Contents

Formaliz. Math. 22 (**4**)

FORMALIZED MATHEMATICS
Vol. 22, No. 4, Pages 277–289, 2014
DOI: 10.2478/forma-2014-0028

DE GRUYTER OPEN
degruyter.com/view/j/forma

Torsion ℤ-module and Torsion-free ℤ-module[1]

Yuichi Futa
Japan Advanced Institute
of Science and Technology
Ishikawa, Japan

Hiroyuki Okazaki
Shinshu University
Nagano, Japan

Kazuhisa Nakasho
Shinshu University
Nagano, Japan

Yasunari Shidama
Shinshu University
Nagano, Japan

Summary. In this article, we formalize a torsion ℤ-module and a torsion-free ℤ-module. Especially, we prove formally that finitely generated torsion-free ℤ-modules are finite rank free. We also formalize properties related to rank of finite rank free ℤ-modules. The notion of ℤ-module is necessary for solving lattice problems, LLL (Lenstra, Lenstra, and Lovász) base reduction algorithm [20], cryptographic systems with lattice [21], and coding theory [11].

MSC: 13C10 15A04 03B35

Keywords: free Z-module; rank of Z-module; homomorphism of Z-module; linearly independent; linear combination

MML identifier: ZMODUL06, version: 8.1.04 5.32.1237

The notation and terminology used in this paper have been introduced in the following articles: [24], [5], [1], [26], [10], [6], [7], [15], [28], [27], [25], [3], [4], [8], [17], [33], [34], [29], [32], [18], [31], [9], [12], [13], [14], and [22].

[1]This work was supported by JSPS KAKENHI 21240001 and 22300285.

ISSN 1426–2630(Print), 1898-9934(Online)

1. Torsion $\mathbb{Z}$-module and Torsion-free $\mathbb{Z}$-module

Now we state the proposition:

(1) Let us consider a $\mathbb{Z}$-module V, and a submodule W of V. Then $1_{\mathbb{Z}^{\mathrm{R}}} \circ W = \Omega_W$.

Let us consider a $\mathbb{Z}$-module V and submodules W_1, W_2, W_3 of V. Now we state the propositions:

(2) $W_1 \cap W_2$ is a submodule of $(W_1 + W_3) \cap W_2$.
Proof: For every vector v of V such that $v \in W_1 \cap W_2$ holds $v \in (W_1 + W_3) \cap W_2$ by [12, (94), (93)]. □

(3) If $W_1 \cap W_2 \neq \mathbf{0}_V$, then $(W_1 + W_3) \cap W_2 \neq \mathbf{0}_V$.

(4) Let us consider a $\mathbb{Z}$-module V, and linearly independent subsets I, I_1 of V. If $I_1 \subseteq I$, then $\mathrm{Lin}(I \setminus I_1) \cap \mathrm{Lin}(I_1) = \mathbf{0}_V$.

From now on V denotes a $\mathbb{Z}$-module, W denotes a submodule of V, v, u denote vectors of V, and i denotes an element of $\mathbb{Z}^{\mathrm{R}}$. Let V be a $\mathbb{Z}$-module and v be a vector of V. We say that v is torsion if and only if

(Def. 1) there exists an element i of $\mathbb{Z}^{\mathrm{R}}$ such that $i \neq 0_{\mathbb{Z}^{\mathrm{R}}}$ and $i \cdot v = 0_V$.

One can verify that 0_V is torsion.

Now we state the propositions:

(5) If v is torsion and u is torsion, then $v + u$ is torsion.

(6) If v is torsion, then $-v$ is torsion.

(7) If v is torsion and u is torsion, then $v - u$ is torsion.

(8) If v is torsion, then $i \cdot v$ is torsion.

(9) Let us consider a vector v of V, and a vector w of W. If $v = w$, then v is torsion iff w is torsion.

Let V be a $\mathbb{Z}$-module. One can verify that there exists a vector of V which is torsion.

Now we state the propositions:

(10) If v is not torsion, then $-v$ is not torsion.

(11) If v is not torsion and $i \neq 0$, then $i \cdot v$ is not torsion.

(12) v is not torsion if and only if $\{v\}$ is linearly independent.
Proof: If v is not torsion, then $\{v\}$ is linearly independent by [9, (33)], [13, (24)]. If $\{v\}$ is linearly independent, then v is not torsion by [14, (1)], [13, (8), (29), (53)]. □

Let V be a $\mathbb{Z}$-module. We say that V is torsion if and only if

(Def. 2) every vector of V is torsion.

Let us note that $\mathbf{0}_V$ is torsion and there exists a $\mathbb{Z}$-module which is torsion.

Now we state the propositions:

(13) Let us consider an element v of $\mathbb{Z}^{\mathrm{R}}$, and an integer v_1. Suppose $v = v_1$. Let us consider a natural number n. Then (Nat-mult-left $\mathbb{Z}^{\mathrm{R}}$)$(n, v) = n \cdot v_1$.
PROOF: Define $\mathcal{P}$[natural number] $\equiv$ (Nat-mult-left $\mathbb{Z}^{\mathrm{R}}$)$(\$_1, v) = \$_1 \cdot v_1$. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$. For every natural number n, $\mathcal{P}[n]$ from [3, Sch. 2]. $\square$

(14) Let us consider an element x of $\mathbb{Z}^{\mathrm{R}}$, an element v of $\mathbb{Z}^{\mathrm{R}}$, and an integer v_1. Suppose $v = v_1$. Then (the left integer multiplication of $(\mathbb{Z}^{\mathrm{R}})$)$(x, v) = x \cdot v_1$. The theorem is a consequence of (13).

Note that there exists a $\mathbb{Z}$-module which is non torsion.

Let V be a non torsion $\mathbb{Z}$-module. Let us observe that there exists a vector of V which is non torsion.

Let V be a $\mathbb{Z}$-module. We say that V is torsion-free if and only if

(Def. 3) for every vector v of V such that $v \neq 0_V$ holds v is not torsion.

Now we state the proposition:

(15) V is cancelable on multiplication if and only if V is torsion-free.

One can verify that every cancelable on multiplication $\mathbb{Z}$-module is torsion-free and every torsion-free $\mathbb{Z}$-module is cancelable on multiplication and every free $\mathbb{Z}$-module is torsion-free and there exists a $\mathbb{Z}$-module which is torsion-free and free.

Now we state the proposition:

(16) Let us consider a torsion-free $\mathbb{Z}$-module V, and a vector v of V. Then v is torsion if and only if $v = 0_V$.

Let V be a torsion-free $\mathbb{Z}$-module. Note that every submodule of V is torsion-free.

Let V be a $\mathbb{Z}$-module. Observe that $\mathbf{0}_V$ is trivial and every non trivial, torsion-free $\mathbb{Z}$-module is non torsion and there exists a $\mathbb{Z}$-module which is trivial.

Let V be a non trivial $\mathbb{Z}$-module. Let us note that there exists a vector of V which is non zero.

Now we state the proposition:

(17) v is not torsion if and only if $\mathrm{Lin}(\{v\})$ is free and $v \neq 0_V$. The theorem is a consequence of (12) and (9).

Let V be a non torsion $\mathbb{Z}$-module and v be a non torsion vector of V. Let us note that $\mathrm{Lin}(\{v\})$ is free.

Now we state the propositions:

(18) Let us consider a $\mathbb{Z}$-module V, a subset A of V, and a vector v of V. If A is linearly independent and $v \in A$, then v is not torsion. The theorem

is a consequence of (12).

(19) Let us consider an object u. Suppose $u \in \mathrm{Lin}(\{v\})$. Then there exists an element i of $\mathbb{Z}^{\mathrm{R}}$ such that $u = i \cdot v$.

(20) $v \in \mathrm{Lin}(\{v\})$.

(21) $i \cdot v \in \mathrm{Lin}(\{v\})$.

(22) $\mathrm{Lin}(\{0_V\}) = \mathbf{0}_V$.

PROOF: For every object x, $x \in \mathrm{Lin}(\{0_V\})$ iff $x \in \mathbf{0}_V$ by [13, (64), (21)], [12, (1)], [13, (66)]. □

Let V be a torsion-free $\mathbb{Z}$-module and v be a vector of V. Let us note that $\mathrm{Lin}(\{v\})$ is free. Now we state the propositions:

(23) Let us consider subsets A_1, A_2 of V. Suppose A_1 is linearly independent and A_2 is linearly independent and $A_1 \cap A_2 = \emptyset$ and $A_1 \cup A_2$ is linearly dependent. Then $\mathrm{Lin}(A_1) \cap \mathrm{Lin}(A_2) \neq \mathbf{0}_V$.

(24) Let us consider a $\mathbb{Z}$-module V, a free submodule W of V, a subset I of V, and a vector v of V. Suppose I is linearly independent and $\mathrm{Lin}(I) = \Omega_W$ and $v \in I$. Then

(i) $\Omega_W = \mathrm{Lin}(I \setminus \{v\}) + \mathrm{Lin}(\{v\})$, and

(ii) $\mathrm{Lin}(I \setminus \{v\}) \cap \mathrm{Lin}(\{v\}) = \mathbf{0}_V$, and

(iii) $\mathrm{Lin}(I \setminus \{v\})$ is free, and

(iv) $\mathrm{Lin}(\{v\})$ is free, and

(v) $v \neq 0_V$.

PROOF: v is not torsion. $\mathrm{Lin}(I \setminus \{v\}) \cap \mathrm{Lin}(\{v\}) = \mathbf{0}_V$ by [16, (24)], [12, (94)], [13, (64), (23), (10)]. □

(25) Let us consider a $\mathbb{Z}$-module V, and a free submodule W of V. Then there exists a subset A of V such that

(i) A is subset of W and linearly independent, and

(ii) $\mathrm{Lin}(A) = \Omega_W$.

(26) Let us consider a $\mathbb{Z}$-module V, and a finite rank, free submodule W of V. Then there exists a finite subset A of V such that

(i) A is finite subset of W and linearly independent, and

(ii) $\mathrm{Lin}(A) = \Omega_W$, and

(iii) $\overline{\overline{A}} = \mathrm{rank}\, W$.

Let us consider a torsion-free $\mathbb{Z}$-module V and vectors v_1, v_2 of V.

Let us assume that $v_1 \neq 0_V$ and $v_2 \neq 0_V$ and $\mathrm{Lin}(\{v_1\}) \cap \mathrm{Lin}(\{v_2\}) \neq \mathbf{0}_V$. Now we state the propositions:

(27) There exists a vector u of V such that

(i) $u \neq 0_V$, and

(ii) $\mathrm{Lin}(\{v_1\}) \cap \mathrm{Lin}(\{v_2\}) = \mathrm{Lin}(\{u\})$.

Proof: Consider x being a vector of V such that $x \in \mathrm{Lin}(\{v_1\}) \cap \mathrm{Lin}(\{v_2\})$ and $x \neq 0_V$. Consider i_3 being an element of $\mathbb{Z}^{\mathrm{R}}$ such that $x = i_3 \cdot v_1$. Consider i_4 being an element of $\mathbb{Z}^{\mathrm{R}}$ such that $x = i_4 \cdot v_2$. Consider i_1, i_2 being integers such that $i_3 = (\gcd(i_3, i_4)) \cdot i_1$ and $i_4 = (\gcd(i_3, i_4)) \cdot i_2$ and i_1 and i_2 are relatively prime. Reconsider $I_1 = i_1$, $I_2 = i_2$ as an element of $\mathbb{Z}^{\mathrm{R}}$. $I_1 \cdot v_1 \in \mathrm{Lin}(\{v_1\})$ and $I_2 \cdot v_2 \in \mathrm{Lin}(\{v_2\})$. For every vector y of V such that $y \in \mathrm{Lin}(\{I_1 \cdot v_1\})$ holds $y \in \mathrm{Lin}(\{v_1\}) \cap \mathrm{Lin}(\{v_2\})$ by (19), [12, (37)]. $\mathrm{Lin}(\{I_1 \cdot v_1\}) = \mathrm{Lin}(\{v_1\}) \cap \mathrm{Lin}(\{v_2\})$ by [12, (46), (94)], (19), [12, (37), (36)]. □

(28) There exists a vector u of V such that

(i) $u \neq 0_V$, and

(ii) $\mathrm{Lin}(\{v_1\}) + \mathrm{Lin}(\{v_2\}) = \mathrm{Lin}(\{u\})$.

Proof: Consider x being a vector of V such that $x \neq 0_V$ and $\mathrm{Lin}(\{v_1\}) \cap \mathrm{Lin}(\{v_2\}) = \mathrm{Lin}(\{x\})$. Consider i_1 being an element of $\mathbb{Z}^{\mathrm{R}}$ such that $x = i_1 \cdot v_1$. Consider i_2 being an element of $\mathbb{Z}^{\mathrm{R}}$ such that $x = i_2 \cdot v_2$. $\gcd(|i_1|, |i_2|) = 1$ by [19, (5)], [23, (2)], [12, (1)], [3, (25)]. Consider j_1, j_2 being elements of $\mathbb{Z}^{\mathrm{R}}$ such that $i_1 \cdot j_1 + i_2 \cdot j_2 = 1$. Reconsider $J_1 = j_1$, $J_2 = j_2$ as an element of $\mathbb{Z}^{\mathrm{R}}$. Reconsider $u = J_1 \cdot v_2 + J_2 \cdot v_1$ as a vector of V. $\mathrm{Lin}(\{v_1\}) + \mathrm{Lin}(\{v_2\}) = \mathrm{Lin}(\{u\})$ by (19), [12, (37), (92), (36)]. □

(29) Let us consider a torsion-free $\mathbb{Z}$-module V, a finite rank, free submodule W of V, and vectors v, u of V. Suppose $v \neq 0_V$ and $u \neq 0_V$ and $W \cap \mathrm{Lin}(\{v\}) = \mathbf{0}_V$ and $(W + \mathrm{Lin}(\{u\})) \cap \mathrm{Lin}(\{v\}) \neq \mathbf{0}_V$ and $\mathrm{Lin}(\{u\}) \cap \mathrm{Lin}(\{v\}) = \mathbf{0}_V$. Then there exist vectors w_1, w_2 of V such that

(i) $w_1 \neq 0_V$, and

(ii) $w_2 \neq 0_V$, and

(iii) $W + \mathrm{Lin}(\{u\}) + \mathrm{Lin}(\{v\}) = W + \mathrm{Lin}(\{w_1\}) + \mathrm{Lin}(\{w_2\})$, and

(iv) $W \cap \mathrm{Lin}(\{w_1\}) \neq \mathbf{0}_V$, and

(v) $(W + \mathrm{Lin}(\{w_1\})) \cap \mathrm{Lin}(\{w_2\}) = \mathbf{0}_V$, and

(vi) $u, v \in \mathrm{Lin}(\{w_1\}) + \mathrm{Lin}(\{w_2\})$, and

(vii) $w_1, w_2 \in \mathrm{Lin}(\{u\}) + \mathrm{Lin}(\{v\})$.

Proof: Consider x being a vector of V such that $x \in (W + \mathrm{Lin}(\{u\})) \cap \mathrm{Lin}(\{v\})$ and $x \neq 0_V$. Consider x_1, x_2 being vectors of V such that $x_1 \in W$ and $x_2 \in \mathrm{Lin}(\{u\})$ and $x = x_1 + x_2$. Consider i_4 being an element of $\mathbb{Z}^{\mathrm{R}}$

such that $x = i_4 \cdot v$. Consider i_3 being an element of $\mathbb{Z}^{\rm R}$ such that $x_2 = i_3 \cdot u$. Consider i_2, i_1 being integers such that $i_4 = (\gcd(i_4, i_3)) \cdot i_2$ and $i_3 = (\gcd(i_4, i_3)) \cdot i_1$ and i_2 and i_1 are relatively prime. Consider J_4, J_3 being elements of $\mathbb{Z}^{\rm R}$ such that $i_2 \cdot J_4 + i_1 \cdot J_3 = 1$. Reconsider $j_4 = J_4$, $j_3 = J_3$ as an element of $\mathbb{Z}^{\rm R}$. Set $w_1 = i_2 \cdot v - i_1 \cdot u$. Set $w_2 = j_4 \cdot u + j_3 \cdot v$. $w_1 \neq 0_V$ by [29, (21)], [12, (37)], (20), [12, (94), (1)]. Reconsider $i_6 = \gcd(i_4, i_3)$ as an element of $\mathbb{Z}^{\rm R}$. $i_6 \cdot w_1 \in W$ by [12, (8)]. $W \cap \mathrm{Lin}(\{w_1\}) \neq \mathbf{0}_V$ by [12, (37)], (20), [12, (94)], [13, (66)]. $u = i_2 \cdot w_2 - j_3 \cdot w_1$ by [12, (8)], [29, (29), (28), (15)]. $v = j_4 \cdot w_1 + i_1 \cdot w_2$ by [12, (8)], [29, (28), (15)]. $u \in \mathrm{Lin}(\{w_1\}) + \mathrm{Lin}(\{w_2\})$ by [12, (37)], (20), [12, (38), (92)]. $v \in \mathrm{Lin}(\{w_1\}) + \mathrm{Lin}(\{w_2\})$ by [12, (37)], (20), [12, (92)]. $w_1 \in \mathrm{Lin}(\{u\}) + \mathrm{Lin}(\{v\})$ by [12, (37)], (20), [12, (38), (92)]. $w_2 \in \mathrm{Lin}(\{u\}) + \mathrm{Lin}(\{v\})$ by [12, (37)], (20), [12, (92)]. For every object x such that $x \in W + \mathrm{Lin}(\{u\}) + \mathrm{Lin}(\{v\})$ holds $x \in W + \mathrm{Lin}(\{w_1\}) + \mathrm{Lin}(\{w_2\})$ by [12, (92)], (19), [12, (37), (36), (96)]. For every object x such that $x \in W + \mathrm{Lin}(\{w_1\}) + \mathrm{Lin}(\{w_2\})$ holds $x \in W + \mathrm{Lin}(\{u\}) + \mathrm{Lin}(\{v\})$ by [12, (92)], (19), [12, (37), (36), (96)]. $w_2 \neq 0_V$ by [29, (6)], [12, (37)], (20), [12, (38), (94), (1)]. $(W + \mathrm{Lin}(\{w_1\})) \cap \mathrm{Lin}(\{w_2\}) = \mathbf{0}_V$ by [16, (24)], [12, (94), (92)], (19). □

(30) Let us consider a torsion-free $\mathbb{Z}$-module V, a finite rank, free submodule W of V, and a vector v of V. Suppose $v \neq 0_V$ and $W \cap \mathrm{Lin}(\{v\}) \neq \mathbf{0}_V$. Then $W + \mathrm{Lin}(\{v\})$ is free.

