Chapter 28
Isomorphism Theorems for Basic Constructive Algebraic Structures with Special Emphasize On Constructive Semigroups with Apartness—An Overview

Melanija Mitrović and Sergei Silvestrov

> "I was just going to say, when I was interrupted, that one of the many ways of classifying minds is under the heads of arithmetical and algebraical intellects. All economical and practical wisdom is an extension of the following arithmetical formula: 2 + 2 = 4. Every philosophical proposition has the more general character of the expression a + b = c. We are mere operatives, empirics, and egotists until we learn to think in letters instead of figures ."
>
> Oliver Wendell Holmes: *The Autocrat of the Breakfast Table*—source [12]

Abstract This overview is an introduction to the basic constructive algebraic structures with apartness with special emphasises on a set and semigroup with apartness. The main purpose of this paper, inspired by Bauer [2], is to make some sort of understanding of constructive algebra in Bishop's style position for those (classical) algebraists as well as for the ones who apply algebraic knowledge who might wonder what is constructive algebra all about. Every effort has been made to produce a reasonably prepared text with such definite need. In the context of basic constructive algebraic structures constructive analogous of isomorphism theorems will be given. Following their development, two points of view on a given subject: classical and constructive will be considered. This overview is not, of course, a comprehensive one.

M. Mitrović (✉)
Department of Mathematics and Informatics, Faculty of Mechanical Engineering,
University of Niš, 18000 Niš, Serbia
e-mail: melanija.mitrovic@masfak.ni.ac.rs

S. Silvestrov
Division of Applied Mathematics, School of Education, Culture and Communication,
Mälardalen University, Box 883, 72123 Västerås, Sweden
e-mail: sergei.silvestrov@mdh.se

S. Silvestrov et al. (eds.), *Algebraic Structures and Applications*,
Springer Proceedings in Mathematics & Statistics 317,
https://doi.org/10.1007/978-3-030-41850-2_28

Keywords Sets with apartness · Groups and rings with tight apartness · Semigroups with apartness · Apartness isomorphism theorems

MSC 2010 Classification 20M15 · 03F65 · 03D45

28.1 Introduction

Throughout this paper *constructive mathematics* is understood as mathematics done in the context of intuitionistic logic, that is, without the law of excluded middle (LEM). There are two main characteristics of constructivist trend. The notion of *truth* is not taken as primitive, and *existence* means constructibility. 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 constructive mathematics *status of existence statement* is much stronger than in **CLASS**. Classical interpretation is that an object exists if its non-existence is contradictory. In constructive mathematics when existence of an object is proved, the proof also demonstrate how to find it. One of the main features of constructive mathematics is that concepts that are equivalent in the presence of LEM, need not be equivalent any more. For example (as we are going to see below in more details), we distinguish nonempty and inhabited set; several types of inequalities; two complements of a given set. More about differences between a classical and a constructive mathematician's view of mathematics can be found in [2, 3, 33].

There is no doubt about deep connections between constructive mathematics and computer science. Moreover, "if programming is understood not as the writing of instructions for this or that computing machine but as the design of methods of computation that is the computer's duty to execute, then it no longer seems possible to distinguish the discipline of programming from constructive mathematics", [28]. Often recommended as a good introduction to constructive mathematics and its application to computer science is [7].

Constructive mathematics is not unique notion. Various form of constructivism have been developed over time. Principle trends include the following varieties: **INT**—Brouwer's intuitionistic mathematics, **RUSS**—the constructive recursive mathematics of the Russian school of Markov, **BISH**—Bishop's constructive mathematics. 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 *algorithm* or *finite routine* is taken as primitive in **INT** and **BISH**, while **RUSS** operates with fixed programming language and algorithm is a sequence of symbols in that language.

We have to emphasize that Errett Bishop—style constructive mathematics, **BISH**, forms the framework for our work. **BISH** originated in 1967 with the publication of the book [4] and with its second, much revised edition in 1985 [5]. There has been a steady stream of publications contributing to Bishop's programme since 1967, see [6, 9, 37]. A ten-year long systematic research of computable topology, using apartness as the fundamental notion, resulted in the first book [10] on topology within **BISH** framework. At heart, Bishop's constructive mathematics is simply mathematics done with intuitionistic logic, and may be regarded as "constructive mathematics for the working mathematician", [37]. The main activity in the field consists in proving theorem rather then demonstrating the unprovability of theorems (or making other metamathematical observations), [3]. Following [4], every effort has been made to follow classical development as closely as possible; every theorem of **CLASS** present a challenge: find a constructive version with a constructive proof; constructive version can be obtained by strengthening the conditions or weakening the conclusion of the theorem. Modern algebra, as is noticed in [7], "contrary to Bishop's expectations, also proved amenable to natural, thoroughgoing, constructive treatment".

Working within classical theory of semigroups over the years [30], one of the authors of this paper "on the odd" day several years ago has decided to change classical background with intuitionistic one. This means, among other things, that perfect safety of classical theory with developed notions, notations and methodologies was left behind. Instead, an adventure of exploring algebraically new area (even without clear stated notions and notations) of *constructive semigroups with apartness* has been started. What we have "in hand" at that moment was experience and knowledge coming from classical semigroup theory and other constructive mathematics disciplines. Following Bishop we make every effort to follow classical case as closely as possible, but our work distinguishes from classical case by two significant aspects: we use intuitionistic logic rather than classical through, and our work is based on the notion of apartness (between elements, elements and sets). This means, that lot of ideas, notions and notations come from other constructive disciplines like, for example, constructive analysis, and, especially, from constructive topology, as well as constructive theories of groups and rings with tight apartness. Path that we have passed from the experience and knowledge of just mentioned classical and constructive theories to the first results in "our" theory will be given. For a classical algebraists like, for example us (who "on the odd day" wonder what constructive algebra is all about, even more) who wants to find out what a feeling is doing it, he/she will understand soon that constructive algebra is more complicated than classical in various ways: algebraic structure as a rule do not carry a decidable equality relation (this difficulty is partly met by the introduction of a strong inequality relation, the so-called apartness relation); there is (sometime) awkward abundance of all kinds of substructures, and hence of quotient structures, [37]. Among additional troubles for working algebraist is so-called the *Constant domain axiom*: folklore type of axiom in **CLASS** algebra

$$\varphi \vee \forall x\, \psi(x) \;\leftrightarrow\; \forall x(\varphi \vee \psi(x)),$$

its constructive version

$$\varphi \vee \forall_x\, \psi(x) \;\rightarrow\; \forall_x(\varphi \vee \psi(x))$$

can be source of troubles at the beginning of his/her constructive experience. Of course good introductory literature can help a lot in overcoming troubles appearing when someone switch from classical to constructive algebra. Our personal feeling, coming from our experience, is that, contrary to the cases with constructive analysis and topology, there is a lack of such type of texts in the case of constructive algebra. This overview is an introductory course to the basic constructive algebraic structures with apartness with special emphasize on a set and semigroup with apartness. The main purpose of this paper, inspired by [2], is to make some sort of understanding of constructive algebra in Bishop's style position for those (classical) algebraists as well as for the ones who apply algebraic knowledge who might wonder what is constructive algebra all about.

In the context of semigroups with apartness the basic notions of special subsets and special relations as well as constructive analogues of classical isomorphism theorems will be presented. Especially, an overview to the development of so called isomorphism theorems in certain algebraic settings—from classical to constructive—will be given. It is not, of course, comprehensive one. Importance of isomorphism theorems in any settings is well-known within mathematical world. Discovery of their importance within computer science community, [16], is, more or less, recent phenomena.

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

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

Definition given above justifies organization of this paper. Classical background of our work, i.e. elementary set theory, group theory, ring theory and semigroup theory is given in Sect. 28.2. Isomorphism theorems for all just mentioned structures are given too. Moreover, contents presented in Sect. 28.2 are, more or less, considered to be introductional one for almost all (abstract) algebraic books. Main properties of constructive set, groups, rings and semigroups with (tight) apartness, as well as adequate apartness isomorphism theorems for all of them are presented in Sect. 28.3. Some possible applications of basic algebraic structures with apartness as well as some final remarks are given in Sect. 28.4.

More background on constructive mathematics can be found in [3, 4, 10, 37]. The standard reference for constructive algebra is [29]. For classical case see [24, 25]. Examples of applications of these ideas can be found in [1, 8, 11, 15, 32].

28.2 Algebraic Structures within CLASS

A very short account of the abstract algebra and its development will be given. Over the course of 19th century, algebra made transition from a subject concerned entirely with the solution of mostly polynomial equations to a discipline that deals with general structures within mathematics. (Loosely speaking, structure may be understood as a set together with one or more operations which are subject to certain conditions.) Term abstract algebra as a name of this area appeared in early 20th century.

An *algebraic structure* can be described as a set with some (not necessarily, but often, binary) operations for combining them. Some fundamental concepts in abstract algebra are:

- set and operation(s) defined on that set;
- certain algebraic lows which all elements of the structure can respect (like, for example, associativity, commutativity);
- some elements with special behavior in connection with operation(s): idempotent elements, identity elements, inverse elements, ...

Combining the above concepts gives some of the most important structures in mathematics: groups, rings, semigroups, ... Centered around an algebraic structure are notions of: substructure, homomorphism, isomorphism, congruence, quotient structure.

In algebra within **CLASS** 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 the concept which goes hand in hand with congruences. Thus concepts of congruence, quotient structure and homomorphism are closely related. Knowing that the congruence ρ on an algebraic structure S is the kernel of the quotient map from S onto S/ρ, we can treat congruence relations on S as kernels of homomorphisms with S as the domain. 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 algebra. The theorems of this type exists for groups, rings, semigroups, vector spaces, modules, Lie algebras and various other algebraic structures. Throughout this section we will limited ourselves to basic algebraic structures: groups, rings and semigroups. But, taking into account that set theory is the proper framework for abstract mathematical thinking as well as fact that an algebraic structure can be viewed as a set with specified additional structure, isomorphism theorems for sets follow first.

28.2.1 Isomorphism Theorems for Sets

The goal of this part is simply to review briefly (some of) the basic concepts of set theory. Our approach to the theory of sets will be quite informal. We will take the intuitive approach that a set is some given collection of objects, called elements or members of the set. Set is considered as a primitive notion which one does not define.

