FORMALIZED MATHEMATICS
Volume 14, Number 1, Pages 1–5
University of Białystok, 2006

Determinant of Some Matrices of Field Elements

Yatsuka Nakamura
Shinshu University
Nagano, Japan

Summary. Here, we present determinants of some square matrices of field elements. First, the determinat of $2*2$ matrix is shown. Secondly, the determinants of zero matrix and unit matrix are shown, which are equal to 0 in the field and 1 in the field respectively. Thirdly, the determinant of diagonal matrix is shown, which is a product of all diagonal elements of the matrix. At the end, we prove that the determinant of a matrix is the same as the determinant of its transpose.

MML identifier: `MATRIX_7`, version: `7.6.01 4.53.937`

The articles [19], [26], [2], [27], [5], [4], [8], [24], [18], [17], [14], [6], [23], [7], [25], [20], [21], [3], [12], [28], [10], [15], [16], [11], [13], [1], [9], and [22] provide the notation and terminology for this paper.

In this paper n, i, l are natural numbers.

The following propositions are true:

(1) For every permutation f of $\operatorname{Seg} 2$ holds $f = \langle 1, 2 \rangle$ or $f = \langle 2, 1 \rangle$.

(2) For every finite sequence f such that $f = \langle 1, 2 \rangle$ or $f = \langle 2, 1 \rangle$ holds f is a permutation of $\operatorname{Seg} 2$.

(3) The permutations of 2-element set $= \{\langle 1, 2 \rangle, \langle 2, 1 \rangle\}$.

(4) For every permutation p of $\operatorname{Seg} 2$ such that p is a transposition holds $p = \langle 2, 1 \rangle$.

(5) Let D be a non empty set, f be a finite sequence of elements of D, and k_2 be a natural number. If $1 \leq k_2$ and $k_2 < \operatorname{len} f$, then $f = (\operatorname{mid}(f, 1, k_2)) \frown \operatorname{mid}(f, k_2 + 1, \operatorname{len} f)$.

(6) For every non empty set D and for every finite sequence f of elements of D such that $2 \leq \operatorname{len} f$ holds $f = (f \restriction (\operatorname{len} f -' 2)) \frown \operatorname{mid}(f, \operatorname{len} f -' 1, \operatorname{len} f)$.

ISSN 1426–2630

(7) For every non empty set D and for every finite sequence f of elements of D such that $1 \leq \operatorname{len} f$ holds $f = (f \restriction (\operatorname{len} f -' 1)) \frown \operatorname{mid}(f, \operatorname{len} f, \operatorname{len} f)$.

(8) Let a be an element of A_2. Given an element q of the permutations of 2-element set such that $q = a$ and q is a transposition. Then $a = \langle 2, 1 \rangle$.

(9) Let n be a natural number, a, b be elements of A_n, and p_2, p_1 be elements of the permutations of n-element set. If $a = p_2$ and $b = p_1$, then $a \cdot b = p_1 \cdot p_2$.

(10) Let a, b be elements of A_2. Suppose that

(i) there exists an element p of the permutations of 2-element set such that $p = a$ and p is a transposition, and

(ii) there exists an element q of the permutations of 2-element set such that $q = b$ and q is a transposition.

Then $a \cdot b = \langle 1, 2 \rangle$.

(11) Let l be a finite sequence of elements of A_2. Suppose that

(i) $\operatorname{len} l \bmod 2 = 0$, and

(ii) for every i such that $i \in \operatorname{dom} l$ there exists an element q of the permutations of 2-element set such that $l(i) = q$ and q is a transposition.

Then $\prod l = \langle 1, 2 \rangle$.

(12) For every field K and for every matrix M over K of dimension 2 holds $\operatorname{Det} M = M_{1,1} \cdot M_{2,2} - M_{1,2} \cdot M_{2,1}$.

Let n be a natural number, let K be a field, let M be a matrix over K of dimension n, and let a be an element of K. Then $a \cdot M$ is a matrix over K of dimension n.

The following three propositions are true:

(13) For every field K and for all natural numbers n, m holds $\operatorname{len}(\begin{pmatrix} 0 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 0 \end{pmatrix}_K^{n \times m}) = n$ and $\operatorname{dom}(\begin{pmatrix} 0 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 0 \end{pmatrix}_K^{n \times m}) = \operatorname{Seg} n$.

(14) Let K be a field, n be a natural number, p be an element of the permutations of n-element set, and i be a natural number. If $i \in \operatorname{Seg} n$, then $p(i) \in \operatorname{Seg} n$.

(15) For every field K and for every natural number n such that $n \geq 1$ holds $\operatorname{Det}(\begin{pmatrix} 0 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 0 \end{pmatrix}_K^{n \times n}) = 0_K$.

Let x, y, a, b be sets. The functor $\operatorname{IFIN}(x, y, a, b)$ is defined by:

(Def. 1) $\operatorname{IFIN}(x, y, a, b) = \begin{cases} a, & \text{if } x \in y, \\ b, & \text{otherwise.} \end{cases}$

We now state the proposition

(16) For every field K and for every natural number n such that $n \geq 1$ holds $\mathrm{Det}(\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}_K^{n \times n}) = 1_K$.

Let K be a field, let n be a natural number, and let M be a matrix over K of dimension n. We say that M being diagonal if and only if:

(Def. 2) For all natural numbers i, j such that $i \in \mathrm{Seg}\, n$ and $j \in \mathrm{Seg}\, n$ and $i \neq j$ holds $M_{i,j} = 0_K$.

One can prove the following propositions:

(17) Let K be a field, n be a natural number, and A be a matrix over K of dimension n. Suppose $n \geq 1$ and A being diagonal. Then $\mathrm{Det}\, A =$ (the multiplication of K) $\circledast$ (the diagonal of A).

(18) Let n be a natural number and p be an element of the permutations of n-element set. Then p^{-1} is an element of the permutations of n-element set.

Let us consider n and let p be an element of the permutations of n-element set. Then p^{-1} is an element of the permutations of n-element set.

Next we state the proposition

(19) Let n be a natural number, K be a field, and A be a matrix over K of dimension n. Then A^{T} is a matrix over K of dimension n.

Let n be a natural number, let K be a field, and let A be a matrix over K of dimension n. The functor A^{T} yields a matrix over K of dimension n and is defined as follows:

(Def. 3) $A^{\mathrm{T}} = (A$ **qua** matrix over $K)^{\mathrm{T}}$.

The following proposition is true

(20) For every group G and for all finite sequences f_1, f_2 of elements of G holds $(\prod(f_1 \frown f_2))^{-1} = (\prod f_2)^{-1} \cdot (\prod f_1)^{-1}$.

Let G be a group and let f be a finite sequence of elements of G. The functor f^{-1} yields a finite sequence of elements of G and is defined by:

(Def. 4) $\mathrm{len}(f^{-1}) = \mathrm{len}\, f$ and for every natural number i such that $i \in \mathrm{Seg}\,\mathrm{len}\, f$ holds $(f^{-1})_i = (f_i)^{-1}$.

One can prove the following propositions:

(21) For every group G holds $(\varepsilon_{(\text{the carrier of } G)})^{-1} = \varepsilon_{(\text{the carrier of } G)}$.

(22) For every group G and for all finite sequences f, g of elements of G holds $(f \frown g)^{-1} = (f^{-1}) \frown g^{-1}$.

(23) For every group G and for every element a of G holds $\langle a \rangle^{-1} = \langle a^{-1} \rangle$.

(24) For every group G and for every finite sequence f of elements of G holds $\prod(f \frown (\mathrm{Rev}(f))^{-1}) = 1_G$.

(25) For every group G and for every finite sequence f of elements of G holds $\prod(((\mathrm{Rev}(f))^{-1}) \frown f) = 1_G$.

(26) For every group G and for every finite sequence f of elements of G holds $(\prod f)^{-1} = \prod((\mathrm{Rev}(f))^{-1})$.

(27) Let I_1 be an element of the permutations of n-element set and I_2 be an element of A_n. If $I_2 = I_1$ and $n \geq 1$, then ${I_1}^{-1} = {I_2}^{-1}$.

(28) Let n be a natural number and I_3 be an element of the permutations of n-element set. If $n \geq 1$, then I_3 is even iff ${I_3}^{-1}$ is even.

(29) Let n be a natural number, K be a field, p be an element of the permutations of n-element set, and x be an element of K. If $n \geq 1$, then $(-1)^{\mathrm{sgn}(p)}x = (-1)^{\mathrm{sgn}(p^{-1})}x$.

(30) Let K be a field and f_1, f_2 be finite sequences of elements of K. Then (the multiplication of K) $\circledast (f_1 \frown f_2) =$ ((the multiplication of K) $\circledast (f_1)) \cdot$ ((the multiplication of K) $\circledast (f_2)$).

(31) Let K be a field and R_1, R_2 be finite sequences of elements of K. Suppose R_1 and R_2 are fiberwise equipotent. Then (the multiplication of K) $\circledast (R_1) =$ (the multiplication of K) $\circledast (R_2)$.

(32) Let n be a natural number, K be a field, p be an element of the permutations of n-element set, and f, g be finite sequences of elements of K. If $n \geq 1$ and $\mathrm{len}\, f = n$ and $g = f \cdot p$, then f and g are fiberwise equipotent.

(33) Let n be a natural number, K be a field, p be an element of the permutations of n-element set, and f, g be finite sequences of elements of K. Suppose $n \geq 1$ and $\mathrm{len}\, f = n$ and $g = f \cdot p$. Then (the multiplication of K) $\circledast f =$ (the multiplication of K) $\circledast g$.

(34) Let n be a natural number, K be a field, p be an element of the permutations of n-element set, and f be a finite sequence of elements of K. If $n \geq 1$ and $\mathrm{len}\, f = n$, then $f \cdot p$ is a finite sequence of elements of K.

(35) Let n be a natural number, K be a field, p be an element of the permutations of n-element set, and A be a matrix over K of dimension n. If $n \geq 1$, then p^{-1}-Path $A^{\mathrm{T}} = (p\text{-Path}\, A) \cdot p^{-1}$.

(36) Let n be a natural number, K be a field, p be an element of the permutations of n-element set, and A be a matrix over K of dimension n. Suppose $n \geq 1$. Then (the product on paths of A^{T})(p^{-1}) = (the product on paths of A)(p).

(37) Let n be a natural number, K be a field, and A be a matrix over K of dimension n. If $n \geq 1$, then $\mathrm{Det}\, A = \mathrm{Det}(A^{\mathrm{T}})$.

References

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

[2] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 1990.
[3] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.
[4] Czesław Byliński. Binary operations. *Formalized Mathematics*, 1(**1**):175–180, 1990.
[5] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.
[6] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.
[7] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.
[8] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.
[9] Czesław Byliński. Some properties of restrictions of finite sequences. *Formalized Mathematics*, 5(**2**):241–245, 1996.
[10] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.
[11] Katarzyna Jankowska. Matrices. Abelian group of matrices. *Formalized Mathematics*, 2(**4**):475–480, 1991.
[12] Katarzyna Jankowska. Transpose matrices and groups of permutations. *Formalized Mathematics*, 2(**5**):711–717, 1991.
[13] Jarosław Kotowicz. Functions and finite sequences of real numbers. *Formalized Mathematics*, 3(**2**):275–278, 1992.
[14] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Formalized Mathematics*, 1(**2**):335–342, 1990.
[15] Yatsuka Nakamura and Roman Matuszewski. Reconstructions of special sequences. *Formalized Mathematics*, 6(**2**):255–263, 1997.
[16] Takaya Nishiyama and Yasuho Mizuhara. Binary arithmetics. *Formalized Mathematics*, 4(**1**):83–86, 1993.
[17] Library Committee of the Association of Mizar Users. Binary operations on numbers. *To appear in Formalized Mathematics.*
[18] Andrzej Trybulec. Subsets of complex numbers. *To appear in Formalized Mathematics.*
[19] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.
[20] Andrzej Trybulec and Agata Darmochwał. Boolean domains. *Formalized Mathematics*, 1(**1**):187–190, 1990.
[21] Wojciech A. Trybulec. Binary operations on finite sequences. *Formalized Mathematics*, 1(**5**):979–981, 1990.
[22] Wojciech A. Trybulec. Groups. *Formalized Mathematics*, 1(**5**):821–827, 1990.
[23] Wojciech A. Trybulec. Pigeon hole principle. *Formalized Mathematics*, 1(**3**):575–579, 1990.
[24] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(**2**):291–296, 1990.
[25] Wojciech A. Trybulec. Lattice of subgroups of a group. Frattini subgroup. *Formalized Mathematics*, 2(**1**):41–47, 1991.
[26] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[27] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.
[28] Katarzyna Zawadzka. The product and the determinant of matrices with entries in a field. *Formalized Mathematics*, 4(**1**):1–8, 1993.

Received January 4, 2006

FORMALIZED MATHEMATICS
Volume 14, Number 1, Pages 7–12
University of Białystok, 2006

Some Properties of Some Special Matrices. Part II

Xiaopeng Yue
Qingdao University of Science and Technology
China

Dahai Hu
Qingdao University of Science and Technology
China

Xiquan Liang
Qingdao University of Science and Technology
China

Summary. This article provides definitions of idempotent, nilpotent, involutory, self-reversible, similar, and congruent matrices, the trace of a matrix and their main properties.

MML identifier: `MATRIX_8`, version: `7.6.01 4.53.937`

The terminology and notation used here are introduced in the following articles: [7], [3], [1], [9], [8], [6], [4], [2], [5], [11], and [10].

We adopt the following convention: n is a natural number, K is a field, and M_1, M_2, M_3, M_4, M_5, M_6 are matrices over K of dimension n.

Let n be a natural number, let K be a field, and let M_1 be a matrix over K of dimension n. We say that M_1 is idempotent if and only if:

(Def. 1) $M_1 \cdot M_1 = M_1$.

We say that M_1 is 2-nilpotent if and only if:

(Def. 2) $$M_1 \cdot M_1 = \begin{pmatrix} 0 & \ldots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \ldots & 0 \end{pmatrix}_K^{n \times n}.$$

We say that M_1 is involutory if and only if:

ISSN 1426–2630

(Def. 3) $M_1 \cdot M_1 = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}_K^{n \times n}$.

We say that M_1 is self invertible if and only if:

(Def. 4) M_1 is invertible and $M_1{}^{\smile} = M_1$.

We now state a number of propositions:

(1) $\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}_K^{n \times n}$ is idempotent and involutory.

(2) If $n > 0$, then $\begin{pmatrix} 0 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 0 \end{pmatrix}_K^{n \times n}$ is idempotent and 2-nilpotent.

(3) If $n > 0$ and $M_2 = M_1{}^{\mathrm{T}}$, then M_1 is idempotent iff M_2 is idempotent.

(4) If M_1 is involutory, then M_1 is invertible.

(5) If M_1 is idempotent and M_2 is idempotent and M_1 is permutable with M_2, then $M_1 \cdot M_1$ is permutable with $M_2 \cdot M_2$.

(6) If $n > 0$ and M_1 is idempotent and M_2 is idempotent and M_1 is permutable with M_2 and $M_1 \cdot M_2 = \begin{pmatrix} 0 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 0 \end{pmatrix}_K^{n \times n}$, then $M_1 + M_2$ is idempotent.

(7) If $n > 0$ and M_1 is idempotent and M_2 is idempotent and $M_1 \cdot M_2 = -M_2 \cdot M_1$, then $M_1 + M_2$ is idempotent.

