FORMALIZED MATHEMATICS
Vol.1, No.**2**, March–April 1990
Université Catholique de Louvain

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`.

The articles [3], [1], and [2] provide the notation and terminology for this paper. We consider group structures which are systems

⟨ a carrier, an addition, a reverse-map, a zero ⟩

where the carrier is a non-empty set, the addition is a binary operation on the carrier, the reverse-map is a unary operation on the carrier, and the zero is an element of the carrier. In the sequel GS denotes a group structure. Let us consider GS. An element of GS is an element of the carrier of GS.

Next we state a proposition

(1) For every element x of the carrier of GS holds x is an element of GS.

We now define three new functors. Let us consider GS. The functor 0_{GS} yields an element of GS and is defined by: 0_{GS} =the zero of GS.
Let x be an element of GS. The functor $-x$ yielding an element of GS, is defined by:

$-x$ =(the reverse-map of GS)(x).

Let y be an element of GS. The functor $x + y$ yielding an element of GS, is defined by:

$x + y$ =(the addition of GS)(x, y).

Next we state three propositions:

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

(3) For every element x of GS holds $-x$ =(the reverse-map of GS)(x).

(4) For all elements x, y of GS holds $x + y$ =(the addition of GS)(x, y).

---

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

ISSN 0777–4028

We now define two new functors. The constant $+_{\mathbb{R}}$ is a binary operation on $\mathbb{R}$ and is defined by:

for all elements x, y of $\mathbb{R}$ holds $+_{\mathbb{R}}(x, y) = x + y$.

The constant $-_{\mathbb{R}}$ is a unary operation on $\mathbb{R}$ and is defined by:

for every element x of $\mathbb{R}$ for every real number x' such that $x' = x$ holds $-_{\mathbb{R}}(x) = -x'$.

The constant $\mathbb{R}_{\mathrm{G}}$ is a group structure and is defined by:

$\mathbb{R}_{\mathrm{G}} = \langle \mathbb{R}, +_{\mathbb{R}}, -_{\mathbb{R}}, 0 \rangle$.

We now state two propositions:

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

(6) 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 $x + (-x) = 0_{\mathbb{R}_{\mathrm{G}}}$.

The mode Abelian group, which widens to the type a group structure, is defined by:

for all elements x, y, z of it holds $x + y = y + x$ and $(x + y) + z = x + (y + z)$ and $x + 0_{\mathrm{it}} = x$ and $x + (-x) = 0_{\mathrm{it}}$.

The following proposition is true

(7) For all elements x, y, z of GS holds $x+y = y+x$ and $(x+y)+z = x+(y+z)$ and $x+0_{GS} = x$ and $x+(-x) = 0_{GS}$ if and only if GS is an Abelian group.

In the sequel G is an Abelian group and x, y, z are elements of G. We now state four propositions:

(8) $x + y = y + x$.

(9) $x + (y + z) = (x + y) + z$.

(10) $x + 0_G = x$.

(11) $x + (-x) = 0_G$.

Let us consider G, x, y. The functor $x - y$ yielding an element of G, is defined by:

$x - y = x + (-y)$.

The following propositions are true:

(12) $x - y = x + (-y)$.

(13) If $x + y = x + z$, then $y = z$ but if $x + y = z + y$, then $x = z$.

(14) $-0_G = 0_G$.

We consider field structures which are systems

⟨ a carrier, a multiplication, an addition, a reverse-map, a unity, a zero ⟩

where the carrier is a non-empty set, the multiplication, the addition are binary operations on the carrier, the reverse-map is a unary operation on the carrier, and the unity, the zero are elements of the carrier. In the sequel FS will denote a field structure. We now define five new functors. Let us consider FS. The functor 1_{FS} yields an element of the carrier of FS and is defined by:

1_{FS} =the unity of FS.

The functor 0_{FS} yields an element of the carrier of FS and is defined by:

0_{FS} =the zero of FS.

Let x be an element of the carrier of FS. The functor $-x$ yields an element of the carrier of FS and is defined by:

$-x =$(the reverse-map of FS)(x).

