in computer algebra.

The concept of involutive division came to algebras from the compatibility studies of systems of partial differential equations, dating back to the works of Riquier [1], Janet [2], Thomas [3]. Since the mid-1990s, V. P. Gerdt and his students A. Yu. Zharkov and Yu. A. Blinkov have published a series of papers in which this concept was developed in an abstract algebraic form and indicated the wide possibilities of using involutive bases as an alternative to



the usual Gröbner bases. The first example of involutive division — Pomare division — was introduced by Zharkov in 1993 [4]–[7].

In general terms, the concept of involutive division was introduced by Gerdt and Blinkov in [8]–[11]. V. P. Gerdt strove for an axiomatic presentation of the concept of involutive division, especially emphasizing this in his report made at RUDN University in November 2020 [12]. In our opinion, the theory of divisions on monoids, cleared of applied issues, looks like a self-sufficient and very elegant theory, which is complete only to the extent that was of interest for applied researchers. We have tried to present it in general terms.

We based on §1.2 from the Dr. Sci. thesis by Blinkov [13], but have significantly revised the terminology. The fact is that the creators of this theory obviously intended to give it a topological interpretation, but, unfortunately, they never did it. Therefore, a number of terms (continuity of division, closure of sets) refer to this so far unknown topology. In our opinion, this topology is the Zariski topology, and therefore incidental analogies taken from the \mathbb{R} topology greatly hinder its development.

2. Divisions on monoids

Definition 1. A set is called a monoid if a binary associative operation called multiplication is specified on it, and there is an element 1 such that $1m = m$ for any $m \in M$.

The set of all finite subsets of the set M will be denoted as $\text{Set } M$. For definiteness, we will assume that $\emptyset \in \text{Set } M$.

Definition 2. By division on the monoid M we mean the mapping

$$d : \text{Set } M \times M \rightarrow \text{Set } M,$$

having the following properties:

1. $d(U, m) \subset U$,
2. $u \in d(U, u)$,
3. if $u \in d(U, m)$, then there is an element $m^* \in M$ such that $m = um^*$,
4. if $u \in d(U, mu)$ and $u \in d(U, m'u)$, then $u \in d(U, mm'u)$,
5. if $U' \subset U$, then $d(U, m) \cap U' \subset d(U', m)$,

valid for any $U, U' \in \text{Set } M$, $u \in U$, $m, m' \in M$. Elements of the image $d(U, m)$ will be called divisors of m in U and m is said divisible by elements of $d(U, m)$.

Remark 1. We have split the definition of involutive division from [13, def. 5] into the definition of division in general and involutive division (def. 4 below). The notation has been changed. The notation $u|_{\mathcal{L}(U)}m$ used in [13] is now changed for $u \in d(U, m)$.

Example 1. Assuming $d(U, m) = \{u \in U : \exists m^* \in M : m^*u = m\}$, we will define the standard division on the monoid.

If there is a set $X \in \text{Set } M$ such that any element of the set M other than 1 can be represented as a product of elements from X , then the monoid is said to be generated by the set X . If such a representation is unique for an element of the set M , then M is said to be a set of monomials, and the elements of the set X are treated as variables.

Definition 3. An element $x \in X$ will be called multiplicative for u with respect to U if $u \in d(U, xu)$.

The set of all multiplicative elements for u relative to U will be denoted as $X_d(U, u)$.

Theorem 1. If x_1, \dots, x_s are multiplicative elements of X for u with respect to U , then $u \in d(U, x_1^{j_1} \dots x_s^{j_s} u)$.

Proof. Corollary of the 4th property of definition 2. □

To define division on a monoid generated by the set X , it is enough to specify X_d .

Theorem 2. Suppose that a finite set X generates a monoid M and some mapping is given $X_d : \text{Set } M \times M \rightarrow \text{Set } X$.