A few remarks about terminology and notations follow in sequel. The notation $a \in S$ means that a is an element of S, and $b \notin S$ means that b is not an element of S. If S and T are sets, $T \subseteq S$ denotes inclusion, i.e. T is a subset of S–all elements of T are also in S. S and T are equal, $S = T$, if $S \subseteq T$ and $T \subseteq S$. The empty set $\emptyset$ is the set with no elements. It is a subset of any set S. T is a proper subset of S if $T \neq \emptyset$ and $T \neq S$. One final, notational remark: a set is frequently formed by taking its elements the ones which have a specific property denoted, for example, as P

$$\{x \, : \, P(x)\}.$$

A subset T of S formed by selecting those elements of S with property Q is written as

$$T = \{x \in S \, : \, Q(x)\}.$$

The *cartesian product* of sets S and T is the set $S \times T$ of all ordered pairs (x, y) with $x \in S$ and $y \in T$. We have

$$(x_1, y_1) = (x_2, y_2) \ \Leftrightarrow \ x_1 = x_2 \wedge y_1 = y_2,$$

for $(x_1, y_1), (x_2, y_2) \in S \times T$.

A *mapping* f from S to T, denoted by $f : S \rightarrow T$, is a subset of $S \times T$ such that for any element $x \in S$ there is precisely one element $y \in Y$ for which $(x, y) \in f$, i.e.

$$(\forall x, y \in S) \, x = y \Rightarrow f(x) = f(y).$$

Instead of $(x, y) \in f$, we usually write $y = f(x)$. Two mappings $f, g : S \rightarrow T$ are equal if they are equal as subsets of $S \times T$, that is $f = g \Leftrightarrow (\forall x \in S) \, (f(x) = g(x))$.

A mapping f is

- *surjective* or *onto*: $(\forall y \in T) \, (\exists x \in S) \, (y = f(x))$;
- *injective* or *one-one*: $f(x) = f(y) \Rightarrow x = y$;
- *bijection*: one-one map from S onto T.

The cartesian product of a set S with itself, $S \times S$ is of special importance. A subset of $S \times S$, or, equivalently, a property applicable to elements of $S \times S$, is called *binary relation on* S. In general, there are many properties (like for example: reflexivity, symmetry, transitivity) that binary relations may satisfy on a given set. As usual, for a relation ρ on S, $a\rho = \{x \in S \, : \, (a, x) \in \rho\}$, and $\rho a = \{x \in S \, : \, (x, a) \in \rho\}$ are the left and the right ρ-class of the element $a \in S$ respectively.

The concept of an *equivalence*, i.e. reflexive, symmetric and transitive relation, is an extremely important one and plays a central role in all of mathematics. Any mapping $f : S \rightarrow T$ gives rise to an equivalence on its domain:

$$ker \, f = \{(x, y) \in S \times S \, : \, f(x) = f(y)\},$$

called *kernel of mapping* f or *the equivalence relation induced by* f. On the other hand, we can define onto (surjective) functions from equivalences.

Lemma 28.2.1 *Let ε be an equivalence on S. Mapping $\pi : S \to S/\varepsilon$ defined by $\pi(x) = x\varepsilon$, $x \in S$, is an onto mapping.*

The set $S/\varepsilon = \{x\varepsilon : x \in S\}$ is called the *quotient set of* S *by* ε, and mapping $\pi : S \to S/\varepsilon$ is the *quotient* (or *natural*) *mapping*.

So, starting from the mapping, we can define an equivalence relation, and starting from that equivalence we can define its quotient mapping. What we can say about connection(s) between the original mapping and the quotient mapping? The *Isomorphism theorem for sets* follows.

Theorem 28.2.2 *Let $f : S \to T$ be a mapping between sets S and T. Then, the mapping $\theta : S/ker\ f \to T$ defined by $\theta(x(ker\ f)) = f(x)$ is one-one such that $f = \theta \circ \pi$. If f maps S onto T, then θ is a bijection.*

Proof Let $x(ker\ f) = y(ker\ f)$. Then $(x, y) \in ker\ f$, thus $f(x) = f(y)$ and θ is well-defined. Let $x \in S$. Using the Lemma 28.2.1, we have

$$(\theta \circ \pi)(x) = \theta(\pi(x)) = \theta(x(ker\ f)) = f(x).$$

If $\theta(x(ker\ f)) = \theta(y(ker\ f))$ then $f(x) = f(y)$, which, further, means that $(x, y) \in ker\ f$. Thus $x(ker\ f) = y(ker\ f)$, and θ is one-one.

If f is onto mapping then for any $y \in T$ there is $x \in S$ such that $y = f(x)$. But then $y = \theta(x(ker\ f))$ and so θ is onto. We have that θ is bijection.

28.2.2 Algebraic Structures—Some Properties

Loosely speaking, algebraic structure (such as a group, ring, or semigroup) may be understood as a set together with one or more operations (not necessarily, but often binary) which are subject to certain conditions.

A mapping $f : S \to T$ between two algebraic structures S and T of the same type (that is of the same name), that preserves the operations or is compatible with the operations of the structures is called homomorphism. This means that if, for example, $\circ$ is an binary operation defined on S and T, then

$$f(x \circ y) = f(x) \circ f(y).$$

When an algebraic structure includes more than one operation, in order to be homomorphisms, mappings are required to be compatible with each operation. Homomorphisms are essential to the study of any class of algebraic objects.

Several types of homomorphisms have a specific name. A homomorphism f is

- *embedding*: f is one-one;

- *onto* or *epimorphism*: $f(S) = T$;
- *isomorphism*: f is onto embedding.

A homomorphism $f : S \to S$ is called *endomorphism*. An endomorphism f is *automorphism* if f is isomorphism.

An equivalence relation ρ on an algebraic structure S (such as a group, a ring, or a semigroup) that is compatible with the structure is called a *congruence*. This means that, if, for example, $\circ$ is an binary operation defined on S, a congruence relation ρ on S is an equivalence satisfying

$$(x, y), (z, w) \in \rho \Rightarrow (x \circ z, y \circ w) \in \rho,$$

for any $x, y, z, w \in S$. When an algebraic structure includes more than one operation, congruence relations are required to be compatible with each operation. The quotient set S/ρ becomes the structure of the same type, in a natural way, by defining the operation(s) as

$$(x\rho) \circ (y\rho) = (x \circ y)\rho.$$

The quotient mapping $\pi : S \to S/\rho$ is an onto homomorphism or an epimorphism.

For any homomorphism $f : S \to T$ between algebraic structures of the same type $ker\ f$ is a congruence on S. By the (First) Isomorphism theorem, the image of S under f is a substructure of T isomorphic to the quotient of S by this congruence.

In the particular case of groups or rings, congruence relations can be described in elementary terms—which will be presented in next two subsections.

28.2.2.1 Isomorphism Theorems for Groups

Group theory is the right place to start the study of abstract algebra. Groups were the first algebraic structures which are characterized axiomatically and developed systematically from an abstract point of view. But more important, groups are one of the fundamental building blocks to the development of more complex abstractions such as rings and fields. This qualifies them to be considered first. Group structure may be axiomatically characterized in several ways. The way given below is considered to be the most direct and convenient.

A *group* $(G, \cdot)$ is a nonempty set G with a binary operation $\cdot$ called the product or multiplication such that:

(G1) $(\forall x, y, z \in G)\ (xy)z = x(yz)$ (the associativity axiom)

(G2) $(\exists e \in G)(\forall x \in G)\ xe = ex = x$ (the identity axiom)

(G3) $(\forall x \in G)(\exists x^{-1} \in G)\ xx^{-1} = x^{-1}x = e$ (the inverse axiom)

(G1), (G1), (G1) are *the axioms of group structure*.

Let $f : G \to H$ be a homomorphism of groups. The kernel of f is

$$ker\ f = \{(x, y) \in G \times G\ :\ f(x) = e_H\}.$$

Theorem 28.2.3 *If $f : G \to H$ is a homomorphism of groups, then f is an embedding if and only if ker $f = \{e_G\}$.*

A nonempty subset H of G is a *subgroup* of G if it is a group in its own right under group multiplication inherited from G. Clearly, nonempty subset H of G is a subgroup if and only if $xy^{-1} \in H$ whenever $x, y \in H$. If H is a subgroup of G and $x \in G$ then

$$Hx = \{hx : h \in H\} \qquad (xH = \{xh : h \in H\})$$

is a *right* (*left*) *coset* of H in G. In general it is not the case that a right coset is also a left coset. A subgroup N possessing one of the three equivalent conditions:

(N1) $(\forall x \in G)\ xN = Nx$,
(N2) $(\forall x \in G)\ x^{-1}Nx = N$,
(N3) $(\forall x \in G)(\forall h \in N)\ x^{-1}hx \in N$,

is called *normal subgroup*. Normal subgroups, introduced by Galois at the beginning of the 19th century, play an important role in determining both the structure of a group G and the nature of homomorphisms with domain G.

Theorem 28.2.4 *If N is a normal subgroup of a group G, then the set of all cosets of N in G denoted by $G/N = \{xN : x \in G\}$ is a group with the multiplication given by $(xN)(yN) = (xy)N$.*

The group G/N from the previous theorem is called *the quotient group* or *factor group* of G by N.

Remark 28.2.5 If group G is written additively, then the group operation in G/N is given by $(x + N) + (y + N) = (x + y) + N$.

In what follows relationships between normal subgroups, quotient groups and homomorphisms will be given.

Theorem 28.2.6 *Let $f : G \to H$ be a homomorphism of groups. Then the kernel of f is a normal subgroup of G. Conversely, if N is a normal subgroup of G, then the mapping $\pi : G \to G/N$ defined by $\pi(x) = xN$, $x \in G$, is an* onto *homomorphism or epimorphism with kernel N.*

The mapping $\pi : G \to G/N$ from the previous theorem is called *the quotient* (*canonical*) *epimorphism*. Finally, the (*First*) *Isomorphism theorem* for groups follows.

Theorem 28.2.7 *Let N be a normal subgroup of a group G. Then, for every homomorphism of groups $f : G \to H$ whose kernel contains N there exists unique homomorphism $\theta : G/N \to H$ such that $f = \theta \circ \pi$. If, in addition, f is* onto*, then θ is an isomorphism.*

Remark 28.2.8 In the particular case of groups congruence relations can be described in terms of normal subgroups. In fact, every congruence corresponds uniquely to some normal subgroup.