Let y be an element of the carrier of FS. The functor $x \cdot y$ yields an element of the carrier of FS and is defined by:

$x \cdot y =$(the multiplication of FS)(x, y).

The functor $x + y$ yielding an element of the carrier of FS, is defined by:

$x + y =$(the addition of FS)(x, y).

One can prove the following propositions:

(15) $1_{FS} =$the unity of FS.

(16) $0_{FS} =$the zero of FS.

(17) For every element x of the carrier of FS holds $-x =$(the reverse-map of FS)(x).

(18) For all elements x, y of the carrier of FS holds $x \cdot y =$(the multiplication of FS)(x, y).

(19) For all elements x, y of the carrier of FS holds $x + y =$(the addition of FS)(x, y).

The constant $\cdot_{\mathbb{R}}$ is a binary operation on $\mathbb{R}$ and is defined by:
for all elements x, y of $\mathbb{R}$ holds $\cdot_{\mathbb{R}}(x, y) = x \cdot y$.

The constant $\mathbb{R}_{\mathrm{F}}$ is a field structure and is defined by:
$\mathbb{R}_{\mathrm{F}} = \langle \mathbb{R}, \cdot_{\mathbb{R}}, +_{\mathbb{R}}, -_{\mathbb{R}}, 1, 0 \rangle$.

We now state two propositions:

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

(21) Let x, y, z be elements of the carrier of $\mathbb{R}_{\mathrm{F}}$. Then

(i) $x + y = y + x$,

(ii) $(x + y) + z = x + (y + z)$,

(iii) $x + 0_{\mathbb{R}_{\mathrm{F}}} = x$,

(iv) $x + (-x) = 0_{\mathbb{R}_{\mathrm{F}}}$,

(v) $x \cdot y = y \cdot x$,

(vi) $(x \cdot y) \cdot z = x \cdot (y \cdot z)$,

(vii) $x \cdot (1_{\mathbb{R}_{\mathrm{F}}}) = x$,

(viii) if $x \neq 0_{\mathbb{R}_{\mathrm{F}}}$, then there exists y being an element of the carrier of $\mathbb{R}_{\mathrm{F}}$ such that $x \cdot y = 1_{\mathbb{R}_{\mathrm{F}}}$,

(ix) $0_{\mathbb{R}_{\mathrm{F}}} \neq 1_{\mathbb{R}_{\mathrm{F}}}$,

(x) $x \cdot (y + z) = x \cdot y + x \cdot z$,

(xi) $(y + z) \cdot x = y \cdot x + z \cdot x$.

The mode field, which widens to the type a field structure, is defined by:
Let x, y, z be elements of the carrier of it . Then

(i) $x + y = y + x$,

(ii) $(x + y) + z = x + (y + z)$,

(iii) $x + 0_{\mathrm{it}} = x$,

(iv) $x + (-x) = 0_{\mathrm{it}}$,

(v) $x \cdot y = y \cdot x$,

(vi) $(x \cdot y) \cdot z = x \cdot (y \cdot z)$,

(vii) $x \cdot (1_{\rm it}) = x$,
(viii) if $x \neq 0_{\rm it}$, then there exists y being an element of the carrier of it such that $x \cdot y = 1_{\rm it}$,
(ix) $0_{\rm it} \neq 1_{\rm it}$,
(x) $x \cdot (y + z) = x \cdot y + x \cdot z$,
(xi) $(y + z) \cdot x = y \cdot x + z \cdot x$.

We now state a proposition

(22) The following conditions are equivalent:
 (i) for all elements x, y, z of the carrier of FS holds $x + y = y + x$ and $(x+y)+z = x+(y+z)$ and $x+0_{FS} = x$ and $x+(-x) = 0_{FS}$ and $x \cdot y = y \cdot x$ and $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ and $x \cdot (1_{FS}) = x$ but if $x \neq 0_{FS}$, then there exists y being an element of the carrier of FS such that $x \cdot y = 1_{FS}$ and $0_{FS} \neq 1_{FS}$ and $x \cdot (y + z) = x \cdot y + x \cdot z$ and $(y + z) \cdot x = y \cdot x + z \cdot x$,
 (ii) FS is a field.

