

# Isomorphism Theorem on Vector Spaces over a Ring<sup>1</sup>

Yuichi Futa  
Tokyo University of Technology  
Tokyo, Japan

Yasunari Shidama  
Shinshu University  
Nagano, Japan

**Summary.** In this article, we formalize in the Mizar system [1, 4] some properties of vector spaces over a ring. We formally prove the first isomorphism theorem of vector spaces over a ring. We also formalize the product space of vector spaces.  $\mathbb{Z}$ -modules are useful for lattice problems such as LLL (Lenstra, Lenstra and Lovász) [5] base reduction algorithm and cryptographic systems [6, 2].

MSC: 15A03 15A04 03B35

Keywords: isomorphism theorem; vector space

MML identifier: VECTSP12, version: 8.1.06 5.44.1305

## 1. BIJECTIVE LINEAR TRANSFORMATION

From now on  $K, F$  denote rings,  $V, W$  denote vector spaces over  $K, l$  denotes a linear combination of  $V$ , and  $T$  denotes a linear transformation from  $V$  to  $W$ .

Now we state the propositions:

- (1) Let us consider a field  $K$ , finite dimensional vector spaces  $V, W$  over  $K$ , a subset  $A$  of  $V$ , a basis  $B$  of  $V$ , a linear transformation  $T$  from  $V$  to  $W$ , and a linear combination  $l$  of  $B \setminus A$ . Suppose  $A$  is a basis of  $\ker T$  and  $A \subseteq B$ . Then  $T(\sum l) = \sum(T @ * l)$ .
- (2) Let us consider a field  $F$ , vector spaces  $X, Y$  over  $F$ , 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  $Y$ .

---

<sup>1</sup>This work was supported by JSPS KAKENHI grant number JP15K00183.

- (3) Let us consider a field  $F$ , vector spaces  $X, Y$  over  $F$ , and a linear transformation  $T$  from  $X$  to  $Y$ . Suppose  $T$  is bijective. Then  $X$  is finite dimensional if and only if  $Y$  is finite dimensional.
- (4) Let us consider a field  $F$ , a finite dimensional vector space  $X$  over  $F$ , a vector space  $Y$  over  $F$ , and a linear transformation  $T$  from  $X$  to  $Y$ . Suppose  $T$  is bijective. Then
- (i)  $Y$  is finite dimensional, and
  - (ii)  $\dim(X) = \dim(Y)$ .

PROOF: For every basis  $I$  of  $X$ ,  $\dim(Y) = \overline{I}$ .  $\square$

- (5) Let us consider a field  $F$ , vector spaces  $X, Y$  over  $F$ , a linear combination  $l$  of  $X$ , and a linear transformation  $T$  from  $X$  to  $Y$ . If  $T$  is one-to-one, then  $T^{\textcircled{a}} l = T \textcircled{*} l$ .

PROOF: For every element  $y$  of  $Y$ ,  $(T^{\textcircled{a}} l)(y) = \sum \text{CFS}(l, T, y)$ .  $\square$

## 2. PROPERTIES OF LINEAR COMBINATIONS OF MODULES OVER A RING

Now we state the proposition:

- (6) Let us consider a field  $K$ , a vector space  $V$  over  $K$ , subspaces  $W_1, W_2$  of  $V$ , a basis  $I_1$  of  $W_1$ , and a basis  $I_2$  of  $W_2$ . If  $V$  is the direct sum of  $W_1$  and  $W_2$ , then  $I_1 \cap I_2 = \emptyset$ .

Let us consider a field  $K$ , a vector space  $V$  over  $K$ , subspaces  $W_1, W_2$  of  $V$ , a basis  $I_1$  of  $W_1$ , a basis  $I_2$  of  $W_2$ , and a subset  $I$  of  $V$ . Now we state the propositions:

- (7) Suppose  $V$  is the direct sum of  $W_1$  and  $W_2$  and  $I = I_1 \cup I_2$ . Then  $\text{Lin}(I) =$  the vector space structure of  $V$ .

