JOURNAL OF FORMALIZED MATHEMATICS
Volume 4, Released 1992, Published 2003
Inst. of Computer Science, Univ. of Białystok

Monoids

Grzegorz Bancerek
Polish Academy of Sciences
Institute of Mathematics
Warsaw

Summary. The goal of the article is to define the concept of monoid. In the preliminary section we introduce the notion of some properties of binary operations. The second section is concerning with structures with a set and a binary operation on this set: there is introduced the notion corresponding to the notion of some properties of binary operations and there are shown some useful clusters. Next, we are concerning with the structure with a set, a binary operation on the set and with an element of the set. Such a structure is called monoid iff the operation is associative and the element is a unity of the operation. In the fourth section the concept of subsystems of monoid (group) is introduced. Subsystems are submonoids (subgroups) or other parts of monoid (group) with are closed w.r.t. the operation. There are presented facts on inheritness of some properties by subsystems. Finally, there are constructed the examples of groups and monoids: the group $\rangle \mathbb{R}, + \langle$ of real numbers with addition, the group $\mathbb{Z}^+$ of integers as the subsystem of the group $\rangle \mathbb{R}, + \langle$, the semigroup $\rangle \mathbb{N}, + \langle$ of natural numbers as the subsystem of $\mathbb{Z}^+$, and the monoid $\rangle \mathbb{N}, +, 0 \langle$ of natural numbers with addition and zero as monoidal extension of the semigroup $\rangle \mathbb{N}, + \langle$. The semigroups of real and natural numbers with multiplication are also introduced. The monoid of finite sequences over some set with concatenation as binary operation and with empty sequence as neutral element is defined in sixth section. Last section deals with monoids with the composition of functions as the operation, i.e. with the monoid of partial and total functions and the monoid of permutations.

MML Identifier: `MONOID_0`.

WWW: `http://mizar.org/JFM/Vol4/monoid_0.html`

The articles [16], [7], [21], [18], [10], [17], [1], [22], [8], [4], [2], [23], [6], [5], [3], [9], [19], [11], [12], [15], [14], [20], and [13] provide the notation and terminology for this paper.

1. Binary operations preliminary

In this paper x, X, Y are sets.

Let G be a 1-sorted structure. A binary operation on G is a binary operation on the carrier of G.

Let I_1 be a 1-sorted structure. We say that I_1 is constituted functions if and only if:

(Def. 1) Every element of I_1 is a function.

We say that I_1 is constituted finite sequences if and only if:

(Def. 2) Every element of I_1 is a finite sequence.

Let us observe that there exists a 1-sorted structure which is constituted functions and there exists a 1-sorted structure which is constituted finite sequences.

Let X be a constituted functions 1-sorted structure. Observe that every element of X is function-like and relation-like.

Let us note that every 1-sorted structure which is constituted finite sequences is also constituted functions.

Let us mention that every groupoid which is constituted finite sequences is also constituted functions.

Let X be a constituted finite sequences 1-sorted structure. One can verify that every element of X is finite sequence-like.

Let D be a set and let p, q be finite sequences of elements of D. Then $p \frown q$ is an element of D^*.

Let g, f be functions. We introduce $f \circ g$ as a synonym of $f \cdot g$.

Let X be a set and let g, f be functions from X into X. Then $f \cdot g$ is a function from X into X.

Let X be a set and let g, f be permutations of X. Then $f \cdot g$ is a permutation of X.

Let D be a non empty set and let I_1 be a binary operation on D. We say that I_1 is left invertible if and only if:

(Def. 3) For all elements a, b of D there exists an element l of D such that $I_1(l, a) = b$.

We say that I_1 is right invertible if and only if:

(Def. 4) For all elements a, b of D there exists an element r of D such that $I_1(a, r) = b$.

We say that I_1 is invertible if and only if:

(Def. 5) For all elements a, b of D there exist elements r, l of D such that $I_1(a, r) = b$ and $I_1(l, a) = b$.

We say that I_1 is left cancelable if and only if:

(Def. 6) For all elements a, b, c of D such that $I_1(a, b) = I_1(a, c)$ holds $b = c$.

We say that I_1 is right cancelable if and only if:

(Def. 7) For all elements a, b, c of D such that $I_1(b, a) = I_1(c, a)$ holds $b = c$.

We say that I_1 is cancelable if and only if:

(Def. 8) For all elements a, b, c of D such that $I_1(a, b) = I_1(a, c)$ or $I_1(b, a) = I_1(c, a)$ holds $b = c$.

