JOURNAL OF FORMALIZED MATHEMATICS
Volume 1, Released 1989, Published 2003
Inst. of Computer Science, Univ. of Białystok

Abelian Groups, Fields and Vector Spaces[1]

Eugeniusz Kusak
Warsaw University
Białystok

Wojciech Leończuk
Warsaw University
Białystok

Michał Muzalewski
Warsaw University
Białystok

Summary. This text includes definitions of the Abelian group, field and vector space over a field and some elementary theorems about them.

MML Identifier: VECTSP_1.

WWW: http://mizar.org/JFM/Vol1/vectsp_1.html

The articles [4], [8], [6], [2], [3], [1], [5], and [7] provide the notation and terminology for this paper.

In this paper G_1 is a non empty loop structure.

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

(Def. 4)[1] For all elements x, y of $\mathbb{R}$ holds $+_{\mathbb{R}}(x, y) = x + y$.

The unary operation $-_{\mathbb{R}}$ on $\mathbb{R}$ is defined as follows:

(Def. 5) For every element x of $\mathbb{R}$ holds $-_{\mathbb{R}}(x) = -x$.

The strict loop structure $\mathbb{R}_{\mathrm{G}}$ is defined as follows:

(Def. 6) $\mathbb{R}_{\mathrm{G}} = \langle \mathbb{R}, +_{\mathbb{R}}, 0 \rangle$.

One can verify that $\mathbb{R}_{\mathrm{G}}$ is non empty.

Let us note that $\mathbb{R}_{\mathrm{G}}$ is Abelian, add-associative, right zeroed, and right complementable.

One can prove the following proposition

(6)[2] For all elements x, y, z of $\mathbb{R}_{\mathrm{G}}$ holds $x + y = y + x$ and $(x + y) + z = x + (y + z)$ and $x + 0_{\mathbb{R}_{\mathrm{G}}} = x$ and $x + -x = 0_{\mathbb{R}_{\mathrm{G}}}$.

Let us note that there exists a non empty loop structure which is strict, add-associative, right zeroed, right complementable, and Abelian.

An Abelian group is an add-associative right zeroed right complementable Abelian non empty loop structure.

Next we state the proposition

(7) For all elements x, y, z of G_1 holds $x + y = y + x$ and $(x + y) + z = x + (y + z)$ and $x + 0_{(G_1)} = x$ and there exists an element x' of G_1 such that $x + x' = 0_{(G_1)}$ if and only if G_1 is an Abelian group.

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

[1] The definitions (Def. 1)–(Def. 3) have been removed.

[2] The propositions (1)–(5) have been removed.

We consider groupoids as extensions of 1-sorted structure as systems
⟨ a carrier, a multiplication ⟩,
where the carrier is a set and the multiplication is a binary operation on the carrier.

One can check that there exists a groupoid which is non empty and strict.

We introduce multiplicative loop structures which are extensions of groupoid and are systems
⟨ a carrier, a multiplication, a unity ⟩,
where the carrier is a set, the multiplication is a binary operation on the carrier, and the unity is an element of the carrier.

Let us observe that there exists a multiplicative loop structure which is non empty and strict.

Let F_1 be a multiplicative loop structure. The functor $\mathbf{1}_{(F_1)}$ yielding an element of F_1 is defined as follows:

(Def. 9)[3] $\mathbf{1}_{(F_1)} =$ the unity of F_1.

We introduce multiplicative loop with zero structures which are extensions of multiplicative loop structure and zero structure and are systems
⟨ a carrier, a multiplication, a unity, a zero ⟩,
where the carrier is a 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.

One can check that there exists a multiplicative loop with zero structure which is non empty and strict.

We introduce double loop structures which are extensions of loop structure and multiplicative loop with zero structure and are systems
⟨ a carrier, an addition, a multiplication, a unity, a zero ⟩,
where the carrier is a set, the addition and the multiplication are binary operations on the carrier, and the unity and the zero are elements of the carrier.

Let us mention that there exists a double loop structure which is non empty and strict.

Let F_1 be a non empty groupoid and let x, y be elements of F_1. The functor $x \cdot y$ yielding an element of F_1 is defined by:

(Def. 10) $x \cdot y = (\text{the multiplication of } F_1)(x, y)$.

Let I_1 be a non empty double loop structure. We say that I_1 is right distributive if and only if:

(Def. 11) For all elements a, b, c of I_1 holds $a \cdot (b + c) = a \cdot b + a \cdot c$.

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

(Def. 12) For all elements a, b, c of I_1 holds $(b + c) \cdot a = b \cdot a + c \cdot a$.

Let I_1 be a non empty multiplicative loop structure. We say that I_1 is right unital if and only if:

(Def. 13) For every element x of I_1 holds $x \cdot \mathbf{1}_{(I_1)} = x$.