PROOF: Reconsider  $I_3 = I_1$  as a subset of  $V$ . Reconsider  $I_4 = I_2$  as a subset of  $V$ . For every vector  $x$  of  $V$ ,  $x \in W_1 + W_2$  iff  $x \in \text{Lin}(I_3) + \text{Lin}(I_4)$ .  $\square$

- (8) If  $V$  is the direct sum of  $W_1$  and  $W_2$  and  $I = I_1 \cup I_2$ , then  $I$  is linearly independent.

PROOF: Consider  $l$  being a linear combination of  $I$  such that  $\sum l = 0_V$  and the support of  $l \neq \emptyset$ .  $I_1 \cap I_2 = \emptyset$ .  $I_1$  misses  $I_2$ . Reconsider  $I_3 = I_1$ ,  $I_4 = I_2$  as a subset of  $V$ . Consider  $l_1$  being a linear combination of  $I_3$ ,  $l_2$  being a linear combination of  $I_4$  such that  $l = l_1 + l_2$ . Reconsider  $l_3 = l_1$  as a linear combination of  $I$ . Set  $v_1 = \sum l_3$ .  $v_1 \neq 0_V$  by [3, (25)].  $\square$

- (9) Let us consider a field  $K$ , a vector space  $V$  over  $K$ , subspaces  $W_1, W_2$  of  $V$ , a basis  $I_1$  of  $W_1$ , and a basis  $I_2$  of  $W_2$ . If  $W_1 \cap W_2 = \mathbf{0}_V$ , then  $I_1 \cup I_2$  is a basis of  $W_1 + W_2$ .

PROOF: Set  $I = I_1 \cup I_2$ . Reconsider  $W = W_1 + W_2$  as a strict subspace of  $V$ . Reconsider  $W_3 = W_1, W_4 = W_2$  as a subspace of  $W$ . Reconsider  $I_0 = I$  as a subset of  $W$ . For every object  $x, x \in W_3 \cap W_4$  iff  $x \in \mathbf{0}_V$ . For every object  $x, x \in W$  iff  $x \in W_3 + W_4$ .  $I_0$  is base.  $\square$

### 3. FIRST ISOMOPHISM THEOREM

Let us consider a field  $K$ , a finite dimensional vector space  $V$  over  $K$ , and a subspace  $W$  of  $V$ . Now we state the propositions:

- (10) There exists a linear complement  $S$  of  $W$  and there exists a linear transformation  $T$  from  $S$  to  $V/W$  such that  $T$  is bijective and for every vector  $v$  of  $V$  such that  $v \in S$  holds  $T(v) = v + W$ .

PROOF: Set  $S =$  the linear complement of  $W$ . Set  $V_1 = V/W$ . Define  $\mathcal{P}[\text{vector of } V, \text{vector of } V_1] \equiv \mathcal{S}_2 = \mathcal{S}_1 + W$ . Consider  $f_1$  being a function from the carrier of  $V$  into the carrier of  $V_1$  such that for every vector  $v$  of  $V, \mathcal{P}[v, f_1(v)]$ . Set  $T = f_1 \upharpoonright (\text{the carrier of } S)$ . For every vector  $v$  of  $V$  such that  $v \in S$  holds  $T(v) = v + W$ . The carrier of  $V_1 \subseteq \text{rng } T$ . For every objects  $x_1, x_2$  such that  $x_1, x_2 \in$  the carrier of  $S$  and  $T(x_1) = T(x_2)$  holds  $x_1 = x_2$ .  $\square$

- (11) (i)  $V/W$  is finite dimensional, and  
 (ii)  $\dim(V/W) + \dim(W) = \dim(V)$ .

The theorem is a consequence of (10) and (4).

Let  $K$  be a ring,  $V, U$  be vector spaces over  $K, W$  be a subspace of  $V$ , and  $f$  be a linear transformation from  $V$  to  $U$ . Assume the carrier of  $W \subseteq$  the carrier of  $\ker f$ . The functor  $f/W$  yielding a linear transformation from  $V/W$  to  $U$  is defined by

- (Def. 1) for every vector  $A$  of  $V/W$  and for every vector  $a$  of  $V$  such that  $A = a + W$  holds  $it(A) = f(a)$ .

The functor CQFunctional  $f$  yielding a linear transformation from  $V/\ker f$  to  $U$  is defined by the term

- (Def. 2)  $f/\ker f$ .

Observe that CQFunctional  $f$  is one-to-one.