28.2.2.2 Isomorphism Theorems for Rings

Another fundamental concept in the study of algebra is that of a ring. We consider rings, homomorphisms, ideals and their relationships. Content which is going to be presented is simply a straightforward generalization to rings of concepts which have proven useful in group theory.

A *ring* $(R, \cdot, +)$ is a nonempty set R with two binary operations $\cdot$ and $+$ called multiplication and addition respectively, such that:

(R1) $(R, +)$ is an abelian group;

(R2) $(\forall x, y, z \in G)$ $(xy)z = x(yz)$ (the associativity axiom for multiplication)

(R3) $(\forall x, y, z \in G)$ $x(y+z) = xy + xz$ and $(x+y)z = xy + xz$ (left and right distributivity)

The additive identity element of a ring is called *the zero* element and denoted by 0.

A mapping $f : R \to S$ between two rings R and S is a *homomorphism of rings* if

$$f(x+y) = f(x) + f(y) \quad \wedge \quad f(xy) = f(x)f(y),$$

for any $x, y \in R$. The kernel of a homomorphism f of rings R and S is its kernel as a map of additive groups, that is

$$ker\ f = \{r \in R \,:\, f(r) = 0\}.$$

A subring I of a ring R is *an ideal* of R if $xr, rx \in I$, for any $x \in I, r \in R$. Ideals play approximately the same role in the theory of rings as normal subgroups do in the theory of groups.

Theorem 28.2.9 *Let $f : R \to S$ be a homomorphism of rings. Then*

$$ker\ f = \{r \in R \,:\, f(r) = 0\}$$

is an ideal of R.

The various isomorphism theorems for groups can be "translated" for rings with normal subgroups and groups replaced by ideals and rings respectively. For example, let R be a ring and I an ideal of R. $(R, +)$ is abelian group, so I is a normal subgroup, which, by Theorem 28.2.4 and Remark 28.2.5, means that $(R/I, +)$ is a quotient group. Moreover, we have

Theorem 28.2.10 *Let R be a ring and I an ideal of R. Then the additive quotient group R/I is a ring with multiplication given by*

$$(x+I)(y+I) = xy + I.$$

Once again, from the analogy with groups, can be deduced that ideals and homomorphisms of rings are closely related.

Theorem 28.2.11 *If $f : R \to S$ is a homomorphism of rings, then ker f is an ideal in R. Conversely, if I ia an ideal of R, then the quotient mapping $\pi : R \to R/I$, $\pi(r) = r + I$, is an* onto *homomorphism with kernel I.*

The *Isomorphism theorem* for rings follows.

Theorem 28.2.12 *Let $f : R \to S$ be a homomorphism of rings, and let I be an ideal of R contained in ker f. Then, there exists unique homomorphism of rings $\theta : R/I \to S$, such that $f = \theta \circ \pi$. If, in addition, f is* onto*, then θ is an isomorphism and $I =$ ker f.*

To conclude, these two examples—groups and rings—suggest that any congruence on an algebraic structure might be determined by a single congruence class of that congruence. Following [17], "very often in mathematics the crucial problem is to recognize and to discover what are the relevant concepts; once this is accomplished the job may be more than half done." It is possible to distinguish *normal subgroups*, in the case of groups, and *ideals*, in the case of rings, which are respectively, the congruence classes containing the unit element of the group and the zero element of the ring. Unfortunately this is not always the case as we are going to see in the next subsection.

28.2.2.3 Isomorphism Theorems for Semigroups

A *semigroup* $(S, \cdot)$ is a nonempty set S with a binary operation $\cdot$ called multiplication such that:

$$(x \cdot y) \cdot z = x \cdot (y \cdot z),$$

for any $x, y, z \in S$. Frequently, xy is written rather than $x \cdot y$.

In the history of mathematics, the algebraic theory of semigroups is a relative newcomer, with the theory proper developing only in the second half of the twentieth century. Historically, it can be viewed as an algebraic abstraction of the properties of the composition of transformations on a set. But, there is no doubt about it, the main sources came from group theory and ring theory. "Of all generalizations of the group and ring concepts the semigroup is the one that has attracted the most interest by far", [23]. (More about the history of semigroups can be found in [22].) However, semigroups are not a direct generalizations of group theory as well as ring theory. Semigroups do not much resemble groups and rings. In fact, semigroups do not much resemble any other algebraic structure.

Let us remember: congruences on groups are uniquely determined by its normal subgroups, and, on the other hand, there is a bijection between congruences and the ideals of rings. Study of congruences on semigroups is more complicated—no such device is available. One must study congruences as such. A *congruence* ρ on a semigroup S is an equivalence with *compatibility property:*

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

for any $x, y, u, v \in S$.

Theorem 28.2.13 *Let $f : S \to T$ be a homomorphism between semigroups S and T. Then*

$$ker\ f = f \circ f^{-1} = \{(x, y) \in S \times S : f(x) = f(y)\}$$

is a congruence on S.

Classically, the quotient set S/ρ is then provided with a semigroup structure.

Theorem 28.2.14 *Let S be a semigroup and ρ a congruence on it.Then S/ρ is a semigroup with respect to the operation defined by $(x\rho)(y\rho) = (xy)\rho$, and the mapping $\pi : S \to S/\rho$, $\pi(x) = x\rho$, $x \in S$, is an* onto *homomorphism.*

We can now extend Theorem 28.2.2 to semigroups and homomorphisms. The (*First*) *Isomorphism theorem for semigroups* follows.

Theorem 28.2.15 *Let $f : S \to T$ be a homomorphism between semigroups S and T. Then, the mapping $\theta : S/ker\ f \to T$ defined by $\theta(x(ker\ f)) = f(x)$ is an embedding such that $f = \theta \circ \pi$. If f maps S onto T, then θ is an isomorphism.*

Proof Taking into account Theorems 28.2.2 and 28.2.14, to prove the theorem we have to prove that θ is a homomorphism. Let $x(ker\ f), y(ker\ f) \in S/ker\ f$. Then

$$\theta(x(ker\ f)y(ker\ f)) = \theta(xy(ker\ f)) = f(xy) = f(x)f(y) = \theta(x(ker\ f))\theta(y(ker\ f)).$$

The theorem which follows is concerned with a more general situation.

Theorem 28.2.16 *Let ρ be a congruence on a semigroup S, and let $f : S \to T$ be a homomorphism between semigroups S and T such that $\rho \subseteq ker\ f$. Then there exists a homomorphism of semigroups $\theta : S/\rho \to T$, such that $f = \theta \circ \pi_\rho$. If, in addition, f is* onto*, then θ is an isomorphism.*

Proof Define $\theta : S/\rho \to T$ by $\theta(x\rho) = f(x)$, $x \in S$. For $x, y \in S$ such that $x\rho = y\rho$ we have $(x, y) \in \rho \subseteq ker\ f$ which, further, implies $f(x) = f(y)$. Thus θ is well-defined. It is a routine matter to prove that θ is a homomorphism. The rest of the proof follows by (similar to) Theorem 28.2.15.

28.3 Algebraic Structures within BISH

> "It is important to keep in mind that constructive algebra is algebra;
> in fact it is a generalization of algebra in that we do not assume the law of excluded middle." [29]

One of the main topics in constructive algebra are constructive algebraic structures with apartness. The principal novelty in treating basic algebraic structures constructively is that apartness becomes a fundamental notion. Beside adopting the classical notions of group, ring, ..., one axiomatizes group, ring, ..., *with apartness*. The study of algebraic structures in the presence of apartness was started by Heyting, [18]. Heyting had given the theory a firm base in [20].

In what follows we will define the notions of group with tight apartness, commutative ring with tight apartness following [35, 37], and semigroup with (not necessarily tight) apartness following [13, 14, 31]. Any of these basic algebraic structures with apartness can be viewed as set with apartness with basic operation(s) defined on it that respect apartness on a proscribed way.

Quotient structures are not part of **BISH**. Quotient structure does not, in general, have a natural apartness relation. So, *the Quotient Structure Problem* (QSP) is one of the very first problem which has to be considered for any structure with apartness. Solution QSP for groups with tight apartness and rings with tight apartness obtained at the beginning of 80s of last century are presented in [35], see also [37]. Those results, as well as the similar ones coming from some other constructive theories, [10, 26], inspired us to give solutions of QSP problems for sets and semigroups with apartness in 2013, [13]. Till the end of this section those solutions will be presented.

28.3.1 QSP for Set with Apartness

We begin this subsection by introducing the constructive framework within which our further considerations lie. Foundation stones for **BISH** include the notion of positive integers, sets and functions. Some results from [13, 31] will be presented too.

The set $\mathbb{N}$ of positive numbers is regarded as basic set, and it is assumed that the positive numbers have the usual algebraic and order properties, including mathematical induction. “Almost equal in importance to number are constructions by which we ascend from number to higher levels of mathematical existence”, [4]. Restriction to a bottom-up construction of sets ‘force’ at each level to use only objects already constructed.

Contrary to classical case a set exists only when it has been defined. In general, to define a set S we have to give two pieces of information: a property that enables us to construct members of S and to describe the equality $=$ between elements of S—which is a meter of convention, except that it must be an equivalence. A set $(S, =)$ is an *inhabited* set if we can construct an element of S. Distinction between notions of nonempty set and inhabited set is a key in constructive set theories.

The notion of equality of elements of different sets is not defined. The only way to regard elements of different sets equal is by realizing those sets as subset of third one. That is why the operations of union and intersection are defined only for sets which are given as subsets of a given set. There is another problem more to be faced with when we consider families of sets that are closed under a suitable operation of complementation. Following [5] “we do not wish to define complementation in the terms of negation; but on the other hand, this seems to be the only method available. The way out of this awkward position is to have a very flexible notion based on the concept of a *set with an apartness* relation," whose axiomatization will be presented later on.

A property P which is applicable to the elements of a set S determines subset of S denoted by $\{x \in S : P(x)\}$. 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, means that it does not depend on the particular description by which x is given to us", [10].