We say that I_1 has uniquely decomposable unity if and only if:

(Def. 9) I_1 has a unity and for all elements a, b of D such that $I_1(a, b) = \mathbf{1}_{(I_1)}$ holds $a = b$ and $b = \mathbf{1}_{(I_1)}$.

We now state three propositions:

(1) Let D be a non empty set and f be a binary operation on D. Then f is invertible if and only if f is left invertible and right invertible.

(2) Let D be a non empty set and f be a binary operation on D. Then f is cancelable if and only if f is left cancelable and right cancelable.

(3) Let f be a binary operation on $\{x\}$. Then

(i) $f = \{\langle x, x\rangle\} \longmapsto x$, and

(ii) f is commutative, associative, idempotent, invertible, and cancelable and has a unity and uniquely decomposable unity.

2. SEMIGROUPS

We adopt the following convention: G denotes a non empty groupoid, D denotes a non empty set, and a, b, c, r, l denote elements of G.

Let I_1 be a non empty groupoid. Let us observe that I_1 is unital if and only if:

(Def. 10) The multiplication of I_1 has a unity.

Let us consider G. Let us observe that G is commutative if and only if:

(Def. 11) The multiplication of G is commutative.

Let us observe that G is associative if and only if:

(Def. 12) The multiplication of G is associative.

Let I_1 be a non empty groupoid. We say that I_1 is idempotent if and only if:

(Def. 13) The multiplication of I_1 is idempotent.

We say that I_1 is left invertible if and only if:

(Def. 14) The multiplication of I_1 is left invertible.

We say that I_1 is right invertible if and only if:

(Def. 15) The multiplication of I_1 is right invertible.

We say that I_1 is invertible if and only if:

(Def. 16) The multiplication of I_1 is invertible.

We say that I_1 is left cancelable if and only if:

(Def. 17) The multiplication of I_1 is left cancelable.

We say that I_1 is right cancelable if and only if:

(Def. 18) The multiplication of I_1 is right cancelable.

We say that I_1 is cancelable if and only if:

(Def. 19) The multiplication of I_1 is cancelable.

We say that I_1 has uniquely decomposable unity if and only if:

(Def. 20) The multiplication of I_1 has uniquely decomposable unity.

Let us observe that there exists a non empty groupoid which is unital, commutative, associative, cancelable, idempotent, invertible, constituted functions, constituted finite sequences, and strict and has uniquely decomposable unity.

One can prove the following propositions:

(4) If G is unital, then $\mathbf{1}_{\text{the multiplication of } G}$ is a unity w.r.t. the multiplication of G.

(5) G is unital iff for every a holds $\mathbf{1}_{\text{the multiplication of } G} \cdot a = a$ and $a \cdot \mathbf{1}_{\text{the multiplication of } G} = a$.

(6) G is unital iff there exists a such that for every b holds $a \cdot b = b$ and $b \cdot a = b$.

(9)[1] G is idempotent iff for every a holds $a \cdot a = a$.

(10) G is left invertible iff for all a, b there exists l such that $l \cdot a = b$.

(11) G is right invertible iff for all a, b there exists r such that $a \cdot r = b$.

[1] The propositions (7) and (8) have been removed.

(12) G is invertible iff for all a, b there exist r, l such that $a \cdot r = b$ and $l \cdot a = b$.

(13) G is left cancelable iff for all a, b, c such that $a \cdot b = a \cdot c$ holds $b = c$.

(14) G is right cancelable iff for all a, b, c such that $b \cdot a = c \cdot a$ holds $b = c$.

(15) G is cancelable iff for all a, b, c such that $a \cdot b = a \cdot c$ or $b \cdot a = c \cdot a$ holds $b = c$.

(16) G has uniquely decomposable unity if and only if the following conditions are satisfied:

(i) the multiplication of G has a unity, and

(ii) for all elements a, b of G such that $a \cdot b = \mathbf{1}_{\text{the multiplication of } G}$ holds $a = b$ and $b = \mathbf{1}_{\text{the multiplication of } G}$.

(17) Suppose G is associative. Then G is invertible if and only if the following conditions are satisfied:

(i) G is unital, and

(ii) the multiplication of G has an inverse operation.

Let us note that every non empty groupoid which is associative and group-like is also invertible and every non empty groupoid which is associative and invertible is also group-like.

One can verify the following observations:

* every non empty groupoid which is invertible is also left invertible and right invertible,
* every non empty groupoid which is left invertible and right invertible is also invertible,
* every non empty groupoid which is cancelable is also left cancelable and right cancelable,
* every non empty groupoid which is left cancelable and right cancelable is also cancelable, and
* every non empty groupoid which is associative and invertible is also unital and cancelable.

3. Monoids

In the sequel M is a non empty multiplicative loop structure.