PROOF: Define $\mathcal{P}$[natural number] $\equiv$ for every finite rank, free submodule W of V for every vector v of V such that $v \neq 0_V$ and $W \cap \mathrm{Lin}(\{v\}) \neq \mathbf{0}_V$ and $\mathrm{rank}\, W = \$_1 + 1$ holds $W + \mathrm{Lin}(\{v\})$ is free. $\mathcal{P}[0]$ by [22, (5)], [12, (25)], [14, (20)], [16, (22), (23)]. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$ by [16, (33)], [12, (25)], [14, (20)], [12, (97), (51), (94)]. For every natural number n, $\mathcal{P}[n]$ from [3, Sch. 2]. Set $r_1 = \mathrm{rank}\, W$. $r_1 - 1$ is a natural number by [22, (1)], [12, (51)], [16, (23)], [12, (107)]. □

Let V be a torsion-free $\mathbb{Z}$-module, v be a vector of V, and W be a finite rank, free submodule of V. Let us note that $W + \mathrm{Lin}(\{v\})$ is free.

Let V be a $\mathbb{Z}$-module and W be a finitely generated submodule of V. One can verify that $W + \mathrm{Lin}(\{v\})$ is finitely generated.

Let W_1, W_2 be finitely generated submodules of V. Observe that $W_1 + W_2$ is finitely generated. Now we state the proposition:

(31) Let us consider a $\mathbb{Z}$-module V, a submodule W of V, submodules W_6, W_8 of W, and submodules W_1, W_2 of V. If $W_6 = W_1$ and $W_8 = W_2$, then $W_6 + W_8 = W_1 + W_2$.

PROOF: Reconsider $S = W_6 + W_8$ as a strict submodule of V. For every vector v of V, $v \in S$ iff $v \in W_1 + W_2$ by [12, (92), (28)]. □

Let V be a torsion-free $\mathbb{Z}$-module and U_1, U_2 be finite rank, free submodules of V. Note that U_1+U_2 is free and every finitely generated, torsion-free $\mathbb{Z}$-module is free.

2. Rank of Finite Rank Free $\mathbb{Z}$-module

Now we state the propositions:

(32) Let us consider a torsion-free $\mathbb{Z}$-module V, and finite rank, free submodules W_1, W_2 of V. Suppose $W_1 \cap W_2 = \mathbf{0}_V$. Then $\operatorname{rank}(W_1 + W_2) = \operatorname{rank} W_1 + \operatorname{rank} W_2$.

(33) Let us consider a finite rank, free $\mathbb{Z}$-module V, and finite rank, free submodules W_1, W_2 of V. Suppose V is the direct sum of W_1 and W_2. Then $\operatorname{rank} V = \operatorname{rank} W_1 + \operatorname{rank} W_2$. The theorem is a consequence of (32).

(34) Let us consider a torsion-free $\mathbb{Z}$-module V, and finite rank, free submodules W_1, W_2 of V. Then $\operatorname{rank}(W_1 \cap W_2) \leqslant \operatorname{rank} W_1$.

(35) Let us consider a torsion-free $\mathbb{Z}$-module V, and a vector v of V. If $v \neq 0_V$, then $\operatorname{rank} \operatorname{Lin}(\{v\}) = 1$.

(36) Let us consider a $\mathbb{Z}$-module V. Then $\operatorname{rank} \mathbf{0}_V = 0$.

(37) Let us consider a torsion-free $\mathbb{Z}$-module V, and vectors v, u of V. Suppose $v \neq 0_V$ and $u \neq 0_V$ and $\operatorname{Lin}(\{v\}) \cap \operatorname{Lin}(\{u\}) \neq \mathbf{0}_V$. Then $\operatorname{rank}(\operatorname{Lin}(\{v\}) + \operatorname{Lin}(\{u\})) = 1$. The theorem is a consequence of (28).

(38) Let us consider a torsion-free $\mathbb{Z}$-module V, a finite rank, free submodule W of V, and a vector v of V. Suppose $v \neq 0_V$ and $W \cap \operatorname{Lin}(\{v\}) \neq \mathbf{0}_V$. Then $\operatorname{rank}(W + \operatorname{Lin}(\{v\})) = \operatorname{rank} W$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ for every finite rank, free submodule W of V for every vector v of V such that $v \neq 0_V$ and $W \cap \operatorname{Lin}(\{v\}) \neq \mathbf{0}_V$ and $\operatorname{rank} W = \$_1 + 1$ holds $\operatorname{rank}(W + \operatorname{Lin}(\{v\})) = \operatorname{rank} W$. $\mathcal{P}[0]$ by [22, (5)], [12, (25), (26), (42)]. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$ by (26), (24), [9, (31)], [2, (44)]. For every natural number n, $\mathcal{P}[n]$ from [3, Sch. 2]. Set $r_1 = \operatorname{rank} W$. $r_1 - 1$ is a natural number by [22, (1)], [12, (51)], [16, (23)], [12, (107)]. $\square$

(39) Let us consider a torsion-free $\mathbb{Z}$-module V, finite rank, free submodules W_1, W_2 of V, and a vector v of V. Suppose $W_1 \cap \operatorname{Lin}(\{v\}) \neq \mathbf{0}_V$ and $W_2 \cap \operatorname{Lin}(\{v\}) \neq \mathbf{0}_V$. Then $(W_1 \cap W_2) \cap \operatorname{Lin}(\{v\}) \neq \mathbf{0}_V$. The theorem is a consequence of (19).

(40) Let us consider $\mathbb{Z}$-modules V, W, a linear transformation T from V to W, and a subset A of V. Then T°(the carrier of $\operatorname{Lin}(A)$) $\subseteq$ the carrier of $\operatorname{Lin}(T^\circ A)$.

PROOF: For every object y such that $y \in T^\circ$(the carrier of Lin(A)) holds $y \in$ the carrier of Lin($T^\circ A$) by [7, (65)], [13, (64)], [22, (44), (46)]. □

Let us consider $\mathbb{Z}$-modules X, Y and a linear transformation L from X to Y. Now we state the propositions:

(41) $L(0_X) = 0_Y$.

(42) If L is bijective, then there exists a linear transformation K from Y to X such that $K = L^{-1}$ and K is bijective.

PROOF: Reconsider $K = L^{-1}$ as a function from Y into X. K is additive by [7, (113)], [6, (34)]. For every element r of $\mathbb{Z}^{\mathrm{R}}$ and for every element x of Y, $K(r \cdot x) = r \cdot K(x)$ by [7, (113)], [6, (34)]. □

(43) Let us consider $\mathbb{Z}$-modules X, Y, a linear combination l of X, and a linear transformation L from X to Y. If L is bijective, then $L\,@{*}\,l = l \cdot L^{-1}$.

PROOF: Reconsider $K = L^{-1}$ as a function from Y into X. For every element a of Y, $(L\,@{*}\,l)(a) = (l \cdot K)(a)$ by [6, (35)], [7, (35)], [6, (12), (34)]. □

(44) Let us consider $\mathbb{Z}$-modules X, Y, a subset X_0 of X, a linear transformation L from X to Y, and a linear combination l of $L^\circ X_0$. Suppose $X_0 =$ the carrier of X and L is one-to-one. Then $L \# l = l \cdot L$.

(45) Let us consider $\mathbb{Z}$-modules X, Y, a subset A of X, and a linear transformation L from X to Y. Suppose L is bijective. Then A is linearly independent if and only if $L^\circ A$ is linearly independent. The theorem is a consequence of (42).

(46) Let us consider $\mathbb{Z}$-modules X, Y, a subset A of X, and a linear transformation T from X to Y. Suppose T is bijective. Then T°(the carrier of Lin(A)) = the carrier of Lin($T^\circ A$). The theorem is a consequence of (40) and (42).

(47) Let us consider a $\mathbb{Z}$-module Y, and a subset A of Y. Then Lin(A) is a strict submodule of Ω_Y.

(48) Let us consider $\mathbb{Z}$-modules X, Y, and a linear transformation T from X to Y. If T is bijective, then X is free iff Y is free. The theorem is a consequence of (42).

(49) Let us consider free $\mathbb{Z}$-modules X, Y, a linear transformation T from X to Y, and a subset A of X. Suppose T is bijective. Then A is a basis of X if and only if $T^\circ A$ is a basis of Y. The theorem is a consequence of (42).

(50) Let us consider free $\mathbb{Z}$-modules X, Y, and a linear transformation T from X to Y. If T is bijective, then X is finite rank iff Y is finite rank. The theorem is a consequence of (42).

(51) Let us consider finite rank, free $\mathbb{Z}$-modules X, Y, and a linear transfor-

mation T from X to Y. If T is bijective, then $\operatorname{rank} X = \operatorname{rank} Y$.

PROOF: For every basis I of X, $\operatorname{rank} Y = \overline{\overline{I}}$ by [1, (5), (33)], (49). □

(52) Let us consider a $\mathbb{Z}$-module V, a finite rank, free submodule W of V, and an element a of $\mathbb{Z}^{\mathrm{R}}$. If $a \neq 0_{\mathbb{Z}^{\mathrm{R}}}$, then $\operatorname{rank}(a \circ W) = \operatorname{rank} W$.

PROOF: Define $\mathcal{P}[\text{element of } W, \text{object}] \equiv \$_2 = a \cdot \$_1$. For every element x of W, there exists an element y of $a \circ W$ such that $\mathcal{P}[x, y]$. Consider F being a function from W into $a \circ W$ such that for every element x of W, $\mathcal{P}[x, F(x)]$ from [7, Sch. 3]. For every objects x_1, x_2 such that x_1, $x_2 \in$ the carrier of W and $F(x_1) = F(x_2)$ holds $x_1 = x_2$ by [12, (10)]. For every object y such that $y \in$ the carrier of $a \circ W$ holds $y \in \operatorname{rng} F$ by [7, (4)]. F is additive by [12, (28)]. For every element r of $\mathbb{Z}^{\mathrm{R}}$ and for every element x of W, $F(r \cdot x) = r \cdot F(x)$ by [12, (29)]. □

(53) Let us consider a $\mathbb{Z}$-module V, finite rank, free submodules W_1, W_2, W_3 of V, and an element a of $\mathbb{Z}^{\mathrm{R}}$. Suppose $a \neq 0_{\mathbb{Z}^{\mathrm{R}}}$ and $W_3 = a \circ W_1$. Then $\operatorname{rank}(W_3 \cap W_2) = \operatorname{rank}(W_1 \cap W_2)$.

PROOF: $W_3 \cap W_2$ is a submodule of $W_1 \cap W_2$ by [12, (105), (42)], [13, (75)]. $a \circ (W_1 \cap W_2)$ is a submodule of $W_3 \cap W_2$ by [12, (42), (25), (94)]. $\operatorname{rank}(W_1 \cap W_2) \leqslant \operatorname{rank}(W_3 \cap W_2)$. □

(54) Let us consider a torsion-free $\mathbb{Z}$-module V, finite rank, free submodules W_1, W_2, W_3 of V, and an element a of $\mathbb{Z}^{\mathrm{R}}$. Suppose $a \neq 0_{\mathbb{Z}^{\mathrm{R}}}$ and $W_3 = a \circ W_1$. Then $\operatorname{rank}(W_3 + W_2) = \operatorname{rank}(W_1 + W_2)$.

PROOF: For every vector v of V such that $v \in W_3 + W_2$ holds $v \in W_1 + W_2$ by [12, (92)]. For every vector v of V such that $v \in a \circ (W_1 + W_2)$ holds $v \in W_3 + W_2$ by [12, (25), (92), (29)]. $\operatorname{rank}(W_1 + W_2) \leqslant \operatorname{rank}(W_3 + W_2)$. □

Let us consider a torsion-free $\mathbb{Z}$-module V, finite rank, free submodules W_1, W_2 of V, and a basis I of W_1. Now we state the propositions:

(55) Suppose for every vector v of V such that $v \in I$ holds $(W_1 \cap W_2) \cap \operatorname{Lin}(\{v\}) \neq \mathbf{0}_V$. Then $\operatorname{rank}(W_1 \cap W_2) = \operatorname{rank} W_1$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ for every finite rank, free submodules W_1, W_2 of V for every basis I of W_1 such that for every vector v of V such that $v \in I$ holds $(W_1 \cap W_2) \cap \operatorname{Lin}(\{v\}) \neq \mathbf{0}_V$ and $\operatorname{rank} W_1 = \$_1$ holds $\operatorname{rank}(W_1 \cap W_2) = \operatorname{rank} W_1$. $\mathcal{P}[0]$. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$ by [12, (25)], [14, (15)], [13, (56)], [14, (20)]. For every natural number n, $\mathcal{P}[n]$ from [3, Sch. 2]. □

(56) Suppose $\operatorname{rank}(W_1 \cap W_2) < \operatorname{rank} W_1$. Then there exists a vector v of V such that

(i) $v \in I$, and

(ii) $(W_1 \cap W_2) \cap \operatorname{Lin}(\{v\}) = \mathbf{0}_V$.

(57) Let us consider a torsion-free $\mathbb{Z}$-module V, finite rank, free submodules W_1, W_2 of V, and a basis I of W_1. Suppose $\operatorname{rank}(W_1 \cap W_2) = \operatorname{rank} W_1$. Let us consider a vector v of V. If $v \in I$, then $(W_1 \cap W_2) \cap \operatorname{Lin}(\{v\}) \neq \mathbf{0}_V$. The theorem is a consequence of (24), (32), and (35).

(58) Let us consider a torsion-free $\mathbb{Z}$-module V, finite rank, free submodules W_1, W_2 of V, and a basis I of W_1. Suppose for every vector v of V such that $v \in I$ holds $(W_1 \cap W_2) \cap \operatorname{Lin}(\{v\}) \neq \mathbf{0}_V$. Then $\operatorname{rank}(W_1 + W_2) = \operatorname{rank} W_2$.
PROOF: Define $\mathcal{P}$[natural number] $\equiv$ for every finite rank, free submodules W_1, W_2 of V for every basis I of W_1 such that for every vector v of V such that $v \in I$ holds $(W_1 \cap W_2) \cap \operatorname{Lin}(\{v\}) \neq \mathbf{0}_V$ and $\operatorname{rank} W_1 = \$_1$ holds $\operatorname{rank}(W_1 + W_2) = \operatorname{rank} W_2$. $\mathcal{P}[0]$ by [22, (1)], [12, (51), (42)], [16, (22)]. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$ by [12, (25)], [14, (15)], [13, (56)], [14, (20)]. For every natural number n, $\mathcal{P}[n]$ from [3, Sch. 2]. □

(59) Let us consider a torsion-free $\mathbb{Z}$-module V, and finite rank, free submodules W_1, W_2 of V. Suppose $\operatorname{rank}(W_1 \cap W_2) = \operatorname{rank} W_1$. Then $\operatorname{rank}(W_1 + W_2) = \operatorname{rank} W_2$. The theorem is a consequence of (57) and (58).

(60) Let us consider a field G, a vector space V over G, and a subset A of V. If A is linearly independent, then A is a basis of $\operatorname{Lin}(A)$.

