INNOVATIVE MECHANICAL ENGINEERING
University of Niš, Faculty of Mechanical Engineering
VOL. 3, NO 3, 2024, PP. 47-66

ISSN 2812-9229 (Online)

Extended version of already published conference paper *

CONSTRUCTIVE SEMIGROUPS WITH APARTNESS: A COMPREHENSIBLE SURVEY FOR EXPERTS AND NON-EXPERTS

Melanija Mitrović[1,2] and Mahouton Norbert Hounkonnou[2]

[1]Faculty of Mechanical Engineering, University of Niš, Serbia
[2]International Chair in Mathematical Physics and Applications (ICMPA-UNESCO Chair),
University of Abomey-Calavi, Benin Republic

Abstract

Our main goal is to provide a clear, understandable picture of constructive semigroups with apartness for both (classical) algebraists and those applying algebraic knowledge. This paper will shed light on our results obtained over the last decades.

Keywords: Set with apartness, semigroup with apartness, co-quasiorder, co-equivalence, co-congruence

"In our own time, algebra has become the most rarefied and demanding of all mental disciplines, whose objects are abstractions of abstractions of abstractions, yet whose results have a power and beauty that are all too little known outside the world of professional mathematicians. Most amazing, most mysterious of all, these ethereal mental objects seem to contain, within their nested abstractions, the deepest, most fundamental secrets of the physical world." (J. Derbyshire, [1])

1 INTRODUCTION

An *algebraic structure* is a set (called carrier set or underlying set) with one or more finitary operations defined on it (called basic operation(s)) that satisfies a list of axioms. Centred around an algebraic structure are notions of: substructure, homomorphism, isomorphism, congruence, quotient structure. A mapping between two algebraic structures of the same type, that preserves the operation(s) of the structures is called *homomorphism*. The formulation of homomorphic images (together with substructures and direct products) is one of the principal tools used to manipulate algebraic structures. In the study of homomorphic images of an algebraic structure, a lot of help comes from the notion of a quotient structure, which captures all homomorphic images, at least up to isomorphism. On the other hand, homomorphism is a concept which goes hand in hand with congruences. The relationship between quotients, homomorphisms and congruences is described by the celebrated *isomorphism theorems*, which are a general and important foundational part of abstract and universal algebras.

Algebraic structures have wide ranging applications in many mathematical, computer science and engineering disciplines. This provides sufficient motivation to researchers to review various concepts and results. So, there are algebraic structures in time, computation and control systems. The structural approach to algebra has provided opportunities for:

*Received: March 19, 2024 / Accepted November 26, 2024.
Corresponding author: Melanija Mitrović
Faculty of Mechanical Engineering, University of Niš, Serbia
E-mail: melanija.mitrovic@masfak.ni.ac.rs

- already solved as well as open problems to give solutions in a more efficient and elegant way,
- appearance of new directions in research in the area in particular, and mathematics in general.

It can be read that "algebra can seem abstract and remote, utterly disconnected from daily life". Axioms may model abstract worlds with no immediate connection to the physical world - the fact which may change over time. Boolean algebra, hardly recognized by the mathematical community when it was developed, is nowadays known as the foundation for most of computer science. Linear algebra is useful in all kinds of applications and situations, such as: the feature-based classification techniques in machine learning and the method for face recognition. Quotient structures have many applications within informatics - in particular in modeling and in automated program analysis. More examples of applications of different algebraic contents within informatics can be found in [2]. Even more, as it is also written in [2], algebraic structures (semigroups, groups, semirings, rings, fields, vector spaces, ...) "provide a very mature mathematical framework in which we may formulate and engineer abstractions through concepts such as homomorphism (i.e., the preservation of structure), substructures (e.g., subgroups in a case of groups), and quotient structures (e.g., the natural numbers modulo a prime number). [...] Inductive approaches and algebraic thinking are combined in the in order to illustrate the art of perfect modeling." More about applications of algebraic structures and, in particular, semigroups can be found in [3].

G. Birkhoff, [4] wrote: "I do not wish to exaggerate the importance for computer science of lattices (including Boolean algebras), or of binary groups and fields. All of these have a quite special structure. A much more general class of algebraic systems is provided by semigroups, which are indeed basic for a great part of algebra". Working within the classical theory of semigroups several years ago we decided to change the classical background with the constructive one. Our theory is partly inspired by the classical case, but it is distinguished from it in two significant aspects: we use intuitionistic logic rather than classical throughout; our work is based on the notion of apartness (between elements of the set, and, later, between elements and its subsets).

The theory of constructive semigroups with apartness is a new approach to semigroup theory and not a new class of semigroups. It presents a semigroup facet of some relatively well established direction of constructive mathematics which, to the best of our knowledge, has not yet been considered within the semigroup community. Inspired by results obtained in interactive theorem proving the approach of formal verifications (more in Mitrović, Hounkonnou and Baroni, 2021, [5]), a new constructive algebraic theory known as the **theory of semigroups with apartness** was developed by Mitrović and co-authors: Hounkonnou, Baroni, Crvenković, Romano, Silvestrov - see: [6], [7], [8], [5], [9], [10].

Results which will be presented are based on the ones published in [5], [8]. and shortly, on the work in progress Mitrović and Hounkonnou, [11]. More background on constructive mathematics can be found in [12], [13], [14], [15]. The standard reference for constructive algebra is [16]. Examples of applications of these theoretical concepts can be found in [5], [8].

The present paper is by no means an attempt to give a complete overview of our existing results to date.

2 FUNDAMENTAL CONCEPTS

All material presented in this section is broad rather than deep, and it is not intended to be comprehensive. It is heavily based on the treatments in other standard constructive mathematics books, such as, for example, [12], [13], [14], [15]. The main novelty is in the selection and arrangement of material.

2.1 Constructive mathematics

"Constructive mathematics is based on the belief that mathematics can have real meaning only if its concepts can be constructed by the human mind, an issue that has divided mathematicians for more than a century", [17].

It is surely impossible to arrive at a clear conception of present-day constructive mathematics without knowing something of its origins. Historical development of constructive mathematics is a subject in its own right. For the purpose of this paper, we will go as briefly as possible through it. Since the time of Plato it has been generally believed that mathematics exists independently of man's knowledge and the work of the mathematician is to discover that truth. In the nineteenth century Leopold Kronecker had advocated a constructive approach to mathematics, i.e. a point of view that the work of the mathematician is to invent mathematics.

"The question of whether mathematics is discovered or invented is not an idle one. Depending on their answer to it mathematicians can have radically divergent views on how the work of mathematics should be conducted", [17]. Anyway, the story of modern constructivism really began with the publication of Brouwer's the doctoral thesis "On the Foundations of Mathematics" from 1907. According to Brouwer: mathematical objects are free creations of the human mind, it is independent of both logic and language, and a mathematical object exist when it is constructed. Following H. Wang [18], we may say that constructive mathematics is a "mathematics of doing" while classical mathematics is a "mathematics of being."

In conclusion, classical and constructive mathematics "should not be treated as rival domains among which one has to choose one (for life), but they should rather be treated as useful reports about a same grand structure which can help us to construct a whole picture that would be more adequate than each taken alone", as written by G. Sommaruga, [19]. Or, "they complement each other, and it would be doing oneself violence to renounce one or other", P. Bernays, [20].

2.1.1 *Why constructive mathematics?*

"Why constructive mathematics?", "Why constructivity?", "Why constructivism?" Constructivity and constructivism are generally considered as two altogether different notions. Whereas constructivity refers to a constructive practice of mathematics and logic, constructivism shares with all the other 'isms' a certain ideological connotation, [21].

We, further, agree with A. S. Troelstra, D. van Dalen, [15], in presenting mathematics containing material which is mathematicaly interesting regardless any philosophical bias. So, "Not to put too fine a point on it, let us identify constructive mathematics and constructivity", [21].

Two fundamental conditions for the constructivist trend are:

- The notion of 'truth' is not taken as primitive; rather, a proposition is considered true only when a proof for the proposition is produced.
- The notion of 'existence' is taken to be constructibility: when an object is proved to exist, the proof also exhibits how to find it.

Such a belief naturally leads to a rejection of existence proofs by contradiction, and a consequent scepticism about the meaning of many of the theorems of classical mathematics. If we accept that existence should always be interpreted constructively, then we are forced to dispense with the unrestricted use of the logical law of excluded middle, **LEM**.

