FORMALIZED MATHEMATICS
Vol.2, No.1, January–February 1991
Université Catholique de Louvain

From Double Loops to Fields

Wojciech Skaba
Toruń University

Michał Muzalewski[1]
Warsaw University
Białystok

Summary. This paper contains the second part of the set of articles concerning the theory of algebraic structures, based on the [9], pp. 9-12 (pages 4-6 of the English edition).

First the basic structure $\langle F, +, \cdot, 1, 0\rangle$ is defined. Following it the consecutive structures are contemplated in detail, including double loop, left quasi-field, right quasi-field, double sided quasi-field, skew field and field. These structures are created by gradually augmenting the basic structure with new axioms of commutativity, associativity, distributivity etc. Each part of the article begins with the set of auxiliary theorems related to the structure under consideration that are necessary for the existence proof of each defined mode. Next the mode and proof of its existence is included. If the current set of axioms may be replaced with a different and equivalent one, the appropriate proof is performed following the definition of that mode. With the introduction of double loop the "−" function is defined. Some interesting features of this function are also included.

MML Identifier: ALGSTR_2.

The terminology and notation used here have been introduced in the following articles: [11], [10], [3], [4], [1], [2], [6], [5], [7], and [8]. We consider double loop structures which are systems

$\langle$a carrier, an addition, a multiplication, a unity, a zero$\rangle$,

where the carrier is a non-empty set, the addition is a binary operation on the carrier, 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 double loop structure and L will be a double 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 $a + b$ yields an element of G_1 and is defined by:

[1]Supported by RPBP.III-24.B5

ISSN 0777–4028

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

Let us consider G_1, a, b. The functor $a \cdot b$ yields an element of G_1 and is defined by:

(Def.2) $a \cdot b =$ (the multiplication of G_1)(a, b).

One can prove the following propositions:

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

(2) $a \cdot b =$ (the multiplication 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.3) $0_{G_1} =$ the zero of G_1.

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

(Def.4) $1_{G_1} =$ the unity of G_1.

The following two propositions are true:

(3) $0_{G_1} =$ the zero of G_1.

(4) $1_{G_1} =$ the unity of G_1.

The double loop structure $\mathrm{loop}_{\mathbb{R}}$ is defined by:

(Def.5) $\mathrm{loop}_{\mathbb{R}} = \langle \mathbb{R}, +_{\mathbb{R}}, \cdot_{\mathbb{R}}, 1, 0 \rangle$.

One can prove the following three propositions:

(5) $\mathrm{loop}_{\mathbb{R}} = \langle \mathbb{R}, +_{\mathbb{R}}, \cdot_{\mathbb{R}}, 1, 0 \rangle$.

(6) For every real numbers q, p there exists a real number y such that $p = q + y$.

(7) For every real numbers q, p there exists a real number y such that $p = y + q$.

A double loop structure is said to be a double loop if:

(Def.6) (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 $x = y$,

(vii) $0_{\mathrm{it}} \neq 1_{\mathrm{it}}$,

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

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

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

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

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

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

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

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

Let us note that it makes sense to consider the following constant. Then $\mathrm{loop}_{\mathbb{R}}$ is a double loop.

Let L be a double loop, and let a be an element of L. The functor $-a$ yielding an element of L is defined as follows:

(Def.7) $a + (-a) = 0_L$.

Next we state the proposition

(9)[2] For every double loop L and for every element a of L holds $a + (-a) = 0_L$.

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

(Def.8) $a - b = a + (-b)$.

We now state the proposition

(10) For every double loop L and for all elements a, b of L holds $a - b = a + (-b)$.

A double loop is said to be a left quasi-field if:

(Def.9) (i) for all elements a, b, c of it holds $(a + b) + c = a + (b + c)$,

(ii) for all elements a, b of it holds $a + b = b + a$,

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

In the sequel a, b, c, x, y are elements of L. The following proposition is true

(12)[3] L is a left quasi-field 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 $a + b = b + a$,

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

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

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

(viii) for all a, b such that $a \neq 0_L$ there exists x such that $a \cdot x = b$,

(ix) for all a, b such that $a \neq 0_L$ there exists x such that $x \cdot a = b$,

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

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

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

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

(xiv) for all a, b, c holds $a \cdot (b + c) = a \cdot b + a \cdot c$.

