# Contents

*Formaliz. Math.* 25 (**2**)

FORMALIZED MATHEMATICS
Vol. 25, No. 2, Pages 87–92, 2017
DOI: 10.1515/forma-2017-0008

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

# Vieta's Formula about the Sum of Roots of Polynomials

Artur Korniłowicz
Institute of Informatics
University of Białystok
Poland

Karol Pąk
Institute of Informatics
University of Białystok
Poland

**Summary.** In the article we formalized in the Mizar system [2] the Vieta formula about the sum of roots of a polynomial $a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ defined over an algebraically closed field. The formula says that $x_1 + x_2 + \cdots + x_{n-1} + x_n = -\frac{a_{n-1}}{a_n}$, where $x_1, x_2, \ldots, x_n$ are (not necessarily distinct) roots of the polynomial [12]. In the article the sum is denoted by `SumRoots`.

MSC: 12E05 03B35

Keywords: roots of polynomials; Vieta's formula

MML identifier: `POLYVIE1`, version: `8.1.06 5.43.1297`

Let $F$ be a finite sequence and $f$ be a function from $\operatorname{dom} F$ into $\operatorname{dom} F$. Observe that $F \cdot f$ is finite sequence-like.

Now we state the propositions:

(1) Let us consider objects $a$, $b$. Suppose $a \neq b$. Then

(i) $\mathrm{CFS}(\{a, b\}) = \langle a, b \rangle$, or

(ii) $\mathrm{CFS}(\{a, b\}) = \langle b, a \rangle$.

(2) Let us consider a finite set $X$. Then $\mathrm{CFS}(X)$ is an enumeration of $X$.

Let $A$ be a set and $X$ be a finite subset of $A$. Observe that $\mathrm{CFS}(X)$ is $A$-valued.

Now we state the proposition:

(3) Let us consider a right zeroed, non empty additive loop structure $L$, and an element $a$ of $L$. Then $2 \cdot a = a + a$.




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

Let $L$ be an almost left invertible multiplicative loop with zero structure. Let us note that every element of $L$ which is non zero is also left invertible.

Let $L$ be an almost right invertible multiplicative loop with zero structure. Observe that every element of $L$ which is non zero is also right invertible.

Let $L$ be an almost left cancelable multiplicative loop with zero structure. Let us observe that every element of $L$ which is non zero is also left mult-cancelable.

Let $L$ be an almost right cancelable multiplicative loop with zero structure. One can verify that every element of $L$ which is non zero is also right mult-cancelable.

Now we state the proposition:

(4) Let us consider a right unital, associative, non trivial double loop structure $L$, and elements $a$, $b$ of $L$. Suppose $b$ is left invertible and right mult-cancelable and $b \cdot \frac{1}{b} = \frac{1}{b} \cdot b$. Then $\frac{a \cdot b}{b} = a$.

Let $L$ be a non degenerated zero-one structure, $z_0$ be an element of $L$, and $z_1$ be a non zero element of $L$. Note that $\langle z_0, z_1 \rangle$ is non-zero and $\langle z_1, z_0 \rangle$ is non-zero.

Let us consider a non trivial zero structure $L$ and a polynomial $p$ over $L$. Now we state the propositions:

(5) If $\operatorname{len} p = 1$, then there exists a non zero element $a$ of $L$ such that $p = \langle a \rangle$.

(6) If $\operatorname{len} p = 2$, then there exists an element $a$ of $L$ and there exists a non zero element $b$ of $L$ such that $p = \langle a, b \rangle$.

(7) If $\operatorname{len} p = 3$, then there exist elements $a$, $b$ of $L$ and there exists a non zero element $c$ of $L$ such that $p = \langle a, b, c \rangle$.

Now we state the propositions:

(8) Let us consider an add-associative, right zeroed, right complementable, associative, commutative, left distributive, well unital, almost left invertible, non empty double loop structure $L$, and elements $a$, $b$, $x$ of $L$. If $b \neq 0_L$, then $\operatorname{eval}(\langle a, b \rangle, -\frac{a}{b}) = 0_L$.

(9) Let us consider a field $L$, elements $a$, $x$ of $L$, and a non zero element $b$ of $L$. Then $x$ is a root of $\langle a, b \rangle$ if and only if $x = -\frac{a}{b}$. The theorem is a consequence of (4) and (8).

Let us consider a field $L$, an element $a$ of $L$, and a non zero element $b$ of $L$. Now we state the propositions:

(10) $\operatorname{Roots}(\langle a, b \rangle) = \{-\frac{a}{b}\}$. The theorem is a consequence of (9).

(11) $\operatorname{multiplicity}(\langle a, b \rangle, -\frac{a}{b}) = 1$. The theorem is a consequence of (9).

(12) $\operatorname{BRoots}(\langle a, b \rangle) = (\{-\frac{a}{b}\}, 1)$-bag. The theorem is a consequence of (10) and (11).

(13) Let us consider a field $L$, elements $a$, $c$ of $L$, and non zero elements $b$, $d$ of $L$. Then $\operatorname{Roots}(\langle a, b \rangle * \langle c, d \rangle) = \{-\frac{a}{b}, -\frac{c}{d}\}$. The theorem is a consequence

of (10).

(14) Let us consider a field $L$, elements $a$, $x$ of $L$, and a non zero element $b$ of $L$. If $x \neq -\frac{a}{b}$, then multiplicity$(\langle a, b\rangle, x) = 0$. The theorem is a consequence of (10).

Let us consider a field $L$, a non-zero polynomial $p$ over $L$, an element $a$ of $L$, and a non zero element $b$ of $L$. Now we state the propositions:

(15) Suppose $-\frac{a}{b} \notin \mathrm{Roots}(p)$. Then $\overline{\overline{\mathrm{Roots}(\langle a, b\rangle * p)}} = 1 + \overline{\overline{\mathrm{Roots}(p)}}$. The theorem is a consequence of (10).

(16) Suppose $-\frac{a}{b} \notin \mathrm{Roots}(p)$. Then $\mathrm{CFS}(\mathrm{Roots}(p)) \frown \langle -\frac{a}{b}\rangle$ is an enumeration of $\mathrm{Roots}(\langle a, b\rangle * p)$. The theorem is a consequence of (10).

(17) Let us consider a field $L$, a non-zero polynomial $p$ over $L$, an element $a$ of $L$, a non zero element $b$ of $L$, and an enumeration $E$ of $\mathrm{Roots}(\langle a, b\rangle * p)$. Suppose $E = \mathrm{CFS}(\mathrm{Roots}(p)) \frown \langle -\frac{a}{b}\rangle$. Then

  (i) $\operatorname{len} E = 1 + \overline{\overline{\mathrm{Roots}(p)}}$, and

  (ii) $E(1 + \overline{\overline{\mathrm{Roots}(p)}}) = -\frac{a}{b}$, and

  (iii) for every natural number $n$ such that $1 \leqslant n \leqslant \overline{\overline{\mathrm{Roots}(p)}}$ holds $E(n) = (\mathrm{CFS}(\mathrm{Roots}(p)))(n)$.

Let $L$ be a non empty double loop structure, $B$ be a bag of the carrier of $L$, and $E$ be a (the carrier of $L$)-valued finite sequence. The functor $B(++)E$ yielding a finite sequence of elements of $L$ is defined by

(Def. 1) $\operatorname{len} it = \operatorname{len} E$ and for every natural number $n$ such that $1 \leqslant n \leqslant \operatorname{len} it$ holds $it(n) = (B \cdot E)(n) \cdot E_n$.

Now we state the propositions:

(18) Let us consider an integral domain $L$, a non-zero polynomial $p$ over $L$, a bag $B$ of the carrier of $L$, and an enumeration $E$ of $\mathrm{Roots}(p)$. If $\mathrm{Roots}(p) = \emptyset$, then $B(++)E = \emptyset$.

(19) Let us consider a left zeroed, add-associative, non empty double loop structure $L$, bags $B_1$, $B_2$ of the carrier of $L$, and a (the carrier of $L$)-valued finite sequence $E$. Then $B_1 + B_2(++)E = (B_1(++)E) + (B_2(++)E)$.

(20) Let us consider a left zeroed, add-associative, non empty double loop structure $L$, a bag $B$ of the carrier of $L$, and (the carrier of $L$)-valued finite sequences $E$, $F$. Then $B(++)E \frown F = (B(++)E) \frown (B(++)F)$.

(21) Let us consider a left zeroed, add-associative, non empty double loop structure $L$, bags $B_1$, $B_2$ of the carrier of $L$, and (the carrier of $L$)-valued finite sequences $E$, $F$. Then $B_1 + B_2(++)E \frown F = (B_1(++)E) \frown (B_1(++)F) + (B_2(++)E) \frown (B_2(++)F)$. The theorem is a consequence of (19) and (20).

(22) Let us consider a field $L$, a non-zero polynomial $p$ over $L$, an element $a$ of $L$, a non zero element $b$ of $L$, an enumeration $E$ of $\mathrm{Roots}(\langle a, b\rangle * p)$, and a permutation $P$ of $\mathrm{dom}\, E$. Then $(\mathrm{BRoots}(\langle a, b\rangle * p)(+\!+)E) \cdot P = \mathrm{BRoots}(\langle a, b\rangle * p)(+\!+)(E \cdot P)$.

PROOF: Set $q = \langle a, b\rangle$. Set $B = \mathrm{BRoots}(q * p)$. Reconsider $P_1 = P$ as a permutation of $\mathrm{dom}(B(+\!+)E)$. $(B(+\!+)E) \cdot P_1 = B(+\!+)(E \cdot P)$ by [13, (27)], [11, (29), (25)], [4, (13)]. $\square$

Let us consider a field $L$, a non-zero polynomial $p$ over $L$, an element $a$ of $L$, a non zero element $b$ of $L$, and an enumeration $E$ of $\mathrm{Roots}(\langle a, b\rangle * p)$. Now we state the propositions:

(23) Suppose $-\frac{a}{b} \notin \mathrm{Roots}(p)$. Then suppose $E = \mathrm{CFS}(\mathrm{Roots}(p))^\frown\langle -\frac{a}{b}\rangle$. Then $(\mathrm{CFS}(\mathrm{Roots}(\langle a, b\rangle * p)))^{-1} \cdot E$ is a permutation of $\mathrm{dom}\, E$. The theorem is a consequence of (15) and (10).

(24) Suppose $-\frac{a}{b} \notin \mathrm{Roots}(p)$. Then suppose $E = \mathrm{CFS}(\mathrm{Roots}(p))^\frown\langle -\frac{a}{b}\rangle$. Then $\sum(\mathrm{BRoots}(\langle a, b\rangle * p)(+\!+)E) = \sum(\mathrm{BRoots}(\langle a, b\rangle * p)(+\!+)\,\mathrm{CFS}(\mathrm{Roots}(\langle a, b\rangle * p)))$.

PROOF: Set $q = \langle a, b\rangle$. Set $B = \mathrm{BRoots}(q * p)$. Set $D = \mathrm{CFS}(\mathrm{Roots}(q * p))$. Reconsider $P = D^{-1} \cdot E$ as a permutation of $\mathrm{dom}\, E$. $E \cdot E^{-1} \cdot D = D$ by [4, (37)], [13, (27)], [4, (35), (12)]. $(B(+\!+)E) \cdot P^{-1} = B(+\!+)(E \cdot P^{-1})$. $\square$

(25) $\sum(\mathrm{BRoots}(\langle a, b\rangle)(+\!+)E) = -\frac{a}{b}$. The theorem is a consequence of (10), (11), and (14).

Let $L$ be an integral domain and $p$ be a non-zero polynomial over $L$. The functor $\mathrm{SumRoots}(p)$ yielding an element of $L$ is defined by the term

(Def. 2) $\sum(\mathrm{BRoots}(p)(+\!+)\,\mathrm{CFS}(\mathrm{Roots}(p)))$.

Now we state the propositions:

(26) Let us consider an integral domain $L$, and a non-zero polynomial $p$ over $L$. If $\mathrm{Roots}(p) = \emptyset$, then $\mathrm{SumRoots}(p) = 0_L$. The theorem is a consequence of (2) and (18).

(27) Let us consider a field $L$, an element $a$ of $L$, and a non zero element $b$ of $L$. Then $\mathrm{SumRoots}(\langle a, b\rangle) = -\frac{a}{b}$. The theorem is a consequence of (10), (2), and (11).

(28) Let us consider a field $L$, a non-zero polynomial $p$ over $L$, an element $a$ of $L$, and a non zero element $b$ of $L$. Then $\mathrm{SumRoots}(\langle a, b\rangle * p) = -\frac{a}{b} + \mathrm{SumRoots}(p)$. The theorem is a consequence of (16), (17), (24), (2), (10), (11), (25), and (19).

(29) Let us consider a field $L$, elements $a$, $c$ of $L$, and non zero elements $b$, $d$ of $L$. Then $\mathrm{SumRoots}(\langle a, b\rangle * \langle c, d\rangle) = -\frac{a}{b} + -\frac{c}{d}$. The theorem is a consequence of (27) and (28).

(30) Let us consider an algebraic closed field $L$, and non-zero polynomials $p$, $q$ over $L$. Suppose $\operatorname{len} p \geqslant 2$. Then $\operatorname{SumRoots}(p * q) = \operatorname{SumRoots}(p) + \operatorname{SumRoots}(q)$.

Proof: Define $\mathcal{P}[\text{natural number}] \equiv$ for every non-zero polynomial $f$ over $L$ such that $\$_1 = \operatorname{len} f$ holds $\operatorname{SumRoots}(f * q) = \operatorname{SumRoots}(f) + \operatorname{SumRoots}(q)$. $\mathcal{P}[2]$. For every non trivial natural number $k$ such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$ by [6, (29)], [1, (11)], [8, (17), (50)]. For every non trivial natural number $k$, $\mathcal{P}[k]$ from [6, Sch. 2]. □

(31) Let us consider an algebraic closed integral domain $L$, a non-zero polynomial $p$ over $L$, and a finite sequence $r$ of elements of $L$. Suppose $r$ is one-to-one and $\operatorname{len} r = \operatorname{len} p -' 1$ and $\operatorname{Roots}(p) = \operatorname{rng} r$. Then $\sum r = \operatorname{SumRoots}(p)$.

Proof: Set $B = \operatorname{BRoots}(p)$. Set $s = \operatorname{support} B$. Set $L_1 = \operatorname{len} r \mapsto 1$. Consider $f$ being a finite sequence of elements of $\mathbb{N}$ such that $\operatorname{degree}(B) = \sum f$ and $f = B \cdot \operatorname{CFS}(s)$. Reconsider $E = \operatorname{CFS}(s)$ as a finite sequence of elements of $L$. For every natural number $j$ such that $j \in \operatorname{Seg} \operatorname{len} r$ holds $f(j) \geqslant L_1(j)$ by [8, (52)], [4, (12)], [3, (57)]. For every natural number $j$ such that $1 \leqslant j \leqslant \operatorname{len} E$ holds $(B(++)E)(j) = E(j)$ by [5, (83)], [3, (57)], [9, (13)]. □

(32) Vieta's formula about the sum of roots:
Let us consider an algebraic closed field $L$, and a non-zero polynomial $p$ over $L$. Suppose $\operatorname{len} p \geqslant 2$. Then $\operatorname{SumRoots}(p) = -\frac{p(\operatorname{len} p -' 2)}{p(\operatorname{len} p -' 1)}$.

Proof: Define $\mathcal{P}[\text{natural number}] \equiv$ for every non-zero polynomial $p$ over $L$ such that $\$_1 = \operatorname{len} p$ holds $\operatorname{SumRoots}(p) = -\frac{p(\$_1 -' 2)}{p(\$_1 -' 1)}$. $\mathcal{P}[2]$ by (6), [7, (38)], (27). For every non trivial natural number $k$ such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$ by [6, (29)], [1, (11)], [8, (17)], [10, (5)]. For every non trivial natural number $k$, $\mathcal{P}[k]$ from [6, Sch. 2]. □

## References


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

[2] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, Karol Pąk, and Josef Urban. Mizar: State-of-the-art and beyond. In Manfred Kerber, Jacques Carette, Cezary Kaliszyk, Florian Rabe, and Volker Sorge, editors, *Intelligent Computer Mathematics*, volume 9150 of *Lecture Notes in Computer Science*, pages 261–279. Springer International Publishing, 2015. ISBN 978-3-319-20614-1. doi:10.1007/978-3-319-20615-8_17.

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

[6] Robert Milewski. Natural numbers. *Formalized Mathematics*, 7(**1**):19–22, 1998.

[7] Robert Milewski. Fundamental theorem of algebra. *Formalized Mathematics*, 9(**3**):461–470, 2001.
[8] Piotr Rudnicki. Little Bezout theorem (factor theorem). *Formalized Mathematics*, 12(**1**):49–58, 2004.
[9] Christoph Schwarzweller. The binomial theorem for algebraic structures. *Formalized Mathematics*, 9(**3**):559–564, 2001.
[10] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.
[11] Wojciech A. Trybulec. Non-contiguous substrings and one-to-one finite sequences. *Formalized Mathematics*, 1(**3**):569–573, 1990.
[12] E. B. Vinberg. *A Course in Algebra*. American Mathematical Society, 2003. ISBN 0821834134.
[13] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.

*Received May 25, 2017*

---

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

FORMALIZED MATHEMATICS
Vol. 25, No. 2, Pages 93–100, 2017
DOI: 10.1515/forma-2017-0009

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

# Basic Formal Properties of Triangular Norms and Conorms

Adam Grabowski
Institute of Informatics
University of Białystok
Poland

**Summary.** In the article we present in the Mizar system [1], [8] the catalogue of triangular norms and conorms, used especially in the theory of fuzzy sets [13]. The name *triangular* emphasizes the fact that in the framework of probabilistic metric spaces they generalize triangle inequality [2].

After defining corresponding Mizar mode using four attributes, we introduced the following t-norms:

- minimum t-norm `minnorm` (Def. 6),
- product t-norm `prodnorm` (Def. 8),
- Łukasiewicz t-norm `Lukasiewicz_norm` (Def. 10),
- drastic t-norm `drastic_norm` (Def. 11),
- nilpotent minimum `nilmin_norm` (Def. 12),
- Hamacher product `Hamacher_norm` (Def. 13),

and corresponding t-conorms:

- maximum t-conorm `maxnorm` (Def. 7),
- probabilistic sum `probsum_conorm` (Def. 9),
- bounded sum `BoundedSum_conorm` (Def. 19),
- drastic t-conorm `drastic_conorm` (Def. 14),
- nilpotent maximum `nilmax_conorm` (Def. 18),
- Hamacher t-conorm `Hamacher_conorm` (Def. 17).

Their basic properties and duality are shown; we also proved the predicate of the ordering of norms [10], [9]. It was proven formally that drastic-norm is the pointwise smallest t-norm and minnorm is the pointwise largest t-norm (maxnorm is the pointwise smallest t-conorm and drastic-conorm is the pointwise largest t-conorm).




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

This work is a continuation of the development of fuzzy sets in Mizar [6] started in [11] and [3]; it could be used to give a variety of more general operations on fuzzy sets. Our formalization is much closer to the set theory used within the Mizar Mathematical Library than the development of rough sets [4], the approach which was chosen allows however for merging both theories [5], [7].

MSC: 03E72 94D05 03B35

Keywords: fuzzy set; triangular norm; triangular conorm; fuzzy logic

MML identifier: `FUZNORM1`, version: `8.1.06 5.43.1297`

## 1. Preliminaries

One can verify that $[0,1]$ is non empty.

Let us consider elements $a$, $b$ of $[0,1]$. Now we state the propositions:

(1) $\min(a,b) \in [0,1]$.

(2) $\max(a,b) \in [0,1]$.

(3) $a \cdot b \in [0,1]$.

(4) $\max(0, a+b-1) \in [0,1]$.

(5) $\min(a+b, 1) \in [0,1]$.

(6) Let us consider elements $a$, $b$, $c$ of $[0,1]$. Then $\max(0, \max(0, a+b-1) + c-1) = \max(0, a + \max(0, b+c-1) - 1)$.

(7) Let us consider an element $a$ of $[0,1]$. Then $1-a \in [0,1]$.

Let us consider elements $a$, $b$ of $[0,1]$. Now we state the propositions:

(8) $a+b-(a \cdot b) \in [0,1]$. The theorem is a consequence of (7) and (3).

(9) $\frac{a \cdot b}{a+b-(a \cdot b)} \in [0,1]$. The theorem is a consequence of (3) and (8).

(10) If $\max(a,b) \neq 1$, then $a \neq 1$ and $b \neq 1$.

(11) Let us consider elements $x$, $y$ of $[0,1]$. If $x \cdot y = x + y$, then $x = 0$. The theorem is a consequence of (7).

Let us consider elements $a$, $b$ of $[0,1]$. Now we state the propositions:

(12) $\max(a,b) = 1 - \min(1-a, 1-b)$.

(13) $\min(a+b, 1) = 1 - \max(0, 1-a+(1-b)-1)$.

(14) $\frac{a+b-(2 \cdot a \cdot b)}{1-(a \cdot b)} \in [0,1]$. The theorem is a consequence of (7) and (3).

Let $f$ be a binary operation on $[0,1]$ and $a$, $b$ be real numbers. Let us observe that $f(a,b)$ is real.

Now we state the propositions:

(15) Let us consider real numbers $a$, $b$, and a binary operation $t$ on $[0,1]$. Then $t(a,b) \in [0,1]$.

(16) Let us consider a binary operation $f$ on $[0,1]$, and real numbers $a$, $b$. Then $1 - f(1-a, 1-b) \in [0,1]$. The theorem is a consequence of (15) and (7).

(17) Let us consider real numbers $x$, $y$, $k$. Suppose $k \leqslant 0$. Then

  (i) $k \cdot \min(x,y) = \max(k \cdot x, k \cdot y)$, and

  (ii) $k \cdot \max(x,y) = \min(k \cdot x, k \cdot y)$.

## 2. Basic Example of a Triangular Norm and Conorm: min and max

Let $A$ be a real-membered set and $f$ be a binary operation on $A$. We say that $f$ is monotonic if and only if

(Def. 1) for every elements $a$, $b$, $c$, $d$ of $A$ such that $a \leqslant c$ and $b \leqslant d$ holds $f(a,b) \leqslant f(c,d)$.

We say that $f$ has 1-identity if and only if

(Def. 2) for every element $a$ of $A$, $f(a,1) = a$.

We say that $f$ has 1-annihilating if and only if

(Def. 3) for every element $a$ of $A$, $f(a,1) = 1$.

We say that $f$ has 0-identity if and only if

(Def. 4) for every element $a$ of $A$, $f(a,0) = a$.

We say that $f$ has 0-annihilating if and only if

(Def. 5) for every element $a$ of $A$, $f(a,0) = 0$.

The scheme *ExBinOp* deals with a non empty, real-membered set $\mathcal{A}$ and a binary functor $\mathcal{F}$ yielding a set and states that

(Sch. 1) There exists a binary operation $f$ on $\mathcal{A}$ such that for every elements $a$, $b$ of $\mathcal{A}$, $f(a,b) = \mathcal{F}(a,b)$

provided

- for every elements $a$, $b$ of $\mathcal{A}$, $\mathcal{F}(a,b) \in \mathcal{A}$.

The functor minnorm yielding a binary operation on $[0,1]$ is defined by

(Def. 6) for every elements $a$, $b$ of $[0,1]$, $it(a,b) = \min(a,b)$.

Observe that minnorm is commutative, associative, and monotonic and has 1-identity and there exists a binary operation on $[0,1]$ which is commutative, associative, and monotonic and has 1-identity.

A t-norm is a commutative, associative, monotonic binary operation on $[0,1]$ with 1-identity. The functor maxnorm yielding a binary operation on $[0,1]$ is defined by

(Def. 7) for every elements $a$, $b$ of $[0,1]$, $it(a,b) = \max(a,b)$.

One can verify that maxnorm is commutative, associative, and monotonic and has 0-identity and there exists a binary operation on $[0,1]$ which is commutative, associative, and monotonic and has 0-identity.

A t-conorm is a commutative, associative, monotonic binary operation on $[0,1]$ with 0-identity. Now we state the propositions:

(18) Let us consider a commutative, monotonic binary operation $t$ on $[0,1]$ with 1-identity, and an element $a$ of $[0,1]$. Then $t(a,0) = 0$. The theorem is a consequence of (15).

(19) Let us consider a commutative, monotonic binary operation $t$ on $[0,1]$ with 0-identity, and an element $a$ of $[0,1]$. Then $t(a,1) = 1$. The theorem is a consequence of (15).

Let us note that every commutative, monotonic binary operation on $[0,1]$ with 1-identity has 0-annihilating and every commutative, monotonic binary operation on $[0,1]$ with 0-identity has 1-annihilating.

## 3. Further Examples of Triangular Norms

The functor prodnorm yielding a binary operation on $[0,1]$ is defined by

(Def. 8) for every elements $a$, $b$ of $[0,1]$, $it(a,b) = a \cdot b$.

Let us observe that prodnorm is commutative, associative, and monotonic and has 1-identity.

The functor probsum-conorm yielding a binary operation on $[0,1]$ is defined by

(Def. 9) for every elements $a$, $b$ of $[0,1]$, $it(a,b) = a + b - (a \cdot b)$.

The functor Lukasiewicz-norm yielding a binary operation on $[0,1]$ is defined by

(Def. 10) for every elements $a$, $b$ of $[0,1]$, $it(a,b) = \max(0, a + b - 1)$.

One can check that Lukasiewicz-norm is commutative, associative, and monotonic and has 1-identity.

The functor drastic-norm yielding a binary operation on $[0,1]$ is defined by

(Def. 11) for every elements $a$, $b$ of $[0,1]$, if $\max(a,b) = 1$, then $it(a,b) = \min(a,b)$ and if $\max(a,b) \neq 1$, then $it(a,b) = 0$.

Now we state the proposition:

(20) Let us consider elements $a$, $b$ of $[0,1]$. Then

(i) if $a = 1$, then $(\text{drastic-norm})(a,b) = b$, and

(ii) if $b = 1$, then $(\text{drastic-norm})(a,b) = a$, and

(iii) if $a \neq 1$ and $b \neq 1$, then (drastic-norm)$(a, b) = 0$.

Note that drastic-norm is commutative, associative, and monotonic and has 1-identity.

The functor nilmin-norm yielding a binary operation on $[0, 1]$ is defined by

(Def. 12) for every elements $a$, $b$ of $[0, 1]$, if $a + b > 1$, then $it(a, b) = \min(a, b)$ and if $a + b \leqslant 1$, then $it(a, b) = 0$.

Observe that nilmin-norm is commutative, associative, and monotonic and has 1-identity.

The functor Hamacher-norm yielding a binary operation on $[0, 1]$ is defined by

(Def. 13) for every elements $a$, $b$ of $[0, 1]$, $it(a, b) = \frac{a \cdot b}{a + b - (a \cdot b)}$.

One can verify that Hamacher-norm is commutative, associative, and monotonic and has 1-identity.

## 4. Basic Triangular Conorms

The functor drastic-conorm yielding a binary operation on $[0, 1]$ is defined by

(Def. 14) for every elements $a$, $b$ of $[0, 1]$, if $\min(a, b) = 0$, then $it(a, b) = \max(a, b)$ and if $\min(a, b) \neq 0$, then $it(a, b) = 1$.

## 5. Translating between Triangular Norms and Conorms

Let $t$ be a binary operation on $[0, 1]$. The functor conorm $t$ yielding a binary operation on $[0, 1]$ is defined by

(Def. 15) for every elements $a$, $b$ of $[0, 1]$, $it(a, b) = 1 - t(1 - a, 1 - b)$.

Let $t$ be a t-norm. Let us observe that conorm $t$ is monotonic, commutative, and associative and has 0-identity.

Now we state the propositions:

(21) maxnorm = conorm minnorm.

PROOF: For every elements $a$, $b$ of $[0, 1]$, (maxnorm)$(a, b) = 1 -$ (minnorm) $(1 - a, 1 - b)$ by (7), (17), [12, (42)]. □

(22) Let us consider a binary operation $t$ on $[0, 1]$. Then conorm conorm $t = t$. The theorem is a consequence of (7).

## 6. The Ordering of Triangular Norms (and Conorms)

Let $f_1$, $f_2$ be binary operations on $[0,1]$. We say that $f_1 \leqslant f_2$ if and only if

(Def. 16) for every elements $a$, $b$ of $[0,1]$, $f_1(a,b) \leqslant f_2(a,b)$.

Let us consider a t-norm $t$. Now we state the propositions:

(23) drastic-norm $\leqslant t$. The theorem is a consequence of (20).

(24) $t \leqslant$ minnorm.

Now we state the proposition:

(25) Let us consider t-norms $t_1$, $t_2$. If $t_1 \leqslant t_2$, then conorm $t_2 \leqslant$ conorm $t_1$. The theorem is a consequence of (7).

## 7. Triangular Conorms Generated from t-Norms

The functor Hamacher-conorm yielding a binary operation on $[0,1]$ is defined by

(Def. 17) for every elements $a$, $b$ of $[0,1]$, if $a = b = 1$, then $it(a,b) = 1$ and if $a \neq 1$ or $b \neq 1$, then $it(a,b) = \frac{a+b-(2 \cdot a \cdot b)}{1-(a \cdot b)}$.

Now we state the proposition:

(26) conorm Hamacher-norm = Hamacher-conorm. The theorem is a consequence of (7).

Let us note that Hamacher-conorm is commutative, associative, and monotonic and has 0-identity.

Now we state the propositions:

(27) conorm drastic-norm = drastic-conorm. The theorem is a consequence of (7).

(28) conorm prodnorm = probsum-conorm. The theorem is a consequence of (7).

One can check that probsum-conorm is commutative, associative, and monotonic and has 0-identity.

The functor nilmax-conorm yielding a binary operation on $[0,1]$ is defined by

(Def. 18) for every elements $a$, $b$ of $[0,1]$, if $a+b < 1$, then $it(a,b) = \max(a,b)$ and if $a+b \geqslant 1$, then $it(a,b) = 1$.

Now we state the proposition:

(29) conorm nilmin-norm = nilmax-conorm. The theorem is a consequence of (7) and (12).

Let us note that nilmax-conorm is commutative, associative, and monotonic and has 0-identity.

The functor BoundedSum-conorm yielding a binary operation on $[0,1]$ is defined by

(Def. 19) for every elements $a$, $b$ of $[0,1]$, $it(a,b) = \min(a+b,1)$.

Now we state the proposition:

(30) conorm Lukasiewicz-norm = BoundedSum-conorm. The theorem is a consequence of (7) and (13).

One can check that BoundedSum-conorm is commutative, associative, and monotonic and has 0-identity.

Let us consider a t-conorm $t$. Now we state the propositions:

(31) maxnorm $\leqslant t$.

(32) $t \leqslant$ drastic-conorm.

## References


[1] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, Karol Pąk, and Josef Urban. Mizar: State-of-the-art and beyond. In Manfred Kerber, Jacques Carette, Cezary Kaliszyk, Florian Rabe, and Volker Sorge, editors, *Intelligent Computer Mathematics*, volume 9150 of *Lecture Notes in Computer Science*, pages 261–279. Springer International Publishing, 2015. ISBN 978-3-319-20614-1. doi:10.1007/978-3-319-20615-8_17.