(61) Let us consider a cancelable on multiplication, finite rank, free $\mathbb{Z}$-module V, and finite rank, free submodules W_1, W_2 of V. Then $\operatorname{rank}(W_1 + W_2) + \operatorname{rank}(W_1 \cap W_2) = \operatorname{rank} W_1 + \operatorname{rank} W_2$.
PROOF: Consider I_1 being a finite subset of V such that I_1 is finite subset of W_1 and linearly independent and $\operatorname{Lin}(I_1) = \Omega_{W_1}$ and $\overline{\overline{I_1}} = \operatorname{rank} W_1$. Consider I_2 being a finite subset of V such that I_2 is finite subset of W_2 and linearly independent and $\operatorname{Lin}(I_2) = \Omega_{W_2}$ and $\overline{\overline{I_2}} = \operatorname{rank} W_2$. Consider I_4 being a finite subset of V such that I_4 is finite subset of $W_1 + W_2$ and linearly independent and $\operatorname{Lin}(I_4) = \Omega_{W_1+W_2}$ and $\overline{\overline{I_4}} = \operatorname{rank}(W_1 + W_2)$. Consider I_3 being a finite subset of V such that I_3 is finite subset of $W_1 \cap W_2$ and linearly independent and $\operatorname{Lin}(I_3) = \Omega_{W_1 \cap W_2}$ and $\overline{\overline{I_3}} = \operatorname{rank}(W_1 \cap W_2)$. Set $I_6 = (\operatorname{MorphsZQ} V)^\circ I_1$. Set $I_8 = (\operatorname{MorphsZQ} V)^\circ I_2$. Set $I_5 = (\operatorname{MorphsZQ} V)^\circ I_4$. Set $I_7 = (\operatorname{MorphsZQ} V)^\circ I_3$. For every vector v of Z MQ VectSp V, $v \in \operatorname{Lin}(I_6) + \operatorname{Lin}(I_8)$ iff $v \in \operatorname{Lin}(I_5)$ by [30, (1)], [31, (7)], [16, (9), (10)]. For every vector v of Z MQ VectSp V, $v \in \operatorname{Lin}(I_6) \cap \operatorname{Lin}(I_8)$ iff $v \in \operatorname{Lin}(I_7)$ by [30, (3)], [31, (7)], [16, (9), (10)]. □

Let us consider a torsion-free $\mathbb{Z}$-module V and finite rank, free submodules W_1, W_2 of V. Now we state the propositions:

(62) $\operatorname{rank}(W_1 + W_2) + \operatorname{rank}(W_1 \cap W_2) = \operatorname{rank} W_1 + \operatorname{rank} W_2$.
PROOF: Set $W_5 = W_1 + W_2$. Reconsider $W_4 = W_1$ as a finite rank, free

submodule of W_5. Reconsider $W_7 = W_2$ as a finite rank, free submodule of W_5. $\operatorname{rank}(W_4 + W_7) + \operatorname{rank}(W_4 \cap W_7) = \operatorname{rank} W_4 + \operatorname{rank} W_7$. For every vector v of V, $v \in W_4 + W_7$ iff $v \in W_1 + W_2$ by [12, (92), (25), (28)]. For every vector v of V, $v \in W_4 \cap W_7$ iff $v \in W_1 \cap W_2$ by [12, (94)]. □

(63) If $\operatorname{rank}(W_1 + W_2) = \operatorname{rank} W_2$, then $\operatorname{rank}(W_1 \cap W_2) = \operatorname{rank} W_1$. The theorem is a consequence of (62).

(64) Let us consider a torsion-free $\mathbb{Z}$-module V, finite rank, free submodules W_1, W_2 of V, and a vector v of V. Suppose $v \neq 0_V$ and $W_1 \cap \operatorname{Lin}(\{v\}) = \mathbf{0}_V$ and $(W_1 + W_2) \cap \operatorname{Lin}(\{v\}) = \mathbf{0}_V$. Then $\operatorname{rank}((W_1 + \operatorname{Lin}(\{v\})) \cap W_2) = \operatorname{rank}(W_1 \cap W_2)$.

PROOF: For every vector u of V such that $u \in W_1 \cap W_2$ holds $u \in (W_1 + \operatorname{Lin}(\{v\})) \cap W_2$ by [12, (94), (93)]. There exists a vector u of V such that $u \in (W_1 + \operatorname{Lin}(\{v\})) \cap W_2$ and $u \notin W_1 \cap W_2$ by [12, (44)], [22, (2)]. Consider u being a vector of V such that $u \in (W_1 + \operatorname{Lin}(\{v\})) \cap W_2$ and $u \notin W_1 \cap W_2$. Consider u_1, u_2 being vectors of V such that $u_1 \in W_1$ and $u_2 \in \operatorname{Lin}(\{v\})$ and $u = u_1 + u_2$. □

Let us consider a torsion-free $\mathbb{Z}$-module V, a finite rank, free submodule W of V, and a vector v of V.

Let us assume that $v \neq 0_V$ and $W \cap \operatorname{Lin}(\{v\}) \neq \mathbf{0}_V$. Now we state the propositions:

(65) $\operatorname{rank}(W \cap \operatorname{Lin}(\{v\})) = 1$.

PROOF: $\operatorname{rank} \operatorname{Lin}(\{v\}) = 1$. $\operatorname{rank}(W \cap \operatorname{Lin}(\{v\})) \neq 0$ by [22, (1)], [12, (51)]. □

(66) There exists a vector u of V such that

(i) $u \neq 0_V$, and

(ii) $W \cap \operatorname{Lin}(\{v\}) = \operatorname{Lin}(\{u\})$.

The theorem is a consequence of (65).

(67) Let us consider a torsion-free $\mathbb{Z}$-module V, a finite rank, free submodule W of V, and vectors u, v of V. Suppose $W \cap \operatorname{Lin}(\{v\}) = \mathbf{0}_V$ and $(W + \operatorname{Lin}(\{u\})) \cap \operatorname{Lin}(\{v\}) \neq \mathbf{0}_V$. Then $W \cap \operatorname{Lin}(\{u\}) = \mathbf{0}_V$. The theorem is a consequence of (19).

(68) Let us consider a torsion-free $\mathbb{Z}$-module V, finite rank, free submodules W_1, W_2 of V, and a vector v of V. Suppose $\operatorname{rank}(W_1 \cap W_2) = \operatorname{rank} W_1$ and $(W_1 + W_2) \cap \operatorname{Lin}(\{v\}) \neq \mathbf{0}_V$. Then $W_2 \cap \operatorname{Lin}(\{v\}) \neq \mathbf{0}_V$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ for every finite rank, free submodules W_1, W_2 of V for every vector v of V such that $\operatorname{rank}(W_1 \cap W_2) = \operatorname{rank} W_1$ and $(W_1 + W_2) \cap \operatorname{Lin}(\{v\}) \neq \mathbf{0}_V$ and $\operatorname{rank} W_1 = \$_1$ holds $W_2 \cap \operatorname{Lin}(\{v\}) \neq \mathbf{0}_V$. $\mathcal{P}[0]$ by [22, (1)], [12, (51), (42)], [16, (22)]. For every natural number

n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$ by (26), [14, (20), (16)], (24). For every natural number n, $\mathcal{P}[n]$ from [3, Sch. 2]. □

(69) Let us consider a torsion-free $\mathbb{Z}$-module V, and finite rank, free submodules W_1, W_2, W_3 of V. Suppose $\operatorname{rank}(W_1 + W_2) = \operatorname{rank} W_2$ and W_3 is a submodule of W_1. Then $\operatorname{rank}(W_3 + W_2) = \operatorname{rank} W_2$.

Proof: For every vector v of V such that $v \in W_3 + W_2$ holds $v \in W_1 + W_2$ by [12, (92), (23)]. □

(70) Let us consider a torsion-free $\mathbb{Z}$-module V, finite rank, free submodules W_1, W_2 of V, and a basis I of W_1. Suppose $\operatorname{rank}(W_1 + W_2) = \operatorname{rank} W_2$. Let us consider a vector v of V. If $v \in I$, then $(W_1 \cap W_2) \cap \operatorname{Lin}(\{v\}) \neq \mathbf{0}_V$.

Proof: For every vector v of V such that $v \in I$ holds $(W_1 \cap W_2) \cap \operatorname{Lin}(\{v\}) \neq \mathbf{0}_V$ by [14, (15)], [13, (57), (65)], [9, (31)]. □

(71) Let us consider a torsion-free $\mathbb{Z}$-module V, and finite rank, free submodules W_1, W_2 of V. Suppose $\operatorname{rank}(W_1 \cap W_2) = \operatorname{rank} W_1$. Then there exists an element a of $\mathbb{Z}^{\mathrm{R}}$ such that $a \circ W_1$ is a submodule of W_2.

Proof: Define $\mathcal{P}[\text{natural number}] \equiv$ for every finite rank, free submodules W_1, W_2 of V such that $\operatorname{rank}(W_1 \cap W_2) = \operatorname{rank} W_1$ and $\operatorname{rank} W_1 = \$_1$ there exists an element a of $\mathbb{Z}^{\mathrm{R}}$ such that $a \circ W_1$ is a submodule of W_2. $\mathcal{P}[0]$ by [22, (1)], [12, (55)], (1). For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$ by [12, (25)], [14, (15)], [13, (56)], [14, (20)]. For every natural number n, $\mathcal{P}[n]$ from [3, Sch. 2]. □

References

[1] Grzegorz Bancerek. Cardinal numbers. *Formalized Mathematics*, 1(**2**):377–382, 1990.
[2] Grzegorz Bancerek. Cardinal arithmetics. *Formalized Mathematics*, 1(**3**):543–547, 1990.
[3] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 1990.
[4] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.
[5] Czesław Byliński. Binary operations. *Formalized Mathematics*, 1(**1**):175–180, 1990.
[6] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.
[7] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.
[8] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.
[9] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.
[10] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.
[11] Wolfgang Ebeling. *Lattices and Codes.* Advanced Lectures in Mathematics. Springer Fachmedien Wiesbaden, 2013.
[12] Yuichi Futa, Hiroyuki Okazaki, and Yasunari Shidama. $\mathbb{Z}$-modules. *Formalized Mathematics*, 20(**1**):47–59, 2012. doi:10.2478/v10037-012-0007-z.
[13] Yuichi Futa, Hiroyuki Okazaki, and Yasunari Shidama. Quotient module of $\mathbb{Z}$-module. *Formalized Mathematics*, 20(**3**):205–214, 2012. doi:10.2478/v10037-012-0024-y.

[14] Yuichi Futa, Hiroyuki Okazaki, and Yasunari Shidama. Free $\mathbb{Z}$-module. *Formalized Mathematics*, 20(**4**):275–280, 2012. doi:10.2478/v10037-012-0033-x.

[15] Yuichi Futa, Hiroyuki Okazaki, Daichi Mizushima, and Yasunari Shidama. Gaussian integers. *Formalized Mathematics*, 21(**2**):115–125, 2013. doi:10.2478/forma-2013-0013.

[16] Yuichi Futa, Hiroyuki Okazaki, and Yasunari Shidama. Submodule of free $\mathbb{Z}$-module. *Formalized Mathematics*, 21(**4**):273–282, 2013. doi:10.2478/forma-2013-0029.

[17] Andrzej Kondracki. Basic properties of rational numbers. *Formalized Mathematics*, 1(**5**): 841–845, 1990.

[18] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Formalized Mathematics*, 1(**2**):335–342, 1990.

[19] Rafał Kwiatek and Grzegorz Zwara. The divisibility of integers and integer relatively primes. *Formalized Mathematics*, 1(**5**):829–832, 1990.

[20] A. K. Lenstra, H. W. Lenstra Jr., and L. Lovász. Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261(4), 1982.

[21] Daniele Micciancio and Shafi Goldwasser. Complexity of lattice problems: a cryptographic perspective. *The International Series in Engineering and Computer Science*, 2002.

[22] Kazuhisa Nakasho, Yuichi Futa, Hiroyuki Okazaki, and Yasunari Shidama. Rank of submodule, linear transformations and linearly independent subsets of $\mathbb{Z}$-module. *Formalized Mathematics*, 22(**3**):189–198, 2014. doi:10.2478/forma-2014-0021.

[23] Jan Popiołek. Some properties of functions modul and signum. *Formalized Mathematics*, 1(**2**):263–264, 1990.

[24] Christoph Schwarzweller. The binomial theorem for algebraic structures. *Formalized Mathematics*, 9(**3**):559–564, 2001.

[25] Christoph Schwarzweller. The ring of integers, Euclidean rings and modulo integers. *Formalized Mathematics*, 8(**1**):29–34, 1999.

[26] Andrzej Trybulec. Domains and their Cartesian products. *Formalized Mathematics*, 1(**1**): 115–122, 1990.

[27] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.

[28] Wojciech A. Trybulec. Groups. *Formalized Mathematics*, 1(**5**):821–827, 1990.

[29] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(**2**):291–296, 1990.

[30] Wojciech A. Trybulec. Operations on subspaces in vector space. *Formalized Mathematics*, 1(**5**):871–876, 1990.

[31] Wojciech A. Trybulec. Basis of vector space. *Formalized Mathematics*, 1(**5**):883–885, 1990.

[32] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.

[33] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1 (**1**):73–83, 1990.

[34] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.

Received November 29, 2014

FORMALIZED MATHEMATICS
Vol. 22, No. 4, Pages 291–301, 2014
DOI: 10.2478/forma-2014-0029

DE GRUYTER
OPEN
degruyter.com/view/j/forma

The First Isomorphism Theorem and Other Properties of Rings

Artur Korniłowicz
Institute of Informatics
University of Białystok
Sosnowa 64, 15-887 Białystok
Poland

Christoph Schwarzweller
Institute of Computer Science
University of Gdańsk
Wita Stwosza 57, 80-952 Gdańsk
Poland

Summary. Different properties of rings and fields are discussed [12], [41] and [17]. We introduce ring homomorphisms, their kernels and images, and prove the First Isomorphism Theorem, namely that for a homomorphism $f : R \longrightarrow S$ we have $R/_{\ker(f)} \cong \mathrm{Im}(f)$. Then we define prime and irreducible elements and show that every principal ideal domain is factorial. Finally we show that polynomial rings over fields are Euclidean and hence also factorial.

MSC: 13A05 13A15 03B35

Keywords: commutative algebra; ring theory; first isomorphism theorem

MML identifier: RING_2, version: 8.1.03 5.26.1224

The notation and terminology used in this paper have been introduced in the following articles: [22], [31], [2], [32], [24], [5], [11], [33], [7], [8], [26], [36], [37], [39], [30], [1], [35], [27], [34], [19], [3], [4], [9], [25], [18], [28], [29], [13], [6], [42], [43], [20], [14], [38], [23], [40], [15], [16], [21], and [10].

1. Preliminaries

Let R be a non empty set, f be a non empty finite sequence of elements of R, and x be an element of $\mathrm{dom}\, f$. Note that the functor $f(x)$ yields an element of R. Let X be a set and F_1, F_2 be X-valued finite sequences. One can verify that $F_1 \frown F_2$ is X-valued.

ISSN 1426–2630(Print), 1898-9934(Online)

Now we state the propositions:

(1) Let us consider an add-associative, right zeroed, right complementable, distributive, well unital, non empty double loop structure R, and a finite sequence F of elements of R. Suppose there exists a natural number i such that $i \in \operatorname{dom} F$ and $F(i) = 0_R$. Then $\prod F = 0_R$.

(2) Let us consider an add-associative, right zeroed, right complementable, well unital, distributive, integral domain-like, non degenerated double loop structure R, and a finite sequence F of elements of R. Then $\prod F = 0_R$ if and only if there exists a natural number i such that $i \in \operatorname{dom} F$ and $F(i) = 0_R$. The theorem is a consequence of (1).

Let X be a set.

A chain of X is a sequence of X. Let X be a non empty set and C be a chain of X. We say that C is ascending if and only if

(Def. 1) for every natural number i, $C(i) \subseteq C(i+1)$.

We say that C is stagnating if and only if

(Def. 2) there exists a natural number i such that for every natural number j such that $j \geqslant i$ holds $C(j) = C(i)$.

Let x be an element of X. One can check that $\mathbb{N} \longmapsto x$ is ascending and stagnating as a chain of X and there exists a chain of X which is ascending and stagnating.

Now we state the proposition:

(3) Let us consider a non empty set X, an ascending chain C of X, and natural numbers i, j. If $i \leqslant j$, then $C(i) \subseteq C(j)$.

Let R be a ring. The functor $\operatorname{Ideals} R$ yielding a family of subsets of the carrier of R is defined by the term

(Def. 3) the set of all I where I is an ideal of R.

One can verify that $\operatorname{Ideals} R$ is non empty.

Now we state the propositions:

(4) Let us consider a commutative ring R, an ideal I of R, and an element a of R. If $a \in I$, then $\{a\}$–ideal $\subseteq I$.

(5) Let us consider a ring R, and an ascending chain C of $\operatorname{Ideals} R$. Then $\bigcup$ the set of all $C(i)$ where i is a natural number is an ideal of R.

Let R be a non empty double loop structure and S be a right zeroed, non empty double loop structure. Let us note that $R \longmapsto 0_S$ is additive.