[2]The proposition (8) was either repeated or obvious.

[3]The proposition (11) was either repeated or obvious.

We follow the rules: G will be a left quasi-field and a, b, x, y will be elements of G. We now state several propositions:

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

(14) $a \cdot (-b) = -a \cdot b$.

(15) $-(-a) = a$.

(16) $(-1_G) \cdot (-1_G) = 1_G$.

(17) $a \cdot (x - y) = a \cdot x - a \cdot y$.

A double loop is called a right quasi-field if:

(Def.10) (i) for all elements a, b, c of it holds $(a + b) + c = a + (b + c)$,
(ii) for all elements a, b of it holds $a + b = b + a$,
(iii) for all elements a, b, c of it holds $(b + c) \cdot a = b \cdot a + c \cdot a$.

In the sequel a, b, c, x, y are elements of L. One can prove the following proposition

(19)[4] L is a right quasi-field 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 $a + b = b + a$,
(v) $0_L \neq 1_L$,
(vi) for every a holds $a \cdot (1_L) = a$,
(vii) for every a holds $(1_L) \cdot a = a$,
(viii) for all a, b such that $a \neq 0_L$ there exists x such that $a \cdot x = b$,
(ix) for all a, b such that $a \neq 0_L$ there exists x such that $x \cdot a = b$,
(x) for all a, x, y such that $a \neq 0_L$ holds if $a \cdot x = a \cdot y$, then $x = y$,
(xi) for all a, x, y such that $a \neq 0_L$ holds if $x \cdot a = y \cdot a$, then $x = y$,
(xii) for every a holds $a \cdot 0_L = 0_L$,
(xiii) for every a holds $0_L \cdot a = 0_L$,
(xiv) for all a, b, c holds $(b + c) \cdot a = b \cdot a + c \cdot a$.

We adopt the following rules: G will be a right quasi-field and a, b, x, y will be elements of G. We now state several propositions:

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

(21) $(-b) \cdot a = -b \cdot a$.

(22) $-(-a) = a$.

(23) $(-1_G) \cdot (-1_G) = 1_G$.

(24) $(x - y) \cdot a = x \cdot a - y \cdot a$.

In the sequel a, b, c, x, y will denote elements of L. A double loop is called a double sided quasi-field if:

(Def.11) (i) for all elements a, b, c of it holds $(a + b) + c = a + (b + c)$,
(ii) for all elements a, b of it holds $a + b = b + a$,
(iii) for all elements a, b, c of it holds $a \cdot (b + c) = a \cdot b + a \cdot c$,
(iv) for all elements a, b, c of it holds $(b + c) \cdot a = b \cdot a + c \cdot a$.

[4]The proposition (18) was either repeated or obvious.

Let us note that it makes sense to consider the following constant. Then $\mathrm{loop}_{\mathbb{R}}$ is a double sided quasi-field.

The following propositions are true:

(26)[5] L is a double sided quasi-field 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 $a + b = b + a$,
(v) $0_L \neq 1_L$,
(vi) for every a holds $a \cdot (1_L) = a$,
(vii) for every a holds $(1_L) \cdot a = a$,
(viii) for all a, b such that $a \neq 0_L$ there exists x such that $a \cdot x = b$,
(ix) for all a, b such that $a \neq 0_L$ there exists x such that $x \cdot a = b$,
(x) for all a, x, y such that $a \neq 0_L$ holds if $a \cdot x = a \cdot y$, then $x = y$,
(xi) for all a, x, y such that $a \neq 0_L$ holds if $x \cdot a = y \cdot a$, then $x = y$,
(xii) for every a holds $a \cdot 0_L = 0_L$,
(xiii) for every a holds $0_L \cdot a = 0_L$,
(xiv) for all a, b, c holds $a \cdot (b + c) = a \cdot b + a \cdot c$,
(xv) for all a, b, c holds $(b + c) \cdot a = b \cdot a + c \cdot a$.