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

[3] Adam Grabowski. The formal construction of fuzzy numbers. *Formalized Mathematics*, 22(**4**):321–327, 2014. doi:10.2478/forma-2014-0032.

[4] Adam Grabowski. On the computer-assisted reasoning about rough sets. In B. Dunin-Kęplicz, A. Jankowski, A. Skowron, and M. Szczuka, editors, *International Workshop on Monitoring, Security, and Rescue Techniques in Multiagent Systems Location*, volume 28 of *Advances in Soft Computing*, pages 215–226, Berlin, Heidelberg, 2005. Springer-Verlag. doi:10.1007/3-540-32370-8_15.

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

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

[7] Adam Grabowski and Takashi Mitsuishi. Initial comparison of formal approaches to fuzzy and rough sets. In Leszek Rutkowski, Marcin Korytkowski, Rafal Scherer, Ryszard Tadeusiewicz, Lotfi A. Zadeh, and Jacek M. Zurada, editors, *Artificial Intelligence and Soft Computing - 14th International Conference, ICAISC 2015, Zakopane, Poland, June 14-18, 2015, Proceedings, Part I*, volume 9119 of *Lecture Notes in Computer Science*, pages 160–171. Springer, 2015. doi:10.1007/978-3-319-19324-3_15.

[8] Adam Grabowski, Artur Korniłowicz, and Adam Naumowicz. Four decades of Mizar. *Journal of Automated Reasoning*, 55(3):191–198, 2015. doi:10.1007/s10817-015-9345-1.

[9] Petr Hájek. *Metamathematics of Fuzzy Logic.* Dordrecht: Kluwer, 1998.

[10] Erich Peter Klement, Radko Mesiar, and Endre Pap. *Triangular Norms.* Dordrecht: Kluwer, 2000.

[11] Takashi Mitsuishi, Noboru Endou, and Yasunari Shidama. The concept of fuzzy set and

membership function and basic properties of fuzzy set operation. *Formalized Mathematics*, 9(**2**):351–356, 2001.

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

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

*Received June 27, 2017*

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

FORMALIZED MATHEMATICS
Vol. 25, No. 2, Pages 101–105, 2017
DOI: 10.1515/forma-2017-0010

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

# Introduction to Stopping Time in Stochastic Finance Theory

Peter Jaeger
Siegmund-Schacky-Str. 18a
80993 Munich, Germany

**Summary.** We start with the definition of stopping time according to [4], p.283. We prove, that different definitions for stopping time can coincide. We give examples of stopping time using constant-functions or functions defined with the operator max or min (defined in [6], pp.37–38). Finally we give an example with some given filtration. Stopping time is very important for stochastic finance. A stopping time is the moment, where a certain event occurs ([7], p.372) and can be used together with stochastic processes ([4], p.283). Look at the following example: we install a function ST: {1,2,3,4} $\rightarrow \{0, 1, 2\} \cup \{+\infty\}$, we define:

a. ST(1)=1, ST(2)=1, ST(3)=2, ST(4)=2.

b. The set {0,1,2} consists of time points: 0=now,1=tomorrow,2=the day after tomorrow.

We can prove:

c. {w, where w is Element of Ω: ST.w=0}=∅ & {w, where w is Element of Ω: ST.w=1}={1,2} & {w, where w is Element of Ω: ST.w=2}={3,4} and

ST is a stopping time.

We use a function Filt as Filtration of {0,1,2}, Σ where Filt(0)=$\Omega_{now}$, Filt(1)=$\Omega_{fut1}$ and Filt(2)=$\Omega_{fut2}$. From a.,b. and c. we know that:

d. {w, where w is Element of Ω: ST.w=0} in $\Omega_{now}$ and

{w, where w is Element of Ω: ST.w=1} in $\Omega_{fut1}$ and

{w, where w is Element of Ω: ST.w=2} in $\Omega_{fut2}$.

The sets in d. are events, which occur at the time points 0(=now), 1(=tomorrow) or 2(=the day after tomorrow), see also [7], p.371. Suppose we have ST(1)=+∞, then this means that for 1 the corresponding event never occurs.

As an interpretation for our installed functions consider the given adapted stochastic process in the article [5].

ST(1)=1 means, that the given element 1 in {1,2,3,4} is stopped in 1 (=tomorrow). That tells us, that we have to look at the value $f_2(1)$ which is equal to 80. The same argumentation can be applied for the element 2 in {1,2,3,4}.




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

ST(3)=2 means, that the given element 3 in {1,2,3,4} is stopped in 2 (=the day after tomorrow). That tells us, that we have to look at the value $f_3(3)$ which is equal to 100.

ST(4)=2 means, that the given element 4 in {1,2,3,4} is stopped in 2 (=the day after tomorrow). That tells us, that we have to look at the value $f_3(4)$ which is equal to 120.

In the real world, these functions can be used for questions like: when does the share price exceed a certain limit? (see [7], p.372).

MSC: 60G40 03B35

Keywords: stopping time; stochastic process

MML identifier: `FINANCE4`, version: `8.1.06 5.43.1297`

## 1. Preliminaries

From now on $\Omega$ denotes a non empty set, $\Sigma$ denotes a $\sigma$-field of subsets of $\Omega$, and $T$ denotes a natural number.

Now we state the proposition:

(1) Let us consider a non empty set $X$, an object $t$, and a function $f$. Suppose $\operatorname{dom} f = X$. Then $\{w$, where $w$ is an element of $X : f(w) = t\} = \operatorname{Coim}(f, t)$.

Proof: Set $A = \{w$, where $w$ is an element of $X : f(w) = t\}$. $A \subseteq \operatorname{Coim}(f, t)$ by [2, (1)]. Consider $y$ being an object such that $\langle x, y \rangle \in f$ and $y \in \{t\}$. $\square$

Let $I$ be an extended real-membered set. The functor $I_{\{+\infty\}}$ yielding a subset of $\overline{\mathbb{R}}$ is defined by the term

(Def. 1) $I \cup \{+\infty\}$.

Let us note that $I_{\{+\infty\}}$ is non empty.

## 2. Definition of Stopping Time

Let $T$ be a natural number. The functor $\bigcup_{t \in \mathbb{N}: 0 \leqslant t \leqslant T}\{t\}$ yielding a subset of $\mathbb{R}$ is defined by the term

(Def. 2) $\{t$, where $t$ is an element of $\mathbb{N} : 0 \leqslant t \leqslant T\}$.

Let us note that $\bigcup_{t \in \mathbb{N}: 0 \leqslant t \leqslant T}\{t\}$ is non empty.

The functor $T_{\{+\infty\}}$ yielding a subset of $\overline{\mathbb{R}}$ is defined by the term

(Def. 3) $\bigcup_{t \in \mathbb{N}: 0 \leqslant t \leqslant T}\{t\} \cup \{+\infty\}$.

Let us note that $T_{\{+\infty\}}$ is non empty.

In the sequel $T_1$ denotes an element of $T_{\{+\infty\}}$, $MF$ denotes a filtration of $\bigcup_{t\in\mathbb{N}:0\leqslant t\leqslant T}\{t\}$ and $\Sigma$, and $k$, $k_1$, $k_2$ denote functions from $\Omega$ into $T_{\{+\infty\}}$.

Let $T$ be a natural number, $F$ be a function, and $R$ be a binary relation. We say that $R$ is StoppingTime($F$,$T$) if and only if

(Def. 4) for every element $t$ of $\bigcup_{t\in\mathbb{N}:0\leqslant t\leqslant T}\{t\}$, $\mathrm{Coim}(R,t) \in F(t)$.

Let $\Omega$ be a non empty set, $MF$ be a function, and $k$ be a function from $\Omega$ into $T_{\{+\infty\}}$. Let us observe that $k$ is StoppingTime($MF$,$T$) if and only if the condition (Def. 5) is satisfied.

(Def. 5) for every element $t$ of $\bigcup_{t\in\mathbb{N}:0\leqslant t\leqslant T}\{t\}$, $\{w$, where $w$ is an element of $\Omega$ : $k(w) = t\} \in MF(t)$.

Now we state the proposition:

(2) $k$ is StoppingTime($MF$,$T$) if and only if for every element $t$ of $\bigcup_{t\in\mathbb{N}:0\leqslant t\leqslant T}\{t\}$, $\{w$, where $w$ is an element of $\Omega$ : $k(w) \leqslant t\} \in MF(t)$.
PROOF: If $k$ is StoppingTime($MF$,$T$), then for every element $t$ of $\bigcup_{t\in\mathbb{N}:0\leqslant t\leqslant T}\{t\}$, $\{w$, where $w$ is an element of $\Omega$ : $k(w) \leqslant t\} \in MF(t)$ by [1, (8), (12), (13)], [8, (21)]. For every element $t$ of $\bigcup_{t\in\mathbb{N}:0\leqslant t\leqslant T}\{t\}$, $\{w$, where $w$ is an element of $\Omega$ : $k(w) = t\} \in MF(t)$ by [1, (13)], [8, (22), (24)], [1, (22)]. $\square$

## 3. EXAMPLES OF STOPPING TIMES

Now we state the proposition:

(3) $\Omega \longmapsto T_1$ is StoppingTime($MF$,$T$).
PROOF: Set $c = \Omega \longmapsto T_1$. For every element $t$ of $\bigcup_{t\in\mathbb{N}:0\leqslant t\leqslant T}\{t\}$, $\{w$, where $w$ is an element of $\Omega$ : $c(w) = t\} \in MF(t)$ by [9, (7)], [8, (5), (4)]. $\square$

Let us consider $\Omega$, $T$, $k_1$, and $k_2$. The functor $\max(k_1, k_2)$ yielding a function from $\Omega$ into $\overline{\mathbb{R}}$ is defined by

(Def. 6) for every element $w$ of $\Omega$, $it(w) = \max(k_1(w), k_2(w))$.

The functor $\min(k_1, k_2)$ yielding a function from $\Omega$ into $\overline{\mathbb{R}}$ is defined by

(Def. 7) for every element $w$ of $\Omega$, $it(w) = \min(k_1(w), k_2(w))$.

Now we state the propositions:

(4) Suppose $k_1$ is StoppingTime($MF$,$T$) and $k_2$ is StoppingTime($MF$,$T$). Then there exists a function $k_3$ from $\Omega$ into $T_{\{+\infty\}}$ such that

(i) $k_3 = \max(k_1, k_2)$, and

(ii) $k_3$ is StoppingTime($MF$,$T$).

PROOF: Set $k_3 = \max(k_1, k_2)$. $k_3$ is a function from $\Omega$ into $T_{\{+\infty\}}$ by [2, (3)], [3, (2)]. $k_3$ is StoppingTime($MF$,$T$) by (2), [8, (19)]. □

(5) Suppose $k_1$ is StoppingTime($MF$,$T$) and $k_2$ is StoppingTime($MF$,$T$). Then there exists a function $k_3$ from $\Omega$ into $T_{\{+\infty\}}$ such that

(i) $k_3 = \min(k_1, k_2)$, and

(ii) $k_3$ is StoppingTime($MF$,$T$).

PROOF: Set $k_3 = \min(k_1, k_2)$. $k_3$ is a function from $\Omega$ into $T_{\{+\infty\}}$ by [2, (3)], [3, (2)]. $k_3$ is StoppingTime($MF$,$T$) by (2), [8, (3)]. □

Let $t$ be an object. The special element of $t_{\{+\infty\}}$ yielding an element of $2_{\{+\infty\}}$ is defined by the term

(Def. 8) IFIN($t, \{1,2\}, 1, 2$).

Now we state the proposition:

(6) Suppose $\Omega = \{1,2,3,4\}$. Let us consider a filtration $MF$ of $\bigcup_{t \in \mathbb{N}: 0 \leqslant t \leqslant 2} \{t\}$ and $\Sigma$. Suppose $MF(0) = \Omega_{now}$ and $MF(1) = \Omega_{fut1}$ and $MF(2) = \Omega_{fut2}$. Then there exists a function $S$ from $\Omega$ into $2_{\{+\infty\}}$ such that

(i) $S$ is StoppingTime($MF$,2), and

(ii) $S(1) = 1$, and

(iii) $S(2) = 1$, and

(iv) $S(3) = 2$, and

(v) $S(4) = 2$, and

(vi) $\{w$, where $w$ is an element of $\Omega : S(w) = 0\} = \emptyset$, and

(vii) $\{w$, where $w$ is an element of $\Omega : S(w) = 1\} = \{1,2\}$, and

(viii) $\{w$, where $w$ is an element of $\Omega : S(w) = 2\} = \{3,4\}$.

PROOF: Define $\mathcal{U}$(element of $\Omega$) = the special element of $\$_{1\{+\infty\}}$. Consider $f$ being a function from $\Omega$ into $2_{\{+\infty\}}$ such that for every element $d$ of $\Omega$, $f(d) = \mathcal{U}(d)$ from [3, Sch. 4]. $f(1) = 1$ and $f(2) = 1$ and $f(3) = 2$ and $f(4) = 2$. $f$ is StoppingTime($MF$,2) and $\{w$, where $w$ is an element of $\Omega$ : $f(w) = 0\} = \emptyset$ and $\{w$, where $w$ is an element of $\Omega : f(w) = 1\} = \{1,2\}$ and $\{w$, where $w$ is an element of $\Omega : f(w) = 2\} = \{3,4\}$ by [1, (9)], [8, (4)], [5, (24)]. □

## References


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

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

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

[4] Hans Föllmer and Alexander Schied. *Stochastic Finance: An Introduction in Discrete Time*, volume 27 of *Studies in Mathematics*. de Gruyter, Berlin, 2nd edition, 2004.

[5] Peter Jaeger. Modelling real world using stochastic processes and filtration. *Formalized Mathematics*, 24(**1**):1–16, 2016. doi:10.1515/forma-2016-0001.

[6] Achim Klenke. *Wahrscheinlichkeitstheorie.* Springer-Verlag, Berlin, Heidelberg, 2006.

[7] Jürgen Kremer. *Einführung in die diskrete Finanzmathematik.* Springer-Verlag, Berlin, Heidelberg, New York, 2006.

[8] Andrzej Nędzusiak. $\sigma$-fields and probability. *Formalized Mathematics*, 1(**2**):401–407, 1990.

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

*Received June 27, 2017*

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

FORMALIZED MATHEMATICS
Vol. 25, No. 2, Pages 107–119, 2017
DOI: 10.1515/forma-2017-0011

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

# Pascal's Theorem in Real Projective Plane

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

**Summary.** In this article we check, with the Mizar system [2], Pascal's theorem in the real projective plane (in projective geometry Pascal's theorem is also known as the Hexagrammum Mysticum Theorem)[1]. Pappus' theorem is a special case of a degenerate conic of two lines.

For proving Pascal's theorem, we use the techniques developed in the section "Projective Proofs of Pappus' Theorem" in the chapter "Pappus' Theorem: Nine proofs and three variations" [11]. We also follow some ideas from Harrison's work. With HOL Light, he has the proof of Pascal's theorem[2]. For a lemma, we use `PROVER9`[3] and `OTT2MIZ` by Josef Urban[4] [12, 6, 7]. We note, that we don't use Skolem/Herbrand functions (see "Skolemization" in [1]).

MSC: 51E15 51N15 03B35

Keywords: Pascal's theorem; real projective plane; Grassman-Plücker relation

MML identifier: `PASCAL`, version: `8.1.06 5.43.1297`

## 1. Preliminaries

From now on $n$ denotes a natural number, $K$ denotes a field, $a$, $b$, $c$, $d$, $e$, $f$, $g$, $h$, $i$, $a_1$, $b_1$, $c_1$, $d_1$, $e_1$, $f_1$, $g_1$, $h_1$, $i_1$ denote elements of $K$, $M$, $N$ denote square matrices over $K$ of dimension 3, and $p$ denotes a finite sequence of elements of $\mathbb{R}$.

Now we state the propositions:

(1) Let us consider points $p$, $q$, $r$ of $\mathcal{E}^3_{\mathrm{T}}$. Then

[1] `https://en.wikipedia.org/wiki/Pascal's_theorem`
[2] `https://github.com/jrh13/hol-light/tree/master/100/pascal.ml`
[3] `https://www.cs.unm.edu/~mccune/prover9/`
[4] `https://github.com/JUrban/ott2miz`




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

(i) $\langle|p, q, r|\rangle = \langle|r, p, q|\rangle$, and

(ii) $\langle|p, q, r|\rangle = \langle|q, r, p|\rangle$.

(2) Suppose $\langle\langle a, b, c\rangle, \langle d, e, f\rangle, \langle g, h, i\rangle\rangle = \langle\langle a_1, b_1, c_1\rangle, \langle d_1, e_1, f_1\rangle, \langle g_1, h_1, i_1\rangle\rangle$. Then

(i) $a = a_1$, and

(ii) $b = b_1$, and

(iii) $c = c_1$, and

(iv) $d = d_1$, and

(v) $e = e_1$, and

(vi) $f = f_1$, and

(vii) $g = g_1$, and

(viii) $h = h_1$, and

(ix) $i = i_1$.

(3) There exists $a$ and there exists $b$ and there exists $c$ and there exists $d$ and there exists $e$ and there exists $f$ and there exists $g$ and there exists $h$ and there exists $i$ such that $M = \langle\langle a, b, c\rangle, \langle d, e, f\rangle, \langle g, h, i\rangle\rangle$.

(4) Suppose $M = \langle\langle a, b, c\rangle, \langle d, e, f\rangle, \langle g, h, i\rangle\rangle$. Then

(i) $a = M_{1,1}$, and

(ii) $b = M_{1,2}$, and

(iii) $c = M_{1,3}$, and

(iv) $d = M_{2,1}$, and

(v) $e = M_{2,2}$, and

(vi) $f = M_{2,3}$, and

(vii) $g = M_{3,1}$, and

(viii) $h = M_{3,2}$, and

(ix) $i = M_{3,3}$.

(5) Suppose $M = \langle\langle a, b, c\rangle, \langle d, e, f\rangle, \langle g, h, i\rangle\rangle$. Then $M^{\mathrm{T}} = \langle\langle a, d, g\rangle, \langle b, e, h\rangle, \langle c, f, i\rangle\rangle$. The theorem is a consequence of (4) and (3).

(6) Suppose $M = \langle\langle a, b, c\rangle, \langle d, e, f\rangle, \langle g, h, i\rangle\rangle$ and $M$ is symmetric. Then

(i) $b = d$, and

(ii) $c = g$, and

(iii) $h = f$.

The theorem is a consequence of (5) and (2).

(7) Let us consider square matrices $M$, $N$ over $\mathbb{R}_{\rm F}$ of dimension 3. If $N$ is symmetric, then $M^{\rm T} \cdot N \cdot M$ is symmetric.

(8) Let us consider a square matrix $M$ over $\mathbb{R}_{\rm F}$ of dimension 3, elements $a$, $b$, $c$, $d$, $e$, $f$, $g$, $h$, $i$, $x$, $y$, $z$ of $\mathbb{R}_{\rm F}$, an element $v$ of $\mathcal{E}^3_{\rm T}$, a finite sequence $u_{10}$ of elements of $\mathbb{R}_{\rm F}$, and a finite sequence $p$ of elements of $\mathbb{R}^1$. Suppose $p = M \cdot u_{10}$ and $v = \mathrm{M2F}(p)$ and $M = \langle\langle a, b, c\rangle, \langle d, e, f\rangle, \langle g, h, i\rangle\rangle$ and $u_{10} = \langle x, y, z\rangle$. Then

  (i) $p = \langle\langle a\cdot x+(b\cdot y)+(c\cdot z)\rangle, \langle d\cdot x+(e\cdot y)+(f\cdot z)\rangle, \langle g\cdot x+(h\cdot y)+(i\cdot z)\rangle\rangle$, and

  (ii) $v = \langle a\cdot x+(b\cdot y)+(c\cdot z), d\cdot x+(e\cdot y)+(f\cdot z), g\cdot x+(h\cdot y)+(i\cdot z)\rangle$.

(9) Let us consider a square matrix $M$ over $\mathbb{R}$ of dimension 3, and elements $a$, $b$, $c$, $d$, $e$, $f$, $g$, $h$, $i$, $p_1$, $p_2$, $p_3$ of $\mathbb{R}$. Suppose $M = \langle\langle a, b, c\rangle, \langle d, e, f\rangle, \langle g, h, i\rangle\rangle$ and $p = \langle p_1, p_2, p_3\rangle$. Then $M \cdot p = \langle a \cdot p_1 + (b \cdot p_2) + (c \cdot p_3), d \cdot p_1 + (e \cdot p_2) + (f \cdot p_3), g \cdot p_1 + (h \cdot p_2) + (i \cdot p_3)\rangle$.

## 2. Conic in Real Projective Plane

Let $a$, $b$, $c$, $d$, $e$, $f$ be real numbers and $u$ be an element of $\mathcal{E}^3_{\rm T}$. The functor $\mathrm{qfconic}(a, b, c, d, e, f, u)$ yielding a real number is defined by the term

(Def. 1) $a \cdot u(1) \cdot u(1) + (b \cdot u(2) \cdot u(2)) + (c \cdot u(3) \cdot u(3)) + (d \cdot u(1) \cdot u(2)) + (e \cdot u(1) \cdot u(3)) + (f \cdot u(2) \cdot u(3))$.

The functor $\mathrm{conic}(a, b, c, d, e, f)$ yielding a subset of the projective space over $\mathcal{E}^3_{\rm T}$ is defined by the term

(Def. 2) $\{P$, where $P$ is a point of the projective space over $\mathcal{E}^3_{\rm T}$ : for every element $u$ of $\mathcal{E}^3_{\rm T}$ such that $u$ is not zero and $P =$ the direction of $u$ holds $\mathrm{qfconic}(a, b, c, d, e, f, u) = 0\}$.

In the sequel $a$, $b$, $c$, $d$, $e$, $f$ denote real numbers, $u$, $u_1$, $u_2$ denote non zero elements of $\mathcal{E}^3_{\rm T}$, and $P$ denotes an element of the projective space over $\mathcal{E}^3_{\rm T}$.

Now we state the propositions:

(10) Suppose the direction of $u_1 =$ the direction of $u_2$ and $\mathrm{qfconic}(a, b, c, d, e, f, u_1) = 0$. Then $\mathrm{qfconic}(a, b, c, d, e, f, u_2) = 0$.

(11) If $P =$ the direction of $u$ and $\mathrm{qfconic}(a, b, c, d, e, f, u) = 0$, then $P \in \mathrm{conic}(a, b, c, d, e, f)$. The theorem is a consequence of (10).

Let $a$, $b$, $c$, $d$, $e$, $f$ be real numbers. The functor $\mathrm{symmetric3}(a, b, c, d, e, f)$ yielding a square matrix over $\mathbb{R}_{\rm F}$ of dimension 3 is defined by the term

(Def. 3) $\langle\langle a, d, e\rangle, \langle d, b, f\rangle, \langle e, f, c\rangle\rangle$.

Now we state the propositions:

(12) symmetric3$(a, b, c, d, e, f)$ is symmetric. The theorem is a consequence of (5).

(13) Let us consider real numbers $a$, $b$, $c$, $d$, $e$, $f$, a point $u$ of $\mathcal{E}^3_{\mathrm{T}}$, and a square matrix $M$ over $\mathbb{R}$ of dimension 3. Suppose $p = u$ and $M =$ symmetric3$(a, b, c, d, e, f)$.
Then SumAll QuadraticForm$(p, M, p) =$ qfconic$(a, b, c, 2 \cdot d, 2 \cdot e, 2 \cdot f, u)$.

(14) Let us consider an invertible square matrix $N$ over $\mathbb{R}_{\mathrm{F}}$ of dimension 3, square matrices $N_1$, $M_1$, $M_2$ over $\mathbb{R}$ of dimension 3, and real numbers $a$, $b$, $c$, $d$, $e$, $f$. Suppose $N_1 = (\mathbb{R}_{\mathrm{F}} \to \mathbb{R})N$ and $M_1 =$ symmetric3$(a, b, c, \frac{d}{2}, \frac{f}{2}, \frac{e}{2})$ and $M_2 = (\mathbb{R}_{\mathrm{F}} \to \mathbb{R})((\mathbb{R} \to \mathbb{R}_{\mathrm{F}}){N_1}^{\mathrm{T}})^{\smile} \cdot M_1 \cdot (\mathbb{R}_{\mathrm{F}} \to \mathbb{R})((\mathbb{R} \to \mathbb{R}_{\mathrm{F}})N_1)^{\smile}$.
Then $(\mathbb{R} \to \mathbb{R}_{\mathrm{F}})M_2$ is symmetric.
Proof: $((\mathbb{R} \to \mathbb{R}_{\mathrm{F}}){N_1}^{\mathrm{T}})^{\mathrm{T}} = (\mathbb{R} \to \mathbb{R}_{\mathrm{F}})N_1$ by [3, (16)]. $(\mathbb{R} \to \mathbb{R}_{\mathrm{F}})M_2$ is symmetric by [3, (16)], (12), (7). □

(15) Let us consider real numbers $a_1$, $a_2$, $a_3$, $a_4$, $a_5$, $a_6$, $b_1$, $b_2$, $b_3$, $b_4$, $b_5$, $b_6$. Suppose symmetric3$(a_1, a_2, a_3, a_4, a_5, a_6) =$ symmetric3$(b_1, b_2, b_3, b_4, b_5, b_6)$. Then

(i) $a_1 = b_1$, and

(ii) $a_2 = b_2$, and

(iii) $a_3 = b_3$, and

(iv) $a_4 = b_4$, and

(v) $a_5 = b_5$, and

(vi) $a_6 = b_6$.

The theorem is a consequence of (2).

(16) Let us consider real numbers $a$, $b$, $c$, $d$, $e$, $f$, a point $P$ of the projective space over $\mathcal{E}^3_{\mathrm{T}}$, and an invertible square matrix $N$ over $\mathbb{R}_{\mathrm{F}}$ of dimension 3. Suppose it is not true that $a = 0$ and $b = 0$ and $c = 0$ and $d = 0$ and $e = 0$ and $f = 0$. Suppose that $P \in$ conic$(a, b, c, d, e, f)$. Let us consider real numbers $f_5$, $f_{12}$, $f_{19}$, $f_{20}$, $f_{21}$, $f_{23}$, $f_{22}$, square matrices $M_1$, $M_2$ over $\mathbb{R}$ of dimension 3, and a square matrix $N_1$ over $\mathbb{R}$ of dimension 3. Suppose $M_1 =$ symmetric3$(a, b, c, \frac{d}{2}, \frac{e}{2}, \frac{f}{2})$ and $N_1 = (\mathbb{R}_{\mathrm{F}} \to \mathbb{R})N$ and $M_2 = (\mathbb{R}_{\mathrm{F}} \to \mathbb{R})((\mathbb{R} \to \mathbb{R}_{\mathrm{F}}){N_1}^{\mathrm{T}})^{\smile} \cdot M_1 \cdot (\mathbb{R}_{\mathrm{F}} \to \mathbb{R})((\mathbb{R} \to \mathbb{R}_{\mathrm{F}})N_1)^{\smile}$ and $M_2 =$ symmetric3$(f_5, f_{21}, f_{23}, f_{12}, f_{19}, f_{22})$. Then

(i) it is not true that $f_5 = 0$ and $f_{21} = 0$ and $f_{23} = 0$ and $f_{12} = 0$ and $f_{22} = 0$ and $f_{19} = 0$, and

(ii) (the homography of $N)(P) \in$ conic$(f_5, f_{21}, f_{23}, 2 \cdot f_{12}, 2 \cdot f_{19}, 2 \cdot f_{22})$.

Proof: Consider $Q$ being a point of the projective space over $\mathcal{E}^3_{\mathrm{T}}$ such that $P = Q$ and for every element $u$ of $\mathcal{E}^3_{\mathrm{T}}$ such that $u$ is not zero and $Q =$ the direction of $u$ holds qfconic$(a, b, c, d, e, f, u) = 0$. Reconsider $M =$ symmetric3$(a, b, c, \frac{d}{2}, \frac{e}{2}, \frac{f}{2})$ as a square matrix over $\mathbb{R}$ of dimension 3. Consider $u_{19}$, $v_3$ being elements of $\mathcal{E}^3_{\mathrm{T}}$, $u_{17}$ being a finite sequence of elements of $\mathbb{R}_{\mathrm{F}}$, $p_{11}$ being a finite sequence of elements of $\mathbb{R}^1$ such that $P =$ the direction of $u_{19}$ and $u_{19}$ is not zero and $u_{19} = u_{17}$ and $p_{11} = N \cdot u_{17}$ and $v_3 = \mathrm{M2F}(p_{11})$ and $v_3$ is not zero and (the homography of $N)(P) =$ the direction of $v_3$. Reconsider $p_{10} = u_{19}$ as a finite sequence of elements of $\mathbb{R}$. SumAll QuadraticForm$(p_{10}, M, p_{10}) =$ qfconic$(a, b, c, 2 \cdot \frac{d}{2}, 2 \cdot \frac{e}{2}, 2 \cdot \frac{f}{2}, u_{19})$. Consider $a_8$, $b_8$, $c_{11}$, $d_4$, $e_5$, $f_{24}$, $g_2$, $h_2$, $i_2$ being elements of $\mathbb{R}_{\mathrm{F}}$ such that $N = \langle \langle a_8, b_8, c_{11} \rangle, \langle d_4, e_5, f_{24} \rangle, \langle g_2, h_2, i_2 \rangle \rangle$. Reconsider $u_{10} = u_{17}$ as a finite sequence of elements of $\mathbb{R}$. Reconsider $N_1 = (\mathbb{R}_{\mathrm{F}} \to \mathbb{R})N$ as a square matrix over $\mathbb{R}$ of dimension 3. Reconsider $M_2 = (\mathbb{R}_{\mathrm{F}} \to \mathbb{R})((\mathbb{R} \to \mathbb{R}_{\mathrm{F}})N_1{}^{\mathrm{T}})^{\smile} \cdot M \cdot (\mathbb{R}_{\mathrm{F}} \to \mathbb{R})((\mathbb{R} \to \mathbb{R}_{\mathrm{F}})N_1)^{\smile}$ as a square matrix over $\mathbb{R}$ of dimension 3. $((\mathbb{R} \to \mathbb{R}_{\mathrm{F}})N_1{}^{\mathrm{T}})^{\mathrm{T}} = (\mathbb{R} \to \mathbb{R}_{\mathrm{F}})N_1$ by [3, (16)]. $(\mathbb{R} \to \mathbb{R}_{\mathrm{F}})M_2$ is symmetric by [3, (16)], (12), (7). Consider $m_1$, $m_2$, $m_3$, $m_4$, $m_5$, $m_6$, $m_7$, $m_8$, $m_9$ being elements of $\mathbb{R}_{\mathrm{F}}$ such that $M_2 = \langle \langle m_1, m_2, m_3 \rangle, \langle m_4, m_5, m_6 \rangle, \langle m_7, m_8, m_9 \rangle \rangle$. $m_2 = m_4$ and $m_3 = m_7$ and $m_8 = m_6$. Reconsider $u_3 = N_1 \cdot u_{10}$ as an element of $\mathcal{E}^3_{\mathrm{T}}$. $u_3$ is not zero by [5, (24)], [14, (59), (86)]. Reconsider $u_2 = N_1 \cdot u_{10}$ as a non zero element of $\mathcal{E}^3_{\mathrm{T}}$. Reconsider $f_5 = m_1$, $f_{12} = m_2$, $f_{19} = m_3$, $f_{21} = m_5$, $f_{22} = m_6$, $f_{23} = m_9$ as a real number. qfconic$(f_5, f_{21}, f_{23}, 2 \cdot f_{12}, 2 \cdot f_{19}, 2 \cdot f_{22}, u_2) = 0$. It is not true that $f_5 = 0$ and $f_{21} = 0$ and $f_{23} = 0$ and $2 \cdot f_{12} = 0$ and $2 \cdot f_{22} = 0$ and $2 \cdot f_{19} = 0$. $u_2 = v_3$. For every real numbers $u_{11}$, $u_{12}$, $u_{13}$, $u_{14}$, $u_{15}$, $u_{18}$, $u_{16}$ and for every square matrices $U_1$, $U_2$ over $\mathbb{R}$ of dimension 3 and for every square matrix $U_3$ over $\mathbb{R}$ of dimension 3 such that $U_1 =$ symmetric3$(a, b, c, \frac{d}{2}, \frac{e}{2}, \frac{f}{2})$ and $U_3 = (\mathbb{R}_{\mathrm{F}} \to \mathbb{R})N$ and $U_2 = (\mathbb{R}_{\mathrm{F}} \to \mathbb{R})((\mathbb{R} \to \mathbb{R}_{\mathrm{F}})U_3{}^{\mathrm{T}})^{\smile} \cdot U_1 \cdot (\mathbb{R}_{\mathrm{F}} \to \mathbb{R})((\mathbb{R} \to \mathbb{R}_{\mathrm{F}})U_3)^{\smile}$ and $U_2 =$ symmetric3$(u_{11}, u_{15}, u_{18}, u_{12}, u_{13}, u_{16})$ holds it is not true that $u_{11} = 0$ and $u_{15} = 0$ and $u_{18} = 0$ and $u_{12} = 0$ and $u_{16} = 0$ and $u_{13} = 0$. (the homography of $N)(P) \in$ conic$(u_{11}, u_{15}, u_{18}, 2 \cdot u_{12}, 2 \cdot u_{13}, 2 \cdot u_{16})$. □

(17) Let us consider real numbers $a$, $b$, $c$, $d$, $e$, $f$, points $P_1$, $P_2$, $P_3$, $P_4$, $P_5$, $P_6$ of the projective space over $\mathcal{E}^3_{\mathrm{T}}$, and an invertible square matrix $N$ over $\mathbb{R}_{\mathrm{F}}$ of dimension 3. Suppose it is not true that $a = 0$ and $b = 0$ and $c = 0$ and $d = 0$ and $e = 0$ and $f = 0$. Suppose that $P_1$, $P_2$, $P_3$, $P_4$, $P_5$, $P_6 \in$ conic$(a, b, c, d, e, f)$. Then there exist real numbers $a_2$, $b_2$, $c_2$, $d_2$, $e_2$, $f_2$ such that

(i) it is not true that $a_2 = 0$ and $b_2 = 0$ and $c_2 = 0$ and $d_2 = 0$ and $e_2 = 0$ and $f_2 = 0$, and

(ii) (the homography of $N)(P_1)$, (the homography of $N)(P_2)$, (the homography of $N$)($P_3$), (the homography of $N$)($P_4$), (the homography of $N$)($P_5$), (the homography of $N$)($P_6$) $\in$ conic($a_2, b_2, c_2, d_2, e_2, f_2$).