Let S be an add-associative, right zeroed, right complementable, right distributive, non empty double loop structure. Observe that $R \longmapsto 0_S$ is multiplicative.

Let R be a well unital, non empty double loop structure and S be a well unital, non degenerated double loop structure. Note that $R \longmapsto 0_S$ is non unity-preserving.

Let R be a non empty double loop structure. One can verify that id_R is additive, multiplicative, and unity-preserving and id_R is monomorphic and epimorphic.

Let S be a right zeroed, non empty double loop structure. Observe that there exists a function from R into S which is additive.

Let S be an add-associative, right zeroed, right complementable, right distributive, non empty double loop structure. Let us observe that there exists a function from R into S which is multiplicative.

Let R, S be well unital, non empty double loop structures. One can verify that there exists a function from R into S which is unity-preserving.

Let R be a non empty double loop structure and S be an add-associative, right zeroed, right complementable, right distributive, non empty double loop structure. One can verify that there exists a function from R into S which is additive and multiplicative.

2. Homomorphisms, Kernel and Image

Let R, S be rings. We say that S is R-homomorphic if and only if

(Def. 4) there exists a function f from R into S such that f inherits ring homomorphism.

Let R be a ring. One can verify that there exists a ring which is R-homomorphic.

Let R be a commutative ring. Let us observe that there exists a commutative ring which is R-homomorphic and there exists a ring which is R-homomorphic.

Let R be a field. Observe that there exists a field which is R-homomorphic and there exists a commutative ring which is R-homomorphic and there exists a ring which is R-homomorphic.

Let R be a ring and S be an R-homomorphic ring. Note that there exists a function from R into S which is additive, multiplicative, and unity-preserving.

A homomorphism from R to S is an additive, multiplicative, unity-preserving function from R into S. Let R, S, T be rings, f be a unity-preserving function from R into S, and g be a unity-preserving function from S into T. Observe that $g \cdot f$ is unity-preserving as a function from R into T.

Let R be a ring and S be an R-homomorphic ring. Note that every S-homomorphic ring is R-homomorphic.

Let R, S be non empty double loop structures. We introduce R and S are isomorphic as a synonym of R is ring isomorphic to S.

Now we state the propositions:

(6) Let us consider an add-associative, right zeroed, right complementable, non empty double loop structure R, an add-associative, right zeroed, right complementable, right distributive, non empty double loop structure S, and an additive function f from R into S. Then $f(0_R) = 0_S$.

(7) Let us consider an add-associative, right zeroed, right complementable, non empty double loop structure R, an add-associative, right zeroed, right complementable, right distributive, non empty double loop structure S, an additive function f from R into S, and an element x of R. Then $f(-x) = -f(x)$. The theorem is a consequence of (6).

(8) Let us consider an add-associative, right zeroed, right complementable, non empty double loop structure R, an add-associative, right zeroed, right complementable, right distributive, non empty double loop structure S, an additive function f from R into S, and elements x, y of R. Then $f(x - y) = f(x) - f(y)$. The theorem is a consequence of (7).

(9) Let us consider a right unital, non empty double loop structure R, an add-associative, right zeroed, right complementable, right unital, Abelian, right distributive, integral domain-like, non empty double loop structure S, and a multiplicative function f from R into S. Then

(i) $f(1_R) = 0_S$, or

(ii) $f(1_R) = 1_S$.

Let us consider fields E, F and an additive, multiplicative function f from E into F. Now we state the propositions:

(10) $f(1_E) = 0_F$ if and only if $f = E \longmapsto 0_F$.

(11) $f(1_E) = 1_F$ if and only if f is monomorphic.

Let E, F be fields. One can check that every function from E into F which is additive, multiplicative, and unity-preserving is also monomorphic.

Let R be a ring and I be an ideal of R. The canonical homomorphism of I into quotient field yielding a function from R into $R/_I$ is defined by

(Def. 5) for every element a of R, $it(a) = [a]_{\mathrm{EqRel}(R,I)}$.

Let us note that the canonical homomorphism of I into quotient field is additive, multiplicative, and unity-preserving and the canonical homomorphism of I into quotient field is epimorphic and $R/_I$ is R-homomorphic.

Let R be an add-associative, right zeroed, right complementable, non empty double loop structure, S be an add-associative, right zeroed, right complementable, right distributive, non empty double loop structure, and f be an additive function from R into S. One can check that $\ker f$ is non empty.

Let R be a non empty double loop structure and S be an add-associative, right zeroed, right complementable, non empty double loop structure. One can check that $\ker f$ is closed under addition.

Let S be an add-associative, right zeroed, right complementable, right distributive, non empty double loop structure and f be a multiplicative function from R into S. Observe that $\ker f$ is left ideal.

Let S be an add-associative, right zeroed, right complementable, distributive, non empty double loop structure. Let us observe that $\ker f$ is right ideal.

Let R be a well unital, non empty double loop structure, S be a well unital, non degenerated double loop structure, and f be a unity-preserving function from R into S. Observe that $\ker f$ is proper.

Now we state the propositions:

(12) Let us consider a ring R, an R-homomorphic ring S, and a homomorphism f from R to S. Then f is monomorphic if and only if $\ker f = \{0_R\}$. The theorem is a consequence of (6) and (8).

(13) Let us consider a ring R, and an ideal I of R. Then $\ker$ the canonical homomorphism of I into quotient field $= I$.

(14) Let us consider a ring R, and a subset I of R. Then I is an ideal of R if and only if there exists an R-homomorphic ring S and there exists a homomorphism f from R to S such that $\ker f = I$. The theorem is a consequence of (13).

Let R be a ring, S be an R-homomorphic ring, and f be a homomorphism from R to S. The functor $\operatorname{Im} f$ yielding a strict double loop structure is defined by

(Def. 6) the carrier of $it = \operatorname{rng} f$ and the addition of $it =$ (the addition of S) $\restriction \operatorname{rng} f$ and the multiplication of $it =$ (the multiplication of S) $\restriction \operatorname{rng} f$ and the one of $it = 1_S$ and the zero of $it = 0_S$.

Note that $\operatorname{Im} f$ is non empty and $\operatorname{Im} f$ is Abelian, add-associative, right zeroed, and right complementable and $\operatorname{Im} f$ is associative, well unital, and distributive.

Let R be a commutative ring and S be an R-homomorphic commutative ring. One can verify that $\operatorname{Im} f$ is commutative.

Let R be a ring and S be an R-homomorphic ring. Let us note that the functor $\operatorname{Im} f$ yields a strict subring of S. The canonical homomorphism of f into quotient field yielding a function from $R/_{\ker f}$ into $\operatorname{Im} f$ is defined by

(Def. 7) for every element a of R, $it([a]_{\mathrm{EqRel}(R,\ker f)}) = f(a)$.

One can check that the canonical homomorphism of f into quotient field is additive, multiplicative, and unity-preserving and the canonical homomorphism of f into quotient field is monomorphic and epimorphic.

Let us consider a ring R, an R-homomorphic ring S, and a homomorphism f from R to S. Now we state the propositions:

(15) $R/_{\ker f}$ and $\operatorname{Im} f$ are isomorphic.

(16) If f is onto, then $R/_{\ker f}$ and S are isomorphic.

Now we state the proposition:

(17) Let us consider a ring R. Then $R/_{\{0_R\}}$ and R are isomorphic. The theorem is a consequence of (12).

Let R be a ring. Let us note that $R/_{\Omega_R}$ is trivial.

3. Units and Non Units

Let L be a right unital, non empty multiplicative loop structure. Let us note that there exists an element of L which is unital.

A unit of L is a unital element of L. Let L be an add-associative, right zeroed, right complementable, left distributive, non degenerated double loop structure. One can check that there exists an element of L which is non unital.

A non-unit of L is a non unital element of L. Note that 0_L is non unital.

Let L be a right unital, non empty multiplicative loop structure. Let us note that 1_L is unital.

Let L be an add-associative, right zeroed, right complementable, left distributive, right unital, non degenerated double loop structure. One can verify that every unit of L is non zero.

Let F be a field. Note that every non zero element of F is unital.

Let R be an integral domain and u, v be unital elements of R. One can check that $u \cdot v$ is unital.

Let us consider a commutative ring R and elements a, b of R. Now we state the propositions:

(18) $a \mid b$ if and only if $b \in \{a\}$–ideal.

(19) $a \mid b$ if and only if $\{b\}$–ideal $\subseteq \{a\}$–ideal. The theorem is a consequence of (18).

Now we state the propositions:

(20) Let us consider a commutative ring R, and an element a of R. Then a is a unit of R if and only if $\{a\}$–ideal $= \Omega_R$. The theorem is a consequence of (18).

(21) Let us consider a commutative ring R, and elements a, b of R. Then a is associated to b if and only if $\{a\}$–ideal $= \{b\}$–ideal.

4. Prime and Irreducible Elements

Let R be a right unital, non empty double loop structure and x be an element of R. We say that x is prime if and only if

(Def. 8) $x \neq 0_R$ and x is not a unit of R and for every elements a, b of R such that $x \mid a \cdot b$ holds $x \mid a$ or $x \mid b$.

We say that x is irreducible if and only if

(Def. 9) $x \neq 0_R$ and x is not a unit of R and for every element a of R such that $a \mid x$ holds a is unit of R or associated to x.

We introduce x is reducible as an antonym for x is irreducible.

Note that there exists an element of R which is non prime and there exists an element of $\mathbb{Z}^{\mathrm{R}}$ which is prime.

Let R be a right unital, non empty double loop structure. Let us observe that every element of R which is prime is also non zero and non unital and every element of R which is irreducible is also non zero and non unital.

Let R be an integral domain. Observe that every element of R which is prime is also irreducible.

Let F be a field. Let us note that every element of F is reducible.

Let R be a right unital, non empty double loop structure. The functor $\mathrm{IRR}(R)$ yielding a subset of R is defined by the term

(Def. 10) $\{x$, where x is an element of $R : x$ is irreducible$\}$.

Let F be a field. One can check that $\mathrm{IRR}(F)$ is empty.

Now we state the propositions:

(22) Let us consider an integral domain R, a non zero element c of R, and elements b, a, d of R. Suppose $a \cdot b$ is associated to $c \cdot d$ and a is associated to c. Then b is associated to d.

(23) Let us consider an integral domain R, and elements a, b of R. Suppose a is irreducible and b is associated to a. Then b is irreducible.

Let us consider a non degenerated commutative ring R and a non zero element a of R. Now we state the propositions:

(24) a is prime if and only if $\{a\}$–ideal is prime. The theorem is a consequence of (18).

(25) If $\{a\}$–ideal is maximal, then a is irreducible. The theorem is a consequence of (19) and (18).

5. Principal Ideal Domains and Factorial Rings

Note that every field is PID and there exists a non empty double loop structure which is PID.

A principal ideal domain is a PID integral domain. Now we state the proposition:

(26) Let us consider a principal ideal domain R, and a non zero element a of R. Then $\{a\}$–ideal is maximal if and only if a is irreducible. The theorem is a consequence of (19), (20), (18), and (25).

Let R be a principal ideal domain. Observe that every element of R which is irreducible is also prime and every commutative ring which is Euclidean is also PID.

Let R be a principal ideal domain. One can verify that every chain of Ideals R which is ascending is also stagnating.

Let R be a right unital, non empty double loop structure, x be an element of R, and F be a non empty finite sequence of elements of R. We say that F is a factorization of x if and only if

(Def. 11) $x = \prod F$ and for every element i of $\operatorname{dom} F$, $F(i)$ is irreducible.

We say that x is factorizable if and only if

(Def. 12) there exists a non empty finite sequence F of elements of R such that F is a factorization of x.

Assume x is factorizable.

A factorization of x is a non empty finite sequence of elements of R and is defined by

(Def. 13) *it* is a factorization of x.

We say that x is uniquely factorizable if and only if

(Def. 14) x is factorizable and for every factorizations F, G of x, there exists a function B from $\operatorname{dom} F$ into $\operatorname{dom} G$ such that B is bijective and for every element i of $\operatorname{dom} F$, $G(B(i))$ is associated to $F(i)$.

One can verify that every element of R which is uniquely factorizable is also factorizable.

Let R be an integral domain. Let us observe that every element of R which is factorizable is also non zero and non unital.

Let R be a right unital, non empty double loop structure. Let us note that every element of R which is irreducible is also factorizable.

Now we state the propositions:

(27) Let us consider a right unital, non empty double loop structure R, and an element a of R. Then a is irreducible if and only if $\langle a \rangle$ is a factorization of a.

(28) Let us consider a well unital, associative, non empty double loop structure R, elements a, b of R, and non empty finite sequences F, G of elements of R. Suppose F is a factorization of a and G is a factorization of b. Then $F \frown G$ is a factorization of $a \cdot b$.

Let R be a principal ideal domain. Observe that every element of R which is factorizable is also uniquely factorizable.

Let R be a non degenerated ring. We say that R is factorial if and only if

(Def. 15) for every non zero element a of R such that a is a non-unit of R holds a is uniquely factorizable.

One can check that there exists a non degenerated ring which is factorial.

Let R be a factorial, non degenerated ring. Note that every element of R which is non zero and non unital is also factorizable.

A factorial ring is a factorial, non degenerated ring. One can check that every integral domain which is PID is also factorial.

6. Polynomial Rings over Fields

Let L be a field and p be a polynomial of L. The functor $\deg* p$ yielding a natural number is defined by the term

(Def. 16) $\begin{cases} \deg p, & \textbf{if } p \neq \mathbf{0}.\, L, \\ 0, & \textbf{otherwise}. \end{cases}$

The functor $\deg* L$ yielding a function from Polynom-Ring L into $\mathbb{N}$ is defined by

(Def. 17) for every polynomial p of L, $it(p) = \deg* p$.

Now we state the propositions:

(29) Let us consider a field L, a polynomial p of L, and a non zero polynomial q of L. Then $\deg(p \bmod q) < \deg q$.

(30) Let us consider a field L, an element p of Polynom-Ring L, and a non zero element q of Polynom-Ring L. Then there exist elements u, r of Polynom-Ring L such that

(i) $p = u \cdot q + r$, and

(ii) $r = 0_{\text{Polynom-Ring}\, L}$ or $(\deg* L)(r) < (\deg* L)(q)$.

The theorem is a consequence of (29).

Let L be a field. One can check that Polynom-Ring L is Euclidean.

Note that the functor $\deg* L$ yields a DegreeFunction of Polynom-Ring L.

References

[1] Jonathan Backer, Piotr Rudnicki, and Christoph Schwarzweller. Ring ideals. *Formalized Mathematics*, 9(**3**):565–582, 2001.

[2] Grzegorz Bancerek. Cardinal numbers. *Formalized Mathematics*, 1(**2**):377–382, 1990.

[3] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 1990.

[4] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.

[5] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.

[6] Józef Białas. Group and field definitions. *Formalized Mathematics*, 1(**3**):433–439, 1990.

[7] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**): 55–65, 1990.

[8] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.

[9] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.

[10] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.

[11] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.

[12] Nathan Jacobson. *Basic Algebra I.* 2nd edition. Dover Publications Inc., 2009.

[13] Andrzej Kondracki. Basic properties of rational numbers. *Formalized Mathematics*, 1(**5**): 841–845, 1990.

[14] Artur Korniłowicz. Quotient rings. *Formalized Mathematics*, 13(**4**):573–576, 2005.

[15] Jarosław Kotowicz. Quotient vector spaces and functionals. *Formalized Mathematics*, 11 (**1**):59–68, 2003.

[16] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Formalized Mathematics*, 1(**2**):335–342, 1990.

[17] Heinz Lüneburg. *Die grundlegenden Strukturen der Algebra (in German).* Oldenbourg Wisenschaftsverlag, 1999.

[18] Robert Milewski. The ring of polynomials. *Formalized Mathematics*, 9(**2**):339–346, 2001.

[19] Michał Muzalewski. Opposite rings, modules and their morphisms. *Formalized Mathematics*, 3(**1**):57–65, 1992.

[20] Michał Muzalewski. Category of rings. *Formalized Mathematics*, 2(**5**):643–648, 1991.

[21] Michał Muzalewski. Construction of rings and left-, right-, and bi-modules over a ring. *Formalized Mathematics*, 2(**1**):3–11, 1991.

[22] Michał Muzalewski and Wojciech Skaba. From loops to Abelian multiplicative groups with zero. *Formalized Mathematics*, 1(**5**):833–840, 1990.

[23] Beata Padlewska. Families of sets. *Formalized Mathematics*, 1(**1**):147–152, 1990.

[24] Konrad Raczkowski and Paweł Sadowski. Equivalence relations and classes of abstraction. *Formalized Mathematics*, 1(**3**):441–444, 1990.

[25] Piotr Rudnicki and Andrzej Trybulec. Multivariate polynomials with arbitrary number of variables. *Formalized Mathematics*, 9(**1**):95–110, 2001.