In the sequel F is a field and x, y, z are elements of the carrier of F. The following propositions are true:

(23) $x + y = y + x$.
(24) $(x + y) + z = x + (y + z)$.
(25) $x + 0_F = x$.
(26) $x + (-x) = 0_F$.
(27) $x \cdot y = y \cdot x$.
(28) $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.
(29) $x \cdot (1_F) = x$.
(30) If $x \neq 0_F$, then there exists y such that $x \cdot y = 1_F$.
(31) $0_F \neq 1_F$.
(32) $x \cdot (y + z) = x \cdot y + x \cdot z$ and $(y + z) \cdot x = y \cdot x + z \cdot x$.
(33) If $x \neq 0_F$ and $x \cdot y = x \cdot z$, then $y = z$.

Let us consider F, x. Let us assume that $x \neq 0_F$. The functor x^{-1} yields an element of the carrier of F and is defined by:

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

We now state a proposition

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

We now define two new functors. Let us consider F, x, y. The functor $x - y$ yielding an element of the carrier of F, is defined by:

$x - y = x + (-y)$.

The functor $\frac{x}{y}$ yielding an element of the carrier of F, is defined by:

$\frac{x}{y} = x \cdot y^{-1}$.

One can prove the following propositions:

(35) $x - y = x + (-y)$.
(36) $\frac{x}{y} = x \cdot y^{-1}$.
(37) If $x + y = x + z$, then $y = z$ but if $x + y = z + y$, then $x = z$.
(38) $-(x + y) = (-x) + (-y)$.

(39) $x \cdot 0_F = 0_F$ and $0_F \cdot x = 0_F$.

(40) $-(-x) = x$.

(41) $(-x) \cdot y = -x \cdot y$.

(42) $(-x) \cdot (-y) = x \cdot y$.

(43) $x \cdot (y - z) = x \cdot y - x \cdot z$.

(44) $x \cdot y = 0_F$ if and only if $x = 0_F$ or $y = 0_F$.

We consider vector space structures which are systems

$\langle$ scalars, a carrier, a multiplication $\rangle$

where the scalars is a field, the carrier is an Abelian group, and the multiplication is a function from $[\!:$ the carrier of the scalars, the carrier of the carrier $:\!]$ into the carrier of the carrier. In the sequel VS will denote a vector space structure. Let us consider VS. A vector of VS is an element of the carrier of VS.

One can prove the following proposition

(45) For every element x of the carrier of VS holds x is a vector of VS.

Let us consider F. The mode vector space structure over F, which widens to the type a vector space structure, is defined by:

the scalars of it $= F$.

One can prove the following proposition

(46) For every VS being a vector space structure holds VS is a vector space structure over F if and only if the scalars of $VS = F$.

In the sequel V is a vector space structure over F. The arguments of the notions defined below are the following: F, V which are objects of the type reserved above; x which is an element of the carrier of F; v which is an element of the carrier of V. The functor $x \cdot v$ yields an element of the carrier of V and is defined by:

for every element x' of the carrier of the scalars of V such that $x' = x$ holds $x \cdot v =$(the multiplication of V)(x', v).

We now state a proposition

(47) For every vector space structure V over F for every element x of the carrier of F for every element v of the carrier of V for every element x' of the carrier of the scalars of V such that $x' = x$ holds $x \cdot v =$(the multiplication of V)(x', v).

Let us consider F. The mode vector space over F, which widens to the type a vector space structure over F, is defined by:

Let x, y be elements of the carrier of F. Let v, w be elements of the carrier of it . 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 $(1_F) \cdot v = v$.

We now state a proposition

(48) The following conditions are equivalent:

(i) for all elements x, y of the carrier of F for all elements v, w of the carrier of V holds $x \cdot (v + w) = x \cdot v + x \cdot w$ and $(x + y) \cdot v = x \cdot v + y \cdot v$ and $(x \cdot y) \cdot v = x \cdot (y \cdot v)$ and $(1_F) \cdot v = v$,

(ii) V is a vector space over F.

We follow a convention: V, V_1 denote vector spaces over F, x, y denote elements of the carrier of F, and v, w denote elements of the carrier of V. Let us consider F, V. The functor Θ_V yielding an element of the carrier of V, is defined by:

$\Theta_V = 0_{\text{the carrier of } V}$.