The theorem is a consequence of (3), (14), (6), and (16).

From now on $a$, $b$, $c$, $d$, $e$, $f$, $g$, $h$, $i$ denote elements of $\mathbb{R}_{\mathrm{F}}$.

Now we state the proposition:

(18) (i) if qfconic($a, b, c, d, e, f, [1, 0, 0]$) $= 0$, then $a = 0$, and

(ii) if qfconic($a, b, c, d, e, f, [0, 1, 0]$) $= 0$, then $b = 0$, and

(iii) if qfconic($a, b, c, d, e, f, [0, 0, 1]$) $= 0$, then $c = 0$, and

(iv) if qfconic($0, 0, 0, d, e, f, [1, 1, 1]$) $= 0$, then $d + e + f = 0$.

## 3. Pascal's Theorem

In the sequel $M$ denotes a square matrix over $\mathbb{R}_{\mathrm{F}}$ of dimension 3, $e_1$, $e_2$, $e_3$, $f_1$, $f_2$, $f_3$ denote elements of $\mathbb{R}_{\mathrm{F}}$, $M_8$, $M_{14}$, $M_{20}$, $M_{21}$, $M_{22}$, $M_{19}$, $M_{13}$, $M_{10}$, $M_9$, $M_{12}$, $M_{16}$, $M_{17}$, $M_{11}$, $M_{15}$, $M_{18}$ denote square matrices over $\mathbb{R}_{\mathrm{F}}$ of dimension 3, and $r_1$, $r_2$ denote real numbers.

Now we state the proposition:

(19) Suppose $M_9 = \langle\langle 1, 0, 0\rangle, \langle 0, 1, 0\rangle, \langle e_1, e_2, e_3\rangle\rangle$ and $M_{12} = \langle\langle 1, 0, 0\rangle, \langle 0, 0, 1\rangle, \langle f_1, f_2, f_3\rangle\rangle$ and $M_{16} = \langle\langle 0, 1, 0\rangle, \langle 1, 1, 1\rangle, \langle f_1, f_2, f_3\rangle\rangle$ and $M_{17} = \langle\langle 0, 0, 1\rangle, \langle 1, 1, 1\rangle, \langle e_1, e_2, e_3\rangle\rangle$ and $M_{10} = \langle\langle 1, 0, 0\rangle, \langle 0, 1, 0\rangle, \langle f_1, f_2, f_3\rangle\rangle$ and $M_{11} = \langle\langle 1, 0, 0\rangle, \langle 0, 0, 1\rangle, \langle e_1, e_2, e_3\rangle\rangle$ and $M_{15} = \langle\langle 0, 1, 0\rangle, \langle 1, 1, 1\rangle, \langle e_1, e_2, e_3\rangle\rangle$ and $M_{18} = \langle\langle 0, 0, 1\rangle, \langle 1, 1, 1\rangle, \langle f_1, f_2, f_3\rangle\rangle$ and ($r_1 \neq 0$ or $r_2 \neq 0$) and $r_1 \cdot e_1 \cdot e_2 + (r_2 \cdot e_1 \cdot e_3) = r_1 + r_2 \cdot e_2 \cdot e_3$ and $r_1 \cdot f_1 \cdot f_2 + (r_2 \cdot f_1 \cdot f_3) = r_1 + r_2 \cdot f_2 \cdot f_3$. Then $\mathrm{Det}\, M_9 \cdot \mathrm{Det}\, M_{12} \cdot \mathrm{Det}\, M_{16} \cdot \mathrm{Det}\, M_{17} = \mathrm{Det}\, M_{10} \cdot \mathrm{Det}\, M_{11} \cdot \mathrm{Det}\, M_{15} \cdot \mathrm{Det}\, M_{18}$.

In the sequel $p_1$, $p_2$, $p_3$, $p_4$, $p_5$, $p_6$ denote points of $\mathcal{E}^3_{\mathrm{T}}$.

(20) Suppose $M_9 = \langle p_1, p_2, p_5\rangle$ and $M_{12} = \langle p_1, p_3, p_6\rangle$ and $M_{16} = \langle p_2, p_4, p_6\rangle$ and $M_{17} = \langle p_3, p_4, p_5\rangle$ and $M_{10} = \langle p_1, p_2, p_6\rangle$ and $M_{11} = \langle p_1, p_3, p_5\rangle$ and $M_{15} = \langle p_2, p_4, p_5\rangle$ and $M_{18} = \langle p_3, p_4, p_6\rangle$. Then

(i) $\mathrm{Det}\, M_9 = \langle |p_1, p_2, p_5|\rangle$, and

(ii) $\mathrm{Det}\, M_{12} = \langle |p_1, p_3, p_6|\rangle$, and

(iii) $\mathrm{Det}\, M_{16} = \langle |p_2, p_4, p_6|\rangle$, and

(iv) $\mathrm{Det}\, M_{17} = \langle |p_3, p_4, p_5|\rangle$, and

(v) $\mathrm{Det}\, M_{10} = \langle |p_1, p_2, p_6|\rangle$, and

(vi) $\mathrm{Det}\, M_{11} = \langle |p_1, p_3, p_5|\rangle$, and

(vii) $\mathrm{Det}\, M_{15} = \langle |p_2, p_4, p_5|\rangle$, and

(viii) $\operatorname{Det} M_{18} = \langle|p_3, p_4, p_6|\rangle$.

From now on $p_7$, $p_8$, $p_9$ denote points of $\mathcal{E}^3_{\rm T}$.

(21) Suppose $\langle|p_1, p_5, p_9|\rangle = 0$. Then $\langle|p_1, p_5, p_7|\rangle \cdot \langle|p_2, p_5, p_9|\rangle = -(\langle|p_1, p_2, p_5|\rangle \cdot \langle|p_5, p_9, p_7|\rangle)$. The theorem is a consequence of (1).

(22) Suppose $\langle|p_1, p_6, p_8|\rangle = 0$. Then $\langle|p_1, p_2, p_6|\rangle \cdot \langle|p_3, p_6, p_8|\rangle = \langle|p_1, p_3, p_6|\rangle \cdot \langle|p_2, p_6, p_8|\rangle$. The theorem is a consequence of (1).

(23) Suppose $\langle|p_2, p_4, p_9|\rangle = 0$. Then $\langle|p_2, p_4, p_5|\rangle \cdot \langle|p_2, p_9, p_7|\rangle = -(\langle|p_2, p_4, p_7|\rangle \cdot \langle|p_2, p_5, p_9|\rangle)$.

(24) Suppose $\langle|p_2, p_6, p_7|\rangle = 0$. Then $\langle|p_2, p_4, p_7|\rangle \cdot \langle|p_2, p_6, p_8|\rangle = -(\langle|p_2, p_4, p_6|\rangle \cdot \langle|p_2, p_8, p_7|\rangle)$.

(25) Suppose $\langle|p_3, p_4, p_8|\rangle = 0$. Then $\langle|p_3, p_4, p_6|\rangle \cdot \langle|p_3, p_5, p_8|\rangle = \langle|p_3, p_4, p_5|\rangle \cdot \langle|p_3, p_6, p_8|\rangle$.

(26) Suppose $\langle|p_3, p_5, p_7|\rangle = 0$. Then $\langle|p_1, p_3, p_5|\rangle \cdot \langle|p_5, p_8, p_7|\rangle = -(\langle|p_1, p_5, p_7|\rangle \cdot \langle|p_3, p_5, p_8|\rangle)$. The theorem is a consequence of (1).

(27) Let us consider non zero real numbers $r_{125}$, $r_{136}$, $r_{246}$, $r_{345}$, $r_{126}$, $r_{135}$, $r_{245}$, $r_{346}$, $r_{157}$, $r_{259}$, $r_{597}$, $r_{368}$, $r_{268}$, $r_{297}$, $r_{247}$, $r_{287}$, $r_{358}$, $r_{587}$. Suppose $r_{125} \cdot r_{136} \cdot r_{246} \cdot r_{345} = r_{126} \cdot r_{135} \cdot r_{245} \cdot r_{346}$ and $r_{157} \cdot r_{259} = -(r_{125} \cdot r_{597})$ and $r_{126} \cdot r_{368} = r_{136} \cdot r_{268}$ and $r_{245} \cdot r_{297} = -(r_{247} \cdot r_{259})$ and $r_{247} \cdot r_{268} = -(r_{246} \cdot r_{287})$ and $r_{346} \cdot r_{358} = r_{345} \cdot r_{368}$ and $r_{135} \cdot r_{587} = -(r_{157} \cdot r_{358})$. Then $r_{287} \cdot r_{597} = r_{297} \cdot r_{587}$.

(28) Suppose $p_1 = \langle 1, 0, 0\rangle$ and $p_2 = \langle 0, 1, 0\rangle$ and $p_3 = \langle 0, 0, 1\rangle$ and $p_4 = \langle 1, 1, 1\rangle$ and $p_5 = \langle e_1, e_2, e_3\rangle$ and $p_6 = \langle f_1, f_2, f_3\rangle$ and $\mathrm{qfconic}(0, 0, 0, r_1, r_2, -(r_1 + r_2), p_5) = 0$ and $\mathrm{qfconic}(0, 0, 0, r_1, r_2, -(r_1 + r_2), p_6) = 0$. Then

(i) $\mathrm{qfconic}(0, 0, 0, r_1, r_2, -(r_1 + r_2), p_1) = 0$, and

(ii) $\mathrm{qfconic}(0, 0, 0, r_1, r_2, -(r_1 + r_2), p_2) = 0$, and

(iii) $\mathrm{qfconic}(0, 0, 0, r_1, r_2, -(r_1 + r_2), p_3) = 0$, and

(iv) $\mathrm{qfconic}(0, 0, 0, r_1, r_2, -(r_1 + r_2), p_4) = 0$, and

(v) $r_1 \cdot e_1 \cdot e_2 + (r_2 \cdot e_1 \cdot e_3) = r_1 + r_2 \cdot e_2 \cdot e_3$, and

(vi) $r_1 \cdot f_1 \cdot f_2 + (r_2 \cdot f_1 \cdot f_3) = r_1 + r_2 \cdot f_2 \cdot f_3$.

(29) Suppose $p_1 = \langle 1, 0, 0\rangle$ and $p_2 = \langle 0, 1, 0\rangle$ and $p_3 = \langle 0, 0, 1\rangle$ and $p_4 = \langle 1, 1, 1\rangle$ and $p_5 = \langle e_1, e_2, e_3\rangle$ and $p_6 = \langle f_1, f_2, f_3\rangle$ and $\langle|p_1, p_2, p_5|\rangle \neq 0$ and $\langle|p_1, p_3, p_6|\rangle \neq 0$ and $\langle|p_2, p_4, p_6|\rangle \neq 0$ and $\langle|p_3, p_4, p_5|\rangle \neq 0$ and $\langle|p_1, p_2, p_6|\rangle \neq 0$ and $\langle|p_1, p_3, p_5|\rangle \neq 0$ and $\langle|p_2, p_4, p_5|\rangle \neq 0$ and $\langle|p_3, p_4, p_6|\rangle \neq 0$ and $\langle|p_1, p_5, p_7|\rangle \neq 0$ and $\langle|p_2, p_5, p_9|\rangle \neq 0$ and $\langle|p_5, p_9, p_7|\rangle \neq 0$ and $\langle|p_3, p_6, p_8|\rangle \neq 0$ and $\langle|p_2, p_6, p_8|\rangle \neq 0$ and $\langle|p_2, p_9, p_7|\rangle \neq 0$ and $\langle|p_2, p_4, p_7|\rangle \neq 0$ and $\langle|p_2, p_8, p_7|\rangle \neq 0$ and $\langle|p_3, p_5, p_8|\rangle \neq 0$ and $\langle|p_5, p_8, p_7|\rangle$

$\neq 0$ and ($r_1 \neq 0$ or $r_2 \neq 0$) and $\mathrm{qfconic}(0,0,0,r_1,r_2,-(r_1+r_2),p_5) = 0$ and $\mathrm{qfconic}(0,0,0,r_1,r_2,-(r_1+r_2),p_6) = 0$ and $\langle|p_1,p_5,p_9|\rangle = 0$ and $\langle|p_1,p_6,p_8|\rangle = 0$ and $\langle|p_2,p_4,p_9|\rangle = 0$ and $\langle|p_2,p_6,p_7|\rangle = 0$ and $\langle|p_3,p_4,p_8|\rangle = 0$ and $\langle|p_3,p_5,p_7|\rangle = 0$. Then $\langle|p_2,p_8,p_7|\rangle \cdot \langle|p_5,p_9,p_7|\rangle = \langle|p_2,p_9,p_7|\rangle \cdot \langle|p_5,p_8,p_7|\rangle$. The theorem is a consequence of (20), (28), (19), (21), (22), (23), (24), (25), (26), and (27).

(30) Suppose $\langle|p_2,p_8,p_7|\rangle \cdot \langle|p_5,p_9,p_7|\rangle = \langle|p_2,p_9,p_7|\rangle \cdot \langle|p_5,p_8,p_7|\rangle$. Then $\langle|p_7,p_2,p_5|\rangle \cdot \langle|p_7,p_8,p_9|\rangle = 0$. The theorem is a consequence of (1).

(31) Let us consider a projective space $P_{10}$ defined in terms of collinearity, and elements $c_1$, $c_2$, $c_3$, $c_4$, $c_5$, $c_6$, $c_7$, $c_8$, $c_9$ of $P_{10}$. Suppose $c_1$, $c_2$ and $c_4$ are not collinear and $c_1$, $c_2$ and $c_5$ are not collinear and $c_1$, $c_6$ and $c_4$ are not collinear and $c_1$, $c_6$ and $c_5$ are not collinear and $c_2$, $c_6$ and $c_4$ are not collinear and $c_3$, $c_4$ and $c_2$ are not collinear and $c_3$, $c_4$ and $c_6$ are not collinear and $c_3$, $c_5$ and $c_2$ are not collinear and $c_3$, $c_5$ and $c_6$ are not collinear and $c_4$, $c_5$ and $c_2$ are not collinear and $c_1$, $c_4$ and $c_7$ are collinear and $c_1$, $c_5$ and $c_8$ are collinear and $c_2$, $c_3$ and $c_7$ are collinear and $c_2$, $c_5$ and $c_9$ are collinear and $c_6$, $c_3$ and $c_8$ are collinear and $c_6$, $c_4$ and $c_9$ are collinear. Then

(i) $c_9$, $c_2$ and $c_4$ are not collinear, and

(ii) $c_1$, $c_4$ and $c_9$ are not collinear, and

(iii) $c_2$, $c_3$ and $c_9$ are not collinear, and

(iv) $c_2$, $c_4$ and $c_7$ are not collinear, and

(v) $c_2$, $c_5$ and $c_8$ are not collinear, and

(vi) $c_2$, $c_9$ and $c_8$ are not collinear, and

(vii) $c_2$, $c_9$ and $c_7$ are not collinear, and

(viii) $c_6$, $c_4$ and $c_8$ are not collinear, and

(ix) $c_6$, $c_5$ and $c_8$ are not collinear, and

(x) $c_4$, $c_9$ and $c_8$ are not collinear, and

(xi) $c_4$, $c_9$ and $c_7$ are not collinear.

PROOF: For every elements $v_{102}$, $v_{103}$, $v_{100}$, $v_{104}$ of $P_{10}$, $v_{100} = v_{104}$ or $v_{104}$, $v_{100}$ and $v_{102}$ are not collinear or $v_{104}$, $v_{100}$ and $v_{103}$ are not collinear or $v_{102}$, $v_{103}$ and $v_{104}$ are collinear by [13, (5), (3)]. For every elements $v_{102}$, $v_{104}$, $v_{100}$, $v_{103}$ of $P_{10}$, $v_{100} = v_{103}$ or $v_{103}$, $v_{100}$ and $v_{102}$ are not collinear or $v_{103}$, $v_{100}$ and $v_{104}$ are not collinear or $v_{102}$, $v_{103}$ and $v_{104}$ are collinear by [13, (5), (3)]. For every elements $v_{102}$, $v_{103}$, $v_{104}$, $v_{101}$ of $P_{10}$, $v_{104} = v_{101}$ or $v_{101}$, $v_{104}$ and $v_{102}$ are not collinear or $v_{101}$, $v_{104}$ and $v_{103}$ are not collinear or $v_{102}$, $v_{103}$ and $v_{104}$ are collinear by [13, (2), (3)]. For every elements $v_{103}$,

$v_{104}$, $v_{102}$, $v_{101}$ of $P_{10}$, $v_{102} = v_{101}$ or $v_{101}$, $v_{102}$ and $v_{103}$ are not collinear or $v_{101}$, $v_{102}$ and $v_{104}$ are not collinear or $v_{102}$, $v_{103}$ and $v_{104}$ are collinear by [13, (2), (3)]. For every elements $v_2$, $v_{101}$, $v_{100}$ of $P_{10}$, $v_{101} = v_{100}$ or $v_{100}$, $v_{101}$ and $v_2$ are not collinear or $v_2$, $v_{101}$ and $v_{100}$ are collinear by [13, (2)]. □

In the sequel $P_1$, $P_2$, $P_3$, $P_4$, $P_5$, $P_6$, $P_7$, $P_8$, $P_9$ denote points of the projective space over $\mathcal{E}^3_{\mathrm{T}}$ and $a$, $b$, $c$, $d$, $e$, $f$ denote real numbers.

Let $P_1$, $P_2$, $P_3$, $P_4$, $P_5$, $P_6$, $P_7$, $P_8$, $P_9$ be points of the projective space over $\mathcal{E}^3_{\mathrm{T}}$. We say that $P_1$, $P_2$, $P_3$, $P_4$, $P_5$, $P_6$, $P_7$, $P_8$, $P_9$ form the Pascal configuration if and only if

(Def. 4) $P_1$, $P_2$ and $P_4$ are not collinear and $P_1$, $P_3$ and $P_4$ are not collinear and $P_2$, $P_3$ and $P_4$ are not collinear and $P_1$, $P_2$ and $P_5$ are not collinear and $P_1$, $P_2$ and $P_6$ are not collinear and $P_1$, $P_3$ and $P_5$ are not collinear and $P_1$, $P_3$ and $P_6$ are not collinear and $P_2$, $P_4$ and $P_5$ are not collinear and $P_2$, $P_4$ and $P_6$ are not collinear and $P_3$, $P_4$ and $P_5$ are not collinear and $P_3$, $P_4$ and $P_6$ are not collinear and $P_2$, $P_3$ and $P_5$ are not collinear and $P_2$, $P_3$ and $P_6$ are not collinear and $P_4$, $P_5$ and $P_1$ are not collinear and $P_4$, $P_6$ and $P_1$ are not collinear and $P_5$, $P_6$ and $P_1$ are not collinear and $P_5$, $P_6$ and $P_2$ are not collinear and $P_1$, $P_5$ and $P_9$ are collinear and $P_1$, $P_6$ and $P_8$ are collinear and $P_2$, $P_4$ and $P_9$ are collinear and $P_2$, $P_6$ and $P_7$ are collinear and $P_3$, $P_4$ and $P_8$ are collinear and $P_3$, $P_5$ and $P_7$ are collinear.

Now we state the propositions:

(32) Suppose $P_1$, $P_2$, $P_3$, $P_4$, $P_5$, $P_6$, $P_7$, $P_8$, $P_9$ form the Pascal configuration. Then

(i) $P_7$, $P_2$ and $P_5$ are not collinear, and

(ii) $P_1$, $P_5$ and $P_7$ are not collinear, and

(iii) $P_2$, $P_4$ and $P_7$ are not collinear, and

(iv) $P_2$, $P_5$ and $P_9$ are not collinear, and

(v) $P_2$, $P_6$ and $P_8$ are not collinear, and

(vi) $P_2$, $P_7$ and $P_8$ are not collinear, and

(vii) $P_2$, $P_7$ and $P_9$ are not collinear, and

(viii) $P_3$, $P_5$ and $P_8$ are not collinear, and

(ix) $P_3$, $P_6$ and $P_8$ are not collinear, and

(x) $P_5$, $P_7$ and $P_8$ are not collinear, and

(xi) $P_5$, $P_7$ and $P_9$ are not collinear.

The theorem is a consequence of (31).

(33) Suppose it is not true that $a = 0$ and $b = 0$ and $c = 0$ and $d = 0$ and $e = 0$ and $f = 0$. Suppose that $\{P_1, P_2, P_3, P_4, P_5, P_6\} \subseteq \mathrm{conic}(a, b, c, d, e, f)$ and $P_1$, $P_2$ and $P_3$ are not collinear and $P_1$, $P_2$ and $P_4$ are not collinear and $P_1$, $P_3$ and $P_4$ are not collinear and $P_2$, $P_3$ and $P_4$ are not collinear and $P_7$, $P_2$ and $P_5$ are not collinear and $P_1$, $P_2$ and $P_5$ are not collinear and $P_1$, $P_2$ and $P_6$ are not collinear and $P_1$, $P_3$ and $P_5$ are not collinear and $P_1$, $P_3$ and $P_6$ are not collinear and $P_1$, $P_5$ and $P_7$ are not collinear and $P_2$, $P_4$ and $P_5$ are not collinear and $P_2$, $P_4$ and $P_6$ are not collinear and $P_2$, $P_4$ and $P_7$ are not collinear and $P_2$, $P_5$ and $P_9$ are not collinear and $P_2$, $P_6$ and $P_8$ are not collinear and $P_2$, $P_7$ and $P_8$ are not collinear and $P_2$, $P_7$ and $P_9$ are not collinear and $P_3$, $P_4$ and $P_5$ are not collinear and $P_3$, $P_4$ and $P_6$ are not collinear and $P_3$, $P_5$ and $P_8$ are not collinear and $P_3$, $P_6$ and $P_8$ are not collinear and $P_5$, $P_7$ and $P_8$ are not collinear and $P_5$, $P_7$ and $P_9$ are not collinear and $P_1$, $P_5$ and $P_9$ are collinear and $P_1$, $P_6$ and $P_8$ are collinear and $P_2$, $P_4$ and $P_9$ are collinear and $P_2$, $P_6$ and $P_7$ are collinear and $P_3$, $P_4$ and $P_8$ are collinear and $P_3$, $P_5$ and $P_7$ are collinear. Then $P_7$, $P_8$ and $P_9$ are collinear.

PROOF: Consider $N$ being an invertible square matrix over $\mathbb{R}_{\mathrm{F}}$ of dimension 3 such that (the homography of $N)(P_1) = \mathrm{Dir100}$ and (the homography of $N)(P_2) = \mathrm{Dir010}$ and (the homography of $N)(P_3) = \mathrm{Dir001}$ and (the homography of $N)(P_4) = \mathrm{Dir111}$. Consider $u_5$ being a point of $\mathcal{E}^3_{\mathrm{T}}$ such that $u_5$ is not zero and (the homography of $N)(P_5) =$ the direction of $u_5$. Reconsider $p_{51} = u_5(1)$, $p_{52} = u_5(2)$, $p_{53} = u_5(3)$ as a real number. Consider $u_6$ being a point of $\mathcal{E}^3_{\mathrm{T}}$ such that $u_6$ is not zero and (the homography of $N)(P_6) =$ the direction of $u_6$. Reconsider $p_{61} = u_6(1)$, $p_{62} = u_6(2)$, $p_{63} = u_6(3)$ as a real number. Consider $u_7$ being a point of $\mathcal{E}^3_{\mathrm{T}}$ such that $u_7$ is not zero and (the homography of $N)(P_7) =$ the direction of $u_7$. Reconsider $p_{71} = u_7(1)$, $p_{72} = u_7(2)$, $p_{73} = u_7(3)$ as a real number. Consider $u_8$ being a point of $\mathcal{E}^3_{\mathrm{T}}$ such that $u_8$ is not zero and (the homography of $N)(P_8) =$ the direction of $u_8$. Reconsider $p_{81} = u_8(1)$, $p_{82} = u_8(2)$, $p_{83} = u_8(3)$ as a real number. Consider $u_9$ being a point of $\mathcal{E}^3_{\mathrm{T}}$ such that $u_9$ is not zero and (the homography of $N)(P_9) =$ the direction of $u_9$. Reconsider $p_{91} = u_9(1)$, $p_{92} = u_9(2)$, $p_{93} = u_9(3)$ as a real number. Consider $a_2$, $b_2$, $c_2$, $d_2$, $e_2$, $f_2$ being real numbers such that it is not true that $a_2 = 0$ and $b_2 = 0$ and $c_2 = 0$ and $d_2 = 0$ and $e_2 = 0$ and $f_2 = 0$. (the homography of $N)(P_1) \in \mathrm{conic}(a_2, b_2, c_2, d_2, e_2, f_2)$ and (the homography of $N)(P_2) \in \mathrm{conic}(a_2, b_2, c_2, d_2, e_2, f_2)$ and (the homography of $N)(P_3) \in \mathrm{conic}(a_2, b_2, c_2, d_2, e_2, f_2)$ and (the homography of $N)(P_4) \in \mathrm{conic}(a_2, b_2, c_2, d_2, e_2, f_2)$ and (the homography of $N)(P_5) \in \mathrm{conic}(a_2, b_2, c_2, d_2, e_2, f_2)$ and (the homography of $N)(P_6) \in \mathrm{conic}(a_2, b_2, c_2, d_2, e_2, f_2)$. Consider $P$ being a point of the projective space over $\mathcal{E}^3_{\mathrm{T}}$ such that the direction of $[1, 0, 0] = P$ and for every element $u$ of $\mathcal{E}^3_{\mathrm{T}}$ such that $u$ is not zero and $P =$ the direction of $u$ holds qfconic$(a_2, b_2, c_2, d_2, e_2, f_2, u) = 0$. qfconic$(a_2, b_2, c_2, d_2, e_2, f_2, [1, 0, 0]) = 0$ and qfconic$(a_2, b_2, c_2, d_2, e_2, f_2, [0, 1, 0]) = 0$ and qfconic$(a_2, b_2, c_2, d_2, e_2, f_2, [0, 0, 1]) = 0$ and qfconic$(a_2, b_2, c_2, d_2, e_2, f_2, [1, 1, 1]) = 0$ and qfconic$(a_2, b_2, c_2, d_2, e_2, f_2, [p_{51}, p_{52}, p_{53}]) = 0$ and qfconic$(a_2, b_2, c_2, d_2, e_2, f_2, [p_{61}, p_{62}, p_{63}]) = 0$ by [4, (10)], [8, (3)]. Reconsider $a_7 = a_2$, $b_7 = b_2$, $c_{10} = c_2$, $d_3 = d_2$, $e_4 = e_2$, $f_4 = f_2$ as an element of $\mathbb{R}_{\mathrm{F}}$. $a_7 = 0$ and $b_7 = 0$ and $c_{10} = 0$. $a_7 = 0$ and $b_7 = 0$ and $c_{10} = 0$ and $d_3 + e_4 + f_4 = 0$. Reconsider $p_2 = \langle 0, 1, 0\rangle$, $p_5 = \langle p_{51}, p_{52}, p_{53}\rangle$, $p_7 = \langle p_{71}, p_{72}, p_{73}\rangle$, $p_8 = \langle p_{81}, p_{82}, p_{83}\rangle$, $p_9 = \langle p_{91}, p_{92}, p_{93}\rangle$ as a point of $\mathcal{E}^3_{\mathrm{T}}$. $\langle|p_7, p_2, p_5|\rangle \neq 0$ by [3, (102)], [8, (3)], [3, (43)], [4, (10)]. $\langle|p_2, p_8, p_7|\rangle \cdot \langle|p_5, p_9, p_7|\rangle = \langle|p_2, p_9, p_7|\rangle \cdot \langle|p_5, p_8, p_7|\rangle$. $\langle|p_7, p_2, p_5|\rangle \cdot \langle|p_7, p_8, p_9|\rangle = 0$. □

(34) Suppose it is not true that $a = 0$ and $b = 0$ and $c = 0$ and $d = 0$ and $e = 0$ and $f = 0$. Suppose that $\{P_1, P_2, P_3, P_4, P_5, P_6\} \subseteq$ conic$(a, b, c, d, e, f)$ and $P_1$, $P_2$ and $P_3$ are not collinear and $P_1$, $P_2$, $P_3$, $P_4$, $P_5$, $P_6$, $P_7$, $P_8$, $P_9$ form the Pascal configuration. Then $P_7$, $P_8$ and $P_9$ are collinear. The theorem is a consequence of (32) and (33).