Let I_1 be a non empty multiplicative loop structure. Let us observe that I_1 is well unital if and only if:

(Def. 21) The unity of I_1 is a unity w.r.t. the multiplication of I_1.

Next we state the proposition

(18) M is well unital iff for every element a of M holds (the unity of $M) \cdot a = a$ and $a \cdot$ the unity of $M = a$.

Let us observe that every non empty multiplicative loop structure which is well unital is also unital.

One can prove the following proposition

(19) Let M be a non empty multiplicative loop structure. Suppose M is well unital. Then the unity of $M = \mathbf{1}_{\text{the multiplication of } M}$.

Let A be a non empty set, let m be a binary operation on A, and let u be an element of A. Observe that $\langle A, m, u \rangle$ is non empty.

One can check that there exists a non empty multiplicative loop structure which is well unital, commutative, associative, cancelable, idempotent, invertible, unital, constituted functions, constituted finite sequences, and strict and has uniquely decomposable unity.

A monoid is a well unital associative non empty multiplicative loop structure.

Let G be a groupoid. A multiplicative loop structure is said to be a monoidal extension of G if:

(Def. 22) The groupoid of it $=$ the groupoid of G.

Let G be a non empty groupoid. Note that every monoidal extension of G is non empty.
The following proposition is true

(20) Let M be a monoidal extension of G. Then
(i) the carrier of $M =$ the carrier of G,
(ii) the multiplication of $M =$ the multiplication of G, and
(iii) for all elements a, b of M and for all elements a', b' of G such that $a = a'$ and $b = b'$ holds $a \cdot b = a' \cdot b'$.

Let G be a groupoid. One can verify that there exists a monoidal extension of G which is strict.
Next we state the proposition

(21) Let G be a non empty groupoid and M be a monoidal extension of G. Then
(i) if G is unital, then M is unital,
(ii) if G is commutative, then M is commutative,
(iii) if G is associative, then M is associative,
(iv) if G is invertible, then M is invertible,
(v) if G has uniquely decomposable unity, then M has uniquely decomposable unity, and
(vi) if G is cancelable, then M is cancelable.

Let G be a constituted functions groupoid. Note that every monoidal extension of G is constituted functions.

Let G be a constituted finite sequences groupoid. Observe that every monoidal extension of G is constituted finite sequences.

Let G be a unital non empty groupoid. One can verify that every monoidal extension of G is unital.

Let G be an associative non empty groupoid. Observe that every monoidal extension of G is associative.

Let G be a commutative non empty groupoid. Observe that every monoidal extension of G is commutative.

Let G be an invertible non empty groupoid. One can verify that every monoidal extension of G is invertible.

Let G be a cancelable non empty groupoid. Observe that every monoidal extension of G is cancelable.

Let G be a non empty groupoid with uniquely decomposable unity. One can check that every monoidal extension of G has uniquely decomposable unity.

Let G be a unital non empty groupoid. Note that there exists a monoidal extension of G which is well unital and strict.

Next we state the proposition

(22) For every unital non empty groupoid G and for all well unital strict monoidal extensions M_1, M_2 of G holds $M_1 = M_2$.

4. Subsystems

Let G be a groupoid. A groupoid is called a subsystem of G if:

(Def. 23) The multiplication of it $\leq$ the multiplication of G.

Let G be a groupoid. Observe that there exists a subsystem of G which is strict.

Let G be a non empty groupoid. Observe that there exists a subsystem of G which is strict and non empty.

Let G be a unital non empty groupoid. Note that there exists a non empty subsystem of G which is unital, associative, commutative, cancelable, idempotent, invertible, and strict and has uniquely decomposable unity.

Let G be a groupoid. A multiplicative loop structure is said to be a monoidal subsystem of G if it satisfies the conditions (Def. 24).

(Def. 24)(i) The multiplication of it $\leq$ the multiplication of G, and

(ii) for every multiplicative loop structure M such that $G = M$ holds the unity of it $=$ the unity of M.

Let G be a groupoid. Note that there exists a monoidal subsystem of G which is strict.

Let G be a non empty groupoid. Note that there exists a monoidal subsystem of G which is strict and non empty.

Let M be a multiplicative loop structure. Let us note that the monoidal subsystem of M can be characterized by the following (equivalent) condition:

(Def. 25) The multiplication of it $\leq$ the multiplication of M and the unity of it $=$ the unity of M.

Let G be a well unital non empty multiplicative loop structure. Note that there exists a non empty monoidal subsystem of G which is well unital, associative, commutative, cancelable, idempotent, invertible, and strict and has uniquely decomposable unity.