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

(Def. 14) For all elements x, y of $\mathbb{R}$ holds $\cdot_{\mathbb{R}}(x, y) = x \cdot y$.

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

(Def. 15) $\mathbb{R}_{\mathrm{F}} = \langle \mathbb{R}, +_{\mathbb{R}}, \cdot_{\mathbb{R}}, 1, 0 \rangle$.

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

(Def. 16) For all elements x, y, z of I_1 holds $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.

We say that I_1 is commutative if and only if:

(Def. 17) For all elements x, y of I_1 holds $x \cdot y = y \cdot x$.

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

[3] The definitions (Def. 7) and (Def. 8) have been removed.

(Def. 18) For all elements x, y, z of I_1 holds $x \cdot (y+z) = x \cdot y + x \cdot z$ and $(y+z) \cdot x = y \cdot x + z \cdot x$.

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

(Def. 19) For every element x of I_1 holds $\mathbf{1}_{(I_1)} \cdot x = x$.

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

(Def. 20) For every element x of I_1 such that $x \neq 0_{(I_1)}$ there exists an element y of I_1 such that $x \cdot y = \mathbf{1}_{(I_1)}$.

Let I_1 be a multiplicative loop with zero structure. We say that I_1 is degenerated if and only if:

(Def. 21) $0_{(I_1)} = \mathbf{1}_{(I_1)}$.

Let us observe that $\mathbb{R}_{\rm F}$ is non empty.

One can verify that $\mathbb{R}_{\rm F}$ is add-associative, right zeroed, right complementable, Abelian, commutative, associative, left unital, right unital, distributive, field-like, and non degenerated.

Let us observe that every non empty double loop structure which is distributive is also left distributive and right distributive and every non empty double loop structure which is left distributive and right distributive is also distributive.

One can verify that there exists a non empty double loop structure which is add-associative, right zeroed, right complementable, Abelian, commutative, associative, left unital, right unital, distributive, field-like, non degenerated, and strict.

Let us note that there exists a non empty groupoid which is commutative and associative.

A field is an add-associative right zeroed right complementable Abelian commutative associative left unital distributive field-like non degenerated non empty double loop structure.

Next we state two propositions:

(21)[4] Let x, y, z be elements of $\mathbb{R}_{\rm F}$. Then $x+y = y+x$ and $(x+y)+z = x+(y+z)$ and $x+0_{\mathbb{R}_{\rm F}} = x$ and $x+-x = 0_{\mathbb{R}_{\rm F}}$ and $x \cdot y = y \cdot x$ and $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ and $\mathbf{1}_{\mathbb{R}_{\rm F}} \cdot x = x$ and if $x \neq 0_{\mathbb{R}_{\rm F}}$, then there exists an element y of $\mathbb{R}_{\rm F}$ such that $x \cdot y = \mathbf{1}_{\mathbb{R}_{\rm F}}$ and $x \cdot (y+z) = x \cdot y + x \cdot z$ and $(y+z) \cdot x = y \cdot x + z \cdot x$.

(22) Let F_1 be a non empty double loop structure. Then the following statements are equivalent

(i) for all elements x, y, z of F_1 holds if $x \neq 0_{(F_1)}$, then there exists an element y of F_1 such that $x \cdot y = \mathbf{1}_{(F_1)}$ and $x \cdot (y+z) = x \cdot y + x \cdot z$ and $(y+z) \cdot x = y \cdot x + z \cdot x$,

(ii) F_1 is a distributive field-like non empty double loop structure.

Let F_1 be a commutative non empty groupoid and let x, y be elements of F_1. Let us observe that the functor $x \cdot y$ is commutative.

The following proposition is true

(33)[5] Let F be an associative commutative left unital distributive field-like non empty double loop structure and x, y, z be elements of F. If $x \neq 0_F$ and $x \cdot y = x \cdot z$, then $y = z$.

Let F be an associative commutative left unital distributive field-like non empty double loop structure and let x be an element of F. Let us assume that $x \neq 0_F$. The functor x^{-1} yields an element of F and is defined by:

(Def. 22) $x \cdot x^{-1} = \mathbf{1}_F$.

Let F be an associative commutative left unital distributive field-like non empty double loop structure and let x, y be elements of F. The functor $\frac{x}{y}$ yields an element of F and is defined as follows:

(Def. 23) $\frac{x}{y} = x \cdot y^{-1}$.

[4] The propositions (8)–(20) have been removed.

[5] The propositions (23)–(32) have been removed.

Next we state several propositions:

(36)[6] Let F be an add-associative right zeroed right complementable right distributive non empty double loop structure and x be an element of F. Then $x \cdot 0_F = 0_F$.

(39)[7] Let F be an add-associative right zeroed right complementable left distributive non empty double loop structure and x be an element of F. Then $0_F \cdot x = 0_F$.

