JOURNAL OF FORMALIZED MATHEMATICS
Volume 2, Released 1990, Published 2003
Inst. of Computer Science, Univ. of Białystok

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 [5]. 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.

WWW: http://mizar.org/JFM/Vol2/algstr_1.html

The articles [6], [9], [7], [1], [2], [8], [4], and [3] provide the notation and terminology for this paper.

We use the following convention: L denotes a non empty loop structure and a, b, c, x denote elements of L.

One can prove the following propositions:

(1) Suppose 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 $(a+b)+c = a+(b+c)$. If $a+b = 0_L$, then $b+a = 0_L$.

(2) 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 $(a+b)+c = a+(b+c)$, then $0_L+a = a+0_L$.

(3) Suppose 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 given a. Then there exists x such that $x+a = 0_L$.

Let x be a set. The functor Extract(x) yields an element of $\{x\}$ and is defined as follows:

(Def. 3)[1] Extract(x) $= x$.

The strict loop structure the trivial loop is defined as follows:

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

[1] The definitions (Def. 1) and (Def. 2) have been removed.

(Def. 4) The trivial loop $= \langle \{\emptyset\}, \mathrm{op}_2, \mathrm{Extract}(\emptyset) \rangle$.

Let us observe that the trivial loop is non empty.
One can prove the following propositions:

(5)[2] For all elements a, b of the trivial loop holds $a = b$.

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

Let I_1 be a non empty loop structure. We say that I_1 is left zeroed if and only if:

(Def. 5) For every element a of I_1 holds $0_{(I_1)} + a = a$.

Let L be a non empty loop structure. We say that L is add-left-cancelable if and only if:

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

We say that L is add-right-cancelable if and only if:

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

We say that L is add-left-invertible if and only if:

(Def. 8) For all elements a, b of L there exists an element x of L such that $x + a = b$.

We say that L is add-right-invertible if and only if:

(Def. 9) For all elements a, b of L there exists an element x of L such that $a + x = b$.

Let I_1 be a non empty loop structure. We say that I_1 is loop-like if and only if:

(Def. 10) I_1 is add-left-cancelable, add-right-cancelable, add-left-invertible, and add-right-invertible.

Let us observe that every non empty loop structure which is loop-like is also add-left-cancelable, add-right-cancelable, add-left-invertible, and add-right-invertible and every non empty loop structure which is add-left-cancelable, add-right-cancelable, add-left-invertible, and add-right-invertible is also loop-like.
Next we state the proposition

(7) Let L be a non empty loop structure. Then L is loop-like if and only if the following conditions are satisfied:

(i) for all elements a, b of L there exists an element x of L such that $a + x = b$,

(ii) for all elements a, b of L there exists an element x of L such that $x + a = b$,

(iii) for all elements a, x, y of L such that $a + x = a + y$ holds $x = y$, and

(iv) for all elements a, x, y of L such that $x + a = y + a$ holds $x = y$.

Let us mention that the trivial loop is add-associative, loop-like, right zeroed, and left zeroed.
Let us observe that there exists a non empty loop structure which is strict, left zeroed, right zeroed, and loop-like.
A loop is a left zeroed right zeroed loop-like non empty loop structure.
Let us mention that there exists a loop which is strict and add-associative.
A group is an add-associative loop.
One can check that every non empty loop structure which is loop-like is also right complementable and every non empty loop structure which is add-associative, right zeroed, and right complementable is also left zeroed and loop-like.
We now state the proposition

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

(9)[3] L is a 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 $a + x = 0_L$, and

(iii) for all a, b, c holds $(a+b)+c = a+(b+c)$.

One can verify that the trivial loop is Abelian.
One can verify that there exists a group which is strict and Abelian.
Next we state the proposition

(11)[4] 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 $(a+b)+c = a+(b+c)$, and

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

The strict multiplicative loop structure the trivial multiplicative loop is defined as follows:

(Def. 11) The trivial multiplicative loop $= \langle \{\emptyset\}, \mathrm{op}_2, \mathrm{Extract}(\emptyset) \rangle$.