Note that $\mathcal{E}^3_{\mathrm{T}}$ is up 3-dimensional.

(35) Suppose it is not true that $a = 0$ and $b = 0$ and $c = 0$ and $d = 0$ and $e = 0$ and $f = 0$. Suppose that $\{P_1, P_2, P_3, P_4, P_5, P_6\} \subseteq$ conic$(a, b, c, d, e, f)$ and $P_1$, $P_2$ and $P_3$ are collinear and $P_1$, $P_2$, $P_3$, $P_4$, $P_5$, $P_6$, $P_7$, $P_8$, $P_9$ form the Pascal configuration. Then $P_7$, $P_8$ and $P_9$ are collinear.

PROOF: Consider $N$ being an invertible square matrix over $\mathbb{R}_{\mathrm{F}}$ of dimension 3 such that (the homography of $N$)$(P_1) =$ Dir100 and (the homography of $N$)$(P_2) =$ Dir010 and (the homography of $N$)$(P_4) =$ Dir001 and (the homography of $N$)$(P_5) =$ Dir111. Consider $u_3$ being a point of $\mathcal{E}^3_{\mathrm{T}}$ such that $u_3$ is not zero and (the homography of $N$)$(P_3) =$ the direction of $u_3$. Reconsider $p_{31} = u_3(1)$, $p_{32} = u_3(2)$, $p_{33} = u_3(3)$ as a real number. Consider $u_6$ being a point of $\mathcal{E}^3_{\mathrm{T}}$ such that $u_6$ is not zero and (the homography of $N$)$(P_6) =$ the direction of $u_6$. Reconsider $p_{61} = u_6(1)$, $p_{62} = u_6(2)$, $p_{63} = u_6(3)$ as a real number. Consider $a_2$, $b_2$, $c_2$, $d_2$, $e_2$, $f_2$ being real numbers such that it is not true that $a_2 = 0$ and $b_2 = 0$ and $c_2 = 0$ and $d_2 = 0$ and $e_2 = 0$ and $f_2 = 0$ and (the homography of $N$)$(P_1) \in$ conic$(a_2, b_2, c_2, d_2, e_2, f_2)$ and (the homography of $N$)$(P_2) \in$ conic$(a_2, b_2, c_2, d_2, e_2, f_2)$ and (the homography of $N$)$(P_3) \in$ conic$(a_2, b_2, c_2, d_2, e_2, f_2)$ and (the homography of $N$)$(P_4) \in$ conic$(a_2, b_2, c_2, d_2, e_2, f_2)$ and (the homography of $N$)$(P_5) \in$ conic$(a_2, b_2, c_2, d_2, e_2, f_2)$ and (the homography of $N$)$(P_6) \in$ conic$(a_2, b_2, c_2, d_2, e_2, f_2)$. Consider $P$ being a point of the projective space over $\mathcal{E}^3_{\mathrm{T}}$ such that the direction of $[1, 0, 0] = P$ and for every element $u$ of $\mathcal{E}^3_{\mathrm{T}}$ such that $u$ is not zero and $P =$ the direction of $u$ holds qfconic$(a_2, b_2, c_2, d_2, e_2, f_2, u) = 0$. qfconic$(a_2, b_2, c_2, d_2, e_2, f_2, [1, 0, 0]) = 0$ and qfconic$(a_2, b_2, c_2, d_2, e_2, f_2, [0, 1, 0]) = 0$ and qfconic$(a_2, b_2, c_2, d_2, e_2, f_2, [0, 0, 1]) = 0$ and qfconic$(a_2, b_2, c_2, d_2, e_2, f_2, [1, 1, 1]) = 0$ and qfconic$(a_2, b_2, c_2, d_2, e_2, f_2, [p_{31}, p_{32}, p_{33}]) = 0$ and qfconic$(a_2, b_2, c_2, d_2, e_2, f_2, [p_{61}, p_{62}, p_{63}]) = 0$ by [4, (10)], [8, (3)]. Reconsider $a_7 = a_2$, $b_7 = b_2$, $c_{10} = c_2$, $d_3 = d_2$, $e_4 = e_2$, $f_4 = f_2$ as an element of $\mathbb{R}_{\mathrm{F}}$. $a_7 = 0$ and $b_7 = 0$ and $c_{10} = 0$. $a_7 = 0$ and $b_7 = 0$ and $c_{10} = 0$ and $d_3 + e_4 + f_4 = 0$. Reconsider $p_1 = \langle 1, 0, 0\rangle$, $p_2 = \langle 0, 1, 0\rangle$, $p_3 = \langle p_{31}, p_{32}, p_{33}\rangle$ as a point of $\mathcal{E}^3_{\mathrm{T}}$. $\langle |p_1, p_2, p_3|\rangle = 0$ by [3, (102)], [10, (23)], [9, (25)], [4, (10)]. $p_{31} \neq 0$ and $p_{32} \neq 0$ by [8, (2), (8), (4)]. □

(36) Pascal's theorem:
Suppose it is not true that $a = 0$ and $b = 0$ and $c = 0$ and $d = 0$ and $e = 0$ and $f = 0$. Suppose that $\{P_1, P_2, P_3, P_4, P_5, P_6\} \subseteq$ conic$(a, b, c, d, e, f)$ and $P_1$, $P_2$, $P_3$, $P_4$, $P_5$, $P_6$, $P_7$, $P_8$, $P_9$ form the Pascal configuration. Then $P_7$, $P_8$ and $P_9$ are collinear. The theorem is a consequence of (35) and (34).

## References


[1] Jesse Alama. Escape to Mizar for ATPs. *arXiv preprint arXiv:1204.6615*, 2012.

[2] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, Karol Pąk, and Josef Urban. Mizar: State-of-the-art and beyond. In Manfred Kerber, Jacques Carette, Cezary Kaliszyk, Florian Rabe, and Volker Sorge, editors, *Intelligent Computer Mathematics*, volume 9150 of *Lecture Notes in Computer Science*, pages 261–279. Springer International Publishing, 2015. ISBN 978-3-319-20614-1. doi:10.1007/978-3-319-20615-8_17.

[3] Roland Coghetto. Homography in $\mathbb{RP}^2$. *Formalized Mathematics*, 24(**4**):239–251, 2016. doi:10.1515/forma-2016-0020.

[4] Roland Coghetto. Group of homography in real projective plane. *Formalized Mathematics*, 25(**1**):55–62, 2017. doi:10.1515/forma-2017-0005.

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

[6] Adam Grabowski. Solving two problems in general topology via types. In *Types for Proofs and Programs, International Workshop, TYPES 2004, Jouy-en-Josas, France, December 15-18, 2004, Revised Selected Papers*, pages 138–153, 2004. doi:10.1007/11617990_9.

[7] Adam Grabowski. Mechanizing complemented lattices within Mizar system. *Journal of Automated Reasoning*, 55:211–221, 2015. doi:10.1007/s10817-015-9333-5.

[8] Kanchun, Hiroshi Yamazaki, and Yatsuka Nakamura. Cross products and tripple vector products in 3-dimensional Euclidean space. *Formalized Mathematics*, 11(**4**):381–383, 2003.

[9] Wojciech Leończuk and Krzysztof Prażmowski. A construction of analytical projective space. *Formalized Mathematics*, 1(**4**):761–766, 1990.

[10] Wojciech Leończuk and Krzysztof Prażmowski. Projective spaces – part I. *Formalized Mathematics*, 1(**4**):767–776, 1990.

[11] Jürgen Richter-Gebert. *Pappos's Theorem: Nine Proofs and Three Variations*, pages 3–31. Springer Berlin Heidelberg, 2011. ISBN 978-3-642-17286-1. doi:10.1007/978-3-642-17286-1_1.

[12] Piotr Rudnicki and Josef Urban. Escape to ATP for Mizar. In *First International Workshop on Proof eXchange for Theorem Proving-PxTP 2011*, 2011.

[13] Wojciech Skaba. The collinearity structure. *Formalized Mathematics*, 1(**4**):657–659, 1990.

[14] Nobuyuki Tamura and Yatsuka Nakamura. Determinant and inverse of matrices of real elements. *Formalized Mathematics*, 15(**3**):127–136, 2007. doi:10.2478/v10037-007-0014-7.

*Received June 27, 2017*

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

FORMALIZED MATHEMATICS
Vol. 25, No. 2, Pages 121–139, 2017
DOI: 10.1515/forma-2017-0012

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

# About Quotient Orders and Ordering Sequences

Sebastian Koch[1]
Johannes Gutenberg University
Mainz, Germany

**Summary.** In preparation for the formalization in Mizar [4] of lotteries as given in [14], this article closes some gaps in the Mizar Mathematical Library (MML) regarding relational structures. The quotient order is introduced by the equivalence relation identifying two elements $x, y$ of a preorder as equivalent if $x \leqslant y$ and $y \leqslant x$. This concept is known (see e.g. chapter 5 of [19]) and was first introduced into the MML in [13] and that work is incorporated here. Furthermore given a set $A$, partition $D$ of $A$ and a finite-support function $f : A \to \mathbb{R}$, a function $\Sigma_f : D \to \mathbb{R}, \Sigma_f(X) = \sum_{x \in X} f(x)$ can be defined as some kind of natural "restriction" from $f$ to $D$. The first main result of this article can then be formulated as:

$$\sum_{x \in A} f(x) = \sum_{X \in D} \Sigma_f(X) \left( = \sum_{X \in D} \sum_{x \in X} f(x) \right)$$

After that (weakly) ascending/descending finite sequences (based on [3]) are introduced, in analogous notation to their infinite counterparts introduced in [18] and [13].

The second main result is that any finite subset of any transitive connected relational structure can be sorted as a ascending or descending finite sequence, thus generalizing the results from [16], where finite sequence of real numbers were sorted.

The third main result of the article is that any weakly ascending/weakly descending finite sequence on elements of a preorder induces a weakly ascending/weakly descending finite sequence on the projection of these elements into the quotient order. Furthermore, weakly ascending finite sequences can be interpreted as directed walks in a directed graph, when the set of edges is described by ordered pairs of vertices, which is quite common (see e.g. [10]).

[1] mailto: skoch02@students.uni-mainz.de




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

Additionally, some auxiliary theorems are provided, e.g. two schemes to find the smallest or the largest element in a finite subset of a connected transitive relational structure with a given property and a lemma I found rather useful: Given two finite one-to-one sequences $s, t$ on a set $X$, such that $\operatorname{rng} t \subseteq \operatorname{rng} s$, and a function $f : X \to \mathbb{R}$ such that $f$ is zero for every $x \in \operatorname{rng} s \setminus \operatorname{rng} t$, we have $\sum f \circ s = \sum f \circ t$.

MSC: 06A05 03B35

Keywords: quotient order; ordered finite sequences

MML identifier: `ORDERS_5`, version: `8.1.06 5.43.1297`

## 1. Preliminaries

Now we state the proposition:

(1) Let us consider sets $A$, $B$, and an object $x$. If $A = B \setminus \{x\}$ and $x \in B$, then $B \setminus A = \{x\}$.

Let $Y$ be a set and $X$ be a subset of $Y$. One can verify that every binary relation which is $X$-defined is also $Y$-defined.

Now we state the propositions:

(2) Let us consider a set $X$, and an object $x$. If $x \in X$ and $\overline{\overline{X}} = 1$, then $\{x\} = X$.

(3) Let us consider a set $X$, and a natural number $k$. Suppose $X \subseteq \operatorname{Seg} k$. Then $\operatorname{rng} \operatorname{Sgm} X \subseteq \operatorname{Seg} k$.

Let $s$ be a finite sequence and $N$ be a subset of $\operatorname{dom} s$. Observe that $s \cdot \operatorname{Sgm} N$ is finite sequence-like.

Let $A$ be a set, $B$ be a subset of $A$, $C$ be a non empty set, $f$ be a finite sequence of elements of $B$, and $g$ be a function from $A$ into $C$. Let us observe that $g \cdot f$ is finite sequence-like.

Let $s$ be a finite sequence. Let us observe that $s \cdot \operatorname{idseq}(\operatorname{len} s)$ is finite sequence-like.

One can verify that $\operatorname{Rev}(\operatorname{Rev}(s))$ reduces to $s$.

Let $X$ be a set. Note that there exists a subset of $X$ which is finite.

The scheme *Finite2* deals with a set $\mathcal{A}$ and a subset $\mathcal{B}$ of $\mathcal{A}$ and a unary predicate $\mathcal{P}$ and states that

(Sch. 1) $\mathcal{P}[\mathcal{A}]$

provided

- $\mathcal{A}$ is finite and
- $\mathcal{P}[\mathcal{B}]$ and

- for every sets $x$, $C$ such that $x \in \mathcal{A} \setminus \mathcal{B}$ and $\mathcal{B} \subseteq C \subseteq \mathcal{A}$ and $\mathcal{P}[C]$ holds $\mathcal{P}[C \cup \{x\}]$.

Let $A$ be an empty set. One can check that every partition of $A$ is empty and there exists a partition of $A$ which is empty.

Let $S$, $T$ be 1-sorted structures, $f$ be a function from $S$ into $T$, and $B$ be a subset of $S$. Let us observe that the functor $f^{\circ}B$ yields a subset of $T$. Now we state the proposition:

(4) Let us consider a set $X$, an order $R$ in $X$, a finite subset $B$ of $X$, and an object $x$. If $B = \{x\}$, then $\mathrm{SgmX}(R, B) = \langle x \rangle$.
PROOF: Set $f = \langle x \rangle$. For every natural numbers $n$, $m$ such that $n, m \in \mathrm{dom}\, f$ and $n < m$ holds $f_n \neq f_m$ and $\langle f_n, f_m \rangle \in R$ by [3, (38), (2)]. □

Let us consider a finite sequence $s$ of elements of $\mathbb{R}$. Now we state the propositions:

(5) If $\sum s \neq 0$, then there exists a natural number $i$ such that $i \in \mathrm{dom}\, s$ and $s(i) \neq 0$.

(6) If $s$ is non-negative yielding and there exists a natural number $i$ such that $i \in \mathrm{dom}\, s$ and $s(i) \neq 0$, then $\sum s > 0$.
PROOF: Consider $i$ being a natural number such that $i \in \mathrm{dom}\, s$ and $s(i) \neq 0$. Set $s_1 = s$. For every natural number $j$ such that $j \in \mathrm{dom}\, s_1$ holds $0 \leqslant s_1(j)$ by [6, (3)]. There exists a natural number $k$ such that $k \in \mathrm{dom}\, s_1$ and $0 < s_1(k)$ by [6, (3)]. □

(7) If $s$ is non-positive yielding and there exists a natural number $i$ such that $i \in \mathrm{dom}\, s$ and $s(i) \neq 0$, then $\sum s < 0$.
PROOF: Reconsider $s_1 = -s$ as a finite sequence of elements of $\mathbb{R}$. There exists a natural number $i$ such that $i \in \mathrm{dom}\, s_1$ and $s_1(i) \neq 0$ by [12, (58)]. $\sum s_1 > 0$. □

(8) Let us consider a set $X$, finite sequences $s$, $t$ of elements of $X$, and a function $f$ from $X$ into $\mathbb{R}$. Suppose $s$ is one-to-one and $t$ is one-to-one and $\mathrm{rng}\, t \subseteq \mathrm{rng}\, s$ and for every element $x$ of $X$ such that $x \in \mathrm{rng}\, s \setminus \mathrm{rng}\, t$ holds $f(x) = 0$. Then $\sum(f \cdot s) = \sum(f \cdot t)$.
PROOF: Define $\mathcal{P}[\text{set}] \equiv$ there exists a finite sequence $r$ of elements of $X$ such that $r$ is one-to-one and $\mathrm{rng}\, t \subseteq \mathrm{rng}\, r$ and $\mathrm{rng}\, r = \$_1$ and $\sum(f \cdot r) = \sum(f \cdot t)$. Reconsider $r_1 = \mathrm{rng}\, t$ as a subset of $\mathrm{rng}\, s$. For every sets $x$, $C$ such that $x \in \mathrm{rng}\, s \setminus r_1$ and $r_1 \subseteq C \subseteq \mathrm{rng}\, s$ and $\mathcal{P}[C]$ holds $\mathcal{P}[C \cup \{x\}]$ by [9, (40)], [3, (38), (31)], [9, (31)]. $\mathcal{P}[\mathrm{rng}\, s]$ from *Finite2*. Consider $r$ being a finite sequence of elements of $X$ such that $r$ is one-to-one and $\mathrm{rng}\, t \subseteq \mathrm{rng}\, r$ and $\mathrm{rng}\, r = \mathrm{rng}\, s$ and $\sum(f \cdot r) = \sum(f \cdot t)$. Define $\mathcal{Q}[\text{object}, \text{object}] \equiv r(\$_1) = s(\$_2)$. For every object $i$ such that $i \in \mathrm{dom}\, r$ there exists an object $j$ such that $j \in \mathrm{dom}\, s$ and $\mathcal{Q}[i, j]$ by [6, (3)]. Consider $p$ being a function

from $\operatorname{dom} r$ into $\operatorname{dom} s$ such that for every object $x$ such that $x \in \operatorname{dom} r$ holds $\mathcal{Q}[x, p(x)]$ from [7, Sch. 1]. $p$ is a permutation of $\operatorname{dom} r$ by [21, (63)]. For every object $i$, $i \in \operatorname{dom} r$ iff $i \in \operatorname{dom} p$ and $p(i) \in \operatorname{dom} s$ by [6, (3)]. For every object $x$, $x \in \operatorname{dom}(f \cdot s)$ iff $x \in \operatorname{dom} s$ by [6, (11), (3)]. $\square$

Let $X$ be a set, $f$ be a function, and $g$ be a positive yielding function from $X$ into $\mathbb{R}$. Let us observe that $g \cdot f$ is positive yielding.

Let $g$ be a negative yielding function from $X$ into $\mathbb{R}$. Note that $g \cdot f$ is negative yielding.

Let $g$ be a non-positive yielding function from $X$ into $\mathbb{R}$. Let us observe that $g \cdot f$ is non-positive yielding.

Let $g$ be a non-negative yielding function from $X$ into $\mathbb{R}$. Note that $g \cdot f$ is non-negative yielding.

Let $s$ be a function. Note that the functor support $s$ yields a subset of $\operatorname{dom} s$. Let $X$ be a set. Let us observe that there exists a function from $X$ into $\mathbb{R}$ which is finite-support and non-negative yielding and there exists a function from $X$ into $\mathbb{C}$ which is non-negative yielding and finite-support.

Now we state the proposition:

(9) Let us consider a set $A$, and a function $f$ from $A$ into $\mathbb{C}$. Then support $f =$ support$(-f)$.

PROOF: For every object $x$, $x \in$ support $f$ iff $x \in$ support$(-f)$ by [15, (5), (66)]. $\square$

Let $A$ be a set and $f$ be a finite-support function from $A$ into $\mathbb{C}$. Observe that $-f$ is finite-support.

Let $f$ be a finite-support function from $A$ into $\mathbb{R}$. One can verify that $-f$ is finite-support.

## 2. Orders

Let us consider a set $X$, a binary relation $R$, and a subset $Y$ of $X$. Now we state the propositions:

(10) If $R$ is irreflexive in $X$, then $R$ is irreflexive in $Y$.

(11) If $R$ is symmetric in $X$, then $R$ is symmetric in $Y$.

(12) If $R$ is asymmetric in $X$, then $R$ is asymmetric in $Y$.

Let $A$ be a relational structure. We say that $A$ is connected if and only if

(Def. 1) the internal relation of $A$ is connected in the carrier of $A$.

We say that $A$ is strongly connected if and only if

(Def. 2) the internal relation of $A$ is strongly connected in the carrier of $A$.

Let us note that there exists a relational structure which is non empty, reflexive, transitive, antisymmetric, connected, strongly connected, strict, and total and every relational structure which is strongly connected is also reflexive and connected and every relational structure which is reflexive and connected is also strongly connected and every relational structure which is empty is also reflexive, antisymmetric, transitive, connected, and strongly connected.

Let $A$ be a relational structure and $a_1$, $a_2$ be elements of $A$. We say that $a_1 \approx a_2$ if and only if

(Def. 3) $a_1 \leqslant a_2 \leqslant a_1$.

Now we state the proposition:

(13) Let us consider a reflexive, non empty relational structure $A$, and an element $a$ of $A$. Then $a \approx a$.

Let $A$ be a reflexive, non empty relational structure and $a_1$, $a_2$ be elements of $A$. One can verify that the predicate $a_1 \approx a_2$ is reflexive.

Let $A$ be a relational structure. We say that $a_1 \lnapprox a_2$ if and only if

(Def. 4) $a_1 \leqslant a_2$ and $a_2 \nleqslant a_1$.

Observe that the predicate is irreflexive.

We introduce the notation $a_2 \gnapprox a_1$ as a synonym of $a_1 \lnapprox a_2$.

Let $A$ be a connected relational structure. One can verify that the predicate $a_1 \lnapprox a_2$ is asymmetric.

Now we state the propositions:

(14) Let us consider a non empty relational structure $A$, and elements $a_1$, $a_2$ of $A$. Suppose $A$ is strongly connected. Then

(i) $a_1 \lnapprox a_2$, or

(ii) $a_1 \approx a_2$, or

(iii) $a_1 \gnapprox a_2$.

(15) Let us consider a transitive relational structure $A$, and elements $a_1$, $a_2$, $a_3$ of $A$. Then

(i) if $a_1 \lnapprox a_2$ and $a_2 \leqslant a_3$, then $a_1 \lnapprox a_3$, and

(ii) if $a_1 \leqslant a_2$ and $a_2 \lnapprox a_3$, then $a_1 \lnapprox a_3$.

(16) Let us consider a non empty relational structure $A$, and elements $a_1$, $a_2$ of $A$. If $A$ is strongly connected, then $a_1 \leqslant a_2$ or $a_2 \leqslant a_1$.

(17) Let us consider a non empty relational structure $A$, a subset $B$ of $A$, and elements $a_1$, $a_2$ of $A$. Suppose the internal relation of $A$ is connected in $B$ and $a_1$, $a_2 \in B$ and $a_1 \neq a_2$. Then

(i) $a_1 \leqslant a_2$, or

(ii) $a_2 \leqslant a_1$.

Let us consider a non empty relational structure $A$ and elements $a_1$, $a_2$ of $A$. Now we state the propositions:

(18) If $A$ is connected and $a_1 \neq a_2$, then $a_1 \leqslant a_2$ or $a_2 \leqslant a_1$.

(19) If $A$ is strongly connected, then $a_1 = a_2$ or $a_1 < a_2$ or $a_2 < a_1$. The theorem is a consequence of (16).

Let us consider a relational structure $A$ and elements $a_1$, $a_2$ of $A$. Now we state the propositions:

(20) If $a_1 \leqslant a_2$, then $a_1, a_2 \in$ the carrier of $A$.

(21) If $a_1 \leqslant a_2$, then $A$ is not empty.

(22) Let us consider a transitive relational structure $A$, and a finite subset $B$ of $A$. Suppose $B$ is not empty and the internal relation of $A$ is connected in $B$. Then there exists an element $x$ of $A$ such that

(i) $x \in B$, and

(ii) for every element $y$ of $A$ such that $y \in B$ and $x \neq y$ holds $x \leqslant y$.

PROOF: Define $\mathcal{P}[\text{set}] \equiv$ if $\$_1$ is not empty, then there exists an element $x$ of $A$ such that $x \in \$_1$ and for every element $y$ of $A$ such that $y \in \$_1$ and $x \neq y$ holds $x \leqslant y$. For every sets $z$, $C$ such that $z \in B$ and $C \subseteq B$ and $\mathcal{P}[C]$ holds $\mathcal{P}[C \cup \{z\}]$ by [9, (31)], (17), [9, (136)], [22, (3)]. $\mathcal{P}[B]$ from [11, Sch. 2]. $\square$

(23) Let us consider a connected, transitive relational structure $A$, and a finite subset $B$ of $A$. Suppose $B$ is not empty. Then there exists an element $x$ of $A$ such that

(i) $x \in B$, and

(ii) for every element $y$ of $A$ such that $y \in B$ and $x \neq y$ holds $x \leqslant y$.

The theorem is a consequence of (22).

(24) Let us consider a transitive relational structure $A$, and a finite subset $B$ of $A$. Suppose $B$ is not empty and the internal relation of $A$ is connected in $B$. Then there exists an element $x$ of $A$ such that

(i) $x \in B$, and

(ii) for every element $y$ of $A$ such that $y \in B$ and $x \neq y$ holds $y \leqslant x$.

PROOF: Define $\mathcal{P}[\text{set}] \equiv$ if $\$_1$ is not empty, then there exists an element $x$ of $A$ such that $x \in \$_1$ and for every element $y$ of $A$ such that $y \in \$_1$ and $x \neq y$ holds $y \leqslant x$. For every sets $z$, $C$ such that $z \in B$ and $C \subseteq B$ and $\mathcal{P}[C]$ holds $\mathcal{P}[C \cup \{z\}]$ by [9, (31)], (17), [9, (136)], [22, (3)]. $\mathcal{P}[B]$ from [11, Sch. 2]. $\square$

(25) Let us consider a connected, transitive relational structure $A$, and a finite subset $B$ of $A$. Suppose $B$ is not empty. Then there exists an element $x$ of $A$ such that

(i) $x \in B$, and

(ii) for every element $y$ of $A$ such that $y \in B$ and $x \neq y$ holds $y \leqslant x$.

The theorem is a consequence of (24).

A preorder is a reflexive, transitive relational structure.

A linear preorder is a strongly connected, transitive relational structure.

An order is a reflexive, antisymmetric, transitive relational structure.

A linear order is a strongly connected, antisymmetric, transitive relational structure. Let us observe that every preorder is quasi-ordered and there exists a linear order which is empty.

Now we state the propositions:

(26) Let us consider a preorder $A$. Then the internal relation of $A$ quasi-orders the carrier of $A$.

(27) Let us consider an order $A$. Then the internal relation of $A$ partially orders the carrier of $A$.

(28) Let us consider a linear order $A$. Then the internal relation of $A$ linearly orders the carrier of $A$.

Let us consider a relational structure $A$. Now we state the propositions:

(29) If the internal relation of $A$ quasi-orders the carrier of $A$, then $A$ is reflexive and transitive.

(30) If the internal relation of $A$ partially orders the carrier of $A$, then $A$ is reflexive, transitive, and antisymmetric.

(31) If the internal relation of $A$ linearly orders the carrier of $A$, then $A$ is reflexive, transitive, antisymmetric, and connected.

The scheme *RelStrMin* deals with a transitive, connected relational structure $\mathcal{A}$ and a finite subset $\mathcal{B}$ of $\mathcal{A}$ and a unary predicate $\mathcal{P}$ and states that

(Sch. 2) There exists an element $x$ of $\mathcal{A}$ such that $x \in \mathcal{B}$ and $\mathcal{P}[x]$ and for every element $y$ of $\mathcal{A}$ such that $y \in \mathcal{B}$ and $y \lnsim x$ holds $\mathcal{P}[y]$

provided

- there exists an element $x$ of $\mathcal{A}$ such that $x \in \mathcal{B}$ and $\mathcal{P}[x]$.

The scheme *RelStrMax* deals with a transitive, connected relational structure $\mathcal{A}$ and a finite subset $\mathcal{B}$ of $\mathcal{A}$ and a unary predicate $\mathcal{P}$ and states that

(Sch. 3) There exists an element $x$ of $\mathcal{A}$ such that $x \in \mathcal{B}$ and $\mathcal{P}[x]$ and for every element $y$ of $\mathcal{A}$ such that $y \in \mathcal{B}$ and $x \lnsim y$ holds $\mathcal{P}[y]$

provided

- there exists an element $x$ of $\mathcal{A}$ such that $x \in \mathcal{B}$ and $\mathcal{P}[x]$.

## 3. Quotient Order

Let $A$ be a set and $D$ be a partition of $A$. The functor EqRelOf$(D)$ yielding an equivalence relation of $A$ is defined by

(Def. 5) $D = \text{Classes}\, it$.

Let $A$ be a preorder. The functor EqRelOf$(A)$ yielding an equivalence relation of the carrier of $A$ is defined by

(Def. 6) for every elements $x$, $y$ of $A$, $\langle x, y\rangle \in it$ iff $x \leqslant y \leqslant x$.

Now we state the proposition:

(32) Let us consider a preorder $A$. Then $\text{EqRelOf}(A) = \text{EqRel}(A)$.

Let $A$ be an empty preorder. Let us note that EqRelOf$(A)$ is empty.

Let $A$ be a non empty preorder. Observe that EqRelOf$(A)$ is non empty.

Now we state the proposition:

(33) Let us consider an order $A$. Then $\text{EqRelOf}(A) = \text{id}_\alpha$, where $\alpha$ is the carrier of $A$.

Let $A$ be a preorder. The functor QuotientOrder$(A)$ yielding a strict relational structure is defined by

(Def. 7) the carrier of $it$ = Classes(EqRelOf$(A)$) and for every elements $X$, $Y$ of Classes(EqRelOf$(A)$), $\langle X, Y\rangle \in$ the internal relation of $it$ iff there exist elements $x$, $y$ of $A$ such that $X = [x]_{\text{EqRelOf}(A)}$ and $Y = [y]_{\text{EqRelOf}(A)}$ and $x \leqslant y$.

Let $A$ be an empty preorder. Observe that QuotientOrder$(A)$ is empty.

Now we state the proposition:

(34) Let us consider a non empty preorder $A$, and an element $x$ of $A$. Then $[x]_{\text{EqRelOf}(A)} \in$ the carrier of QuotientOrder$(A)$.

Let $A$ be a non empty preorder. One can verify that QuotientOrder$(A)$ is non empty.

Now we state the proposition:

(35) Let us consider a preorder $A$. Then the internal relation of QuotientOrder$(A) = \leqslant_E A$. The theorem is a consequence of (32).

Let $A$ be a preorder. Observe that QuotientOrder$(A)$ is reflexive, total, antisymmetric, and transitive.

Let $A$ be a linear preorder. Let us note that QuotientOrder$(A)$ is connected and strongly connected.

Let $A$ be a preorder. The functor the projection onto $A$ yielding a function from $A$ into QuotientOrder($A$) is defined by

(Def. 8) for every element $x$ of $A$, $it(x) = [x]_{\mathrm{EqRelOf}(A)}$.

Let $A$ be an empty preorder. One can check that the projection onto $A$ is empty.

Let $A$ be a non empty preorder. Note that the projection onto $A$ is non empty.