Next we state the proposition

(23) For every groupoid G holds every monoidal subsystem of G is a subsystem of G.

Let G be a groupoid and let M be a monoidal extension of G. We see that the subsystem of M is a subsystem of G.

Let G_1 be a groupoid and let G_2 be a subsystem of G_1. We see that the subsystem of G_2 is a subsystem of G_1.

Let G_1 be a groupoid and let G_2 be a monoidal subsystem of G_1. We see that the subsystem of G_2 is a subsystem of G_1.

Let G be a groupoid and let M be a monoidal subsystem of G. We see that the monoidal subsystem of M is a monoidal subsystem of G.

Next we state the proposition

(24) G is a subsystem of G and M is a monoidal subsystem of M.

In the sequel H is a non empty subsystem of G and N is a non empty monoidal subsystem of G.

One can prove the following propositions:

(25) The carrier of $H \subseteq$ the carrier of G and the carrier of $N \subseteq$ the carrier of G.

(26) Let G be a non empty groupoid and H be a non empty subsystem of G. Then the multiplication of $H =$ (the multiplication of G)$\restriction$[:the carrier of H, the carrier of H:].

(27) For all elements a, b of H and for all elements a', b' of G such that $a = a'$ and $b = b'$ holds $a \cdot b = a' \cdot b'$.

(28) Let H_1, H_2 be non empty subsystems of G. Suppose the carrier of $H_1 =$ the carrier of H_2. Then the groupoid of $H_1 =$ the groupoid of H_2.

(29) Let H_1, H_2 be non empty monoidal subsystems of M. Suppose the carrier of $H_1 =$ the carrier of H_2. Then the multiplicative loop structure of $H_1 =$ the multiplicative loop structure of H_2.

(30) Let H_1, H_2 be non empty subsystems of G. Suppose the carrier of $H_1 \subseteq$ the carrier of H_2. Then H_1 is a subsystem of H_2.

(31) Let H_1, H_2 be non empty monoidal subsystems of M. Suppose the carrier of $H_1 \subseteq$ the carrier of H_2. Then H_1 is a monoidal subsystem of H_2.

(32) Suppose G is unital and $\mathbf{1}_{\text{the multiplication of } G} \in$ the carrier of H. Then H is unital and $\mathbf{1}_{\text{the multiplication of } G} = \mathbf{1}_{\text{the multiplication of } H}$.

(33) For every well unital non empty multiplicative loop structure M holds every non empty monoidal subsystem of M is well unital.

(34) If G is commutative, then H is commutative.

(35) If G is associative, then H is associative.

(36) If G is idempotent, then H is idempotent.

(37) If G is cancelable, then H is cancelable.

(38) Suppose $\mathbf{1}_{\text{the multiplication of } G} \in$ the carrier of H and G has uniquely decomposable unity. Then H has uniquely decomposable unity.

(39) Let M be a well unital non empty multiplicative loop structure with uniquely decomposable unity. Then every non empty monoidal subsystem of M has uniquely decomposable unity.

Let G be a constituted functions non empty groupoid. Observe that every non empty subsystem of G is constituted functions and every non empty monoidal subsystem of G is constituted functions.

Let G be a constituted finite sequences non empty groupoid. Observe that every non empty subsystem of G is constituted finite sequences and every non empty monoidal subsystem of G is constituted finite sequences.

Let M be a well unital non empty multiplicative loop structure. One can verify that every non empty monoidal subsystem of M is well unital.

Let G be a commutative non empty groupoid. Observe that every non empty subsystem of G is commutative and every non empty monoidal subsystem of G is commutative.

Let G be an associative non empty groupoid. One can verify that every non empty subsystem of G is associative and every non empty monoidal subsystem of G is associative.

Let G be an idempotent non empty groupoid. Note that every non empty subsystem of G is idempotent and every non empty monoidal subsystem of G is idempotent.

Let G be a cancelable non empty groupoid. One can check that every non empty subsystem of G is cancelable and every non empty monoidal subsystem of G is cancelable.

Let M be a well unital non empty multiplicative loop structure with uniquely decomposable unity. One can check that every non empty monoidal subsystem of M has uniquely decomposable unity.

In this article we present several logical schemes. The scheme *SubStrEx1* deals with a non empty groupoid $\mathcal{A}$ and a non empty subset $\mathcal{B}$ of $\mathcal{A}$, and states that:

There exists a strict non empty subsystem H of $\mathcal{A}$ such that the carrier of $H = \mathcal{B}$

provided the following requirement is met:

- For all elements x, y of $\mathcal{B}$ holds $x \cdot y \in \mathcal{B}$.