Now we state the proposition:

- (12) Let us consider a ring  $K$ , vector spaces  $V, U$  over  $K$ , and a linear transformation  $f$  from  $V$  to  $U$ . Then there exists a linear transformation  $T$  from  $V/\ker f$  to  $\text{im } f$  such that  
 (i)  $T = \text{CQFunctional } f$ , and  
 (ii)  $T$  is bijective.

PROOF: Set  $T = \text{CQFunctional } f$ . For every object  $x$ ,  $x \in \text{rng } T$  iff  $x \in \text{rng } f$ .  $\square$

Let  $K$  be a ring,  $V, U, W$  be vector spaces over  $K$ ,  $f$  be a linear transformation from  $V$  to  $U$ , and  $g$  be a linear transformation from  $U$  to  $W$ . One can verify that the functor  $g \cdot f$  yields a linear transformation from  $V$  to  $W$ .

#### 4. THE PRODUCT SPACE OF VECTOR SPACES

Let  $K$  be a ring.

A sequence of vector spaces over  $K$  is a non empty finite sequence and is defined by

(Def. 3) for every set  $S$  such that  $S \in \text{rng } it$  holds  $S$  is a vector space over  $K$ .

Note that every sequence of vector spaces over  $K$  is Abelian group yielding.

Let  $G$  be a sequence of vector spaces over  $K$  and  $j$  be an element of  $\text{dom } G$ . One can check that the functor  $G(j)$  yields a vector space over  $K$ . Let  $j$  be an element of  $\text{dom } \overline{G}$ . One can verify that the functor  $G(j)$  yields a vector space over  $K$ . The functor  $\text{multop } G$  yielding a multi-operation of the carrier of  $K$  and  $\overline{G}$  is defined by

(Def. 4)  $\text{len } it = \text{len } \overline{G}$  and for every element  $j$  of  $\text{dom } \overline{G}$ ,  $it(j) =$  the left multiplication of  $G(j)$ .

The functor  $\prod G$  yielding a strict, non empty vector space structure over  $K$  is defined by the term

(Def. 5)  $\langle \prod \overline{G}, \prod^\circ \langle +_{G_i} \rangle_i, \langle 0_{G_i} \rangle_i, \prod^\circ \text{multop } G \rangle$ .

Let us note that  $\prod G$  is Abelian, add-associative, right zeroed, right complementable, vector distributive, scalar distributive, scalar associative, and scalar unital.

#### 5. CARTESIAN PRODUCT OF VECTOR SPACES

From now on  $K$  denotes a ring.

Let  $K$  be a ring and  $G, F$  be non empty vector space structures over  $K$ . The functor  $\text{prodmlt}(G, F)$  yielding a function from (the carrier of  $K$ )  $\times$  ((the carrier of  $G$ )  $\times$  (the carrier of  $F$ )) into (the carrier of  $G$ )  $\times$  (the carrier of  $F$ ) is defined by

(Def. 6) for every element  $r$  of  $K$  and for every vector  $g$  of  $G$  and for every vector  $f$  of  $F$ ,  $it(r, \langle g, f \rangle) = \langle r \cdot g, r \cdot f \rangle$ .

The functor  $G \times F$  yielding a strict, non empty vector space structure over  $K$  is defined by the term

(Def. 7)  $\langle (\text{the carrier of } G) \times (\text{the carrier of } F), \text{prodadd}(G, F), \text{prodzero}(G, F), \text{prodmult}(G, F) \rangle$ .

Let  $G, F$  be Abelian, non empty vector space structures over  $K$ . Note that  $G \times F$  is Abelian.

Let  $G, F$  be add-associative, non empty vector space structures over  $K$ . One can verify that  $G \times F$  is add-associative.

Let  $G, F$  be right zeroed, non empty vector space structures over  $K$ . One can verify that  $G \times F$  is right zeroed.

Let  $G, F$  be right complementable, non empty vector space structures over  $K$ . One can check that  $G \times F$  is right complementable.