Now we state the propositions:

(36) Let us consider a non empty preorder $A$, and elements $x$, $y$ of $A$. Suppose $x \leqslant y$. Then (the projection onto $A$)($x$) $\leqslant$ (the projection onto $A$)($y$).

(37) Let us consider a preorder $A$, and elements $x$, $y$ of $A$. Suppose $x \approx y$. Then (the projection onto $A$)($x$) $=$ (the projection onto $A$)($y$). The theorem is a consequence of (20).

Let $A$ be a preorder and $R$ be an equivalence relation of the carrier of $A$. We say that $R$ is EqRelOf-like if and only if

(Def. 9) $R = \mathrm{EqRelOf}(A)$.

Let us note that EqRelOf($A$) is EqRelOf-like and there exists an equivalence relation of the carrier of $A$ which is EqRelOf-like.

Let $R$ be an EqRelOf-like equivalence relation of the carrier of $A$ and $x$ be an element of $A$. One can check that the functor $[x]_R$ yields an element of QuotientOrder($A$). Now we state the propositions:

(38) Let us consider a preorder $A$. Then the carrier of QuotientOrder($A$) is a partition of the carrier of $A$.

(39) Let us consider a non empty preorder $A$, and a non empty partition $D$ of the carrier of $A$. Suppose $D =$ the carrier of QuotientOrder($A$). Then the projection onto $A =$ the projection onto $D$.

Proof: For every object $x$ such that $x \in$ dom(the projection onto $A$) holds (the projection onto $A$)($x$) $=$ (the projection onto $D$)($x$) by [17, (23)]. □

Let $A$ be a set and $D$ be a partition of $A$.

The functor PreorderFromPartition($D$) yielding a strict relational structure is defined by the term

(Def. 10) $\langle A, \mathrm{EqRelOf}(D) \rangle$.

Let $A$ be a non empty set. Let us observe that PreorderFromPartition($D$) is non empty.

Let $A$ be a set. One can verify that PreorderFromPartition($D$) is reflexive and transitive and PreorderFromPartition($D$) is symmetric.

Let us consider a set $A$ and a partition $D$ of $A$. Now we state the propositions:

(40) EqRelOf$(D)$ = EqRelOf(PreorderFromPartition$(D)$).
PROOF: For every elements $x$, $y$ of $A$ such that $\langle x, y\rangle \in$ EqRelOf$(D)$ holds $\langle x, y\rangle \in$ EqRelOf(PreorderFromPartition$(D)$) by [17, (6)]. For every elements $x$, $y$ of $A$ such that $\langle x, y\rangle \in$ EqRelOf(PreorderFromPartition$(D)$) holds $\langle x, y\rangle \in$ EqRelOf$(D)$. $\square$

(41) $D$ = Classes(EqRelOf(PreorderFromPartition$(D)$)). The theorem is a consequence of (40).

(42) $D$ = the carrier of QuotientOrder(PreorderFromPartition$(D)$). The theorem is a consequence of (41).

Let $A$ be a set, $D$ be a partition of $A$, $X$ be an element of $D$, and $f$ be a function. The functor eqSupport$(f, X)$ yielding a subset of $A$ is defined by the term

(Def. 11) support $f \cap X$.

Let $A$ be a preorder and $X$ be an element of QuotientOrder$(A)$. The functor eqSupport$(f, X)$ yielding a subset of $A$ is defined by

(Def. 12) there exists a partition $D$ of the carrier of $A$ and there exists an element $Y$ of $D$ such that $D$ = the carrier of QuotientOrder$(A)$ and $Y = X$ and $it$ = eqSupport$(f, Y)$.

Observe that the functor eqSupport$(f, X)$ is defined by the term

(Def. 13) support $f \cap X$.

Let $A$ be a set, $D$ be a partition of $A$, $f$ be a finite-support function, and $X$ be an element of $D$. One can verify that eqSupport$(f, X)$ is finite.

Let $A$ be a preorder and $X$ be an element of QuotientOrder$(A)$. Let us note that eqSupport$(f, X)$ is finite.

Let $A$ be an order, $X$ be an element of the carrier of QuotientOrder$(A)$, and $f$ be a finite-support function from $A$ into $\mathbb{R}$. Observe that eqSupport$(f, X)$ is trivial.

Now we state the propositions:

(43) Let us consider a set $A$, a partition $D$ of $A$, an element $X$ of $D$, and a function $f$ from $A$ into $\mathbb{R}$. Then eqSupport$(f, X)$ = eqSupport$(-f, X)$. The theorem is a consequence of (9).

(44) Let us consider a preorder $A$, an element $X$ of QuotientOrder$(A)$, and a function $f$ from $A$ into $\mathbb{R}$. Then eqSupport$(f, X)$ = eqSupport$(-f, X)$. The theorem is a consequence of (43).

Let $A$ be a set, $D$ be a partition of $A$, and $f$ be a finite-support function from $A$ into $\mathbb{R}$. The functor $\Sigma_D f$ yielding a function from $D$ into $\mathbb{R}$ is defined by

(Def. 14) for every element $X$ of $D$ such that $X \in D$ holds $it(X) = \sum(f \cdot \mathrm{CFS}(\mathrm{eqSupport}(f, X)))$.

Let $A$ be a preorder.

The functor $\Sigma_{\approx} f$ yielding a function from QuotientOrder($A$) into $\mathbb{R}$ is defined by

(Def. 15) there exists a partition $D$ of the carrier of $A$ such that $D =$ the carrier of QuotientOrder($A$) and $it = \Sigma_D f$.

One can verify that the functor $\Sigma_{\approx} f$ is defined by

(Def. 16) for every element $X$ of QuotientOrder($A$) such that $X \in$ the carrier of QuotientOrder($A$) holds $it(X) = \sum(f \cdot \mathrm{CFS}(\mathrm{eqSupport}(f, X)))$.

Now we state the propositions:

(45) Let us consider a set $A$, a partition $D$ of $A$, and a finite-support function $f$ from $A$ into $\mathbb{R}$. Then $\Sigma_D(-f) = -\Sigma_D f$.
PROOF: For every object $X$ such that $X \in \mathrm{dom}(\Sigma_D(-f))$ holds $(\Sigma_D(-f))(X) = (-\Sigma_D f)(X)$ by (43), [1, (83)], [7, (2)], [6, (11)]. $\square$

(46) Let us consider a preorder $A$, and a finite-support function $f$ from $A$ into $\mathbb{R}$. Then $\Sigma_{\approx} -f = -\Sigma_{\approx} f$. The theorem is a consequence of (38) and (45).

Let $A$ be a preorder and $f$ be a non-negative yielding, finite-support function from $A$ into $\mathbb{R}$. Observe that $\Sigma_{\approx} f$ is non-negative yielding.

Let $A$ be a set and $D$ be a partition of $A$. Let us note that $\Sigma_D f$ is non-negative yielding.

Now we state the propositions:

(47) Let us consider a set $A$, a partition $D$ of $A$, and a finite-support function $f$ from $A$ into $\mathbb{R}$. If $f$ is non-positive yielding, then $\Sigma_D f$ is non-positive yielding. The theorem is a consequence of (45).

(48) Let us consider a preorder $A$, and a finite-support function $f$ from $A$ into $\mathbb{R}$. Suppose $f$ is non-positive yielding. Then $\Sigma_{\approx} f$ is non-positive yielding. The theorem is a consequence of (38) and (47).

(49) Let us consider a preorder $A$, a finite-support function $f$ from $A$ into $\mathbb{R}$, and an element $x$ of $A$. Suppose for every element $y$ of $A$ such that $x \approx y$ holds $x = y$. Then $(\Sigma_{\approx} f \cdot (\text{the projection onto } A))(x) = f(x)$.

(50) Let us consider an order $A$, and a finite-support function $f$ from $A$ into $\mathbb{R}$. Then $\Sigma_{\approx} f \cdot (\text{the projection onto } A) = f$.
PROOF: Set $F = \Sigma_{\approx} f \cdot (\text{the projection onto } A)$. For every object $x$ such that $x \in \mathrm{dom}\, f$ holds $f(x) = F(x)$ by [22, (2)], (49). $\square$

(51) Let us consider an order $A$, and finite-support functions $f_1$, $f_2$ from $A$ into $\mathbb{R}$. If $\Sigma_{\approx} f_1 = \Sigma_{\approx} f_2$, then $f_1 = f_2$. The theorem is a consequence of

(50).

(52) Let us consider a preorder $A$, and a finite-support function $f$ from $A$ into $\mathbb{R}$. Then $\operatorname{support}(\Sigma_{\approx} f) \subseteq$ (the projection onto $A)^{\circ}(\operatorname{support} f)$.

PROOF: For every object $X$ such that $X \in \operatorname{support}(\Sigma_{\approx} f)$ holds $X \in$ (the projection onto $A)^{\circ}(\operatorname{support} f)$ by [5, (24), (32)], (5), [6, (11), (13), (3)]. □

(53) Let us consider a non empty set $A$, a non empty partition $D$ of $A$, and a finite-support function $f$ from $A$ into $\mathbb{R}$. Then $\operatorname{support}(\Sigma_D f) \subseteq$ (the projection onto $D)^{\circ}(\operatorname{support} f)$. The theorem is a consequence of (42), (39), and (52).

(54) Let us consider a preorder $A$, and a finite-support function $f$ from $A$ into $\mathbb{R}$. Suppose $f$ is non-negative yielding. Then (the projection onto $A)^{\circ}(\operatorname{support} f) = \operatorname{support}(\Sigma_{\approx} f)$.

PROOF:

For every object $X$ such that $X \in$ (the projection onto $A)^{\circ}(\operatorname{support} f)$ holds $X \in \operatorname{support}(\Sigma_{\approx} f)$ by [7, (36)], [5, (24), (32)], [17, (20)]. □

(55) Let us consider a non empty set $A$, a non empty partition $D$ of $A$, and a finite-support function $f$ from $A$ into $\mathbb{R}$. Suppose $f$ is non-negative yielding. Then (the projection onto $D)^{\circ}(\operatorname{support} f) = \operatorname{support}(\Sigma_D f)$. The theorem is a consequence of (42), (39), and (54).

(56) Let us consider a preorder $A$, and a finite-support function $f$ from $A$ into $\mathbb{R}$. Suppose $f$ is non-positive yielding. Then (the projection onto $A)^{\circ}(\operatorname{support} f) = \operatorname{support}(\Sigma_{\approx} f)$. The theorem is a consequence of (9), (54), and (46).

(57) Let us consider a non empty set $A$, a non empty partition $D$ of $A$, and a finite-support function $f$ from $A$ into $\mathbb{R}$. Suppose $f$ is non-positive yielding. Then (the projection onto $D)^{\circ}(\operatorname{support} f) = \operatorname{support}(\Sigma_D f)$. The theorem is a consequence of (42), (39), and (56).

Let $A$ be a preorder and $f$ be a finite-support function from $A$ into $\mathbb{R}$. Observe that $\Sigma_{\approx} f$ is finite-support.

Let $A$ be a set and $D$ be a partition of $A$. Let us note that $\Sigma_D f$ is finite-support.

Let us consider a non empty set $A$, a non empty partition $D$ of $A$, a finite-support function $f$ from $A$ into $\mathbb{R}$, a one-to-one finite sequence $s_1$ of elements of $A$, and a one-to-one finite sequence $s_2$ of elements of $D$. Now we state the propositions:

(58) Suppose $\operatorname{rng} s_2 =$ (the projection onto $D)^{\circ}(\operatorname{rng} s_1)$ and for every element $X$ of $D$ such that $X \in \operatorname{rng} s_2$ holds $\operatorname{eqSupport}(f, X) \subseteq \operatorname{rng} s_1$. Then $\sum(\Sigma_D f \cdot s_2) = \sum(f \cdot s_1)$.

Proof: Define $\mathcal{P}$[natural number] $\equiv$ for every one-to-one finite sequence $t_1$ of elements of $A$ for every one-to-one finite sequence $t_2$ of elements of $D$ such that $\operatorname{rng} t_2 =$ (the projection onto $D)^\circ(\operatorname{rng} t_1)$ and for every element $X$ of $D$ such that $X \in \operatorname{rng} t_2$ holds $\operatorname{eqSupport}(f, X) \subseteq \operatorname{rng} t_1$ holds if $\operatorname{len} t_2 = \$_1$, then $\sum(\Sigma_D f \cdot t_2) = \sum(f \cdot t_1)$. $\mathcal{P}[0]$. For every natural number $j$ such that $\mathcal{P}[j]$ holds $\mathcal{P}[j+1]$ by [5, (19)], [3, (38)], [20, (91)], [9, (48)]. For every natural number $i$, $\mathcal{P}[i]$ from [2, Sch. 2]. $\square$

(59) If $\operatorname{rng} s_1 = \operatorname{support} f$ and $\operatorname{rng} s_2 = \operatorname{support}(\Sigma_D f)$, then $\sum(\Sigma_D f \cdot s_2) = \sum(f \cdot s_1)$. The theorem is a consequence of (58), (53), and (8).

Now we state the proposition:

(60) Let us consider a preorder $A$, a finite-support function $f$ from $A$ into $\mathbb{R}$, a one-to-one finite sequence $s_1$ of elements of $A$, and a one-to-one finite sequence $s_2$ of elements of QuotientOrder($A$). Suppose $\operatorname{rng} s_1 = \operatorname{support} f$ and $\operatorname{rng} s_2 = \operatorname{support}(\Sigma_\approx f)$. Then $\sum(\Sigma_\approx f \cdot s_2) = \sum(f \cdot s_1)$. The theorem is a consequence of (59).

## 4. Ordering Finite Sequences

Let $A$ be a relational structure and $s$ be a finite sequence of elements of $A$. We say that $s$ is weakly ascending if and only if

(Def. 17) for every natural numbers $n, m$ such that $n, m \in \operatorname{dom} s$ and $n < m$ holds $s_n \leqslant s_m$.

We say that $s$ is ascending if and only if

(Def. 18) for every natural numbers $n, m$ such that $n, m \in \operatorname{dom} s$ and $n < m$ holds $s_n \lnapprox s_m$.

Let us observe that every finite sequence of elements of $A$ which is ascending is also weakly ascending.

Let $A$ be an antisymmetric relational structure and $s$ be a finite sequence of elements of $A$. Observe that $s$ is ascending if and only if the condition (Def. 19) is satisfied.

(Def. 19) for every natural numbers $n, m$ such that $n, m \in \operatorname{dom} s$ and $n < m$ holds $s_n < s_m$.

Let $A$ be a relational structure. We say that $s$ is weakly descending if and only if

(Def. 20) for every natural numbers $n, m$ such that $n, m \in \operatorname{dom} s$ and $n < m$ holds $s_m \leqslant s_n$.

We say that $s$ is descending if and only if

(Def. 21) for every natural numbers $n$, $m$ such that $n, m \in \operatorname{dom} s$ and $n < m$ holds $s_m \lesssim s_n$.

One can verify that every finite sequence of elements of $A$ which is descending is also weakly descending.

Let $A$ be an antisymmetric relational structure and $s$ be a finite sequence of elements of $A$. Let us observe that $s$ is descending if and only if the condition (Def. 22) is satisfied.

(Def. 22) for every natural numbers $n$, $m$ such that $n, m \in \operatorname{dom} s$ and $n < m$ holds $s_m < s_n$.

Note that every finite sequence of elements of $A$ which is one-to-one and weakly ascending is also ascending and every finite sequence of elements of $A$ which is one-to-one and weakly descending is also descending and every finite sequence of elements of $A$ which is weakly ascending and weakly descending is also constant.

Let $A$ be a reflexive relational structure. Note that every finite sequence of elements of $A$ which is constant is also weakly ascending and weakly descending.

Let $A$ be a relational structure. Note that $\varepsilon_{(\text{the carrier of } A)}$ is ascending, weakly ascending, descending, and weakly descending and there exists a finite sequence of elements of $A$ which is empty, ascending, weakly ascending, descending, and weakly descending.

Let $A$ be a non empty relational structure and $x$ be an element of $A$. Let us observe that $\langle x \rangle$ is ascending, weakly ascending, descending, and weakly descending as a finite sequence of elements of $A$ and there exists a finite sequence of elements of $A$ which is non empty, one-to-one, ascending, weakly ascending, descending, and weakly descending.

Let $A$ be a relational structure and $s$ be a finite sequence of elements of $A$. We say that $s$ is asc-ordering if and only if

(Def. 23) $s$ is one-to-one and weakly ascending.

We say that $s$ is desc-ordering if and only if

(Def. 24) $s$ is one-to-one and weakly descending.

Let us note that every finite sequence of elements of $A$ which is asc-ordering is also one-to-one and weakly ascending and every finite sequence of elements of $A$ which is one-to-one and weakly ascending is also asc-ordering and every finite sequence of elements of $A$ which is desc-ordering is also one-to-one and weakly descending and every finite sequence of elements of $A$ which is one-to-one and weakly descending is also desc-ordering and every finite sequence of elements of $A$ which is ascending is also asc-ordering and every finite sequence of elements of $A$ which is descending is also desc-ordering.

Let $B$ be a subset of $A$ and $s$ be a finite sequence of elements of $A$. We say that $s$ is $B$-asc-ordering if and only if

(Def. 25) $s$ is asc-ordering and $\operatorname{rng} s = B$.

We say that $s$ is $B$-desc-ordering if and only if

(Def. 26) $s$ is desc-ordering and $\operatorname{rng} s = B$.

Let us observe that every finite sequence of elements of $A$ which is $B$-asc-ordering is also asc-ordering and every finite sequence of elements of $A$ which is $B$-desc-ordering is also desc-ordering.

Let $B$ be an empty subset of $A$. Let us note that every finite sequence of elements of $A$ which is $B$-asc-ordering is also empty and every finite sequence of elements of $A$ which is $B$-desc-ordering is also empty.

Let us consider a relational structure $A$ and a finite sequence $s$ of elements of $A$. Now we state the propositions:

(61) $s$ is weakly ascending if and only if $\operatorname{Rev}(s)$ is weakly descending.

(62) $s$ is ascending if and only if $\operatorname{Rev}(s)$ is descending.

Let us consider a relational structure $A$, a subset $B$ of $A$, and a finite sequence $s$ of elements of $A$. Now we state the propositions:

(63) $s$ is $B$-asc-ordering if and only if $\operatorname{Rev}(s)$ is $B$-desc-ordering. The theorem is a consequence of (61).

(64) If $s$ is $B$-asc-ordering or $B$-desc-ordering, then $B$ is finite.

Let $A$ be an antisymmetric relational structure. One can check that every finite sequence of elements of $A$ which is asc-ordering is also ascending and every finite sequence of elements of $A$ which is desc-ordering is also descending.

Let us consider an antisymmetric relational structure $A$, a subset $B$ of $A$, and finite sequences $s_1$, $s_2$ of elements of $A$. Now we state the propositions:

(65) If $s_1$ is $B$-asc-ordering and $s_2$ is $B$-asc-ordering, then $s_1 = s_2$.
Proof: Define $\mathcal{P}[\text{natural number}] \equiv$ if $\$_1 \in \operatorname{dom} s_1$ and $\$_1 \in \operatorname{dom} s_2$, then $s_{1\$_1} = s_{2\$_1}$. For every natural number $k$ such that for every natural number $n$ such that $n < k$ holds $\mathcal{P}[n]$ holds $\mathcal{P}[k]$ by [5, (10)], [22, (2)]. For every natural number $k$, $\mathcal{P}[k]$ from [2, Sch. 4]. For every natural number $k$ such that $k \in \operatorname{dom} s_1$ holds $s_1(k) = s_2(k)$. □

(66) If $s_1$ is $B$-desc-ordering and $s_2$ is $B$-desc-ordering, then $s_1 = s_2$. The theorem is a consequence of (63) and (65).

(67) Let us consider a linear order $A$, a finite subset $B$ of $A$, and a finite sequence $s$ of elements of $A$. Then $s$ is $B$-asc-ordering if and only if $s = \operatorname{SgmX}((\text{the internal relation of } A), B)$.
Proof: If $s$ is $B$-asc-ordering, then $s = \operatorname{SgmX}((\text{the internal relation of } A), B)$ by [8, (4)]. The internal relation of $A$ linearly orders $B$. For every

natural numbers $n$, $m$ such that $n, m \in \operatorname{dom} s$ and $n < m$ holds $s_n < s_m$. $\square$

Let $A$ be a linear order and $B$ be a finite subset of $A$.

Observe that SgmX((the internal relation of $A$), $B$) is $B$-asc-ordering.

Let us consider a relational structure $A$, subsets $B$, $C$ of $A$, and a finite sequence $s$ of elements of $A$. Now we state the propositions:

(68) If $s$ is $B$-asc-ordering and $C \subseteq B$, then there exists a finite sequence $s_2$ of elements of $A$ such that $s_2$ is $C$-asc-ordering.

PROOF: Set $s_2 = s \cdot \mathrm{Sgm}(s^{-1}(C))$. Consider $n$ being a natural number such that $\operatorname{dom} s = \operatorname{Seg} n$. For every object $x$, $x \in \operatorname{rng} s_2$ iff $x \in C$ by [6, (11), (3), (12)]. For every natural numbers $n$, $m$ such that $n, m \in \operatorname{dom} s_2$ and $n < m$ holds $s_{2n} \leqslant s_{2m}$ by [3, (6)], [6, (11)], [3, (1)], [6, (12)]. $\square$

(69) If $s$ is $B$-desc-ordering and $C \subseteq B$, then there exists a finite sequence $s_2$ of elements of $A$ such that $s_2$ is $C$-desc-ordering. The theorem is a consequence of (63) and (68).

(70) Let us consider a relational structure $A$, a subset $B$ of $A$, a finite sequence $s$ of elements of $A$, and an element $x$ of $A$. Suppose $B = \{x\}$ and $s = \langle x \rangle$. Then $s$ is $B$-asc-ordering and $B$-desc-ordering.

PROOF: For every natural numbers $n$, $m$ such that $n, m \in \operatorname{dom} s$ and $n < m$ holds $s_n \leqslant s_m \leqslant s_n$ by [3, (38), (2)]. $\square$

Let us consider a relational structure $A$, a subset $B$ of $A$, and a finite sequence $s$ of elements of $A$. Now we state the propositions:

(71) If $s$ is $B$-asc-ordering, then the internal relation of $A$ is connected in $B$.

PROOF: For every objects $x$, $y$ such that $x, y \in B$ and $x \neq y$ holds $\langle x, y \rangle \in$ the internal relation of $A$ or $\langle y, x \rangle \in$ the internal relation of $A$ by [5, (10)]. $\square$

(72) If $s$ is $B$-desc-ordering, then the internal relation of $A$ is connected in $B$. The theorem is a consequence of (63) and (71).

Let us consider a transitive relational structure $A$, subsets $B$, $C$ of $A$, a finite sequence $s_1$ of elements of $A$, and an element $x$ of $A$. Now we state the propositions:

(73) Suppose $s_1$ is $C$-asc-ordering and $x \notin C$ and $B = C \cup \{x\}$ and for every element $y$ of $A$ such that $y \in C$ holds $x \leqslant y$. Then there exists a finite sequence $s_2$ of elements of $A$ such that

(i) $s_2 = \langle x \rangle \frown s_1$, and

(ii) $s_2$ is $B$-asc-ordering.

PROOF: Set $s_3 = \langle x \rangle$. Set $s_2 = s_3 \frown s_1$. For every natural numbers $n$, $m$ such that $n, m \in \operatorname{dom} s_2$ and $n < m$ holds $s_{2n} \leqslant s_{2m}$ by [3, (25), (38), (2)]. □

(74) Suppose $s_1$ is $C$-asc-ordering and $x \notin C$ and $B = C \cup \{x\}$ and for every element $y$ of $A$ such that $y \in C$ holds $y \leqslant x$. Then there exists a finite sequence $s_2$ of elements of $A$ such that

(i) $s_2 = s_1 \frown \langle x \rangle$, and

(ii) $s_2$ is $B$-asc-ordering.

Proof: Set $s_3 = \langle x \rangle$. Set $s_2 = s_1 \frown s_3$. For every natural numbers $n$, $m$ such that $n, m \in \operatorname{dom} s_2$ and $n < m$ holds $s_{2n} \leqslant s_{2m}$ by [3, (25), (1), (2)], [2, (13)]. □

(75) Suppose $s_1$ is $C$-desc-ordering and $x \notin C$ and $B = C \cup \{x\}$ and for every element $y$ of $A$ such that $y \in C$ holds $x \leqslant y$. Then there exists a finite sequence $s_2$ of elements of $A$ such that

(i) $s_2 = s_1 \frown \langle x \rangle$, and

(ii) $s_2$ is $B$-desc-ordering.

The theorem is a consequence of (63) and (73).

(76) Suppose $s_1$ is $C$-desc-ordering and $x \notin C$ and $B = C \cup \{x\}$ and for every element $y$ of $A$ such that $y \in C$ holds $y \leqslant x$. Then there exists a finite sequence $s_2$ of elements of $A$ such that

(i) $s_2 = \langle x \rangle \frown s_1$, and

(ii) $s_2$ is $B$-desc-ordering.

The theorem is a consequence of (63) and (74).

Let us consider a transitive relational structure $A$ and a finite subset $B$ of $A$. Now we state the propositions:

(77) If the internal relation of $A$ is connected in $B$, then there exists a finite sequence $s$ of elements of $A$ such that $s$ is $B$-asc-ordering.

Proof: Define $\mathcal{P}[\text{natural number}] \equiv$ for every subset $C$ of $A$ such that $C \subseteq B$ and $\overline{\overline{C}} = \$_1$ there exists a finite sequence $s$ of elements of $A$ such that $s$ is $C$-asc-ordering. $\mathcal{P}[0]$. For every natural number $k$ such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$ by (2), [3, (74)], (70), (22). For every natural number $k$, $\mathcal{P}[k]$ from [2, Sch. 2]. □

(78) If the internal relation of $A$ is connected in $B$, then there exists a finite sequence $s$ of elements of $A$ such that $s$ is $B$-desc-ordering. The theorem is a consequence of (77) and (63).

Let us consider a connected, transitive relational structure $A$ and a finite subset $B$ of $A$. Now we state the propositions:

(79) There exists a finite sequence $s$ of elements of $A$ such that $s$ is $B$-asc-ordering. The theorem is a consequence of (77).

(80) There exists a finite sequence $s$ of elements of $A$ such that $s$ is $B$-desc-ordering. The theorem is a consequence of (79) and (63).

Let $A$ be a connected, transitive relational structure and $B$ be a finite subset of $A$. Note that there exists a finite sequence of elements of $A$ which is $B$-asc-ordering and there exists a finite sequence of elements of $A$ which is $B$-desc-ordering.

Now we state the proposition:

(81) Let us consider a preorder $A$, and a subset $B$ of $A$. Suppose the internal relation of $A$ is connected in $B$. Then the internal relation of QuotientOrder($A$) is connected in (the projection onto $A)^\circ B$. The theorem is a consequence of (36).

Let us consider a preorder $A$, a subset $B$ of $A$, and a finite sequence $s_1$ of elements of $A$. Now we state the propositions:

(82) Suppose $s_1$ is $B$-asc-ordering. Then there exists a finite sequence $s_2$ of elements of QuotientOrder($A$) such that $s_2$ is ((the projection onto $A)^\circ B$)-asc-ordering. The theorem is a consequence of (71), (81), and (77).

(83) Suppose $s_1$ is $B$-desc-ordering. Then there exists a finite sequence $s_2$ of elements of QuotientOrder($A$) such that $s_2$ is ((the projection onto $A)^\circ B$)-desc-ordering. The theorem is a consequence of (63) and (82).

Acknowledgement: I thank Dr. Adam Grabowski for his encouragement and the team behind `mus@mizar.uwb.edu.pl` for their quick and helpful replies to my beginner's questions.

## References

[1] Grzegorz Bancerek. Tarski's classes and ranks. *Formalized Mathematics*, 1(**3**):563–567, 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] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, Karol Pąk, and Josef Urban. Mizar: State-of-the-art and beyond. In Manfred Kerber, Jacques Carette, Cezary Kaliszyk, Florian Rabe, and Volker Sorge, editors, *Intelligent Computer Mathematics*, volume 9150 of *Lecture Notes in Computer Science*, pages 261–279. Springer International Publishing, 2015. ISBN 978-3-319-20614-1. doi:10.1007/978-3-319-20615-8_17.

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

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

[10] Thomas H. Cormen, Charles E. Leiserson, and Ronald L. Rivest. *Introduction to algorithms*. MIT Press, 3. ed. edition, 2009. ISBN 0-262-53305-7, 978-0-262-53305-8, 978-0-262-03384-8. http://scans.hebis.de/HEBCGI/show.pl?21502893_toc.pdf.

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

[12] Jarosław Kotowicz. Partial functions from a domain to the set of real numbers. *Formalized Mathematics*, 1(**4**):703–709, 1990.

[13] Gilbert Lee and Piotr Rudnicki. Dickson's lemma. *Formalized Mathematics*, 10(**1**):29–37, 2002.

[14] Michael Maschler, Eilon Solan, and Shmuel Zamir. *Game theory*. Cambridge Univ. Press, 2013. ISBN 978-1-107-00548-8. doi:10.1017/CBO9780511794216.

[15] Takashi Mitsuishi, Katsumi Wasaki, and Yasunari Shidama. Property of complex functions. *Formalized Mathematics*, 9(**1**):179–184, 2001.

[16] Yatsuka Nakamura. Sorting operators for finite sequences. *Formalized Mathematics*, 12 (**1**):1–4, 2004.

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

[18] Piotr Rudnicki and Andrzej Trybulec. On same equivalents of well-foundedness. *Formalized Mathematics*, 6(**3**):339–343, 1997.

[19] Bernd S.W. Schröder. *Ordered Sets: An Introduction*. Birkhäuser Boston, 2003. ISBN 978-1-4612-6591-7. https://books.google.de/books?id=hg8GCAAAQBAJ.

[20] Wojciech A. Trybulec. Non-contiguous substrings and one-to-one finite sequences. *Formalized Mathematics*, 1(**3**):569–573, 1990.

[21] Wojciech A. Trybulec. Pigeon hole principle. *Formalized Mathematics*, 1(**3**):575–579, 1990.

[22] Wojciech A. Trybulec and Grzegorz Bancerek. Kuratowski – Zorn lemma. *Formalized Mathematics*, 1(**2**):387–393, 1990.


*Received June 27, 2017*

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

FORMALIZED MATHEMATICS
Vol. 25, No. 2, Pages 141–147, 2017
DOI: 10.1515/forma-2017-0013

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

# Basel Problem – Preliminaries

Artur Korniłowicz
Institute of Informatics
University of Białystok
Poland

Karol Pąk
Institute of Informatics
University of Białystok
Poland

**Summary.** In the article we formalize in the Mizar system [4] preliminary facts needed to prove the Basel problem [7, 1]. Facts that are independent from the notion of structure are included here.

MSC: 11M06 03B35

Keywords: Basel problem

MML identifier: `BASEL_1`, version: `8.1.06 5.43.1297`

## 1. Preliminaries

From now on $X$ denotes a set, $k$, $m$, $n$ denote natural numbers, $i$ denotes an integer, $a$, $b$, $c$, $d$, $e$, $g$, $p$, $r$, $x$, $y$ denote real numbers, and $z$ denotes a complex.