(27) For every double sided quasi-field L holds L is a left quasi-field.

(28) For every double sided quasi-field L holds L is a right quasi-field.

We adopt the following rules: G will be a double sided quasi-field and a, b, x, y will be elements of G. Next we state two propositions:

(29) $a \cdot (-b) = -a \cdot b$ and $(-b) \cdot a = -b \cdot a$.

(30) $a \cdot (x - y) = a \cdot x - a \cdot y$ and $(x - y) \cdot a = x \cdot a - y \cdot a$.

We see that the double sided quasi-field is a left quasi-field.

In the sequel a, b, c, x will be elements of L. A double sided quasi-field is called a skew field if:

(Def.12) for all elements a, b, c of it holds $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

Let us note that it makes sense to consider the following constant. Then $\mathrm{loop}_{\mathbb{R}}$ is a skew field.

The following proposition is true

(32)[6] L is a skew field 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 $a + b = b + a$,
(v) $0_L \neq 1_L$,
(vi) for every a holds $a \cdot (1_L) = a$,

[5]The proposition (25) was either repeated or obvious.
[6]The proposition (31) was either repeated or obvious.

(vii) for every a such that $a \neq 0_L$ there exists x such that $a \cdot x = 1_L$,
(viii) for every a holds $a \cdot 0_L = 0_L$,
(ix) for every a holds $0_L \cdot a = 0_L$,
(x) for all a, b, c holds $(a \cdot b) \cdot c = a \cdot (b \cdot c)$,
(xi) for all a, b, c holds $a \cdot (b + c) = a \cdot b + a \cdot c$,
(xii) for all a, b, c holds $(b + c) \cdot a = b \cdot a + c \cdot a$.

A skew field is said to be a field if:

(Def.13) for all elements a, b of it holds $a \cdot b = b \cdot a$.

Let us note that it makes sense to consider the following constant. Then $\mathrm{loop}_{\mathbb{R}}$ is a field.

The following proposition is true

(34)[7] L is a field 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 $a + b = b + a$,
(v) $0_L \neq 1_L$,
(vi) for every a holds $a \cdot (1_L) = a$,
(vii) for every a such that $a \neq 0_L$ there exists x such that $a \cdot x = 1_L$,
(viii) for every a holds $a \cdot 0_L = 0_L$,
(ix) for all a, b, c holds $(a \cdot b) \cdot c = a \cdot (b \cdot c)$,
(x) for all a, b, c holds $a \cdot (b + c) = a \cdot b + a \cdot c$,
(xi) for all a, b holds $a \cdot b = b \cdot a$.

References

[1] Czesław Byliński. Basic functions and operations on functions. *Formalized Mathematics*, 1(**1**):245–254, 1990.
[2] Czesław Byliński. Binary operations. *Formalized Mathematics*, 1(**1**):175–180, 1990.
[3] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.
[4] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.
[5] Krzysztof Hryniewiecki. Basic properties of real numbers. *Formalized Mathematics*, 1(**1**):35–40, 1990.
[6] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Formalized Mathematics*, 1(**2**):335–342, 1990.
[7] Michał Muzalewski. Midpoint algebras. *Formalized Mathematics*, 1(**3**):483–488, 1990.
[8] Michał Muzalewski and Wojciech Skaba. From loops to abelian multiplicative groups with zero. *Formalized Mathematics*, 1(**5**):833–840, 1990.
[9] Wanda Szmielew. *From Affine to Euclidean Geometry.* Volume 27, PWN – D.Reidel Publ. Co., Warszawa – Dordrecht, 1983.
[10] Andrzej Trybulec. Enumerated sets. *Formalized Mathematics*, 1(**1**):25–34, 1990.

[7]The proposition (33) was either repeated or obvious.

[11] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.

Received September 27, 1990