Throughout this paper constructive mathematics, **CM**, is viewed as mathematics done using intuitionistic logic.

2.1.2 *(Informal) Intuitionistic logic*

The role of logic in mathematics (and computer science) is two-fold - a tool for applications in both areas, and a technique for laying the foundations.

Constructive mathematics is not based on a prior notion of logic; rather, our interpretations of the logical connectives and quantifiers grow out of our mathematical intuition and experience. The point of departure is that a statement φ is considered to be true (or to hold) if we have a proof for it. By a proof we mean a mathematical construction that establishes φ, not a deduction in some formal system. From the classical mathematics, **CLASS**, point of view, mathematics consists of a preexisting mathematical truth. From a constructive viewpoint, the judgement φ *is true* means that *there is a proof of* φ. In conclusion, "In actual building of constructive mathematics we do not need logic; nevertheless we find it convenient to use logical symbolism", [15].

Constructive reasoning differs from its classical counterpart in that it attaches a stronger meaning to some of the logical operators.

In the history of ideas it often looks as if a certain idea has to be discovered several times, by different people, before it really enters into the 'consciousness' of science. In what follows an idea, connected with the constructivistic trend in the foundations of mathematics, developed within mathematical logic will be given the so-called proof interpretation of intuitionistic logic, also known as the *Brouwer-Heyting-Kolmogorov* (**BHK**-)*interpretation*.

The **BHK**-interpretation gives each of the logical symbols $\wedge$, $\vee$, $\Rightarrow$, $\neg$, $\forall$, $\exists$ a distinct meaning. Classically, the propositional connectivities can be defined from $\wedge$ and $\neg$, while $\exists$ can be defined from $\forall$ and $\neg$, so $\vee$, $\Rightarrow$ and $\exists$ are unnecessary. Intuitionistic logic, in contrast, makes full use of the expressive power of the formal language.

More on intuitionistic logics and **BHK**-interpreation can be found, for example, in [13] or [15].

2.1.3 *Constructivity and too many principles*

In constructive mathematics there are a number of competing notions of constructivity, i.e. there are various incompatible systems of constructive mathematics. The main exponents of constructivity are Brouwer's intuitionistic mathematics, **INT**, the constructive recursive mathematics of the Russian school of Markov, **RUSS**, Bishop's constructive mathematics, **BISH**. In addition there were (and still are) a number of minor ones with a specific constructive program, [21]. Every form has intuitionistic logic at its core. Different schools have different additional principles or axioms given by the particular approach to constructivism. For example, the notion of an *algorithm* or a *finite routine* is taken as primitive in **INT** and **BISH**, while **RUSS** operates with a fixed programming language and an algorithm is a sequence of symbols in that language, [5]. Constructivism in the broad sense is by no means homogeneous. Even the views expressed by different representatives of one "school", or by a single mathematician at different times are not always homogeneous.

Throughout this chapter constructive mathematics is understood as Bishop-style mathematics, **BISH**. The Bishop-style of constructive mathematics enables one to interpret the results both in classical mathematics, **CLASS**, and other varieties of constructivism.

2.2 Constructively valid arguments

Following Bishop, every classical theorem presents the challenge: find a constructive version with a constructive proof. As stated by Bishop, [13]: "The extent to which good constructive substitutes exist for the theorems of classical mathematics can be regarded as a demonstration that classical mathematics has a substantial underpinning of constructive truth". Following the standard literature on constructive mathematics, the term "constructive theorem" refers to a theorem with a constructive proof. A classical theorem that is proven in a constructive manner is a constructive theorem. This

constructive version can be obtained by strengthening the conditions or weakening the conclusion of the theorem. Although constructive theorems might look like the corresponding classical versions, they often have more complicated hypotheses and proofs. There are, often, several constructively different versions of the same classical theorem, see, for example, [5] . Some classical theorems are neither provable nor disprovable, that is, they are independent of **BISH**. For some classical theorems it is shown that they are not provable constructively.

To the end of this section, following [5], we introduce the idea of omniscience principle and of Brouwerian counterexample. The law of excluded middle, **LEM**, can be regarded as the main source of nonconstructivity. It was Brouwer, [22], who first observed that **LEM** was extended without justification to statements about infinite sets. Several consequences of **LEM** are not accepted in Bishop's constructivism. We will mention two such nonconstructive principles - the ones which will be used latter.

- **The limited principle of omniscience**, **LPO**: for each binary sequence $(a_n)_{n\geq 1}$, either $a_n = 0$ for all n, or else there exists n with $a_n = 1$.

- **Markov's principle**, **MP**: For each binary sequence $(a_n)_{n\geq 1}$, if it is impossible that $a_n = 0$ for all n, then there exists n with $a_n = 1$.

Within constructive mathematics, a statement P, as in classical mathematics, can be disproved by giving a counterexample. However, it is also possible to give a *Brouwerian counterexample* to show that the statement is nonconstructive. A Brouwerian counterexample to a statement P is a constructive proof that P implies some nonconstructive principle, such as, for example, **LEM**, and its weaker versions **LPO**, **MP**. It is not a counterexample in the true sense of the word - it is just an indication that P does not admit a constructive proof.

2.3 INFORMAL FOUNDATIONS OF CM

In one sense, the purpose of a foundation of mathematics is to describe, or otherwise provide for, the objects of mathematics, [19]. In what follows within this section the constructive view in the Bishop's style of the fundamental notions will be given.

2.3.1 *Primitive notions*

The set of positive numbers and algorithm (construction) are two primitive notions, and, as such, they cannot be defined. The cornerstones for **BISH** include the notions of sets, functions and relations.

The ***set of positive numbers*** is regarded as a basic set, and it is assumed that the positive numbers have the usual algebraic and order properties, including mathematical induction. Following [23], "The primary concern of mathematics is number, and this means the positive integers. We feel about number the way Kant felt about space. The positive integers and their arithmetic are presupposed by the very nature of our intelligence and, we are tempted to believe, by the very nature of intelligence in general. The development of the positive integers from the primitive concept of the unit, the concept of adjoining a unit, and the process of mathematical induction carries complete conviction".

The notion of ***algorithm*** (algorithmic process, finite routine, rule, mechanical operation) is primitive. The idea that the notion of an algorithm is primitive has also been advanced by the Russian mathematicians V. A. Uspenskii and A. L. Semenov, [24]: "The concept of algorithm like that of set and of natural number is a such a fundamental concept that it cannot be explained through other concepts and should be regarded as [an]undefinable one", (source [16]).

2.3.2 *Informal constructive set theory*

Constructive set theory is a variant of classical set theory which uses intuitionistic logic.

Constructive set theory provides a standard set theoretical framework for development of constructive mathematics in the style of Errett Bishop and one of several such frameworks for constructive mathematics that have been considered. In the words of P. Aczel, M. Rathjen, [25]: "There are just sets as in classical set theory. This means that mathematics in constructive set theory can look very much like ordinary ordinary classical mathematics. The advantage of this is that the ideas, conventions and practice of the set theoretical presentation of ordinary mathematics can be used also in set theoretical development of constructive mathematics, provided that a suitable discipline is adhered to. In the first place only the methods of logical reasoning available in intuitionistic logic should be used".

Contrary to the classical case, a set exists only when it is defined. A *set* $(S, =)$ is considered defined when we have

(a) said what must be done to construct a member of S;

(b) said what must be done to prove members of S equal;

(c) proved that equality = on S as defined in (b) is an equivalence relation.

The issue of equality seems to get more attention in constructive mathematics than it does in classical mathematics. In the customary approach to set theory, one does not regard a set as "coming equppied" with a special equality relation of its own. There is the "universal" or "absolute" equality relation on the entire universe. In constructive mathematics, no such thing is assumed: we have only those equality relations which we can construct.

In some (constructive) mathematics' books one can find that the use of equivalence relations rather than intensional equality (that is, identity of description) in classical mathematics often goes unnoticed. For example, we call the rational numbers $\frac{1}{2}$ and $\frac{3}{6}$ equal, even though, strictly speaking, they are equivalent and not intensionally identical.

As usual, we write $x \in S$ to signify that x is an element of the set S, and $x \notin S$ instead of $\neg(x \in S)$.