Let us define the function $d : \text{Set } M \times M \rightarrow \text{Set } M$ as follows: $u \in d(U, m)$ if and only if $u \in U$ and there exists a product of m^* elements from $X_d(U, u)$ such that $m = m^*u$. The function d defines division by M if and only if the embedding $U' \subset U$ implies

$$X_d(U, u) \subset X_d(U', u) \quad \forall u \in U'. \tag{1}$$

Remark 2. In [13] it was noted that “involutive division for a monomial can be specified by defining sets of multiplicative and non-multiplicative variables”. We have formulated this idea in the form of theorems 1 and 2. They seem to be mutually inverse. However, according to theorem 1

$$v = \prod_{x \in X} x^{j_x} \implies u \in d(U, vu),$$

and theorem 2 does not reverse the arrow, but asserts that if the condition (1) is satisfied, we can define a division by M such that

$$v = \prod_{x \in X} x^{j_x} \iff u \in d(U, vu).$$

Proof. Property 1 of definition 2 is fulfilled, since by construction of d , the element $u \in d(U, m)$ only if $u \in U$. Property 2 is satisfied, since for $m = u$ one can take $m^* = 1$. Property 3 is fulfilled because m^* is explicitly specified when constructing d .

Property 4 is fulfilled, since by the construction of d the embeddings $u \in d(U, mu)$ and $u \in d(U, m'u)$ mean that there exist products v, v' of elements from $X_d(U, u)$ such that $mu = vu$ and $m'u = v'u$. But then $mm'u = vv'u$ and, since vv' is the product of elements from $X_d(U, u)$, $u \in d(U, mm'u)$.

Now we turn to property 5. Let $U' \subset U$ and $u \in d(U, m) \cap U'$, then $u \in U'$ and there exists a product of m^* of elements from $X_d(U, u)$ such that $m = m^*u$. From this it follows that $u \in d(V, m)$ if and only if $X_d(U, u) \subset X_d(U', u)$, i.e., the ratio (1) is true. □

Example 2. Consider the set M of all monomials generated by the n variables $X = (x_1, \dots, x_n)$. Let us agree to write $\partial_i x_1^{j_1} \dots x_n^{j_n} = j_i$.

Thomas division is determined by the formula

$$x_i \in X_d(U, u) \Leftrightarrow \partial_i u = \max_{v \in U} \partial_i v.$$

Let us check the condition (1). Let $u \in U' \subset U$. If $x_i \in X_d(U, u)$, then the maximum of $\partial_i v$ on U is achieved when $v = u \in U'$. Since $U' \subset U$,

$$\max_{v \in U'} \partial_i v \leq \max_{v \in U} \partial_i v$$

and, therefore, the maximum is attained at $v = u$. This is what condition (1) asserts.

3. Involutive divisions on monoids

Definition 4. A division d will be called involutive if for any $U \in \text{Set } M$ and $m \in M$ the set $d(U, m)$

1. is empty,
2. consists of one element,
3. consists of several elements, and then for any $u, u' \in d(U, m)$, it is strictly true that either $u \in d(U, u')$, or $u' \in d(U, u)$.

The maximum number of distinct elements that make up $d(U, m)$ for any $U \in \text{Set } M$ and $m \in M$ will be called the rank of the involutive division of d .

Remark 3. Simultaneous execution of equalities $u \in d(U, u')$, $u' \in d(U, u)$ by virtue of property 3 of definition 2, implies the existence of two elements $v, v' \in M$ such that $u' = vu$ and $u = v'u'$. In a monomial set, the simultaneous fulfillment of these equalities means that $v = v' = 1$ and therefore $u = u'$. Thus, only one of them can be fulfilled in definition 4. Definition 4 implies that only one of these equalities holds in the case of an arbitrary monoid.

Definition 4 allows ordering the linearly finite set $d(U, m)$:

$$u \in d(U, u') \text{ and } u \neq u' \Leftrightarrow u < u'.$$

Therefore, there exists a single maximal element, i.e., an element u such that $d(U, m) \subset d(U, u)$. This can be taken as a definition of involutivity, equivalent to the previous one.