Now we state the propositions:

- (13) Let us consider non empty vector space structures  $G, F$  over  $K$ . Then
- (i) for every set  $x$ ,  $x$  is a vector of  $G \times F$  iff there exists a vector  $x_1$  of  $G$  and there exists a vector  $x_2$  of  $F$  such that  $x = \langle x_1, x_2 \rangle$ , and
  - (ii) for every vectors  $x, y$  of  $G \times F$  and for every vectors  $x_1, y_1$  of  $G$  and for every vectors  $x_2, y_2$  of  $F$  such that  $x = \langle x_1, x_2 \rangle$  and  $y = \langle y_1, y_2 \rangle$  holds  $x + y = \langle x_1 + y_1, x_2 + y_2 \rangle$ , and
  - (iii)  $0_{G \times F} = \langle 0_G, 0_F \rangle$ , and
  - (iv) for every vector  $x$  of  $G \times F$  and for every vector  $x_1$  of  $G$  and for every vector  $x_2$  of  $F$  and for every element  $a$  of  $K$  such that  $x = \langle x_1, x_2 \rangle$  holds  $a \cdot x = \langle a \cdot x_1, a \cdot x_2 \rangle$ .

- (14) Let us consider add-associative, right zeroed, right complementable, non empty vector space structures  $G, F$  over  $K$ , a vector  $x$  of  $G \times F$ , a vector  $x_1$  of  $G$ , and a vector  $x_2$  of  $F$ . Suppose  $x = \langle x_1, x_2 \rangle$ . Then  $-x = \langle -x_1, -x_2 \rangle$ .

Let  $K$  be a ring and  $G, F$  be vector distributive, non empty vector space structures over  $K$ . Let us note that  $G \times F$  is vector distributive.

Let  $G, F$  be scalar distributive, non empty vector space structures over  $K$ . One can check that  $G \times F$  is scalar distributive.

Let  $G, F$  be scalar associative, non empty vector space structures over  $K$ . Let us note that  $G \times F$  is scalar associative.

Let  $G, F$  be scalar unital, non empty vector space structures over  $K$ . Let us observe that  $G \times F$  is scalar unital.

Let  $G$  be a vector space over  $K$ . One can check that the functor  $\langle G \rangle$  yields a sequence of vector spaces over  $K$ . Let  $G, F$  be vector spaces over  $K$ . Let us note that the functor  $\langle G, F \rangle$  yields a sequence of vector spaces over  $K$ . Now we state the proposition:

- (15) Let us consider a vector space  $X$  over  $K$ . Then there exists a function  $I$  from  $X$  into  $\prod\langle X \rangle$  such that
- (i)  $I$  is one-to-one and onto, and
  - (ii) for every vector  $x$  of  $X$ ,  $I(x) = \langle x \rangle$ , and
  - (iii) for every vectors  $v, w$  of  $X$ ,  $I(v + w) = I(v) + I(w)$ , and
  - (iv) for every vector  $v$  of  $X$  and for every element  $r$  of the carrier of  $K$ ,  $I(r \cdot v) = r \cdot I(v)$ , and
  - (v)  $I(0_X) = 0_{\prod\langle X \rangle}$ .

PROOF: Set  $C_3 =$  the carrier of  $X$ . Consider  $I$  being a function from  $C_3$  into  $\prod\langle C_3 \rangle$  such that  $I$  is one-to-one and onto and for every object  $x$  such that  $x \in C_3$  holds  $I(x) = \langle x \rangle$ . For every vectors  $v, w$  of  $X$ ,  $I(v + w) = I(v) + I(w)$ . For every vector  $v$  of  $X$  and for every element  $r$  of the carrier of  $K$ ,  $I(r \cdot v) = r \cdot I(v)$ .  $\square$

Let  $K$  be a ring and  $G, F$  be sequences of vector spaces over  $K$ . One can verify that the functor  $G \frown F$  yields a sequence of vector spaces over  $K$ . Now we state the propositions:

- (16) Let us consider vector spaces  $X, Y$  over  $K$ . Then there exists a function  $I$  from  $X \times Y$  into  $\prod\langle X, Y \rangle$  such that
- (i)  $I$  is one-to-one and onto, and
  - (ii) for every vector  $x$  of  $X$  and for every vector  $y$  of  $Y$ ,  $I(x, y) = \langle x, y \rangle$ , and
  - (iii) for every vectors  $v, w$  of  $X \times Y$ ,  $I(v + w) = I(v) + I(w)$ , and
  - (iv) for every vector  $v$  of  $X \times Y$  and for every element  $r$  of  $K$ ,  $I(r \cdot v) = r \cdot I(v)$ , and
  - (v)  $I(0_{X \times Y}) = 0_{\prod\langle X, Y \rangle}$ .