An inhabited subset 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. Some of them are "brand new" (for example: consistency, irreflexivity, cotransitivity), and/or some of them, inherited from classical mathematics (**CLASS**) (like: reflexivity, symmetry, transitivity), "play game" under constructive rules. In **CLASS** equivalence is the natural generalization of equality. A theory with equivalence involves the equivalence and functions and relations respecting this equivalence. In constructive mathematics the same works without difficulty. Many sets come with binary relation called inequality satisfying certain properties, and denoted by $\neq$, # or $\not\simeq$. In general, more computational information is required to distinguish elements of a set S, then to show that elements are equal. Comparing with **CLASS**, the situation for inequality is more complicated. There are different types of inequalities (denial inequality, diversity, apartness, tight apartness—to mention few), some of them completely independent, which only in **CLASS** are equal to one standard inequality, [36]. So, in **CLASS** the study of equivalence relation suffices, but, in constructive mathematics inequality becomes a "basic notion in intuitionistic axiomatics". For example, apartness is a basic ingredient of constructive real numbers: two real numbers are apart if it can positively be decided that they are distinct from each other. Apartness, as a positive version of inequality, "is yet another fundamental notion developed in intuitionism which shows up in computer science," [27].

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 implies that $x\#y$ and vice versa: given x and y, we may have neither a proof that $x = y$ nor a proof that $x\#y$. Negation of apartness is an equivalence $(\approx) =_{def} (\neg\,\#)$ called *weak equality* on S.

Remark 28.3.1 The statement that every equivalence relation is the negation of some apartness relation is equivalent to excluded middle. The statement that the negation of an equivalence relation is always an apartness relation is equivalent to the nonconstructive de Morgan law.

The apartness on a set S is *tight* if

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

Apartness is tight just when $\approx$ and $=$ are the same, i.e. $\neg(x\#y) \ \Leftrightarrow\ x \approx y$. In what follows we will denote tight apartness by $\sharp$. Set with tight apartness will be denoted by $(S, \approx, \sharp)$, or, shortly by $(S, \sharp)$. In some books and papers, like [37], the term "preapartness" is used for an apartness relation, while "apartness" means tight apartness. Tight apartness on the real numbers was introduced by L. Brouwer in the early 1920s. Brouwer introduced the notion of apartness as a positive intuitionistic basic concept. A formal treatment of apartness relations began with A. Heyting's formalization of elementary intuitionistic geometry in [19]. Intuitionistic axiomatizations of apartness is given in [21].

By extensionality we have

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

which equivalent form is

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

A *set with apartness* $(S, =, \#)$ is the starting point for our further considerations, and will be simply denoted by S. The existence of an apartness relation on a structure often gives rise to apartness relation on another structure. For example, given two sets with apartness $(S, =_S, \#_S)$ and $(T, =_T, \#_T)$, it is permissable to construct the set of mappings between these. Let $f : S \to T$ be a mapping (function) of sets with apartness S and T. The *well-definedness* or *weak extensionality* of f, i.e.

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

follows by extensionality. Constructively, as apartness is more fundamental then equality, the property of strong extensionality is more fundamental then well-definedness. A mapping $f : S \to T$ is *strongly extensional* mapping, or, for short, *se-mapping*, if

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

Furthermore, f is

- *apartness injective*, shortly *a-injective*: $\forall_{x,y\in S}\,(x\#_S y \ \Rightarrow\ f(x)\#_T f(y))$;
- *apartness bijection* between S and T if it is a-injective, bijective se-mapping.

Folklore type of result is next

Theorem 28.3.2 ([29]) *Let $(A, =, \#)$ be a set with apartness. If $S = A^A$ is the set of all se-mappings from A to A, then $(S, =, \#)$ with*

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

and

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

is a set with apartness.

Given 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

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

Presence of apartness implies appearance of different types of substructures connected to it. Inspired by constructive topology with apartness, [10], we define relation $\bowtie$ between an element $x \in S$ and a subset Y of S by

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

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

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

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

$$\sim Y \;=_{def}\; \{x \in S \;:\; x \bowtie Y\}.$$

The properties of # ensures that, in general, $\sim Y \subseteq \neg Y$.

Complements (both of them) are used for classification of subsets of a given set. A subset Y of S is

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

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

– *an strongly extensional* subset of S, shortly *an se-subset of* S, if

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

– *an SE-subset of* S, if

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

Proposition 28.3.3 *Let Y be a subset of S. Then:*

(i) *any se-subset is an SE-subset of S;*
(ii) *any SE-subset Y of S satisfies $\sim Y = \neg Y$;*
(iii) *any se-subset is a d-subset of S.*

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

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

(ii). Let Y be an SE-subset, and let $a\in\neg Y$. By the 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 $a\in{\sim}Y$.

(iii). Follows immediately by (ii) and the definition of d-subsets.

In what follows se-subsets will be one of the main objects of investigation.

Let $(S\times S,=,\#)$ be a set with apartness. A subset of $S\times S$ is called a (*binary*) *relation* on S. If α and β are relations on S, then α is *associated* with β if

(1) $\forall_{x,y,z\in S}\,((x,y)\in\alpha\wedge(y,z)\in\beta\ \Rightarrow\ (x,z)\in\alpha).$

If α and β are, respectively, apartness and equality on S, then (1) is, in fact, (A5).

Let $\alpha\subseteq S\times S$ be a relation on S. Then

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

for any $(a,b)\in S\times S$. Apartness complement of α is a relation on S

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

Example 28.3.4 Let $S=\{1,2,3\}$ be a set with apartness $\#=\{(1,3),(3,1),(2,3),(3,2)\}$. Let $\alpha=\{(1,3),(3,1)\}$ be a relation on S. Its a-complement

$$\sim\alpha=\{(1,1),(2,2),(3,3),(1,2),(2,1)\}$$

is a proper subset of its logical complement $\neg\alpha$.

Among relations defined on S we consider only those which are related to the apartness in the following way. A binary relation α defined on a set with apartness S is

– consistent if $\alpha\subseteq\#$;
– cotransitive if $(x,z)\in\alpha\ \Rightarrow\ \forall_y\,((x,y)\in\alpha\ \vee\ (y,z)\in\alpha)$.

In the constructive order theory the notion of *cotransitivity*, i.e. 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. In what follows some connections between relations of certain kind and their a-complements will be given.

Lemma 28.3.5 *Let α be a relation on S. Then*

(i) *α is consistent if and only if $\sim\alpha$ is reflexive;*
(ii) *if α is reflexive then $\sim\alpha$ is consistent;*
(iii) *if α is symmetric then $\sim\alpha$ is symmetric.*

Proof (i) Let α be a consistent relation on S. Reflexivity of $\sim\alpha$ is almost obvious.

Let $\sim\alpha$ be reflexive, i.e. $(x, x) \in\sim\alpha$, for any $x \in S$. On the other hand, definition of a-complement implies $(x, y)\#(x, x)$ for any $(x, y) \in \alpha$. So, $x\#x$ or $x\#y$. Thus, by the assumption, $x\#y$, i.e. α is consistent.

(ii) Let α be reflexive. Then

$$\begin{aligned}(x, y) \in\sim\alpha &\Leftrightarrow \forall_{(a,b)\in\alpha}\,((x, y)\#(a, b))\\ &\Rightarrow x\#a \;\vee\; y\#b\\ &\Rightarrow x\#a \;\vee\; x\#y \;\vee\; x\#b\\ &\Rightarrow (x, x)\#(a, b) \;\vee\; x\#y,\end{aligned}$$

which, by the assumption, implies $x\#y$.

(iii) If α is symmetric, then

$$\begin{aligned}(x, y) \in\sim\alpha &\Leftrightarrow \forall_{(a,b)\in\alpha}\,((x, y)\#(a, b))\\ &\Rightarrow \forall_{(b,a)\in\alpha}\,((x, y)\#(b, a))\\ &\Rightarrow \forall_{(b,a)\in\alpha}\,(x\#b \;\vee\; y\#a)\\ &\Rightarrow \forall_{(a,b)\in\alpha}\,((y, x)\#(a, b))\\ &\Leftrightarrow (y, x) \in\sim\alpha.\end{aligned}$$

In general, by Example 28.3.4, a-complement of a relation is a proper subset of its logical complement. Relations for which both complements coincide are considered below. Consistent and cotransitive relation τ is called a *coquasiorder*. Their important property is given below.

Proposition 28.3.6 *Let τ be a coquasiorder on S. Then:*

(i) *τ is an SE-subset of $S \times S$;*
(ii) *$\sim\tau = \neg\tau$.*

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

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

that is, τ is an SE-subset.

(ii) Follows by (i) and Proposition 28.3.3(ii).

Coquasiorders are one of the main building block for the order theory of semigroups with apartness we develop.

Quotient structures are not part of **BISH**. Quotient structure does not have, in general, a natural apartness relation. For most purposes we overcome this problem using a *coequivalence*–symmetric coquasiorder–instead of an equivalence. Existing properties of a coequivalence guarantees its a-complement be an equivalence as well as quotient set of that equivalence will inherit an apartness.

For what follows we will need the following definition. For any two relations α and β on S we say that α *defines apartness on* $\boldsymbol{S/\beta}$ if

(Aq6) $x\beta \# y\beta \Leftrightarrow_{def} (x, y) \in \alpha$.

(AP5), i.e. its equivalent form, gives

(Aq6') $((x, a) \in \beta \wedge (y, b) \in \beta) \Rightarrow ((x, y) \in \alpha \Leftrightarrow (a, b) \in \alpha)$.

It is easy to check that condition (A6') is equivalent with condition (1), i.e. we can say that α *is extensional on* S/β. Next theorem is the key for the solution of QSP for sets with apartness.

Theorem 28.3.7 *If κ is a coequivalence on S, then the relation $\sim\kappa(= \neg\kappa)$ is an equivalence on S, and κ defines apartness on $S/\sim\kappa$.*

Proof As the reflexivity and symmetry of $\sim\kappa$ follow by Lemma 28.3.5 we prove only the transitivity. If $(x, y) \in\sim\kappa$ and $(y, z) \in\sim\kappa$, then, by the definition of $\sim\kappa$, we have that $(x, y) \bowtie \kappa$ and $(y, z) \bowtie \kappa$. For an element $(a, b) \in \kappa$, by cotransitivity of κ, we have $(a, x) \in \kappa$ or $(x, y) \in \kappa$ or $(y, z) \in \kappa$ or $(z, b) \in \kappa$. Thus $(a, x) \in \kappa$ or $(z, b) \in \kappa$, which implies that $a\#x$ or $b\#z$, i.e. $(x, z)\#(a, b)$. So $(x, z) \bowtie \kappa$ and $(x, z) \in\sim\kappa$. Therefore $\sim\kappa$ is an equivalence on S.