Definition 5. A division d will be called involutive if, for any $U \in \text{Set } M$ and $m \in M$, there exists and, moreover, a unique element $u \in U$ such that

$$d(U, m) \subset d(U, u).$$

Example 3. Let us describe the Thomas division in more detail. Let U be a finite subset of the set M_n of all monomials in n variables. For brevity we put

$$r_i = \max_{w \in U} \partial_i w.$$

These numbers only depend on U . Let $u \in d(U, m)$, then there is a product of v variables from $X_d(U, u)$ such that $m = uv$. Then $\partial_i m = \partial_i u + \partial_i v$.

If $x_i \in X_d(U, u)$, then $\partial_i v \geq 0$ and $\partial_i u = r_i$, whence $\partial_i v = \partial_i m - r_i \geq 0$.

If $x_i \notin X_d(U, u)$, then $\partial_i v = 0$ and $\partial_i u < r_i$, where $r_i > \partial_i u = \partial_i m - 0$.

Thus, combining both cases,

$$\partial_i v = \begin{cases} \partial_i m - r_i & \partial_i m \geq r_i \\ 0 & \partial_i m < r_i \end{cases}$$

and

$$\partial_i u = \partial_i \frac{m}{v} = \begin{cases} r_i & \partial_i m \geq r_i \\ \partial_i m & \partial_i m < r_i \end{cases} = \min(\partial_i m, r_i).$$

Thus, u is uniquely determined by specifying U and m . It is already clear from this that the Thomas division is an involutive division of the 1st rank. However, we also obtained an explicit formula for $d(U, m)$. If $\partial_i u = \min(\partial_i m, r_i)$ specifies an element u from U , then $d(U, m)$ consists of this one element. If this element does not belong to U , then $d(U, m)$ is empty.

4. Complete sets and completely involutive divisions

Let again $U \in \text{Set } M$.

Definition 6. A set of elements of the form mu , where $u \in U$ and $m \in M$, will be called a cone generated by the set U and denoted as $C(U)$.

Definition 7. The set of elements $m \in M$ such that $d(U, m) \neq \emptyset$, will be called an involutive cone generated by the set U and denoted as $I_d(U)$.

By virtue of property 3 of definition 2, $I_d(U) \subseteq C(U)$.

Definition 8. A set $U \in \text{Set } M$ is called complete with respect to the involutive division of d if the involutive cone generated by it coincides with the usual one, i.e., $I_d(U) = C(U)$.

Remark 4. In [13], instead of 'complete sets', the term 'closed sets' is used. We prefer the term 'complete' because it does not give rise to connotations with some topology on $\text{Set } M$.

Example 4. In M_n the embedding $m \in C(U)$ means that there is an element $u \in U$ such that $\partial_i m \geq \partial_i u \quad \forall i = 1, 2, \dots, n$. With respect to Thomas

division, $m \in C(U)$ is divisible by U if and only if v with $\partial_i v = \min(\partial_i m, r_i)$ belongs to U . Let U contain all monomials u satisfying the inequalities

$$c_i \leq \partial_i u \leq r_i \quad \forall i = 1, 2, \dots, n,$$

where c_1, \dots, c_n are non-negative integers. Then

$$\partial_i m \geq \partial_i u \geq c_i \quad \forall i = 1, 2, \dots, n,$$

and therefore $c_i \leq \partial_i v = \min(\partial_i m, r_i) \leq r_i$ and $v \in U$. Therefore, such a set U is complete with respect to the Thomas division.

Definition 9. A set $U^* \in \text{Set } M$ is called a completion of the set $U \in \text{Set } M$ with respect to division d if

1. U is a subset of the set U^* ,
2. U^* is a complete set with respect to division of d , that is, $I_d(U^*) = C(U^*)$,
3. $C(U) = C(U^*)$.

Definition 10. An involutive division d is called completely involutive if each set from $\text{Set } M$ has completion with respect to this division.

Remark 5. In [13], such divisions are called Noetherian, which requires a rather lengthy explanation of the connection between the issue and the finiteness of the ideal bases.

Example 5. For the Thomas division, the completion can be described explicitly: the completion of U is the set $U^* \in \text{Set } M_n$ formed by the monomials v with the following property: there exists a monomial $u \in U$ such that

$$\partial_i u \leq \partial_i v \leq r_i.$$

Indeed, by the construction of U^* , $U \subseteq U^*$ holds, that is, property 1 of definition 9. The fulfillment of the 3rd property is also obvious, since $U^* \subset C(U)$ by construction.