(8) If M_1 is idempotent and M_2 is invertible, then $M_2{}^{\smile} \cdot M_1 \cdot M_2$ is idempotent.

(9) If $n > 0$ and M_1 is invertible and idempotent, then $M_1{}^{\smile}$ is idempotent.

(10) If M_1 is invertible and idempotent, then $M_1 = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}_K^{n \times n}$.

(11) If M_1 is idempotent and M_2 is idempotent and M_1 is permutable with M_2, then $M_1 \cdot M_2$ is idempotent.

(12) If $n > 0$ and M_1 is idempotent and M_2 is idempotent and M_1 is permutable with M_2 and $M_3 = M_1{}^{\mathrm{T}} \cdot M_2{}^{\mathrm{T}}$, then M_3 is idempotent.

(13) If M_1 is idempotent and M_2 is idempotent and M_1 is invertible, then $M_1 \cdot M_2$ is idempotent.

(14) If $n > 0$ and M_1 is idempotent and orthogonal, then M_1 is symmetrical.

(15) If M_1 is idempotent and M_2 is idempotent and $M_2 \cdot M_1 = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}_K^{n\times n}$, then $M_1 \cdot M_2$ is idempotent.

(16) If M_1 is idempotent and orthogonal, then $M_1 = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}_K^{n\times n}$.

(17) If $n > 0$ and M_1 is symmetrical and $M_2 = {M_1}^{\mathrm{T}}$, then $M_1 \cdot M_2$ is symmetrical.

(18) If $n > 0$ and M_1 is symmetrical and $M_2 = {M_1}^{\mathrm{T}}$, then $M_2 \cdot M_1$ is symmetrical.

(19) If M_1 is invertible and $M_1 \cdot M_2 = M_1 \cdot M_3$, then $M_2 = M_3$.

(20) If M_1 is invertible and $M_2 \cdot M_1 = M_3 \cdot M_1$, then $M_2 = M_3$.

(21) If $n > 0$ and M_1 is invertible and $M_2 \cdot M_1 = \begin{pmatrix} 0 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 0 \end{pmatrix}_K^{n\times n}$, then
$M_2 = \begin{pmatrix} 0 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 0 \end{pmatrix}_K^{n\times n}$.

(22) If $n > 0$ and M_1 is invertible and $M_2 \cdot M_1 = \begin{pmatrix} 0 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 0 \end{pmatrix}_K^{n\times n}$, then
$M_2 = \begin{pmatrix} 0 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 0 \end{pmatrix}_K^{n\times n}$.

(23) If M_1 is 2-nilpotent and permutable with M_2 and $n > 0$, then $M_1 \cdot M_2$ is 2-nilpotent.

(24) If $n > 0$ and M_1 is 2-nilpotent and M_2 is 2-nilpotent and M_1 is permutable with M_2 and $M_1 \cdot M_2 = \begin{pmatrix} 0 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 0 \end{pmatrix}_K^{n\times n}$, then $M_1 + M_2$ is 2-nilpotent.

(25) If M_1 is 2-nilpotent and M_2 is 2-nilpotent and $M_1 \cdot M_2 = -M_2 \cdot M_1$ and $n > 0$, then $M_1 + M_2$ is 2-nilpotent.

(26) If M_1 is 2-nilpotent and $M_2 = {M_1}^{\mathrm{T}}$ and $n > 0$, then M_2 is 2-nilpotent.

(27) If M_1 is 2-nilpotent and idempotent, then $M_1 = \begin{pmatrix} 0 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 0 \end{pmatrix}_K^{n \times n}$.

(28) If $n > 0$, then $\begin{pmatrix} 0 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 0 \end{pmatrix}_K^{n \times n} \neq \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}_K^{n \times n}$.

(29) If $n > 0$ and M_1 is 2-nilpotent, then M_1 is not invertible.

(30) If M_1 is self invertible, then M_1 is involutory.

(31) $\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}_K^{n \times n}$ is self invertible.

(32) If M_1 is self invertible and idempotent, then $M_1 = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}_K^{n \times n}$.

(33) If M_1 is self invertible and symmetrical, then M_1 is orthogonal.

Let n be a natural number, let K be a field, and let M_1, M_2 be matrices over K of dimension n. We say that M_1 is similar to M_2 if and only if:

(Def. 5) There exists a matrix M over K of dimension n such that M is invertible and $M_1 = M^{\smile} \cdot M_2 \cdot M$.

Let us notice that the predicate M_1 is similar to M_2 is reflexive and symmetric.

The following propositions are true:

(34) If M_1 is similar to M_2 and M_2 is similar to M_3 and $n > 0$, then M_1 is similar to M_3.

(35) If M_1 is similar to M_2 and M_2 is idempotent, then M_1 is idempotent.

(36) If M_1 is similar to M_2 and M_2 is 2-nilpotent and $n > 0$, then M_1 is 2-nilpotent.

(37) If M_1 is similar to M_2 and M_2 is involutory, then M_1 is involutory.

(38) If M_1 is similar to M_2 and $n > 0$, then $M_1 + \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}_K^{n \times n}$ is similar to $M_2 + \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}_K^{n \times n}$.

(39) If M_1 is similar to M_2 and $n > 0$, then $M_1 + M_1$ is similar to $M_2 + M_2$.

(40) If M_1 is similar to M_2 and $n > 0$, then $M_1 + M_1 + M_1$ is similar to $M_2 + M_2 + M_2$.

(41) If M_1 is invertible, then $M_2 \cdot M_1$ is similar to $M_1 \cdot M_2$.

(42) If M_2 is invertible and M_1 is similar to M_2 and $n > 0$, then M_1 is invertible.

(43) If M_2 is invertible and M_1 is similar to M_2 and $n > 0$, then $M_1{}^{\smile}$ is similar to $M_2{}^{\smile}$.

Let n be a natural number, let K be a field, and let M_1, M_2 be matrices over K of dimension n. We say that M_1 is congruent to M_2 if and only if:

(Def. 6) There exists a matrix M over K of dimension n such that M is invertible and $M_1 = M^{\mathrm{T}} \cdot M_2 \cdot M$.

Next we state several propositions:

(44) If $n > 0$, then M_1 is congruent to M_1.

(45) If M_1 is congruent to M_2 and $n > 0$, then M_2 is congruent to M_1.

(46) If M_1 is congruent to M_2 and M_2 is congruent to M_3 and $n > 0$, then M_1 is congruent to M_3.

(47) If M_1 is congruent to M_2 and $n > 0$, then $M_1 + M_1$ is congruent to $M_2 + M_2$.

(48) If M_1 is congruent to M_2 and $n > 0$, then $M_1 + M_1 + M_1$ is congruent to $M_2 + M_2 + M_2$.

(49) If M_1 is orthogonal, then $M_2 \cdot M_1$ is congruent to $M_1 \cdot M_2$.

(50) If M_2 is invertible and M_1 is congruent to M_2 and $n > 0$, then M_1 is invertible.

(51) If M_2 is invertible and M_1 is congruent to M_2 and $n > 0$ and $M_5 = M_1{}^{\mathrm{T}}$ and $M_6 = M_2{}^{\mathrm{T}}$, then M_5 is congruent to M_6.

(52) If M_4 is orthogonal and $M_1 = M_4{}^{\mathrm{T}} \cdot M_2 \cdot M_4$, then M_1 is similar to M_2.

Let n be a natural number, let K be a field, and let M be a matrix over K of dimension n. The functor $\mathrm{Trace}(M)$ yields an element of K and is defined by:

(Def. 7) $\mathrm{Trace}(M) = \sum(\text{the diagonal of } M)$.

The following propositions are true:

(53) If $M_2 = M_1{}^{\mathrm{T}}$, then $\mathrm{Trace}(M_1) = \mathrm{Trace}(M_2)$.

(54) $\mathrm{Trace}(M_1 + M_2) = \mathrm{Trace}(M_1) + \mathrm{Trace}(M_2)$.

(55) $\mathrm{Trace}(M_1 + M_2 + M_3) = \mathrm{Trace}(M_1) + \mathrm{Trace}(M_2) + \mathrm{Trace}(M_3)$.

(56) $\mathrm{Trace}(\begin{pmatrix} 0 & \ldots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \ldots & 0 \end{pmatrix}^{n \times n}_{K}) = 0_K$.

(57) If $n > 0$, then $\mathrm{Trace}(-M_1) = -\mathrm{Trace}(M_1)$.

(58) If $n > 0$, then $-\mathrm{Trace}(-M_1) = \mathrm{Trace}(M_1)$.

(59) If $n > 0$, then $\mathrm{Trace}(M_1 + -M_1) = 0_K$.

(60) If $n > 0$, then $\mathrm{Trace}(M_1 - M_2) = \mathrm{Trace}(M_1) - \mathrm{Trace}(M_2)$.

(61) If $n > 0$, then $\mathrm{Trace}((M_1 - M_2) + M_3) = (\mathrm{Trace}(M_1) - \mathrm{Trace}(M_2)) + \mathrm{Trace}(M_3)$.

(62) If $n > 0$, then $\mathrm{Trace}((M_1 + M_2) - M_3) = (\mathrm{Trace}(M_1) + \mathrm{Trace}(M_2)) - \mathrm{Trace}(M_3)$.

(63) If $n > 0$, then $\mathrm{Trace}(M_1 - M_2 - M_3) = \mathrm{Trace}(M_1) - \mathrm{Trace}(M_2) - \mathrm{Trace}(M_3)$.

References

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

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

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

[4] Katarzyna Jankowska. Matrices. Abelian group of matrices. *Formalized Mathematics*, 2(**4**):475–480, 1991.

[5] Katarzyna Jankowska. Transpose matrices and groups of permutations. *Formalized Mathematics*, 2(**5**):711–717, 1991.

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

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

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

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

[10] Xiaopeng Yue, Xiquan Liang, and Zhongpin Sun. Some properties of some special matrices. *Formalized Mathematics*, 13(**4**):541–547, 2005.

[11] Katarzyna Zawadzka. The product and the determinant of matrices with entries in a field. *Formalized Mathematics*, 4(**1**):1–8, 1993.

Received January 4, 2006

FORMALIZED MATHEMATICS
Volume 14, Number 1, Pages 13–20
University of Białystok, 2006

On the Permanent of a Matrix

Ewa Romanowicz[1]
Institute of Mathematics
University of Białystok
Akademicka 2, 15-267 Białystok, Poland

Adam Grabowski[2]
Institute of Mathematics
University of Białystok
Akademicka 2, 15-267 Białystok, Poland

Summary. We introduce the notion of a permanent [13] of a square matrix. It is a notion somewhat related to a determinant, so we follow closely the approach and theorems already introduced in the Mizar Mathematical Library for the determinant. Unfortunately, the formalization of the latter notion is at its early stage, so we had to prove many very elementary auxiliary facts.

MML identifier: `MATRIX_9`, version: `7.6.01 4.53.937`

The articles [18], [25], [14], [1], [16], [9], [26], [4], [6], [5], [2], [3], [15], [20], [21], [12], [23], [17], [24], [7], [19], [10], [22], [8], [11], and [27] provide the terminology and notation for this paper.

1. Preliminaries

In this paper i, n are natural numbers and K is a field.

We now state the proposition

(1) For all sets a, A such that $a \in A$ holds $\{a\} \in \operatorname{Fin} A$.

[1]This is a part of the author's MSc thesis.

[2]This work has been partially supported by the KBN grant 4 T11C 039 24 and the FP6 IST grant TYPES No. 510996.

ISSN 1426–2630

Let n be a natural number. Observe that there exists an element of Fin (the permutations of n-element set) which is non empty.

The scheme *NonEmptyFiniteX* deals with a natural number $\mathcal{A}$, a non empty element $\mathcal{B}$ of Fin the permutations of $\mathcal{A}$-element set, and a unary predicate $\mathcal{P}$, and states that:

$\mathcal{P}[\mathcal{B}]$

provided the following conditions are met:

- For every element x of the permutations of $\mathcal{A}$-element set such that $x \in \mathcal{B}$ holds $\mathcal{P}[\{x\}]$, and
- Let x be an element of the permutations of $\mathcal{A}$-element set and B be a non empty element of Fin (the permutations of $\mathcal{A}$-element set). If $x \in \mathcal{B}$ and $B \subseteq \mathcal{B}$ and $x \notin B$ and $\mathcal{P}[B]$, then $\mathcal{P}[B \cup \{x\}]$.

Let us consider n. Observe that there exists a function from $\mathrm{Seg}\, n$ into $\mathrm{Seg}\, n$ which is one-to-one and finite sequence-like.

Let us consider n. Observe that $\mathrm{id}_{\mathrm{Seg}\, n}$ is finite sequence-like.

One can prove the following two propositions:

(2) $(\mathrm{Rev}(\mathrm{idseq}(2)))(1) = 2$ and $(\mathrm{Rev}(\mathrm{idseq}(2)))(2) = 1$.

(3) For every one-to-one function f such that $\mathrm{dom}\, f = \mathrm{Seg}\, 2$ and $\mathrm{rng}\, f = \mathrm{Seg}\, 2$ holds $f = \mathrm{id}_{\mathrm{Seg}\, 2}$ or $f = \mathrm{Rev}(\mathrm{id}_{\mathrm{Seg}\, 2})$.

2. Permutations

One can prove the following propositions:

(4) $\mathrm{Rev}(\mathrm{idseq}(n)) \in$ the permutations of n-element set.

(5) Let f be a finite sequence. Suppose $n \neq 0$ and $f \in$ the permutations of n-element set. Then $\mathrm{Rev}(f) \in$ the permutations of n-element set.

(6) The permutations of 2-element set $= \{\mathrm{idseq}(2), \mathrm{Rev}(\mathrm{idseq}(2))\}$.

3. The Permanent of a Matrix

Let us consider n, K and let M be a matrix over K of dimension n. The functor PPath M yielding a function from the permutations of n-element set into the carrier of K is defined by:

(Def. 1) For every element p of the permutations of n-element set holds $(\mathrm{PPath}\, M)(p) = (\text{the multiplication of } K) \circledast (p\text{-}\mathrm{Path}\, M)$.

Let us consider n, K and let M be a matrix over K of dimension n. The functor Per M yielding an element of K is defined as follows:

(Def. 2) $\mathrm{Per}\, M = (\text{the addition of } K)\text{-}\sum_{\Omega^{\mathrm{f}}_{\text{the permutations of } n\text{-element set}}} \mathrm{PPath}\, M$.

In the sequel a, b, c, d denote elements of K.

The following propositions are true:

(7) $\mathrm{Per}\langle\langle a\rangle\rangle = a$.

(8) For every field K and for every natural number n such that $n \geq 1$ holds $\mathrm{Per}(\begin{pmatrix} 0 & \ldots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \ldots & 0 \end{pmatrix}_K^{n \times n}) = 0_K$.

(9) For every element p of the permutations of 2-element set such that $p = \mathrm{idseq}(2)$ holds p-Path $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \langle a, d\rangle$.

(10) For every element p of the permutations of 2-element set such that $p = \mathrm{Rev}(\mathrm{idseq}(2))$ holds p-Path $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \langle b, c\rangle$.

(11) (The multiplication of K) $\circledast \langle a, b\rangle = a \cdot b$.

4. Matrices with the Dimension 2 and 3

One can check that there exists a permutation of $\mathrm{Seg}\,2$ which is odd.

Let n be a natural number. Observe that there exists a permutation of $\mathrm{Seg}\,n$ which is even.

One can prove the following four propositions:

(12) $\langle 2, 1\rangle$ is an odd permutation of $\mathrm{Seg}\,2$.

