FORMALIZED MATHEMATICS
Vol.1, No.5, November–December 1990
Université Catholique de Louvain

From Loops to Abelian Multiplicative Groups with Zero [1]

Michał Muzalewski
Warsaw University
Białystok

Wojciech Skaba
Nicolaus Copernicus University
Toruń

Summary. Elementary axioms and theorems on the theory of algebraic structures, taken from the book [4]. First a loop structure $\langle G, 0, + \rangle$ is defined and six axioms corresponding to it are given. Group is defined by extending the set of axioms with $(a+b)+c = a+(b+c)$. At the same time an alternate approach to the set of axioms is shown and both sets are proved to yield the same algebraic structure. A trivial example of loop is used to ensure the existence of the modes being constructed. A multiplicative group is contemplated, which is quite similar to the previously defined additive group (called simply a group here), but is supposed to be of greater interest in the future considerations of algebraic structures. The final section brings a slightly more sophisticated structure i.e: a multiplicative loop/group with zero: $\langle G, \cdot, 1, 0 \rangle$. Here the proofs are a more challenging and the above trivial example is replaced by a more common (and comprehensive) structure built on the foundation of real numbers.

MML Identifier: ALGSTR_1.

The notation and terminology used in this paper are introduced in the following articles: [1], [2], and [3]. We consider loop structures which are systems
⟨a carrier, an addition, a zero⟩,
where the carrier is a non-empty set, the addition is a binary operation on the carrier, and the zero is an element of the carrier. In the sequel G_1 will denote a loop structure. Let us consider G_1. An element of G_1 is an element of the carrier of G_1.

In the sequel a, b will denote elements of G_1. Let us consider G_1, a, b. The functor $a + b$ yielding an element of G_1 is defined as follows:

(Def.1) $a + b =$ (the addition of G_1)(a, b).

We now state the proposition

[1] Supported by RPBP.III-24.C6.

ISSN 0777–4028

(1) $a + b =$ (the addition of G_1)(a, b).

Let us consider G_1. The functor 0_{G_1} yielding an element of G_1 is defined as follows:

(Def.2) $0_{G_1} =$ the zero of G_1.

One can prove the following proposition

(2) $0_{G_1} =$ the zero of G_1.

Let x be arbitrary. The functor Extract(x) yielding an element of $\{x\}$ is defined by:

(Def.3) Extract$(x) = x$.

One can prove the following proposition

(3) For an arbitrary x holds Extract$(x) = x$.

The trivial loop a loop structure is defined as follows:

(Def.4) the trivial loop $= \langle \{0\}, zo, \mathrm{Extract}(0) \rangle$.

One can prove the following three propositions:

(4) The trivial loop $= \langle \{0\}, zo, \mathrm{Extract}(0) \rangle$.

(5) If a is an element of the trivial loop, then $a = 0_{\text{the trivial loop}}$.

(6) For all elements a, b of the trivial loop holds $a + b = 0_{\text{the trivial loop}}$.

A loop structure is called a loop if:

(Def.5) (i) for every element a of it holds $a + 0_{\mathrm{it}} = a$,
(ii) for every element a of it holds $0_{\mathrm{it}} + a = a$,
(iii) for every elements a, b of it there exists an element x of it such that $a + x = b$,
(iv) for every elements a, b of it there exists an element x of it such that $x + a = b$,
(v) for all elements a, x, y of it such that $a + x = a + y$ holds $x = y$,
(vi) for all elements a, x, y of it such that $x + a = y + a$ holds $x = y$.

The following proposition is true

(7) Let G_1 be a loop structure. Then G_1 is a loop if and only if the following conditions are satisfied:
(i) for every element a of G_1 holds $a + 0_{G_1} = a$,
(ii) for every element a of G_1 holds $0_{G_1} + a = a$,
(iii) for every elements a, b of G_1 there exists an element x of G_1 such that $a + x = b$,
(iv) for every elements a, b of G_1 there exists an element x of G_1 such that $x + a = b$,
(v) for all elements a, x, y of G_1 such that $a + x = a + y$ holds $x = y$,
(vi) for all elements a, x, y of G_1 such that $x + a = y + a$ holds $x = y$.

Let us note that it makes sense to consider the following constant. Then the trivial loop is a loop.

A loop is called a group if:

(Def.6) for all elements a, b, c of it holds $(a + b) + c = a + (b + c)$.

We now state the proposition

(8) For every loop G_1 holds G_1 is a group if and only if for all elements a, b, c of G_1 holds $(a+b)+c = a+(b+c)$.

We follow the rules: L will be a loop structure and a, b, c, x will be elements of L. We now state the proposition

(9) L is a group if and only if for every a holds $a + 0_L = a$ and for every a there exists x such that $a + x = 0_L$ and for all a, b, c holds $(a+b)+c = a+(b+c)$.