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

Let $a(\sim\kappa)\#b(\sim\kappa)$ and $u(\sim\kappa) \in S/\sim\kappa$. Then $(a, b) \in \kappa$, and, by the cotransitivity of κ, we have $(a, u) \in \kappa$ or $(u, b) \in \kappa$. Finally we have that $a(\sim\kappa)\#u(\sim\kappa)$ or $u(\sim\kappa)\#b(\sim\kappa)$, so the relation # is cotransitive.

The irreflexivity of # is implied by its definition and by the irreflexivity of κ. Therefore κ defines apartness on $S/\sim\kappa$.

Corollary 28.3.8 *The quotient mapping $\pi : S \to S/\sim\kappa$, defined by $\pi(x) = x(\sim\kappa)$, is an onto se-mapping.*

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

Let $a(\sim\kappa) \in S/\sim\kappa$ and $x \in a(\sim\kappa)$. Then $(a, x) \in\sim\kappa$, i.e. $a(\sim\kappa) = x(\sim\kappa)$, which implies that $a(\sim\kappa) = x(\sim\kappa) = \pi(x)$. Thus π is an onto mapping.

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

Theorem 28.3.9 *Let $f : S \to T$ be an se-mapping between sets with apartness. Then*

(i) *the relation*

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

is a coequivalence on S (which we call the ***cokernel*** *of f) which defines apartness on $S/\ker f$, and*

$$\ker f \subseteq\sim \text{coker}\, f.$$

(ii) *the mapping* $\theta : S/\ker f \to T$, *defined by* $\theta(x(\ker f)) = f(x)$, *is a one-one, a-injective se-mapping such that* $f = \theta \circ \pi$;

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

Proof (i) The consistency of 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 coker f is a coequivalence on S.

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 coker f defines an apartness on $S/\ker f$.

Now let $(x, y) \in \ker f$, so $f(x) = f(y)$. If $(u, v) \in \operatorname{coker} f$, then, by the cotransitivity of 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 consistency of coker f, either $u\#x$ or $y\#v$; whence we have $(x, y) \neq (u, v)$. Thus $(x, y) \bowtie \operatorname{coker} f$, or, equivalently $(x, y) \in \sim \operatorname{coker} f$.

(ii) Let us first prove that θ 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 θ, means that $\theta(x(\ker f)) = \theta(y(\ker f))$. Now let $\theta(x(\ker f)) = \theta(y(\ker f))$; then $f(x) = f(y)$. Hence $(x, y) \in \ker f$, which implies that $x(\ker f) = y(\ker f)$. Thus θ is one-one.

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

Let $x(\ker f)\#y(\ker f)$; that is, by (i), $(x, y) \in \operatorname{coker} f$. So we have $f(x)\#f(y)$, which, by the definition of θ means $\theta(x(\ker f))\#\theta(y(\ker f))$. Thus θ is injective. On the other hand, by the Corollary 28.3.8 and the definition of θ, for each $x \in S$ we have

$$(\theta \circ \pi)(x) = \theta(\pi(x)) = \theta(x(\ker f)) = f(x).$$

(iii) Taking into account (ii), we have to prove only that θ is onto. 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 (ii), we now have

$$y = f(x) = (\theta \circ \pi)(x) = \theta(\pi(x)) = \theta(x(\ker f)).$$

Thus θ is onto.

By Theorem 28.3.7, starting from coequivalence we have that its a-complement is an equivalence, and, furthermore, this coequivalence defines apartness on a factor set. Now we are going to look at the problem from a slightly different perspective.

Proposition 28.3.10 *Let κ be any relation on S satisfying the following:*

(i) *$\sim\kappa$ is an equivalence;*
(ii) *κ defines an apartness relation on the factor set $S/\sim\kappa$.*

Then κ is a coequivalence.

Proof By (i) and Lemma 28.3.5(i), κ is consistent. Symmetry and cotransitivity of κ is a consequence of (ii), i.e. follow immediately from the axioms of an apartness relation.

Proposition 28.3.11 *Let ε be an equivalence, and κ an coequivalence on S. Then κ defines apartness on the factor set S/ε if and only if $\varepsilon \cap \kappa = \emptyset$.*

Proof ($\Rightarrow$) Let $x, y \in S$, and assume that $(x, y) \in \varepsilon \cap \kappa$. Then $(x, y) \in \varepsilon$ and $(y, y) \in \varepsilon$, which, by extensionality of κ, i.e. (Ap6'), and $(x, y) \in \kappa$ gives $(y, y) \in \kappa$, which is impossible. Thus, $\varepsilon \cap \kappa = \emptyset$.

($\Leftarrow$) Let $x\varepsilon x'$ and $y\varepsilon y'$, and assume that $x\kappa y$. Since $\neg(x\kappa x')$ and $\neg(y\kappa y')$, we have

$$x\kappa y \;\Rightarrow\; x\kappa x' \vee x'\kappa y \;\Rightarrow\; x\kappa x' \vee x'\kappa y' \vee y'\kappa y \;\Rightarrow\; x'\kappa y',$$

which proves extensionality of κ on the factor set S/ε.

The following theorem is a generalised version of Theorem 28.3.9.

Theorem 28.3.12 *Let $f : S \to T$ be a mapping between sets with aparteness, and let ζ be a coequivalence on S such that $\zeta \cap \ker f = \emptyset$. Then:*

(i) *ζ defines apartness on factor set $S/\ker f$;*
(ii) *the projection $\pi : S \to S/\ker f$ defined by $\pi(x) = x(\ker f)$ is an onto se-mapping;*
(iii) *the mapping f induces a one-one mapping $\theta : S/\ker f \to T$ given by $\theta(x(\ker f)) = f(x)$, and $f = \theta \circ \pi$;*
(iv) *θ is an se-mapping if and only if $\operatorname{coker} f \subseteq \zeta$;*
(v) *θ is a-injective if and only if $\zeta \subseteq \operatorname{coker} f$.*

Proof (i) This was proven in Proposition 28.3.11.

(ii) The projection $\pi : S \to S/\ker f$ is onto by Corollary 28.3.8. Strong extensionality follows from consistency of ζ:

$$\pi(x)\#\pi(y) \;\Leftrightarrow\; x\zeta y \;\Rightarrow\; x\#y.$$

(iii) This was shown in Theorem 28.3.9.

(iv) Let θ be an se-mapping. Let $(x, y) \in \operatorname{coker} f$ for some $x, y \in S$. Then, by definition of $\operatorname{coker} f$ and θ, the assumption and (i), we have

$$\begin{aligned} f(x)\#f(y) &\Leftrightarrow \theta(x(\ker f))\#\theta(y(\ker f)) \\ &\Rightarrow x(\ker f)\#y(\ker f) \\ &\Leftrightarrow (x, y) \in \zeta. \end{aligned}$$

Conversely, let coker $f \subseteq \zeta$. By the assumption, (i), and definitions of θ and coker f, we have

$$\begin{aligned}\theta(x(\ker f))\#\theta(y(\ker f)) &\Leftrightarrow f(x)\#f(y)\\ &\Leftrightarrow (x,y)\in \operatorname{coker} f\\ &\Rightarrow (x,y)\in\zeta\\ &\Leftrightarrow x(\ker f)\#y(\ker f).\end{aligned}$$

(v). Let θ be a-injective, and let $(x, y) \in \zeta$. Then, by (i), we have

$$\begin{aligned}x(\ker f)\#y(\ker f) &\Rightarrow \theta(x(\ker f))\#\theta(y(\ker f))\\ &\Leftrightarrow f(x)\#f(y)\\ &\Leftrightarrow (x,y)\in \operatorname{coker} f.\end{aligned}$$

Conversely, let $\zeta \subseteq$ coker f. Then

$$\begin{aligned}x(\ker f)\#y(\ker f) &\Leftrightarrow (x,y)\in\zeta\\ &\Rightarrow (x,y)\in \operatorname{coker} f\\ &\Leftrightarrow f(x)\#f(y)\\ &\Leftrightarrow \theta(x(\ker f))\#\theta(y(\ker f)).\end{aligned}$$

Remark 28.3.13 The mapping f in the theorem above is strongly extensional if and only if coker f is consistent. By (iv), if θ is strongly extensional then coker $f \subseteq \zeta \subseteq (\#) \subseteq S \times S$, implying that f is strongly extensional as well.

Remark 28.3.14 Let $(S, \sharp)$ be set with tight apartness. Then $\sim Y = \neg Y$ for any subset Y of S.

$$x \in\sim Y \Leftrightarrow x \bowtie Y \Leftrightarrow \forall_{y\in Y}(x\sharp y) \Rightarrow \forall_{y\in Y}(\neg\,(x=y)) \Leftrightarrow \neg\,(x\in Y) \Leftrightarrow x\in\neg\,Y.$$

28.3.2 Algebraic Structures with Apartness

Principal novelty in treating basic algebraic structures constructively is that apartness becomes a fundamental notion. One axiomatizes group, rings, semigroups with apartness. Descriptive definition of a structure with apartness includes two main parts:

- the notion of certain classical algebraic structure is straightforwardly adopted;
- a structure is equipped with an apartness with standard operations which are strongly extensional.

Latest means that if S is an structure with apartness with $\circ$ as (one of) binary operation defined on S, then $\circ$ is strongly extensional if

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

If $f : S \to T$ is a homomorphism of algebraic structures with apartness, then f is

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

28.3.2.1 QSP for Groups with Tight Apartness

A *group with tight apartness* $(G, \cdot, e, \sharp)$ is a structure satisfying $(G, \cdot, e)$ is a group, $(G, \sharp)$ is a set with tight apartness and

$$\forall_{a,b,x,y \in S}\ (ax \sharp by \Rightarrow (a \sharp b \vee x \sharp y)),$$

$$\forall_{x,y \in S}\ (x^{-1} \sharp y^{-1} \Rightarrow x \sharp y)).$$

Remark 28.3.15 Consider the real numbers $\mathbb{R}$, we cannot assume that x^{-1} exists unless we know that x is apart from zero, i.e. that $\mid x \mid > 0$. Constructively, that is not the same thing as $x \neq 0$. ([3])

In **CLASS** (see Sect. 28.2.2.1), it is possible to construct from a group G and a normal subgroup N a quotient group G/N. This may not work in **BISH** because we may loose apartness on the quotient group–quotient group does not in general have a natural apartness relation. For most purposes we overcome this problem using a cogroup instead of an subgroup. A subset C of a group G is a *cogroup* of G if
$\neg(e \in C)$,
$xy \in C \Rightarrow x \in C \vee y \in C$,
$x^{-1} \in C \Rightarrow x \in C$.
C is *a normal cogroup* if it satisfies one of the following three conditions:
$xy \in C \Rightarrow yx \in C$,
$x \in C \Rightarrow yxy^{-1} \in C$,
$yxy^{-1} \in C \Rightarrow x \in C$,
for any $x, y \in C$.