(13) $\mathrm{Det}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = a \cdot d - b \cdot c$.

(14) $\mathrm{Per}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = a \cdot d + b \cdot c$.

(15) $\mathrm{Rev}(\mathrm{idseq}(3)) = \langle 3, 2, 1\rangle$.

In the sequel D is a non empty set.

One can prove the following propositions:

(16) For all elements x, y, z of D and for every finite sequence f of elements of D such that $f = \langle x, y, z\rangle$ holds $\mathrm{Rev}(f) = \langle z, y, x\rangle$.

(17) Let f, g be finite sequences. Suppose $f \frown g \in$ the permutations of n-element set. Then $f \frown \mathrm{Rev}(g) \in$ the permutations of n-element set.

(18) Let f, g be finite sequences. Suppose $f \frown g \in$ the permutations of n-element set. Then $g \frown f \in$ the permutations of n-element set.

(19) The permutations of 3-element set $= \{\langle 1, 2, 3\rangle, \langle 3, 2, 1\rangle, \langle 1, 3, 2\rangle, \langle 2, 3, 1\rangle, \langle 2, 1, 3\rangle, \langle 3, 1, 2\rangle\}$.

(20) Let a, b, c, d, e, f, g, h, i be elements of K and M be a matrix over K of dimension 3. Suppose $M = \langle\langle a, b, c\rangle, \langle d, e, f\rangle, \langle g, h, i\rangle\rangle$. Let p be an element of the permutations of 3-element set. If $p = \langle 1, 2, 3\rangle$, then p-Path $M = \langle a, e, i\rangle$.

(21) Let a, b, c, d, e, f, g, h, i be elements of K and M be a matrix over K of dimension 3. Suppose $M = \langle\langle a, b, c\rangle, \langle d, e, f\rangle, \langle g, h, i\rangle\rangle$. Let p be an element of the permutations of 3-element set. If $p = \langle 3, 2, 1\rangle$, then p-Path $M = \langle c, e, g\rangle$.

(22) Let a, b, c, d, e, f, g, h, i be elements of K and M be a matrix over K of dimension 3. Suppose $M = \langle\langle a, b, c\rangle, \langle d, e, f\rangle, \langle g, h, i\rangle\rangle$. Let p be an element of the permutations of 3-element set. If $p = \langle 1, 3, 2\rangle$, then p-Path $M = \langle a, f, h\rangle$.

(23) Let a, b, c, d, e, f, g, h, i be elements of K and M be a matrix over K of dimension 3. Suppose $M = \langle\langle a, b, c\rangle, \langle d, e, f\rangle, \langle g, h, i\rangle\rangle$. Let p be an element of the permutations of 3-element set. If $p = \langle 2, 3, 1\rangle$, then p-Path $M = \langle b, f, g\rangle$.

(24) Let a, b, c, d, e, f, g, h, i be elements of K and M be a matrix over K of dimension 3. Suppose $M = \langle\langle a, b, c\rangle, \langle d, e, f\rangle, \langle g, h, i\rangle\rangle$. Let p be an element of the permutations of 3-element set. If $p = \langle 2, 1, 3\rangle$, then p-Path $M = \langle b, d, i\rangle$.

(25) Let a, b, c, d, e, f, g, h, i be elements of K and M be a matrix over K of dimension 3. Suppose $M = \langle\langle a, b, c\rangle, \langle d, e, f\rangle, \langle g, h, i\rangle\rangle$. Let p be an element of the permutations of 3-element set. If $p = \langle 3, 1, 2\rangle$, then p-Path $M = \langle c, d, h\rangle$.

(26) (The multiplication of K) $\circledast \langle a, b, c\rangle = a \cdot b \cdot c$.

(27)(i) $\langle 1, 3, 2\rangle \in$ the permutations of 3-element set,
(ii) $\langle 2, 3, 1\rangle \in$ the permutations of 3-element set,
(iii) $\langle 2, 1, 3\rangle \in$ the permutations of 3-element set,
(iv) $\langle 3, 1, 2\rangle \in$ the permutations of 3-element set,
(v) $\langle 1, 2, 3\rangle \in$ the permutations of 3-element set, and
(vi) $\langle 3, 2, 1\rangle \in$ the permutations of 3-element set.

(28) $\langle 2, 3, 1\rangle^{-1} = \langle 3, 1, 2\rangle$.

(29) For every element a of A_3 such that $a = \langle 2, 3, 1\rangle$ holds $a^{-1} = \langle 3, 1, 2\rangle$.

5. Transpositions

The following propositions are true:

(30) For every permutation p of Seg 3 such that $p = \langle 1, 3, 2\rangle$ holds p is a transposition.

(31) For every permutation p of Seg 3 such that $p = \langle 2, 1, 3\rangle$ holds p is a transposition.

(32) For every permutation p of Seg 3 such that $p = \langle 3, 2, 1\rangle$ holds p is a transposition.

(33) For every permutation p of $\mathrm{Seg}\,n$ such that $p = \mathrm{id}_{\mathrm{Seg}\,n}$ holds p is not a transposition.

(34) For every permutation p of $\mathrm{Seg}\,3$ such that $p = \langle 3, 1, 2\rangle$ holds p is not a transposition.

(35) For every permutation p of $\mathrm{Seg}\,3$ such that $p = \langle 2, 3, 1\rangle$ holds p is not a transposition.

6. Even and Odd Permutations

One can prove the following propositions:

(36) Every permutation of $\mathrm{Seg}\,n$ is a finite sequence of elements of $\mathrm{Seg}\,n$.

(37) $\langle 2, 1, 3\rangle \cdot \langle 1, 3, 2\rangle = \langle 2, 3, 1\rangle$ and $\langle 1, 3, 2\rangle \cdot \langle 2, 1, 3\rangle = \langle 3, 1, 2\rangle$ and $\langle 2, 1, 3\rangle \cdot \langle 3, 2, 1\rangle = \langle 3, 1, 2\rangle$ and $\langle 3, 2, 1\rangle \cdot \langle 2, 1, 3\rangle = \langle 2, 3, 1\rangle$ and $\langle 3, 2, 1\rangle \cdot \langle 3, 2, 1\rangle = \langle 1, 2, 3\rangle$ and $\langle 2, 1, 3\rangle \cdot \langle 2, 1, 3\rangle = \langle 1, 2, 3\rangle$ and $\langle 1, 3, 2\rangle \cdot \langle 1, 3, 2\rangle = \langle 1, 2, 3\rangle$ and $\langle 1, 3, 2\rangle \cdot \langle 2, 3, 1\rangle = \langle 3, 2, 1\rangle$ and $\langle 2, 3, 1\rangle \cdot \langle 2, 3, 1\rangle = \langle 3, 1, 2\rangle$ and $\langle 2, 3, 1\rangle \cdot \langle 3, 1, 2\rangle = \langle 1, 2, 3\rangle$ and $\langle 3, 1, 2\rangle \cdot \langle 2, 3, 1\rangle = \langle 1, 2, 3\rangle$ and $\langle 3, 1, 2\rangle \cdot \langle 3, 1, 2\rangle = \langle 2, 3, 1\rangle$ and $\langle 1, 3, 2\rangle \cdot \langle 3, 2, 1\rangle = \langle 2, 3, 1\rangle$ and $\langle 3, 2, 1\rangle \cdot \langle 1, 3, 2\rangle = \langle 3, 1, 2\rangle$.

(38) For every permutation p of $\mathrm{Seg}\,3$ such that p is a transposition holds $p = \langle 2, 1, 3\rangle$ or $p = \langle 1, 3, 2\rangle$ or $p = \langle 3, 2, 1\rangle$.

(39) For all elements f, g of the permutations of n-element set holds $f \cdot g \in$ the permutations of n-element set.

(40) Let l be a finite sequence of elements of A_n. Suppose that
(i) $\mathrm{len}\,l \bmod 2 = 0$, and
(ii) for every natural number i such that $i \in \mathrm{dom}\,l$ there exists an element q of the permutations of n-element set such that $l(i) = q$ and q is a transposition.
Then $\prod l$ is an even permutation of $\mathrm{Seg}\,n$.

(41) Let l be a finite sequence of elements of A_3. Suppose that
(i) $\mathrm{len}\,l \bmod 2 = 0$, and
(ii) for every natural number i such that $i \in \mathrm{dom}\,l$ there exists an element q of the permutations of 3-element set such that $l(i) = q$ and q is a transposition.
Then $\prod l = \langle 1, 2, 3\rangle$ or $\prod l = \langle 2, 3, 1\rangle$ or $\prod l = \langle 3, 1, 2\rangle$.

Let us mention that there exists a permutation of $\mathrm{Seg}\,3$ which is odd.

We now state four propositions:

(42) $\langle 3, 2, 1\rangle$ is an odd permutation of $\mathrm{Seg}\,3$.

(43) $\langle 2, 1, 3\rangle$ is an odd permutation of $\mathrm{Seg}\,3$.

(44) $\langle 1, 3, 2\rangle$ is an odd permutation of $\mathrm{Seg}\,3$.

(45) For every odd permutation p of $\operatorname{Seg} 3$ holds $p = \langle 3, 2, 1 \rangle$ or $p = \langle 1, 3, 2 \rangle$ or $p = \langle 2, 1, 3 \rangle$.

7. Determinant and Permanent

One can prove the following propositions:

(46) Let a, b, c, d, e, f, g, h, i be elements of K and M be a matrix over K of dimension 3. If $M = \langle \langle a, b, c \rangle, \langle d, e, f \rangle, \langle g, h, i \rangle \rangle$, then $\operatorname{Det} M = (((a \cdot e \cdot i - c \cdot e \cdot g - a \cdot f \cdot h) + b \cdot f \cdot g) - b \cdot d \cdot i) + c \cdot d \cdot h$.

(47) Let a, b, c, d, e, f, g, h, i be elements of K and M be a matrix over K of dimension 3. If $M = \langle \langle a, b, c \rangle, \langle d, e, f \rangle, \langle g, h, i \rangle \rangle$, then $\operatorname{Per} M = a \cdot e \cdot i + c \cdot e \cdot g + a \cdot f \cdot h + b \cdot f \cdot g + b \cdot d \cdot i + c \cdot d \cdot h$.

(48) Let i, n be natural numbers and p be an element of the permutations of n-element set. If $i \in \operatorname{Seg} n$, then there exists a natural number k such that $k \in \operatorname{Seg} n$ and $i = p(k)$.

(49) Let M be a matrix over K of dimension n. Given a natural number i such that $i \in \operatorname{Seg} n$ and for every natural number k such that $k \in \operatorname{Seg} n$ holds $M_{\square,i}(k) = 0_K$. Let p be an element of the permutations of n-element set. Then there exists a natural number l such that $l \in \operatorname{Seg} n$ and $(p\text{-Path}\, M)(l) = 0_K$.

(50) Let p be an element of the permutations of n-element set and M be a matrix over K of dimension n. Given a natural number i such that $i \in \operatorname{Seg} n$ and for every natural number k such that $k \in \operatorname{Seg} n$ holds $M_{\square,i}(k) = 0_K$. Then (the product on paths of M)$(p) = 0_K$.

(51) Let M be a matrix over K of dimension n. Given a natural number i such that $i \in \operatorname{Seg} n$ and for every natural number k such that $k \in \operatorname{Seg} n$ holds $M_{\square,i}(k) = 0_K$. Then (the addition of K)-$\sum_{\Omega^{\mathrm{f}}_{\text{the permutations of } n\text{-element set}}}$(the product on paths of M) $= 0_K$.

(52) Let p be an element of the permutations of n-element set and M be a matrix over K of dimension n. Given a natural number i such that $i \in \operatorname{Seg} n$ and for every natural number k such that $k \in \operatorname{Seg} n$ holds $M_{\square,i}(k) = 0_K$. Then $(\operatorname{PPath} M)(p) = 0_K$.

(53) Let M be a matrix over K of dimension n. Given a natural number i such that $i \in \operatorname{Seg} n$ and for every natural number k such that $k \in \operatorname{Seg} n$ holds $M_{\square,i}(k) = 0_K$. Then $\operatorname{Det} M = 0_K$.

(54) Let M be a matrix over K of dimension n. Given a natural number i such that $i \in \operatorname{Seg} n$ and for every natural number k such that $k \in \operatorname{Seg} n$ holds $M_{\square,i}(k) = 0_K$. Then $\operatorname{Per} M = 0_K$.

8. On the Paths of Matrices

One can prove the following two propositions:

(55) Let M, N be matrices over K of dimension n. Suppose $i \in \operatorname{Seg} n$. Let p be an element of the permutations of n-element set. Then there exists a natural number k such that $k \in \operatorname{Seg} n$ and $i = p(k)$ and $(N_{\square,i})_k = (p\text{-Path}\, N)_k$.

(56) Let a be an element of K and M, N be matrices over K of dimension n. Given a natural number i such that

(i) $i \in \operatorname{Seg} n$,

(ii) for every natural number k such that $k \in \operatorname{Seg} n$ holds $M_{\square,i}(k) = a \cdot (N_{\square,i})_k$, and

(iii) for every natural number l such that $l \neq i$ and $l \in \operatorname{Seg} n$ holds $M_{\square,l} = N_{\square,l}$.

Let p be an element of the permutations of n-element set. Then there exists a natural number l such that $l \in \operatorname{Seg} n$ and $(p\text{-Path}\, M)_l = a \cdot (p\text{-Path}\, N)_l$.

References

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

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

[3] Czesław Byliński. Finite sequences and tuples of elements of a non-empty sets. *Formalized Mathematics*, 1(**3**):529–536, 1990.

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

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

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

[7] Czesław Byliński. Semigroup operations on finite subsets. *Formalized Mathematics*, 1(**4**):651–656, 1990.

[8] Czesław Byliński. Some properties of restrictions of finite sequences. *Formalized Mathematics*, 5(**2**):241–245, 1996.

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

[10] Katarzyna Jankowska. Matrices. Abelian group of matrices. *Formalized Mathematics*, 2(**4**):475–480, 1991.

[11] Katarzyna Jankowska. Transpose matrices and groups of permutations. *Formalized Mathematics*, 2(**5**):711–717, 1991.

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

[13] H. Minc. *Permanents*. Addison-Wesley, 1978.

[14] Andrzej Trybulec. Subsets of complex numbers. *To appear in Formalized Mathematics.*

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

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

[17] Andrzej Trybulec. Semilattice operations on finite subsets. *Formalized Mathematics*, 1(**2**):369–376, 1990.

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

[19] Andrzej Trybulec and Agata Darmochwał. Boolean domains. *Formalized Mathematics*, 1(**1**):187–190, 1990.

[20] Wojciech A. Trybulec. Binary operations on finite sequences. *Formalized Mathematics*, 1(**5**):979–981, 1990.
[21] Wojciech A. Trybulec. Groups. *Formalized Mathematics*, 1(**5**):821–827, 1990.
[22] Wojciech A. Trybulec. Pigeon hole principle. *Formalized Mathematics*, 1(**3**):575–579, 1990.
[23] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(**2**):291–296, 1990.
[24] Wojciech A. Trybulec. Lattice of subgroups of a group. Frattini subgroup. *Formalized Mathematics*, 2(**1**):41–47, 1991.
[25] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[26] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.
[27] Katarzyna Zawadzka. The product and the determinant of matrices with entries in a field. *Formalized Mathematics*, 4(**1**):1–8, 1993.