[26] Christoph Schwarzweller. The correctness of the generic algorithms of Brown and Henrici concerning addition and multiplication in fraction fields. *Formalized Mathematics*, 6(**3**): 381–388, 1997.

[27] Christoph Schwarzweller. The ring of integers, Euclidean rings and modulo integers. *Formalized Mathematics*, 8(**1**):29–34, 1999.

[28] Christoph Schwarzweller. The field of quotients over an integral domain. *Formalized Mathematics*, 7(**1**):69–79, 1998.

[29] Christoph Schwarzweller. Introduction to rational functions. *Formalized Mathematics*, 20 (**2**):181–191, 2012. doi:10.2478/v10037-012-0021-1.

[30] Christoph Schwarzweller and Agnieszka Rowińska-Schwarzweller. Schur's theorem on the stability of networks. *Formalized Mathematics*, 14(**4**):135–142, 2006. doi:10.2478/v10037-006-0017-9.

[31] Yasunari Shidama, Hikofumi Suzuki, and Noboru Endou. Banach algebra of bounded

functionals. *Formalized Mathematics*, 16(**2**):115–122, 2008. doi:10.2478/v10037-008-0017-z.

[32] Andrzej Trybulec. Domains and their Cartesian products. *Formalized Mathematics*, 1(**1**): 115–122, 1990.

[33] Andrzej Trybulec. Binary operations applied to functions. *Formalized Mathematics*, 1 (**2**):329–334, 1990.

[34] Andrzej Trybulec. On the sets inhabited by numbers. *Formalized Mathematics*, 11(**4**): 341–347, 2003.

[35] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.

[36] Wojciech A. Trybulec. Groups. *Formalized Mathematics*, 1(**5**):821–827, 1990.

[37] Wojciech A. Trybulec. Lattice of subgroups of a group. Frattini subgroup. *Formalized Mathematics*, 2(**1**):41–47, 1991.

[38] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(**2**):291–296, 1990.

[39] Wojciech A. Trybulec and Michał J. Trybulec. Homomorphisms and isomorphisms of groups. Quotient group. *Formalized Mathematics*, 2(**4**):573–578, 1991.

[40] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.

[41] B.L. van der Waerden. *Algebra I.* 4th edition. Springer, 2003.

[42] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1 (**1**):73–83, 1990.

[43] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.

Received November 29, 2014

FORMALIZED MATHEMATICS
Vol. 22, No. 4, Pages 303–311, 2014
DOI: 10.2478/forma-2014-0030

DE GRUYTER OPEN
degruyter.com/view/j/forma

Bidual Spaces and Reflexivity of Real Normed Spaces[1]

Keiko Narita
Hirosaki-city
Aomori, Japan

Noboru Endou
Gifu National College of Technology
Gifu, Japan

Yasunari Shidama
Shinshu University
Nagano, Japan

Summary. In this article, we considered bidual spaces and reflexivity of real normed spaces. At first we proved some corollaries applying Hahn-Banach theorem and showed related theorems. In the second section, we proved the norm of dual spaces and defined the natural mapping, from real normed spaces to bidual spaces. We also proved some properties of this mapping. Next, we defined real normed space of $\mathbb{R}$, real number spaces as real normed spaces and proved related theorems. We can regard linear functionals as linear operators by this definition. Accordingly we proved Uniform Boundedness Theorem for linear functionals using the theorem (5) from [21]. Finally, we defined reflexivity of real normed spaces and proved some theorems about isomorphism of linear operators. Using them, we proved some properties about reflexivity. These formalizations are based on [19], [20], [8] and [1].

MSC: 46B10 46A25 03B35

Keywords: continuous dual space; topological duality; reflexivity

MML identifier: DUALSP02, version: 8.1.03 5.26.1224

The notation and terminology used in this paper have been introduced in the following articles: [2], [14], [7], [3], [4], [16], [22], [24], [15], [18], [13], [5], [10], [29], [25], [26], [11], [28], [12], and [6].

[1]This work was supported by JSPS KAKENHI 22300285 and 23500029.

ISSN 1426–2630(Print), 1898-9934(Online)

1. The Application of Hahn-Banach Theorem

Now we state the propositions:

(1) Let us consider a real normed space V, a real normed subspace X of V, a point x_0 of V, and a real number d. Suppose there exists a non empty subset Z of $\mathbb{R}$ such that $Z = \{\|x - x_0\|$, where x is a point of $V : x \in X\}$ and $d = \inf Z > 0$. Then

   (i) $x_0 \notin X$, and

   (ii) there exists a point G of DualSp(V) such that for every point x of V such that $x \in X$ holds (Bound2Lipschitz(G, V))(x) $= 0$ and (Bound2Lipschitz(G, V))(x_0) $= 1$ and $\|G\| = \frac{1}{d}$.

Proof: Consider Z being a non empty subset of $\mathbb{R}$ such that $Z = \{\|x - x_0\|$, where x is a point of $V : x \in X\}$ and $d = \inf Z > 0$. Set $M_0 = \{z + a \cdot x_0$, where z is a point of V, a is a real number : $z \in X\}$. Set $M =$ NLin M_0. M_0 is linearly closed by [25, (20), (21)]. For every point v of M, there exists a point x of V and there exists a real number a such that $v = x + a \cdot x_0$ and $x \in X$ by [13, (31)]. Reconsider $r_0 = 0$ as a real number. For every extended real r such that $r \in Z$ holds $r_0 \leqslant r$. For every points x_1, x_2 of V and for every real numbers a_1, a_2 such that x_1, $x_2 \in X$ and $x_1 + a_1 \cdot x_0 = x_2 + a_2 \cdot x_0$ holds $x_1 = x_2$ and $a_1 = a_2$ by [26, (5), (35), (15)]. Define $\mathcal{P}[\text{object}, \text{object}] \equiv$ there exists a point z of V and there exists a real number a such that $z \in X$ and $\$_1 = z + a \cdot x_0$ and $\$_2 = a$. For every element v of M, there exists an element a of $\mathbb{R}$ such that $\mathcal{P}[v, a]$. Consider f being a function from M into $\mathbb{R}$ such that for every element x of M, $\mathcal{P}[x, f(x)]$ from [4, Sch. 3]. For every point v of M and for every point z of V and for every real number a such that $z \in X$ and $v = z + a \cdot x_0$ holds $f(v) = a$. f is a linear functional in M by [13, (28)], [25, (20), (21)]. For every point v of M, $|f(v)| \leqslant \frac{1}{d} \cdot \|v\|$ by [17, (2)], [18, (2)], [26, (30), (25)]. Reconsider $F = f$ as a point of DualSp(M). Consider g being a Lipschitzian linear functional in V, G being a point of DualSp(V) such that $g = G$ and $g \restriction$(the carrier of M) $= f$ and $\|G\| = \|F\|$. For every point x of V such that $x \in X$ holds (Bound2Lipschitz(G, V))(x) $= 0$ by [26, (10)], [3, (49)]. □

(2) Let us consider a real normed space V, a non empty subset Y of V, and a point x_0 of V. Suppose Y is linearly closed and closed and $x_0 \notin Y$. Then there exists a point G of DualSp(V) such that

   (i) for every point x of V such that $x \in Y$ holds (Bound2Lipschitz(G, V))(x) $= 0$, and

(ii) $(\text{Bound2Lipschitz}(G, V))(x_0) = 1$.

Proof: Set $X = \text{NLin}\,Y$. Set $Z = \{\|x - x_0\|$, where x is a point of $V : x \in X\}$. Reconsider $r_0 = 0$ as a real number. For every extended real r such that $r \in Z$ holds $r_0 \leqslant r$. Reconsider $d = \inf Z$ as a real number. $d > 0$ by [9, (16), (7)], [18, (7)]. Consider G being a point of $\text{DualSp}(V)$ such that for every point x of V such that $x \in X$ holds $(\text{Bound2Lipschitz}(G, V))(x) = 0$ and $(\text{Bound2Lipschitz}(G, V))(x_0) = 1$ and $\|G\| = \frac{1}{d}$. □

Let us consider a real normed space V and a point x_0 of V.

Let us assume that $x_0 \neq 0_V$. Now we state the propositions:

(3) There exists a point G of $\text{DualSp}(V)$ such that

(i) $(\text{Bound2Lipschitz}(G, V))(x_0) = 1$, and

(ii) $\|G\| = \frac{1}{\|x_0\|}$.

Proof: Set $X = \text{NLin}\{0_V\}$. Set $Y =$ the carrier of $\text{Lin}(\{0_V\})$. For every object s, $s \in Y$ iff $s \in \{0_V\}$ by [27, (8)]. Set $Z = \{\|x - x_0\|$, where x is a point of $V : x \in X\}$. For every object s, $s \in Z$ iff $s \in \{\|x_0\|\}$ by [18, (2)]. Reconsider $d = \inf Z$ as a real number. Consider G being a point of $\text{DualSp}(V)$ such that for every point x of V such that $x \in X$ holds $(\text{Bound2Lipschitz}(G, V))(x) = 0$ and $(\text{Bound2Lipschitz}(G, V))(x_0) = 1$ and $\|G\| = \frac{1}{d}$. □

(4) There exists a point F of $\text{DualSp}(V)$ such that

(i) $\|F\| = 1$, and

(ii) $(\text{Bound2Lipschitz}(F, V))(x_0) = \|x_0\|$.

The theorem is a consequence of (3).

Let us consider a real normed space V.

Let us assume that V is not trivial. Now we state the propositions:

(5) There exists a point F of $\text{DualSp}(V)$ such that $\|F\| = 1$. The theorem is a consequence of (4).

(6) $\text{DualSp}(V)$ is not trivial. The theorem is a consequence of (5).

2. Bidual Spaces of Real Normed Spaces

Let us consider a real normed space V and a point x of V. Now we state the propositions:

(7) Suppose V is not trivial. Then

(i) there exists a non empty subset X of $\mathbb{R}$ such that $X = \{|(\text{Bound2Lipschitz}(F, V))(x)|$, where F is a point of $\text{DualSp}(V) : \|F\| = 1\}$ and $\|x\| = \sup X$, and

(ii) there exists a non empty subset Y of $\mathbb{R}$ such that $Y = \{|(\text{Bound2Lipschitz}(F, V))(x)|$, where F is a point of $\text{DualSp}(V)$: $\|F\| \leqslant 1\}$ and $\|x\| = \sup Y$.

The theorem is a consequence of (5) and (4).

(8) If for every Lipschitzian linear functional f in V, $f(x) = 0$, then $x = 0_V$. The theorem is a consequence of (3).

Let X be a real normed space and x be a point of X. The functor Bidual x yielding a point of DualSp(DualSp(X)) is defined by

(Def. 1) for every point f of DualSp(X), $it(f) = f(x)$.

The functor BidualFunc X yielding a function from X into DualSp(DualSp(X)) is defined by

(Def. 2) for every point x of X, $it(x) = \text{Bidual}\, x$.

Let us observe that BidualFunc X is additive and homogeneous and BidualFunc X is one-to-one.

Let us consider a real normed space X.

Let us assume that X is not trivial. Now we state the propositions:

(9) (i) BidualFunc X is a linear operator from X into DualSp(DualSp(X)), and

(ii) for every point x of X, $\|x\| = \|(\text{BidualFunc}\, X)(x)\|$.

(10) There exists a real normed subspace D of DualSp(DualSp(X)) and there exists a Lipschitzian linear operator L from X into D such that L is bijective and $D = \Im(\text{BidualFunc}\, X)$ and for every point x of X, $L(x) = \text{Bidual}\, x$ and for every point x of X, $\|x\| = \|L(x)\|$.

PROOF: Set $F = \text{BidualFunc}\, X$. Set $V_1 = \text{rng}\, F$. $V_1 \neq \emptyset$ by [29, (42)]. Reconsider $L = \text{BidualFunc}\, X$ as a function from X into $\Im(F)$. L is additive by [13, (28)]. L is homogeneous by [13, (28)]. For every point x of X, $\|x\| = \|L(x)\|$ by [13, (28)]. □

3. Uniform Boundedness Theorem for Linear Functionals

The real normed space of $\mathbb{R}$ yielding a real normed space is defined by the term

(Def. 3) $\langle \mathbb{R}, 0 (\in \mathbb{R}), +_{\mathbb{R}}, \cdot_{\mathbb{R}}, |\square|_{\mathbb{R}} \rangle$.

Now we state the proposition:

(11) Let us consider a real normed space X, an element x of $\mathbb{R}$, and a point v of the real normed space of $\mathbb{R}$. If $x = v$, then $-x = -v$.

Let us consider a real normed space X and an object x. Now we state the propositions:

(12) x is an additive, homogeneous function from X into $\mathbb{R}$ if and only if x is an additive, homogeneous function from X into the real normed space of $\mathbb{R}$.

(13) x is a Lipschitzian, additive, homogeneous function from X into $\mathbb{R}$ if and only if x is a Lipschitzian, additive, homogeneous function from X into the real normed space of $\mathbb{R}$. The theorem is a consequence of (12).

Now we state the propositions:

(14) Let us consider a real normed space X. Then the carrier of $\mathrm{DualSp}(X)$ = the carrier of the real norm space of bounded linear operators from X into the real normed space of $\mathbb{R}$. The theorem is a consequence of (13).

(15) Let us consider a real normed space X, points x, y of $\mathrm{DualSp}(X)$, and points v, w of the real norm space of bounded linear operators from X into the real normed space of $\mathbb{R}$. If $x = v$ and $y = w$, then $x + y = v + w$.
PROOF: Reconsider $z = x + y$ as a point of $\mathrm{DualSp}(X)$. Reconsider $u = v + w$ as a point of the real norm space of bounded linear operators from X into the real normed space of $\mathbb{R}$. For every object t such that $t \in \mathrm{dom}\, z$ holds $z(t) = u(t)$ by [14, (29)], [22, (35)]. □

(16) Let us consider a real normed space X, an element a of $\mathbb{R}$, a point x of $\mathrm{DualSp}(X)$, and a point v of the real norm space of bounded linear operators from X into the real normed space of $\mathbb{R}$. If $x = v$, then $a \cdot x = a \cdot v$.
PROOF: Reconsider $z = a \cdot x$ as a point of $\mathrm{DualSp}(X)$. Reconsider $u = a \cdot v$ as a point of the real norm space of bounded linear operators from X into the real normed space of $\mathbb{R}$. For every object t such that $t \in \mathrm{dom}\, z$ holds $z(t) = u(t)$ by [14, (30)], [22, (36)]. □

Let us consider a real normed space X, a point x of $\mathrm{DualSp}(X)$, and a point v of the real norm space of bounded linear operators from X into the real normed space of $\mathbb{R}$.

Let us assume that $x = v$. Now we state the propositions:

(17) $-x = -v$. The theorem is a consequence of (16).

(18) $\|x\| = \|v\|$.

Now we state the propositions:

(19) Let us consider a real normed space X, and a subset L of X. Suppose X is not trivial and for every point f of $\mathrm{DualSp}(X)$, there exists a real number K_1 such that $0 \leqslant K_1$ and for every point x of X such that $x \in L$ holds $|f(x)| \leqslant K_1$. Then there exists a real number M such that

(i) $0 \leqslant M$, and

(ii) for every point x of X such that $x \in L$ holds $\|x\| \leqslant M$.

The theorem is a consequence of (14) and (18).

(20) Let us consider a real normed space X, and a non empty subset L of X. Suppose X is not trivial and for every point f of DualSp(X), there exists a subset Y_1 of $\mathbb{R}$ such that $Y_1 = \{|f(x)|$, where x is a point of $X : x \in L\}$ and $\sup Y_1 < +\infty$. Then there exists a subset Y of $\mathbb{R}$ such that

(i) $Y = \{\|x\|$, where x is a point of $X : x \in L\}$, and

(ii) $\sup Y < +\infty$.

PROOF: For every point f of DualSp(X), there exists a real number K_1 such that $0 \leqslant K_1$ and for every point x of X such that $x \in L$ holds $|f(x)| \leqslant K_1$ by [2, (46)]. Consider M being a real number such that $0 \leqslant M$ and for every point x of X such that $x \in L$ holds $\|x\| \leqslant M$. Consider x_0 being an object such that $x_0 \in L$. Set $Y = \{\|x\|$, where x is a point of $X : x \in L\}$. $Y \subseteq \mathbb{R}$. For every extended real r such that $r \in Y$ holds $r \leqslant M$. □

4. Reflexivity of Real Normed Spaces

Let X be a real normed space. We say that X is reflexive if and only if

(Def. 4) BidualFunc X is onto.

Let us consider a real normed space X. Now we state the propositions:

(21) X is reflexive if and only if for every point f of DualSp(DualSp(X)), there exists a point x of X such that for every point g of DualSp(X), $f(g) = g(x)$.

(22) X is reflexive if and only if $\Im$(BidualFunc X) = DualSp(DualSp(X)).

(23) If X is non trivial and reflexive, then X is a real Banach space.