Let us observe that the trivial multiplicative loop is non empty.
The following two propositions are true:

(18)[5] For all elements a, b of the trivial multiplicative loop holds $a = b$.

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

Let I_1 be a non empty multiplicative loop structure. We say that I_1 is invertible if and only if the conditions (Def. 12) are satisfied.

(Def. 12)(i) For all elements a, b of I_1 there exists an element x of I_1 such that $a \cdot x = b$, and

(ii) for all elements a, b of I_1 there exists an element x of I_1 such that $x \cdot a = b$.

We say that I_1 is cancelable if and only if the conditions (Def. 13) are satisfied.

(Def. 13)(i) For all elements a, x, y of I_1 such that $a \cdot x = a \cdot y$ holds $x = y$, and

(ii) for all elements a, x, y of I_1 such that $x \cdot a = y \cdot a$ holds $x = y$.

Let us note that there exists a non empty multiplicative loop structure which is strict, well unital, invertible, and cancelable.

A multiplicative loop is a well unital invertible cancelable non empty multiplicative loop structure.

Let us note that the trivial multiplicative loop is well unital, invertible, and cancelable.
Let us observe that there exists a multiplicative loop which is strict and associative.
A multiplicative group is an associative multiplicative loop.
We adopt the following convention: L denotes a non empty multiplicative loop structure and a, b, c, x denote elements of L.
One can prove the following proposition

(22)[6] L is a multiplicative group if and only if for every a holds $a \cdot \mathbf{1}_L = a$ and for every a there exists x such that $a \cdot x = \mathbf{1}_L$ and for all a, b, c holds $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

Let us note that the trivial multiplicative loop is associative.
Let us note that there exists a multiplicative group which is strict and commutative.
One can prove the following proposition

[3] The proposition (8) has been removed.
[4] The proposition (10) has been removed.
[5] The propositions (12)–(17) have been removed.
[6] The propositions (20) and (21) have been removed.

(24)[7] L is a commutative multiplicative group if and only if for every a holds $a \cdot \mathbf{1}_L = a$ and for every a there exists x such that $a \cdot x = \mathbf{1}_L$ and for all a, b, c holds $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ and for all a, b holds $a \cdot b = b \cdot a$.

Let L be an invertible cancelable non empty multiplicative loop structure and let a be an element of L. The functor a^{-1} yielding an element of L is defined as follows:

(Def. 16)[8] $a \cdot a^{-1} = \mathbf{1}_L$.

In the sequel G denotes a multiplicative group and a denotes an element of G.
One can prove the following proposition

(26)[9] $a \cdot a^{-1} = \mathbf{1}_G$ and $a^{-1} \cdot a = \mathbf{1}_G$.

Let L be an invertible cancelable non empty multiplicative loop structure and let a, b be elements of L. The functor $\frac{a}{b}$ yielding an element of L is defined by:

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

The strict multiplicative loop with zero structure the trivial multiplicative loop$_0$is defined by:

(Def. 21)[10] The trivial multiplicative loop$_0$= $\langle \mathbb{R}, \cdot_{\mathbb{R}}, 1, 0 \rangle$.

One can verify that the trivial multiplicative loop$_0$is non empty.
The following two propositions are true:

(32)[11] 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 $p = y \cdot q$.

Let I_1 be a non empty multiplicative loop with zero structure. We say that I_1 is almost invertible if and only if the conditions (Def. 22) are satisfied.

(Def. 22)(i) For all elements a, b of I_1 such that $a \neq 0_{(I_1)}$ there exists an element x of I_1 such that $a \cdot x = b$, and

(ii) for all elements a, b of I_1 such that $a \neq 0_{(I_1)}$ there exists an element x of I_1 such that $x \cdot a = b$.

We say that I_1 is almost cancelable if and only if the conditions (Def. 23) are satisfied.