Now we state the proposition:

(1) If $0 < a$, then there exists $m$ such that $0 < a \cdot m + b$.

Let $f$ be a real-valued finite sequence. Let us consider $n$. Observe that $f \restriction n$ is $\mathbb{R}$-valued.

Let $f$ be a complex-valued finite sequence. Let us observe that $f^{\mathbf{2}}$ is $(\operatorname{len} f)$-element and $f^{-1}$ is $(\operatorname{len} f)$-element.

Let $c$ be a complex. Note that $c + f$ is $(\operatorname{len} f)$-element.

Now we state the propositions:

(2) Let us consider complexes $c$, $z$. Then $c + \langle z \rangle = \langle c + z \rangle$.

(3) Let us consider complex-valued finite sequences $f$, $g$, and a complex $c$. Then $c + f \frown g = (c + f) \frown (c + g)$.




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

(4) Let us consider a complex-valued finite sequence $f$, and a complex $c$. Then $\sum(c+f) = c \cdot \operatorname{len} f + \sum f$.
PROOF: Define $\mathcal{P}[\text{complex-valued finite sequence}] \equiv \sum(c+\$_1) = c \cdot \operatorname{len} \$_1 + \sum \$_1$. For every finite sequence $p$ of elements of $\mathbb{C}$ and for every element $x$ of $\mathbb{C}$ such that $\mathcal{P}[p]$ holds $\mathcal{P}[p \frown \langle x \rangle]$ by [3, (39), (22)], (2), [17, (32)]. For every finite sequence $p$ of elements of $\mathbb{C}$, $\mathcal{P}[p]$ from [5, Sch. 2]. □

## 2. Limits of Sequences $\frac{an+b}{cn+d}$

Let $a$, $b$, $c$, $d$ be complexes. The functor Rat-Exp-Seq$(a, b, c, d)$ yielding a complex sequence is defined by

(Def. 1) $it(n) = \frac{\text{Polynom}(a,b,n)}{\text{Polynom}(c,d,n)}$.

Let us consider $a$, $b$, $c$, and $d$. The functor rseq$(a, b, c, d)$ yielding a sequence of real numbers is defined by the term

(Def. 2) $\Re(\text{Rat-Exp-Seq}(a, b, c, d))$.

Now we state the propositions:

(5) $(\text{rseq}(a, b, c, d))(n) = \frac{a \cdot n+b}{c \cdot n+d}$.

(6) $(\text{rseq}(0, b, 0, d))(n) = \frac{b}{d}$. The theorem is a consequence of (5).

Let us consider $a$ and $b$. Let us note that rseq$(a, b, 0, 0)$ is constant.

Let us consider $d$. One can verify that rseq$(0, b, 0, d)$ is constant.

Now we state the propositions:

(7) (i) $\text{rseq}(0, b, c, d) = b \cdot \text{rseq}(0, 1, c, d)$, and

(ii) $\text{rseq}(0, b, c, d) = (-b) \cdot \text{rseq}(0, 1, -c, -d)$.

The theorem is a consequence of (5).

(8) (i) $\text{rseq}(a, 0, c, d) = a \cdot \text{rseq}(1, 0, c, d)$, and

(ii) $\text{rseq}(a, 0, c, d) = (-a) \cdot \text{rseq}(1, 0, -c, -d)$.

The theorem is a consequence of (5).

Let us consider $b$, $c$, and $d$. Let us observe that rseq$(0, b, c, d)$ is convergent.

Now we state the propositions:

(9) $\lim \text{rseq}(0, b, 0, d) = \frac{b}{d}$. The theorem is a consequence of (6).

(10) Let us consider a non zero real number $c$. Then $\lim \text{rseq}(0, b, c, d) = 0$. The theorem is a consequence of (5).

Let $c$ be a non zero real number. Let us consider $a$, $b$, and $d$. Note that rseq$(a, b, c, d)$ is convergent.

Let $a$, $d$ be positive real numbers and $b$ be a real number. Let us observe that rseq$(a, b, 0, d)$ is non upper bounded.

Let $a$, $d$ be negative real numbers. Let us consider $b$. One can check that $\text{rseq}(a, b, 0, d)$ is non upper bounded.

Let $a$ be a positive real number and $d$ be a negative real number. Note that $\text{rseq}(a, b, 0, d)$ is non lower bounded.

Let $a$ be a negative real number and $d$ be a positive real number. Let us note that $\text{rseq}(a, b, 0, d)$ is non lower bounded.

Let $a$, $d$ be non zero real numbers. One can check that $\text{rseq}(a, b, 0, d)$ is non bounded and $\text{rseq}(a, b, 0, d)$ is non convergent.

Now we state the propositions:

(11) Let us consider a non zero real number $c$. Then $\lim \text{rseq}(a, b, c, d) = \frac{a}{c}$. The theorem is a consequence of (5) and (10).

(12) Let us consider a non zero real number $a$. Then $\lim \text{rseq}(a, b, a, d) = 1$. The theorem is a consequence of (11).

## 3. Trigonometry

Now we state the propositions:

(13) $\sin(\pi \cdot i) = 0$.

(14) $\cos(\frac{\pi}{2} + (\pi \cdot i)) = 0$.

(15) (i) $\tan r = (\cot r)^{-1}$, and

(ii) $\cot r = (\tan r)^{-1}$.

(16) $\text{dom}(\text{the function tan}) = \bigcup \text{the set of all } ]-\frac{\pi}{2} + (\pi \cdot i), \frac{\pi}{2} + (\pi \cdot i)[$ where $i$ is an integer.

Proof: Set $S =$ the set of all $]-\frac{\pi}{2}+(\pi \cdot i), \frac{\pi}{2}+(\pi \cdot i)[$ where $i$ is an integer. Set $T = \text{dom}(\text{the function tan})$. $T \subseteq \bigcup S$ by (14), [24, (29)]. For every set $X$ such that $X \in S$ holds $X \subseteq T$ by [16, (11)], [8, (9)], [21, (1)], [16, (13)]. □

Observe that dom(the function tan) is open as a subset of $\mathbb{R}$.

Now we state the propositions:

(17) If $0 \leqslant r$, then $(\text{the function sin})(r) \leqslant r$.

Proof: Reconsider $A = [0, r]$ as a non empty, closed interval subset of $\mathbb{R}$. Reconsider $c = (\text{the function cos}) \restriction A$ as a function from $A$ into $\mathbb{R}$. $c \restriction A$ is bounded and $c$ is integrable by [11, (11), (10)]. $\text{integral}\, c = (\text{the function sin})(r)$ by [11, (19)], [22, (24)], [26, (30)]. Set $Z_0 = \square^0$. Reconsider $Z_3 = Z_0 \restriction A$ as a function from $A$ into $\mathbb{R}$. $Z_3 \restriction A$ is bounded and $Z_3$ is integrable by [11, (11), (10)]. $\text{integral}\, Z_3 = r$ by [14, (21)], [19, (35)], [11, (19)], [22, (30)]. For every $r$ such that $r \in A$ holds $c(r) \leqslant Z_3(r)$ by [6, (49)], [19, (34)], [13, (6)]. □

(18) If $0 \leqslant r < \frac{\pi}{2}$, then $r \leqslant$ (the function tan)$(r)$.
PROOF: Reconsider $A = [0, r]$ as a non empty, closed interval subset of $\mathbb{R}$. Set $Z_0 = \Box^0$. Reconsider $Z_3 = Z_0 \restriction A$ as a function from $A$ into $\mathbb{R}$. $Z_3 \restriction A$ is bounded and $Z_3$ is integrable by [11, (11), (10)]. integral $Z_3 = r$ by [14, (21)], [19, (35)], [11, (19)], [22, (30)]. Set $T = \mathrm{dom}$(the function tan). Set $c_2 =$ (the function cos) $\cdot$ (the function cos). Set $c_3 = c_2 \restriction T$. Set $Z_1 = \frac{Z_0}{c_3}$. ${c_3}^{-1}(\{0\}) = \emptyset$ by [6, (47)]. Reconsider $Z_2 = Z_1 \restriction A$ as a function from $A$ into $\mathbb{R}$. $Z_1 \restriction A$ is continuous and $Z_2 \restriction A$ is bounded and $Z_2$ is integrable by [20, (24)], [11, (11), (10)]. For every real number $s$ such that $s \in T$ holds $Z_1(s) = \frac{1}{(\text{the function cos})(s)^{\mathbf{2}}}$ and (the function cos)$(s) \neq 0$ by [19, (34)], [6, (47)]. integral $Z_2 =$ (the function tan)$(r)$ by [12, (19)], [18, (59)], [15, (41)]. For every $r$ such that $r \in A$ holds $Z_3(r) \leqslant Z_2(r)$ by [6, (49)], [19, (34)], [16, (11)], [13, (6)]. $\Box$

## 4. Some Special Functions and Sequences

Let $f$ be a real-valued function. The functors: $\cot f$ and $\mathrm{cosec}\, f$ yielding functions are defined by conditions

(Def. 3) $\mathrm{dom} \cot f = \mathrm{dom}\, f$ and for every object $x$ such that $x \in \mathrm{dom}\, f$ holds $\cot f(x) = \cot(f(x))$,

(Def. 4) $\mathrm{dom}\, \mathrm{cosec}\, f = \mathrm{dom}\, f$ and for every object $x$ such that $x \in \mathrm{dom}\, f$ holds $\mathrm{cosec}\, f(x) = \mathrm{cosec}(f(x))$,

respectively. Note that $\cot f$ is $\mathbb{R}$-valued and $\mathrm{cosec}\, f$ is $\mathbb{R}$-valued.

Let $f$ be a real-valued finite sequence. Let us observe that $\cot f$ is finite sequence-like and $\mathrm{cosec}\, f$ is finite sequence-like.

Let us consider a real-valued finite sequence $f$. Now we state the propositions:

(19) $\mathrm{len} \cot f = \mathrm{len}\, f$.

(20) $\mathrm{len}\, \mathrm{cosec}\, f = \mathrm{len}\, f$.

Let $f$ be a real-valued finite sequence. Note that $\cot f$ is $(\mathrm{len}\, f)$-element and $\mathrm{cosec}\, f$ is $(\mathrm{len}\, f)$-element.

Let us consider $m$. The functor x-r-seq$(m)$ yielding a finite sequence is defined by the term

(Def. 5) $\frac{\pi}{2 \cdot m+1} \cdot \mathrm{idseq}(m)$.

Now we state the propositions:

(21) (i) len x-r-seq$(m) = m$, and

(ii) for every $k$ such that $1 \leqslant k \leqslant m$ holds (x-r-seq$(m))(k) = \frac{k \cdot \pi}{2 \cdot m+1}$.

(22) rng x-r-seq$(m) \subseteq ]0, \frac{\pi}{2}[$. The theorem is a consequence of (21).

Let us consider $m$. Let us note that x-r-seq($m$) is $\mathbb{R}$-valued.

Now we state the proposition:

(23) If $1 \leqslant k \leqslant m$, then $0 < (\text{x-r-seq}(m))(k) < \frac{\pi}{2}$. The theorem is a consequence of (22) and (21).

Note that x-r-seq(0) is empty.

(24) If $1 \leqslant k \leqslant m$, then $\frac{2}{k \cdot \pi} + (\text{x-r-seq}(m))^{-1}(k) = (\text{x-r-seq}(m+1))^{-1}(k)$. The theorem is a consequence of (21).

(25) If $1 \leqslant k \leqslant m$, then $2 \cdot m + 1 \cdot (\text{x-r-seq}(m))(k) = k \cdot \pi$. The theorem is a consequence of (21).

(26) ${}^2\text{cosec}\,\text{x-r-seq}(m) = 1 + {}^2\text{cot}\,\text{x-r-seq}(m)$. The theorem is a consequence of (21) and (23).

(27) x-r-seq($n$) is one-to-one. The theorem is a consequence of (21).

(28) ${}^2\text{cot}\,\text{x-r-seq}(n)$ is one-to-one.

Proof: Set $f = \text{x-r-seq}(n)$. $f$ is one-to-one. $0 < f(x_1) < \frac{\pi}{2}$ and $0 < f(x_2) < \frac{\pi}{2}$ and $\frac{\pi}{2} < \pi$. $\cot(f(x_1)) = \cot(f(x_2))$ by [23, (40)]. $f(x_1) = f(x_2)$ by [15, (2)], [25, (57)], [6, (47)], [15, (10)]. □

(29) $\sum({}^2\text{cot}\,\text{x-r-seq}(m)) \leqslant \sum({}^2\text{x-r-seq}(m))^{-1}$. The theorem is a consequence of (21), (19), (15), (23), (16), and (18).

(30) $\sum({}^2\text{x-r-seq}(m))^{-1} \leqslant \sum({}^2\text{cosec}\,\text{x-r-seq}(m))$. The theorem is a consequence of (21), (20), (23), and (17).

The functors: Basel-seq, Basel-seq$^1$, and Basel-seq$^2$ yielding sequences of real numbers are defined by terms

(Def. 6) $\text{rseq}(0,1,1,0) \cdot \text{rseq}(0,1,1,0)$,

(Def. 7) $(\frac{\pi^{\mathbf{2}}}{6} \cdot \text{rseq}(2,0,2,1)) \cdot \text{rseq}(2,-1,2,1)$,

(Def. 8) $(\frac{\pi^{\mathbf{2}}}{6} \cdot \text{rseq}(2,0,2,1)) \cdot \text{rseq}(2,2,2,1)$,

respectively. Now we state the propositions:

(31) $(\text{Basel-seq})(n) = \frac{1}{n^{\mathbf{2}}}$.

(32) $(\text{Basel-seq}^1)(n) = \frac{\pi^{\mathbf{2}}}{6} \cdot \frac{2 \cdot n}{2 \cdot n+1} \cdot \frac{2 \cdot n-1}{2 \cdot n+1}$. The theorem is a consequence of (5).

(33) $(\text{Basel-seq}^2)(n) = \frac{\pi^{\mathbf{2}}}{6} \cdot \frac{2 \cdot n}{2 \cdot n+1} \cdot \frac{2 \cdot n+2}{2 \cdot n+1}$. The theorem is a consequence of (5).

Let us observe that Basel-seq is convergent and Basel-seq$^1$ is convergent and Basel-seq$^2$ is convergent.

(34) $\lim \text{Basel-seq}^1 = \frac{\pi^{\mathbf{2}}}{6} = \lim \text{Basel-seq}^2$.

(35) $\sum({}^2\text{x-r-seq}(m))^{-1} = \frac{(2 \cdot m+1)^{\mathbf{2}}}{\pi^{\mathbf{2}}} \cdot \sum_{\kappa=0}^{m} \text{Basel-seq}(\kappa)$.

Proof: Set $a = \pi^{\mathbf{2}}$. Set $b = (2 \cdot m + 1)^{\mathbf{2}}$. Set $B = \text{Basel-seq}$. Set $S = \text{Shift}(B{\restriction}\mathbb{Z}_{m+1}, 1)$. Set $M = \text{x-r-seq}(m)$. Set $G = ({}^2M)^{-1}$. Set $F = \langle 0 \rangle \frown G$. $B(0) = \frac{1}{0^{\mathbf{2}}}$. $F = \frac{b}{a} \cdot S$ by [9, (3)], [2, (11)], [10, (47)], (31). □

## References


[1] M. Aigner and G. M. Ziegler. *Proofs from THE BOOK*. Springer-Verlag, Berlin Heidelberg New York, 2004.

[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] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, Karol Pąk, and Josef Urban. Mizar: State-of-the-art and beyond. In Manfred Kerber, Jacques Carette, Cezary Kaliszyk, Florian Rabe, and Volker Sorge, editors, *Intelligent Computer Mathematics*, volume 9150 of *Lecture Notes in Computer Science*, pages 261–279. Springer International Publishing, 2015. ISBN 978-3-319-20614-1. doi:10.1007/978-3-319-20615-8_17.

[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] Augustin Louis Cauchy. *Cours d'analyse de l'Ecole royale polytechnique*. de l'Imprimerie royale, 1821.

[8] Wenpai Chang, Yatsuka Nakamura, and Piotr Rudnicki. Inner products and angles of complex numbers. *Formalized Mathematics*, 11(**3**):275–280, 2003.

[9] Wenpai Chang, Hiroshi Yamazaki, and Yatsuka Nakamura. The inner product and conjugate of finite sequences of complex numbers. *Formalized Mathematics*, 13(**3**):367–373, 2005.

[10] Noboru Endou. Double series and sums. *Formalized Mathematics*, 22(**1**):57–68, 2014. doi:10.2478/forma-2014-0006.

[11] Noboru Endou, Katsumi Wasaki, and Yasunari Shidama. Definition of integrability for partial functions from $\mathbb{R}$ to $\mathbb{R}$ and integrability for continuous functions. *Formalized Mathematics*, 9(**2**):281–284, 2001.

[12] Adam Grabowski and Yatsuka Nakamura. Some properties of real maps. *Formalized Mathematics*, 6(**4**):455–459, 1997.

[13] Artur Korniłowicz and Yasunari Shidama. Inverse trigonometric functions arcsin and arccos. *Formalized Mathematics*, 13(**1**):73–79, 2005.

[14] Jarosław Kotowicz. Partial functions from a domain to the set of real numbers. *Formalized Mathematics*, 1(**4**):703–709, 1990.

[15] Xiquan Liang and Bing Xie. Inverse trigonometric functions arctan and arccot. *Formalized Mathematics*, 16(**2**):147–158, 2008. doi:10.2478/v10037-008-0021-3.

[16] Robert Milewski. Trigonometric form of complex numbers. *Formalized Mathematics*, 9(**3**):455–460, 2001.

[17] Keiichi Miyajima and Takahiro Kato. The sum and product of finite sequences of complex numbers. *Formalized Mathematics*, 18(**2**):107–111, 2010. doi:10.2478/v10037-010-0014-x.

[18] Cuiying Peng, Fuguo Ge, and Xiquan Liang. Several integrability formulas of special functions. *Formalized Mathematics*, 15(**4**):189–198, 2007. doi:10.2478/v10037-007-0023-6.

[19] Konrad Raczkowski. Integer and rational exponents. *Formalized Mathematics*, 2(**1**):125–130, 1991.

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

[21] Piotr Rudnicki and Andrzej Trybulec. Abian's fixed point theorem. *Formalized Mathematics*, 6(**3**):335–338, 1997.

[22] Yasunari Shidama, Noboru Endou, and Katsumi Wasaki. Riemann indefinite integral of functions of real variable. *Formalized Mathematics*, 15(**2**):59–63, 2007. doi:10.2478/v10037-007-0007-6.

[23] Andrzej Trybulec and Czesław Byliński. Some properties of real numbers. *Formalized Mathematics*, 1(**3**):445–449, 1990.

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

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

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

*Received June 27, 2017*

---

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

FORMALIZED MATHEMATICS
Vol. 25, No. 2, Pages 149–155, 2017
DOI: 10.1515/forma-2017-0014

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

# Basel Problem[1]

Karol Pąk
Institute of Informatics
University of Białystok
Poland

Artur Korniłowicz
Institute of Informatics
University of Białystok
Poland

**Summary.** A rigorous elementary proof of the Basel problem [6, 1]

$$\Sigma_{n=1}^{\infty}\frac{1}{n^2}=\frac{\pi^2}{6}$$

is formalized in the Mizar system [3]. This theorem is item `#14` from the "Formalizing 100 Theorems" list maintained by Freek Wiedijk at `http://www.cs.ru.nl/F.Wiedijk/100/` .

MSC: 11M06 03B35

Keywords: Basel problem

MML identifier: `BASEL_2`, version: `8.1.06 5.43.1297`

## 1. Preliminaries

From now on $k$, $m$, $n$ denote natural numbers, $R$ denotes a commutative ring, $p$, $q$ denote polynomials over $R$, and $z_0$, $z_1$ denote elements of $R$.

Let $L$ be a right zeroed, non empty double loop structure. Let us consider $n$. Let us note that $n \cdot 0_L$ reduces to $0_L$.

Now we state the proposition:

(1) Let us consider a complex $z$, and an element $e$ of $\mathbb{C}_{\rm F}$. If $z = e$, then $n \cdot z = n \cdot e$.

Let $e$ be an element of $\mathbb{C}_{\rm F}$ and $z$ be a complex. Let us consider $n$. We identify $n \cdot z$ with $n \cdot e$. Now we state the propositions:

[1] This work has been financed by the resources of the Polish National Science Centre granted by decision no. DEC-2015/19/D/ST6/01473.

(2) Let us consider a complex-valued finite sequence $Z$, and a finite sequence $E$ of elements of $\mathbb{C}_{\mathrm{F}}$. If $E = Z$, then $\sum Z = \sum E$.

PROOF: Consider $f$ being a sequence of $\mathbb{C}_{\mathrm{F}}$ such that $\sum E = f(\operatorname{len} E)$ and $f(0) = 0_{\mathbb{C}_{\mathrm{F}}}$ and for every natural number $j$ and for every element $v$ of $\mathbb{C}_{\mathrm{F}}$ such that $j < \operatorname{len} E$ and $v = E(j+1)$ holds $f(j+1) = f(j) + v$. Define $\mathcal{P}[\text{natural number}] \equiv$ if $\$_1 \leqslant \operatorname{len} Z$, then $\sum(Z \restriction \$_1) = f(\$_1)$. If $\mathcal{P}[n]$, then $\mathcal{P}[n+1]$ by [2, (11)], [15, (25)], [5, (10)], [2, (13)]. $\mathcal{P}[n]$ from [2, Sch. 2]. $\square$

(3) $(\mathbf{1}_{\mathbb{C}_{\mathrm{F}}})^n = \mathbf{1}_{\mathbb{C}_{\mathrm{F}}}$.

(4) Let us consider a left zeroed, right zeroed, non empty additive loop structure $L$, and elements $z_0$, $z_1$ of $L$. Then $\langle z_0, z_1 \rangle = \langle z_0 \rangle + \langle 0_L, z_1 \rangle$.

(5) Let us consider an add-associative, right zeroed, right complementable, distributive, non empty double loop structure $L$, and elements $a$, $b$, $c$, $d$ of $L$. Then $\langle a, b \rangle * \langle c, d \rangle = \langle a \cdot c, a \cdot d + (b \cdot c), b \cdot d \rangle$.

(6) Let us consider an Abelian, add-associative, right zeroed, right complementable, well unital, commutative, distributive, non empty double loop structure $L$. Then $\langle 0_L, 0_L, 1_L \rangle = \langle 0_L, 1_L \rangle^2$. The theorem is a consequence of (5).

(7) Let us consider a right zeroed, add-associative, right complementable, right distributive, non empty double loop structure $L$, an element $z$ of $L$, and a polynomial $p$ over $L$. Then $(p * \langle z \rangle)(n) = p(n) \cdot z$.

PROOF: Set $Z = \langle z \rangle$. Consider $r$ being a finite sequence of elements of the carrier of $L$ such that $\operatorname{len} r = n+1$ and $(p * \langle z \rangle)(n) = \sum r$ and for every element $k$ of $\mathbb{N}$ such that $k \in \operatorname{dom} r$ holds $r(k) = p(k -' 1) \cdot Z(n + 1 -' k)$. Set $l = \operatorname{len} r$. For every element $k$ of $\mathbb{N}$ such that $k \in \operatorname{dom} r$ and $k \neq l$ holds $r_k = 0_L$ by [15, (25)], [2, (14)], [11, (32)]. $\square$

(8) Let us consider an Abelian, add-associative, right zeroed, right complementable, well unital, associative, commutative, distributive, non empty double loop structure $L$, and an element $x$ of $L$. Then $\langle x \rangle^n = \langle x^n \rangle$.

PROOF: Set $X = \langle x \rangle$. Define $\mathcal{P}[\text{natural number}] \equiv X^{\$_1} = \langle x^{\$_1} \rangle$. $\mathcal{P}[0]$ by [13, (8)], [2, (14)], [11, (32)], [9, (30)]. For every $n$ such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$ by [11, (19)], [2, (14)], [11, (32)], [13, (8)]. For every $n$, $\mathcal{P}[n]$ from [2, Sch. 2]. $\square$

(9) (i) $\langle z_0, z_1 \rangle^0(0) = 1_R$, and

(ii) if $n > 0$, then $\langle 0_R, z_1 \rangle^n(n) = {z_1}^n$, and

(iii) if $k \neq n$, then $\langle 0_R, z_1 \rangle^n(k) = 0_R$.

PROOF: Set $P = \langle 0_R, z_1 \rangle$. Define $\mathcal{P}[\text{natural number}] \equiv$ if $\$_1 > 0$, then $P^{\$_1}(\$_1) = {z_1}^{\$_1}$ and for every $k$ such that $k \neq \$_1$ holds $P^{\$_1}(k) = 0_R$. $\mathcal{P}[0]$ by [11, (15)], [9, (30)]. For every natural number $i$ such that $\mathcal{P}[i]$ holds

$\mathcal{P}[i+1]$ by [11, (19), (16), (38)], [13, (8)]. For every natural number $i$, $\mathcal{P}[i]$ from [2, Sch. 2]. □

(10) (i) $\langle 0_R, 0_R, \mathbf{1}_R \rangle^n (2 \cdot n) = \mathbf{1}_R$, and

(ii) for every $k$ such that $k \neq 2 \cdot n$ holds $\langle 0_R, 0_R, \mathbf{1}_R \rangle^n (k) = 0_R$.

Proof: Set $x_1 = \langle 0_R, \mathbf{1}_R \rangle$. Set $x_2 = \langle 0_R, 0_R, \mathbf{1}_R \rangle$. Define $\mathcal{P}$[natural number] $\equiv {x_2}^{\$_1} = {x_1}^{2 \cdot \$_1}$. If $\mathcal{P}[k]$, then $\mathcal{P}[k+1]$ by (6), [11, (17), (19)], [9, (33)]. $\mathcal{P}[k]$ from [2, Sch. 2]. Define $\mathcal{Q}$[natural number] $\equiv (\mathbf{1}_R)^{\$_1} = \mathbf{1}_R$. If $\mathcal{Q}[k]$, then $\mathcal{Q}[k+1]$. $\mathcal{Q}[k]$ from [2, Sch. 2]. □

(11) Let us consider an integral domain $L$, and a non-zero polynomial $p$ over $L$. Then $\overline{\overline{\mathrm{Roots}(p)}} < \mathrm{len}\, p$.

Proof: Define $\mathcal{P}$[natural number] $\equiv$ for every non-zero polynomial $p$ over $L$ such that $\mathrm{len}\, p = \$_1$ holds $\overline{\overline{\mathrm{Roots}(p)}} < \mathrm{len}\, p$. For every natural number $n$ such that $n \geqslant 1$ and $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$ by [12, (47)], [10, (3)], [12, (50), (23), (48)]. For every natural number $n$ such that $n \geqslant 1$ holds $\mathcal{P}[n]$ from [2, Sch. 8]. □

Let $L$ be an add-associative, right zeroed, right complementable, distributive, non empty double loop structure and $a$ be a polynomial over $L$. The functor ${}^{@}a$ yielding an element of PolyRing($L$) is defined by the term

(Def. 1) $a$.

Let $n$ be a natural number. The functor $n \cdot a$ yielding a polynomial over $L$ is defined by the term

(Def. 2) $n \cdot {}^{@}a$.

Now we state the propositions:

(12) Let us consider an add-associative, right zeroed, right complementable, distributive, non empty double loop structure $L$, and a polynomial $a$ over $L$. Then $(n \cdot a)(k) = n \cdot a(k)$.

(13) $\langle z_0, z_1 \rangle^n (k) = \binom{n}{k} \cdot ({z_1}^k \cdot {z_0}^{n-'k})$.

Proof: Set $Z_0 = \langle z_0 \rangle$. Set $Z_1 = \langle 0_R, z_1 \rangle$. Set $C = \binom{n}{k} \cdot ({z_1}^k \cdot {z_0}^{n-'k})$. Set $P_2 = \mathrm{PolyRing}(R)$. $\langle z_0, z_1 \rangle = Z_0 + Z_1$. Consider $F$ being a finite sequence of elements of PolyRing($R$) such that $\langle z_0, z_1 \rangle^n = \sum F$ and $\mathrm{len}\, F = n+1$ and for every natural number $k$ such that $k \leqslant n$ holds $F(k+1) = \binom{n}{k} \cdot {Z_1}^k * {Z_0}^{n-'k}$. For every natural number $i$ such that $i \leqslant n$ and for every polynomial $F_1$ over $R$ such that $F_1 = F(i+1)$ holds if $k \neq i$, then $F_1(k) = 0_R$ and if $k = i$, then $F_1(k) = C$ by (12), (8), (7), (9). Consider $f$ being a sequence of the carrier of $P_2$ such that $\sum F = f(\mathrm{len}\, F)$ and $f(0) = 0_{P_2}$ and for every natural number $j$ and for every element $v$ of $P_2$ such that $j < \mathrm{len}\, F$ and $v = F(j+1)$ holds $f(j+1) = f(j)+v$. For every polynomial $p$ over $R$ such that $p = f(0)$ holds $p(k) = 0_R$ by [14, (7)]. □

## 2. Imaginary Complex Numbers

Let $z$ be a complex. We say that $z$ is imaginary if and only if

(Def. 3) $\Re(z) = 0$.

Note that $i$ is imaginary and every complex which is real and imaginary is also zero and every complex which is zero is also imaginary.

Let $z_1$, $z_2$ be imaginary complexes. One can verify that $z_1 \cdot z_2$ is real and $z_1 + z_2$ is imaginary.

Let $z$ be an imaginary complex and $r$ be a real complex. Note that $z \cdot r$ is imaginary and $0_{\mathbb{C}_{\mathrm{F}}}$ is real and imaginary and there exists an element of $\mathbb{C}_{\mathrm{F}}$ which is real and imaginary.

Let $z$ be a real element of $\mathbb{C}_{\mathrm{F}}$ and $n$ be a natural number. Observe that $n \cdot z$ is real.

Let $z$ be an imaginary element of $\mathbb{C}_{\mathrm{F}}$. Observe that $n \cdot z$ is imaginary.

Let $z$ be an imaginary complex and $n$ be an even natural number. Let us observe that $\mathrm{power}_{\mathbb{C}_{\mathrm{F}}}(z, n)$ is real.

Let $n$ be an odd natural number. One can check that $\mathrm{power}_{\mathbb{C}_{\mathrm{F}}}(z, n)$ is imaginary as a complex.

Let $r$ be a real element of $\mathbb{C}_{\mathrm{F}}$ and $n$ be a natural number. Let us note that $\mathrm{power}_{\mathbb{C}_{\mathrm{F}}}(r, n)$ is real and every element of $\mathbb{C}_{\mathrm{F}}$ which is zero is also imaginary and real.

Let $p$ be a sequence of $\mathbb{C}_{\mathrm{F}}$. We say that $p$ is imaginary if and only if

(Def. 4) for every natural number $i$, $p(i)$ is imaginary.

Let $i_1$ be an imaginary element of $\mathbb{C}_{\mathrm{F}}$. One can check that $\langle i_1 \rangle$ is imaginary.

Let $i_2$ be an imaginary element of $\mathbb{C}_{\mathrm{F}}$. Observe that $\langle i_1, i_2 \rangle$ is imaginary and there exists a polynomial over $\mathbb{C}_{\mathrm{F}}$ which is imaginary.