PROOF: For every sequence s_1 of X such that s_1 is Cauchy sequence by norm holds s_1 is convergent by [23, (8)], [3, (13)], [26, (16)], [4, (113)]. □

Now we state the propositions:

(24) Let us consider a real Banach space X, and a non empty subset M of X. Suppose X is reflexive and M is linearly closed and closed. Then NLin M is reflexive.

PROOF: Set M_0 = NLin M. For every point y of DualSp(DualSp(M_0)), there exists a point x of M_0 such that for every point g of DualSp(M_0), $y(g) = g(x)$ by [4, (32)], [13, (28)], [3, (49)], [14, (26), (29), (30)]. □

(25) Let us consider real normed spaces X, Y, a Lipschitzian linear operator L from X into Y, and a Lipschitzian linear functional y in Y. Then $y \cdot L$ is a Lipschitzian linear functional in X.

PROOF: Consider M being a real number such that $0 \leqslant M$ and for every vector x of X, $\|L(x)\| \leqslant M \cdot \|x\|$. Set $x = y \cdot L$. For every vectors v, w of X, $x(v+w) = x(v) + x(w)$ by [3, (13)]. For every vector v of X and for every real number r, $x(r \cdot v) = r \cdot x(v)$ by [3, (13)]. Consider N being a real number such that $0 \leqslant N$ and for every vector v of Y, $|y(v)| \leqslant N \cdot \|v\|$. For every vector v of X, $|x(v)| \leqslant M \cdot N \cdot \|v\|$ by [3, (13)]. □

(26) Let us consider real normed spaces X, Y, and a Lipschitzian linear operator L from X into Y. Suppose L is isomorphism. Then there exists a Lipschitzian linear operator T from DualSp(X) into DualSp(Y) such that

(i) T is isomorphism, and

(ii) for every point x of DualSp(X), $T(x) = x \cdot L^{-1}$.

PROOF: Consider K being a Lipschitzian linear operator from Y into X such that $K = L^{-1}$ and K is isomorphism. Define $\mathcal{P}[\text{function}, \text{function}] \equiv \$_2 = \$_1 \cdot K$. For every element x of DualSp(X), there exists an element y of DualSp(Y) such that $\mathcal{P}[x, y]$. Consider T being a function from DualSp(X) into DualSp(Y) such that for every element x of DualSp(X), $\mathcal{P}[x, T(x)]$ from [4, Sch. 3]. For every points v, w of DualSp(X), $T(v+w) = T(v) + T(w)$ by [3, (13)], [14, (29)]. For every point v of DualSp(X) and for every real number r, $T(r \cdot v) = r \cdot T(v)$ by [3, (13)], [14, (30)]. For every object v such that $v \in$ the carrier of DualSp(Y) there exists an object s such that $s \in$ the carrier of DualSp(X) and $v = T(s)$ by (25), [29, (36)], [3, (39)], [29, (51)]. For every point v of DualSp(X), $\|T(v)\| = \|v\|$ by [3, (34), (13)], [14, (23)]. For every objects x_1, x_2 such that $x_1, x_2 \in$ the carrier of DualSp(X) and $T(x_1) = T(x_2)$ holds $x_1 = x_2$ by [26, (16), (5)], [18, (6)]. □

(27) Let us consider real normed spaces X, Y, a Lipschitzian linear operator L from X into Y, and a Lipschitzian linear operator T from DualSp(X) into DualSp(Y). Suppose L is isomorphism and T is isomorphism and for every point x of DualSp(X), $T(x) = x \cdot L^{-1}$. Then there exists a Lipschitzian linear operator S from DualSp(Y) into DualSp(X) such that

(i) S is isomorphism, and

(ii) $S = T^{-1}$, and

(iii) for every point y of DualSp(Y), $S(y) = y \cdot L$.

PROOF: Consider K being a Lipschitzian linear operator from Y into X such that $K = L^{-1}$ and K is isomorphism. Consider S being a Lipschitzian linear operator from DualSp(Y) into DualSp(X) such that S is isomorphism and for every point y of DualSp(Y), $S(y) = y \cdot K^{-1}$. For every objects y, x, $y \in$ the carrier of DualSp(Y) and $S(y) = x$ iff $x \in$ the carrier of DualSp(X) and $T(x) = y$ by [4, (5)], [29, (36)], [3, (39)], [29, (51)]. □

(28) Let us consider real normed spaces X, Y. Suppose there exists a Lipschitzian linear operator L from X into Y such that L is isomorphism. Then X is reflexive if and only if Y is reflexive.

(29) Let us consider a real normed space X. Suppose X is not trivial. Then there exists a Lipschitzian linear operator L from X into $\Im$(BidualFunc X) such that L is isomorphism. The theorem is a consequence of (10).

(30) Let us consider a real Banach space X. Suppose X is not trivial. Then X is reflexive if and only if DualSp(X) is reflexive.

PROOF: DualSp(X) is not trivial. Consider L being a Lipschitzian linear operator from X into $\Im$(BidualFunc X) such that L is isomorphism. Set $f =$ BidualFunc X. rng $f \neq \emptyset$ by [29, (42)]. $\Im(f)$ is reflexive. □

References

[1] Haim Brezis. *Functional Analysis, Sobolev Spaces and Partial Differential Equations.* Springer, 2011.

[2] Czesław Byliński. The complex numbers. *Formalized Mathematics*, 1(**3**):507–513, 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] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.

[6] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.

[7] Agata Darmochwał. The Euclidean space. *Formalized Mathematics*, 2(**4**):599–603, 1991.

[8] Peter D. Dax. *Functional Analysis.* Pure and Applied Mathematics: A Wiley Series of Texts, Monographs and Tracts. Wiley Interscience, 2002.

[9] Noboru Endou, Yasunari Shidama, and Katsumasa Okamura. Baire's category theorem and some spaces generated from real normed space. *Formalized Mathematics*, 14(**4**): 213–219, 2006. doi:10.2478/v10037-006-0024-x.

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

[11] Jarosław Kotowicz. Convergent real sequences. Upper and lower bound of sets of real numbers. *Formalized Mathematics*, 1(**3**):477–481, 1990.

[12] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Formalized Mathematics*, 1(**2**):335–342, 1990.

[13] Kazuhisa Nakasho, Yuichi Futa, and Yasunari Shidama. Topological properties of real normed space. *Formalized Mathematics*, 22(**3**):209–223, 2014. doi:10.2478/forma-2014-0024.

[14] Keiko Narita, Noboru Endou, and Yasunari Shidama. Dual spaces and Hahn-Banach theorem. *Formalized Mathematics*, 22(**1**):69–77, 2014. doi:10.2478/forma-2014-0007.

[15] Takaya Nishiyama, Keiji Ohkubo, and Yasunari Shidama. The continuous functions on normed linear spaces. *Formalized Mathematics*, 12(**3**):269–275, 2004.

[16] Bogdan Nowak and Andrzej Trybulec. Hahn-Banach theorem. *Formalized Mathematics*, 4(**1**):29–34, 1993.

[17] Jan Popiołek. Some properties of functions modul and signum. *Formalized Mathematics*, 1(**2**):263–264, 1990.

[18] Jan Popiołek. Real normed space. *Formalized Mathematics*, 2(**1**):111–115, 1991.

[19] Michael Reed and Barry Simon. *Methods of modern mathematical physics*. Vol. 1. Academic Press, New York, 1972.

[20] Walter Rudin. *Functional Analysis*. New York, McGraw-Hill, 2nd edition, 1991.

[21] Hideki Sakurai, Hisayoshi Kunimune, and Yasunari Shidama. Uniform boundedness principle. *Formalized Mathematics*, 16(**1**):19–21, 2008. doi:10.2478/v10037-008-0003-5.

[22] Yasunari Shidama. Banach space of bounded linear operators. *Formalized Mathematics*, 12(**1**):39–48, 2004.

[23] Yasumasa Suzuki, Noboru Endou, and Yasunari Shidama. Banach space of absolute summable real sequences. *Formalized Mathematics*, 11(**4**):377–380, 2003.

[24] Andrzej Trybulec. On the sets inhabited by numbers. *Formalized Mathematics*, 11(**4**): 341–347, 2003.

[25] Wojciech A. Trybulec. Subspaces and cosets of subspaces in real linear space. *Formalized Mathematics*, 1(**2**):297–301, 1990.

[26] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(**2**):291–296, 1990.

[27] Wojciech A. Trybulec. Subspaces of real linear space generated by one, two, or three vectors and their cosets. *Formalized Mathematics*, 3(**2**):271–274, 1992.

[28] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.

[29] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1 (**1**):73–83, 1990.

Received November 29, 2014

FORMALIZED MATHEMATICS
Vol. 22, No. 4, Pages 313–319, 2014
DOI: 10.2478/forma-2014-0031

DE GRUYTER OPEN
degruyter.com/view/j/forma

Some Facts about Trigonometry and Euclidean Geometry

Roland Coghetto
Rue de la Brasserie 5
7100 La Louvière, Belgium

Summary. We calculate the values of the trigonometric functions for angles: $\frac{\pi}{3}$ and $\frac{\pi}{6}$, by [16]. After defining some trigonometric identities, we demonstrate conventional trigonometric formulas in the triangle, and the geometric property, by [14], of the triangle inscribed in a semicircle, by the proposition 3.31 in [15]. Then we define the diameter of the circumscribed circle of a triangle using the definition of the area of a triangle and prove some identities of a triangle [9]. We conclude by indicating that the diameter of a circle is twice the length of the radius.

MSC: 51M04 03B35

Keywords: Euclidean geometry; trigonometry; circumcircle; right-angled

MML identifier: `EUCLID10`, version: `8.1.03 5.26.1224`

The notation and terminology used in this paper have been introduced in the following articles: [1], [10], [11], [19], [25], [3], [12], [5], [21], [2], [28], [6], [7], [24], [29], [23], [18], [26], [27], [13], and [8].

1. Values of the Trigonometric Functions for Angles: $\frac{\pi}{3}$ and $\frac{\pi}{6}$

Let us consider a real number a. Now we state the propositions:

(1) $\sin(\pi - a) = \sin a$.

(2) $\cos(\pi - a) = -\cos a$.

(3) $\sin(2 \cdot \pi - a) = -\sin a$.

(4) $\cos(2 \cdot \pi - a) = \cos a$.

(5) $\sin(-2 \cdot \pi + a) = \sin a$.

ISSN 1426–2630(Print), 1898-9934(Online)

(6) $\cos(-2 \cdot \pi + a) = \cos a$.

(7) $\sin(\frac{3 \cdot \pi}{2} + a) = -\cos a$.

(8) $\cos(\frac{3 \cdot \pi}{2} + a) = \sin a$.

(9) $\sin(\frac{3 \cdot \pi}{2} + a) = -\sin(\frac{\pi}{2} - a)$. The theorem is a consequence of (7).

(10) $\cos(\frac{3 \cdot \pi}{2} + a) = \cos(\frac{\pi}{2} - a)$. The theorem is a consequence of (8).

(11) $\sin(\frac{2 \cdot \pi}{3} - a) = \sin(\frac{\pi}{3} + a)$.

(12) $\cos(\frac{2 \cdot \pi}{3} - a) = -\cos(\frac{\pi}{3} + a)$.

(13) $\sin(\frac{2 \cdot \pi}{3} + a) = \sin(\frac{\pi}{3} - a)$.

Now we state the propositions:

(14) $\cos \frac{\pi}{3} = \frac{1}{2}$.

(15) $\sin \frac{\pi}{3} = \frac{\sqrt{3}}{2}$.

Proof: $\sin \frac{\pi}{3} \geqslant 0$ by [20, (5)], [29, (79), (81)]. □

(16) $\operatorname{tg} \frac{\pi}{3} = \sqrt{3}$. The theorem is a consequence of (14) and (15).

(17) $\sin \frac{\pi}{6} = \frac{1}{2}$. The theorem is a consequence of (14).

(18) $\cos \frac{\pi}{6} = \frac{\sqrt{3}}{2}$. The theorem is a consequence of (15).

(19) $\operatorname{tg} \frac{\pi}{6} = \frac{\sqrt{3}}{3}$. The theorem is a consequence of (17) and (18).

(20) (i) $\sin(-\frac{\pi}{6}) = -\frac{1}{2}$, and

(ii) $\cos(-\frac{\pi}{6}) = \frac{\sqrt{3}}{2}$, and

(iii) $\operatorname{tg}(-\frac{\pi}{6}) = -\frac{\sqrt{3}}{3}$, and

(iv) $\sin(-\frac{\pi}{3}) = -\frac{\sqrt{3}}{2}$, and

(v) $\cos(-\frac{\pi}{3}) = \frac{1}{2}$, and

(vi) $\operatorname{tg}(-\frac{\pi}{3}) = -\sqrt{3}$.

(21) (i) $\arcsin \frac{1}{2} = \frac{\pi}{6}$, and

(ii) $\arcsin \frac{\sqrt{3}}{2} = \frac{\pi}{3}$.

The theorem is a consequence of (15) and (17).

(22) $\sin \frac{2 \cdot \pi}{3} = \frac{\sqrt{3}}{2}$. The theorem is a consequence of (11) and (15).

(23) $\cos \frac{2 \cdot \pi}{3} = -\frac{1}{2}$. The theorem is a consequence of (12) and (14).

2. Some Trigonometric Identities

Now we state the proposition:

(24) Let us consider a real number x. Then $(\sin(-x))^{\mathbf{2}} = (\sin x)^{\mathbf{2}}$.

Let us consider real numbers x, y, z. Now we state the propositions:

(25) If $x + y + z = \pi$, then $(\sin x)^{\mathbf{2}} + (\sin y)^{\mathbf{2}} - 2 \cdot \sin x \cdot \sin y \cdot \cos z = (\sin z)^{\mathbf{2}}$.

(26) If $x - y + z = \pi$, then $(\sin x)^{\mathbf{2}} + (\sin y)^{\mathbf{2}} + 2 \cdot \sin x \cdot \sin y \cdot \cos z = (\sin z)^{\mathbf{2}}$. The theorem is a consequence of (24) and (25).

(27) Suppose $x - (-2 \cdot \pi + y) + z = \pi$. Then $(\sin x)^{\mathbf{2}} + (\sin y)^{\mathbf{2}} + 2 \cdot \sin x \cdot \sin y \cdot \cos z = (\sin z)^{\mathbf{2}}$. The theorem is a consequence of (24), (5), and (25).

(28) If $\pi - x - (\pi - y) + z = \pi$, then $(\sin x)^{\mathbf{2}} + (\sin y)^{\mathbf{2}} + 2 \cdot \sin x \cdot \sin y \cdot \cos z = (\sin z)^{\mathbf{2}}$. The theorem is a consequence of (24), (1), and (25).

Now we state the proposition:

(29) Let us consider a real number a. Then $\sin(3 \cdot a) = 4 \cdot \sin a \cdot \sin(\frac{\pi}{3} + a) \cdot \sin(\frac{\pi}{3} - a)$. The theorem is a consequence of (15).

3. Trigonometric Functions and Right Triangle

Let us consider points A, B, C of $\mathcal{E}^2_{\rm T}$.

Let us assume that A, B, C form a triangle. Now we state the propositions:

(30) (i) $\measuredangle(A, B, C)$ is not zero, and

(ii) $\measuredangle(B, C, A)$ is not zero, and

(iii) $\measuredangle(C, A, B)$ is not zero, and

(iv) $\measuredangle(A, C, B)$ is not zero, and

(v) $\measuredangle(C, B, A)$ is not zero, and

(vi) $\measuredangle(B, A, C)$ is not zero.

(31) (i) $\measuredangle(A, B, C) = 2 \cdot \pi - \measuredangle(C, B, A)$, and

(ii) $\measuredangle(B, C, A) = 2 \cdot \pi - \measuredangle(A, C, B)$, and

(iii) $\measuredangle(C, A, B) = 2 \cdot \pi - \measuredangle(B, A, C)$, and

(iv) $\measuredangle(B, A, C) = 2 \cdot \pi - \measuredangle(C, A, B)$, and

(v) $\measuredangle(A, C, B) = 2 \cdot \pi - \measuredangle(B, C, A)$, and

(vi) $\measuredangle(C, B, A) = 2 \cdot \pi - \measuredangle(A, B, C)$.

Now we state the proposition:

(32) Suppose A, B, C form a triangle and $|(B - A, C - A)| = 0$. Then

(i) $|C - B| \cdot \sin \measuredangle(C, B, A) = |A - C|$, or

(ii) $|C - B| \cdot (-\sin \measuredangle(C, B, A)) = |A - C|$.

Let us assume that A, B, C form a triangle and $\measuredangle(B, A, C) = \frac{\pi}{2}$. Now we state the propositions:

(33) $\measuredangle(C, B, A) + \measuredangle(A, C, B) = \frac{\pi}{2}$.

(34) (i) $|C - B| \cdot \sin \measuredangle(C, B, A) = |A - C|$, and

(ii) $|C - B| \cdot \sin \measuredangle(A, C, B) = |A - B|$, and
(iii) $|C - B| \cdot \cos \measuredangle(C, B, A) = |A - B|$, and
(iv) $|C - B| \cdot \cos \measuredangle(A, C, B) = |A - C|$.