A property P, which is applicable to the elements of a set S, determines a subset X of S denoted by $X = \{x \in S : P(x)\}$. Clearly, two elements of a subset of S are equal if and only if they are equal as elements of S. If X is a subset of S, then we write $X \subseteq S$. Furthermore, we will be interested only in properties $P(x)$ which are *extensional* in the sense that for all $x_1, x_2 \in S$ with $x_1 = x_2$, $P(x_1)$ and $P(x_2)$ are equivalent. Informally, it means that "it does not depend on the particular description by which x is given to us".

A set $(S, =)$ is an *inhabited* set if we can construct an element of S. The distinction between the notions of a nonempty set and an inhabited set is a key in constructive set theories. While an inhabited set is nonempty, the converse does not hold in general.

The notion of equality of different sets is not defined. The only way in which elements of two different sets can be regarded as equal is by requiring them to be subsets of a third set.

Given two sets $(S, =_S)$ and $(T, =_T)$, it is permissible to construct the set $(T^S, =)$ of mappings between them. A *mapping* $f : S \to T$ is an algorithm which produces an element $f(x)$ of T when applied to an element x of S, which is extensional, that is

$$\forall_{x,y \in S} \, (x =_S y \;\Rightarrow\; f(x) =_T f(y)).$$

As usual, equality between two elements f and g from T^S is defined by

$$f = g \overset{\text{def}}{\Leftrightarrow} \forall_{x \in X} \, (f(x) = g(x)).$$

Mappings $f : S \to T$ and $g : T \to U$ can be composed, giving a mapping $f \circ g : S \to U$ defined by $(f \circ g)(x) = f(g(x)), x \in S$.

Lemma 1 *Composition of mappings is associative, i.e.*

$$f \circ (g \circ h) = (f \circ g) \circ h$$

whenever the compositions are well defined.

Corollary 1 $(S^S, =; \circ)$ *is a semigroup.*

A mapping $f : S \to T$ is:

- *onto S* or *surjection*: $\forall_{y \in T}\ \exists_{x \in S}\ (y =_T f(x))$;
- *one-one* or *injection*: $\forall_{x,y \in S}\ (f(x) =_T f(y)\ \Rightarrow\ x =_S y)$;
- *bijection* between S and T: it is a one-one and onto.

The *cartesian product* of two sets $(S, =_S)$ and $(T, =_T)$ is the set $(S \times T, =_{S \times T})$ defined by

$$S \times T \stackrel{\text{def}}{=} \{(x, y) : x \in S \wedge y \in T\}$$

$$(x, y) =_{S \times T} (u, v) \stackrel{\text{def}}{\Leftrightarrow} x =_S u \wedge y =_T v.$$

In what follows of particular interest will be the cartesian product of a set S by itself, $S \times S$.

An inhabited subset ρ of $S \times S$, or, equivalently, a property applicable to elements of $S \times S$, is called a *binary relation* on S. In general, there are many properties that binary relations may satisfy on a given set:

(R) reflexive: $(x, x) \in \rho$

(IR) irreflexive: $\neg((x, x) \in \rho)$

(S) symmetric : $(x, y) \in \rho\ \Rightarrow\ (y, x) \in \rho$

(T) transitive: $(x, y) \in \rho \wedge (y, z) \in \rho\ \Rightarrow\ (x, z) \in \rho$

(coT) co-transitive: $(x, y) \in \rho\ \Rightarrow\ (x, z) \in \rho \vee (z, y) \in \rho$

Inherited from classical mathematics, **CLASS**, they "play game" under constructive rules.

Compared with **CLASS**, the situation for inequality is more complicated. There are different types of inequalities (denial inequality, diversity, apartness, tight apartness - to mentione few), some of them completely independent, which only in **CLASS** are equal to one standard inequality. So, in constructive mathematics inequality becomes a "basic notion in intuitionistic axiomatics".

An inequality relation is often denoted by $\neq$. A tuple $(S, =_S, \neq_S)$ is called a *set with inequality*. It has to be emphasized that $\neq$ is not, in general, the negation of $=$. The interpretation of the symbol $x \neq y$ depends on the context. Going through the literature on constructive mathematics, an *inequality relation* is often considered to be a binary relation that is irreflexive and symmetric.

Specific types of inequality relations include:

- the *denial inequality*: $x \neq y \stackrel{\text{def}}{\Leftrightarrow} \neg(x = y)$;
- a *tight inequality*: an inequality with $x = y \Rightarrow x = y$;
- an *apartness* relation: co-transitive inequality ((IR), (S), (coT));
- a *tight apartness*: an apartness with $\neg\,(x \# y) \Rightarrow \neg(x \neq y)$.

One of the main features of constructive mathematics is that the concepts that are equivalent in the presence of **LEM**, need not be equivalent any more. For example, we distinguish nonempty and inhabited sets, several types of inequalities, etc. We have to be careful which of several classically equivalent definitions we use.

3 Set with apartness

There are many decisions a mathematician must make when deciding to replace classical logic with intuitionisitic logic. Let us mention some of them. First of all - choice of variant of constructive mathematics. Our choice was the Errett Bishop - style constructive mathematics, **BISH**.

Going through the literature there are several variants of what is considered to be a set with apartness - depending on the relations between equality and apartness defined on a set. Our choice - our starting structure - is a **set with apartness** $(S, =, \#)$ where

- equality and apartness are basic notions,
- equality and apartness are independent of each other,
- apartness is not, in general, tight.

Such a choice was and is a novelty within constructive circles.

3.1 Basic concepts

Let $(S, =)$ be an *inhabited* set. By an ***apartness*** on S we mean a binary relation $\#$ on S which satisfies the axioms of irreflexivity, symmetry and cotransitivity:

(Ap1) $\neg(x\#x)$

(Ap2) $x\#y \Rightarrow y\#x$,

(Ap3) $x\#z \Rightarrow \forall_y (x\#y \vee y\#z)$.

If $x\#y$, then x and y are different, or distinct. Roughly speaking, $x = y$ means that we have a proof that x equals y while $x\#y$ means that we have a proof that x and y are different. Therefore, the negation of $x = y$ does not necessarily imply that $x\#y$ and vice versa: given x and y, we may have neither a proof that $x = y$ nor a proof that $x\#y$.

The apartness on a set S is *tight* if

(Ap4) $\neg(x\#y) \Rightarrow x = y$.

Apartness is tight just when $\neg(x\#y) \Leftrightarrow x = y$.

By extensionality, we have

(Ap5) $x\#y \wedge y = z \Rightarrow x\#z$,

the equivalent form of which is

(Ap5') $x\#y \wedge x = x' \wedge y = y' \Rightarrow x'\#y'$.

A *set with apartness* $(S, =, \#)$ is the starting point for our considerations, and will be simply denoted by S.

The existence of an apartness relation on a structure often gives rise to an apartness relation on another structure. For example, given two sets with apartness $(S, =_S, \#_S)$ and $(T, =_T, \#_T)$, it is permissible to construct the set of mappings between them. Let $f : S \to T$ be a mapping between sets with apartness S and T. An important property applicable to mapping f is that of strong extensionality. Namely, a mapping $f : S \to T$ is a *strongly extensional* mapping, or, for short, an *se-mapping*, if

$$\forall_{x,y \in S} (f(x)\#_T f(y) \Rightarrow x\#_S y).$$

An se-mapping f is:

- an *se-surjection* if it is surjective;
- an *se-injection* if it is injective;
- an *se-bijection* if it is bijective;

- *apartness injective*, shortly *a-injective*: $\forall_{x,y\in S}\,(x\#_S y \;\Rightarrow\; f(x)\#_T f(y))$;
- *apartness bijective*: a-injective, se-bijective.