Let us note that it makes sense to consider the following constant. Then the trivial loop is a group.

A group is called an Abelian group if:

(Def.7) for all elements a, b of it holds $a + b = b + a$.

Next we state two propositions:

(10) For every group G holds G is an Abelian group if and only if for all elements a, b of G holds $a + b = b + a$.

(11) L is an Abelian group if and only if the following conditions are satisfied:
- (i) for every a holds $a + 0_L = a$,
- (ii) for every a there exists x such that $a + x = 0_L$,
- (iii) for all a, b, c holds $(a+b)+c = a+(b+c)$,
- (iv) for all a, b holds $a + b = b + a$.

Let L be a group, and let a be an element of L. The functor $-a$ yielding an element of L is defined by:

(Def.8) $a + (-a) = 0_L$.

We now state the proposition

(12) For every group L and for every element a of L holds $a + (-a) = 0_L$.

In the sequel G will denote a group and a, b will denote elements of G. One can prove the following proposition

(13) $a + (-a) = 0_G$ and $(-a) + a = 0_G$.

Let us consider G, a, b. The functor $a - b$ yields an element of G and is defined as follows:

(Def.9) $a - b = a + (-b)$.

Next we state the proposition

(14) $a - b = a + (-b)$.

We consider mutiplicative loop structures which are systems

⟨a carrier, a multiplication, a unity⟩,

where the carrier is a non-empty set, the multiplication is a binary operation on the carrier, and the unity is an element of the carrier. In the sequel G_1 is a mutiplicative loop structure. Let us consider G_1. An element of G_1 is an element of the carrier of G_1.

In the sequel a, b are elements of G_1. Let us consider G_1, a, b. The functor $a \cdot b$ yields an element of G_1 and is defined as follows:

(Def.10) $a \cdot b =$ (the multiplication of G_1)(a, b).

One can prove the following proposition

(15) $a \cdot b =$ (the multiplication of G_1)(a, b).

Let us consider G_1. The functor 1_{G_1} yields an element of G_1 and is defined by:

(Def.11) $1_{G_1} =$ the unity of G_1.

One can prove the following proposition

(16) $1_{G_1} =$ the unity of G_1.

The trivial multiplicative loop a mutiplicative loop structure is defined as follows:

(Def.12) the trivial multiplicative loop $= \langle\{0\}, zo, \mathrm{Extract}(0)\rangle$.

The following propositions are true:

(17) The trivial multiplicative loop $= \langle\{0\}, zo, \mathrm{Extract}(0)\rangle$.

(18) If a is an element of the trivial multiplicative loop, then $a = 1_{\text{the trivial multiplicative loop}}$.

(19) For all elements a, b of the trivial multiplicative loop holds $a \cdot b = 1_{\text{the trivial multiplicative loop}}$.

A mutiplicative loop structure is said to be a multiplicative loop if:

(Def.13) (i) for every element a of it holds $a \cdot (1_{\text{it}}) = a$,

(ii) for every element a of it holds $(1_{\text{it}}) \cdot a = a$,

(iii) for every elements a, b of it there exists an element x of it such that $a \cdot x = b$,

(iv) for every elements a, b of it there exists an element x of it such that $x \cdot a = b$,

(v) for all elements a, x, y of it such that $a \cdot x = a \cdot y$ holds $x = y$,

(vi) for all elements a, x, y of it such that $x \cdot a = y \cdot a$ holds $x = y$.

We now state the proposition

(20) Let L be a mutiplicative loop structure. Then L is a multiplicative loop if and only if the following conditions are satisfied:

(i) for every element a of L holds $a \cdot (1_L) = a$,

(ii) for every element a of L holds $(1_L) \cdot a = a$,

(iii) for every elements a, b of L there exists an element x of L such that $a \cdot x = b$,

(iv) for every elements a, b of L there exists an element x of L such that $x \cdot a = b$,

(v) for all elements a, x, y of L such that $a \cdot x = a \cdot y$ holds $x = y$,

(vi) for all elements a, x, y of L such that $x \cdot a = y \cdot a$ holds $x = y$.

Let us note that it makes sense to consider the following constant. Then the trivial multiplicative loop is a multiplicative loop.

A multiplicative loop is said to be a multiplicative group if:

(Def.14) for all elements a, b, c of it holds $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

One can prove the following proposition

(21) For every multiplicative loop L holds L is a multiplicative group if and only if for all elements a, b, c of L holds $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

We follow the rules: L is a mutiplicative loop structure and a, b, c, x are elements of L. One can prove the following proposition

(22) L is a multiplicative group if and only if for every a holds $a \cdot (1_L) = a$ and for every a there exists x such that $a \cdot x = 1_L$ and for all a, b, c holds $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

Let us note that it makes sense to consider the following constant. Then the trivial multiplicative loop is a multiplicative group.