PROOF: Set  $C_3 =$  the carrier of  $X$ . Set  $C_4 =$  the carrier of  $Y$ . Consider  $I$  being a function from  $C_3 \times C_4$  into  $\prod\langle C_3, C_4 \rangle$  such that  $I$  is one-to-one and onto and for every objects  $x, y$  such that  $x \in C_3$  and  $y \in C_4$  holds  $I(x, y) = \langle x, y \rangle$ . For every vectors  $v, w$  of  $X \times Y$ ,  $I(v + w) = I(v) + I(w)$ . For every vector  $v$  of  $X \times Y$  and for every element  $r$  of  $K$ ,  $I(r \cdot v) = r \cdot I(v)$ .  $\square$

- (17) Let us consider sequences of vector spaces  $X, Y$  over  $K$ . Then there exists a function  $I$  from  $\prod X \times \prod Y$  into  $\prod\langle X \frown Y \rangle$  such that
- (i)  $I$  is one-to-one and onto, and
  - (ii) for every vector  $x$  of  $\prod X$  and for every vector  $y$  of  $\prod Y$ , there exist finite sequences  $x_1, y_1$  such that  $x = x_1$  and  $y = y_1$  and  $I(x, y) = x_1 \frown y_1$ , and

- (iii) for every vectors  $v, w$  of  $\prod X \times \prod Y$ ,  $I(v + w) = I(v) + I(w)$ , and
- (iv) for every vector  $v$  of  $\prod X \times \prod Y$  and for every element  $r$  of the carrier of  $K$ ,  $I(r \cdot v) = r \cdot I(v)$ , and
- (v)  $I(0_{\prod X \times \prod Y}) = 0_{\prod(X \cap Y)}$ .

PROOF: Reconsider  $C_1 = \overline{X}$ ,  $C_2 = \overline{Y}$  as a non-empty, non empty finite sequence. Consider  $I$  being a function from  $\prod C_1 \times \prod C_2$  into  $\prod(C_1 \cap C_2)$  such that  $I$  is one-to-one and onto and for every finite sequences  $x, y$  such that  $x \in \prod C_1$  and  $y \in \prod C_2$  holds  $I(x, y) = x \cap y$ . Set  $P_1 = \prod X$ . Set  $P_2 = \prod Y$ . For every natural number  $k$  such that  $k \in \text{dom } \overline{X \cap Y}$  holds  $\overline{X \cap Y}(k) = (C_1 \cap C_2)(k)$ . For every vector  $x$  of  $\prod X$  and for every vector  $y$  of  $\prod Y$ , there exist finite sequences  $x_1, y_1$  such that  $x = x_1$  and  $y = y_1$  and  $I(x, y) = x_1 \cap y_1$ . For every vectors  $v, w$  of  $P_1 \times P_2$ ,  $I(v + w) = I(v) + I(w)$ . For every vector  $v$  of  $P_1 \times P_2$  and for every element  $r$  of the carrier of  $K$ ,  $I(r \cdot v) = r \cdot I(v)$  by [7, (9)].  $\square$

(18) Let us consider vector spaces  $G, F$  over  $K$ . Then

- (i) for every set  $x$ ,  $x$  is a vector of  $\prod\langle G, F \rangle$  iff there exists a vector  $x_1$  of  $G$  and there exists a vector  $x_2$  of  $F$  such that  $x = \langle x_1, x_2 \rangle$ , and
- (ii) for every vectors  $x, y$  of  $\prod\langle G, F \rangle$  and for every vectors  $x_1, y_1$  of  $G$  and for every vectors  $x_2, y_2$  of  $F$  such that  $x = \langle x_1, x_2 \rangle$  and  $y = \langle y_1, y_2 \rangle$  holds  $x + y = \langle x_1 + y_1, x_2 + y_2 \rangle$ , and
- (iii)  $0_{\prod\langle G, F \rangle} = \langle 0_G, 0_F \rangle$ , and
- (iv) for every vector  $x$  of  $\prod\langle G, F \rangle$  and for every vector  $x_1$  of  $G$  and for every vector  $x_2$  of  $F$  such that  $x = \langle x_1, x_2 \rangle$  holds  $-x = \langle -x_1, -x_2 \rangle$ , and
- (v) for every vector  $x$  of  $\prod\langle G, F \rangle$  and for every vector  $x_1$  of  $G$  and for every vector  $x_2$  of  $F$  and for every element  $a$  of  $K$  such that  $x = \langle x_1, x_2 \rangle$  holds  $a \cdot x = \langle a \cdot x_1, a \cdot x_2 \rangle$ .