(35) (i) $\operatorname{tg} \measuredangle(A, C, B) = \frac{|A-B|}{|A-C|}$, and
(ii) $\operatorname{tg} \measuredangle(C, B, A) = \frac{|A-C|}{|A-B|}$.

The theorem is a consequence of (34).

4. Triangle Inscribed in a Semicircle is a Right Triangle

Let a, b be real numbers and r be a negative real number. Let us note that circle(a, b, r) is empty.

Now we state the proposition:

(36) Let us consider real numbers a, b. Then circle$(a, b, 0) = \{[a, b]\}$.

Let a, b be real numbers. One can verify that circle$(a, b, 0)$ is trivial.

Now we state the propositions:

(37) Let us consider points A, B, C of $\mathcal{E}^2_{\mathrm{T}}$, and real numbers a, b, r. Suppose A, B, C form a triangle and A, $B \in$ circle(a, b, r). Then r is positive. The theorem is a consequence of (36).

(38) Let us consider a point A of $\mathcal{E}^2_{\mathrm{T}}$, real numbers a, b, and a positive real number r. If $A \in$ circle(a, b, r), then $A \neq [a, b]$.

(39) Let us consider points A, B, C of $\mathcal{E}^2_{\mathrm{T}}$, and real numbers a, b, r. Suppose A, B, C form a triangle and $\measuredangle(C, B, A)$, $\measuredangle(B, A, C) \in]0, \pi[$ and A, B, $C \in$ circle(a, b, r) and $[a, b] \in \mathcal{L}(A, C)$. Then $\measuredangle(C, B, A) = \frac{\pi}{2}$.

Proof: Set $O = [a, b]$. Consider J_1 being a point of $\mathcal{E}^2_{\mathrm{T}}$ such that $A = J_1$ and $|J_1 - [a, b]| = r$. Consider J_2 being a point of $\mathcal{E}^2_{\mathrm{T}}$ such that $B = J_2$ and $|J_2 - [a, b]| = r$. Consider J_3 being a point of $\mathcal{E}^2_{\mathrm{T}}$ such that $C = J_3$ and $|J_3 - [a, b]| = r$. r is positive. $O \neq A$ and $O \neq C$. $\measuredangle(C, B, O) < \pi$ by [25, (16), (9)], [19, (47)]. A, O, B form a triangle and C, O, B form a triangle by (37), (38), [6, (72), (75)]. $\measuredangle(C, B, O) + \measuredangle(O, C, B) + \measuredangle(O, B, A) + \measuredangle(B, A, O) = \pi$ or $\measuredangle(C, B, O) + \measuredangle(O, C, B) + \measuredangle(O, B, A) + \measuredangle(B, A, O) = -\pi$ by [25, (13)], [19, (47)]. $\measuredangle(O, C, B) = \measuredangle(C, B, O)$ and $\measuredangle(B, A, O) = \measuredangle(O, B, A)$. □

(40) Let us consider points A, B, C of $\mathcal{E}^2_{\mathrm{T}}$, and a positive real number r. Suppose $\measuredangle(A, B, C)$ is not zero. Then $\sin(r \cdot \measuredangle(C, B, A)) = \sin(r \cdot 2 \cdot \pi) \cdot \cos(r \cdot \measuredangle(A, B, C)) - \cos(r \cdot 2 \cdot \pi) \cdot \sin(r \cdot \measuredangle(A, B, C))$.

(41) Let us consider points A, B, C of $\mathcal{E}^2_{\mathrm{T}}$. Suppose $\measuredangle(A, B, C)$ is not zero. Then $\sin \frac{\measuredangle(C,B,A)}{3} = \frac{\sqrt{3}}{2} \cdot \cos \frac{\measuredangle(A,B,C)}{3} + \frac{1}{2} \cdot \sin \frac{\measuredangle(A,B,C)}{3}$. The theorem is a consequence of (40), (22), and (23).

5. Diameter of the Circumcircle of a Triangle

Let us consider points A, B, C of $\mathcal{E}^2_{\mathrm{T}}$. Now we state the propositions:

(42) (i) area of $\triangle(A,B,C) =$ area of $\triangle(B,C,A)$, and

(ii) area of $\triangle(A,B,C) =$ area of $\triangle(C,A,B)$.

(43) area of $\triangle(A,B,C) = -($area of $\triangle(B,A,C))$.

Let A, B, C be points of $\mathcal{E}^2_{\mathrm{T}}$. The functor $\varnothing_{\circ}(A,B,C)$ yielding a real number is defined by the term

(Def. 1) $\frac{\frac{|A-B|\cdot|B-C|\cdot|C-A|}{2}}{\text{area of } \triangle(A,B,C)}$.

Let us consider points A, B, C of $\mathcal{E}^2_{\mathrm{T}}$.

Let us assume that A, B, C form a triangle. Now we state the propositions:

(44) $\varnothing_{\circ}(A,B,C) = \frac{|C-A|}{\sin\measuredangle(C,B,A)}$.

(45) $\varnothing_{\circ}(A,B,C) = -\frac{|C-A|}{\sin\measuredangle(A,B,C)}$. The theorem is a consequence of (44).

Now we state the proposition:

(46) $\varnothing_{\circ}(A,B,C) = \varnothing_{\circ}(B,C,A)$.

Let us assume that A, B, C form a triangle. Now we state the propositions:

(47) $\varnothing_{\circ}(A,B,C) = -\varnothing_{\circ}(B,A,C)$. The theorem is a consequence of (43).

(48) $\varnothing_{\circ}(A,B,C) = -\varnothing_{\circ}(A,C,B)$. The theorem is a consequence of (42) and (47).

(49) $\varnothing_{\circ}(A,B,C) = -\varnothing_{\circ}(C,B,A)$. The theorem is a consequence of (48) and (42).

6. Some Identities of a Triangle

Let us consider points A, B, C of $\mathcal{E}^2_{\mathrm{T}}$.

Let us assume that A, B, C form a triangle. Now we state the propositions:

(50) (i) $|A-B| = \varnothing_{\circ}(A,B,C)\cdot\sin\measuredangle(A,C,B)$, and

(ii) $|B-C| = \varnothing_{\circ}(A,B,C)\cdot\sin\measuredangle(B,A,C)$, and

(iii) $|C-A| = \varnothing_{\circ}(A,B,C)\cdot\sin\measuredangle(C,B,A)$.

The theorem is a consequence of (42).

(51) $|A-B| = \varnothing_{\circ}(A,B,C)\cdot 4\cdot\sin\frac{\measuredangle(A,C,B)}{3}\cdot\sin(\frac{\pi}{3}+\frac{\measuredangle(A,C,B)}{3})\cdot\sin(\frac{\pi}{3}-\frac{\measuredangle(A,C,B)}{3})$. The theorem is a consequence of (29).

Let us consider points A, B, C, P of $\mathcal{E}^2_{\mathrm{T}}$. Now we state the propositions:

(52) Suppose A, B, P are mutually different and $\measuredangle(P,B,A) = \frac{\measuredangle(C,B,A)}{3}$ and $\measuredangle(B,A,P) = \frac{\measuredangle(B,A,C)}{3}$ and $\measuredangle(A,P,B) < \pi$. Then $|A-P|\cdot\sin(\pi - (\frac{\measuredangle(C,B,A)}{3}+\frac{\measuredangle(B,A,C)}{3})) = |A-B|\cdot\sin\frac{\measuredangle(C,B,A)}{3}$.

(53) Suppose A, B, P are mutually different and $\measuredangle(P, B, A) = \frac{\measuredangle(C,B,A)}{3}$ and $\measuredangle(B, A, P) = \frac{\measuredangle(B,A,C)}{3}$ and $\measuredangle(A, P, B) < \pi$ and $\frac{\measuredangle(C,B,A)}{3} + \frac{\measuredangle(B,A,C)}{3} + \frac{\measuredangle(A,C,B)}{3} = \frac{\pi}{3}$. Then $|A - P| \cdot \sin(\frac{2 \cdot \pi}{3} + \frac{\measuredangle(A,C,B)}{3}) = |A - B| \cdot \sin \frac{\measuredangle(C,B,A)}{3}$.

Now we state the proposition:

(54) Let us consider points A, B, C of $\mathcal{E}^2_{\mathrm{T}}$. Suppose A, B, C form a triangle and $\measuredangle(C, A, B) < \pi$. Then

(i) $\measuredangle(C, B, A) + \measuredangle(B, A, C) + \measuredangle(A, C, B) = 5 \cdot \pi$, and

(ii) $\measuredangle(C, A, B) + \measuredangle(A, B, C) + \measuredangle(B, C, A) = \pi$.

Let us consider points A, B, C, P of $\mathcal{E}^2_{\mathrm{T}}$. Now we state the propositions:

(55) Suppose A, B, C form a triangle and $\measuredangle(C, B, A) < \pi$ and A, B, P are mutually different and $\measuredangle(P, B, A) = \frac{\measuredangle(C,B,A)}{3}$ and $\measuredangle(B, A, P) = \frac{\measuredangle(B,A,C)}{3}$ and $\measuredangle(A, P, B) < \pi$. Then $|A - P| \cdot \sin(\frac{\pi}{3} - \frac{\measuredangle(A,C,B)}{3}) = |A - B| \cdot \sin \frac{\measuredangle(C,B,A)}{3}$. The theorem is a consequence of (1).

(56) Suppose A, B, C form a triangle and A, B, P form a triangle and $\measuredangle(C, B, A) < \pi$ and $\measuredangle(A, P, B) < \pi$ and $\measuredangle(P, B, A) = \frac{\measuredangle(C,B,A)}{3}$ and $\measuredangle(B, A, P) = \frac{\measuredangle(B,A,C)}{3}$ and $\sin(\frac{\pi}{3} - \frac{\measuredangle(A,C,B)}{3}) \neq 0$. Then $|A - P| = -\varnothing_{\measuredangle}(C, B, A) \cdot 4 \cdot \sin \frac{\measuredangle(A,C,B)}{3} \cdot \sin(\frac{\pi}{3} + \frac{\measuredangle(A,C,B)}{3}) \cdot \sin \frac{\measuredangle(C,B,A)}{3}$. The theorem is a consequence of (53), (29), (50), (13), and (49).

7. Diameter of a Circle

Now we state the propositions:

(57) Let us consider points A, B, C of $\mathcal{E}^2_{\mathrm{T}}$. Suppose A, B, C are mutually different and $C \in \mathcal{L}(A, B)$. Then $|A - B| = |A - C| + |C - B|$.

(58) Let us consider points A, B of $\mathcal{E}^2_{\mathrm{T}}$, real numbers a, b, and a positive real number r. Suppose A, B, $[a, b]$ are mutually different and A, $B \in$ circle(a, b, r) and $[a, b] \in \mathcal{L}(A, B)$. Then $|A - B| = 2 \cdot r$. The theorem is a consequence of (57).

(59) Let us consider real numbers a, b, a positive real number r, and a subset C of $\mathcal{E}^2$. If $C =$ circle(a, b, r), then $\varnothing C = 2 \cdot r$.

Proof: For every points x, y of $\mathcal{E}^2$ such that $x, y \in C$ holds $\rho(x, y) \leqslant 2 \cdot r$ by [11, (22), (67)], [17, (4)], [22, (5)]. For every real number s such that for every points x, y of $\mathcal{E}^2$ such that $x, y \in C$ holds $\rho(x, y) \leqslant s$ holds $2 \cdot r \leqslant s$ by [11, (62)], [4, (12)], [19, (24)], [26, (22)]. □

References

[1] Grzegorz Bancerek. Cardinal numbers. *Formalized Mathematics*, 1(**2**):377–382, 1990.
[2] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.
[3] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.
[4] Czesław Byliński. The complex numbers. *Formalized Mathematics*, 1(**3**):507–513, 1990.
[5] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**): 55–65, 1990.
[6] Czesław Byliński. Introduction to real linear topological spaces. *Formalized Mathematics*, 13(**1**):99–107, 2005.
[7] Czesław Byliński. The sum and product of finite sequences of real numbers. *Formalized Mathematics*, 1(**4**):661–668, 1990.
[8] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.
[9] H.S.M. Coxeter and S.L. Greitzer. *Geometry Revisited*. The Mathematical Association of America (Inc.), 1967.
[10] Agata Darmochwał. Compact spaces. *Formalized Mathematics*, 1(**2**):383–386, 1990.
[11] Agata Darmochwał. The Euclidean space. *Formalized Mathematics*, 2(**4**):599–603, 1991.
[12] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.
[13] Alicia de la Cruz. Totally bounded metric spaces. *Formalized Mathematics*, 2(**4**):559–562, 1991.
[14] Nikolai Vladimirovich Efimov. *Géométrie supérieure*. Mir, 1981.
[15] Richard Fitzpatrick. *Euclid's Elements*. Lulu.com, 2007.
[16] Robin Hartshorne. *Geometry: Euclid and beyond*. Springer, 2000.
[17] Stanisława Kanas, Adam Lecko, and Mariusz Startek. Metric spaces. *Formalized Mathematics*, 1(**3**):607–610, 1990.
[18] Artur Korniłowicz and Yasunari Shidama. Inverse trigonometric functions arcsin and arccos. *Formalized Mathematics*, 13(**1**):73–79, 2005.
[19] Akihiro Kubo and Yatsuka Nakamura. Angle and triangle in Euclidean topological space. *Formalized Mathematics*, 11(**3**):281–287, 2003.
[20] Robert Milewski. Trigonometric form of complex numbers. *Formalized Mathematics*, 9 (**3**):455–460, 2001.
[21] Yatsuka Nakamura. General Fashoda meet theorem for unit circle and square. *Formalized Mathematics*, 11(**3**):213–224, 2003.
[22] Yatsuka Nakamura and Czesław Byliński. Extremal properties of vertices on special polygons. Part I. *Formalized Mathematics*, 5(**1**):97–102, 1996.
[23] Chanapat Pacharapokin, Kanchun, and Hiroshi Yamazaki. Formulas and identities of trigonometric functions. *Formalized Mathematics*, 12(**2**):139–141, 2004.
[24] Beata Padlewska. Families of sets. *Formalized Mathematics*, 1(**1**):147–152, 1990.
[25] Marco Riccardi. Heron's formula and Ptolemy's theorem. *Formalized Mathematics*, 16 (**2**):97–101, 2008. doi:10.2478/v10037-008-0014-2.
[26] Andrzej Trybulec and Czesław Byliński. Some properties of real numbers. *Formalized Mathematics*, 1(**3**):445–449, 1990.
[27] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[28] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1 (**1**):73–83, 1990.
[29] Yuguang Yang and Yasunari Shidama. Trigonometric functions and existence of circle ratio. *Formalized Mathematics*, 7(**2**):255–263, 1998.

Received September 29, 2014

FORMALIZED MATHEMATICS
Vol. 22, No. 4, Pages 321–327, 2014
DOI: 10.2478/forma-2014-0032

DE GRUYTER OPEN
degruyter.com/view/j/forma

The Formal Construction of Fuzzy Numbers

Adam Grabowski
Institute of Informatics
University of Białystok
Akademicka 2, 15-267 Białystok
Poland

Summary. In this article, we continue the development of the theory of fuzzy sets [23], started with [14] with the future aim to provide the formalization of fuzzy numbers [8] in terms reflecting the current state of the Mizar Mathematical Library. Note that in order to have more usable approach in [14], we revised that article as well; some of the ideas were described in [12]. As we can actually understand fuzzy sets just as their membership functions (via the equality of membership function and their set-theoretic counterpart), all the calculations are much simpler. To test our newly proposed approach, we give the notions of (normal) triangular and trapezoidal fuzzy sets as the examples of concrete fuzzy objects. Also α-cuts, the core of a fuzzy set, and normalized fuzzy sets were defined. Main technical obstacle was to prove continuity of the glued maps, and in fact we did this not through its topological counterpart, but extensively reusing properties of the real line (with loss of generality of the approach, though), because we aim at formalizing fuzzy numbers in our future submissions, as well as merging with rough set approach as introduced in [13] and [11]. Our base for formalization was [9] and [10].

MSC: 03E72 94D99 03B35

Keywords: fuzzy sets; formal models of fuzzy sets; triangular fuzzy numbers

MML identifier: `FUZNUM_1`, version: `8.1.03 5.29.1227`

The notation and terminology used in this paper have been introduced in the following articles: [16], [3], [4], [5], [14], [2], [19], [1], [6], [17], [21], [22], [20], and [7].

1. Preliminaries: Affine Maps

Now we state the proposition:

(1) Let us consider real numbers a, b. Suppose $a \leqslant b$. Then $\mathbb{R} \setminus]a, b[\neq \emptyset$.

From now on a, b, c, x denote real numbers.

Now we state the propositions:

(2) $(\mathrm{AffineMap}(\frac{1}{b-a}, -\frac{a}{b-a}))(a) = 0$.