Given the two sets with apartness S and T it is permissible to construct the set of ordered pairs $(S\times T, =, \#)$ of these sets defining apartness by

$$(s,t)\,\#\,(u,v) \;\overset{\text{def}}{\Leftrightarrow}\; s\,\#_S\,u \;\vee\; t\,\#_T\,v.$$

3.2 Distinguishing subsets

The presence of apartness implies the appearance of different types of substructures connected to it. Following [14], we define the relation $\bowtie$ between an element $x\in S$ and a subset Y of S by

$$x\bowtie Y \;\overset{\text{def}}{\Leftrightarrow}\; \forall_{y\in Y}(x\#y).$$

A subset Y of S has two natural complementary subsets: *the logical complement* of Y

$$\neg Y \overset{\text{def}}{=} \{x\in S : x\notin Y\},$$

and *the apartness complement* or, shortly, the *a-complement* of Y

$$\sim Y \overset{\text{def}}{=} \{x\in S \,:\, x\bowtie Y\}.$$

Denote by $\widetilde{x}$ the a-complement of the singleton $\{x\}$. Then it can be easily shown that $x\in\sim Y$ if and only if $Y\subseteq\widetilde{x}$. If the apartness is not tight we can find subsets Y with $\sim Y\subset\neg Y$. (More in [5])

The complements are used for the classification of subsets of a given set. A subset Y of S is

- *a detachable* subset in S or, in short, a *d-subset* in S if

$$\forall_{x\in S}\,(x\in Y\vee x\in\neg Y);$$

- *a strongly detachable* subset of S, shortly *an sd-subset of* S, if

$$\forall_{x\in S}\,(x\in Y\vee x\in\sim Y),$$

- *a quasi-detachable* subset of S, shortly *a qd-subset of* S, if

$$\forall_{x\in S}\,\forall_{y\in Y}\,(x\in Y\vee x\#y).$$

Questions which naturally arise here are: For which type of subset of a set with apartness do we have equality between its two complements? What kind of relationships exist between distinguished subsets? It turns out that the answers initiated a development of order theory for sets and semigroups with apartness.

Theorem 1 *Let Y be a subset of S. Then:*

(i) *Any sd-subset is a qd-subset of S. The converse implication entails* **LPO**.

(ii) *Any qd-subset Y of S satisfies $\sim Y=\neg Y$.*

(iii) *If any qd-subset is a d-subset, then* **LPO** *holds.*

(iv) *If any d-subset is a qd-subset, then* **MP** *holds.*

(v) *Any sd-subset is a d-subset of S. The converse implication entails* **MP**.

(vi) *If any subset of a set with apartness S is a qd-subset, then* **LPO** *holds.*

Proof. (i). Let Y be an sd-subset of S. Then, applying the definition and logical axiom we have

$$\begin{aligned} \forall_{x\in S}\,(x \in Y \vee x \in {\sim}Y) \quad &\Leftrightarrow \quad \forall_{x\in S}\,(x \in Y \ \vee\ \forall_{y\in Y}(x\#y)) \\ &\Rightarrow \quad \forall_{x\in S}\,\forall_{y\in Y}\,(x \in Y \vee x\#y). \end{aligned}$$

In order to prove the second part of this statement, we consider the real number set $\mathbb{R}$ with the usual (tight) apartness and the subset $Y = \widetilde{0}$. Then, for each real number x and for each $y \in Y$ it follows, from the co-transitivity of #, either $y\#x$ or $x\#0$, that is, either $x \in Y$ or $x\#y$. Consequently, Y is a qd-subset of $\mathbb{R}$. On the other hand, if Y is an sd-subset of $\mathbb{R}$, then for each $x \in \mathbb{R}$, either $x \in Y$ or $x \in {\sim} Y$. In the former case, $x\#0$ and in the latter $x = 0$, hence **LPO** holds.

(ii). Let Y be a qd-subset, and let $a \in \neg Y$. By assumption we have

$$\forall_{x\in S}\,\forall_{y\in Y}\,(x \in Y \vee x\#y),$$

so substituting a for x, we get $\forall_{y\in Y}\,(a \in Y \vee a\#y)$, and since, by assumption, $\neg(a \in Y)$, it follows that $a\#y$ for all $y \in Y$. Hence $a \in {\sim} Y$. See also [10].

(iii). Let S be the real number set $\mathbb{R}$ with the usual apartness #. As in the proof of (i), consider the qd-subset $\widetilde{0}$ of $\mathbb{R}$. If $\widetilde{0}$ is a d-subset of $\mathbb{R}$, then $x \in \widetilde{0}$ or $\neg(x \in \widetilde{0})$, for all real numbers x. In the latter case $\neg(x\#0)$, which is equivalent to $x = 0$. Thus we obtain the property $\forall_{x\in\mathbb{R}}\ (x\#0 \vee x = 0)$ which, in turn, is equivalent to **LPO**.

(iv). Consider a real number a with $\neg(a = 0)$ and let S be the set $\{0, a\}$ endowed with the usual apartness of $\mathbb{R}$. For $Y = \{0\}$, since $0 \in Y$ and $a \in \neg Y$, it follows that Y is a d-subset of S. On the other hand, if Y is a qd-subset of S, then $a\#0$. It follows that for any real number with $\neg(a = 0)$, $a\#0$ which entails the Markov Principle, **MP**.

(v). The first part follows immediately from (i), (ii) and the definition of d-subsets. The converse follows from (i) and (iv).

(vi). Consider again $\mathbb{R}$ with the usual apartness and define $Y = \{0\}$. If Y is a qd-subset of $\mathbb{R}$, then for all $x \in \mathbb{R}$, we have $x = 0$ or $x\#0$, hence **LPO** holds. □

For all subsets Y of the set with apartness S for which two distinguished complements coincide, we will adopt the following notation:

$$\boldsymbol{Y^c} = {\sim} Y = \neg Y.$$

3.3 Co-quasiorders

Let $(S \times S, =, \#)$ be a set with apartness. An inhabited subset of $S \times S$, or, equivalently, a property applicable to the elements of $S \times S$, is called a *binary relation* on S. Let α be a relation on S. Then

$$(a, b) \ \bowtie\ \alpha \ \Leftrightarrow\ \forall_{(x,y)\in\alpha}\,((a, b)\,\#\,(x, y)),$$

for any $(a, b) \in S \times S$. The apartness complement of α is the relation

$${\sim}\,\alpha \ = \ \{(x, y) \in S \times S : (x, y) \bowtie \alpha\}.$$

In general, we have ${\sim}\,\alpha \subseteq \neg\alpha$.

The relation α defined on a set with apartness S is

- irreflexive if $\forall_{x\in S}\,\neg((x, x) \in \alpha)$;
- strongly irreflexive if $(x, y) \in \alpha \ \Rightarrow\ x\#y$;
- co-transitive if $(x, y) \in \alpha \ \Rightarrow\ \forall_{z\in S}\,((x, z) \in \alpha \ \vee\ (z, y) \in \alpha)$.

It is easy to check that a strongly irreflexive relation is also irreflexive. For a tight apartness, the two notions of irreflexivity are classically equivalent but not so constructively. More precisely, if each irreflexive relation were strongly irreflexive then **MP** would hold. In the constructive order theory, the notion of co-transitivity, that is the property that for every pair of related elements, any other element is related to one of the original elements in the same order as the original pair is a constructive counterpart to classical transitivity

A relation τ defined on a set with apartness S is a

- *weak co-quasiorder* if it is irreflexive and co-transitive,
- *co-quasiorder* if it is strongly irreflexive and co-transitive.

Even if the two classically (but not constructively) equivalent variants of a co-quasiorder are constructive counterparts of a quasiorder in the case of (a tight) apartness, the stronger variant, co-quasiorder, is, of course, the most appropriate for a constructive development of the theory of semigroups with apartness we develop, which will be evident in the continuation of this paper. The weaker variant, that is, weak co-quasiorder, could be relevant in analysis. (More in [5])

A co-quasiorder has the following important properties:

Proposition 1 *Let τ be a co-quasiorder on S. Then:*

(i) *τ is a qd-subset of $S \times S$;*

(ii) *$\sim \tau = \neg \tau = \tau^c$;*

(iii) *τ^c is a quasiorder on S.*

Proof.

(i). Let $(x, y) \in S \times S$. Then, for all $(a, b) \in \tau$,

$$\begin{aligned} (a,x) \in \tau \vee (x,b) \in \tau \quad &\Rightarrow \quad (a,x) \in \tau \vee (x,y) \in \tau \vee (y,b) \in \tau \\ &\Rightarrow \quad a\#x \vee (x,y) \in \tau \vee y\#b \\ &\Rightarrow \quad (a,b)\#(x,y) \vee (x,y)\tau, \end{aligned}$$

that is, τ is a qd-subset.

(ii). It follows from (i) and Theorem 1(ii).