Received January 4, 2006

FORMALIZED MATHEMATICS
Volume 14, Number 1, Pages 21–28
University of Białystok, 2006

A Theory of Matrices of Real Elements

Yatsuka Nakamura
Shinshu University
Nagano, Japan

Nobuyuki Tamura
Shinshu University
Nagano, Japan

Wenpai Chang
Shinshu University
Nagano, Japan

Summary. Here, the concept of matrix of real elements is introduced. This is defined as a special case of the general concept of matrix of a field. For such a real matrix, the notions of addition, subtraction, scalar product are defined. For any real finite sequences, two transformations to matrices are introduced. One of the matrices is of width 1, and the other is of length 1. By such transformations, two products of a matrix and a finite sequence are defined. Also the linearity of such product is shown.

MML identifier: `MATRIXR1`, version: `7.6.02 4.59.938`

The papers [16], [19], [6], [3], [10], [18], [15], [1], [14], [12], [20], [7], [2], [17], [13], [22], [8], [11], [5], [4], [21], and [9] provide the terminology and notation for this paper.

1. Preliminaries

In this paper i, j are natural numbers.

We now state a number of propositions:

(1) For all real numbers r_1, r_2 and for all elements f_1, f_2 of $\mathbb{R}_{\rm F}$ such that $r_1 = f_1$ and $r_2 = f_2$ holds $r_1 + r_2 = f_1 + f_2$.

(2) For all real numbers r_1, r_2 and for all elements f_1, f_2 of $\mathbb{R}_{\rm F}$ such that $r_1 = f_1$ and $r_2 = f_2$ holds $r_1 \cdot r_2 = f_1 \cdot f_2$.

(3) For every finite sequence F of elements of $\mathbb{R}$ holds $F + -F = \langle\underbrace{0, \ldots, 0}_{\mathrm{len}\, F}\rangle$ and $F - F = \langle\underbrace{0, \ldots, 0}_{\mathrm{len}\, F}\rangle$.

ISSN 1426–2630

(4) For all finite sequences F_1, F_2 of elements of $\mathbb{R}$ such that $\operatorname{len} F_1 = \operatorname{len} F_2$ holds $F_1 - F_2 = F_1 + -F_2$.

(5) For every finite sequence F of elements of $\mathbb{R}$ holds $F - \langle \underbrace{0, \ldots, 0}_{\operatorname{len} F} \rangle = F$.

(6) For every finite sequence F of elements of $\mathbb{R}$ holds $\langle \underbrace{0, \ldots, 0}_{\operatorname{len} F} \rangle - F = -F$.

(7) For all finite sequences F_1, F_2 of elements of $\mathbb{R}$ such that $\operatorname{len} F_1 = \operatorname{len} F_2$ holds $F_1 - -F_2 = F_1 + F_2$.

(8) For all finite sequences F_1, F_2 of elements of $\mathbb{R}$ such that $\operatorname{len} F_1 = \operatorname{len} F_2$ holds $-(F_1 - F_2) = F_2 - F_1$.

(9) For all finite sequences F_1, F_2 of elements of $\mathbb{R}$ such that $\operatorname{len} F_1 = \operatorname{len} F_2$ holds $-(F_1 - F_2) = -F_1 + F_2$.

(10) For all finite sequences F_1, F_2 of elements of $\mathbb{R}$ such that $\operatorname{len} F_1 = \operatorname{len} F_2$ and $F_1 - F_2 = \langle \underbrace{0, \ldots, 0}_{\operatorname{len} F_1} \rangle$ holds $F_1 = F_2$.

(11) For all finite sequences F_1, F_2, F_3 of elements of $\mathbb{R}$ such that $\operatorname{len} F_1 = \operatorname{len} F_2$ and $\operatorname{len} F_2 = \operatorname{len} F_3$ holds $F_1 - F_2 - F_3 = F_1 - (F_2 + F_3)$.

(12) For all finite sequences F_1, F_2, F_3 of elements of $\mathbb{R}$ such that $\operatorname{len} F_1 = \operatorname{len} F_2$ and $\operatorname{len} F_2 = \operatorname{len} F_3$ holds $F_1 + (F_2 - F_3) = (F_1 + F_2) - F_3$.

(13) For all finite sequences F_1, F_2, F_3 of elements of $\mathbb{R}$ such that $\operatorname{len} F_1 = \operatorname{len} F_2$ and $\operatorname{len} F_2 = \operatorname{len} F_3$ holds $F_1 - (F_2 - F_3) = (F_1 - F_2) + F_3$.

(14) For all finite sequences F_1, F_2 of elements of $\mathbb{R}$ such that $\operatorname{len} F_1 = \operatorname{len} F_2$ holds $F_1 = (F_1 + F_2) - F_2$.

(15) For all finite sequences F_1, F_2 of elements of $\mathbb{R}$ such that $\operatorname{len} F_1 = \operatorname{len} F_2$ holds $F_1 = (F_1 - F_2) + F_2$.

2. Matrices of Real Elements

The following propositions are true:

(16) Let K be a non empty groupoid, p be a finite sequence of elements of K, and a be an element of K. Then $\operatorname{len}(a \cdot p) = \operatorname{len} p$.

(17) Let r be a real number, f_3 be an element of $\mathbb{R}_{\mathrm{F}}$, p be a finite sequence of elements of $\mathbb{R}$, and f_4 be a finite sequence of elements of $\mathbb{R}_{\mathrm{F}}$. If $r = f_3$ and $p = f_4$, then $r \cdot p = f_3 \cdot f_4$.

(18) Let K be a field, a be an element of K, and A be a matrix over K. Then the indices of $a \cdot A =$ the indices of A.

(19) Let K be a field, a be an element of K, and M be a matrix over K. If $1 \leq i$ and $i \leq \operatorname{width} M$, then $(a \cdot M)_{\square,i} = a \cdot M_{\square,i}$.

(20) Let K be a field, a be an element of K, M be a matrix over K, and i be a natural number. If $1 \leq i$ and $i \leq \operatorname{len} M$, then $\operatorname{Line}(a \cdot M, i) = a \cdot \operatorname{Line}(M, i)$.

(21) Let K be a field and A, B be matrices over K. Suppose $\operatorname{width} A = \operatorname{len} B$. Then there exists a matrix C over K such that $\operatorname{len} C = \operatorname{len} A$ and $\operatorname{width} C = \operatorname{width} B$ and for all i, j such that $\langle i, j \rangle \in$ the indices of C holds $C_{i,j} = \operatorname{Line}(A, i) \cdot B_{\square,j}$.

(22) Let K be a field, a be an element of K, and A, B be matrices over K. If $\operatorname{width} A = \operatorname{len} B$ and $\operatorname{len} A > 0$ and $\operatorname{len} B > 0$, then $A \cdot (a \cdot B) = a \cdot (A \cdot B)$.

Let A be a matrix over $\mathbb{R}$. The functor $(\mathbb{R} \to \mathbb{R}_{\rm F})A$ yielding a matrix over $\mathbb{R}_{\rm F}$ is defined as follows:

(Def. 1) $(\mathbb{R} \to \mathbb{R}_{\rm F})A = A$.

Let A be a matrix over $\mathbb{R}_{\rm F}$. The functor $(\mathbb{R}_{\rm F} \to \mathbb{R})A$ yielding a matrix over $\mathbb{R}$ is defined by:

(Def. 2) $(\mathbb{R}_{\rm F} \to \mathbb{R})A = A$.

We now state two propositions:

(23) Let D_1, D_2 be sets, A be a matrix over D_1, and B be a matrix over D_2. Suppose $A = B$. Let given i, j. If $\langle i, j \rangle \in$ the indices of A, then $A_{i,j} = B_{i,j}$.

(24) For every field K and for all matrices A, B over K holds the indices of $A + B =$ the indices of A.

Let A, B be matrices over $\mathbb{R}$. The functor $A + B$ yields a matrix over $\mathbb{R}$ and is defined by:

(Def. 3) $A + B = (\mathbb{R}_{\rm F} \to \mathbb{R})((\mathbb{R} \to \mathbb{R}_{\rm F})A + (\mathbb{R} \to \mathbb{R}_{\rm F})B)$.

One can prove the following two propositions:

(25) Let A, B be matrices over $\mathbb{R}$. Then $\operatorname{len}(A + B) = \operatorname{len} A$ and $\operatorname{width}(A + B) = \operatorname{width} A$ and for all i, j such that $\langle i, j \rangle \in$ the indices of A holds $(A + B)_{i,j} = A_{i,j} + B_{i,j}$.

(26) Let A, B, C be matrices over $\mathbb{R}$. Suppose $\operatorname{len} A = \operatorname{len} B$ and $\operatorname{width} A = \operatorname{width} B$ and $\operatorname{len} C = \operatorname{len} A$ and $\operatorname{width} C = \operatorname{width} A$ and for all i, j such that $\langle i, j \rangle \in$ the indices of A holds $C_{i,j} = A_{i,j} + B_{i,j}$. Then $C = A + B$.

Let A be a matrix over $\mathbb{R}$. The functor $-A$ yields a matrix over $\mathbb{R}$ and is defined as follows:

(Def. 4) $-A = (\mathbb{R}_{\rm F} \to \mathbb{R})(-(\mathbb{R} \to \mathbb{R}_{\rm F})A)$.

Let A, B be matrices over $\mathbb{R}$. The functor $A - B$ yielding a matrix over $\mathbb{R}$ is defined as follows:

(Def. 5) $A - B = (\mathbb{R}_{\rm F} \to \mathbb{R})((\mathbb{R} \to \mathbb{R}_{\rm F})A - (\mathbb{R} \to \mathbb{R}_{\rm F})B)$.

The functor $A \cdot B$ yielding a matrix over $\mathbb{R}$ is defined by:

(Def. 6) $A \cdot B = (\mathbb{R}_{\rm F} \to \mathbb{R})((\mathbb{R} \to \mathbb{R}_{\rm F})A \cdot (\mathbb{R} \to \mathbb{R}_{\rm F})B)$.

Let a be a real number and let A be a matrix over $\mathbb{R}$. The functor $a \cdot A$ yields a matrix over $\mathbb{R}$ and is defined as follows:

(Def. 7) For every element e_1 of $\mathbb{R}_{\mathrm{F}}$ such that $e_1 = a$ holds $a \cdot A = (\mathbb{R}_{\mathrm{F}} \to \mathbb{R})(e_1 \cdot (\mathbb{R} \to \mathbb{R}_{\mathrm{F}})A)$.

The following propositions are true:

(27) For every real number a and for every matrix A over $\mathbb{R}$ holds $\operatorname{len}(a \cdot A) = \operatorname{len} A$ and $\operatorname{width}(a \cdot A) = \operatorname{width} A$.

(28) For every real number a and for every matrix A over $\mathbb{R}$ holds the indices of $a \cdot A =$ the indices of A.

(29) Let a be a real number, A be a matrix over $\mathbb{R}$, and i_2, j_2 be natural numbers. If $\langle i_2, j_2 \rangle \in$ the indices of A, then $(a \cdot A)_{i_2,j_2} = a \cdot A_{i_2,j_2}$.

(30) For every real number a and for every matrix A over $\mathbb{R}$ such that $\operatorname{len} A > 0$ and $\operatorname{width} A > 0$ holds $(a \cdot A)^{\mathrm{T}} = a \cdot A^{\mathrm{T}}$.

(31) Let a be a real number, i be a natural number, and A be a matrix over $\mathbb{R}$. Suppose $\operatorname{len} A > 0$ and $i \in \operatorname{dom} A$. Then

(i) there exists a finite sequence p of elements of $\mathbb{R}$ such that $p = A(i)$, and

(ii) for every finite sequence q of elements of $\mathbb{R}$ such that $q = A(i)$ holds $(a \cdot A)(i) = a \cdot q$.

(32) For every matrix A over $\mathbb{R}$ holds $1 \cdot A = A$.

(33) For every matrix A over $\mathbb{R}$ holds $A + A = 2 \cdot A$.

(34) For every matrix A over $\mathbb{R}$ holds $A + A + A = 3 \cdot A$.

Let n, m be natural numbers. The functor $\begin{pmatrix} 0 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 0 \end{pmatrix}_{\mathbb{R}}^{n \times m}$ yields a matrix over $\mathbb{R}$ and is defined by:

(Def. 8) $$\begin{pmatrix} 0 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 0 \end{pmatrix}_{\mathbb{R}}^{n \times m} = (\mathbb{R}_{\mathrm{F}} \to \mathbb{R})(\begin{pmatrix} 0 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 0 \end{pmatrix}_{\mathbb{R}_{\mathrm{F}}}^{n \times m}).$$

One can prove the following propositions:

(35) For all matrices A, B over $\mathbb{R}$ such that $\operatorname{len} B > 0$ holds $A - -B = A + B$.

(36) Let n, m be natural numbers and A be a matrix over $\mathbb{R}$. If $\operatorname{len} A = n$ and $\operatorname{width} A = m$ and $n > 0$, then $A + \begin{pmatrix} 0 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 0 \end{pmatrix}_{\mathbb{R}}^{n \times m} = A$ and $\begin{pmatrix} 0 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 0 \end{pmatrix}_{\mathbb{R}}^{n \times m} + A = A$.

(37) For all matrices A, B over $\mathbb{R}$ such that $\operatorname{len} A = \operatorname{len} B$ and $\operatorname{width} A = \operatorname{width} B$ and $\operatorname{len} A > 0$ and $A = A + B$ holds $B = \begin{pmatrix} 0 & \ldots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \ldots & 0 \end{pmatrix}_{\mathbb{R}}^{\operatorname{len} A \times \operatorname{width} A}$.

(38) For all matrices A, B over $\mathbb{R}$ such that $\operatorname{len} A = \operatorname{len} B$ and $\operatorname{width} A = \operatorname{width} B$ and $\operatorname{len} A > 0$ and $A + B = \begin{pmatrix} 0 & \ldots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \ldots & 0 \end{pmatrix}_{\mathbb{R}}^{\operatorname{len} A \times \operatorname{width} A}$ holds $B = -A$.

(39) For all matrices A, B over $\mathbb{R}$ such that $\operatorname{len} A = \operatorname{len} B$ and $\operatorname{width} A = \operatorname{width} B$ and $\operatorname{len} A > 0$ and $B - A = B$ holds $A = \begin{pmatrix} 0 & \ldots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \ldots & 0 \end{pmatrix}_{\mathbb{R}}^{\operatorname{len} A \times \operatorname{width} A}$.

(40) For every real number a and for all matrices A, B over $\mathbb{R}$ such that $\operatorname{width} A = \operatorname{len} B$ and $\operatorname{len} A > 0$ and $\operatorname{len} B > 0$ holds $A \cdot (a \cdot B) = a \cdot (A \cdot B)$.

(41) Let a be a real number and A, B be matrices over $\mathbb{R}$. If $\operatorname{width} A = \operatorname{len} B$ and $\operatorname{len} A > 0$ and $\operatorname{len} B > 0$ and $\operatorname{width} B > 0$, then $(a \cdot A) \cdot B = a \cdot (A \cdot B)$.

(42) For every matrix M over $\mathbb{R}$ such that $\operatorname{len} M > 0$ holds $M + \begin{pmatrix} 0 & \ldots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \ldots & 0 \end{pmatrix}_{\mathbb{R}}^{\operatorname{len} M \times \operatorname{width} M} = M$.

(43) For every real number a and for all matrices A, B over $\mathbb{R}$ such that $\operatorname{len} A = \operatorname{len} B$ and $\operatorname{width} A = \operatorname{width} B$ and $\operatorname{len} A > 0$ holds $a \cdot (A + B) = a \cdot A + a \cdot B$.