A multiplicative group is called a multiplicative Abelian group if:

(Def.15) for all elements a, b of it holds $a \cdot b = b \cdot a$.

The following propositions are true:

(23) For every multiplicative group G holds G is a multiplicative Abelian group if and only if for all elements a, b of G holds $a \cdot b = b \cdot a$.

(24) L is a multiplicative Abelian group if and only if the following conditions are satisfied:

(i) for every a holds $a \cdot (1_L) = a$,

(ii) for every a there exists x such that $a \cdot x = 1_L$,

(iii) for all a, b, c holds $(a \cdot b) \cdot c = a \cdot (b \cdot c)$,

(iv) for all a, b holds $a \cdot b = b \cdot a$.

Let L be a multiplicative group, and let a be an element of L. The functor a^{-1} yields an element of L and is defined by:

(Def.16) $a \cdot (a^{-1}) = 1_L$.

The following proposition is true

(25) For every multiplicative group L and for every element a of L holds $a \cdot a^{-1} = 1_L$.

In the sequel G is a multiplicative group and a, b are elements of G. The following proposition is true

(26) $a \cdot a^{-1} = 1_G$ and $a^{-1} \cdot a = 1_G$.

Let us consider G, a, b. The functor $\frac{a}{b}$ yields an element of G and is defined by:

(Def.17) $\frac{a}{b} = a \cdot b^{-1}$.

One can prove the following proposition

(27) $\frac{a}{b} = a \cdot b^{-1}$.

We consider mutiplicative loop with zero structures which are systems

⟨a carrier, a multiplication, a unity, a zero⟩,

where the carrier is a non-empty set, the multiplication is a binary operation on the carrier, the unity is an element of the carrier, and the zero is an element of the carrier. In the sequel G_1 will be a mutiplicative loop with zero structure. Let us consider G_1. An element of G_1 is an element of the carrier of G_1.

In the sequel a, b will denote elements of G_1. Let us consider G_1, a, b. The functor $a \cdot b$ yielding an element of G_1 is defined by:

(Def.18) $a \cdot b =$ (the multiplication of G_1)(a, b).

The following proposition is true

(28) $a \cdot b =$ (the multiplication of G_1)(a, b).

Let us consider G_1. The functor 1_{G_1} yields an element of G_1 and is defined as follows:

(Def.19) $1_{G_1} =$ the unity of G_1.

One can prove the following proposition

(29) $1_{G_1} =$ the unity of G_1.

Let us consider G_1. The functor 0_{G_1} yielding an element of G_1 is defined as follows:

(Def.20) $0_{G_1} =$ the zero of G_1.

One can prove the following proposition

(30) $0_{G_1} =$ the zero of G_1.

The trivial multiplicative loop$_0$ a mutiplicative loop with zero structure is defined by:

(Def.21) the trivial multiplicative loop$_0$ $= \langle \mathbb{R}, \cdot_{\mathbb{R}}, 1, 0 \rangle$.

One can prove the following three propositions:

(31) The trivial multiplicative loop$_0$ $= \langle \mathbb{R}, \cdot_{\mathbb{R}}, 1, 0 \rangle$.

(32) For all real numbers q, p such that $q \neq 0$ there exists a real number y such that $p = q \cdot y$.

(33) For all real numbers q, p such that $q \neq 0$ there exists a real number y such that $p = y \cdot q$.

A mutiplicative loop with zero structure is called a multiplicative loop with zero if:

(Def.22) (i) $0_{\rm it} \neq 1_{\rm it}$,

(ii) for every element a of it holds $a \cdot (1_{\rm it}) = a$,

(iii) for every element a of it holds $(1_{\rm it}) \cdot a = a$,

(iv) for all elements a, b of it such that $a \neq 0_{\rm it}$ there exists an element x of it such that $a \cdot x = b$,

(v) for all elements a, b of it such that $a \neq 0_{\rm it}$ there exists an element x of it such that $x \cdot a = b$,

(vi) for all elements a, x, y of it such that $a \neq 0_{\rm it}$ holds if $a \cdot x = a \cdot y$, then $x = y$,

(vii) for all elements a, x, y of it such that $a \neq 0_{\rm it}$ holds if $x \cdot a = y \cdot a$, then $x = y$,

(viii) for every element a of it holds $a \cdot 0_{\rm it} = 0_{\rm it}$,

(ix) for every element a of it holds $0_{\rm it} \cdot a = 0_{\rm it}$.