(40) Let F be an add-associative right zeroed right complementable right distributive non empty double loop structure and x, y be elements of F. Then $x \cdot -y = -x \cdot y$.

(41) Let F be an add-associative right zeroed right complementable left distributive non empty double loop structure and x, y be elements of F. Then $(-x) \cdot y = -x \cdot y$.

(42) Let F be an add-associative right zeroed right complementable distributive non empty double loop structure and x, y be elements of F. Then $(-x) \cdot -y = x \cdot y$.

(43) Let F be an add-associative right zeroed right complementable right distributive non empty double loop structure and x, y, z be elements of F. Then $x \cdot (y - z) = x \cdot y - x \cdot z$.

(44) Let F be an add-associative right zeroed right complementable associative commutative left unital field-like distributive non empty double loop structure and x, y be elements of F. Then $x \cdot y = 0_F$ if and only if $x = 0_F$ or $y = 0_F$.

(45) Let K be an add-associative right zeroed right complementable left distributive non empty double loop structure and a, b, c be elements of K. Then $(a - b) \cdot c = a \cdot c - b \cdot c$.

Let F be a 1-sorted structure. We introduce vector space structures over F which are extensions of loop structure and are systems

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

where the carrier is a set, the addition is a binary operation on the carrier, the zero is an element of the carrier, and the left multiplication is a function from $[:$the carrier of F, the carrier$:]$ into the carrier.

Let F be a 1-sorted structure. Observe that there exists a vector space structure over F which is non empty and strict.

Let F be a 1-sorted structure, let A be a non empty set, let a be a binary operation on A, let Z be an element of A, and let l be a function from $[:$the carrier of F, $A:]$ into A. One can verify that $\langle A, a, Z, l \rangle$ is non empty.

Let F be a 1-sorted structure. A scalar of F is an element of F.

Let F be a 1-sorted structure and let V_1 be a vector space structure over F. A scalar of V_1 is a scalar of F. A vector of V_1 is an element of V_1.

Let F be a non empty 1-sorted structure, let V be a non empty vector space structure over F, let x be an element of F, and let v be an element of V. The functor $x \cdot v$ yielding an element of V is defined by:

(Def. 24) $x \cdot v =$ (the left multiplication of V)(x, v).

Let F be a non empty loop structure. The functor $\mathrm{comp} F$ yielding a unary operation on the carrier of F is defined by:

(Def. 25) For every element x of F holds $(\mathrm{comp} F)(x) = -x$.

Let F be a non empty double loop structure and let I_1 be a non empty vector space structure over F. We say that I_1 is vector space-like if and only if the condition (Def. 26) is satisfied.

(Def. 26) Let x, y be elements of F and v, w be elements of I_1. Then $x \cdot (v + w) = x \cdot v + x \cdot w$ and $(x + y) \cdot v = x \cdot v + y \cdot v$ and $(x \cdot y) \cdot v = x \cdot (y \cdot v)$ and $\mathbf{1}_F \cdot v = v$.

[6] The propositions (34) and (35) have been removed.
[7] The propositions (37) and (38) have been removed.

Let F be an add-associative right zeroed right complementable Abelian associative left unital distributive non empty double loop structure. Observe that there exists a non empty vector space structure over F which is vector space-like, add-associative, right zeroed, right complementable, Abelian, and strict.

Let F be an add-associative right zeroed right complementable Abelian associative left unital distributive non empty double loop structure. A vector space over F is a vector space-like add-associative right zeroed right complementable Abelian non empty vector space structure over F.

In the sequel F denotes a field, x denotes an element of F, V denotes a vector space-like add-associative right zeroed right complementable non empty vector space structure over F, and v denotes an element of V.

We now state several propositions:

(59)[8] Let F be an add-associative right zeroed right complementable Abelian associative left unital distributive non empty double loop structure, x be an element of F, V be an add-associative right zeroed right complementable vector space-like non empty vector space structure over F, and v be an element of V. Then $0_F \cdot v = 0_V$ and $(-\mathbf{1}_F) \cdot v = -v$ and $x \cdot 0_V = 0_V$.

(60) $x \cdot v = 0_V$ iff $x = 0_F$ or $v = 0_V$.

(63)[9] Let V be an add-associative right zeroed right complementable non empty loop structure and v, w be elements of V. Then $v + w = 0_V$ if and only if $-v = w$.

(64) Let V be an add-associative right zeroed right complementable non empty loop structure and u, v, w be elements of V. Then $-(v+w) = -w-v$ and $-(w+-v) = v-w$ and $-(v-w) = w+-v$ and $-(-v-w) = w+v$ and $u-(w+v) = u-v-w$.