Let us check the second property. Let $m \in C(U^*)$, that is, there is a monomial $u^* \in U^*$ and a monomial $v \in M_n$ such that $m = u^* v$, where $\partial_i m \geq \partial_i u^*$.

By the construction of U^* , this implies that for m one can specify a monomial $u \in U$ such that $\partial_i m \geq \partial_i u$. On the other hand, the monomial m is divisible by U^* if and only if the monomial u^* with $\partial_i u^* = \min(\partial_i m, r_i)$ belongs to U^* . But this is indeed the case, since $\partial_i u \leq \min(\partial_i m, r_i) \leq r_i$.

This means that $C(U^*) = I_T(U^*)$, that is, U^* is a complete set. This is the second property.

Remark 6. Historically, the concept of Pomare division was first introduced, it is involutive, and not completely involutive, which is a source of various kinds of pathological examples, see [13, example 55] and also [4], [14], [15].

5. Necessary and sufficient conditions for the completeness of a set

Theorem 3 (necessary completeness condition). *Let the monoid M be generated by elements of a finite set X . For the set M to be complete with respect to the division of d , it is necessary that*

$$d(U, xu) \neq \emptyset \quad \forall u \in U, \forall x \in X. \tag{2}$$

This condition is sufficient only for a certain class of divisions.

Definition 11. A sequence $\{u_0, u_1, \dots\}$ of elements of the set U will be called fundamental if for any i there is an element $x_i \in X$ such that:

1. $u_i \notin d(U, x_i u_i)$,
2. $u_{i+1} \in d(U, x_i u_i)$.

Definition 12. A division of d by the monoid M will be called finite if every fundamental sequence is finite.

Remark 7. In [13], division is called continuous if every finite fundamental sequence does not contain two identical terms. In this case, any piece of an infinite fundamental sequence is shorter than the total number of elements in U and the division is finite in the sense of our definition. However, to prove theorem 4, the 'continuity' requirement can be weakened to that described in our definition.

Remark 8. In our opinion, this construction is much more similar to the concept of a completely continuous mapping, and not just a continuous one. For this reason, we call the sequences from definition 11 fundamental, and the property described in the definition 10, complete involutivity.

Theorem 4. *If d is a finite involutive division on the monoid M generated by elements of the finite set X , then for the set U to be complete it is necessary and sufficient that condition (2) be satisfied.*

Proof. Let condition (2) be satisfied for the set U . Take $u \in U$ and $m \in M$ in an arbitrary way and construct a divisor of mu in U as follows.

Let us take u as the first element u_0 of the sequence of elements U . If $u_0 \in d(U, um)$, then we will not do anything. If $u_0 \notin d(U, um)$, then among the factors m from X there is x_0 such that $u_0 \notin d(U, u_0 x_0)$ by theorem 1. But by virtue of (2) then there exists $u_1 \in U$ such that $u_1 \in d(U, u_0 x_0)$.

If $u_1 \in d(U, um)$, then we will not do anything. Otherwise, there is an element $x_1 \in X$ such that $u_1 \notin d(U, u_1 x_1)$.

Then, by virtue of (2), there is an element $u_2 \in U$ such that $u_2 \in d(U, u_1 x_1)$.

Proceeding on like this, we get a sequence $\{u_0, u_1, \dots\}$ of U elements.

The described sequence is fundamental (definition 11). Under the conditions of the theorem being proved, it is indicated that d is a finite division, therefore every fundamental sequence is finite. By construction, its last element is a divisor of um in U .

Thus, every element um has a divisor in U , that is, U is a complete set. \square

Example 6. In the case of Thomas division, the set $d(U, u_i x_{k_i})$ consists of one element u_{i+1} , and $\partial_j u_{i+1} = \min(\partial_j u_i x_{k_i}, r_j)$.