(44) For every matrix A over $\mathbb{R}$ such that $\operatorname{len} A > 0$ holds $0 \cdot A = \begin{pmatrix} 0 & \ldots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \ldots & 0 \end{pmatrix}_{\mathbb{R}}^{\operatorname{len} A \times \operatorname{width} A}$.

Let x be a finite sequence of elements of $\mathbb{R}$. Let us assume that $\operatorname{len} x > 0$. The functor $\operatorname{ColVec2Mx} x$ yields a matrix over $\mathbb{R}$ and is defined as follows:

(Def. 9) $\operatorname{len} \operatorname{ColVec2Mx} x = \operatorname{len} x$ and $\operatorname{width} \operatorname{ColVec2Mx} x = 1$ and for every j such that $j \in \operatorname{dom} x$ holds $(\operatorname{ColVec2Mx} x)(j) = \langle x(j) \rangle$.

The following three propositions are true:

(45) Let x be a finite sequence of elements of $\mathbb{R}$ and M be a matrix over $\mathbb{R}$. If $\operatorname{len} x > 0$, then $M = \operatorname{ColVec2Mx} x$ iff $M_{\square,1} = x$ and $\operatorname{width} M = 1$.

(46) For all finite sequences x_1, x_2 of elements of $\mathbb{R}$ such that $\operatorname{len} x_1 =$

$\operatorname{len} x_2$ and $\operatorname{len} x_1 > 0$ holds $\mathrm{ColVec2Mx}(x_1 + x_2) = \mathrm{ColVec2Mx}\, x_1 + \mathrm{ColVec2Mx}\, x_2$.

(47) For every real number a and for every finite sequence x of elements of $\mathbb{R}$ such that $\operatorname{len} x > 0$ holds $\mathrm{ColVec2Mx}(a \cdot x) = a \cdot \mathrm{ColVec2Mx}\, x$.

Let x be a finite sequence of elements of $\mathbb{R}$. The functor $\mathrm{LineVec2Mx}\, x$ yielding a matrix over $\mathbb{R}$ is defined as follows:

(Def. 10) $\operatorname{width} \mathrm{LineVec2Mx}\, x = \operatorname{len} x$ and $\operatorname{len} \mathrm{LineVec2Mx}\, x = 1$ and for every j such that $j \in \operatorname{dom} x$ holds $(\mathrm{LineVec2Mx}\, x)_{1,j} = x(j)$.

The following propositions are true:

(48) Let x be a finite sequence of elements of $\mathbb{R}$ and M be a matrix over $\mathbb{R}$. Then $M = \mathrm{LineVec2Mx}\, x$ if and only if the following conditions are satisfied:

(i) $\mathrm{Line}(M, 1) = x$, and

(ii) $\operatorname{len} M = 1$.

(49) For every finite sequence x of elements of $\mathbb{R}$ such that $\operatorname{len} x > 0$ holds $(\mathrm{LineVec2Mx}\, x)^{\mathrm{T}} = \mathrm{ColVec2Mx}\, x$ and $(\mathrm{ColVec2Mx}\, x)^{\mathrm{T}} = \mathrm{LineVec2Mx}\, x$.

(50) For all finite sequences x_1, x_2 of elements of $\mathbb{R}$ such that $\operatorname{len} x_1 = \operatorname{len} x_2$ and $\operatorname{len} x_1 > 0$ holds $\mathrm{LineVec2Mx}(x_1 + x_2) = \mathrm{LineVec2Mx}\, x_1 + \mathrm{LineVec2Mx}\, x_2$.

(51) For every real number a and for every finite sequence x of elements of $\mathbb{R}$ holds $\mathrm{LineVec2Mx}(a \cdot x) = a \cdot \mathrm{LineVec2Mx}\, x$.

Let M be a matrix over $\mathbb{R}$ and let x be a finite sequence of elements of $\mathbb{R}$. The functor $M \cdot x$ yields a finite sequence of elements of $\mathbb{R}$ and is defined as follows:

(Def. 11) $M \cdot x = (M \cdot \mathrm{ColVec2Mx}\, x)_{\Box,1}$.

The functor $x \cdot M$ yielding a finite sequence of elements of $\mathbb{R}$ is defined as follows:

(Def. 12) $x \cdot M = \mathrm{Line}(\mathrm{LineVec2Mx}\, x \cdot M, 1)$.

Next we state a number of propositions:

(52) Let x be a finite sequence of elements of $\mathbb{R}$ and A be a matrix over $\mathbb{R}$. If $\operatorname{len} A > 0$ and if $\operatorname{width} A > 0$ and if $\operatorname{len} A = \operatorname{len} x$ or $\operatorname{width}(A^{\mathrm{T}}) = \operatorname{len} x$, then $A^{\mathrm{T}} \cdot x = x \cdot A$.

(53) Let x be a finite sequence of elements of $\mathbb{R}$ and A be a matrix over $\mathbb{R}$. If $\operatorname{len} A > 0$ and if $\operatorname{width} A > 0$ and if $\operatorname{width} A = \operatorname{len} x$ or $\operatorname{len}(A^{\mathrm{T}}) = \operatorname{len} x$, then $A \cdot x = x \cdot A^{\mathrm{T}}$.

(54) Let A, B be matrices over $\mathbb{R}$. Suppose $\operatorname{len} A = \operatorname{len} B$ and $\operatorname{width} A = \operatorname{width} B$. Let i be a natural number. If $1 \leq i$ and $i \leq \operatorname{width} A$, then $(A + B)_{\Box,i} = A_{\Box,i} + B_{\Box,i}$.

(55) Let A, B be matrices over $\mathbb{R}$. Suppose $\operatorname{len} A = \operatorname{len} B$ and $\operatorname{width} A = \operatorname{width} B$. Let i be a natural number. If $1 \leq i$ and $i \leq \operatorname{len} A$, then $\mathrm{Line}(A+$

$B, i) = \mathrm{Line}(A, i) + \mathrm{Line}(B, i)$.

(56) Let a be a real number, M be a matrix over $\mathbb{R}$, and i be a natural number. If $1 \leq i$ and $i \leq \mathrm{width}\, M$, then $(a \cdot M)_{\square, i} = a \cdot M_{\square, i}$.

(57) Let x_1, x_2 be finite sequences of elements of $\mathbb{R}$ and A be a matrix over $\mathbb{R}$. If $\mathrm{len}\, x_1 = \mathrm{len}\, x_2$ and $\mathrm{width}\, A = \mathrm{len}\, x_1$ and $\mathrm{len}\, x_1 > 0$ and $\mathrm{len}\, A > 0$, then $A \cdot (x_1 + x_2) = A \cdot x_1 + A \cdot x_2$.

(58) Let x_1, x_2 be finite sequences of elements of $\mathbb{R}$ and A be a matrix over $\mathbb{R}$. If $\mathrm{len}\, x_1 = \mathrm{len}\, x_2$ and $\mathrm{len}\, A = \mathrm{len}\, x_1$ and $\mathrm{len}\, x_1 > 0$, then $(x_1 + x_2) \cdot A = x_1 \cdot A + x_2 \cdot A$.

(59) Let a be a real number, x be a finite sequence of elements of $\mathbb{R}$, and A be a matrix over $\mathbb{R}$. If $\mathrm{width}\, A = \mathrm{len}\, x$ and $\mathrm{len}\, x > 0$ and $\mathrm{len}\, A > 0$, then $A \cdot (a \cdot x) = a \cdot (A \cdot x)$.

(60) Let a be a real number, x be a finite sequence of elements of $\mathbb{R}$, and A be a matrix over $\mathbb{R}$. If $\mathrm{len}\, A = \mathrm{len}\, x$ and $\mathrm{len}\, x > 0$ and $\mathrm{width}\, A > 0$, then $(a \cdot x) \cdot A = a \cdot (x \cdot A)$.

(61) Let x be a finite sequence of elements of $\mathbb{R}$ and A be a matrix over $\mathbb{R}$. If $\mathrm{width}\, A = \mathrm{len}\, x$ and $\mathrm{len}\, x > 0$ and $\mathrm{len}\, A > 0$, then $\mathrm{len}(A \cdot x) = \mathrm{len}\, A$.

(62) Let x be a finite sequence of elements of $\mathbb{R}$ and A be a matrix over $\mathbb{R}$. If $\mathrm{len}\, A = \mathrm{len}\, x$ and $\mathrm{len}\, x > 0$ and $\mathrm{width}\, A > 0$, then $\mathrm{len}(x \cdot A) = \mathrm{width}\, A$.

(63) Let x be a finite sequence of elements of $\mathbb{R}$ and A, B be matrices over $\mathbb{R}$. If $\mathrm{len}\, A = \mathrm{len}\, B$ and $\mathrm{width}\, A = \mathrm{width}\, B$ and $\mathrm{width}\, A = \mathrm{len}\, x$ and $\mathrm{len}\, A > 0$ and $\mathrm{len}\, x > 0$, then $(A + B) \cdot x = A \cdot x + B \cdot x$.

(64) Let x be a finite sequence of elements of $\mathbb{R}$ and A, B be matrices over $\mathbb{R}$. If $\mathrm{len}\, A = \mathrm{len}\, B$ and $\mathrm{width}\, A = \mathrm{width}\, B$ and $\mathrm{len}\, A = \mathrm{len}\, x$ and $\mathrm{width}\, A > 0$ and $\mathrm{len}\, x > 0$, then $x \cdot (A + B) = x \cdot A + x \cdot B$.

(65) Let n, m be natural numbers and x be a finite sequence of elements of $\mathbb{R}$. If $\mathrm{len}\, x = m$ and $n > 0$ and $m > 0$, then $\begin{pmatrix} 0 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 0 \end{pmatrix}_{\mathbb{R}}^{n \times m} \cdot x = \langle \underbrace{0, \dots, 0}_{n} \rangle$.

(66) Let n, m be natural numbers and x be a finite sequence of elements of $\mathbb{R}$. If $\mathrm{len}\, x = n$ and $n > 0$ and $m > 0$, then $x \cdot \begin{pmatrix} 0 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 0 \end{pmatrix}_{\mathbb{R}}^{n \times m} = \langle \underbrace{0, \dots, 0}_{m} \rangle$.

References

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

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

[3] Czesław Byliński. Binary operations. *Formalized Mathematics*, 1(**1**):175–180, 1990.

[4] Czesław Byliński. Binary operations applied to finite sequences. *Formalized Mathematics*, 1(**4**):643–649, 1990.

[5] Czesław Byliński. Finite sequences and tuples of elements of a non-empty sets. *Formalized Mathematics*, 1(**3**):529–536, 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. The sum and product of finite sequences of real numbers. *Formalized Mathematics*, 1(**4**):661–668, 1990.

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

[10] Katarzyna Jankowska. Matrices. Abelian group of matrices. *Formalized Mathematics*, 2(**4**):475–480, 1991.

[11] Jarosław Kotowicz and Yatsuka Nakamura. Introduction to Go-board – part I. *Formalized Mathematics*, 3(**1**):107–115, 1992.

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

[13] Yatsuka Nakamura and Hiroshi Yamazaki. Calculation of matrices of field elements. Part I. *Formalized Mathematics*, 11(**4**):385–391, 2003.

[14] Library Committee of the Association of Mizar Users. Binary operations on numbers. *To appear in Formalized Mathematics.*

[15] Andrzej Trybulec. Subsets of complex numbers. *To appear in Formalized Mathematics.*

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

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

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

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

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

[21] Katarzyna Zawadzka. The sum and product of finite sequences of elements of a field. *Formalized Mathematics*, 3(**2**):205–211, 1992.

[22] Katarzyna Zawadzka. The product and the determinant of matrices with entries in a field. *Formalized Mathematics*, 4(**1**):1–8, 1993.

Received February 20, 2006

FORMALIZED MATHEMATICS
Volume 14, Number 1, Pages 29–36
University of Białystok, 2006

On the Properties of the Möbius Function

Magdalena Jastrzębska[1]
Institute of Mathematics
University of Białystok
Akademicka 2, 15-267 Białystok, Poland

Adam Grabowski[2]
Institute of Mathematics
University of Białystok
Akademicka 2, 15-267 Białystok, Poland

Summary. We formalized some basic properties of the Möbius function which is defined classically as

$$\mu(n) = \begin{cases} 1, \text{ if } n = 1, \\ 0, \text{ if } p^2 | n \text{ for some prime } p, \\ (-1)^r, \text{ if } n = p_1 p_2 \cdots p_r, \text{ where } p_i \text{ are distinct primes.} \end{cases}$$

as e.g., its multiplicativity. To enable smooth reasoning about the sum of this number-theoretic function, we introduced an underlying many-sorted set indexed by the set of natural numbers. Its elements are just values of the Möbius function.

The second part of the paper is devoted to the notion of the radical of number, i.e. the product of its all prime factors.

The formalization (which is very much like the one developed in Isabelle proof assistant connected with Avigad's formal proof of Prime Number Theorem) was done according to the book [13].

MML identifier: `MOEBIUS1`, version: `7.7.01 4.60.940`

The notation and terminology used here are introduced in the following papers: [26], [31], [12], [6], [3], [4], [1], [24], [2], [19], [18], [29], [32], [8], [9], [5], [17], [16], [28], [33], [22], [23], [11], [14], [20], [10], [15], [27], [25], [7], [30], and [21].

[1]This is a part of the author's MSc thesis.

[2]This work has been partially supported by the KBN grant 4 T11C 039 24 and the FP6 IST grant TYPES No. 510996.

ISSN 1426–2630

1. Preliminaries

The scheme *LambdaNATC* deals with an element $\mathcal{A}$ of $\mathbb{N}$, a set $\mathcal{B}$, and a unary functor $\mathcal{F}$ yielding a set, and states that:

There exists a function f from $\mathbb{N}$ into $\mathcal{B}$ such that $f(0) = \mathcal{A}$ and for every non zero natural number x holds $f(x) = \mathcal{F}(x)$

provided the parameters have the following properties:

- $\mathcal{A} \in \mathcal{B}$, and
- For every non zero natural number x holds $\mathcal{F}(x) \in \mathcal{B}$.

One can check that there exists a natural number which is non prime and non zero.

One can prove the following propositions:

(1) For every non zero natural number n such that $n \neq 1$ holds $n \geq 2$.

(2) For all natural numbers k, n, i such that $1 \leq k$ holds $i \in \mathrm{Seg}\, n$ iff $k \cdot i \in \mathrm{Seg}(k \cdot n)$.

(3) For all natural numbers m, n such that m and n are relative prime holds $m > 0$ or $n > 0$.

(4) For every non prime natural number n such that $n \neq 1$ there exists a prime number p such that $p \mid n$ and $p \neq n$.

(5) For every natural number n such that $n \neq 1$ there exists a prime number p such that $p \mid n$.

(6) For every prime number p and for every non zero natural number n holds $p \mid n$ iff p-count$(n) > 0$.

(7) $\mathrm{support}\, \mathrm{PPF}(1) = \emptyset$.

(8) For every prime number p holds $\mathrm{support}\, \mathrm{PPF}(p) = \{p\}$.

In the sequel m, n are natural numbers.

We now state the proposition

(9) For every prime number p such that $n \neq 0$ and $m \leq p$-count(n) holds $p^m \mid n$.

Let us observe that every natural number which is odd is also non zero.

The following propositions are true:

(10) For every natural number a and for every prime number p such that $p^2 \mid a$ holds $p \mid a$.