(iii). Let τ be a strongly irreflexive relation on S. For each $a \in S$, it can be easily proved that $(a, a)\#(x, y)$ for all $(x, y) \in \tau$. Thus, τ^c is strongly irreflexive.

If $(x, y), (y, z) \in \tau^c$, then, by the definition of $\tau^c = \sim \tau$, we have that $(x, y) \bowtie \tau$ and $(y, z) \bowtie \tau$. For an element $(a, b) \in \tau$, by co-transitivity of τ, we have $(a, x) \in \tau$ or $(x, y) \in \tau$ or $(y, z) \in \tau$ or $(z, b) \in \tau$. Thus $(a, x) \in \tau$ or $(z, b) \in \tau$, which implies that $a\#x$ or $b\#z$, that is $(x, z)\#(a, b)$. So, $(x, z) \bowtie \tau$ and $(x, z) \in \sim \tau = \tau^c$. Therefore, τ^c is transitive. □

3.4 Apartness isomorphism theorems

A quotient structure does not have, in general, a natural apartness relation. For most purposes, we overcome this problem using a *co-equivalence*, that is symmetric co-quasiorder, instead of an equivalence. Existing properties of a co-equivalence guarantee that its a-complement is an equivalence and that the quotient set of that equivalence will inherit an apartness. The following notion will be necessary. For any two relations α and β on S we can say that *α defines an apartness on* $\mathbf{S}/\beta$ if we have

$$\text{(Ap 6)} \qquad x\beta \,\#\, y\beta \overset{\text{def}}{\Leftrightarrow} (x, y) \in \alpha.$$

Lemma 2 *If α is a co-quasiorder and β an equivalence on a set S, then* (Ap 6) implies

$$(\text{Ap } 6') \qquad ((\mathrm{x},\mathrm{a}) \in \beta \ \wedge \ (\mathrm{y},\mathrm{b}) \in \beta) \ \Rightarrow \ ((\mathrm{x},\mathrm{y}) \in \alpha \ \Leftrightarrow \ (\mathrm{a},\mathrm{b}) \in \alpha).$$

Proof. Indeed, let α be a co-quasiorder and β an equivalence on S such that α defines an apartness on $\mathbf{S}/\beta$. Let $(x,a),(y,b) \in \beta$, i.e. $a \in x\beta$ and $b \in y\beta$, which, by the assumption, gives $a\beta = x\beta$ and $b\beta = y\beta$. If $(x,y) \in \alpha$, then, by (Ap6), $x\beta \# y\beta$, which, by (Ap5'), gives $a\beta \# b\beta$. By (Ap6) we have $(a,b) \in \alpha$. In a similar manner, starting from $(a,b) \in \alpha$ we can conclude $(x,y) \in \alpha$. □

Let α and β be relations on S. Then α is *associated* with β, $\alpha \leftrightarrows \beta$, if

$$\alpha \leftrightarrows \beta \overset{\text{def}}{\Leftrightarrow} \forall_{x,y,z \in S} \ ((x,y) \in \alpha \wedge (y,z) \in \beta \ \Rightarrow \ (x,z) \in \alpha).$$

Theorem 2 *Let κ be a co-equivalence on S. Then*

(i) *the relation κ^c is an equivalence on S such that $\kappa \leftrightarrows \kappa^c$;*

(ii) *$(S/\kappa^c, =, \#)$ is a set with apartness where*

$$\begin{aligned} a\kappa^c = b\kappa^c \quad &\Leftrightarrow \ (a,b) \bowtie \kappa \\ a\kappa^c \# b\kappa^c \quad &\Leftrightarrow \ (a,b) \in \kappa; \end{aligned}$$

(iii) *The quotient mapping $\pi : S \to S/\kappa^c$, defined by $\pi(x) = x\kappa^c$, is an se-surjection.*

Proof. (i). By the Proposition 1(iii), κ^c is a quasiorder on S. If κ is symmetric, then

$$\begin{aligned} (x,y) \in\sim \kappa \quad &\Leftrightarrow \quad \forall_{(a,b)\in\kappa} \ ((x,y)\#(a,b)) \\ &\Rightarrow \quad \forall_{(b,a)\in\kappa} \ ((x,y)\#(b,a)) \\ &\Rightarrow \quad \forall_{(b,a)\in\kappa} \ (x\#b \ \vee \ y\#a) \\ &\Rightarrow \quad \forall_{(a,b)\in\kappa} \ ((y,x)\#(a,b)) \\ &\Leftrightarrow \quad (y,x) \in\sim \kappa = \kappa^c. \end{aligned}$$

Thus, κ^c is an equivalence.

Let $(x,y) \in \kappa$ and $(y,z) \in \kappa^c$. Thus $(x,y) \in \kappa$ and $(y,z) \bowtie \kappa$. By the co-transitivity of κ we have $(x,z) \in \kappa$ or $(y,z) \in \kappa$. Thus $(x,z) \in \kappa$, and $\kappa \leftrightarrows \kappa^c$.

(ii). The strong irreflexivity of # is implied by its definition and by the strong irreflexivity of κ.

Let $a\kappa^c \# b\kappa^c$. Then $(a,b) \in \kappa$ implies that $(b,a) \in \kappa$, that is $b\kappa^c \# a\kappa^c$.

Let $a\kappa^c \# b\kappa^c$ and $u\kappa^c \in S/\kappa^c$. Then $(a,b) \in \kappa$, and, by the co-transitivity of κ, we have $(a,u) \in \kappa$ or $(u,b) \in \kappa$. Finally we have that $a\kappa^c \# u\kappa^c$ or $u\kappa^c \# b\kappa^c$, so the relation # is co-transitive.

(iii). Let $\pi(x)\#\pi(y)$, i.e. $x\kappa^c \# y\kappa^c$, which, by what we have just proved, means that $(x,y) \in \kappa$. Then, by the strong irreflexivity of κ, we have $x\#y$. So π is an se-mapping.

Let $a\kappa^c \in S/\kappa^c$ and $x \in a\kappa^c$. Then $(a,x) \in \kappa^c$, i.e. $a\kappa^c = x\kappa^c$, which implies that $a\kappa^c = x\kappa^c = \pi(x)$. Thus π is an se-surjection. □

Let $f : S \to T$ be an se-mapping between sets with apartness. Then the relation

$$\operatorname{coker} f \overset{\text{def}}{=} \{(x,y) \in S \times S : f(x) \# f(y)\}$$

defined on S is called the *co-kernel* of f.

Now, *the First apartness isomorphism theorem* for sets with apartness follows.

Theorem 3 *Let $f : S \to T$ be an se-mapping between sets with apartness. Then*

(i) $\operatorname{coker} f$ *is a co-equivalence on S;*

(ii) $\operatorname{coker} f \leftarrow\!\!\!\!\circ \ker f$ *and* $\ker f \subseteq (\operatorname{coker} f)^c$*;*

(iii) $(S/\ker f, =, \#)$ *is a set with apartness, where*

$$a(\ker f) = b(\ker f) \Leftrightarrow (a, b) \in \ker f$$
$$a(\ker f) \# b(\ker f) \Leftrightarrow (a, b) \in \operatorname{coker} f;$$

(iv) *the mapping* $\varphi : S/\ker f \to T$*, defined by* $\varphi(x(\ker f)) = f(x)$*, is an a-injective se-injection such that* $f = \varphi\pi$*;*

(v) *if* f *maps* S *onto* T*, then* φ *is an apartness bijection.*

Proof. (i). The strong irreflexivity of $\operatorname{coker} f$ is easy to prove: if $(x, y) \in \operatorname{coker} f$, then $f(x)\#f(y)$ and therefore $x\#y$.

If $(x, y) \in \operatorname{coker} f$, then, by the symmetry of apartness in T, $f(y)\#f(x)$; so $(y, x) \in \operatorname{coker} f$.

If $(x, y) \in \operatorname{coker} f$ and $z \in S$, i.e. $f(x)\#f(y)$ and $f(z) \in T$, then either $f(x)\#f(z)$ or $f(z)\#f(y)$; that is, either $(x, z) \in \operatorname{coker} f$ or $(z, y) \in \operatorname{coker} f$. Hence $\operatorname{coker} f$ is a co-equivalence on S.

(ii). Let $(x, y) \in \operatorname{coker} f$ and $(y, z) \in \ker$ f. Then $f(x)\#f(y)$ and $f(y) = f(z)$. Hence $f(x)\#f(z)$, that is, $(x, z) \in \operatorname{coker} f$, and $\operatorname{coker} f \leftarrow\!\!\!\!\circ \ker f$.