Now we state the propositions:

(14) Let us consider an imaginary polynomial $I$ over $\mathbb{C}_{\mathrm{F}}$, and a real element $r$ of $\mathbb{C}_{\mathrm{F}}$. Then $\mathrm{eval}(I, r)$ is imaginary.

Proof: Consider $H$ being a finite sequence of elements of $\mathbb{C}_{\mathrm{F}}$ such that $\mathrm{eval}(I, r) = \sum H$ and $\mathrm{len}\, H = \mathrm{len}\, I$ and for every element $n$ of $\mathbb{N}$ such that $n \in \mathrm{dom}\, H$ holds $H(n) = I(n -' 1) \cdot \mathrm{power}_{\mathbb{C}_{\mathrm{F}}}(r, n -' 1)$. Consider $h$ being a sequence of the carrier of $\mathbb{C}_{\mathrm{F}}$ such that $\sum H = h(\mathrm{len}\, H)$ and $h(0) = 0_{\mathbb{C}_{\mathrm{F}}}$ and for every natural number $j$ and for every element $v$ of $\mathbb{C}_{\mathrm{F}}$ such that $j < \mathrm{len}\, H$ and $v = H(j+1)$ holds $h(j+1) = h(j) + v$. Define $\mathcal{P}[$natural number$] \equiv$ if $\$_1 \leqslant \mathrm{len}\, H$, then $h(\$_1)$ is imaginary. If $\mathcal{P}[n]$, then $\mathcal{P}[n+1]$ by [2, (11)], [15, (25)], [2, (13)]. $\mathcal{P}[n]$ from [2, Sch. 2]. □

(15) Let us consider a real polynomial $R$ over $\mathbb{C}_{\mathrm{F}}$, and a real element $r$ of $\mathbb{C}_{\mathrm{F}}$. Then $\mathrm{eval}(R, r)$ is real.

PROOF: Consider $H$ being a finite sequence of elements of $\mathbb{C}_{\mathrm{F}}$ such that $\mathrm{eval}(I, r) = \sum H$ and $\mathrm{len}\, H = \mathrm{len}\, I$ and for every element $n$ of $\mathbb{N}$ such that $n \in \mathrm{dom}\, H$ holds $H(n) = I(n -' 1) \cdot \mathrm{power}_{\mathbb{C}_{\mathrm{F}}}(r, n -' 1)$. Consider $h$ being a sequence of the carrier of $\mathbb{C}_{\mathrm{F}}$ such that $\sum H = h(\mathrm{len}\, H)$ and $h(0) = 0_{\mathbb{C}_{\mathrm{F}}}$ and for every natural number $j$ and for every element $v$ of $\mathbb{C}_{\mathrm{F}}$ such that $j < \mathrm{len}\, H$ and $v = H(j + 1)$ holds $h(j + 1) = h(j) + v$. Define $\mathcal{P}$[natural number] $\equiv$ if $\$_1 \leqslant \mathrm{len}\, H$, then $h(\$_1)$ is real. If $\mathcal{P}[n]$, then $\mathcal{P}[n + 1]$ by [2, (11)], [15, (25)], [2, (13)]. $\mathcal{P}[n]$ from [2, Sch. 2]. □

Let us consider an imaginary element $i_3$ of $\mathbb{C}_{\mathrm{F}}$ and a real element $r$ of $\mathbb{C}_{\mathrm{F}}$.

(16) If $n$ is even, then the even part of $\langle i_3, r\rangle^n$ is real and the odd part of $\langle i_3, r\rangle^n$ is imaginary. The theorem is a consequence of (13).

(17) If $n$ is odd, then the even part of $\langle i_3, r\rangle^n$ is imaginary and the odd part of $\langle i_3, r\rangle^n$ is real. The theorem is a consequence of (13).

(18) Let us consider a non empty zero structure $L$, and a polynomial $p$ over $L$. Suppose len(the even part of $p$) $\neq 0$. Then len(the even part of $p$) is odd.

PROOF: Set $E =$ the even part of $p$. Consider $n$ such that $2 \cdot n = \mathrm{len}\, E$. Reconsider $n_1 = n - 1$ as a natural number. The length of $E$ is at most $n + n_1$ by [2, (13)]. □

## 3. Main Facts

Let $L$ be a non empty set, $p$ be a sequence of $L$, and $m$ be a natural number. The functor $\mathrm{sieve}_m(p)$ yielding a sequence of $L$ is defined by

(Def. 5) for every natural number $i$, $it(i) = p(m \cdot i)$.

Let $L$ be a non empty zero structure, $p$ be a finite-Support sequence of $L$, and $m$ be a non zero natural number. Let us observe that $\mathrm{sieve}_m(p)$ is finite-Support.

Now we state the propositions:

(19) Let us consider a non empty zero structure $L$, and a sequence $p$ of $L$. Then $\mathrm{sieve}_{(2 \cdot k)}(p) = \mathrm{sieve}_{(2 \cdot k)}$(the even part of $p$).

(20) Let us consider a non empty zero structure $L$, and a polynomial $p$ over $L$. Suppose len(the even part of $p$) is odd. Then $2 \cdot \mathrm{len}\, \mathrm{sieve}_2(p) =$ len(the even part of $p$) $+ 1$.

PROOF: Set $E =$ the even part of $p$. Set $C = \mathrm{sieve}_2(E)$. Consider $n$ such that $\mathrm{len}\, E = 2 \cdot n + 1$. Set $n_1 = n + 1$. The length of $C$ is at most $n_1$ by [2, (13)]. For every natural number $m$ such that the length of $C$ is at most $m$ holds $n_1 \leqslant m$ by [2, (13)]. $C = \mathrm{sieve}_2(p)$. □

(21) Let us consider a non empty zero structure $L$, and a polynomial $p$ over $L$. Suppose len(the even part of $p$) $= 0$. Let us consider a non zero natural number $n$. Then $\operatorname{len}\operatorname{sieve}_{(2\cdot n)}(p) = 0$.

(22) Let us consider a field $L$, and a polynomial $p$ over $L$. Then the even part of $p = (\operatorname{sieve}_2(p))[\langle 0_L, 0_L, \mathbf{1}_L\rangle]$. The theorem is a consequence of (10), (18), (20), and (21).

(23) $(\operatorname{sieve}_2(\langle i_{\mathbb{C}_{\mathrm{F}}}, 1_{\mathbb{C}_{\mathrm{F}}}\rangle^{2\cdot n+1}))(n) = \binom{2\cdot n+1}{1} \cdot i_{\mathbb{C}_{\mathrm{F}}}$. The theorem is a consequence of (3) and (13).

(24) Suppose $n \geqslant 1$. Then $(\operatorname{sieve}_2(\langle i_{\mathbb{C}_{\mathrm{F}}}, 1_{\mathbb{C}_{\mathrm{F}}}\rangle^{2\cdot n+1}))(n-1) = \binom{2\cdot n+1}{3} \cdot -i_{\mathbb{C}_{\mathrm{F}}}$. The theorem is a consequence of (3) and (13).

(25) $\operatorname{len}\operatorname{sieve}_2(\langle i_{\mathbb{C}_{\mathrm{F}}}, 1_{\mathbb{C}_{\mathrm{F}}}\rangle^{2\cdot n+1}) = n+1$.
PROOF: Set $P_1 = \langle i_{\mathbb{C}_{\mathrm{F}}}, 1_{\mathbb{C}_{\mathrm{F}}}\rangle^{2\cdot n+1}$. The length of $\operatorname{sieve}_2(P_1)$ is at most $n+1$. For every $m$ such that the length of $\operatorname{sieve}_2(P_1)$ is at most $m$ holds $n+1 \leqslant m$ by [2, (13)], (23). □

Let $n$ be a natural number. Let us note that $\operatorname{sieve}_2(\langle i_{\mathbb{C}_{\mathrm{F}}}, 1_{\mathbb{C}_{\mathrm{F}}}\rangle^{2\cdot n+1})$ is non-zero.

(26) $\operatorname{rng}({}^2\cot \text{x-r-seq}(n)) \subseteq \operatorname{Roots}(\operatorname{sieve}_2(\langle i_{\mathbb{C}_{\mathrm{F}}}, 1_{\mathbb{C}_{\mathrm{F}}}\rangle^{2\cdot n+1}))$.
PROOF: Set $f = \text{x-r-seq}(n)$. Set $f_1 = {}^2\cot f$. Set $P_1 = \langle i_{\mathbb{C}_{\mathrm{F}}}, 1_{\mathbb{C}_{\mathrm{F}}}\rangle^{2\cdot n+1}$. Consider $x$ being an object such that $x \in \operatorname{dom} f_1$ and $f_1(x) = y$. Reconsider $c = \cot(f(x))$ as an element of $\mathbb{C}_{\mathrm{F}}$. Set $N = 2\cdot n+1$. $(\cot(f(x))+i)^N$ is real by [7, (21)], [15, (29), (25)], [7, (23)]. eval(the even part of $P_1, c) = 0$ by [8, (74)], [4, (6)], [8, (8)], (17). Set $X_2 = \langle 0_{\mathbb{C}_{\mathrm{F}}}, 0_{\mathbb{C}_{\mathrm{F}}}, \mathbf{1}_{\mathbb{C}_{\mathrm{F}}}\rangle$. The even part of $P_1 = (\operatorname{sieve}_2(P_1))[X_2]$. □

(27) $\operatorname{Roots}(\operatorname{sieve}_2(\langle i_{\mathbb{C}_{\mathrm{F}}}, 1_{\mathbb{C}_{\mathrm{F}}}\rangle^{2\cdot n+1})) = \operatorname{rng}({}^2\cot \text{x-r-seq}(n))$.
The theorem is a consequence of (26), (11), and (25).

(28) $\sum({}^2\cot \text{x-r-seq}(m)) = \frac{2\cdot m\cdot(2\cdot m-1)}{6}$. The theorem is a consequence of (25), (27), (23), (24), and (2).

(29) $\sum({}^2\operatorname{cosec} \text{x-r-seq}(m)) = \frac{2\cdot m\cdot(2\cdot m+2)}{6}$. The theorem is a consequence of (28).

(30) $(\text{Basel-seq}^1)(m) \leqslant \sum_{\kappa=0}^{m} \text{Basel-seq}(\kappa)$. The theorem is a consequence of (28).

(31) $\sum_{\kappa=0}^{m} \text{Basel-seq}(\kappa) \leqslant (\text{Basel-seq}^2)(m)$. The theorem is a consequence of (29).

(32) BASEL PROBLEM:
$\sum \text{Basel-seq} = \frac{\pi^{\mathbf{2}}}{6}$. The theorem is a consequence of (30) and (31).

Note that $(\sum_{\alpha=0}^{\kappa}(\text{Basel-seq})(\alpha))_{\kappa\in\mathbb{N}}$ is non summable as a sequence of real numbers.

## References


[1] M. Aigner and G. M. Ziegler. *Proofs from THE BOOK*. Springer-Verlag, Berlin Heidelberg New York, 2004.

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

[3] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, Karol Pąk, and Josef Urban. Mizar: State-of-the-art and beyond. In Manfred Kerber, Jacques Carette, Cezary Kaliszyk, Florian Rabe, and Volker Sorge, editors, *Intelligent Computer Mathematics*, volume 9150 of *Lecture Notes in Computer Science*, pages 261–279. Springer International Publishing, 2015. ISBN 978-3-319-20614-1. doi:10.1007/978-3-319-20615-8_17.

[4] Czesław Byliński. The complex numbers. *Formalized Mathematics*, 1(**3**):507–513, 1990.

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

[6] Augustin Louis Cauchy. *Cours d'analyse de l'Ecole royale polytechnique*. de l'Imprimerie royale, 1821.

[7] Artur Korniłowicz and Karol Pąk. Basel problem – preliminaries. *Formalized Mathematics*, 25(**2**):141–147, 2017. doi:10.1515/forma-2017-0013.

[8] Anna Justyna Milewska. The field of complex numbers. *Formalized Mathematics*, 9(**2**): 265–269, 2001.

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

[10] Robert Milewski. The evaluation of polynomials. *Formalized Mathematics*, 9(**2**):391–395, 2001.

[11] Robert Milewski. Fundamental theorem of algebra. *Formalized Mathematics*, 9(**3**):461–470, 2001.

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

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

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

[15] Wojciech A. Trybulec. Non-contiguous substrings and one-to-one finite sequences. *Formalized Mathematics*, 1(**3**):569–573, 1990.


*Received June 27, 2017*

---

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

FORMALIZED MATHEMATICS
Vol. 25, No. 2, Pages 157–169, 2017
DOI: 10.1515/forma-2017-0015

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

# Dual Lattice of $\mathbb{Z}$-module Lattice[1]

Yuichi Futa
Tokyo University of Technology
Tokyo, Japan

Yasunari Shidama
Shinshu University
Nagano, Japan

**Summary.** In this article, we formalize in Mizar [5] the definition of dual lattice and their properties. We formally prove that a set of all dual vectors in a rational lattice has the construction of a lattice. We show that a dual basis can be calculated by elements of an inverse of the Gram Matrix. We also formalize a summation of inner products and their properties. Lattice of $\mathbb{Z}$-module is necessary for lattice problems, LLL(Lenstra, Lenstra and Lovász) base reduction algorithm and cryptographic systems with lattice [20], [10] and [19].

MSC: 15A03 15A09 03B35

Keywords: $\mathbb{Z}$-lattice; dual lattice of $\mathbb{Z}$-lattice; dual basis of $\mathbb{Z}$-lattice

MML identifier: ZMODLAT3, version: 8.1.06 5.43.1297

## 1. Summation of Inner Products

Now we state the proposition:

(1) Let us consider a rational $\mathbb{Z}$-lattice $L$, and a $\mathbb{Z}$-lattice $L_1$. Suppose $L_1$ is a submodule of DivisibleMod$(L)$ and the scalar product of $L_1$ = ScProductDM$(L) \restriction$ (the carrier of $L_1$). Then $L_1$ is rational.

Proof: For every vectors $v$, $u$ of $L_1$, $\langle v, u\rangle \in \mathbb{Q}$ by [14, (25)], [7, (49)]. $\square$

Let $L$ be a rational $\mathbb{Z}$-lattice. Observe that EMLat$(L)$ is rational.

Let $r$ be an element of $\mathbb{F}_{\mathbb{Q}}$. Let us note that EMLat$(r, L)$ is rational.

Let $L$ be a $\mathbb{Z}$-lattice, $F$ be a finite sequence of elements of $L$, $f$ be a function from $L$ into $\mathbb{Z}^{\mathrm{R}}$, and $v$ be a vector of $L$. The functor ScFS$(v, f, F)$ yielding a finite sequence of elements of $\mathbb{R}_{\mathrm{F}}$ is defined by

[1]This work was supported by JSPS KAKENHI grant number JP15K00183.




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

(Def. 1) $\operatorname{len} it = \operatorname{len} F$ and for every natural number $i$ such that $i \in \operatorname{dom} it$ holds $it(i) = \langle v, f(F_i) \cdot F_i \rangle$.

Now we state the propositions:

(2) Let us consider a $\mathbb{Z}$-lattice $L$, a function $f$ from $L$ into $\mathbb{Z}^{\mathrm{R}}$, a finite sequence $F$ of elements of $L$, vectors $v$, $u$ of $L$, and a natural number $i$. Suppose $i \in \operatorname{dom} F$ and $u = F(i)$. Then $(\operatorname{ScFS}(v, f, F))(i) = \langle v, f(u) \cdot u \rangle$.

(3) Let us consider a $\mathbb{Z}$-lattice $L$, a function $f$ from $L$ into $\mathbb{Z}^{\mathrm{R}}$, and vectors $v$, $u$ of $L$. Then $\operatorname{ScFS}(v, f, \langle u \rangle) = \langle \langle v, f(u) \cdot u \rangle \rangle$.

(4) Let us consider a $\mathbb{Z}$-lattice $L$, a function $f$ from $L$ into $\mathbb{Z}^{\mathrm{R}}$, finite sequences $F$, $G$ of elements of $L$, and a vector $v$ of $L$. Then $\operatorname{ScFS}(v, f, F \frown G) = \operatorname{ScFS}(v, f, F) \frown \operatorname{ScFS}(v, f, G)$.

Let $L$ be a $\mathbb{Z}$-lattice, $l$ be a linear combination of $L$, and $v$ be a vector of $L$. The functor $\operatorname{SumSc}(v, l)$ yielding an element of $\mathbb{R}_{\mathrm{F}}$ is defined by

(Def. 2) there exists a finite sequence $F$ of elements of $L$ such that $F$ is one-to-one and $\operatorname{rng} F =$ the support of $l$ and $it = \sum \operatorname{ScFS}(v, l, F)$.

Now we state the propositions:

(5) Let us consider a $\mathbb{Z}$-lattice $L$, and a vector $v$ of $L$. Then $\operatorname{SumSc}(v, \mathbf{0}_{\mathrm{LC}_L}) = 0_{\mathbb{R}_{\mathrm{F}}}$.

(6) Let us consider a $\mathbb{Z}$-lattice $L$, a vector $v$ of $L$, and a linear combination $l$ of $\emptyset_\alpha$. Then $\operatorname{SumSc}(v, l) = 0_{\mathbb{R}_{\mathrm{F}}}$, where $\alpha$ is the carrier of $L$. The theorem is a consequence of (5).

(7) Let us consider a $\mathbb{Z}$-lattice $L$, a vector $v$ of $L$, and a linear combination $l$ of $L$. Suppose the support of $l = \emptyset$. Then $\operatorname{SumSc}(v, l) = 0_{\mathbb{R}_{\mathrm{F}}}$. The theorem is a consequence of (5).

(8) Let us consider a $\mathbb{Z}$-lattice $L$, vectors $v$, $u$ of $L$, and a linear combination $l$ of $\{u\}$. Then $\operatorname{SumSc}(v, l) = \langle v, l(u) \cdot u \rangle$. The theorem is a consequence of (5) and (3).

(9) Let us consider a $\mathbb{Z}$-lattice $L$, a vector $v$ of $L$, and linear combinations $l_1$, $l_2$ of $L$. Then $\operatorname{SumSc}(v, l_1 + l_2) = \operatorname{SumSc}(v, l_1) + \operatorname{SumSc}(v, l_2)$.
PROOF: Set $A =$ ((the support of $l_1+l_2$)$\cup$(the support of $l_1$))$\cup$(the support of $l_2$). Set $C_1 = A \setminus$ (the support of $l_1$). Consider $p$ being a finite sequence such that $\operatorname{rng} p = C_1$ and $p$ is one-to-one. Set $C_3 = A \setminus$ (the support of $l_1+l_2$). Consider $r$ being a finite sequence such that $\operatorname{rng} r = C_3$ and $r$ is one-to-one. Set $C_2 = A \setminus$ (the support of $l_2$). Consider $q$ being a finite sequence such that $\operatorname{rng} q = C_2$ and $q$ is one-to-one. Consider $F$ being a finite sequence of elements of $L$ such that $F$ is one-to-one and $\operatorname{rng} F =$ the support of $l_1+l_2$ and $\operatorname{SumSc}(w, l_1+l_2) = \sum \operatorname{ScFS}(w, l_1+l_2, F)$. Set $F_1 = F \frown r$. Consider $G$ being a finite sequence of elements of $L$ such that $G$ is one-to-one and

rng $G$ = the support of $l_1$ and $\mathrm{SumSc}(w, l_1) = \sum \mathrm{ScFS}(w, l_1, G)$. Set $G_3 = G \frown p$. rng $F$ misses rng $r$. rng $G$ misses rng $p$. Define $\mathcal{F}(\text{natural number}) = F_1 \leftarrow (G_3(\$_1))$. Consider $P$ being a finite sequence such that len $P$ = len $F_1$ and for every natural number $k$ such that $k \in \operatorname{dom} P$ holds $P(k) = \mathcal{F}(k)$ from [4, Sch. 2]. rng $P \subseteq \operatorname{dom} F_1$ by [22, (29)], [23, (8)]. $\operatorname{dom} F_1 \subseteq$ rng $P$ by [7, (33)], [27, (28), (36)], [7, (39)]. Set $g = \mathrm{ScFS}(w, l_1, G_3)$. Set $f = \mathrm{ScFS}(w, l_1 + l_2, F_1)$. Consider $H$ being a finite sequence of elements of $L$ such that $H$ is one-to-one and rng $H$ = the support of $l_2$ and $\sum \mathrm{ScFS}(w, l_2, H) = \mathrm{SumSc}(w, l_2)$. Set $H_1 = H \frown q$. rng $H$ misses rng $q$. Define $\mathcal{F}(\text{natural number}) = H_1 \leftarrow (G_3(\$_1))$. Consider $R$ being a finite sequence such that len $R$ = len $H_1$ and for every natural number $k$ such that $k \in \operatorname{dom} R$ holds $R(k) = \mathcal{F}(k)$ from [4, Sch. 2]. rng $R \subseteq \operatorname{dom} H_1$ by [22, (29)], [23, (8)]. $\operatorname{dom} H_1 \subseteq$ rng $R$ by [7, (33)], [27, (28), (36)], [7, (39)]. Set $h = \mathrm{ScFS}(w, l_2, H_1)$. $\sum h = \sum(\mathrm{ScFS}(w, l_2, H) \frown \mathrm{ScFS}(w, l_2, q))$. $\sum g = \sum(\mathrm{ScFS}(w, l_1, G) \frown \mathrm{ScFS}(w, l_1, p))$. Reconsider $H_2 = h \cdot R$ as a finite sequence of elements of $\mathbb{R}_{\mathrm{F}}$. $\sum f = \sum(\mathrm{ScFS}(w, l_1 + l_2, F) \frown \mathrm{ScFS}(w, l_1 + l_2, r))$. Define $\mathcal{F}(\text{natural number}) = g_{\$_1} + H_{2\$_1}$. Consider $I$ being a finite sequence such that len $I$ = len $G_3$ and for every natural number $k$ such that $k \in \operatorname{dom} I$ holds $I(k) = \mathcal{F}(k)$ from [4, Sch. 2]. rng $I \subseteq$ the carrier of $\mathbb{R}_{\mathrm{F}}$. □

(10) Let us consider a $\mathbb{Z}$-lattice $L$, a linear combination $l$ of $L$, and a vector $v$ of $L$. Then $\langle v, \sum l \rangle = \mathrm{SumSc}(v, l)$.

Proof: Define $\mathcal{P}[\text{natural number}] \equiv$ for every $\mathbb{Z}$-lattice $L$ for every linear combination $l$ of $L$ for every vector $v$ of $L$ such that $\overline{\overline{\text{the support of } l}} = \$_1$ holds $\langle v, \sum l \rangle = \mathrm{SumSc}(v, l)$. $\mathcal{P}[0]$ by [24, (19)], [11, (12)], (7). For every natural number $n$ such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$ by [2, (44)], [9, (31)], [2, (42)], [24, (7)]. For every natural number $n$, $\mathcal{P}[n]$ from [3, Sch. 2]. □

Let $L$ be a $\mathbb{Z}$-lattice, $F$ be a finite sequence of elements of DivisibleMod($L$), $f$ be a function from DivisibleMod($L$) into $\mathbb{Z}^{\mathrm{R}}$, and $v$ be a vector of DivisibleMod($L$). The functor $\mathrm{ScFS}(v, f, F)$ yielding a finite sequence of elements of $\mathbb{R}_{\mathrm{F}}$ is defined by

(Def. 3) len *it* = len $F$ and for every natural number $i$ such that $i \in \operatorname{dom} it$ holds $it(i) = (\mathrm{ScProductDM}(L))(v, f(F_i) \cdot F_i)$.

Now we state the propositions:

(11) Let us consider a $\mathbb{Z}$-lattice $L$, a function $f$ from DivisibleMod($L$) into $\mathbb{Z}^{\mathrm{R}}$, a finite sequence $F$ of elements of DivisibleMod($L$), vectors $v$, $u$ of DivisibleMod($L$), and a natural number $i$. Suppose $i \in \operatorname{dom} F$ and $u = F(i)$. Then $(\mathrm{ScFS}(v, f, F))(i) = (\mathrm{ScProductDM}(L))(v, f(u) \cdot u)$.

(12) Let us consider a $\mathbb{Z}$-lattice $L$, a function $f$ from DivisibleMod($L$) into

$\mathbb{Z}^{\mathrm{R}}$, and vectors $v$, $u$ of DivisibleMod($L$).
Then $\mathrm{ScFS}(v, f, \langle u \rangle) = \langle (\mathrm{ScProductDM}(L))(v, f(u) \cdot u) \rangle$.

(13) Let us consider a $\mathbb{Z}$-lattice $L$, a function $f$ from DivisibleMod($L$) into $\mathbb{Z}^{\mathrm{R}}$, finite sequences $F$, $G$ of elements of DivisibleMod($L$), and a vector $v$ of DivisibleMod($L$). Then $\mathrm{ScFS}(v, f, F \frown G) = \mathrm{ScFS}(v, f, F) \frown \mathrm{ScFS}(v, f, G)$.

Let $L$ be a $\mathbb{Z}$-lattice, $l$ be a linear combination of DivisibleMod($L$), and $v$ be a vector of DivisibleMod($L$). The functor SumSc($v, l$) yielding an element of $\mathbb{R}_{\mathrm{F}}$ is defined by

(Def. 4) there exists a finite sequence $F$ of elements of DivisibleMod($L$) such that $F$ is one-to-one and $\mathrm{rng}\, F =$ the support of $l$ and $it = \sum \mathrm{ScFS}(v, l, F)$.

Now we state the propositions:

(14) Let us consider a $\mathbb{Z}$-lattice $L$, and a vector $v$ of DivisibleMod($L$). Then $\mathrm{SumSc}(v, \mathbf{0}_{\mathrm{LC}_{\mathrm{DivisibleMod}(L)}}) = 0_{\mathbb{R}_{\mathrm{F}}}$.

(15) Let us consider a $\mathbb{Z}$-lattice $L$, a vector $v$ of DivisibleMod($L$), and a linear combination $l$ of $\emptyset_{\alpha}$. Then $\mathrm{SumSc}(v, l) = 0_{\mathbb{R}_{\mathrm{F}}}$, where $\alpha$ is the carrier of DivisibleMod($L$). The theorem is a consequence of (14).

(16) Let us consider a $\mathbb{Z}$-lattice $L$, a vector $v$ of DivisibleMod($L$), and a linear combination $l$ of DivisibleMod($L$). Suppose the support of $l = \emptyset$. Then $\mathrm{SumSc}(v, l) = 0_{\mathbb{R}_{\mathrm{F}}}$. The theorem is a consequence of (14).

(17) Let us consider a $\mathbb{Z}$-lattice $L$, vectors $v$, $u$ of DivisibleMod($L$), and a linear combination $l$ of $\{u\}$. Then $\mathrm{SumSc}(v, l) = (\mathrm{ScProductDM}(L))(v, l(u) \cdot u)$. The theorem is a consequence of (14) and (12).

(18) Let us consider a $\mathbb{Z}$-lattice $L$, a vector $v$ of DivisibleMod($L$), and linear combinations $l_1$, $l_2$ of DivisibleMod($L$). Then $\mathrm{SumSc}(v, l_1 + l_2) = \mathrm{SumSc}(v, l_1) + \mathrm{SumSc}(v, l_2)$.
PROOF: Set $A =$ ((the support of $l_1 + l_2$) $\cup$ (the support of $l_1$)) $\cup$ (the support of $l_2$). Set $C_1 = A \setminus$ (the support of $l_1$). Consider $p$ being a finite sequence such that $\mathrm{rng}\, p = C_1$ and $p$ is one-to-one. Set $C_3 = A \setminus$ (the support of $l_1 + l_2$). Consider $r$ being a finite sequence such that $\mathrm{rng}\, r = C_3$ and $r$ is one-to-one. Set $C_2 = A \setminus$ (the support of $l_2$). Consider $q$ being a finite sequence such that $\mathrm{rng}\, q = C_2$ and $q$ is one-to-one. Consider $F$ being a finite sequence of elements of DivisibleMod($L$) such that $F$ is one-to-one and $\mathrm{rng}\, F =$ the support of $l_1 + l_2$ and $\mathrm{SumSc}(w, l_1 + l_2) = \sum \mathrm{ScFS}(w, l_1 + l_2, F)$. Set $F_1 = F \frown r$. Consider $G$ being a finite sequence of elements of DivisibleMod($L$) such that $G$ is one-to-one and $\mathrm{rng}\, G =$ the support of $l_1$ and $\mathrm{SumSc}(w, l_1) = \sum \mathrm{ScFS}(w, l_1, G)$. Set $G_3 = G \frown p$. $\mathrm{rng}\, F$ misses $\mathrm{rng}\, r$. $\mathrm{rng}\, G$ misses $\mathrm{rng}\, p$. Define $\mathcal{F}(\text{natural number}) = F_1 \leftarrow (G_3(\$_1))$. Consider $P$ being a finite sequence such that $\mathrm{len}\, P = \mathrm{len}\, F_1$ and for every natural number $k$ such that $k \in \mathrm{dom}\, P$ holds $P(k) = \mathcal{F}(k)$ from

[4, Sch. 2]. $\operatorname{rng} P \subseteq \operatorname{dom} F_1$ by [22, (29)], [23, (8)]. $\operatorname{dom} F_1 \subseteq \operatorname{rng} P$ by [7, (33)], [27, (28), (36)], [7, (39)]. Set $g = \mathrm{ScFS}(w, l_1, G_3)$. Set $f = \mathrm{ScFS}(w, l_1 + l_2, F_1)$. Consider $H$ being a finite sequence of elements of DivisibleMod$(L)$ such that $H$ is one-to-one and $\operatorname{rng} H =$ the support of $l_2$ and $\sum \mathrm{ScFS}(w, l_2, H) = \mathrm{SumSc}(w, l_2)$. Set $H_1 = H \frown q$. $\operatorname{rng} H$ misses $\operatorname{rng} q$. Define $\mathcal{F}$(natural number) $= H_1 \leftarrow (G_3(\$_1))$. Consider $R$ being a finite sequence such that $\operatorname{len} R = \operatorname{len} H_1$ and for every natural number $k$ such that $k \in \operatorname{dom} R$ holds $R(k) = \mathcal{F}(k)$ from [4, Sch. 2]. $\operatorname{rng} R \subseteq \operatorname{dom} H_1$ by [22, (29)], [23, (8)]. $\operatorname{dom} H_1 \subseteq \operatorname{rng} R$ by [7, (33)], [27, (28), (36)], [7, (39)]. Set $h = \mathrm{ScFS}(w, l_2, H_1)$. $\sum h = \sum(\mathrm{ScFS}(w, l_2, H) \frown \mathrm{ScFS}(w, l_2, q))$. $\sum g = \sum(\mathrm{ScFS}(w, l_1, G) \frown \mathrm{ScFS}(w, l_1, p))$. Reconsider $H_2 = h \cdot R$ as a finite sequence of elements of $\mathbb{R}_{\mathrm{F}}$. $\sum f = \sum(\mathrm{ScFS}(w, l_1 + l_2, F) \frown \mathrm{ScFS}(w, l_1 + l_2, r))$. Define $\mathcal{F}$(natural number) $= g_{\$_1} + H_{2\$_1}$. Consider $I$ being a finite sequence such that $\operatorname{len} I = \operatorname{len} G_3$ and for every natural number $k$ such that $k \in \operatorname{dom} I$ holds $I(k) = \mathcal{F}(k)$ from [4, Sch. 2]. $\operatorname{rng} I \subseteq$ the carrier of $\mathbb{R}_{\mathrm{F}}$. □

(19) Let us consider a $\mathbb{Z}$-lattice $L$, a linear combination $l$ of DivisibleMod$(L)$, and a vector $v$ of DivisibleMod$(L)$. Then $(\mathrm{ScProductDM}(L))(v, \sum l) = \mathrm{SumSc}(v, l)$.