The scheme *SubStrEx2* deals with a non empty groupoid $\mathcal{A}$ and a unary predicate $\mathcal{P}$, and states that:

There exists a strict non empty subsystem H of $\mathcal{A}$ such that for every element x of $\mathcal{A}$ holds $x \in$ the carrier of H if and only if $\mathcal{P}[x]$

provided the parameters meet the following conditions:

- For all elements x, y of $\mathcal{A}$ such that $\mathcal{P}[x]$ and $\mathcal{P}[y]$ holds $\mathcal{P}[x \cdot y]$, and
- There exists an element x of $\mathcal{A}$ such that $\mathcal{P}[x]$.

The scheme *MonoidalSubStrEx1* deals with a non empty multiplicative loop structure $\mathcal{A}$ and a non empty subset $\mathcal{B}$ of $\mathcal{A}$, and states that:

There exists a strict non empty monoidal subsystem H of $\mathcal{A}$ such that the carrier of $H = \mathcal{B}$

provided the parameters meet the following conditions:

- For all elements x, y of $\mathcal{B}$ holds $x \cdot y \in \mathcal{B}$, and
- The unity of $\mathcal{A} \in \mathcal{B}$.

The scheme *MonoidalSubStrEx2* deals with a non empty multiplicative loop structure $\mathcal{A}$ and a unary predicate $\mathcal{P}$, and states that:

There exists a strict non empty monoidal subsystem M of $\mathcal{A}$ such that for every element x of $\mathcal{A}$ holds $x \in$ the carrier of M if and only if $\mathcal{P}[x]$

provided the following conditions are met:

- For all elements x, y of $\mathcal{A}$ such that $\mathcal{P}[x]$ and $\mathcal{P}[y]$ holds $\mathcal{P}[x \cdot y]$, and
- $\mathcal{P}$[the unity of $\mathcal{A}$].

Let us consider G, a, b. Then $a \cdot b$ is an element of G. We introduce $a \otimes b$ as a synonym of $a \cdot b$.

5. The Examples of Monoids of Numbers

The unital associative invertible commutative cancelable strict non empty groupoid $\langle \mathbb{R}, + \rangle$ is defined by:

(Def. 26) $\langle \mathbb{R}, + \rangle = \langle \mathbb{R}, +_{\mathbb{R}} \rangle$.

We now state several propositions:

(40)(i) The carrier of $\langle \mathbb{R}, + \rangle = \mathbb{R}$,

(ii) the multiplication of $\langle \mathbb{R}, + \rangle = +_{\mathbb{R}}$, and

(iii) for all elements a, b of $\langle \mathbb{R}, + \rangle$ and for all real numbers x, y such that $a = x$ and $b = y$ holds $a \cdot b = x + y$.

(41) x is an element of $\langle \mathbb{R}, + \rangle$ iff x is a real number.

(42) $\mathbf{1}_{\text{the multiplication of } \langle \mathbb{R}, + \rangle} = 0$.

(43) Let N be a non empty subsystem of $\langle \mathbb{R}, + \rangle$, a, b be elements of N, and x, y be real numbers. If $a = x$ and $b = y$, then $a \cdot b = x + y$.

(44) For every unital non empty subsystem N of $\langle \mathbb{R}, + \rangle$ holds $\mathbf{1}_{\text{the multiplication of } N} = 0$.

Let G be a unital non empty groupoid. Observe that every non empty subsystem of G which is associative and invertible is also unital, cancelable, and group-like.

$\mathbb{Z}^+$ is a unital invertible strict non empty subsystem of $\langle \mathbb{R}, + \rangle$.

One can prove the following two propositions:

(46)[2] For every strict non empty subsystem G of $\langle \mathbb{R}, + \rangle$ holds $G = \mathbb{Z}^+$ iff the carrier of $G = \mathbb{Z}$.

(47) x is an element of $\mathbb{Z}^+$ iff x is an integer.

The unital strict non empty subsystem $\langle \mathbb{N}, + \rangle$ of $\mathbb{Z}^+$ with uniquely decomposable unity is defined by:

(Def. 27) The carrier of $\langle \mathbb{N}, + \rangle = \mathbb{N}$.

(Def. 28) $\langle \mathbb{N}, +, 0 \rangle$ is a well unital strict non empty monoidal extension of $\langle \mathbb{N}, + \rangle$.

The binary operation $+_{\mathbb{N}}$ on $\mathbb{N}$ is defined as follows:

(Def. 29) $+_{\mathbb{N}} =$ the multiplication of $\langle \mathbb{N}, + \rangle$.

One can prove the following propositions:

(49)[3] $\langle \mathbb{N}, + \rangle = \langle \mathbb{N}, +_{\mathbb{N}} \rangle$.