Now let $(x, y) \in \ker f$, so $f(x) = f(y)$. If $(u, v) \in \operatorname{coker} f$, then, by the co-transitivity of $\operatorname{coker} f$, it follows that $(u, x) \in \operatorname{coker} f$ or $(x, y) \in \operatorname{coker} f$ or $(y, v) \in \operatorname{coker} f$. Thus either $(u, x) \in \operatorname{coker} f$ or $(y, v) \in \operatorname{coker} f$, and, by the strong irreflexivity of $\operatorname{coker} f$, either $u\#x$ or $y\#v$; whence we have $(x, y)\#(u, v)$. Thus $(x, y) \bowtie \operatorname{coker} f$, or, equivalently $(x, y) \in (\operatorname{coker} f)^c$.

(iii). This follows from the definition of # in $S/\ker f$ and (i).

(iv). Let us first prove that φ is well defined. Let $x(\ker f), y(\ker f) \in S/\ker f$ be such that $x(\ker f) = y(\ker f)$, that is, $(x, y) \in \ker f$. Then we have $f(x) = f(y)$, which, by the definition of φ, means that $\varphi(x(\ker f)) = \varphi(y(\ker f))$.

Now let $\varphi(x(\ker f)) = \varphi(y(\ker f))$; then $f(x) = f(y)$. Hence $(x, y) \in \ker f$, which implies that $x(\ker f) = y(\ker f)$. Thus φ is an injection.

Next let $\varphi(x(\ker f))\#\varphi(y(\ker f))$; then $f(x)\#f(y)$. Hence $(x, y) \in \operatorname{coker} f$, which, by (iii), implies that $x(\ker f)\#y(\ker f)$. Thus φ is an se-mapping.

Let $x(\ker f)\#y(\ker f)$; that is, by (iii), $(x, y) \in \operatorname{coker} f$. So we have $f(x)\#f(y)$, which, by the definition of φ means $\varphi(x(\ker f))\#\varphi(y(\ker f))$. Thus φ is a-injective.

By the definition of composition of functions, Theorem 2, and the definition of φ, for each $x \in S$ we have

$$(\varphi\pi)(x) = \varphi(\pi(x)) = \varphi(x(\ker f)) = f(x).$$

(v). Taking into account (iv), we have to prove only that φ is a surjection. Let $y \in T$. Then, as f is onto, there exists $x \in S$, such that $y = f(x)$. On the other hand $\pi(x) = x(\ker f)$. By (iv), we now have

$$y = f(x) = (\varphi\,\pi)(x) = \varphi(\pi(x)) = \varphi(x(\ker f)).$$

Thus φ is a surjection. □

4 SEMIGROUPS WITH APARTNESS

The theory of semigroups with apartness is a new approach to semigroup theory and not a new class of semigroups. It presents a semigroup facet of some relatively well established direction of constructive mathematics which, to the best of our knowledge, has not yet been considered within the semigroup community. Starting our work on constructive semigroups with apartness, as pointed out above, we faced an algebraically completely new area. What we had in "hand" at that moment were the experience and knowledge coming from the classical semigroup theory, other constructive mathematics disciplines, and computer science.

4.1 Background and motivation

Constructive algebra is a relatively old discipline developed among others by L. Kronecker, van der Waerden, A. Heyting. One of the main topics in constructive algebra is constructive algebraic structures with the relation of (tight) apartness #, the second most important relation in constructive mathematics. The principal novelty in treating basic algebraic structures constructively is that (tight) apartness becomes a fundamental notion. (Consider the reals: we cannot assert that x^{-1} exists unless we know that x is apart from zero, i.e. $|x| > 0$ - constructively that is not the same thing as $x \neq 0$. Furthermore, in fields x^{-1} exists only if x is apart from 0, [12]). For more information on the history of the topics see [15], [16].

Roughly, the descriptive definition of a structure with apartness includes two main parts:

- the notion of a certain classical algebraic structure is straightforwardly adopted;
- a structure is equipped with an apartness with standard operations respecting that apartness.

Proof assistants are computer systems which give a user the possibility to do mathematics on a computer: from (numerical and symbolical) computing aspects to the aspects of defining and proving. The latter ones, doing proofs, are the main focus. It is believed that, besides their great future within the area of mathematics formalization, their applications within computer-aided modelling and verification of the systems are and will be more important. One of the most popular, with the intuitionistic background, is the proof assistant computer system Coq.

Coq is used for formal proofs of well known mathematical theorems, such as, for example, the Fundamental Theorem of Algebra, FTA, [26]. For that purpose, the *constructive algebraic hierarchy* for Coq was developed, [27], consisting of constructive basic algebraic structures (semigroups, monoids, groups, rings, fields) with *tight* apartness. In addition, all these structures are limited to the commutative case. As it is noticed in [27] "that algebraic hierarchy has been designed to prove FTA. This means that it is not rich as one would like. For instance, we do not have noncommutative structure because they did not occur in our work". We put noncommutative constructive semigroups with non-tight apartness in the core of our study, proving first, of course, that such semigroups do exist, [6].

A lot of ideas, notions and notations come from, for example, the constructive analysis, and, especially, from the constructive topology, as well as from constructive theories of groups and rings with *tight* apartness. Although the area of constuctive semigroups with apartness is still in its infancy, we can already conclude that, similarly to the clasical case, the semigroups with apartness do not much resemble groups and rings. In fact, they do not much resemble any other constructive algebraic structures with apartness.

Following Bishop, we made "every effort to follow classical development along the lines suggested by familiar classical theories or in all together new directions." Although it is a pretty common point of view that classical theorem becomes more enlightening when it is seen from the constructive viewpoint, it can not be said that the theory of constructive semigroups with apartness aims at revising the whole classical framework in nature. More on background and motivation can be found at [5].

4.2 Basic concepts

Given a set with apartness $(S, =, \#)$, the tuple $(S, =, \#, \cdot)$ is a *semigroup with apartness* if the binary operation $\cdot$ is associative

(A) $\quad \forall_{a,b,c \in S}\ [(a \cdot b) \cdot c = a \cdot (b \cdot c)]$,

and strongly extensional

(S) $\quad \forall_{a,b,x,y \in S}\ (a \cdot x \# b \cdot y \Rightarrow (a \# b \vee x \# y))$.

As usual, we are going to write ab instead of $a \cdot b$. Example 1 provides a concrete instance of a semigroup with apartness.

Example 1 Let $S = \{a, b, c, d, e\}$ be a set with diagonal $\triangle_S$ as the equality relation. If we denote by $K = \triangle_S \cup \{(a, b), (b, a)\}$, then we can define an apartness # on S to be $(S \times S) \setminus K$. Thus, $(S, =, \#)$ is a set with apartness. If we define multiplication on the set S as

·	a	b	c	d	e
g	a	b	c	d	e
a	b	b	d	d	d
b	b	b	d	d	d
c	d	d	c	d	c
d	d	d	d	d	d
e	d	d	c	d	c

then $(S, =, \#; \cdot)$ is a semigroup with apartness. $\diamond$

For a given set with apartness A we can construct a semigroup with apartness $S = A^A$ in the following way.

Theorem 4 *Let S be the set of all se-functions from A to A with the standard equality $=$*

$$f = g \Leftrightarrow \forall_{x \in A} (f(x) = g(x))$$

and apartness

$$f \# g \Leftrightarrow \exists_{x \in A} (f(x) \# g(x)).$$

Then $(S, =, \#, \circ)$ is a semigroup with respect to the binary operation $\circ$ of composition of functions.

Until the end of this paper, we adopt the convention that *semigroup* means *semigroup with apartness*. Apartness from Theorem 4 does not have to be tight, [6].

Let S and T be semigroups with apartness. A mapping $f : S \to T$ is a homomorphism if

$$\forall_{x,y \in S} (f(xy) = f(x)f(y)).$$

A homomorphism f is

- an *se-embedding* if it is one-one and strongly extensional;
- an *apartness embedding* if it is a-injective se-embedding;
- an *apartness isomorphism* if it is apartness bijection and se-homomorphism.