For $j \neq k_i$

$$\partial_j u_{i+1} = \min(\partial_j u_i, r_j) = \partial_j u_i.$$

since $u_i \in U$. For $j = k_i$

$$\partial_{k_i} u_{i+1} = \min(\partial_{k_i} u_i + 1, r_{k_i}) = \partial_{k_i} u_i + 1,$$

because otherwise it would be $\partial_{k_i} u_i + 1 > r_{k_i}$, which contradicts $u_i \in U$. Thus, $u_{i+1} = u_i x_{k_i}$.

From this, in particular, it is clear that there are no coinciding elements among the elements. Since there is a finite number of products of U and X , the fundamental sequence is finite.

6. Set completion

Problem. Given $U \in \text{Set } M$ and a finite completely involutive division of d by M , it is required to find its completion with respect to d .

In the specified class of divisions, this problem always has a solution (definition 10). For Thomas division, we know its explicit solution (example 5). For other divisions, it would be desirable to solve the problem, gradually supplementing U with new elements.

So, let U be given. By searching over two finite sets, we seek all pairs $u \in U$ and $x \in X$ such that $d(U, xu) = \emptyset$.

If there is no such pair, then the completion $U^* = U$ (theorem 4) and the problem is solved. If there are such pairs, then we add one of the products xu obtained in this way to the set U and obtain the set U_1 . Proceeding on like this, we will expand U more and more, while remaining inside the cone $C(U)$. If this process is interrupted at the n -th step, then the resulting set is complete by virtue of theorem 4. This will be the completion U^* of the set U by definition 9. However, the finiteness of U^* does not imply finiteness of the described process, since we can get sets that contain elements that are absent in U^* . To avoid this, it is necessary to indicate a rule for choosing a pair from the set of pairs $u \in U_n$ and $x \in X$ such that $d(U_n, xu) = \emptyset$, which guarantees the embedding $U_n \subset U^*$ at each step.

The simplest option is to take an element that is in some sense minimal, but for this purpose we have to restrict ourselves to the special case when the monoid is the set of monomials in n variables that make up the set X . Let this set be given a monomial order, say, deglex.

Given U , among the pairs $u \in U$ and $x \in X$ such that $d(U, xu) = \emptyset$, we take the one for which the product ux is minimal. By virtue of property 5 of definition 2

$$d(U^*, xu) \cap U \subset d(U, xu) = \emptyset.$$

That is why $v \in d(U^*, xu) \notin U$.

By virtue of property 3 of definition 2 there is an element $m \in M$ such that $xu = vm$. If $m = 1$, then $xu = v \in U^*$ and $U_1 = U \cup \{xu\} \subset U^*$ and you can go to the next step.

Regarding the second option, when $m > 1$, one can notice the following.

Theorem 5. *If $m > 1$, then $d(U, v)$ is not empty.*

Proof. Since $v \in U^* \subset C(U)$, there exists a pair $u_1 \in U$ and $m_1 \in M$ such that $v = m_1 u_1$.

If $m_1 = 1$, then $v = u_1 \in U$, which is impossible. Therefore, $m_1 > 1$. Therefore, $xu = u_1 m m_1$, $m, m_1 > 1$.

This means that $u_1 y < ux$ for any $y \in X$. Since we initially chose the minimum pair, $d(U, u_1 y) \neq \emptyset \quad \forall y \in X$.

Let us denote the set of variables that are included in m_1 as Y .

If $u_1 \in d(U, u_1 y) \quad \forall y \in Y$, then by virtue of theorem 1, $u_1 \in d(U, u_1 m_1) = d(U, v)$, i.e., $d(U, v)$ is not empty.

Otherwise, there is $y_1 \in Y$ such that $u_1 \notin d(U, u_1 y_1)$.

The set $d(U, u_1 y_1)$ itself is not empty, let $u_2 \in U$ belong to it, then $u_1 \neq u_2$ and there exists $m_2 \in M$ such that $u_1 y_1 = u_2 m'$. But then

$$v = u_1 m_1 = u_2 m_2, \quad m_2 = \frac{m_1 m'}{y_1},$$

and m_1 is divisible by y_1 , since $y_1 \in Y$. Thus, we get the first elements u_1, u_2 of the fundamental sequence, and $v = u_1 m_1 = u_2 m_2$.