(65) Let V be an add-associative right zeroed right complementable non empty loop structure and v be an element of V. Then $0_V - v = -v$ and $v - 0_V = v$.

(66) Let F be an add-associative right zeroed right complementable non empty loop structure and x, y be elements of F. Then

(i) $x + -y = 0_F$ iff $x = y$, and

(ii) $x - y = 0_F$ iff $x = y$.

(67) If $x \neq 0_F$, then $x^{-1} \cdot (x \cdot v) = v$.

(68) Let F be an add-associative right zeroed right complementable Abelian associative left unital distributive non empty double loop structure, V be a vector space-like add-associative right zeroed right complementable non empty vector space structure over F, x be an element of F, and v, w be elements of V. Then $-x \cdot v = (-x) \cdot v$ and $w - x \cdot v = w + (-x) \cdot v$.

Let us observe that every non empty multiplicative loop structure which is commutative and left unital is also right unital.

We now state several propositions:

(69) Let F be an add-associative right zeroed right complementable Abelian associative left unital right unital distributive non empty double loop structure, V be a vector space-like add-associative right zeroed right complementable non empty vector space structure over F, x be an element of F, and v be an element of V. Then $x \cdot -v = -x \cdot v$.

(70) Let F be an add-associative right zeroed right complementable Abelian associative left unital right unital distributive non empty double loop structure, V be a vector space-like add-associative right zeroed right complementable non empty vector space structure over F, x be an element of F, and v, w be elements of V. Then $x \cdot (v - w) = x \cdot v - x \cdot w$.

[8] The propositions (46)–(58) have been removed.

[9] The propositions (61) and (62) have been removed.

(73)[10] Let F be an add-associative right zeroed right complementable commutative associative left unital non degenerated field-like distributive non empty double loop structure and x be an element of F. If $x \neq 0_F$, then $(x^{-1})^{-1} = x$.

(74) For every field F and for every element x of F such that $x \neq 0_F$ holds $x^{-1} \neq 0_F$ and $-x^{-1} \neq 0_F$.

(78)[11] $\mathbf{1}_{\mathbb{R}_\mathrm{F}} + \mathbf{1}_{\mathbb{R}_\mathrm{F}} \neq 0_{\mathbb{R}_\mathrm{F}}$.

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

(Def. 28)[12] For every element a of I_1 such that $a + a = 0_{(I_1)}$ holds $a = 0_{(I_1)}$.

Let us observe that there exists a non empty loop structure which is Fanoian.

Let F be an add-associative right zeroed right complementable commutative associative left unital field-like non degenerated distributive non empty double loop structure. Let us observe that F is Fanoian if and only if:

(Def. 29) $\mathbf{1}_F + \mathbf{1}_F \neq 0_F$.

Let us observe that there exists a field which is strict and Fanoian.

One can prove the following propositions:

(81)[13] Let F be an add-associative right zeroed right complementable non empty loop structure and a, b be elements of F. Then $-(a - b) = b - a$.

(84)[14] Let F be an add-associative right zeroed right complementable non empty loop structure and a, b be elements of F. If $a - b = 0_F$, then $a = b$.

(86)[15] Let F be an add-associative right zeroed right complementable non empty loop structure and a be an element of F. If $-a = 0_F$, then $a = 0_F$.

(87) Let F be an add-associative right zeroed right complementable non empty loop structure and a, b be elements of F. If $a - b = 0_F$, then $b - a = 0_F$.

(88) Let a, b, c be elements of F. Then

(i) if $a \neq 0_F$ and $a \cdot c - b = 0_F$, then $c = b \cdot a^{-1}$, and

(ii) if $a \neq 0_F$ and $b - c \cdot a = 0_F$, then $c = b \cdot a^{-1}$.

(89) Let F be an add-associative right zeroed right complementable non empty loop structure and a, b be elements of F. Then $a + b = -(-b + -a)$.

(90) Let F be an add-associative right zeroed right complementable non empty loop structure and a, b, c be elements of F. Then $(b + a) - (c + a) = b - c$.

(91) For every Abelian add-associative non empty loop structure F and for all elements a, b, c of F holds $(a + b) - c = (a - c) + b$.

(92) Let G be an add-associative right zeroed right complementable non empty loop structure and v, w be elements of G. Then $-(-v + w) = -w + v$.

(93) Let G be an Abelian add-associative right zeroed right complementable non empty loop structure and u, v, w be elements of G. Then $u - v - w = u - w - v$.

[10] The propositions (71) and (72) have been removed.
[11] The propositions (75)–(77) have been removed.
[12] The definition (Def. 27) has been removed.
[13] The propositions (79) and (80) have been removed.
[14] The propositions (82) and (83) have been removed.
[15] The proposition (85) has been removed.

References

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

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

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

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

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

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

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

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

Received November 23, 1989

Published January 2, 2004