PROOF: Define $\mathcal{P}$[natural number] $\equiv$ for every $\mathbb{Z}$-lattice $L$ for every linear combination $l$ of DivisibleMod$(L)$ for every vector $v$ of DivisibleMod$(L)$ such that $\overline{\overline{\text{the support of } l}} = \$_1$ holds $(\mathrm{ScProductDM}(L))(v, \sum l) = \mathrm{SumSc}(v, l)$. $\mathcal{P}[0]$ by [24, (19)], [12, (14)], (16). For every natural number $n$ such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$ by [2, (44)], [9, (31)], [2, (42)], [24, (7)]. For every natural number $n$, $\mathcal{P}[n]$ from [3, Sch. 2]. □

(20) Let us consider a natural number $n$, a square matrix $M$ over $\mathbb{R}_{\mathrm{F}}$ of dimension $n$, and a square matrix $H$ over $\mathbb{F}_{\mathbb{Q}}$ of dimension $n$. Suppose $M = H$ and $M$ is invertible. Then

(i) $H$ is invertible, and

(ii) $M^{\smile} = H^{\smile}$.

PROOF: For every natural numbers $i$, $j$ such that $\langle i, j \rangle \in$ the indices of $M^{\smile}$ holds $M^{\smile}{}_{i,j} = H^{\smile}{}_{i,j}$ by [9, (87)], [12, (52), (54), (47)]. □

(21) Let us consider a natural number $n$, and a square matrix $M$ over $\mathbb{R}_{\mathrm{F}}$ of dimension $n$. Suppose $M$ is square matrix over $\mathbb{F}_{\mathbb{Q}}$ of dimension $n$ and invertible. Then $M^{\smile}$ is a square matrix over $\mathbb{F}_{\mathbb{Q}}$ of dimension $n$. The theorem is a consequence of (20).

(22) Let us consider a non trivial, rational, positive definite $\mathbb{Z}$-lattice $L$, and an ordered basis $b$ of $L$. Then $(\mathrm{GramMatrix}(b))^{\smile}$ is a square matrix over $\mathbb{F}_{\mathbb{Q}}$ of dimension $\dim(L)$. The theorem is a consequence of (21).

(23) Let us consider a finite subset $X$ of $\mathbb{Q}$. Then there exists an element $a$ of $\mathbb{Z}$ such that

(i) $a \neq 0$, and

(ii) for every element $r$ of $\mathbb{Q}$ such that $r \in X$ holds $a \cdot r \in \mathbb{Z}$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ for every finite subset $X$ of $\mathbb{Q}$ such that $\overline{\overline{X}} = \$_1$ there exists an element $a$ of $\mathbb{Z}$ such that $a \neq 0$ and for every element $r$ of $\mathbb{Q}$ such that $r \in X$ holds $a \cdot r \in \mathbb{Z}$. $\mathcal{P}[0]$. For every natural number $n$ such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$ by [26, (41)], [2, (44)], [1, (30)], [17, (1)]. For every natural number $n$, $\mathcal{P}[n]$ from [3, Sch. 2]. $\square$

(24) Let us consider a non trivial, rational, positive definite $\mathbb{Z}$-lattice $L$, and an ordered basis $b$ of $L$. Then there exists an element $a$ of $\mathbb{R}_{\mathrm{F}}$ such that

(i) $a$ is an element of $\mathbb{Z}^{\mathrm{R}}$, and

(ii) $a \neq 0$, and

(iii) $a \cdot (\mathrm{GramMatrix}(b))^{\smile}$ is a square matrix over $\mathbb{Z}^{\mathrm{R}}$ of dimension $\dim(L)$.

PROOF: Set $G = (\mathrm{GramMatrix}(b))^{\smile}$. For every natural numbers $i$, $j$ such that $\langle i, j\rangle \in$ the indices of $G$ holds $G_{i,j} \in$ the carrier of $\mathbb{F}_{\mathbb{Q}}$ by [9, (87)], [7, (3)]. Define $\mathcal{F}(\text{natural number}, \text{natural number}) = G_{\$_1,\$_2}$. Set $D_3 = \{\mathcal{F}(u,v)$, where $u$ is an element of $\mathbb{N}, v$ is an element of $\mathbb{N} : u \in \mathrm{Seg}\,\mathrm{len}\,G$ and $v \in \mathrm{Seg}\,\mathrm{width}\,G\}$. $D_3$ is finite from [21, Sch. 22]. $\{G_{i,j}$, where $i, j$ are natural numbers : $\langle i, j\rangle \in$ the indices of $G\} \subseteq D_3$ by [9, (87)]. $\{G_{i,j}$, where $i, j$ are natural numbers : $\langle i, j\rangle \in$ the indices of $G\} \subseteq$ the carrier of $\mathbb{F}_{\mathbb{Q}}$. Reconsider $X = \{G_{i,j}$, where $i, j$ are natural numbers : $\langle i, j\rangle \in$ the indices of $G\}$ as a finite subset of $\mathbb{F}_{\mathbb{Q}}$. Consider $a$ being an element of $\mathbb{Z}$ such that $a \neq 0$ and for every element $r$ of $\mathbb{Q}$ such that $r \in X$ holds $a \cdot r \in \mathbb{Z}$. For every natural numbers $i$, $j$ such that $\langle i, j\rangle \in$ the indices of $a \cdot G$ holds $(a \cdot G)_{i,j} \in$ the carrier of $\mathbb{Z}^{\mathrm{R}}$. $\square$

(25) Let us consider a non trivial, rational, positive definite $\mathbb{Z}$-lattice $L$, an ordered basis $b$ of $\mathrm{EMLat}(L)$, and a natural number $i$. Suppose $i \in \mathrm{dom}\,b$. Then there exists a vector $v$ of $\mathrm{DivisibleMod}(L)$ such that

(i) $(\mathrm{ScProductDM}(L))(b_i, v) = 1$, and

(ii) for every natural number $j$ such that $i \neq j$ and $j \in \mathrm{dom}\,b$ holds $(\mathrm{ScProductDM}(L))(b_j, v) = 0$.

PROOF: Consider $a$ being an element of $\mathbb{R}_{\mathrm{F}}$ such that $a$ is an element of $\mathbb{Z}^{\mathrm{R}}$ and $a \neq 0$ and $a \cdot (\mathrm{GramMatrix}(b))^{\smile}$ is a square matrix over $\mathbb{Z}^{\mathrm{R}}$ of dimension $\dim(L)$. For every natural number $j$ such that $i \neq j$ and $j \in \mathrm{dom}\,b$ holds $\mathrm{Line}(a \cdot (\mathrm{GramMatrix}(b))^{\smile}, i) \cdot (\mathrm{GramMatrix}(b))_{\square,j} = 0$ by [9, (87)]. Reconsider $I = \mathrm{rng}\,b$ as a basis of $\mathrm{EMLat}(L)$. Define

$\mathcal{P}$[object, object] $\equiv$ if $\$_1 \in I$, then for every natural number $n$ such that $n = b^{-1}(\$_1)$ and $n \in \operatorname{dom} b$ holds $\$_2 = (a \cdot (\mathrm{GramMatrix}(b))^{\smile})_{i,n}$ and if $\$_1 \notin I$, then $\$_2 = 0_{\mathbb{Z}^{\mathrm{R}}}$. For every element $x$ of EMLat($L$), there exists an element $y$ of $\mathbb{Z}^{\mathrm{R}}$ such that $\mathcal{P}[x, y]$ by [7, (32)], [9, (87)], [16, (1)]. Consider $l$ being a function from EMLat($L$) into $\mathbb{Z}^{\mathrm{R}}$ such that for every element $x$ of EMLat($L$), $\mathcal{P}[x, l(x)]$ from [8, Sch. 3]. Reconsider $a_2 = a$ as an element of $\mathbb{Z}^{\mathrm{R}}$. For every natural number $k$ such that $1 \leqslant k \leqslant \operatorname{len} \mathrm{ScFS}(b_i, l, b)$ holds $(\mathrm{Line}(a \cdot (\mathrm{GramMatrix}(b))^{\smile}, i) \bullet (\mathrm{GramMatrix}(b))_{\square,i})(k) = (\mathrm{ScFS}(b_i, l, b))(k)$ by [22, (25)], [7, (3), (34)], [6, (72)]. The support of $l \subseteq \operatorname{rng} b$. For every natural number $j$ such that $i \neq j$ and $j \in \operatorname{dom} b$ holds $\langle b_j, \sum l \rangle = 0$ by [6, (72)], [22, (25)], [7, (3), (34)]. Consider $u$ being a vector of DivisibleMod($L$) such that $a_2 \cdot u = \sum l$. For every natural number $j$ such that $i \neq j$ and $j \in \operatorname{dom} b$ holds $(\mathrm{ScProductDM}(L))(b_j, u) = 0$ by [14, (24)], [12, (13), (8)]. □

## 2. Dual Lattice

Let $L$ be a $\mathbb{Z}$-lattice.

A dual of $L$ is a vector of DivisibleMod($L$) and is defined by

(Def. 5) for every vector $v$ of DivisibleMod($L$) such that $v \in \mathrm{Embedding}(L)$ holds $(\mathrm{ScProductDM}(L))(it, v) \in \mathbb{Z}^{\mathrm{R}}$.

Now we state the propositions:

(26) Let us consider a $\mathbb{Z}$-lattice $L$. Then $0_{\mathrm{DivisibleMod}(L)}$ is a dual of $L$.

(27) Let us consider a $\mathbb{Z}$-lattice $L$, and duals $v$, $u$ of $L$. Then $v + u$ is a dual of $L$.

Proof: For every vector $x$ of DivisibleMod($L$) such that $x \in \mathrm{Embedding}(L)$ holds $(\mathrm{ScProductDM}(L))(v + u, x) \in \mathbb{Z}^{\mathrm{R}}$ by [12, (6)]. □

(28) Let us consider a $\mathbb{Z}$-lattice $L$, a dual $v$ of $L$, and an element $a$ of $\mathbb{Z}^{\mathrm{R}}$. Then $a \cdot v$ is a dual of $L$.

Proof: For every vector $x$ of DivisibleMod($L$) such that $x \in \mathrm{Embedding}(L)$ holds $(\mathrm{ScProductDM}(L))(a \cdot v, x) \in \mathbb{Z}^{\mathrm{R}}$ by [12, (6)]. □

Let $L$ be a $\mathbb{Z}$-lattice. The functor DualSet($L$) yielding a non empty subset of DivisibleMod($L$) is defined by the term

(Def. 6) the set of all $v$ where $v$ is a dual of $L$.

Note that DualSet($L$) is linearly closed.

The functor DualLatMod($L$) yielding a strict, non empty structure of $\mathbb{Z}$-lattice over $\mathbb{Z}^{\mathrm{R}}$ is defined by

(Def. 7) the carrier of $it$ = DualSet($L$) and the addition of $it$ = (the addition of DivisibleMod($L$)) $\restriction$ DualSet($L$) and the zero of $it$ = $0_{\mathrm{DivisibleMod}(L)}$ and the left multiplication of $it$ = (the left multiplication of DivisibleMod($L$))$\restriction$ ((the carrier of $\mathbb{Z}^{\mathrm{R}}$) $\times$ DualSet($L$)) and the scalar product of $it$ = ScProductDM($L$)$\restriction$(DualSet($L$) $\times$ DualSet($L$)).

Now we state the propositions:

(29) Let us consider a $\mathbb{Z}$-lattice $L$. Then DualLatMod($L$) is a submodule of DivisibleMod($L$).

(30) Let us consider a $\mathbb{Z}$-lattice $L$, a vector $v$ of DivisibleMod($L$), and a basis $I$ of Embedding($L$). Suppose for every vector $u$ of DivisibleMod($L$) such that $u \in I$ holds (ScProductDM($L$))$(v, u) \in \mathbb{Z}^{\mathrm{R}}$. Then $v$ is a dual of $L$.
PROOF: Define $\mathcal{P}$[natural number] $\equiv$ for every finite subset $I$ of Embedding ($L$) such that $\overline{\overline{I}} = \$_1$ and $I$ is linearly independent and for every vector $u$ of DivisibleMod($L$) such that $u \in I$ holds (ScProductDM($L$))$(v, u) \in \mathbb{Z}^{\mathrm{R}}$ for every vector $w$ of DivisibleMod($L$) such that $w \in$ Lin($I$) holds (ScProductDM($L$))$(v, w) \in \mathbb{Z}^{\mathrm{R}}$. $\mathcal{P}[0]$ by [15, (67), (66)], [12, (6)]. For every natural number $n$ such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$ by [26, (41)], [2, (44)], [1, (30)], [9, (31)]. For every natural number $n$, $\mathcal{P}[n]$ from [3, Sch. 2]. $\square$

Let $L$ be a rational, positive definite $\mathbb{Z}$-lattice and $I$ be a basis of EMLat($L$). The functor DualBasis($I$) yielding a subset of DivisibleMod($L$) is defined by

(Def. 8) for every vector $v$ of DivisibleMod($L$), $v \in it$ iff there exists a vector $u$ of EMLat($L$) such that $u \in I$ and (ScProductDM($L$))$(u, v) = 1$ and for every vector $w$ of EMLat($L$) such that $w \in I$ and $u \neq w$ holds (ScProductDM($L$))$(w, v) = 0$.

The functor B2DB($I$) yielding a function from $I$ into DualBasis($I$) is defined by

(Def. 9) dom $it = I$ and rng $it$ = DualBasis($I$) and for every vector $v$ of EMLat($L$) such that $v \in I$ holds (ScProductDM($L$))$(v, it(v)) = 1$ and for every vector $w$ of EMLat($L$) such that $w \in I$ and $v \neq w$ holds (ScProductDM($L$))$(w, it(v)) = 0$.

Observe that B2DB($I$) is onto and one-to-one.

Now we state the proposition:

(31) Let us consider a rational, positive definite $\mathbb{Z}$-lattice $L$, and a basis $I$ of EMLat($L$). Then $\overline{\overline{I}} = \overline{\overline{\mathrm{DualBasis}(I)}}$.

Let $L$ be a rational, positive definite $\mathbb{Z}$-lattice and $I$ be a basis of EMLat($L$). Note that DualBasis($I$) is finite.

Let $L$ be a non trivial, rational, positive definite $\mathbb{Z}$-lattice.

Note that DualBasis($I$) is non empty.

Now we state the propositions:

(32) Let us consider a rational, positive definite $\mathbb{Z}$-lattice $L$, a basis $I$ of $\mathrm{EMLat}(L)$, a vector $v$ of $\mathrm{DivisibleMod}(L)$, and a linear combination $l$ of $\mathrm{DualBasis}(I)$. If $v \in I$, then $(\mathrm{ScProductDM}(L))(v, \sum l) = l((\mathrm{B2DB}(I))(v))$. The theorem is a consequence of (19), (17), and (18).

(33) Let us consider a rational, positive definite $\mathbb{Z}$-lattice $L$, a basis $I$ of $\mathrm{EMLat}(L)$, and a vector $v$ of $\mathrm{DivisibleMod}(L)$. If $v$ is a dual of $L$, then $v \in \mathrm{Lin}(\mathrm{DualBasis}(I))$.
PROOF: Set $f = (\mathrm{B2DB}(I))^{-1}$. Define $\mathcal{P}[\text{object}, \text{object}] \equiv$ if $\$_1 \in \mathrm{DualBasis}(I)$, then $\$_2 = (\mathrm{ScProductDM}(L))(f(\$_1), v)$ and if $\$_1 \notin \mathrm{DualBasis}(I)$, then $\$_2 = 0_{\mathbb{Z}^{\mathrm{R}}}$. For every object $x$ such that $x \in$ the carrier of $\mathrm{DivisibleMod}(L)$ there exists an object $y$ such that $y \in$ the carrier of $\mathbb{Z}^{\mathrm{R}}$ and $\mathcal{P}[x, y]$ by [7, (33), (3)], [13, (24)], [14, (25)]. Consider $l$ being a function from $\mathrm{DivisibleMod}(L)$ into the carrier of $\mathbb{Z}^{\mathrm{R}}$ such that for every object $x$ such that $x \in$ the carrier of $\mathrm{DivisibleMod}(L)$ holds $\mathcal{P}[x, l(x)]$ from [8, Sch. 1]. The support of $l \subseteq \mathrm{DualBasis}(I)$ by [24, (2)]. Consider $b$ being a finite sequence such that $\mathrm{rng}\, b = I$ and $b$ is one-to-one. For every natural number $n$ such that $n \in \mathrm{dom}\, b$ holds $(\mathrm{ScProductDM}(L))(b_n, v) = (\mathrm{ScProductDM}(L))(b_n, \sum l)$ by [12, (20)], [14, (25)], [7, (3)], [18, (14)]. $\square$

Let $L$ be a rational, positive definite $\mathbb{Z}$-lattice and $I$ be a basis of $\mathrm{EMLat}(L)$. Let us note that $\mathrm{DualBasis}(I)$ is linearly independent.

The functor $\mathrm{DualLat}(L)$ yielding a strict $\mathbb{Z}$-lattice is defined by

(Def. 10) the carrier of $it = \mathrm{DualSet}(L)$ and $0_{it} = 0_{\mathrm{DivisibleMod}(L)}$ and the addition of $it =$ (the addition of $\mathrm{DivisibleMod}(L)$) $\restriction$ (the carrier of $it$) and the left multiplication of $it =$ (the left multiplication of $\mathrm{DivisibleMod}(L)$) $\restriction$ ((the carrier of $\mathbb{Z}^{\mathrm{R}}$) $\times$ (the carrier of $it$)) and the scalar product of $it = \mathrm{ScProductDM}(L) \restriction$ (the carrier of $it$).

Now we state the propositions:

(34) Let us consider a rational, positive definite $\mathbb{Z}$-lattice $L$, and a vector $v$ of $\mathrm{DivisibleMod}(L)$. Then $v \in \mathrm{DualLat}(L)$ if and only if $v$ is a dual of $L$.

(35) Let us consider a rational, positive definite $\mathbb{Z}$-lattice $L$. Then $\mathrm{DualLat}(L)$ is a submodule of $\mathrm{DivisibleMod}(L)$.

Let us consider a $\mathbb{Z}$-lattice $L$. Now we state the propositions:

(36) Every basis of $\mathrm{EMLat}(L)$ is a basis of $\mathrm{Embedding}(L)$.

(37) Every basis of $\mathrm{Embedding}(L)$ is a basis of $\mathrm{EMLat}(L)$.

(38) Let us consider a rational, positive definite $\mathbb{Z}$-lattice $L$, a basis $I$ of $\mathrm{EMLat}(L)$, and a vector $v$ of $\mathrm{DivisibleMod}(L)$. If $v \in \mathrm{DualBasis}(I)$, then

$v$ is a dual of $L$.

PROOF: Consider $u$ being a vector of EMLat($L$) such that $u \in I$ and (ScProductDM($L$))($u, v$) $= 1$ and for every vector $w$ of EMLat($L$) such that $w \in I$ and $u \neq w$ holds (ScProductDM($L$))($w, v$) $= 0$. Reconsider $J = I$ as a basis of Embedding($L$). For every vector $w$ of DivisibleMod($L$) such that $w \in J$ holds (ScProductDM($L$))($v, w$) $\in \mathbb{Z}^{\mathrm{R}}$ by [12, (6)]. □

(39) Let us consider a rational, positive definite $\mathbb{Z}$-lattice $L$, and a basis $I$ of EMLat($L$). Then DualBasis($I$) is a basis of DualLat($L$).

PROOF: Reconsider $D =$ DualLat($L$) as a submodule of DivisibleMod($L$). For every vector $v$ of DivisibleMod($L$) such that $v \in$ DualBasis($I$) holds $v \in$ the carrier of DualLat($L$). For every vector $v$ of DivisibleMod($L$) such that $v \in$ the vector space structure of $D$ holds $v \in$ Lin(DualBasis($I$)). For every vector $v$ of DivisibleMod($L$) such that $v \in$ Lin(DualBasis($I$)) holds $v \in$ the vector space structure of $D$ by [25, (7)], (36), (32), [7, (3)]. □

(40) Let us consider a rational, positive definite $\mathbb{Z}$-lattice $L$, an ordered basis $b$ of EMLat($L$), and a basis $I$ of EMLat($L$). Suppose $I = \operatorname{rng} b$. Then B2DB($I$) $\cdot\, b$ is an ordered basis of DualLat($L$). The theorem is a consequence of (39).

(41) Let us consider a positive definite, finite rank, free $\mathbb{Z}$-lattice $L$, an ordered basis $b$ of $L$, and an ordered basis $e$ of EMLat($L$). Suppose $e =$ MorphsZQ($L$) $\cdot\, b$. Then GramMatrix(InnerProduct $L, b$) $=$ GramMatrix (InnerProduct EMLat($L$), $e$).

PROOF: For every natural numbers $i$, $j$ such that $\langle i, j \rangle \in$ the indices of GramMatrix(InnerProduct $L, b$) holds (GramMatrix(InnerProduct $L, b$))$_{i,j}$ $=$ (GramMatrix(InnerProduct EMLat($L$), $e$))$_{i,j}$ by [9, (87)], [7, (13)]. □

(42) Let us consider a positive definite, finite rank, free $\mathbb{Z}$-lattice $L$. Then GramDet(InnerProduct $L$) $=$ GramDet(InnerProduct EMLat($L$)). The theorem is a consequence of (41).

(43) Let us consider a rational, positive definite $\mathbb{Z}$-lattice $L$. Then $\operatorname{rank} L =$ rank DualLat($L$). The theorem is a consequence of (39) and (31).

(44) Let us consider an integral, positive definite $\mathbb{Z}$-lattice $L$. Then EMLat($L$) is a $\mathbb{Z}$-sublattice of DualLat($L$).

PROOF: DualLat($L$) is a submodule of DivisibleMod($L$). For every vector $v$ of DivisibleMod($L$) such that $v \in$ EMLat($L$) holds $v \in$ DualLat($L$) by (36), [12, (28), (8)], (30). □

(45) Let us consider a $\mathbb{Z}$-lattice $L$, and an ordered basis $b$ of $L$. Suppose GramMatrix(InnerProduct $L, b$) is a square matrix over $\mathbb{Z}^{\mathrm{R}}$ of dimension $\dim(L)$. Then $L$ is integral.

PROOF: Set $I = \operatorname{rng} b$. For every vectors $v$, $u$ of $L$ such that $v, u \in I$ holds

$\langle v, u \rangle \in \mathbb{Z}$ by [6, (10)], [16, (49)], [9, (87)], [16, (1)]. □

(46) Let us consider a $\mathbb{Z}$-lattice $L$, a finite subset $I$ of $L$, and a vector $u$ of $L$. Suppose for every vector $v$ of $L$ such that $v \in I$ holds $\langle v, u \rangle \in \mathbb{Q}$. Let us consider a vector $v$ of $L$. If $v \in \mathrm{Lin}(I)$, then $\langle v, u \rangle \in \mathbb{Q}$.

PROOF: Define $\mathcal{P}$[natural number] $\equiv$ for every finite subset $I$ of $L$ such that $\overline{\overline{I}} = \$_1$ and for every vector $v$ of $L$ such that $v \in I$ holds $\langle v, u \rangle \in \mathbb{Q}$ for every vector $v$ of $L$ such that $v \in \mathrm{Lin}(I)$ holds $\langle v, u \rangle \in \mathbb{Q}$. $\mathcal{P}[0]$ by [15, (67)], [11, (12)]. For every natural number $n$ such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$ by [9, (40)], [15, (72)], [2, (44)], [9, (31)]. For every natural number $n$, $\mathcal{P}[n]$ from [3, Sch. 2]. □

(47) Let us consider a $\mathbb{Z}$-lattice $L$, and a basis $I$ of $L$. Suppose for every vectors $v$, $u$ of $L$ such that $v$, $u \in I$ holds $\langle v, u \rangle \in \mathbb{Q}$. Let us consider vectors $v$, $u$ of $L$. Then $\langle v, u \rangle \in \mathbb{Q}$.

PROOF: Define $\mathcal{P}$[natural number] $\equiv$ for every finite subset $I$ of $L$ such that $\overline{\overline{I}} = \$_1$ and for every vectors $v$, $u$ of $L$ such that $v$, $u \in I$ holds $\langle v, u \rangle \in \mathbb{Q}$ for every vectors $v$, $u$ of $L$ such that $v$, $u \in \mathrm{Lin}(I)$ holds $\langle v, u \rangle \in \mathbb{Q}$. $\mathcal{P}[0]$ by [15, (67)], [11, (12)]. For every natural number $n$ such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$ by [9, (40)], [15, (72)], [2, (44)], [9, (31)]. For every natural number $n$, $\mathcal{P}[n]$ from [3, Sch. 2]. □

(48) Let us consider a $\mathbb{Z}$-lattice $L$, and a basis $I$ of $L$. Suppose for every vectors $v$, $u$ of $L$ such that $v$, $u \in I$ holds $\langle v, u \rangle \in \mathbb{Q}$. Then $L$ is rational. The theorem is a consequence of (47).

(49) Let us consider a $\mathbb{Z}$-lattice $L$, and an ordered basis $b$ of $L$. Suppose $\mathrm{GramMatrix}(\mathrm{InnerProduct}\, L, b)$ is a square matrix over $\mathbb{F}_{\mathbb{Q}}$ of dimension $\dim(L)$. Then $L$ is rational.

PROOF: Set $I = \mathrm{rng}\, b$. For every vectors $v$, $u$ of $L$ such that $v$, $u \in I$ holds $\langle v, u \rangle \in \mathbb{Q}$ by [6, (10)], [16, (49)], [9, (87)], [16, (1)]. □

Let $L$ be a rational, positive definite $\mathbb{Z}$-lattice. One can check that $\mathrm{DualLat}(L)$ is rational.

Now we state the propositions:

(50) Let us consider a rational $\mathbb{Z}$-lattice $L$, a $\mathbb{Z}$-lattice $L_1$, and an ordered basis $b$ of $L_1$. Suppose $L_1$ is a submodule of $\mathrm{DivisibleMod}(L)$ and the scalar product of $L_1 = \mathrm{ScProductDM}(L) \restriction$ (the carrier of $L_1$). Then $\mathrm{GramMatrix}(\mathrm{InnerProduct}\, L_1, b)$ is a square matrix over $\mathbb{F}_{\mathbb{Q}}$ of dimension $\dim(L_1)$. The theorem is a consequence of (1).

(51) Let us consider a rational, positive definite $\mathbb{Z}$-lattice $L$, and an ordered basis $b$ of $\mathrm{DualLat}(L)$. Then $\mathrm{GramMatrix}(\mathrm{InnerProduct}\, \mathrm{DualLat}(L), b)$ is a square matrix over $\mathbb{F}_{\mathbb{Q}}$ of dimension $\dim(L)$. The theorem is a consequence of (35), (43), and (50).

(52) Let us consider a positive definite $\mathbb{Z}$-lattice $L$, and a $\mathbb{Z}$-lattice $L_1$. Suppose $L_1$ is a submodule of DivisibleMod($L$) and the scalar product of $L_1$ = ScProductDM($L$) $\restriction$ (the carrier of $L_1$). Then $L_1$ is positive definite.

PROOF: For every vector $v$ of $L_1$ such that $v \neq 0_{L_1}$ holds $\|v\| > 0$ by [14, (25)], [7, (49)], [13, (29)], [12, (13), (6), (8)]. $\square$

Let $L$ be a rational, positive definite $\mathbb{Z}$-lattice. Note that DualLat($L$) is positive definite.

Let $L$ be a non trivial, rational, positive definite $\mathbb{Z}$-lattice. Let us note that DualLat($L$) is non trivial.

## References


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

[2] Grzegorz Bancerek. Cardinal arithmetics. *Formalized Mathematics*, 1(**3**):543–547, 1990.

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

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

[5] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, Karol Pąk, and Josef Urban. Mizar: State-of-the-art and beyond. In Manfred Kerber, Jacques Carette, Cezary Kaliszyk, Florian Rabe, and Volker Sorge, editors, *Intelligent Computer Mathematics*, volume 9150 of *Lecture Notes in Computer Science*, pages 261–279. Springer International Publishing, 2015. ISBN 978-3-319-20614-1. doi:10.1007/978-3-319-20615-8_17.

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

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

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

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

[10] Wolfgang Ebeling. *Lattices and Codes*. Advanced Lectures in Mathematics. Springer Fachmedien Wiesbaden, 2013.

[11] Yuichi Futa and Yasunari Shidama. Lattice of $\mathbb{Z}$-module. *Formalized Mathematics*, 24 (**1**):49–68, 2016. doi:10.1515/forma-2016-0005.

[12] Yuichi Futa and Yasunari Shidama. Embedded lattice and properties of Gram matrix. *Formalized Mathematics*, 25(**1**):73–86, 2017. doi:10.1515/forma-2017-0007.

[13] Yuichi Futa and Yasunari Shidama. Divisible $\mathbb{Z}$-modules. *Formalized Mathematics*, 24 (**1**):37–47, 2016. doi:10.1515/forma-2016-0004.

[14] Yuichi Futa, Hiroyuki Okazaki, and Yasunari Shidama. $\mathbb{Z}$-modules. *Formalized Mathematics*, 20(**1**):47–59, 2012. doi:10.2478/v10037-012-0007-z.

[15] Yuichi Futa, Hiroyuki Okazaki, and Yasunari Shidama. Quotient module of $\mathbb{Z}$-module. *Formalized Mathematics*, 20(**3**):205–214, 2012. doi:10.2478/v10037-012-0024-y.

[16] Yuichi Futa, Hiroyuki Okazaki, and Yasunari Shidama. Matrix of $\mathbb{Z}$-module. *Formalized Mathematics*, 23(**1**):29–49, 2015. doi:10.2478/forma-2015-0003.

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

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

[19] A. K. Lenstra, H. W. Lenstra Jr., and L. Lovász. Factoring polynomials with rational

coefficients. *Mathematische Annalen*, 261(4):515–534, 1982. doi:10.1007/BF01457454.

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

[21] Andrzej Trybulec. Function domains and Frænkel operator. *Formalized Mathematics*, 1(**3**):495–500, 1990.

[22] Wojciech A. Trybulec. Non-contiguous substrings and one-to-one finite sequences. *Formalized Mathematics*, 1(**3**):569–573, 1990.

[23] Wojciech A. Trybulec. Pigeon hole principle. *Formalized Mathematics*, 1(**3**):575–579, 1990.

[24] Wojciech A. Trybulec. Linear combinations in vector space. *Formalized Mathematics*, 1(**5**):877–882, 1990.

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

[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.

*Received June 27, 2017*

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