Cogroup C is *compatible with apartness* if
$x \in C \Rightarrow x \sharp e$.

Each group with tight apartness satisfy

$$x \sharp y \Leftrightarrow xy^{-1} \sharp e.$$

We are going to use this without special announcement.

Existing properties of a normal cogroup guarantees its logical complement be an normal subgroup as well as the quotient group of that normal subgroup will inherit a tight apartness.

Theorem 28.3.16 *Let C be a normal cogroup of a group G with tight apartness, then $\neg\, C$ is a normal subgroup of G and $(G/\neg\, C,\ \sharp)$ is a quotient group with tight apartness defined by*

$$x(\neg\, C) \sharp\, y(\neg\, C) \text{ iff } \mathrm{xy}^{-1} \in \mathrm{C}.$$

The quotient map $\pi : G \to G/(\neg\, C),\ \pi(x) = x(\neg\, C)$ is an onto *se-homomorphism.*

Proof Let us, first, check the properties of tight apartness.

(Ap1) Let $\neg\,(x(\neg\, C) \sharp\, x(\neg\, C))$. By the definition of apartness, $\neg\,(xx^{-1} \in C)$, i.e. $\neg\, e \in C$. So consistency is proved.

(Ap2) Symmetry is obvious.

(Ap3) Cotransitivity:

$$\begin{aligned} x(\neg\, C) \sharp\, y(\neg\, C) &\Leftrightarrow xy^{-1} \in C \\ &\Leftrightarrow (xz^{-1})(zy^{-1}) \in C \\ &\Rightarrow xz^{-1} \in C \ \vee\ zy^{-1} \in C \\ &\Leftrightarrow x(\neg\, C) \sharp\, z(\neg\, C) \ \vee\ z(\neg\, C) \sharp\, y(\neg\, C). \end{aligned}$$

(Ap4) Tightness:

$$\begin{aligned} \neg\,(x(\neg\, C) \sharp\, y(\neg\, C)) &\Leftrightarrow \neg\,(xy^{-1} \in C) \\ &\Leftrightarrow xy^{-1} \in (\neg\, C) \\ &\Leftrightarrow\ x(\neg\, C) = y(\neg\, C). \end{aligned}$$

Now, we will prove that standard operations are strongly extensional.

$$\begin{aligned} xa(\neg\, C) \sharp\, yb(\neg\, C) &\Leftrightarrow a^{-1}x^{-1}yb \in C \\ &\Rightarrow x^{-1}yba^{-1} \in C \\ &\Rightarrow x^{-1}y \in C \ \vee\ ba^{-1} \in C \\ &\Leftrightarrow x(\neg\, C) \sharp\, y(\neg\, C) \ \vee\ a(\neg\, C) \sharp\, b(\neg\, C). \end{aligned}$$

$$\begin{aligned} x^{-1}(\neg\, C) \sharp\, y^{-1}(\neg\, C) &\Leftrightarrow x^{-1}y \in C \\ &\Leftrightarrow x(\neg\, C) \sharp\, y(\neg\, C). \end{aligned}$$

Finally, let us show that π is an se-mapping.

$$\begin{aligned}\pi(x) \sharp \pi(y) &\Leftrightarrow x(\neg C) \sharp y(\neg C)\\ &\Leftrightarrow xy^{-1} \in C\\ &\Leftrightarrow xy^{-1} \sharp e\\ &\Leftrightarrow x \sharp y.\end{aligned}$$

The Tight apartness isomorphism theorem follows next.

Theorem 28.3.17 *Let $f : G \to H$ be an se-homomorphism between groups with tight apartness. Then*

(i) *$C_f = \{x \in G : f(x) \sharp e_H\}$ ia a normal cogroup of G.*
(ii) *Mapping $\theta : G/(\neg C_f) \to H$, $\theta(x(\neg C_f)) = f(x)$, is an apartness embedding such that $\theta \circ \pi = f$.*

Proof (i) We will prove properties of normal cogroup.

- As $f(e_G) = e_H$, then $e_G \notin G_f$.
- Let $xy \in C_f$. Then

$$\begin{aligned}xy \in C_f &\Leftrightarrow f(xy) \sharp e_H\\ &\Leftrightarrow f(x)f(y) \sharp e_H\\ &\Rightarrow f(x) \sharp e_H \ \vee \ f(y) \sharp e_H\\ &\Leftrightarrow x \in C_f \ \vee \ y \in C_f.\end{aligned}$$

- Let $x^{-1} \in C_f$. Then

$$\begin{aligned}x^{-1} \in C_f &\Leftrightarrow f(x^{-1}) \sharp e_H\\ &\Leftrightarrow (f(x))^{-1} \sharp e_H\\ &\Leftrightarrow x \in C_f.\end{aligned}$$

- If $xy \in C_f$, then $yx \in C_f$ can be proved in a similar manner as above.

(ii) By Theorem 28.3.16, $G/(\neg C_f)$ is a factor group with tight apartness with $\pi : G \to G/(\neg C_f)$ onto se-homomorphism.

Let us prove that $\theta : G/(\neg C_f) \to H$ is an se-homomorphism.

$$\begin{aligned}\theta(x(\neg C_f)) \sharp \theta(y(\neg C_f)) &\Leftrightarrow f(x) \sharp f(y)\\ &\Rightarrow x(\neg C_f)\# y(\neg C_f).\end{aligned}$$

Finally, in order to prove apartness embeddability, we have to prove a-injectivity of θ.

$$\begin{aligned} x(\neg C_f) \sharp y(\neg C_f) &\Leftrightarrow xy^{-1} \in C_f \\ &\Leftrightarrow f(xy^{-1}) \sharp e_H \\ &\Leftrightarrow f(x)(f(y))^{-1} \sharp e_H \\ &\Leftrightarrow f(x) \sharp f(y) \\ &\Leftrightarrow \theta(x(\neg C_f)) \sharp \theta(y(\neg C_f)). \end{aligned}$$

.

Remark 28.3.18 Cogroup is a term used in [3, 35], while in [37] term antisubgroup is used instead.

28.3.2.2 QSP for Commutative Rings with Tight Apartness

As it is written in [37], for demonstration of the solution of QSP commutative rings with unity and a tight apartness relation do very well.

Commutative rings with unity and a tight apartness $(R, \sharp, +, \cdot, -, 0, 1)$ is a structure satisfying $(R, +, \cdot, -, 0, 1)$ is a commutative ring with unity, $(R, \sharp)$ is a set with tight apartness and

$a + x \sharp b + y \Rightarrow (a \sharp b \vee x \sharp y)$,
$ax \sharp by \Rightarrow (a \sharp b \vee x \sharp y)$,
$0 \sharp 1$.

Lemma 28.3.19 *Let R be a ring with tight apartness and let x, y be any two its elements. Then the following is true:*

(i) $x + y \sharp 0 \;\Rightarrow\; x \sharp 0 \;\vee\; y \sharp 0$;
(ii) $xy \sharp 0 \;\Rightarrow\; x \sharp 0 \;\wedge\; y \sharp 0$;
(iii) $x + z \sharp y + z \;\Rightarrow\; x \sharp y$.

Proof (i) Follows immediately from the strong extensionality of $+$.

(ii) If the strong extensionality of the multiplication is applied to $xy \sharp x0$ and to $xy \sharp 0y$ then we have required.

(iii) Follows immediately from the strong extensionality of $+$.

In what follows the previous lemma will be used without special announcement.

Similarly as in Sect. 28.3.2.1, the Tight apartness isomorphism theorem for groups can be "translated" for rings with normal cogroups and groups replaced by coideals and rings respectively. Coideals are the tools for introducing an apartness relation on quotient ring (see Sect. 28.2.2.2). A subset C of a ring R is a *coideal* of R if

$0 \notin C$,
$x + y \in C \;\Rightarrow\; x \in C \;\vee\; y \in C$,
$xy \in C \;\Rightarrow\; x \in C \;\wedge\; y \in C$.

Remark 28.3.20 The definition of a coideal allows $\emptyset$ to be a coideal. Inhabited coideals are characterized by the fact that 1 belongs to them. If $a \in C$ then, by the definition of coideal, $a = a1$ implies $1 \in C$.

Existing properties of a coideal guarantees its a-complement be an ideal as well as the quotient ring of that ideal will inherit a tight apartness.

Theorem 28.3.21 *Let R be a ring with tight apartness and let C be a subset of R.*

(i) *If C is a coideal, then $\neg C$ is an ideal, and $\neg C$ is proper if C is inhabited.*
(ii) *If C an inhabited coideal, then $R/(\neg C)$ is a ring with tight apartness given by $a + (\neg C) \sharp b + (\neg C)$* iff a − b ∈ C.
(iii) *The quotient map $\pi : R \to R/(\neg C)$, $\pi(x) = x(\neg C)$ is an* onto *se-homomorphism.*

Proof (i) Routine.

(ii) and (iii) Proof is similar to those in Theorem 28.3.16.

The solution of QSP for rings, the *Tight apartness isomorphism theorem*, follows next.

Theorem 28.3.22 *Let $f : R \to S$ an se-homomorphism between commutative rings with tight apartness, then*

$$C_f = \{x \in R : f(x) \sharp 0\}$$

is an inhabited coideal. There is a unique apartness embedding $\theta : R/(\neg C_f) \to S$ such that $\theta \circ \pi = f$.

Proof It is obvious that $1 \in C_f$. Let us prove C_f ia a coideal of R.