(50) x is an element of $\langle \mathbb{N}, +, 0 \rangle$ iff x is a natural number.

(51) For all natural numbers n_1, n_2 and for all elements m_1, m_2 of $\langle \mathbb{N}, +, 0 \rangle$ such that $n_1 = m_1$ and $n_2 = m_2$ holds $m_1 \cdot m_2 = n_1 + n_2$.

---

[2] The proposition (45) has been removed.

[3] The proposition (48) has been removed.

(52) $\langle \mathbb{N}, +, 0 \rangle = \langle \mathbb{N}, +_{\mathbb{N}}, 0 \rangle$.

(53) $+_{\mathbb{N}} = +_{\mathbb{R}} \restriction ([\!: \mathbb{N}, \mathbb{N} :\!]$ **qua** set$)$ and $+_{\mathbb{N}} = (+_{\mathbb{Z}}) \restriction ([\!: \mathbb{N}, \mathbb{N} :\!]$ **qua** set$)$.

(54)(i) 0 is a unity w.r.t. $+_{\mathbb{N}}$,

(ii) $+_{\mathbb{N}}$ has a unity,

(iii) $\mathbf{1}_{+_{\mathbb{N}}} = 0$,

(iv) $+_{\mathbb{N}}$ is commutative,

(v) $+_{\mathbb{N}}$ is associative, and

(vi) $+_{\mathbb{N}}$ has uniquely decomposable unity.

The unital commutative associative strict non empty groupoid $\langle \mathbb{R}, \cdot \rangle$ is defined as follows:

(Def. 30) $\langle \mathbb{R}, \cdot \rangle = \langle \mathbb{R}, \cdot_{\mathbb{R}} \rangle$.

Next we state several propositions:

(55)(i) The carrier of $\langle \mathbb{R}, \cdot \rangle = \mathbb{R}$,

(ii) the multiplication of $\langle \mathbb{R}, \cdot \rangle = \cdot_{\mathbb{R}}$, and

(iii) for all elements a, b of $\langle \mathbb{R}, \cdot \rangle$ and for all real numbers x, y such that $a = x$ and $b = y$ holds $a \cdot b = x \cdot y$.

(56) x is an element of $\langle \mathbb{R}, \cdot \rangle$ iff x is a real number.

(57) $\mathbf{1}_{\text{the multiplication of } \langle \mathbb{R}, \cdot \rangle} = 1$.

(58) Let N be a non empty subsystem of $\langle \mathbb{R}, \cdot \rangle$, a, b be elements of N, and x, y be real numbers. If $a = x$ and $b = y$, then $a \cdot b = x \cdot y$.

(60)[4] For every unital non empty subsystem N of $\langle \mathbb{R}, \cdot \rangle$ holds $\mathbf{1}_{\text{the multiplication of } N} = 0$ or $\mathbf{1}_{\text{the multiplication of } N} = 1$.

The unital strict non empty subsystem $\langle \mathbb{N}, \cdot \rangle$ of $\langle \mathbb{R}, \cdot \rangle$ with uniquely decomposable unity is defined as follows:

(Def. 31) The carrier of $\langle \mathbb{N}, \cdot \rangle = \mathbb{N}$.

(Def. 32) $\langle \mathbb{N}, \cdot, 1 \rangle$ is a well unital strict non empty monoidal extension of $\langle \mathbb{N}, \cdot \rangle$.

The binary operation $\cdot_{\mathbb{N}}$ on $\mathbb{N}$ is defined as follows:

(Def. 33) $\cdot_{\mathbb{N}} =$ the multiplication of $\langle \mathbb{N}, \cdot \rangle$.

One can prove the following propositions:

(61) $\langle \mathbb{N}, \cdot \rangle = \langle \mathbb{N}, \cdot_{\mathbb{N}} \rangle$.

(62) For all natural numbers n_1, n_2 and for all elements m_1, m_2 of $\langle \mathbb{N}, \cdot \rangle$ such that $n_1 = m_1$ and $n_2 = m_2$ holds $m_1 \cdot m_2 = n_1 \cdot n_2$.

(63) $\mathbf{1}_{\text{the multiplication of } \langle \mathbb{N}, \cdot \rangle} = 1$.

(64) For all natural numbers n_1, n_2 and for all elements m_1, m_2 of $\langle \mathbb{N}, \cdot, 1 \rangle$ such that $n_1 = m_1$ and $n_2 = m_2$ holds $m_1 \cdot m_2 = n_1 \cdot n_2$.