The following proposition is true

(34) Let L be a mutiplicative loop with zero structure. Then L is a multiplicative loop with zero if and only if the following conditions are satisfied:

(i) $0_L \neq 1_L$,

(ii) for every element a of L holds $a \cdot (1_L) = a$,

(iii) for every element a of L holds $(1_L) \cdot a = a$,

(iv) for all elements a, b of L such that $a \neq 0_L$ there exists an element x of L such that $a \cdot x = b$,

(v) for all elements a, b of L such that $a \neq 0_L$ there exists an element x of L such that $x \cdot a = b$,

(vi) for all elements a, x, y of L such that $a \neq 0_L$ holds if $a \cdot x = a \cdot y$, then $x = y$,

(vii) for all elements a, x, y of L such that $a \neq 0_L$ holds if $x \cdot a = y \cdot a$, then $x = y$,

(viii) for every element a of L holds $a \cdot 0_L = 0_L$,

(ix) for every element a of L holds $0_L \cdot a = 0_L$.

Let us note that it makes sense to consider the following constant. Then the trivial multiplicative loop_0 is a multiplicative loop with zero.

A multiplicative loop with zero is called a multiplicative group with zero if:

(Def.23) for all elements a, b, c of it holds $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

One can prove the following proposition

(35) For every multiplicative loop L with zero holds L is a multiplicative group with zero if and only if for all elements a, b, c of L holds $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

We follow a convention: L denotes a mutiplicative loop with zero structure and a, b, c, x denote elements of L. One can prove the following proposition

(36) L is a multiplicative group with zero if and only if the following conditions are satisfied:

(i) $0_L \neq 1_L$,

(ii) for every a holds $a \cdot (1_L) = a$,

(iii) for every a such that $a \neq 0_L$ there exists x such that $a \cdot x = 1_L$,

(iv) for all a, b, c holds $(a \cdot b) \cdot c = a \cdot (b \cdot c)$,

(v) for every a holds $a \cdot 0_L = 0_L$,

(vi) for every a holds $0_L \cdot a = 0_L$.

Let us note that it makes sense to consider the following constant. Then the trivial multiplicative loop_0 is a multiplicative group with zero.

A multiplicative group with zero is said to be a multiplicative commutative group with zero if:

(Def.24) for all elements a, b of it holds $a \cdot b = b \cdot a$.

We now state two propositions:

(37) For every multiplicative group L with zero holds L is a multiplicative commutative group with zero if and only if for all elements a, b of L holds $a \cdot b = b \cdot a$.

(38) L is a multiplicative commutative group with zero if and only if the following conditions are satisfied:
  (i) $0_L \neq 1_L$,
  (ii) for every a holds $a \cdot (1_L) = a$,
  (iii) for every a such that $a \neq 0_L$ there exists x such that $a \cdot x = 1_L$,
  (iv) for all a, b, c holds $(a \cdot b) \cdot c = a \cdot (b \cdot c)$,
  (v) for every a holds $a \cdot 0_L = 0_L$,
  (vi) for every a holds $0_L \cdot a = 0_L$,
  (vii) for all a, b holds $a \cdot b = b \cdot a$.

Let L be a multiplicative group with zero, and let a be an element of L. Let us assume that $a \neq 0_L$. The functor a^{-1} yielding an element of L is defined as follows:

(Def.25) $a \cdot (a^{-1}) = 1_L$.

We now state the proposition

(39) For every multiplicative group L with zero and for every element a of L such that $a \neq 0_L$ holds $a \cdot a^{-1} = 1_L$.

In the sequel G will be a multiplicative group with zero and a, b will be elements of G. One can prove the following proposition

(40) If $a \neq 0_G$, then $a \cdot a^{-1} = 1_G$ and $a^{-1} \cdot a = 1_G$.

Let us consider G, a, b. Let us assume that $b \neq 0_G$. The functor $\frac{a}{b}$ yields an element of G and is defined by:

(Def.26) $\frac{a}{b} = a \cdot b^{-1}$.

We now state the proposition

(41) If $b \neq 0_G$, then $\frac{a}{b} = a \cdot b^{-1}$.

References

[1] Czesław Byliński. Binary operations. *Formalized Mathematics*, 1(**1**):175–180, 1990.

[2] Krzysztof Hryniewiecki. Basic properties of real numbers. *Formalized Mathematics*, 1(**1**):35–40, 1990.

[3] Michał Muzalewski. Midpoint algebras. *Formalized Mathematics*, 1(**3**):483–488, 1990.

[4] Wanda Szmielew. *From Affine to Euclidean Geometry.* Volume 27, PWN – D.Reidel Publ. Co., Warszawa – Dordrecht, 1983.

Received July 10, 1990