PROOF: Consider  $I$  being a function from  $G \times F$  into  $\prod\langle G, F \rangle$  such that  $I$  is one-to-one and onto and for every vector  $x$  of  $G$  and for every vector  $y$  of  $F$ ,  $I(x, y) = \langle x, y \rangle$  and for every vectors  $v, w$  of  $G \times F$ ,  $I(v + w) = I(v) + I(w)$  and for every vector  $v$  of  $G \times F$  and for every element  $r$  of  $K$ ,  $I(r \cdot v) = r \cdot I(v)$  and  $0_{\prod\langle G, F \rangle} = I(0_{G \times F})$ . For every set  $x$ ,  $x$  is a vector of  $\prod\langle G, F \rangle$  iff there exists a vector  $x_1$  of  $G$  and there exists a vector  $x_2$  of  $F$  such that  $x = \langle x_1, x_2 \rangle$ . For every vectors  $x, y$  of  $\prod\langle G, F \rangle$  and for every vectors  $x_1, y_1$  of  $G$  and for every vectors  $x_2, y_2$  of  $F$  such that  $x = \langle x_1, x_2 \rangle$  and  $y = \langle y_1, y_2 \rangle$  holds  $x + y = \langle x_1 + y_1, x_2 + y_2 \rangle$ .  $0_{\prod\langle G, F \rangle} = \langle 0_G, 0_F \rangle$ . For every vector  $x$  of  $\prod\langle G, F \rangle$  and for every vector  $x_1$  of  $G$  and for every vector  $x_2$  of  $F$  such

that  $x = \langle x_1, x_2 \rangle$  holds  $-x = \langle -x_1, -x_2 \rangle$ . For every vector  $x$  of  $\prod \langle G, F \rangle$  and for every vector  $x_1$  of  $G$  and for every vector  $x_2$  of  $F$  and for every element  $a$  of  $K$  such that  $x = \langle x_1, x_2 \rangle$  holds  $a \cdot x = \langle a \cdot x_1, a \cdot x_2 \rangle$ .  $\square$

## REFERENCES

- [1] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, Karol Pał, and Josef Urban. Mizar: State-of-the-art and beyond. In Manfred Kerber, Jacques Carette, Cezary Kaliszyk, Florian Rabe, and Volker Sorge, editors, *Intelligent Computer Mathematics*, volume 9150 of *Lecture Notes in Computer Science*, pages 261–279. Springer International Publishing, 2015. ISBN 978-3-319-20614-1. doi:10.1007/978-3-319-20615-8\_17.
- [2] Wolfgang Ebeling. *Lattices and Codes*. Advanced Lectures in Mathematics. Springer Fachmedien Wiesbaden, 2013.
- [3] 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.
- [4] Adam Grabowski, Artur Korniłowicz, and Adam Naumowicz. Four decades of Mizar. *Journal of Automated Reasoning*, 55(3):191–198, 2015. doi:10.1007/s10817-015-9345-1.
- [5] A. K. Lenstra, H. W. Lenstra Jr., and L. Lovász. Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261(4):515–534, 1982. doi:10.1007/BF01457454.
- [6] Daniele Micciancio and Shafi Goldwasser. Complexity of lattice problems: a cryptographic perspective. *The International Series in Engineering and Computer Science*, 2002.
- [7] Yasunari Shidama. Differentiable functions on normed linear spaces. *Formalized Mathematics*, 20(1):31–40, 2012. doi:10.2478/v10037-012-0005-1.

*Received August 30, 2017*

---



The English version of this volume of Formalized Mathematics was financed under agreement 548/P-DUN/2016 with the funds from the Polish Minister of Science and Higher Education for the dissemination of science.