(65) $\langle \mathbb{N}, \cdot, 1 \rangle = \langle \mathbb{N}, \cdot_{\mathbb{N}}, 1 \rangle$.

(66) $\cdot_{\mathbb{N}} = \cdot_{\mathbb{R}} \restriction ([\!: \mathbb{N}, \mathbb{N} :\!]$ **qua** set$)$.

[4] The proposition (59) has been removed.

(67)(i) 1 is a unity w.r.t. $\cdot_{\mathbb{N}}$,

(ii) $\cdot_{\mathbb{N}}$ has a unity,

(iii) $\mathbf{1}_{\cdot_{\mathbb{N}}} = 1$,

(iv) $\cdot_{\mathbb{N}}$ is commutative,

(v) $\cdot_{\mathbb{N}}$ is associative, and

(vi) $\cdot_{\mathbb{N}}$ has uniquely decomposable unity.

6. The Monoid of Finite Sequences over the Set

Let D be a non empty set. The functor $\langle D^*, ^\frown \rangle$ yielding a unital associative cancelable constituted finite sequences strict non empty groupoid with uniquely decomposable unity is defined as follows:

(Def. 34) The carrier of $\langle D^*, ^\frown \rangle = D^*$ and for all elements p, q of $\langle D^*, ^\frown \rangle$ holds $p \otimes q = p ^\frown q$.

Let us consider D.

(Def. 35) $\langle D^*, ^\frown, \varepsilon \rangle$ is a well unital strict non empty monoidal extension of $\langle D^*, ^\frown \rangle$.

The concatenation of D yields a binary operation on D^* and is defined as follows:

(Def. 36) The concatenation of $D =$ the multiplication of $\langle D^*, ^\frown \rangle$.

The following propositions are true:

(68) $\langle D^*, ^\frown \rangle = \langle D^*, \text{the concatenation of } D \rangle$.

(69) $\mathbf{1}_{\text{the multiplication of } \langle D^*, ^\frown \rangle} = \emptyset$.

(70) The carrier of $\langle D^*, ^\frown, \varepsilon \rangle = D^*$ and the multiplication of $\langle D^*, ^\frown, \varepsilon \rangle =$ the concatenation of D and the unity of $\langle D^*, ^\frown, \varepsilon \rangle = \emptyset$.

(71) For all elements a, b of $\langle D^*, ^\frown, \varepsilon \rangle$ holds $a \otimes b = a ^\frown b$.

(72) For every non empty subsystem F of $\langle D^*, ^\frown \rangle$ and for all elements p, q of F holds $p \otimes q = p ^\frown q$.

(73) For every unital non empty subsystem F of $\langle D^*, ^\frown \rangle$ holds $\mathbf{1}_{\text{the multiplication of } F} = \emptyset$.

(74) Let F be a non empty subsystem of $\langle D^*, ^\frown \rangle$. Suppose $\emptyset$ is an element of F. Then F is unital and $\mathbf{1}_{\text{the multiplication of } F} = \emptyset$.

(75) For all non empty sets A, B such that $A \subseteq B$ holds $\langle A^*, ^\frown \rangle$ is a subsystem of $\langle B^*, ^\frown \rangle$.

(76) The concatenation of D has a unity and $\mathbf{1}_{\text{the concatenation of } D} = \emptyset$ and the concatenation of D is associative.

7. Monoids of Mappings

Let X be a set. The semigroup of partial functions onto X yielding a unital associative constituted functions strict non empty groupoid is defined by the conditions (Def. 37).

(Def. 37)(i) The carrier of the semigroup of partial functions onto $X = X \dot{\rightarrow} X$, and

(ii) for all elements f, g of the semigroup of partial functions onto X holds $f \otimes g = f \circ g$.

Let X be a set.

(Def. 38) The monoid of partial functions onto X is a well unital strict non empty monoidal extension of the semigroup of partial functions onto X.

The composition of X yielding a binary operation on $X \dot{\rightarrow} X$ is defined by:

(Def. 39) The composition of $X =$ the multiplication of the semigroup of partial functions onto X.

One can prove the following propositions:

(77) x is an element of the semigroup of partial functions onto X if and only if x is a partial function from X to X.

(78) $\mathbf{1}_{\text{the multiplication of the semigroup of partial functions onto } X} = \mathrm{id}_X$.

(79) Let F be a non empty subsystem of the semigroup of partial functions onto X and f, g be elements of F. Then $f \otimes g = f \circ g$.

(80) Let F be a non empty subsystem of the semigroup of partial functions onto X. Suppose id_X is an element of F. Then F is unital and $\mathbf{1}_{\text{the multiplication of } F} = \mathrm{id}_X$.