(11) Let p be a prime natural number and m, n be non zero natural numbers. If m and n are relative prime and $p^2 \mid m \cdot n$, then $p^2 \mid m$ or $p^2 \mid n$.

(12) For every real bag N over $\mathbb{N}$ such that $\mathrm{support}\, N = \{n\}$ holds $\sum N = N(n)$.

Let us mention that $\mathrm{CFS}(\emptyset)$ is empty.

The following propositions are true:

(13) Let p be a prime number. Suppose $p \mid n$. Then $\{d; d$ ranges over natural numbers: $d > 0 \ \wedge \ d \mid n \ \wedge \ p \mid d\} = \{p \cdot d; d$ ranges over natural numbers: $d > 0 \ \wedge \ d \mid n \div p\}$.

(14) For every non zero natural number n there exists a natural number k such that $\operatorname{support} \mathrm{PPF}(n) \subseteq \operatorname{Seg} k$.

(15) For every non zero natural number n and for every prime number p such that $p \notin \operatorname{support} \mathrm{PPF}(n)$ holds $p\text{-count}(n) = 0$.

(16) Let k be a natural number and n be a non zero natural number. If $\operatorname{support} \mathrm{PPF}(n) \subseteq \operatorname{Seg}(k+1)$ and $\operatorname{support} \mathrm{PPF}(n) \not\subseteq \operatorname{Seg} k$, then $k+1$ is a prime number.

(17) For all non zero natural numbers m, n such that for every prime number p holds $p\text{-count}(m) \leq p\text{-count}(n)$ holds $\operatorname{support} \mathrm{PPF}(m) \subseteq \operatorname{support} \mathrm{PPF}(n)$.

(18) Let k be a natural number and n be a non zero natural number. Suppose $\operatorname{support} \mathrm{PPF}(n) \subseteq \operatorname{Seg}(k+1)$. Then there exists a non zero natural number m and there exists a natural number e such that $\operatorname{support} \mathrm{PPF}(m) \subseteq \operatorname{Seg} k$ and $n = m \cdot (k+1)^e$ and for every prime number p holds if $p \in \operatorname{support} \mathrm{PPF}(m)$, then $p\text{-count}(m) = p\text{-count}(n)$ and if $p \notin \operatorname{support} \mathrm{PPF}(m)$, then $p\text{-count}(m) \leq p\text{-count}(n)$.

(19) For all non zero natural numbers m, n such that for every prime number p holds $p\text{-count}(m) \leq p\text{-count}(n)$ holds $m \mid n$.

2. Squarefree Numbers

Let x be a natural number. We say that x is square-containing if and only if:

(Def. 1) There exists a prime number p such that $p^2 \mid x$.

One can prove the following proposition

(20) Let n be a natural number. Given a non zero natural number p such that $p \neq 1$ and $p^2 \mid n$. Then n is square-containing.

Let x be a natural number. We introduce x is squarefree as an antonym of x is square-containing.

The following propositions are true:

(21) 0 is square-containing.

(22) 1 is squarefree.

(23) Every prime number is squarefree.

Let us observe that every element of $\mathbb{N}$ which is prime is also squarefree.

The subset SCNAT of $\mathbb{N}$ is defined as follows:

(Def. 2) For every natural number n holds $n \in \mathrm{SCNAT}$ iff n is squarefree.

Let us mention that there exists a natural number which is squarefree and there exists a natural number which is square-containing.

One can check that every natural number which is square and non trivial is also square-containing.

We now state several propositions:

(24) If n is squarefree, then for every prime number p holds p-count$(n) \leq 1$.

(25) If $m \cdot n$ is squarefree, then m is squarefree.

(26) If m is squarefree and $n \mid m$, then n is squarefree.

(27) Let p be a prime number and m, d be natural numbers. If m is squarefree and $p \mid m$ and $d \mid m \div p$, then $d \mid m$ and $p \nmid d$.

(28) For every prime number p and for all natural numbers m, d such that $p \mid m$ and $d \mid m$ and $p \nmid d$ holds $d \mid m \div p$.

(29) Let p be a prime number and m be a natural number. Suppose m is squarefree and $p \mid m$. Then $\{d; d$ ranges over natural numbers: $0 < d \wedge d \mid m \wedge p \nmid d\} = \{d; d$ ranges over natural numbers: $0 < d \wedge d \mid m \div p\}$.

3. Möbius Function

Let n be a natural number. The functor $\mu(n)$ yielding a real number is defined by:

(Def. 3)(i) $\mu(n) = 0$ if n is square-containing,

(ii) there exists a non zero natural number n' such that $n' = n$ and $\mu(n) = (-1)^{\mathrm{card\,support\,PPF}(n')}$, otherwise.

One can prove the following four propositions:

(30) $\mu(1) = 1$.

(31) $\mu(2) = -1$.

(32) $\mu(3) = -1$.

(33) For every natural number n such that n is squarefree holds $\mu(n) \neq 0$.

Let n be a squarefree natural number. Observe that $\mu(n)$ is non zero.

We now state several propositions:

(34) For every prime number p holds $\mu(p) = -1$.

(35) For all non zero natural numbers m, n such that m and n are relative prime holds $\mu(m \cdot n) = \mu(m) \cdot \mu(n)$.

(36) For every prime number p and for every natural number n such that $1 \leq n$ and $n \cdot p$ is squarefree holds $\mu(n \cdot p) = -\mu(n)$.

(37) For all non zero natural numbers m, n such that m and n are not relative prime holds $\mu(m \cdot n) = 0$.

(38) For every natural number n holds $n \in \mathrm{SCNAT}$ iff $\mu(n) \neq 0$.

4. Natural Divisors

Let n be a natural number. The functor $\mathrm{NatDivisors}\, n$ yields a subset of $\mathbb{N}$ and is defined by:

(Def. 4) $\mathrm{NatDivisors}\, n = \{k; k$ ranges over elements of $\mathbb{N}$: $k \neq 0 \ \wedge \ k \mid n\}$.

We now state two propositions:

(39) For all natural numbers n, k holds $k \in \mathrm{NatDivisors}\, n$ iff $0 < k$ and $k \mid n$.

(40) For every non zero natural number n holds $\mathrm{NatDivisors}\, n \subseteq \mathrm{Seg}\, n$.

Let n be a non zero natural number. Note that $\mathrm{NatDivisors}\, n$ is finite and has non empty elements.

One can prove the following proposition

(41) $\mathrm{NatDivisors}\, 1 = \{1\}$.

5. The Sum of Values of Möbius Function

Let X be a set. The functor $\mathrm{SMoebius}\, X$ yielding a many sorted set indexed by $\mathbb{N}$ is defined as follows:

(Def. 5) $\mathrm{support}\, \mathrm{SMoebius}\, X = X \cap \mathrm{SCNAT}$ and for every natural number k such that $k \in \mathrm{support}\, \mathrm{SMoebius}\, X$ holds $(\mathrm{SMoebius}\, X)(k) = \mu(k)$.

Let X be a set. One can check that $\mathrm{SMoebius}\, X$ is real-yielding.

Let X be a finite set. Note that $\mathrm{SMoebius}\, X$ is finite-support.

One can prove the following three propositions:

(42) $\sum \mathrm{SMoebius}\, \mathrm{NatDivisors}\, 1 = 1$.

(43) For all finite subsets X, Y of $\mathbb{N}$ such that X misses Y holds $\mathrm{support}\, \mathrm{SMoebius}\, X \cup \mathrm{support}\, \mathrm{SMoebius}\, Y = \mathrm{support}(\mathrm{SMoebius}\, X + \mathrm{SMoebius}\, Y)$.

(44) For all finite subsets X, Y of $\mathbb{N}$ such that X misses Y holds $\mathrm{SMoebius}(X \cup Y) = \mathrm{SMoebius}\, X + \mathrm{SMoebius}\, Y$.

6. Prime Factors of a Number

Let n be a non zero natural number. The functor $\mathrm{PFactors}\, n$ yields a many sorted set indexed by Prime and is defined by:

(Def. 6) $\mathrm{support}\, \mathrm{PFactors}\, n = \mathrm{support}\, \mathrm{PFExp}(n)$ and for every natural number p such that $p \in \mathrm{support}\, \mathrm{PFExp}(n)$ holds $(\mathrm{PFactors}\, n)(p) = p$.

Let n be a non zero natural number. Note that $\mathrm{PFactors}\, n$ is finite-support and natural-yielding.

One can prove the following propositions:

(45) $\mathrm{PFactors}\, 1 = \mathrm{EmptyBag}\, \mathrm{Prime}$.

(46) For every prime number p holds $\mathrm{PFactors}\, p \cdot \langle p \rangle = \langle p \rangle$.

(47) For every prime number p and for every non zero natural number n holds $\mathrm{PFactors}(p^n) \cdot \langle p \rangle = \langle p \rangle$.

(48) For every prime number p and for every non zero natural number n such that $p\text{-count}(n) = 0$ holds $(\mathrm{PFactors}\, n)(p) = 0$.

(49) For every non zero natural number n and for every prime number p such that $p\text{-count}(n) \neq 0$ holds $(\mathrm{PFactors}\, n)(p) = p$.

(50) For all non zero natural numbers m, n such that m and n are relative prime holds $\mathrm{PFactors}(m \cdot n) = \mathrm{PFactors}\, m + \mathrm{PFactors}\, n$.

(51) Let n be a non zero natural number and A be a finite subset of $\mathbb{N}$. Suppose $A = \{k; k$ ranges over elements of $\mathbb{N}$: $0 < k \ \wedge \ k \mid n \ \wedge \ k$ is square-containing$\}$. Then $\mathrm{SMoebius}\, A = \mathrm{EmptyBag}\, \mathbb{N}$.

7. The Radical of a Number

Let n be a non zero natural number. The functor $\mathrm{Rad}(n)$ yields a natural number and is defined as follows:

(Def. 7) $\mathrm{Rad}(n) = \prod \mathrm{PFactors}\, n$.

The following proposition is true

(52) For every non zero natural number n holds $\mathrm{Rad}(n) > 0$.

Let n be a non zero natural number. Observe that $\mathrm{Rad}(n)$ is non zero.

One can prove the following propositions:

(53) For every prime number p holds $p = \mathrm{Rad}(p)$.

(54) For every prime number p and for every non zero natural number n holds $\mathrm{Rad}(p^n) = p$.

(55) For every non zero natural number n holds $\mathrm{Rad}(n) \mid n$.

(56) For every prime number p and for every non zero natural number n holds $p \mid n$ iff $p \mid \mathrm{Rad}(n)$.

(57) For every non zero natural number k such that k is squarefree holds $\mathrm{Rad}(k) = k$.

(58) For every non zero natural number n holds $\mathrm{Rad}(n) \leq n$.

(59) For every prime number p and for every non zero natural number n holds $p\text{-count}(\mathrm{Rad}(n)) \leq p\text{-count}(n)$.

(60) For every non zero natural number n holds $\mathrm{Rad}(n) = 1$ iff $n = 1$.

(61) For every prime number p and for every non zero natural number n holds $p\text{-count}(\mathrm{Rad}(n)) \leq 1$.

Let n be a non zero natural number. Note that $\mathrm{Rad}(n)$ is squarefree.

One can prove the following propositions:

(62) For every non zero natural number n holds $\mathrm{Rad}(\mathrm{Rad}(n)) = \mathrm{Rad}(n)$.

(63) Let n be a non zero natural number and p be a prime number. Then $\{k; k$ ranges over elements of $\mathbb{N}$: $0 < k \ \wedge \ k \mid \mathrm{Rad}(n) \ \wedge \ p \mid k\} \subseteq \mathrm{Seg}\, n$.

(64) Let n be a non zero natural number and p be a prime number. Then $\{k; k$ ranges over elements of $\mathbb{N}$: $0 < k \ \wedge \ k \mid \mathrm{Rad}(n) \ \wedge \ p \nmid k\} \subseteq \mathrm{Seg}\, n$.

(65) For all non zero natural numbers k, n holds $k \mid n$ and k is squarefree iff $k \mid \mathrm{Rad}(n)$.

(66) Let n be a non zero natural number. Then $\{k; k$ ranges over natural numbers: $0 < k \ \wedge \ k \mid n \ \wedge \ k$ is squarefree$\} = \{k; k$ ranges over natural numbers: $0 < k \ \wedge \ k \mid \mathrm{Rad}(n)\}$.

References

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

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

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

[4] Grzegorz Bancerek. Sequences of ordinal numbers. *Formalized Mathematics*, 1(**2**):281–290, 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. Finite sequences and tuples of elements of a non-empty sets. *Formalized Mathematics*, 1(**3**):529–536, 1990.

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

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

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

[11] Czesław Byliński. The sum and product of finite sequences of real numbers. *Formalized Mathematics*, 1(**4**):661–668, 1990.

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

[13] G.H. Hardy and E.M. Wright. *An Introduction to the Theory of Numbers*. Oxford University Press, 1980.

[14] Andrzej Kondracki. The Chinese Remainder Theorem. *Formalized Mathematics*, 6(**4**):573–577, 1997.

[15] Artur Korniłowicz and Piotr Rudnicki. Fundamental Theorem of Arithmetic. *Formalized Mathematics*, 12(**2**):179–186, 2004.

[16] Jarosław Kotowicz. Monotone real sequences. Subsequences. *Formalized Mathematics*, 1(**3**):471–475, 1990.

[17] Jarosław Kotowicz. Real sequences and basic operations on them. *Formalized Mathematics*, 1(**2**):269–272, 1990.

[18] Rafał Kwiatek. Factorial and Newton coefficients. *Formalized Mathematics*, 1(**5**):887–890, 1990.

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

[20] Library Committee of the Association of Mizar Users. Binary operations on numbers. *To appear in Formalized Mathematics*.

[21] Piotr Rudnicki. Little Bezout theorem (factor theorem). *Formalized Mathematics*, 12(**1**):49–58, 2004.

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

[23] Christoph Schwarzweller and Andrzej Trybulec. The evaluation of multivariate polynomials. *Formalized Mathematics*, 9(**2**):331–338, 2001.

[24] Andrzej Trybulec. Subsets of complex numbers. *To appear in Formalized Mathematics.*
[25] Andrzej Trybulec. Domains and their Cartesian products. *Formalized Mathematics*, 1(**1**):115–122, 1990.
[26] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.
[27] Andrzej Trybulec. Tuples, projections and Cartesian products. *Formalized Mathematics*, 1(**1**):97–105, 1990.
[28] Andrzej Trybulec. Many-sorted sets. *Formalized Mathematics*, 4(**1**):15–22, 1993.
[29] Andrzej Trybulec. On the sets inhabited by numbers. *Formalized Mathematics*, 11(**4**):341–347, 2003.
[30] Wojciech A. Trybulec. Pigeon hole principle. *Formalized Mathematics*, 1(**3**):575–579, 1990.
[31] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[32] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.
[33] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.

Received March 21, 2006

FORMALIZED MATHEMATICS
Volume 14, Number 1, Pages 37–45
University of Białystok, 2006

Several Differentiation Formulas of Special Functions. Part III

Bo Li
Qingdao University of Science and Technology
China

Yan Zhang
Qingdao University of Science and Technology
China

Xiquan Liang
Qingdao University of Science and Technology
China

Summary. In this article, we give several differentiation formulas of special and composite functions including trigonometric function, inverse trigonometric function, polynomial function and logarithmic function.

MML identifier: `FDIFF_7`, version: `7.7.01 4.60.940`

The articles [13], [15], [16], [1], [4], [10], [11], [17], [5], [14], [12], [2], [6], [9], [7], [8], and [3] provide the terminology and notation for this paper.