Within **CLASS**, the semigroups can be viewed, historically, as an algebraic abstraction of the properties of the composition of transformations on a set. Here we can formulate the constructive Cayley's theorem for semigroups with apartness as follows.

Theorem 5 *Every semigroup with apartness se-embeds into the semigroup of all strongly extensional self-maps on a set.*

4.3 Apartness isomorphism theorems

Quotient structures are not part of **BISH**. A quotient structure does not, in general, have a natural apartness relation. So, *the Quotient Structure Problem* - **QSP** is one of the very first problems which has to be considered for any structure with apartness. Talking about the **QSP** for sets and semigroups with apartness and its history - solution of the **QSP** for sets with apartness is for the first time given in [6].

Let us remember that in **CLASS** the compatibility property given by

$$(x, y), (u, v) \in \alpha \Rightarrow (xu, yv) \in \alpha,$$

for any x, y, u, v from a semigroup S, is an important condition for providing the semigroup structure on quotient sets. Now we are looking for the tools for introducing an apartness relation on a factor semigroup. Our starting point are the results from Subsection 3.4 as well as the next definitions.

A relation τ defined on a semigroup S with apartness is called

- *left co-compatible*: $(zx, zy) \in \tau \Rightarrow (x, y) \in \tau$,
- *right co-compatible*: $(xz, yz) \in \tau \Rightarrow (x, y) \in \tau$,
- *co-compatible*: $(xz, yt) \in \tau \Rightarrow (x, y) \in \tau \vee (z, t) \in \tau$,

for any $x, y, z, t \in S$.

The lemma which follows will be used without special announcement.

Lemma 3 *Let τ be a co-quasiorder on a semigroup with apartness S. Then, τ is co-compatible if and only if τ is a left and a right co-compatible.*

Proof. Let τ be a co-compatible co-quasiorder on S, and let $x, y, z \in S$. Then $(zx, zy) \in \tau$ implies $(x, y) \in \tau$ or $(z, z) \in \tau$. The latter is impossible because of strong irreflexivity of τ. Thus $(x, y) \in \tau$, i.e. τ is left co-compatible.

Conversely, let τ be a left and a right co-compatible co-quasiorder on S. Let $x, y, z, t \in S$ be such that $(xz, yt) \in \tau$. By the co-transitivity of τ, it follows either $(xz, yz) \in \tau$ or $(yz, yt) \in \tau$. Now, by the assumption, we have $(x, y) \in \tau$ or $(z, t) \in \tau$, as required. □

A co-equivalence $\boldsymbol{\kappa}$ is a *co-congruence* if it is *co-compatible*.

Theorem 6 *Let S be a semigroup with apartness, and let κ be a co-congruence on S. Define*

$$\begin{aligned} a\kappa^c = b\kappa^c &\Leftrightarrow (a, b) \bowtie \kappa, \\ a\kappa^c \# b\kappa^c &\Leftrightarrow (a, b) \in \kappa, \\ a\kappa^c \, b\kappa^c &= (ab)\kappa^c. \end{aligned}$$

Then $(S/\kappa^c, =, \#, \cdot)$ is a semigroup with apartness. Moreover, the quotient mapping $\pi : S \to S/\kappa^c$, defined by $\pi(x) = x\kappa^c$, is an se-epimorphism.

Proof. By Theorem 2, $(S/\kappa^c, =, \neq)$ is a set with apartness. The associativity of multiplication in S/κ^c follows from that of multiplication on S.

Let $a\kappa^c \, x\kappa^c \# b\kappa^c \, y\kappa^c$. Then $(ax)\kappa^c \#(by)\kappa^c$. By Theorem 2, we have that $(ax, by) \in \kappa$. But κ is a co-congruence, so either $(a, b) \in \kappa$ or $(x, y) \in \kappa$. Thus, by the definition of $\#$ in S/κ^c, either $a\kappa^c \# b\kappa^c$ or $x\kappa^c \# y\kappa^c$. So $(S/\kappa^c, =, \#, \cdot)$ is a semigroup with apartness. Using that fact and the definition of π, we have

$$\pi(xy) = (xy)\kappa^c = x\kappa^c \, y\kappa^c = \pi(x)\pi(y).$$

Hence π is a homomorphism, and, by Theorem 2, π is an se-surjection. □

The *First apartness isomorphism theorem for semigroups with apartness* follows.

Theorem 7 *Let $f : S \to T$ be an se-homomorphism between sets with apartness. Then*

(i) $\operatorname{coker} f$ *is a co-congruence on S;*

(ii) $\operatorname{coker} f \leftarrow\!\!\shortmid \ker f$ *and* $\ker f \subseteq (\operatorname{coker} f)^c$*;*

(iii) $(S/\ker f, =, \#; \cdot)$ *is a semigroup with apartness, where*

$$\begin{aligned} a(\ker f) = b(\ker f) &\Leftrightarrow (a, b) \in \ker f \\ a(\ker f) \# b(\ker f) &\Leftrightarrow (a, b) \in \operatorname{coker} f; \end{aligned}$$

(iv) *The mapping* $\varphi : S/\ker f \to T$, *defined by* $\varphi(x(\ker f)) = f(x)$, *is an apartness embedding such that* $f = \varphi\pi$;

(v) *If* f *maps* S *onto* T, *then* φ *is an apartness isomorphism.*

Proof. (i). Taking into account Theorem 3, it is enough to prove that coker f is co-compatible with multiplication in S. Let $(ax, by) \in \text{coker } f$, i.e. $f(ax)\#f(by)$. Since f is a homomorphism, we have $f(a)f(x)\#f(b)f(y)$. The strong extensionality of multiplication implies that either $f(a)\#f(b)$ or $f(x)\#f(y)$. Thus either $(a, b) \in \text{coker } f$ or $(x, y) \in \text{coker } f$, and therefore coker f is a co-congruence on S.

(ii). This is Theorem 3(ii).

(iii). This follows by Theorem 3 and Theorem 6.

(iv). Using (iii) and the assumption that f is a homomorphism, we have

$$\begin{aligned}\varphi(x(ker\, f)\, y(ker\, f)) &= \varphi((xy)(ker\, f))\\ &= f(xy)\\ &= f(x)f(y)\\ &= \varphi(x(ker\, f))\, \varphi(y(ker\, f)).\end{aligned}$$

Now, by Theorem 3, φ is an apartness embedding.

(v). This follows by Theorem 3 and (iv). □

5 CONCLUDING REMARKS

We live in the era of AI and, as it is pointed out in [28], the era of mathematics.

"Everything we do is based on some mathematical structure, and although mathematics is often considered abstract, it is fundamental to how we understand nature, the larger universe, with its time and space dimensions and a myriad of uncertainties", [29].

Following S. Russell and P. Norvig, [30], there is no the unique definition of AI, rather "The main unifying theme is the idea of an intelligent agent [...] An agent is just something that acts (agent comes from the Latin agere, to do). Of course, all computer programs do something, but computer agents are expected to do more: operate autonomously, perceive their environment, persist over a prolonged time period, adapt to change, and create and pursue goals."

Algebraic structures, as often considered, represent templates for solving problems. Within a scope of an algebraic structure can be found details enabling us with possibility to think clearly about the bigger picture. This can give us a precise way to communicate with other (AI) scientists providing clarity of thought and precise communication.

Within classical mathematics the algebraic theory of semigroups is a relative newcomer, with the theory proper developing only in the second half of the twentieth century. Nowadays, classical semigroup theory is an enormously broad topic with applications which have advanced on a very broad front including AI areas, see, for example, [3], [8]. On the other hand, constructive mathematics has not paid much attention to semigroup theory. Although one of the main motivators for initiating and developing the theory of semigroups with apartness comes from the computer science area, in order to have profound applications, our priority is to work on the growing the general theory. Contrary to the classical case, the applications of constructive semigroups with apartness, due to their novelty, constitute an unexplored area. There are promises of a prospective of applications in other (constructive) mathematics disciplines, certain areas of computer science, social sciences, economics.

Applications of our theory present the second important line of our work. We believe that the theory of constructive semigroups with apartness can be applied in solving problems like the ones

described in D. McAlister, [31]: "A group can be defined as an algebra with one binary operation satisfying certain non-equational conditions, or it can be defined as an algebra with a binary operation, a unary operation (inverse) and a constant (the identity) satisfying certain equations. These two definitions result in technically disjoint classes of objects. Can an automated reasoning system search for, and hopefully find, equivalences between technically distinct definitions, such as the equivalence between foo spaces and topological spaces, or the equivalence between a group as an algebra with one operation and a group as an algebra with two operations and a constant?"