Let $x \in C_f$. Then $f(x) \sharp 0$ and, as f is an se-homomorphism, we have $x \sharp 0$, i.e. $0 \notin C_f$. Let $x + y \in C_f$. Then

$$\begin{aligned} x + y \in C_f &\Leftrightarrow f(x + y) \sharp 0 \\ &\Leftrightarrow f(x) + f(y) \sharp 0 \\ &\Rightarrow f(x) \sharp 0 \ \vee \ f(y) \sharp 0 \\ &\Leftrightarrow x \in C_f \ \vee \ y \in C_f. \end{aligned}$$

Let $xy \in C_f$. Then

$$\begin{aligned} xy \in C_f &\Leftrightarrow f(xy) \sharp 0 \\ &\Leftrightarrow f(x)f(y) \sharp 0 \\ &\Rightarrow f(x) \sharp 0 \ \wedge \ f(y) \sharp 0 \\ &\Leftrightarrow x \in C_f \ \wedge \ y \in C_f. \end{aligned}$$

Thus C_f is a coideal of R. Let $-a \in C_f$ for some $a \in R$. Then $f(-a) \sharp 0$, i.e. $-f(a) \sharp 0$, which implies $f(a) \sharp 0$. So $a \in C_f$.

By Theorem 28.3.21, $\neg C_f$ is an ideal of R, and a factor ring $R/(\neg C_f)$ is a ring with tight apartness inherited from R. The rest of the proof is similar to the one of the Theorem 28.3.17 for the group case.

Remark 28.3.23 Coideal is a term used in [3, 34, 35], while in [37] term anti-ideal is used instead.

28.3.2.3 QSP for Semigroups with Apartness

Results of several years of investigation, presented in [13, 14], present 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. Some of them will be listed in the remaining part of this section. In some sense they are consequence of the ones presented in Sect. 28.3.1.

We define the notion of a semigroup in a constructive way. A tuple $(S, =, \#, \cdot)$ is a *semigroup with apartness* with $(S, =, \#)$ as a set with apartness, $\cdot$ a binary operation on S which is associative

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

and strongly extensional

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

As usual, we are going to write ab instead of $a \cdot b$. Hereinafter we will consider only semigroups with apartness, calling them, in short, semigroups, and denoting them by S. First thing which has to be done is to give an evidence that such ones—with apartness which is not tight—do exist.

Theorem 28.3.24 *Let $(A, =, \#)$ be a set with apartness, and let $f : A \to A$ be an se-mapping. If S is a set of all se-functions from A to A, and $\circ$ composition of functions, then $(S, =, \#, \circ)$ with*

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

and

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

is a semigroup with apartness.

Proof By Theorem 28.3.2 $(S, =, \#)$ is a set with apartness. Let $f, g \in S$ and suppose that $(f \circ g)(x) \# (f \circ g)(y)$ for some $x, y \in A$. Then, by the definition of the composition, $f(g(x)) \# f(g(y))$, and, as f is an se-mapping, we have $g(x) \# g(y)$. Finally, as g is an se-mapping as well, we have $x \# y$. Thus, $f \circ g$ is an se-mapping and $f \circ g \in S$. As in the classical case, composition of functions is associative, [4], so $(S, \circ)$ is a semigroup.

Let $f, g, h, w \in S$ and $f \circ h \# g \circ w$. Then, by the definition of apartness in S, there is an element $x \in A$ such that $(f \circ h)(x) \# (g \circ w)(x)$, i.e. $f(h(x)) \# g(w(x))$. Now we have

$$f(h(x))\#f(w(x)) \vee f(w(x))\#g(w(x)),$$

which, further, implies $h(x)\#w(x)$ (because f is an se-mapping) or $f\#g$ (by the definition of the apartness relation on S). Thus $f\#g \vee h\#w$, that is, composition $\circ$ is an se-operation and $(S, =, \#, \circ)$ is a semigroup with apartness.

Apartness from the previous theorem does not have to be tight. It is well known that if the standard apartness on the additive semigroup $\mathbb{R}$ is tight, then we can prove the constructively questionable **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 $a_n = 1$.

The following example shows that we cannot prove constructively that the apartness on every *finite* semigroup is tight.

Example 28.3.25 Let $A = \{0, 1, 2\}$ with the usual equality relation—that is, the diagonal Δ_A of $A \times A$. Let

$$K = \Delta_A \cup \{(1, 2), (2, 1)\},$$

and define an apartness # on A by

$$x\#y \Leftrightarrow (x, y) \notin K.$$

Then, as we observed above (Theorem 28.3.24), $S = A^A$ becomes a semigroup with apartness in a standard way. Define mappings $f, g : A \to A$ by

$$f(0) = 1,\ f(1) = 1,\ f(2) = 2,$$
$$g(0) = 2,\ g(1) = 1,\ g(2) = 2.$$

In view of our definition of the apartness on A, there is no element x of A with $f(x)\#g(x)$; so, in particular, f and g are se-functions. However, if $f = g$, then $1 = 2$, which, by our definition of the equality on A, is not the case. Hence the apartness on S is not tight. $\diamond$

Corollary 28.3.26 *Every semigroup with apartness embeds into the semigroup of all strongly extensional self-maps on a set.*

Proof Let $(S, =, \#, \cdot)$ be a semigroup with apartness. The semigroup S embeds into the monoid with apartness $S^1 = (S \cup \{1\}, =_1, \#_1, \cdot)$ with equality $=_1$ which consists of all pairs in $=$ and the pair $(1, 1)$, and with apartness $\#_1$ which consists of all pairs in # and the pairs $(a, 1)$, $(1, a)$ for each $a \in S$.

Let f_a be a left translation of S^1, i.e. $f_a(x) = a \cdot x$, for all $x \in S^1$. Then f_a is an se-function. Indeed, $f_a(x)\#_1 f_a(y)$ is equivalent to $ax\#_1 ay$. The strong extensionality of multiplication implies $x\#_1 y$.

Denote by T the set of all se-functions from S^1 to S^1. As in **CLASS**, define a mapping $\varphi\colon S^1 \longrightarrow T$ letting

$$\varphi(a) = f_a,$$

for each $a \in S^1$. It is routine to verify that

$$\varphi(ab) = f_{ab} = f_a \circ f_b = \varphi(a)\varphi(b),$$

as well as

$$\varphi(a)\#_T\varphi(b) \;\Rightarrow\; a\#_1 b.$$

Thus, φ is an se-homomorphism. Also, $\varphi(a) =_T \varphi(b)$ iff $ax =_1 bx$ for all $x \in S^1$, and, for $x = 1$, we have $a =_1 b$. Therefore, φ is an embedding.

Let us remember that in **CLASS** the compatibility property is an important condition for providing the semigroup structure on quotient sets. Now we are looking for the tools for introducing apartness relation on a factor semigroup. Our starting point are the results from the Sect. 28.3.1, as well as the next definition. A coequivalence $\boldsymbol{\kappa}$ is *cocongruence* if it is *cocompatible*, i.e.

$$\forall_{a,b,x,y\in S}\,((ax, by) \in \kappa \;\Rightarrow\; (a, b) \in \kappa \vee (x, y) \in \kappa)$$

Theorem 28.3.27 *If κ is a cocongruence on S, then the relation $\sim\kappa(= \neg\kappa)$ is an congruence on S, and κ defines apartness on $S/\sim\kappa$.*

Proof By Theorem 28.3.7, $\sim\kappa$ is an equivalence on S such that κ defines apartness on $S/\sim\kappa$. If $(a, b), (x, y) \in\sim\kappa$ then for any $(u, v) \in \kappa$ we have both $(a, b)\#(u, v)$ and $(x, y)\#(u, v)$. Now, we also have $(u, ax) \in \kappa$ or $(ax, by) \in \kappa$ or $(by, v) \in \kappa$. If $(ax, by) \in \kappa$, then by the cocompatibility of κ, either $(a, b) \in \kappa$ or $(x, y) \in \kappa$, which is impossible. Thus $(u, ax) \in \kappa$ or $(by, v) \in \kappa$; so either $u\#ax$ or $by\#v$, and therefore $(ax, by)\#(u, v)$. Hence $(ax, by) \bowtie \kappa$. Thus $(ax, by) \in\sim\kappa$, and $\sim\kappa$ is a congruence on S.

Let $a(\sim\kappa)x(\sim\kappa) \neq b(\sim\kappa)y(\sim\kappa)$; then $(ax)(\sim\kappa)\#(by)(\sim\kappa)$. By Theorem 28.3.7, we have that $(ax, by) \in \kappa$. But κ is a cocongruence, so either $(a, b) \in \kappa$ or $(x, y) \in \kappa$. Thus, by the definition of # in $S/\sim\kappa$, either $a(\sim\kappa)\#b(\sim\kappa)$ or $x(\sim\kappa)\#y(\sim\kappa)$. So $(S/\sim\kappa, =, \#, \cdot)$ is a semigroup with apartness.

Corollary 28.3.28 *The quotient mapping $\pi : S \to S/\sim\kappa$, defined by $\pi(x) = x(\sim\kappa)$, is an onto se-homomorphism.*

Proof By Corollary 28.3.8 π is an onto se-mapping. By the previous theorem and the assumption we have

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

Hence π is a homomorphism.

The Apartness isomorphism theorem for semigroups follows.

Theorem 28.3.29 *Let $f : S \to T$ be an se-homomorphism between semigroups with apartness. Then:*

(i) coker f *is a cocongruence on* S *which defines apartness on* $S/\ker f$*, and*

$$\ker f \subseteq \sim \operatorname{coker} f.$$

(ii) *the mapping* $\theta : S/\ker f \to T$*, defined by* $\theta(x(\ker f)) = f(x)$*, is an apartness embedding such that* $f = \theta \circ \pi$*; and*

(iii) *if* f *maps* S *onto* T*, then* θ *is an apartness isomorphism.*

Proof (i) Taking into account Theorems 28.3.9 and 28.3.27, it is enough to prove that coker f is cocompatible with multiplication in S. Let $(ax, by) \in$ 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 $(a, b) \in$ coker f or $(x, y) \in$ coker f, and therefore coker f is a cocongruence on S.

(ii) Using Theorem 28.3.27 and the assumption that f is a homomorphism, we have

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

By Theorem 28.3.9, θ is a one-one, a-injective se-homomorphism—that is, an apartness embedding.