For simplicity, we follow the rules: x, r, a, b denote real numbers, n denotes a natural number, Z denotes an open subset of $\mathbb{R}$, and f, f_1, f_2, f_3 denote partial functions from $\mathbb{R}$ to $\mathbb{R}$.

One can prove the following propositions:

(1) $x_{\mathbb{Z}}^{2} = x^{\mathbf{2}}$.

(2) If $x > 0$, then $x_{\mathbb{R}}^{\frac{1}{2}} = \sqrt{x}$.

(3) If $x > 0$, then $x_{\mathbb{R}}^{-\frac{1}{2}} = \frac{1}{\sqrt{x}}$.

(4) Suppose $Z \subseteq]-1, 1[$ and $Z \subseteq \mathrm{dom}(r\,(\text{the function arcsin}))$. Then

(i) $r\,(\text{the function arcsin})$ is differentiable on Z, and

(ii) for every x such that $x \in Z$ holds $(r\,(\text{the function arcsin}))'_{\restriction Z}(x) = \frac{r}{\sqrt{1-x^{\mathbf{2}}}}$.

ISSN 1426–2630

(5) Suppose $Z \subseteq]-1,1[$ and $Z \subseteq \mathrm{dom}(r\,(\text{the function arccos}))$. Then
(i) $r\,(\text{the function arccos})$ is differentiable on Z, and
(ii) for every x such that $x \in Z$ holds $(r\,(\text{the function arccos}))'_{\restriction Z}(x) = -\frac{r}{\sqrt{1-x^{2}}}$.

(6) Suppose f is differentiable in x and $f(x) > -1$ and $f(x) < 1$. Then (the function arcsin) $\cdot f$ is differentiable in x and $((\text{the function arcsin}) \cdot f)'(x) = \frac{f'(x)}{\sqrt{1-f(x)^{2}}}$.

(7) Suppose f is differentiable in x and $f(x) > -1$ and $f(x) < 1$. Then (the function arccos) $\cdot f$ is differentiable in x and $((\text{the function arccos}) \cdot f)'(x) = -\frac{f'(x)}{\sqrt{1-f(x)^{2}}}$.

(8) Suppose $Z \subseteq \mathrm{dom}(\log\_(e) \cdot (\text{the function arcsin}))$ and $Z \subseteq]-1,1[$ and for every x such that $x \in Z$ holds $(\text{the function arcsin})(x) > 0$. Then
(i) $\log\_(e) \cdot (\text{the function arcsin})$ is differentiable on Z, and
(ii) for every x such that $x \in Z$ holds $(\log\_(e) \cdot (\text{the function arcsin}))'_{\restriction Z}(x) = \frac{1}{\sqrt{1-x^{2}} \cdot (\text{the function arcsin})(x)}$.

(9) Suppose $Z \subseteq \mathrm{dom}(\log\_(e) \cdot (\text{the function arccos}))$ and $Z \subseteq]-1,1[$ and for every x such that $x \in Z$ holds $(\text{the function arccos})(x) > 0$. Then
(i) $\log\_(e) \cdot (\text{the function arccos})$ is differentiable on Z, and
(ii) for every x such that $x \in Z$ holds $(\log\_(e) \cdot (\text{the function arccos}))'_{\restriction Z}(x) = -\frac{1}{\sqrt{1-x^{2}} \cdot (\text{the function arccos})(x)}$.

(10) Suppose $Z \subseteq \mathrm{dom}((\binom{n}{\mathbb{Z}}) \cdot (\text{the function arcsin}))$ and $Z \subseteq]-1,1[$. Then
(i) $(\binom{n}{\mathbb{Z}}) \cdot (\text{the function arcsin})$ is differentiable on Z, and
(ii) for every x such that $x \in Z$ holds $((\binom{n}{\mathbb{Z}}) \cdot (\text{the function arcsin}))'_{\restriction Z}(x) = \frac{n \cdot (\text{the function arcsin})(x)^{n-1}_{\mathbb{Z}}}{\sqrt{1-x^{2}}}$.

(11) Suppose $Z \subseteq \mathrm{dom}((\binom{n}{\mathbb{Z}}) \cdot (\text{the function arccos}))$ and $Z \subseteq]-1,1[$. Then
(i) $(\binom{n}{\mathbb{Z}}) \cdot (\text{the function arccos})$ is differentiable on Z, and
(ii) for every x such that $x \in Z$ holds $((\binom{n}{\mathbb{Z}}) \cdot (\text{the function arccos}))'_{\restriction Z}(x) = -\frac{n \cdot (\text{the function arccos})(x)^{n-1}_{\mathbb{Z}}}{\sqrt{1-x^{2}}}$.

(12) Suppose $Z \subseteq \mathrm{dom}(\frac{1}{2}\,((\binom{2}{\mathbb{Z}}) \cdot (\text{the function arcsin})))$ and $Z \subseteq]-1,1[$. Then
(i) $\frac{1}{2}\,((\binom{2}{\mathbb{Z}}) \cdot (\text{the function arcsin}))$ is differentiable on Z, and
(ii) for every x such that $x \in Z$ holds $(\frac{1}{2}\,((\binom{2}{\mathbb{Z}}) \cdot (\text{the function arcsin})))'_{\restriction Z}(x) = \frac{(\text{the function arcsin})(x)}{\sqrt{1-x^{2}}}$.

(13) Suppose $Z \subseteq \mathrm{dom}(\frac{1}{2}\,((\binom{2}{\mathbb{Z}}) \cdot (\text{the function arccos})))$ and $Z \subseteq]-1,1[$. Then
(i) $\frac{1}{2}\,((\binom{2}{\mathbb{Z}}) \cdot (\text{the function arccos}))$ is differentiable on Z, and
(ii) for every x such that $x \in Z$ holds $(\frac{1}{2}\,((\binom{2}{\mathbb{Z}}) \cdot (\text{the function arccos})))'_{\restriction Z}(x) = -\frac{(\text{the function arccos})(x)}{\sqrt{1-x^{2}}}$.

(14) Suppose $Z \subseteq \mathrm{dom}((\text{the function arcsin}) \cdot f)$ and for every x such that $x \in Z$ holds $f(x) = a \cdot x + b$ and $f(x) > -1$ and $f(x) < 1$. Then
  (i) (the function arcsin) $\cdot f$ is differentiable on Z, and
  (ii) for every x such that $x \in Z$ holds $((\text{the function arcsin}) \cdot f)'_{\restriction Z}(x) = \frac{a}{\sqrt{1-(a \cdot x+b)^{\mathbf{2}}}}$.

(15) Suppose $Z \subseteq \mathrm{dom}((\text{the function arccos}) \cdot f)$ and for every x such that $x \in Z$ holds $f(x) = a \cdot x + b$ and $f(x) > -1$ and $f(x) < 1$. Then
  (i) (the function arccos) $\cdot f$ is differentiable on Z, and
  (ii) for every x such that $x \in Z$ holds $((\text{the function arccos}) \cdot f)'_{\restriction Z}(x) = -\frac{a}{\sqrt{1-(a \cdot x+b)^{\mathbf{2}}}}$.

(16) Suppose $Z \subseteq \mathrm{dom}(\mathrm{id}_Z\,(\text{the function arcsin}))$ and $Z \subseteq\,]-1, 1[$. Then
  (i) id_Z (the function arcsin) is differentiable on Z, and
  (ii) for every x such that $x \in Z$ holds $(\mathrm{id}_Z\,(\text{the function arcsin}))'_{\restriction Z}(x) = (\text{the function arcsin})(x) + \frac{x}{\sqrt{1-x^{\mathbf{2}}}}$.

(17) Suppose $Z \subseteq \mathrm{dom}(\mathrm{id}_Z\,(\text{the function arccos}))$ and $Z \subseteq\,]-1, 1[$. Then
  (i) id_Z (the function arccos) is differentiable on Z, and
  (ii) for every x such that $x \in Z$ holds $(\mathrm{id}_Z\,(\text{the function arccos}))'_{\restriction Z}(x) = (\text{the function arccos})(x) - \frac{x}{\sqrt{1-x^{\mathbf{2}}}}$.

(18) Suppose $Z \subseteq \mathrm{dom}(f\,(\text{the function arcsin}))$ and $Z \subseteq\,]-1, 1[$ and for every x such that $x \in Z$ holds $f(x) = a \cdot x + b$. Then
  (i) f (the function arcsin) is differentiable on Z, and
  (ii) for every x such that $x \in Z$ holds $(f\,(\text{the function arcsin}))'_{\restriction Z}(x) = a \cdot (\text{the function arcsin})(x) + \frac{a \cdot x+b}{\sqrt{1-x^{\mathbf{2}}}}$.

(19) Suppose $Z \subseteq \mathrm{dom}(f\,(\text{the function arccos}))$ and $Z \subseteq\,]-1, 1[$ and for every x such that $x \in Z$ holds $f(x) = a \cdot x + b$. Then
  (i) f (the function arccos) is differentiable on Z, and
  (ii) for every x such that $x \in Z$ holds $(f\,(\text{the function arccos}))'_{\restriction Z}(x) = a \cdot (\text{the function arccos})(x) - \frac{a \cdot x+b}{\sqrt{1-x^{\mathbf{2}}}}$.

(20) Suppose $Z \subseteq \mathrm{dom}(\frac{1}{2}\,((\text{the function arcsin}) \cdot f))$ and for every x such that $x \in Z$ holds $f(x) = 2 \cdot x$ and $f(x) > -1$ and $f(x) < 1$. Then
  (i) $\frac{1}{2}\,((\text{the function arcsin}) \cdot f)$ is differentiable on Z, and
  (ii) for every x such that $x \in Z$ holds $(\frac{1}{2}\,((\text{the function arcsin}) \cdot f))'_{\restriction Z}(x) = \frac{1}{\sqrt{1-(2 \cdot x)^{\mathbf{2}}}}$.

(21) Suppose $Z \subseteq \mathrm{dom}(\frac{1}{2}\,((\text{the function arccos}) \cdot f))$ and for every x such that $x \in Z$ holds $f(x) = 2 \cdot x$ and $f(x) > -1$ and $f(x) < 1$. Then
  (i) $\frac{1}{2}\,((\text{the function arccos}) \cdot f)$ is differentiable on Z, and
  (ii) for every x such that $x \in Z$ holds $(\frac{1}{2}\,((\text{the function arccos}) \cdot f))'_{\restriction Z}(x) = -\frac{1}{\sqrt{1-(2 \cdot x)^{\mathbf{2}}}}$.

(22) Suppose $Z \subseteq \mathrm{dom}((\frac{1}{\mathbb{R}}^{\frac{1}{2}}) \cdot f)$ and $f = f_1 - f_2$ and $f_2 = \frac{2}{\mathbb{Z}}$ and for every x such that $x \in Z$ holds $f_1(x) = 1$ and $f(x) > 0$. Then $(\frac{1}{\mathbb{R}}^{\frac{1}{2}}) \cdot f$ is differentiable on Z and for every x such that $x \in Z$ holds $((\frac{1}{\mathbb{R}}^{\frac{1}{2}}) \cdot f)'_{\restriction Z}(x) = -x \cdot (1 - x^{2}_{\mathbb{Z}})_{\mathbb{R}}^{-\frac{1}{2}}$.

(23) Suppose that
 (i) $Z \subseteq \mathrm{dom}(\mathrm{id}_Z\,(\text{the function arcsin}) + (\frac{1}{\mathbb{R}}^{\frac{1}{2}}) \cdot f)$,
 (ii) $Z \subseteq]-1, 1[$,
 (iii) $f = f_1 - f_2$,
 (iv) $f_2 = \frac{2}{\mathbb{Z}}$, and
 (v) for every x such that $x \in Z$ holds $f_1(x) = 1$ and $f(x) > 0$ and $x \neq 0$.
Then
 (vi) $\mathrm{id}_Z\,(\text{the function arcsin}) + (\frac{1}{\mathbb{R}}^{\frac{1}{2}}) \cdot f$ is differentiable on Z, and
 (vii) for every x such that $x \in Z$ holds $(\mathrm{id}_Z\,(\text{the function arcsin}) + (\frac{1}{\mathbb{R}}^{\frac{1}{2}}) \cdot f)'_{\restriction Z}(x) = (\text{the function arcsin})(x)$.

(24) Suppose that
 (i) $Z \subseteq \mathrm{dom}(\mathrm{id}_Z\,(\text{the function arccos}) - (\frac{1}{\mathbb{R}}^{\frac{1}{2}}) \cdot f)$,
 (ii) $Z \subseteq]-1, 1[$,
 (iii) $f = f_1 - f_2$,
 (iv) $f_2 = \frac{2}{\mathbb{Z}}$, and
 (v) for every x such that $x \in Z$ holds $f_1(x) = 1$ and $f(x) > 0$ and $x \neq 0$.
Then
 (vi) $\mathrm{id}_Z\,(\text{the function arccos}) - (\frac{1}{\mathbb{R}}^{\frac{1}{2}}) \cdot f$ is differentiable on Z, and
 (vii) for every x such that $x \in Z$ holds $(\mathrm{id}_Z\,(\text{the function arccos}) - (\frac{1}{\mathbb{R}}^{\frac{1}{2}}) \cdot f)'_{\restriction Z}(x) = (\text{the function arccos})(x)$.

(25) Suppose $Z \subseteq \mathrm{dom}(\mathrm{id}_Z\,((\text{the function arcsin}) \cdot f))$ and for every x such that $x \in Z$ holds $f(x) = \frac{x}{a}$ and $f(x) > -1$ and $f(x) < 1$. Then
 (i) $\mathrm{id}_Z\,((\text{the function arcsin}) \cdot f)$ is differentiable on Z, and
 (ii) for every x such that $x \in Z$ holds $(\mathrm{id}_Z\,((\text{the function arcsin}) \cdot f))'_{\restriction Z}(x) = (\text{the function arcsin})(\frac{x}{a}) + \frac{x}{a \cdot \sqrt{1 - (\frac{x}{a})^{\mathbf{2}}}}$.

(26) Suppose $Z \subseteq \mathrm{dom}(\mathrm{id}_Z\,((\text{the function arccos}) \cdot f))$ and for every x such that $x \in Z$ holds $f(x) = \frac{x}{a}$ and $f(x) > -1$ and $f(x) < 1$. Then
 (i) $\mathrm{id}_Z\,((\text{the function arccos}) \cdot f)$ is differentiable on Z, and
 (ii) for every x such that $x \in Z$ holds $(\mathrm{id}_Z\,((\text{the function arccos}) \cdot f))'_{\restriction Z}(x) = (\text{the function arccos})(\frac{x}{a}) - \frac{x}{a \cdot \sqrt{1 - (\frac{x}{a})^{\mathbf{2}}}}$.

(27) Suppose $Z \subseteq \mathrm{dom}((\frac{1}{\mathbb{R}}^{\frac{1}{2}}) \cdot f)$ and $f = f_1 - f_2$ and $f_2 = \frac{2}{\mathbb{Z}}$ and for every x such that $x \in Z$ holds $f_1(x) = a^{\mathbf{2}}$ and $f(x) > 0$. Then $(\frac{1}{\mathbb{R}}^{\frac{1}{2}}) \cdot f$ is differentiable on Z and for every x such that $x \in Z$ holds $((\frac{1}{\mathbb{R}}^{\frac{1}{2}}) \cdot f)'_{\restriction Z}(x) = -x \cdot (a^{\mathbf{2}} - x^{2}_{\mathbb{Z}})_{\mathbb{R}}^{-\frac{1}{2}}$.