One can prove the following propositions:

(49) $\Theta_V = 0_{\text{the carrier of } V}$.

(50) $\Theta_V + v = v$.

(51) $v + \Theta_V = v$.

(52) $v + (-v) = \Theta_V$.

(53) $(-v) + v = \Theta_V$.

(54) $-\Theta_V = \Theta_V$.

(55) $x \cdot (v + w) = x \cdot v + x \cdot w$.

(56) $(x + y) \cdot v = x \cdot v + y \cdot v$.

(57) $(x \cdot y) \cdot v = x \cdot (y \cdot v)$.

(58) $(1_F) \cdot v = v$.

(59) $0_F \cdot v = \Theta_V$ and $(-1_F) \cdot v = -v$ and $x \cdot (\Theta_V) = \Theta_V$.

(60) $x \cdot v = \Theta_V$ if and only if $x = 0_F$ or $v = \Theta_V$.

Let us consider F, V. The mode VSS of V, which widens to the type a vector space over F, is defined by: the carrier of the carrier of it $\subseteq$the carrier of the carrier of V and for all elements v, w of the carrier of it for all elements x, y of the carrier of F holds $x \cdot v + y \cdot w$ is an element of the carrier of it .

The following proposition is true

(61) the carrier of the carrier of V_1 $\subseteq$the carrier of the carrier of V and for all elements v, w of the carrier of V_1 for all elements x, y of the carrier of F holds $x \cdot v + y \cdot w$ is an element of the carrier of V_1 if and only if V_1 is a VSS of V.

In the sequel u, v, w will be elements of the carrier of V. We now state a number of propositions:

(62) $v - w = v + (-w)$.

(63) $v + w = \Theta_V$ if and only if $-v = w$.

(64) (i) $-(v + w) = (-v) - w$,

(ii) $-(-v) = v$,

(iii) $-((-v) + w) = v - w$,

(iv) $-(v - w) = (-v) + w$,

(v) $-((-v) - w) = v + w$,

(vi) $u - (v + w) = (u - v) - w$.

(65) $\Theta_V - v = -v$ and $v - \Theta_V = v$.

(66) $x + (-y) = 0_F$ if and only if $x = y$ but $x - y = 0_F$ if and only if $x = y$.

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

(68) $-x \cdot v = (-x) \cdot v$ and $w - x \cdot v = w + (-x) \cdot v$.

(69) $x \cdot (-v) = -x \cdot v$.

(70) $x \cdot (v - w) = x \cdot v - x \cdot w$.

(71) $v - x \cdot (y \cdot w) = v - (x \cdot y) \cdot w$.

(72) $\mathbb{R}_{\rm F}$ is a field.

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

(74) If $x \neq 0_F$, then $x^{-1} \neq 0_F$ and $-x^{-1} \neq 0_F$.

(75) For all elements x, y of $\mathbb{R}$ holds $+_{\mathbb{R}}(x, y) = x + y$.

(76) For every element x of $\mathbb{R}$ for every real number x' such that $x' = x$ holds $-_{\mathbb{R}}(x) = -x'$.

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

(78) $1_{\mathbb{R}_{\rm F}} + 1_{\mathbb{R}_{\rm F}} \neq 0_{\mathbb{R}_{\rm F}}$.

The mode Fano field, which widens to the type a field, is defined by:

$1_{\rm it} + 1_{\rm it} \neq 0_{\rm it}$.

The following proposition is true

(79) For every field F holds F is a Fano field if and only if $1_F + 1_F \neq 0_F$.

In the sequel F will denote a field and a, b, c will denote elements of the carrier of F. One can prove the following propositions:

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

(81) $-(a - b) = b - a$.

(82) $0_F + a = a$.

(83) $(-a) + a = 0_F$.

(84) If $a - b = 0_F$, then $a = b$.

(85) $-0_F = 0_F$.

(86) If $-a = 0_F$, then $a = 0_F$.

(87) If $a - b = 0_F$, then $b - a = 0_F$.

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

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

(90) $(a + b) - (a + c) = b - c$.

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

Received November 23, 1989