(iii) This follows by Theorem 28.3.9 and (ii).

As a consequence of the Theorem 28.3.12 we have the following generalization of the Theorem 28.3.29.

Theorem 28.3.30 *Let $f : S \to T$ be a mapping between sets with aparteness, and let ζ be a coequivalence on S such that $\zeta \cap \ker f = \emptyset$. If S is semigroup with apartness and ζ a cocongruence, then $S/ker\ f$ is a semigroup with apartness, and π an se-homomorphism. If, in addition, T is a semigroup with apartness and f an se-homomorphism, then θ is also an se-homomorphism.*

28.4 Conclusion Remarks

Although the title of this paper suggest that (certain topics like, for example, isomorphism theorems, of) basic constructive algebraic structures are in the center of consideration, we brought to speak of two points of view on a given subject: classical and constructive. The classical point of view presented in the Sect. 28.2 is introductional part of almost all (classical) abstract algebra books. The contents presented throughout that section have useful role as intuition guides and to at least link with the presentations given in the Sect. 28.3 written in the style of classical mathematics. So far we have considered basic structures—groups, rings, semigroups—in classical setting; in an intuitionistic one, however, it is appropriate to consider them with an extra structure—apartness. A groups, rings, semigroups with apartness satisfies a number of extra conditions. In the first place the well known axioms of apartness. In the second place the operations have to be strongly extensional.

Following [33], **BISH** (constructive mathematics in general) is not the study of constructive things it is a constructive study of things. In constructive proofs of (some) classical theorems only constructive methods are used. More generally, constructive theorem is a theorem with a constructive proof. Although it might looks like familiar one from classical case it is often with more complicated hypothesis and proof. One of the main aims of this paper is to give a constructive treatment of well-known classical isomorphism theorems for basic classical algebraic structures. Comparing Theorems 28.2.2 and 28.3.9 for set and set with apartness; Theorems 28.2.7 and 28.3.17 for group and group with tight apartness; Theorems 28.2.12 and 28.3.22 for ring and ring with tight apartness; Theorems 28.2.15 and 28.3.29 for semigroup and semigroup with apartness, we can notice that Theorems 28.3.9, 28.3.17, 28.3.22 and 28.3.29 are with more complicated hypothesis. On the other hands comparing proofs of Theorems 28.2.2 and 28.3.9 as well as of Theorems 28.2.15 and 28.3.29 we can notice that constructive versions Theorems 28.3.9 and 28.3.29 are with more complicated ones.

The constructive results presented in Sect. 28.3 do not follow their historical appearance. Results on groups and rings with tight apartness are from 80s of the last century, [34, 35, 37]; while the ones on set and semigroups of apartness are newcomers, [13, 14, 31]. As it is pointed in Remark 28.3.14, for algebraic structures with tight apartness we have only one complement of a given subset. On contrary, for algebraic structures with apartness complement is a proper subset of a logical one, Example 28.3.4. Obtained solutions of QSP for groups and rings with tight apartness, Theorems 28.3.17 and 28.3.22, put a complements of a certain subsets (cogroups or coideals) in the central position. Getting inspiration from these cases, in solving QSP for sets and semigroups with apartness the distinguishing subsets for which two complements coincide is first to be done. Of course, appropriate developed order theory for these structures is needful as well.

Why to study basic constructive algebraic structures with apartness? Instead put some answer(s) let us give some examples of applications of ideas presented in the previous section. We will start with constructive analysis. Proof of one of the direction of constructive version of the Spectral Mapping Theorem is based on some elementary constructive semigroups with inequality techniques, [8]. Worth to be mentioned are applications of commutative basic algebraic structures with tight apartness within automated reasoning area, [11, 15]. For possible applications within computational linguistic see [32]. Some topics from mathematical economics can be approached constructively too (using some order theory for sets with apartness), [1]. The study of basic constructive algebraic structures with apartness as well as constructive algebra as a whole can have an effect on development of other areas of constructive mathematics. On the other hand, it can make both proof engineering and programming more flexible.

At the very end we can say that our experience of doing constructive algebra suggests that we are dealing with "normal" mathematical objects, and we are working only with intuitionistic logic. Why (we choose to do constructive algebra "on the odd day")? Because it is interesting in its own right, and, what is more important, it can be fun and challenging.

Acknowledgements Melanija Mitrović is financially supported by the Ministry of Education, Science and Technological Development of the Republic of Serbia, Grant 174026, and by the Faculty of Mechanical Engineering, University of Niš, Serbia, Grant "Research and development of new generation machine systems in the function of the technological development of Serbia". Melanija Mitrovicć is grateful to Mathematics and Applied Mathematics Research Environment MAM, Division of Applied Mathematics at the School of Education, Culture and Communication at Mälardalen University for cordial hospitality and excellent environment for research and cooperation during her visit.

References

1. Baroni, M., Bridges, D.S.: Continuity properties of preference relations. Math. Log. Q. **54**(5), 454–459 (2008)
2. Bauer, A.: Five stages of accepting constructive mathematics. Bull. (New Ser.) Am. Math. Soc. vol. 54(3), 481–498 (2017)
3. Beeson, M.J.: Foundations of Constructive Mathematics. Springer, Berlin (1985)
4. Bishop, E.: Foundations of Constructive Analysis. McGraw-Hill, New York (1967)
5. Bishop, E., Bridges, D.S.: Constructive Analysis, Grundlehren der mathematischen Wissenschaften 279. Springer, Berlin (1985)
6. Bridges, D.S., Richman, F.: Varieties of Constructive Mathematics. London Mathematical Society Lecture Notes, vol. 97. Cambridge University Press, Cambridge (1987)
7. Bridges, D.S., Reeves, S.: Constructive mathematics in theory and programming practice. Philos. Math. **7**(3), 63–104 (1999)
8. Bridges, D.S., Havea, R.: A constructive version of the spectral mapping theorem. Math. Log. Q. **47**(3), 299–304 (2001)
9. Bridges, D.S., Vîta, L.S.: Techniques in Constructive Analysis. Universitext. Springer, Berlin (2006)
10. Bridges, D.S., Vîta, L.S.: Apartness and Uniformity - A Constructive Development. CiE Series on Theory and Applications of Computability. Springer, Berlin (2011)
11. Calderón, G.: Formalizing constructive projective geometry in Agda. Electronic Notes in Theoretical Computer Science, **338**, 61–77 (2018)
12. Clark, A.: Elements of Abstract Algebra, p. 1984. Dover Publications, Inc., New York (1974)
13. Crvenković, S., Mitrović, M., Romano, D.A.: Semigroups with apartness. Math. Log. Q. **59**(6), 407–414 (2013)
14. Crvenković, S., Mitrović, M., Romano, D.A.: Basic otions of (constructive) semigroups with apartness. Semigroup Forum **92**(3), 659–674 (2016)
15. Geuvers, H., Pollack, R., Wiedijk, F., Zwanenburg, J.: A constructive algebraic hierarchy in coq. J. Symb. Comput. **34**, 271–286 (2002)

16. Gunther, E., Gadea, A., Pagano, M.: Formalization of universal algebra in Agda. Electronic Notes in Theoretical Computer Science, **338**, 147–166 (2018)
17. Herstein, I.N.: Topics in Algebra, 2nd edn. Wiley, New Jersey (1975)
18. Heyting, A.: Intuitionistische axiomatick der projectieve meetkunde. Thesis, P. Noordhoof (1925)
19. Heyting, A.: Zur intuitionistischen Axiomatik der projektiven Geometrie. Math. Ann. **98**, 491–538 (1927)
20. Heyting, A.: Untersuchungen über intuitionistische Algebra. Nederl. Akad. Wetensch. Verh. Tweede Afd. Nat. **18**(2) (1941)
21. Heyting, A.: Intuitionism, an Introduction. North-Holland (1956)
22. Hollings, C.: Mathematics Across the Iron Curtain: A History of the Algebraic Theory of Semigroups. American Mathematical Society, Providence (2014)
23. Howie, J.M.: Why Study Semigroups? Lecture given to the New Zealand Mathematical Colloquium (1986)
24. Howie, J.M.: Fundamentals of Semigroup Theory. London Mathematical Society Monographs, New Series. Clarendon Press, Oxford (1995)
25. Hungerford, T.W.: Algebra. Springer, Berlin (2003). (Twelfth printing)
26. Ishihara, H., Palmgren, E.: Quotient topologies in constructive set theory and type theory. Ann. Pure Appl. Log. **141**, 257–265 (2006)
27. Jacobs, B.: Bisimulation and Apartness in Coalgebraic Specification; 1995 - Notes of Lectures Given in January 1995 at the Joint TYPES/CLICS Workshop in Gothenburg and BRICS Seminar in Aarhus
28. Martin-Löf, P.: Constructive mathematics and computer programming. In: Kohen, L.J., Los, J., Pfeiffer, H., Podewski, K.-P. (eds.) The Proceedings of the Sixth International Congress of Logic. Methodology and Philosophy of Science, pp. 153–175. North-Holland Publishing Company, Amsterdam (1982)
29. Mines, R., Richman, F., Ruitenburg, W.: A Course of Constructive Algebra. Springer, New York (1988)
30. Mitrović, M.: Semilattices of Archimedean Semigroups. University of Niš - Faculty of Mechanical Engineering, Niš (2003)
31. Mitrović, M., Darpö, E.: Apartness complements of Subsets of Constructive Sets and Semigroups with Apartness, (in preparation)
32. Moshier, M.A.: A rational reconstruction of the domain of feature structures. J. Log., Lang. Inf. **4**(2), 111–143 (1995)
33. Richman, F.: Interview with a constructive mathematician. Mod. Log. **6**, 247–271 (1996)
34. Romano, D.A.: Rings and fields, a constructive view. Math. Log. Q. (Formerly: Z. Math. Logik Grundl. Math.) **34**(1) 25–40 (1988)
35. Ruitenburg, W.B.G.: Intuitionistic Algebra, Theory and Sheaf Models, Ph.D. (1982)
36. Ruitenburg, W.: Inequality in constructive mathematics. Notre Dame J. Form. Log. **32**, 533–553 (1991)
37. Troelstra, A.S., van Dalen, D.: Constructivism in Mathematics, An Introduction, (Two volumes). North-Holland, Amsterdam (1988)