Repeating the above considerations in relation to the representation $v = u_2 m_2$, we get either $u_2 \in d(U, v)$, or the next element of the sequence. Since every fundamental sequence is finite, at some step we get $u_n \in d(U, v)$, that is, $d(U, v) \neq \emptyset$. □

The process of solving the problem described above will stop if the following condition is met:

$$d(U, v) = \emptyset \quad \forall v \in (U^* - U). \tag{3}$$

It does not follow from property 5 of definition 2 and should be somehow imposed on the division in question.

Example 7. For the Thomas division, the completion U^* of the set U was described in example 5: it is formed by monomials v for which there exists a monomial $u \in U$ such that $\partial_i u \leq \partial_i v \leq r_i$.

The criterion of emptiness for $d(U, v)$ is indicated at the end of example 3: $d(U, v)$ is empty if and only if $\partial_i w = \min(\partial_i v, r_i)$ specifies an element w that is not in U . For $v \in U^*$ this equality reduces to the trivial $\partial_i w = \partial_i v$, that is, $w = v$. By hypothesis, $v \notin U$, so $d(U, v)$ is empty.

7. Discussion

As easily seen, all the basic concepts are introduced for arbitrary monoids. The sufficient criterion for completeness (theorem 4) is proved for monoids generated by a finite set, and the algorithm for successive completion of a set only for a set of monomials. Moreover, axiom 5 of definition 2 of division appears only in the last section and, by and large, it is lacking in the proof of the correctness of the completion algorithm. Possibly, this part of the definition of division could be slightly corrected.

This axiom is the only one that suggests changing the domain. In fact, all the results presented, except for theorem 5, are satisfied for a fixed U , that is, the function d is considered as a function of one argument. Division is not a good functor from Set M to Set M . Many questions here seem to be unclear. The focus was on the completion of a set, but not the uniqueness of such a completion. Moreover, there can be obviously sets enclosed between a complete set and its cone, 'overfull' sets. They hamper proving theorem 5, but what is their true role in division theory?

Acknowledgments

This work is supported by the Russian Science Foundation (grant no. 20-11-20257).

References

- [1] C. Riquier, *Les Systèmes d'Equations aux Dérivées Partielles*. Paris: Gauthier-Villars, 1910.
- [2] M. Janet, "Systèmes d'équations aux dérivées partielles," *Journals de mathématiques, 8e série*, vol. 3, pp. 65–151, 1920.
- [3] J. Thomas, *Differential systems*. New York: American Mathematical Society, 1937.
- [4] A. Y. Zharkov, "Involutive polynomial bases: general case," in *Preprint JINR E5-94-224*. Dubna, 1994.
- [5] A. Y. Zharkov and Y. A. Blinkov, "Involutive bases of zero-dimensional ideals," in *Preprint JINR E5-94-318*. Dubna, 1994.
- [6] A. Y. Zharkov and Y. A. Blinkov, "Solving zero-dimensional involutive systems," in *Progress in Mathematics*. Basel: Birkhauser, 1996, vol. 143, pp. 389–399. DOI: 10.1007/978-3-0348-9104-2_20.
- [7] A. Y. Zharkov and Y. A. Blinkov, "Involution approach to investigating polynomial systems," *Mathematics and Computers in Simulation*, vol. 42, pp. 323–332, 1996. DOI: 10.1016/S0378-4754(96)00006-7.
- [8] V. P. Gerdt and Y. A. Blinkov, "Involutive bases of polynomial ideals," *Mathematics and Computers in Simulation*, vol. 45, no. 5–6, pp. 519–541, 1998. DOI: 10.1016/s0378-4754(97)00127-4.
- [9] V. P. Gerdt, "Gröbner bases and involutive methods for algebraic and differential equations," *Mathematical and computer modelling*, vol. 25, no. 8–9, pp. 75–90, 1997. DOI: 10.1016/S0895-7177(97)00060-5.
- [10] V. P. Gerdt and Y. A. Blinkov, "Involutive divisions of monomials," *Programming and Computer Software*, vol. 24, no. 6, pp. 283–285, 1998.
- [11] Y. A. Blinkov, "Division and algorithms in the ideal membership problem [Deleniye i algoritmy v zadache o prinadlezhnosti k idealu]," *Izvestija Saratovskogo universiteta*, vol. 1, no. 2, pp. 156–167, 2001, in Russian.
- [12] V. P. Gerdt. "Compact involutive monomial bases." (2020), [Online]. Available: <https://events.rudn.ru/event/102>.