(28) Suppose that

(i) $Z \subseteq \mathrm{dom}(\mathrm{id}_Z\,((\text{the function arcsin}) \cdot f_3) + (\frac{1}{2}_{\mathbb{R}}) \cdot f)$,
(ii) $Z \subseteq\,]-1, 1[$,
(iii) $f = f_1 - f_2$,
(iv) $f_2 = \frac{2}{\mathbb{Z}}$, and
(v) for every x such that $x \in Z$ holds $f_1(x) = a^{\mathbf{2}}$ and $f(x) > 0$ and $f_3(x) = \frac{x}{a}$ and $f_3(x) > -1$ and $f_3(x) < 1$ and $x \neq 0$ and $a > 0$.
Then
(vi) $\mathrm{id}_Z\,((\text{the function arcsin}) \cdot f_3) + (\frac{1}{2}_{\mathbb{R}}) \cdot f$ is differentiable on Z, and
(vii) for every x such that $x \in Z$ holds $(\mathrm{id}_Z\,((\text{the function arcsin}) \cdot f_3) + (\frac{1}{2}_{\mathbb{R}}) \cdot f)'_{\restriction Z}(x) = (\text{the function arcsin})(\frac{x}{a})$.

(29) Suppose that
(i) $Z \subseteq \mathrm{dom}(\mathrm{id}_Z\,((\text{the function arccos}) \cdot f_3) - (\frac{1}{2}_{\mathbb{R}}) \cdot f)$,
(ii) $Z \subseteq\,]-1, 1[$,
(iii) $f = f_1 - f_2$,
(iv) $f_2 = \frac{2}{\mathbb{Z}}$, and
(v) for every x such that $x \in Z$ holds $f_1(x) = a^{\mathbf{2}}$ and $f(x) > 0$ and $f_3(x) = \frac{x}{a}$ and $f_3(x) > -1$ and $f_3(x) < 1$ and $x \neq 0$ and $a > 0$.
Then
(vi) $\mathrm{id}_Z\,((\text{the function arccos}) \cdot f_3) - (\frac{1}{2}_{\mathbb{R}}) \cdot f$ is differentiable on Z, and
(vii) for every x such that $x \in Z$ holds $(\mathrm{id}_Z\,((\text{the function arccos}) \cdot f_3) - (\frac{1}{2}_{\mathbb{R}}) \cdot f)'_{\restriction Z}(x) = (\text{the function arccos})(\frac{x}{a})$.

(30) Suppose $Z \subseteq \mathrm{dom}((-\frac{1}{n})\,((\frac{n}{\mathbb{Z}}) \cdot \frac{1}{\text{the function sin}}))$ and $n > 0$ and for every x such that $x \in Z$ holds $(\text{the function sin})(x) \neq 0$. Then
(i) $(-\frac{1}{n})\,((\frac{n}{\mathbb{Z}}) \cdot \frac{1}{\text{the function sin}})$ is differentiable on Z, and
(ii) for every x such that $x \in Z$ holds $((-\frac{1}{n})\,((\frac{n}{\mathbb{Z}}) \cdot \frac{1}{\text{the function sin}}))'_{\restriction Z}(x) = \frac{(\text{the function cos})(x)}{(\text{the function sin})(x)^{n+1}_{\mathbb{Z}}}$.

(31) Suppose $Z \subseteq \mathrm{dom}(\frac{1}{n}\,((\frac{n}{\mathbb{Z}}) \cdot \frac{1}{\text{the function cos}}))$ and $n > 0$ and for every x such that $x \in Z$ holds $(\text{the function cos})(x) \neq 0$. Then
(i) $\frac{1}{n}\,((\frac{n}{\mathbb{Z}}) \cdot \frac{1}{\text{the function cos}})$ is differentiable on Z, and
(ii) for every x such that $x \in Z$ holds $(\frac{1}{n}\,((\frac{n}{\mathbb{Z}}) \cdot \frac{1}{\text{the function cos}}))'_{\restriction Z}(x) = \frac{(\text{the function sin})(x)}{(\text{the function cos})(x)^{n+1}_{\mathbb{Z}}}$.

(32) Suppose $Z \subseteq \mathrm{dom}((\text{the function sin}) \cdot \log\_(e))$ and for every x such that $x \in Z$ holds $x > 0$. Then
(i) $(\text{the function sin}) \cdot \log\_(e)$ is differentiable on Z, and
(ii) for every x such that $x \in Z$ holds $((\text{the function sin}) \cdot \log\_(e))'_{\restriction Z}(x) = \frac{(\text{the function cos})((\log\_(e))(x))}{x}$.

(33) Suppose $Z \subseteq \mathrm{dom}((\text{the function cos}) \cdot \log\_(e))$ and for every x such that $x \in Z$ holds $x > 0$. Then

(i) (the function cos) $\cdot$log_(e) is differentiable on Z, and

(ii) for every x such that $x \in Z$ holds ((the function cos) $\cdot$log_$(e))'_{\restriction Z}(x) = -\frac{\text{(the function sin)((log_}(e))(x))}{x}$.

(34) Suppose $Z \subseteq$ dom((the function sin) $\cdot$(the function exp)). Then

(i) (the function sin) $\cdot$(the function exp) is differentiable on Z, and

(ii) for every x such that $x \in Z$ holds ((the function sin) $\cdot$(the function exp))$'_{\restriction Z}(x)$ = (the function exp)(x) $\cdot$ (the function cos)((the function exp)(x)).

(35) Suppose $Z \subseteq$ dom((the function cos) $\cdot$(the function exp)). Then

(i) (the function cos) $\cdot$(the function exp) is differentiable on Z, and

(ii) for every x such that $x \in Z$ holds ((the function cos) $\cdot$(the function exp))$'_{\restriction Z}(x) =$
$-$(the function exp)(x) $\cdot$ (the function sin)((the function exp)(x)).

(36) Suppose $Z \subseteq$ dom((the function exp) $\cdot$(the function cos)). Then

(i) (the function exp) $\cdot$(the function cos) is differentiable on Z, and

(ii) for every x such that $x \in Z$ holds ((the function exp) $\cdot$(the function cos))$'_{\restriction Z}(x) =$
$-$(the function exp)((the function cos)(x)) $\cdot$ (the function sin)(x).

(37) Suppose $Z \subseteq$ dom((the function exp) $\cdot$(the function sin)). Then

(i) (the function exp) $\cdot$(the function sin) is differentiable on Z, and

(ii) for every x such that $x \in Z$ holds ((the function exp) $\cdot$(the function sin))$'_{\restriction Z}(x)$ = (the function exp)((the function sin)(x)) $\cdot$ (the function cos)(x).

(38) Suppose $Z \subseteq$ dom((the function sin)+(the function cos)). Then

(i) (the function sin)+(the function cos) is differentiable on Z, and

(ii) for every x such that $x \in Z$ holds ((the function sin)+(the function cos))$'_{\restriction Z}(x)$ = (the function cos)(x) $-$ (the function sin)(x).

(39) Suppose $Z \subseteq$ dom((the function sin)$-$(the function cos)). Then

(i) (the function sin)$-$(the function cos) is differentiable on Z, and

(ii) for every x such that $x \in Z$ holds ((the function sin)$-$(the function cos))$'_{\restriction Z}(x)$ = (the function cos)(x) + (the function sin)(x).

(40) Suppose $Z \subseteq$ dom((the function exp) ((the function sin)$-$(the function cos))). Then

(i) (the function exp) ((the function sin)$-$(the function cos)) is differentiable on Z, and

(ii) for every x such that $x \in Z$ holds ((the function exp) ((the function sin)$-$(the function cos)))$'_{\restriction Z}(x)$ = $2 \cdot$ (the function exp)(x) $\cdot$ (the function sin)(x).

(41) Suppose $Z \subseteq$ dom((the function exp) ((the function sin)+(the function cos))). Then

(i) (the function exp) ((the function sin)+(the function cos)) is differentiable on Z, and

(ii) for every x such that $x \in Z$ holds ((the function exp) ((the function sin)+(the function cos)))$'_{\restriction Z}(x) = 2 \cdot$ (the function exp)$(x) \cdot$ (the function cos)(x).

(42) Suppose $Z \subseteq \mathrm{dom}(\frac{\text{(the function sin)+(the function cos)}}{\text{the function exp}})$. Then

(i) $\frac{\text{(the function sin)+(the function cos)}}{\text{the function exp}}$ is differentiable on Z, and

(ii) for every x such that $x \in Z$ holds $(\frac{\text{(the function sin)+(the function cos)}}{\text{the function exp}})'_{\restriction Z}(x) = -\frac{2\cdot\text{(the function sin)}(x)}{\text{(the function exp)}(x)}$.

(43) Suppose $Z \subseteq \mathrm{dom}(\frac{\text{(the function sin)}-\text{(the function cos)}}{\text{the function exp}})$. Then

(i) $\frac{\text{(the function sin)}-\text{(the function cos)}}{\text{the function exp}}$ is differentiable on Z, and

(ii) for every x such that $x \in Z$ holds $(\frac{\text{(the function sin)}-\text{(the function cos)}}{\text{the function exp}})'_{\restriction Z}(x) = \frac{2\cdot\text{(the function cos)}(x)}{\text{(the function exp)}(x)}$.

(44) Suppose $Z \subseteq$ dom((the function exp) (the function sin)). Then

(i) (the function exp) (the function sin) is differentiable on Z, and

(ii) for every x such that $x \in Z$ holds ((the function exp) (the function sin))$'_{\restriction Z}(x) =$ (the function exp)$(x) \cdot$ ((the function sin)(x) + (the function cos)(x)).

(45) Suppose $Z \subseteq$ dom((the function exp) (the function cos)). Then

(i) (the function exp) (the function cos) is differentiable on Z, and

(ii) for every x such that $x \in Z$ holds ((the function exp) (the function cos))$'_{\restriction Z}(x) =$ (the function exp)$(x) \cdot$ ((the function cos)(x) − (the function sin)(x)).

(46) Suppose (the function cos)$(x) \neq 0$. Then

(i) $\frac{\text{the function sin}}{\text{the function cos}}$ is differentiable in x, and

(ii) $(\frac{\text{the function sin}}{\text{the function cos}})'(x) = \frac{1}{\text{(the function cos)}(x)^{\mathbf{2}}}$.

(47) Suppose (the function sin)$(x) \neq 0$. Then

(i) $\frac{\text{the function cos}}{\text{the function sin}}$ is differentiable in x, and

(ii) $(\frac{\text{the function cos}}{\text{the function sin}})'(x) = -\frac{1}{\text{(the function sin)}(x)^{\mathbf{2}}}$.

(48) Suppose $Z \subseteq \mathrm{dom}((\frac{2}{\mathbb{Z}}) \cdot \frac{\text{the function sin}}{\text{the function cos}})$ and for every x such that $x \in Z$ holds (the function cos)$(x) \neq 0$. Then

(i) $(\frac{2}{\mathbb{Z}}) \cdot \frac{\text{the function sin}}{\text{the function cos}}$ is differentiable on Z, and

(ii) for every x such that $x \in Z$ holds $((\frac{2}{\mathbb{Z}}) \cdot \frac{\text{the function sin}}{\text{the function cos}})'_{\restriction Z}(x) = \frac{2\cdot\text{(the function sin)}(x)}{\text{(the function cos)}(x)^{3}_{\mathbb{Z}}}$.

(49) Suppose $Z \subseteq \mathrm{dom}((\frac{2}{\mathbb{Z}}) \cdot \frac{\text{the function cos}}{\text{the function sin}})$ and for every x such that $x \in Z$ holds (the function sin)$(x) \neq 0$. Then

(i) $(\frac{2}{\mathbb{Z}}) \cdot \frac{\text{the function cos}}{\text{the function sin}}$ is differentiable on Z, and

(ii) for every x such that $x \in Z$ holds $((\frac{2}{\mathbb{Z}}) \cdot \frac{\text{the function cos}}{\text{the function sin}})'_{\restriction Z}(x) = -\frac{2 \cdot (\text{the function cos})(x)}{(\text{the function sin})(x)^{3}_{\mathbb{Z}}}$.

(50) Suppose that

(i) $Z \subseteq \mathrm{dom}(\frac{\text{the function sin}}{\text{the function cos}} \cdot f)$, and

(ii) for every x such that $x \in Z$ holds $f(x) = \frac{x}{2}$ and (the function cos)$(f(x)) \neq 0$.

Then

(iii) $\frac{\text{the function sin}}{\text{the function cos}} \cdot f$ is differentiable on Z, and

(iv) for every x such that $x \in Z$ holds $(\frac{\text{the function sin}}{\text{the function cos}} \cdot f)'_{\restriction Z}(x) = \frac{1}{1+(\text{the function cos})(x)}$.

(51) Suppose that

(i) $Z \subseteq \mathrm{dom}(\frac{\text{the function cos}}{\text{the function sin}} \cdot f)$, and

(ii) for every x such that $x \in Z$ holds $f(x) = \frac{x}{2}$ and (the function sin)$(f(x)) \neq 0$.

Then

(iii) $\frac{\text{the function cos}}{\text{the function sin}} \cdot f$ is differentiable on Z, and

(iv) for every x such that $x \in Z$ holds $(\frac{\text{the function cos}}{\text{the function sin}} \cdot f)'_{\restriction Z}(x) = -\frac{1}{1-(\text{the function cos})(x)}$.

References

[1] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.
[2] Krzysztof Hryniewiecki. Basic properties of real numbers. *Formalized Mathematics*, 1(**1**):35–40, 1990.
[3] Artur Korniłowicz and Yasunari Shidama. Inverse trigonometric functions arcsin and arccos. *Formalized Mathematics*, 13(**1**):73–79, 2005.
[4] Jarosław Kotowicz. Partial functions from a domain to a domain. *Formalized Mathematics*, 1(**4**):697–702, 1990.
[5] Jarosław Kotowicz. Partial functions from a domain to the set of real numbers. *Formalized Mathematics*, 1(**4**):703–709, 1990.
[6] Jarosław Kotowicz. Real sequences and basic operations on them. *Formalized Mathematics*, 1(**2**):269–272, 1990.
[7] Konrad Raczkowski. Integer and rational exponents. *Formalized Mathematics*, 2(**1**):125–130, 1991.
[8] Konrad Raczkowski and Andrzej Nędzusiak. Real exponents and logarithms. *Formalized Mathematics*, 2(**2**):213–216, 1991.
[9] Konrad Raczkowski and Paweł Sadowski. Real function differentiability. *Formalized Mathematics*, 1(**4**):797–801, 1990.
[10] Konrad Raczkowski and Paweł Sadowski. Topological properties of subsets in real numbers. *Formalized Mathematics*, 1(**4**):777–780, 1990.
[11] Yasunari Shidama. The Taylor expansions. *Formalized Mathematics*, 12(**2**):195–200, 2004.
[12] Andrzej Trybulec. Subsets of complex numbers. *To appear in Formalized Mathematics.*
[13] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.
[14] Andrzej Trybulec and Czesław Byliński. Some properties of real numbers. *Formalized Mathematics*, 1(**3**):445–449, 1990.
[15] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[16] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.

[17] Yuguang Yang and Yasunari Shidama. Trigonometric functions and existence of circle ratio. *Formalized Mathematics*, 7(**2**):255–263, 1998.

Received March 22, 2006

Contents

Formaliz. Math. 14 (**1**)

Continued on inside back cover