(Def. 23)(i) For all elements a, x, y of I_1 such that $a \neq 0_{(I_1)}$ holds if $a \cdot x = a \cdot y$, then $x = y$, and

(ii) for all elements a, x, y of I_1 such that $a \neq 0_{(I_1)}$ holds if $x \cdot a = y \cdot a$, then $x = y$.

Let I_1 be a non empty multiplicative loop with zero structure. We say that I_1 is multiplicative loop with zero-like if and only if the conditions (Def. 24) are satisfied.

(Def. 24)(i) I_1 is almost invertible and almost cancelable,

(ii) for every element a of I_1 holds $a \cdot 0_{(I_1)} = 0_{(I_1)}$, and

(iii) for every element a of I_1 holds $0_{(I_1)} \cdot a = 0_{(I_1)}$.

One can prove the following proposition

[7] The proposition (23) has been removed.
[8] The definitions (Def. 14) and (Def. 15) have been removed.
[9] The proposition (25) has been removed.
[10] The definitions (Def. 18)–(Def. 20) have been removed.
[11] The propositions (27)–(31) have been removed.

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

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

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

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

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

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

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

Let us note that every non empty multiplicative loop with zero structure which is multiplicative loop with zero-like is also almost invertible and almost cancelable.

Let us note that there exists a non empty multiplicative loop with zero structure which is strict, well unital, multiplicative loop with zero-like, and non degenerated.

A multiplicative loop with zero is a well unital non degenerated multiplicative loop with zero-like non empty multiplicative loop with zero structure.

One can check that the trivial multiplicative loop$_0$is well unital and multiplicative loop with zero-like.

Let us observe that there exists a multiplicative loop with zero which is strict, associative, and non degenerated.

A multiplicative group with zero is an associative non degenerated multiplicative loop with zero.

We adopt the following rules: L denotes a non empty multiplicative loop with zero structure and a, b, c, x denote elements of L.

Next we state the proposition

(36)[12] L is a multiplicative group with zero if and only if the following conditions are satisfied:

(i) $0_L \neq \mathbf{1}_L$,

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

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

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

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

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

One can check that the trivial multiplicative loop$_0$is associative.

Let us note that there exists a multiplicative group with zero which is strict and commutative.

The following proposition is true

(38)[13] L is a commutative multiplicative group with zero if and only if the following conditions are satisfied:

$0_L \neq \mathbf{1}_L$ and for every a holds $a \cdot \mathbf{1}_L = a$ and for every a such that $a \neq 0_L$ there exists x such that $a \cdot x = \mathbf{1}_L$ and for all a, b, c holds $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ and for every a holds $a \cdot 0_L = 0_L$ and for every a holds $0_L \cdot a = 0_L$ and for all a, b holds $a \cdot b = b \cdot a$.

Let L be an almost invertible almost cancelable non empty multiplicative loop with zero structure 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) $a \cdot a^{-1} = \mathbf{1}_L$.

In the sequel G is an associative almost invertible almost cancelable well unital non empty multiplicative loop with zero structure and a is an element of G.

We now state the proposition

[12] The proposition (35) has been removed.

[13] The proposition (37) has been removed.

(40)[14] If $a \neq 0_G$, then $a \cdot a^{-1} = \mathbf{1}_G$ and $a^{-1} \cdot a = \mathbf{1}_G$.

Let L be an almost invertible almost cancelable non empty multiplicative loop with zero structure and let a, b be elements of L. The functor $\frac{a}{b}$ yields an element of L and is defined as follows:

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

REFERENCES

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

[2] 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`.

[3] Michał Muzalewski. Midpoint algebras. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/midsp_1.html`.

[4] 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`.

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

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

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

[8] Wojciech A. Trybulec. Vectors in real linear space. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/rlvect_1.html`.

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

Received July 10, 1990

Published January 2, 2004

[14] The proposition (39) has been removed.