In developing, widening and propagating our theory we have in mind, and we are strongly motivated by AI historical development. The history of AI is one of the newest fields in science and engineering. The work started in earnest soon after World War II, and the name itself was coined in 1956. The history of AI has had cycles of success, misplaced optimism, and resulting cutbacks in enthusiasm and funding. There have also been cycles of introducing new creative approaches and systematically refining the best ones, (source [30]). Nowdays we live in the era of AI.

Let us finish with P. C. Jackson's words, [32]: "Are there some things mathematics cannot describe completely? It is argued in an informal, yet mathematical way that the answer is YES. There are limitations in the method of AI research because it is based (as is all science) on mathematics and the capacities of mathematical disciplines [...] The scientific method is basically a way of selecting mathematical descriptions of the universe."

Acknowledgements

The authors are grateful to anonymous referees for careful reading of the manuscript and helpful comments.

References

[1] Derbyshire, J., 2006, *Unknown Quantity: A Real And Imaginary History of Algebra*, Joseph Henry Press, 374p.

[2] Steffen B., Rüthing O., Huth M., 2018, *Mathematical Foundations of Advanced Informatics - Volume I - Inductive Approach*, Springer, 249p.

[3] Hounkonnou, M. N., Mitrović, M., 2024, *Problematic of mathematics and social sciences and arts: an ubiquitous constructive interaction in algebraic modeling*, pp. 3-30, In Mathematics for Social Sciences and Arts – Algebraic Modeling (Semigroups, arts and social sciences: ubiquitous interactions), Hounkonnou, M. N., Martinovic, D., Mitrović, M., Pattison, P. (Eds.): MATHEMATICS IN MIND, Springer, 2024.

[4] Birkhoff, G., 1971, *The role of modern algebra in computing*, pp. 1-47, In Computers in Algebra and Number Theory, Proceedings Sympos. Appl. Math., New York, 1970, SIAM-AMS Prec., AMS, Providence, R. I. 4.

[5] Mitrović, M., Hounkonnou, M. N., Baroni, M. A., 2021, *Theory of constructive semigroups with apartness - foundations, development and practice*, Fundamenta Informaticae, 184(3), pp. 233-271.

[6] Crvenković, S., Mitrović, M., Romano, D. A., 2013, *Semigroups with Apartness*, Mathematical Logic Quarterly, 59 (6), pp. 407-414.

[7] Crvenković, S., Mitrović, M., Romano, D. A., 2016, *Basic Notions of (Constructive) Semigroups with Apartness*, Semigroup Forum, Volume 92, Issue 3, pp. 659-674.

[8] Mitrović, M., Hounkonnou M. N., Catarino P., 2024, *Constructive semigroups with apartness - a state of the art*, pp. 127-176, In Mathematics for Social Sciences and Arts – Algebraic Modeling (Semigroups, arts and social sciences: ubiquitous interactions), Hounkonnou, M. N., Martinovic, D., Mitrović, M., Pattison, P. (Eds.): MATHEMATICS IN MIND, Springer, 2024.

[9] Mitrović, M., Silvestrov, S., 2020, *(Apartness) Isomorphism theorems for basic constructive algebraic structures with special emphasize on constructive semigroups with apartness - an overview*, pp. 653-686, In Stochastic Processes and Algebraic Structures -From Theory Towards Applications, Volume II: Algebraic Structures and Applications, Västerås and Stockholm, Sweden, October 4-6, Silvestrov, S., Malyarenko, M., Rančić, M. (Eds.), Springer.

[10] Mitrović, M., Silvestrov, S., Crvenković, S., Romano, D. A., 2019, *Constructive semigroups with apartness: towards new algebraic theory*, Journal of Physics : Conference Series (JPCS), Volume 1194, IOP Publishing, 012076, doi:10.1088/1742-6596/1194/1/012076.

[11] Mitrović, M., Hounkonnou, M. N., *Constructive binary structures with apartness vs. classical ones*, Book in progress.

[12] Beeson, M. J., 1985, *Foundations of Constructive Mathematics*, Springer-Verlag, 492p.

[13] Bishop, E., 1967, *Foundations of Constructive Analysis*, McGraw-Hill, New York, 382p.

[14] Bridges D. S., Vîţā, L. S., 2011, *Apartness and Uniformity - A Constructive Development*, CiE series on Theory and Applications of Computability, Springer, 210p.

[15] Troelstra, A. S., Dalen, van D., 1988, *Constructivism in Mathematics, An Introduction, (two volumes)*, North - Holland, Amsterdam, 355+606p.

[16] Mines, R., Richman, F., Ruitenburg, W., 1988, *A Course of Constructive Algebra*. New York: Springer-Verlag, 361p.

[17] Calder, A., 1979, *Constructive Mathematics*, Scientific American , Vol. 241, No. 4, pp. 146-171.

[18] Wang, H., 1958, *Eighty Years of Foundational Studies*, Dialectica, 12, pp. 466-497.

[19] Sommaruga, G., 2011, *Introduction*, Pp 1-49, In Foundational Theories of Classical and Constructive Mathematics, Sommaruga G. (Ed.), Springer, 327p.

[20] Bernays, P., 1964, *On Platonism in mathematics*, pp. 274-286, In Philosophy of Mathematics: Selected Readings, Benacerraf, P., Putnam, H. (Eds.), Prentice-Hall, Englewood Cliffs, NJ.

[21] Dalen, van D., 1995, *Why constructive mathematics?* pp. 141-158, In The Foundational Debate - Complexity and Constructivity in Mathematics and Physics, Depauli-Schimanovich W., Köhler E., Stadler F. (Eds.), SPRINGER-SCIENCE+BUSINESS MEDIA, B.V

[22] Brouwer, L. E. J., 1908, *De onbetrouwbaarheid der logische principes, Tijdschrijt voor wijsbegeerte 2*, pp. 152-158. English translation: *The unreliability of the logical principles*, in Collected Works, Vol. 1, Heyting, A. Ed., North-Holland, Amsterdam, 1975, pp. 107-111.

[23] Bishop, E., Bridges, D. S., 1985, *Constructive Analysis*, Grundlehren der mathematischen Wissenschaften 279, Springer, Berlin, 495p.

[24] Uspenskii, V. A., Semenov, A. L. (Eds.), 1981, Lecture Notes in Computer Science, 122, Springer.

[25] Aczel, P., Rathjen, M., 2000/2001, *Notes on Constructive Set Theory*, REPORT No. 40, 2000/2001, ISSN 1103-467X, ISRN IML-R- -40-00/01- -SE, Institut Mittag-Leffler, The Royal Swedish Academy of Science.

[26] Geuvers, H., Wiedijk, F., Zwanenburg, J., 2002, *A constructive proof of the Fundamental theorem of algebra without using the rationals*, pp. 96-111, In Proceedings of TYPES 2000 Workshop Durham UK, Callaghan, P., Luo, Z., McKinna, J., Pollack, R. (Eds.), Springer-Verlag. LNCS 2277.

[27] Geuvers, H., Pollack, R., Wiedijk, F., Zwanenburg J., 2002, *A Constructive algebraic hierarchy in Coq*, J. Symb. Comput., 34, pp. 271-286.

[28] Bond P., Professor, 2018, THE ERA OF MATHEMATICS, An Independent Review of Knowledge Exchange in the Mathematical Sciences, EPSRC, 68p. https://www.ukri.org/publications/the-era-of-mathematics/

[29] Shapiro, S., 2000, *Philosophy of Mathematics: Structure and Ontology*, Oxford University Press, 296p.

[30] Russell, S., Norvig, P., Eds., 2010, *Artificial Intelligence - A Modern Approach*, Third Edition, PRENTICE HALL SERIES IN ARTIFICIAL INTELLIGENCE, 1151p.

[31] McAllester, D., 1991, *Three Universal Relations*, In Artificial intelligence at MIT: expanding frontiers, MIT Press, 1991.

[32] Jackson, P. C., Jr., 2019, *Introduction to Artificial Intelligence*: Third Edition, Paperback – 14 August (1974, 1985), Dover Publications, Inc., New York, 513p.