- [13] Y. A. Blinkov, “Involutive methods applied to models described by systems of algebraic and differential equations [Involyutivnyye metody issledovaniya modeley, opisyyvayemykh sistemami algebraicheskikh i differentsial’nykh uravneniy],” in Russian, Ph.D. dissertation, Saratov State University, Saratov, 2009.
- [14] J. Apel, “A Gröbner approach to involutive bases,” *Journal of Symbolic Computation*, vol. 19, no. 5, pp. 441–458, 1995. DOI: 10.1006/jSCO.1995.1026.
- [15] A. Y. Zharkov and Y. A. Blinkov, “Involution approach to solving systems of algebraic equations,” in *Proceedings of the 1993 International IMACS Symposium on Symbolic Computation*. Laboratoire d’Informatique Fondamentale de Lille, France, 1993, pp. 11–16.

For citation:

O. K. Kroytor, M. D. Malykh, On involutive division on monoids, *Discrete and Continuous Models and Applied Computational Science* 29 (4) (2021) 387–398. DOI: 10.22363/2658-4670-2021-29-4-387-398.

Information about the authors:

Kroytor, Oleg K. — PhD student of Department of Applied Probability and Informatics of Peoples’ Friendship University of Russia (RUDN University) (e-mail: kroytor_ok@pfur.ru, phone: +7(495)9550927, ORCID: <https://orcid.org/0000-0002-5691-7331>)

Malykh, Mikhail D. — Doctor of Physical and Mathematical Sciences, Assistant professor of Department of Applied Probability and Informatics of Peoples’ Friendship University of Russia (RUDN University); Researcher in Meshcheryakov Laboratory of Information Technologies, Joint Institute for Nuclear Research (e-mail: malykh_md@pfur.ru, phone: +7(495)9550927, ORCID: <https://orcid.org/0000-0001-6541-6603>, ResearcherID: P-8123-2016, Scopus Author ID: 6602318510)

УДК 519.872:519.217

PACS 07.05.Tr, 02.60.Pn, 02.70.Bf

DOI: 10.22363/2658-4670-2021-29-4-387-398

Об инволютивном делении на моноидах

О. К. Кройтор¹, М. Д. Малых^{1,2}

¹ *Российский университет дружбы народов
ул. Миклухо-Маклая, д. 6, Москва, 117198, Россия*

² *Лаборатория информационных технологий им. М. Г. Мещерякова
Объединённый институт ядерных исследований
ул. Жолио-Кюри, д. 6, Дубна, Московская область, 141980, Россия*

Рассматривается произвольный моноид M , на котором введено инволютивное деление, и множество всех его конечных подмножеств $\text{Set } M$. Деление рассматривается как отображение $d : \text{Set } M \times M$, образ которого $d(U, m)$ — множество делителей m в U . Свойства деления и инволютивного деления задаются аксиоматически. Понятия инволютивного деления введено в соответствии с определением инволютивного мономиального деления, введённым В. П. Гердтом и Ю. А. Блинковым. Предложен ряд новых обозначений, позволяющих кратко, но явно учитывать зависимость деления от элемента $\text{Set } M$. Теория инволютивного пополнения (замыкания) множеств изложена для произвольных моноидов, необходимые и достаточные условия полноты (замкнутости) — для моноидов, порождённых конечным множеством X . Подчёркнута аналогия между этой теорией и теорией вполне непрерывных операторов. В последнем разделе обсуждена возможность решения задачи о пополнении заданного множества путём последовательного расширения исходной области и её связь с аксиомами, используемыми в определении деления. Все результаты проиллюстрированы примерами о мономиальном делении Томаса.

Ключевые слова: инволютивное мономиальное деление, базис Грёбнера