(3) If $b - a \neq 0$, then $(\mathrm{AffineMap}(\frac{1}{b-a}, -\frac{a}{b-a}))(b) = 1$.

(4) If $c - b \neq 0$, then $(\mathrm{AffineMap}(-\frac{1}{c-b}, \frac{c}{c-b}))(b) = 1$.

(5) $(\mathrm{AffineMap}(-\frac{1}{c-b}, \frac{c}{c-b}))(c) = 0$.

(6) If $b-a \neq 0$ and $(\mathrm{AffineMap}(\frac{1}{b-a}, -\frac{a}{b-a}))(x) = 1$, then $x = b$. The theorem is a consequence of (3).

(7) If $c-b \neq 0$ and $(\mathrm{AffineMap}(-\frac{1}{c-b}, \frac{c}{c-b}))(x) = 1$, then $x = b$. The theorem is a consequence of (4).

(8) $\mathrm{rng}(\mathrm{AffineMap}(0, a)) = \{a\}$.

(9) Let us consider a non empty subset C of $\mathbb{R}$.
Then $\mathrm{rng}((\mathrm{AffineMap}(0, a)) \restriction C) = \{a\}$.
Proof: Set $f = (\mathrm{AffineMap}(0, a)) \restriction C$. $\mathrm{rng}\, f \subseteq \{a\}$ by [3, (49)]. $\square$

(10) If $b - a > 0$, then $\mathrm{rng}((\mathrm{AffineMap}(\frac{1}{b-a}, -\frac{a}{b-a})) \restriction [a, b]) = [0, 1]$.
Proof: Set $f = \mathrm{AffineMap}(\frac{1}{b-a}, -\frac{a}{b-a})$. Set $g = f \restriction [a, b]$. $\mathrm{rng}\, g \subseteq [0, 1]$ by [21, (57)], [3, (47)], (2), [16, (53)]. $\square$

Let us assume that $c - b > 0$. Now we state the propositions:

(11) $\mathrm{rng}((\mathrm{AffineMap}(-\frac{1}{c-b}, \frac{c}{c-b})) \restriction]b, c]) = [0, 1[$.
Proof: Set $f = \mathrm{AffineMap}(-\frac{1}{c-b}, \frac{c}{c-b})$. Set $g = f \restriction]b, c]$. $\mathrm{rng}\, g \subseteq [0, 1[$ by [21, (57)], [3, (47)], (4), [16, (52), (54)]. $\square$

(12) $\mathrm{rng}((\mathrm{AffineMap}(-\frac{1}{c-b}, \frac{c}{c-b})) \restriction [b, c]) = [0, 1]$.
Proof: Set $f = \mathrm{AffineMap}(-\frac{1}{c-b}, \frac{c}{c-b})$. Set $g = f \restriction [b, c]$. $\mathrm{rng}\, g \subseteq [0, 1]$ by [21, (57)], [3, (47)], (4), [16, (54)]. $\square$

Now we state the propositions:

(13) $(\mathrm{AffineMap}(0, 0))(x) \neq 1$.

(14) $(\mathrm{AffineMap}(0, 1))(b) = 1$.

(15) Let us consider a real number a. Then $(\mathrm{AffineMap}(0, b))(a) = b$.

2. Towards Development of Fuzzy Numbers

In the sequel C denotes a non empty set.

Let C be a non empty set.

A fuzzy set of C is a membership function of C. Let F be a fuzzy set of C. We say that F is normalized if and only if

(Def. 1) there exists an element x of C such that $F(x) = 1$.

We introduce F is normal as a synonym of F is normalized.

We introduce F is subnormal as an antonym for F is normal.

We say that F is strictly normalized if and only if

(Def. 2) there exists an element x of C such that $F(x) = 1$ and for every element y of C such that $F(y) = 1$ holds $y = x$.

One can verify that every fuzzy set of C which is strictly normalized is also normalized.

Let F be a fuzzy set of C and α be a real number. The functor $\alpha\text{-cut}(F)$ yielding a subset of C is defined by the term

(Def. 3) $\{x$, where x is an element of $C : F(x) \geqslant \alpha\}$.

Now we state the proposition:

(16) Let us consider a fuzzy set F of C, and a real number α. Then $\alpha\text{-cut}(F) = F^{-1}([\alpha, 1])$.
PROOF: $\alpha\text{-cut}(F) \subseteq F^{-1}([\alpha, 1])$ by [6, (4)]. $\square$

Let us consider C. Let us note that UMF C is normalized and there exists a fuzzy set of C which is normalized.

Let F be a fuzzy set of C. The functor Core F yielding a subset of C is defined by the term

(Def. 4) $\{x$, where x is an element of $C : F(x) = 1\}$.

Now we state the propositions:

(17) Core UMF $C = C$.

(18) Core EMF $C = \emptyset$.

Let us consider C. One can check that Core EMF C is empty.

Let us consider a fuzzy set F of C. Now we state the propositions:

(19) Core $F = F^{-1}(\{1\})$.

(20) Core $F = 1\text{-cut}(F)$. The theorem is a consequence of (16) and (19).

3. Convexity and the Height of a Fuzzy Set

Let F be a fuzzy set of $\mathbb{R}$. We say that F is convex if and only if

(Def. 5) for every real numbers x_1, x_2 and for every real number l such that $0 \leqslant l \leqslant 1$ holds $F(l \cdot x_1 + (1 - l) \cdot x_2) \geqslant \min(F(x_1), F(x_2))$.

Observe that UMF $\mathbb{R}$ is convex and EMF $\mathbb{R}$ is convex.

Let C be a non empty set and F be a fuzzy set of C. The functor height F yielding an extended real is defined by the term

(Def. 6) $\sup \operatorname{rng} F$.

Now we state the propositions:

(21) Let us consider a fuzzy set F of C. Then $0 \leqslant \operatorname{height} F \leqslant 1$.
PROOF: 0 is a lower bound of $\operatorname{rng} F$ by [15, (1)]. 1 is a upper bound of $\operatorname{rng} F$ by [15, (1)]. □

(22) Let us consider a fuzzy set F of C. If F is normalized, then $\operatorname{height} F = 1$. The theorem is a consequence of (21).

4. Pasting aka Glueing Lemmas

Let us consider partial functions f, g from $\mathbb{R}$ to $\mathbb{R}$. Now we state the proposition:

(23) Suppose f is continuous and g is continuous and there exists an object x such that $\operatorname{dom} f \cap \operatorname{dom} g = \{x\}$ and for every object x such that $x \in \operatorname{dom} f \cap \operatorname{dom} g$ holds $f(x) = g(x)$. Then there exists a partial function h from $\mathbb{R}$ to $\mathbb{R}$ such that

(i) $h = f {+\cdot} g$, and

(ii) for every real number x such that $x \in \operatorname{dom} f \cap \operatorname{dom} g$ holds h is continuous in x.

PROOF: Reconsider $h = f {+\cdot} g$ as a partial function from $\mathbb{R}$ to $\mathbb{R}$. For every real number r such that $0 < r$ there exists a real number s such that $0 < s$ and for every real number x_1 such that $x_1 \in \operatorname{dom} h$ and $|x_1 - x| < s$ holds $|h(x_1) - h(x)| < r$ by [21, (57)], [16, (3)], [5, (12)], [3, (47)]. □

Let us assume that f is continuous and non empty and g is continuous and non empty and there exist real numbers a, b, c such that $\operatorname{dom} f = [a, b]$ and $\operatorname{dom} g = [b, c]$ and $f \approx g$. Now we state the propositions:

(24) There exists a partial function h from $\mathbb{R}$ to $\mathbb{R}$ such that

(i) $h = f {+\cdot} g$, and

(ii) for every real number x such that $x \in \operatorname{dom} h$ holds h is continuous in x.

(25) $f{+}\cdot g$ is continuous. The theorem is a consequence of (24).

Now we state the proposition:

(26) Suppose g is not empty and $f = (\mathrm{AffineMap}(0,0)){\restriction}(\mathbb{R} \setminus]a,b[)$ and $\operatorname{dom} g = [a,b]$ and $g(a) = 0$ and $g(b) = 0$. Then $f \approx g$.

Proof: For every object x such that $x \in \operatorname{dom} f \cap \operatorname{dom} g$ holds $f(x) = g(x)$ by [18, (1)], [3, (47)], (15). □

Let us assume that g is continuous and non empty and $f = (\mathrm{AffineMap}(0,0)){\restriction}(\mathbb{R} \setminus]a,b[)$ and $\operatorname{dom} g = [a,b]$ and $g(a) = 0$ and $g(b) = 0$. Now we state the propositions:

(27) There exists a partial function h from $\mathbb{R}$ to $\mathbb{R}$ such that

(i) $h = f{+}\cdot g$, and

(ii) for every real number x such that $x \in \operatorname{dom} h$ holds h is continuous in x.

The theorem is a consequence of (26).

(28) $f{+}\cdot g$ is continuous. The theorem is a consequence of (27).

Note that there exists a subset of $\mathbb{R}$ which is non trivial, closed interval, and closed.

5. Triangular and Trapezoidal Fuzzy Sets

Let a, b, c be real numbers. Assume $a < b$ and $b < c$.

The functor TriangularFS(a, b, c) yielding a fuzzy set of $\mathbb{R}$ is defined by the term

(Def. 7) $((\mathrm{AffineMap}(0,0)){\restriction}(\mathbb{R} \setminus]a,c[){+}\cdot$ $(\mathrm{AffineMap}(\frac{1}{b-a}, -\frac{a}{b-a})){\restriction}[a,b]){+}\cdot$ $(\mathrm{AffineMap}(-\frac{1}{c-b}, \frac{c}{c-b})){\restriction}[b,c]$.

Let us consider real numbers a, b, c. Let us assume that $a < b < c$. Now we state the propositions:

(29) TriangularFS(a, b, c) is strictly normalized.

Proof: Set $F = \mathrm{TriangularFS}(a,b,c)$. Reconsider $b_1 = b$ as an element of $\mathbb{R}$. For every element y of $\mathbb{R}$ such that $F(y) = 1$ holds $y = b_1$ by [21, (57)], [5, (11), (13)], [3, (49)]. □

(30) TriangularFS(a, b, c) is continuous.

Proof: Set $f_1 = \mathrm{AffineMap}(0,0)$. Set $f = f_1{\restriction}(\mathbb{R} \setminus]a,c[)$. Set $g_1 = \mathrm{AffineMap}(\frac{1}{b-a}, -\frac{a}{b-a})$. Reconsider $g = g_1{\restriction}[a,b]$ as a partial function from

$\mathbb{R}$ to $\mathbb{R}$. Set $h_1 = \mathrm{AffineMap}(-\frac{1}{c-b}, \frac{c}{c-b})$. Reconsider $h = h_1 \restriction [b, c]$ as a partial function from $\mathbb{R}$ to $\mathbb{R}$. For every object x such that $x \in \mathrm{dom}\, g \cap \mathrm{dom}\, h$ holds $g(x) = h(x)$ by [3, (49)], (4), (3). Set $\mathfrak{h} = g{+\cdot}h$. Consider h_2 being a partial function from $\mathbb{R}$ to $\mathbb{R}$ such that $h_2 = f{+\cdot}\mathfrak{h}$ and for every real number x such that $x \in \mathrm{dom}\, h_2$ holds h_2 is continuous in x. □

Let a, b, c, d be real numbers. Assume $a < b$ and $b < c$ and $c < d$. The functor TrapezoidalFS(a, b, c, d) yielding a fuzzy set of $\mathbb{R}$ is defined by the term

(Def. 8) $(((\mathrm{AffineMap}(0, 0)) \restriction (\mathbb{R} \setminus]a, d[) {+\cdot}$ $(\mathrm{AffineMap}(\frac{1}{b-a}, -\frac{a}{b-a})) \restriction [a, b]) {+\cdot}$ $(\mathrm{AffineMap}(0, 1)) \restriction [b, c]) {+\cdot} (\mathrm{AffineMap}(-\frac{1}{d-c}, \frac{d}{d-c})) \restriction [c, d]$.

Let us consider real numbers a, b, c, d. Let us assume that $a < b < c < d$. Now we state the propositions:

(31) TrapezoidalFS(a, b, c, d) is normalized. The theorem is a consequence of (4).

(32) TrapezoidalFS(a, b, c, d) is continuous.

PROOF: Set $f_1 = \mathrm{AffineMap}(0, 0)$. Set $f = f_1 \restriction (\mathbb{R} \setminus]a, d[)$. Set $g_1 = \mathrm{AffineMap}(\frac{1}{b-a}, -\frac{a}{b-a})$. Reconsider $g = g_1 \restriction [a, b]$ as a partial function from $\mathbb{R}$ to $\mathbb{R}$. Set $h_1 = \mathrm{AffineMap}(-\frac{1}{d-c}, \frac{d}{d-c})$. Reconsider $h = h_1 \restriction [c, d]$ as a partial function from $\mathbb{R}$ to $\mathbb{R}$. Set $i_1 = \mathrm{AffineMap}(0, 1)$. Reconsider $i = i_1 \restriction [b, c]$ as a partial function from $\mathbb{R}$ to $\mathbb{R}$. For every object x such that $x \in \mathrm{dom}\, g \cap \mathrm{dom}\, i$ holds $g(x) = i(x)$ by [3, (49)], (15), (3). Set $\mathfrak{h} = g{+\cdot}i$. $\mathfrak{h}$ is continuous. For every object x such that $x \in \mathrm{dom}\, \mathfrak{h} \cap \mathrm{dom}\, h$ holds $\mathfrak{h}(x) = h(x)$ by [5, (13)], [3, (49)], (15). Set $g_2 = \mathfrak{h}{+\cdot}h$. Consider h_2 being a partial function from $\mathbb{R}$ to $\mathbb{R}$ such that $h_2 = f{+\cdot}g_2$ and for every real number x such that $x \in \mathrm{dom}\, h_2$ holds h_2 is continuous in x. □

Let F be a fuzzy set of $\mathbb{R}$. We say that F is triangular if and only if

(Def. 9) there exist real numbers a, b, c such that $F = \mathrm{TriangularFS}(a, b, c)$.

We say that F is trapezoidal if and only if

(Def. 10) there exist real numbers a, b, c, d such that $F = \mathrm{TrapezoidalFS}(a, b, c, d)$.

One can verify that there exists a fuzzy set of $\mathbb{R}$ which is triangular and there exists a fuzzy set of $\mathbb{R}$ which is trapezoidal.

References

[1] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.

[2] Józef Białas. Properties of the intervals of real numbers. *Formalized Mathematics*, 3(**2**): 263–269, 1992.

[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] Czesław Byliński. The modification of a function by a function and the iteration of the composition of a function. *Formalized Mathematics*, 1(**3**):521–527, 1990.

[6] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.

[7] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.

[8] Didier Dubois and Henri Prade. Operations on fuzzy numbers. *International Journal of System Sciences*, 9(6):613–626, 1978.

[9] Didier Dubois and Henri Prade. *Fuzzy Sets and Systems: Theory and Applications*. Academic Press, New York, 1980.

[10] Didier Dubois and Henri Prade. Rough fuzzy sets and fuzzy rough sets. *International Journal of General Systems*, 17(2-3):191–209, 1990.

[11] Adam Grabowski. Efficient rough set theory merging. *Fundamenta Informaticae*, 135(4): 371–385, 2014. doi:10.3233/FI-2014-1129.

[12] Adam Grabowski. On the computer certification of fuzzy numbers. In M. Ganzha, L. Maciaszek, and M. Paprzycki, editors, *2013 Federated Conference on Computer Science and Information Systems (FedCSIS)*, Federated Conference on Computer Science and Information Systems, pages 51–54, 2013.

[13] Adam Grabowski. Basic properties of rough sets and rough membership function. *Formalized Mathematics*, 12(**1**):21–28, 2004.

[14] Takashi Mitsuishi, Noboru Endou, and Yasunari Shidama. The concept of fuzzy set and membership function and basic properties of fuzzy set operation. *Formalized Mathematics*, 9(**2**):351–356, 2001.

[15] Takashi Mitsuishi, Katsumi Wasaki, and Yasunari Shidama. Basic properties of fuzzy set operation and membership function. *Formalized Mathematics*, 9(**2**):357–362, 2001.

[16] Konrad Raczkowski and Paweł Sadowski. Real function continuity. *Formalized Mathematics*, 1(**4**):787–791, 1990.

[17] Konrad Raczkowski and Paweł Sadowski. Topological properties of subsets in real numbers. *Formalized Mathematics*, 1(**4**):777–780, 1990.

[18] Andrzej Trybulec. Enumerated sets. *Formalized Mathematics*, 1(**1**):25–34, 1990.

[19] Andrzej Trybulec. On the sets inhabited by numbers. *Formalized Mathematics*, 11(**4**): 341–347, 2003.

[20] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.

[21] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1 (**1**):73–83, 1990.

[22] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.

[23] Lotfi Zadeh. Fuzzy sets. *Information and Control*, 8(3):338–353, 1965.

Received December 31, 2014