(81) Suppose $Y \subseteq X$. Then the semigroup of partial functions onto Y is a subsystem of the semigroup of partial functions onto X.

Let X be a set. The semigroup of functions onto X yielding a unital strict non empty subsystem of the semigroup of partial functions onto X is defined by:

(Def. 40) The carrier of the semigroup of functions onto $X = X^X$.

Let X be a set.

(Def. 41) The monoid of functions onto X is a well unital strict monoidal extension of the semigroup of functions onto X.

One can prove the following propositions:

(82) x is an element of the semigroup of functions onto X iff x is a function from X into X.

(83) The multiplication of the semigroup of functions onto $X =$ (the composition of $X) \restriction [: X^X, X^X :]$.

(84) $\mathbf{1}_{\text{the multiplication of the semigroup of functions onto } X} = \mathrm{id}_X$.

(85)(i) The carrier of the monoid of functions onto $X = X^X$,

(ii) the multiplication of the monoid of functions onto $X =$ (the composition of $X) \restriction [: X^X, X^X :]$, and

(iii) the unity of the monoid of functions onto $X = \mathrm{id}_X$.

Let X be a set. The group of permutations onto X yields a unital invertible strict non empty subsystem of the semigroup of functions onto X and is defined by the condition (Def. 42).

(Def. 42) Let f be an element of the semigroup of functions onto X. Then $f \in$ the carrier of the group of permutations onto X if and only if f is a permutation of X.

We now state three propositions:

(86) x is an element of the group of permutations onto X iff x is a permutation of X.

(87)(i) $\mathbf{1}_{\text{the multiplication of the group of permutations onto } X} = \mathrm{id}_X$, and

(ii) $1_{\text{the group of permutations onto } X} = \mathrm{id}_X$.

(88) For every element f of the group of permutations onto X holds $f^{-1} = (f$ **qua** function$)^{-1}$.

REFERENCES

[1] Grzegorz Bancerek. The fundamental properties of natural numbers. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/nat_1.html.

[2] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/finseq_1.html.

[3] Czesław Byliński. Binary operations. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/binop_1.html.

[4] Czesław Byliński. Functions and their basic properties. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/funct_1.html.

[5] Czesław Byliński. Functions from a set to a set. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/funct_2.html.

[6] Czesław Byliński. Partial functions. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/partfun1.html.

[7] Czesław Byliński. Some basic properties of sets. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/zfmisc_1.html.

[8] Czesław Byliński. Binary operations applied to finite sequences. *Journal of Formalized Mathematics*, 2, 1990. http://mizar.org/JFM/Vol2/finseqop.html.

[9] Czesław Byliński. Finite sequences and tuples of elements of a non-empty sets. *Journal of Formalized Mathematics*, 2, 1990. http://mizar.org/JFM/Vol2/finseq_2.html.

[10] Krzysztof Hryniewiecki. Basic properties of real numbers. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/real_1.html.

[11] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/vectsp_1.html.

[12] Michał Muzalewski. Construction of rings and left-, right-, and bi-modules over a ring. *Journal of Formalized Mathematics*, 2, 1990. http://mizar.org/JFM/Vol2/vectsp_2.html.

[13] Dariusz Surowik. Cyclic groups and some of their properties — part I. *Journal of Formalized Mathematics*, 3, 1991. http://mizar.org/JFM/Vol3/gr_cy_1.html.

[14] Andrzej Trybulec. Binary operations applied to functions. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/funcop_1.html.

[15] Andrzej Trybulec. Semilattice operations on finite subsets. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/setwiseo.html.

[16] Andrzej Trybulec. Tarski Grothendieck set theory. *Journal of Formalized Mathematics*, Axiomatics, 1989. http://mizar.org/JFM/Axiomatics/tarski.html.

[17] Andrzej Trybulec. Tuples, projections and Cartesian products. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/mcart_1.html.

[18] Andrzej Trybulec. Subsets of real numbers. *Journal of Formalized Mathematics*, Addenda, 2003. http://mizar.org/JFM/Addenda/numbers.html.

[19] Michał J. Trybulec. Integers. *Journal of Formalized Mathematics*, 2, 1990. http://mizar.org/JFM/Vol2/int_1.html.

[20] Wojciech A. Trybulec. Groups. *Journal of Formalized Mathematics*, 2, 1990. http://mizar.org/JFM/Vol2/group_1.html.

[21] Zinaida Trybulec. Properties of subsets. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/subset_1.html.

[22] Edmund Woronowicz. Relations and their basic properties. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/relat_1.html.

[23] Edmund Woronowicz. Relations defined on sets. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/relset_1.html.

Received December 29, 1992

Published January 2, 2004